[INSTALLING THE M2SYS BIOMETRIC SCANNING SYSTEM]

1 TABLE OF CONTENTS

2 FIGURES INDEX

Installing the M2SYS BIOMetric Scanning System

3 INTRODUCTION

Fellowship Technologies has tested and verified the functionality of the M2Sys Bio-SnapON fingerprint scanning technology with Fellowship One Check-in. This document will outline the steps for configuring the hardware, the software, and for using it with Fellowship One Check-in.

Figure 1- Fingerprint Scanning Process

The M2Sys System is a third-part application which means that the software and fingerprint data exists outside of Fellowship One. The way to best understand this is to follow the steps of a Check-in process using Fellowship One Check-in and the M2Sys system.

Step 1- Church Member approaches Check-in Station and places their finger on the Fingerprint scanner.

Step 2- Fellowship One Check-in running in the foreground waiting for a check-in.

Step 3- The Scanner sends the fingerprint to the M2Sys Client that is running in the background on the same computer. The church member sees only Check-in on the screen.

Step 4- The M2Sys Client sends the fingerprint to the M2Sys server which holds the database of IDs and fingerprint information. This server is the server software that can be running on the same Check-in computer, another Check-in computer, or a central server.

Step 5- The server sends the ID that is assigned to the fingerprint back to the M2Sys client.

Step 6- The M2Sys Client passes the ID to Check-in.

Step 7- Check-in sends the ID to the Fellowship One database which confirms the ID and Check-in information.

Step 8- The Check-in label(s) prints.

In the above steps, the process only took seconds.

There are a few key items to be aware of:

1. The Fingerprint Biometric data is not stored in Fellowship One but instead is stored in a local database.
2. The M2Sys local database can run on a Check-in computer, a non-Check-in computer connected to the network, another Check-in computer, or a central server.
3. There needs to be only one M2Sys "server" computer on the network.
4. The local M2Sys database needs to be backed up regularly to avoid loss of data.
5. There is a process of matching IDs and capturing the fingerprints that has to occur before the system is fully configured for use.
6. The choice needs to be made as to whether the requirement for storing Biometric information will be based on two fingers or one. The two finger option means that when the fingerprints are captured during the Biometric setup process that the person being configured for fingerprint scanning will need to scan two fingers. This means that they can use two fingers to Check-in or that one finger from both parents can be used to Check-in. This is advisable. One finger is the other option but is limiting when used with Check-in.

4 HARDWARE OPTIONS

There are two primary options for the fingerprint scanning hardware. Our primary recommendation is the M2-S model. The M2-Easyscan is a lower cost scanner but is less ergonomic, but does work well otherwise. Both scanners mentioned connect via USB.

Figure 2 - M2-S

4.1.1 The M2-S

The M2-S ergonomic design forces good finger placement with each fingerprint scan. It is currently supported only on 32-bit Microsoft Windows.

Figure 3 - M2-Easyscan

4.1.2 M2-Easyscan

The M2-Easyscan is a good lower cost option. Its design is less ergonomic but it still works well. The M2-Easyscan supports both 32-bit and 64-bit Microsoft Windows.

Figure 4 - M2-Paln Vein Reader

4.1.3 M2-Easyscan

The M2-PalmVein palm vein scanner from M2SYS uses a near-infrared light to create a "vein map" of the users palm to perform highly accurate and secure biometric recognition.

5 INSTALLATION

There are two parts to the installation – the hardware and the software.

The M2Sys client software will run on the workstation that is also running Fellowship One Check-in.

The M2Sys server software can run on the same Check-in computer, a non-Check-in computer connected to the network, another Check-in computer, or a central server.

It is also extremely important to be sure that there is a way to back-up the M2Sys Server database since this is the only place that the Fingerprint Biometric information is stored.

5.1 SOFTWARE INSTALLATION AND CONFIGURATION

The software installation is the same regardless of the location of the M2Sys Server.

Once the M2Sys software is purchased from our vendor POS Systems, an email with the download links and the process to acquire the Server license will set to you.

5.1.1 M2Sys Server Installation and Configuration

The M2Sys Server software will be installed on one computer that will host the M2Sys Biometric database.

It is important to install the 64-bit or 32-bit version on the appropriate hardware/operating system platform.

The M2Sys Server can use an access formatted database for most configurations. It will be an Access datafile that will be used by the M2Sys server. Microsoft Access is not required. There is also an option for higher capacity options like Microsoft SQL server, MYSQL server, and Oracle Database Server for high capacity larger installations when speed is critical to support large numbers of finger print scanning stations (100s).

