TRU 650
Fingerprint Reader Unit – Access Control System

USER’S GUIDE
Rev 2.1.xc

아이비코리아
INTEGRATED BIOMETRICS KOREA

IBKorea. Ltd.
#818, Woolim Lions Valley 311-3, Sangdaewon-dong
Jungwon-gu, Seoungnam-si, Gyeonggi-do
www.ibkr.co.kr

1.0 Bio-I BACS Enroll & Management Software

1.1 Logging In.

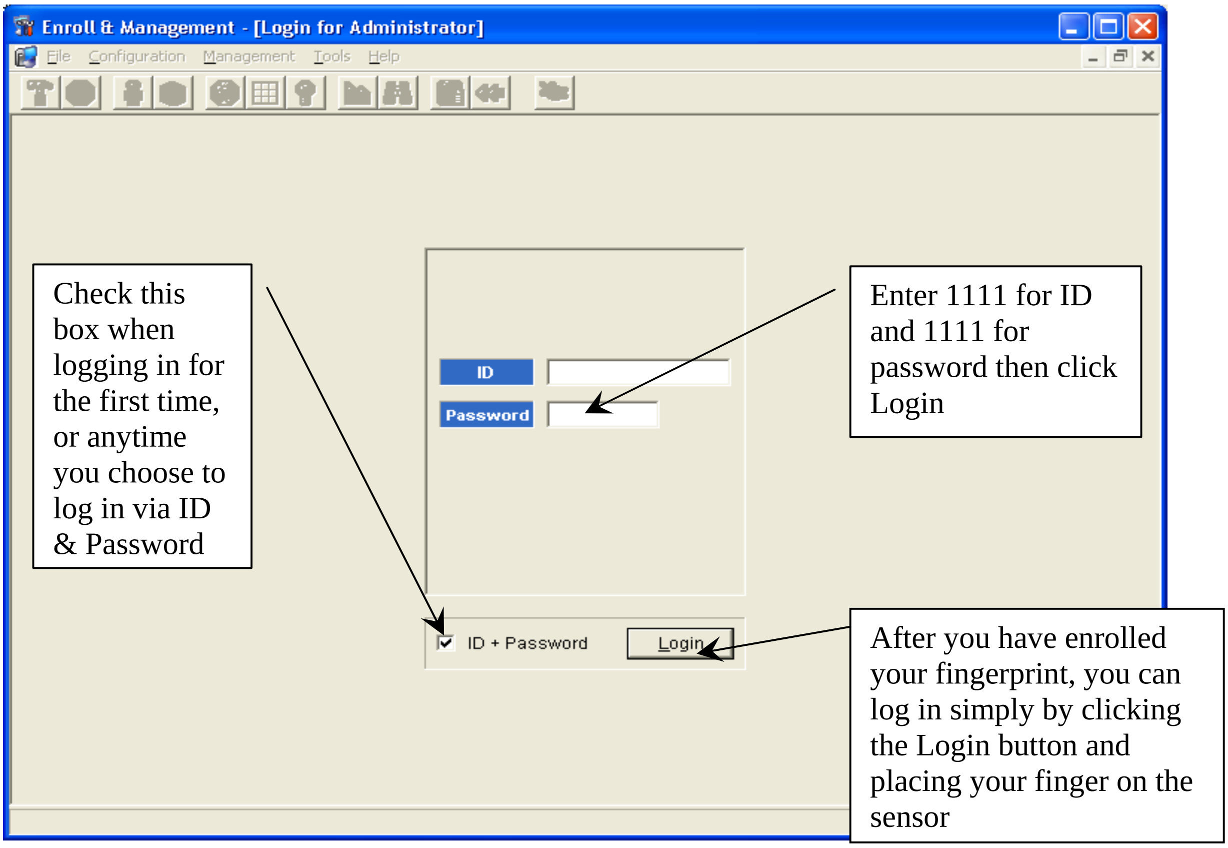
1.1.1 Start the Enroll & Management software by double clicking on the “Bio-I BACS” Icon found on your desktop. You may also log on to the software through “Start\All Programs\Integrated Biometrics LLC\Bio-IBACS.”

1.1.2 This will bring up the “Enroll & Management – [Login for Administrator]” window shown below.

1.1.3 The first time someone logs in, you will need to log in as the default user “Admin”, using default settings, since no one is enrolled yet. Click on the box “ID + Password.” The default “ID” is “1111” and the default “Password” is “1111.” Enter these in the appropriate boxes and Click “Login.”

1.1.4 The “[Identified]” window should appear and read “User: Admin, Type: Administrator.” Click “OK.” You should now be logged into the “Bio-I BACS” program and the “Enroll & Management – [Log Monitor]” window should appear. You have successfully logged in.

1.1.5 After you have enrolled as an “Administrator” User, and have enrolled your fingerprint, you can log in from this screen simply by clicking the “Login” button, and placing your finger on the sensor.



Check this box when logging in for the first time, or anytime you choose to log in via ID & Password

Enter 1111 for ID and 1111 for password then click Login

After you have enrolled your fingerprint, you can log in simply by clicking the Login button and placing your finger on the sensor

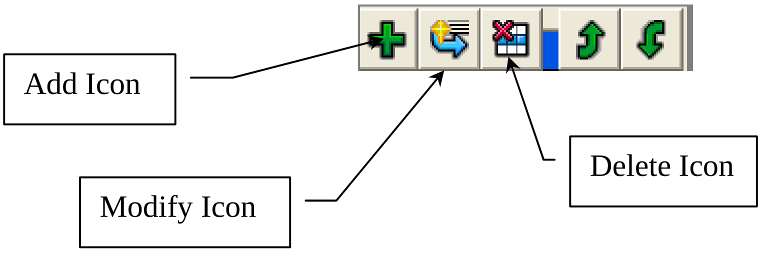
1.2 Screen Navigation

1.2.1 The software can be navigated by two methods. The Menu Selections File, Configuration, Management, etc., are across the top of each window. Each of these selections has a drop down menu for the various functions. See example below.

1.2.2 Under the Menu Selections, there are Icons that are short cuts to these functions. See the example below.

1.2.3 Another method of Modifying **active** Users, or Groups, or TRU's, etc., is to click on an active line, which will highlight it. Then right click, which will display a menu box with selections such as "Modify", "Delete", "Detach", etc. See example below.

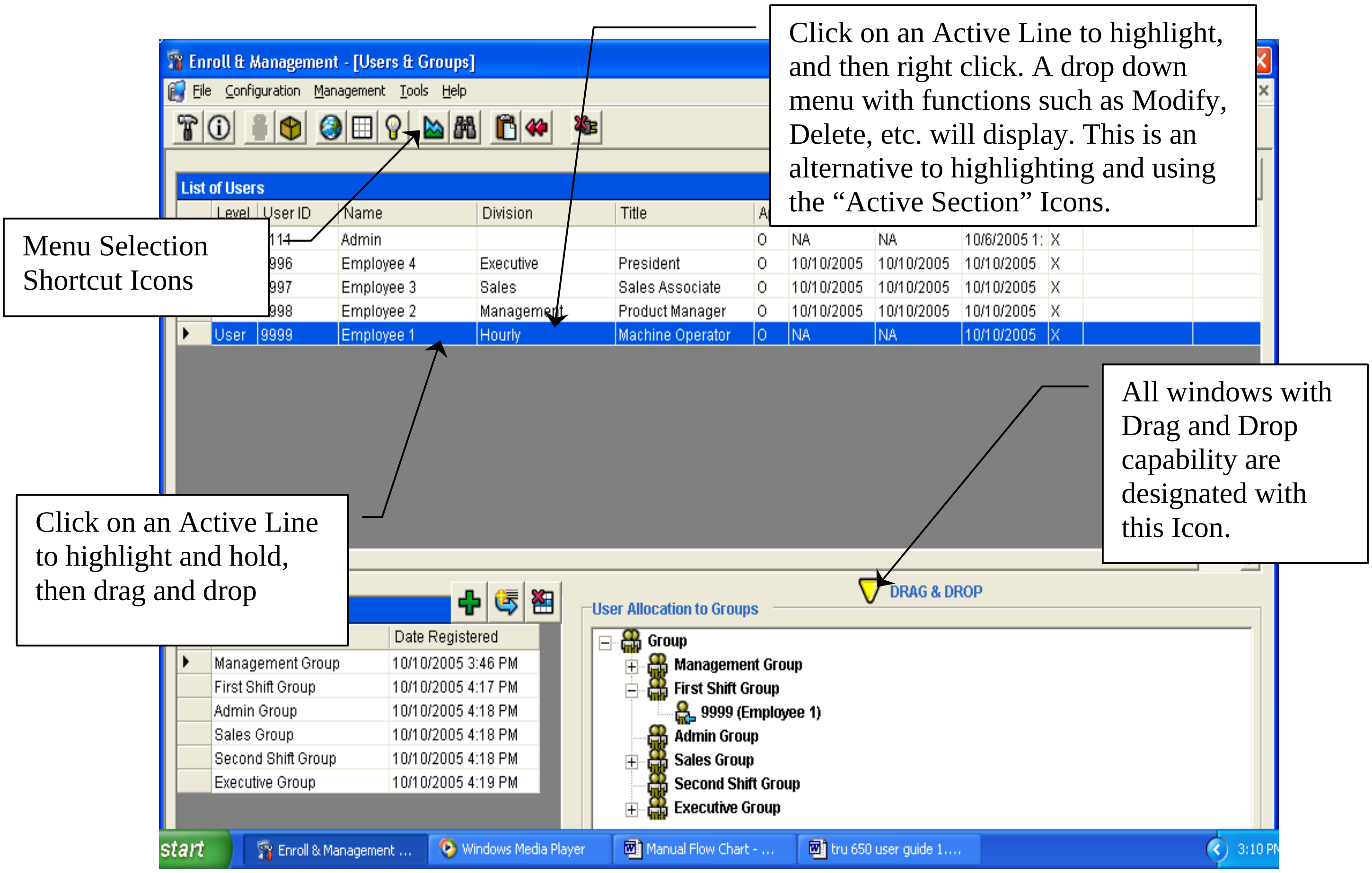
1.2.4 Attaching "Users" and "Access Times" to "Groups", and attaching "Groups" to "TRU's" is accomplished by simply Dragging and Dropping. See example below.



Add Icon

Modify Icon

Delete Icon



Enroll & Management - [Users & Groups]
File Configuration Management Tools Help

Click on an Active Line to highlight, and then right click. A drop down menu with functions such as Modify, Delete, etc. will display. This is an alternative to highlighting and using the "Active Section" Icons.

Menu Selection Shortcut Icons

List of Users

Level	User ID	Name	Division	Title	A				
	114	Admin			O	NA	NA	10/6/2005 1:	X
	996	Employee 4	Executive	President	O	10/10/2005	10/10/2005	10/10/2005	X
	997	Employee 3	Sales	Sales Associate	O	10/10/2005	10/10/2005	10/10/2005	X
	998	Employee 2	Management	Product Manager	O	10/10/2005	10/10/2005	10/10/2005	X
User	9999	Employee 1	Hourly	Machine Operator	O	NA	NA	10/10/2005	X

Click on an Active Line to highlight and hold, then drag and drop

All windows with Drag and Drop capability are designated with this Icon.

	Date Registered
Management Group	10/10/2005 3:46 PM
First Shift Group	10/10/2005 4:17 PM
Admin Group	10/10/2005 4:18 PM
Sales Group	10/10/2005 4:18 PM
Second Shift Group	10/10/2005 4:18 PM
Executive Group	10/10/2005 4:19 PM

1.2.5 Some windows also contain "Tabs." These tabs are located at the top or bottom of some windows. Click on these tabs to access options for the windows that are displayed.

1.2.6 In the active sections of each window, the sections where you can add or modify etc., there are function Icons. These Icons are shown below.

1.3 Menu Selection "Configuration"

1.3.1 Settings

Click on Menu Selection "Configuration." The Drop Down menu will present two choices. Click on "Settings." You will see the "Enroll & Management – [Settings]" screen shown below. The manufacturer's settings should not need changing. Only your Network Administrator can make that decision.

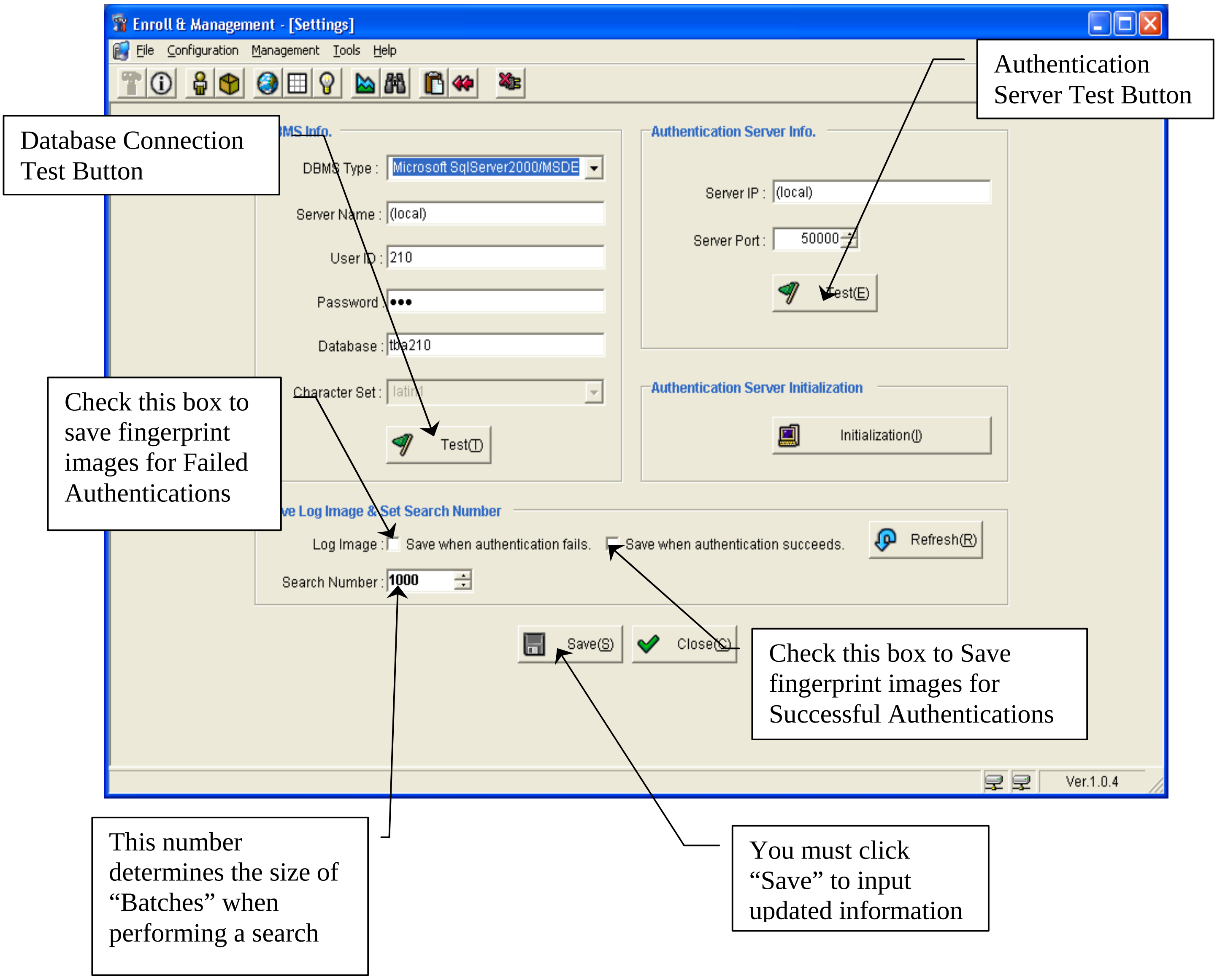
1.3.1.1 The Database Connection. Click on the "Test(T)" button in the left side of the screen in the "DBMS Info" section. The window that appears should read "Database Connections Succeeded." This confirms the Database Connection. Click "Yes" to save.

1.3.1.2 Test the Authentication Server Connection. Click on the "Test(E)" button in the "Authentication Server Info" section on the right side. The window that appears should read "Authentication Server Connection Succeeded." This confirms the Authentication Server connection. Click "Yes" to save.

1.3.1.3 "Log Image, save when authentication fails" box in bottom left. Checking this box will save the images when Authentication fails. This can be useful in examining Failed Authentications, in Log Search function, to look for problems with the image.

1.3.1.4 "Save when authentication succeeds" box in lower middle. Checking this box will give you a log of succeeded images for examination.

1.3.1.5 "Search Number" box in lower left. When you search images in the "Tools Menu", this number determines how many images will be retrieved in "Batches." The Manufacturers setting is 1000. The higher the setting the longer it will take to retrieve each "Batch."


Enroll & Management - [Settings]
File
Configuration
Management
Tools
Help
MS Info.
Authentication Server Info.
Test(T)
Test(E)
Authentication Server Initialization
Initialization(I)
ve Log Image & Set Search Number
Refresh(R)
Save(S)
Close(C)
Ver.1.0.4

DBMS Type : Microsoft SqlServer2000/MSDE

Server Name : (local)

User ID : 210

Password : •••

Database : tba210

Character Set : latin1

Server IP : (local)

Server Port : 50000

Log Image : ☐ Save when authentication fails. ☐ Save when authentication succeeds.

