

SK-NET™

Version 2

Installation and Operating Manual

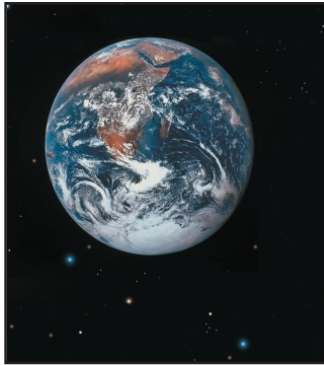
Version Note: This manual covers features available in SK-NET™ Version 2.40. A few features described in this manual are only available with SK-ACP and 28SA-PLUS units that have Firmware Version 2.30 and later. A few additional features require Firmware Version 2.40 and later. SK-NET™ Version 2.40 software will work with older firmware versions, but a few of the most recent features will not be available.

USING THIS MANUAL

The material in this manual has been organized to make SK-NET™ easy to use. We suggest that you read over section 1, the Introduction, to get an overview of the system. Once you have installed your equipment, follow the Quick Start Guide, section 2, to get the system up and running. Refer to sections 3 and 4 for instructions if you want to further customize your system. Section 5, Daily Operations, and section 6, Reports, cover the operations that the end-user of the system will need to perform. Sections 7, 8 and the Appendices provide additional technical information.

COPYRIGHT© 2001
SECURA KEY division of SOUNDCRAFT INC.
PRINTED IN U.S.A.

TABLE OF CONTENTS



1.0 INTRODUCTION	1
What is SK-NET™?	
System Requirements	
Windows® Functions	
Installing SK-NET™	
The SK-NET™ Desktop	
SK-NET™ Explorer	
SK-NET™ Default Reader Groups	
SK-NET™ Time/Date; Time Zones/ Holidays	
Transactions	
User Manager	
2.0 QUICK START GUIDE TO BASIC PROGRAMMING	6
Installation	
Configure the Primary Location	
Enter Reader Names	
Set Latch Timers	
Define Time Zones	
Create Access Groups	
Block Load Cards	
Enter Card Users	
Test Your Programming	
3.0 CUSTOMIZING YOUR SYSTEM	10
Custom System Configuration	
IN and OUT Readers	
Holidays	
Change Default Password	
Set/Change System Password	
Set Network (Reader) Password	
Door Zone	
Inputs and Outputs	
Configure Inputs	
Configure Output	
Change Transaction Colors	
Change Reader Icon	
4.0 ADVANCED SYSTEM CONFIGURATION	15
Edit Time Zones	
Delay Start and Delay End	
Zone Valid Dates	
Antipassback	
Real Antipassback	
Setting Up Real Antipassback	
Timed Antipassback	
Setting Up Times Antipassback	
Limited Use Programming	
Multiple Location Option	
Individual Reader Configuration	
Reader Configuration — Cards Tab	
Reader Configuration — Door Controls Tab	
Reader Configuration — Settings Tab	
Reader Configuration — Configuration Tab	
Reader Configuration — Transactions Tab	
Reader Configuration — Utilities Tab	
Reader Configuration — Service Tab	

Facility Codes	
Bits and Parity	
Setting Reader Group Properties	
Access Groups with Different Time Zones for Individual Readers	
Software Preferences	
User Defined Cardholder Information	
Check Readers	
5.0 DAILY OPERATION	23
Editing Cards	
Adding Cards	
Voiding Cards	
Deleting Cards	
Filter Users	
Opening Doors	
Setting Readers to Inactive (Locked Mode)	
Setting Readers to Unlocked Mode	
Monitoring System Activity	
Filter Transactions	
Forgive (Reset)	
6.0 REPORTS	26
SK-NET™ Reader Report	
Print/Display Card User Reports	
Print Transactions Reports	
7.0 MAINTENANCE	27
System Backup and Restore	
Backup and Restore Individual Readers	
Archiving Transactions	
Database Erase	
8.0 TROUBLESHOOTING	29
COM Ports	
Adding/Replacing A Reader	
APPENDIX - A	A-1
SK-ACP OR 28SA-PLUS TROUBLE SHOOTING GUIDE	
Erratic or No Communication Between Readers and PC	
System Using NET-CONV-P (RS232 to RS485 Converter)	
System Using A Reader Gateway	
APPENDIX - B	B-1
WINDOWS® 95/98 HYPER TERMINAL SETUP	
APPENDIX - C	C-1
CONNECTING A MODEM TO SK-ACP	
APPENDIX - D	D-1
CONNECTING AN SK-ACP OR 28SA-PLUS TO A LOCAL AREA NETWORK	
APPENDIX - E	E-1
PREVENTING LIGHTING DAMAGE	

1.0 INTRODUCTION

1.1 What is SK-NET™?

SK-NET™ is a Windows® (95/NT4.0 or higher) compatible software application program designed to monitor and control a network of up to 128 Secura Key ENTRACOMP® 28SA-Plus Smart Access Control Units, or 100 SK-ACP Two Door Advanced Access Control Panels.

If you are already familiar with other access control programs, you will find that SK-NET™ is different than what you are used to. The user interface follows Microsoft Windows® conventions, rather than a traditional menu structure. SK-NET™ Explorer works similarly to the Windows® Explorer. As in other Windows® applications, right-click menus are used extensively.

The basic version of SK-NET™ allows a single reader network connected to the PC; the Multiple Location Dialup version (SK-NET™-MLD) allows modem communications, TCP/IP and unlimited remote locations.

1.2 System Requirements

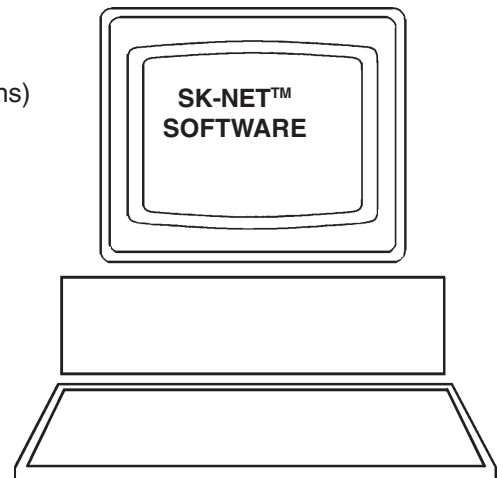
SK-NET™ Minimum PC Requirements

- IBM-compatible, Pentium 200 or comparable processor
- Windows® 95/98/2000 or Windows® NT 4.0 or higher
- 64 MB RAM
- 100 MB Hard disk capacity (more for multiple locations)
- CD-ROM drive
- High speed serial COM port (38.4 K or better)
- VGA Monitor or better
- IBM-compatible parallel printer (for reports)

Recommended System for Large Systems *

- ZIP™ drive or equivalent for system backup
- Windows® 2000
- Pentium 1.06 GHz or comparable processor
- 128 MB RAM
- 500 MB Hard disk capacity

* Larger systems may not run properly at the minimum requirements.



1.3 Windows® Functions

SK-NET™ uses many common functions available in Windows® 95 and later operating systems. For users who are new to Windows® software these are the functions you will need to know to use SK-NET™.

Icons and Tool Bars

Icons are little pictures that represent functions or files in the software. Most of the operations you will perform in SK-NET™ begin by pointing at and clicking on an icon. Most icons in SK-NET™ will display a “prompt”, a word description of the icon, when you point the cursor at it.

Toolbars appear at the top of each screen in SK-NET™. Toolbars contain icons that allow you to perform functions or open files in the program. The topmost toolbar will be comprised of words. Clicking on these words brings “drop-down menus” listing functions that you may select.

Mouse Buttons

When we direct you to “CLICK” on something, we mean that you move your cursor with the mouse to point at that item and then you tap the left button on the mouse once. *This is usually done to select or highlight an item.*

When we tell you to “DOUBLE CLICK”, the only difference is that you tap on the left button twice in rapid succession. *This is usually done to launch a program or to start a function.*

When we tell you to “RIGHT CLICK”, tap on the right mouse button once. *This is used to bring up a menu box that pertains to the item you are pointing at.*

When we tell you to “DRAG-AND-DROP” you first point the cursor at the item, then hold down the left mouse button and, while holding that button down, move the cursor to the location where you want to “drop” the item you are “dragging”. When the item is in the new location, release the left mouse button to “drop” it. *We use drag-and-drop in the Explorer screen to make it easy for you to add individual readers to access groups and hardware groups.*

Explorer

One of the principal screens in SK-NET™ is SK-NET™ EXPLORER. This screen is modeled after the well-known Windows® Explorer. On the left-hand side of the screen you will see all of the elements of your system in a “tree” format. If an item in the tree has a plus (+) or minus (-) symbol next to it, it represents a folder. Clicking on the + symbol “opens” that folder and displays what is inside. For example, the folder called “ALL READERS” contains an icon for every reader in the system. Clicking on the + symbol next to the ALL READERS icon will display icons for each reader, underneath the ALL READERS heading.

On the right-hand side of the screen you will see icons representing whichever part of the Explorer tree you have highlighted. For, example, if you CLICK on ALL READERS the right-hand side of the screen will display one icon for every reader in that location.

Help

SK-NET™ has extensive help, which you can access by clicking on Help on the top menu bar, or by pressing F1. Much of the information in this manual is also included in the on-line Help System.

To learn more about the functions of various icons or “buttons”, click on Help or press F1, select Contents, Getting Started, then SK-NET™ Desktop. Pressing F1 in the main windows (Explorer, Transactions or User Manager) also offers context-specific help for those screens.

1.4 Installing SK-NET™

NOTE: Do not install SK-NET™ onto a network server. SK-NET™ is designed to function on a single PC or network workstation only.

If you are loading SK-NET™ from a CD-ROM, insert the disk in your CD-ROM drive. Click on Windows® START (at the bottom left corner of your desktop).

1. Select RUN. Enter (CD-ROM drive letter):\setup.exe. This will start the installation process.
2. The installation program (or “wizard”) will ask you for a number of responses. Click on the appropriate answer to each prompt.
3. When the installation is complete, drag-and-drop a copy of the SK-NET™ icon to the Windows® desktop. This will make it easy for you to launch SK-NET™ whenever you want to. Double-click on the SK-NET™ icon to launch the program.

If you are installing SK-NET™ from our website (www.securakey.com):

1. Click on DOWNLOADS button.
2. Click on SK-NET™ software.
3. Choose a single file download if the program is going on your hard drive. Choose a three file download if you are going to copy the program from your hard drive onto 3.5” floppy disks.
4. The rest of the procedure is the same as above.

1.5 The SK-NET™ Desktop

SK-NET™ has three main screen displays:

Transactions

User Manager

SK-NET™ Explorer

Select one of the first three icons on the left side of the main toolbar:



Figure 1 - SK-NET™ Toolbar, 3 main icons.

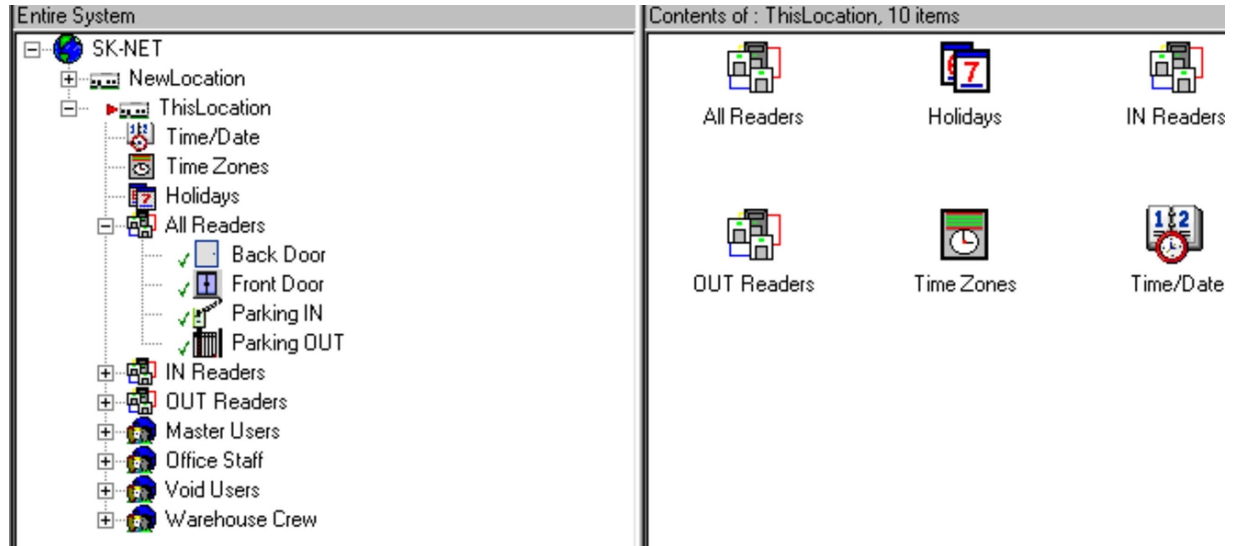
Transactions is the first screen which displays when SK-NET™ is started; it shows any real-time activity for the all Locations.

User Manager is the screen where card user data and access privileges can be entered into the system.

SK-NET™ Explorer is the screen which allows the user to configure the reader network and create or modify access groups and reader groups. This is the first screen you will use to configure your system.

Many other menus or screens are available from the toolbar; these menus pop up over the three primary screens.

