BioPointe Central

for Windows

Notices

Information in this document is subject to change without notice.

NO WARRANTY OF ANY KIND IS MADE WITH REGARD TO THIS MATERIAL INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

No liability is assumed for errors contained herein or for incidental damages in connection with the furnishing, performance, use of this material.

Release: January 2005
Revision 1.8
Part Number: 01953-001

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

A. How BioPointe Central Works

BioPointe Central is used for maintaining and administering BioPointe devices. The BioPointe device is an authentication system specifically designed to provide irrefutable personal identification.

B. Features

BioPointe Central has many distinct advantages:

- Flexible software expandability
- Multiple security levels (supervisor, user or custom)
- Communication via serial, Ethernet or modem
- Verifying status of devices
- Log record reporting
- Log record exporting into ASCII text format
- Time and Date synchronization
- Device Properties configuration
- Central enrolment of the users
- Provides data synchronization between PC and the BioPointe device
- Ease of use

C. Style and Conventions

Icons

Occasionally, an icon will appear in the left margin. Each icon has a specific meaning. The paragraphs that follow identify the icons and their intended use.

NOTE: Notes alert you to information of special interest or provide clarification on the use of a particular feature. Notes supplement standard content and are not required reading.

WARNING: Warnings contain critical information. Failure to read a warning may cause unexpected results from the application.

Terminology and Type

- Fields are referenced by their proper names
- Literal entries (commands and such) appear in **bold**
- Important new terms appear in *italics*
- Optional entries appear in (brackets)

Chapter 2

GETTING STARTED

A. System Requirements

You will need the following:

- Pentium PC or compatible
- 32 MB RAM
- 50 MB (minimum) available hard disk space
- CDROM drive
- Microsoft Windows 95/98 ,Windows 2000 or Windows XP
- RS232 or RS485/RS422 (additional adaptor board to convert the RS232 signal to the RS422/RS485 signal is required)
  - or -
- 1 network card for Ethernet interface (TCP/IP)

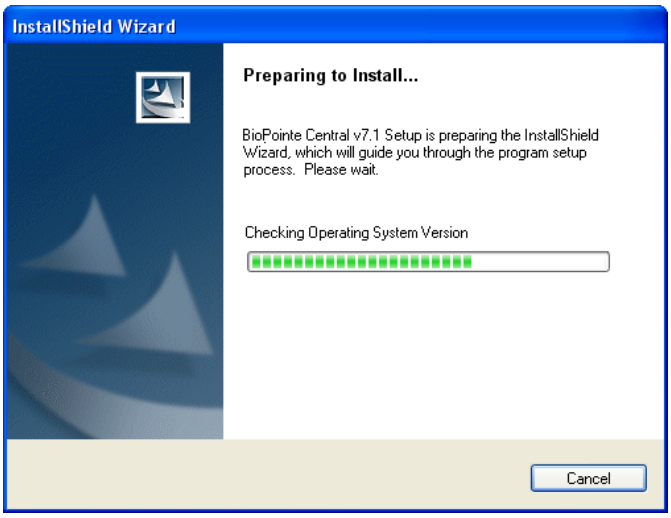
B. Installing BioPointe Central

1) Insert the Keri Systems CD into the CD drive.

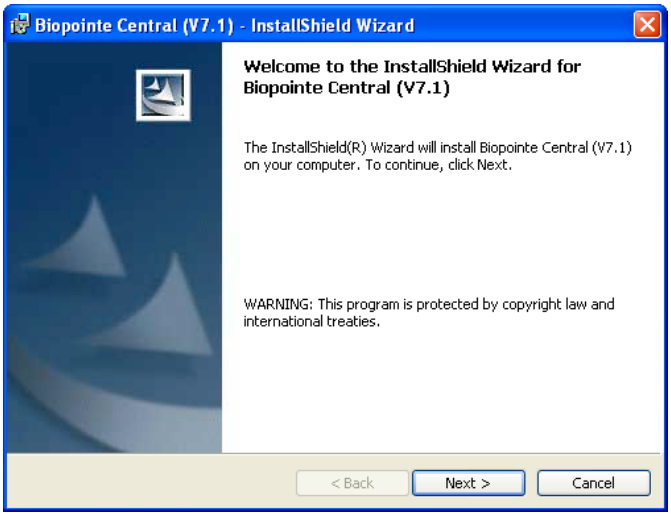
2) The autorun menu will appear.

3) Click on the BioPointe Software and Documentation link. The BioPointe installation window appears.

4) Click on the Install BioPointe Software link.



5) Wait as the InstallShield Wizard prepares to install BioPointe to your system.

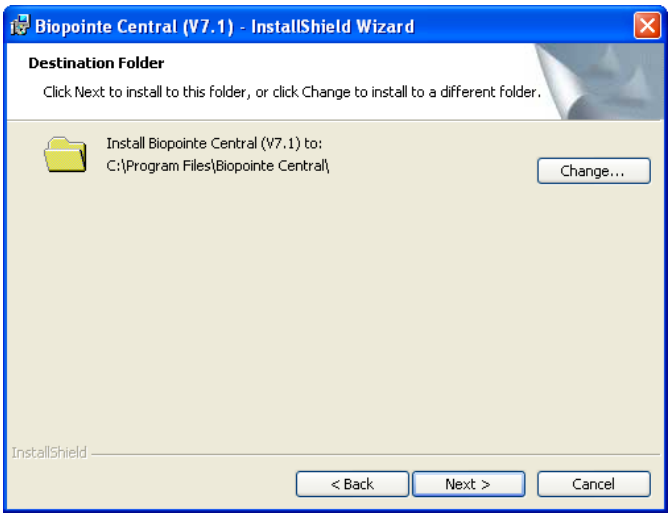


6) Once the Welcome to the InstallShield Wizard window appears, click on the 

button to proceed. The Software License Agreement appears.

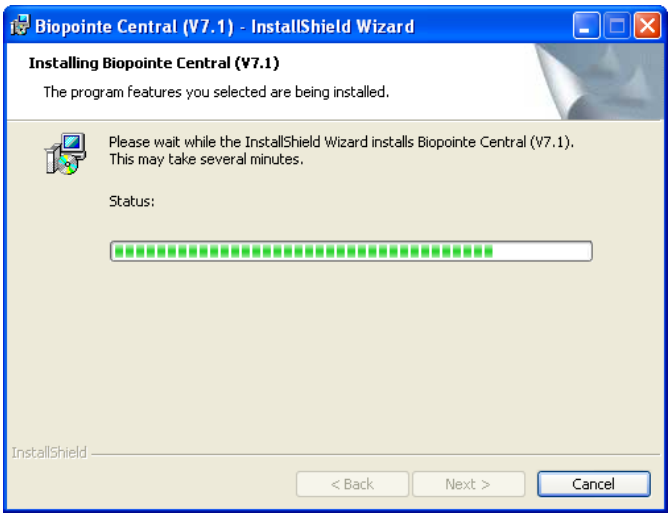
7) To not accept the license agreement and cancel the installation, click on the "I do not accept" button. The installation program will exit without installing the software.

8) To accept the license agreement and continue with the installation, click on the "I accept" button. The destination folder window appears.

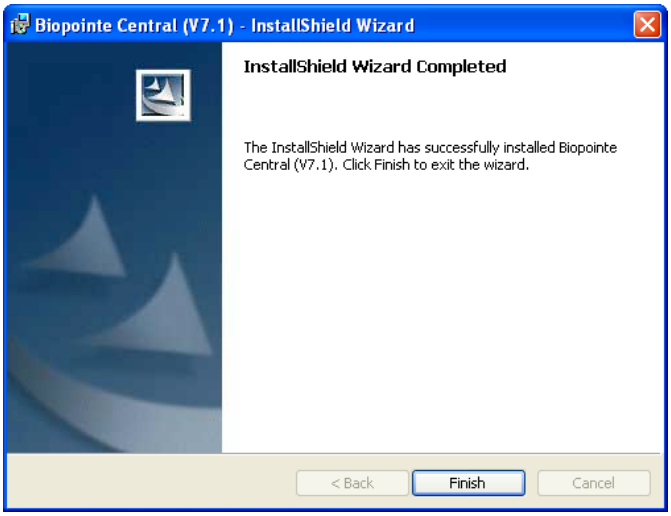


9) Verify the correct folder is selected for installation. Keri recommends using the default destination folder, but if you need to use a different folder, click the [Change...] button and navigate to the desired folder for BioPointe.

10) Click on the [Next >] button once the correct folder has been selected. A status window appears showing the progress of the installation.

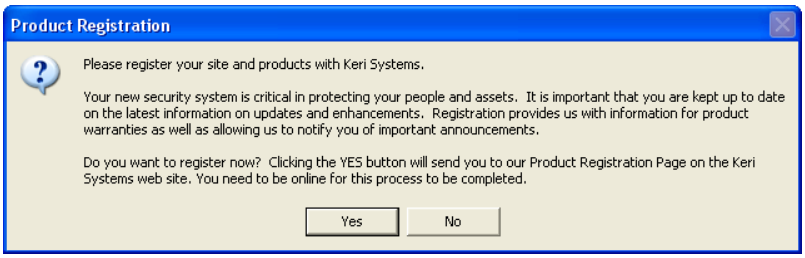


11) When installation is complete, the InstallShield Wizard Complete window appears.



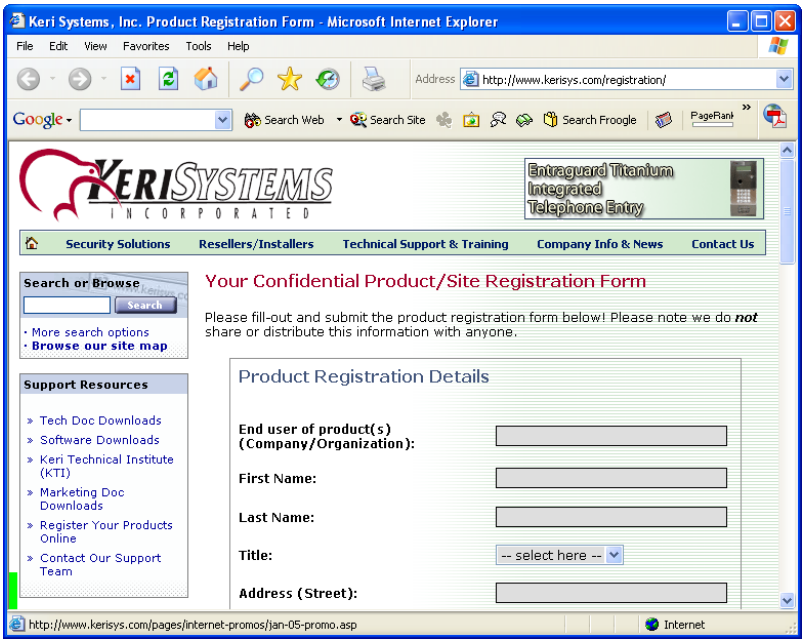
12) Click on the [Finish] button and the installation is complete and a shortcut is installed on the desktop. You are now ready to use the BioPointe Central program.

13) Finally, a Product Registration window appears.



14) Click on the [No] button to register BioPointe Central at another time. Registration may be concluded through the Keri Systems, Inc. web site at: http://www.kerisys.com/registration/index.asp.

15) Click on the [Yes] button to register BioPointe Central. Your browser program will be open and you will be automatically routed to the Keri software registration page.



16) Enter information as requested and submit it when ready.

C. Uninstalling BioPointe Central

For both Windows 95/98 and Windows 2000/XP un-installation processes, the BioPointe Central databases, which comprise the user logon information, user fingerprint database, device configuration and the log records, will be removed from the system. User has to backup this information if needed before starting the un-installation process. Following are the location where all the information is stored.

User Logon Information -- installed directory/data
Device Configuration, user Fingerprint Data and Log Records -- installed directory /database

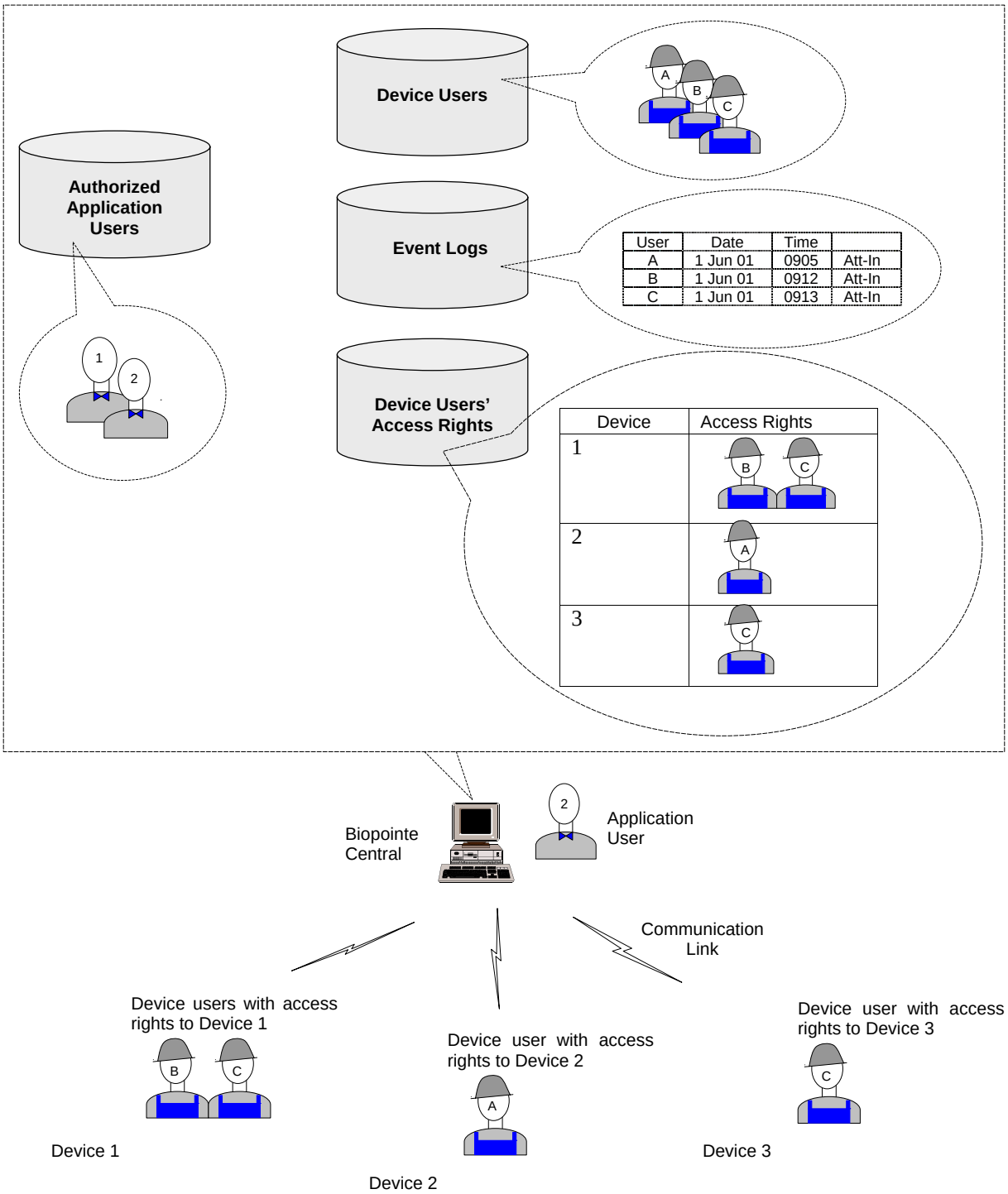
D. Database File in the Install Directory

There are two categories of database file used by the application. These two categories of files are:

(1) System Data Files – These files store the logon information. These files are located at the installed directory/data directory.
(2) BioPointe Data Files – These files store the user information (eg fingerprint template, schedule etc),device information (eg device ID, device configuration etc) and the log information (eg Error log). User should only open the FPUSER.DBF file during the user enrolment process. These files are located at the installed directory/database directory.

Chapter 3

System Overview



Encompassed within BioPointe Central are a few databases. The first stores a list of application users. These are people with authorized access to BioPointe Central. With authorized access, the application user can do a variety of tasks:

An application user can enroll new device users (stored in the Device Users database), assign access rights to them (Device Users' Access Rights database) and dispatch them to the respective devices via the communication link.

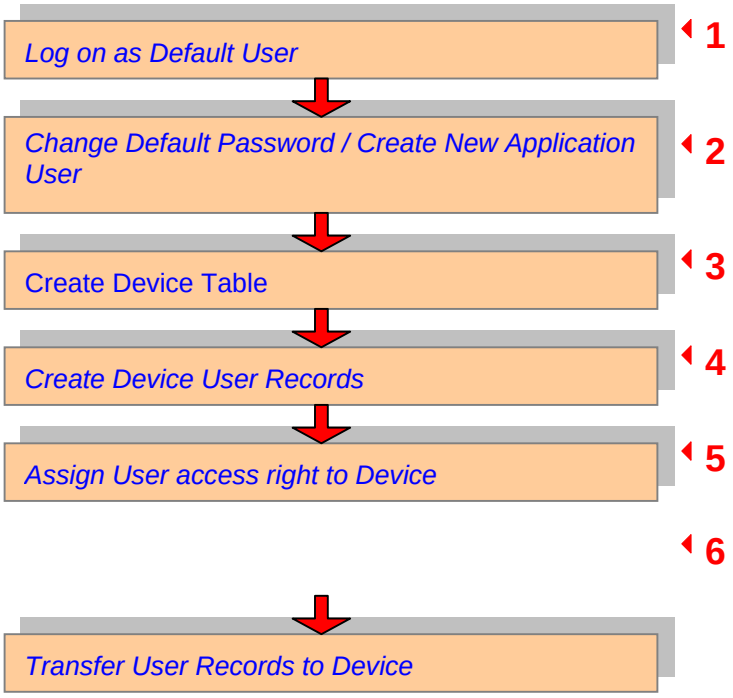
The fingerprint templates are stored locally in the devices, allowing the device users to perform their authentication or attendance logging locally at the devices.

The application user can also upload these event's logs from the individual devices and store them in an Event Logs database.

Chapter 4

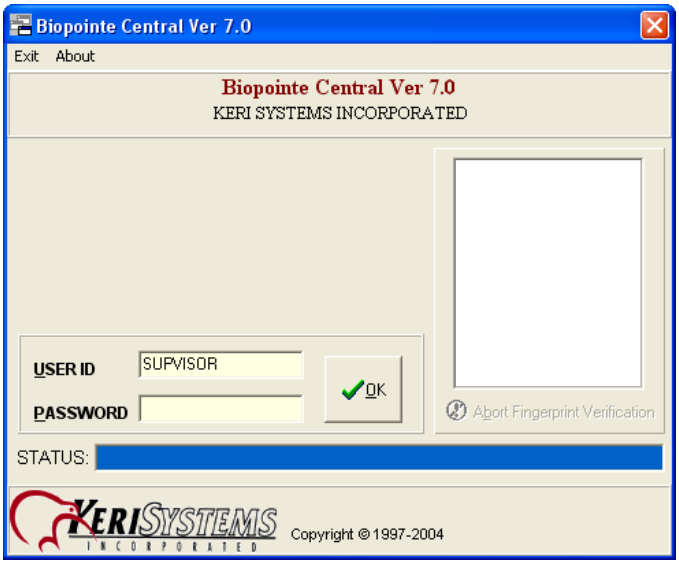
Basic operation

This chapter gives you quick and concise instructions to perform basic functions in BioPointe Central. You will be charted through this chapter according to the flow diagram below.



A. Log on as Default User

When you start BioPointe Central, you will be prompted to enter the UserID and Password. As this is the first time you are using BioPointe Central, the default UserID is "SUPVISOR" and the Password is "PASSWORD". The words are in capital letters.



To log on to BioPointe Central:

1. Enter "SUPVSIOR" in the USERID box.
2. Type "PASSWORD" in the PASSWORD box.

NOTE:
The maximum characters allowed for each entry is 8.

Difference between a Supervisor and a User is that Supervisor has the right to add additional Users or Supervisors. In addition, a Supervisor has the rights to perform all tasks provided by the application.

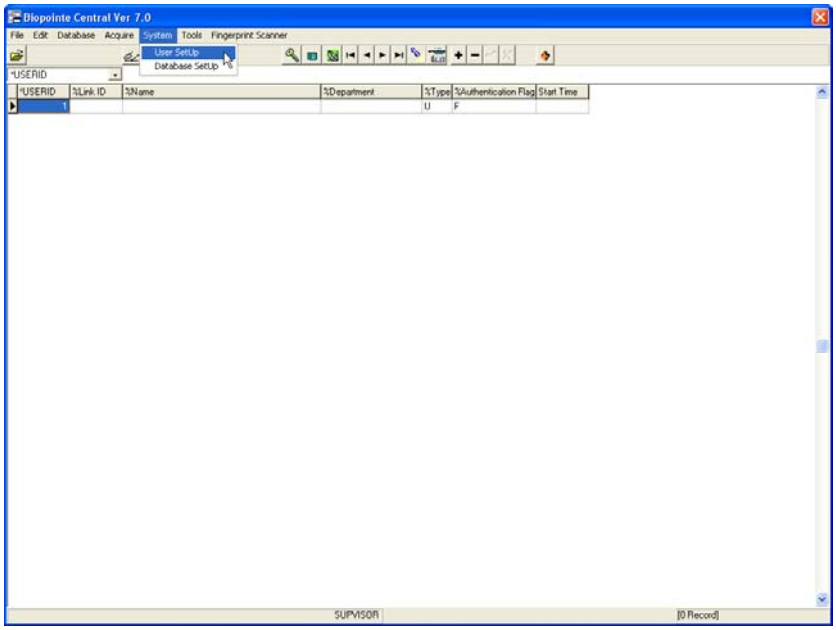
A First Time User is advised to change the password after this step.

You can also logon using your fingerprint instead of password; the white box on the right will display the captured fingerprint image. The fingerprint unit will need to be plugged into the computer prior to starting BioPointe Central.

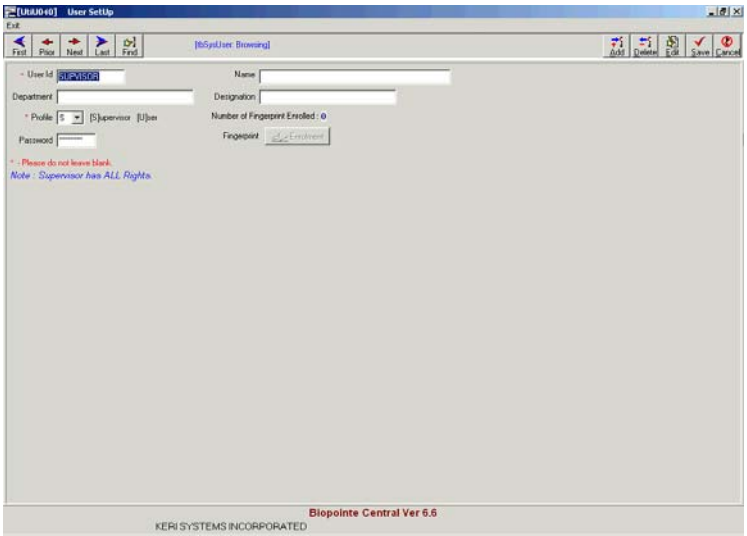
B. Change Default Password

For security reasons, you may decide to change the default password ("PASSWORD") to something else.

