701 Client/Server

Installers Manual

701 SERVER

701 CLIENT

November 2017

Version 1.1

CONTENTS

701 SERVER

701 CLIENT

INTRODUCTION

Soyal Access Control Systems use Tokens and/or Cards and/or PIN numbers to provide users with access to doors. Each Token/Card within the system will have a unique user number which they are identified to during programming. Each Token or Card can be provided with access rights that can be defined by individual doors and individual times. As the installer you may be asked to set up Time Zones and Door Groups if your client has requested them.

701 Server acts as the communication software allowing Controllers to communicate via RS485 and/or TCP/IP.

701 SERVER

701 Client is the User interface for monitoring the access control system and modifying the access rights of users.

701 CLIENT

Follow the instructions in the “Software Installation and setup Manual” to install the RS485 to USB driver (if required) Soyal Device tools, 701 Server and 701 Client.

Always install the latest versions of the software which are available on our website : http://www.raytelsecurity.co.uk/downloads.cfm

Once installed User Access levels can be set for 701 Server and 701 Client. User access levels will enable you as the installer to have access to all of the functions in 701 Server and 701 Client. By setting up suitable User access levels for your customer you can limit the level of interaction they are able to have with 701 Server and 701 Client. Further setup may include the adding of Tokens/Cards, setting access rights for Tokens/Cards, naming Doors, creating Door Groups and setting Time Zones.

Once a system is configured and operating it is not advisable turn off the computer or disconnect the interface (USB or Ethernet) as this will stop communication to the controllers. If the communication is interrupted , when it is re-established there may be a period where the software runs very slowly. This is because the software will be updating with all of the events that have taken place at each controller whilst the interface has been disconnected.

701 Client can be minimised and will continue to run in the background if required.

Once a system is configured and controllers have been updated all controllers will function as stand alone devices if for any reason the network connection fails.

Door controllers have limits for the number of users that can be stored. For most systems this will be 1024 users. More complex systems can have higher numbers of users available.

701 Client is a database. Any changes made in 701 Client are stored within the database.

NO CHANGES MADE WITHIN 701 Client WILL TAKE EFFECT UNTIL THE REVISED DATA IS DOWNLOADED TO THE CONTROLLER(S)

701 Client when connected to the controller network stores every transaction reported to it. 701 client is therefore able to provide reports on Time and attendance by individual and groups of individuals. The software can also filter results by numerous parameters. For further information on report formats contact Raytel Technical support.

Essential steps for a new installation

701 Server

Set the controller Node ID's at the controllers (Node ID 2 onwards)-Page 6-9
Set Door and Reader identities at the controllers-Page 6-9
Select the correct controller identities in 701 Server LAN settings-Page 10
Check all of the connected controllers are on line-Page 11
Download the date and time to all controllers on line-Page 11

701 Client

Enable Huge-Door-Group mode if there is more than one door-Page 21
Check the daily event log is showing-Page 16
Present a token to each controller and reader (or each door if it is a multi door controller) check that the token details appear on the daily event log-Page 16
Name the Doors (if required)-Page 22
Set the Door Groups (If required)-Page 23
Set the Time Zones (If required)-Page 24
Add user information to the 701 Client database-Page 25
Download user details to controllers-Page 30
Test the system with tokens and/or PIN numbers-Page 16
Fill in the "System User information" table-Page 38

HARDWARE SPECIFICATION

Below is a table of controllers supplied by Raytel Security Systems with basic functionality identified. All of these controllers can be networked.

Reference	Series	Description	Keypad	Display	Internal Reader	External Reader	No of Users
K50	Raytel H	PIN and /or Card Access	Y	N	N	Y (WG)	1,024
AR-888H	H	PIN and/or Card Access	Y	N	Y	Y (WG)	3,000
AR-727H	H	Card Access Only	Y	Y	Y	Y (WG)	1,024
AR-727HB-RAY	Raytel H	2 Door Controller Card Access only	Y	Y	N**	Y (RS485 x 2)	1,024
AR-829EV5	E	Card Access Only	Y	Y	Y	Y (WG)	15,000
AR-716E	N/A	16 Door Controller	N	N	N	Y (RS485 x 14, WG x 2)	15,000
AR-331EF AR-881EF	E	Fingerprint and /or PIN and/or Card Access	Y N	N N	Y Y	Y (WG) Y (WG)	16,000 16,000

N** Controller has a built in reader But only for adding tokens.

This manual assumes all hardware has been installed as per our installation manuals, is physically connected to the network and is functional. The critical checks are as listed below:

All controllers in the network MUST have unique node ID's (Node ID 2 onwards) if TCP/IP is being used all controllers in the network MUST have a unique node ID AND a unique IP address.

All readers must have their dip switches set correctly as per the individual controller installation instructions. If readers are connected to multi door controllers each reader must also have a unique node ID.

Controllers connected to an RS485 network must be daisy chained, star wiring is not acceptable.

In TCP/IP networks the maximum distance between the controller and Network switch or other repeater device must not exceed 100m.

In RS485 networks it is recommended that an RS485 repeater is inserted after 30 controllers OR 300m

WG readers must not exceed 30M from their controller, WG repeaters can be used if greater distance is required.

SETTING CONTROLLER NODE ID & DOOR NUMBERING AT CONTROLLERS

Node ID's are used within 701 Server to identify controllers. Door Numbers are used to identify specific doors within 701 Client. Both must be set at the controller(s) to enable the correct operation of the software.

ALL CONTROLLERS MUST HAVE A UNIQUE NODE ID

Setting Node ID and door numbers on controllers with LCD displays

H SERIES CONTROLLERS—(AR-727H)
We would recommend for all H series controllers with Wiegand readers that
Door Num H = Node ID and Door Num L is set to 1
EG if the Node ID of the controller is 16 set Door Num H to 16 and Door Num L to 1
See page 7

E SERIES CONTROLLERS—(AR-829Ev5, AR-881EF)
We would recommend for all E series controllers with Wiegand readers that
Main Door Number = Node ID, WG Door Number = Node ID
See pages 8-9

Raytel AR-727HB-RAY, AR-716E-RAY, EAR-727HB-RAY CONTROLLERS
For two Door controllers (AR-727HB-RAY, AR-716E-RAY) we would recommend that
Door Num H = Node ID, Door Num 0 is set to 1 and Door Num 1 set to 2
Refer to the specific controller manual for setting reader node ID's if required.

For AR-716E multi door controllers refer to Raytel Technical

Setting Node ID and door numbers on non LCD display controllers.

Raytel K50 Keypad and AR-888H Controller / Reader

Enter *123456# or Master code *MASTER CODE# to access programming mode

Then enter 00*NNN*VVV*nnn# = 00*Node ID*Virtual node*door no#

We would recommend that:
Node ID (NNN) = Virtual node ID(VVV) and the Door number (nnn) is set to 1

Where: NNN = 3 digit node ID i.e. Node ID=1 enter 001
VVV = 3 digit virtual node i.e for 3 enter 003
nnn = Door no i.e. for Door no 6 enter 006

Each code must be 3 digits in length.

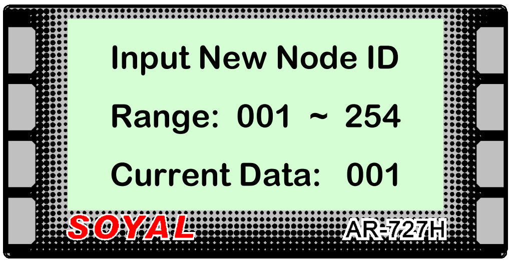
NODE ID & DOOR NUMBERING H SERIES

Enter Programming mode *123456# or *MASTER CODE#

Use F1 or F2 to scroll to 3. Parameters (1) and press #

Use F1 or F2 to scroll to 1. Node ID and press #

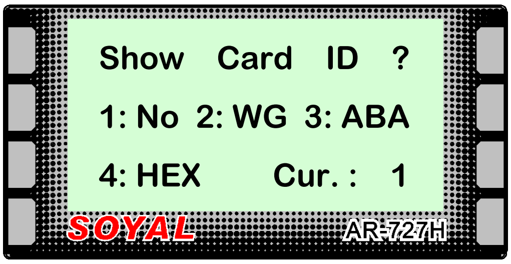
The Display will Show :-



Input New Node ID
Range: 001 ~ 254
Current Data: 001

Enter the required Node ID number and press #

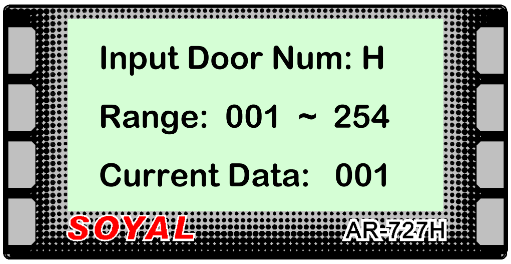
The Display will Show :-



Show   Card   ID   ?
1: No 2: WG 3: ABA
4: HEX   Cur. :   1

Enter the number for the option required. Default=2

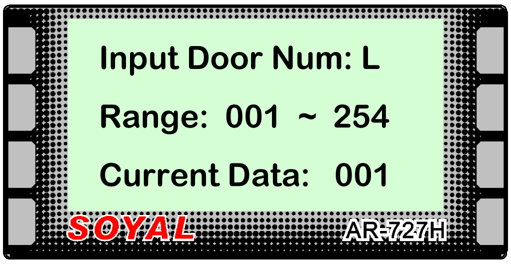
The Display will Show :-



Input Door Num: H
Range: 001 ~ 254
Current Data: 001

Input the Door Number and press #
This is the High level Door Number of the controller. We recommend H=Node ID (see page 6 for further info)

The Display will Show :-



Input Door Num: L
Range: 001 ~ 254
Current Data: 001

Input the Door Number and press #
This is the Low level Door Number of the controller. We recommend L=1(see page 6 for further info)

The Display will show Succeeded!

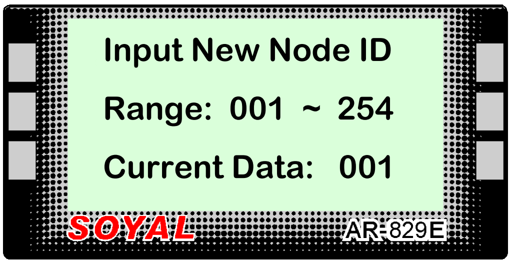
NODE ID & DOOR NUMBERING E SERIES

Enter Programming mode *123456# or *MASTER CODE#

Use F1 or F2 to scroll to 3. Parameters (1) and press #

Use F1 or F2 to scroll to 1. Node ID and press #

The Display will Show :-



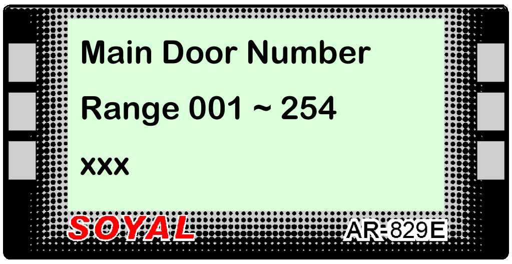
Input New Node ID

Range: 001 ~ 254

Current Data: 001

Enter the required Node ID number and press #

The Display will Show :-
Where xxx is the
current setting.



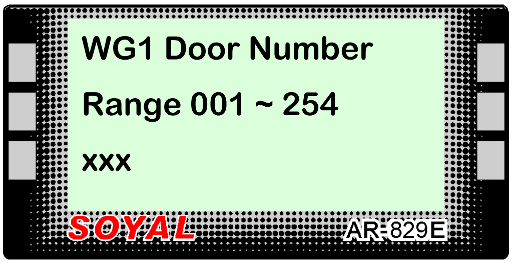
Main Door Number

Range 001 ~ 254

xxx

Enter the required Main Door Number and press # We would recommend Main Door Number=Node ID (See page 6 for further info)

The Display will Show :-
Where xxx is the
current setting.



WG1 Door Number

Range 001 ~ 254

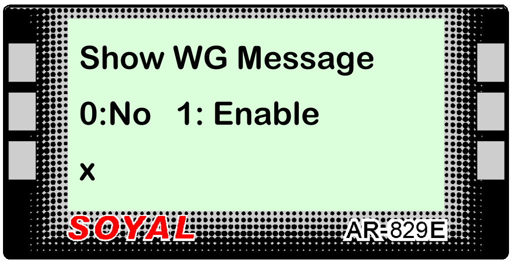
xxx

Enter the required WG1 Door Number and press # We would recommend WG1 Door number=Node ID (See page 6 for further info)

Continued on Page 9

NODE ID & DOOR NUMBERING E SERIES

The Display will Show :-
Where x is the current
setting.



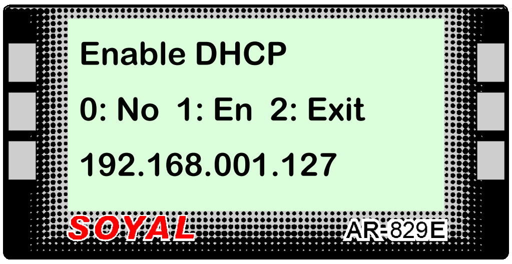
Show WG Message

0:No   1: Enable

x

Enter the number for the option required. Default = 1

The Display will Show :-



Enable DHCP

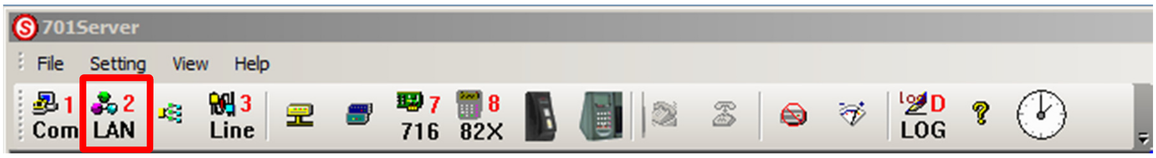
0: No 1: En 2: Exit

192.168.001.127

Enter the number for the option required.

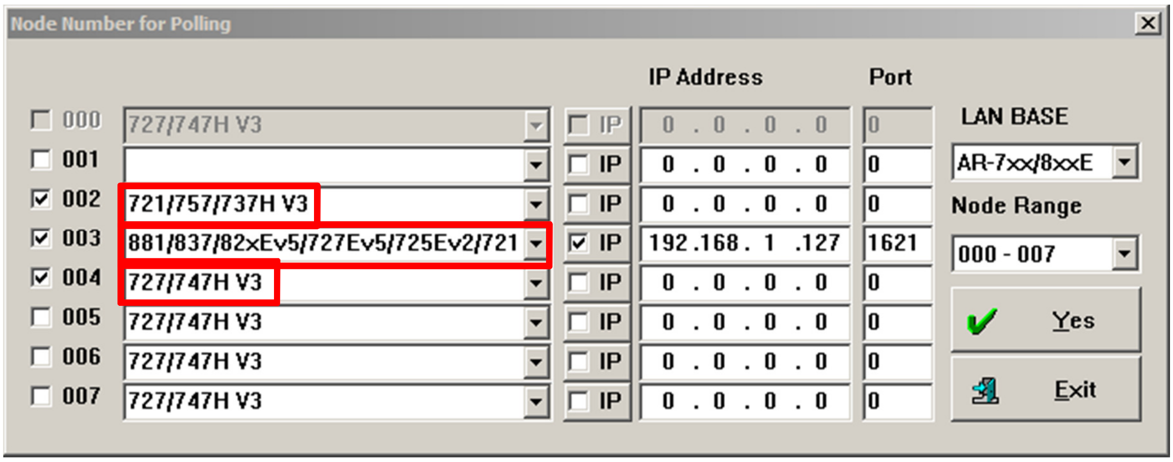
We would suggest that unless IP address etc is to be set select 2 for Exit, then press * until the quit menu is reached then press # to quit programming mode.

701 SERVER CONTROLLER NODE ID & TYPE



Each controller on a network must have a unique Node ID. We would recommend setting controller Node ID's from ID=2 upwards (This will enable a USB desktop reader to be used if required) Select 2 LAN as shown above from the 701 Server header strip to access Node ID setting.

When setting up controllers in 701 Server LAN base use the following selections for the controllers as identified below.



Node Number for Polling

			IP Address	Port
□ 000	727/747H V3	□ IP	0 . 0 . 0 . 0	0
□ 001		□ IP	0 . 0 . 0 . 0	0
☑ 002	721/757/737H V3	□ IP	0 . 0 . 0 . 0	0
☑ 003	881/837/82xEv5/727Ev5/725Ev2/721	☑ IP	192 .168 . 1 .127	1621
☑ 004	727/747H V3	□ IP	0 . 0 . 0 . 0	0
□ 005	727/747H V3	□ IP	0 . 0 . 0 . 0	0
□ 006	727/747H V3	□ IP	0 . 0 . 0 . 0	0
□ 007	727/747H V3	□ IP	0 . 0 . 0 . 0	0

LAN BASE: AR-7xx/8xxE

Node Range: 000 - 007

727/747H V3 For AR-727H single door controller.

727/747H V3 For AR-727HB-RAY, AR-716E-RAY and EAR-727HB-RAY 2 door controllers

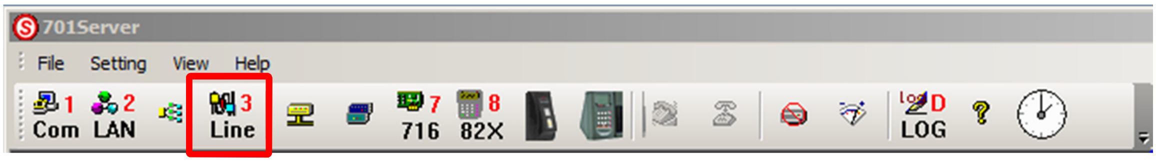
721/757/737H V3 For Raytel K50 Keypad and AR-888H/U Keypad

881/837/82xEv5/727Ev5/725Ev2/721… For AR-829EV5 single door controller

For other controllers refer to the relevant installation manual or contact Raytel Technical.

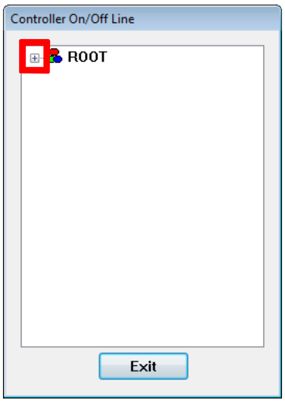
Please note: Controller 003 is shown with an IP address as well as a Node ID this will be required if the device is communicating via TCP/IP, please refer to the Raytel "Soyal Advanced Networking Manual" for additional setup and configuration information.

701 SERVER CONTROLLERS ON LINE

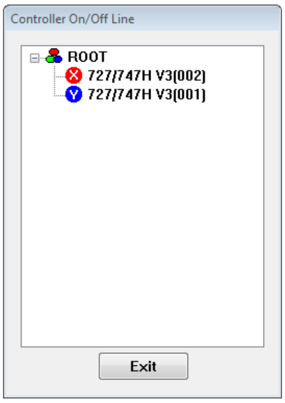


Select 3 Line from the 701 Server header strip as shown above to access the Controller On/Off Line screen.

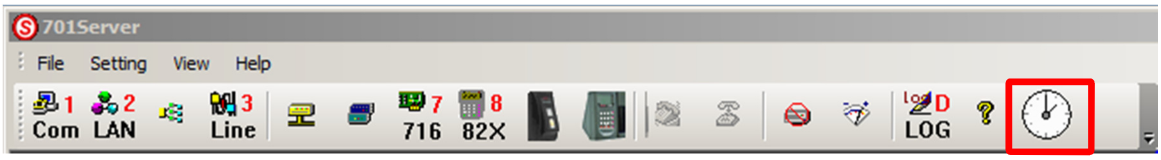
Once the Controller On/Off Line screen opens, left click on the + to the left of the icon.