1.5.1 SK-NET™ Explorer (Figure 2)



SK-NET™ Explorer shows the current configuration of all Locations, Reader Groups and Access Groups in the system. It allows you to add, delete, configure, or change Locations, groups or readers. When the Explorer screen is displayed, you may use various toolbar buttons to print a reader report, show properties of selected items, delete items, connect to or disconnect from Locations, log in to or logout from readers, control doors for a selected reader group or a reader, or change the configuration display format.

The SK-NET™ Explorer screen is divided into two sections: The left side shows the system configuration in an indented multi-level format (similar to Windows® Explorer). Each location, group, or reader is represented by an icon on screen. The right side of the screen shows individual icons for the currently highlighted location or group.

The highest level in the Explorer configuration window is SK-NET™ (the entire system) which includes all locations, groups, and readers controlled from the PC being used.

The second highest level is Location. A location includes all readers on a single network connected to the PC via a single COM port or a single modem location. Each Location can contain up to 128 28SA-PLUS units or 100 SK-ACP two-door panels.

A red triangle adjacent to the Location icon indicates that you are connected to that Location. Green check marks next to individual reader icons indicate that you are “logged in” to those readers. Being logged in means that transactions stored in the reader have been copied into the software and that you may view transactions as they occur in the Transaction screen.

The third level in the system is Groups. Each Location contains five default Groups: All Readers, IN and OUT Readers, Master Users and Void Users.

Refer to Section 2.5, Create Access Groups, for detailed information about creating additional custom Access Groups for various types of card users at your facility.

Because readers can belong to multiple groups, you will see the same icon appearing several times in the system configuration display.

To expand SK-NET™, a Location, or a Group to the detail level, click on the “+” icon just to the left of the item you want to expand. The “+” icon changes to - when it is expanded. If there is no “+” or - icon next to a Location or Group that indicates that nothing has been assigned to that Location or Group.

1.5.1.1 SK-NET™ Default Reader Groups

These are the group icons which automatically appear when you set up a location:

All Readers - When a Location is first defined, SK-NET™ searches the network for readers and adds them to the All Readers Group. The All Readers Group can then be used to configure all readers at a Location with common parameters. The All Readers Group is also used as a “source” from which to copy readers when creating other Access Groups and Reader Groups.

IN and OUT Reader Groups - These special purpose reader groups are used to set up Antipassback. Readers can be quickly defined as Real Antipassback IN or OUT readers by dragging and dropping to one of these groups.

Master Users and Void Users - These Access Groups are pre-configured to allow rapid Card User Database configuration. The Master Users Group contains all readers in the Location, and is assigned Time Zone 1, which gives users 24 Hour / 7 Day unrestricted access, exempt from Antipassback and Limited Use. The Void Users Group contains all readers in the Location and is assigned Time Zone 0, which gives users no access at any time.

1.5.1.2 SK-NET™ Time/Date; Time Zones; Holidays

Under each Location, there are icons for Time/Date; Time Zones and Holidays.

Double Click on Time/Date to change the time or date in the system. *NOTE: The time and date is automatically set to match the computer time and date when you are connected locally. If you are connected via modem you must set the appropriate date and time for the system manually.*

Double click on Time Zones to edit the time zones for the selected location.

Double click on Holidays to edit the holidays for the selected location.

1.5.2 Transactions (Figure 3)

Time	Date	Card #	User Name	Transaction Type	Reader ID/Location
12:23	11/6/2001	4	Gordon Morris	Valid Entry	parking in/ This Location
12:23	11/6/2001	34	Jeaneth Hernandez	Valid Access	Prox Reader/ This Location
12:23	11/6/2001	4	Gordon Morris	Valid Exit	parking out/ This Location
12:23	11/6/2001			Door Unlocked via Door Zone	parking in/ This Location
12:23	11/6/2001	620	Paul Chandler	Valid Access	Keypad/ This Location
12:23	11/6/2001	4	Gordon Morris	Antipassback Violation	parking in/ This Location
12:24	11/6/2001			Reader Active - Door Zone Off	parking in/ This Location
12:35	11/6/2001	151	Ken Cecil	Valid Access	Keypad/ This Location
12:35	11/6/2001	620	Paul Chandler	Valid Access	Keypad/ This Location
12:35	11/6/2001	533		Void Card	Keypad/ This Location
12:35	11/6/2001	789		Void Card	Keypad/ This Location
12:35	11/6/2001	9	Vicki Mills	Valid Access	Keypad/ This Location
16:12	11/6/2001			Door locked	Front Door/ This Location
16:12	11/6/2001	2	Martin Casden	Valid Special Use	Front Door/ This Location
16:12	11/6/2001			door unlocked	Front Door/ This Location
16:12	11/6/2001	2	Martin Casden	Valid Special Use	Front Door/ This Location
16:12	11/6/2001			Door locked	Front Door/ This Location

The Transaction Window shows the latest system events as they occur, for the Location which is currently connected to SK-NET™.

System events include card usage, input point status changes, reader status changes, and system messages. Each event is displayed on a single line, and includes the time and date of the event, card number (for card transactions), User Name (if the name is stored in the database), Transaction Type (what happened), and

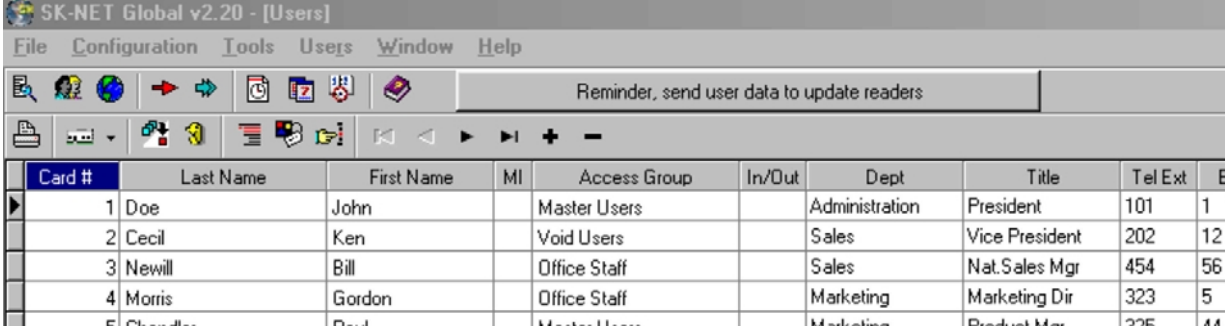
Reader ID/Location (name of the reader and the Location to which the reader is connected).

The Transaction Window allows you to view the entire Transaction Database, by using the navigation buttons or the scroll bar to browse through the transaction records.

Transaction Database options include Print Transaction Reports, Erase, Change Colors, and Zoom In.

The Transaction Window normally shows data for all Locations (when filtering is not applied). Whenever SK-NET™ connects to a Location, all new transactions stored at the readers are automatically uploaded.

1.5.3 User Manager (Figure 4)



The screenshot shows the SK-NET Global v2.20 - [Users] window. The menu bar includes File, Configuration, Tools, Users, Window, and Help. The toolbar contains various icons for file operations, navigation, and user management. A status bar at the top right displays the message: "Reminder, send user data to update readers". Below the toolbar is a table with the following columns: Card #, Last Name, First Name, MI, Access Group, In/Out, Dept, Title, Tel Ext, and E. The table contains the following data:

Card #	Last Name	First Name	MI	Access Group	In/Out	Dept	Title	Tel Ext	E
1	Doe	John		Master Users		Administration	President	101	1
2	Cecil	Ken		Void Users		Sales	Vice President	202	12
3	Newill	Bill		Office Staff		Sales	Nat. Sales Mgr	454	56
4	Morris	Gordon		Office Staff		Marketing	Marketing Dir	323	5
5	Chandler	Paul		Master Users		Marketing	Product Mgr	225	44

The User Manager Window allows you to display or change the Card User Database. You can add new card users or edit current user records. You may use the scroll bar or navigation buttons to view the entire Card User Database. You can also print user reports, search for an individual user, or optionally, select user databases for multiple locations.

The User Manager window defaults to a List format, one line per record. If you click on Zoom, the User Detail Screen is displayed for the currently selected user. You can also select a user from the list and double-click to display the record in User Detail format. Editing or adding cards is done by displaying the User Detail screen. The Navigation buttons work in either List or User Detail format.

To add a card user to the system, click on the "+" icon. To edit an existing card record, select that record, then click on the Edit button. To save a new or modified card user record, click on Save.

To send database changes to the readers at the connected Location click on Send. You can send records one at a time, or you can make changes to many records, and click Send when you are done; this will send all changes to all connected readers.

If your system has the Multiple Location Dialup Option (and if any cards belong to multiple locations) you must send data to each Location separately. You can use the Location drop-down box on the Card User Database tool bar to select each Location. SK-NET™ will prompt you to log on to each location. Remember to click Send when you have completed your User Database changes.

Only the card number and Time Zone number (derived from the Access Group) are sent to the reader. The User Name and other information is stored at the PC.

Voiding a user allows you to cancel a cardholder's access privileges from the system without removing that person's detailed information from the User Database. It also enables the Transaction Report to display that user's name if the voided card is subsequently used to make an unauthorized access attempt.

Sorting the User Database - Click once on the Card Number, Last Name, or Access Group column headings to sort the User Database by the content of the selected field.

Finding Card Data - The Find button will search according to the order in which the database is currently sorted. To find a record by last name, display the User Manager in List format, click on the Last Name column heading to sort the data by last name, then click Find and enter the last name into the search field. The cursor will move to the first record where a match is found.

2.0 QUICK START GUIDE

SK-ACP Advanced Control Panel with SK-NET™ Software

2.1 Installation

2.1.1 Make a Site Plan

For multi-reader systems you should begin by making a simple diagram of the job site, noting the location of each reader and panel. List the serial number of each SK-ACP. The reader connected to the right side will be serial number + “-1” and the reader connected to the left side will be serial number + “-2”.

2.1.2 Install Panels and Readers

Install all readers and panels as per instructions provided, being sure to use the correct types of wire. Do not apply power until all connections are made.

2.1.3 Power Up

After all connections are made apply power to the panels. The LEDs on the readers will flash alternately Green and Red. Hold a card with the correct facility code near each reader to set the facility code in the panel.

2.1.4 Install Software

Install SK-NET™ on your PC according to instructions in section 1.4.

2.2 Configure the System

2.2.1 Configure the Primary Location (Figure 5)

A Location is a single contiguous network of readers connected to a single PC COM port. *SK-NET™-MLD can support more than one location.*

1. Click on Explorer (globe icon)
2. Right click on “This Location” *Select “Rename”* if you want to change the name of the location. In this manual we will continue to refer to it as “This Location”.
3. Select “Properties”. This brings up a box called “Location: This Location”. Under the “Properties” tab you may enter the address and phone number of the Location, if you desire. You may also uncheck “Auto Login” if you do not want to download transactions every time you connect to the system.
4. Click on the “Connection” tab. The system must be connected to a PC in one of four ways. For each possibility, follow the appropriate directions:
 - a. Gateway RS-232. (You have made a direct connection from a COM port on the PC to a gateway reader or panel.)
 1. Be sure the “Gateway(RS232)” box is checked.
 2. Click on the “Connection Wizard”
 3. Click on “YES”. Connection Wizard will try every COM port at every baud rate until the system is located.
 4. When asked to accept the settings, click on “YES”.
 5. Click on “Connect”
 - b. Using the NET-CONV. (An RS-232 to RS-485 converter has been plugged into a COM port on your PC and connected to the system with two, twisted-pair, shielded cable.)
 1. Uncheck “Gateway(RS232)”. (Baud rate should change to 38,400)
 2. In the box labeled “Connect Using” select the COM port number where the NET-CONV has been installed.
 3. Click on “Connect”.



(Figure 5)

- c. Dial-up modems. (An external modem has been connected to the gateway reader or panel at the Location and you have installed SK-NET-MLD version in your PC.)
 1. Uncheck the box labeled “Local Connect”.
 2. In the box labeled “Connect Using” select the COM port where your modem is located. (If you do not know which COM port this is, exit SK-NET, and from your desktop go to “My Computer” go to “Control Panel” and go to “Modems”.)
 3. Enter the phone number of the modem at the remote Location.
 4. Click on “Connect”.
- d. LAN or TCP/IP. The gateway panel has been connected to an external device server and you have installed SK-NET-MLD version in your PC. The external device server has had an IP address set (see Addendum D).
 1. In the box labeled “Connect Using” select “LAN/Internet (TCP/IP)”.
 2. Enter the Host IP Address (the address set in the external device server)
 3. Enter the Host Port number (the port number set in the external device server).
 4. Click on “Connect”.
5. When you get the message “There are no readers in This Location, scan for new readers now?” Click on “YES”.
6. When you see the question “Are there more than 20 readers in this location?” choose “YES” or “NO”.
7. A box should appear showing the correct number of readers and listing their serial numbers. Click on “OK”
8. When you see the question, “Do you wish to login all readers at this time?” click on “YES”, then click on “OK”.
9. Click on “Close” to close the “Location: This Location” box.

2.2.2 Enter Reader Names

1. There should now be a “+” symbol next to ALL READERS. Click on the “+” symbol to display readers found. Note that each reader name will be the same as the serial number. Right click on any reader and select “Rename”. Replace the serial number with the name you have chosen for that reader and click “OK”. Repeat for each reader.

