

# SK-NET™ 4.0 Tutorial



SK-NET™ is a Windows® based software program designed to monitor and control a network of Secura Key SK-ACP 2-door control panels or the Secura Key 28SA Plus control units.

Smart. Reliable. Secure.

[Main Menu](#)

**Secura Key**  
A Division of SOUNDCRAFT Inc.

# Main Menu

- [SK-NET™ Versions](#)
- [Getting Started](#)
- [Enter MLD serial number](#)
- [Quick Start Guide](#)
- [RS232 connection](#)
- [LAN connection](#)
- [Modem connection](#)
- [Connection Group](#)
- [Multiple Connections](#)
- [Connecting to a Location](#)
- [Transaction screen](#)
- [Transaction reports](#)
- [Archive transactions](#)
- [View single transaction](#)
- [User Manager](#)
- [Enter block of cards](#)
- [Add/Delete/Void user](#)
- [Find/Filter users](#)
- [User reports](#)
- [View In/Out status](#)
- [Time Zones](#)
- [Access Groups](#)
- [Holidays](#)
- [Limited Use](#)
- [Timed Antipassback](#)
- [Real Antipassback](#)
- [Inputs](#)
- [Outputs](#)
- [Door Controls](#)
- [Add new readers to your system](#)
- [Add new cards to your system](#)
- [Contact Us](#)

Select One or Left Click to View All

# SK-NET™ Versions

## **SK-NET™ Basic Version**

Free download from our website at [www.securakey.com](http://www.securakey.com)

SK-NET-DM (CD ROM with manual)

Supports: RS232 communications  
RS232 to RS485 communications  
**NEW** Single LAN connection version 4.0 or higher

## **SK-NET™-MLD Version**

SK-NET-MLD (CD ROM with manual)

Supports: All above  
Multiple locations  
**NEW** Multiple LAN TCP/IP communications in a single location  
Modem dial up communications

## **SK-NET-MLD™-Client Server Version**

SK-NET-MLD-CS XX (CD ROM with manual)

Supports: All above  
Client Server license available for 2,5,10, or 15 workstations

# Getting Started



To start SK-NET™ double click on the Icon



**First time startup:**

Default User Name is: **Admin**

Default Password is: **12345**

Smart. Reliable. Secure.

[Main Menu](#)

**Secura Key**  
A Division of SOUNDCRAFT Inc.

# Setting up the MLD Version



Go to Help, and select **Upgrade System**

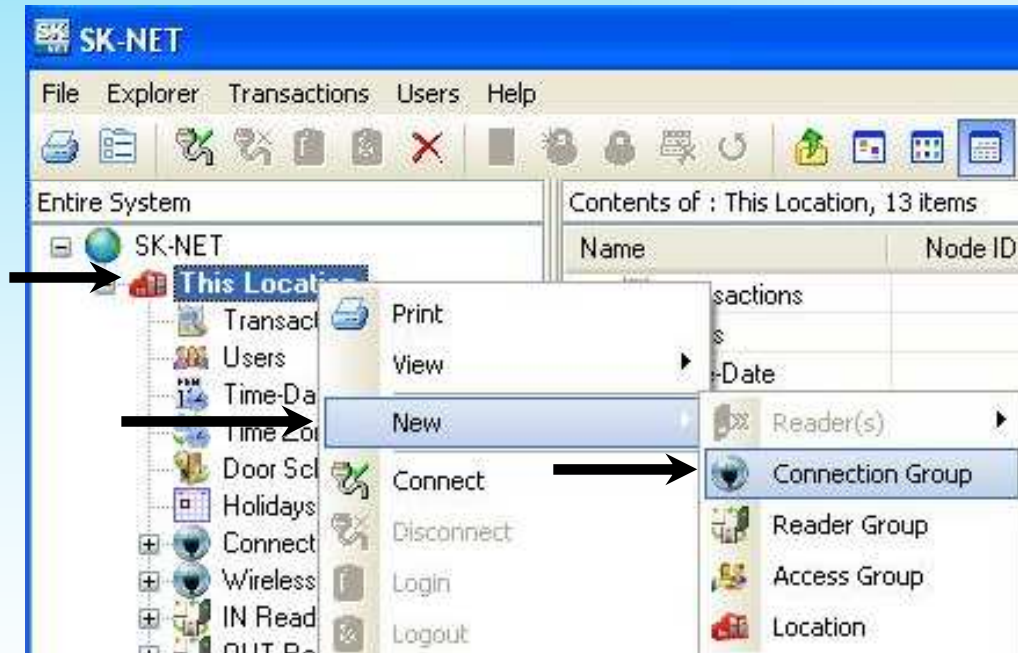


Select **MLD** and enter the 12 digit serial number located on the inside cover of the SK-NET™ manual

# Connection Group

Connection Groups define a means to access a reader gateway. It contains all Readers that are visible through the reader gateway via RS-232, LAN connection or by Modem. In the MLD and Client Server systems, more than one Connection Group can be created and connected simultaneously by connecting to a location.

To create a new Connection Group:



Right click on the **Location Name**  
Select **New**  
Select **Connection Group**



Enter **Name**  
Click **OK**



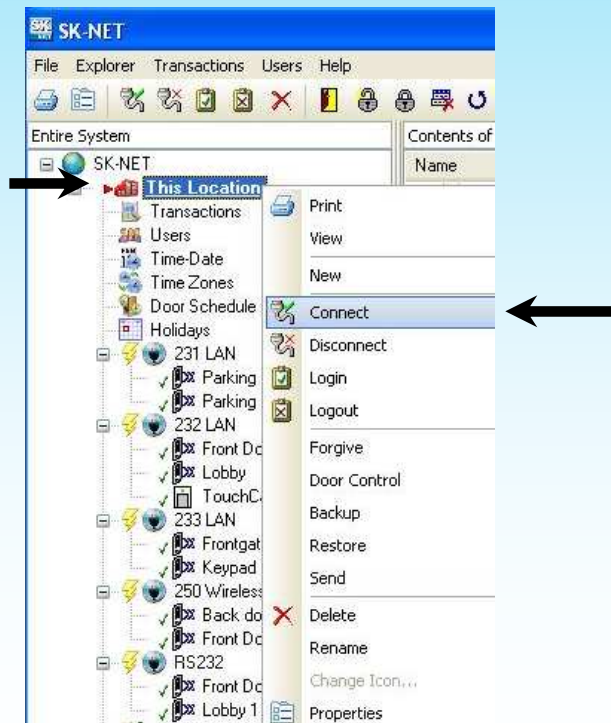
# Multiple Connections

When using multiple Connection Groups, you can connect to all Connection Groups at the same time. You may also connect to just one Connection Group at a time, this will be very helpful and save a lot of time while troubleshooting communications for a specific Connection Group.

**NEW**

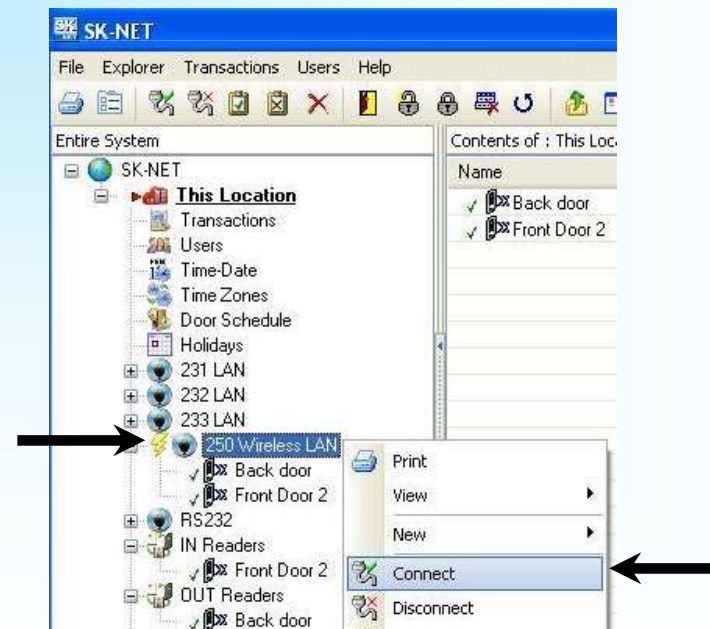
To connect to all Connection Groups.

Right click on the **Location Name**  
Select **Connect**



To connect to a single Connection Group.

Right click on the **Connection Group**  
Select **Connect**



Smart. Reliable. Secure.

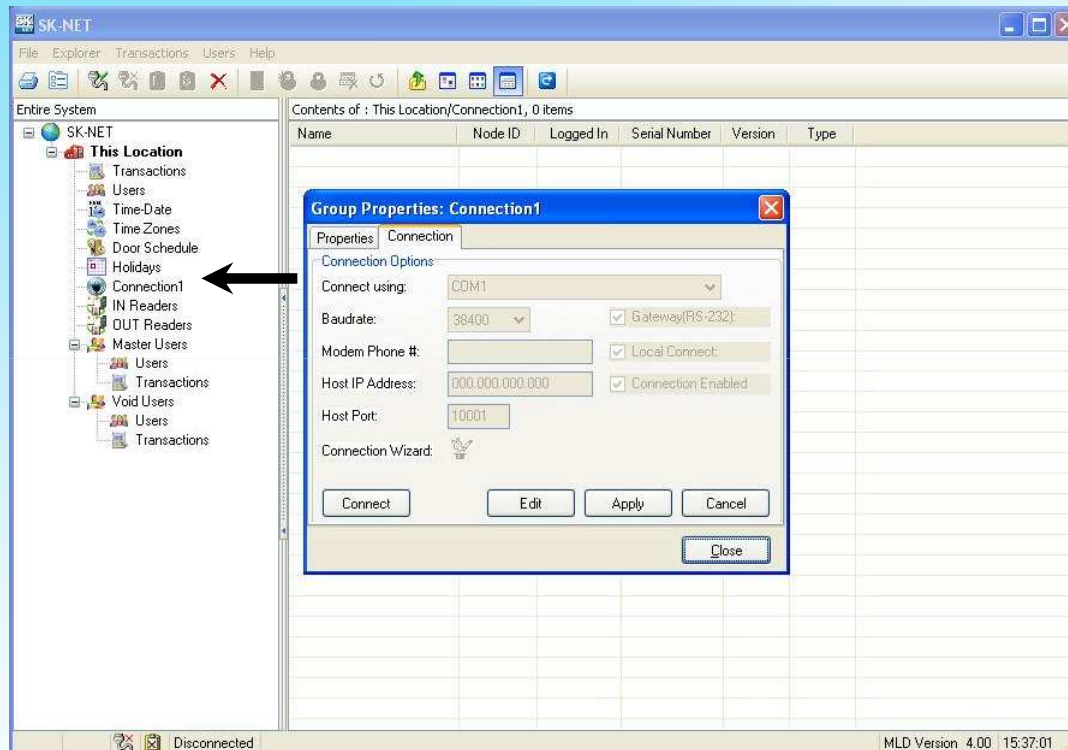
[Main Menu](#)

**Secura Key**  
A Division of SOUNDCRAFT Inc.

# Communications

The first thing to do is make a connection to find your readers using the “**Connection1 Group**”

To setup the communications:



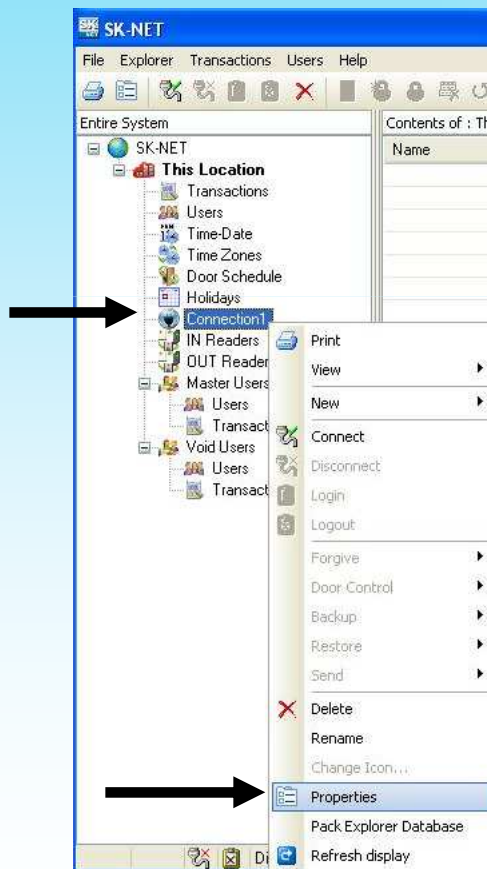
Enter the Connection Group:  
Right click on **Connection1**  
and select **Properties**

**Note:** You can rename the Connection Group. Just right click on **Connection1** and select **Rename**.

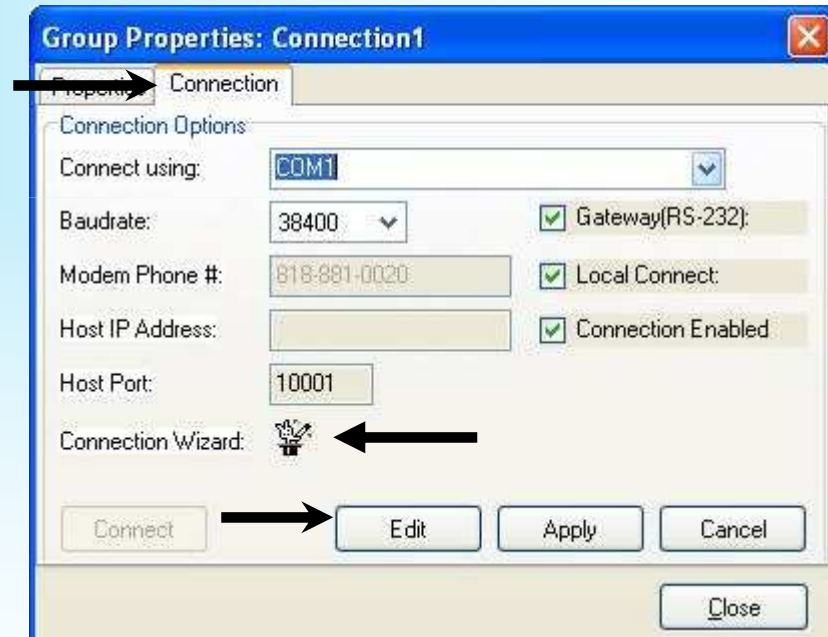


# Connection Wizard RS232

Making a connection for RS232 or RS485 using a converter. Right click on **Connection1** and select **Properties**



Click on the **Connection** tab  
To Run the Connection Wizard, click on **Edit**, then the **Connection Wizard**

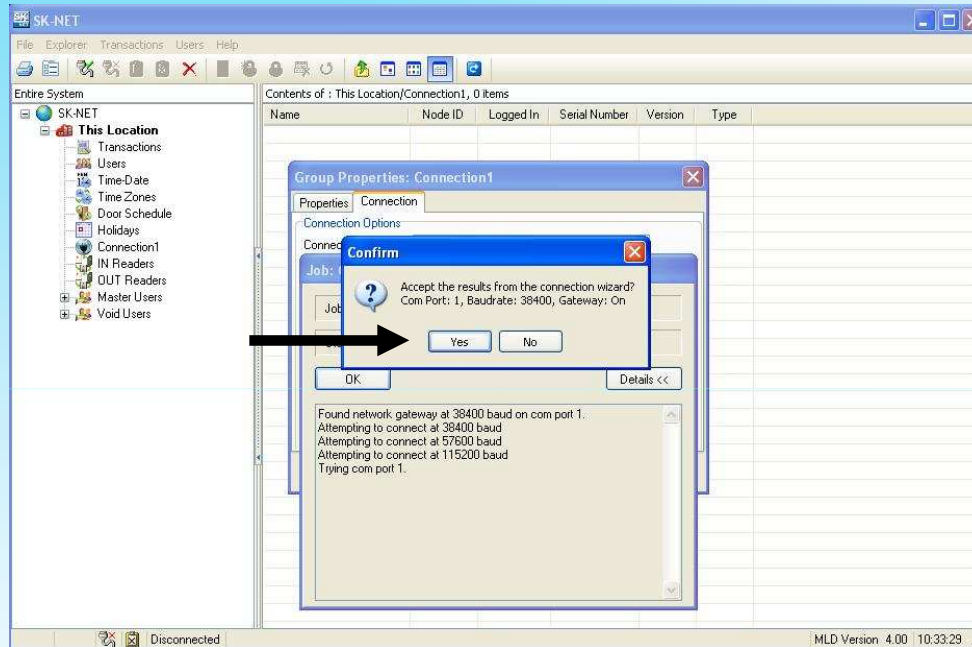


This will find the connection and then setup the proper com port and baud rate settings in the software.

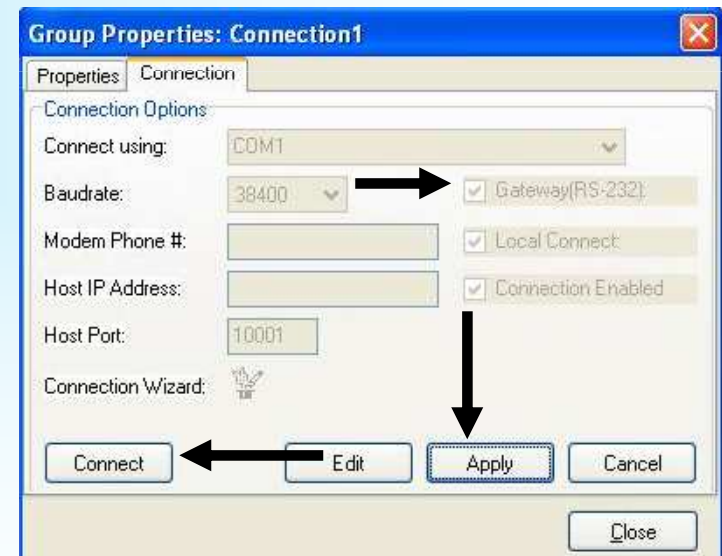
# RS232 Connection

Connection found.