This will then show a display of all controllers selected in the Node Number for Polling screen. If the device is selected but NOT on line it will have a RED X ❌ to the left of the description. If the device is selected and is on line it will have a BLUE Y Ⓨ to the left of the description, as shown to the right.



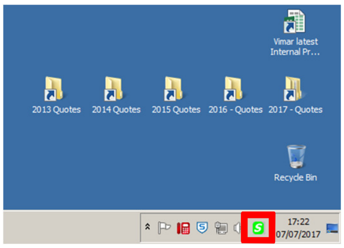
Once controller node ID’s have been selected, the correct device descriptions have been selected and the devices are confirmed as ON line Exit the Controllers On/Off Line window.
From the main menu click on “Time and Date” as shown below. This will download the current Date and Time to all connected controllers.



701 Server can now be minimised to the tool bar.

701 SERVER ACCESS LEVELS

701 Server is a programme that loads at startup and constantly runs in the background whilst the PC is turned on. The connection status of 701 Server can be identified from the notification icon in the bottom right section of the computers display (see below) The colour of the ‘S’ denotes the status of the software.

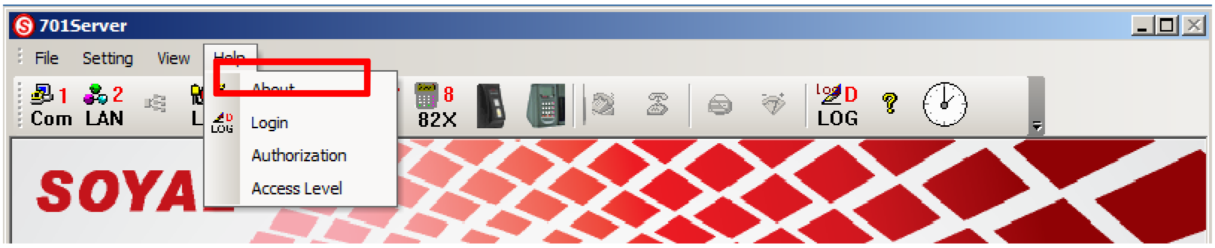


A White S with a Red surround shows that the software is loaded and running but not communicating.

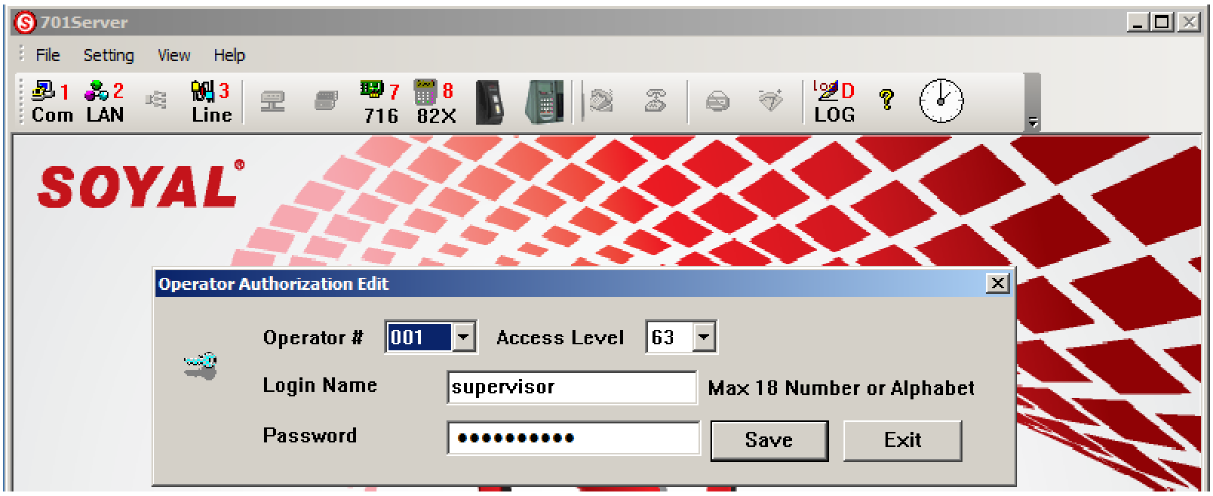
A White S with a Green surround shows that the software is loaded and running and attempting to communicate.

A Red S with a white surround shows that the software is loaded and running and communicating via RS485 or TCP/IP. This may alternate with the above White S with a Green background.

To set Access Levels for 701 Server log in to Server by double clicking the S icon identified above. At the login screen use the Login name “supervisor” and the Password “supervisor”



Once logged in select “Authorisation” from the Help menu . The Operator Authorisation Edit screen shown below will open.



Operator Authorization Edit

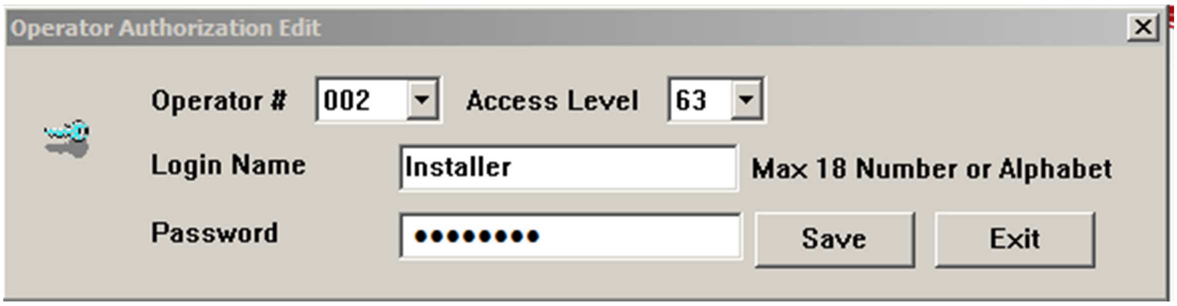
Operator # 001
Access Level 63
Login Name supervisor
Max 18 Number or Alphabet
Password ••••••••••

Suggested Access levels are identified on the next page.
****Do not change the settings for Operator# 001****

701 SERVER ACCESS LEVELS

Installer Access

We recommend selecting Operator 002 from the drop down and setting this as below. Login Name and Password are case sensitive and can be set to any combination of characters and numbers to suit your requirements. This will give the installer full access to all of the settings in 701 Server.



Operator Authorization Edit

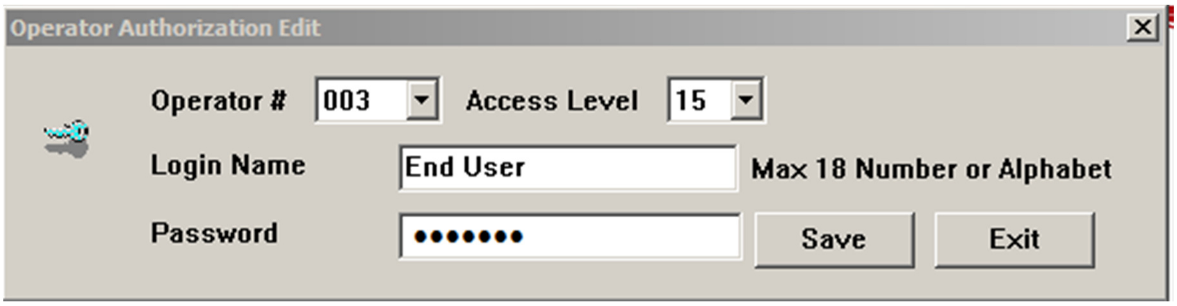
Operator # 002 Access Level 63

Login Name Installer Max 18 Number or Alphabet

Password ••••••••

All Customer Access

We recommend selecting Operator 003 from the drop down and setting the Access level to 15 as below. Login Name and Password are case sensitive and can be set to any combination of characters and numbers to suit your requirements. This will enable the end user to view controllers on line only with no ability to change any parameters.



Operator Authorization Edit

Operator # 003 Access Level 15

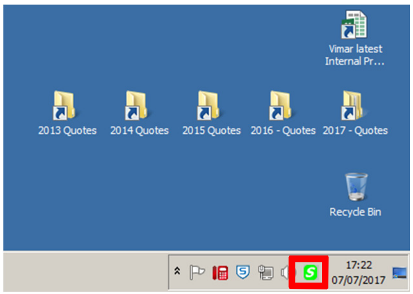
Login Name End User Max 18 Number or Alphabet

Password •••••••

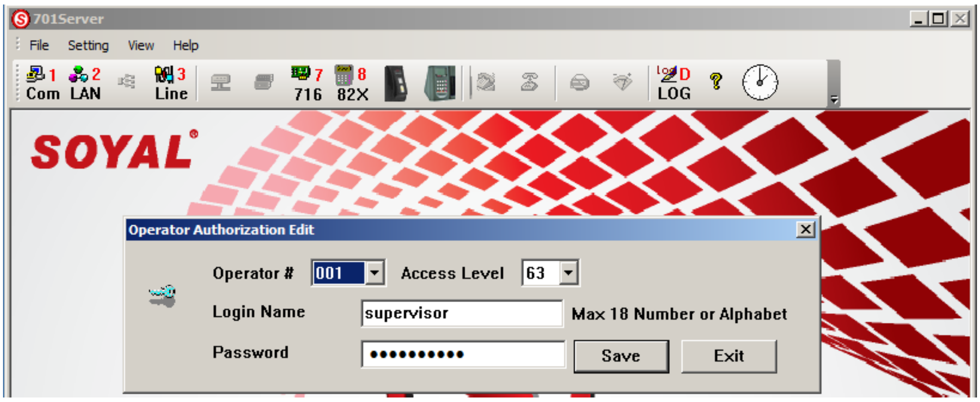
Up to 120 Operators can be set up each with unique Login Names, Passwords and Access Levels. Contact Raytel Technical if you require any further information on 701 Server Operator settings.

701 SERVER INITIAL SETTINGS

If the number of users is likely to exceed 5,000 proceed as follows:



**Open 701 Server by double clicking the S icon in the system tray (shown above)
Log in using the master password or your installer password as shown below.**



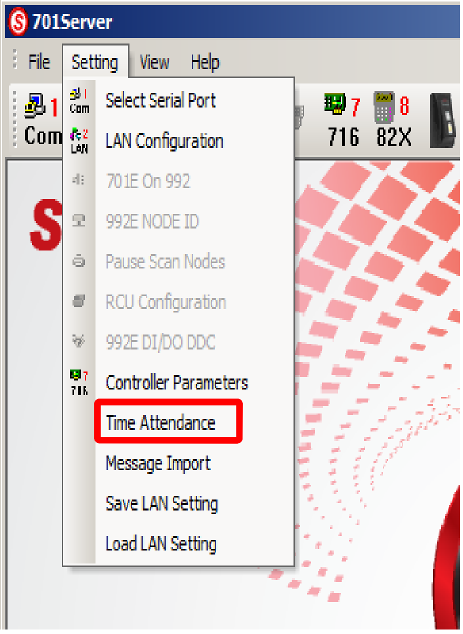
Operator Authorization Edit

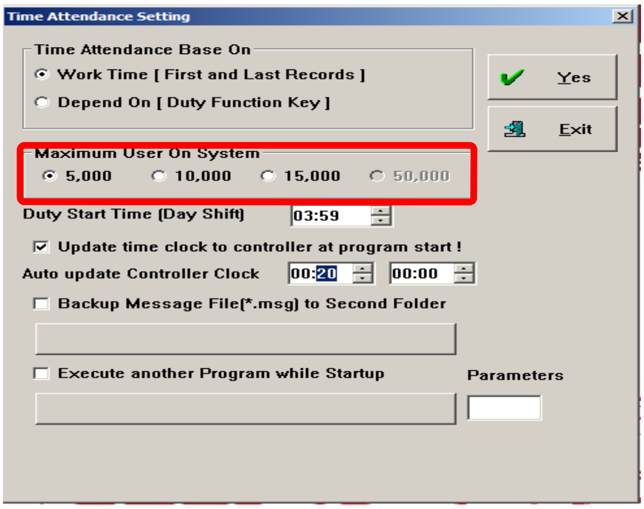
Operator # 001 Access Level 63

Login Name supervisor Max 18 Number or Alphabet

Password •••••••••• Save Exit

Once logged in select "Time Attendance" from the Setting menu. When the "Time Attendance" window opens you can select the Maximum number of users as shown below. Either click Yes to accept the modification or Exit if no changes are required.





Time Attendance Setting

Time Attendance Base On

● Work Time [First and Last Records]

○ Depend On [Duty Function Key]

Maximum User On System

● 5,000 ○ 10,000 ○ 15,000 ○ 50,000

Duty Start Time (Day Shift) 03:59

☑ Update time clock to controller at program start !

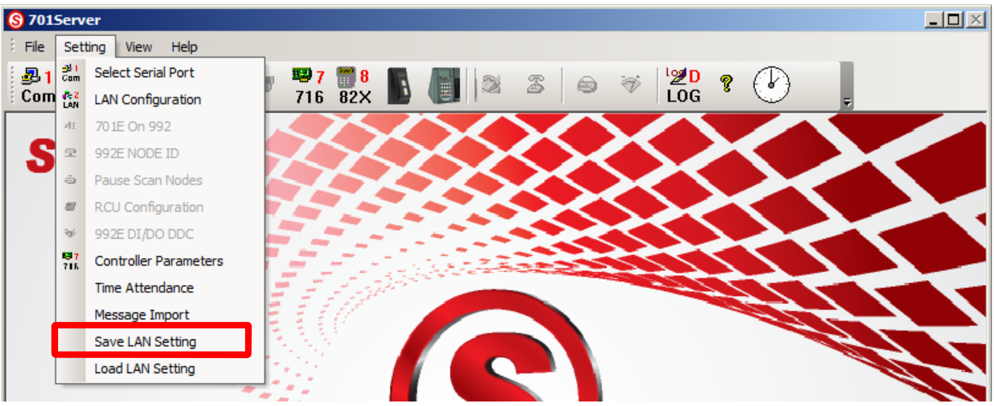
Auto update Controller Clock 00:20 00:00

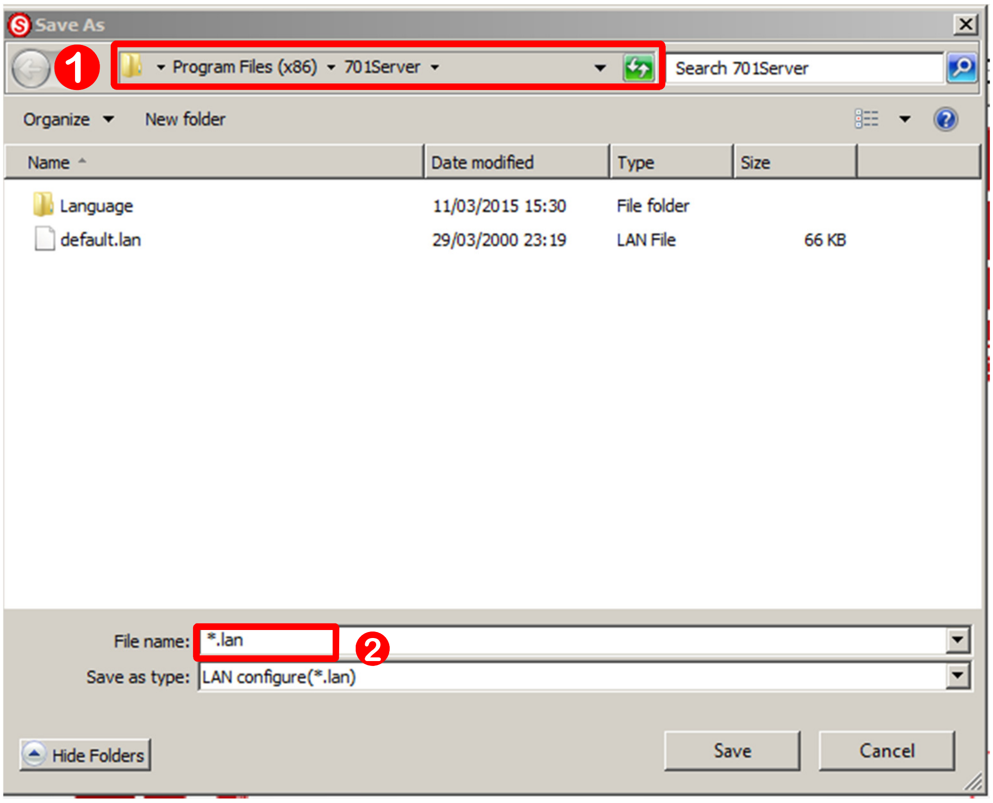
□ Backup Message File(*.msg) to Second Folder

□ Execute another Program while Startup Parameters

701 SERVER BACKING UP LAN CONFIGURATION

We would recommend making a copy of the LAN configuration once it is set up and functioning correctly. To do this initially create a folder on the desktop called "LAN settings" select "Save LAN Setting" from the 701 Server Setting drop down menu.

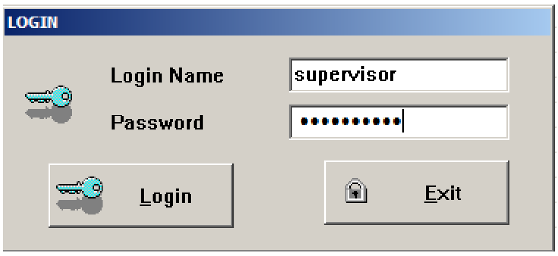




When the Save As window opens Navigate to the folder created earlier in the selection window identified above at 1, save the file as *****.lan where ****** is a title of your choosing selected by over writing * in the file name 2. Click on save, the window will close.**

701 CLIENT INITIAL CHECKS

To access 701Client software double click the short cut icon on the desktop or select 701Client from the "Start" menu.

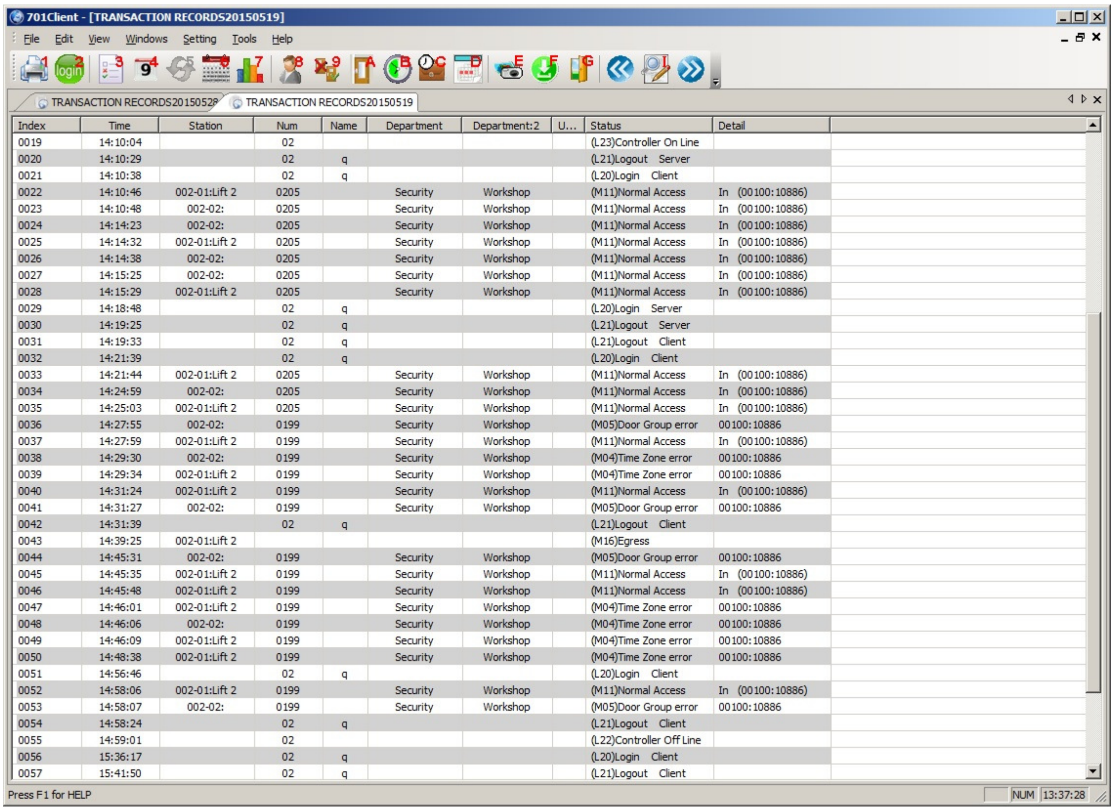


Login Name: supervisor

Password: ••••••••••

At the login screen use the Login Name "supervisor" and the Password "supervisor"

The initial screen will be as below, showing live current transaction Records.