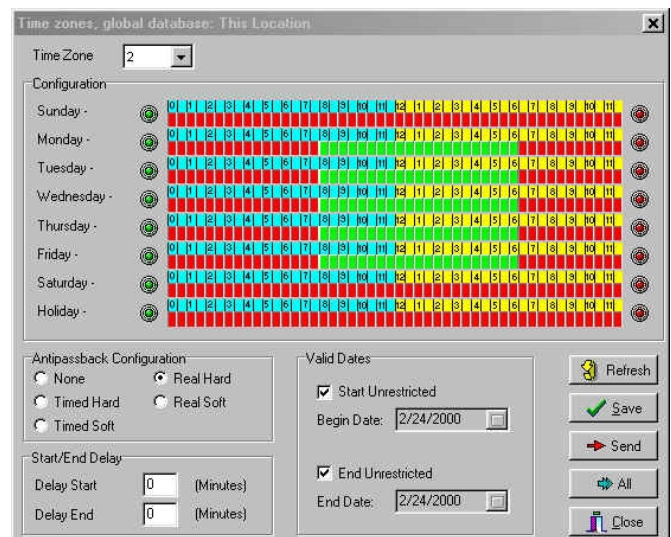
2.2.3 Set Latch Timers

1. Right click on “All Readers”.
2. Select Properties.
3. Click on “Configuration”.
4. Change latch timer to appropriate time.
5. Click on “Send” Then Click on “Close” *This sets all readers to the same latch time. If you want a different latch time on a specific reader see section 4.4 of the SK-NET™ manual.*

2.2.4 Define Time Zones (Figure 6)

There are 16 Time Zones in this system. Time Zone 0 is always void and Time Zone 1 is always valid. These may not be edited. You may edit Time Zones 2-15 to meet your specific needs. Time Zones may be unique in every reader but it is usually better to set them for the entire location. To set Time Zones globally:

1. Double click on “Time Zones” under This Location.
2. Select the time zone you wish to edit (2-15). *Each time zone is predefined and you may find one that already meets your needs by browsing through them all. If not, you will need to edit a time zone.*



(Figure 6)

3. Each Time Zone has seven daily schedules and a special holiday schedule. Each green block represents a half-hour time increment when cards in this time zone will work and each red block represents a period when they will not work. You may turn an entire day green or red by clicking on the buttons at either side of the row. You may turn any single block to another color by clicking on it. You may turn a group of blocks in a single day from red to green by holding down the “CONTROL” key, clicking on the first block and then clicking on the last block of the group. *As you point at a block you will see a prompt describing exactly what that half-hour increment represents.*
4. Other settings in each Time Zone allow delayed start and end, antipassback and date restrictions. If you need these features see section 3.7 of the SK-NET™ manual for more details.
5. After you edit each Time Zone, click on “Save”. After you have edited all the Time Zones that you need, click on the double green arrow key to send all time zones to all readers.
6. Click on “Close”.

2.2.5 Create Access Groups (Figure 7)

An Access Group is used to give a group of cardholders access to a specified list of readers during a specified Time Zone. You may create as many Access Groups as you wish.

1. Right click on “This Location”.
2. Select “New”, then click on “Access Group”.
3. Type in the name of the Access Group and the time zone that should apply. Click “OK”.
4. The new group should appear in the left part of the screen under the location. There will not be a “+” symbol next to this Access Group yet.
5. Click on “ALL READERS”. On the right-hand side of the screen icons should appear representing every reader in the location. Drag-and Drop the readers you want from the right side of the screen into the new Access Group. You may place one or more readers in the group. *After you drop the first reader into the group you will notice a “+” symbol appears next to the group name. Click on the “+” symbol to see which readers are in that group.*
6. SHORTCUT: If the new access group is going to have all of the readers assigned to it you do not have to drag-and-drop each icon:
 - a. Right Click on access group name
 - b. Select “Properties”
 - c. Select “Readers” tab
 - d. Click on “Add All”
 - e. Click on “Send”
 - f. Click on “Close”

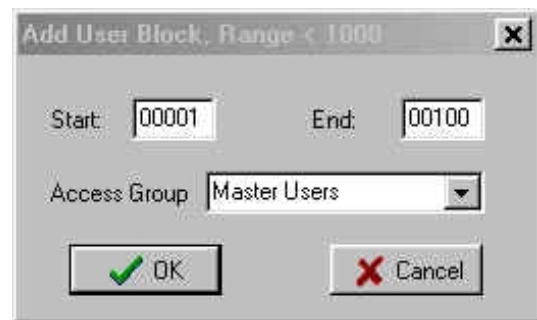


(Figure 7)

2.2.6 Block Load Cards (Figure 8)

In most new installations you will start with a block of cards. You may load all of these cards quickly and easily into the system and then assign them to users individually later.

1. Click on the User Manager Icon (2 faces).
2. Click on “Users” in the top toolbar.
3. Select “Add User Block”.
4. Enter the lowest card number and the highest card number you want to add.



(Figure 8)

5. Select an Access Group. *Placing the block in “Void Users” is safest because lost or stolen cards will not open any doors. Cards can be changed to the appropriate Access Group later when they are assigned to specific users.*
6. Click “OK” and “OK” again. Then click on the double green arrows on the toolbar to send all cards to all readers. **Any changes you make in the software are meaningless until you send them to the readers.**

2.2.7 Enter Card Users (Figure 9)

1. Click on the User Manager Icon (2 faces).
2. Double click on the first card number you wish to assign.
3. Enter the cardholder’s first name, last name and middle initial. Tab past the card number and select an appropriate Access Group for this cardholder. The remaining fields are optional. See Section 3.8 for instructions for attaching a photograph to the user record. Click on “OK”.
4. Double click on the next card number you wish to assign and repeat the process.
5. Click on the red arrow icon in the toolbar to send all of your card changes to the readers.
6. The installer may wish to activate a single *card in his own name and assign it to the Master User group so he can go out and test all of the readers at this time.*

(Figure 9)

2.2.8 Test Your Programming

1. Take a Master User card to each reader and try it. You should get a long green LED and the latch relay should activate.
2. Click on Transactions (magnifying glass icon). Each card presentation should appear in Transactions with accurate time and date.

This Quick Start Guide describes basic programming of a system. Your system should now be up and running. Refer to Sections 3 and 4 of the SK-NET™ manual to learn how to activate additional features. Section 5 of the SK-NET™ manual provides the basic day-to-day operating instructions that the end-user will need to know.

3.0 Custom System Configuration

SK-NET™ has many features which are not covered in the basic programming described in section 2 (Quick Start Guide). Some of these custom features are fairly popular while others are needed for just a few special applications. Section 3 covers the most common system configuration topics. Section 4 deals with the most specialized configuration issues.

3.1 IN and OUT readers.

The “IN READERS” and “OUT READERS” Reader Groups are automatically created for each Location. You may want to designate some readers as “In” and some as “Out” so you can monitor user status and/or for real antipassback.

1. Click on Explorer (globe icon).
2. Click on “All Readers”.
3. Drag-and-Drop readers from the right side of the screen into the “IN READERS” and the “OUT READERS” groups on the left side of the screen as required. *After you drop one reader in either group you will notice a “+” symbol next to that group. Click on the “+” symbol to see which readers are in each group.*

3.2 Holidays

Any day designated as a Holiday will follow the Holiday schedule in each Time Zone rather than the day-of-the-week schedule.

1. Click on Explorer (globe icon).
2. Double click on Holidays under the desired Location.
3. Click on “+”.
4. Enter the Holiday date. *You may type in the date or click on the calendar icon and locate the date wanted on a calendar, then click on that date.*
5. Type in the description.
6. Check “Yearly” for Holidays that occur on the same calendar date each year.
7. Click on “OK”.
8. Repeat for each Holiday.
9. If the system is located in a state or country that does not follow the U.S. schedule for daylight savings time, uncheck the “Daylight Savings Time” box.
10. Click on “SEND”. Click on “OK”. Click on “CLOSE”.

3.3 Change Default Password

Once your system is operational, you should change the passwords to prevent unauthorized personnel from making changes to the system or viewing sensitive information. The SK-NET™ system has two passwords: the system password and the reader/location password.

3.3.1 Set/Change System Password

This password appears when the user logs on to SK-NET™, and is used to prevent unauthorized use of the SK-NET™ software. When the software is first installed, no password is required. Although the software can be left without a password; it is recommended that you select one.

Note that passwords are case sensitive. Be cautious about using the Shift or Caps Lock Key when entering passwords. “Secret” is not the same password as “SECRET.”

1. Select File on top menu bar.
2. Select System Password.
3. If system is new, press Tab key to bypass Current Password. If changing the password, type the current password and press Tab.
4. Enter New Password and press Tab. Characters, numbers or symbols may be used. Up to a line of text may be entered.
5. Enter New Password again and Click OK.

The next time SK-NET™ is started, you will be prompted to enter the new Password, and click OK.

3.3.2 Set Network (Reader) Password

The Network/Location Password is used by the system software to communicate with readers connected to the communications network. This prevents substitution of another reader without authorization. With multi-location software, a different password can be set for each location.

Note that passwords are case sensitive. Be cautious about using the Shift or Caps Lock Key when entering passwords. (“Secret” is not the same password as “SECRET”).

To set the Network Password:

1. Click on the SK-NET™ Explorer (the globe icon).
2. Right click on a selected location. Select the properties menu.
3. Click on the key icon.
4. Enter New Password and press Tab. Characters, numbers or symbols can be used. Maximum length is 15 characters.
5. Enter New Password again and Click Save.
6. Click Close to close the location window.

3.4 Door Zone

A door zone is a schedule for locking and unlocking a door. You can set a door zone that will apply to all of the doors in your system in the same way that you set Time Zones (section 2.2.4) Usually door zones are specific to a particular door. To set a door zone for a single door:

1. Click on Explorer (globe icon).
2. Right click on a selected reader.
3. Click on Properties. This brings up a box with several tabs. The first tab displayed is always “Settings”.
4. Click on “Zones”. Use the selection arrow to find the Zone called “Door”.
5. Any time segment that is green in the Door Zone represents a time when the door will be unlocked. Time segments in red are periods when a valid card is required for access. Change to green the segments representing the half-hour time periods when you want this door to remain unlocked.
6. If you want the door to unlock and/or lock at a time other than on the half-hour you may set a Delay Start and/or a Delay End time of up to 29 minutes.
7. You may make the Door Zone “Automatic”, which means that it will unlock at the selected time, no matter what, or you can make the Door Zone “Card Activate” which means that when the selected unlock time comes the door remains locked until the next valid card is presented (sometimes called “first man in”).
8. After setting the Door Zone click on “Send”.
9. Click on “Close”, then click on “YES”.

3.5 Inputs and Outputs

3.5.1 Configure Inputs

The 28SA-PLUS has 3 programmable inputs and the SK-ACP has 2 programmable inputs. If you have connected circuits or switches to these Inputs you must define how these are to be used here.

1. Click on Explorer (globe icon).
2. Right click on a selected reader.
3. Click on Properties.
4. Click on “Configuration” tab.
5. Click on “Edit”.
6. Click on “Change” next to one of the inputs. You will have the following menu:
 - A. Disabled – The Input is off.
 - B. Tamper – If this input is closed the reader will be disabled and a Tamper message will be logged.

- C. Arming Circuit – The reader will operate only when the input is closed; a card presented when the input is open is logged but access is denied. This input is usually connected to a vehicle presence sensor (loop). It may also be connected to the relay output of a digital keypad so that a PIN and a card are required for access.
- D. Door Monitor – Connected to a door contact switch, this input will activate the anti-tailgate feature. This input should be connected to a normally closed switch (unless a jumper is removed from the panel to enable normally open switches).
- E. Door Bell – Sends an ASCII Bell character to PC/Printer, causing a beep.
- F. Remote Inactive – If this input is closed the reader is disabled. Often connected to a keyswitch.
- G. Remote Open – If this input is closed the latch relay is activated just as it would be for a valid card; a remote open message is logged.
- H. User Defined – This input may be a Remote Open or just a Doorbell. Type in the message you want to log. The User Defined input may also be used as an alarm reset for the auxiliary relay output in the SK-ACP.

3.5.2 Configure Output

The SK-ACP has a DPDT auxiliary relay output. Repeat steps I-V above and then click on “Change” next to the Output and you will see this menu:

- A. Disabled – The Output is turned off.
- B. Input 1 Follow/Latch – Whenever Input 1 is activated the auxiliary relay will be activated until:
 - A valid card is presented, or
 - A User Defined Input 2 is activated, or
 - A user-selected amount of time is elapsed, or
 - Input 1 is restored to normal.
- B. Input 2 Follow/Latch – Whenever Input 2 is activated the auxiliary relay will be activated until:
 - A valid card is presented, or
 - A User Defined Input 1 is activated, or
 - A user-selected amount of time is elapsed, or
 - Input 2 is restored to normal.
- C. Door Monitor Alarm – If an Input is designated as “Door Monitor” and the Output is designated as “Door Monitor Alarm” you must set an expiration time after which a door is considered held open too long. Then, if the Input is activated without being preceded by a valid card or “Remote Open” Input the Output will be activated. If a valid card or “Remote Open” Input is provided, but the “Door Monitor” Input is not restored before the end of the expiration time, the Output will activate. If the Output activates for either condition it will remain activated until:
 - A valid card is presented, or
 - A user-defined Input is activated, or
 - A user-selected amount of time is elapsed.
- E. Door Forced Alarm – If an Input is designated as “Door Monitor” and the Output is designated as “Door Forced Alarm” the Output will be activated whenever the Input is activated without being preceded by a valid card or “Remote Open” input. The Output will remain activated until:
 - A valid card is presented, or
 - A user-defined Input is activated, or
 - A user-selected amount of time is elapsed.
- F. Door Held Open – If an Input is designated as “Door Monitor” and the Output is designated as “Door Held Open” you must set an expiration time after which a door is considered held open too long. Then, if the Input is activated after a valid card or “Remote Open” input and the Input is not restored before the end of the expiration time, the Output will be activated until:
 - A valid card is presented, or
 - A user-defined input is activated, or
 - A user-selected amount of time is elapsed.