Click on **Yes** to accept the settings



Select **Apply** and then **Connect** to find your readers



**Note:** When using a RS232 to RS485 converter, **Gateway RS232** is turned off.

Smart. Reliable. Secure.

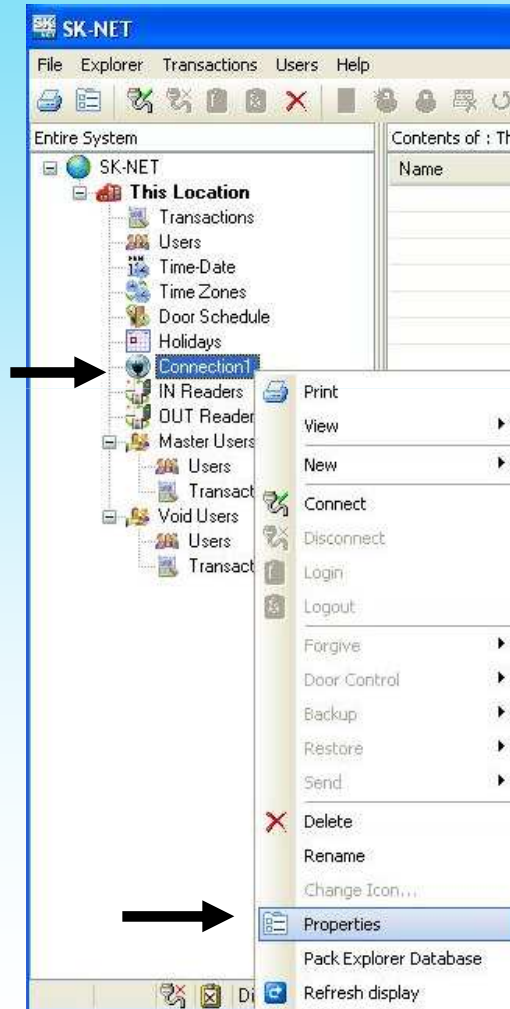
[Main Menu](#)

**Secura Key**  
A Division of SOUNDCRAFT Inc.

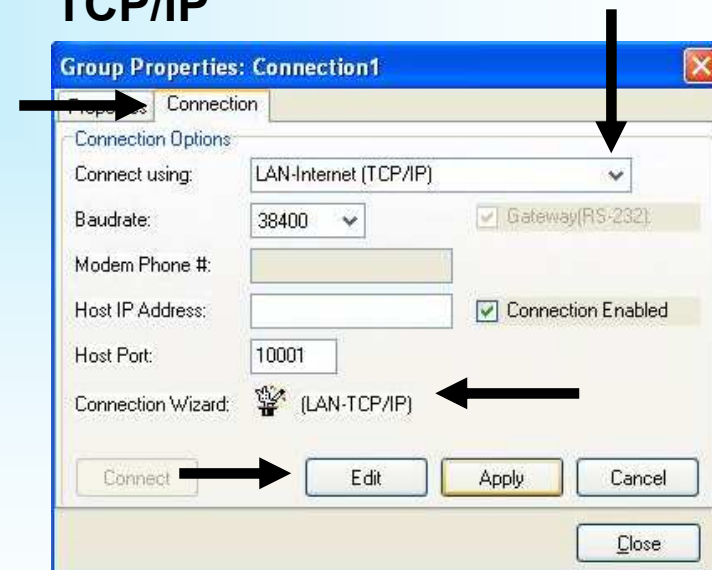
# Connection Wizard LAN

Making a connection for the LAN network device.  
Right click on **Connection1** and select properties

**NEW**



Select the **Connection** tab, click on **Edit**, select **LAN internet TCP/IP**



Run the LAN Connection Wizard

Smart. Reliable. Secure.

[Main Menu](#)

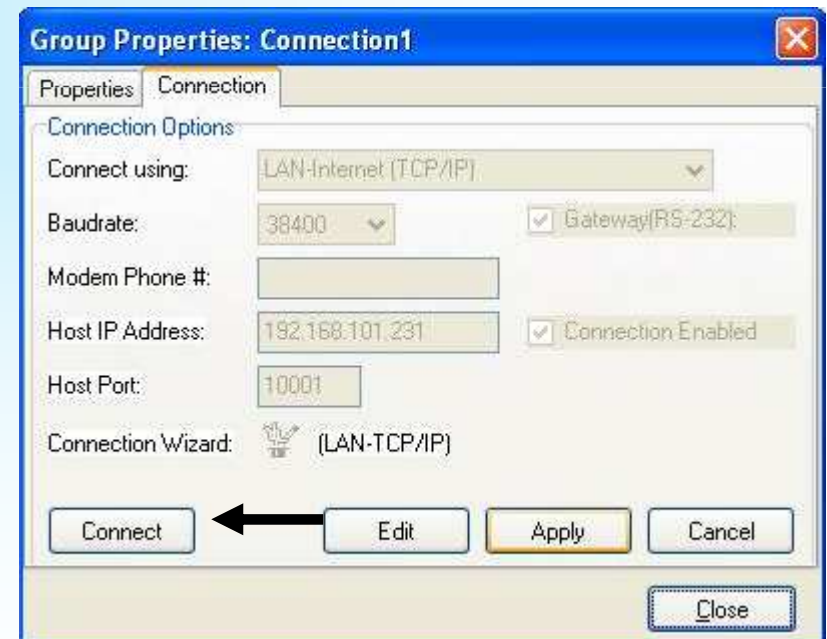
**Secura Key**  
A Division of SOUNDCRAFT Inc.

# LAN Connection

Select the proper LAN connection and click on **Accept**

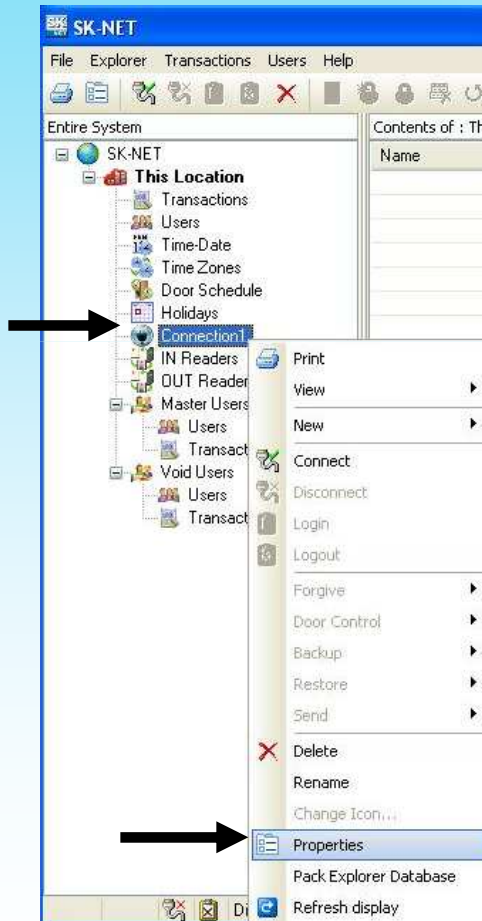


Select **Connect**

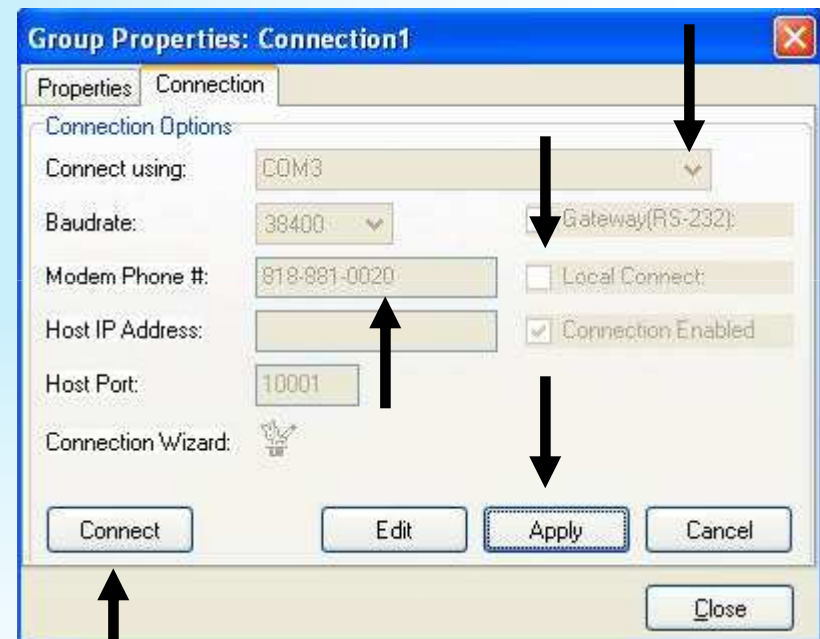


# Modem Connection

Making a connection for the Modem.  
Right click on **Connection1** and  
select **Properties**



Select the **Com Port** the modem is  
connected to



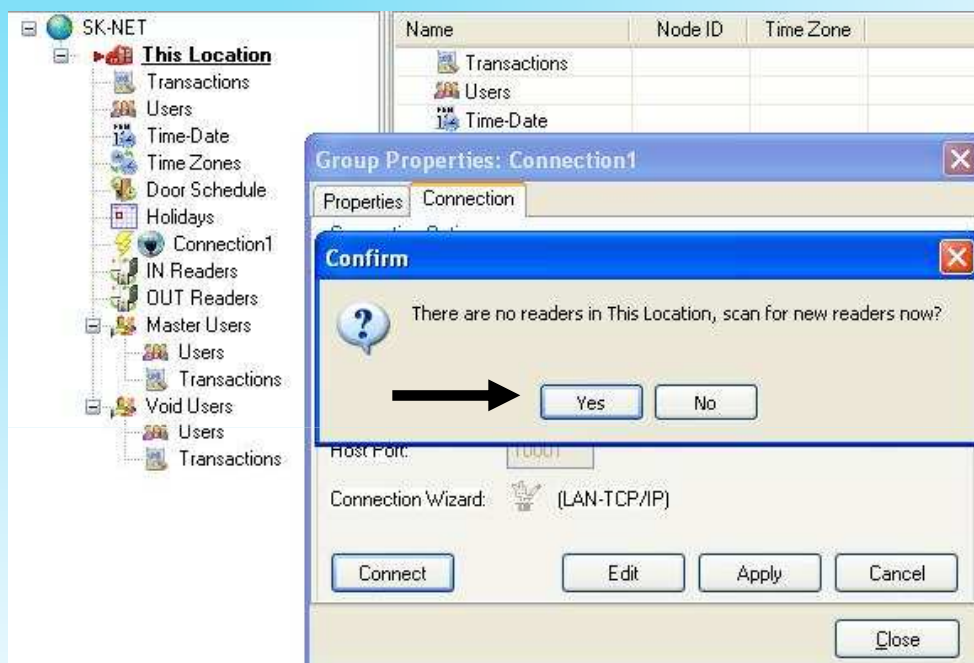
Uncheck **Local Connect**

Enter the **Modem Phone Number**, click  
on **Apply**, and select **Connect**

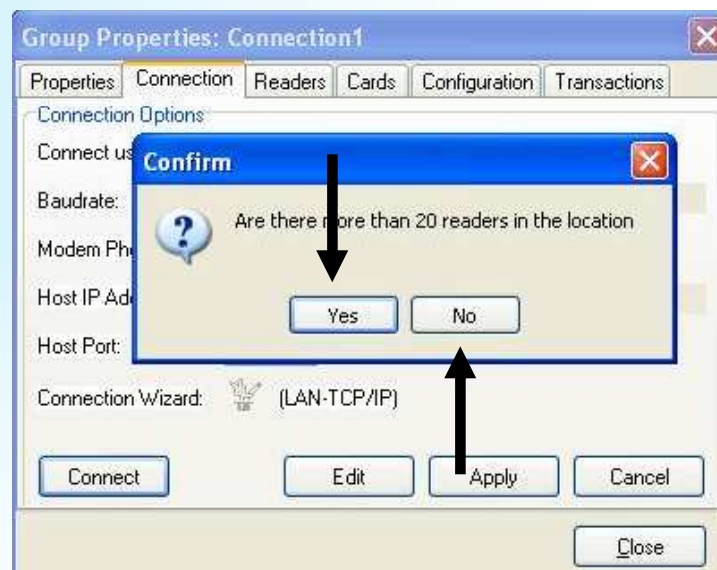


# Scan for new Readers

Select **Yes** to scan for new readers



More than 20 readers, **YES**

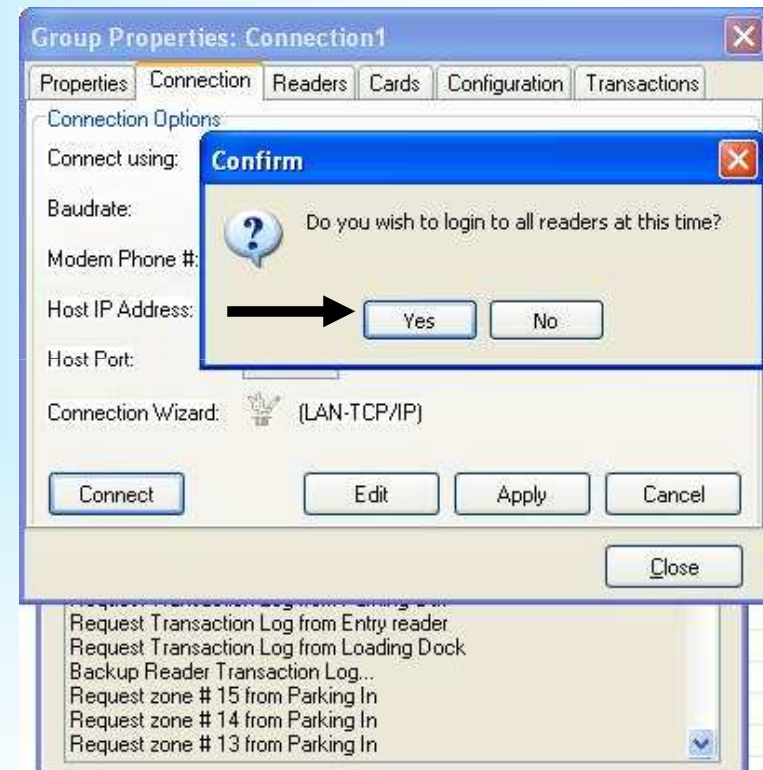
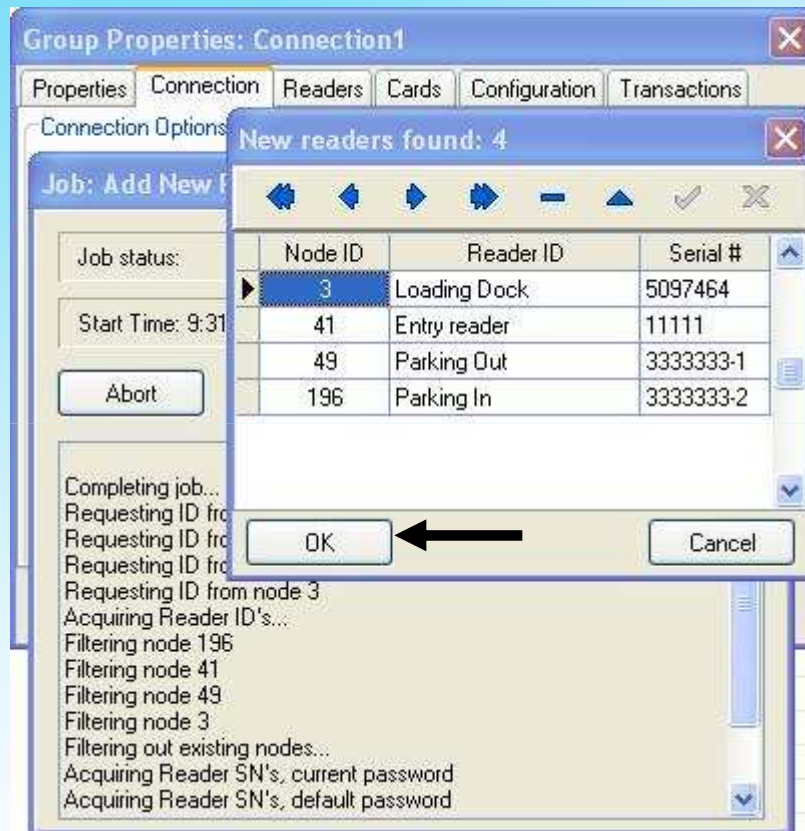


Less than 20 readers, **NO**



# New Readers Found

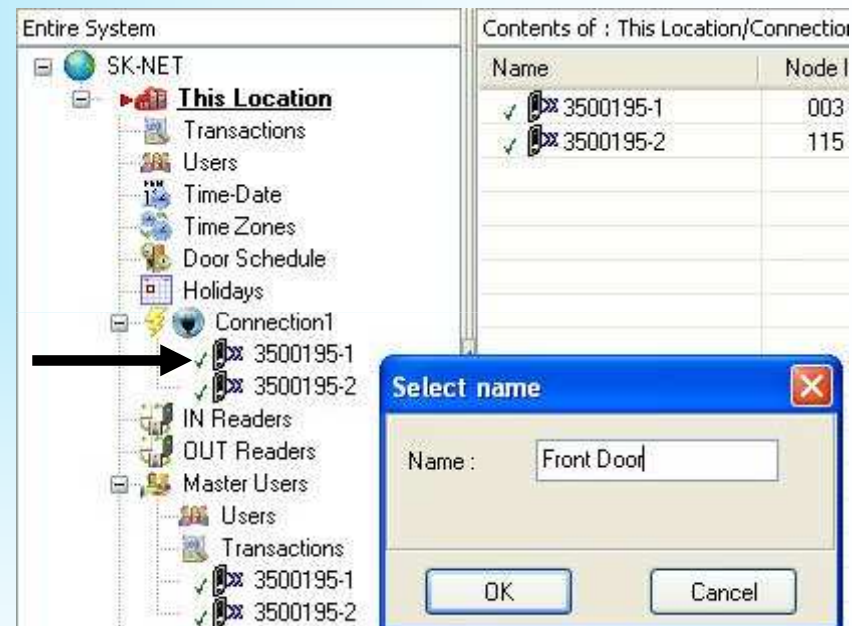
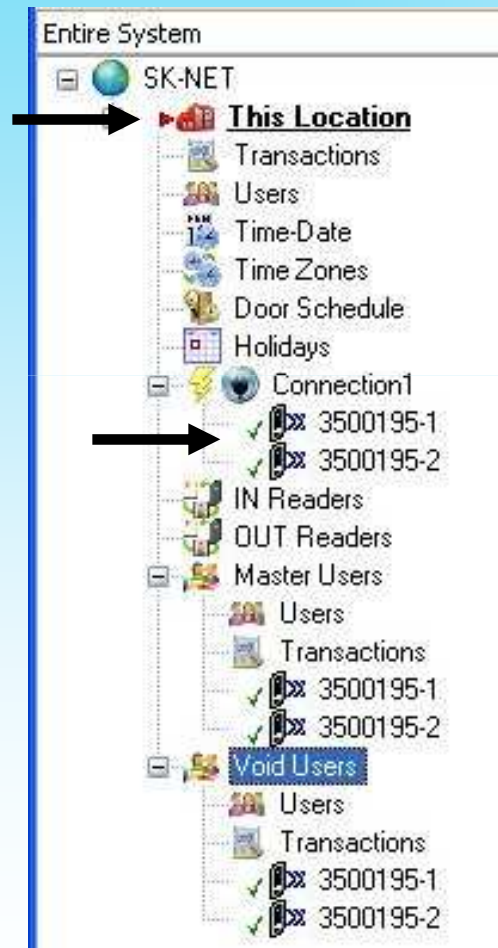
Click **OK** to bring the readers in to your system



Click **YES** to login, Login will download all stored transactions to the Transaction Screen

# Rename Readers

Red Arrow confirms you are connected to the location, the Green Check Marks confirms the readers are logged in.