Search Number : 1000

Database Connection Test Button

Authentication Server Test Button

Check this box to save fingerprint images for Failed Authentications

Check this box to Save fingerprint images for Successful Authentications

This number determines the size of “Batches” when performing a search

You must click “Save” to input updated information

1.3.2 Divisions & Titles

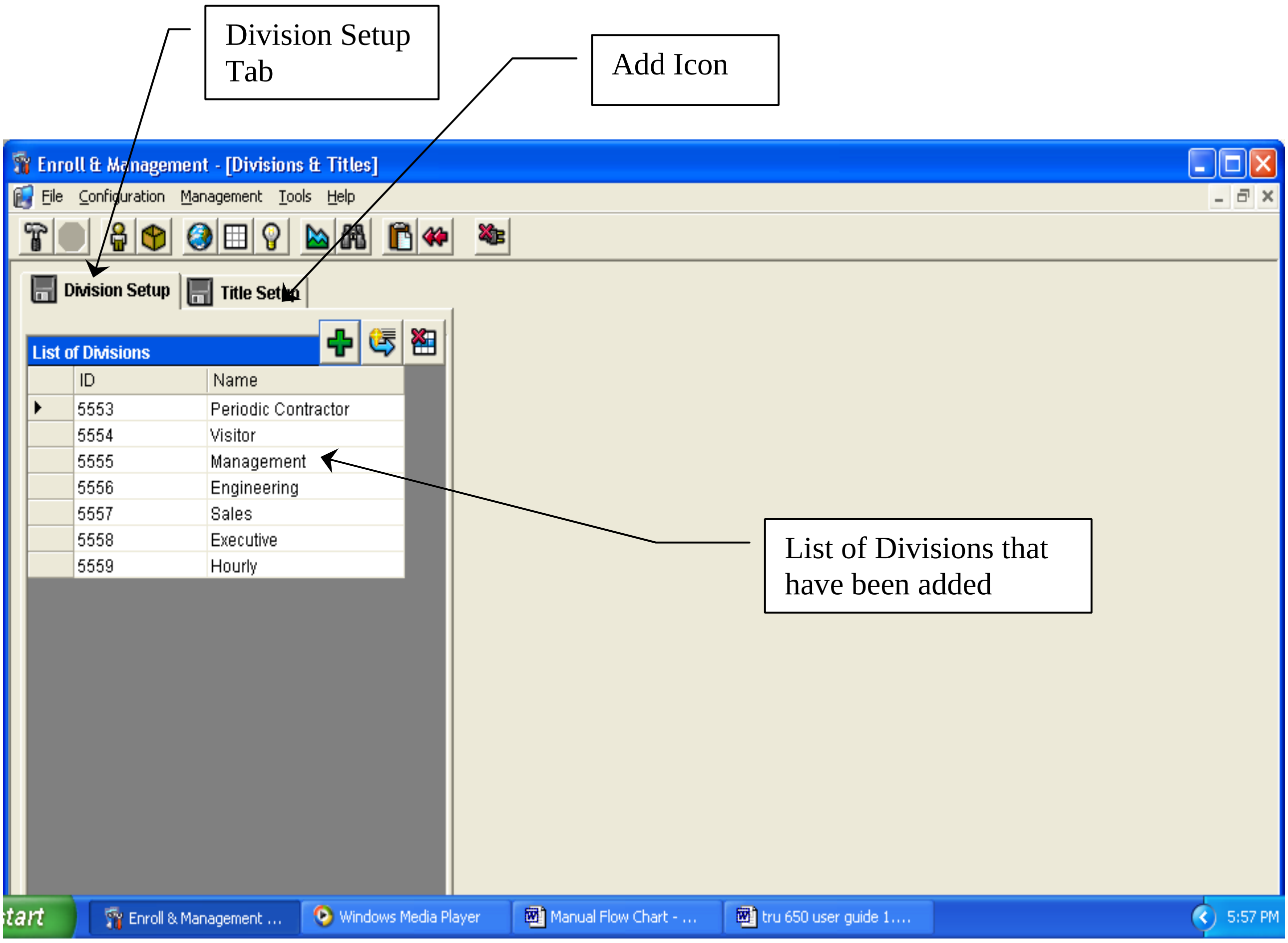
1.3.2.1 Click on the Menu Selection “Configuration.” The Drop Down menu will present two choices. Click on “Divisions & Titles.”

1.3.2.2 You will see the window “Enroll & Management – [Divisions & Titles] shown below.

1.3.2.3 Click on the “Division Setup” tab. Click on the “Add” Icon. The “Division Setup” box shown below will appear. Fill in a unique “Div. ID” number and a “Div. Name.” Click “Save.” The new entry will show in the “List of Divisions.”

1.3.2.4 Next, click on the “Title Setup” tab. Go through the same process as with Division Setup.

Note: Divisions and Titles are not required for the operations of the access control system. They are for descriptive purposes only and have no effect on the granting of access privileges.

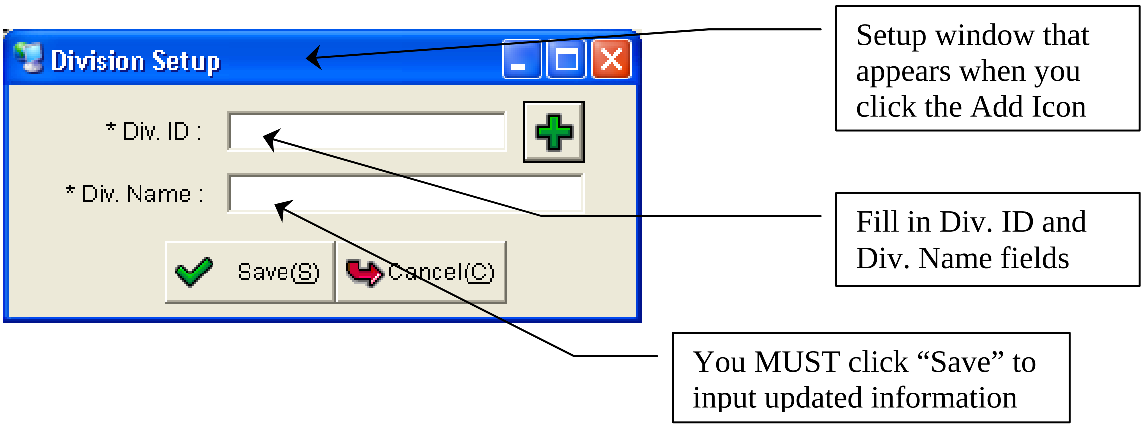


Division Setup Tab

Add Icon

	ID	Name
▶	5553	Periodic Contractor
	5554	Visitor
	5555	Management
	5556	Engineering
	5557	Sales
	5558	Executive
	5559	Hourly

List of Divisions that have been added



Setup window that appears when you click the Add Icon

Fill in Div. ID and Div. Name fields

You MUST click "Save" to input updated information

1.4 Menu Selection “Management”

1.4.1 User & Group

1.4.1.1 Enrolling Users.

1.4.1.1.1 Click on the Menu Selection “Management” and select “User & Group” from the Dropdown Menu.

1.4.1.1.2 In the top section, “List of Users”, click on the “Add” Icon. The “Users” window shown below will appear.

1.4.1.1.3 Click on the “User Info” tab. Fill in a unique “ID” number. This field only accepts numeric characters. Note: This is the ID that will be used to logon the Bio-I BACS software if they do not choose to log in biometrically.

1.4.1.1.4 Fill in the name field.

1.4.1.1.5 Click “User Type” radio button “User,” “Administrator,” or “Visitor.” User Type assigned should be based on the following.

- Administrator – Has full access to the Bio-i BACS software and available to be assigned door access.
- User – Available to be assigned door access, but does not have access to Bio-I BACS software.
- Visitor – Same as user but you must supply an expiration date.

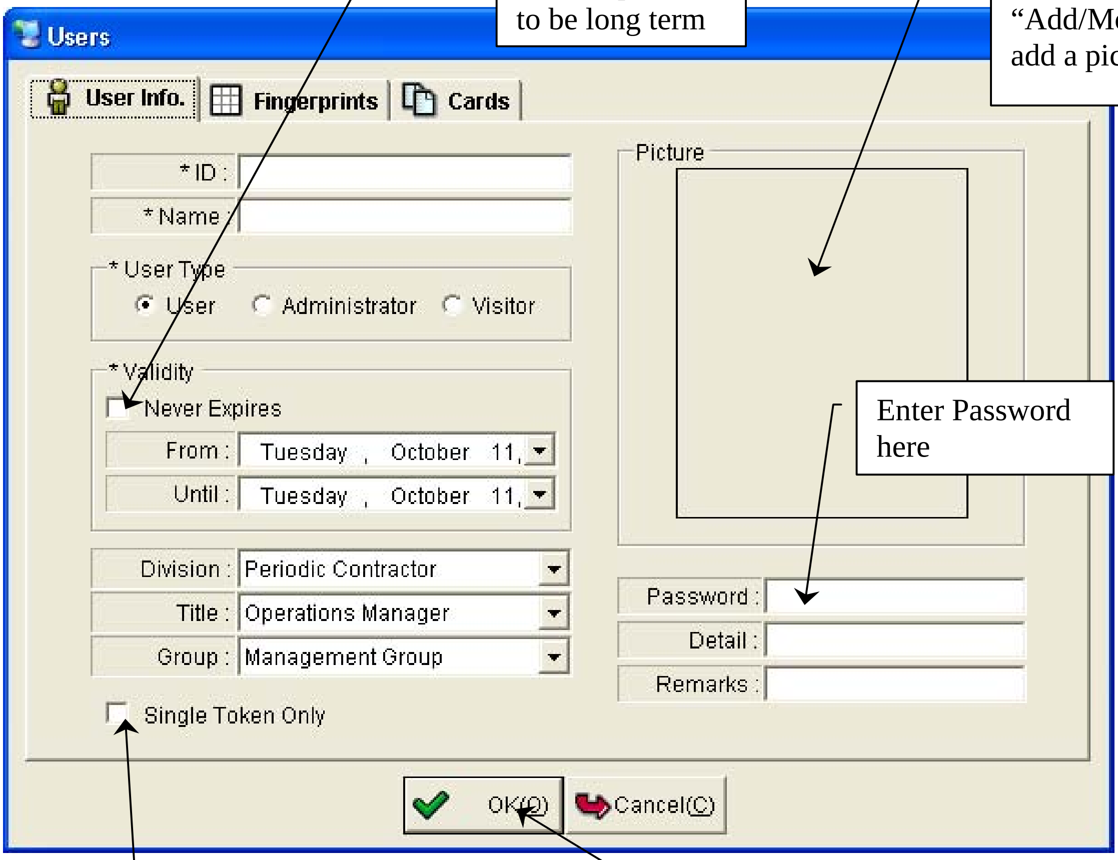
1.4.1.1.6 Use the drop down menus beside “Division”, “Title”, and “Group” to assign these. Note: Division and Title are used for descriptive purposes only and are not required for access system use. Note: A User must be assigned to a Group to be granted access privileges, but they do not have to be assigned in this window. A User can also be assigned to a Group by Drag and Drop in the “Management\User & Groups” window.

1.4.1.1.7 Assign a password of their choice in the “Password” field. Note: This is the password that will be used to logon to the Bio-i BACS software, if they choose not to logon biometrically then when you log on, you will use your ID and this password..

1.4.1.1.8 The “Detail” and “Remarks” fields are for descriptive purposes only and can be left blank or filled in with any desired information.

1.4.1.1.9 In the “Picture” section in the top right, a photo of the User can be entered by placing your cursor in the picture window and right clicking. Then click on “Add/Modify Picture” and a search window will appear to enable you to select a picture.

1.4.1.1.10 Click on the “Single Token Only” box to allow Access by Fingerprint only. This setting for individual Users, will override TRU’s that have been designated as Multi-Token use.



* ID :

* Name :

* User Type ● User ○ Administrator ○ Visitor

* Validity

□ Never Expires

From : Tuesday , October 11,

Until : Tuesday , October 11,

Division : Periodic Contractor

Title : Operations Manager

Group : Management Group

□ Single Token Only

Password :

Detail :

Remarks :

Check Never Expires for users expected to be long term

Right Click here and choose "Add/Modify" to add a picture

Enter Password here

Check the Single Token box to allow access only with Fingerprint for this User on TRU's that are set up for Multi Token use.

On ALL input windows, you MUST click "OK", to save inputted information. You can navigate to other tabs, on any window, prior to saving.

1.4.2 Enrolling Fingerprints

1.4.2.1 Click on the Menu Selection "Management" and select "User & Group" from the Dropdown Menu.

1.4.2.2 In the top section "List of Users" click on the "Add" Icon. The "Users" window will appear. Click on the "Fingerprints" tab. The window shown below will appear. If the user exists, you can choose the user by double-clicking on their line or right clicking and choosing modify.

1.4.2.3 To Enroll a Fingerprint, first choose which finger to enroll by clicking on that finger. Example – R2 is right index.

1.4.2.4 Next, click on the "Add" Icon. There is a prompt field at the bottom of this window. The prompt will instruct to "Scan your finger." Place your finger on the USB enrollment sensor. The prompt will then instruct you to "Remove your finger." Take your finger off the sensor. This prompt will instruct you three times to Scan, and then remove, to obtain three images.

1.4.2.5 At this point the prompt will read "Fingerprint capture succeeded" or "Fingerprint capture failed." If it reads "Succeeded", you can exit this screen by clicking "OK", or proceed to add another fingerprint image, for a different finger, by clicking on that finger and repeating this process. If it reads "Failed", you can attempt enrollment of the same finger again, or try a different finger. It is recommended to enroll at least two fingers per user, one from each hand.

1.4.1.6 After successful fingerprint enrollment you may exit this window by clicking "OK" or select one of the other tabs in this window. If you choose to exit this window you MUST click "OK" to save inputted information. **NOTE: IT IS RECOMMENDED TO CHECK THE BOX TO STORE THE USERS FINGERPRINT IN THE DATABASE!** This is very useful for troubleshooting poor quality enrollments.

1.4.2.7 After successful enrollment, the section on the right of this screen "List of Finger Prints", will list all enrolled fingers for this User. There are two functions that can be set in this section.

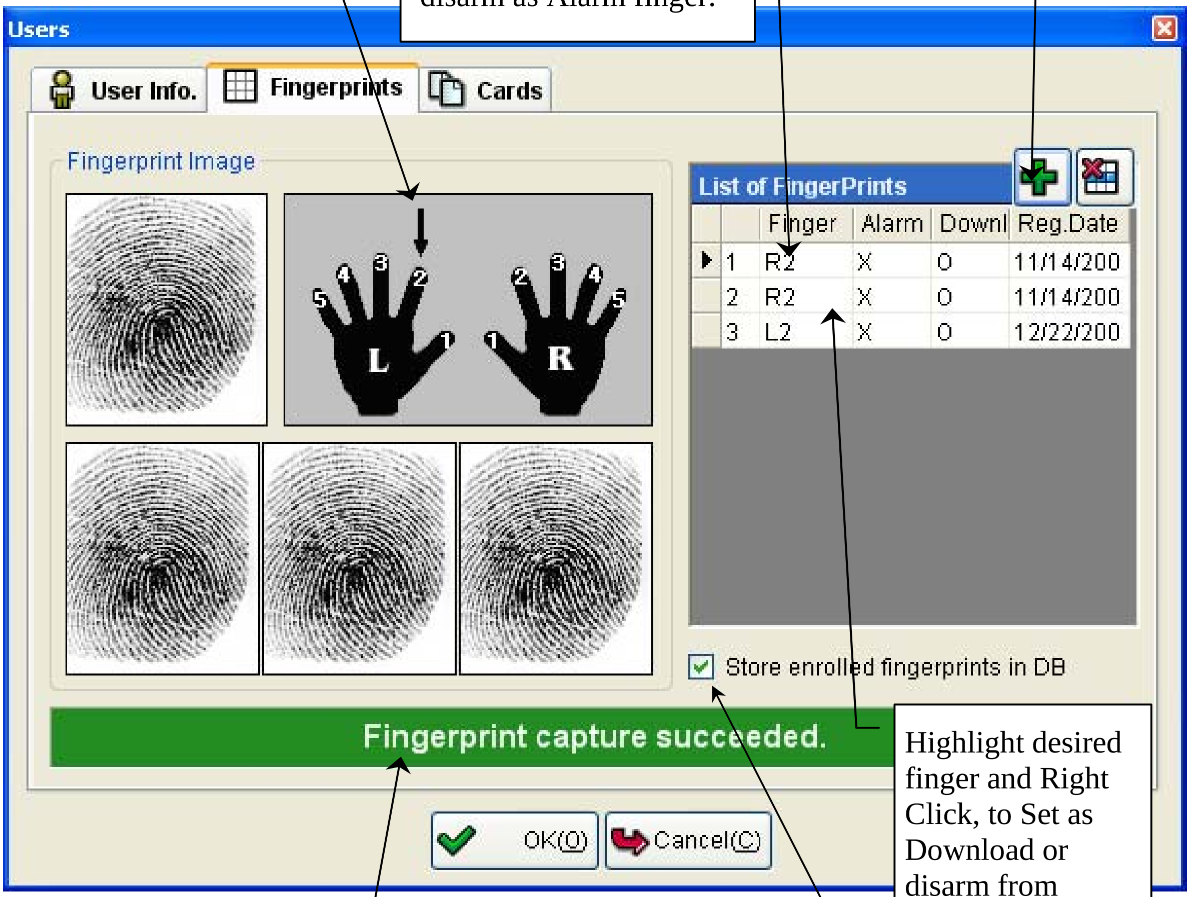
1.4.2.8 The first function is to designate as an Alarm Finger, or not. Highlight the desired enrollment finger by clicking on that line, example shown – R2. If there is an "X" in the "Alarm" box, it designates this finger is "NOT" set as an alarm finger. Right Click on this line. You will receive three options. We will address alarm option "Set to Alarm Finger" first. If you click on this option it will set this finger, when used, to trigger the Alarm that your System Administrator configures. When you designate as Alarm Finger with this option, there will be an "O" in the alarm field. You disarm this finger from the Alarm function by the same process.

1.4.2.9 Next, with the desired enrollment finger highlighted, right click. This time choose the function "Set to Download." The default for this function sets all fingers enrolled to download. This setting is shown with an "O" in the download column. If for some reason the TRU looses Network connection, the selected finger enrollments that have been downloaded will still be able to be used. They are downloaded to the memory in the TRU itself. It is recommended to set only one finger to download, as memory in the TRU is limited. Authentication Time will increase with the number of templates stored. Set with an "X", in this column, finger enrollments are not to be downloaded.

Click on the finger to be enrolled

Highlight desired finger and Right Click, to Set as Alarm finger or disarm as Alarm finger.

Click on Add Icon



	Finger	Alarm	Downl	Reg.Date
1	R2	X	O	11/14/200
2	R2	X	O	11/14/200
3	L2	X	O	12/22/200

☑ Store enrolled fingerprints in DB

Fingerprint capture succeeded.

Highlight desired finger and Right Click, to Set as Download or disarm from downloading

Prompt Field will read “Scan your finger”, then “Remove your finger” three times. Then it will prompt fingerprint capture Succeeded or Failed.