To Change the Default Password:



1. Click **System** from the top menu of the **User Database** screen and then select **User SetUp** by clicking on it.
2. The **User SetUp** screen pops up as shown.

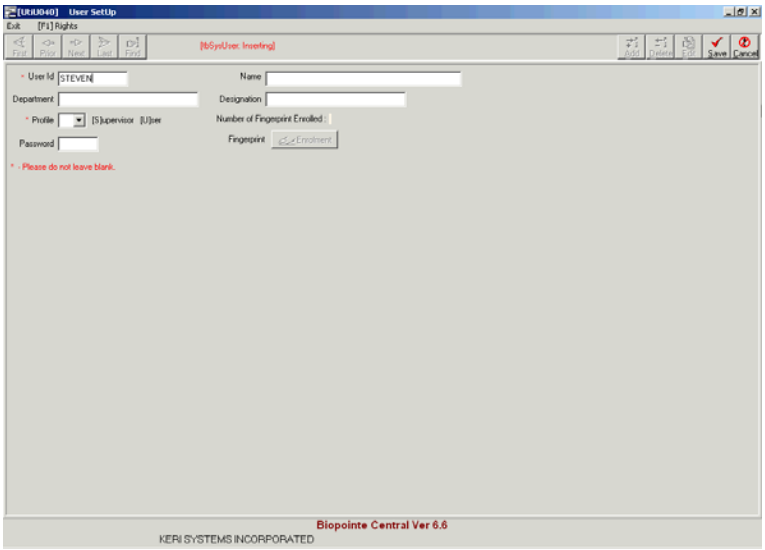


3. Click the **Edit** button to place the fields to be in the edit mode.
4. Change the password to one that you prefer

C. Create New Application's User

You can create a new application user or supervisor through **User SetUp**.

To Create New Application's User or Supervisor:



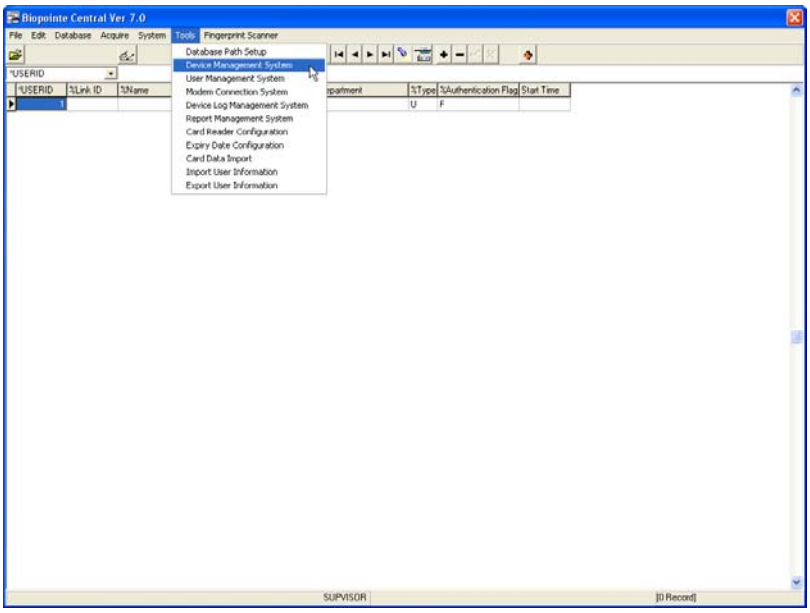
1. Click the **Add** button to place the fields to be in the insert mode.
2. Enter a preferred User Id of the new User or Supervisor in the **User Id** field.
3. Assign the person as a "Supervisor" or "User" in the **Profile** field.
4. Enter the person's preferred password in the **Password** field.

D. Create Device Table

This section shows you how to add a Device into the Device Table and perform basic configurations.

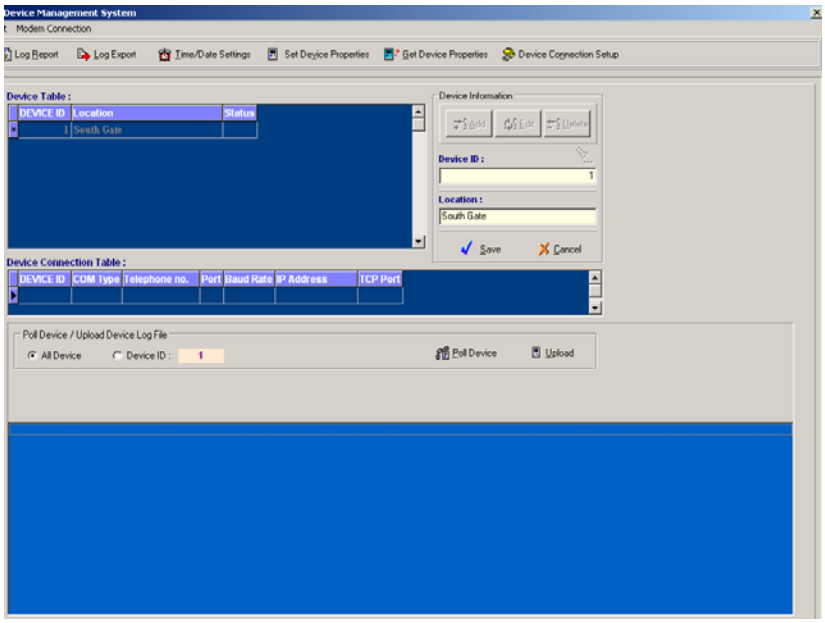
The Device Table maintains the list of devices in your BioPointe network system. When you first use BioPointe Central, no devices are listed in the Device Table. You can follow the steps below to add a new Device into the Device Table.

To add a new Device into the Device Table:



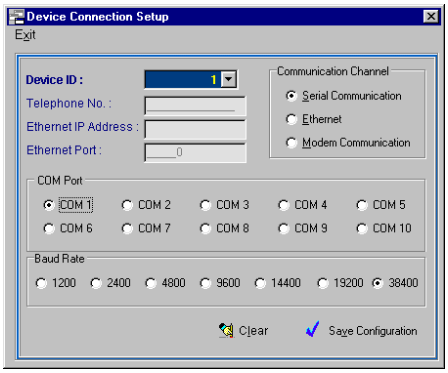
1. Click Tools from the top menu and select **Device Management System** from the drop-down menu.

2. The **Device Management System** screen pops up as shown.



3. Click the **Add** button on the **Device Information** group box.
4. Enter the Device ID in the **Device ID** field. You can optionally enter the location of your device in the **Location** field.
5. Click the **Save** button to save the device information.

6. To change the communication settings, click the **Device Connection Setup** button. The Device Connection Setup menu will pop up as shown.



7. You can change the communication settings from here. When you have completed making changes, click "**Save Configuration**" to save the settings.

After you have setup the device table, you can proceed to check the connectivity of the device by execute the polling command to the device. This will ensure that there is a physical connection between the Device and your PC.

1. In **Device Management System**, Click the **Poll Device** button.
2. A message box will pop up asking you whether you want to continue with the polling. Click **Yes**.
3. If the polling is successful, an **ON** status will be reflected. If it is not successful, an **OFF** status will be shown after a short while.

NOTE:

The *Status* is only valid after user has executed the poll command to the device connected. Therefore, if user exits from the device management system and comes back later, the status will show "off". This does not mean the device is not connected physically. To obtain the connection status, user needs to execute the poll command to update the status.

Under the Poll Device/Upload Log File group box, there are two radio-buttons, "All Device" and "Device ID". You can poll one device at a time or all the devices simultaneously if you have several devices connected, by selecting the appropriate radio-button first.

WARNING:
All devices configured in the system must have a unique Device ID. The Device ID should be the same as the device ID configured in the device for serial communication channel. Please refer to the BioPointe User's Manual on how to configure the device ID for this type of channel. In addition, the report generator will base on the device ID for report generation.

E. Create Device User Records

This process is also known as enrollment, where you can enroll new device users. By device users, we are referring to the users who would be performing their fingerprint authentication at the Device.

NOTE:

Each user must be enrolled separately in BioPointe Central and Keri Systems' *Doors* program. For information on enrolling users in *Doors*, refer to the *Doors* Users Guide (P/N 01914-100).

To create a new Device User record:

1. If you were not in the **User Database** main menu, you would need to return to it. The menu is as shown below:

Database edit buttons:

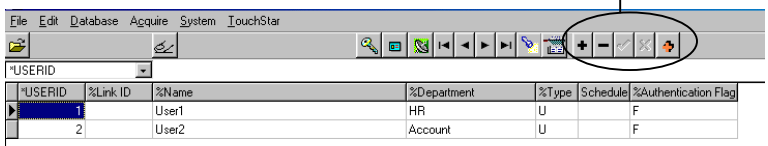
Append

Cancel

Save

Delete

Insert



Database edit buttons

User records

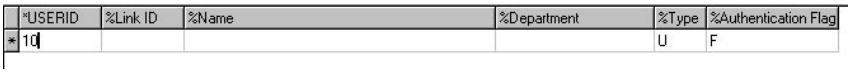
Database mode indicators:

Browse mode

Edit mode

Insert mode

2. First click the Insert button.



3. The **UserID** field is filled in with a default ID that increments every time a new record is created. You can change the ID to the desired ID of the user whom you are adding.

NOTE:

The *Type* field refers to whether the device user record is to be assigned as a normal *User* or a *Master*. By default, this field is filled as a *User*

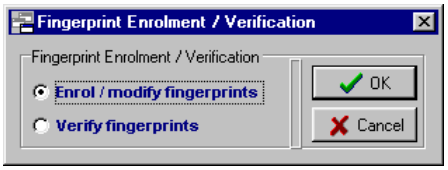
- **The *Authentication Flag* field refers to the method of authenticating this user. By default too, this field is filled as *Fingerprint*.**

The optional fields are the *Link ID*, *Name* and *Department*

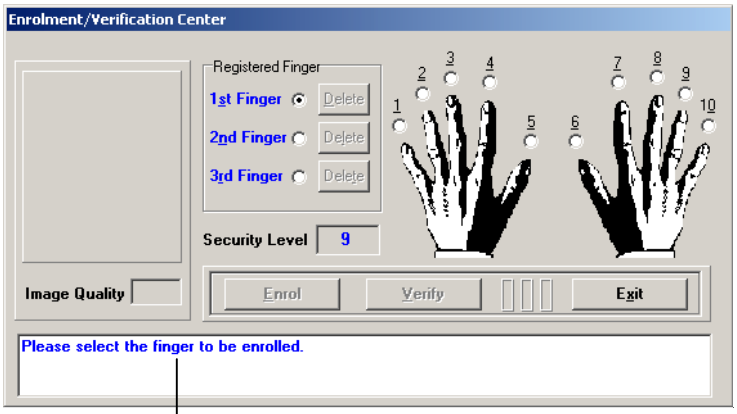
During the log record export operation, if the *Link ID* for a particular user record is not empty, then this *Link ID* information will replace the *USERID* information. This is especially useful if user want to co-relate the *USERID* to the *Link ID*.

---

4. Click the **Save** button to save the settings you have made for this user record.
5. You have now created a Device User record. However, no fingerprint(s) has been enrolled for this user yet. You can note this by an icon displayed at the bottom left hand of the User Database menu. For this user you will see a cross over a fingerprint image implying that no fingerprint(s) has been enrolled for this user. 
6. To enrol the user's fingerprint(s), click this button  found on the task bar while the database pointer is pointing to this user record. This leads you to a menu box shown below.



7. Select **Enrol / modify fingerprints** since we are performing an enrollment and click **OK**.
8. You will see the **Fingerprint Enrollment / Verification Center**. Follow the instructions from the instruction screen to perform your enrollment.



Instruction screen

9. You will see the **Fingerprint Enrollment / Verification Center**. The instructions from the instruction screen will guide you in your enrollment. We would like you to take note that:

- Each enrollment of a finger requires 2 image scans.
- Between each image scan, you need to lift your finger and place it back onto the enrollment scanner again.
- The **Image Quality** of each scan has to be greater than 80% in order for the scan to be accepted.
- When the 2 instances of scan are successful, the **Verify** button will be highlighted to ask you to do a verification of the finger you have just enrolled.
- When the verification is also completed, you may click **Exit** to begin saving the fingerprint you have just enrolled and exit, or you may wish to go on to enroll another finger before exiting.

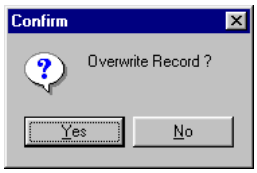
NOTE:

Maximum number of fingerprints allowed for each User

Each user can enroll up to 3 fingerprints. This is indicated by the 3 selections in the *Registered Finger* group box.

---

10. Upon clicking on **Exit**, you will be asked whether you really want save the record. Click **Yes** to proceed.



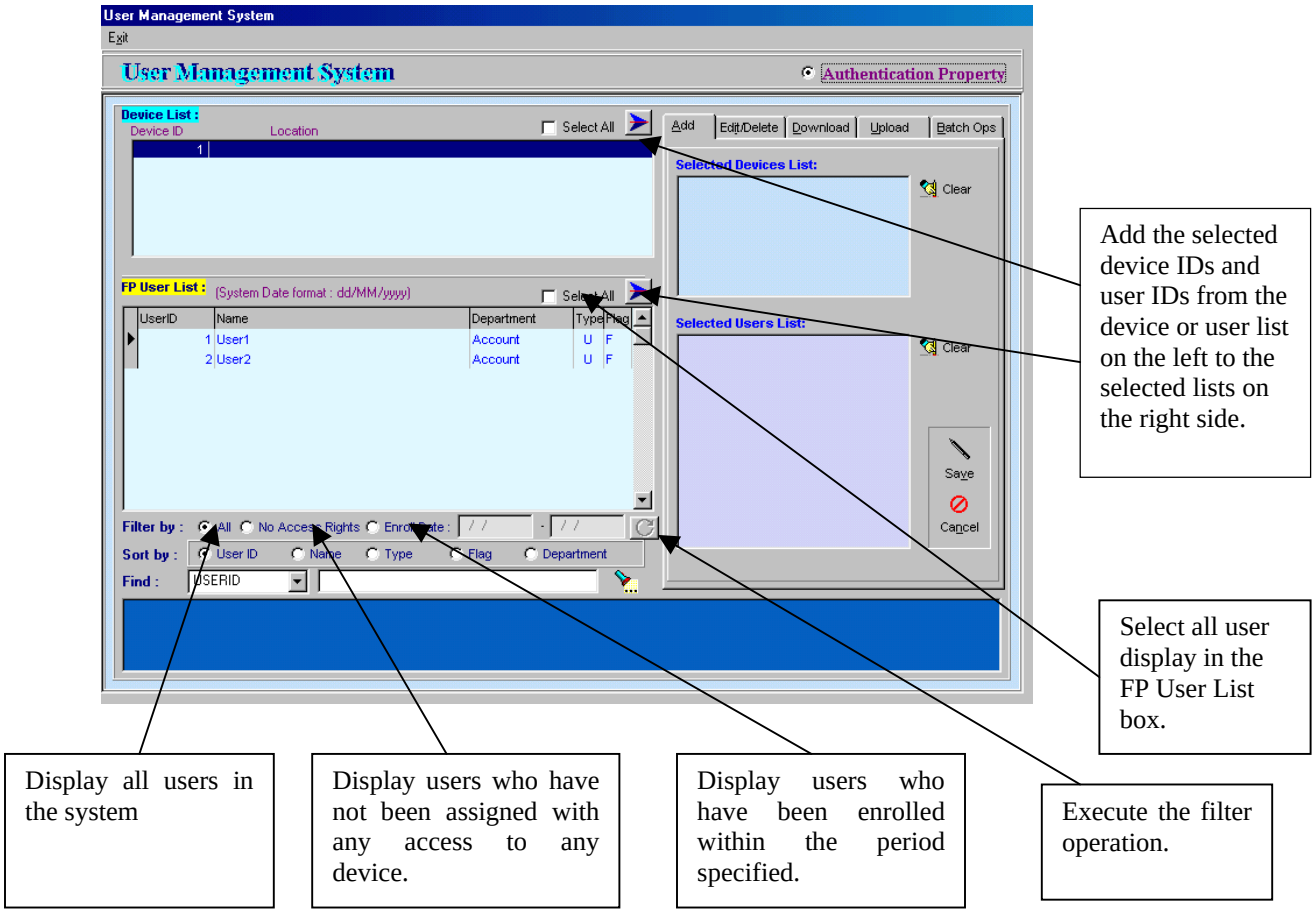
F. Assign User Access Right to a BioPointe Device

Once the user has been given access rights to a specific device, that user is ready to access the device locally.

To assign user access right to a device:

1. Click Tools from the top menu and select **User Management System** from the drop-down menu.

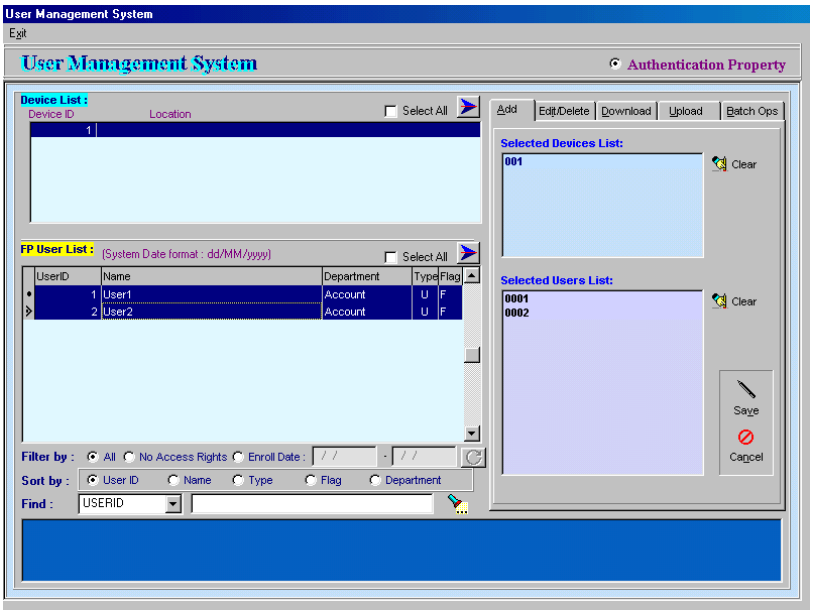
2. Select the **Add** page on the left pane, Click to add the selected device Id into the Selected Devices List box.



3. Click to move the multiple-select User Ids into the Selected User List

NOTE:

To select multiple user ids from the FP User List, press the "CTRL" key and left mouse click on the item to be selected. The currently selected item will have icon as shown. The selected item will have icon as shown.



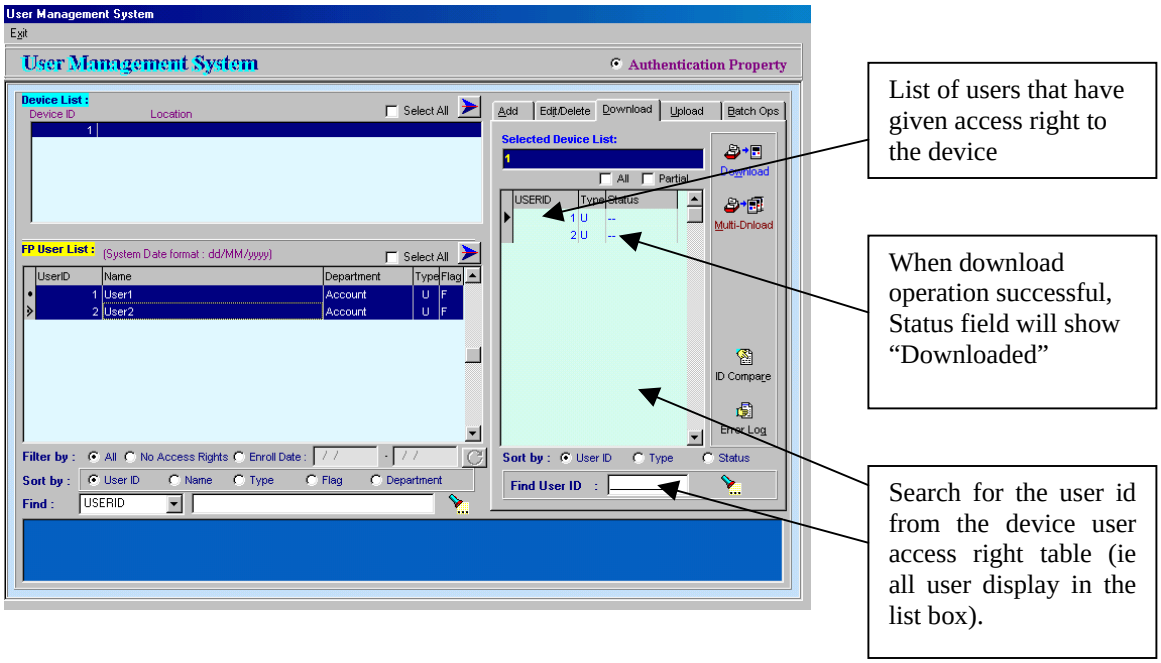
4. Click **Save** button to commit changes.

G. Transfer User Records to a BioPointe Device

When you have created some Device User records, the next step is to transfer the User records to the Device. The process of transferring data from PC to Device is known here as **Download**. This section shows you how to download User records to the Device.

To download user records to the device:

1. Select **User Management System** from the Tools drop-down menu. Upon doing so, you will see the User Management System screen as shown below:



2. Select **Download** page.
3. Check the **All** check box to select all the users in the user's list for download operation or select the specific user in the user's list box. To select multiple users, mouse click on the user with the "Ctrl" key press down.
4. Click **Download** to start the download operation.

NOTE:

If the *partial* option selected, the application will only download user record that has not been downloaded before. (ie. user record with "downloaded" status with be skip).

Chapter 5

Advance Features

This chapter describes the advance features provided by the BioPointe Central package. These features assist the administrator to distribute user records efficiently. In addition, it also allows the administrator to upload device log records from the device and store into the event log database. From the event log database, the software provides the function to export the data into ASCII text file to a third party data crunching software application.