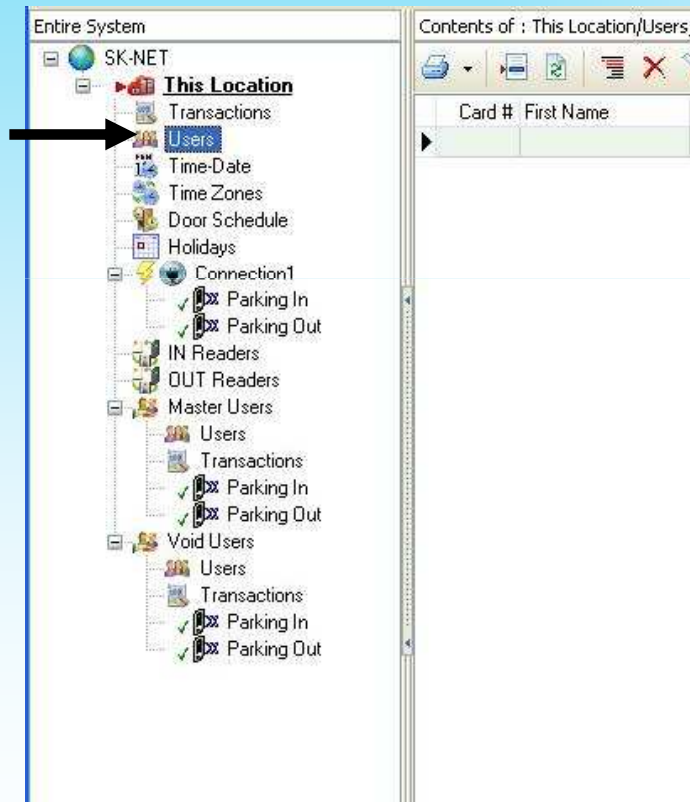


You can name your readers, just right click on the readers **Serial Number** and select **Rename**.  
The -1 serial number is connected to J5, and the -2 serial number is connected to J6.

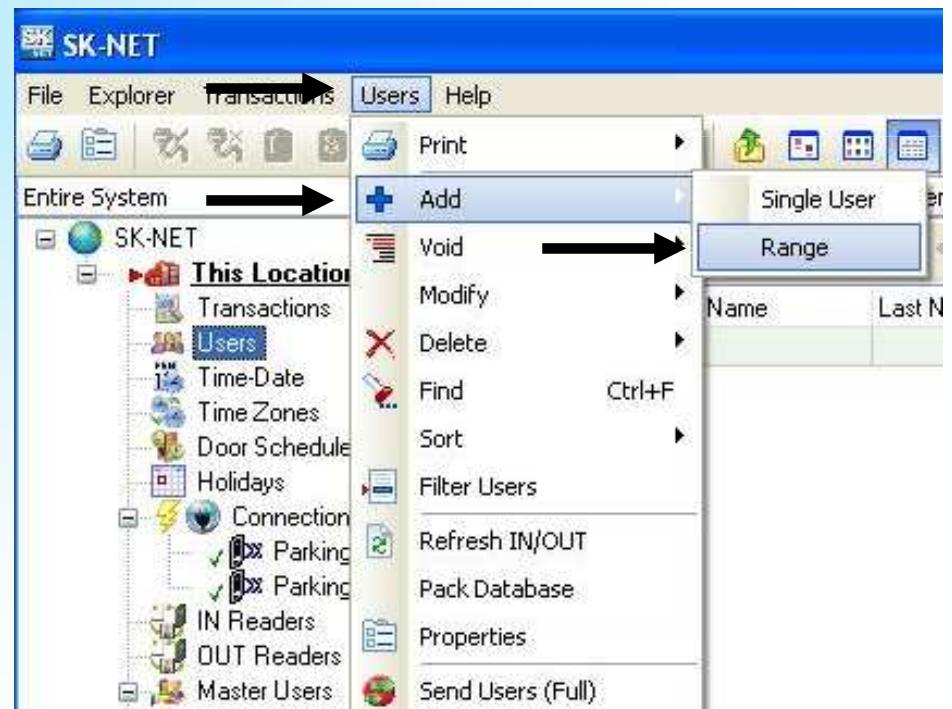
# User Manager

The User Manager displays all cards and associated cardholders. This is where you can add a card, edit card details, monitor In/Out status and generate user reports.

Select the User Manager by clicking on **Users**



Select **Users**, Select **ADD**, Select **Range**





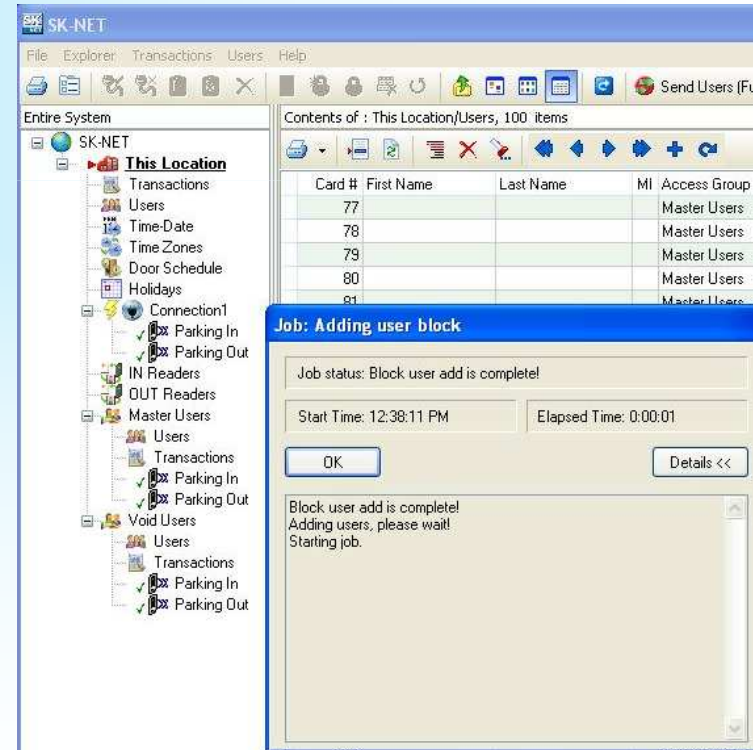
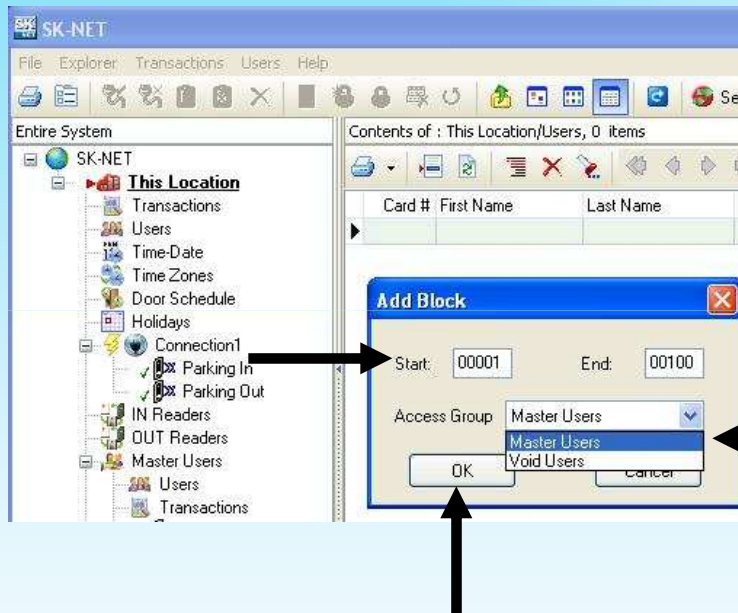
# Enter Range of Cards

Enter **Start** and **End** numbers

Select the proper **Access Group**

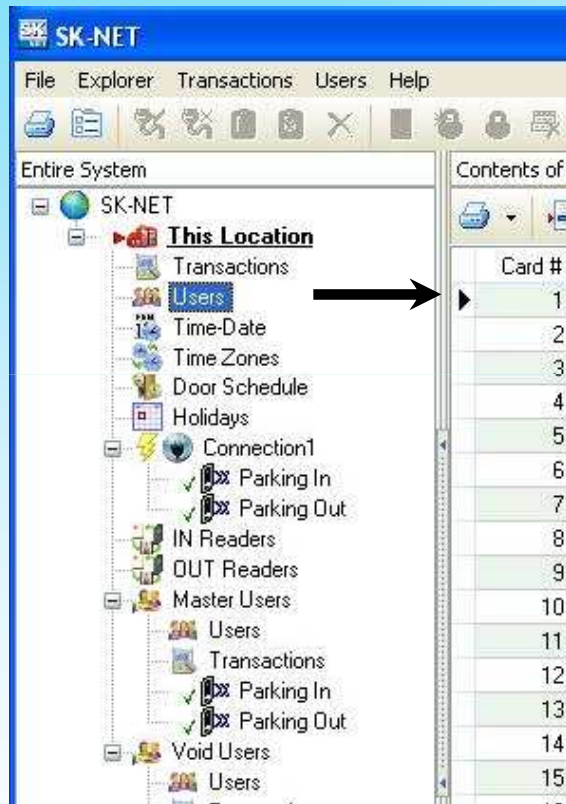
Click **OK**

Once the block of cards have been entered in to the **User Manager**, they are ready to be sent to the readers, or add the users information.



# User Properties

To enter the users information just point to the users **Card Number** and double click

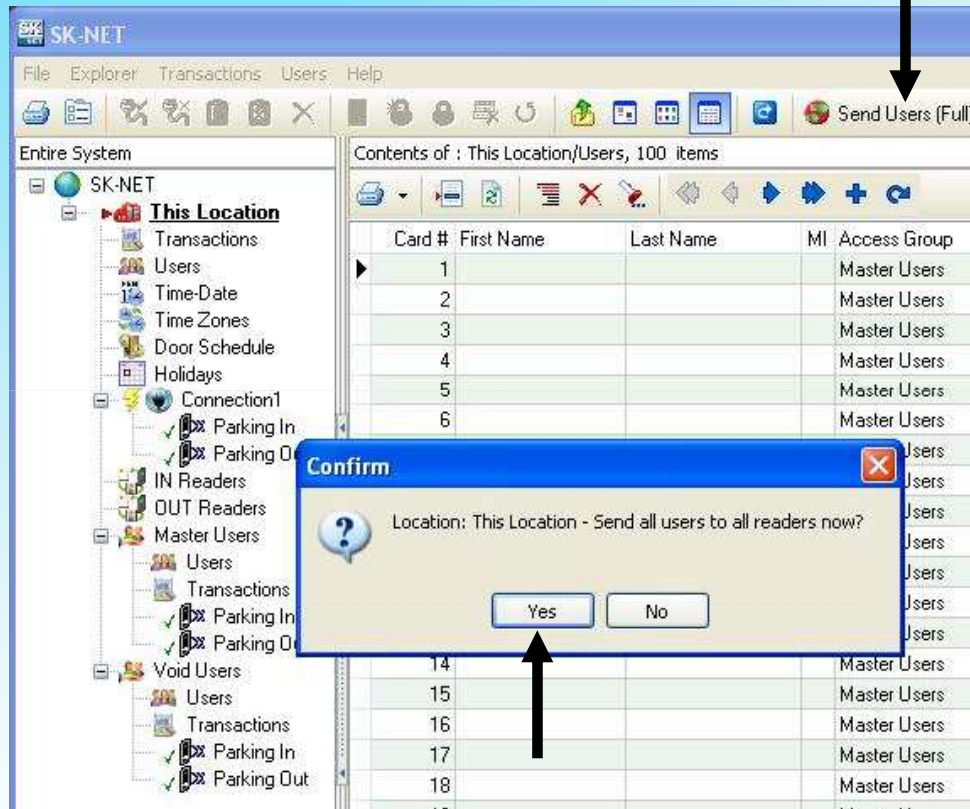


Enter all the **Users** information.  
Select the proper **Access Group**

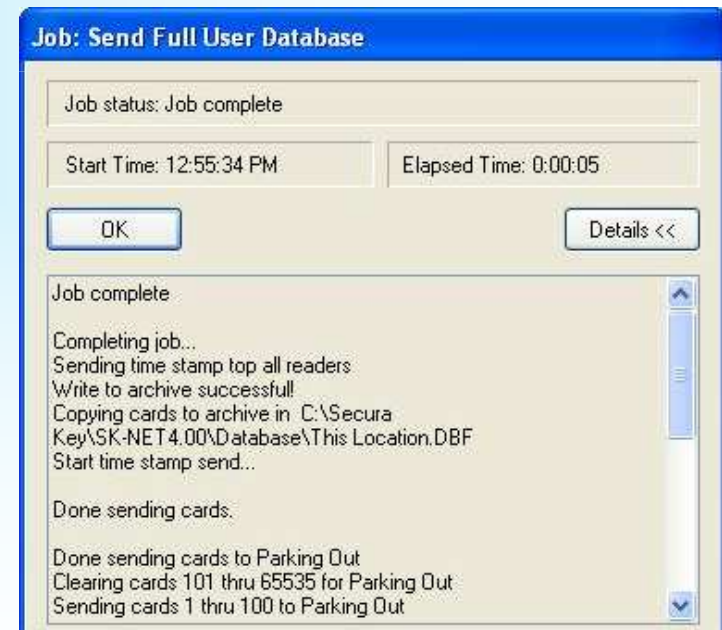
SK-NET also supports a photo for each user, just click on **Load**, and enter any photo in the **JPG Format**

# Card Send

After you have connected and logged in to the readers, the **Send Users Full** icon appears



Just left click on the (**Send Users Full**) icon to Send all users to all the readers now? Then select **Yes**

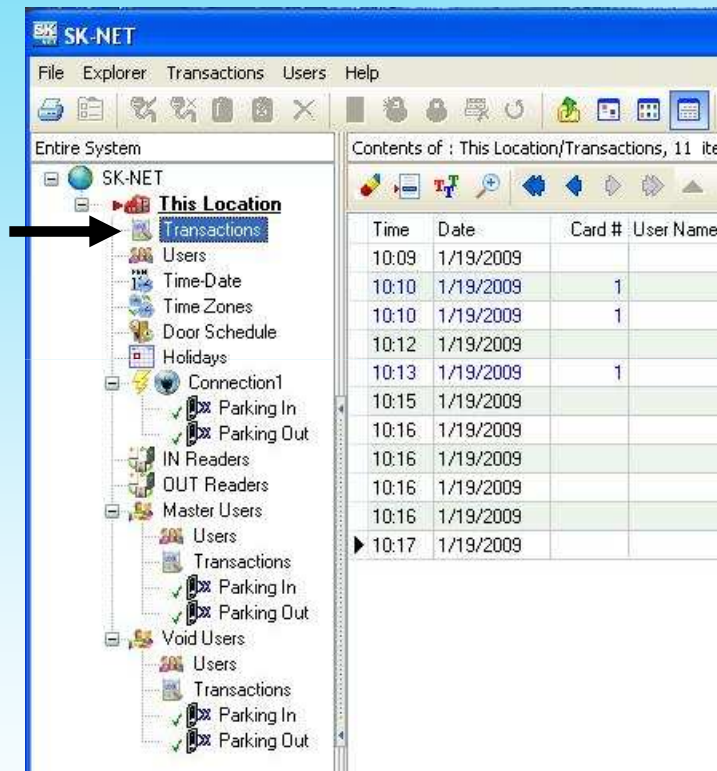




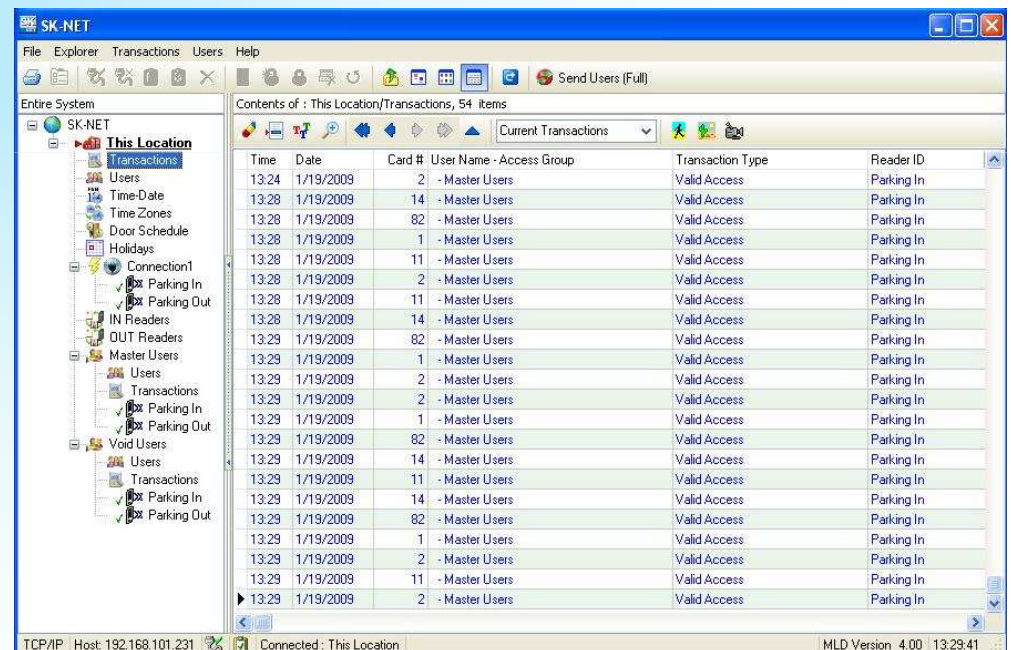
# Testing the System

To test the cards you have just programmed in to your system, take one of the cards and read it a couple of times on each reader to verify it works.