- G. Emergency Exit Alarm – If an Input is designated “Remote Open” and the Output is designated “Emergency Exit Alarm” activating the Input will unlock the door and also activate the Output until:
 - A valid card is presented, or
 - A user-defined input is activated, or
 - A user-selected amount of time is elapsed.
- H. Card Range – When “Card Range” is selected for the Output you must enter the lowest and highest card numbers that will activate the Output. You must also designate whether the Main Relay should activate when the selected range of cards are presented. If you select “Card Mode Toggle” the Output will remain activated until another card from the selected range is presented. If you select “Card Mode Timed” you must enter the amount of time the Output should be activated after the card is presented.
- I. Error Alarm – When any one of the selected “Error” conditions occur the auxiliary Output will activate and remain activated until a valid card is presented. Options include:
 - Door Forced; Door Held; Tamper Input; Void User; Invalid FAC; Antipassback Violation; Arming; Tamper Card; Inactive; Invalid ID; Time Zone Error; Time Zone Date; Limited Use Violation.
- J. Serious Alarm – When any of the following “Error” conditions occur the auxiliary Output will be activated and remain activated until a valid card is presented. Conditions include:
 - Void Card; Invalid Facility Code; Tamper; Door Forced; Door Held Open.
- K. Time Zone – The auxiliary Output will activate during the “green” segments of any time zone or door zone selected.
- L. Tamper Alarm – If a “Tamper” input is activated the auxiliary Output will be activated until:
 - A valid card is presented, or
 - A user-defined input is activated, or
 - A user-selected amount of time is elapsed.
- M. Door Bell – If a “Door Bell” Input is activated the auxiliary Output will be activated until:
 - The Input is restored to normal, or
 - A user-selected amount of time has elapsed.
- N. Alarm Shunt – Whenever the main relay is activated (by a valid card or a “Remote Open” Input) the auxiliary Output will be activated and will remain activated until:
 - The main relay returns to normal, or
 - A user-selected amount of time has elapsed.

3.6 Change Transaction Colors.

Transactions are divided into “Valid Use Events”, “Invalid Use Events” and “System Events”. Each category of transaction may appear in a different color. To change these colors:

1. Click on the word “Configuration” in the top tool bar.
2. Click on “Preferences”.
3. Click on the “Transaction Colors” tab.
4. Click on “Change” next to the color you want to change.
5. Select a color from the pallet. Click on “OK”.
6. After changing any colors you wish, click on “OK”.

3.7 Change Reader Icon

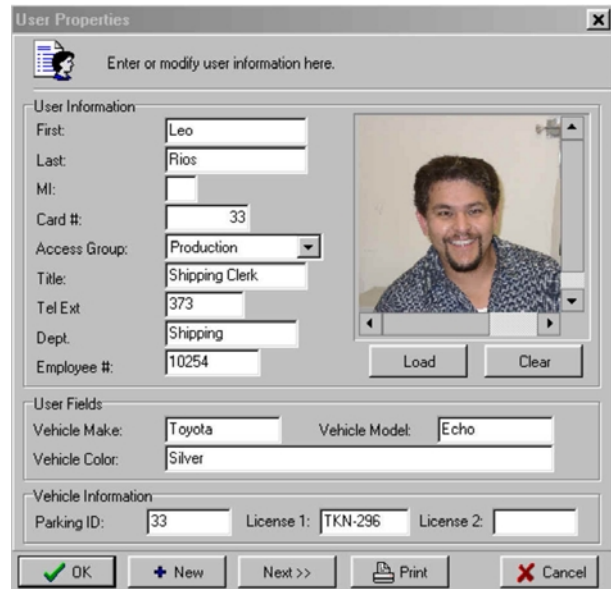
SK-NET™ contains a variety of descriptive icons which may be used to represent the different readers in your system. To change the icon for a reader:

1. Click on Explorer (globe icon).
2. Right click on the desired reader.
3. Click on “Change Icon”.
4. Click on the icon you wish to select. Click “OK”.

3.8 Attach Photograph to User Record (Figure 10)

You can import a photograph in .jpg format and attach it to the User Record.

1. Click on User Master Icon (Two Faces).
2. Double click on the user name.
3. Click on “LOAD”.
4. Locate your .jpg file.
5. Click on “Open”.
6. Click on “OK”.



The screenshot shows the 'User Properties' dialog box with the following fields and values:

User Information	
First:	Leo
Last:	Rios
MI:	
Card #:	33
Access Group:	Production
Title:	Shipping Clerk
Tel Ext:	373
Dept:	Shipping
Employee #:	10254

Below the user information is a photograph of a man with a goatee and a patterned shirt. To the right of the photo are 'Load' and 'Clear' buttons.

User Fields	
Vehicle Make:	Toyota
Vehicle Model:	Echo
Vehicle Color:	Silver

Vehicle Information					
Parking ID:	33	License 1:	TKN-296	License 2:	

At the bottom of the dialog box are the following buttons: OK, + New, Next >>, Print, and Cancel.

4.0 ADVANCED SYSTEM CONFIGURATION

The following sections describe a number of configuration options which address specific programming needs.

4.1 Edit Time Zones

In section 2.2.4 we explained how to set Time Zones 2 through 15 so that cards are valid or invalid at various times of day and days of the week. There are three additional features we can activate in the Time Zone menu.

4.1.1 Delay Start and Delay End

If you do not want a time zone to begin or end on the half-hour, you may set a delay start and/or a delay end time of up to 29 minutes. This will effect the start and/or end of every “card valid” period.

1. Double click on Time Zones.
2. Select the Time Zone (2-15) you want to edit.
3. Enter a “Delay Start” period and/or a “Delay End” period (1-29 minutes.)
4. Click on “Save”. Click on “OK”. Click on “Send”. Click on “OK”. Click on “Close”.

4.1.2 Zone Valid Dates

This field allows you to associate a beginning and ending date with a time zone. This is useful for granting temporary access to a group of cardholders.

1. Double click on Time Zones.
2. Select the Time Zone (2-15) you want to edit.
3. Uncheck “Start Unrestricted” and/or “End Unrestricted”.
4. Enter the starting and/or ending dates. *You can either type in the desired dates or click on the calendar icon, locate the date on a calendar display and click on it.*
5. Click on “Save”. Click on “OK”. Click on “Send”. Click on “OK”. Click on “Close”.

4.1.3 Antipassback

Passback is a common form of access control system abuse, particularly in parking applications. The authorized cardholder uses his card to enter a gate or turnstile, then passes the card back to an unauthorized person who re-uses the card to enter the facility. The Antipassback feature helps to prevent card passback by temporarily voiding the card once it is used to enter.

Antipassback parameters are set in two menus: the Time Zone menu and the Reader Configuration menu. To set up Antipassback, you must decide:

1. Type of Antipassback: Timed or Real
2. If Antipassback will be Hard (deny access) or Soft (report violation only)
3. Which Access Groups (card holders) will be subject to Antipassback
4. Which Readers will be subject to Antipassback
5. If Real Antipassback, which readers are In and which are Out

4.1.3.1 Real Antipassback

Real Antipassback prevents unauthorized card reuse by changing the card’s antipassback status so that it cannot be used to enter an area twice in a row, unless it has exited that area first.

This requires that during system configuration, certain readers are designated as IN and other readers are designated as OUT. Every reader keeps a status table with the current IN / OUT status of every cardholder in the system. A card’s status changes from OUT to IN when used in an IN reader, and changes from IN to OUT when used in an OUT reader. If a card’s status is the same as the reader type, it will be denied access until changed by use in a reader of the opposite type.

Readers can also be defined with no antipassback type, at locations where IN/OUT status checking is not desired. Real Antipassback requires a networked reader at each entrance and exit.

4.1.3.2 Setting Up Real Antipassback

Real Antipassback operation is defined in the Time Zone Configuration Screen. To apply Real Antipassback to card users, you must define Antipassback in the Time Zones used to create their Access Groups. Note that Time Zone 1 is not affected by Antipassback, so don't assign a card holder with Antipassback to an Access Group using Time Zone 1.

If Antipassback-exempt card users require the same access schedule as those who are subject to Antipassback, you may have to create additional Time Zones and Access Groups that are identical except for their Antipassback definitions.

1. Identify the Access Groups to be affected by Real Antipassback, and determine which Time Zones are used to create those Access Groups.

2. Select the desired Real Antipassback option for the appropriate Time Zones. Choose from:

Real Hard — Cards must be used alternately at IN, then OUT readers or be denied access.

Real Soft — similar to Real Hard, except that access is granted – if card is used twice in succession at an IN reader or OUT reader, an exception is logged for administrative use.

None — Antipassback is disabled for this Time Zone.

Click on the appropriate radio button, click on Save, then Send.

3. Add Readers to IN/OUT Reader Groups. Click on SK-NET™ Explorer, select the desired Location, then click the “+” button to expand the All Readers Group.

To designate a reader as Antipassback IN, simply “copy” it from the All Readers group by clicking on the reader icon and dragging it into the IN Readers Group. To designate a reader as Antipassback OUT, “copy” it from the All Readers group by clicking on the reader icon and dragging it into the OUT Readers Group.

4. If you are using Remote Readers for Antipassback or if you need to set a Daily Antipassback Forgive time, you must use the Reader Configuration Screen. To configure all readers at one Location alike, right click on the All Readers, select Properties and select Configuration. (NOTE: After you make changes to the Global Reader Configuration, verify that all information of this screen is correct. When you click on Send all these settings will be sent to all the readers.) To configure a single reader, click on SK-NET™ Explorer, then double-click on the desired reader icon. Select the Configuration tab, Click on Edit, make the desired settings and Send.

Remote Reader Type — This allows you to set the Antipassback type for a remote reader connected to a 28SA-Plus. Set type to IN, OUT or NONE, click on Send, then Close.

Daily RAPB Forgive Time — This can be set to any hour, 0 - 23 (Military Time). This automatically resets all cards that are subject to Real Antipassback to Neutral IN/OUT status. Once “forgiven,” cards will be granted access regardless of their previous status. It is recommended to set Forgive Time via Global Reader Configuration or to set all affected readers alike. To set, click the ON button, enter the time, click Send, then Close.

4.1.3.3 Timed Antipassback

Timed Antipassback prevents card reuse by temporarily voiding the card when it is first used at the reader, until a pre-defined time period expires. Timed Antipassback is recommended when the area to be controlled has only one entrance, or if it is not possible to have networked readers at every entrance and exit. The disadvantage of Timed Antipassback is that in a multi-reader facility, the unauthorized person can circumvent antipassback by simply seeking access at another entry.

The Antipassback Time Period applies only at a specific reader and any connected remote reader; the time period is not broadcast to other readers on the network.

4.1.3.4 Setting Up Timed Antipassback

Timed Antipassback operation is defined in the Time Zone Configuration Screen. To apply Timed Antipassback to

card users, you must define Antipassback in the Time Zones used to create their Access Groups. Note that Time Zone 1 is not affected by Antipassback, so don't assign a card holder with Antipassback to an Access Group using Time Zone 1.

If Antipassback-exempt card users require the same access schedule as those who are subject to Antipassback, you may have to create additional Time Zones and Access Groups that are identical except for their Antipassback definitions.

1. Identify the Access Groups to be affected by Timed Antipassback, and determine which Time Zones are used to create those Access Groups.
2. Select the desired Timed Antipassback option for the appropriate Time Zones. Choose from:
 - Timed Hard — Cards used in reader must wait for programmed antipassback time (1-30 minutes) or access will be denied.
 - Timed Soft — similar to Timed Hard except access is granted — if card is reused before antipassback time expires, an exception is logged for administrative use
 - None — Antipassback is disabled for this Time Zone.

Click on the desired radio button, click on Save, then Send.

3. Set Antipassback Time - To set all readers at one Location alike, click on the Global Reader Configuration icon; to configure individual readers, click on SK-NET™ Explorer, and double-click on the desired reader icon. Select the Configuration tab, click on Edit, then set the Timed Antipassback time period from 1 - 30 minutes.
4. Click on Send, then Close.

4.2 Limited Use Programming

Limited Use Programming allows you to assign a specific number of card uses, days, or weeks of usage to one or more cards. Every time the card is used (or a unit of time passes) the card user's stored count is decreased by one, until no counts are left, at which time the card user's is denied access until the user's card is "recharged" with more uses.

When the Limited Use feature is set to Count, it only counts usage and does not restrict access.

Limited Use status is communicated to all readers on the network, meaning that when a card's Limited Use count is decreased at one reader, it is decreased at all readers. Limited Use works only at a single Location; limited use card status is not broadcast to multiple locations.

For correct operation, Limited Use programming for multiple readers should be done by using Global Reader Configuration, or by configuring properties for a reader group. If individual reader configuration is used and some readers are set up differently than others, Limited Use operation will be unpredictable.

If using the Multiple Location Option, first connect to the desired Location.

1. To configure all readers at one Location alike, right click on the All Readers, select Properties and select Configuration. (NOTE: After you make changes to the Global Reader Configuration, verify that all information of this screen is correct. When you click on Send all these settings will be sent to all the readers.)
2. Set Start and End card numbers for Limited Use Card Range. This must be a contiguous block of no more than 4000 numbers, with the highest number being 65,535.
3. Click Send.
4. Click the Cards tab.
5. Select Limited Use count type (days, uses, days after first use, counter, weeks or none). Click the appropriate radio button
6. Select starting and ending card numbers (no more than 4000 total in a contiguous block).
7. Value - enter the number of units with which each card will start (default is 500). Click Send, then Close.