A. BioPointe Central Administration

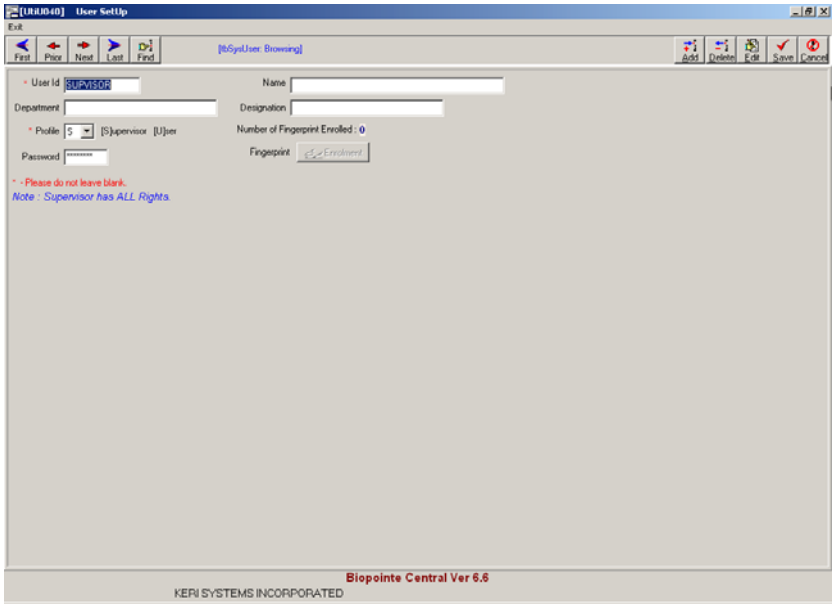
Two types of user profiles are supported by the BioPointe Central application. One of them is the "Supervisor" profile and the other is the "User" profile. Administrator with "Supervisor" profile has all the rights to perform any task provided by the application. Administrator with the "User" profile can has restricted access to some of the tasks provided by the application.

The default authentication method for the administrator during application logon is password authentication. However, the authentication method can be converted to use fingerprint. If the BioPointe device is configured to use secure communication mode, then the administrator is require to use fingerprint during application logon. This is because the same fingerprint template used during the application logon will also be used for the secure communication session. Please refer to the BioPointe manual on how to enable the secure communication mode in the BioPointe device.

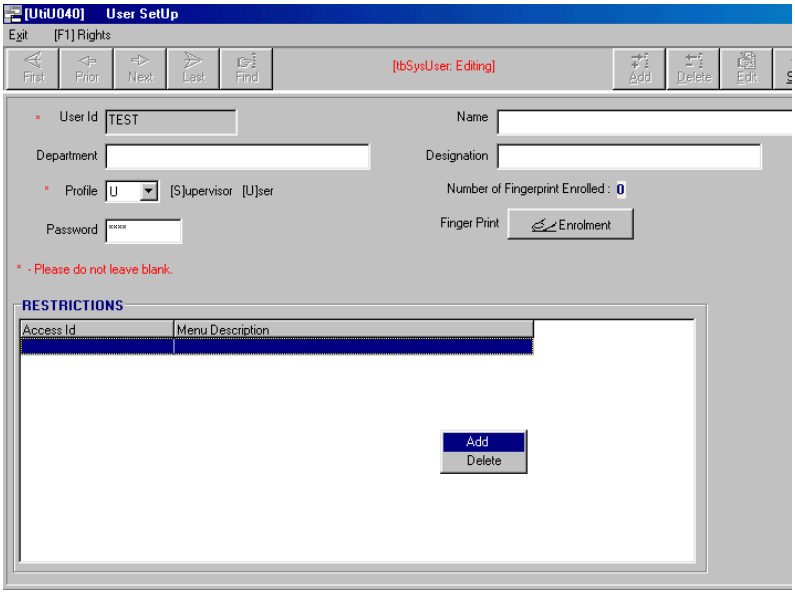
"User" Profile access restriction setting

To configure the access restriction:

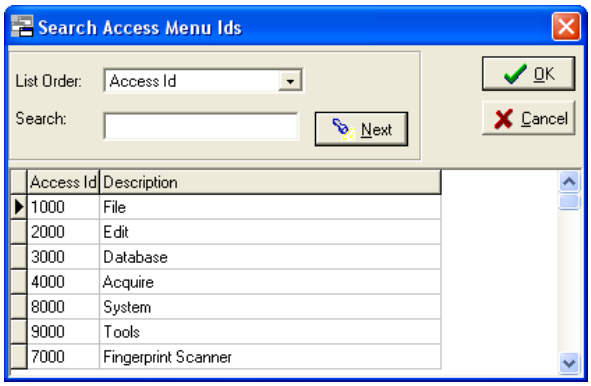
(1) Click **System** from the top menu and select **User Setup** from the drop-down menu.



(2) Click the **Edit** button to open the fields for edit mode.
(3) Click the **Add** button. The following dialogue box will be shown:



(4) Right click within the **RESTRICTIONS** and select **Add** to add the restriction entry.



(5) Select the features by double clicking on the **Access Id** and click **OK** to commit the change.

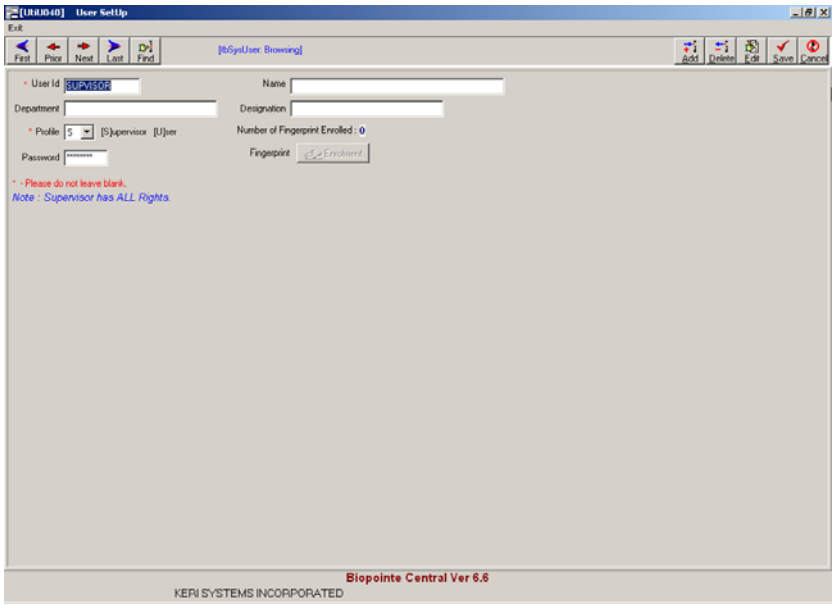
NOTE:

Only users with USER profile can have restricted access. User with the SUPERVISOR profile has all accessed right. Therefore, the access restriction cannot be configured.

Convert the logon authentication using fingerprint

To change the logon authentication:

(1) Click **System** from the top menu and select **User Setup** from the drop-down menu.



(2) Click the **Edit** button to open the fields for edit mode.
(3) Click the **Enrollment** button to start the fingerprint enrollment process.
(4) Upon completion on the fingerprint enrollment, click the **Save** button to commit the change.
(5) Click **Exit** to quit.

NOTE:

If the Biopointe device has enabled the secure communication mode (ie master fingerprint template needs to be sent over to the device before any command will be accepted by the device), the application will automatically send this fingerprint to the device for authentication. Therefore, if the logon user did not register into the Biopointe device as master user, he will not be able to execute any command to the device except the poll command.

B. Device Management System

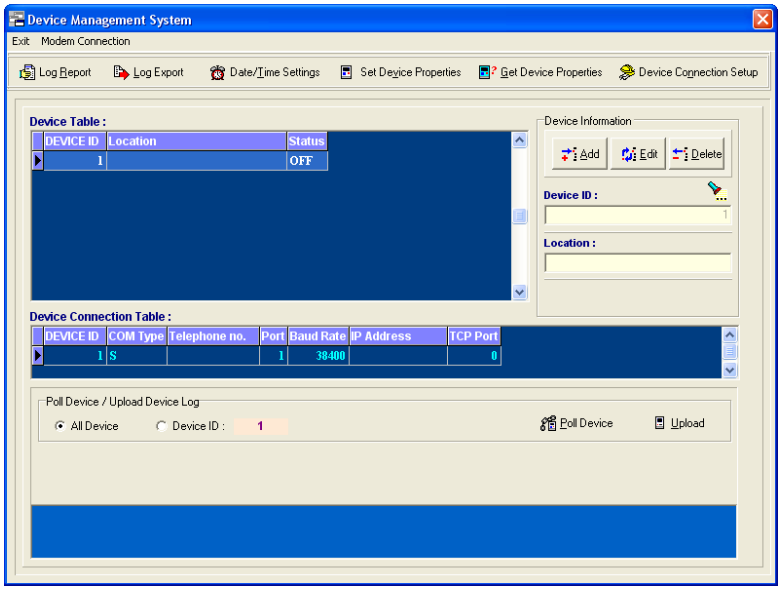
The Device Management System provides the following advance features:

(1) Device date/time setting.
(2) Device parameters setting.
(3) Upload device event log records.
(4) Export uploaded event log records.
(5) Event log records report

Device date/time setting

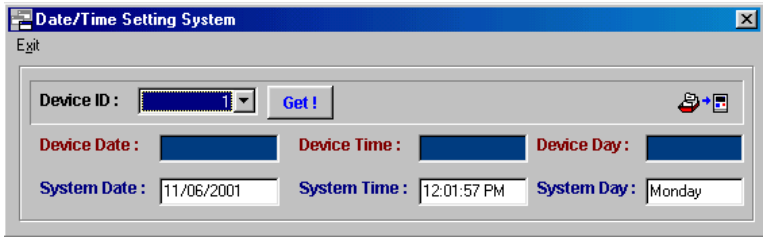
This feature allows administrator to synchronize the PC system time with the Biopointe device time.

Under the Device Management System, click **Time/Date Settings**.



Time/Date Settings

You can use this command to synchronize the time and date of a certain device with the PC.



To read and set device time and date

(1) Select Device ID.
(2) Click **Get** button to read the date and time from the device.
(3) Click to download the new date and time (PC's system date and time) into the device.
(4) Click to exit.

Device parameters setting

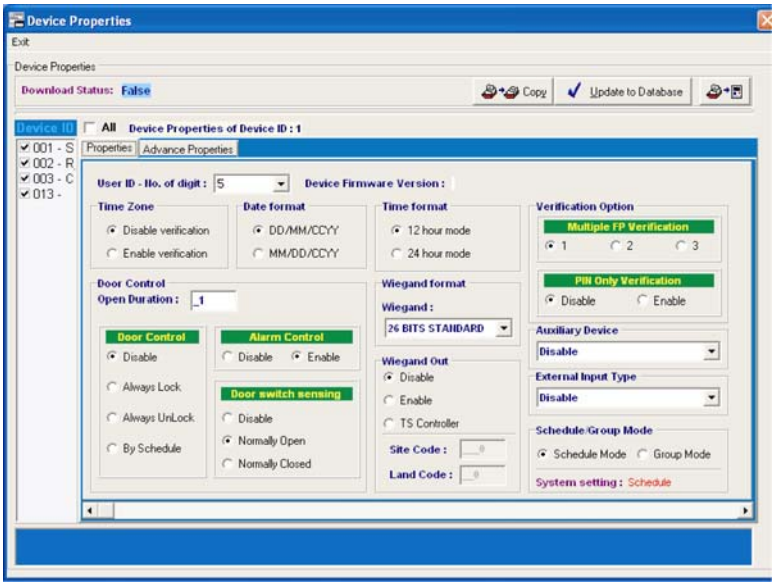
When a new device is added, the default device parameters will be created and saved into the database. This feature allows administrators to edit the device parameters and save it in the database. The saved parameters can then be downloaded to the devices. In addition, the application provides the function to compare the parameters that is downloaded to the device with the parameters saved in the database. Users can also backup the device parameters by uploading the device parameter settings and saving into the database.

To download the device properties and store the database to the device:

(1) Click **Set Device Properties**
(2) Select the Device ID.
(3) Select and enter the correct settings for individual parameter.

NOTE:

If a BioPointe with Prox unit is in use, the "User ID - No of Digit" field <u>MUST</u> be changed to "5" for each device that will use cards.



(4) Click **Save** button to save changes into the database.

(5) Click  to download the new configuration to assigned device.

(6) Click  to exit.

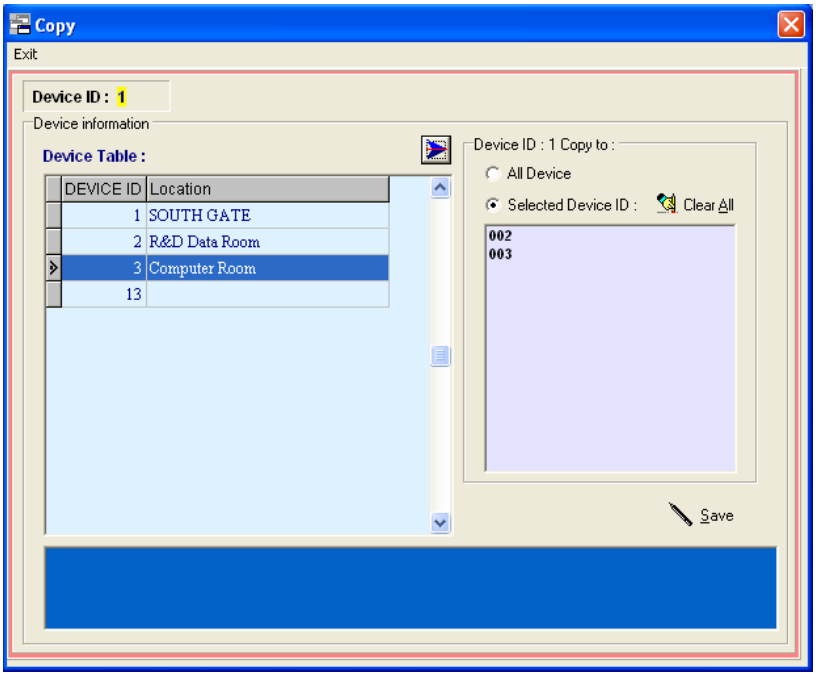
Or

(2) Select multiple device IDs.

(3) Click  to download the new configuration to assigned device.

(4) Click  to exit.

The **Copy** option allows you to copy the configuration of a device to multiple devices based on the configuration stored in the database. Note: This only copies the configuration, its does not update the device based on the new setting. The user has to manually download the modified configuration to those particular devices.



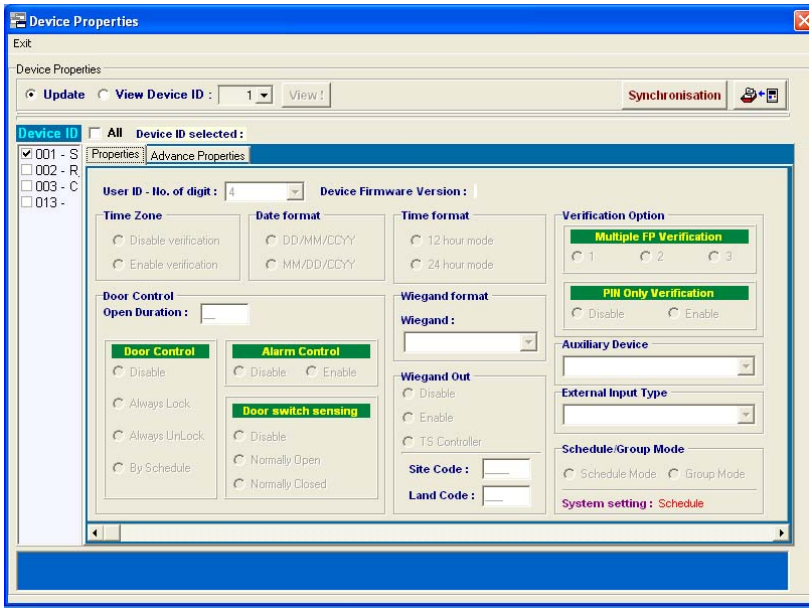
To Copy from device to multiple devices:

1) Select the source device and then click on the "**Copy**" Button from the Set Device Properties module.

2) Select the target devices from the device Table and click on the to put the selected devices into the selected device list.

Click on "**Save**" button to save the source device properties to all the selected target device properties resided in the database.

To upload device properties from the device:



To use upload device configuration feature:

1) Select Device ID.

2) Click **Get** button to see the device current settings.

3) Click  to exit.

To use the synchronization feature:

1) Select Device ID.

2) Click **Synchronization** button to perform a data comparison between the device configuration data stored in the database and the device configuration data stored in the device. At the end of the operation, a report will be generated if there are any differences. If there is no difference, the message "no record " will be displayed.

3) Click  to exit.

To backup the device parameters setting:

1) Select Device ID.

2) Click  button to upload the device parameters from the device and save the uploaded information into the database.

3) Click  to exit.

Device properties

Properties	**Options**	**Description**
User ID	3 – 10	# of user digits used as the User ID. When using a card, this **MUST** be set to 5.
Date format	DD/MM/CCYY	Set the date format of the device. Eg. 25/02/2003 or 02/25/2003
	MM/DD/CCYY	
Time format	12 hour mode	Set the time format of the device. 12 hour mode - hh:mm:ss tt time format. 24 hour mode – HH:mm:ss time format
	24 hour mode	
Multiple FP Verification	1 – 3	Device allows one to three Fingerprint verification.
Pin Only Verification	Disable	Once this option is enabled. The device only allows PIN Only verification. It does not require fingerprint or card.
	Enable	
Wiegand	26 bits – 40 bits	The types of wiegand format.
Wiegand out	Disable	Refers to the wiegand data is being sent out to the external controller upon a successful authentication. TS Controller option meant Biopointe controller not other vendor external controller.
	Enabled	
	TS Controller	
Site Code	--	The two parameters that existed in the format of the contactless card.
Land Code	--	
Auxiliary Device	Disable	These reader options are auxiliary devices supported by Biopointe. An example of a use of such an input device is to read in the ID of the associated card instead of using the keypad.
	Legic	
	Mifare	
	Barcode	
	Magstripe	
External Input Type	Disable	An external sensing is provided by Biopointe to detect the occurrence of a specific event. These types of events that can currently be detected and supported by Biopointe
	Wiegand Ack	
	One-To-Many	
	Station locking	
	Switch To Card	

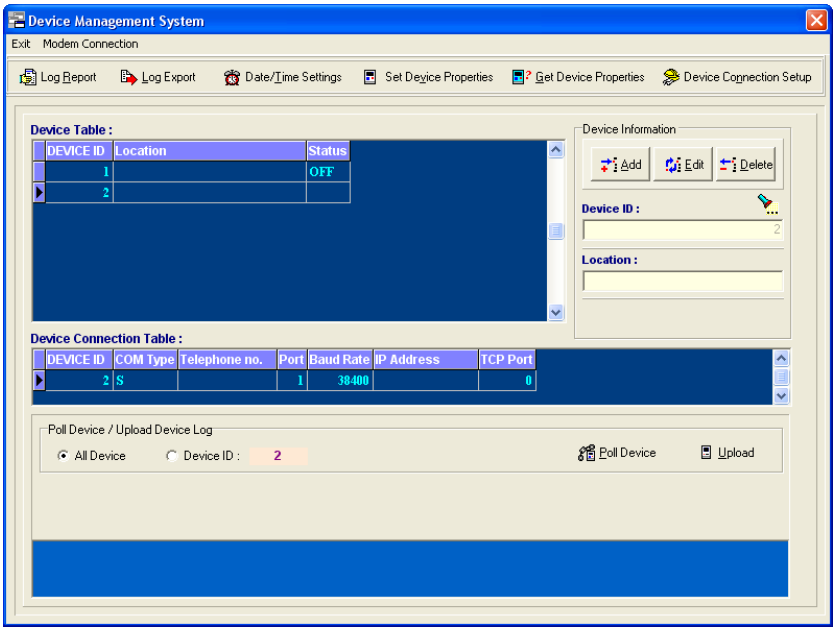
Device advance properties

Properties	**Options**	**Description**
Verify level	Normal	The security verification level of the fingerprint scanner. Either normal security or high security
	High	
One to Many	Disable	Enabled to let user do one to many verification of the fingerprint. Eg. User just verifies once without keying his/her user id, the device will auto search for his/her user record and verify that this user is accessible.
	Enable	
TA Mode	Disable	N/A. Leave at default.
	Enable	
Trace Log	Disable	The device will log all the options and functions a user/administrator has done with the device.
	Enable	
Fail attempt Log	Disable	Enabled to log the failed authentication of a user access the device.
	Enable	
Numeric Keys	Disable	Disable to prevent the usage of the keypad.
	Enable	

Upload event log records

To upload device log records:

(1) Click Tools from the top menu and select **Device Management System** from the drop-down menu.
(2) Select the device to be uploaded by clicking on the device in the Device Table list box.



(3) Click **Device ID** to upload event log records from the selected device only.
(4) Click **Upload** to start the device log record uploads operation.

WARNING:

Before you proceed, check your Regional Settings in Control Panel. Ensure that your date style is not set to dd/mm/yyyy or dd-mm yyyy. The date format should not be in character-based. (Eg 12-Jan 2001 ← this is not allowed.)

Export uploaded event log records

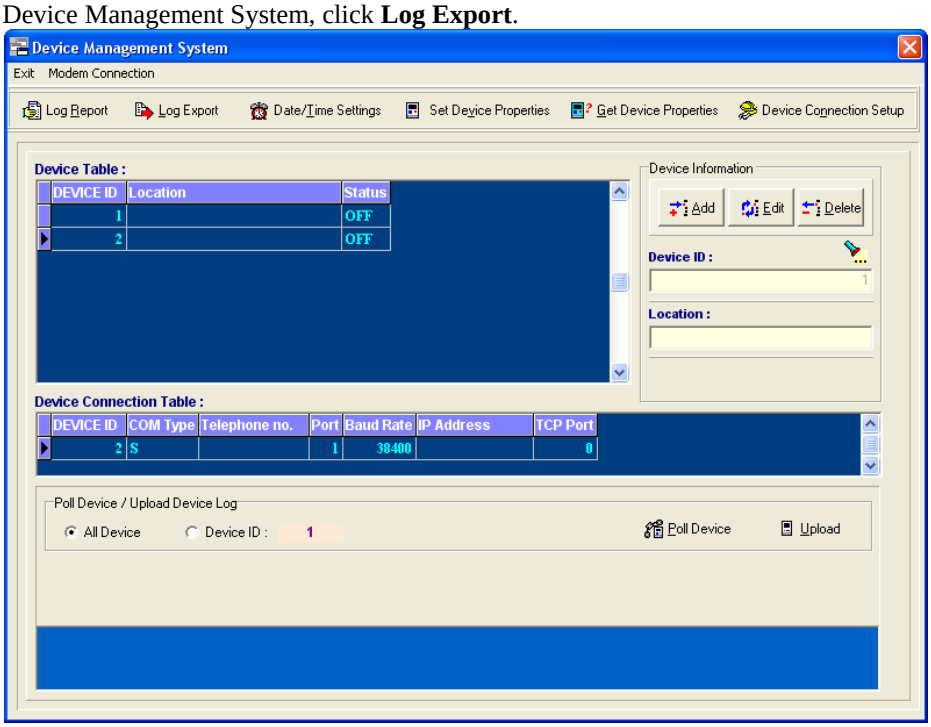
The log records stored in the event log database is password protected. However, in order for the third party software application to use the log record data for data crunching (i.e. to generate pay roll report, time attendance report etc), the Biopointe Central application provides the feature that allows user to export the log record data into a ASCII text file. With this ASCII text file, users can easily import the log record into the third party software application.