## Select Transactions



Look at the transactions, you will see the Time, Date, Card Number, Users name if already entered, Access Group, Transaction Type, Reader Name.



Verify that all transactions are valid.

# Transaction Screen

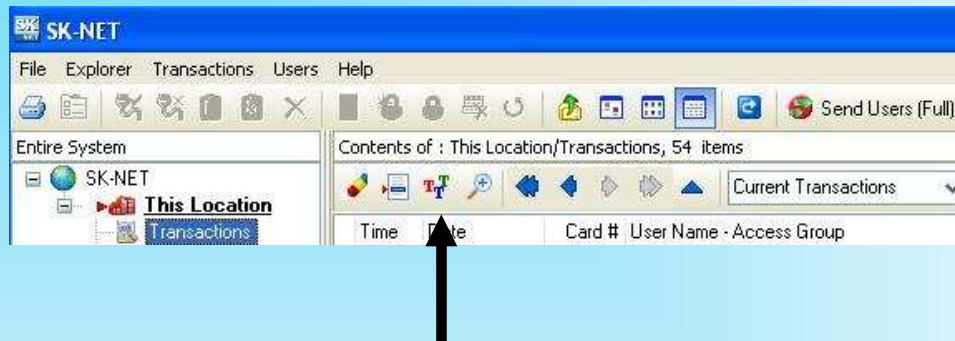
The Transaction screen displays all system activity. Card events that are valid, system violations such as void cards, and system generated events such as door opened via PC. Transactions are displayed in a list, with the most recent event displayed at the bottom of the screen. There are many different filters available to generate specialized reports which can be printed in color.

The screenshot shows the SK-NET software interface. The left sidebar displays a tree view of the system structure, including 'This Location', 'Users', 'Time-Date', 'Time Zones', 'Door Schedule', 'Holidays', 'Connection1', 'Parking In', 'Parking Out', 'IN Readers', 'OUT Readers', 'Master Users', 'Users', 'Transactions', 'Void Users', and 'Users'. The main window displays a table of transactions for 'This Location/Transactions, 54 items'. The table has columns for Time, Date, Card #, User Name - Access Group, Transaction Type, and Reader ID. The transactions are listed in descending order of time, with the most recent at the bottom. The status bar at the bottom shows 'TCP/IP Host: 192.168.101.231', 'Connected : This Location', and 'MLD Version 4.00 13:29:41'.

Time	Date	Card #	User Name - Access Group	Transaction Type	Reader ID
13:24	1/19/2009	2	- Master Users	Valid Access	Parking In
13:28	1/19/2009	14	- Master Users	Valid Access	Parking In
13:28	1/19/2009	82	- Master Users	Valid Access	Parking In
13:28	1/19/2009	1	- Master Users	Valid Access	Parking In
13:28	1/19/2009	11	- Master Users	Valid Access	Parking In
13:28	1/19/2009	2	- Master Users	Valid Access	Parking In
13:28	1/19/2009	11	- Master Users	Valid Access	Parking In
13:28	1/19/2009	14	- Master Users	Valid Access	Parking In
13:29	1/19/2009	82	- Master Users	Valid Access	Parking In
13:29	1/19/2009	1	- Master Users	Valid Access	Parking In
13:29	1/19/2009	2	- Master Users	Valid Access	Parking In
13:29	1/19/2009	2	- Master Users	Valid Access	Parking In
13:29	1/19/2009	1	- Master Users	Valid Access	Parking In
13:29	1/19/2009	82	- Master Users	Valid Access	Parking In
13:29	1/19/2009	14	- Master Users	Valid Access	Parking In
13:29	1/19/2009	11	- Master Users	Valid Access	Parking In
13:29	1/19/2009	14	- Master Users	Valid Access	Parking In
13:29	1/19/2009	82	- Master Users	Valid Access	Parking In
13:29	1/19/2009	1	- Master Users	Valid Access	Parking In
13:29	1/19/2009	2	- Master Users	Valid Access	Parking In
13:29	1/19/2009	11	- Master Users	Valid Access	Parking In
13:29	1/19/2009	2	- Master Users	Valid Access	Parking In

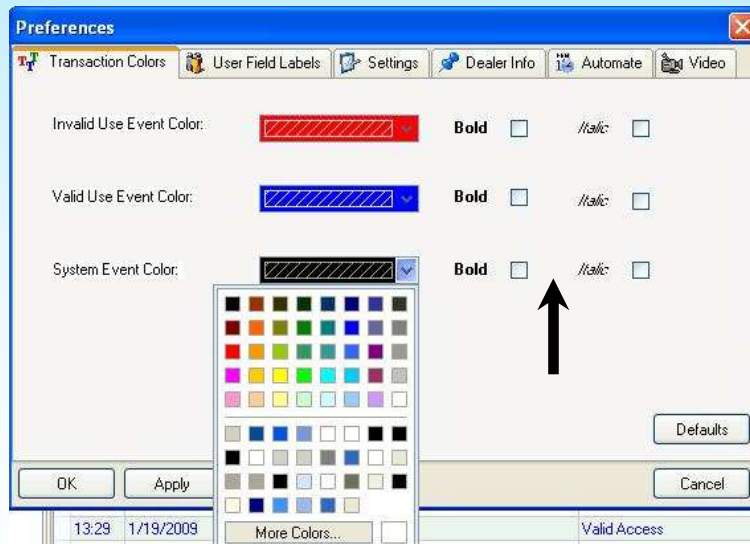
# Transaction Type Colors

Select the **Change Colors** Icon



New

Font style either in Bold or Italic.  
Just click on the appropriate box.



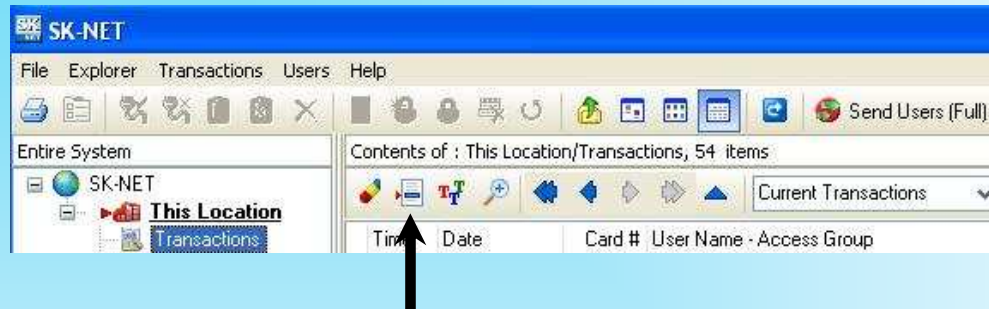
By having different colors available it is easy to recognize the different event types with a quick view of the transaction screen.

Red is a good choice for **Invalid Use** or **System Violations**. You know that something is wrong with a quick glance of the transaction screen.



# Transaction Filters

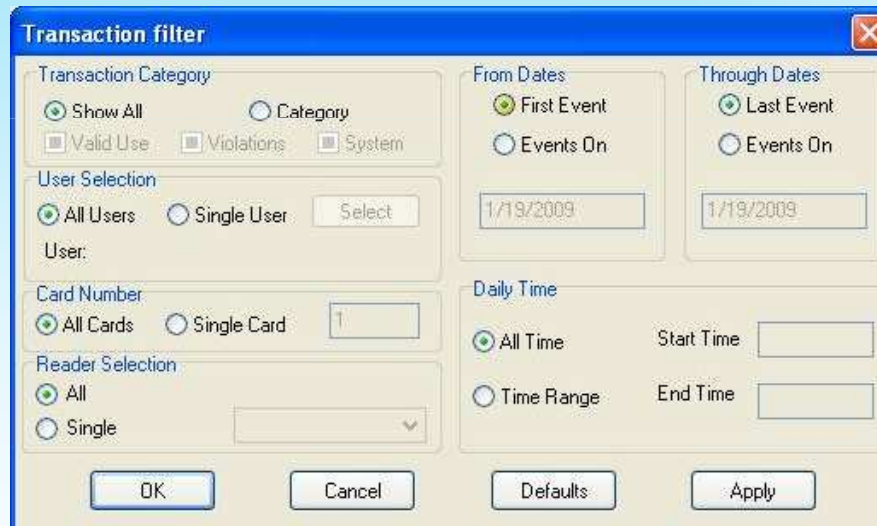
Select the **Filter** Icon



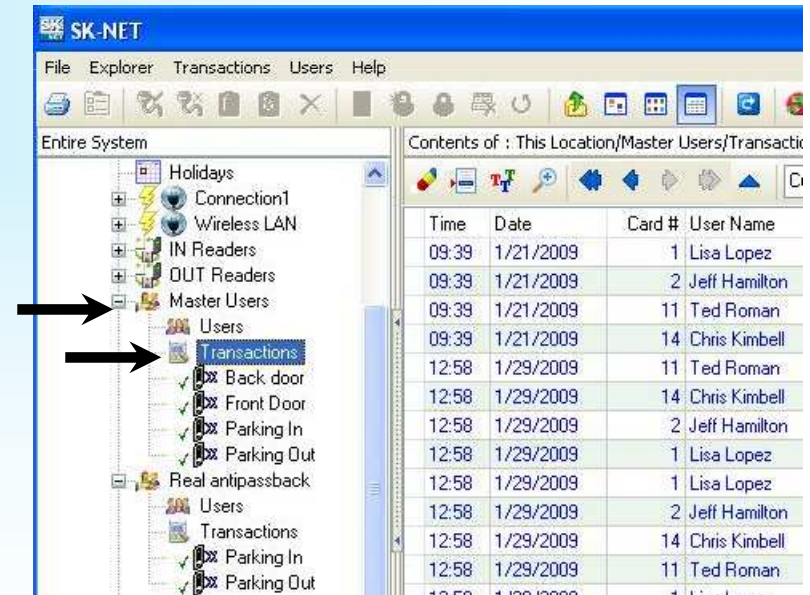
**NEW**

Quick Transaction Filter for any Access Group.

Select an Access Group  
Select Transactions



The **Transaction Filter** screen allows you to select any combination of filters to generate your customized reports.



Smart. Reliable. Secure.

[Main Menu](#)

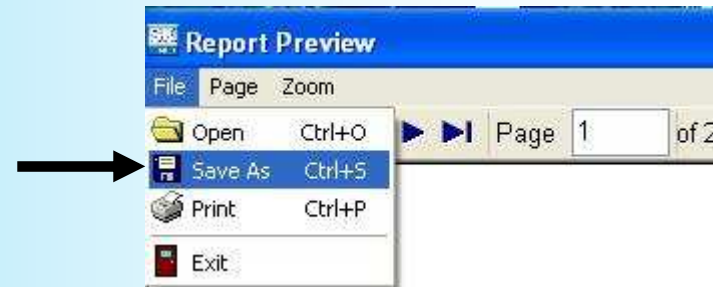
**Secura Key**  
A Division of SOUNDCRAFT Inc.

# Print Reports

Select the **Printer** Icon



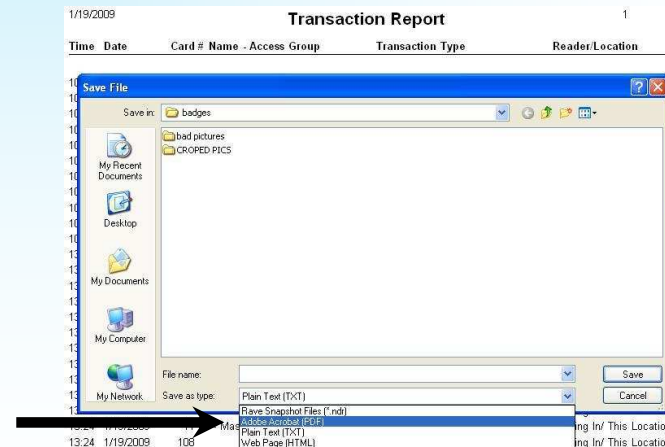
Select **Save As**



Select **Preview** to show report on the screen



You can either Print the report, or save the report in a **PDF or XLS** (Excel) format to be saved or sent by e-mail



Smart. Reliable. Secure.

[Main Menu](#)

**Secura Key**  
A Division of SOUNDCRAFT Inc.

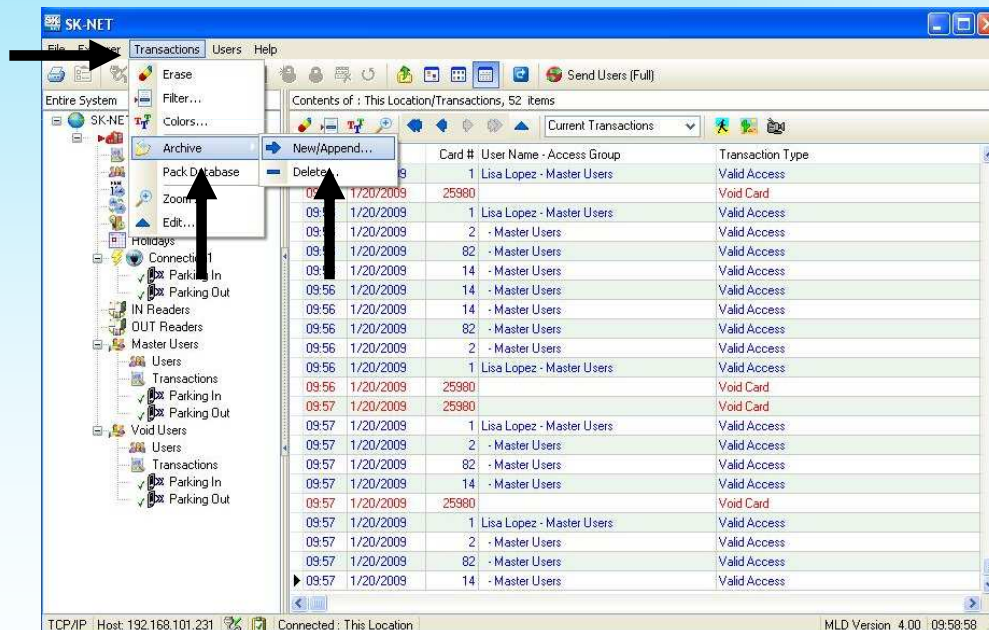
# Archive Transactions

It is a good idea to archive your transactions, if the file gets too large it will start to slow down your PC. It is recommended depending on how much activity your system has to archive monthly, or by each quarter.

Left click on **Transactions**

Select **Archive**

Select **New/Append**



Append will add these files to an existing file, or you may start with a new one.



Smart. Reliable. Secure.