701Client - [TRANSACTION RECORDS20150519]
File
Edit
View
Windows
Setting
Tools
Help
TRANSACTION RECORDS20150528
TRANSACTION RECORDS20150519

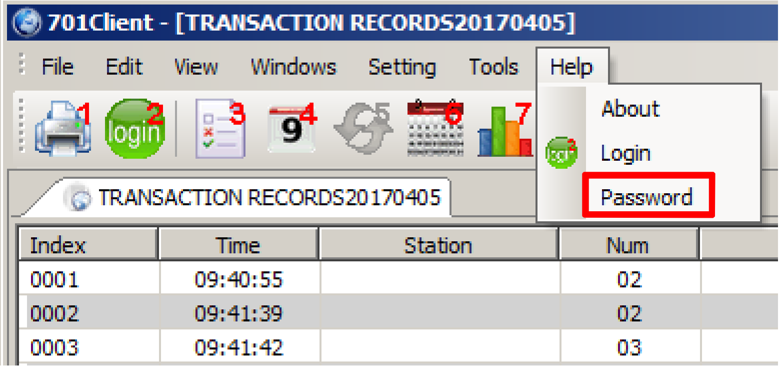
Index	Time	Station	Num	Name	Department	Department:2	U...	Status	Detail
0019	14:10:04		02					(L23)Controller On Line	
0020	14:10:29		02	q				(L21)Logout Server	
0021	14:10:38		02	q				(L20)Login Client	
0022	14:10:46	002-01:Lift 2	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0023	14:10:48	002-02:	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0024	14:14:23	002-02:	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0025	14:14:32	002-01:Lift 2	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0026	14:14:38	002-02:	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0027	14:15:25	002-02:	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0028	14:15:29	002-01:Lift 2	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0029	14:18:48		02	q				(L20)Login Server	
0030	14:19:25		02	q				(L21)Logout Server	
0031	14:19:33		02	q				(L21)Logout Client	
0032	14:21:39		02	q				(L20)Login Client	
0033	14:21:44	002-01:Lift 2	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0034	14:24:59	002-02:	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0035	14:25:03	002-01:Lift 2	0205		Security	Workshop		(M11)Normal Access	In (00100:10886)
0036	14:27:55	002-02:	0199		Security	Workshop		(M05)Door Group error	00100:10886
0037	14:27:59	002-01:Lift 2	0199		Security	Workshop		(M11)Normal Access	In (00100:10886)
0038	14:29:30	002-02:	0199		Security	Workshop		(M04)Time Zone error	00100:10886
0039	14:29:34	002-01:Lift 2	0199		Security	Workshop		(M04)Time Zone error	00100:10886
0040	14:31:24	002-01:Lift 2	0199		Security	Workshop		(M11)Normal Access	In (00100:10886)
0041	14:31:27	002-02:	0199		Security	Workshop		(M05)Door Group error	00100:10886
0042	14:31:39		02	q				(L21)Logout Client	
0043	14:39:25	002-01:Lift 2						(M16)Egress	
0044	14:45:31	002-02:	0199		Security	Workshop		(M05)Door Group error	00100:10886
0045	14:45:35	002-01:Lift 2	0199		Security	Workshop		(M11)Normal Access	In (00100:10886)
0046	14:45:48	002-01:Lift 2	0199		Security	Workshop		(M11)Normal Access	In (00100:10886)
0047	14:46:01	002-01:Lift 2	0199		Security	Workshop		(M04)Time Zone error	00100:10886
0048	14:46:06	002-02:	0199		Security	Workshop		(M04)Time Zone error	00100:10886
0049	14:46:09	002-01:Lift 2	0199		Security	Workshop		(M04)Time Zone error	00100:10886
0050	14:48:38	002-01:Lift 2	0199		Security	Workshop		(M04)Time Zone error	00100:10886
0051	14:56:46		02	q				(L20)Login Client	
0052	14:58:06	002-01:Lift 2	0199		Security	Workshop		(M11)Normal Access	In (00100:10886)
0053	14:58:07	002-02:	0199		Security	Workshop		(M05)Door Group error	00100:10886
0054	14:58:24		02	q				(L21)Logout Client	
0055	14:59:01		02					(L22)Controller Off Line	
0056	15:36:17		02	q				(L20)Login Client	
0057	15:41:50		02	q				(L21)Logout Client	

Press F1 for HELP NUM 13:37:28

The first check we would recommend is to present a token to all readers and/or controllers in the system to confirm details are logged on the Transaction Records screen. If transactions are not recognised ensure the correct time and date information has been downloaded to the controllers (see p30 of the Soyal Software Installation and setup Manual, or p11 of this manual) re-present a token to all readers and/or controllers and confirm the transactions are recognised.

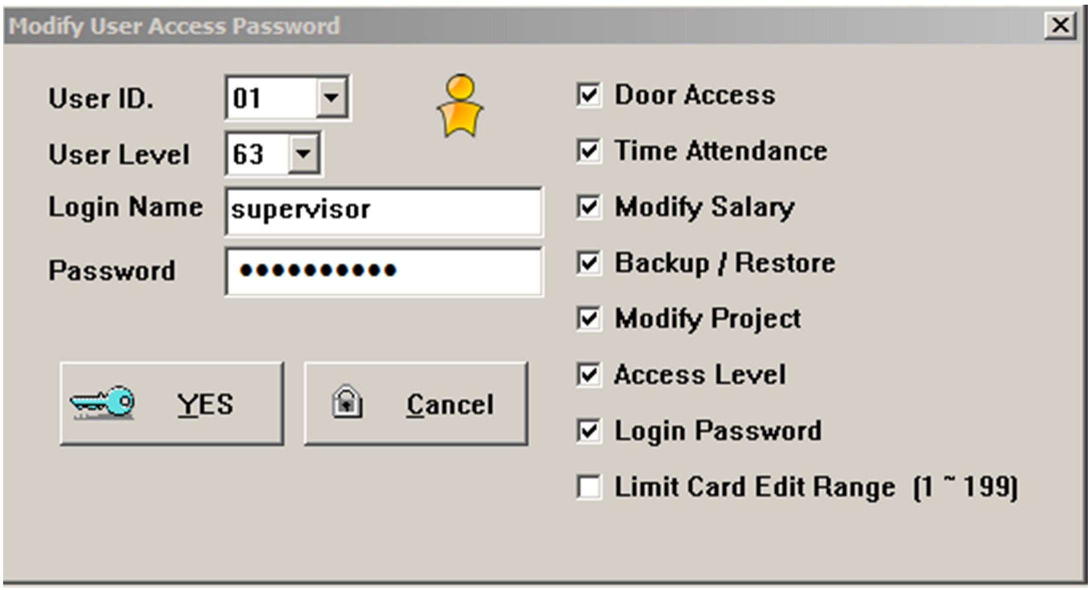
701 CLIENT ACCESS LEVELS

Once 701 Client is confirmed as functional with the previous checks we would recommend setting access levels for installer and user. To set access levels select “Password” from the “Help” menu as shown below.


701Client - [TRANSACTION RECORDS20170405]
File
Edit
View
Windows
Setting
Tools
Help
1
login 2
3
4
5
6
7
About
Login
Password
TRANSACTION RECORDS20170405

Index	Time	Station	Num
0001	09:40:55		02
0002	09:41:39		02
0003	09:41:42		03

Once Password has been selected the “Modify User Access Password” screen will open as shown below.



User ID. 01

User Level 63

Login Name supervisor

Password ●●●●●●●●●●

☑ Door Access
☑ Time Attendance
☑ Modify Salary
☑ Backup / Restore
☑ Modify Project
☑ Access Level
☑ Login Password
☐ Limit Card Edit Range (1 ~ 199)

We would recommend setting User ID. 02 for you the installer with exactly the same parameters as above, select a suitable Login Name and Password. Please note that both Login Name and Password are case sensitive. Set additional Software User ID’s to suit the requirements of your customer (up to 100 ID’s can be set) Please refer to the next pages for information on access levels.

701 CLIENT ACCESS LEVELS

There are a number of different parameters that you may or may not wish your customer to be able to modify. These are:

User card details - including modifying user details and the access rights of the user.

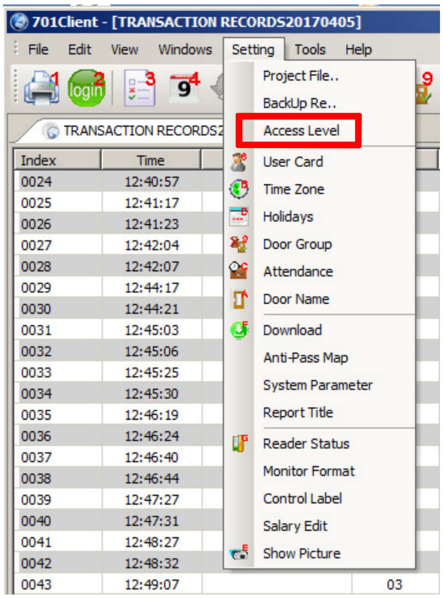
Time zones - These can be pre set by the installer OR they can be available for the user to set and modify.

Door Names - These can be pre set by the installer OR they can be available for the user to set and modify.

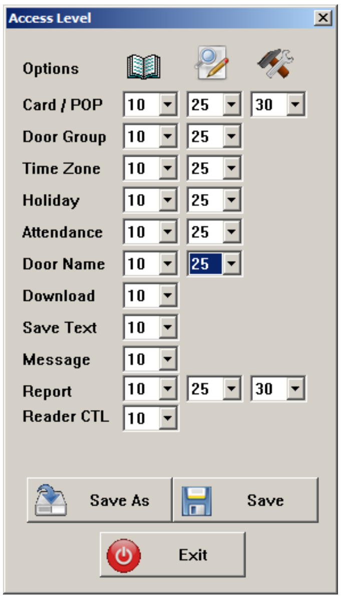
Door Groups - These can be pre set by the installer OR they can be available for the user to set and modify.

Download data to controllers - You may or may not wish your customer to be able to download modified data to controllers.

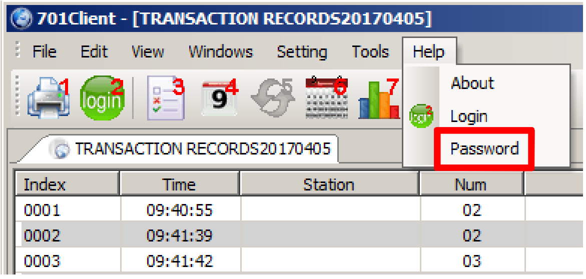
By configuring “Access Levels” and “User Access Password” you can prevent modification to certain data whilst still allowing it to be viewed. The software “Access Level” can be selected as shown below, the “User Access Password” can be selected as previously described. See next page for recommended settings.



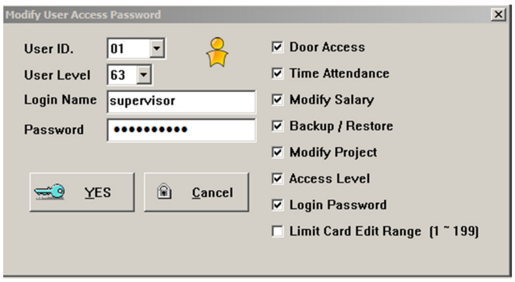
Index	Time	
0024	12:40:57	
0025	12:41:17	
0026	12:41:23	
0027	12:42:04	
0028	12:42:07	
0029	12:44:17	
0030	12:44:21	
0031	12:45:03	
0032	12:45:06	
0033	12:45:25	
0034	12:45:30	
0035	12:46:19	
0036	12:46:24	
0037	12:46:40	
0038	12:46:44	
0039	12:47:27	
0040	12:47:31	
0041	12:48:27	
0042	12:48:32	
0043	12:49:07	03



Options			
Card / POP	10	25	30
Door Group	10	25	
Time Zone	10	25	
Holiday	10	25	
Attendance	10	25	
Door Name	10	25	
Download	10		
Save Text	10		
Message	10		
Report	10	25	30
Reader CTL	10		


701Client - [TRANSACTION RECORDS20170405]
File
Edit
View
Windows
Setting
Tools
Help
About
Login
Password
TRANSACTION RECORDS20170405

Index	Time	Station	Num
0001	09:40:55		02
0002	09:41:39		02
0003	09:41:42		03



User ID. 01

User Level 63

Login Name supervisor

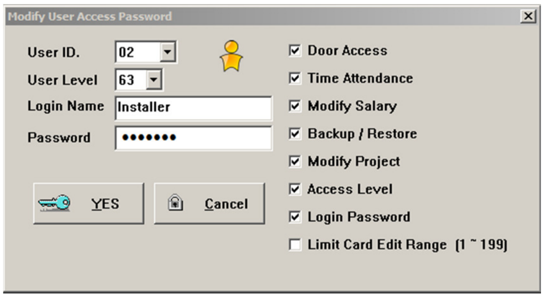
Password ••••••••••

☑ Door Access
☑ Time Attendance
☑ Modify Salary
☑ Backup / Restore
☑ Modify Project
☑ Access Level
☑ Login Password
☐ Limit Card Edit Range (1 ~ 199)

701 CLIENT ACCESS LEVELS

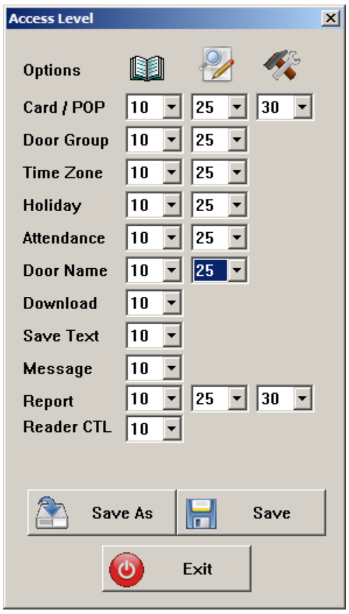
** Do not change the access parameters for User ID 01**
The following combinations of Access Levels and User Access Passwords are suggested for the Access rights described.

Recommended for Installer (User ID 02)
Set parameters as detailed below:
Login Name and Password can be selected to suit individual preferences.



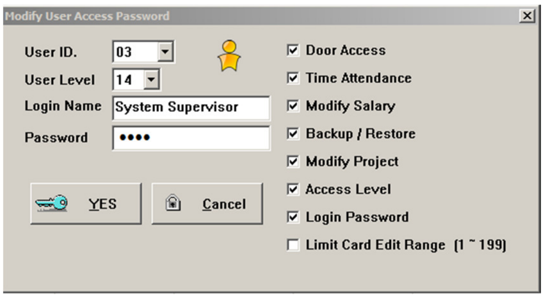
User ID. 02
User Level 63
Login Name Installer
Password •••••••

☑ Door Access
☑ Time Attendance
☑ Modify Salary
☑ Backup / Restore
☑ Modify Project
☑ Access Level
☑ Login Password
□ Limit Card Edit Range (1 ~ 199)



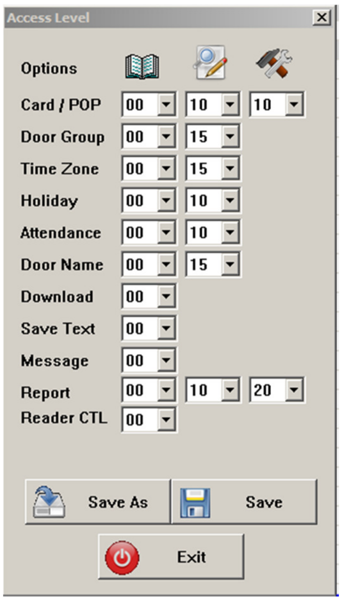
Options			
Card / POP	10	25	30
Door Group	10	25	
Time Zone	10	25	
Holiday	10	25	
Attendance	10	25	
Door Name	10	25	
Download	10		
Save Text	10		
Message	10		
Report	10	25	30
Reader CTL	10		

Recommended for Customer (User ID 03)
With the need to modify/add/delete user data and download data to controllers set parameters as detailed below:
Login Name and Password can be selected to suit individual preferences.



User ID. 03
User Level 14
Login Name System Supervisor
Password ••••

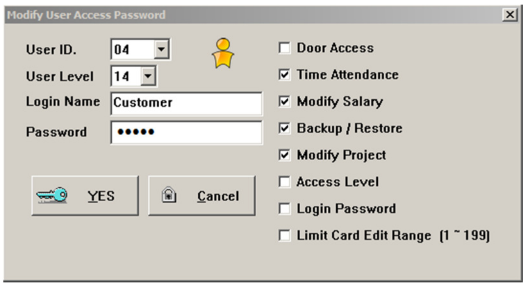
☑ Door Access
☑ Time Attendance
☑ Modify Salary
☑ Backup / Restore
☑ Modify Project
☑ Access Level
☑ Login Password
□ Limit Card Edit Range (1 ~ 199)



Options			
Card / POP	00	10	10
Door Group	00	15	
Time Zone	00	15	
Holiday	00	10	
Attendance	00	10	
Door Name	00	15	
Download	00		
Save Text	00		
Message	00		
Report	00	10	20
Reader CTL	00		

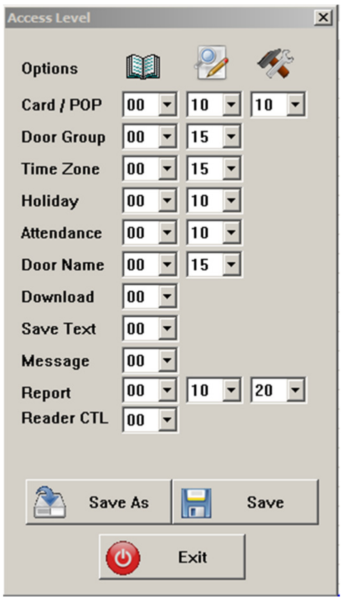
701 CLIENT ACCESS LEVELS

Recommended for Customer (User ID 04)
With the need to view user data, daily event logs and run reports from the database
Login Name and Password can be selected to suit individual preferences.