NOTE: This check box will cause the fingerprint image to be stored in the database. We recommend that this be checked

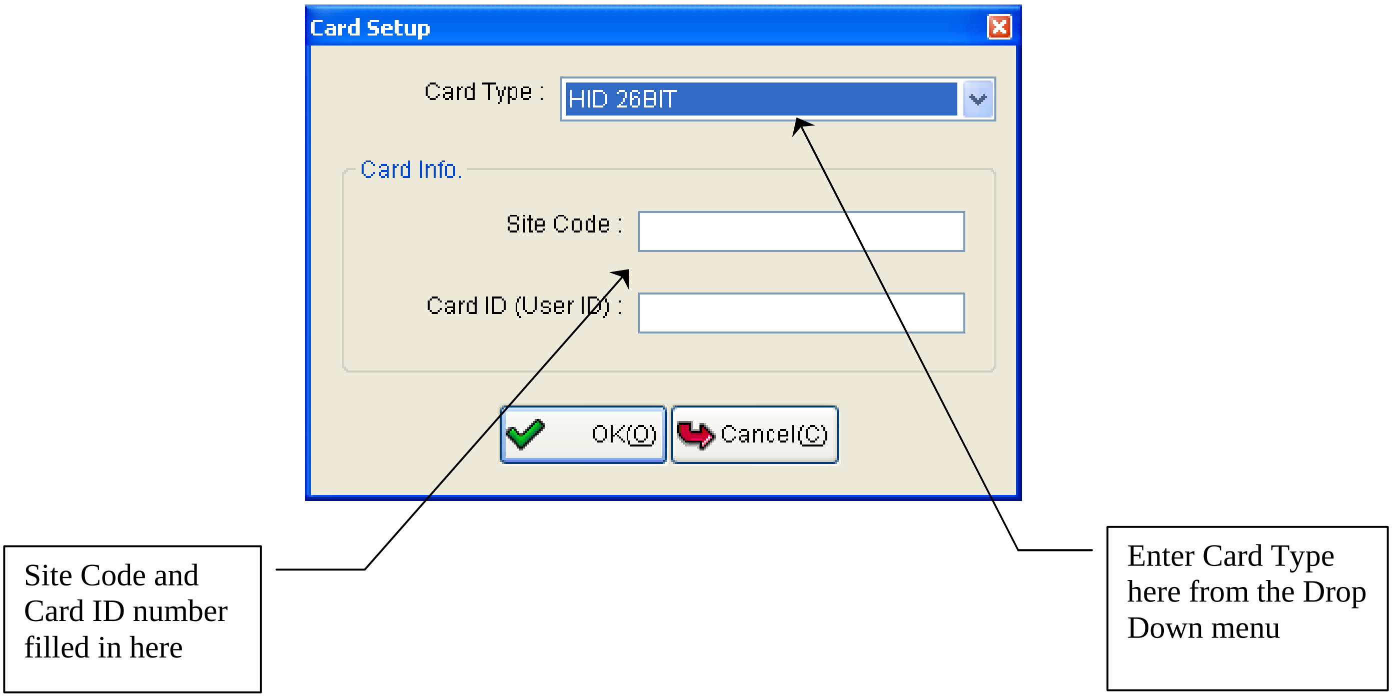
1.4.3 Enrolling Prox Cards

1.4.3.1 The final tab on this window is “Cards.” Click on this tab to assign a Prox card to the user. Click on the “Add” Icon and the “Card Setup” window shown below will appear.

1.4.3.2 Enter Card Type from drop down menu. Default card type is HID. See your System Administrator.

1.4.3.3 Next, fill in the "Site Code" and "Card ID (User ID)" fields. The information for inputting in these fields is provided by the Card Manufacturer.

1.4.3.4 Click "OK" to save and exit.



Card Type : HID 26BIT

Site Code :

Card ID (User ID) :

Site Code and Card ID number filled in here

Enter Card Type here from the Drop Down menu

1.5.1 Setting up Groups

Click on Menu Selection "Management" and select "User & Group."

1.5.1.1 In the lower left section "List of Groups", click on the "Add" Icon.

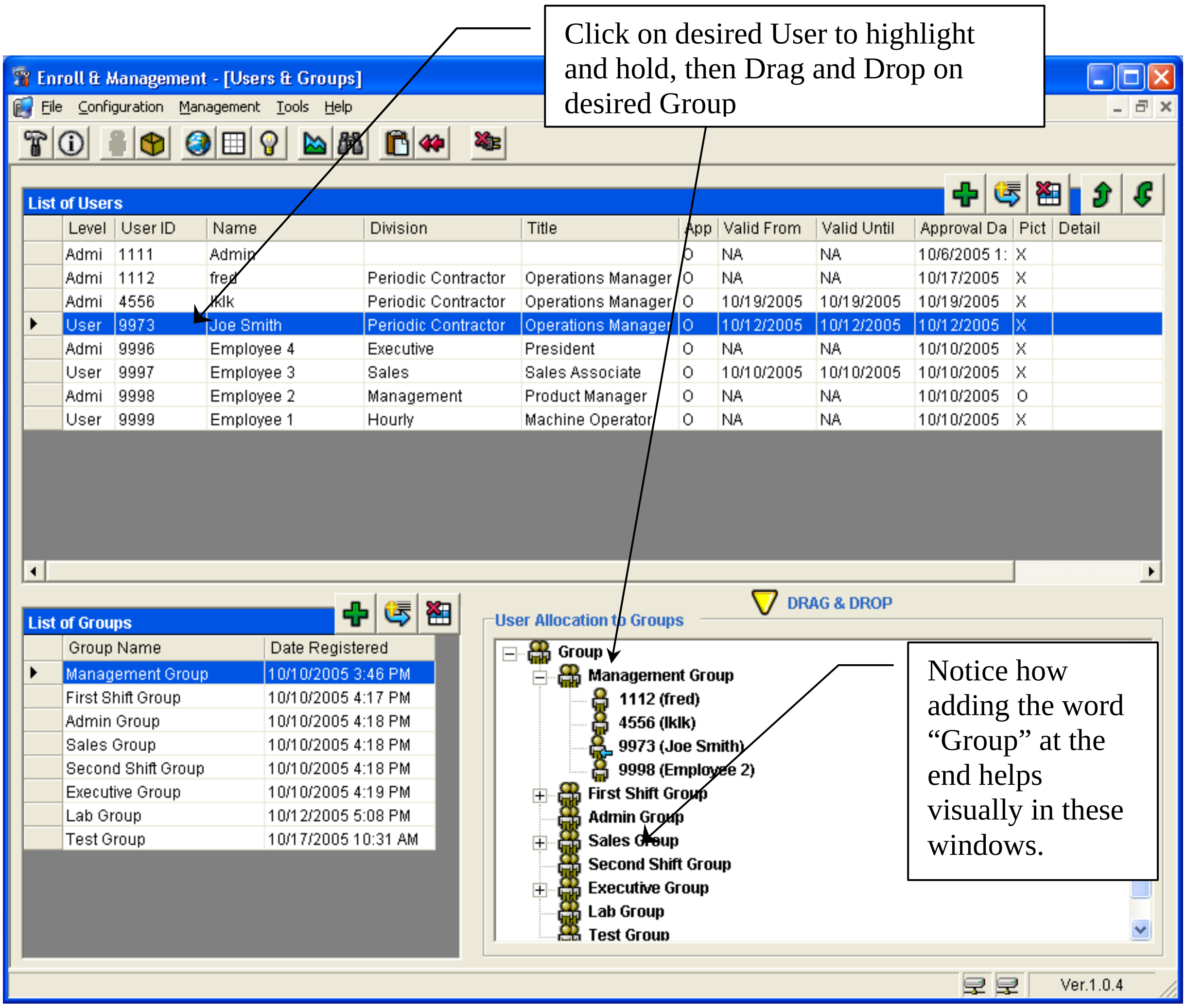
1.5.1.2 This will bring up the "Groups" window. Fill in a unique name.

1.5.1.3 Helpful hint - When naming Groups, it can be helpful to add to the end of the name the word "Group." For instance, instead of naming the Group "First Shift", name it "First Shift Group." This helps in the screens where you visually check Groups, and Access Times, and Users.

1.5.2 Assigning Users to Groups

Click on Menu Selection "Management" and select "User & Group." The screen shown below will appear.

1.5.2.1 Click on to highlight and hold the desired User in the top left “List of Users” section. Drag and Drop on the desired Group in the bottom right section “User Allocation to Groups.”



Click on desired User to highlight and hold, then Drag and Drop on desired Group

Enroll & Management - [Users & Groups]
File Configuration Management Tools Help

List of Users

Level	User ID	Name	Division	Title	App	Valid From	Valid Until	Approval Da	Pict	Detail
Admi	1111	Admin			O	NA	NA	10/6/2005 1:	X	
Admi	1112	fred	Periodic Contractor	Operations Manager	O	NA	NA	10/17/2005	X	
Admi	4556	lklk	Periodic Contractor	Operations Manager	O	10/19/2005	10/19/2005	10/19/2005	X	
User	9973	Joe Smith	Periodic Contractor	Operations Manager	O	10/12/2005	10/12/2005	10/12/2005	X	
Admi	9996	Employee 4	Executive	President	O	NA	NA	10/10/2005	X	
User	9997	Employee 3	Sales	Sales Associate	O	10/10/2005	10/10/2005	10/10/2005	X	
Admi	9998	Employee 2	Management	Product Manager	O	NA	NA	10/10/2005	O	
User	9999	Employee 1	Hourly	Machine Operator	O	NA	NA	10/10/2005	X	

List of Groups

Group Name	Date Registered
Management Group	10/10/2005 3:46 PM
First Shift Group	10/10/2005 4:17 PM
Admin Group	10/10/2005 4:18 PM
Sales Group	10/10/2005 4:18 PM
Second Shift Group	10/10/2005 4:18 PM
Executive Group	10/10/2005 4:19 PM
Lab Group	10/12/2005 5:08 PM
Test Group	10/17/2005 10:31 AM

```
Group
  Management Group
    1112 (fred)
    4556 (lklk)
    9973 (Joe Smith)
    9998 (Employee 2)
  First Shift Group
  Admin Group
  Sales Group
  Second Shift Group
  Executive Group
  Lab Group
  Test Group
```

Notice how adding the word “Group” at the end helps visually in these windows.

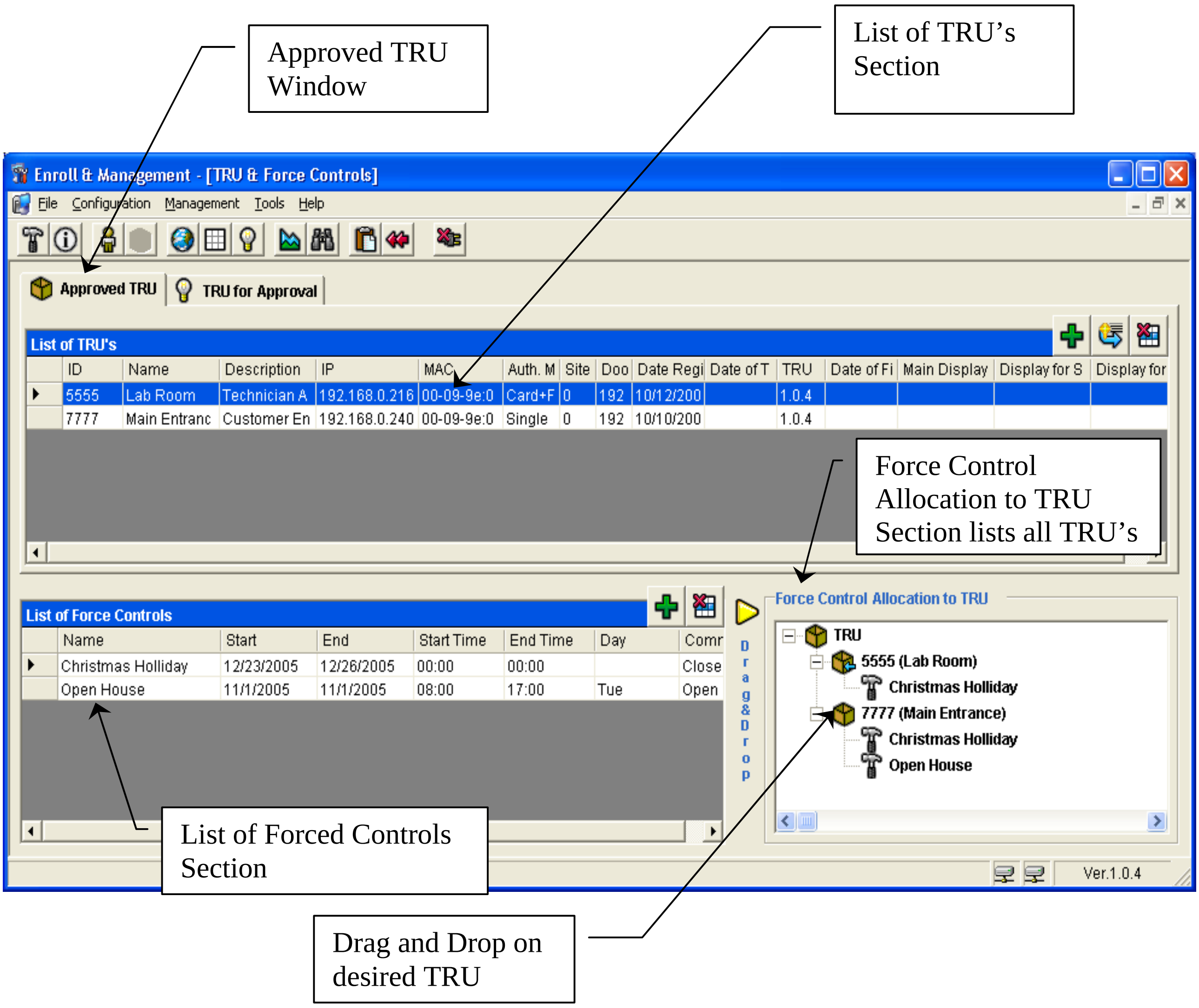
1.6 TRU & Forced Controls

Click on Menu Selection “Management”, then select “TRU & Forced Controls” from the Dropdown Menu. There are two tabs at the top of this window, “Approved TRU” and “TRU for Approval.”

1.6.1 Approved TRU Tab

1.6.1.1 We will describe the “Approve TRU” tab first. Click on the “Approve TRU” tab and the window shown below will appear.

1.6.1.2 There are three sections in this window, “List of TRU’s”, “List of Forced Controls”, and “Force Control Allocation to TRU.” We will go over each of these.



List of TRU's

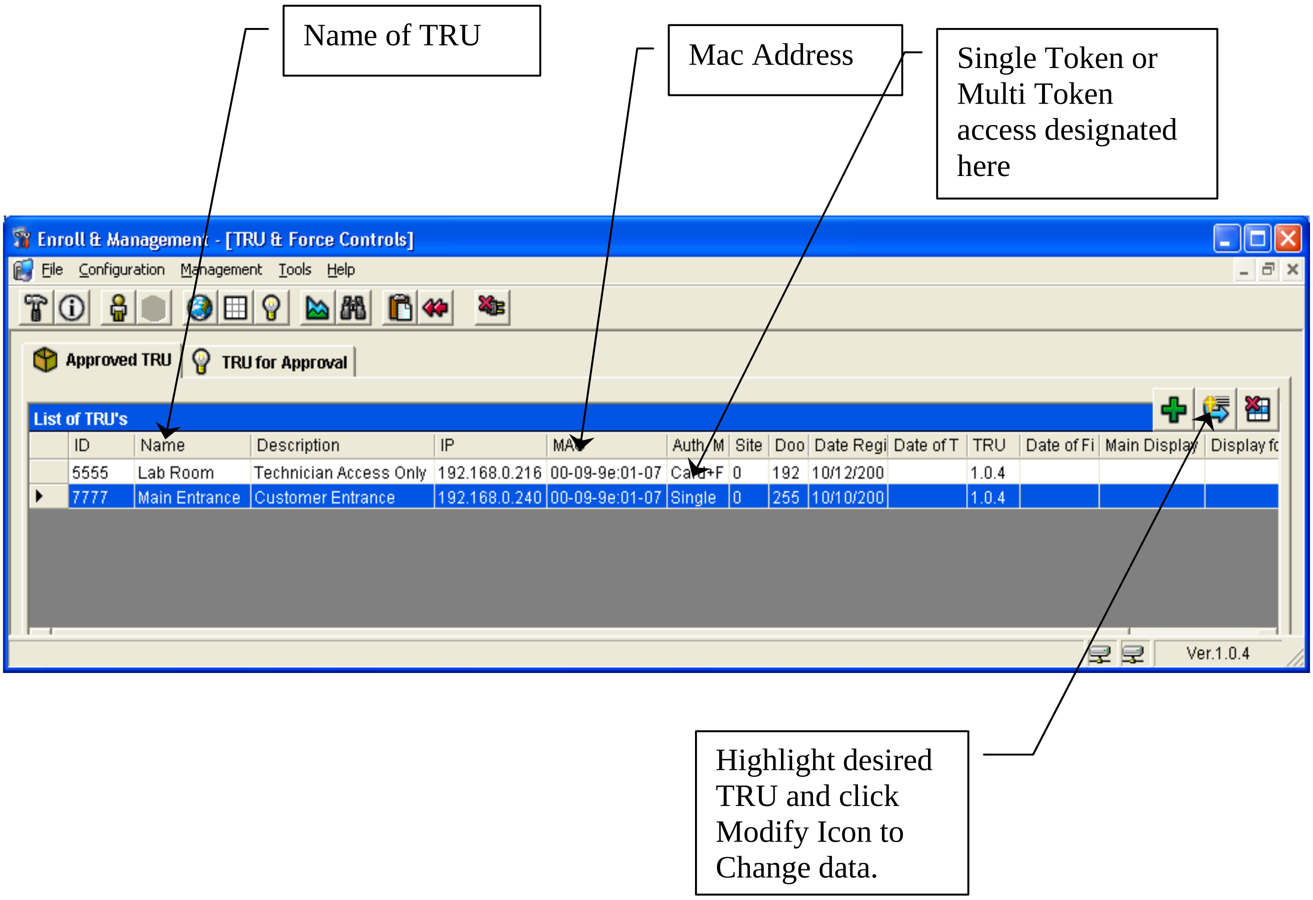
ID	Name	Description	IP	MAC	Auth. M	Site	Doo	Date Regi	Date of T	TRU	Date of Fi	Main Display	Display for S	Display for
5555	Lab Room	Technician A	192.168.0.216	00-09-9e:0	Card+F	0	192	10/12/200		1.0.4				
7777	Main Entranc	Customer En	192.168.0.240	00-09-9e:0	Single	0	192	10/10/200		1.0.4				

List of Force Controls

Name	Start	End	Start Time	End Time	Day	Comr
Christmas Holliday	12/23/2005	12/26/2005	00:00	00:00		Close
Open House	11/1/2005	11/1/2005	08:00	17:00	Tue	Open

1.6.1.3 This section will show a list of all TRU's that have been configured and approved for use. Pertinent information such as Name, Description, IP, Mac Address, etc. is shown for each approved TRU.

1.6.1.4 You can Modify or Delete a TRU here by clicking on and highlighting a TRU, then clicking on the Modify or Delete Icons. You can also Right Click to get the same options.