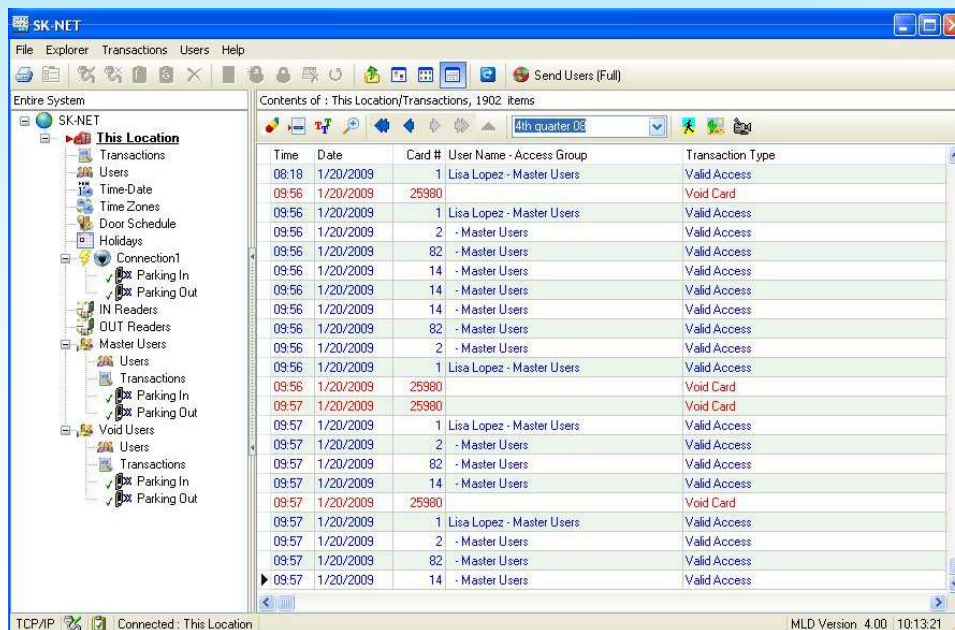
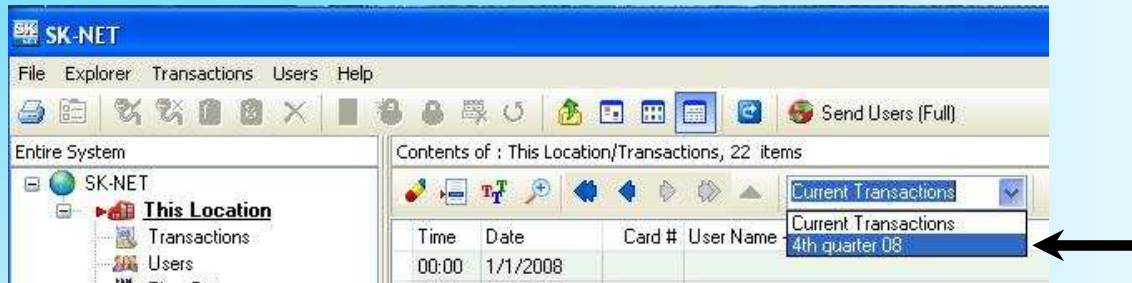
[Main Menu](#)

**Secura Key**  
A Division of SOUNDCRAFT Inc.



# Viewing Archived Transactions

Select archived file



After retrieving the archived file, you can use any of the filters required to generate custom reports as needed.

Smart. Reliable. Secure.

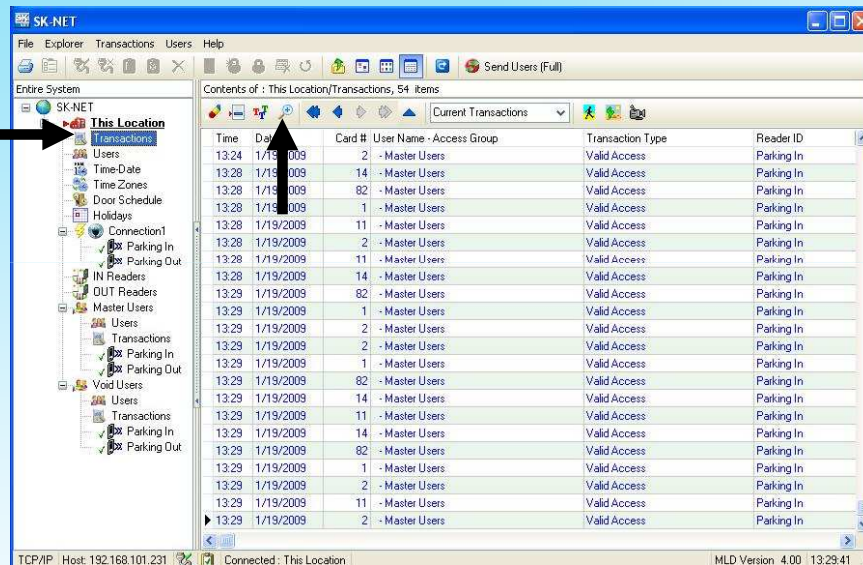
[Main Menu](#)

**Secura Key**  
A Division of SOUNDCRAFT Inc.

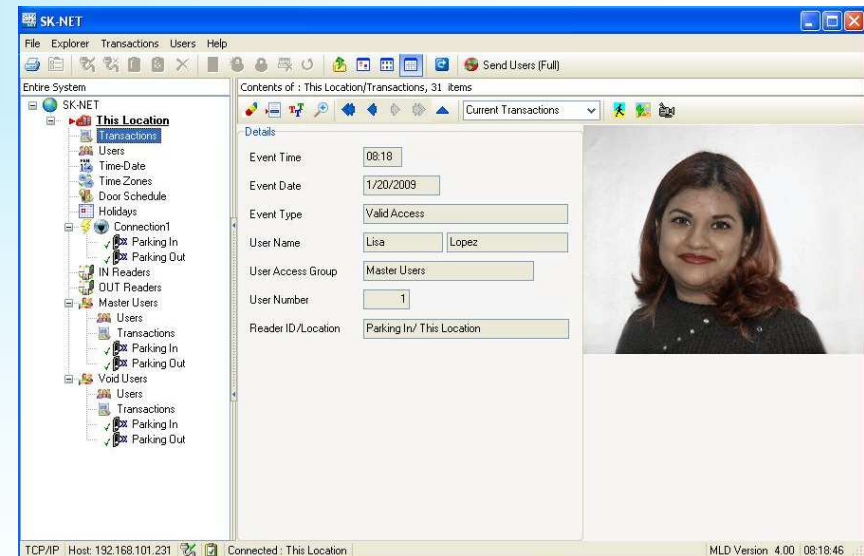
# View Single Transaction

You can view the details of a single transaction including a photo with two clicks of the mouse.

Just left click on the **Transactions**  
Left click on the **Zoom** Icon



This view is important if you want to verify the person entering is the correct card user.



**Note:** There must be a photo entered into the User Properties.

Smart. Reliable. Secure.

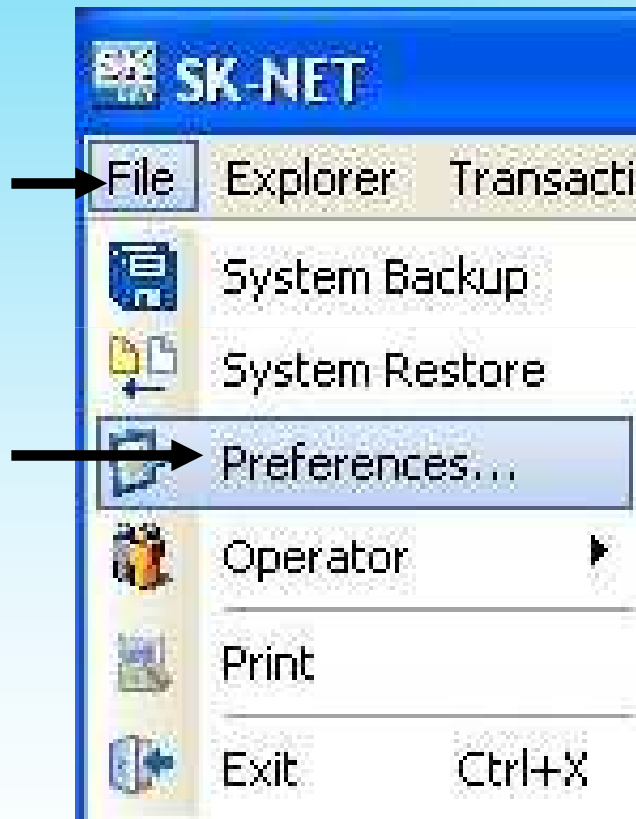
[Main Menu](#)

**Secura Key**  
A Division of SOUNDCRAFT Inc.

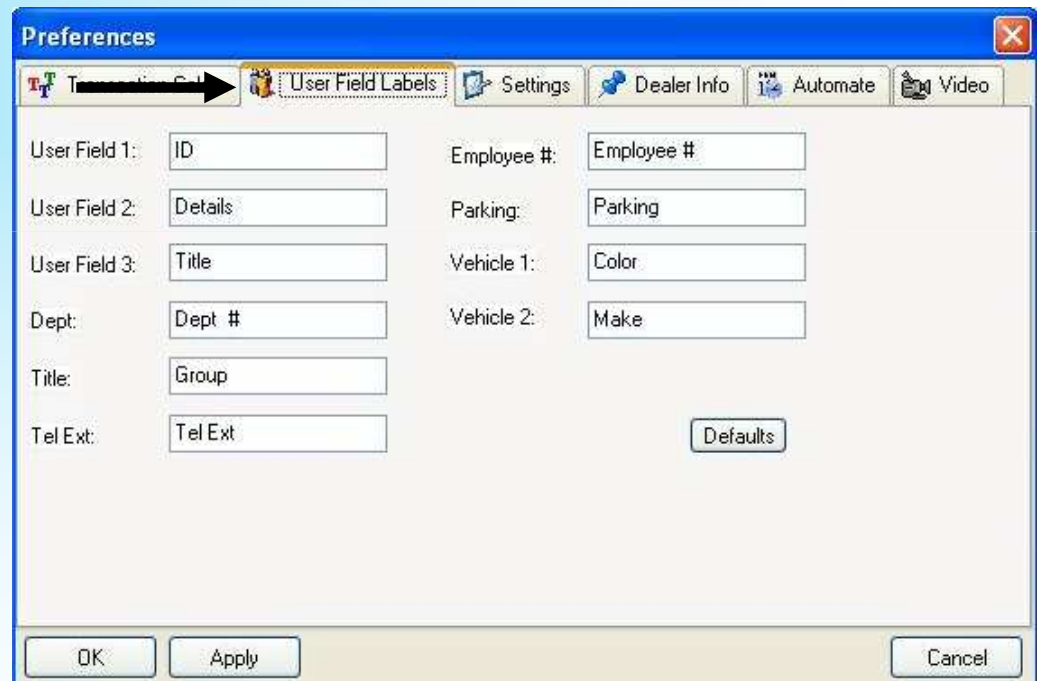
# Customize User Fields

If the current User Fields do not match your needs, then you may change them.

Just left click on **File**  
Select **Preferences**



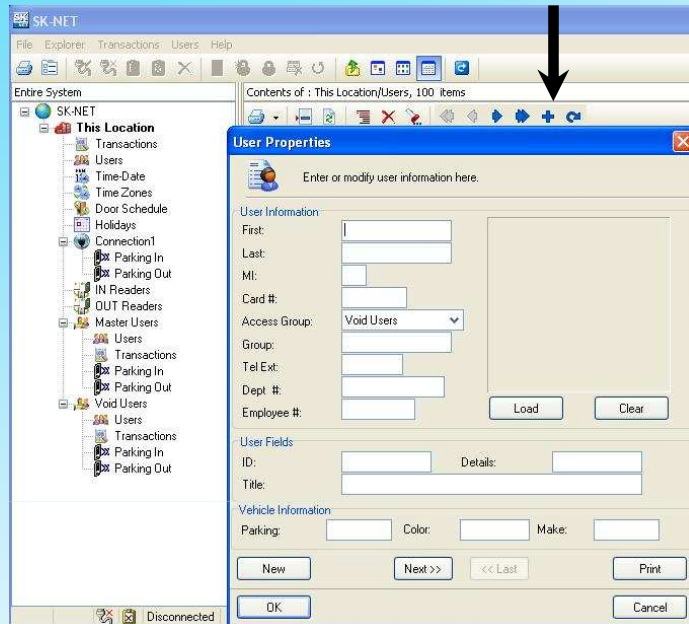
Select the **User Field Labels** tab



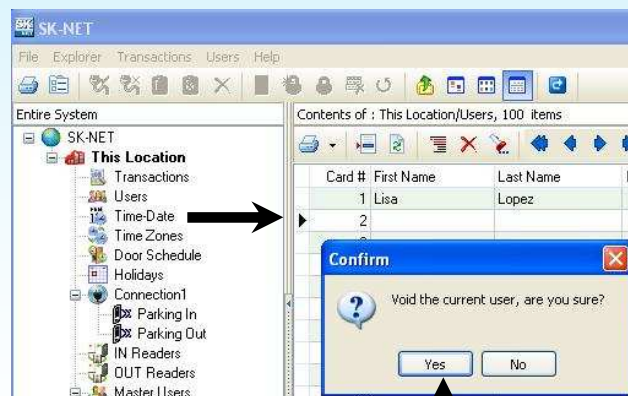
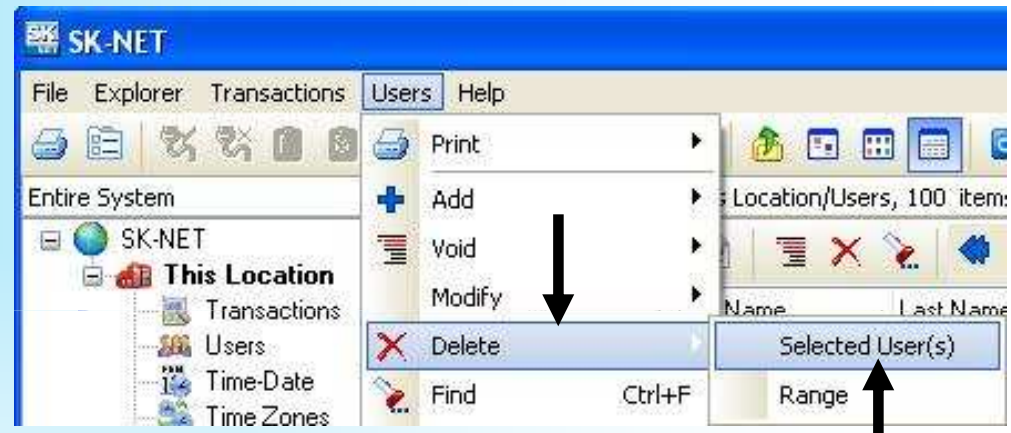
In the **Preferences Screen**, just edit each field you would like to change.

# Add/Delete or Void Single User

To add a single user, Left click on the +



To delete a user, select the **User Number**  
Select **Delete**, then click on **Selected Users**



To void a user right click on the **User**, select **Void**  
Click on **Yes**, then send **Users Full**

**NOTE:** If a User keeps their card, it is best add the card number to the **Void Users** group in case they try to gain entry again. This way it shows the name of user in the transaction screen.

Smart. Reliable. Secure.

[Main Menu](#)

**Secura Key**  
A Division of SOUNDCRAFT Inc.

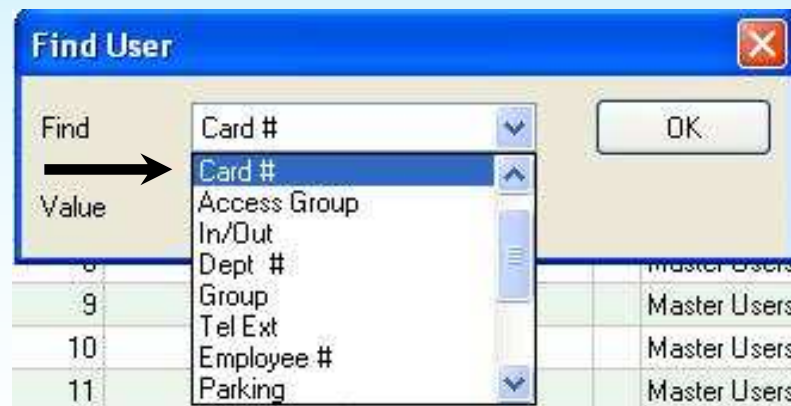


# Find User

Click on the **Find User** icon



Select the desired **Filter Value**



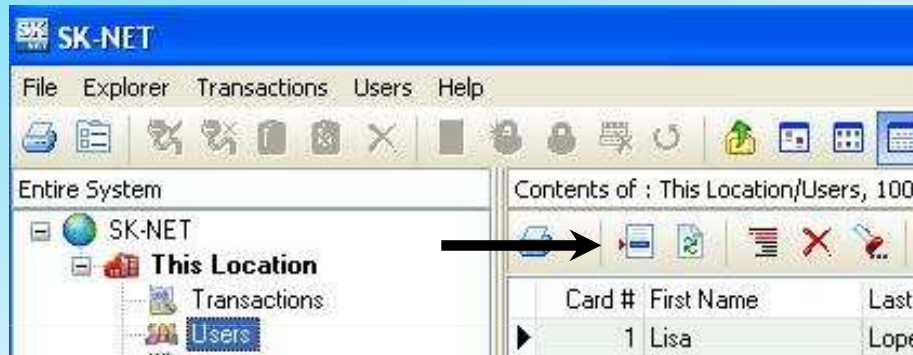
Enter the **Value** for your search



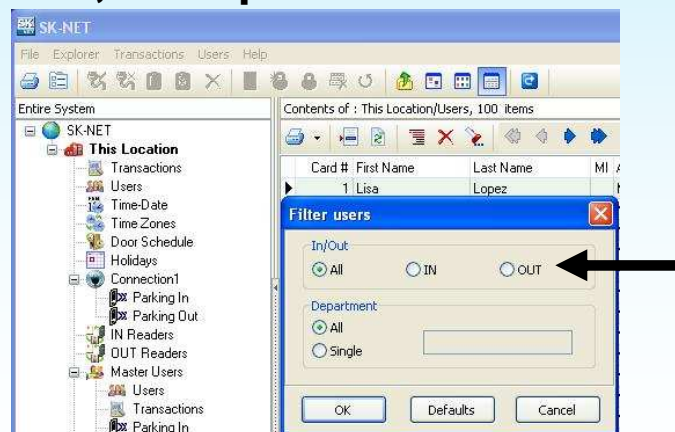
# Filter Users

Filters allow you to temporarily remove unwanted records from the list. This allows a limited user report to be generated, for example, users in a single department or users who are out of the building.