4.3 Multiple Location Option

A Location is a single network of up to 128 of the 28SA-PLUS units or 100 of the SK-ACP panels, connected to the PC via a single PC COM Port, or via modem at a remote location with a single phone number. Basic SK-NET™ software allows one “hard-wired” location; the Multiple Location Software Option allows both modem communications and unlimited remote locations.

If you have already installed SK-NET™ Basic software and later decide that you need the Multiple Location Software, Secura Key can provide a serial number which can be used to upgrade your program. (There is a charge for the upgrade.) Once you have been issued a serial number for your software click on Help. Select Update System. Click on Global. Enter the serial number. Click on OK.

To create an additional local location (hard-wired to the PC) connect a network of readers to an additional PC COM Port.

To create a remote location, connect a network of readers to a modem. A modem will also be required back at the PC; both modems must be PC compatible and connected to standard dialup telephone lines.

To create a new Location in the software:

1. Click on SK-NET™ Explorer.
2. Right-click on the SK-NET™ icon, select New, then Location.
3. Enter a Location name, then click OK. The Location Configuration window then appears.
4. Configure the location for the correct COM port (and modem phone number, if applicable) using the same steps described earlier in section 2.2.1.
5. Then add new readers, as described in sections 2.21.

4.3.1 Special Considerations for Multiple Locations

If your system has the Multiple Location / Dialup Option, you should be aware of the following when sending commands or making any database or configuration changes:

1. To send parameters to any Location, or to open doors, you must be **connected** to that location.
2. Once you have set up Global Time Zones or Global Reader Configuration, you must connect to each location and send them.
3. The Transaction Database includes all locations, and is immediately updated whenever you connect to a remote location. To keep remote location activity up to date, you should connect to each location on a regular basis. Keep in mind that each 28SA-Plus Unit stores a maximum of 5000 transactions and each SK-ACP stores a maximum of 4864 transactions, so if your remote site is very busy and you fail to connect frequently, transaction history may be lost.
4. The Card User Database is unique for each location. Note the drop down Location window on the User Manager screen. Cards will not work at multiple locations unless they are programmed into each database for each location, and Sent when connected to the appropriate location.
5. To void or delete a card from multiple locations, you must Connect to each Location, select User Manager and select the card database for that Location, void or delete the card and Send.

4.4 Individual Reader Configuration

If you need to set operating parameters uniquely for one reader, you must display the Configuration screen for that particular reader.

To configure an individual reader:

1. Click on SK-NET™ Explorer, and select the Location.
2. Expand All Readers by clicking on the “+” button.
3. Double click on the desired reader icon (or right-click, then select Properties). A window appears with tabs labeled: Cards, Door Controls, Settings, Configuration, Transactions and Utilities.
4. Select the appropriate tabs, click on Edit for Settings and Configuration only, set the desired parameters.
5. Click Send, then Close.

The following sections explain the parameters you can set on each tab.

4.4.1 Reader Configuration — Cards Tab

Program Cards into a Time Zone — This allows you to program a range of cards for a specified Time Zone for the selected reader. This is a quick way of programming cards, but is not recommended, because it bypasses the User Database, and introduces cards into the system without assigning Names and Access Groups.

1. Select and enter a Time Zone.
2. Enter starting and ending card numbers for the range to be programmed.
3. Click Send.

Program Limited Use Cards — See Section 4.2

Display Card Range (maximum 5000 at a time). — This allows you to display the actual local card data from the reader, including Time Zone, Limited Use Type and Count. Card User Name data is also displayed, but this is retrieved from the PC database. The ability to display local card data is helpful when diagnosing a problem.

1. Enter starting ending card numbers for the range to be displayed
2. Click Display. Click Close when done viewing cards.

4.4.2 Reader Configuration — Door Controls Tab

Allows you to display or change the current state of the selected reader. Options include:

Open — activate strike relay for standard access time

Unlock — activate strike relay indefinitely

Inactive — disables reader indefinitely

Normal — cancels Unlock or Inactive.

The Refresh button will query the reader to redisplay the latest status.

4.4.3 Reader Configuration — Settings Tab

Allows you to display or change various parameter settings for the selected reader. To change parameters, click on Edit. To query the reader for the latest information, click Refresh. To view or change Time Zones, click on Zones.

Parameters include:

Time — 24-hour, normally sent from PC

Date — also normally sent from PC

Latch Timer — set duration of Strike/Shunt Relay from 0 to 30 seconds for a valid access

Timed Antipassback — Set amount of time a card is temporarily voided following use at this reader - requires that card be assigned to a Time Zone with TAPB enabled at this reader.

Baudrate — Set communications speed for a PC, printer or modem directly connected to this reader via the RJ-11 data jack or Communications inputs on the terminal block.

Reader ID — Reader Name used in all reports, status display, etc; you can also set this from SK-NET™ Explorer.

Software Version — Indicates the software version installed in the reader — information only, field can not be edited.

Zones — Displays the Time Zone screen which allows Time Zones 2-15 and Door Zone to be displayed or uniquely defined for the selected reader. Unless required for special circumstances, programming Time Zones uniquely at individual readers is not recommended, because it makes system management difficult, and also because it is easy to overwrite unique local Time Zones when working in the Global Time Zone menu.

Holidays — Displays the holidays screen which shows the dates of all the defined holidays.

Reader Icon — Allows you to select a different icon for the reader.

4.4.4 Reader Configuration — Configuration Tab

This tab allows various additional parameters to be displayed and defined for the individual reader.

Inputs - Displays current configuration status of reader inputs. Click on Edit, then on individual “Change” buttons to view various input type options. For details, see Section 3.5.1.

Output (SK-ACP only) – Displays the current configuration status of the auxiliary output relay. Click on “Edit”, then on “Change” to view various output options. For details, see Section 3.5.2.

Limited Use Card Range — See Section 4.2

Daily RAPB Forgive Time — Select hour of the day (1-24) when all cards at the selected reader will be set to Neutral Antipassback status, allowing the next access, regardless of the card's current antipassback status. Click on Off to defeat this feature.

Network Node ID — This is normally assigned by the system. Do not change unless instructed by Secura Key Product Support.

Primary Reader Type — For RAPB operation at the selected reader. Set to None if RAPB is not used at this reader.

Remote Reader Type — (28SA Plus only) Also for RAPB operation at any remote reader connected to selected reader. Set to None if RAPB is not used at this reader.

4.4.5 Reader Configuration — Transactions Tab

Displays current history buffer status, and allows you to view or clear transactions for the selected reader. Options include:

View All — Displays all stored transactions

As Occur — Displays incoming transactions in real time

Clear All — Deletes all transaction data from selected reader

Refresh will redisplay latest memory statistics.

4.4.5.1 Exclude Transaction Types

You may select transactions which will not be logged in the panel or 28SA-Plus. By choosing to exclude certain types of transactions, more memory is available to store transactions that are important to you. For example, you may choose to exclude "Type 37" events (opened via sensor) if you do not need to know every time the door is opened by a "Remote Open" input.

1. Click on "Edit".
2. Check event types to be excluded.
3. Click on "Send".
4. Click on "Close".

NOTE: This function only works with firmware versions. 2.30 and higher.

4.4.6 Reader Configuration — Utilities Tab

Self Test — This allows the user to run the self test for the selected reader. This test is also the preferred method of recalibrating the reader's Hall Effect sensors, eliminating the need to go out to the reader. Initially, test result fields are blank; click on Refresh to run the test.

Panel/Reader Data — displays current service hours and reader serial number. Service Hours are updated when you click Refresh; serial number is programmed at the factory.

Backup / Restore — This option allows you to do a full backup of an individual reader to your PC hard drive. This backup is distinct from the reader and card configuration databases that you create with the SK-NET™ software. A reader Backup is useful to restore reader settings if a reader must be replaced in the field. Click on Backup to back up all data from selected reader to the PC. Click on Restore to send stored data for selected reader from the PC.

4.4.7 Reader Configuration — Service Tab (SK-ACP Only)

The Service Tab is used for viewing and/or changing the facility codes in the panel. It is also used for setting up the SK-ACP to work with readers other than Secura Key. SK-ACP panels come with a factory default setting that recognizes 26, 31 and 32 bit Wiegand formats with standard parity. If the cards and readers you use have a different bit format, lack parity or have unconventional parity, you may customize the panel for this. *Before using a reader with the SK-ACP we recommend that you send us a card, and possibly a reader too, so that we can decode it.*

4.4.7.1 Facility Codes

The left-hand side of the box displays the facility code or codes in the panel. The numbers shown are blind codes, call Secura Key to learn what card codes they correspond to. To add or change a facility code:

1. Click on "Edit".
2. To add a facility code click on "ADD++". Enter the value. Click on "Close".
3. To delete a facility code, locate the code then click on "Delete". Click on "Close".
4. To edit a facility code, locate the code and type in the new value. Click on "Close".
5. Click on "Send" to change facility codes in just one panel or click on "Send to All" to make changes throughout the network.

4.4.7.2 Bits and Parity

To change the panel from defaults to a custom setting:

1. Click on "Edit" on the right-hand side of the box.
2. Uncheck "Use Defaults" box.
3. Set the bits and parity you need.
4. To change just one panel click on "Send". To change all panels in the Location click on "Send to All".
5. Click on "Close".

4.5 Setting Reader Group Properties

A Reader Group consists of one or more readers which are associated for the purpose of being simultaneously controlled or identically configured. SK-NET™ has three default Reader Groups: All Readers (for global configuration and control), and IN and OUT Readers (for Antipassback setup).

The user can create 29 custom reader groups for applications that require common configuration or control, such as perimeter doors, parking gates, turnstile readers, fire exits, etc. To create a Reader Group:

1. Click on SK-NET™ Explorer.
2. Select desired Location.
3. Right-click, select New, then Reader Group.
4. Enter the desired Reader Group name in the Name field (type over "New Group"), then click OK.
5. Click on each appropriate reader in All Readers Group, then drag and drop to the new Reader Group that you just created.

The Group Properties screen allows you to set parameters which will apply to all readers in a reader group. For Group Properties, right-click on the desired group icon, then select Properties. The following options are available.

Properties / Door Controls – Displays the Group Name and Group ID, and allows you to add a Group Description. Also allows you to Open the door/gate for the programmed Access Time, Unlock the door/gate for an indefinite period, Inactive - to disable the reader indefinitely, and Normal to cancel either the Unlock or Inactive modes.

Readers – lists all reader IDs and Location Data. Cannot edit.

Cards – It is always preferable to program cards by using the User Manager. However, this option allows you to quickly program a range of cards into a group of readers. To program cards into a Time Zone (for all readers in group) specify TZ, starting card number, ending card number, and click on Apply. To program Limited Use Cards, see Section 3.5.

Configuration – The following configuration options are available for reader groups, and function identically to the options on the individual Reader Configuration Screens (see Section 3.1.2 for a detailed description).

- Set Limited Use Card Range
- Set Daily RAPB Forgive Time
- Set Remote Reader Type
- Set Latch Timer
- Set Timed Antipassback Time
- Set Baud Rate (reader's local com port)

Transactions – You may choose to exclude certain types of events from being logged in a group of readers. By choosing not to log certain events more memory becomes available for storing the events you do consider important. Select the Transactions tab. Place a check mark next to each transaction type to be excluded. Click on “Send”. NOTE: This feature only works with firmware versions 2.30 or higher.

4.6 Access Groups with Different Time Zones for Individual Readers

You may need to create an access group that restricts access to certain readers at different times from other readers. Suppose that you want to allow Office Staff to access the building from 8 AM to 8PM, but you want to restrict them from the Supply Room after 5 PM.

1. Create a Time Zone with a 9AM - 5PM M-F Schedule
2. Create a Time Zone with an 8 AM to 8 PM M-F Schedule
3. Create a new Access Group with the 8AM - 8 PM Time Zone, as described above.
4. From SK-Explorer, right click on that access group and select Properties.
5. Click on the Reader Tab. Select Edit.
6. Change the TZ for the Supply Room reader to the 9-5 Time Zone.
7. Select Save, Click on Send, Click on Close.

4.7 Software Preferences

4.7.1 User Defined Cardholder Information

1. Click on “Configuration” in the top toolbar.
2. Click on “Preferences”.
3. Click on “ User Field Labels” tab.
4. Type in field labels.
5. Click on “OK”.

4.7.2 Check Readers

1. Click on “Configuration” in the top toolbar.
2. Click on “Preferences”.
3. Click on “Check Readers” tab.
4. Select reader self check interval. *Longer times recommended for larger systems.*

4.7.3 Messages

1. Click on “Configuration” in the top toolbar.
2. Click on “Preferences”.
3. Click on “Settings” tab.
4. Select “Don’t ask for backup at shutdown” to eliminate backup prompt.
5. Select “View Net Messages” to display details of network communications at bottom of screen. *This is used for diagnostics.*

5.0 DAILY OPERATION

5.1 Editing Cards

Any card already enrolled may be edited. The users name and other information and/or the Access Group may be changed.

1. Click on the User Manager icon.
2. Double click on the desired card number.
3. Add or change cardholder information and/or select a new Access Group for this card.
4. Click on "Save".
5. After all cards have been edited, click on "Send".

5.2 Adding Cards

To add Card Users into the User Manager database:

1. Select the User Manager Icon.
2. Select Insert User "+", enter card user name and card number.
3. Select Access Group.
4. Enter any additional card user data.
5. Click on Save.
6. After all new users have been added, click on send.