Name of TRU

Mac Address

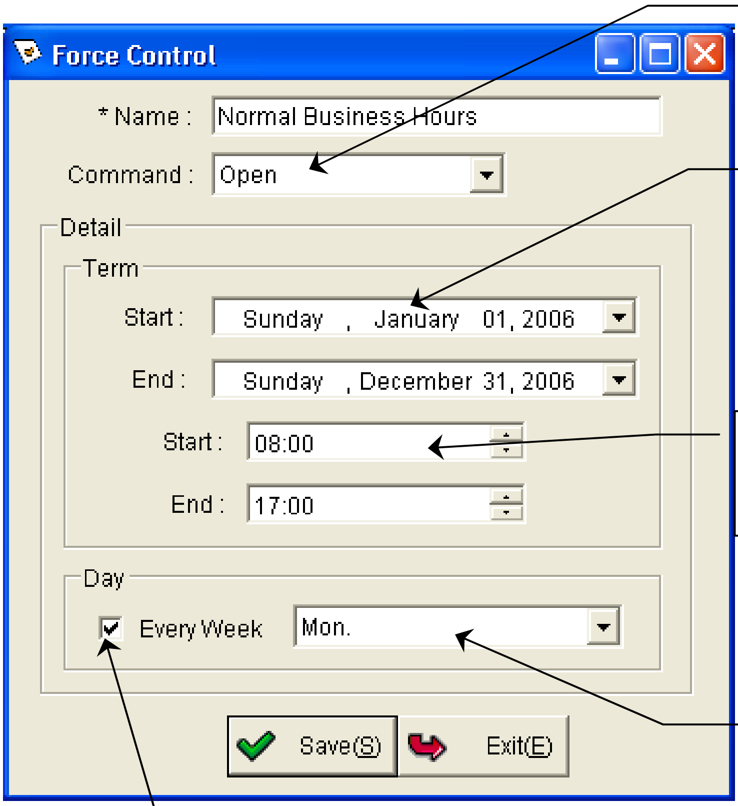
Single Token or Multi Token access designated here

Highlight desired TRU and click Modify Icon to Change data.

ID	Name	Description	IP	MAC	Auth M	Site	Doo	Date Regi	Date of T	TRU	Date of Fi	Main Display	Display fc
5555	Lab Room	Technician Access Only	192.168.0.216	00-09-9e:01-07	Card+F	0	192	10/12/200		1.0.4			
7777	Main Entrance	Customer Entrance	192.168.0.240	00-09-9e:01-07	Single	0	255	10/10/200		1.0.4			

1.6.1.5 This section shows a list of programmed forced controls, with information about these controls such as Dates, Times, Day, and command Open or Closed.

1.6.1.6 To Add new forced controls click on the "Add" Icon. The "Force Control" window shown below will appear.



Force Control

* Name : Normal Business Hours

Command : Open

Detail

Term

Start : Sunday , January 01, 2006

End : Sunday , December 31, 2006

Start : 08:00

End : 17:00

Day

☑ Every Week Mon.

Enter command to Force "Open" or "Closed" here.

Must Enter Start and End Dates here to cover the range of dates for entered Force Control to be in effect

Enter Start and End times that Force Control will be in effect here.

You **Must** fill in the day of the week here from the Drop Down Menu if you Check the Every Week box. The Force Control will apply to the selected day for all weeks in the date range programmed above.

Check here only if the forced control is being programmed for a day of the week, for multiple weeks.

1.7 "Force Control Allocation to TRU" section.

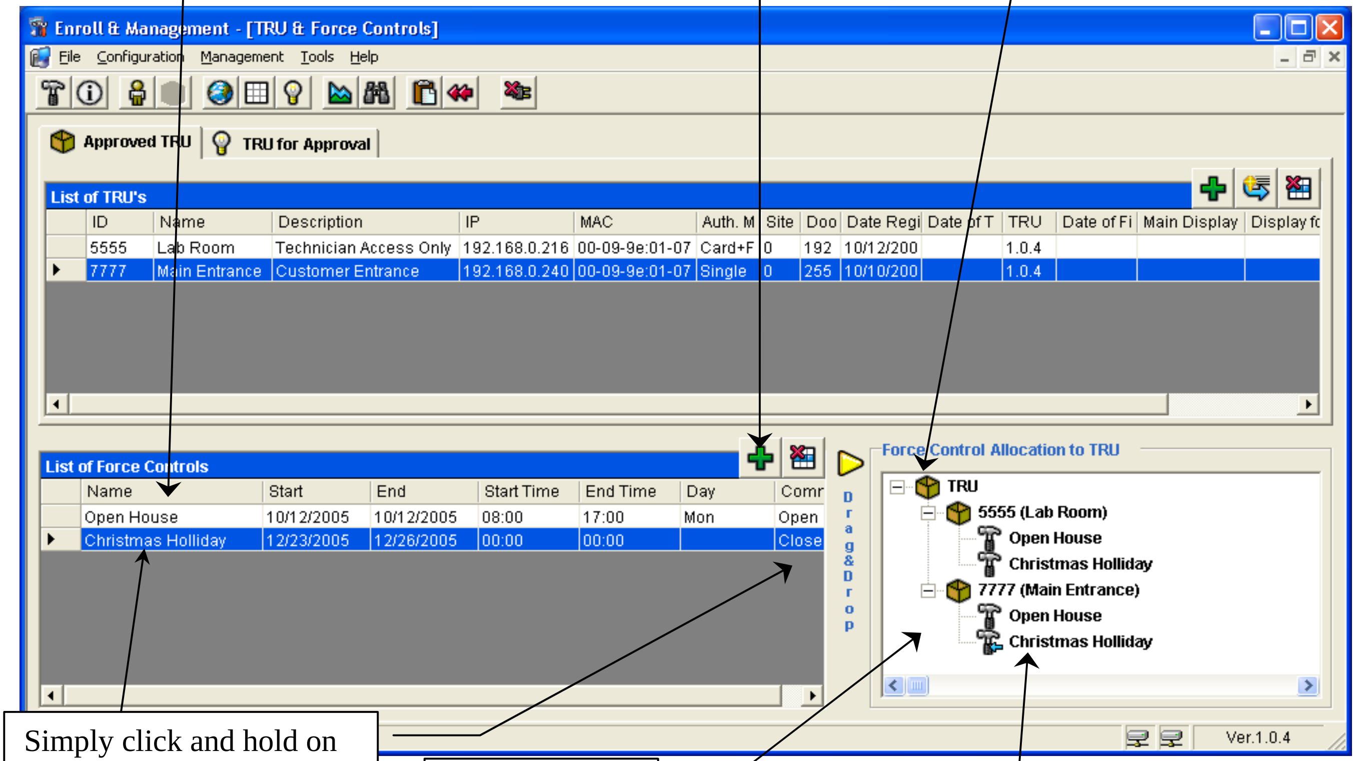
1.7.1 This section performs two functions. The first function is to attach Force Controls to TRU's. Simply click and hold on the Force Control in the "List of Force Controls" section that you want to attach, and Drag and Drop it on the TRU in the "Force Control Allocation to TRU" section.

1.7.2 The second is a visual look at all TRU's, and if there are any Force Controls attached to them. In the example shown below you will see that both TRU's have "Christmas Holliday" and "Open House" attached. One is programmed to Force Open, while the other is programmed to Force Closed.

List of programmed Forced Controls

Click Add Icon to program new Force Control

List of Approved TRU's



Enroll & Management - [TRU & Force Controls]

List of TRU's

	ID	Name	Description	IP	MAC	Auth. M	Site	Doo	Date Regi	Date of T	TRU	Date of Fi	Main Display	Display fc
	5555	Lab Room	Technician Access Only	192.168.0.216	00-09-9e:01-07	Card+F	0	192	10/12/200		1.0.4			
▶	7777	Main Entrance	Customer Entrance	192.168.0.240	00-09-9e:01-07	Single	0	255	10/10/200		1.0.4			

List of Force Controls

	Name	Start	End	Start Time	End Time	Day	Comr
	Open House	10/12/2005	10/12/2005	08:00	17:00	Mon	Open
▶	Christmas Holliday	12/23/2005	12/26/2005	00:00	00:00		Close

Force Control Allocation to TRU

- TRU
  - 5555 (Lab Room)
    - Open House
    - Christmas Holliday
  - 7777 (Main Entrance)
    - Open House
    - Christmas Holliday

Simply click and hold on the Force Control and Drag and Drop on the TRU to attach.

Visual of Force Controls that are attached to TRU's

Right Click on the Force Control here and it will give you the option to Detach or Delete the Force Control

1.7.3 The TRU **MUST** be updated when a Force Control is attached to a TRU for the Force Control to be in effect. Click on Menu Selection "Tools" and select "TRU Update". Check the box next to the TRU you would like to Update, and then click the Update Button at the bottom of the screen. This will apply the force control to the TRU.

1.8 TRU for Approval Tab

1.8.1 Click on Menu Selection "Management" and select "TRU & Forced Controls" from the Dropdown Menu.

1.8.2 There are two tabs at the top of this window, "Approved TRU" and "TRU for Approval."

1.8.3 Click on the "TRU for Approval" tab and the window shown below will appear.

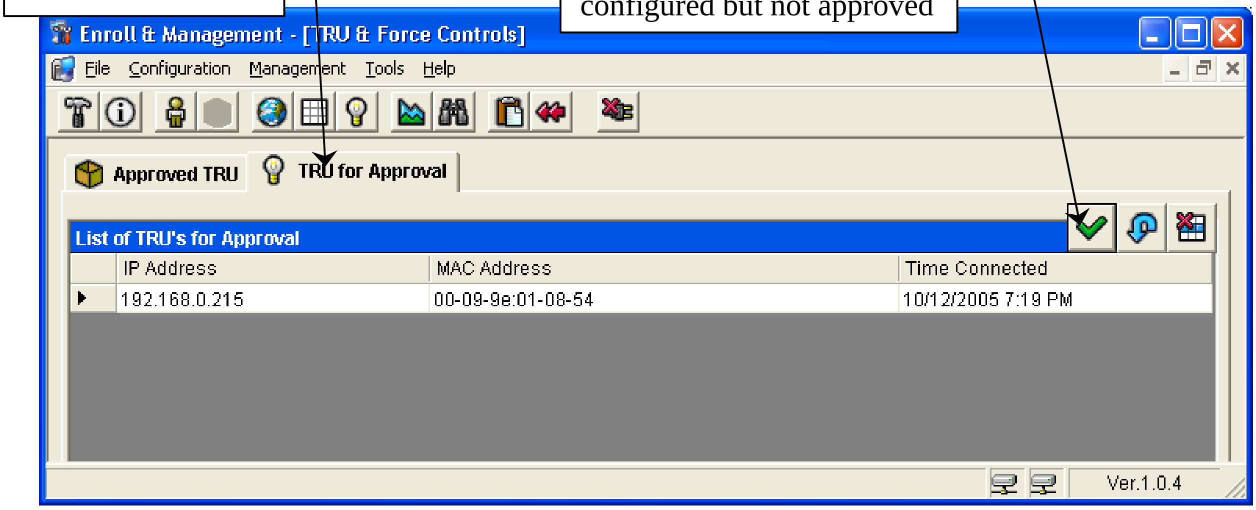
1.8.4 This window contains the "List of TRU's for Approval" section. It also contains two sections, "List of Force Controls" and "Force Control allocation to TRU" that were also contained in the tab, "Approved TRU," that we just covered. These two sections perform exactly the same in this window and we will not address them here.

1.8.5 When a TRU is configured in the TermIPConfig program, covered later in this manual. This window is used to approve that TRU for use.

1.8.6 Click on the "Refresh" Icon (Check Mark) to display any TRU's that have been configured but not yet approved.

Click on the TRU for Approval tab to display this window

Click on the Refresh Icon to bring up in this window any TRU's that have been configured but not approved



List of TRU's for Approval

IP Address	MAC Address	Time Connected
192.168.0.215	00-09-9e:01-08-54	10/12/2005 7:19 PM

1.8.7 Click on the "Approve" Icon (U shaped arrow) or right click on the desired TRU and select Approve. The "TRU" window that appears is shown below.

1.8.8 Fill in a unique ID number and a Name. The Mac Address field will already be filled in for the TRU that was configured for approval.

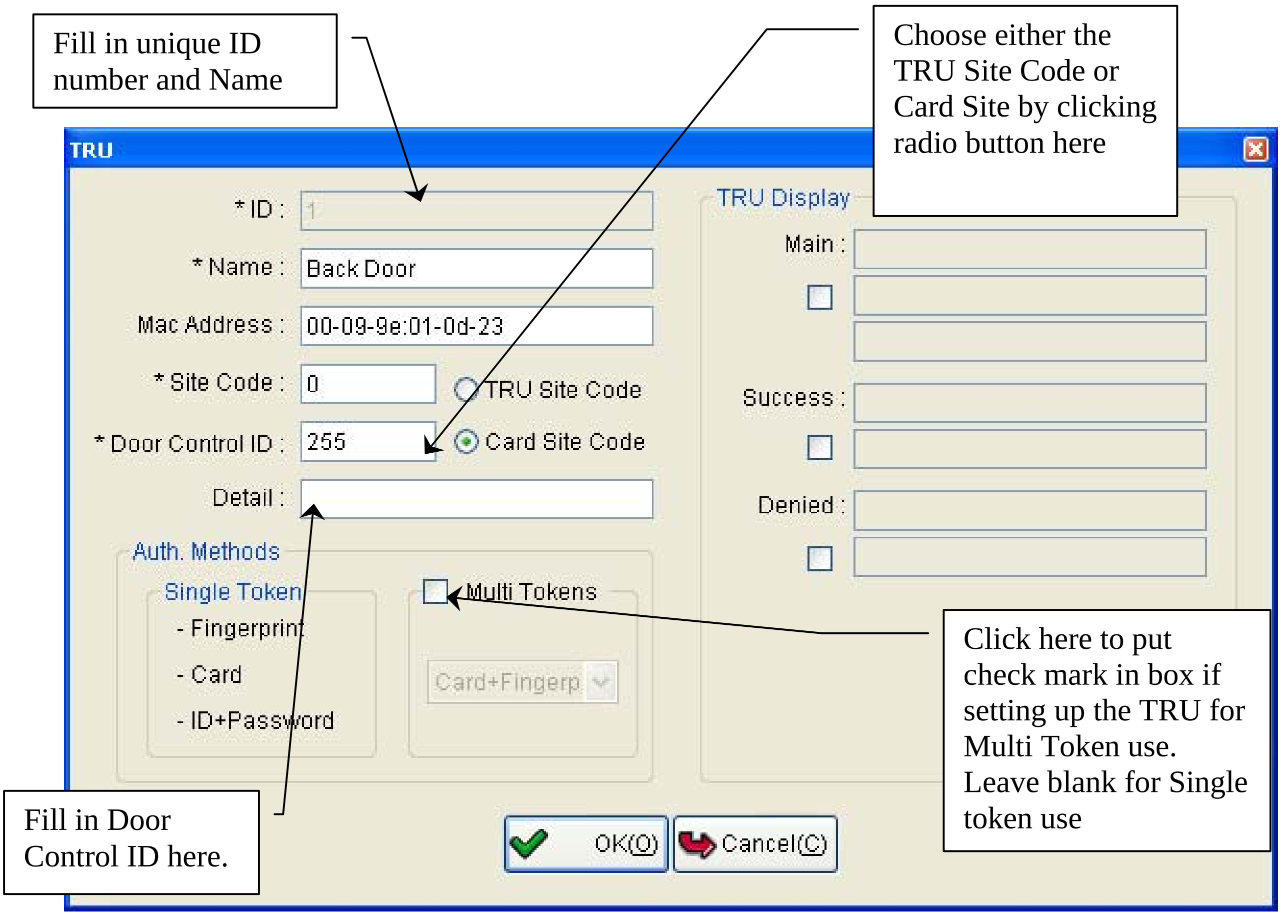
1.8.9 Choose the “TRU Site Code” or “Card Site Code” radio button. Choose “Card Site Code” if Door Control is to be handled by an Access Control system other than provided by Integrated Biometrics. Choose “TRU Site Code” if handled by Integrated Biometrics system.

1.8.10 Fill in the “Door Control ID” field if you choose “TRU Site Code.” The manufacturers default setting is 255. See Hardware Manual for the programming of different Door ID’s.

1.8.11 The “Detail” field is a free form descriptive field for your use. It is not required to be filled in.

1.8.12 The “Multi Tokens” check box determines whether you are setting up this TRU for Single Token Access or Multi Token Access. If you leave this check box blank, the TRU will be Single Token. Either Biometric **<u>or</u>** Prox Card will allow Access.

1.8.13 If Multi-Token identification for access is desired, check the “Multi Token” box, and choose “Card & Fingerprint” from the drop down Menu. To activate programming of Multi-Token, you must update the TRU in the “Tools/TRU Update” menu selection. When Multi-Token is set, present Prox card first, then finger. It is not necessary to press the enter button before presenting finger after Prox card. If Multi-Token is then unchecked to set this TRU back to single token, again you must update the TRU to reset it.