Click on the **Filter Users** icon



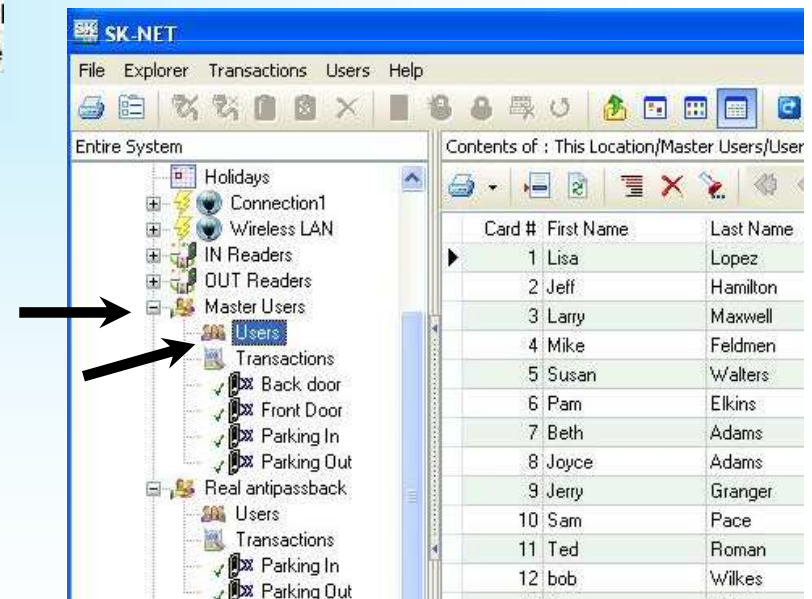
In the Filter Users detail box, select **IN**, **OUT**, or **Department**



**NEW**

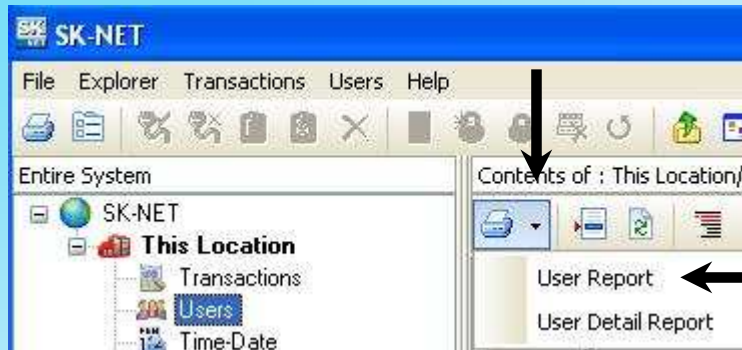
Quick **Users** Filter for any **Access Group**.

Select an **Access Group**  
Select **Users**





# User Report



To print a User Report left click on the **Printer** icon down arrow  
Select **User Report**

## Select Printer



2/26/2008

Secura Key Tag/User Report

File Options Navigator

Close 100% Page: 1/3 100.0%

User Report

Card #	Last Name	First Name	MI	Dept	Access Grp	In/Out	Title	Tel Ext	Employee #
1	Lopez	Maria	L	Production	Master Users		Operator	334	1255135
2	Hamilton	Jeff		Engineering	Master Users		Techsupport Eng	331	1239431
3	Ruby	Dave			Master Users				
4	Smith	Jim			Master Users				
5	Winn	Cathy			Master Users				
6	Culver	Porter			Master Users				
7	Watkins	Randy			Master Users				
8	Haskel	Brandon			Master Users				
9	Jones	William			Master Users				
10	Nunn	Tracy			Master Users				
11	Maxwell	Larry		Production	Master Users		Technician	335	1237765
12	Jones	Sherry		Manufacturing	Master Users		Operator	332	1238847
13	Olivens	Berry			Master Users				

# User Detail Report



To print a **User Detail Report** left click on the **Printer** icon down arrow  
Select **User Detail Report**

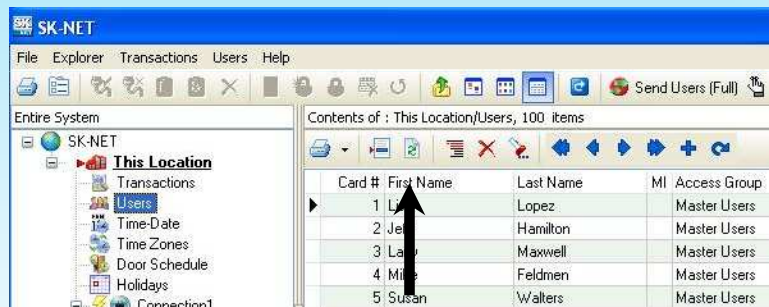
## Select Printer



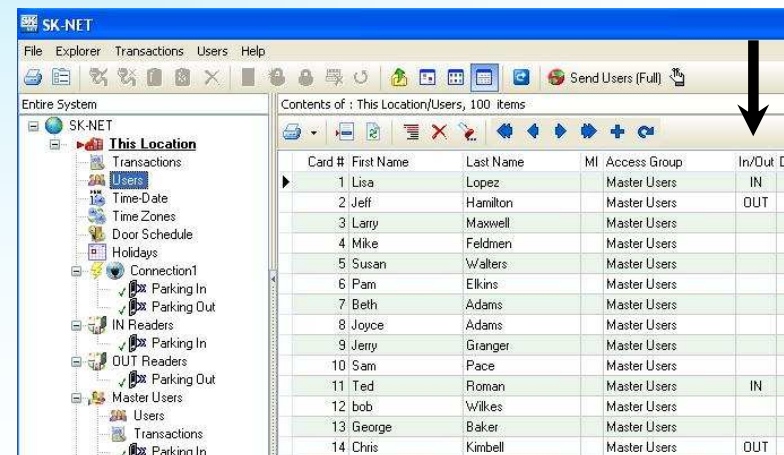
# IN/OUT Status

SK-NET™ automatically creates a Reader Group for IN readers and OUT readers. If you have defined your readers in these groups, you can check the IN/OUT status of your users right from the User Screen.

If you are just starting SK-NET™ you can view the IN/OUT status for the users who have already entered or exited by left clicking on the **Refresh IN/OUT** status icon. If you are already logged in, then the user screen is automatically updated with each card read.

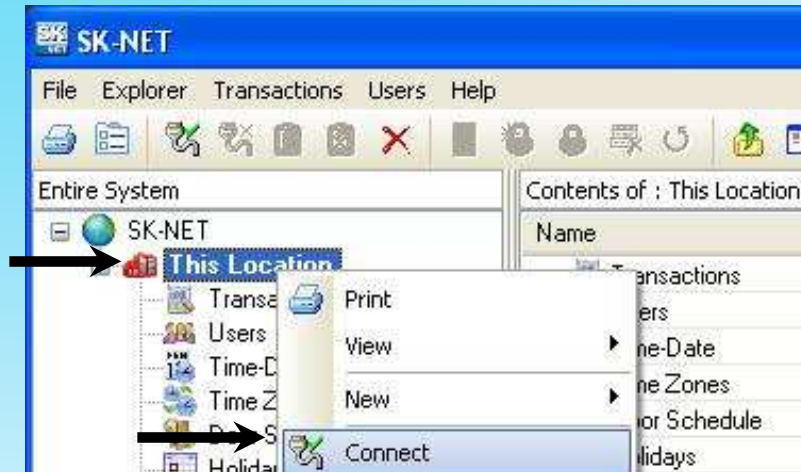


To view who is IN or Out, just look at the IN/OUT column in the **User Screen**

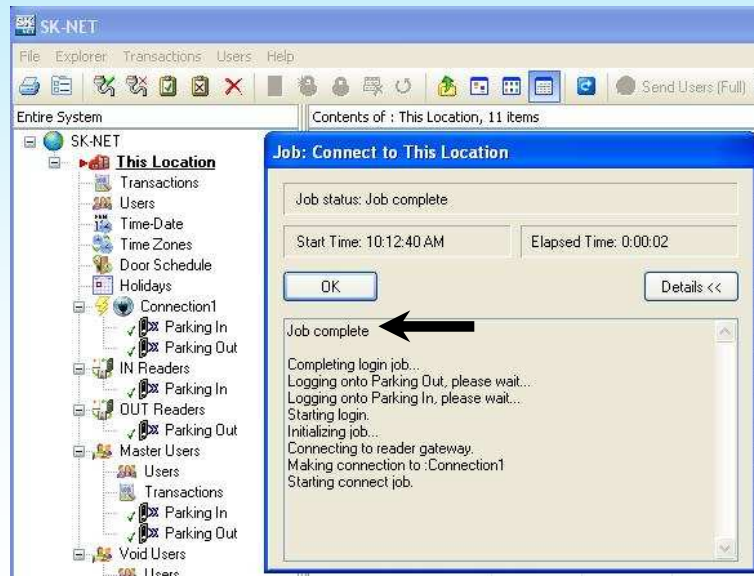


**Note:** If a users card has not been used in the last 24 hours, there will be no **In** or **Out** status.

# Connecting to a Location



To Connect to a Location, right click on the **Location Name**  
Select **Connect**



This **Location** is setup to automatically **Login**

**Note:** If you are Connected to a Location, and exit the software, it will automatically connect the next time you start SK-NET™.



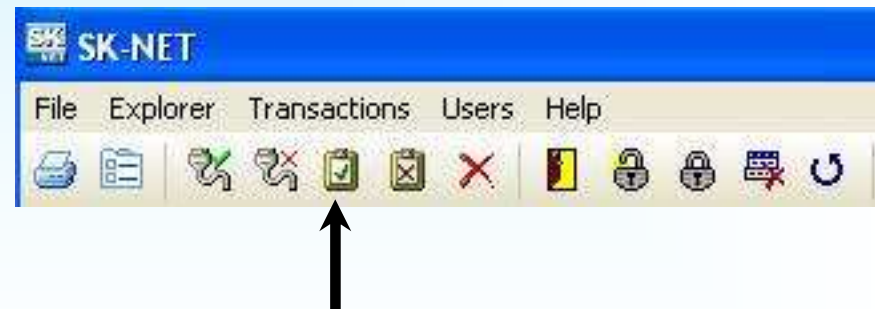
# Login to Readers

**Logging in** tells all the readers to download all stored transactions in memory (from the last time you were connected) of each reader to the transaction screen. Once you have connected to the location, any live transactions will automatically be sent to your transaction screen. Once a transaction has been sent to the transaction screen, it can not be sent again.

To set Auto Login right click on **Location Name** and select **Properties**, then check the **Auto Login** box



To manually Login, after connecting left click on the **Login** icon



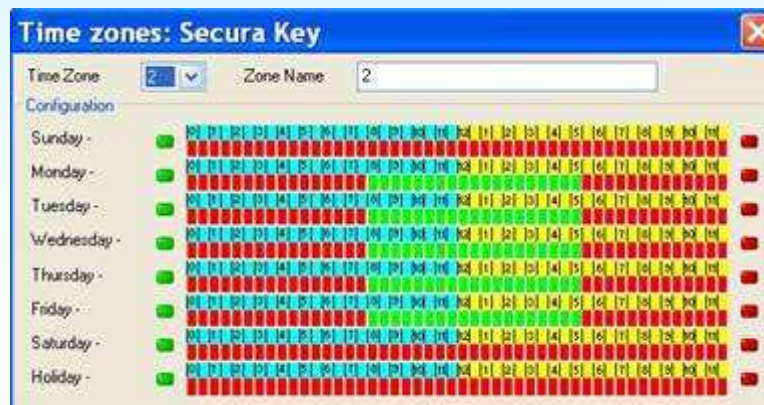
# Time Zones

A Time Zone is a schedule that governs when a card is valid (allowed access) and when it is invalid (denied access).

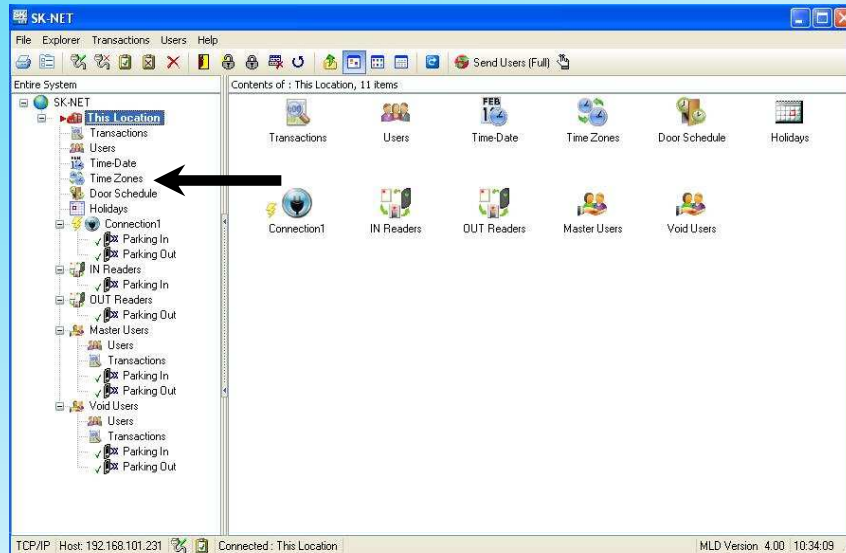
Each Time Zone has a 24 hour schedule for each day of the week, as well as an 8<sup>th</sup> day programmed as a Holiday. Any date defined as a Holiday will follow the programming in the Time Zone for the Holiday section.

SK-NET™ has 16 Time Zones. Time Zone 0 is always Void (Void Users access group). Time Zone 1 is always Valid (Master Users access group), and they can not be edited. **Time Zones 2 through 15** can be edited any way you choose.

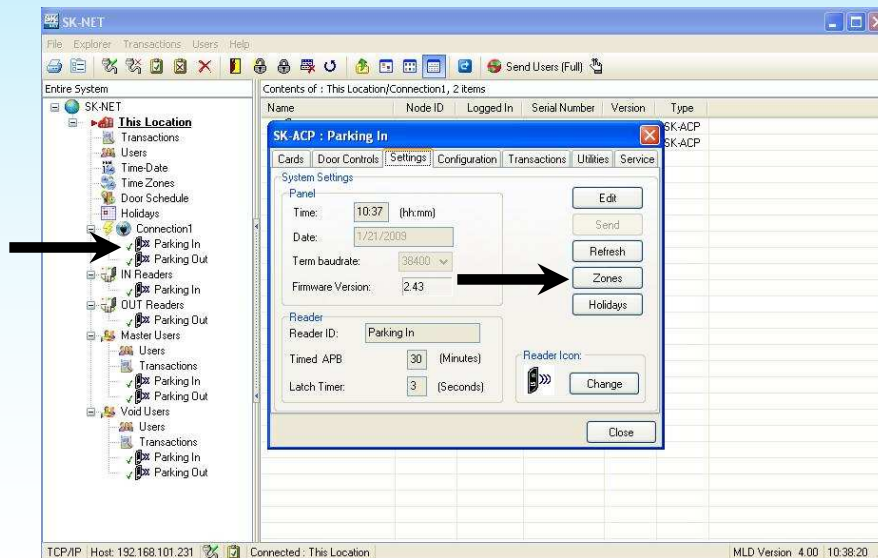
Location (global) Time Zones can be edited for all readers from the Explorer screen. You can also edit a Time Zone for a specific reader.



# Global and Reader Time Zones



To select a Global Time to edit, double click on **Time Zones** from the Explorer Tree



To select a Reader Time Zone to edit, right click on the Reader and select **Properties**

Left click on the **Zones** button

# Edit a Time Zone

You can **Name** each Time Zone, it is recommended to describe what the zone is being used for.

The **Green Blocks** are valid times, and the **Red Blocks** are void times. To change the color of the block, just click on it.

The **Holiday** settings are used for any defined Holidays in the system.

**Antipassback** settings are selected if you are going to use either **Timed Antipassback** or **Real Antipassback** (in/out).

**Start/End Delay** is if you need to start or end time between the half hour block.

**Valid Dates**, if you want to give a Time Zone a beginning start date or a final end date, just uncheck the box and enter the desired date.

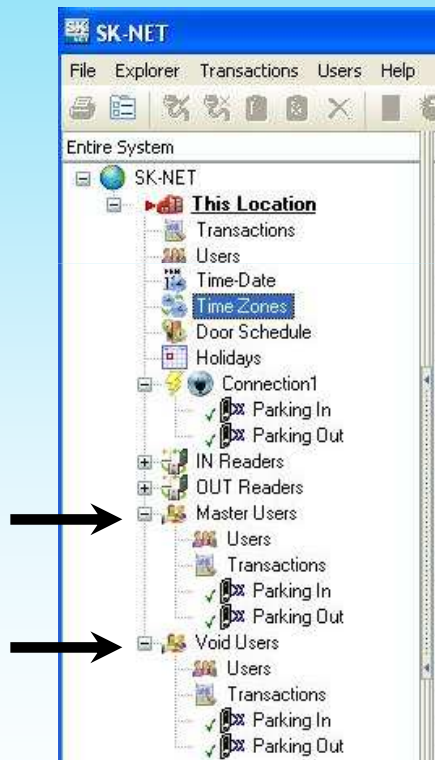
**Note:** To change a whole block of times, just **press and hold** the **Control Key** and select the first and last block, this will fill in all the blocks in between.



# Access Groups

An **Access Group** is assigned to each user which defines which readers they have access to, and what times the readers can be used.

SK-NET™ automatically creates 2 default Access Groups.



The **Master User Group** always includes all the readers in the location and uses Time Zone 1 (always valid). A Master User will always have access to all readers.

The **Void User Group** always includes all readers in the location and will never be granted access, but it will always show a transaction when the card is used.

# Creating an Access Group

The first thing you need to do before creating a new Access Group is define a Time Zone for the proper times the group is allowed access.