NOTE:

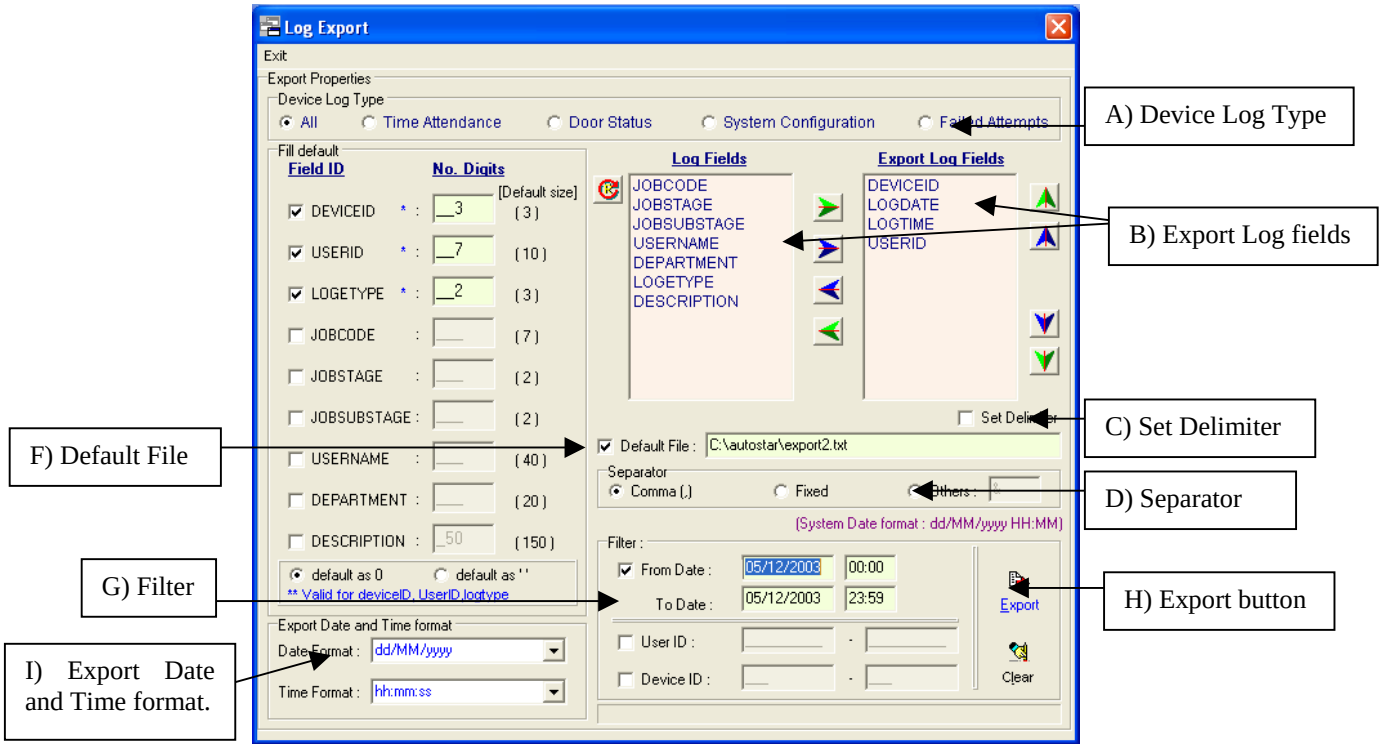
Most of the third party software (for payroll or time attendance application) support import of data through the ASCII text file.

To start the log export function:

Under the Device Management System, click **Log Export**.



Following section provide a full description on all the functions provide by the export log interface.



Reset all the log fields into the original position. Clear the export log fields. (User need to add in the export log fields again.)

Add **ALL** the log fields into the export log field list. (All the fields will be exported.)

Add the **Selected** log fields into the export log field list. (Add some of the selected log fields for exporting.)

Remove the **Selected** Export fields from the export list into the log field list. (Remove selected field from exporting)

Remove **ALL** Export fields from the export list into the log field list. (No fields are to be exported.)

Move the selected Export Field to the first position of the export list. (The first field to be exported.)

Move the selected Export Field forward.

Move the selected Export Field downward.

Move the selected Export Field to the last position of the export list.

Export All Data of the fields in the Export list into a ASCII text file.

Clear all the Text values.

A) Device Log Type

Device Log allows you to select which kind of Log information is to be exported namely: All, Time Attendance, Door Status, System Configuration and Failed Attempts. Please refer to Log Report for the definition of the type of logs. The default setting is All Log where all the 4 types of Log information are to be exported.

B) Export Log List

Export Log List allows you to select the fields of the information that is to be exported. All the Log fields are listed in the Log Fields List. You can add the fields of interest from this list to the export list or remove the unwanted field from the export list. You can also arrange the position of the fields in the Export List so that the data will be exported according to the position of the fields listed.

NOTE:
The first field on the top of the export list is the first field to be exported.

C) Set Delimiter

When the Delimiter option is enabled, the character fields that are exported into the ASCII text file will be enclosed with a double quotation mark. If the option is disabled, the double quotation marks will not be present. (Eg. Field1, "Field2", "Field3", "Field4" where field2, field3 and field4 are character fields.)

D) Separator

Separator option allows you to choose which kind of separator that the ASCII text file has. A Separator Character separates the fields in the ASCII text file. There are 3 kinds of separators provided in this option namely *Comma*, *Fixed* and *Other*.

Comma separator separates the field with a comma (,). Eg field1, field2, field3, field4, field5

Fixed separator separates the field using fixed field length. Please refer to the Appendix B: Log Field Table for the field size. Eg field1 field2field3 field4 field5

Other separator separates the field with a user-defined character. Eg. Selected Other: &. The txt file: field1&field2& field3&field4&field5

NOTE:
When the fixed separator selection is chosen, fields will be separated based on the defined size for each field in the Fill Default Box. The size defined for each field will take its respective default value if the checkbox is not checked for that particular field. On the other hand, if the checked box is checked, the size defined for the field will take the user entered value.

E) Fill Default

Fill Default option allows you to control the size of the exported fields. When the checkbox for any field is checked, the system will use this field size defined by the user. This field size must be enough to avoid any truncation of the data for that field. For example, if the field size is less than the total length of the data, the data will be truncated in the exported file. However, if the field size is more than the total length of the data, the data will be preceded with spacing. Take note that, this will apply for all the fields except for USERID field where it will be preceded with zeros instead of spacing.

F) Default File

Default File option allows user to set a default export text file in the selected directory. When the checkbox is checked. The system will automatically overwrite the selected file with exported data. If the checkbox is not checked, the system will always prompt user for the directory and filename before exporting the data.

G) Filter

Filter option provides the user with a way to filter unwanted data before exporting the data into the text file. The user can filter the data according to log date/time range, user id range and device id range. For keying a date range, you have to follow the system date format. You can double-click to pick a date from the calendar.

NOTE:
The date filter does not support system date format : dd-mm-yy. (Eg:01-Dec-00)

H) Export Button

Click **Export** button to export the log data into an ASCII text file.

Below is a sample of the exported log file in ASCII text format with comma separator.

DeviceID,LogDate,LogTime,UserID,LogType,LandCode,SiteCode,User Name,Department,Description

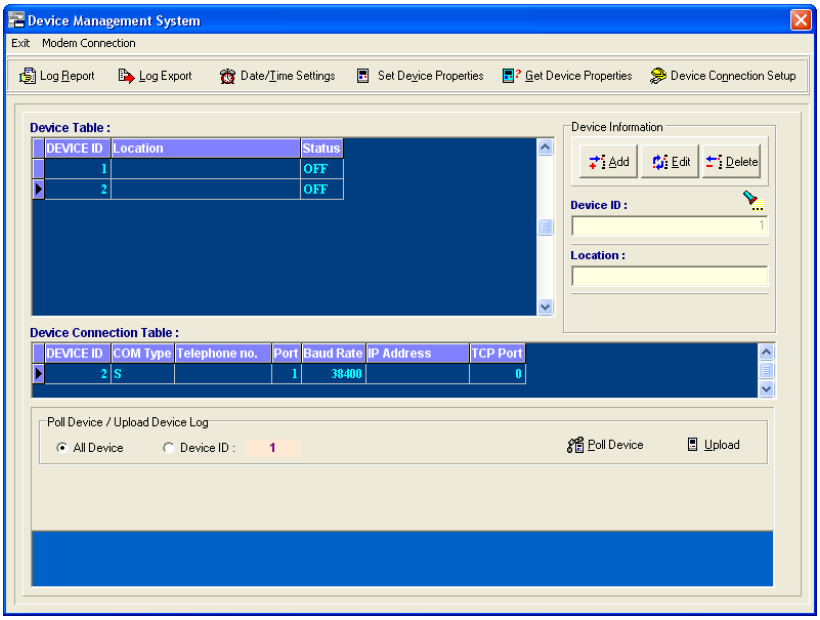
2,02/08/2000,17:30:40,0,24,0,0,,,Door switch open
2,02/08/2000,17:30:52,0,161,0,0,,,Setup Mode exit status
2,02/08/2000,17:57:07,2222,1,0,0,User1,,,Attendance-in
2,02/08/2000,17:59:59,2222,1,0,0,User1,,,Attendance-in
2,02/08/2000,18:00:22,2222,1,0,0,User1,,,Attendance-in

I) Export Date and Time format

Select which kind of Log Date and Log Time format to be exported into the text file.

Event Log Records report

Under the Device Management System, click **Log Report**.

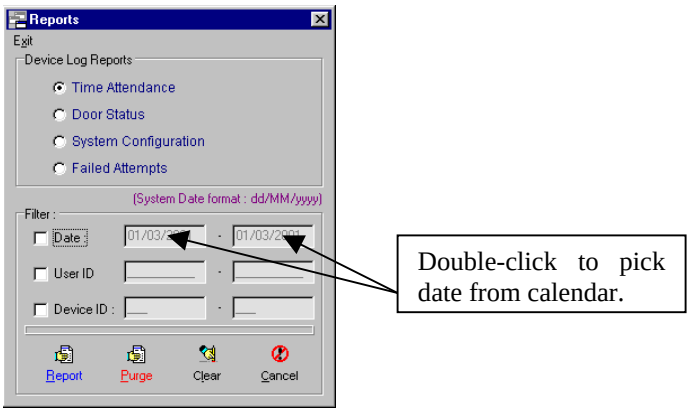


There are 4 types of log reports

- **Time Attendance**
  This report refers to a log record with status ranging from 0x01 – 0x06. It shows all the user's logging in and out of the device.
- **Door Status**
  This report refers to a log record with status ranging from 0x10 – 0x1F. It shows the status of the door at the time the user is accessing the device.
- **System Configuration**
  This report refers to a log record with status ranging from 0x30 – 0xC0. It shows the trace log and the log of all supervisors' accessing the setup mode of the device.
- **Failed Attempts**
  This report refers to a log record with status ranging from 0xE7 – 0xEC. It shows the transaction log when the user fails to obtain a successful authentication with the device.

Please refer to Appendix A for the interpretation of log record status.

NOTE:
Each report displays the following fields: Date, Time, Device ID, UserID, Link No., User Name, Department, Land Code, Site Code and Access Mode Status.
If the device trace function is turned off, no Door Status and System Configuration Log record will be generated by the device. Please refer to the Biopointe User Manual on how to turn on/off the trace function.



Icons

Generate selected type of report based on the filter setting.

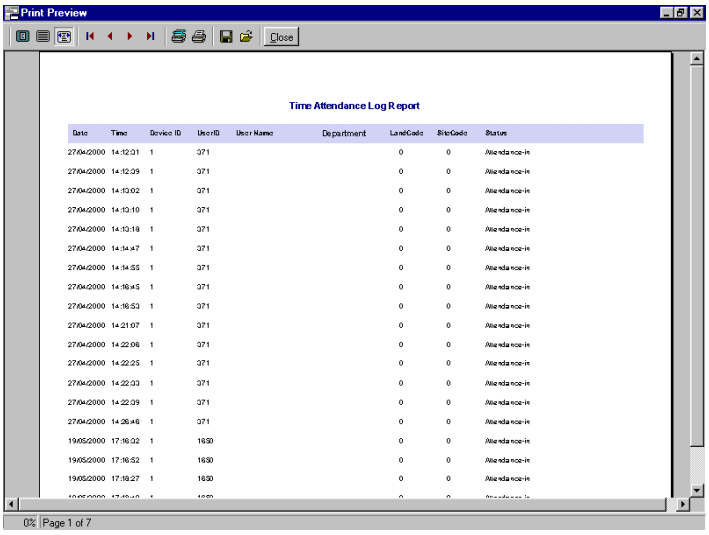
Purge selected type of record in the database based on the filter setting

Clear all filters range setting.

Exit from the report generator

To generate report

(1) Select type of log report.
(2) Check the filter checkbox if filtering is needed and enter the range. Otherwise all records will be displayed.
(3) Click **Report** button to view.



To purge log records

(1) Select which type of log report you want to purge.
(2) Check the filter checkbox if filter is needed and enter the range. Otherwise all log records will be deleted.
(3) Click **Purge** button to remove the records from uploaded log.

WARNING:
Purged data is not recoverable.
Make sure that the Windows system has the appropriate printer driver installed or else the report preview may not function properly.

Log Export

This command allows the user to export the uploaded log records into a file in ASCII text format. It provides the user with variable ways to export the log information.

Log Field Table :

Definition	Size	Description
Device ID	3	ID of the device. All devices connected in the chain should have unique ID
LogDate	-	Date of the Log record. (Size according to the format selected.)
LogTime	-	Time of the Log record. (Size according to the format selected.)
UserID	10	User ID or Card ID for user accesses through card/fingerprint. For log record related to the system configuration, the ID will be zero.
LogType	3	Log record status value. Please refer to Appendix A for all the supported status.
JobCode	7	This value is valid only if Work in Progress Mode in the Biopointe Device is enabled.
JobStage	2	This value is valid only if Work in Progress Mode in the Biopointe Device is enabled
JobSubStage	2	This value is valid only if Work in Progress Mode in the Biopointe Device is enabled
UserName	40	The user name that is located in the user database. This is only valid for the full version of the Biopointe Central.
Department	20	The department that is located in the user database. This is only valid for the full version of the Biopointe Central.
Description	150	This is the description of the log record status.

NOTE:
For the Biopointe Central application, if there is a value in the Link ID field in the User database, the LINK ID field value will overwrite the value in USERID field during log export process.

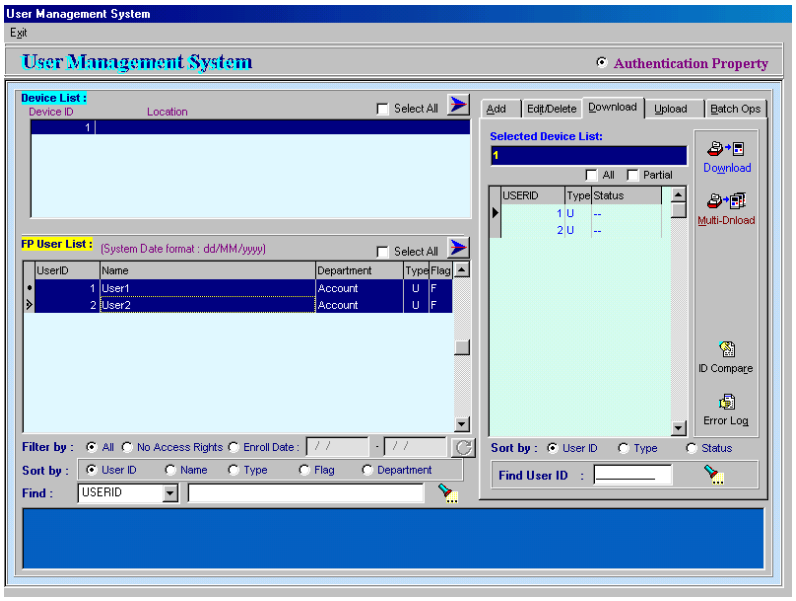
C. User Management System

The user management system provides the following advance features:
(1) Batch download of user records to multiple devices.
(2) Batch delete of user record from multiple devices
(3) Upload user records from a device and update to the device user database.
(4) Combine access right assignment and record download in one operation.
(5) Duplicate device users' access right records for multiple devices.
(6) Device users' access right cross check.
(7) User records cross check.
(8) Error log report.

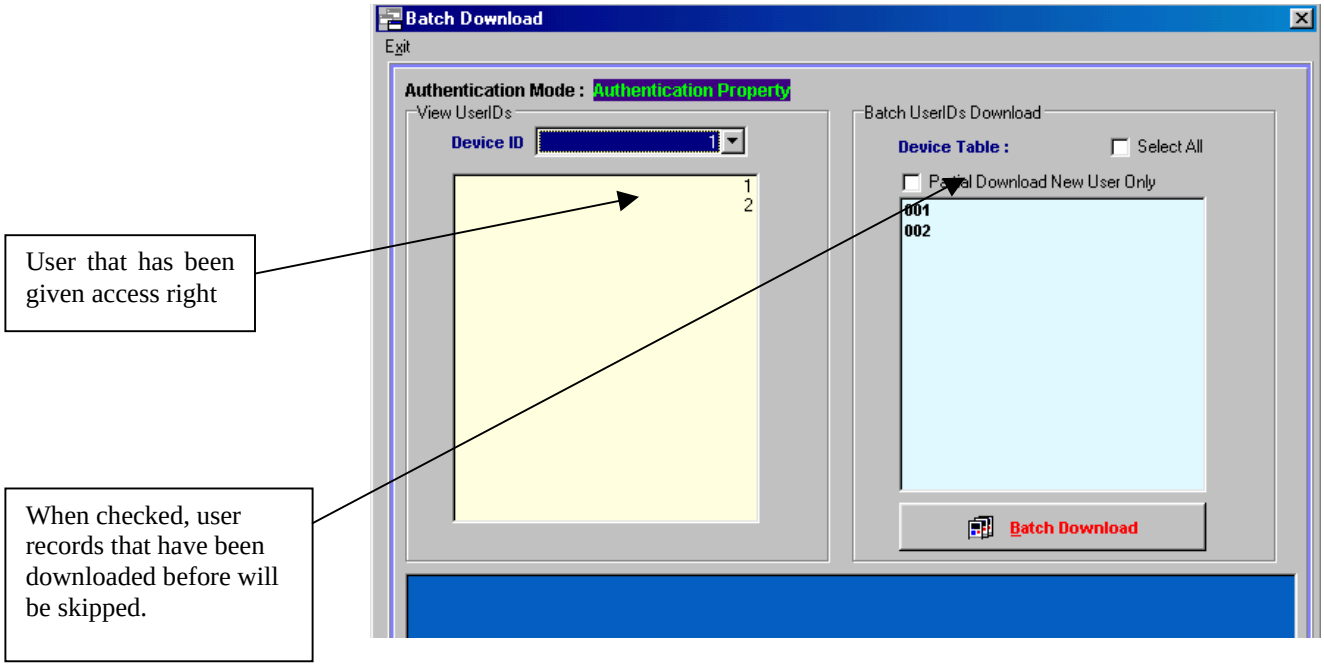
Batch download of user records to multiple devices

To perform a batch download of user records to multiple devices:

(1) Select **User Management System** from the Tools drop-down menu. Upon doing so, you will see the User Management System screen as shown below:



(2) Click **Multi-Dnload.**



(3) Select the devices and click **Batch Download**. Note to select multiple devices, press "Ctrl" key together with the left mouse click.

NOTE:

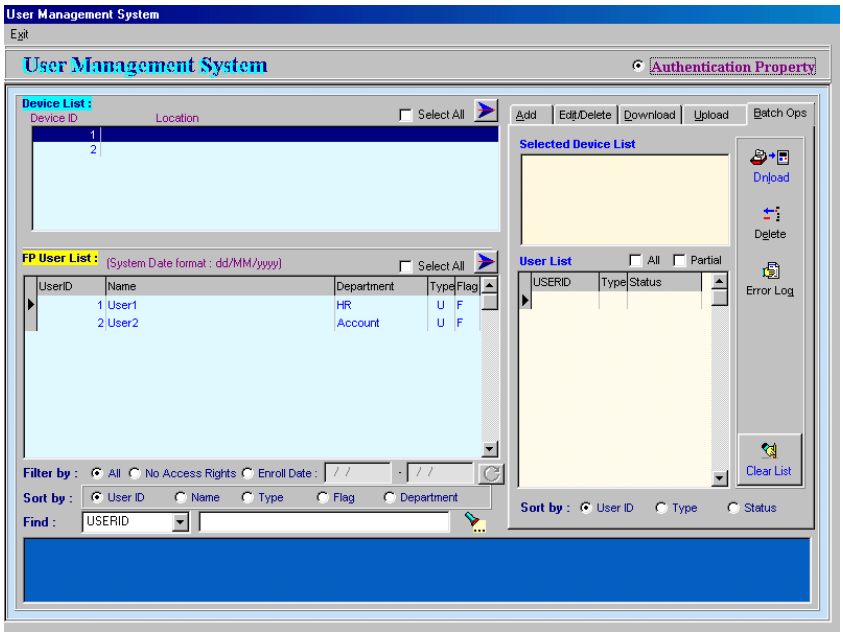
Make sure that the user access rights operation has been completed before this operation can be carried out.

Batch delete of device user record from the device.

This feature allows administrators to remove unwanted user records from multiple devices. In addition, if all the user records have been successfully removed from all the devices, the application will prompt the administrator to remove the user records from the device user database.

To perform a batch delete operation:

(1) Select **User Management System** from the Tools drop-down menu.
(2) Select the **Batch Ops** page.



(3) Select the device id from the **Device List** and click  .

(4) Select the user id from the **FP User List** and click  .