5.3 Voiding Cards

Voiding a card changes its Access Group to "Void Users," but leaves all the rest of the user's information in the database. If a voided user attempts to gain entry at a reader, the user's name will appear in the log as part of the "access denied" transaction.

To void a card:

1. Click on User Manager
2. Select desired card user record.
3. Click on the Void Button (or right click on the record and select Void User).
4. Click on yes.
5. After all users have been voided, click on send.

If the card is used at multiple locations, Connect to each location, select that Location in the User Manager Location field (in the User Manager Toolbar), and repeat the steps above.

Voided cards can be re-validated later: Select the card, Click on Edit, select a valid Access Group, Save and Send.

5.4 Deleting Cards

Deleting a card removes it completely from the database. The procedure follows:

1. Click on User Manager.
2. Select desired card user record.
3. Right-click, choose Delete, click OK.
Or...
Single click, click on "-", then click OK.
4. After all users have been deleted, click on send.

NOTE: If the card is used at multiple locations, link to each location, select that location in the User Manager, and repeat the steps above.

If you accidentally delete a card, and have not yet exited SK-NET™, you can right-click anywhere in the User Manager screen and click on Undo Delete. The last deleted card will be restored to the database.

5.5 Filter Users

You may filter the User Manager screen two way, by Access Group and/or by In/Out status.

1. Click on User Manager icon.
2. Click on “Filter Users” icon in bottom toolbar.
3. Check “All” to view all cardholders or “Access Group” and select Access Group to view just cardholders in just one Group.
4. Check “All” to view cardholders regardless of in/out status; “IN” to view only those who are in or “OUT” to view only those who are out.
5. Check “All” to view cardholders in all departments or select “Single” and type in the name of a department as it appears in the User Master database. (NOTE: Spelling and capitalization must match database exactly.)
6. Click on “OK”.

5.6 Opening Doors

To Open Doors, you must select a reader group or a reader.

1. Click on SK-NET™ Explorer.
2. Choose a Location
3. Click on a group, such as All Readers. For a single reader, click “+” to expand the group and select an individual reader icon.
4. Click on the Open Door Icon on the toolbar. The selected door(s) will unlock for their programmed access time.

5.7 Setting Readers to Inactive (Locked) Mode

To Set Readers to Inactive (Locked) mode, you must select a reader or a reader group.

1. Click on SK-NET™ Explorer.
2. Choose a Location
3. Click on a group, such as All Readers (or any desired reader group). For a single reader, click “+” to expand the group, and select an individual reader icon.
4. Click on the “Locked” Icon on the toolbar.

The selected door(s) will change to inactive (locked) mode, indefinitely.

To Cancel this mode, be sure that the same readers are selected, then click the Return to Normal button.

5.8 Setting Readers to Unlocked Mode

To Set Readers to Unlocked mode, you must select a reader or a reader group.

1. Click on SK-NET™ Explorer.
2. Choose a Location.
3. Click on a group, such as All Readers (or any desired reader group). For a single reader, click on “+” to expand the group, then select the individual reader icon.
4. Click on the “Unlocked” Icon on the toolbar.

The selected door(s) will unlock indefinitely.

To Cancel this mode, be sure that the same readers are selected, then click the Return to Normal button.

5.9 Door Zone Override

If you have a door zone for a particular door you may choose to override it. (i.e. during a plant shutdown period, etc.) If the door zone has been overridden you can reinstate it by following the same procedure.

1. Click on SK-NET Explorer.
2. Right click on the desired reader name.
3. Select “Properties”
4. Select “Door Controls” tab.
5. Click on “Edit”.
6. Check (or un-check) the box next to “Door Zone Disabled”.
7. Click on “Send”.
8. Click on “Close”.

5.10 Monitoring System Activity

To view real time system activity for the currently connected Location you must be “logged in” to the readers (green check marks). Click on Transactions. The newest transactions appear at the bottom of the screen. You can page or scroll up to view earlier data.

You can also restrict the Transaction screen to display only certain data by clicking on the Filter button, selecting the desired parameters and clicking OK. Remember to remove filtering later: click the Filter button, select Defaults and click OK.

5.10.1 Filter Transactions

You may apply a variety of filters to the transaction screen to limit which transaction you will view.

1. Click on Transactions” icon.
2. Click on “Filter” icon in bottom toolbar. The following filter menus will appear:
 - A. Transaction Category. Select “ALL” or select “Category” and indicate “Valid Use”, “Violations” and/or “System”.
 - B. User Selection. Select “All Users” or select “Single User”, click on “Select” and highlight user.
 - C. Daily Time. Select “All Time” or select “Time Range” and enter start time and end time desired.
 - D. From Dates. Select “First Event” or select “Events On” and enter beginning date.
 - E. To Dates. Select “Last Event” or select “Events On” and enter ending date.
 - F. Reader Selection. Select “All” or select “Single” and highlight desired reader.
 - G. Location Selection. Select “All” or select “Single” and highlight desired Location. *This applies to multilocation-dialup software only.*

The Transaction screen contains transactions from all locations, but you can only see real time data for the location to which the system is currently connected (assuming the readers are logged in). If you wish to view real time transactions from another location, click on SK-NET™ Explorer to select the new Location, right-click and choose Connect. Then, click on Transactions.

5.11 Forgive (Reset) Antipassback

For cardholders subject to Real Antipassback, this feature allows card users’ Antipassback Status to be set to a Neutral state. This is necessary in the event that card users are locked out because their IN/OUT status has become out of sync.

1. Click on SK-NET™ Explorer.
2. Right-click on the appropriate Location. Select Forgive.
3. Choose All (to forgive all Card Users), Range (to enter a range of card numbers) or User (to specify one Card User). Click OK.

SK-NET™ will set all specified cards at the appropriate readers to Neutral Antipassback status, which will give them one “free” entry at either an IN or OUT reader regardless of their previous Antipassback status.

6.0 REPORTS

Reports are produced by clicking on the Print Icon in any one of the three main screen displays:
SK-NET™ Explorer, User Manager, or Transactions.

6.1 SK-NET™ Reader Report

This report lists all readers in the system, and includes the Name, Serial Number, Location, Type, Software Version, and Node ID.

1. Click on SK-NET™ Explorer.
2. Click on Print Icon.
3. Select destination (Printer or Screen). Make any other adjustments as necessary.
4. Click on Print

6.2 Print/Display Card User Reports

This report lists all card users for the selected location.

1. Click on User Manager. Select a Location, if using the Multi-Location Option.
2. Select User Report or User Detail Report.
3. Select destination as Printer or Screen. Make any other adjustments as necessary.
4. Click on Print

6.3 Print Transaction Reports

This report lists all events in the Transaction History Database. The Filter option allows you to select specific transactions for inclusion in the report.

1. Click on Transactions.
2. Click on Filter.
3. Click on Show All or Category. If Category is selected, click on the check boxes to select which Transaction Categories will appear in the report.
4. Select All Users or Single User. If Single User is selected, then click on the Select button, select a user from the drop-down box (use the scroll bar button to scroll through the list), then click OK.
5. Select All Time or Time Range. If Time Range is selected, enter Start and End Times for reporting, using 24-hour time format. This time range will apply for each day covered by the report.
6. In the From Date box select First Event or Events On. If First Event is selected, the report will start with the oldest event in the transaction database. If Events On is selected, then you must enter a specific start date for the report.
7. In the Through Date box, select Last Event or Events On. If Last Event is selected, the report will end with the most recent event in the transaction database. If Events On is selected, then you must enter a specific end date for the report.
8. In the Reader Selection box, Select All Readers or Single Reader. If Single Reader is selected, click the down arrow on the adjacent drop down box and select a reader. Use the scroll bar button to scroll through the reader list.
9. In the Location Selection box, Select All Locations or Single Location. If Single Location is selected, click the down arrow on the adjacent drop down box and select a location. Use the scroll bar button to scroll through the location list.
10. To view results of the current filter selection, click on Apply. To Undo filtering, click Defaults. To accept current filtering, click OK.
11. Click on the Print icon. Select Destination as Printer or Screen. Make other adjustments as necessary. Click on Print.
12. After the report is printed, be sure to reset the transaction filter by clicking on Filter, then Defaults, then click OK.

7.0 MAINTENANCE

7.1 System Backup and Restore

This function allows you to make a complete safety backup of all your system configuration data. If your SK-NET Database files ever become corrupted, or if your hard drive ever fails, backups will allow you to restore your system. Note that when restoring from an older backup, any configuration or programming changes that you made since the backup will be deleted. Backed up databases include readers, cards, locations, history, time zones, reader groups, access groups, and time zones.

You can send a backup to a folder in your local hard drive, but this does not protect you if your computer crashes. Better options are to save the backup to a folder on your local area network server or to a portable media such as a ZIP drive, a CD-R or floppy disk. Be aware, however, that a floppy disk does not have much memory space and large backups (lots of transactions and/or photographs attached to user files) will make the backup too large to copy.

To backup SK-NET™ databases:

1. Click on File on the top menu bar, then select System Backup.
2. Select a location for the backup. You can enter the drive letter for your ZIP drive or other large capacity removable backup device.
3. The system will create the backup automatically. Click OK when done.

NOTE: Every time you close SK-NET™ you will be prompted to backup your system. Select Yes and designate where the backup is to be located.

To restore SK-NET™ databases from a backup.

1. Click on File on the top menu bar, then select System Restore .
2. Select the location of your backup. You can enter the drive letter for your ZIP drive or other large capacity removable backup device.
3. The system will restore the database automatically. Click OK when done.

NOTE: When restoring SK-NET™ databases, that all database changes and transactions which occurred since the last backup will be lost when the databases are restored.

7.2 Backup and Restore Individual Readers

SK-NET™ stores a binary image of each reader's local memory on the PC's hard drive. If a reader is vandalized or damaged, the new reader can be reprogrammed quickly by using this backup information. (This is different from SK-NET™ System Backup and Restore, which refers to system database files on the PC.)

To Backup a reader:

1. Click on SK-NET™ Explorer
2. Click on the "+" button for the desired Location, then click on the "+" button for All Readers to display individual reader icons.
3. Click to select the desired reader icon, then right-click and select Backup, and choose Single Reader to backup the selected reader, or All Readers to back up all readers at the location.
4. SK-NET™ does the backup automatically.

NOTE: After you change any reader configuration or settings you will be prompted to backup the reader. Select Yes and SK-NET™ will automatically backup that reader.

To Restore a reader:

If you are replacing an old reader with a new reader, or if a reader has been repaired and put back on line, first refer to Section 7.2, Adding / Replacing a Reader. Once the reader is communicating, here is how to restore the reader:

1. Click on SK-NET™ Explorer.
2. Click on the "+" button for the desired Location, then click on the "+" button for All Readers to display individual reader icons.

3. Click to select the desired reader icon, the right-click and select Restore, and choose Single Reader to restore the selected reader or choose All Readers to restore all readers at the location.
4. SK-NET™ does the restore automatically.

NOTE: When restoring a reader that any database changes or transactions that occurred since the last reader backup will be lost when the reader is restored.

7.3 Archiving Transaction

The Archiving Transactions option should be used when the SK-NET™ transaction history file becomes too large, affecting system performance. Depending upon the capabilities of the PC, a large transaction database may slow down the system.

Archiving renames the current transaction file, and creates a new empty transaction file. The Archive defaults to SKTRANSARC.dbf, in the SKNET directory, but can be saved to any directory, or to a removable storage device, such as a ZIP™ Drive or equivalent.

To archive transactions:

1. Click on the Transactions icon.
2. Select Transactions from the top menu bar, then click on Archive.
3. The Archive file name window is displayed. Accept the defaults or select the drive/directory where you would like to save the archive, and click Save, then OK.

If you change your mind about archiving you can use Windows Explorer to rename SKTRANSARC.dbf to SKNET/SKTRANS.DBF (the name for the current transaction file).

You can also do a report from an archive by temporarily renaming the current transaction file (such as SKTRANS.SAV), and then renaming the archived file as the current transaction file (SKNET/SKTRANS.DBF). Be careful not to delete or overwrite your history files, and remember to restore them to their original directories and file names when you are done.

7.4 Database Erase

This option allows you to delete all transactions from the PC. This should only be done if the transaction database has become seriously corrupted, as once the transaction database is deleted, there is no way to retrieve previously uploaded data from the readers into the database.

After a Database Erase, you can still do an individual report from each reader by selecting the reader, Properties, Transaction, View All and Print; but the filtering and selection is not available, and name data is not included in these individual reader history reports.

To erase the Transaction Database:

1. Click on Database Erase icon. System prompts "Are You Sure?"
2. Click OK. The transaction database is deleted from the PC.

8.0 TROUBLESHOOTING

8.1 COM Ports

PC Serial Communication Ports (COM 1, COM 2, COM 3, COM 4) are used to connect a PC with SK-NET™ software to the reader network.

On the back of most PCs, there are two male D-type connectors; one 9-pin and one 25-pin. The 9-pin connector is usually COM 1, and the 25-pin connector is usually COM 2. Note that the pins must be protruding from the connector; the D-type female connector is usually LPT-1, the parallel printer port.

Frequently, a serial mouse will be connected to COM 1, but if your PC has a PS/2 mouse or a bus mouse (using a small round connector), COM 1 may be available.

If the PC has an external modem, it may be connected to COM 2. Internal modems are usually configured to use COM 2, so even if the external connector appears empty, it might be unusable.