5.1.1.1 Server Installation

1. Run the applicable M2Sys Server installer.

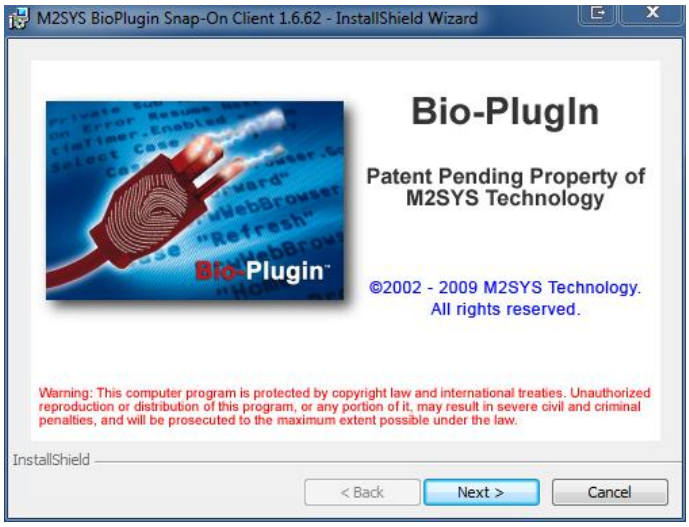

Figure 5 - License Agreement

2. Click Next at the Bio-Plugin Intro Screen.

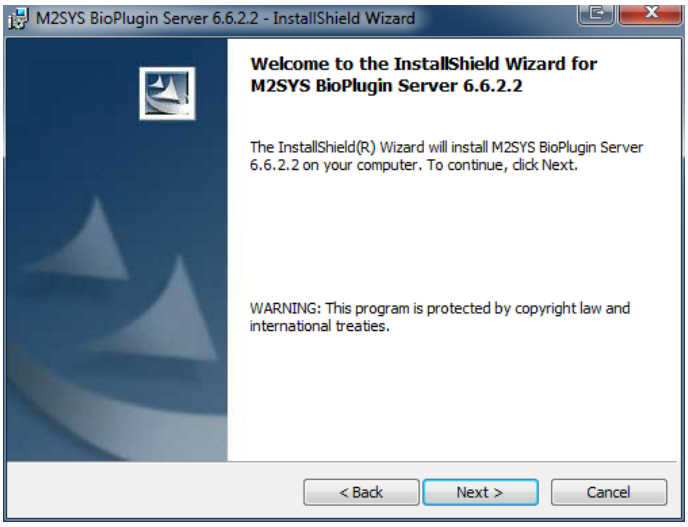

Figure 6 - Welcome Screen

3. Click Next at the Welcome screen.

Figure 7 - License Agreement

4. Accept the license Agreement.
5. Click Next.

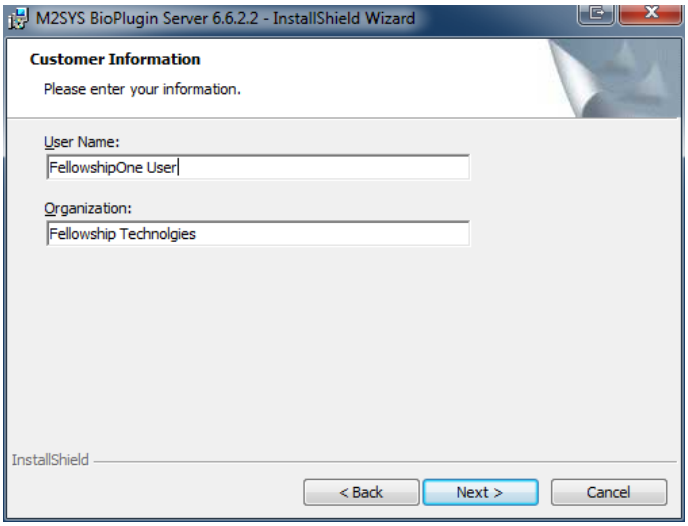

Figure 8 - Customer Information

6. Enter your name and Organization name.
7. Click Next.

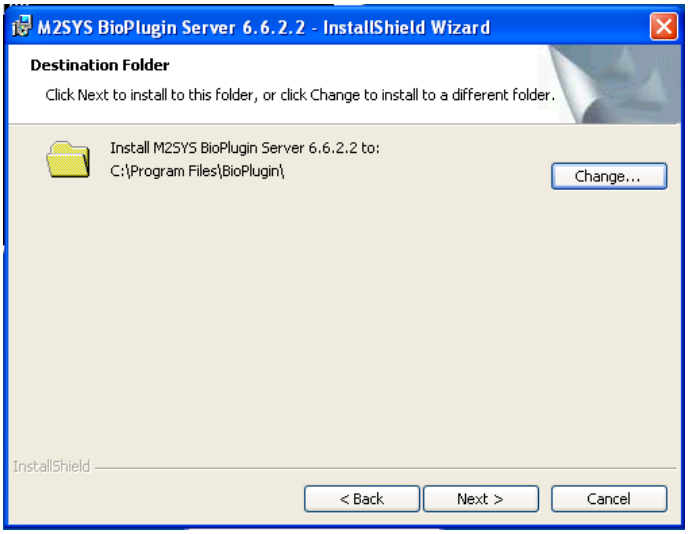

Figure 9 - Driver Install

8. Accept the default location for the server files. You can change it if required by selecting Change.
9. Click Next.

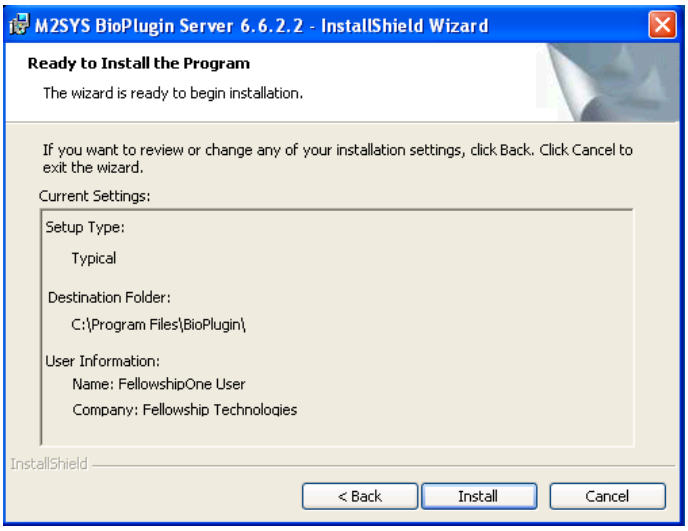

Figure 10 - Ready to Install