Modify User Access Password

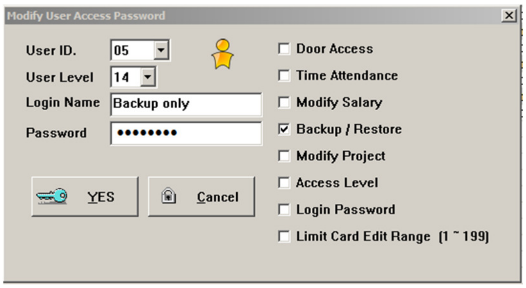
User ID.	04
User Level	14
Login Name	Customer
Password	•••••

☐ Door Access
☑ Time Attendance
☑ Modify Salary
☑ Backup / Restore
☑ Modify Project
☐ Access Level
☐ Login Password
☐ Limit Card Edit Range (1 ~ 199)


Access Level

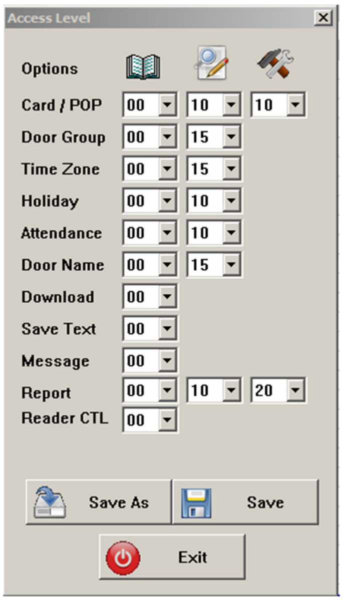
Options			
Card / POP	00	10	10
Door Group	00	15	
Time Zone	00	15	
Holiday	00	10	
Attendance	00	10	
Door Name	00	15	
Download	00		
Save Text	00		
Message	00		
Report	00	10	20
Reader CTL	00		

Recommended for Concierge (User ID 05)
To carry out day to day monitoring and backup the database.
Login Name and Password can be selected to suit individual preferences


Modify User Access Password

User ID.	05
User Level	14
Login Name	Backup only
Password	••••••••

☐ Door Access
☐ Time Attendance
☐ Modify Salary
☑ Backup / Restore
☐ Modify Project
☐ Access Level
☐ Login Password
☐ Limit Card Edit Range (1 ~ 199)

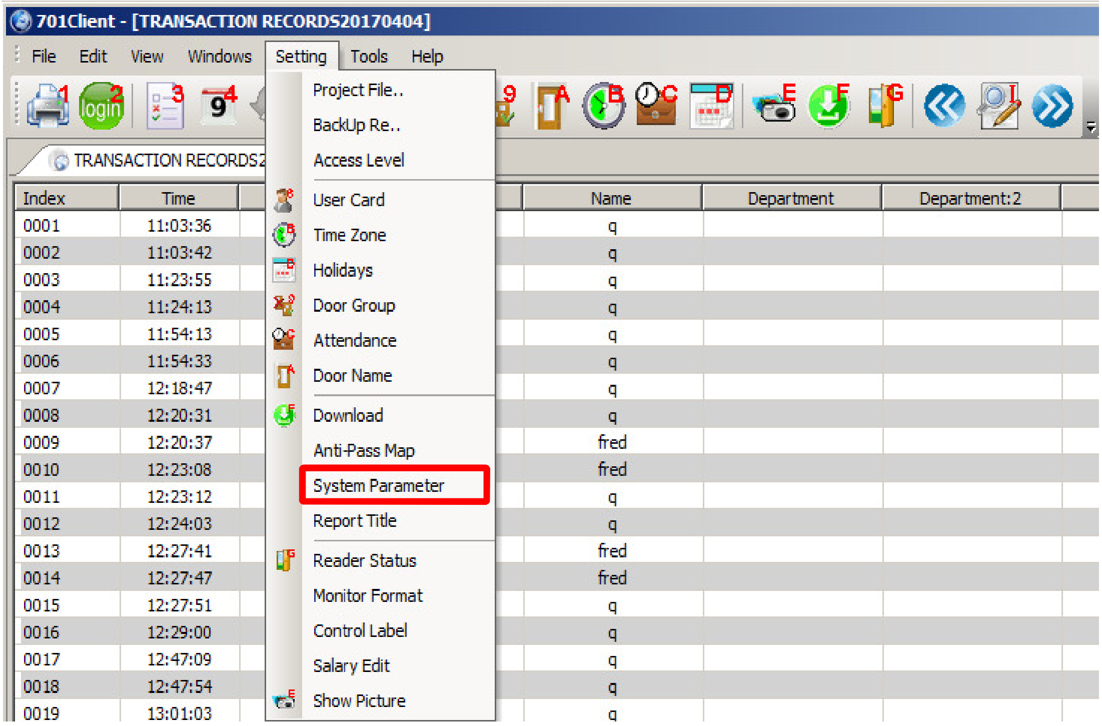

Access Level

Options			
Card / POP	00	10	10
Door Group	00	15	
Time Zone	00	15	
Holiday	00	10	
Attendance	00	10	
Door Name	00	15	
Download	00		
Save Text	00		
Message	00		
Report	00	10	20
Reader CTL	00		

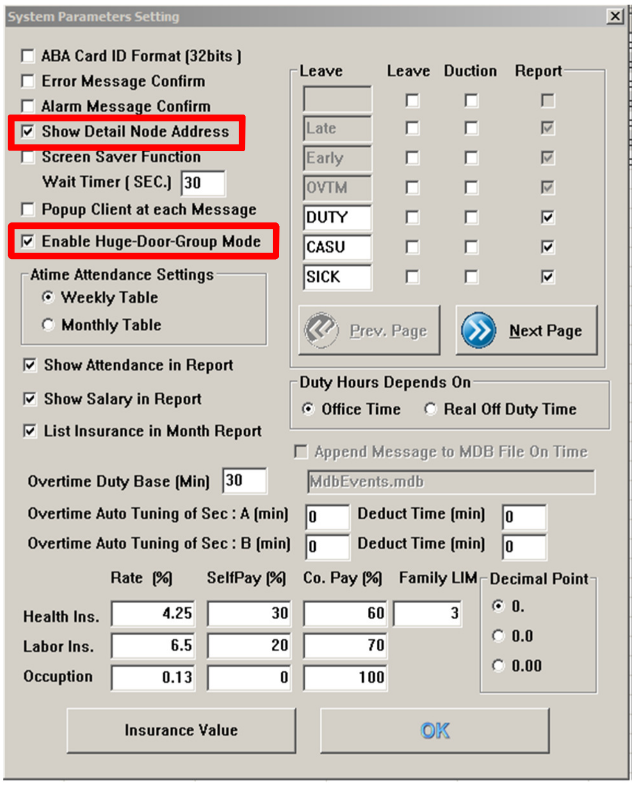
For other 701 Client user access levels please consult Raytel Technical support.

701 CLIENT INITIAL SETTINGS

For systems with more than one door select “System Parameter” from the “Setting” menu as shown below.



Index	Time	Name	Department	Department:2
0001	11:03:36	q		
0002	11:03:42	q		
0003	11:23:55	q		
0004	11:24:13	q		
0005	11:54:13	q		
0006	11:54:33	q		
0007	12:18:47	q		
0008	12:20:31	q		
0009	12:20:37	fred		
0010	12:23:08	fred		
0011	12:23:12	q		
0012	12:24:03	q		
0013	12:27:41	fred		
0014	12:27:47	fred		
0015	12:27:51	q		
0016	12:29:00	q		
0017	12:47:09	q		
0018	12:47:54	q		
0019	13:01:03	q		



☐ ABA Card ID Format (32bits)
☐ Error Message Confirm
☐ Alarm Message Confirm
☑ Show Detail Node Address
☐ Screen Saver Function
Wait Timer (SEC.) 30
☐ Popup Client at each Message
☑ Enable Huge-Door-Group Mode

Atime Attendance Settings
● Weekly Table
○ Monthly Table

☑ Show Attendance in Report
☑ Show Salary in Report
☑ List Insurance in Month Report

Overtime Duty Base (Min) 30
Overtime Auto Tuning of Sec : A (min) 0 Deduct Time (min) 0
Overtime Auto Tuning of Sec : B (min) 0 Deduct Time (min) 0

Leave	Leave	Duction	Report
	☐	☐	☐
Late	☐	☐	☑
Early	☐	☐	☑
OVTM	☐	☐	☑
DUTY	☐	☐	☑
CASU	☐	☐	☑
SICK	☐	☐	☑

Duty Hours Depends On
● Office Time ○ Real Off Duty Time

☐ Append Message to MDB File On Time
MdbEvents.mdb

	Rate (%)	SelfPay (%)	Co. Pay (%)	Family LIM
Health Ins.	4.25	30	60	3
Labor Ins.	6.5	20	70	
Occuption	0.13	0	100	

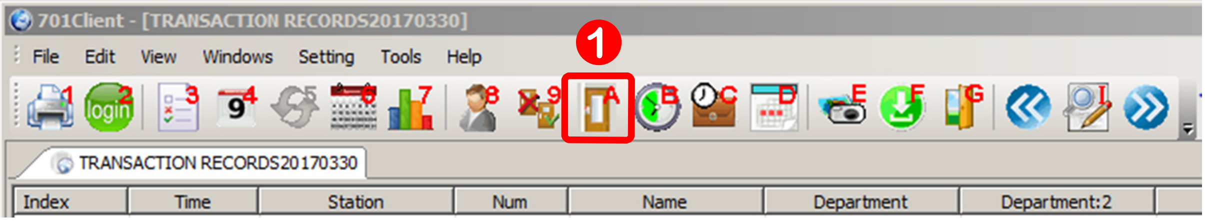
Decimal Point
● 0.
○ 0.0
○ 0.00

When the “System Parameter Setting” window opens put a tick in the “Enable Huge Door Group Mode” as shown to the left. Click “OK” to close the window.

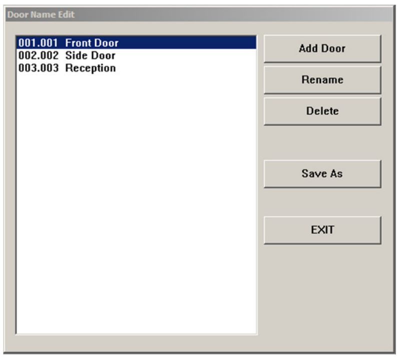
For diagnostics purposes it can be useful to select “Show Detail Node Address” This will provide more detail in the Transaction Records window.

NAMING DOORS (OPTIONAL)

Doors can be named to provide user friendly identification i.e. Main Front Door, Side Door etc. To name doors proceed as follows:



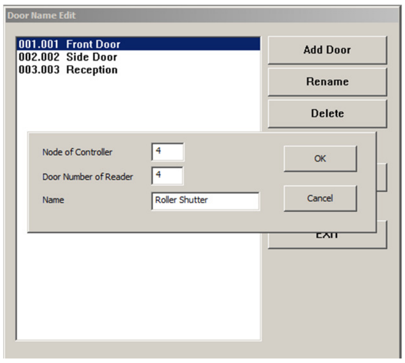
Click “Door Name edit” A as above. 1



001.001 Front Door
002.002 Side Door
003.003 Reception

The Door Name Editor window will open as shown above.
To add a door and name it click on “Add Door” and see below.
To rename an existing door, highlight the door to be renamed and click on “Rename”
To delete a named door highlight the door to be deleted and select “Delete”

There is no need to Save any of the changes above, the 701 Client software automatically saves any changes in this
window. Simply select Exit when finished.



001.001 Front Door
002.002 Side Door
003.003 Reception

Node of Controller 4
Door Number of Reader 4
Name Roller Shutter

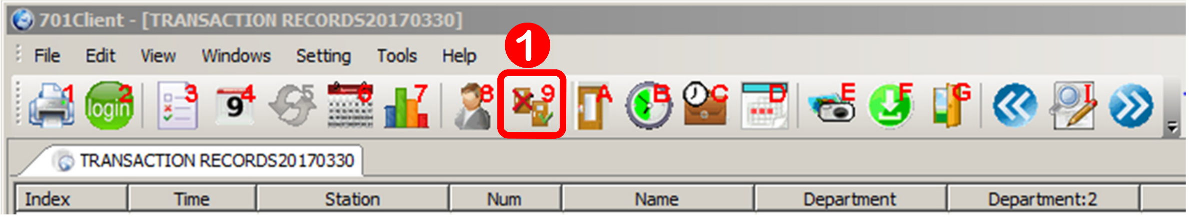
If you are naming a door or renaming a door the window above will open. If you have followed our recommendations on page 6 the format will be:

H series controllers
Node of controller=Node ID of controller, Door No of Reader=1
E Series controllers
Node of Controller=Node ID of controller, Door No of Reader=node ID of controller.
Multi Door Controllers
Node of Controller=Node ID of controller, Door No of Reader=1 or 2 dependant on door
K50 and AR-888H Keypad Controllers
Node of Controller=Node ID of controller, Door No of Reader=1

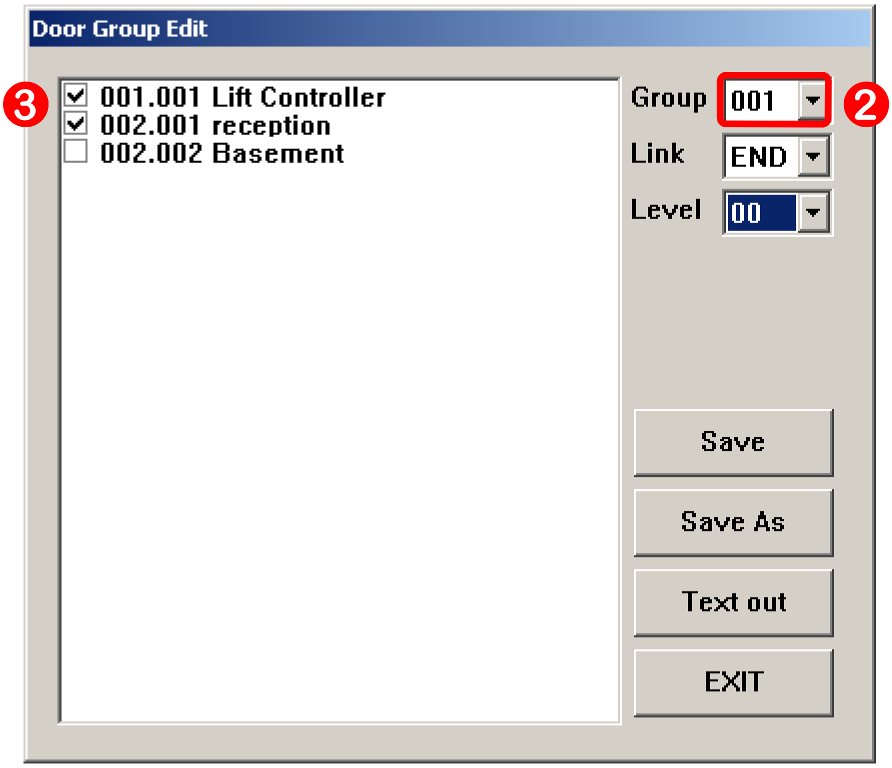
“Name” = the name you allocate to the door.
If you are renaming a door simply highlight the name and over write it.

DOOR GROUPS (OPTIONAL)

Access through doors can be restricted so that certain users are only allowed through certain doors. This is done by allocating users to Door Groups. You may wish to pre-configure Door Groups as follows:


701Client - [TRANSACTION RECORDS20170330]
File Edit View Windows Setting Tools Help
1
login
1 2 3 4 5 6 7 8 9 A B C D E F G I
TRANSACTION RECORDS20170330
Index Time Station Num Name Department Department:2

❶ To modify Door Groups Click button 9 “Door Group Edit”, the Door Group Edit window will open as shown below:



☑ 001.001 Lift Controller
☑ 002.001 reception
□ 002.002 Basement

Group 001
Link END
Level 00

The Door Group can be selected by number on the drop down shown at ❷
Each Door Group can contain any of the Doors that are named on the system. Doors that are ticked as in ❸ above are part of that Door Group.

Up to 255 Door Groups can be created.

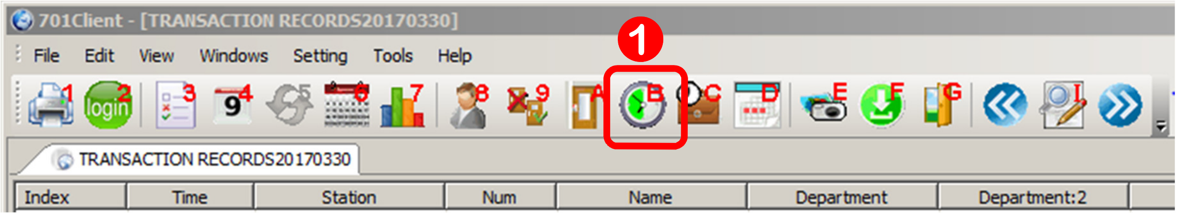
For basic Door Groups LINK should be left set at END and the Level should remain set at 00

For more complex Door Group configurations refer to Raytel Technical.

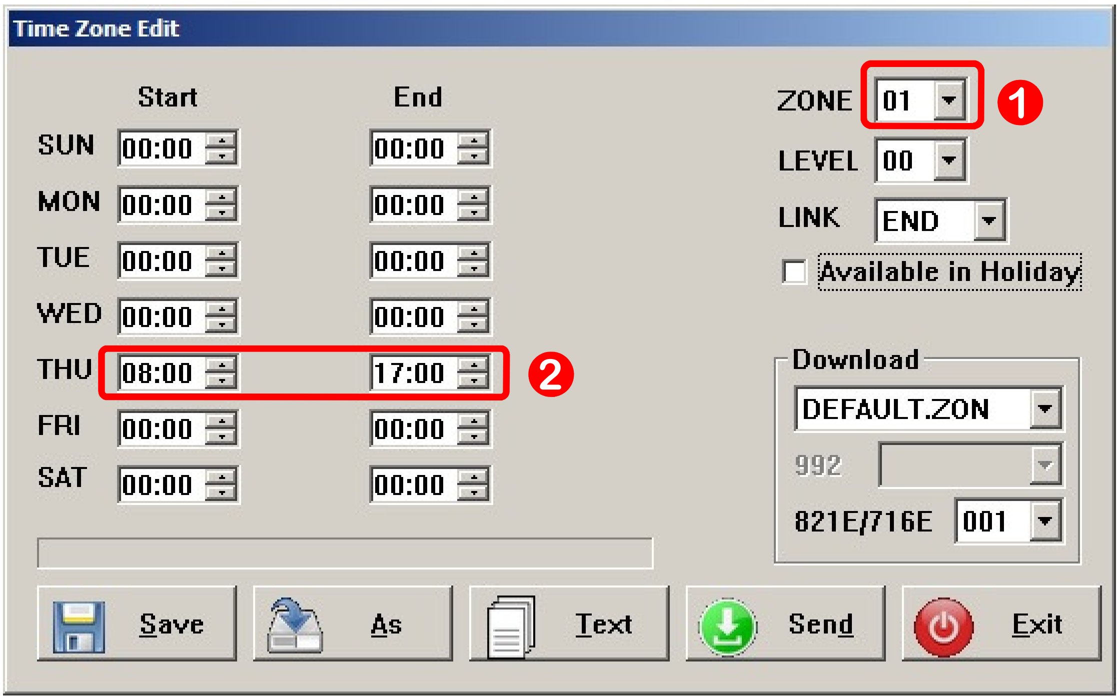
If the Door Group is set for a user in the ‘User Card Edit Screen’ the user will be able to access the doors selected within the “Door Group”

TIME ZONES (OPTIONAL)

Users can be allowed access by Time Zones. This enables access only at certain times and can also be configured so that access is restricted by day or a combination of time and day. For example a cleaner could be allowed access only between Monday to Friday from 5:00 AM to 7:00 AM To set time zones proceed as follows:


701Client - [TRANSACTION RECORDS20170330]
File Edit View Windows Setting Tools Help
1
login 2
3
4
7
8
9
A
B
C
D
E
F
G
I
TRANSACTION RECORDS20170330
Index
Time
Station
Num
Name
Department
Department:2

❶ To access and modify Time Zone settings click button B "Time Zone Edit" The "Time Zone Edit" window will open as shown below:


Time Zone Edit

	Start	End
SUN	00:00	00:00
MON	00:00	00:00
TUE	00:00	00:00
WED	00:00	00:00
THU	08:00	17:00
FRI	00:00	00:00
SAT	00:00	00:00

ZONE 01

LEVEL 00

LINK END

□ Available in Holiday

Download

DEFAULT.ZON

992

821E/716E 001

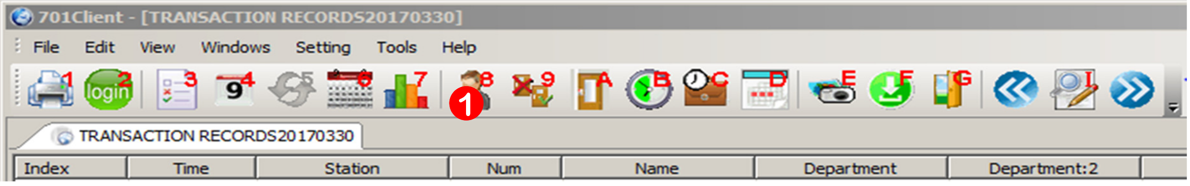
In this example Time Zone 1 ❶ is enabled for Thursday only between 8:00 AM and 5:00 PM Shown at ❷
By using the drop down menu at ❶ the different Time Zones can be set. Time Zones can be allocated to users on the User card Edit screen as shown on Page 25.