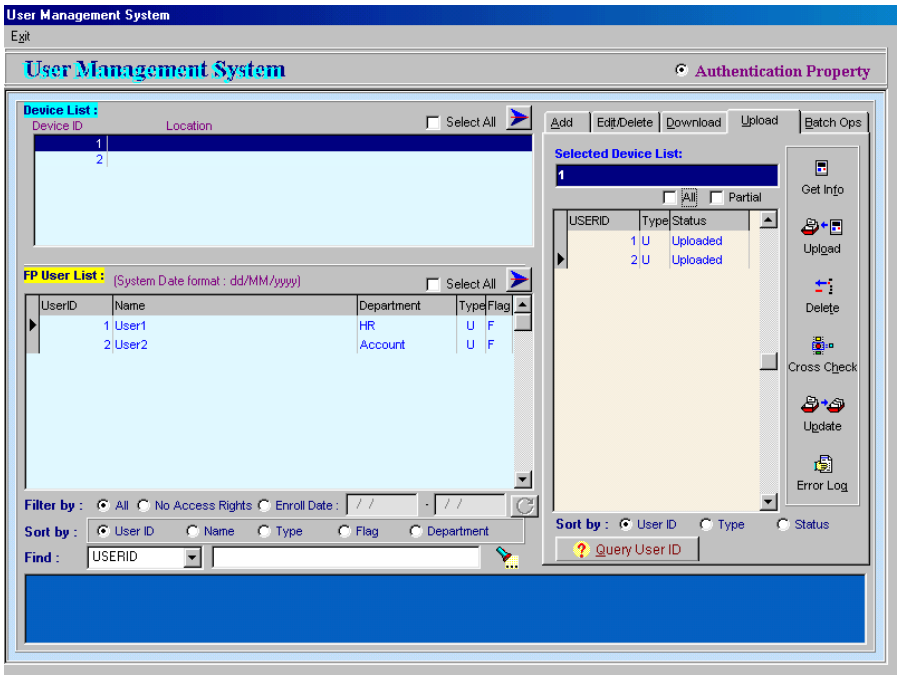
(5) Check the **All** check box and Click **Delete** to start the delete operation.

Upload user records from the device and update to the device user database

This feature allows administrators to backup the user records stored in the device to the device user database. There are three ways that the administrator can upload the user records from the device. The first method will enable administrator to upload all the user record from the device. The second method allows administrator select the desire user record to upload. The third method is to query the existence of the user record in the device, if the user is found, this user id can be added to the list and subsequently upload from the device.

Method 1:

(1) Select **User Management System** from the Tools drop-down menu.
(2) Select the **Upload** page.
(3) Click **Upload** button to start to upload all the user records stored in the device.



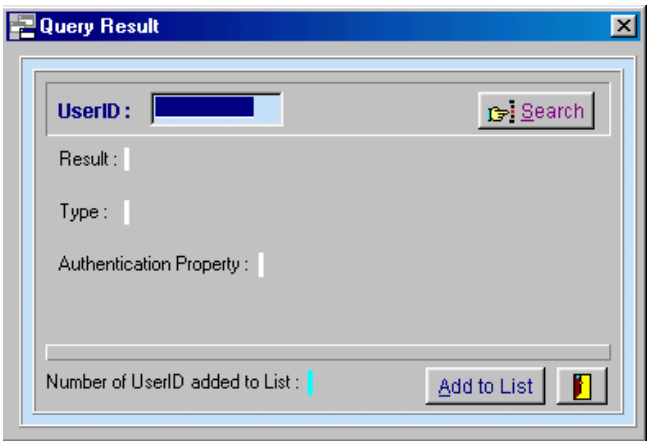
(4) Upon completion on the upload process, select the desired user id from the upload user list and do an update operation to update data into the device user database. To perform the update operation, click on the **Update** button.

Method 2:

(1) Select **User Management System** from the Tools drop-down menu.
(2) Select the **Upload** page.
(3) Click **Get Info** button to start retrieving all the user ids stored in the device.
(4) Select the desire user ids from the retrieved list and click **Upload**.
(5) Upon completion on the upload process, select the desire user id from the upload user list and do an update operation to update data into the device user database. To perform the update operation, click on the **Update** button.

Method 3:

(1) Select **User Management System** from the Tools drop-down menu.
(2) Select the **Upload** page.
(3) Click **Query User ID**.



(4) Enter the desire user id into the **UserID** edit box and click **Search**.
(5) If the user id is found in the device, click **Add to List**.
(6) Select the desire user ids from the retrieved list and click **Upload**.
(7) Upon completion on the upload process, select the desire user id from the upload user list and do an update operation to update data into the device user database. To perform the update operation, click on the **Update** button.

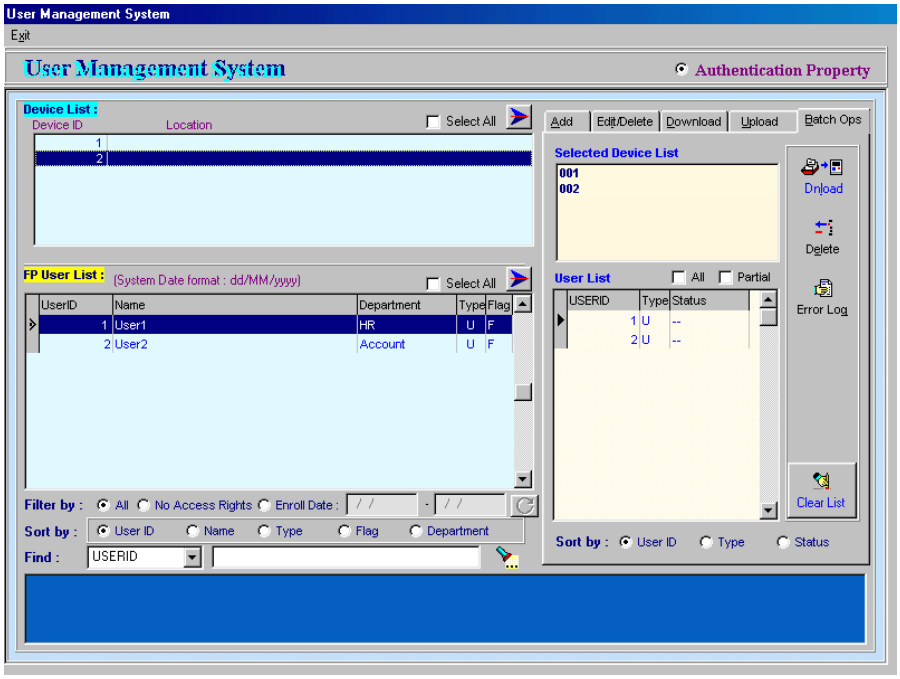
NOTE:

To delete a user record from one device at a time, the administrator can use the above methods with the *delete* operation.

Combine access right assignment and record download in one operation

Reference to the basic operation procedure of downloading user records to multiple devices, the administrator needs to first assign all the individual users to respective devices (assignment of access right to device) before a batch download operation can be carried out. However, if all the devices should have the same user records, then the administrator can perform the access right assignment and record download in one operation.

(1) Select **User Management System** from the Tools drop-down menu.
(2) Select the **Batch Ops** page.



(3) Select the device id from the **Device List** and click  .

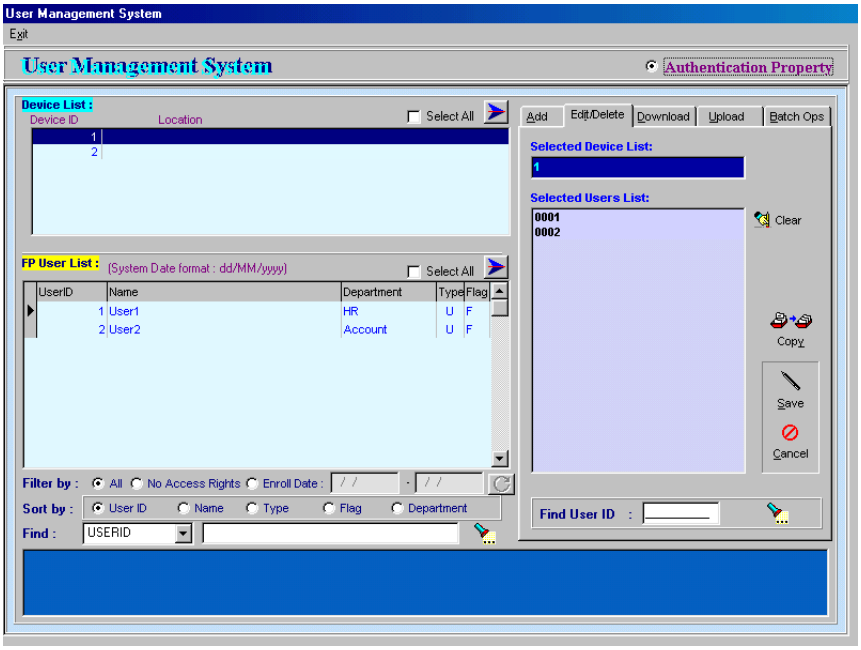
(4) Select the user id from the **FP User List** and click  .

(5) Check the **All** check box and Click **Dnload** to start the delete operation.

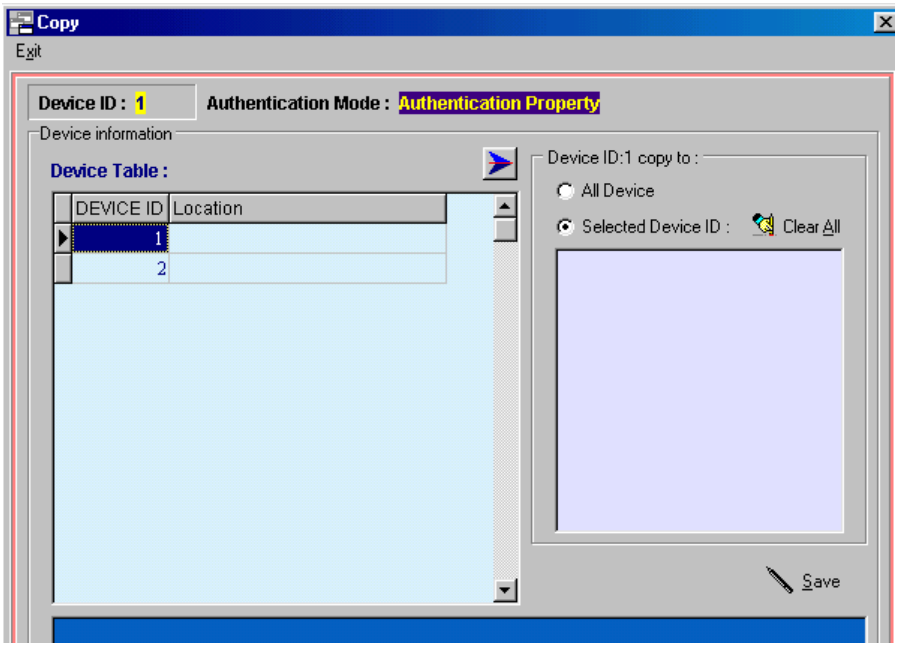
Duplicate access rights records for multiple devices

If there is a requirement that more than one device needs to have the same user records, the administrator can duplicate the access right information for multiple devices with reference to one device.

(1) Select **User Management System** from the Tools drop-down menu.
(2) Select the **Edit/Delete** page.
(3) Select the reference device id from the **Device List** box.



(4) Click **Copy** and the following dialogue box will be shown:

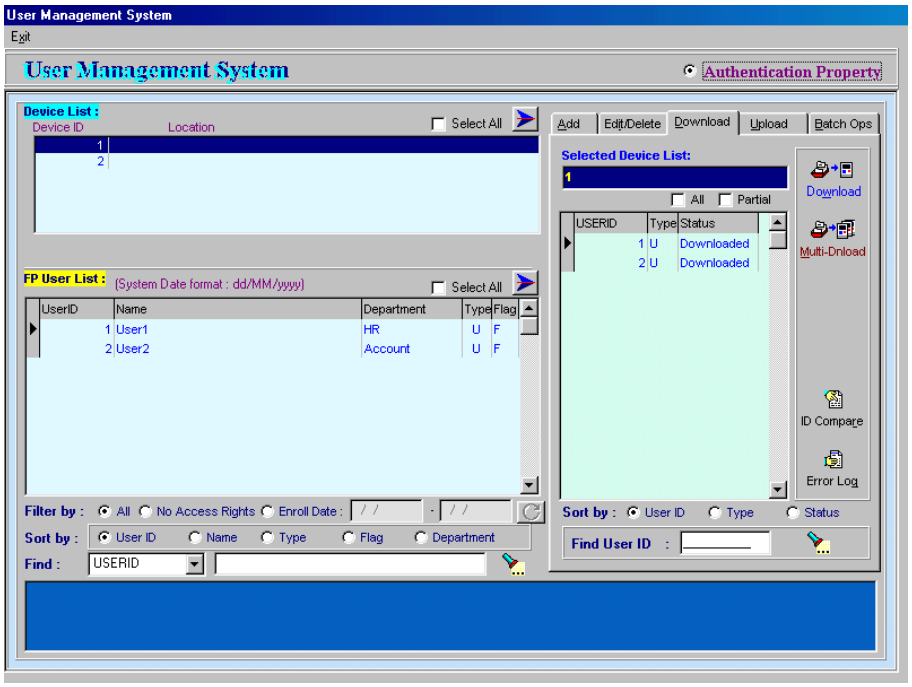


(5) Select the device from the **Device Table** and click .
(6) Click **All Device** and **Save** to start the copy operation.

Device users' access right cross check

This feature allows administrators to verify whether the device users' access right stored in the database is synchronized with the device.

(1) Select **User Management System** from the Tools drop-down menu.
(2) Select the **Download** page.



(3) click **ID Compare** to start the verification process. A report will be generated at the end of the process.

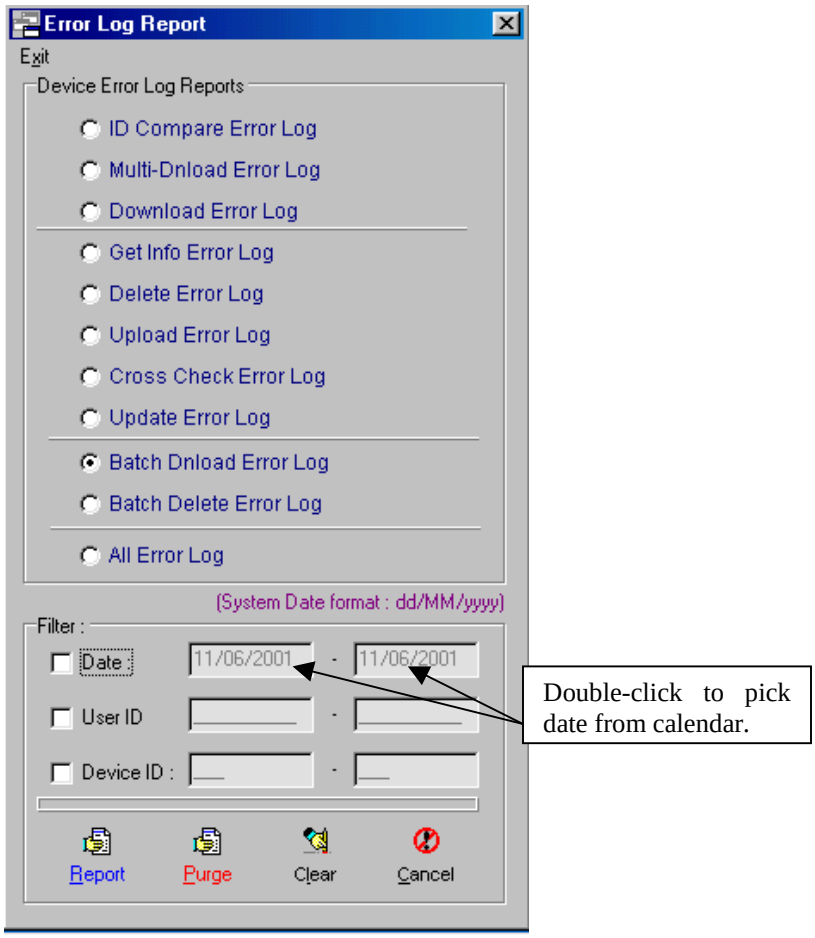
User records cross check

This feature allows administrator to compare the user records stored in the device user database with the user records store in the device.

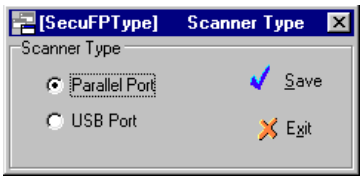
Perform a check is similar to the procedure to upload user records from the device except that instead of executing the **Upload** command, the administrator should execute the **Cross Check** command under the **Upload** page. At the end of the operation, a report will be generated. Please refer to the previous section on *Upload user records from the device and update to the device user database.*

Error log report

This feature allows administrators to check for any error during operation like download user records, upload user records etc. Under the download page, upload page and the batch ops page, administrators can open the error log report as shown below:



D. Setting Finger Print Scanner

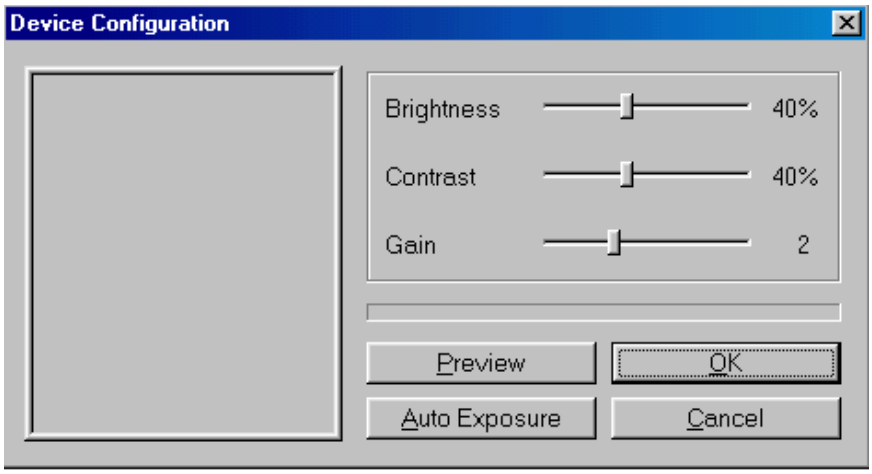


Setting the Finger Scanner Type is used to define which model fingerprint scanner is being used. There are two types of scanner namely parallel port scanner and USB port scanner.

E. Calibrate Finger Print Scanner

This feature allows administrators to perform a calibration on the fingerprint scanner.

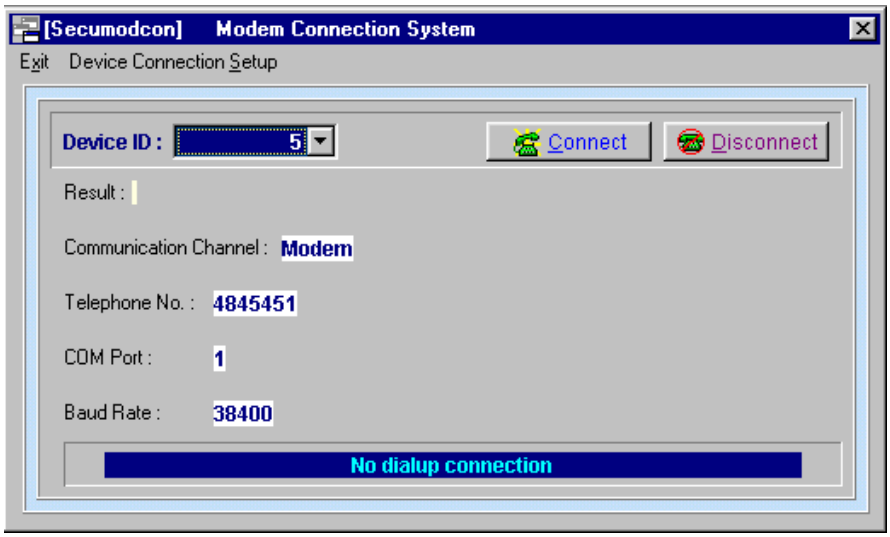
(1) Select **Calibrate** from the **Fingerprint Scanner** drop-down menu.



(2) Place the finger on the scanner and click **Auto Exposure**. Do not remove the finger until the progress bar indicates operation has completed.

F. Modem Connection System

Modem Connection System is a module that allows user to manually connect to a remote Biopointe device through a modem. The modem connection must be established before any other commands (i.e. upload log records, download fingerprint template) can be carried out. To establish the communication, the Biopointe device must be configured to modem communication mode. Once the communication is established, the connection will stay connected until user manually disconnect or exit the Biopointe Central application.



NOTE:
Once the modem is manually connected, the modem will stay connected until you have manually disconnected the modem or you have terminated the Biopointe Central application. So remember to disconnect modem after use.

To start the connection to the Biopointe device through modem:

(1) Select the device ID that is configured as a modem communication channel.
(2) Click on the **Connect** button to start dialing up.
(3) Once connected, the status will show **"Connected to remote station".**

To disconnect from the Biopointe device through the modem:

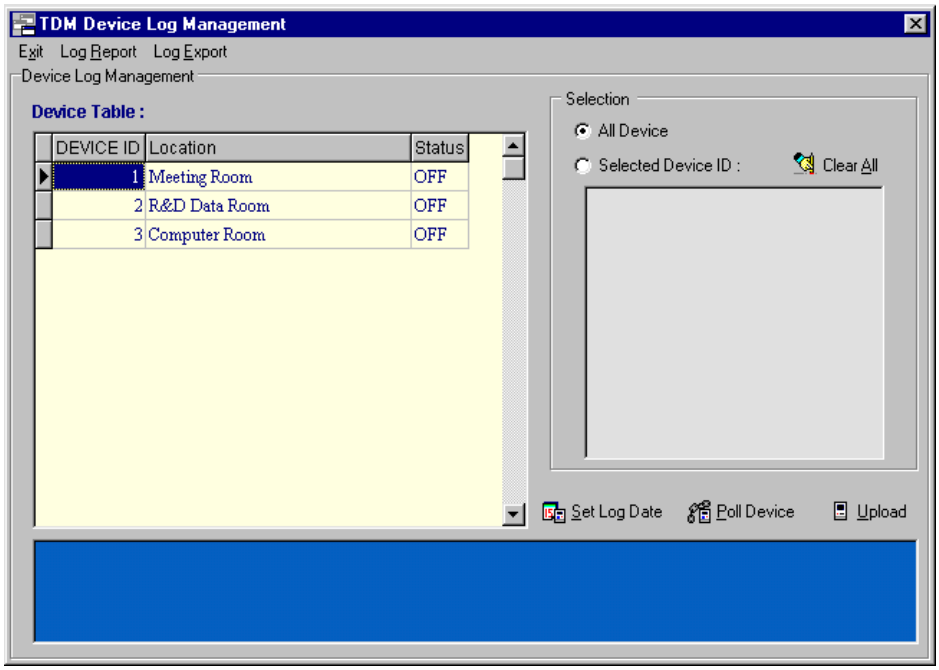
(1) Click on the **Disconnect** button to start dialing up.
(2) Once disconnected, the status will show **"Connection terminated.".**

G. Device Log Management System

This feature allows administrators to control the uploading of event log records from multiple devices, generate event log reports and export the log records to ASCII text file. All these features can also be found in the Device Management System. However, in the case when administrator want to control the access on some of the logon user from accessing the Device Management System, but still allow the user to manage the log records, then the administrator can disable to Device Management System and enable the Device Log Management System.