10. This window will show the setting that you configured. Click Next.

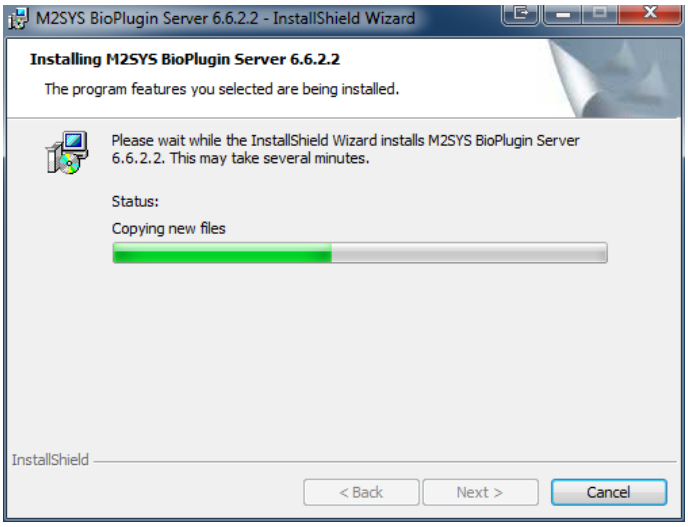

Figure 11 - File Load

11. The Server application will begin to install the files.

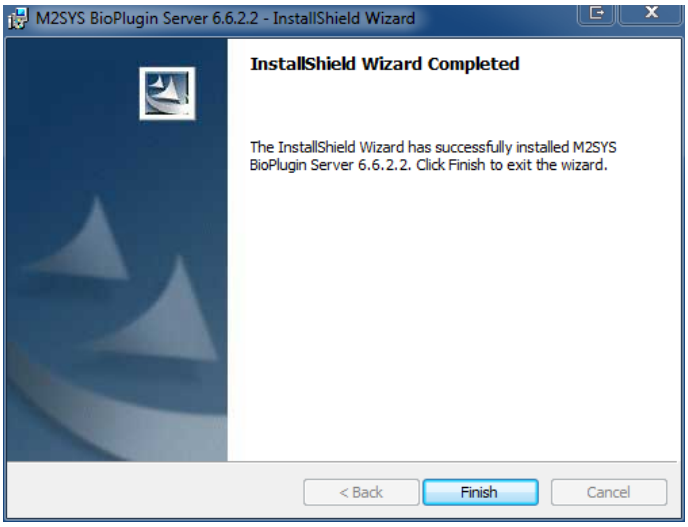

Figure 12 - Install Wizard Complete

12. The M2Sys Server will finish. Click Finish.

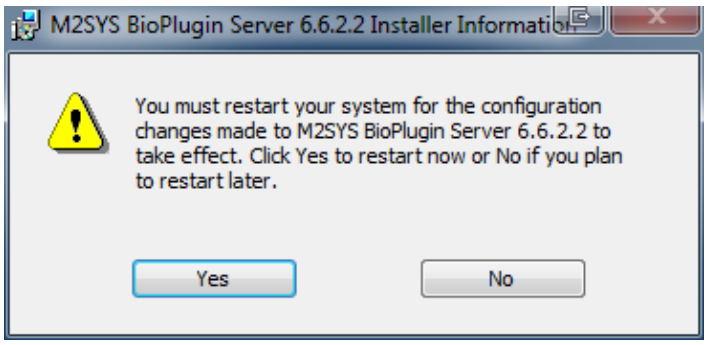

Figure 13 - Reboot Request

13. After the install the "server" computer will need to be rebooted. Close all other applications and then click Yes.

5.1.1.2 Server Configuration

Once the M2Sys Server installation is complete, the configuration of the database setup and the licensing of the Server need to occur.

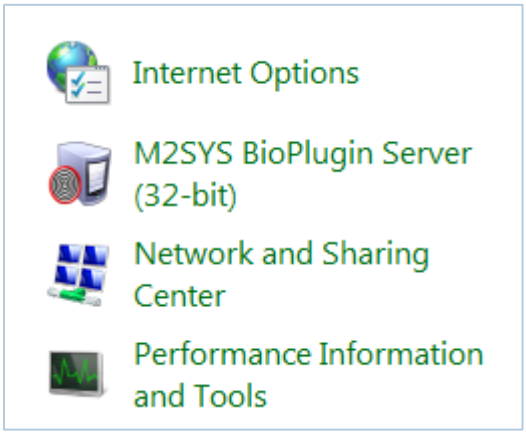

Figure 14 - Control Panel Server Manager