To make room for your reader network connection, you could remove the external modem cable and install an A/B switchbox, which would allow you to switch COM 2 to the Modem or the reader network.

To view your PC's current COM port configuration, close SK-NET™, double-click on My Computer (on the Windows desktop), click on Control Panel, Modems, then Diagnostics. The current COM port configuration is displayed.

If COM 1 and 2 are both in use, you will have to install additional connectors and cables for COMs 3 and 4. Most serial interface boards already have COM 3 and 4, they just don't have the cables and rear panel connectors. Refer to the instruction manual for your PC, or the manual for your serial interface board. Note that some PCs have serial ports COM 1 and COM 2 built into the Motherboard; you will have to add a serial interface card to obtain COM 3 and COM 4.

On PC's there is a conflict between devices used simultaneously on COM 1 and 3, or between devices used simultaneously on COM 2 and COM 4. Therefore, if you have a mouse on COM 1, you should attach your reader network to COM 2 or 4. If your mouse is on COM 2, connect the reader network to COM 1 or COM 3. If you also have a modem, do not use it while communicating with the local (hard-wired) reader network.

8.2 Adding/Replacing A Reader

1. Connect power and data cables to the reader.
2. Set the facility code in the new reader.
3. Click on SK-NET™ Explorer, then select the desired Location.
4. Right-click on the Location, select New, then Readers.
5. Choose "Quick Find" if there are less than 20 readers in the system. Choose "Search" for 20 or more readers. "Search" takes longer but it is more thorough.
6. SK-NET™ will scan the location for new readers. If readers are found, the New Readers Found screen will display.
7. Enter new reader names into the New Readers Found screen and click OK. Note that icons for the new readers will now appear under All Readers under the correct location.
8. If you are replacing a previously existing reader, the old reader icon will still appear with a red X through it. Drag the new reader icon and drop it over the old icon. SK-NET™ will prompt "Do you wish to replace reader "reader name"? Click on Yes and the new reader will then assume all of the old reader's attributes in the system database.
9. If you are adding a completely new reader, add it to the appropriate Access Groups and Reader Groups now.
10. To download card status to the new reader, Click on User Manager, verify (or Select) the correct Location, then click on Send. SK-NET™ will automatically send the appropriate card data to the reader.
11. To download Time Zones to the new reader, click on the Time Zone Global Database icon and click on All.

To rename existing readers:

1. Click on SK-NET™ Explorer.
2. Select the desired reader icon, right-click, select Rename.
3. Type in a new name for the reader and click OK.

APPENDIX A:

SK-ACP OR 28SA-Plus TROUBLE SHOOTING GUIDE

1.0 Erratic or No Communication Between Readers and PC

One of the most common problems with on-line systems is communications between reader stations and the PC. There are two different configurations for connecting the PC to the network, through the RS-232 Gateway, or with a Converter. Select the configuration of your system from the list below and follow all the troubleshooting steps listed in the appropriate section.

1. System Using the NET-CONV-P (RS 485 to RS232 converter).
 - a) See section 2.0
2. System Using the Reader Gateway (RS232 com port).
 - a) See section 3.0

2.0 System Using NET-CONV-P (RS232 to RS485 Converter)

2.1 Recommended Wiring

Check the following connections to the NET-CONV-P:

1. Cable Type: Eastman 725-5780PK or equivalent (2 **twisted pair** with overall shield - includes one spare conductor).
2. The **SK-NM 485 module** must be installed into each reader. (For 28SA-Plus only, SK-ACP has a built-in 485 module)
3. Verify that both the brown and red wires from the SK-NM 485 module (s) are connected as a **twisted pair**.
4. Verify that the brown wire is connected to TD (A), and that TD (A) and RD (A) are jumpered together.
5. Verify that the red wire is connected to RD (B), and that RD (B) and TD (B) are jumpered together.
6. Verify that the black wire is connected using one conductor of the second pair, and then to the converters GND or (-) side of the power supply.
7. Verify the converters power supply is connected to the 485 power input.
8. Verify JP1 is open (not jumpered), and JP2 is jumpered.

2.2 Setup Location Properties

1. Select SK-NET™'s Explorer (Globe Icon).
2. Right click on the location name, and select Properties from the pull down menu.

Click on the "Connection" tab.

 - a) Uncheck "Gateway (RS232)". Baud rate should automatically change to 38,400.
 - b) In the box labeled "Connect Using" select the PC serial COM port to which the converter is connected.
 - c) Be sure the "Local Connect" box is checked.
 - d) Click on "Connect".

2.3 Voltage Measurements

1. Voltages: Measure voltages at the converter.
 - a) Measure input voltage from the converter power supply. Should read from 9vDC to 16 vDC.
 - b) Measure the voltage from the GND or (- side of the power supply) to TD (A), should read 0 v DC, from GND to TD (B), should read from 2.5 to 5v DC.

2.4 Power Reset (for initial setup only!)

1. Power Reset: This will change the node address, set password to 12345 (default), and set the baud rate to 38,400 (default).
 - a) Turn off the power to the reader, push the reset button, turn on the power with reset button pushed for approximately 3 seconds after turning on power. Repeat for all readers.

2.5 Steps to find new readers

1. Right click on location name.
2. Select Connect. Message on Screen: "Connecting to location (Name), continue." Click OK.
3. Message on Screen: "There are no readers in Location (Name), to be logged in. Scan for new readers now?" Click YES. Message on screen: "Are there more than 20 readers in this location? Select "YES" or "NO".
4. Message on Screen: "New Readers Found!", select OK. Now the software will make backup files for all the settings in all of the readers except for the card status.
5. If no readers are found, continue to section 2.6.

3.0 System Using A Reader Gateway (PC to Unit RS232 port)

3.1 Recommended Wiring

1. Cable Type: Eastman 725-5720 SJ, or equivalent (5 conductor shield, not twisted).
2. If you are using the a 28SA-Plus unit, the **SK-NM 485 module** must be installed into the reader. This is not necessary for the SK-ACP.
3. DB9 Connector: verify wiring using a DB9 connector to the terminal block of the reader per figure 2.
4. DB25 Connector: verify wiring using a DB25 connector to the terminal block of the reader per figure 2.

3.2 Setup Location Properties

1. Select SK-NET™'s Explorer (Globe Icon).
2. Right click on the location name, and select Properties from the pull down menu.
 - Click on the "Connection" tab.
 - a) Be sure "Gateway(RS232)" and "Local Connect" are checked.
 - b) Click on the Connection Wizard icon.
 - c) Click on "YES". Connection Wizard will try every COM port at every baud rate until the system is located.
 - d) When asked to accept the settings, click on "YES".
 - e) Click on "Connect"

3.3 Voltage Measurements

1. Voltages: Measure voltages at the gateway reader's terminal block, communications pins 1 to 5. Connect the ground lead to pin 1 (logic ground) for all measurements.
 - a) Pin 2 (Receive Data, RXD). The voltage should read between -5 VDC to -12 VDC. This voltage comes from the PC. If the voltage is wrong or missing, disconnect the reader from the PC, and measure the voltages at the reader (should be 0.0 VDC) and at the PC (should be between -5 VDC to -12 VDC).
 - b) Pin 3 (Clear to Send, CTS). The voltage should read between +5 VDC to +12 VDC. This voltage comes from the PC. If the voltage is wrong or missing, disconnect the reader from the PC, and measure the voltages at the reader (should be 0.0 VDC) and at the PC (should be between +5 VDC to +12 VDC).
 - c) Pin 4 (Request to Send, RTS). The voltage should read between -5 VDC to -12 VDC. This voltage comes from the Card Reader. If the voltage is wrong or missing, disconnect the reader from the PC, and measure the voltages at the reader (should be -9.5 VDC) and at the PC (should be 0.0 VDC).
 - d) Pin 5 (Transmit Data, TXD). The voltage should read between -5 VDC to -12 VDC. This voltage comes from the Card Reader. If the voltage is wrong or missing, disconnect the reader from the PC, and measure the voltages at the reader (should be -9.5 VDC) and at the PC (should be 0.0 VDC).

3.4 Power Reset *(for initial setup only!)*

1. Power Reset: This will change the node address, set password to 12345 (default), and set the baud rate to 38,400 (default).
 - a) Turn off the power to the reader, push the reset button, turn on the power with reset button pushed for approximately 3 seconds after turning on power. Do not have any cards near the reader while this process is being done. Repeat for all readers.

3.5 Steps to find new readers

1. Right click on location name.
2. Select Connect. Message on Screen: "Connecting to location (Name), continue." Click OK.
3. Message on Screen: "There are no readers in Location (Name). To be logged in, scan for new readers now?" Click YES. Message on screen: "Are there more than 20 readers in this location? Select "YES" or "NO".
4. Message on Screen: "New Readers Found!", select OK. Now the software will make backup files for all the settings in all of the readers except for the card status.
5. If no readers are found, continue to section 3.6.

Recommended Tools & Supplies

- 1) Laptop PC with Pentium 200 or compatible processor
Window® 95/98/2000 or Windows® NT 4.0 or greater
64 MB RAM
100 mb Hard Drive Capacity
CD-ROM drive
High Speed Serial Com Port (38.4k or better)
- 2) CBLSA Cable Kit
- 3) Multimeter to measure DC volts and resistance
- 4) Hand tools required for the reader installation, and connection.

Tech Support Options

Web Page: www.securakey.com • *E-Mail:* techsupport@securakey.com

Fax: 818-882-7052

Toll-Free Telephone: 800-891-0020

Tech Support Hours:

7:30 am to 5:00 pm P.S.T. Best Time to call: Afternoons P.S.T.

APPENDIX B:

WINDOWS® 95/98 HYPER TERMINAL SETUP

In order to connect to a ENTRACOMP® 28SA-Plus OR SK-ACP access control unit using Windows follow these steps:

1. Click on the start button on the lower left corner of the screen.
2. Select Programs.
3. Select Accessories.
4. Select Hyper Terminal.
5. Double click on Hypertrm.
6. Type Secura Key in the name field.
7. Click OK.
8. The next window will have a selection at the bottom of "Connect Using". Be sure it is set to "Direct to Com1", or whatever com port is available.
9. Click the settings tab at the top of the box.
10. Under Emulation, select VT100.
11. Click OK.
12. Verify the following setting in the next properties box:
 - (a) Bits per second: 38,400
 - (b) Data bits: 8
 - (c) Stop bits: 1
 - (d) Flow control: None
13. Click OK.
14. The next box should display the greeting and the "Enter Password" prompt. Enter 12345, or the appropriate password.
15. If this greeting does not appear, press the Enter or Return key once.
16. If the greeting still does not appear, check the wiring between the unit and the PC and test the com port.
17. To exit, click the (X) box on the upper right. Be sure to answer Yes to save the session.

APPENDIX C:

CONNECTING A MODEM TO SK-ACP

Using the SK-MDM Modem with the Secura Key 28SA-Plus Access Control Unit and/or SK-ACP Advanced Control Panel

The SK-MDM Modem (Best Data Smart One 56SPX) has been selected by Secura Key for use with 28SA-Plus Access Control Unit and the SK-ACP at remote locations. The SK-MDM is connected directly to the RS232 port of a 28SA-Plus or an SK-ACP.

The 28SA-Plus and SK-ACP contain the configuration data or “setup string” for the SK-MDM, which allows the modem to be configured in the field by the reader without the use of a computer, and without setting DIP switches.

Note that the setup string stored in the 28SA-Plus and SK-ACP is only used for modems at remote locations. If you are using a SK-MDM at the PC location, use the setup information provided with the modem for installation with your PC.

MODEM REAR PANEL CONNECTIONS - REMOTE SITE

Line	Connect to the phone line at the remote site (not the RJ-11 Jack on the panel).
Phone	Not required.
Serial Port	Connect to 28SA-Plus or SK-ACP RS232 Port (see Manuals for wiring details).
Power	Connect the 9VAC plug-in transformer supplied with the unit.

SETTING UP THE BEST DATA 56SPX MODEM

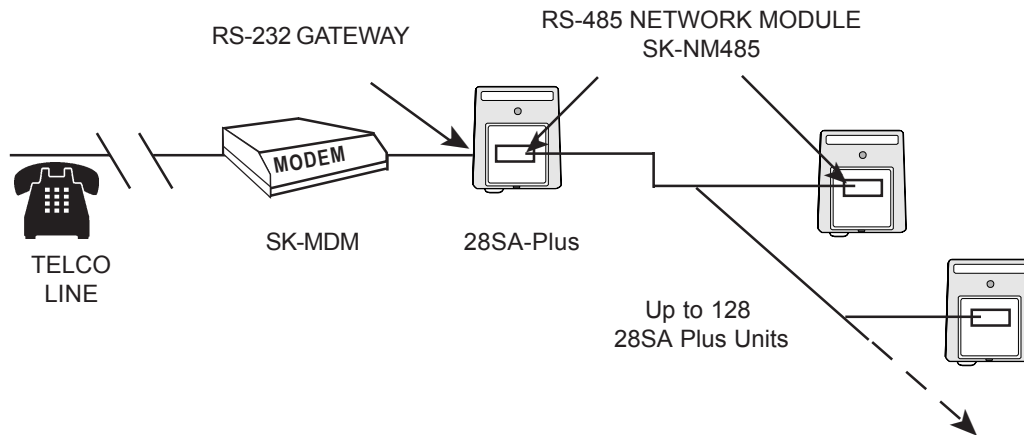
The order of these steps is critical, particularly when turning power on to the modem and reader or SK-ACP.