To create a new Access Group, right click on the **Location Name**

Select **New**

Select **Access Group**



Enter a Name for the new Access Group, we recommend a name which describes the group of Users

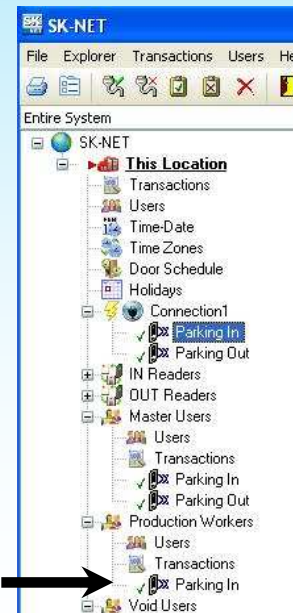
Then enter the **Time Zone** you have defined for the group

# Adding Readers to a New Access Group



After creating a new **Access Group**, notice that there are no readers listed in it.

To add a reader or readers to an Access Group, select a reader from an **Connection Group** and left click keeping the button pressed and drag it to the new Access Group (drag and drop).



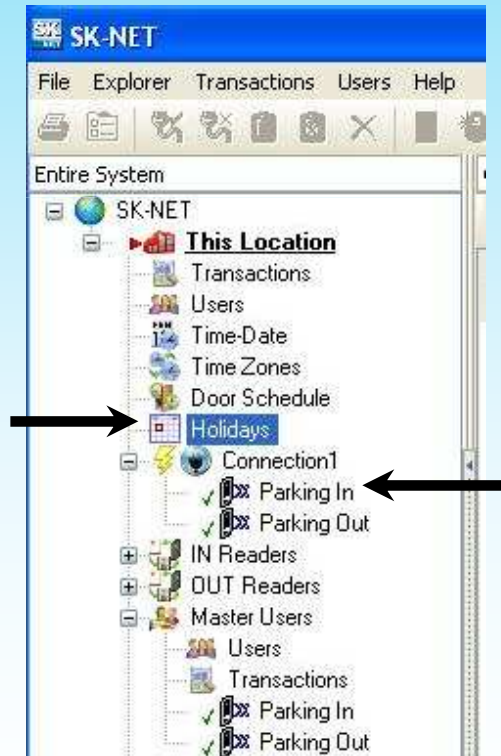
Verify that all the proper readers have been dragged and dropped in to the new **Access Group**.

Next, all you need to do is go to the **User Manager** and reprogram the users Access Group, then Click on **Send Users Full** to complete your changes.

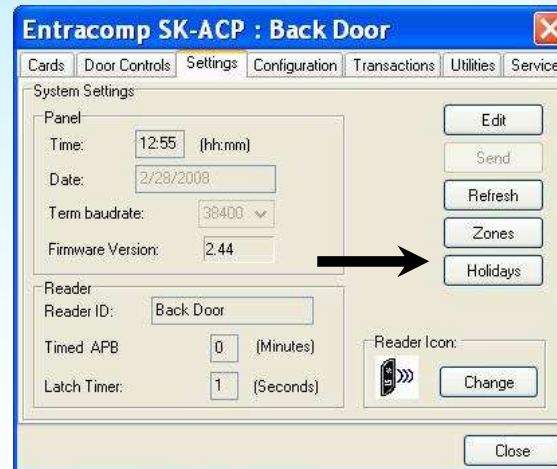
# Holidays

Any date that is designated as a Holiday will follow the **Holiday Schedule** in **Time Zones 2-15** and in the Door Schedules you have created. You can program up to 32 holidays. You may create Holidays globally or separately for each reader.

To program Global Holidays, just left click on **Holidays**



To program Holidays into the reader. Just right click on the **Reader Name**  
Select **Properties**

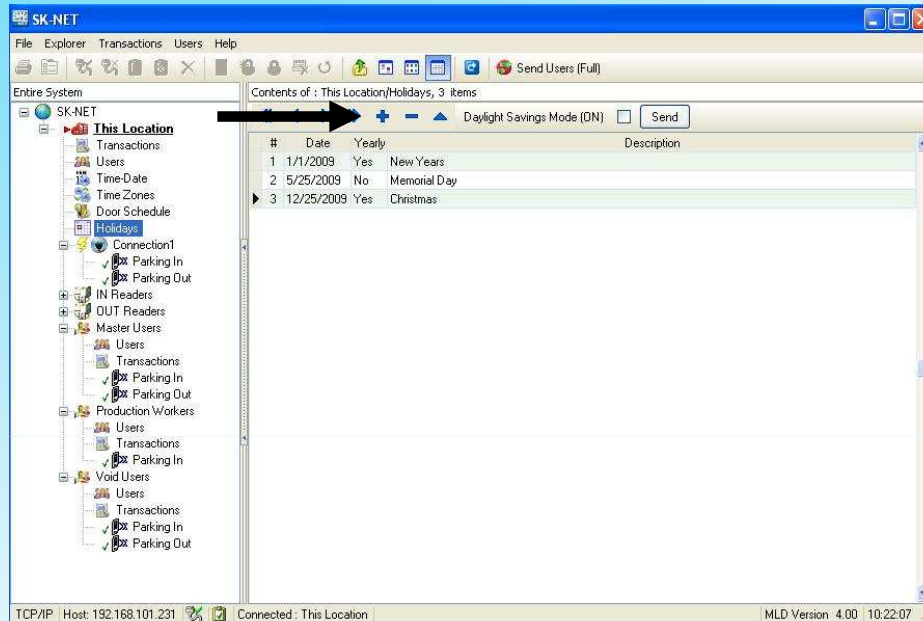


Then select **Holidays**

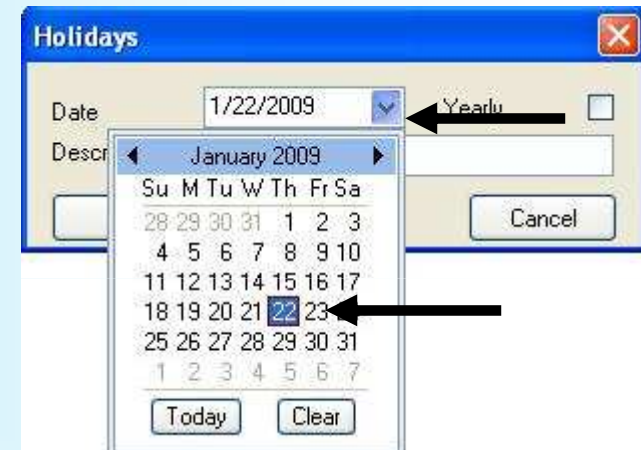


# Program Global Holidays

To add a Global Holiday left click on the +



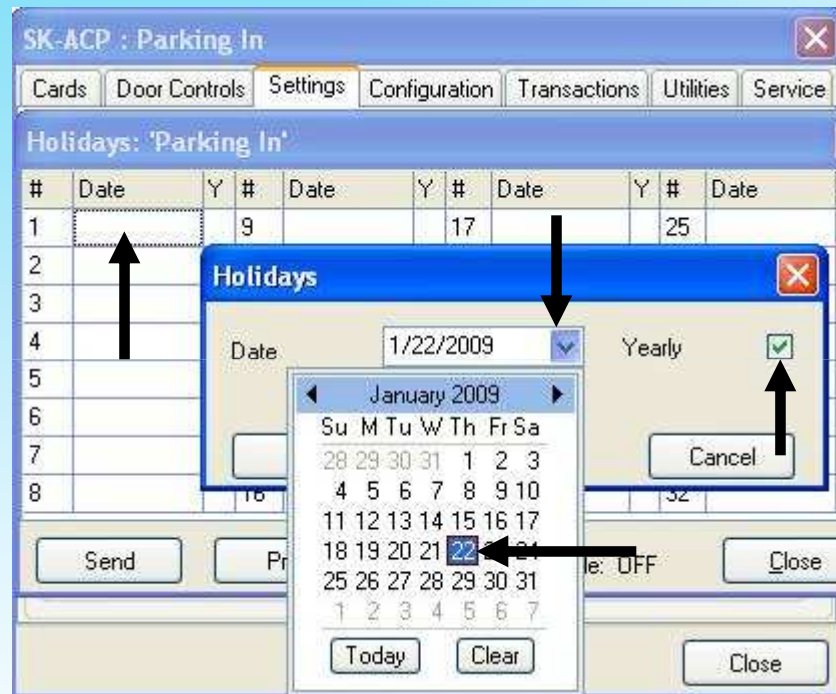
Left click on the **Down Arrow** and select the proper **Date**



Enter the **Description** and place a check mark in the **Yearly Box** if the holiday is on the same date every year.

# Program Reader Holidays

To add a new Holiday, just double click in the **Date** column, left click on the **Down Arrow**, and select the proper **Date**



Click on the **Send** button to send the holidays to the reader, and then **Close**



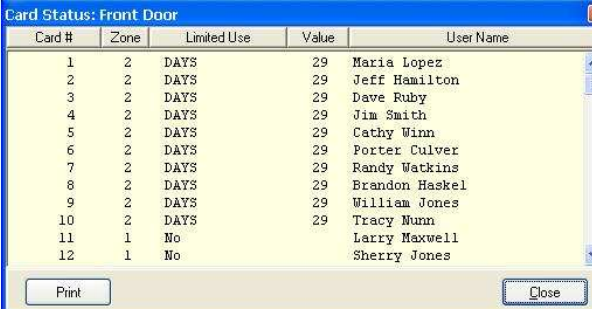
**Note:** Be sure to check the **Yearly** box if the Holiday is on the same date every year. At the beginning of year, you can review the Holidays and know which ones need to be changed at the beginning of each year.

# Limited Use Cards

Limited Use Cards are valid for a specific number of uses, days, days after the first use, or weeks. After the limit is reached, the cards become void. Limited Use Cards can also be set to count how many times a card has been used.

Limited Card usage is shared between all of the readers in a **Connection Group**. It is usually best to setup Limited Use Cards globally, but they can also be programmed in a single reader.

A maximum of 4000 cards can be used as Limited Use Cards. By default the Limited Use Card range is set from 1 to 4000. This can be changed in the **Connection Group Properties**.



The screenshot shows a window titled 'Card Status: Front Door' with a table of card information. The table has five columns: Card #, Zone, Limited Use, Value, and User Name. The data is as follows:

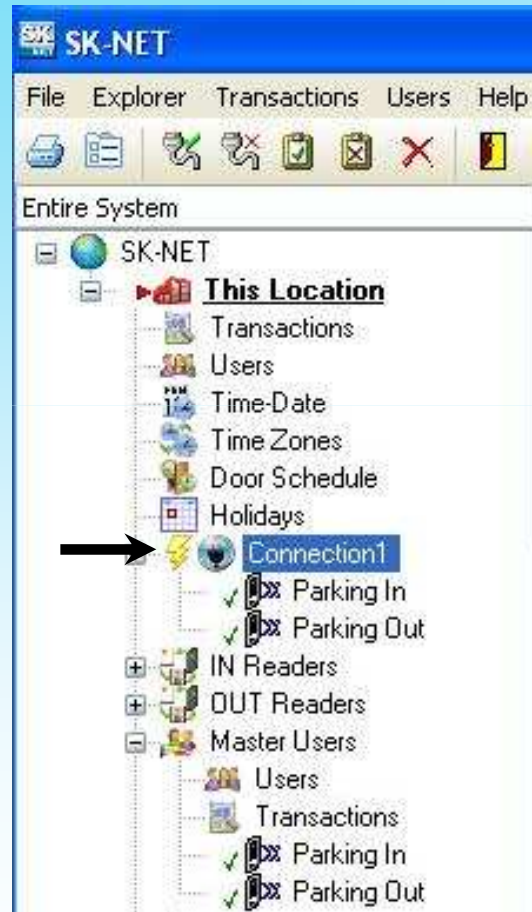
Card #	Zone	Limited Use	Value	User Name
1	2	DAYS	29	Maria Lopez
2	2	DAYS	29	Jeff Hamilton
3	2	DAYS	29	Dave Ruby
4	2	DAYS	29	Jim Smith
5	2	DAYS	29	Cathy Winn
6	2	DAYS	29	Porter Culver
7	2	DAYS	29	Randy Watkins
8	2	DAYS	29	Brandon Haskel
9	2	DAYS	29	William Jones
10	2	DAYS	29	Tracy Nunn
11	1	No		Larry Maxwell
12	1	No		Sherry Jones

At the bottom of the window are 'Print' and 'Close' buttons.

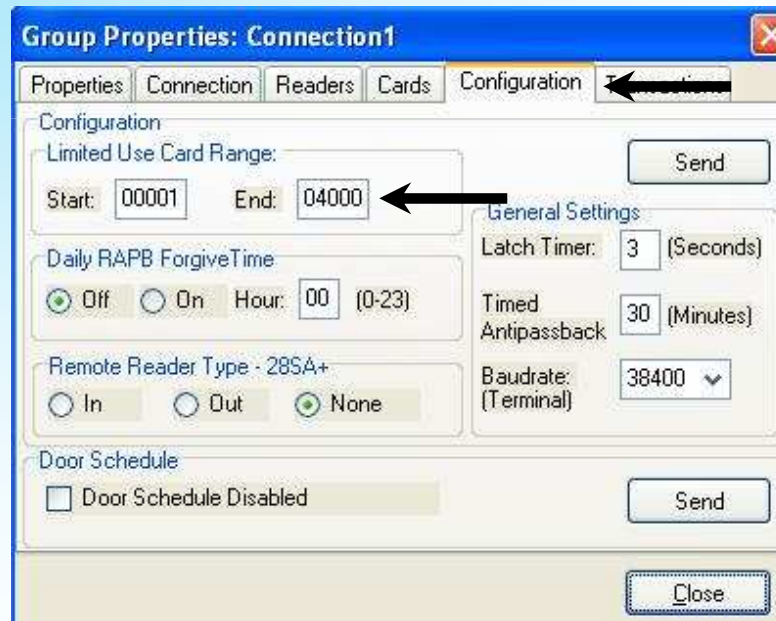
**Note: Time Zone 1 will always be valid and Limited use cards will not work ( do not use the Masters Access Group), you must create a separate Access Group using Time Zones 2 to 15 to use the Limited Use feature.**

# Limited Use Card Range

To setup the Card Range to match the block of cards you are using in your system, just right click on **Connection1** and select **Properties**



Select the **Configuration** tab  
Enter the **Card Range** you are currently using in your system

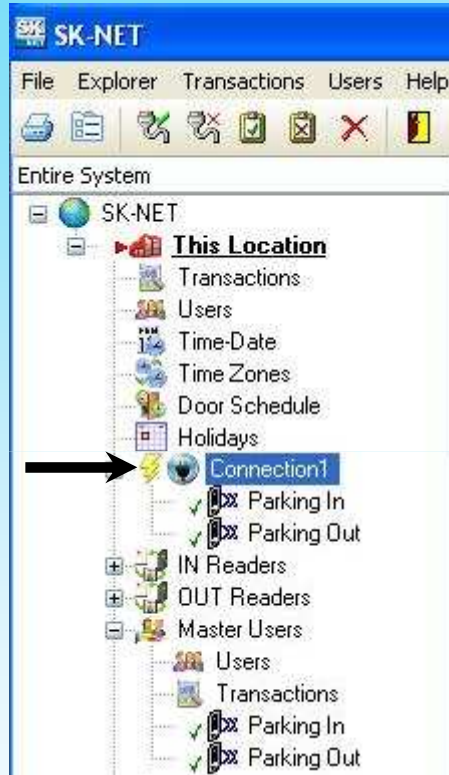


**Note:** Do not exceed more than **4000** cards or **Limited Use Will NOT WORK!**



# Global Limited Use

To program Limited Use Cards to all the readers in your system , just right click on **Connection1** and select **Properties**

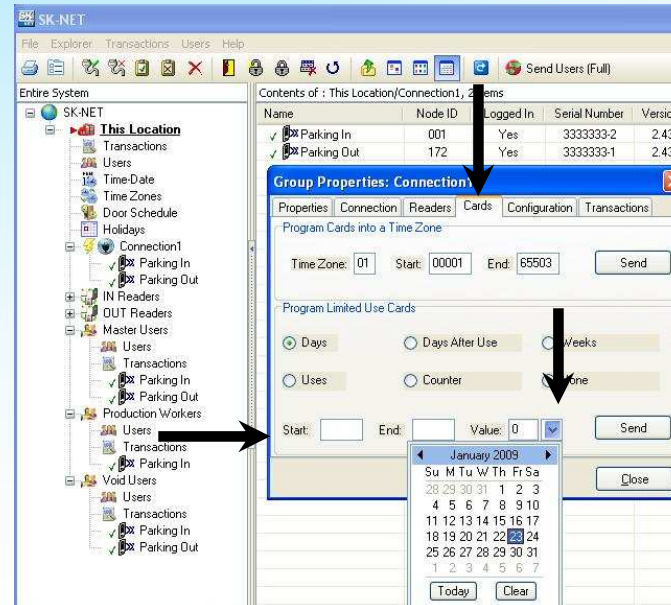


Select the **Cards** tab

Enter a **Card Number** or block of Cards

If you choose to use **Days**, you will get a drop down calendar.

Now select the **Last Day** you want the card to work and SK-NET™ will enter the **Value** or how many days the card will be valid for.