1. The M2Sys Server manager application is located in the Control Panel and is labeled as the M2Sys BioPlugin Server.
2. Double click on the icon.

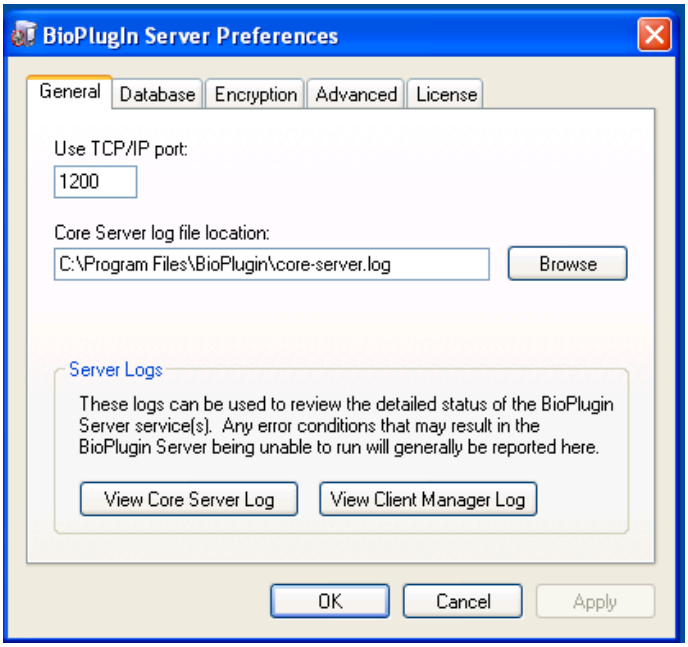

Figure 15 - Server Configuration General Tab

3. The General tab provides the ability for the following:
    a. Configure TCP/IP Port – Normally the default would be fine. It would only be changed in more advanced configurations where there are multiple "server" applications running on the same machine.
    b. Core Server Log Location – The default would the same directory to which the M2Sys Server was installed.
    c. Server logs – The logs could be viewed to verify that the server has started correctly and that clients are connecting to the server. These logs are great for troubleshooting.