Up to 63 Time Zones can be created. For basic Time Zone setting the Level should remain at 00 and the LINK should be set to END.

For more complex Time Zone programming refer to Raytel Technical

ADDING AND MANAGING USERS

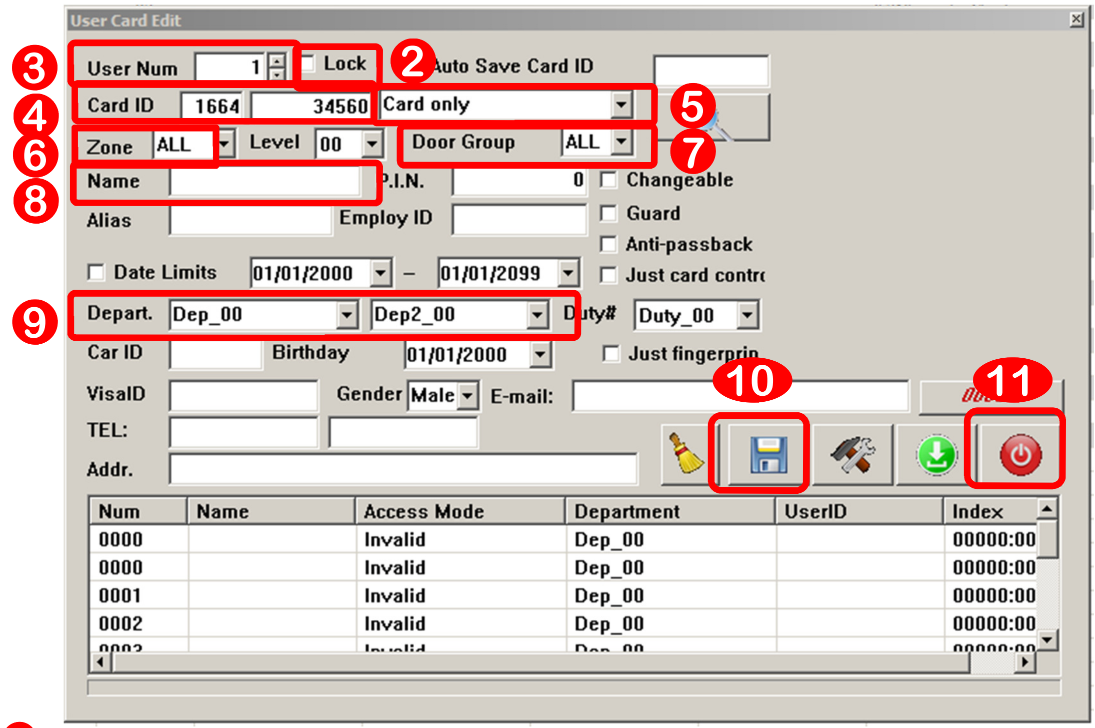
Tokens can be added individually or in sequential batches.



701Client - [TRANSACTION RECORDS20170330]

Index	Time	Station	Num	Name	Department	Department:2

1 Click button 8 “Users”, the User Card Edit window will open.



User Card Edit

User Num 1 □ Lock

Auto Save Card ID

Card ID 1664 34560 Card only

Zone ALL Level 00 Door Group ALL

Name P.I.N. 0 □ Changeable

Alias Employ ID □ Guard

□ Anti-passback

□ Date Limits 01/01/2000 – 01/01/2099 □ Just card contro

Depart. Dep_00 Dep2_00 Duty# Duty_00

Car ID Birthday 01/01/2000 □ Just fingerprin

VisaID Gender Male E-mail:

TEL:

Addr.

Num	Name	Access Mode	Department	UserID	Index
0000		Invalid	Dep_00		00000:00
0000		Invalid	Dep_00		00000:00
0001		Invalid	Dep_00		00000:00
0002		Invalid	Dep_00		00000:00

2 Tick the “Lock” box, this locks the screen on a live system to enable adding, editing or deleting of tokens. If the screen is unlocked, it will jump to the user number of every valid token presented to a reader.

3 Select the relevant User Number with the up and down arrows.

4 Input the token number in the two boxes, the token number is made up of a Site Code and a Card Code. The Site Code goes in the left hand box and the Card Code goes in the right hand box (see picture below) If sequential tokens are to be added input the details of the lowest numbered token.

5 Select Card Only with the drop down arrow.

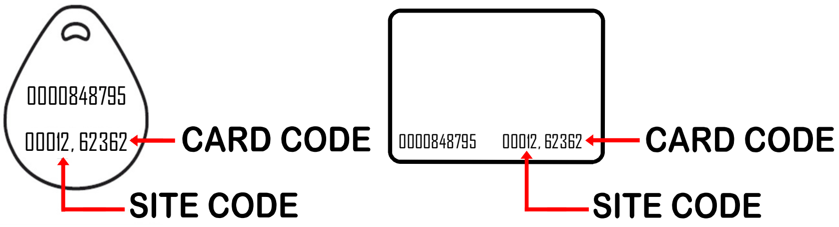
6 Select relevant Time Zone if set, if not required leave as default which is “ALL”

7 Select relevant Door Group if set, if not required leave as default which is “ALL”

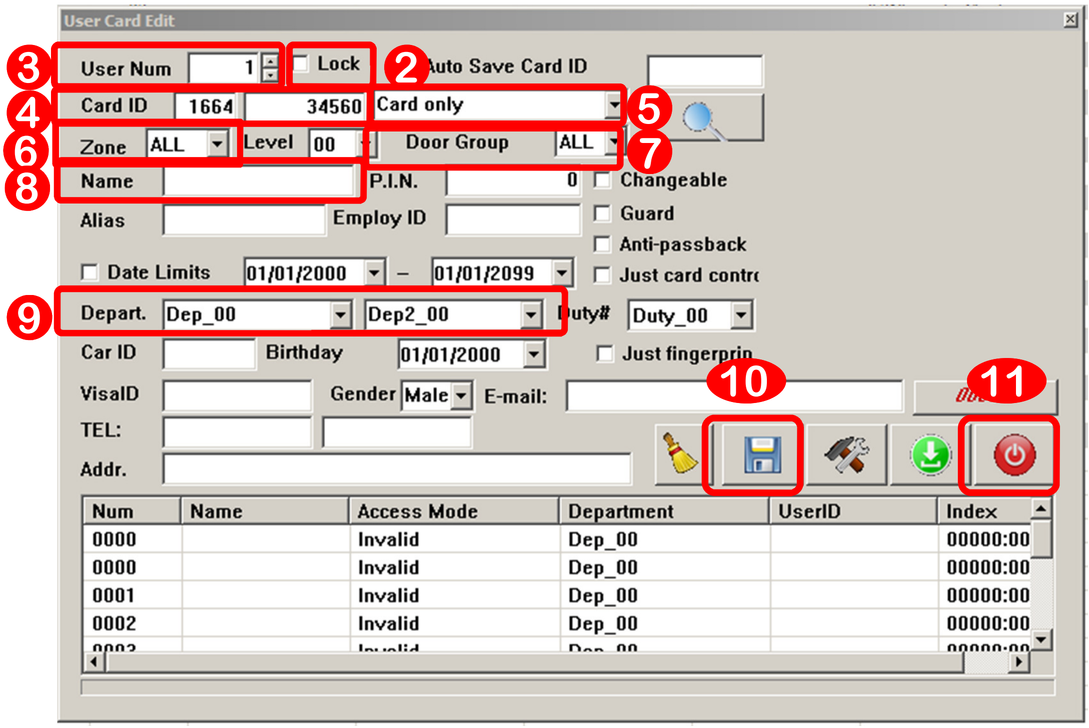
8 Enter Name of User if required.

9 Enter Department names if required. To edit the department names, highlight the text showing “ Dep_00” and “Dep2_00” and type in the required name.

10 Click Save. Once all card modifications are complete click Exit 11



ADDING AND MANAGING USERS



User Num 1 □ Lock Auto Save Card ID

Card ID 1664 34560 Card only

Zone ALL Level 00 Door Group ALL

Name P.I.N. 0 □ Changeable

Alias Employ ID □ Guard

□ Anti-passback

□ Date Limits 01/01/2000 – 01/01/2099 □ Just card contr

Depart. Dep_00 Dep2_00 Duty# Duty_00

Car ID Birthday 01/01/2000 □ Just fingerprin

VisaID Gender Male E-mail:

TEL:

Addr.

Num	Name	Access Mode	Department	UserID	Index
0000		Invalid	Dep_00		00000:00
0000		Invalid	Dep_00		00000:00
0001		Invalid	Dep_00		00000:00
0002		Invalid	Dep_00		00000:00
0003		Invalid	Dep_00		00000:00

Tick the “Lock” box, this locks the screen on a live system to enable adding, editing or deleting of tokens. If the screen is unlocked, it will jump to the user number of every valid token presented to a reader.

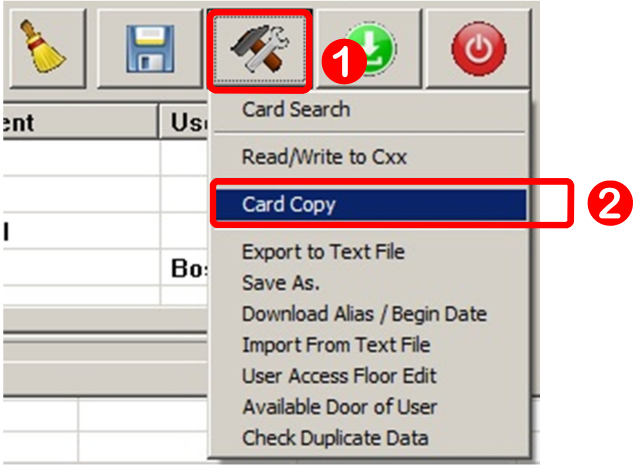
Select the relevant User Number with the up and down arrows.

If only the Name of the user ⑧ and department detail s ⑨ are being added then no download of data to controllers is required. These details are only stored in the 701 Client database. Simply save ⑩ any modifications.

If Card ID ④ Zone ⑥ or Door Group ⑦ have been modified then the modified data <u>must</u> be downloaded to the controllers.

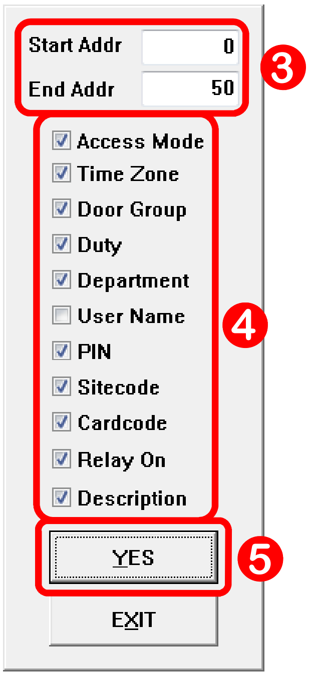
COPYING USER DETAILS

Multiple sequential Tokens can be added by entering the details of the lowest numbered Token and copying the details into the database using the Card Copy function.



1 Click on the "Tools" button.

2 Click "Card Copy", the following window will open.



Start Addr 0

End Addr 50

☑ Access Mode
☑ Time Zone
☑ Door Group
☑ Duty
☑ Department
□ User Name
☑ PIN
☑ Sitecode
☑ Cardcode
☑ Relay On
☑ Description

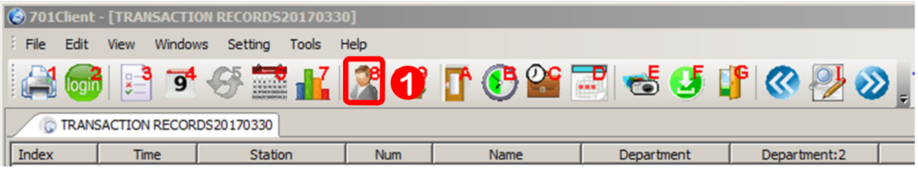
3 Enter the Start and End Addresses. The Start Address is the User Number of the Token to be copied, the End Address is the User Number of the final Token to be added. For example, If the Token to be copied is entered as User Number 14, and 20 Tokens need to be programmed, the Start Address is 14 and the End Address is 33.

4 Select the parameters as shown, leaving User Name unticked.

5 Click "YES", the Tokens will be copied into the database and the window will close.

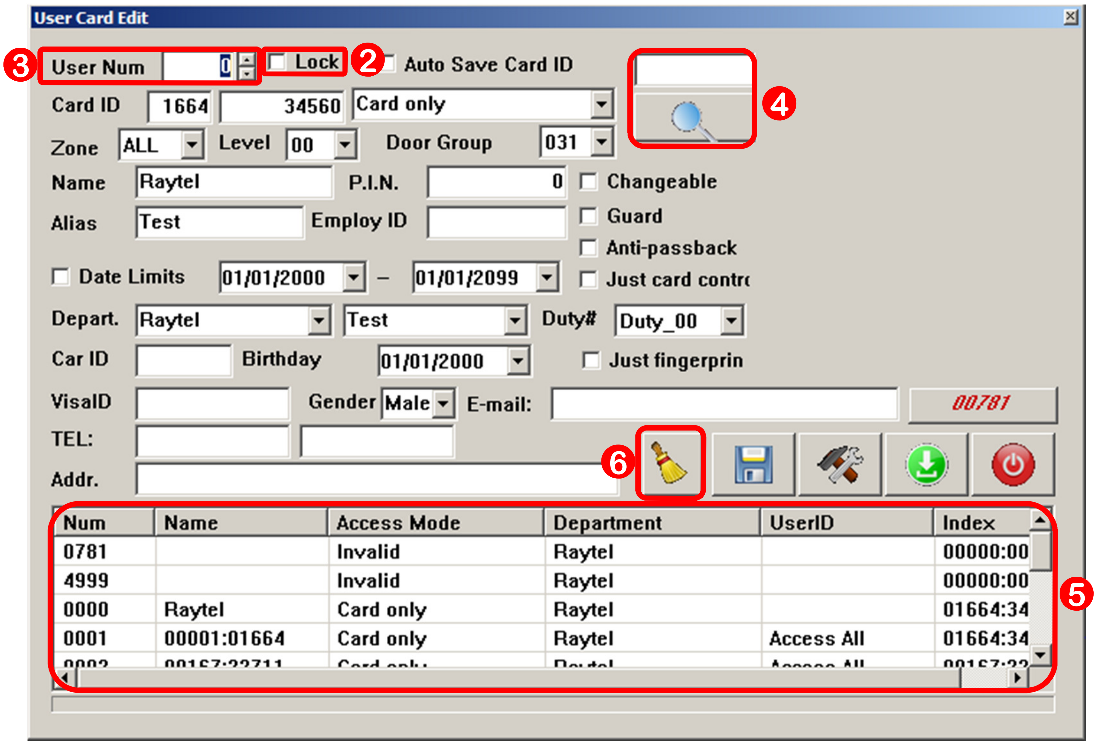
DELETING USER DETAILS

Tokens can be deleted individually or in sequential batches. To delete individual tokens:-



701Client - [TRANSACTION RECORDS20170330]

1 Click button 8 “Users”, the User Card Edit window will open.



User Card Edit

User Num: 0 ☐ Lock ☐ Auto Save Card ID

Card ID: 1664 34560 Card only

Zone: ALL Level: 00 Door Group: 031

Name: Raytel P.I.N.: 0 ☐ Changeable

Alias: Test Employ ID: ☐ Guard

☐ Anti-passback

☐ Date Limits 01/01/2000 – 01/01/2099 ☐ Just card contrc

Depart.: Raytel Test Duty#: Duty_00

Car ID: Birthday: 01/01/2000 ☐ Just fingerprin

VisaID: Gender: Male E-mail: 00781

TEL:

Addr.:

Num	Name	Access Mode	Department	UserID	Index
0781		Invalid	Raytel		00000:00
4999		Invalid	Raytel		00000:00
0000	Raytel	Card only	Raytel		01664:34
0001	00001:01664	Card only	Raytel	Access All	01664:34
0002	00167:22711	Card only	Raytel	Access All	00167:22

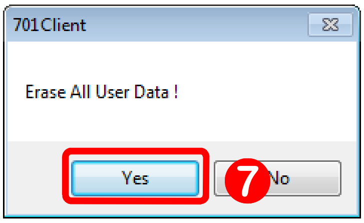
2 Tick the “Lock” box, this locks the screen on a live system to enable adding, editing or deleting of tokens. If the screen is unlocked, it will jump to the user number of every valid token presented to a reader.

3 Select the relevant User Number with the up and down arrows.

4 If the User Number is unknown, enter the User Name or Card Code of the token to be deleted in the search box and click the “Search “ button.

5 The search results will be shown in this section. To select the Token to be deleted, double click on the line containing the user data.

6 Click the “Clear Data Field” button, the following window will open.



701Client

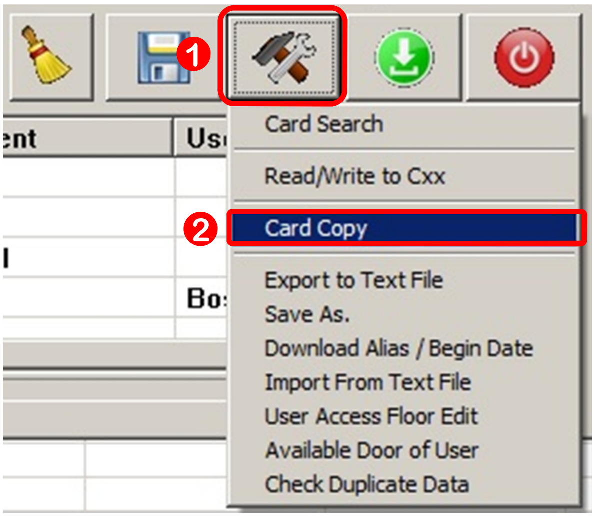
Erase All User Data !

7

Click the “Yes” button, the details for the current user card will be deleted. Repeat for all cards to be deleted.

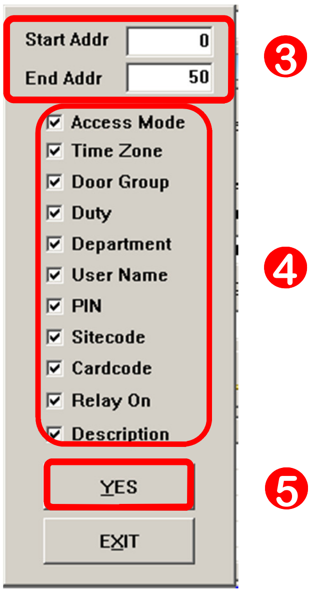
DELETING SEQUENTIAL USER DETAILS

Multiple sequential user details can be deleted by entering the details of the lowest numbered blank user and copying the details into the database using the card copy function. Delete all of the data for the lowest numbered user in the sequence as detailed on Page 28.
Then proceed as follows to remove all data from the range of user numbers selected.