# Reader Limited Use

To program Limited Use cards to a Single Reader only, right click on the **Reader** and select **Properties**

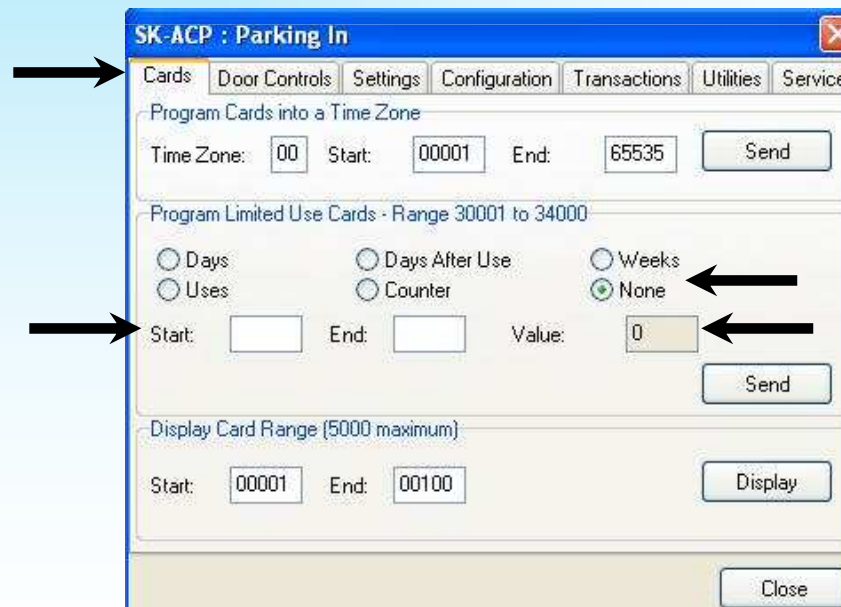


Select the **Cards Tab**

Select the appropriate **Limited Use Parameter**

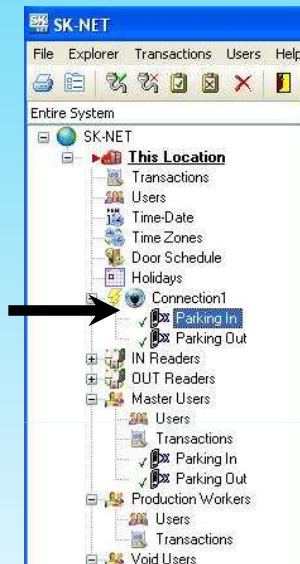
Enter the **Card Number or Block of Cards**

Enter the **Value**



# Viewing Limited Use Status

To view Limited Use cards in a Single Reader, right click on the **Reader** and select **Properties**.



SK-ACP : Parking In

Program Cards into a Time Zone

Time Zone: 00 Start: 00001 End: 65535 Send

Program Limited Use Cards - Range 30001 to 34000

☐ Days ☐ Days After Use ☐ Weeks  
☐ Uses ☐ Counter ☒ None

Start: End: Value: 0 Send

Display Card Range (5000 maximum)

Start: 00001 End: 00100 Display

Close

Select the **Cards** tab  
Enter a **Range** of cards  
Click on **Display**

Card #	Zone	Limited Use	Value	User Name
1	2	DAYS	29	Maria Lopez
2	2	DAYS	29	Jeff Hamilton
3	2	DAYS	29	Dave Ruby
4	2	DAYS	29	Jim Smith
5	2	DAYS	29	Cathy Winn
6	2	DAYS	29	Porter Culver
7	2	DAYS	29	Randy Watkins
8	2	DAYS	29	Brandon Haskel
9	2	DAYS	29	William Jones
10	2	DAYS	29	Tracy Nunn
11	1	No		Larry Maxwell
12	1	No		Sherry Jones

Print Close

This view shows the Cards setup as **Limited Use**, and how many days are they are valid for.

**Note:** You can only view the status of Limited Use cards in a Single Reader.

# Timed Antipassback

Timed Antipassback is a feature designed to prevent card sharing or to prevent a user to pass their card to someone else to gain access. After a card is used at a reader programmed with TAPB, that card will now be void at that reader for up to 30 minutes.

To setup the time for Timed Antipassback, just right click on the **Reader** and select **Properties**.



From the **Settings** tab.

Left click on **Edit**

Enter the required time for **Timed APB** up to 30 minutes

Then click on **Send**



# Timed Antipassback in a Time Zone

The first thing you need to do is setup an [Access Group](#) which uses Time Zones 2 to 15 whenever using Timed Antipassback.

**Time zones: Secura Key**

Time Zone: 2 Zone Name: 6am to 6pm M-F

**Configuration**

Day	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Sunday	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Monday	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Tuesday	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Wednesday	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Thursday	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Friday	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Saturday	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Holiday	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

**Antipassback Configuration**

☒ None ☐ Real Hard

☐ Timed Hard ☐ Real Soft

☐ Timed Soft

**Start/End Delay**

Delay Start: 0 (Minutes)

Delay End: 0 (Minutes)

**Valid Dates**

☒ Start Unrestricted

Begin Date: 2/14/2008

☒ End Unrestricted

End Date: 2/14/2008

Refresh Save Send All Close

You must select the correct **Timed Antipassback** setting from the Time Zone.

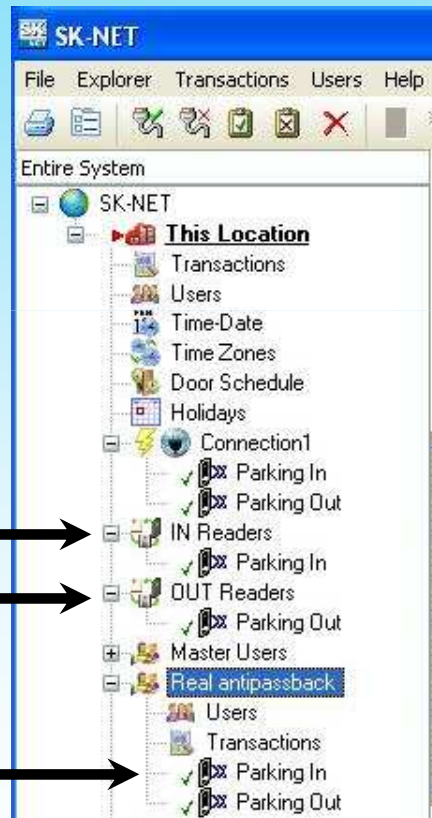
**Timed Hard** Antipassback means the card will be Void after the first read and an “Antipassback Violation” will appear in the Transaction history.

**Timed Soft** Antipassback means the card will be Valid after the first read but an “Antipassback Violation” will still appear in the Transaction history.

**Note:** This feature does not apply to Time Zones 0 or 1 (Master or Void Groups).

# Real Antipassback

**Real Antipassback** is a feature designed to prevent card sharing and/or to enforce use of IN and Out readers. **Real Antipassback** requires readers for coming IN and going OUT. If a card was last used at an IN reader, it must be used at an OUT reader before it will be valid again at an IN reader.



To setup Real Antipassback create an [Access Group](#) using Time Zones 2 to 15.

Define your readers as IN or OUT readers by dragging them into the **IN** and **OUT** Reader Groups.

Also be sure to add the readers into the **Access Group**.

**Note:** This feature does not apply to Time Zones 0 or 1 (Master or Void Groups).

# Real Antipassback in a Time Zone

The first thing you need to do is setup an [Access Group](#) which uses Time Zones 2 to 15 whenever using Real Antipassback.

Time zones: Secura Key

Time Zone: 2 Zone Name: 6am to 6pm M-F

Configuration:

Sunday - [Calendar Grid]

Monday - [Calendar Grid]

Tuesday - [Calendar Grid]

Wednesday - [Calendar Grid]

Thursday - [Calendar Grid]

Friday - [Calendar Grid]

Saturday - [Calendar Grid]

Holiday - [Calendar Grid]

Antipassback Configuration:

☒ None ☐ Real Hard ☐ Timed Hard ☐ Real Soft ☐ Timed Soft

Valid Dates:

☒ Start Unrestricted

Begin Date: 2/14/2008

☒ End Unrestricted

End Date: 2/14/2008

Start/End Delay:

Delay Start: 0 (Minutes)

Delay End: 0 (Minutes)

Buttons: Refresh, Save, Send, All, Close

You must select the correct **Real Antipassback** setting from the Time Zone.

**Real Hard** Antipassback means the card will be Void after the second read on the same reader and an “Antipassback Violation” will appear in the Transaction history.

**Real Soft** Antipassback means the card will be Valid after the second read on the same reader but an “Antipassback Violation” will still appear in the Transaction history.

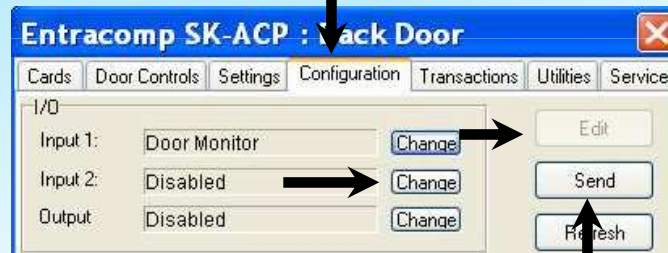
**Note:** This feature does not apply to Time Zones 0 or 1 (Master or Void Groups).

# Inputs

**Inputs** are circuits that connect external sensors or switches to and SK-ACP or 28SA+. They are used to initiate special functions or to generate messages in Transactions. There are 8 different Input definitions you can choose in SK-NET™.



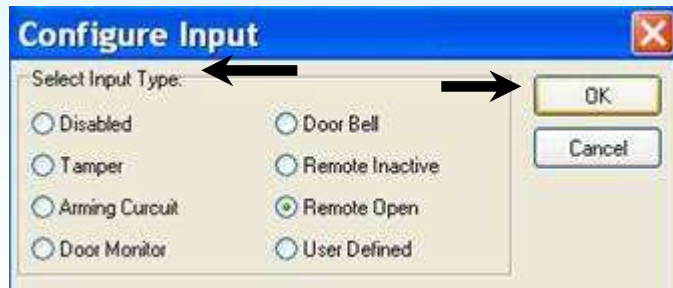
To select an input right click on a reader and select **Properties**.



Select the **Configuration** tab

Click on **Edit**

Click on **Change**



Select the desired **Input Type**

Click **OK**

Then **Send** to the reader



# Input Definitions

**Disabled:** The input is not used.

**Tamper:** A switch or sensor that has been installed to detect interference with a component of the Access Control system. If this circuit is closed, the reader will be disabled and a Tamper message will appear in Transactions.

**Arming Circuit:** The reader is disabled until this input is closed. Cards presented while the Arming Circuit is open will show in the transaction as a violation and access will be denied. This input is most often used with a loop detector which must sense a vehicle is present before a card can be valid.

**Door Monitor:** Connected to a door position switch, this input activates anti-tailgate feature. It is also used to detect a door forced or held open too long.

**Door Bell:** Sends an ASCII Bell character to a PC or printer, causing an audible tone.

**Remote Inactive:** Closing this input makes the reader inactive (lockout).

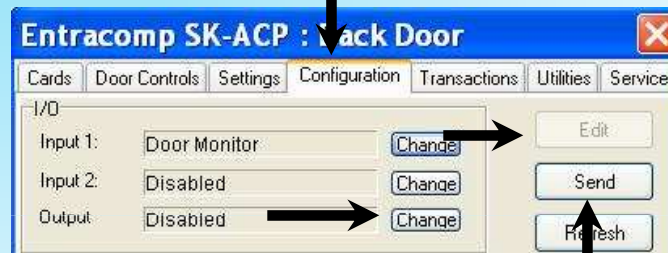
**Remote Open:** This input activates the latch relay for the same time as a valid card use. A 'Door Opened Via Sensor' message appears in the Transactions.

**User Defined:** This input allows you to write a custom message that will appear in Transactions. The input can be a variation of Remote Open or it can simulate Door Bell.

# Outputs

The SK-ACP has a Latch relay and an auxiliary relay for each reader. This extra relay can be activated by a variety of means to accomplish various functions.

To program an Output right click on a reader and select **Properties**.



Select the **Configuration** tab  
Click on **Edit**  
Click on **Change**



Select the desired **Output** Type  
Click **OK**  
Then **Send** to the reader

**Note:** The 28SA+ does not have an auxiliary output.

# Output Definitions

**Input 1 Follow/Latch:** Whenever Input 1 is shorted the aux relay will activate.

**Input 2 Follow/Latch:** Whenever Input 2 is shorted the aux relay will activate.

**Door Monitor Alarm:** If one of the inputs is configured as Door Monitor, this output will activate if the door is forced open or if it is left open too long. This Output is typically connected to a local alarm signal or to a remote monitoring station.

**Door Forced Alarm:** If one of the inputs is configured as Door Monitor, this output will activate if the door is forced open. This Output is typically connected to a local alarm signal or to a remote monitoring station.

**Door Held Open:** If one of the inputs is configured as Door Monitor, the output will activate if the door is left open too long. This Output is typically connected to a local alarm signal or to a remote monitoring station.

**Emergency Exit Alarm:** Used when one of the Inputs is designated as Remote Open, the auxiliary relay will activate whenever the main relay is triggered via the Remote Open Input. This is typically used to sound a local alarm when the door has been used for egress.

# Output Definitions continued

**Card Range:** Cards in a selected range will activate the auxiliary relay only or both the auxiliary and main relays. Typically this is used so specific cards can cause something special or extra to happen. The relay can be set to toggle mode.

**Error Alarm:** When any one of selected “error” conditions occur, the auxiliary relay will activate. There are many error conditions you may select from.

**Serious Alarm:** When any one of the following “error” conditions occur the auxiliary relay will be activated. Void Card, Invalid Facility Code, Tamper, Door Forced, or Door Held.

**Time Zone:** The auxiliary relay will be activated during the green blocks in a selected Time Zone. This is like having an 8 day timer including holidays.

**Tamper Alarm:** If a Tamper is closed, the auxiliary relay will be activated.

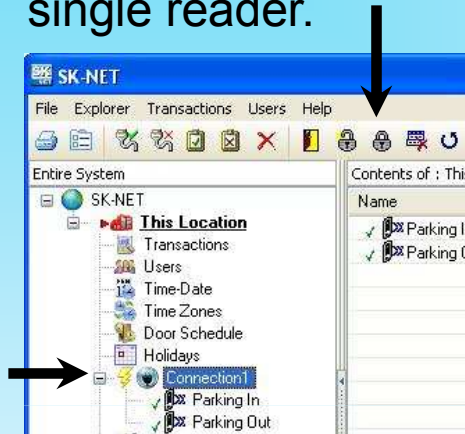
**Door Bell:** If a Door Bell input is closed the auxiliary relay will be activated.

**Alarm Shunt:** Whenever the main relay is activated by a valid card or a Remote Open, the auxiliary relay will be activated.



# Door Controls

**Door Controls** are functions that you can initiate from SK-NET™ that affect the door or gate at a connected Location. **Door Control** icons appear at the top of the Explorer screen. You can send a **Door Control** command as global or to a single reader.



To send a global Door Control to all the readers, just left click on **Connection1** to highlight it

Select the proper **Icon**



**Open Door Now:** This icon opens the doors for the set time of the latch relay.



**Unlock the Door:** This icon unlocks the doors until it is returned to normal. The LED at the readers will flash green.



**Make Inactive (locked):** This icon locks the doors until it is returned to normal. The LED at the readers will flash red.



**Disable Door Schedule:** This icon overrides and relocks the doors.



**Make Active Normal:** This icon restores the readers to normal.

# Door Controls for a Single Reader



Right Click on the **Reader** and Select **Properties**



Select the **Door Controls** tab

**Open:** This button opens the doors for the set time of the latch relay.

**Unlock:** This button unlocks the doors until it is returned to Normal. The LED at the readers will flash green.

**Inactive (locked):** This button locks the doors until it is returned to Normal. The LED at the readers will flash red.

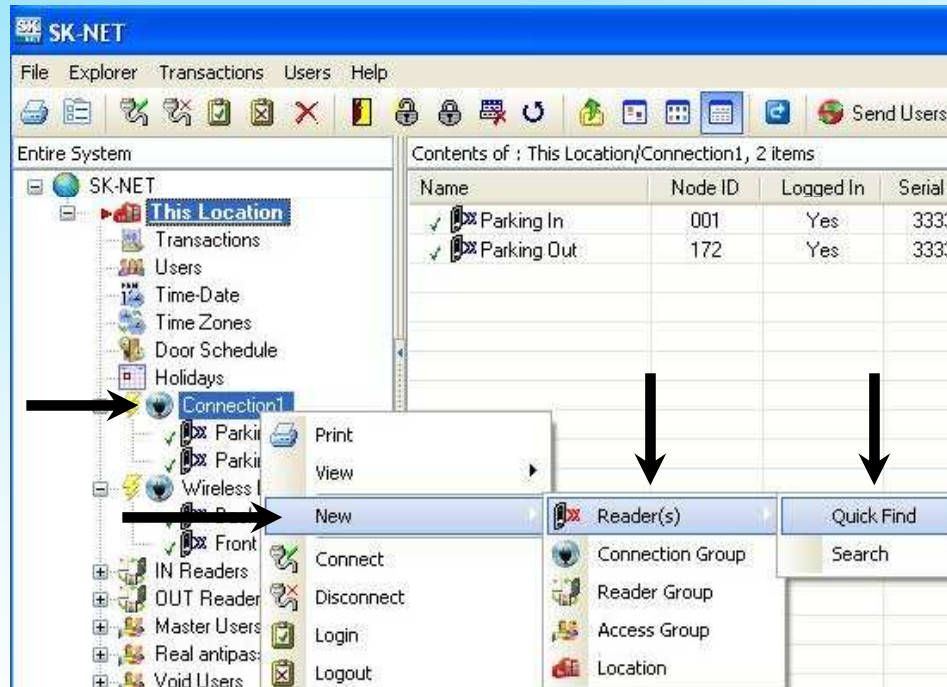
**Disable Door Schedule:** Click on the **Edit** button, then place a check in the **Disabled box** and then **Send**.

**Normal:** This button restores the Reader to **Normal**.

# Add New Readers

After the new hardware has been installed and wired into the system, hold in the reset button while turning on the power. Hold for 3 seconds and release.

Right click on the Connection Group and select **New**



Select **Reader(s)**

Select **Quick Find** if you have a total of 20 readers or less

Select **Search** if you have more than 20 readers

# The End

If you require additional information  
please visit our website:

[www.securakey.com](http://www.securakey.com), email us at  
[info@securakey.com](mailto:info@securakey.com)

or call us at  
(800) 891-0020

Thank You!