* ID : 1

* Name : Back Door

Mac Address : 00-09-9e:01-0d-23

* Site Code : 0 ○ TRU Site Code

* Door Control ID : 255 ● Card Site Code

Detail :

Fill in unique ID number and Name

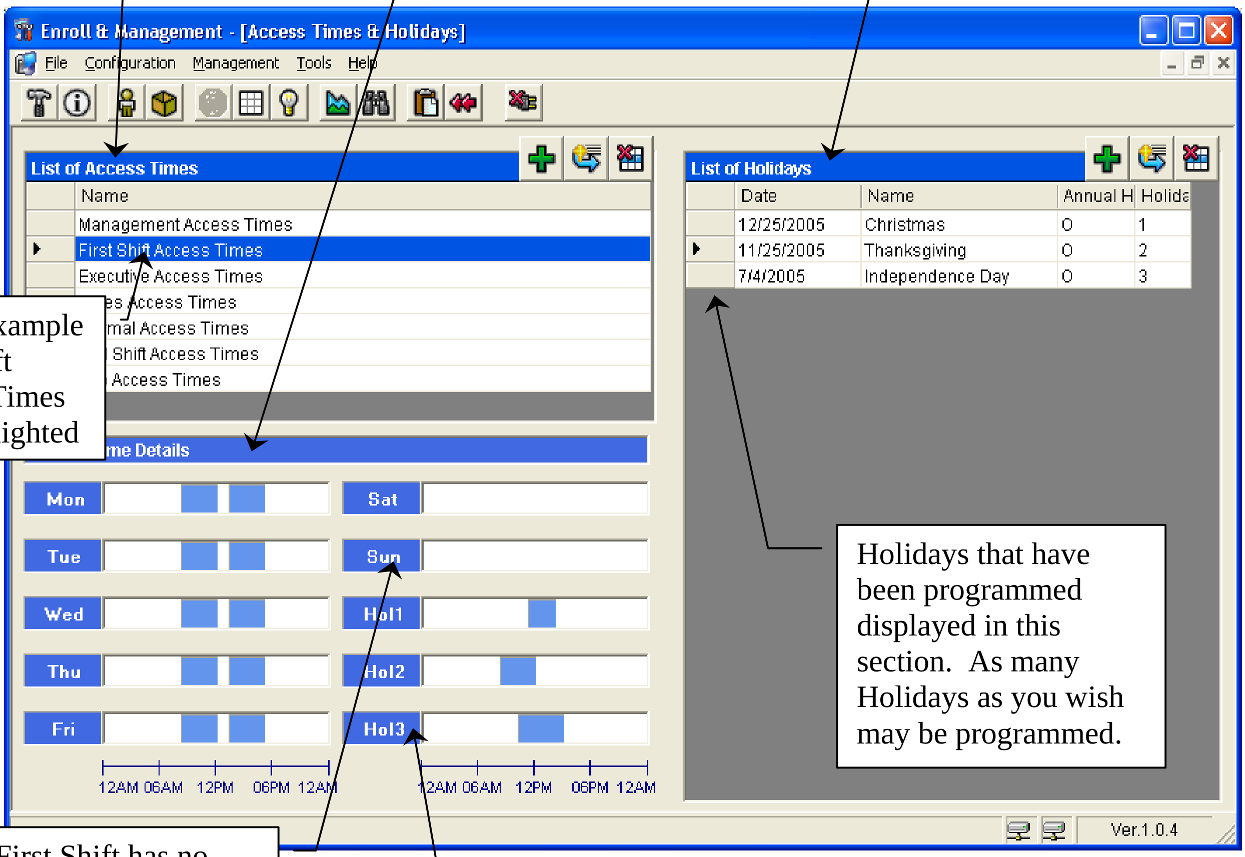
Choose either the TRU Site Code or Card Site by clicking radio button here

Fill in Door Control ID here.

Click here to put check mark in box if setting up the TRU for Multi Token use. Leave blank for Single token use

1.9 Access Time Setup

Click on Menu Selection “Management.” Select “Access Time Setup” from the Dropdown Menu. The three sections in this window are “List of Access Times”, “Access Time Details” and “List of Holidays.” An example is shown below. We will review these by section.



Name
Management Access Times
First Shift Access Times
Executive Access Times
...es Access Times
...mal Access Times
... Shift Access Times
... Access Times

Date	Name	Annual H	Holida
12/25/2005	Christmas	0	1
11/25/2005	Thanksgiving	0	2
7/4/2005	Independence Day	0	3

“List of Access Times” section

“Access Time Details” section

“List of Holidays” section

In this example First shift Access Times are highlighted

Holidays that have been programmed displayed in this section. As many Holidays as you wish may be programmed.

First Shift has no programmed access on Saturday and Sunday

“First Shift Access Times” are highlighted above. Access Time Details shows a Bar Graph of the programmed access times. Notice that it shows times for Hol 1, Hol 2, and Hol 3. The dates for these Holidays were programmed in the “List of Holidays” section above right.

1.9.1 Access Times Section

The “List of Access Times” section is used to set up and modify Access times.

1.9.1.1 To set up a new Access Time click on the “Add” icon in this section. The window shown below will appear. To modify an existing Access Time, click on the desired line to highlight, and click on the “Modify” Icon.

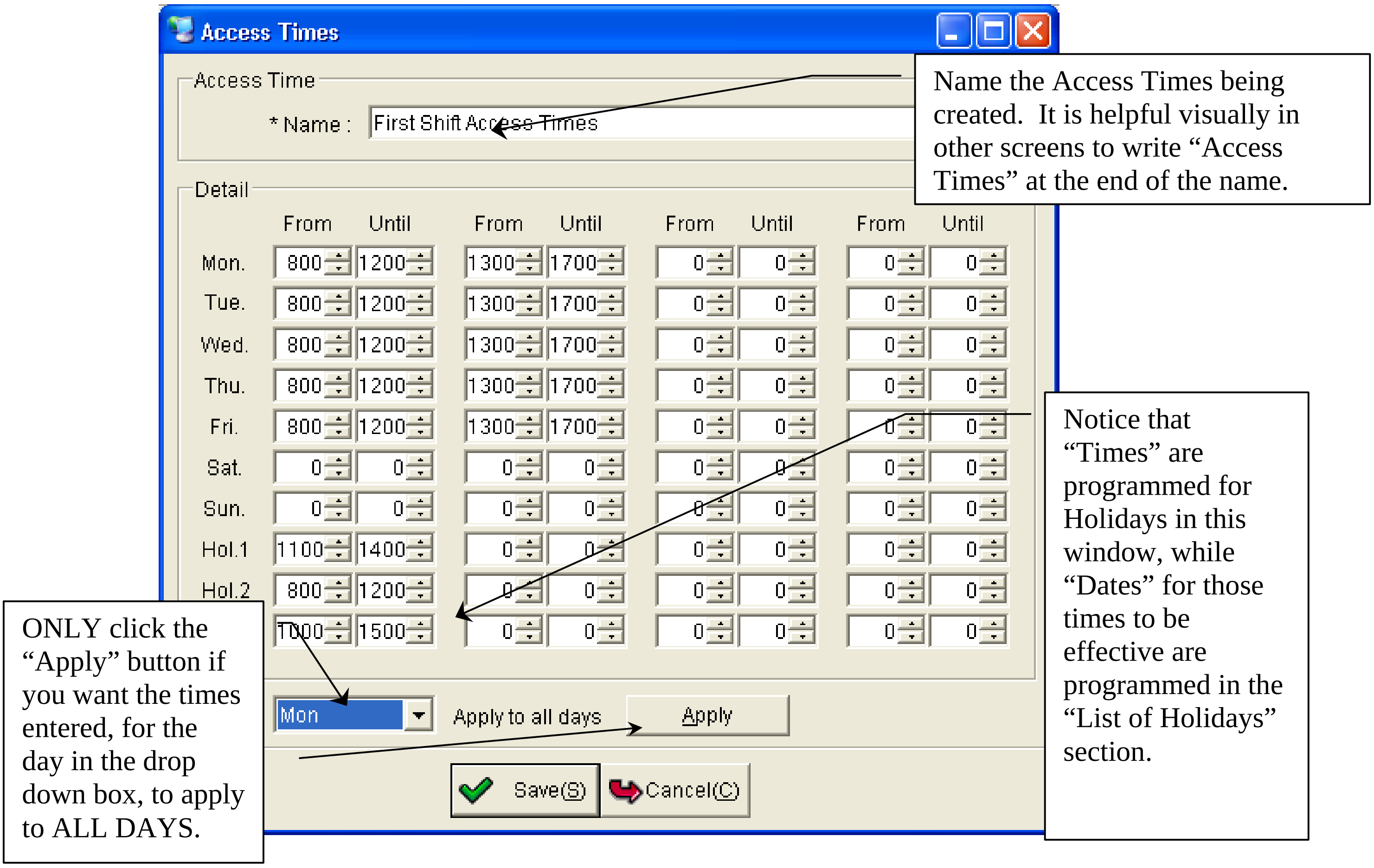
1.9.1.2 This window gives the option of four breaks in access times, such as 0800 to 1200, then 1300 to 1700, etc. This would give access in all hours between 0800 and 1700, except for 1200 to 1300. Each day can be set up for different access times, or all days can be set the same. The times can be set with the up and down arrows, or by clicking on the box and typing in the desired times.

1.9.1.3 If setting all days with the same times, example 0800 to 1700, simply fill in any day Monday through Friday, select that day, example Monday, from the drop down menu at the bottom left of this window, and click the “Apply” button. This will apply this time to all days.

1.9.1.4 Do not click the “Apply” button, **unless**, you want to apply the same times to all days. If access times vary by day, do not click the “Apply” button. Simply click the “Save” button.

1.9.1.5 Helpful hint. When naming Access times, it can be helpful to add to the end of the name the words “Access Times.” For instance, in the example shown below, instead of naming these times “First Shift”, they were named “First Shift Access Times.” This helps in the screens where you visually check Groups, and Access Times, and Users. \

1.9.1.6 Note that when inputting a set of Access Times, the times that are inputted for Hol1, Hol2, and Hol3 will apply as the access times, to the Holidays shown under the “List of Holidays” in the right side of this window that are input as Hol1 or Hol2 or Hol3.



* Name : First Shift Access Times

	From	Until	From	Until	From	Until	From	Until
Mon.	800	1200	1300	1700	0	0	0	0
Tue.	800	1200	1300	1700	0	0	0	0
Wed.	800	1200	1300	1700	0	0	0	0
Thu.	800	1200	1300	1700	0	0	0	0
Fri.	800	1200	1300	1700	0	0	0	0
Sat.	0	0	0	0	0	0	0	0
Sun.	0	0	0	0	0	0	0	0
Hol.1	1100	1400	0	0	0	0	0	0
Hol.2	800	1200	0	0	0	0	0	0
	1000	1500	0	0	0	0	0	0

Mon

Name the Access Times being created. It is helpful visually in other screens to write "Access Times" at the end of the name.

Notice that "Times" are programmed for Holidays in this window, while "Dates" for those times to be effective are programmed in the "List of Holidays" section.

ONLY click the "Apply" button if you want the times entered, for the day in the drop down box, to apply to ALL DAYS.

1.10.1 List of Holidays Section

The "List of Holidays" section is in the top right of this window. It is used to Name and Assign the Date of any programmed Holidays.

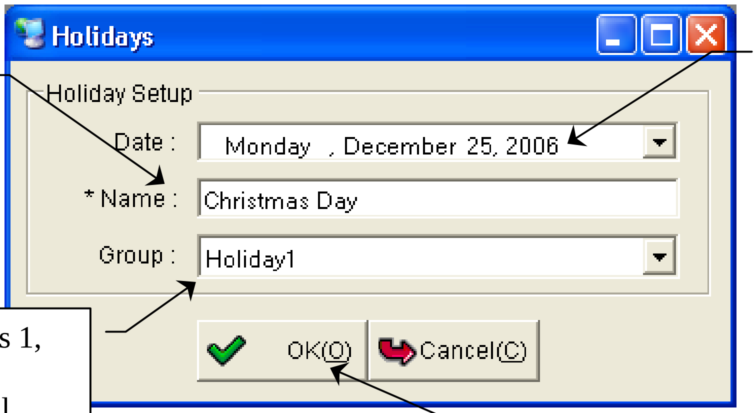
1.10.1.1 When you click the "Add" Icon in this section the window shown below appears.

1.10.1.2 Choose the date from the drop down menu.

1.10.1.3 Choose a name for the Holiday.

1.10.1.4 Assign as Holiday 1, 2, or 3 in the "Group" blank from the drop down menu. This will match the Date to the programmed Access Times for Holliday 1, 2, or 3, as set up in the "Access Times" window shown above.

1.10.1.4 As many Holidays as you wish may be programmed. All Holidays are programmed to be annual.



Date : Monday , December 25, 2006

* Name : Christmas Day

Group : Holiday1

Name the Holliday

Select the date for assigned Access Times to apply.

Assign the Holiday as 1, 2, or 3 from the drop down menu. This will match it with Holiday 1, 2, or 3 as programmed in “Access Times” in the section above

Click “OK” to save inputted data.

1.10.2 Access Time Detail Section

This section simply shows programmed Access Times in Bar Graph form.

1.10.3 Using a Wiegand Based Access Control System

Please refer to the separate document titled “Wiegand operation for 3rd party access control”.

1.11 [Group: Access Time] Setup

Click on the Menu Selection “Management” and select “[Group: Access Time] Setup” from the Drop down Menu.

1.11.1 This window is used to attach “Access Times” to “Groups.” Note: You may drag group from the left side “List of Groups” to the right side “Access Time Allocation to Groups” multiple times. This enables the attaching of different Access Times to the same Group. By doing this you may assign a Group different Access Times to different TRU’s (different times to different doors/areas) in the “[TRU: Group-Access Time] Setup” window. In the example shown below the “Sales Group” has been assigned “Sales Access Times” and “2nd Shift Access Times.”

1.11.2 Simply click on the set of “Access Times” in the bottom left section, “List of Access Times”, and drag and drop it on the desired “Group” in the top right section, “Access Time Allocation to Groups.”

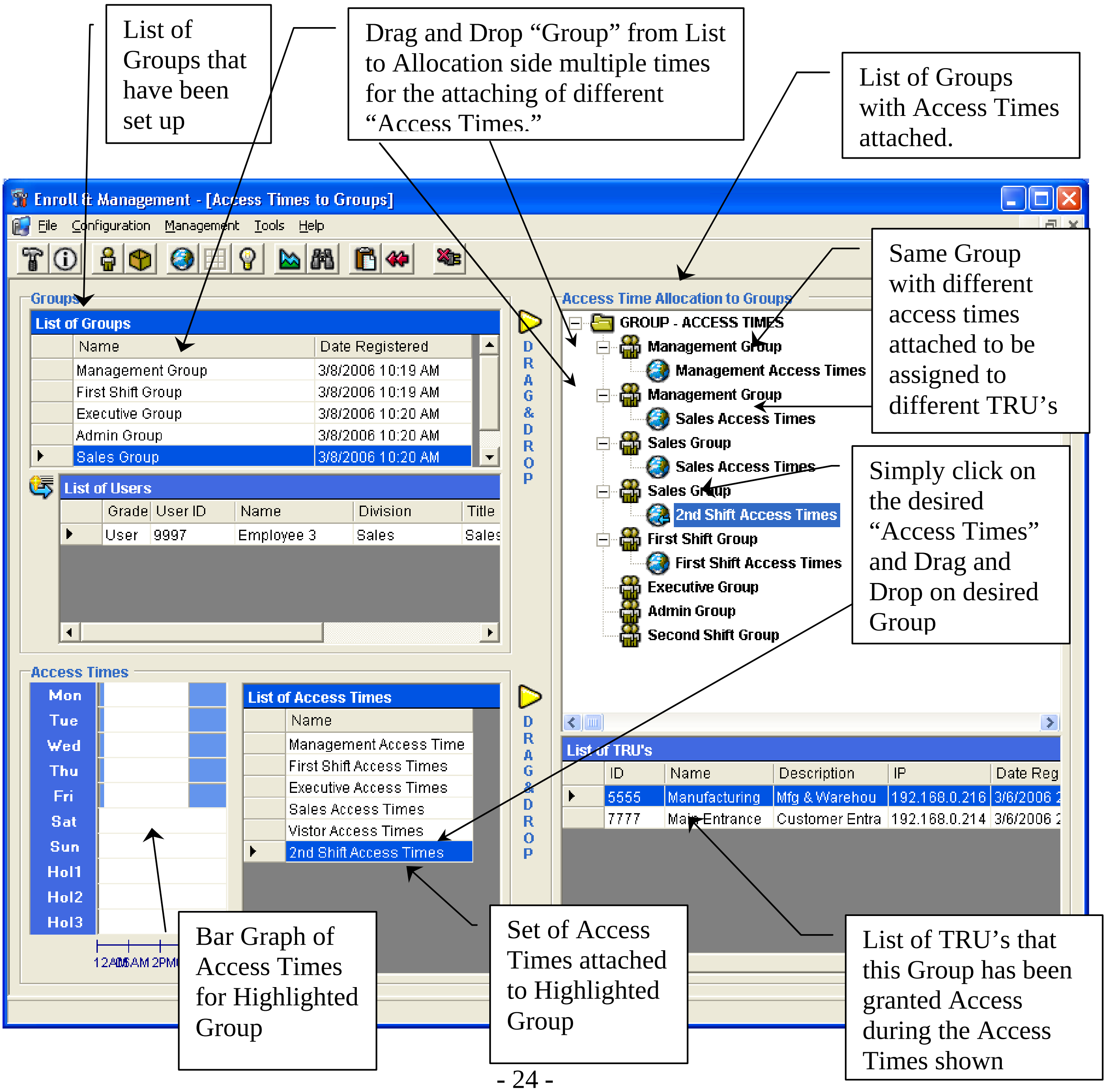
1.11.3 Notice that this screen gives a great deal of information about Groups and Access Times. The group “Sales Group” in the top left section “List of Groups,” is highlighted. In the section “List of Users”, it displays the users assigned to this group.

1.11.4 In the top right section, “Access Time Allocation to Groups,” it shows “Sales Group” with the attached “Sales Access Times.” It also shows “Sales Group” with the attached “2nd Shift Access Times.” The group in this example “Sales Group” must be dragged from the left, “List of Groups”, and dropped on the right, “Access Time Allocation to Groups” for it to appear more than once. As discussed above this allows the same group to be assigned different Access Times to different TRU’s (doors/areas).

1.11.5 In the bottom left is the “Access Times” section that shows the Access Times this group has been assigned in Bar Graph form.

1.11.6 The bottom middle section, “List of Access Times,” highlights the set of Access Times that have been assigned to this group.

1.11.7 The bottom right section, “List of TRU’s,” shows the TRU’s, or doors, that this group has been granted access.



List of Groups that have been set up

Drag and Drop “Group” from List to Allocation side multiple times for the attaching of different “Access Times.”

List of Groups with Access Times attached.

Same Group with different access times attached to be assigned to different TRU’s

Simply click on the desired “Access Times” and Drag and Drop on desired Group

Bar Graph of Access Times for Highlighted Group

Set of Access Times attached to Highlighted Group

List of TRU’s that this Group has been granted Access during the Access Times shown

Enroll It Management - [Access Times to Groups]

List of Groups

Name	Date Registered
Management Group	3/8/2006 10:19 AM
First Shift Group	3/8/2006 10:19 AM
Executive Group	3/8/2006 10:20 AM
Admin Group	3/8/2006 10:20 AM
Sales Group	3/8/2006 10:20 AM

List of Users

Grade	User ID	Name	Division	Title
User	9997	Employee 3	Sales	Sales

List of Access Times

Name
Management Access Time
First Shift Access Times
Executive Access Times
Sales Access Times
Vistor Access Times
2nd Shift Access Times

Access Time Allocation to Groups

- GROUP - ACCESS TIMES
  - Management Group
    - Management Access Times
  - Management Group
    - Sales Access Times
  - Sales Group
    - Sales Access Times
  - Sales Group
    - 2nd Shift Access Times
  - First Shift Group
    - First Shift Access Times
  - Executive Group
  - Admin Group
  - Second Shift Group

List of TRU's

ID	Name	Description	IP	Date Reg
5555	Manufacturing	Mfg & Warehou	192.168.0.216	3/6/2006
7777	Main Entrance	Customer Entra	192.168.0.214	3/6/2006

1.12 [TRU : Group – Access Time] Setup

Click on the Menu Selection "Management" and select "[TRU: Group: Access time] Setup" from the Drop down Menu. This window is used to assign Groups, with attached Access Times, to Approved TRU's. It is also a visual check to determine Access Privileges Granted to any User.