❶ Click on the “Tools” button within the User Card Edit window.

❷ Select “Card Copy” from the drop down menu, the following window will open.



Start Addr 0
End Addr 50

☑ Access Mode
☑ Time Zone
☑ Door Group
☑ Duty
☑ Department
☑ User Name
☑ PIN
☑ Sitecode
☑ Cardcode
☑ Relay On
☑ Description

❸ Enter the start and end addresses. The start address will be the user number that had all data deleted earlier. The end address will be the address of the final token to be cleared.

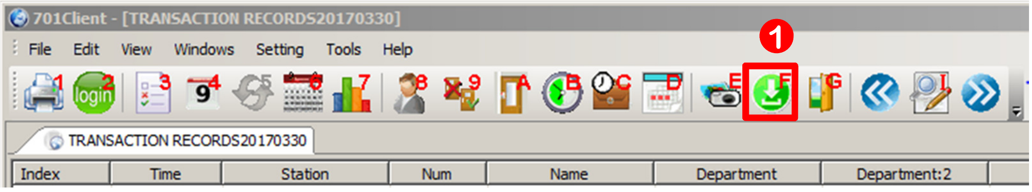
❹ Select all of the parameters as shown.

❺ Click “YES” the blank tokens will be copied into the database.

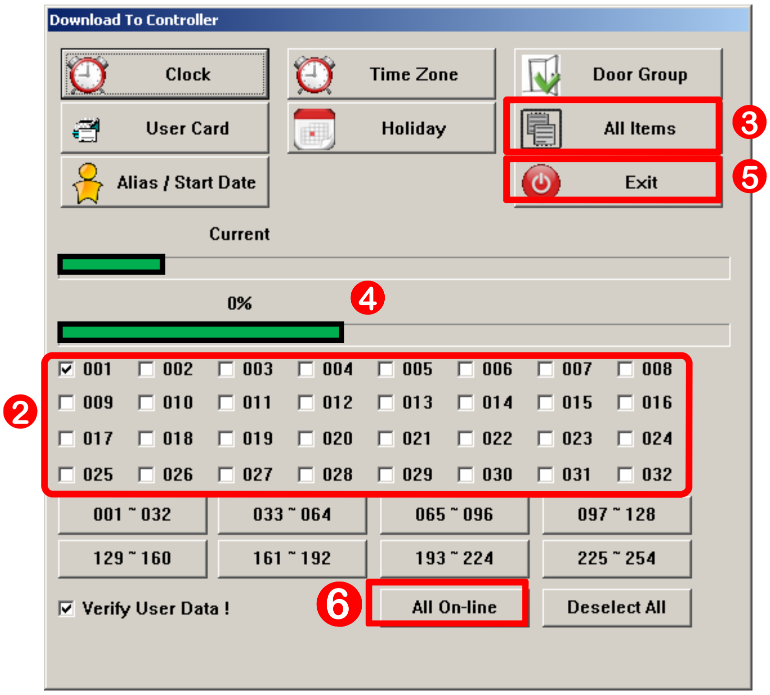
When the “Card Copy” window is closed the “User Card Edit” window will remain open. Either continue editing user data or Save and Exit.

DOWNLOADING ALL DATA TO ALL CONTROLLERS

Once changes have been made they must be downloaded to the controllers.



❶ Click button F “Download Data” the Download To Controller window will open.



☑ 001 □ 002 □ 003 □ 004 □ 005 □ 006 □ 007 □ 008
□ 009 □ 010 □ 011 □ 012 □ 013 □ 014 □ 015 □ 016
□ 017 □ 018 □ 019 □ 020 □ 021 □ 022 □ 023 □ 024
□ 025 □ 026 □ 027 □ 028 □ 029 □ 030 □ 031 □ 032

☑ Verify User Data !

❷ Select the controllers to be updated (If it is all controllers click “All On-Line” ❻

❸ Click “All Items” button.

❹ The green progress bars and percentage indicator will slowly increase.
When the downloads have finished the window will close.

❺ If you do not wish to continue with downloads click “Exit”

If you only wish to download specific areas of data i.e. Door groups then the individual buttons can be used.

It is important that the correct controllers are selected for the Download otherwise communication errors will occur.

“Clock” downloads time and date from the PC to controllers.
“Time Zone” downloads any Time Zone data that has been created or modified.
“Door Group” downloads any User Cards that have been created or modified.
“User Card” downloads any User Cards that have been created or modified.

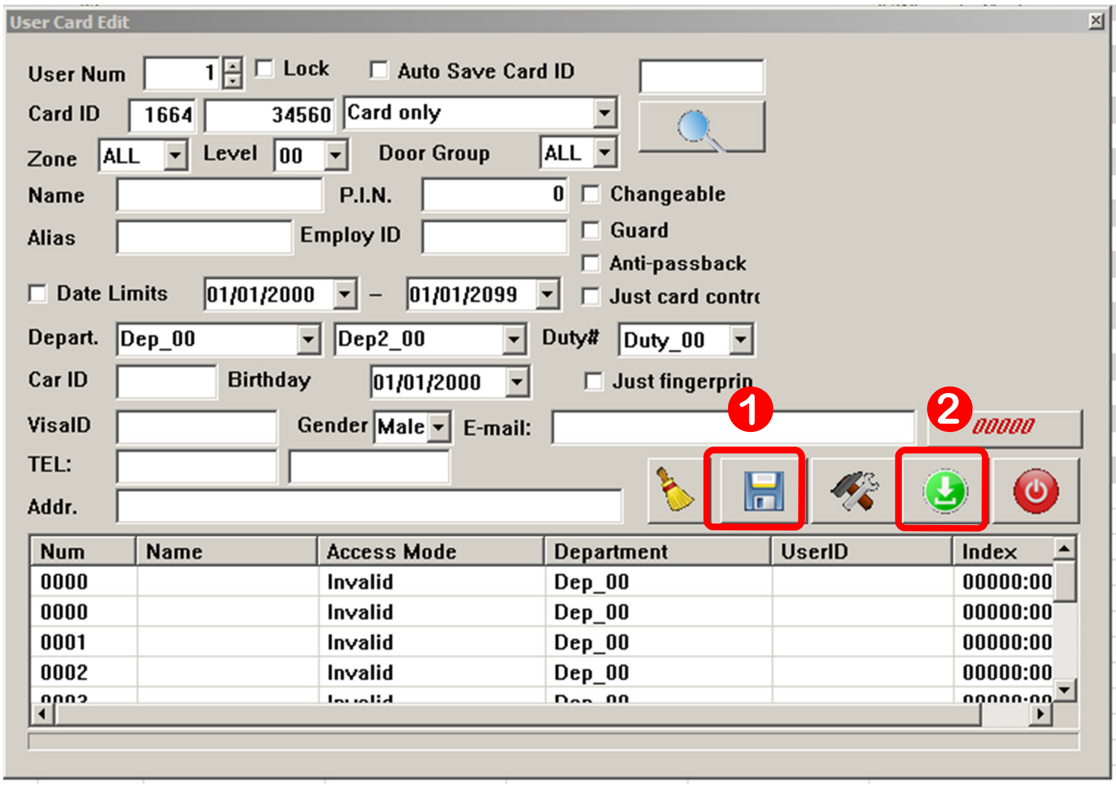
“Alias/Start Date” and “Holiday” are not currently used.

See the next page for downloading changes to User Data as it is modified.

DOWNLOADING INDIVIDUAL USER DETAILS

WARNING : We would recommend using the “Downloading all data to all controllers” process on page 30 unless there is a specific requirement to download individual user data.

Within the “User Card Edit” screen there is the ability to download changes to User Data as each record is modified. It is important that the correct controllers have already been selected in the previous section “downloading all data to all controllers”



User Num 1 □ Lock □ Auto Save Card ID

Card ID 1664 34560 Card only

Zone ALL Level 00 Door Group ALL

Name P.I.N. 0 □ Changeable

Alias Employ ID □ Guard

□ Anti-passback

□ Date Limits 01/01/2000 – 01/01/2099 □ Just card contr

Depart. Dep_00 Dep2_00 Duty# Duty_00

Car ID Birthday 01/01/2000 □ Just fingerprin

VisaID Gender Male E-mail: 00000

TEL:

Addr.

Num	Name	Access Mode	Department	UserID	Index
0000		Invalid	Dep_00		00000:00
0000		Invalid	Dep_00		00000:00
0001		Invalid	Dep_00		00000:00
0002		Invalid	Dep_00		00000:00
0003		Invalid	Dep_00		00000:00

Select the User Number of the record you wish to edit. Once all changes are completed click on the Save icon ❶

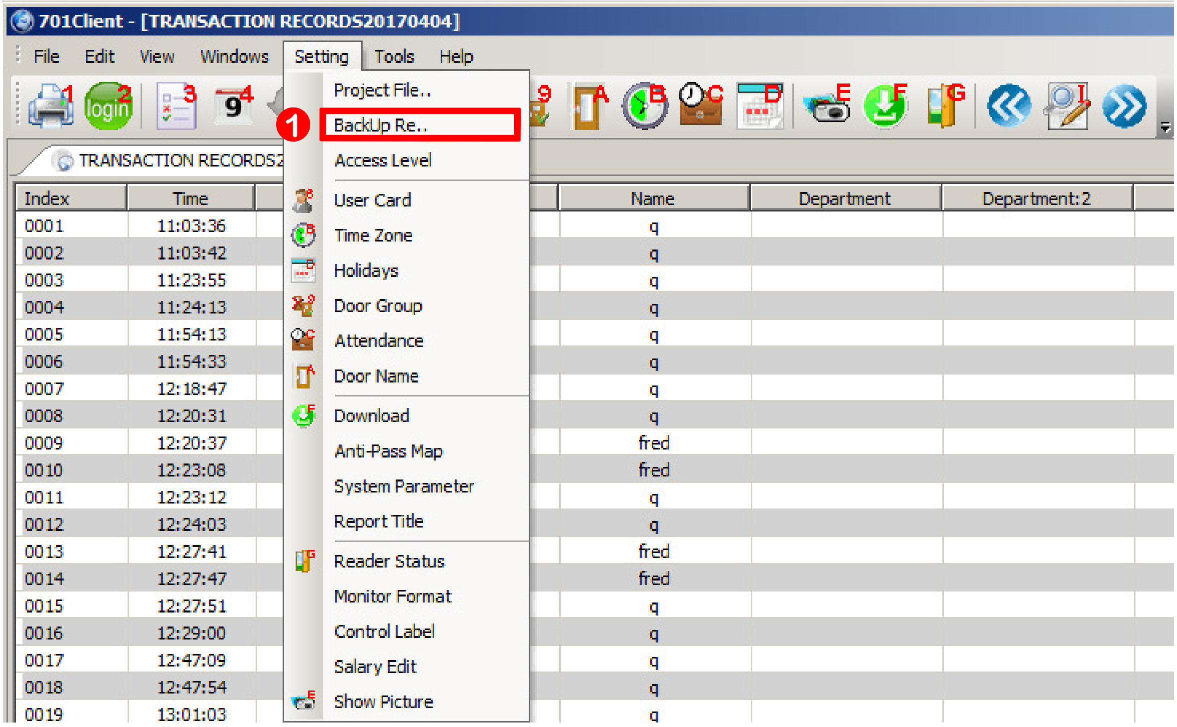
To download the details of the revised User Data to controllers click the Download Button ❷

Please note that only the single User Record showing on the screen will be downloaded to the controller(s) For any other Data downloads use the procedure identified on Page 30.

The correct Node identities of the controllers must be selected in the “Download Data to Controllers” window, see page 30. If the correct controllers are not identified data will not be downloaded to all connected controllers or a communication error will be reported.

BACKING UP THE DATABASE

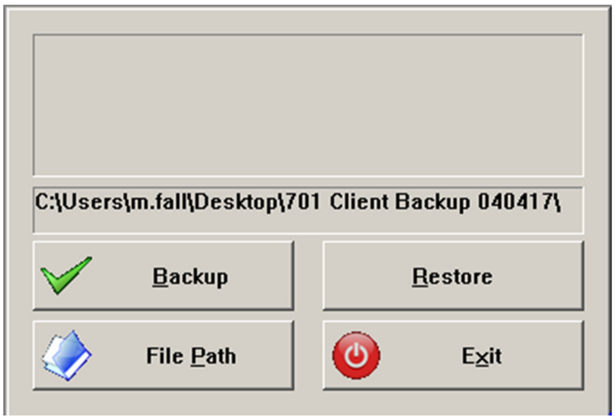
We would recommend backing up the database manually before any major changes are made and also on a regular schedule. Changes are stored within the 701 Client software automatically however a system crash or inadvertent deletion of data may render the software inoperable. Regular external backups will enable the system to be restored to the configuration at the time of the last backup. Before proceeding with the Backup process shown below create a folder in an appropriate location where the data is to be saved.



Index	Time	Name	Department	Department:2
0001	11:03:36	q		
0002	11:03:42	q		
0003	11:23:55	q		
0004	11:24:13	q		
0005	11:54:13	q		
0006	11:54:33	q		
0007	12:18:47	q		
0008	12:20:31	q		
0009	12:20:37	fred		
0010	12:23:08	fred		
0011	12:23:12	q		
0012	12:24:03	q		
0013	12:27:41	fred		
0014	12:27:47	fred		
0015	12:27:51	q		
0016	12:29:00	q		
0017	12:47:09	q		
0018	12:47:54	q		
0019	13:01:03	q		

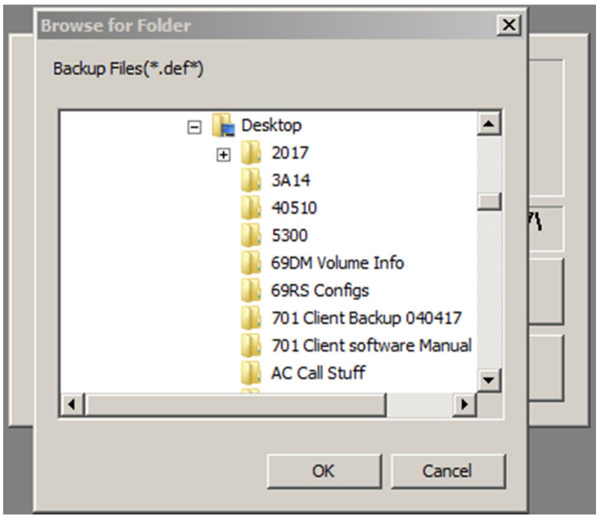
To back up the 701Client Data to an external source:

1 Select “Backup Re…” from the Setting menu. The screen below will then appear.


C:\Users\m.fall\Desktop\701 Client Backup 040417\

Once the Backup/Restore screen has appeared click on the button marked File Path the screen on the next page will then appear.

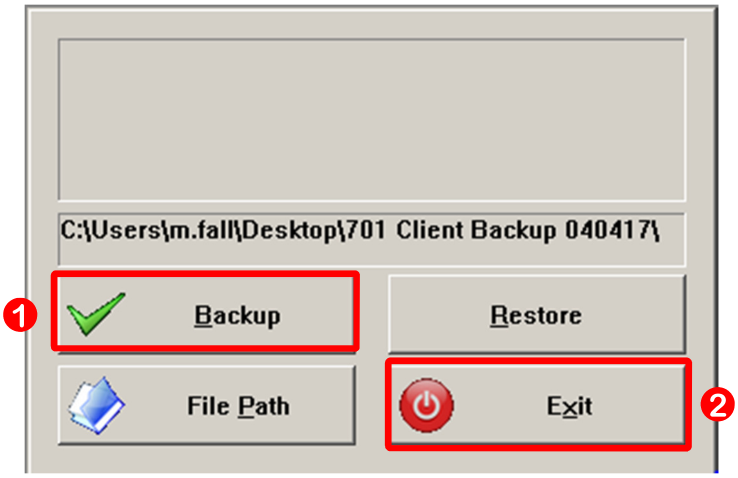
BACKING UP THE DATABASE


Browse for Folder

Backup Files(*.def*)

- Desktop
  - 2017
  - 3A14
  - 40510
  - 5300
  - 69DM Volume Info
  - 69RS Configs
  - 701 Client Backup 040417
  - 701 Client software Manual
  - AC Call Stuff

Use the “Browse for Folder” window to locate the folder created earlier for the backup data. Highlight the folder by left clicking once, then left click the OK button. The “Browse for Folder” window will then close. The window below will then show the File Path i.e. C:\Users\m.fall\Desktop\701 Client Backup 040417\
The backup folder in this case has been named “701 Client Backup 040417”

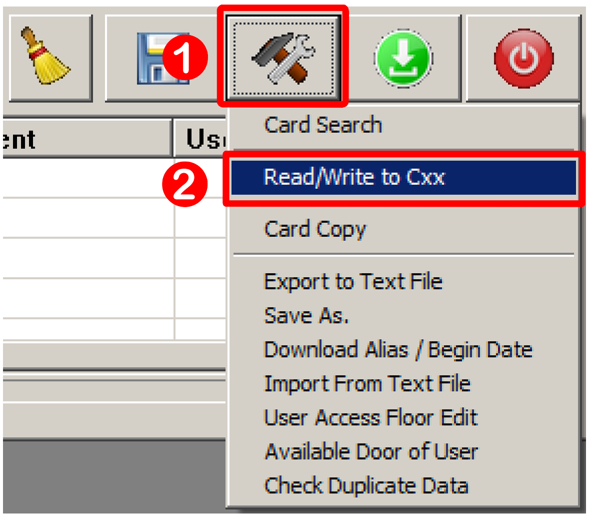

C:\Users\m.fall\Desktop\701 Client Backup 040417\

Check the file path is correct.

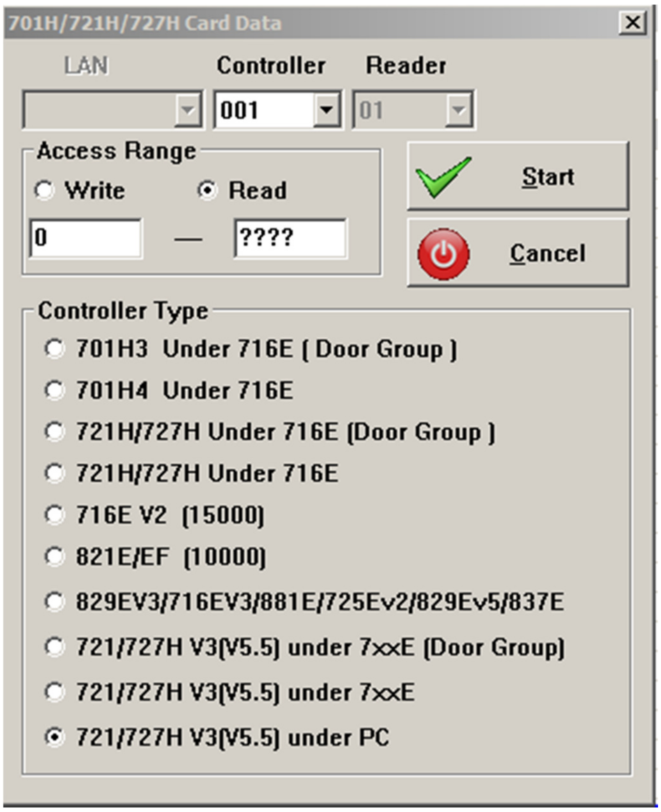
❶ Left click “Backup” to backup the data.
Once the backup is complete Left Click the Exit Button ❷

NETWORKING EXISTING STANDALONE CONTROLLERS

There may be occasions where an existing collection of standalone controllers are Subsequently networked. Once the physical network connections are completed and the controllers are identified as “On Line” user data can be extracted from one of the controllers to form the basis of the 701 Client database. To extract existing data from a controller open the User Card Edit window (refer to p25) and proceed as follows:



Select the Tools icon ❶ and then select “Read/Write to Cxx” ❷ from the drop down menu. The “701H/721H/727H Card Data” window will then open as below.