To upload event log records from the device:

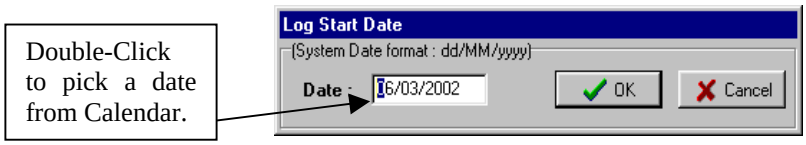
(1) Select **Device Log Management System** from the Tools drop-down menu.



(2) Select the device from the **Device Table** and click on the **Selected Device ID** button. Or click on the **All Device** button to select all the device in the **Device Table**.
(3) Click **Upload** to start the upload log records process.

To retrieve older data records from device:

(1) Click on **Set Log Date** button.



(2) Key in a desired log Date that you want to retrieve from.

(3) Click on the **OK** button to set the device date pointer back to the desired date.

(4) Click **Upload** to start the upload log records process.

Please refer to the Device Management System on how to generate event log report and export log records.

NOTE:

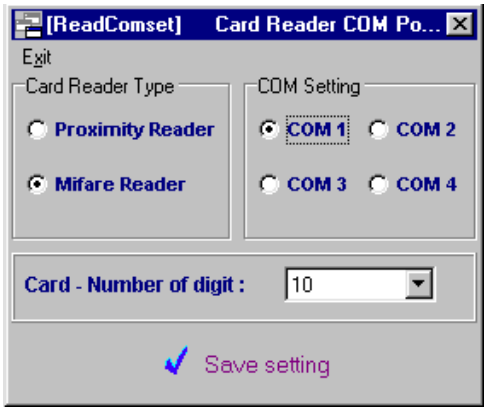
To select multiple devices from the *Device Table*, press the "CTRL" key and left mouse click on the item to be selected. The currently selected item will have icon as shown. The selected item will have icon as shown.

H. Card Reader Com Port Settings

This feature allows administrator to configure the proximity card reader connected to the system. With the proximity card reader, administrator can scan the proximity card id and replace user id field with the card id.

To configure the card reader:

(1) Select **Card Reader Com Port Settings** from the Tools drop-down menu.



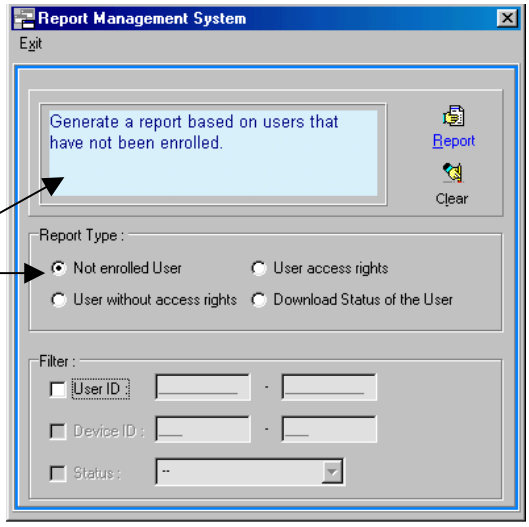
(2) Select which type of Card Reader.
(3) Select the com port that the card reader is connected to and choose the maximum number of digit to be captured from the reader by specifying the **Card-Number of digit**.
(4) Click **Save setting** to commit the changes.

I. Report Management System

This features allows administrators to generate reports on the enrollment status of all the user records in the device user database and the access rights of all the user records in the device users' access right database. From the generated report, administrators will have a better view on which user record has not been registered and which user record has not been given any access right to any device.

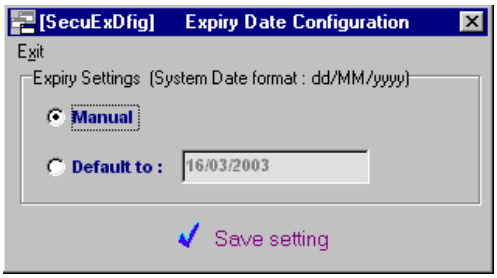
Select **Report Management System** from the Tools drop-down menu.

When the mouse is over the Report Type item, a description of the report to be generated will be shown within the blue text box.



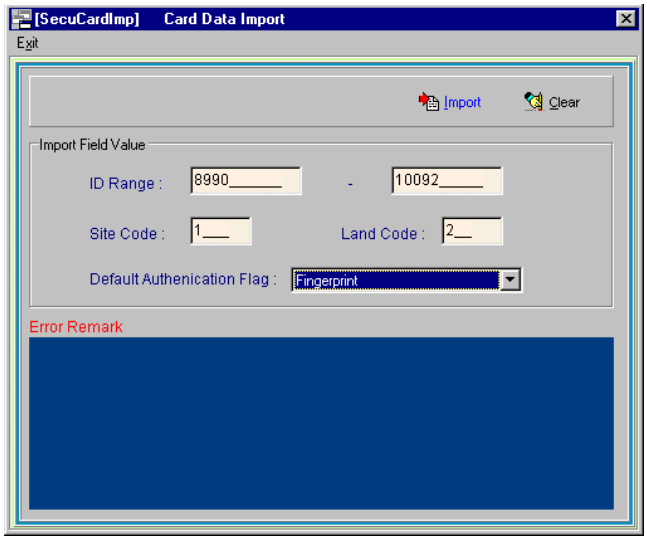
J. Expiry Date Configuration

Expiry Date Configuration function allows user to set a default expiry date or manually allow user to set a expiry date for that particular record.



K. Card Data Import

Card Data Import function provides a way for the user to import pre-defined Card number with defined Site Code and Land Code. This enables the administrator to pre-determine the User IDs in the system based on the range of Card IDs which the administrator is holding before actually issuing a User ID to the actual user.



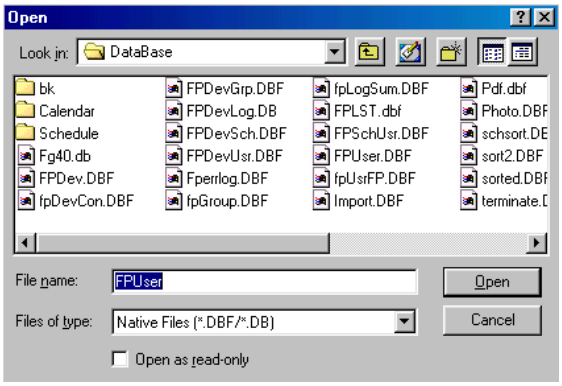
NOTE:

If an Import Card ID existed in the system database as a UserID. The System will <u>NOT</u> overwrite the information with the Imported Card ID Data.

L. Database Path Setup

The Biopointe Data Files (i.e. device user database, event logs database and device users' access right database) are stored in a default directory during the installation process. However, if user wants to place this information in a network drive, the user can copy all the database files from the installed directory (Biopointe Central\database) to the network directory. By storing the database into the network drive, multiple user can logon at different client station and share the same database.

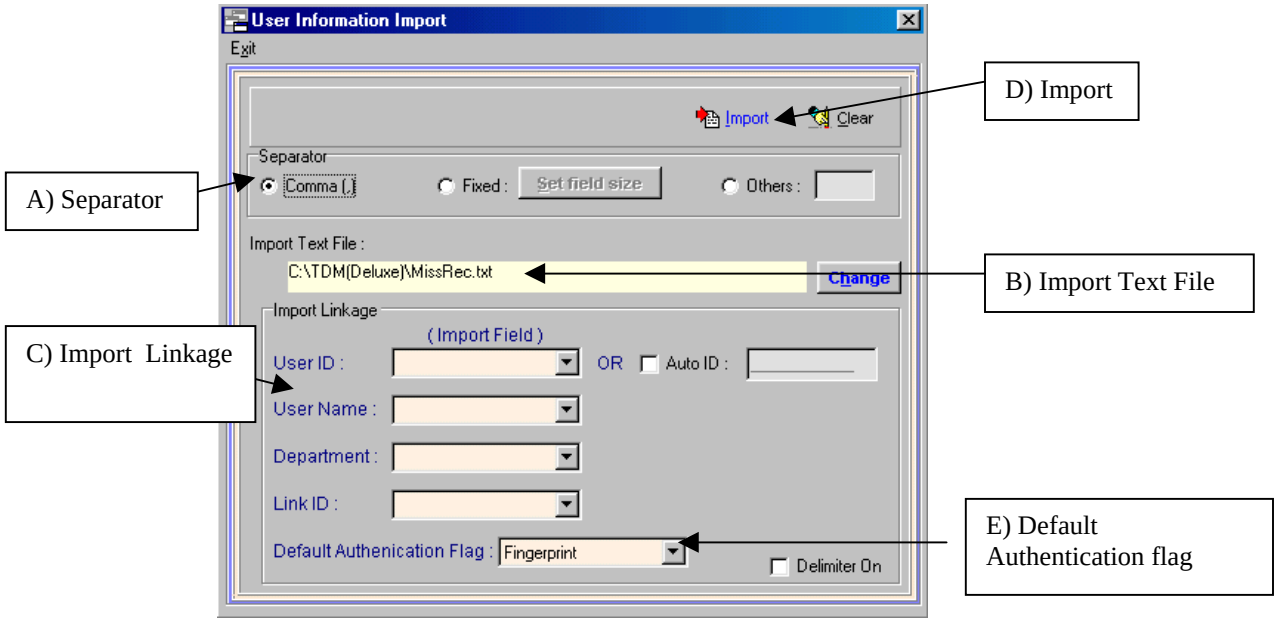
(1) Copy all the files under the sub-directory (database) of the installed directory (Biopointe Central) to a desired network directory.



(2) Click Tools from the top menu and select **Database Path Setup** from the drop-down menu.
(3) Select the file FPUser.DBF in the network directory and click **Open**.

M. Import User Information

Import User Information Module allows you to accept an ASCII text file and add the data in the text file into the User database. If the User ID of the import text file is the same as the User ID in the user database, the system will prompt you to overwrite the particular record in the database. If you select No option, the system will stop the import operation. Once activated, the system will prompt you to open the import text file. After the import file is opened, you need to select which separator and then link the correct import field to the User ID, User Name, Department and Link ID fields.

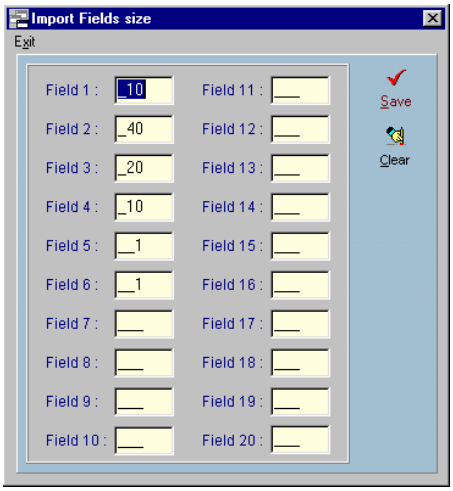


A) Separator

Separator option allows you to choose which kind of separator that the ASCII text file has. A Separator Character separates the fields in the ASCII text file. There are 3 kind of separator provided in this option namely *Comma*, *Fixed* and *Other*.

Comma separator separates the field with a comma (,). Eg field1, field2, field3, field4, field5

Fixed separator separates the field using fixed field length. Eg field1 field2field3 field4 field5
You need to pre-define the field size of each field in the text field by selecting the set field size button. Below shows the set field size screen:



To Use,

1) Key in all the field size of each different field of the import text file.

2) Click **save** buttons to save the settings.

WARNING:
Limit to 20 fields only.
Make sure that the field size is not set to 0.

Other separator separates the field with a user-defined character. Eg. Selected Other: &. The txt file: field1&field2& field3&field4&field5

B) Import Text File

Import Text File option allows you to select another text file for importing to the user database. For usage, click on the **Change** button and select another text file to import.

C) Import Linkage

Import Linkage option allows you to link User ID, User Name, Department and Link ID fields to the import text fields. Beside these, you can auto generate the user id by selecting the Auto ID checkbox. Once checked, you must key in a starting number. The system will import the file's data with the auto-generated User ID with the file's data in sequence.

NOTE:
The pull down list of each database field is automatically updated when the correct separator is selected.

D) Import

Import option allows you to import all the text file's data into the user database. System will prompt you if there is any duplicate User id.

E) Default Authentication Flag

During the import operation, the application will automatically fill in the Authentication Flag field based on the selection.

WARNING:
Make sure that the field separator is correct as it affects the import of correct data into the system.

N. Export User Information

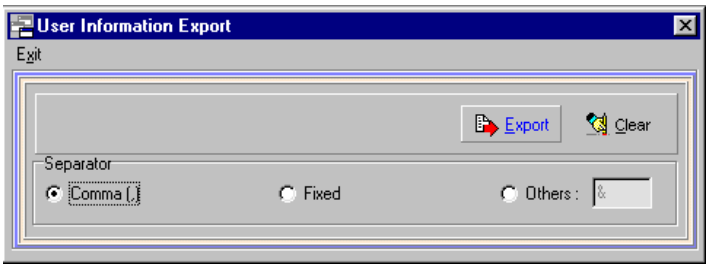
Export User Information Module allows you to export all records in the user database into an ASCII text file. It also provides user a separator option for user to export into the different kind of separator Text file.

Separator option allows you to choose which kind of separator that the ASCII text file has. A Separator Character separates the fields in the ASCII text file. There are 3 kind of separator provided in this option namely *Comma*, *Fixed* and *Other*.

Comma separator separates the field with a comma (,). Eg field1, field2, field3, field4, field5

Fixed separator separates the field using fixed field length. Please refer to the Appendix B: Export Field Table for the field size. Eg field1 field2field3 field4 field5

Other separator separates the field with a user-defined character. Eg. Selected Other: &. The txt file: field1&field2& field3&field4&field5



To Export data,

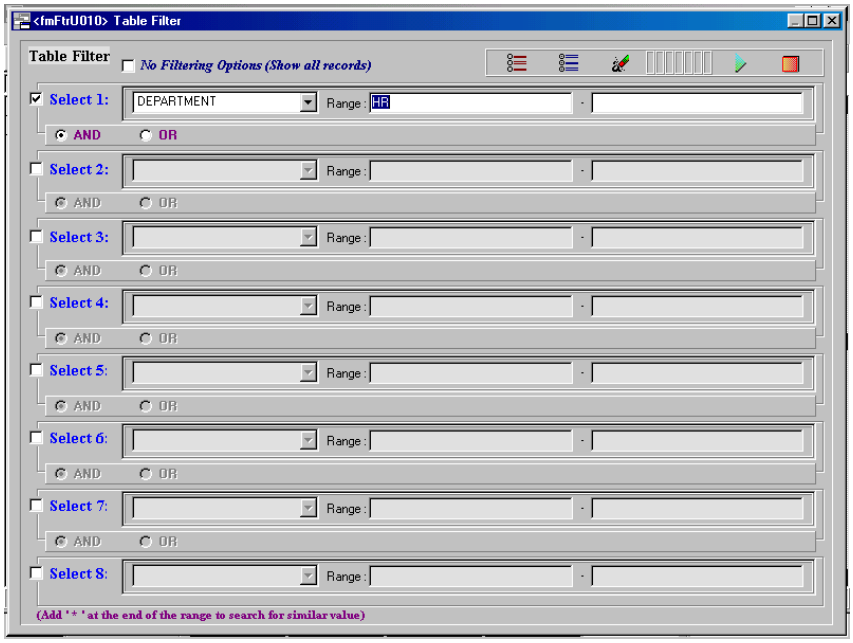
(1) Select which kind of separator you wanted to export to.
(2) Click on the export button to start exporting data.
(3) Key in the directory and the file name when the system prompted.
(4) Wait until a message box shows that the exporting of data has finished.

O. User Records Filtering

When user log on to the application, all the user records will be shown and the log on user can edit or modify all the records shown. If the logon user want to manage only a group of user records, the application provides the feature that allow logon user to set a filter criteria on the records to be shown.

To set filter criteria for the records shown:

(1) Click **Edit** from the top menu and select **Filter** from the drop-down menu or click .



(2) Check the **Select 1** box , select the record field for the filter criteria and enter the range value . As shown in the above example, record with department equal to HR will be filter out and shown for edit or modify.

(3) Click to commit the changes.

NOTE:

The filter criteria are case sensitive.

When the Run button is executed, if no record meet the criteria set, then the filter operation will be canceled and the filter criteria will be disabled.

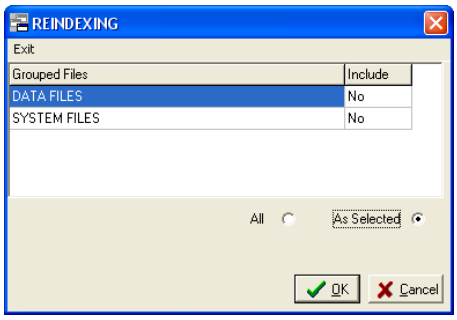
Once the filter criteria are accepted, all subsequent logon user will view/edit records based on the filter criteria.

P. Database Maintenance

The application provides the features like re-index, pack, empty, backup, restore and setting the database path as tasks for database maintenance. Re-index operation should be carried out when the database sorting or filtering function is not working. Packing operation should be carried out when there are many delete operations done on the device user database. This is because a delete operation does not remove records completely from the database until a packing operation is carried out. As for backup operation, users should it carry out periodically. The database being backed up include system database, event logs database, device user database and device users' access right database. All the database files will be compressed into 1 zip file. The default zip file name is YYYYMMDD.zip. (Eg: User did a backup on 08-11-2000, the default backup file name will be 20001108.zip.) If user does not want to name the zip file this way, system allows user to change the zip filename before zipping all the database files. The zip file will be stored in the default backup directory or in the directory specified by the user. Make sure all the database files are closed before backing up. Restore Option allows user to restore all the database files from a zip file. All the files will be restored to Data directory. The restored system files will overwrite the current system files located in the data directory. User needs to select which zip file to restore. This function is only enabled if the logon user has supervisor right.

To re-index the database file:

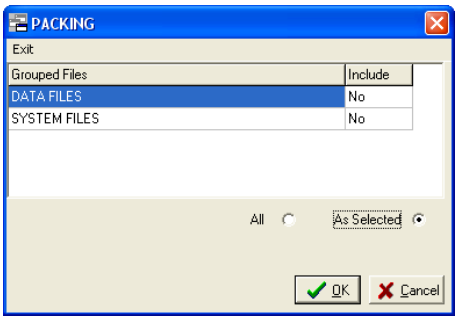
(1) Click **Database** from the top menu and select **ReIndex** from the drop-down menu.
(2) Click on the **Include** column to select the item to be re-indexed.



(3) Click **OK** to start the re-index operation.

To pack the database:

(1) Click **Database** from the top menu and select **Pack** from the drop-down menu.
(2) Click on the **Include** column to select the item to be packed.



(3) Click **OK** to start the packing operation.

To empty the database:

(1) Click **Database** from the top menu and select **Empty** from the drop-down menu.
(2) Click on the **Include** column to select the item to be emptied.
(3) Click **OK** to start the empty operation.

NOTE:

BIOPOINTE DATA FILES include the Device User Database, the Event Logs Database and the Device Users' access right Database.

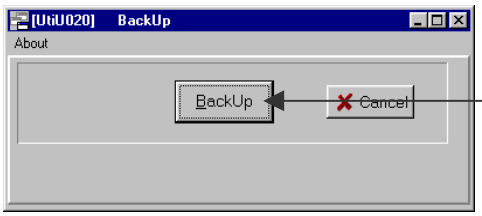
SYSTEM FILES include the Authorized Application Users Database.

WARNING:

The empty operation is an irreversible operation.

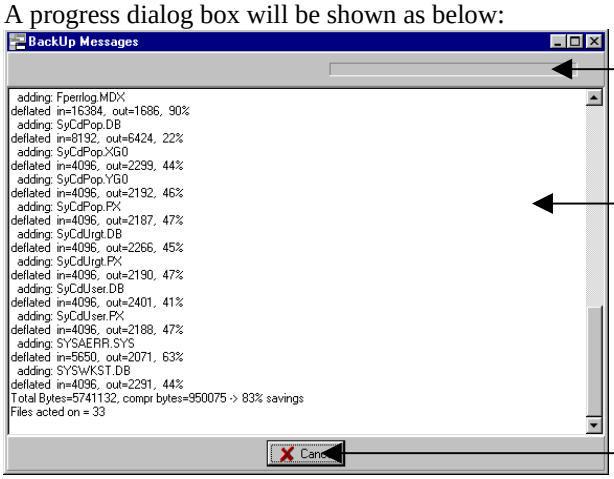
To backup database:

(1) Click **Database** from the top menu and select **Backup** from the drop-down menu.



Click this to backup all the System and Biopointe Data Files. (Please refer to Appendix B for the files to be backup)

A progress dialog box will be shown as below:



Progress bar shows the progress of the files being zipped.

Shows all the files being zipped and its zip status.

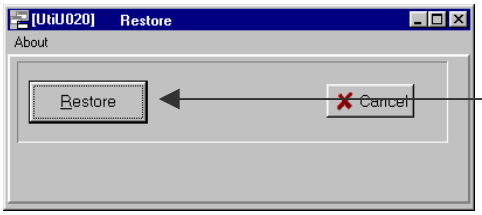
Click this to exit after reading the status.

Users are able to view the zip status and the files being zipped up.

NOTE:
Do a backup occasionally on the database files to help user recover any data loss. Close any opened database file: FPUser.DBF first before backing up the database files.

To restore data:

(1) Click **Database** from the top menu and select **Restore** from the drop-down menu.



Click this to restore all the System and Biopointe Data Files. (Please refer to Appendix B for the files to be backup)

User is able to view the restore status and the files being unzipped to.

WARNING:
The Database files that had been restored overwrite the current existing files in the directory. Once they have overwritten, all the database files cannot be recovered.

Q. Proximity Card Registration

Biopointe device supports the card only, card and fingerprint, card and pin authentication mode. Therefore, this feature allows administrators to retrieve the proximity card information and store into the user record.

To registered a card:

(1) Select the user record to be edited or registered.