1.12.1 The top left section, "List of Groups and Access Times," shows all Groups with Access Times assigned those Groups.

1.12.2 The top right section, "Group & Access Time allocation to TRU's," shows all approved TRU's.

1.12.3 Simply click on the desired Group with Access Times attached, in the top left section, and Drag and Drop on the desired TRU, in the top right section, to grant this group the assigned Assess Times to the TRU. This is the final step to grant a User privileges.

1.12.4 In this example "Management Group" is highlighted. The left middle section "List of Users" shows all Users in this Group.

1.12.5 The bottom left section "Access Time Details," shows in Bar Graph form; the Access Times assigned this group.

1.12.6 If you click on a TRU in the top right section, the bottom right section, "Information of TRU," will display information about this TRU.

2.0 Checks to confirm Set-up and Access Privileges for a User

2.1 Confirm TRU.

In the section on the upper right of this window, "Group & Access Time Allocation to TRU's," click on the plus sign beside "TRU." This will display all approved TRU's.

2.2 Confirm Access Times assigned to Group.

On the upper left side of this window is the section "List of Groups & Access Times." This is a full listing of the Groups that have had Access Times attached. Notice that if you click on and highlight a listing here, the "List of Users" section below it lists assigned Users, and the "Access Time Details" shows Access Times granted with a bar graph at the bottom.

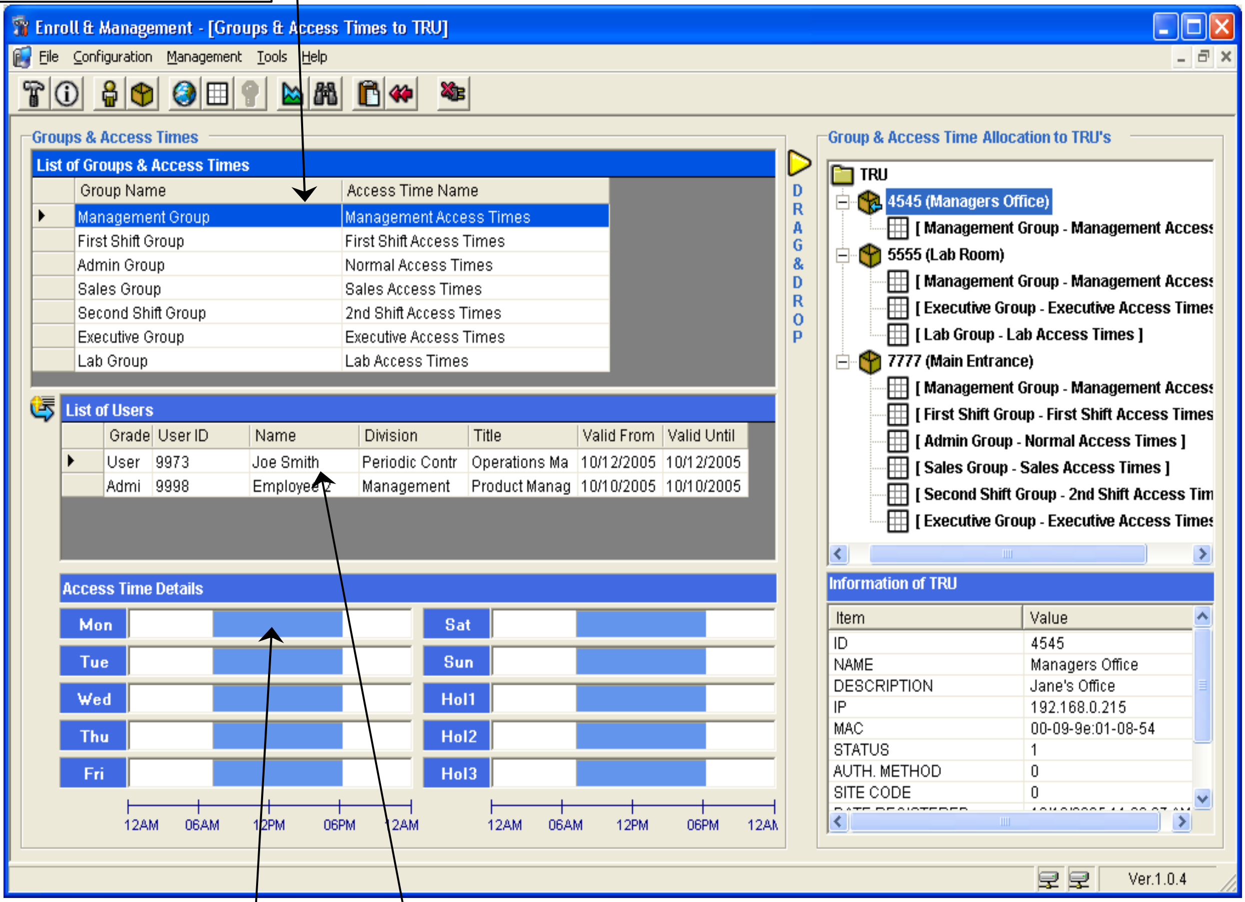
2.3 Confirm Group and Access Times assigned to TRU.

Click on the plus sign next to the TRU that you are checking in the upper right section "Group& Access Time Allocation to TRU's." All assignments in the left upper side "List of Groups & Access Times" assigned to this TRU will display below the TRU.

2.3 Confirm User assigned to Group with Access Times.

Click on and highlight the desired Group/Access Times in the upper left section, “List of Groups and Access Times.” All users assigned this Group will display in the middle left of this window in the section, “List of Users.” You may also note that the Access times are shown in Bar Graph form in lower left section “Access Time Details.”

List of Groups that have Access Times attached



List of Groups & Access Times

Group Name	Access Time Name
Management Group	Management Access Times
First Shift Group	First Shift Access Times
Admin Group	Normal Access Times
Sales Group	Sales Access Times
Second Shift Group	2nd Shift Access Times
Executive Group	Executive Access Times
Lab Group	Lab Access Times

List of Users

Grade	User ID	Name	Division	Title	Valid From	Valid Until
User	9973	Joe Smith	Periodic Contr	Operations Ma	10/12/2005	10/12/2005
Admi	9998	Employee 2	Management	Product Manag	10/10/2005	10/10/2005

TRU
- 4545 (Managers Office)
  - [Management Group - Management Access
- 5555 (Lab Room)
  - [Management Group - Management Access
  - [Executive Group - Executive Access Times
  - [Lab Group - Lab Access Times]
- 7777 (Main Entrance)
  - [Management Group - Management Access
  - [First Shift Group - First Shift Access Times
  - [Admin Group - Normal Access Times]
  - [Sales Group - Sales Access Times]
  - [Second Shift Group - 2nd Shift Access Tim
  - [Executive Group - Executive Access Times

Information of TRU

Item	Value
ID	4545
NAME	Managers Office
DESCRIPTION	Jane's Office
IP	192.168.0.215
MAC	00-09-9e:01-08-54
STATUS	1
AUTH. METHOD	0
SITE CODE	0

Bar Graph of Access Times for the Group highlighted above

List of Users attached to Highlighted Group

3.0 Menu Selection “Tools”

3.1 Monitoring

Click on Menu Selection “Tools.” Select “Monitoring” from the Drop Down Menu. There are two tabs at the top of this window.

3.1.1 Logs tab

Click on the “Logs” tab. The window shown below will appear.

3.1.1.1 This is a real-time capture of transactions as they happen. When someone attempts access by a TRU while this window is displayed, the information shown below appears in the “List of Logs” section.

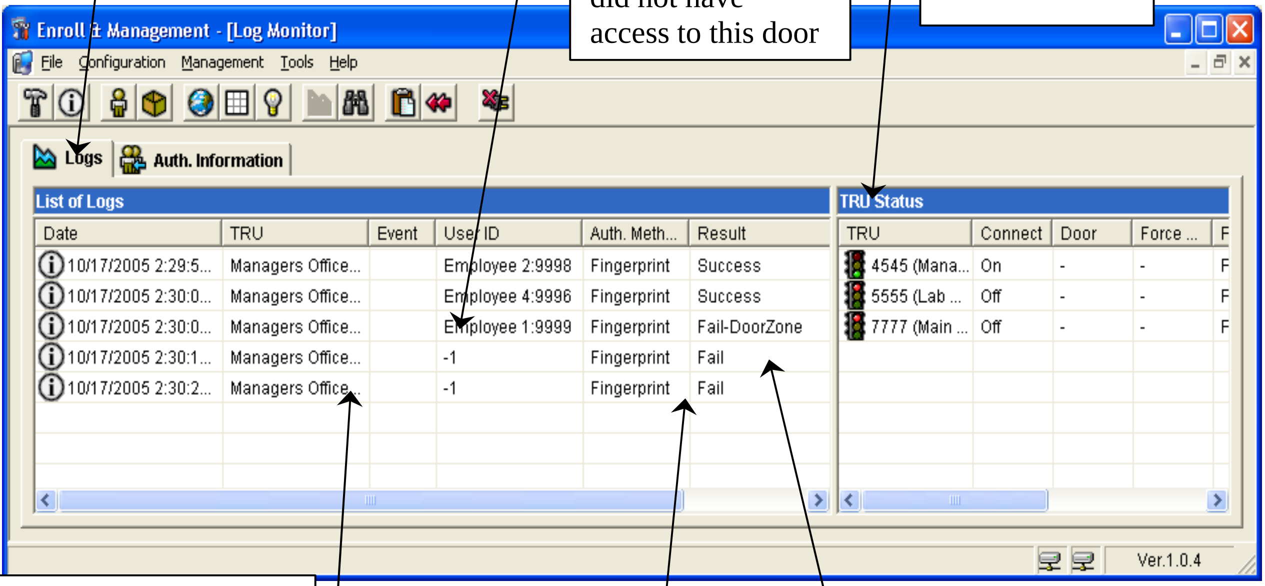
3.1.1.2 Note the results column in the example below. It shows when successful access is granted. It also shows when access fails, and the reason, such as “Fail-DoorZone.”

3.1.1.3 The section on the right, “TRU Status,” lists all approved TRU’s and whether “On” or “Off” etc.

Click on the Logs tab to display this window

Notice Employee 1 was recognized but did not have access to this door

List of TRU’s and Status



List of Logs

Date	TRU	Event	User ID	Auth. Meth...	Result
10/17/2005 2:29:5...	Managers Office...		Employee 2:9998	Fingerprint	Success
10/17/2005 2:30:0...	Managers Office...		Employee 4:9996	Fingerprint	Success
10/17/2005 2:30:0...	Managers Office...		Employee 1:9999	Fingerprint	Fail-DoorZone
10/17/2005 2:30:1...	Managers Office...		-1	Fingerprint	Fail
10/17/2005 2:30:2...	Managers Office...		-1	Fingerprint	Fail

TRU Status

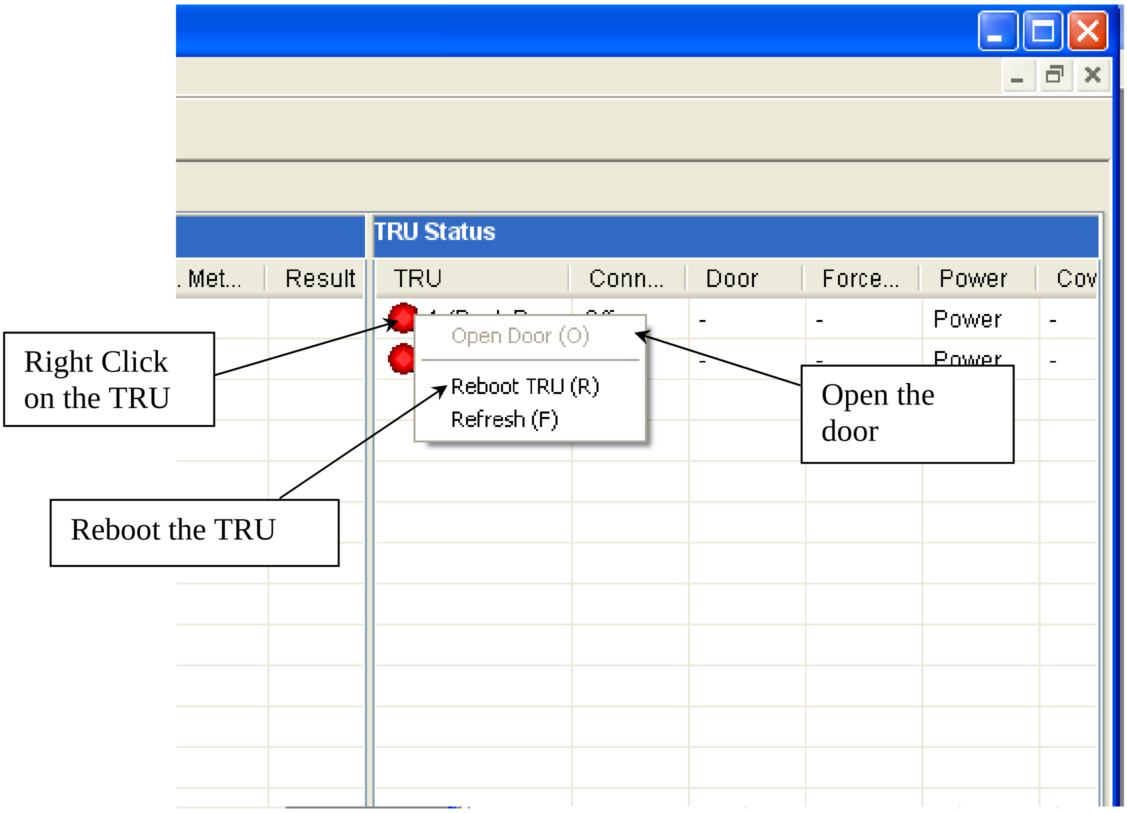
TRU	Connect	Door	Force ...	F
4545 (Mana...	On	-	-	F
5555 (Lab ...	Off	-	-	F
7777 (Main ...	Off	-	-	F

Each attempted access while this window is displayed will generate an information line in the List of Logs

If the fingerprint is not identified “Fail” is the result.

Results column will show result and also reason for failure if not successful

3.1.1.4 This same screen can also be used to control the TRU and door by right clicking the TRU as shown below.



Right Click on the TRU

Open the door

Reboot the TRU

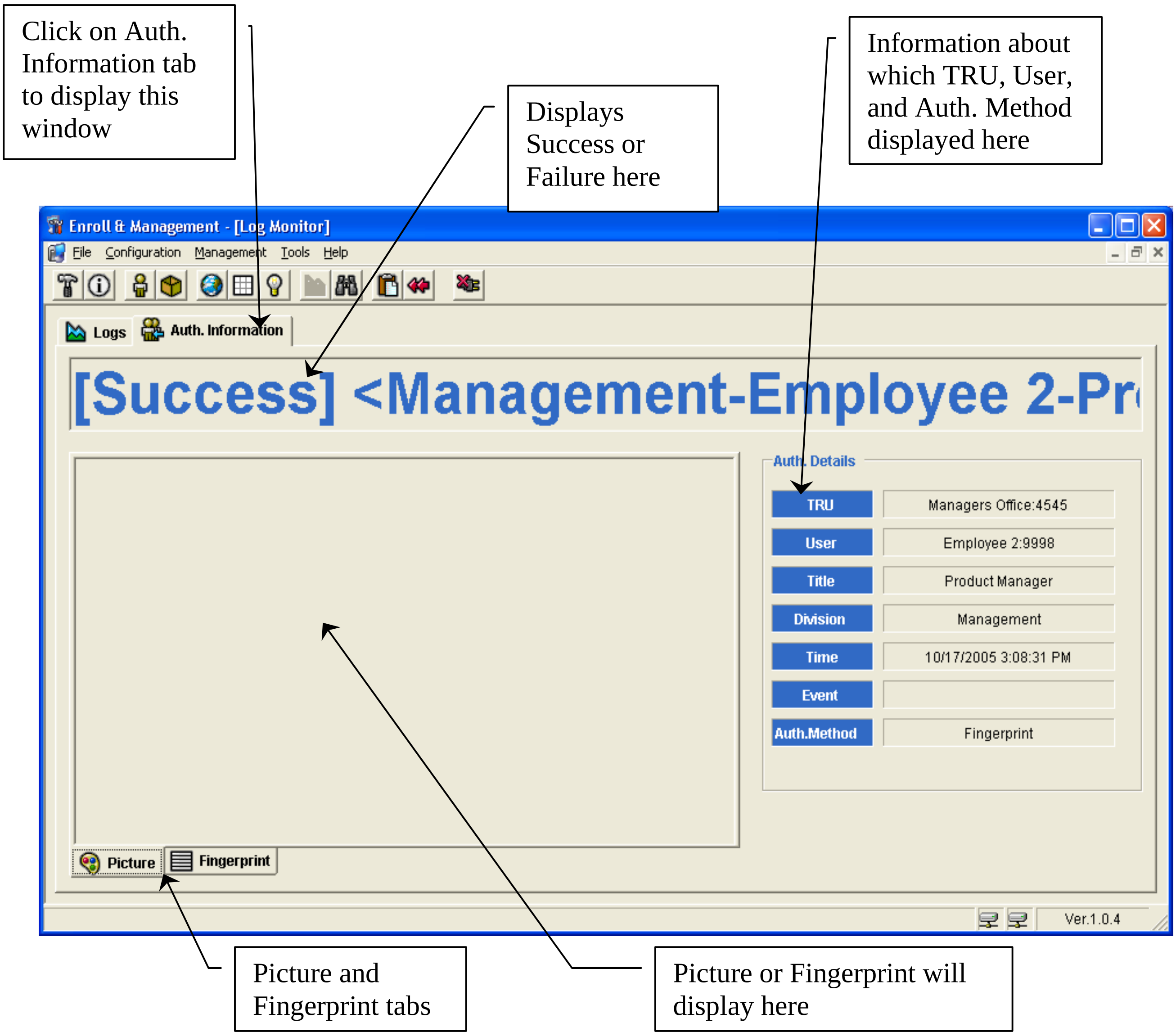
3.1.2 Auth. Information tab

Click on the “Auth. Information” tab. The window shown below will appear.