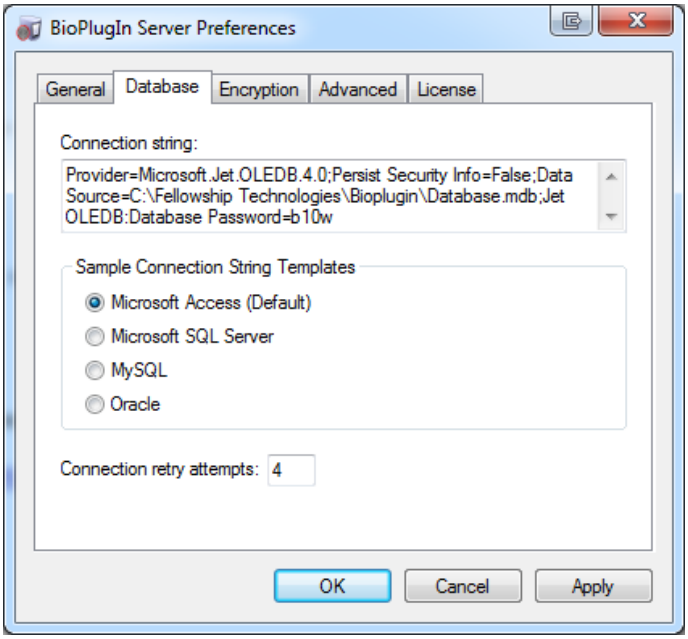

Figure 16 - Server Configuration Database Tab

4. The database tab allows for the configuration of the database type that will be used. The Default Microsoft Access is best for almost all configurations. Microsoft Access will not need to be installed on the M2Sys Server computer. The Connection retry should stay at 4.

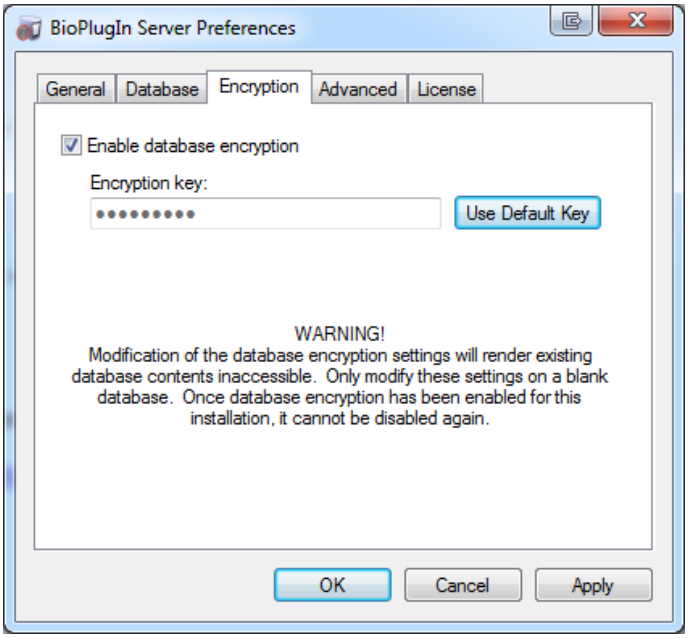

Figure 17 - Server Configuration Encryption Tab

5. The Encryption option is only chosen when server is first configured. It is not to be enabled after the M2Sys Server database has been populated with Biometric data.
6. It's advisable to enable Encryption at install. Using the Default Key is acceptable instead of entering a key manually.