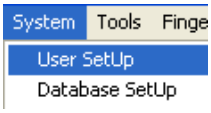
(2) Click  to start the card id capturing process.

(3) Place the proximity card over the proximity card reader.

(4) Once the card reader capture the card id, it will replace the selected user record:USERID field with the card id automatically.

(5) Click on the save(tick) button to save the modified user record's data.

R. Database Setup



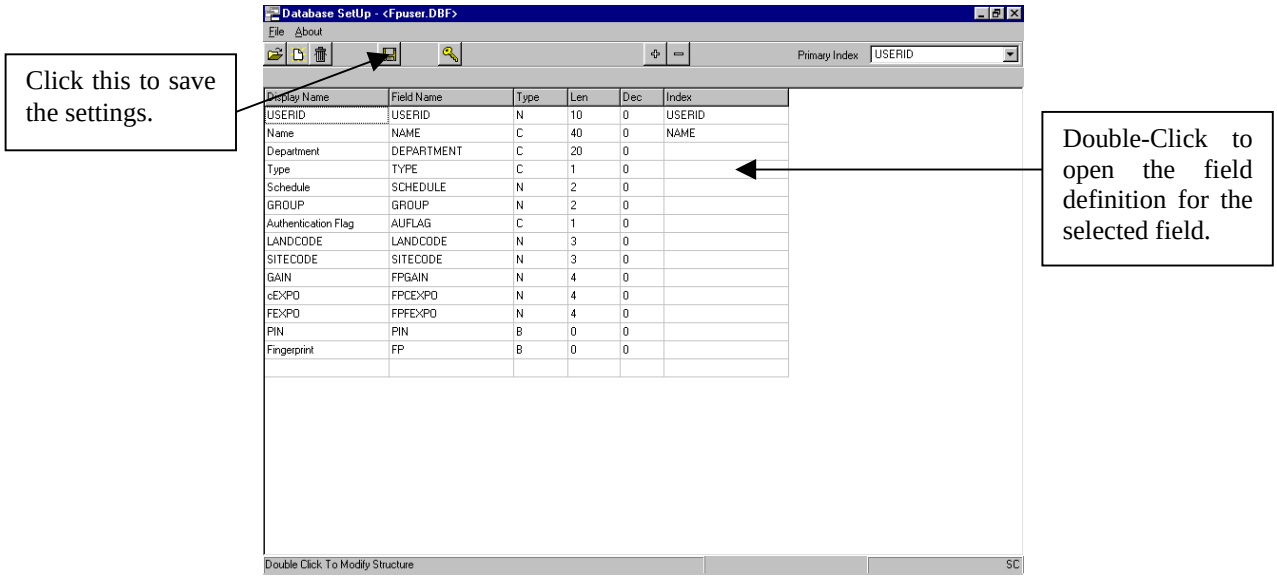
You can create; edit database properties in the Biopointe Central.

Database Setup allows user to change the properties of the displayed database table. User cannot change the field type or add or delete fields. But user can add a counter to a particular field to increment an ID number as user adds a record. User can set the field to invisible during display or user can set the field to viewable but not editable. Or user can add in default values and have a selection list in the table. This Option allows the user to control some of the database field definitions.

NOTE:
Make sure the entire database table is closed. They are no active table in the System before changing the Database Settings.

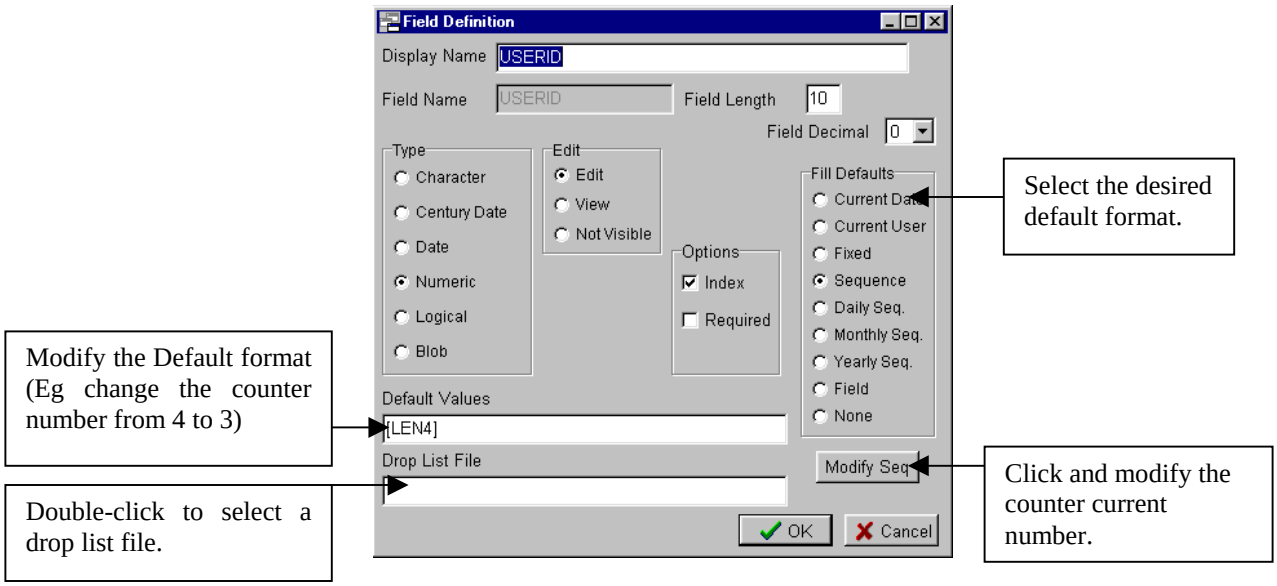
Edit Database Settings,

(1) Close the active database table by selecting File Main Menu, then Close Option.
(2) Open the Database Setup by selecting System Menu, then Database Setup.
(3) Open the FPUSER.DBF from the Database setup File option.



Double-click on each of the field and the Field Definition dialog box will be shown.

The following illustration identifies and names each part of the window. The text explains how each part functions.



Field Definition module allows user to change the display name and the properties of the display field. Beside these, user is able to have a selection list for that particular field by double clicking on the drop list file and select which file from the drop down list. It also provides user ways to set the default values for this field once user adds a record during runtime. Below is a set of default formats that are provided by the system.

Fill default	***Format***	***Description***
Current Date	--	The field will have the current date as default.
Current	--	This field will be set to the log on user as default.
Fixed	User input	Set this field to a fixed default value.
Sequence	[LEN16]	Set this field with a number count with 16 digits.
Daily Seq.	[YYYYMMDD][LEN8]	Set the field with the current date format as yyyymmdd plus a number counter with 8 digits.
Monthly Seq.	[YYYYMM][LEN10]	Set the field with the current month format as YYYYMM plus a number counter with 10 digits.
Yearly Seq.	[YYYY][LEN6]	Set the field with the current year format as YYYY plus a number counter with 6 digits.
Field	[L:FIELDNAME]	Set the field to another Field with the Field ID as FIELDNAME.
None	--	No default settings.

NOTE:
Make sure user click on the "None" Default format before clicking on the desired default format to change the default format.

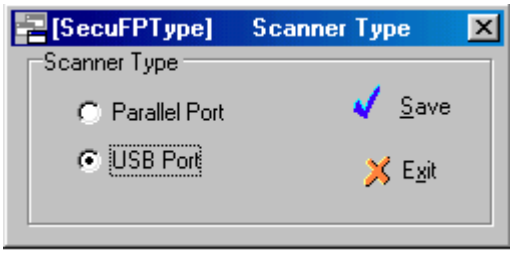
1) Select or modify settings.
2) Click on the **OK** button after modifications are completed. (Note: The values are not saved yet.)
3) After modifying the fields.
4) Click on the **Save** button of the database setup module to save the information.

S. Configure FingerPrint Scanner Type

The Biopointe Central package supports two types of fingerprint scanner for the enrollment process. The default fingerprint scanner used is the parallel port scanner.

To select the fingerprint scanner type:

(1) Select **Scanner Type** from the **Fingerprint Scanner** drop-down menu.



(2) Click on the scanner type and press the **Save** button to commit the changed.

NOTE:

Changes will only take effect after user has exit from the Biopointe Central application.

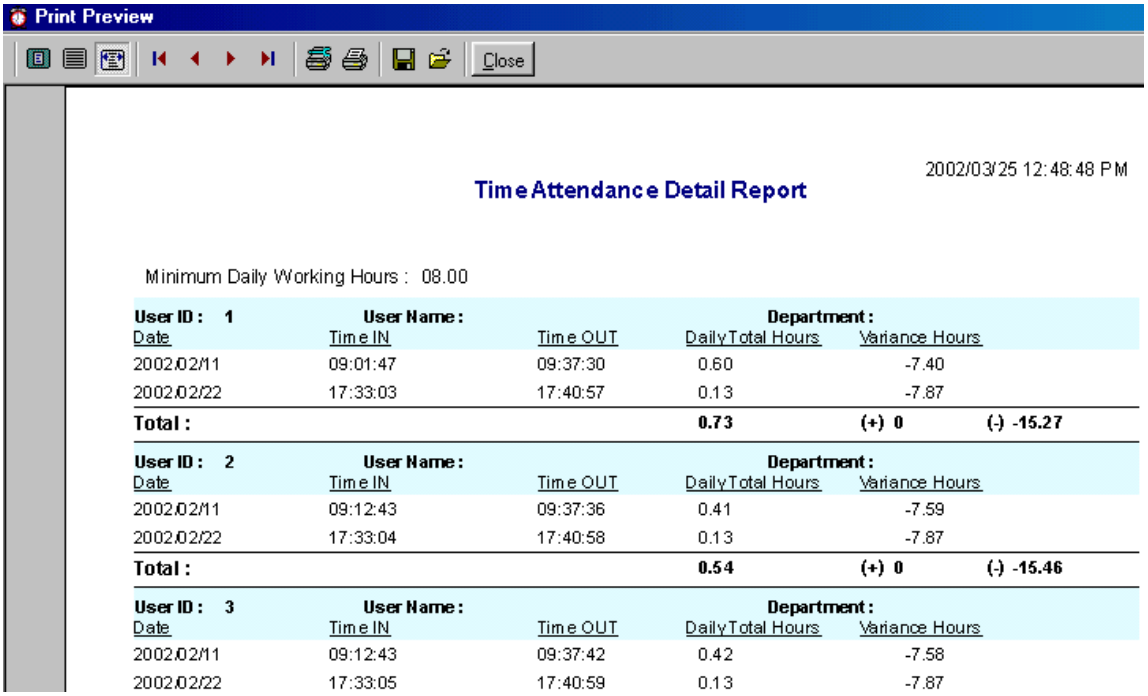
For the USB port scanner, a separate fingerprint scanner driver needs to be installed. For the Win95 system, make sure the USB supplement component is installed before the fingerprint scanner driver.

T. Support Multiple Export Formats for Report

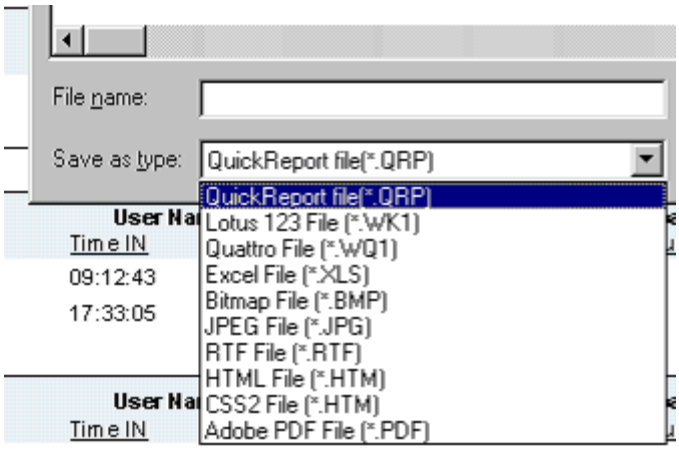
The Biopointe Central Package support the following export formats on report being generated.

(1) Lotus 123 File
(2) Excel File
(3) HTML File
(4) Adobe File
(5) Quattro File
(6) Bitmap File
(7) JPEG File
(8) CSS2 File
(9) RTF File

To export the specific file format from the report :



(a) Press the button.



(b) Select the required format from the drop list and provide the file name.
(c) Press the **Save** button to start the exporting process.

Chapter 5

TROUBLESHOOTING

If you have any difficulty using Biopointe Central, the troubleshooting suggestions in this section should, in most cases, solve the problem. If you still have difficulty after trying these suggestions, contact your authorized reseller for technical assistance.

A. Problems and Solutions

Q1) The STATUS of every device in the table is OFF after polling.

CAUSE	What to do
Wrong communication channel selected.	Check **Communication Channel**.
Wrong COM port selected.	Check **Communication Port Settings**
Wrong DeviceID, IP and PORT settings.	Check with the device for the correct settings.

Q2) During log uploading, a message pops up " '02/08/00' is not a valid date and time. "

CAUSE	What to do
Wrong date format.	Go to Regional Settings Properties in Control Panel. Under Date folder, check **Short date style** is either **dd/mm/yyyy** or **mm/dd/yyyy**.

B. Contacting Customer Support

If you cannot solve your problem with the troubleshooting information in this manual, contact customer support services for assistance.

Keri Systems, Inc. Customer Support

Contact us below:

Keri Systems, Inc.
1530 Old Oakland Road, Suite 100
San Jose, CA 95112 USA
Phone: **800-260-5265**
408-451-2520
FAX: 408-441-0309
Email: techsupport@kerisys.com

Appendix

Appendix A

List of Log Record States

Table **4.6(a)** to **4.6(f)** lists the different class of log records.

Logs can be generally classified into Time-Attendance logs, Failed Transaction logs and Trace logs.

Time-Attendance logs describe the attendance status of the user when they have their fingerprint or card successfully matched at the Reader.

Failed Attempts logs describe the failure status of the user when they did not have their fingerprint or card successfully matched at the Reader.

Trace logs traces specific events (or trace events) that happened at the Reader such as when the door was opened or when the alarm was activated. Trace events are classified into the following types:

- Door and Tamper Switch Events
- Alarm Events
- System Power Up
- Setup Mode Events

Time-Attendance logs are always recorded. On the other hand, Failed Attempts and Trace logs can be disabled so that these events will not recorded even when it happened. Disabling of Failed Attempts and Trace events can only be done at the Reader.

Each type of log is differentiated from the other by an identifier. The identifier, in this release of the library is referenced by the variable, **EnterLeaveStatus** in the log record structure.

Table 4.6(a): Time Attendance

	Identifier (hex)	**Identifier (dec)**	**Description (according to display types)**				
			'Welcome'	**Attd (6 Levels)**	**Attd (2 Levels)**	**Attd / Access**	**Attd / Access V1**
1	0x01	1	Welcome	Attendance In	In	Attendance	-
2	0x02	2	-	Leaving Out	Out	Access Control	Access Control
3	0x03	3	-	Early Leave	-	-	-
4	0x04	4	-	Going Out	-	-	-
5	0x05	5	-	Return	-	-	-
6	0x06	6	-	Others	-	-	-
7	0x07	7	-	-	-	-	In
8	0x08	8	-	-	-	-	Out

Time-Attendance logs will record one of the following events in the table above. This event is selected by the user at the time he or she is using the device. The collection of events follows each display type. There are currently 5 different display types listed above. For example, if the display type, 'Welcome' is selected, there is only one event that can be selected by the user. On the other hand, if the user selects the 'Attd (6 levels)' display type, they can appropriately select from a list of 6 different events before clocking.

Table 4.6(b): Door And Tamper Switch Events (Trace Event)

	Identifier (hex)	Identifier (dec)	Description
1	0x12	18	Door Opened
2	0x18	24	Door Switch Opened
3	0x19	25	Door Switch Closed
4	0x1A	26	Door Override Switch Opened
5	0x1B	27	Door Override Switch Closed
6	0x1C	28	Tamper Switch Opened
7	0x1D	29	Tamper Switch Closed

If trace logs are enabled and the system is used as a Door Access system, the Door Events logs will record events that happened at the door.
For example, the event, [Door Opened] will be recorded when the user has his or her fingerprint or card successfully matched at the Reader.

Note that this event will only be recorded if the **DoorLockUnLock** property is set to <Disabled>, as setting this property to <Disabled> allows the door to be unlocked when matching is successful.

> If this log is recorded, it can be seen upon retrieval of logs that this door event is always recorded following one of the Time-Attendance events, such as [Attendance In]. This is because the Time-Attendance event acts as a request to open the door.

The 2nd and 3rd events, [Door Switch Opened] and [Door Switch Closed] are recorded when the door is locked or unlocked.

The 4th and 5th events, [Door Override Switch Opened] and [Door Override Switch Closed] are recorded when the Door Override Switch is used. When the Override Switch is closed, the door is forced to be unlocked. The Override Switch is always opened under normal conditions.

The 6th and 7th events, [Tamper Switch Opened] and [Tamper Switch Closed] are recorded when the device's casing is being tampered with. The Tamper Switch is always closed under normal conditions. When the device' casing is opened, the Tamper Switch is opened.

Tamper switch sensing can be disabled through the Arm/Disarm selection in the device. When the device is disarmed and the device's casing is opened, the tamper switch events will not be triggered.

Table 4.6(c): Alarm Events (Trace Event)

	Identifier (hex)	Identifier (dec)	Description
1	0x30	48	Alarm Activated
2	0x31	49	Alarm Deactivated
3	0x81	129	Activated Alarm was Acknowledged and Disabled

The event, [Alarm Activated] is recorded whenever the alarm is triggered. The alarm will only be triggered if the **AlarmType** property is NOT <Disabled>.

The alarm can be triggered under a few types of conditions.

For example, the alarm can be triggered if the door switch sensing is found to be different from the **DoorSwitchSense** property. As an example, if the **DoorSwitchSense** property is <Normally Closed> while the connection is opened, then the alarm will be activated. Similarly, if the **DoorSwitchSense** property is <Normally Opened> while the connection is closed, then the alarm will also be activated. When the condition is correct, the alarm stops and the event, [Alarm Deactivated] will be recorded.

In addition, the alarm can also be triggered when the Door Override Switch is closed and when the Tamper Switch is opened.

When the alarm has been activated, it can be acknowledged and stopped by forcing the **AlarmType** property to <Disabled>. In this case, the event, [Activated Alarm was Acknowledged and Disabled] will be recorded.

Notes on Alarm Events Logs and Door / Device Tamper Events Logs :

The following events trigger the alarm:

1. Door Override Switch was closed.
2. Tamper Switch was opened.
3. Door Switch Sensing was found to be reverse.

The first 2 events already have their own event description, namely, [Door Override Switch Closed] and [Tamper Switch Opened]. To avoid generating too many logs, the event, [Alarm Activated] will not be recorded although the alarm will be triggered.

Table 4.6(d): System Power Up (Trace Event)

	Identifier (hex)	Identifier (dec)	Description
1	0x90	144	System Powered Up
2	0x91	145	Startup Error

When the system is successfully powered up, the event, [System Powered Up] will be recorded. When the system fails to power up successfully, the event, [Startup Error] will be recorded.

Table 4.6(e): Setup Mode Events (Trace Event)

	Identifier (hex)	Identifier (dec)	Description
1	0xA0	160	Setup Mode Entered
2	0xA1	161	Setup Mode Exited
3	0xB1	177	A user's fingerprint was changed
4	0xB2	178	A user was added
5	0xB3	179	A user was deleted
6	0xB4	180	A Master was added
7	0xB5	181	A Master was deleted
8	0xC0	192	Device date and time was changed
9	0xC1	193	Door Configuration was changed
10	0xC2	194	Alarm Configuration was changed
11	0xD0	208	A Card/PIN was changed
12	0xD1	209	Door secure – The door is configured to always locked.
13	0xD2	210	Door Unsecured – The door control was set to always unlocked.
14	0xD3	211	Door Normal – The door is configured to be "**Disable**" i.e. Door will unlock upon successful verification.

Setup Mode Events record critical events that happen in the setup mode.

When accessing the setup mode, the event, [Setup Mode Entered] will be recorded. When the user subsequently quits from the setup mode, the event, [Setup Mode Exited] will be recorded.

When the supervisor is in the setup mode, he may add or delete a user, change the date and time, change the alarm configuration or change the door configuration. Each of these events (as listed in the table above) will be recorded.

Table 4.6(f): Failed Attempts

	Identifier (hex)	Identifier (dec)	Description
1	0xE7	231	Failed matching (for users registered with fingerprint)
2	0xE8	232	Failed matching (for users registered with card)
3	0xE9	233	Failed matching (for users registered with card/PIN)
4	0xEA	234	ID not found in device database
5	0xEB	235	Fingerprint match could not be found using partial search
6	0xEC	236	Matching was aborted

Failed Attempts logs comprise the events in the table above. Each event describes the reason for the failure to achieve a successful authentication.

Appendix B

List of Database files

There are two types of database files namely, Biopointe Data Files and System Files. Biopointe Data files are those database files belong to Biopointe Device. System Files are database files that belong to the System. These files will be compressed into 1 zip file and will be stored in the backup directory or user specified directory once user selects the backup option

Types of Database Files :

Type	Database Filename
System Files	SyCdIx.DB
System Files	SyCdIx.PX
System Files	SyCdIx.XG0
System Files	SyCdIx.YG0
System Files	SyCdIxdt.DB
System Files	SyCdIxdt.PX
System Files	SyCdLog.DB
System Files	SyCdLog.PX
System Files	SyCdPop.DB
System Files	SyCdPop.PX
System Files	SyCdPop.XG0
System Files	SyCdPop.YG0
System Files	SyCdUrgt.DB
System Files	SyCdUrgt.PX
System Files	SyCdUser.DB
System Files	SyCdUser.MB
System Files	SyCdUser.PX
System Files	SysWkSt.db
Biopointe Data Files	FPDev.DBF
Biopointe Data Files	FPDev.MDX
Biopointe Data Files	FPDevCon.DBF
Biopointe Data Files	FPDevCon.MDX
Biopointe Data Files	FPDevGrp.DBF
Biopointe Data Files	FPDevGrp.MDX
Biopointe Data Files	FPDevLog.DB
Biopointe Data Files	FPDevLog.PX
Biopointe Data Files	FPDevUsr.DBF
Biopointe Data Files	FPDevUsr.MDX
Biopointe Data Files	Fperrlog.DBF
Biopointe Data Files	Fperrlog.MDX
Biopointe Data Files	FpGroup.DBF
Biopointe Data Files	FpGroup.MDX
Biopointe Data Files	FPSchUsr.DBF

Biopointe Data Files	FPSchUsr.MDX
Biopointe Data Files	FPUplTem.DBF
Biopointe Data Files	FPUplTem.DBT
Biopointe Data Files	FPUplTem.MDX
Biopointe Data Files	FPUser.ACD
Biopointe Data Files	FPUser.DBF
Biopointe Data Files	FPUser.DBT
Biopointe Data Files	FPUser.MDX

Log Field Table

Definition	Size	Description
Device ID	3	ID of the device. All devices connected in the chain should have unique ID
LogDate	-	Date of the Log record. (According to the System short date format)
LogTime	8	Time of the Log record.
UserID	10	User ID or Card ID for user accesses through card/fingerprint. For log record relate to the system configuration, the ID will be zero.
LogType	3	Log record status value. Please refer to Appendix A for all the supported status.
JobCode	7	This value is valid only if Work in Progress Mode in the Biopointe Device is enabled.
JobStage	2	This value is valid only if Work in Progress Mode in the Biopointe Device is enabled
JobSubStage	2	This value is valid only if Work in Progress Mode in the Biopointe Device is enabled
Department	20	The department that is located in the user database. This is only valid for the full version of the Biopointe Central.
Description	150	This is the description of the log record status.