3.1.2.1 This window gives Success or Failure information in real-time.

3.1.2.2 If a picture is enrolled with a User it will display here if the “Picture” tab at the bottom is clicked.

3.1.2.3 The fingerprint image will display if the “Fingerprint” tab at the bottom is clicked.



Click on Auth. Information tab to display this window

Displays Success or Failure here

Information about which TRU, User, and Auth. Method displayed here

[Success] <Management-Employee 2-Pr

TRU	Managers Office:4545
User	Employee 2:9998
Title	Product Manager
Division	Management
Time	10/17/2005 3:08:31 PM
Event	
Auth.Method	Fingerprint

Picture and Fingerprint tabs

Picture or Fingerprint will display here

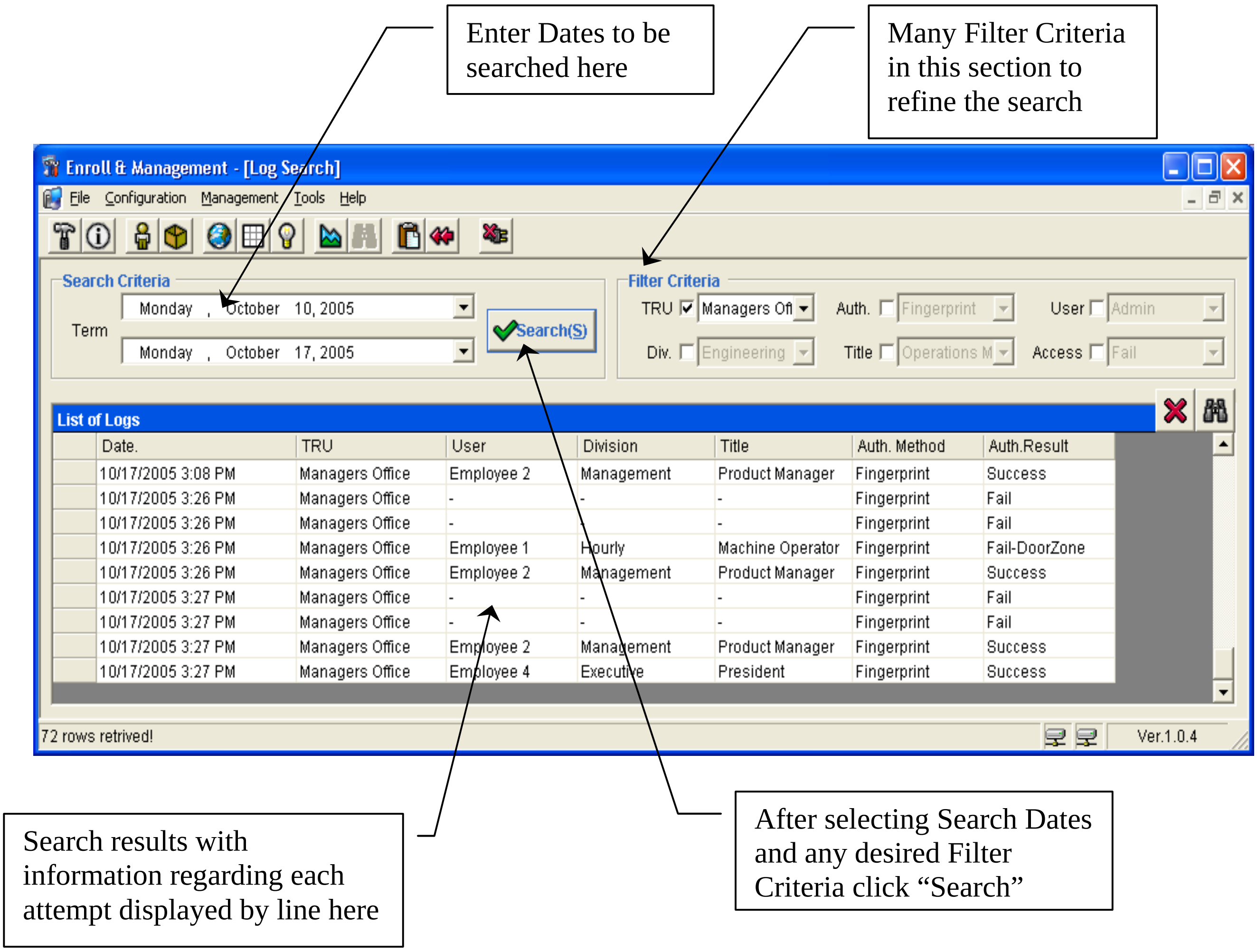
3.2 Logs

Click on Menu Selection "Tools" and select "Logs" from the Drop Down Menu. The window shown below will appear.

3.2.1 This is a specific search window with many search options. First, you must pick the Dates from the drop down menu that are to be searched. This is the only required entry before clicking "Search."

3.2.2 There are many "Filter Criteria" to narrow the search. In the example below only the TRU was checked as a Filter Criteria. Click "Search." All the attempts for access on this TRU, whether successful or not, will display for this period of time.

3.2.3 As shown, there are many Filter Criteria. Even a particular User can be searched.



Enter Dates to be searched here

Many Filter Criteria in this section to refine the search

Enroll & Management - [Log Search]
File Configuration Management Tools Help
Search Criteria
Filter Criteria
Search(S)
List of Logs

Term: Monday , October 10, 2005 — Monday , October 17, 2005

TRU ☑ Managers Off Auth. □ Fingerprint User □ Admin

Div. □ Engineering Title □ Operations M Access □ Fail

Date.	TRU	User	Division	Title	Auth. Method	Auth.Result
10/17/2005 3:08 PM	Managers Office	Employee 2	Management	Product Manager	Fingerprint	Success
10/17/2005 3:26 PM	Managers Office	-	-	-	Fingerprint	Fail
10/17/2005 3:26 PM	Managers Office	-	-	-	Fingerprint	Fail
10/17/2005 3:26 PM	Managers Office	Employee 1	Hourly	Machine Operator	Fingerprint	Fail-DoorZone
10/17/2005 3:26 PM	Managers Office	Employee 2	Management	Product Manager	Fingerprint	Success
10/17/2005 3:27 PM	Managers Office	-	-	-	Fingerprint	Fail
10/17/2005 3:27 PM	Managers Office	-	-	-	Fingerprint	Fail
10/17/2005 3:27 PM	Managers Office	Employee 2	Management	Product Manager	Fingerprint	Success
10/17/2005 3:27 PM	Managers Office	Employee 4	Executive	President	Fingerprint	Success

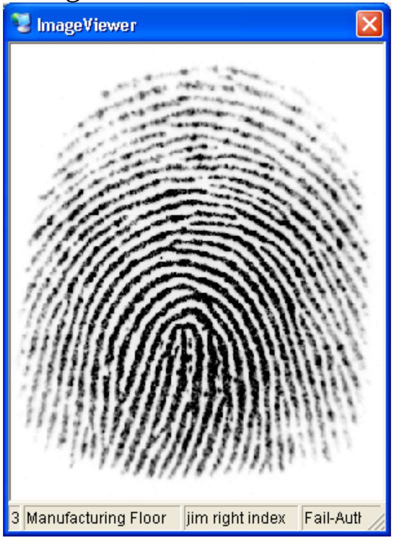
72 rows retrived!

Ver.1.0.4

Search results with information regarding each attempt displayed by line here

After selecting Search Dates and any desired Filter Criteria click “Search”

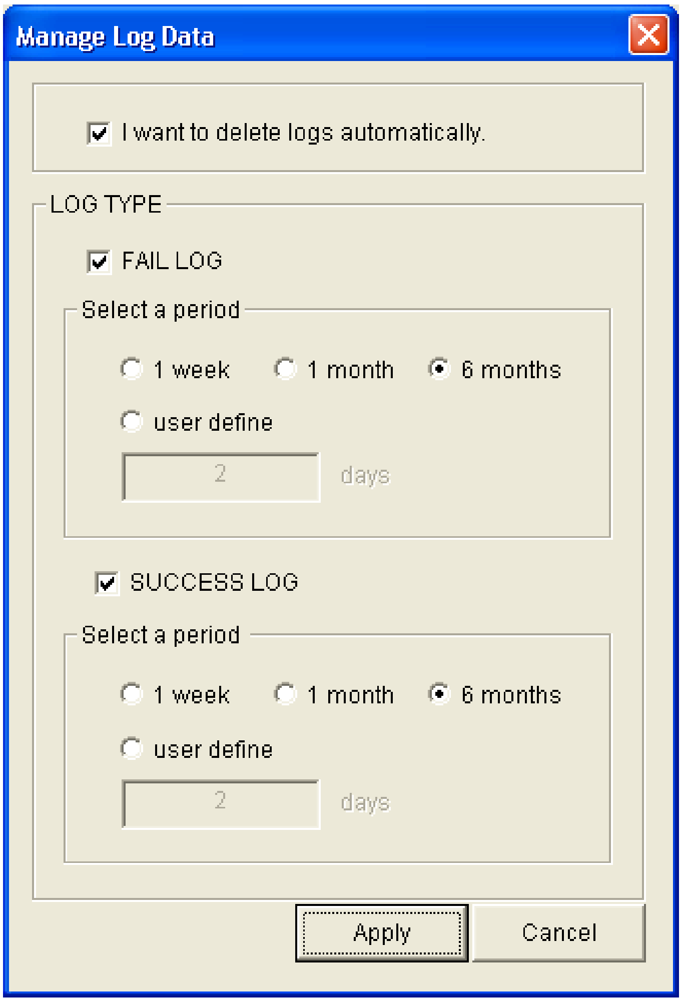
3.2.4 To view the image from this screen, simply right click on the desired search line and choose “Image View” and the window shown below will appear.



3 Manufacturing Floor | jim right index | Fail-Aut

3.2.5 To delete logs, right click on any line and choose “Delete Search Results.” Caution: This will delete **ALL** the results of the search you just performed.

3.2.6 To program the length of time logs are saved, right click on the Server Manager Icon in the bottom right taskbar. Choose “Configure Log” and the window shown below will appear. Select the period of time you would like to save Fail Logs and Success Logs and click “Apply.”



Manage Log Data

☑ I want to delete logs automatically.

LOG TYPE

☑ FAIL LOG

Select a period

○ 1 week ○ 1 month ● 6 months

○ user define

2 days

☑ SUCCESS LOG

Select a period

○ 1 week ○ 1 month ● 6 months

○ user define

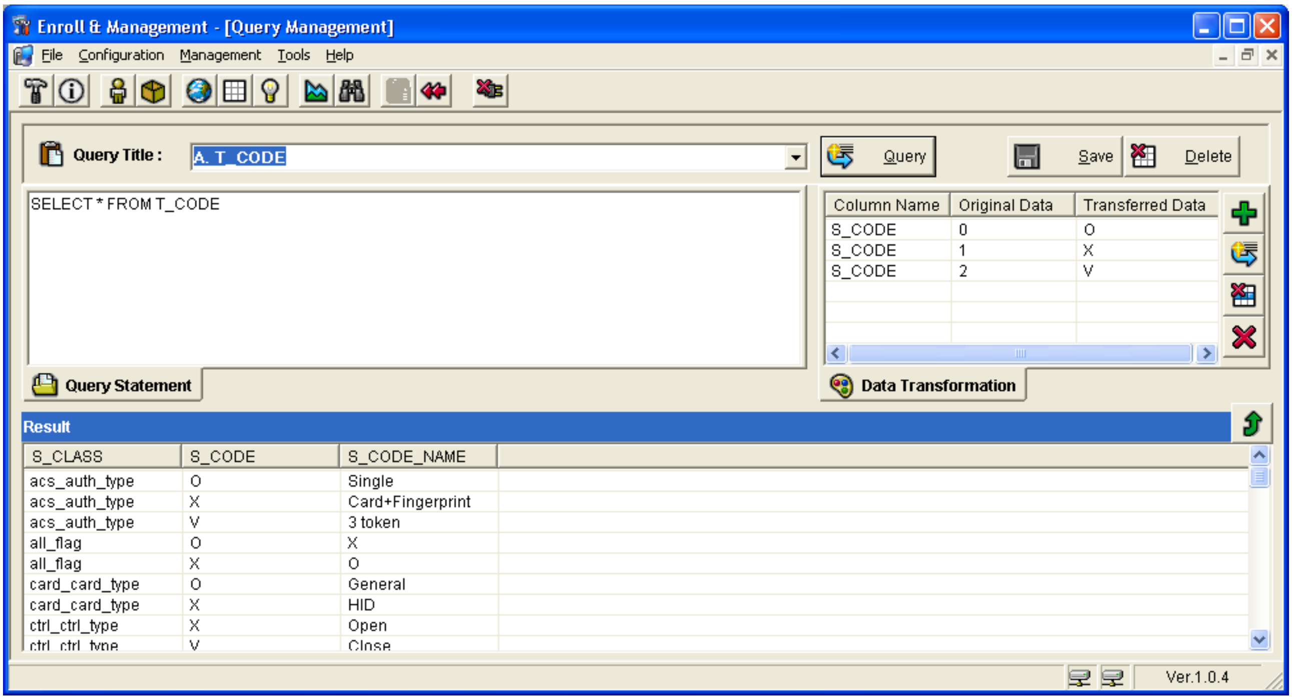
2 days

3.3 Query Manager

Click on Menu Selection “Tools.” Select “Query Manager” from the Drop Down Menu. The window shown below will appear.

3.3.1 The system allows the experienced IT person to enter Standard Query Language statements to extract data from the database.

3.3.2 Enter query statements in the upper left window and press the “Query” button to execute the statements.



Query Title : A. T_CODE

```
SELECT * FROM T_CODE
```

Column Name	Original Data	Transferred Data
S_CODE	0	O
S_CODE	1	X
S_CODE	2	V

S_CLASS	S_CODE	S_CODE_NAME
acs_auth_type	O	Single
acs_auth_type	X	Card+Fingerprint
acs_auth_type	V	3 token
all_flag	O	X
all_flag	X	O
card_card_type	O	General
card_card_type	X	HID
ctrl_ctrl_type	X	Open
ctrl_ctrl_type	V	Close

3.4 TRU Update

Click on the Menu Selection “Tools” and select “TRU Update” from the Drop Down Menu.

3.4.1 DATA Update tab

3.4.1.1 Choose the “DATA Update” tab at the top of this window. The window shown below will appear.

3.4.1.2 Information about all approved TRU’s will be displayed.

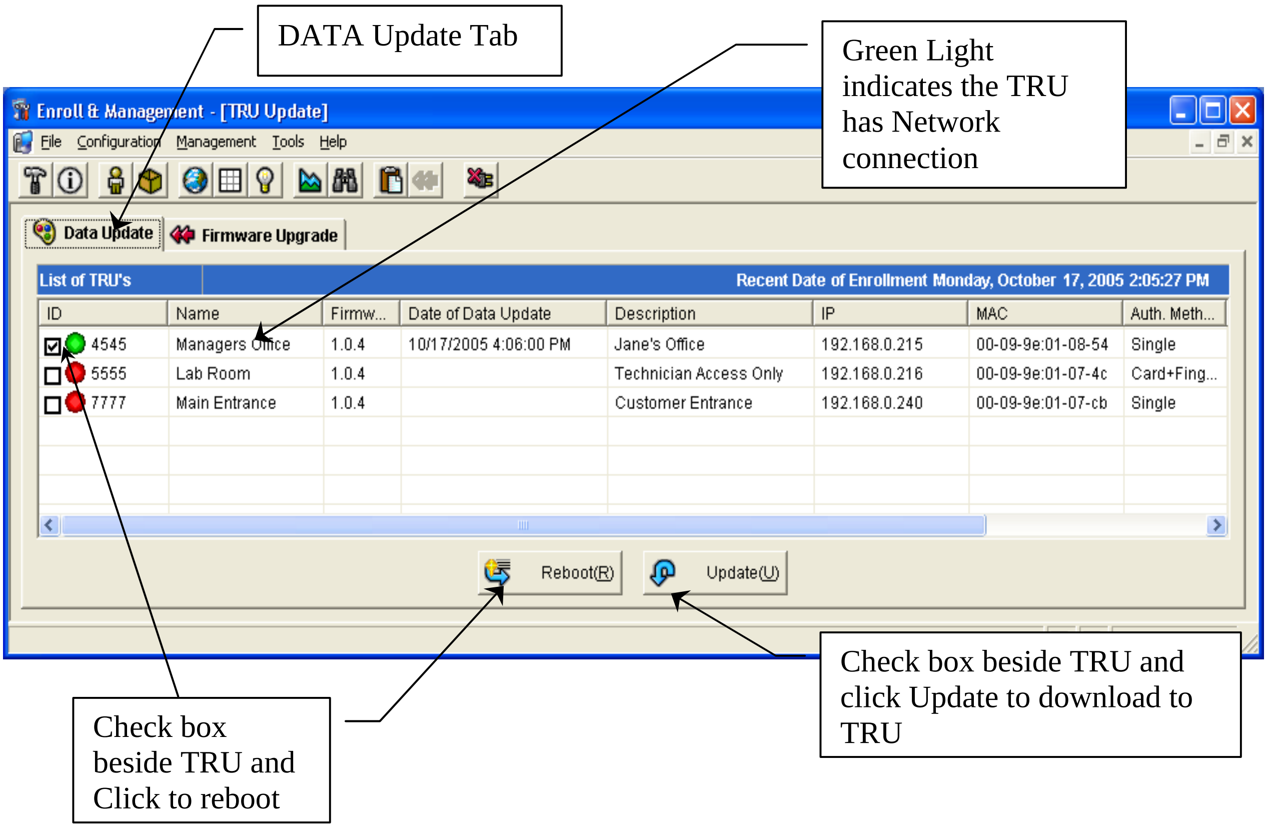
3.4.1.3 The TRU will show online with a Green light, and offline with a red light.

3.4.1.4 Other descriptive information will show including date of last TRU Update and Authentication Method required for the TRU.

3.4.1.5 A TRU can also be rebooted from this window by checking the box next to the desired TRU and clicking the “Reboot” button at the bottom of the window.

3.4.1.6 Each TRU has stand alone memory in case the Network connection is lost. Check the box next to the TRU to be updated. Click the “Update” button at the bottom of this window. The finger enrollments designated to be downloaded will download to TRU memory.