701H/721H/727H Card Data

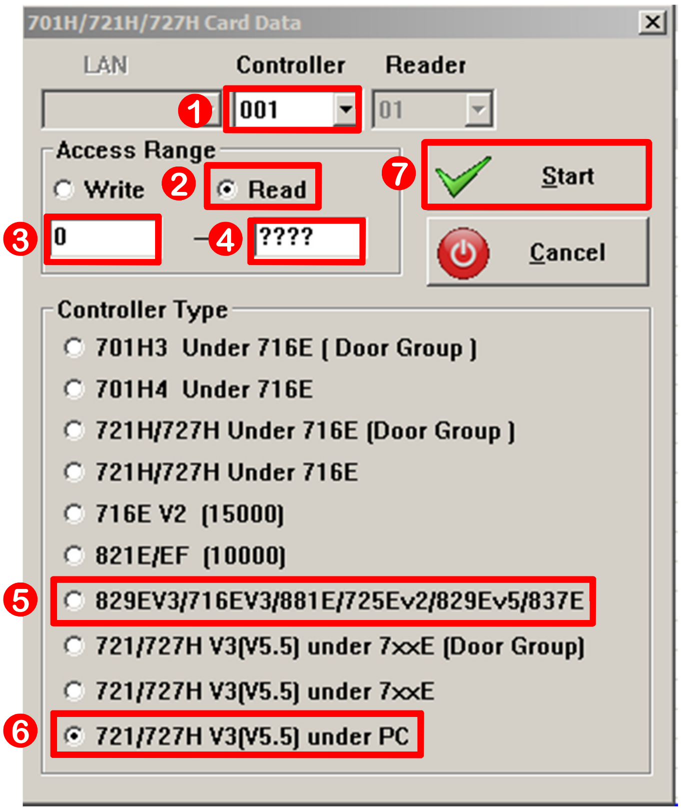
LAN:
Controller: 001
Reader: 01

Access Range
○ Write ● Read
0 — ????

Controller Type
○ 701H3 Under 716E (Door Group)
○ 701H4 Under 716E
○ 721H/727H Under 716E (Door Group)
○ 721H/727H Under 716E
○ 716E V2 (15000)
○ 821E/EF (10000)
○ 829EV3/716EV3/881E/725Ev2/829Ev5/837E
○ 721/727H V3(V5.5) under 7xxE (Door Group)
○ 721/727H V3(V5.5) under 7xxE
● 721/727H V3(V5.5) under PC

See next page.

NETWORKING EXISTING STANDALONE CONTROLLERS



701H/721H/727H Card Data

LAN Controller 001 Reader 01

Access Range

○ Write ● Read

0 – ????

Start

Cancel

Controller Type

○ 701H3 Under 716E (Door Group)
○ 701H4 Under 716E
○ 721H/727H Under 716E (Door Group)
○ 721H/727H Under 716E
○ 716E V2 (15000)
○ 821E/EF (10000)
○ 829EV3/716EV3/881E/725Ev2/829Ev5/837E
○ 721/727H V3(V5.5) under 7xxE (Door Group)
○ 721/727H V3(V5.5) under 7xxE
● 721/727H V3(V5.5) under PC

❶ Select the Node identity of the controller you wish to extract the user data from.

❷ Ensure “Read” is selected.

❸❹ Select “Start” and “End” address

Usually
Start = 0, End = 1023 for AR-727H, AR-727HB-Ray, K50 Keypad controllers
Start = 0, End = 3000 for AR-888H controllers
Start = 0, End = 15000 for E series controllers

Select controller type as identified below.

❺ For AR-331EF, AR-829EV5, AR-881EF

❻ For AR-727H, AR-727HB-RAY, K50, AR-888H

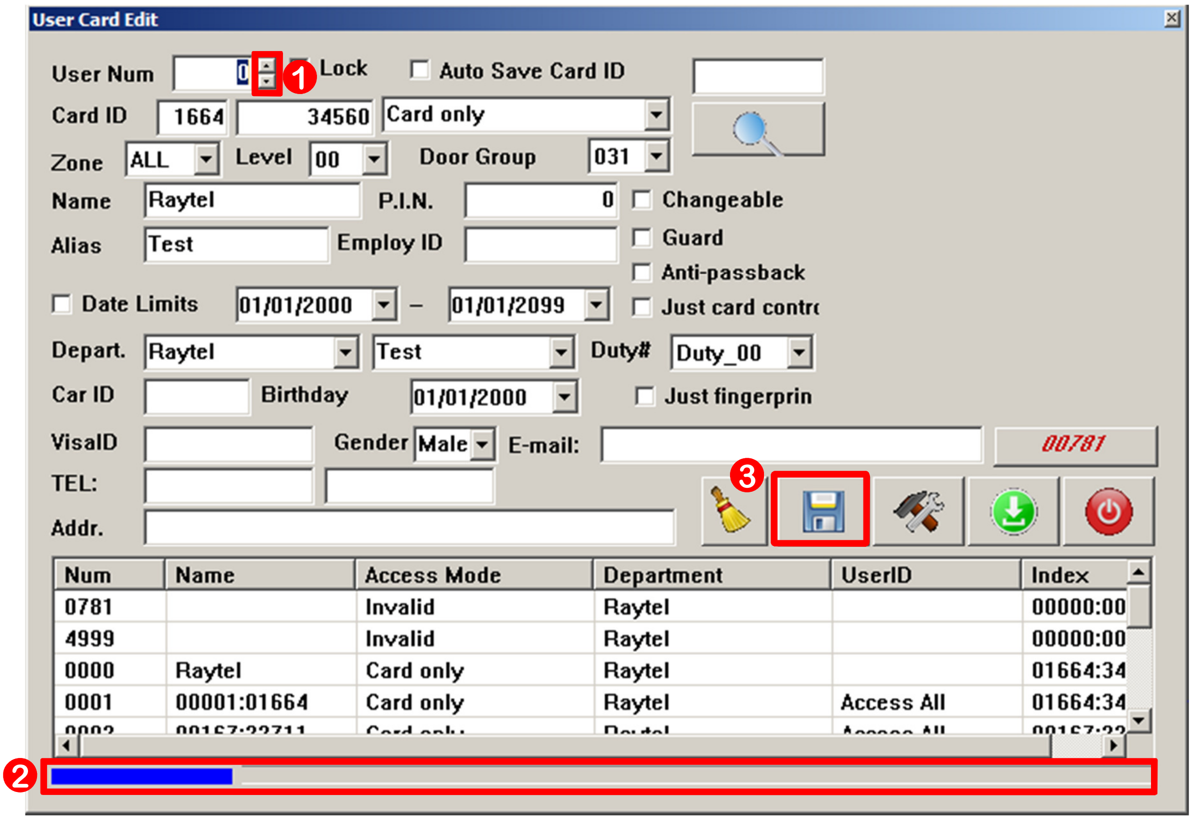
Check all of the above are correct. Once checked select “Start” ❼

And proceed to the next page for further information.

For any controllers NOT identified above refer to Raytel Technical.

NETWORKING EXISTING STANDALONE CONTROLLERS

When “Start” is selected on the previous screen the “701H/721H/727H Card Data” window will close. The “User Card Edit” window will remain open and a blue progress bar will move from left to right as shown below.



User Card Edit

User Num 0 Lock □ Auto Save Card ID

Card ID 1664 34560 Card only

Zone ALL Level 00 Door Group 031

Name Raytel P.I.N. 0 □ Changeable

Alias Test Employ ID □ Guard

□ Anti-passback

□ Date Limits 01/01/2000 – 01/01/2099 □ Just card contr

Depart. Raytel Test Duty# Duty_00

Car ID Birthday 01/01/2000 □ Just fingerprin

VisaID Gender Male E-mail: 00781

TEL:

Addr.

Num	Name	Access Mode	Department	UserID	Index
0781		Invalid	Raytel		00000:00
4999		Invalid	Raytel		00000:00
0000	Raytel	Card only	Raytel		01664:34
0001	00001:01664	Card only	Raytel	Access All	01664:34
0002	00167:22711	Card only	Raytel	Access All	00167:22

2 Once the progress bar has completed it’s progress all of the token data from the controller will be available.

1 Use the arrows beside the “User Num” to scroll up or down through the User Numbers.

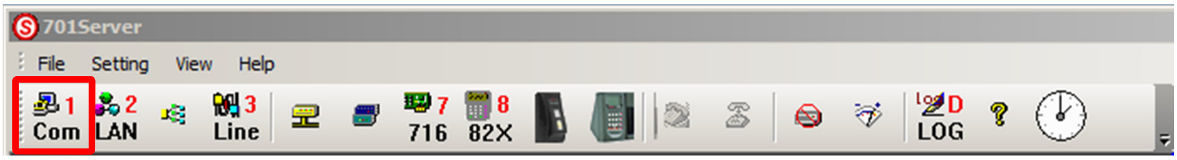
You can then add additional information to each User Number such as name, Door Group, Time Zone etc.

When you have finished revising users data remember to save any changes using the “save” button 3

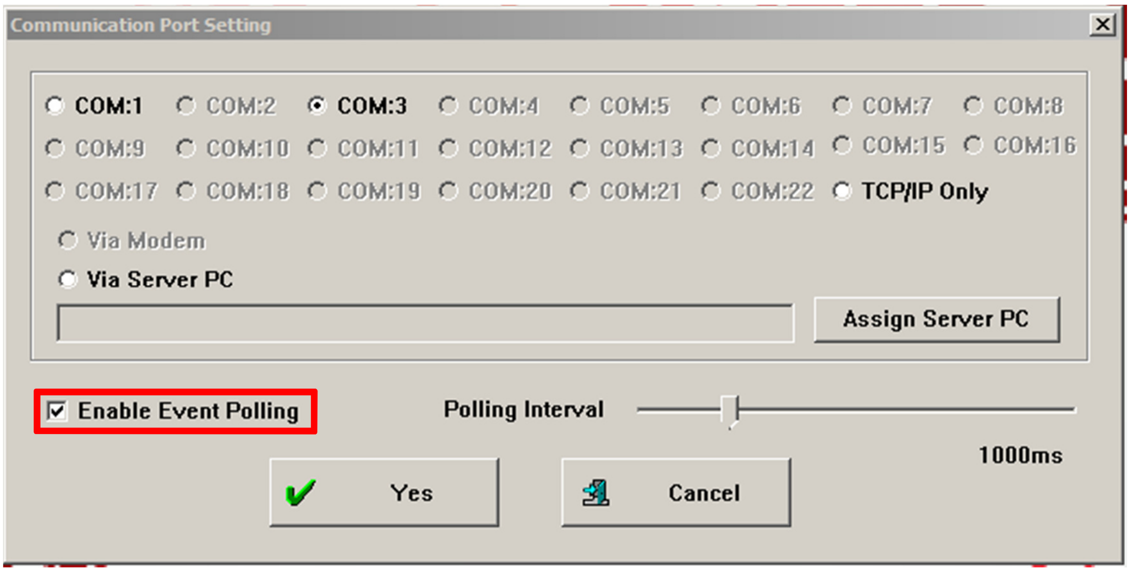
Once all changes to user data are completed and saved, download the revised data to the controller(s) if required (see page 30)

701 SERVER CHECKING COMMUNICATION SETTINGS

If no transactions are appearing on the 701 Client Transactions screen and the correct time and date have been downloaded to the controllers, check that the correct parameters have been set in 701 Server communications. To check the parameters proceed as below:



Select the Com icon as identified above. This will open the Communication Port Setting screen shown below. Check that the box marked “Enable Event Polling” is ticked, if it is not select “Enable Event Polling” and close the window by selecting “Yes”



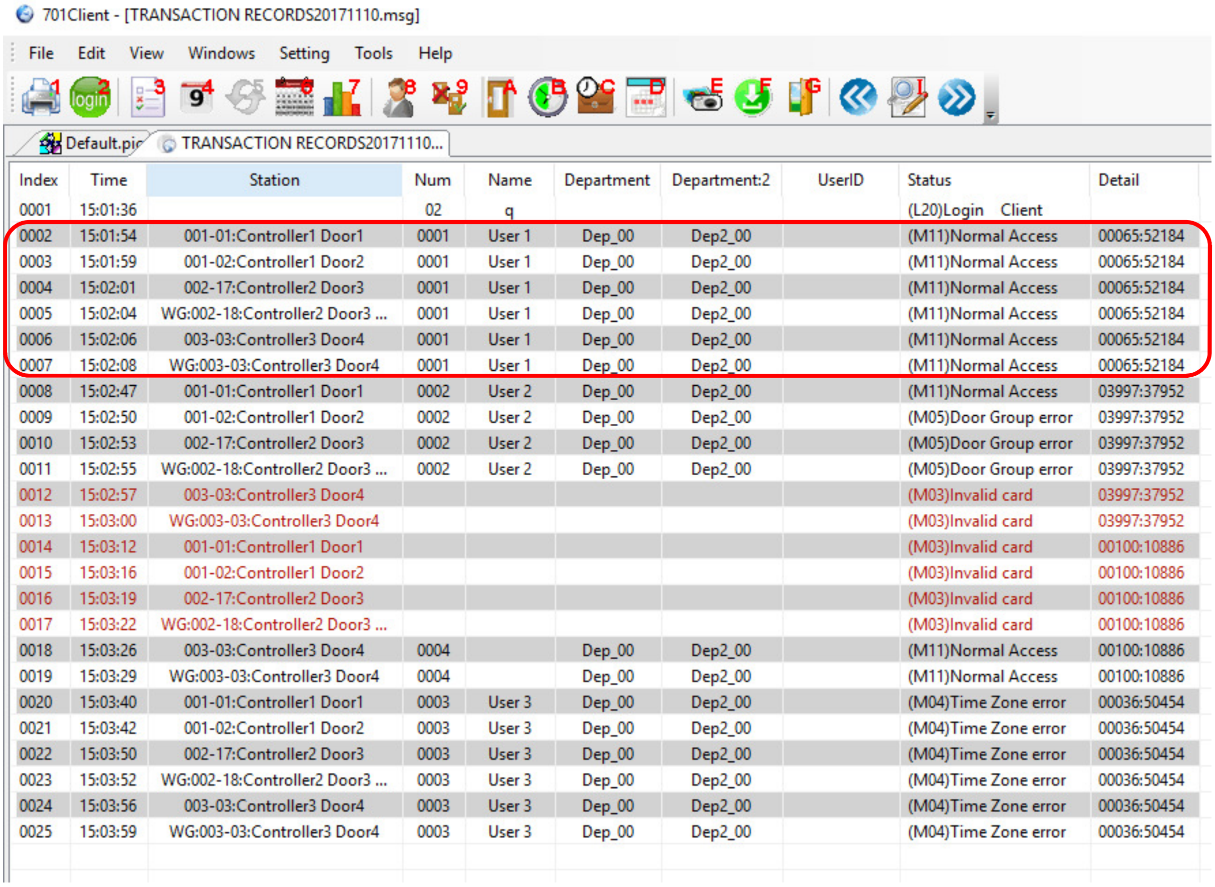
○ COM:1 ○ COM:2 ● COM:3 ○ COM:4 ○ COM:5 ○ COM:6 ○ COM:7 ○ COM:8
○ COM:9 ○ COM:10 ○ COM:11 ○ COM:12 ○ COM:13 ○ COM:14 ○ COM:15 ○ COM:16
○ COM:17 ○ COM:18 ○ COM:19 ○ COM:20 ○ COM:21 ○ COM:22 ○ TCP/IP Only

○ Via Modem
○ Via Server PC

☑ Enable Event Polling

Polling Interval 1000ms

TROUBLESHOOTING WITH VALID 701 CLIENT EVENT LOG MESSAGES


701Client - [TRANSACTION RECORDS20171110.msg]
File
Edit
View
Windows
Setting
Tools
Help
1
login
2
3
4
5
6
7
8
9
A
B
C
D
E
F
G
Default.pic
TRANSACTION RECORDS20171110...

Index	Time	Station	Num	Name	Department	Department:2	UserID	Status	Detail
0001	15:01:36		02	q				(L20)Login Client	
0002	15:01:54	001-01:Controller1 Door1	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0003	15:01:59	001-02:Controller1 Door2	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0004	15:02:01	002-17:Controller2 Door3	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0005	15:02:04	WG:002-18:Controller2 Door3 ...	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0006	15:02:06	003-03:Controller3 Door4	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0007	15:02:08	WG:003-03:Controller3 Door4	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0008	15:02:47	001-01:Controller1 Door1	0002	User 2	Dep_00	Dep2_00		(M11)Normal Access	03997:37952
0009	15:02:50	001-02:Controller1 Door2	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0010	15:02:53	002-17:Controller2 Door3	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0011	15:02:55	WG:002-18:Controller2 Door3 ...	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0012	15:02:57	003-03:Controller3 Door4						(M03)Invalid card	03997:37952
0013	15:03:00	WG:003-03:Controller3 Door4						(M03)Invalid card	03997:37952
0014	15:03:12	001-01:Controller1 Door1						(M03)Invalid card	00100:10886
0015	15:03:16	001-02:Controller1 Door2						(M03)Invalid card	00100:10886
0016	15:03:19	002-17:Controller2 Door3						(M03)Invalid card	00100:10886
0017	15:03:22	WG:002-18:Controller2 Door3 ...						(M03)Invalid card	00100:10886
0018	15:03:26	003-03:Controller3 Door4	0004		Dep_00	Dep2_00		(M11)Normal Access	00100:10886
0019	15:03:29	WG:003-03:Controller3 Door4	0004		Dep_00	Dep2_00		(M11)Normal Access	00100:10886
0020	15:03:40	001-01:Controller1 Door1	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0021	15:03:42	001-02:Controller1 Door2	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0022	15:03:50	002-17:Controller2 Door3	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0023	15:03:52	WG:002-18:Controller2 Door3 ...	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0024	15:03:56	003-03:Controller3 Door4	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0025	15:03:59	WG:003-03:Controller3 Door4	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454

The controllers in the above example are as follows:

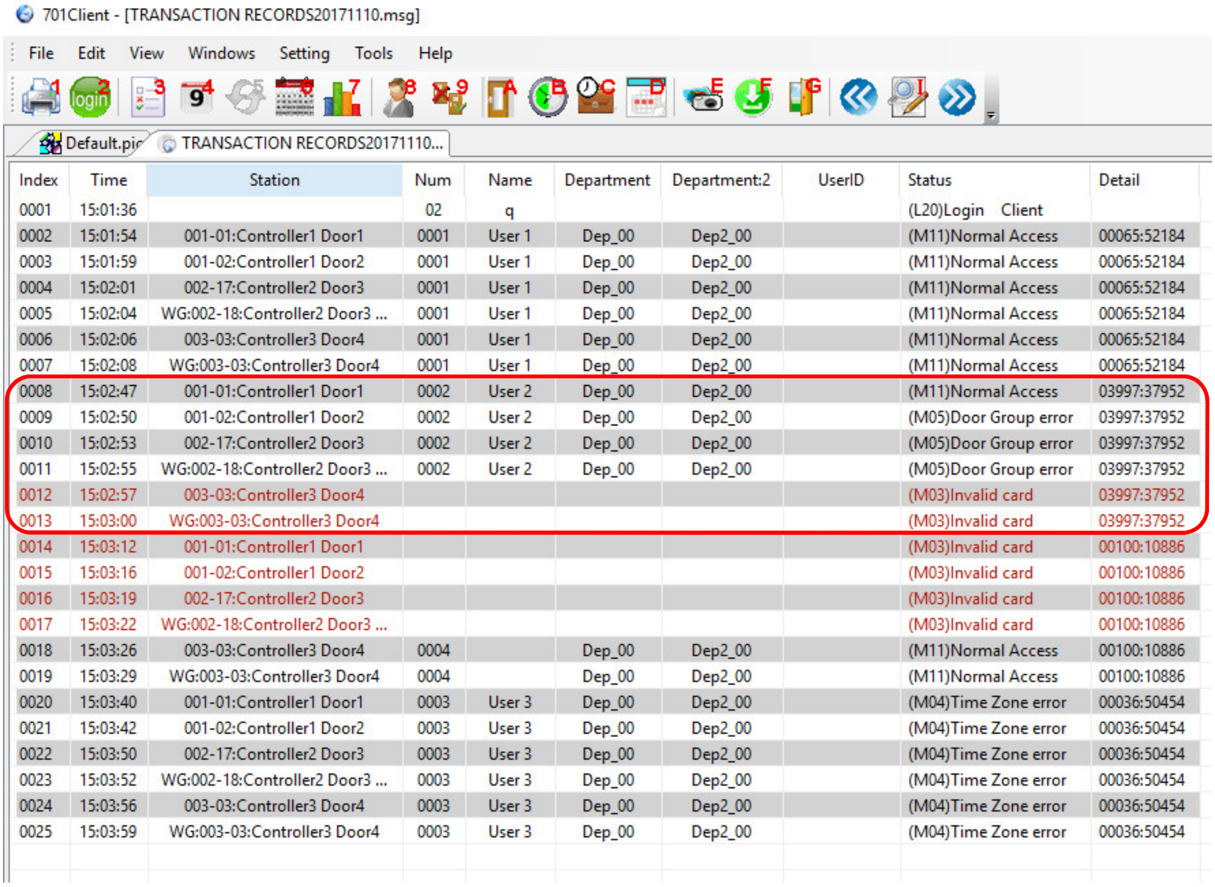
Node ID=1	AR-727HB-RAY H Series 2 Door Controller	-	Controller 1, Doors 1 and 2
Node ID=2	AR-331EF E series Controller	-	Controller 2, Door 3
Node ID=3	AR-727H H Series Controller	-	Controller 3, Door 4

System Parameters (see Page 21) have been set for : Huge Door Group Mode and Show Detail Node Address. The transactions highlighted above show a valid User Token being presented to each reader and/or controller in turn. All of the data in the database has been downloaded to the connected controllers.