Export User Information Table

Definition	Size
User ID	10
User Name	40
Department	20
Link ID	10
Type	1
Authenication Flag	1

Appendix C

List of Function Status and Reader Error Code

This section describes the Function Status and Reader Error Codes. The function status is that returned by a function. A value of zero indicates that the function was executed successfully, while a non-zero value indicates that that the function had failed.

If the function status is FAL_RECEIVED, it indicates that the Reader has responded with a Reader Error Code indicating why the operation had failed. The table of Reader Error Codes can then be referred to.

Table 6(a): List of Function Status (For serial communication)

	Constant	Value	Description
1	COM_PORT_INIT_FAIL	0xC0	Fail to initialize the communication port
2	COM_PORT_WAS_NOT_INITIALIZED	0xC1	Before commands can be sent, the Com Port has to be initialized
3	PURGE_COMM_FAILED	0xC2	Fail to clear the receive and transmit buffers for the Com Port
4	SEND_CMD_FAILED	0xC3	Fail to execute sending of command
5	RECEIVE_DATA_FAILED	0xC4	Fail to execute receiving of data
6	INVALID_REPLY	0xC5	Received packet was not expected although the footer and header were properly received, and the checksum was correct
7	RECEIVE_FOOTER_WRONG	0xC6	Expected ETX, indicating the end of a packet, was not received
8	RECEIVE_HEADER_WRONG	0xC7	Expected STX, indicating the start of a packet, was not received
9	DEVICE_ID_MISMATCH	0xC8	Host sends a command to Device A. Packet received indicates reply was from Device B. (Indicate that the Host-received reply was not from the Reader the Host had earlier sent a command to).
10	HOST_ID_MISMATCH	0xC9	Host receives a packet from Reader that is addressed to another Host. If there is only one Host in the system, this may indicate a corrupted packet.
11	CRC_MISMATCH_AT_HOST	0xCA	CRC performed and derived at the Host side for the received packet does not match that of the received packet
12	ZERO_BYTE_RECEIVED	0xCB	No data was received from Reader for command that was sent out (time-out).
13	FAL_RECEIVED	0xCC	Error Code received from Reader. Check the returned Error Code.
14	NAK_RECEIVED	0xCD	Not-Acknowledge received from Reader (Reader is busy)
15	FAIL_TO_LOAD_CONVERT_DLL	0xCE	Fail to load the DLL needed to convert the template to proper format

16	FAIL_TO_CONVERT_TEMPLATE	0xCF	Fail to convert template to proper format
17	ABORT_FINGER_CAPTURE	0xD0	Fingerprint capture was aborted
18	SCHEDULE_NUMBER_NOT_FOUND	0xD1	Specified schedule number was not found
19	CALENDAR_YEAR_NOT_FOUND	0xD2	Specified calendar year was not found
20	INVALID_PARAMETER	0xD3	An invalid parameter was passed in to a function
21	INVALID_COM_PORT	0xD4	Invalid Com port number
22	INVALID_BAUD_RATE	0xD5	Invalid baud rate
23	INVALID_PARITY	0xD6	Invalid parity
24	INVALID_DATA_BIT	0xD7	Invalid number of data bits
25	INVALID_STOP_BIT	0xD8	Invalid number of stop bits
26	COMMAND_IN_PROGRESS	0xD9	Command in progress. This error is obtained if one command is tried to be executed while another is in progress
27	NO_SCHEDULE_SETS_TO_UPLOAD	0xDA	No schedules to upload from the device
28	FAIL_TO_INIT_MODEM	0xDB	Modem could not be initialized
29	MODEM_COMMAND_FAIL	0xDC	A command to the modem could not be carried out successfully
30	NO_RESPONSE_FROM_MODEM	0xDD	Modem did not response to commands
31	FAIL_TO_CONNECT	0xDE	Unable to connect to a remote dialing location. (Possible reason is for example, a carrier could not be established with the remote modem)
32	LINE_BUSY	0xDF	Unable to dial to remote modem due to the line being busy
33	NO_ANSWER	0xE0	Unable to connect to remote dialing location due to there being no answer from remote modem
34	NO_DIAL_TONE	0xE1	There was no dial tone in the local modem. Possible reason is that the telephone line was not connected to the modem
35	MODEM_IS_NOT_ONLINE	0xE2	The modem was not online.
36	WIEGAND_FORMAT_NOT_SUPPORTED_BY_DEVICE	0xE3	The Wiegand Format specified during setting of device properties command is not supported by the firmware of the device used.
37	RETURN_CMD_MISMATCH	0xE4	-
38	TOO_MANY_CALENDAR_YEARS_TO_DNLOAD	0x90	The max calendar years to download have exceeded the limited of 2.
39	NO_CALENDAR_YEARS_CREATED_AT_HOST	0x91	No calendar years created at Host system.
40	NO_CALENDAR_DATA_TO_UPLOAD	0x92	-
41	NO_SCHEDULE_SETS_CREATED_AT_HOST	0x93	No Schedule sets were created at the Host system.
42	EXCEPTION_GENERATED	0x95	Errors during file access
43	FILE_NOT_FOUND	0x96	Errors during file access
44	ERROR_FILE_READ	0x97	Errors during file access
45	ERROR_FILE_WRITE	0x98	Errors during file access
46	ERROR_FILE_CREATE	0x99	Errors during file access

47	INVALID_SCHEDULE_CNT_IN_INI_FILE	0x9a	There was a invalid entry in the Sch.ini file
48	GENERAL_FILE_SYSTEM_ERROR	0x9b	Errors during file access
Template On Card Function Status			
1	NO_CARD	0xE5	No card was presented on the card reader
2	WRONG_KEY	0xE6	A wrong key was used to access the card
3	WRONG_SIGNATURE	0xE7	The card does not have a signature personalized by Keri Systems, Inc.
4	FAIL_WRITEVERIFY	0xE8	Fail Write verify
5	FAIL_WRITE	0xE9	Fail to write to card
6	FAIL_TO_READ_KEY	0xEA	Unable to read the system key
7	FAIL_TO_INIT_HARDKEY	0xEB	Unable to initialize the HardKey
8	FAIL_TO_LOAD_COMP_LIB	0xEC	Unable to load the component library
9	FAIL_TO_GET_COMP_FN	0xED	Unable to load the component function
10	TEMPLATE_NON_EXIST	0xEE	User request for a template from the card that does not exist.
11	FAIL_LOAD_CONVERT_LIB	0xEF	Fail to load covert library
12	WRONG_CARDTYPE	0xF0	The card type the user selected while doing an verify is not the same as the actual card type of the card.
13	WRONG_PIN	0xF1	The pin the user tries to verify with is not the actual pin registered in the card.
14	UNDEFINE_USER_MASTER	0xF2	Attempt to register a card with an invalid master/user type selection
15	FAIL_TO_RESET_READER	0xF3	Command to reset the reader (Mifare) did not execute successfully.
16	USER_ID_EXCEED_LIMIT	0xF4	-
17	UNKNOWN_ERROR	0xF5	Unknown error
18	READER_RETURN_ERRORCODE	0xF6	An error code has been returned by the reader (Legic)
19	CMD_EXEC_FAIL	0xF7	Fail to execute CMD
20	INVALID_DATE	0xF8	An invalid expiry date was selected while trying to set.
21	INVALID_CALENDAR_YEAR_TO_DOWNLOAD	0xF9	The calendar year to download is invalid.

Table 6(b): List of Function Status (For TCP/IP communication)

	Constant	Value	Description
1	COMMAND_SUCCESS	0	Command was successful
2	COMMAND_IN_PROGRESS	0xA0	Command in progress
3	CONNECT_IN_PROGRESS	0xA1	Connection in progress
4	COMMAND_TIMEOUT	0xA2	Command timeout
5	CONNECTION_FAIL	0xA3	Connection fail
6	DEVICE_CONNECTED	0xA4	Device was connected
7	DEVICE_DISCONNECTED	0xA5	Device was disconnected

8	INVALID_PARAMETER	0xA6	An invalid parameter was passed in to the function
9	RECEIVE_FOOTER_WRONG	0xA7	Expected ETX, indicating the end of a packet, was not received
10	RECEIVE_HEADER_WRONG	0xA8	Expected STX, indicating the start of a packet, was not received
11	**FAL_RECEIVED**	0xA9	Error code received from Reader
12	NAK_RECEIVED	0xAA	Not-Acknowledge received from Reader (Reader is busy)
13	SCHEDULE_NUMBER_NOT_FOUND	0xAB	Specified schedule number was not found
14	CALENDAR_YEAR_NOT_FOUND	0xAC	Specified calendar year was not found
15	ABORT_FINGER_CAPTURE	0xAD	Fingerprint capture was aborted
16	FAIL_TO_LOAD_CONVERT_DLL	0xAE	Fail to load the DLL needed to convert the template to proper format
17	FAIL_TO_CONVERT_TEMPLATE	0xAF	Fail to convert template to proper format
18	CRC_MISMATCH_AT_HOST	0xB0	CRC mismatch of the Host received packet
19	NO_SCHEDULE_SETS_TO_UPLOAD	0xB1	No schedules to upload from the device
20	INVALID_REPLY	0xB2	Received packet was not expected for the command executed although the packet was received without any errors.
21	WIEGAND_FORMAT_NOT_SUPPORTED_BY_DEVICE	0xB3	The Wiegand Format specified during setting of device properties command is not supported by the firmware of the device used.
22	INVALID_CALENDAR_YEAR_TO_DOWNLOAD	0xB4	The calendar year to download is invalid.
23	TOO_MANY_CALENDAR_YEARS_TO_DNLOAD	0x90	The max calendar years to download have exceeded the limited of 2.
24	NO_CALENDAR_YEARS_CREATED_AT_HOST	0x91	No calendar years created at Host system.
25	NO_CALENDAR_DATA_TO_UPLOAD	0x92	-
26	NO_SCHEDULE_SETS_CREATED_AT_HOST	0x93	No Schedule sets were created at the Host system.
27	EXCEPTION_GENERATED	0x95	Errors during file access
28	FILE_NOT_FOUND	0x96	Errors during file access
29	ERROR_FILE_READ	0x97	Errors during file access
30	ERROR_FILE_WRITE	0x98	Errors during file access
31	ERROR_FILE_CREATE	0x99	Errors during file access
32	INVALID_SCHEDULE_CNT_IN_INI_FILE	0x9a	There was a invalid entry in the Sch.ini file
33	GENERAL_FILE_SYSTEM_ERROR	0x9b	Errors during file access
34	ERROR_FILE_SIZE	0x9c	Error during file access
35	FAIL_TO_READ_KEY	0xEA	Unable to read the system key

The Reader returns this list of error codes (Table 6(b)) if the command fails.

Table 6(c): List of Error Codes

	Constant	Value	*Description*
1	OK	0x00	No error, successful
2	NOT_OK	0x01	General Reader error
3	VALID_DATA	0x02	-
4	NO_VALID_DATA	0x03	-
5	CRC_MISMATCH	0x04	CRC check fail
6	PORT_ID_MISMATCH	0x05	Device ID mismatch
7	INVALID_CMD	0x06	Command was invalid
8	ERROR_IN_READING_FLASH	0x07	Error in reading from the flash
9	ERROR_IN_WRITING_FLASH	0x08	Error in writing to the flash
10	DATA_MISCOMPARE	0x09	Mismatch when data read back from flash is different from that just written
11	ALL_TEMPLATE_SLOTS_FILLED	0x0A	User has enrolled all 3 fingerprints
12	WRONG_FINGER_PRINT_SEQ	0x0B	Expected minutiae (either 1 or 2) was not received by the Reader during a download operation
13	INCOMPATIBLE_PKT	0x0C	Subsequent packet from Host was not the expected one (during a handshaking transmission)
14	FLASH_IS_FULL	0x0D	Flash storage limit has been reached
15	INVALID_TEMPLATE_NUM	0x0E	Fingerprint number to enroll can only be 1, 2 or 3. (Invalid parameter)
16	REQ_TEMPLATE_NUM_IS_NOT_FILLED	0x0F	The requested fingerprint number has not been enrolled
17	USER_NOT_FOUND	0x10	User was not found in the Reader's database
18	SEQ_NO_BEYOND_RANGE	0x11	Sequence number (or record number) used to query User's ID or Master's ID has exceeded either the maximum number of Users or Masters
19	RECORD_ALREADY_A_MASTER	0x12	-
20	RECORD_ALREADY_A_USER	0x13	-
21	SCHEDULE_NUMBER_NOT_WRITTEN	0x14	Schedule number was not assigned to User
22	GROUP_NUMBER_NOT_WRITTEN	0x15	Group number was not assigned to User
23	AUX_DEVICE_NOT_SUPPORTED	0x16	Auxiliary device is not found in the device
24	YEAR_NOT_FOUND	0x17	Requested year (to upload) was not found in the Reader
25	INVALID_TEMPLATE_COUNT	0x18	-
26	AUTHENTICATE_FAILED	0x19	Authenticating the Master fingerprint fail
27	ERROR_IN_WRITE_OR_ERASE_EEPROM	0x1A	Error in writing or erasing the EEPROM

28	TIME_OUT	0x1B	Reader has timed-out while waiting for a packet from Host
29	DATA_BEING_PURGED	0x1C	Data from Host has been purged. May due to an incomplete packet received
30	NO_RECORDS_TO_SEND	0x1D	Reader has no more log records to sent
31	INVALID_SCHEDULE_NUMBER	0x1E	Schedule number assigned to User was invalid (ie. it has the value of either 0 or 0xFF)
32	SCHEDULE_SET_NOT_WRITTEN	0x1F	The Schedule Set was not written yet
33	GROUP_DETAILS_NOT_WRITTEN	0x20	The Group Details Set was not written yet
34	EEPROM_DATA_MISCOMPARE	0x21	Data read back from EEPROM is different from that just written
35	ID_NOT_USED	0x22	-
36	ID_USED	0x23	-
37	INCONSISTENT_MASTER_OR_USER_TYPE	0x24	A user is already enrolled with a status indicating either a USER or MASTER, but subsequent 2nd or 3rd fingerprint enrolment tries to enroll a different status
38	ERROR_WRITING_TO_ENGINE	0x25	Error writing to the fingerprint engine
39	ERROR_READING_FROM_ENGINE	0x26	Error reading from the fingerprint engine
40	ERROR_IN_DELETING_RECORD_FROM_ENGINE	0x27	Error in deleting a record from the fingerprint engine
41	ERROR_IN_DELETING_ALL_REC_FROM_ENGINE	0x28	Error in deleting all records from the fingerprint engine
42	ERROR_IN_REC_CNT_AFTER_OPS	0x29	-
43	ERROR_IN_GETTING_REC_CNT	0x2A	Error in getting the record count from the fingerprint engine
44	NO_TEMPLATEID_EXIST_FOR_USER	0x2B	User has not enrolled any fingerprints
45	INVALID_TEMPLATE_ID	0x2C	Template ID assigned was zero
46	CURRENT_DATE_OUTSIDE_VALIDITY_PERIOD	0x2D	-
47	SPECIFIED_GROUP_NOT_FOUND	0x2E	-
48	INVALID_MASTER_USER_FLAG	0x2F	Master User flag passed in during enrolment is invalid
49	INVALID_SEQUENCE_NUMBER	0x30	Sequence number passed in during querying of User's ID or Master's ID was zero
50	MAX_SCHEDULE_SETS_COUNT_EXCEEDED	0x31	Number of schedule sets to download has exceeded the maximum allowed
51	ACCESS_DENIED_OUTSIDE_SCHEDULE	0x32	-
52	INVALID_DAY_TYPE	0x33	-
53	TIME_ZONE_INFO_NOT_WRITTEN_FOR_DAY_TYPE	0x34	-
54	SPECIFIED_SCH_SET_NOT_IN_STORE	0x35	-
55	INVALID_OPERATION_MODE	0x36	-
56	INVALID_MAX_FINGERPRINT	0x37	-

57	INVALID_PIN_NUMBER	0x38	PIN number must not be zero during enrolment
58	NO_PIN_WRITTEN	0x39	No PIN was registered for this User
59	ERROR_ATTEMPT_TO_USE_PIN_WITH_FP	0x3A	User was already fingerprint-enrolled
60	PIN_ALREADY_ASSIGNED_TO_USER	0x3B	User was already Card/PIN enrolled
61	CAPACITY_OF_FP_ENGINE_REACHED	0x3C	Capacity of fingerprint engine has reached
62	WIEGAND_CODES_MISCOMPARE	0x3D	Mismatch detected during comparison of the Wiegand codes
63	WIEGAND_CODES_NOT_WRITTEN	0x3E	Wiegand codes has not been written yet for Card user
64	INVALID_PARAMETER_SENT_TO_DEVICE	0x3F	An invalid parameter was passed in and sent to the Reader
65	AUTHENTICATED_SEQUENCE_WAS_NOT_STARTED	0x40	The authentication sequence has not been initiated yet
66	AUTHENTICATED_SEQUENCE_HAS_EXPIRED	0x41	The authenticated sequence has already expired by its timeout.
67	LOG_DATE_NOT_FOUND	0x42	When requesting for log record to be sent starting from a specific date, this date was not found.
68	GAIN_AND_EXPOSURE_NOT_WRITTEN	0x43	The engine gain and exposure values for the particular user were not written.
69	WRITE_FLASH_PROHIBITED	0x44	Not permitted to write to the data flash because it has already been written. Used for log records only.
70	LOG_DATE_TO_SET_LATER_THAN_LAST_SENT_DATE	0x45	This error will occur during pointing the log upload pointer to a specific date, if the desired date is later the date of the last record sent.
71	JOB_CODE_DOES_NOT_EXIST	0x46	-
72	EXCEPTION_LIST_FULL	0x47	-
73	NO_JOB_RECORDS_IN_DEVICE	0x48	-
Specific errors related to the Fingerprint Engine			
1	M2ERROR_FLASH_OPEN	0x51	Command from main memory or host to access flash memory failed due to problem(s) in flash memory
2	M2ERROR_SENSOR_OPEN	0x52	Failed due to optical unit
3	M2ERROR_REGISTER_FAILED	0x53	Registering fingerprint failed
4	M2ERROR_VERIFY_FAILED	0x54	Verifying fingerprint failed
5	M2ERROR_ALREADY_REGISTERED_USER	0x55	UserID already exists
6	M2ERROR_USER_NOT_FOUND	0x56	UserID is not found in FP database
7	M2ERROR_INVALID_PASSWORD	0x57	Password of Master is incorrect
8	M2ERROR_TIMEOUT	0x58	Failed to capture fingerprint in preset time
9	M2ERROR_DB_FULL	0x59	FP database has insufficient space to enroll a new user
10	M2ERROR_DB_WRONG_USERID	0x5A	Failure in removing or verifying unregistered user

11	M2ERROR_DB_NO_DATA	0x5B	Database has no data
12	M2ERROR_EXTRACT_FAIL	0x5C	Failed capturing feature points of fingerprint
13	M2ERROR_MEMALLOC_FAILED	0x5D	Memory allocation failed
14	M2ERROR_SERIAL_OPEN	0x5E	Communication with main Controller and Host through serial port failed
15	M2ERROR_NOT_IMPLEMENTED	0x5F	Function not installed
16	M2ERROR_FUNCTION_FAILED	0x60	Call of function failed
17	M2ERROR_INSUFFICIENT_DATA	0x61	Received data size does not match the size defined in ExtraData
18	M2ERROR_FLASH_WRITE_ERROR	0x62	Writing in Flash Memory failed
19	M2ERROR_FLASH_READ_ERROR	0x63	Reading Flash Memory failed
20	M2ERROR_INVALID_PARAM	0x64	Parameter of packet is invalid
21	M2ERROR_MASTERFP_NOT_FOUND	0x65	Fingerprint of Master cannot be found (occurs when trying to proceed without Master registration)
22	M2ERROR_MASTERCOUNT_EXCEED	0x66	The number of master exceeds 5. No more than 5 masters can be registered
23	M2ERROR_AUTHENTICATE_FAIL	0x67	Verification of Master failed
24	M2ERROR_FPCHANGE_FAILED	0x6A	Changing fingerprint failed
25	M2ERROR_IDENTIFY_FAILED	0x6B	No fingerprint in database identifies fingerprint on input window
26	M2ERROR_FLASH_ERASE_ERROR	0x6C	Failed to clear flash memory
27	M2ERROR_VERIFY_FAKE	0x6D	Fingerprint to be verified is the same as previous fingerprint. Occurs when the fingerprint is input continually without taking off once.
28	M2ERROR_TIME_ERROR	0x6E	It appears when error for time setting happens
29	M2ERROR_SEARCHING_FOR_IDENTIFY	0x6F	FP engine sends ACK with error whenever searching 100 user inside for identity (in case taking long searching time). This value does not mean error. Host should wait next ACK when getting ACK with error
30	M2ERROR_INVALID_USERDATA_SIZE	0x70	The size of data is exceeded for the user portion when recording the value for host in user portion
31	M2ERROR_INVALID_USERDATA_ADDRESS	0x71	The portion of data is exceeded for user portion when recording the value for host in user portion
32	M2ERROR_MUST_BE_SET_DATA_LENGTH	0x72	The size of user portion for host is not set
33	M2ERROR_DUPLICATE_TEMPLATE	0xF5	Duplicate template
34	M2ERROR_TIMEOUT	0xFA	Timeout by the FP Engine
35	M2ERROR_COMMAND_MISMATCH	0xFB	Command mismatch between transmitted command and received reply
36	M2ERROR_RX_LENGTH_ERROR	0xFC	Received packet length error
37	M2ERROR_ACK_TIME_OUT	0xFD	ACK time-out

38	M2ERROR_CHECKSUM_ERROR	0xFE	Checksum error
39	M2ERROR_UNKNOWN_COMMAND	0xFF	Command was not recognized