3.4.1.7 System Administrator should periodically update memory of TRU’s by this process.


Enroll & Management - [TRU Update]
File Configuration Management Tools Help
Data Update
Firmware Upgrade
Reboot(R)
Update(U)

List of TRU's — Recent Date of Enrollment Monday, October 17, 2005 2:05:27 PM

ID	Name	Firmw...	Date of Data Update	Description	IP	MAC	Auth. Meth...
☑ 🟢 4545	Managers Office	1.0.4	10/17/2005 4:06:00 PM	Jane's Office	192.168.0.215	00-09-9e:01-08-54	Single
□ 🔴 5555	Lab Room	1.0.4		Technician Access Only	192.168.0.216	00-09-9e:01-07-4c	Card+Fing...
□ 🔴 7777	Main Entrance	1.0.4		Customer Entrance	192.168.0.240	00-09-9e:01-07-cb	Single

DATA Update Tab

Green Light indicates the TRU has Network connection

Check box beside TRU and click Update to download to TRU

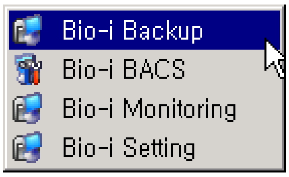
Check box beside TRU and Click to reboot

3.4.2 Firmware Upgrade tab

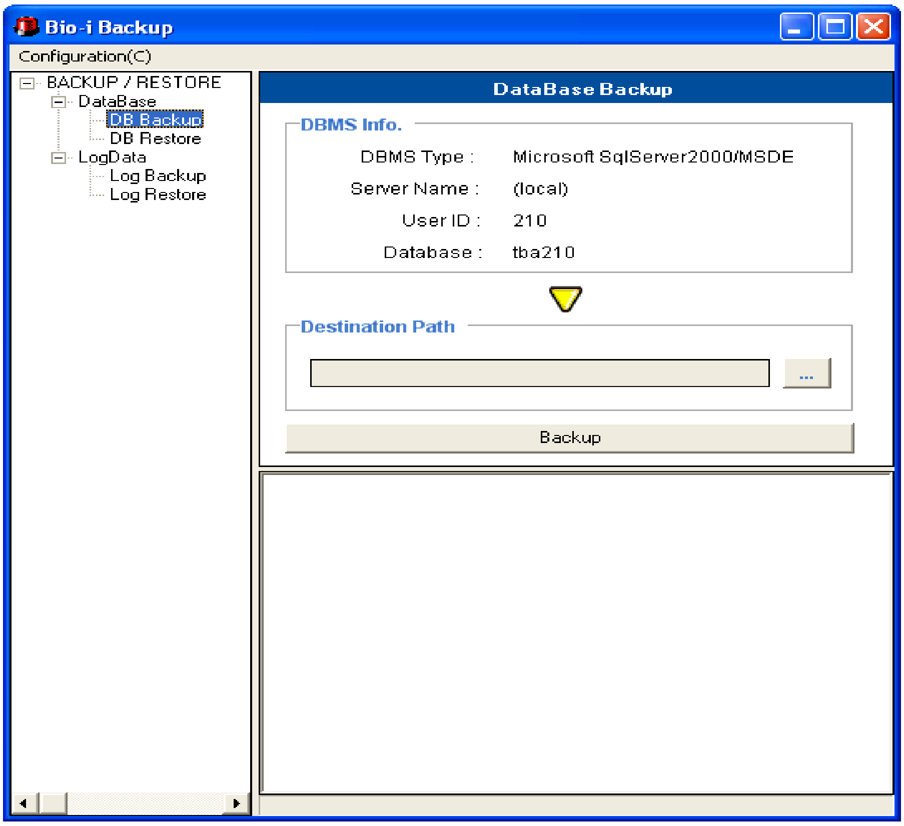
Note: **DO NOT ATTEMPT Firmware Upgrades** unless you have been trained by the Manufacturer or their Representative.

4.0 Backing-up Data

To backup user data that has been accumulating on the system go to start/ All Programs/ Integrated Biometrics LLC / Bio-I ACS / Bio-I Backup

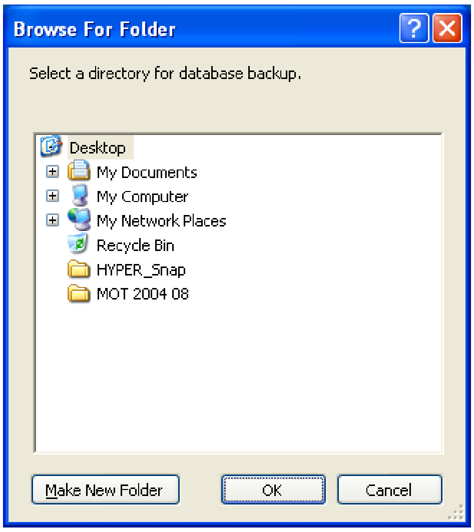


4.1 Database Back-up



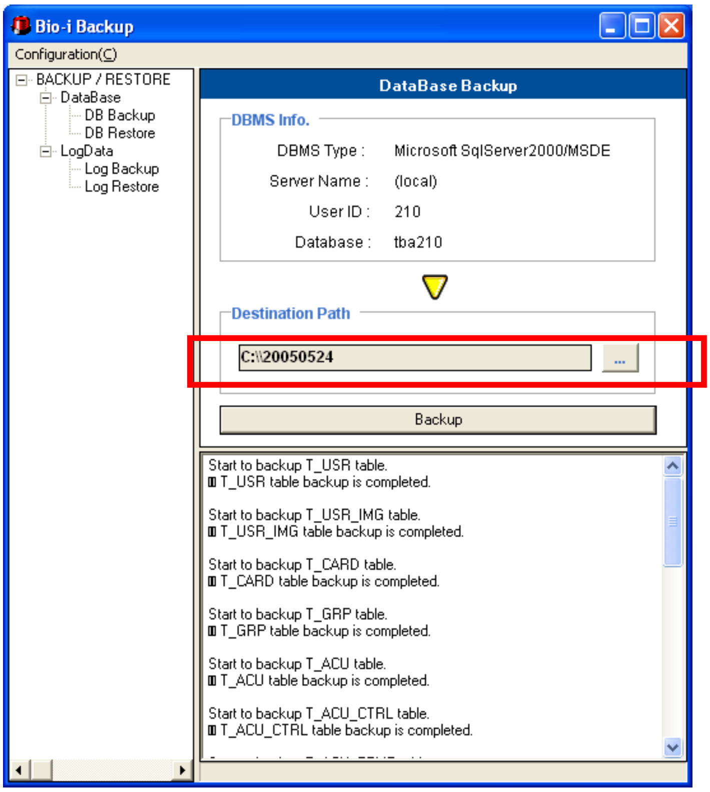
DBMS Type : Microsoft SqlServer2000/MSDE
Server Name : (local)
User ID : 210
Database : tba210

4.1.1 You will see as below picture after click the […] button



Select a directory for database backup.

4.1.2 If you select the folder from above, A new folder will be created with the date of the DB. Then, click the ‘Backup’ button. You will see the Table List and back-up procedure as shown below



DBMS Type : Microsoft SqlServer2000/MSDE

Server Name : (local)

User ID : 210

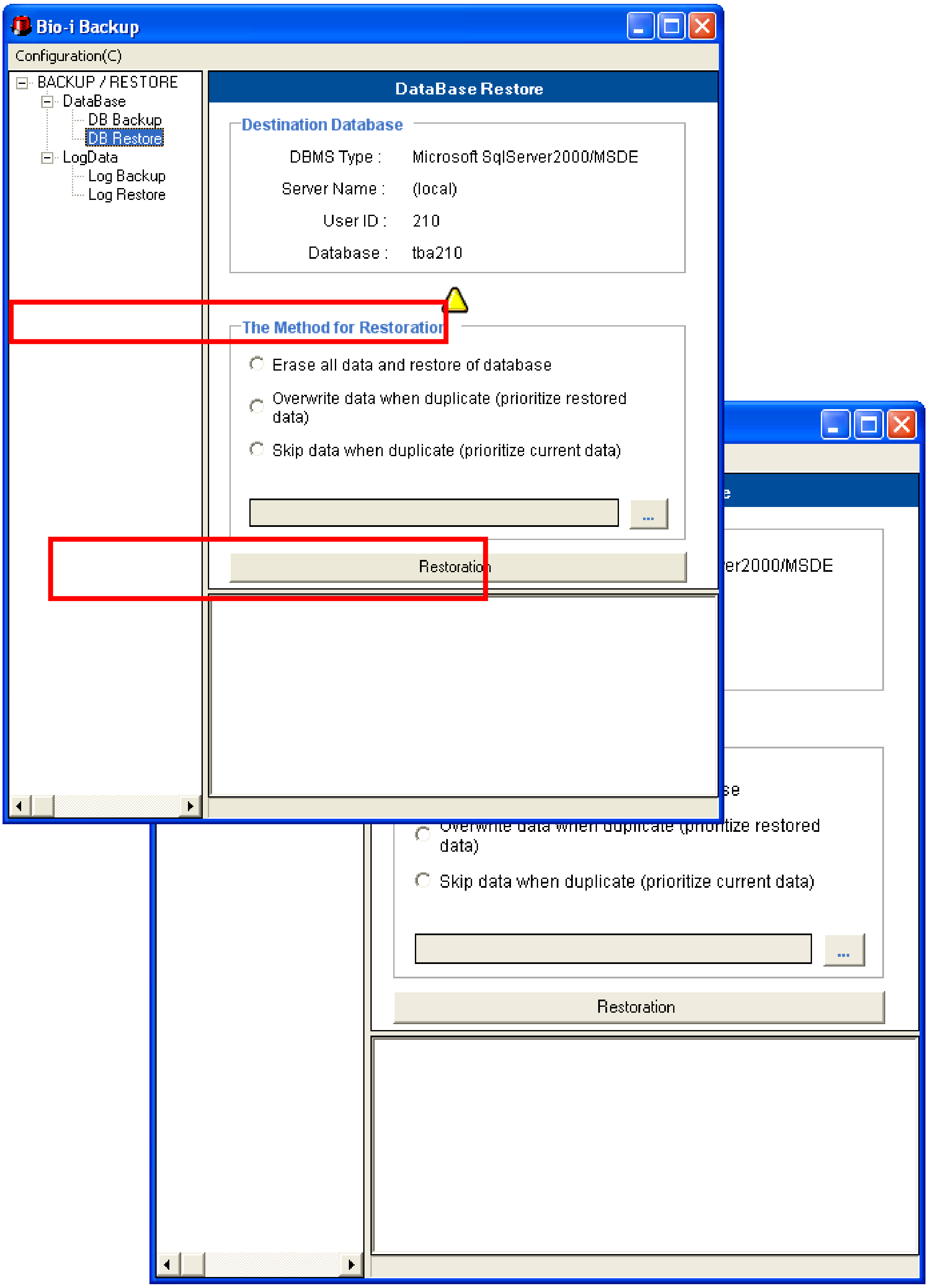
Database : tba210

C:\\20050524

```
Start to backup T_USR table.
▯ T_USR table backup is completed.

Start to backup T_USR_IMG table.
▯ T_USR_IMG table backup is completed.

Start to backup T_CARD table.
▯ T_CARD table backup is completed.

Start to backup T_GRP table.
▯ T_GRP table backup is completed.

Start to backup T_ACU table.
▯ T_ACU table backup is completed.

Start to backup T_ACU_CTRL table.
▯ T_ACU_CTRL table backup is completed.
```

4.1.3 Back-up will be done into one file for each database table. The type back-up file is : *.tbu.

4.2 Database Restore



Destination Database

DBMS Type : Microsoft SqlServer2000/MSDE

Server Name : (local)

User ID : 210

Database : tba210

The Method for Restoration

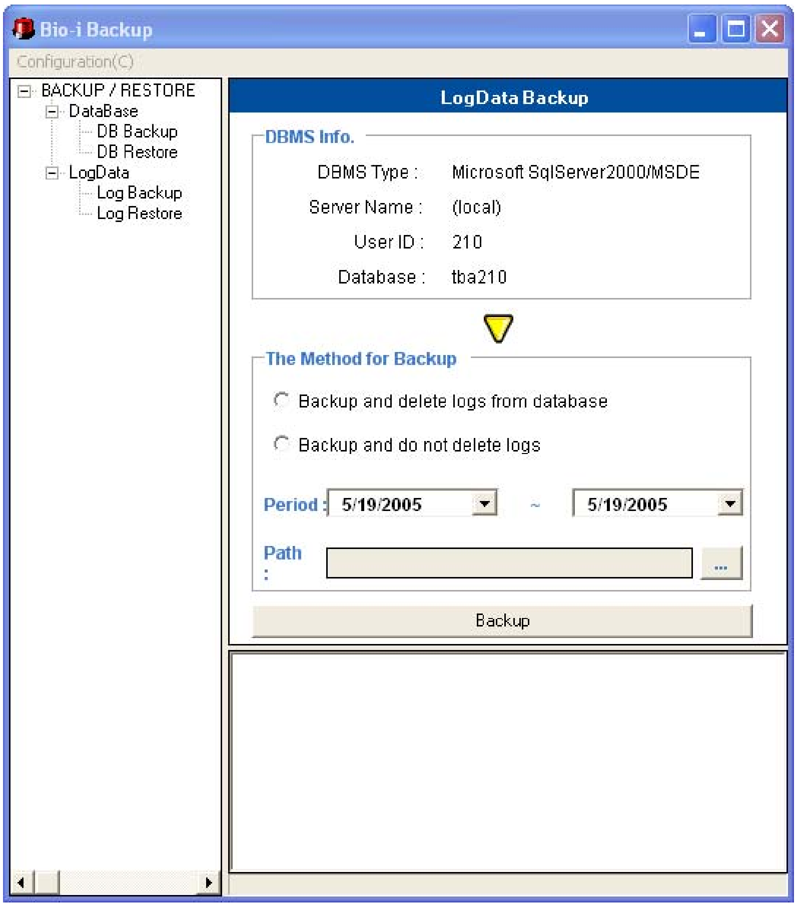
○ Erase all data and restore of database

○ Overwrite data when duplicate (prioritize restored data)

○ Skip data when duplicate (prioritize current data)

4.2.1 Select the method from the ‘Method for Restoration’ and click the Restoration button → Restoration Completed

4.3 Log data Back-up



DBMS Info.

DBMS Type : Microsoft SqlServer2000/MSDE

Server Name : (local)

User ID : 210

Database : tba210

The Method for Backup

○ Backup and delete logs from database

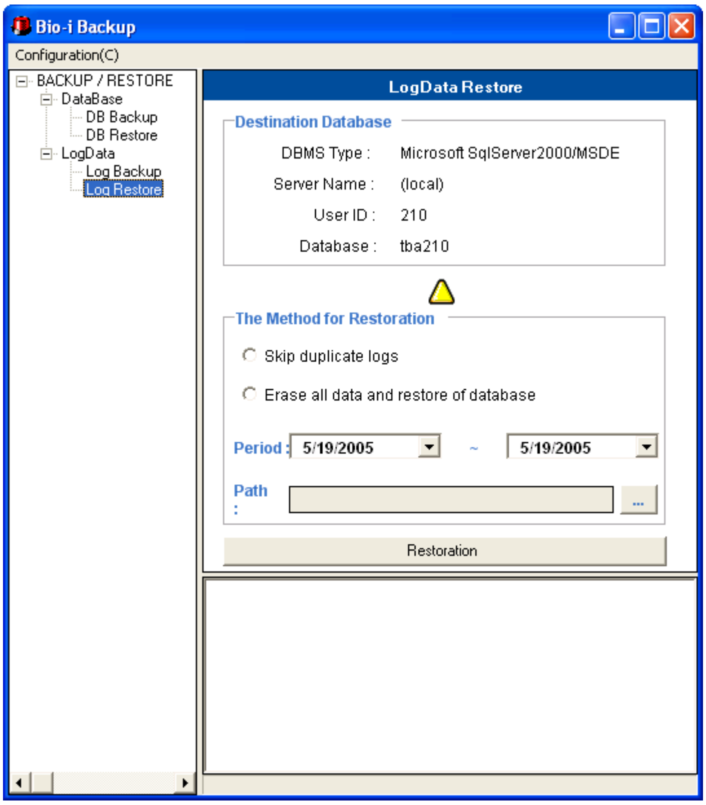
○ Backup and do not delete logs

Period : 5/19/2005 ~ 5/19/2005

Path :

4.3.1 As shown in the picture above, select the ‘Method for Backup’ and path. And then select the ‘logdata back-up’

4.4 Log Restore



Destination Database

DBMS Type : Microsoft SqlServer2000/MSDE

Server Name : (local)

User ID : 210

Database : tba210

The Method for Restoration

○ Skip duplicate logs

○ Erase all data and restore of database

Period : 5/19/2005 ~ 5/19/2005

Path :

4.4.1 Select the ‘Method for restoration’ and then select the file on […] folder. Log data restoration will be completed by clicking ’Restoration’.

5.0 **Bio-i BACS Key Word Definitions**

5.1 **Access Times** – Programmed times of Access. Note: can ONLY be given to Groups.

5.2 **Authentication Server** – Sometimes called the verification server, this is the software that does the actual matching of fingerprints.

5.3 **BACS** – Biometric Access Control System. The name for the Enroll and Management Software.

5.4 **Database** – The area on the computer disk where the systems information is organized in to tables.

5.5 **Database Server** – Sometimes call the database engine, it is the software provided by Microsoft or other database providers that handles request by programs for information from the database.

5.6 **Firmware** – Programs that resides inside the hardware.

5.7 **Group** – Set of enrolled Users that are to be granted the same Access Times. Note: A User MUST be assigned to a group to be granted Access Privileges. If a User has unique access, that User still MUST be assigned to a Group, even if it is a group of one.

5.8 **Mac Address** – Media Access Control address, a hardware address that uniquely identifies each node of a network. This address is “physically” part of the device and can not be changed.

5.9 **MSDE** – Microsoft’s Database Engine is a Database server provided by Microsoft and is free but very restricted version of their Microsoft SQL Server product.

5.10 **ODBC** – Open Database Connectivity is a standard or open application programming interface (API) for accessing a database.

5.11 **Radio Button** – A round active button, similar to a box that you check by clicking on it, except it is a circle that you click on that puts in a dot, to activate.

5.12 **Server IP Address** – A unique identifier assigned to the server computer on the TCP/IP network.

5.13 **TBA210** – For purposes of this Manual, TBA210 means the same thing as TRU 650.

5.14 **Testech** - Integrated Biometrics’ Hardware Division.

5.15 **TRU 650** – 650 DPI Terminal Reader Unit. This is the Biometric/Prox device mounted by the door.

5.16 **TRU 650 IP Address** – A unique identifier assigned to the TRU 650 computer on the TCP/IP network.

5.17 **USB Finger Sensor** – The fingerprint scanner provided with the system that connects to the computer via USB port to be used for enrolling users. (USB=Universal Serial Bus).

5.18 **User** – Individual enrolled in the system.

FCC Statement

Caution : Any changes or modifications in construction of this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference, and
2) This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, any cause harmful interference to radio communications. However,there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmfulinterference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.