Index 0002 shows a valid token gaining access on Controller 1 via the reader at Door 1
Index 0003 shows a valid token gaining access on Controller 1 via the reader at Door 2
Index 0004 shows a valid token gaining access on Controller 2 Door 3 via it's built in reader.
Index 0005 shows a valid token gaining access on Controller 2 Door 3 via it's external WG reader.
Index 0006 shows a valid token gaining access on Controller 3 Door 4 via it's built in reader.
Index 0007 shows a valid token gaining access on Controller 3 Door 4 via it's external WG reader.

A WG prefix in the Station column indicates an external WG reader connected to the controller.

TROUBLESHOOTING WITH 701 CLIENT
DOOR GROUP ERROR MESSAGES


701Client - [TRANSACTION RECORDS20171110.msg]
File
Edit
View
Windows
Setting
Tools
Help
login
Default.pic
TRANSACTION RECORDS20171110...

Index	Time	Station	Num	Name	Department	Department:2	UserID	Status	Detail
0001	15:01:36		02	q				(L20)Login Client	
0002	15:01:54	001-01:Controller1 Door1	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0003	15:01:59	001-02:Controller1 Door2	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0004	15:02:01	002-17:Controller2 Door3	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0005	15:02:04	WG:002-18:Controller2 Door3 ...	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0006	15:02:06	003-03:Controller3 Door4	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0007	15:02:08	WG:003-03:Controller3 Door4	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0008	15:02:47	001-01:Controller1 Door1	0002	User 2	Dep_00	Dep2_00		(M11)Normal Access	03997:37952
0009	15:02:50	001-02:Controller1 Door2	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0010	15:02:53	002-17:Controller2 Door3	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0011	15:02:55	WG:002-18:Controller2 Door3 ...	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0012	15:02:57	003-03:Controller3 Door4						(M03)Invalid card	03997:37952
0013	15:03:00	WG:003-03:Controller3 Door4						(M03)Invalid card	03997:37952
0014	15:03:12	001-01:Controller1 Door1						(M03)Invalid card	00100:10886
0015	15:03:16	001-02:Controller1 Door2						(M03)Invalid card	00100:10886
0016	15:03:19	002-17:Controller2 Door3						(M03)Invalid card	00100:10886
0017	15:03:22	WG:002-18:Controller2 Door3 ...						(M03)Invalid card	00100:10886
0018	15:03:26	003-03:Controller3 Door4	0004		Dep_00	Dep2_00		(M11)Normal Access	00100:10886
0019	15:03:29	WG:003-03:Controller3 Door4	0004		Dep_00	Dep2_00		(M11)Normal Access	00100:10886
0020	15:03:40	001-01:Controller1 Door1	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0021	15:03:42	001-02:Controller1 Door2	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0022	15:03:50	002-17:Controller2 Door3	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0023	15:03:52	WG:002-18:Controller2 Door3 ...	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0024	15:03:56	003-03:Controller3 Door4	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0025	15:03:59	WG:003-03:Controller3 Door4	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454

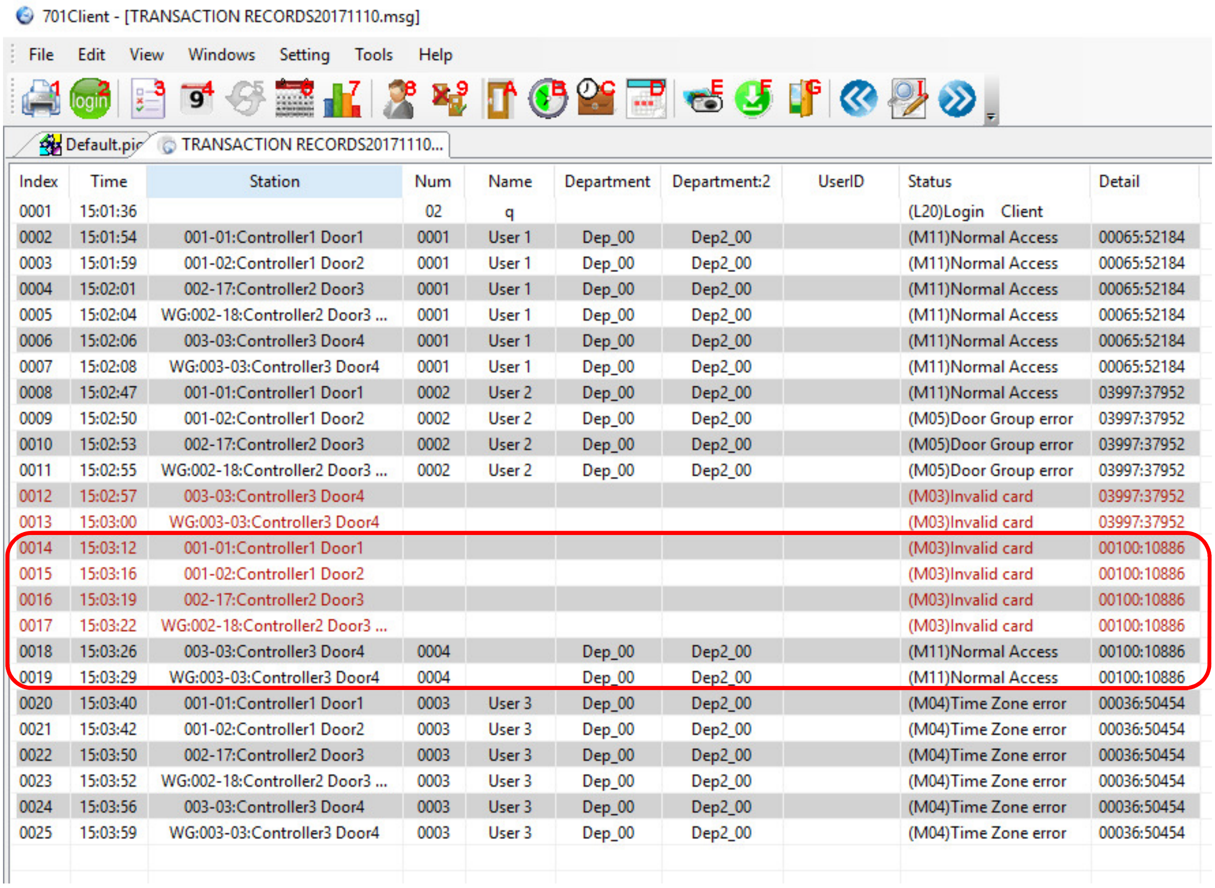
The above examples show the messages associated with User 2 attempting to access each Door in turn. User 2 has been allocated to a Door Group that only enables access to Door 1 on Controller 1.

Door Groups function differently with different types of controllers.

Controllers 1 and 2 show a Door Group error where the User card is not valid for the door.

Controller 3 shows the User card as invalid and no user number is shown in the Num column, this is because this particular type of controller “suspends” the User card if it is not valid for the controller.

TROUBLESHOOTING WITH 701 CLIENT
INVALID CARD MESSAGES


701Client - [TRANSACTION RECORDS20171110.msg]
File
Edit
View
Windows
Setting
Tools
Help
login
Default.pic
TRANSACTION RECORDS20171110...

Index	Time	Station	Num	Name	Department	Department:2	UserID	Status	Detail
0001	15:01:36		02	q				(L20)Login Client	
0002	15:01:54	001-01:Controller1 Door1	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0003	15:01:59	001-02:Controller1 Door2	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0004	15:02:01	002-17:Controller2 Door3	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0005	15:02:04	WG:002-18:Controller2 Door3 ...	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0006	15:02:06	003-03:Controller3 Door4	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0007	15:02:08	WG:003-03:Controller3 Door4	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0008	15:02:47	001-01:Controller1 Door1	0002	User 2	Dep_00	Dep2_00		(M11)Normal Access	03997:37952
0009	15:02:50	001-02:Controller1 Door2	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0010	15:02:53	002-17:Controller2 Door3	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0011	15:02:55	WG:002-18:Controller2 Door3 ...	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0012	15:02:57	003-03:Controller3 Door4						(M03)Invalid card	03997:37952
0013	15:03:00	WG:003-03:Controller3 Door4						(M03)Invalid card	03997:37952
0014	15:03:12	001-01:Controller1 Door1						(M03)Invalid card	00100:10886
0015	15:03:16	001-02:Controller1 Door2						(M03)Invalid card	00100:10886
0016	15:03:19	002-17:Controller2 Door3						(M03)Invalid card	00100:10886
0017	15:03:22	WG:002-18:Controller2 Door3 ...						(M03)Invalid card	00100:10886
0018	15:03:26	003-03:Controller3 Door4	0004		Dep_00	Dep2_00		(M11)Normal Access	00100:10886
0019	15:03:29	WG:003-03:Controller3 Door4	0004		Dep_00	Dep2_00		(M11)Normal Access	00100:10886
0020	15:03:40	001-01:Controller1 Door1	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0021	15:03:42	001-02:Controller1 Door2	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0022	15:03:50	002-17:Controller2 Door3	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0023	15:03:52	WG:002-18:Controller2 Door3 ...	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0024	15:03:56	003-03:Controller3 Door4	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0025	15:03:59	WG:003-03:Controller3 Door4	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454

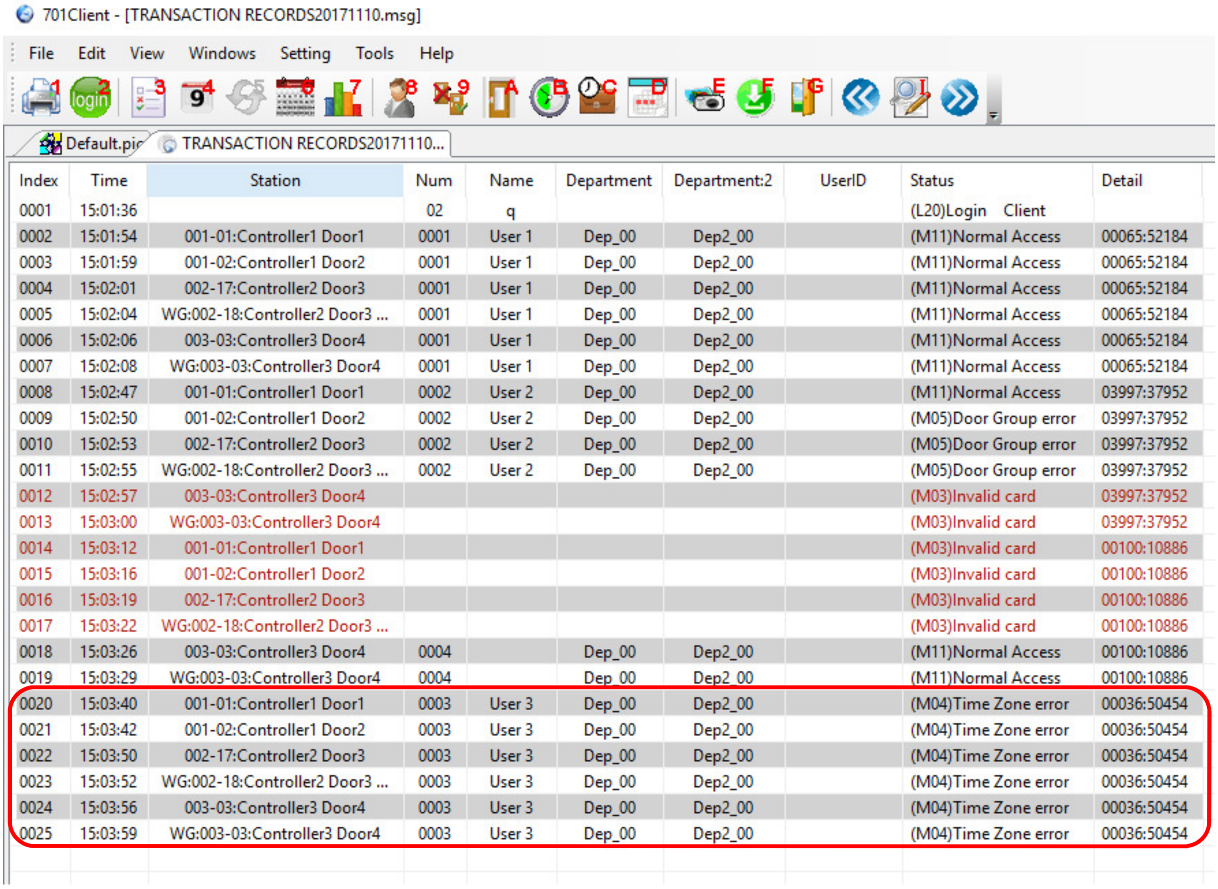
The above examples show messages associated with an unknown user attempting to access each door in turn.

The user has been added to controller 3 locally as user 4 but does not exist in the 701 Client User database.

This can be verified from the event log because an identity is only shown in the Num column for the controller at which it has been added manually.

All other controllers show the card detail but no User in the Num column.

TROUBLESHOOTING WITH 701 CLIENT TIME ZONE ERROR MESSAGES



701Client - [TRANSACTION RECORDS20171110.msg]

Index	Time	Station	Num	Name	Department	Department:2	UserID	Status	Detail
0001	15:01:36		02	q				(L20)Login Client	
0002	15:01:54	001-01:Controller1 Door1	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0003	15:01:59	001-02:Controller1 Door2	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0004	15:02:01	002-17:Controller2 Door3	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0005	15:02:04	WG:002-18:Controller2 Door3 ...	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0006	15:02:06	003-03:Controller3 Door4	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0007	15:02:08	WG:003-03:Controller3 Door4	0001	User 1	Dep_00	Dep2_00		(M11)Normal Access	00065:52184
0008	15:02:47	001-01:Controller1 Door1	0002	User 2	Dep_00	Dep2_00		(M11)Normal Access	03997:37952
0009	15:02:50	001-02:Controller1 Door2	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0010	15:02:53	002-17:Controller2 Door3	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0011	15:02:55	WG:002-18:Controller2 Door3 ...	0002	User 2	Dep_00	Dep2_00		(M05)Door Group error	03997:37952
0012	15:02:57	003-03:Controller3 Door4						(M03)Invalid card	03997:37952
0013	15:03:00	WG:003-03:Controller3 Door4						(M03)Invalid card	03997:37952
0014	15:03:12	001-01:Controller1 Door1						(M03)Invalid card	00100:10886
0015	15:03:16	001-02:Controller1 Door2						(M03)Invalid card	00100:10886
0016	15:03:19	002-17:Controller2 Door3						(M03)Invalid card	00100:10886
0017	15:03:22	WG:002-18:Controller2 Door3 ...						(M03)Invalid card	00100:10886
0018	15:03:26	003-03:Controller3 Door4	0004		Dep_00	Dep2_00		(M11)Normal Access	00100:10886
0019	15:03:29	WG:003-03:Controller3 Door4	0004		Dep_00	Dep2_00		(M11)Normal Access	00100:10886
0020	15:03:40	001-01:Controller1 Door1	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0021	15:03:42	001-02:Controller1 Door2	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0022	15:03:50	002-17:Controller2 Door3	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0023	15:03:52	WG:002-18:Controller2 Door3 ...	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0024	15:03:56	003-03:Controller3 Door4	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454
0025	15:03:59	WG:003-03:Controller3 Door4	0003	User 3	Dep_00	Dep2_00		(M04)Time Zone error	00036:50454

The above examples show messages associated with User 3 attempting to access each Door in turn.
User 3 has been allocated to a time zone that only allows access between 08:00 and 09:00 therefore any attempt to access with User card 3 will be reported as a Time zone error and access will not be granted.

701 CLIENT EVENT LOG
MESSAGE DESCRIPTIONS

701 Client Message ID's	
M01	Invalid PIN
M02	Keypad Locked
M03	Invalid Card *(Card Code in event detail)*
M04	Time Zone Error
M05	Door Group Error
M06	User Card—Date expired
M08	Incorrect PIN
M09	Duress Code Used
M11	Normal Access
M14	Arming
M15	Disarming
M16	Egress (RTE)
M17	Alarming (*description in event detail*)
L20	Server or Client Login
L21	Server or Client Logout
L22	Controller OFF line (*controller ID etc*)
L23	Controller ON line (*controller ID etc*)
M24	(*Device type*) Power ON
M28	Access by Pin
M30	Anti-pass back error
M31	Reader disconnected at controller
M32	Reader reconnected at controller
M33	User changed PIN code
M34	User changed PIN code error
M35	Controller entered Auto Open procedure
M36	Controller exited Auto Open procedure
M37	Disarmed by auto time procedure
M38	Armed by auto time procedure
M39	Access by Finger/Vein
M56	Fingerprint Access Failed

L is software generated, M is controller generated.

701 CLIENT

SYSTEM USER INFORMATION

Name of On-Site Programmer(s): ....

Installation Company: ....

Controller Default Master Code:- ✶ 123456 #

Tel: ....

Date: ....

Controller Installer Master Code:- ....

Lock Time: ....

Lock Type: ....

User Address	Users Name	Card ID	Door Group	Time Zone	PIN
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			
		;			

We recommend this page should be filled in and regularly updated and kept in a safe and secure location by the person responsible for the upkeep of the system.