1. Remove power to the 28SA-Plus or SK-ACP
2. Connect cable from reader to modem
3. Turn power to the modem on
4. Turn on power to the 28SA-Plus or SK-ACP

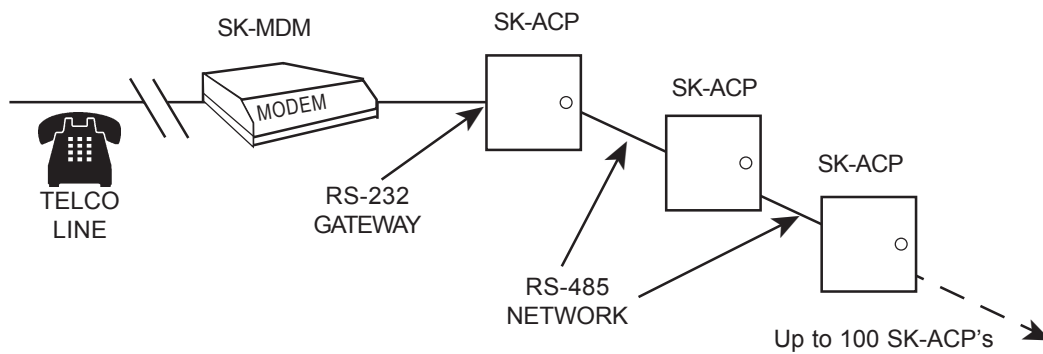
The modem is now set to “auto answer” and “dumb” mode. You can now connect to reader from the PC location. Verify that the TR, CD and AA lights are lighted (on) on the modem display.

NOTE: The default baud rate is 38,400 baud. You can change the baud rate of a 28SA-Plus using the PD-26 program deck, and the SK-ACP using SK-NET™ or a terminal program.

REMOTE SITE MODEM CONFIGURATION with 28SA-PLUS



REMOTE SITE MODEM CONFIGURATION WITH SK-ACP



APPENDIX D:

CONNECTING AN SK-ACP OR 28SA-PLUS TO A LOCAL AREA NETWORK

Using the SK-LAN External Device Server with the Secura Key SK-ACP and/or 28SA-PLUS.

The SK-LAN External Device Server (Lantronix UDS-10-01) has been selected by Secura Key for use with our networkable access control system to permit connection over a 10BASE-T Local Area Network. The SK-LAN is connected directly to the RS-232 port of the gateway panel or reader.

Before installation, the LAN Network Administrator needs to assign an address to the SK-LAN. **To avoid duplicate IP address conflicts, be sure to reserve this address in your DHCP server.**

1. Connect a PC to the SK-LAN with a serial cable. Do not power up the SK-LAN yet.
2. Run Hyper Terminal (Start/Programs/Accessories/Communication/Hyper Terminal)
3. Select the appropriate COM port.
4. Set Baud rate (Bits per second) to 9600; Data Bits to 8; Parity to 0; Stop bits to 1 and Flow Control to None. Click OK and OK.
5. Holding down the "X" key, power up the SK-LAN. Release "X" key when prompted to hit the "enter" key.
6. "Enter" to go to setup mode.
7. Select "0" for server configuration.
8. Enter the IP address assigned to the SK-LAN by the Network Administrator.
9. Enter the Gateway address provided by the Network Administrator.
10. Enter the SubNet Mask, provided by the Network Administrator.
11. Accept the remaining default settings.
12. Enter "1" to go to Channel 1 configuration.
13. Change the baud rate to match the SK-ACP or 28SA-PLUS. The default baud rate for these products with firmware version 2.40 or later is 38,400. (Older products had a default of 9600.)
14. Accept the other default settings.
15. Enter "9" to save the settings and exit.

Install the SK-LAN in the field. Connect the Gateway panel or reader to the DB25 serial output using the provided cable. Connect the 10BASE-T port to a network jack with an Ethernet cable. Connect the included power supply to 110VAC.

DO NOT:

- **Plug the Ethernet cable into a telephone jack.**
- **Substitute another power supply.**
- **Mount the unit in a wet location or a location where temperatures may exceed 120 degree F.**

Test the unit.

1. Ping.

Go to "Start" / "Run".

Type "command". Click OK. (This brings up a command prompt.)

Type "ping <IP address>". Press "Enter".

If the reply indicates "Request Timeouts" there is an error in the setup or connections.

If the reply shows "Packets sent" and "0% Loss". The setup and connections are good.

2. Communicate with SK-LAN.

Go to "Start" / "Run".

Type "telnet <IP address> 9999". Click OK.

The setup menu of the SK-LAN should appear. Exit

3. Find the Gateway reader/panel.

Go to "Start" / "Run".

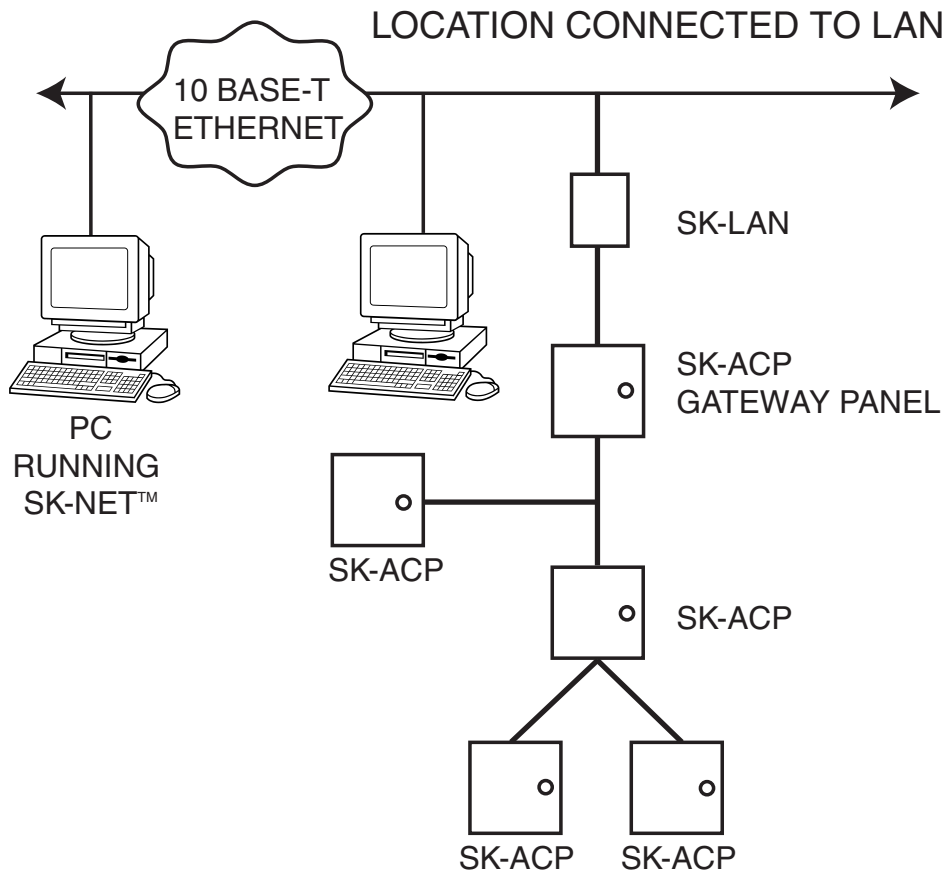
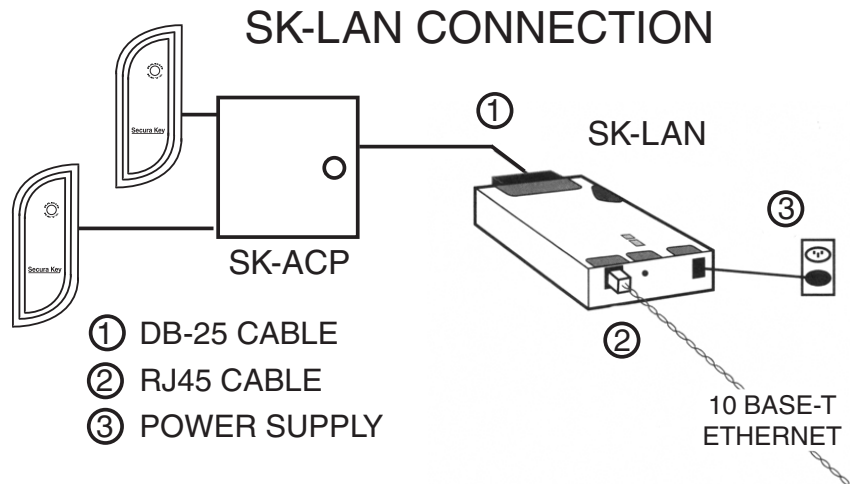
Type "telnet <IP address> 10001". Click OK. Enter.

The internal menu of the reader or panel should appear. Exit.

You are now ready to configure your system using SK-NET-MLD software. See Section 2.2.1.4 d for instructions.

NOTES:

- 1) Always close SK-NET before closing WINDOWS to avoid LAN communications failures.
- 2) The manufacturer's instruction manual is included with the SK-LAN. Keep this document for additional troubleshooting and setup information.



APPENDIX E:

PREVENTING LIGHTNING DAMAGE

Surge Protection for Access Control Systems

Access Control equipment is susceptible to damage from lightning, especially when installed outdoors. Voltage spikes which travel through buried data cables, telephone lines or AC power lines can damage Access Control equipment indoors, as well.

While nothing can protect equipment from a direct lightning hit, surge protectors can help to minimize the damage caused by nearby lightning strikes. Surge protectors operate by connecting Transorbs or Varistors from data lines to ground. Surge protectors have no effect on normal circuit voltages, but can act quickly to divert large voltage spikes to ground and away from sensitive components.

Secura Key SA-Series Access Control Units are equipped with surge protection on all inputs and outputs. PC's, Printers, and Modems are designed for an indoor, office environment and do not have surge protection. However, by properly installing aftermarket surge protection devices on all inputs and outputs, these devices can also be protected from lightning damage.

Where to Install Surge Protection

- On the AC line voltage input to the PC.
- On the AC line voltage input to any transformer or DC Power Supply connected to a 28SA-Plus or Modem.
- On RS-485 data lines connecting a 28SA-Plus Units or to a PC, Printer or Modem, using a NET-CONV-P converter.
- On RS-232 data lines from SA Units (Readers) to PC's, Printers or Modems.
- On Telephone lines connected to Modems.

Protect Both Ends of Data Lines

Surge Protectors should be installed at both ends of all Data Lines.

Wire Distance from the Surge Protector

You must **locate the protector at least three wire feet away from the device being protected**. The additional wire resistance will dissipate the energy from leading edge of the spike. The wire can be coiled; a three-foot physical distance is not required.

Grounding the Surge Protector

Surge protectors **must be connected to a verified good, nearby earth ground**. This can be AC Power Ground, a 10' Copper Ground Stake, or Building Ground. Run 16 AWG or heavier wire as short a distance as possible, and avoid any bends in the wire.

Self-grounding Surge Protectors

Do not use surge protectors unless they are equipped with a separate ground wire or ground screw. Self-grounding Surge Protectors use the connector shell or Pin 1 as a ground path; however, the shell and Pin 1 are not always grounded.

AC Power Surge Protectors

AC Power Surge Protectors must be plugged into a properly grounded 3-wire socket. If a 3-wire socket is not available, have one installed by an electrician; do not use a 2-prong socket by cutting off the 3rd prong on the plug, or by using a 3/2 converter, or the surge protector will be rendered useless.

Terminating Cable Shields

Connect cable shields on data cables at one end only. You may terminate the cable shield to the same ground as the surge protector. Leave the cable shield unconnected at the opposite end.

Grounding the Access Control Unit

At the Access Control Unit, connect the Green Ground Screw on the mounting plate to a good earth ground, to allow the built-in surge protection to work properly.

Recommended Surge Protectors

There are many manufacturers of Surge Protectors for , RS-485, RS-232, AC power and telephone line applications; while we don't specifically endorse a particular product, we have listed several below. These manufacturers can give you details on price, performance and installation methods. The model numbers specified below are the minimum protection needed. Some areas may require additional protection. If lightning damage persists, consult these manufacturers.

Diversified Technologies (Ditek) Tel: (800) 753-2345.

RS-485 Surge protectors with screw terminals, ground wire, clamping level 7 VRMS

- 4 wire, DTK-2LVLP-D

RS-232 Surge Protectors with screw terminals, ground wire, clamping level 7 VRMS

- 6 wire, DTK-3LVLP-D

Telephone Line Surge Protectors w/screw terminals, ground wire, clamping level 130VRMS

- 2 wire, DTK-1LVLPSCP-RUV

Stormin Protection Products, Inc. Tel: (888-471-1038) or (813) 548-5418

RS-485 Surge protectors with screw terminals, ground wire, clamping level 15 VRMS

- 4 wire, DDUAL-3W-DTV/G-7V

RS-232 Surge Protectors with screw terminals, ground wire, clamping level 15VRMS

- 5 wire, DDUAL-5W-DTV/G-7V

(With Screw Terminals one side, with DB-25 other side (pin # 2, 3, 4, 7 & 8))

Telephone Line Surge Protectors w/screw terminals, ground wire, clamping level 130VRMS

- 2 wire, DLT-TOS-200V (Specify Screw Terminals or RJ11)

Secura Key

A Division of SOUNDCRAFT Inc.

20447 Nordhoff Street, Chatsworth, CA 91311

Phone: (818) 882-0020 • *Fax:* (818) 882-7052

TOLL-FREE: (800) 891-0020

Website: www.securakey.com

E-mail: mail@securakey.com