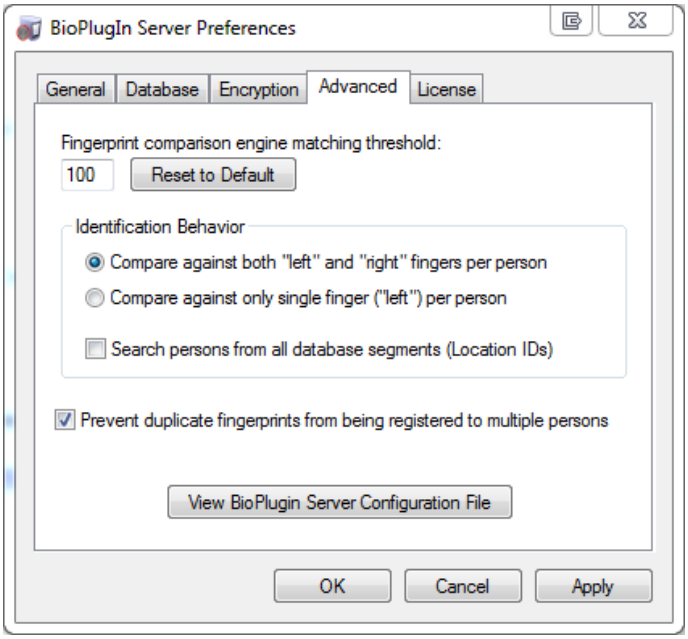

Figure 18 - Server Configuration Advanced Tab

7. The Advanced tab has several important settings:
    a. The Fingerprint comparison threshold is defaulted at 100. This default is advisable.
    b. Identification Behavior – The choice needs to be made as to whether the requirement for storing Biometric information will be based on two fingers or one. The two finger option ("Compare against both "left" and "Right" fingers per person") means that when the fingerprints are captured during the Biometric setup process the person being configured for fingerprint scanning will need to scan two fingers. This means that they can use two fingers to Check-in or that one finger from both parents can be used to Check-in. This is advisable. One finger is the other option ("Compare against only single finger("Left") per person")but is limiting when used with Check-in.
    c. Search persons from all database segments should be left unchecked.
    d. Prevent duplicate fingerprints from being registered to multiple persons should be checked.

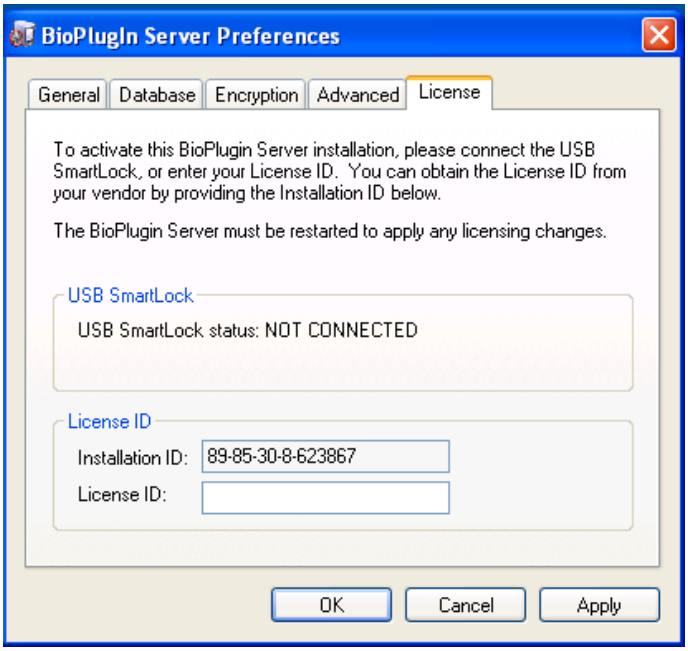

Figure 19 - Server Configuration License Tab

8. The Licensing instructions will be sent via email when the M2Sys Software is purchased. The instructions will provide the instructions for retrieving a License ID. The Installation ID is automatically generated based on the hardware so it is unique to the computer on which the M2Sys Server is being installed.
9. Once all of the settings are configured then click OK.

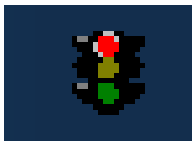

Figure 20 - M2Sys Server Notification Icon

10. Once the M2Sys Server is installed the Server Windows Process needs to be stopped and started. This is done by right-clicking the Server notification Icon in the Notification bar on the Server's start bar.

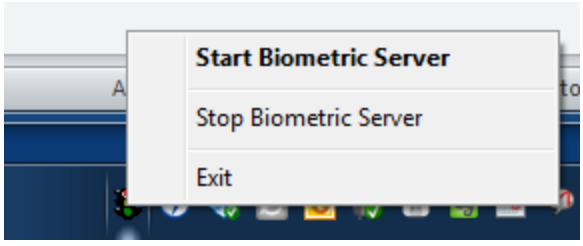

Figure 21 - M2Sys Server Notification Icon Menu

It is also extremely important to be sure that there is a way to back-up the M2Sys Server database since this is the only place that the Fingerprint Biometric information is stored.

5.1.2 M2Sys Client Installation and Configuration

This process begins before the fingerprint scanner is plugged in the computer.

The M2Sys Client software will be installed on every Check-in station that will support fingerprint scanning.

It is important to install the 64-bit version of the M2Sys software on the 64-bit Windows Operating system and that it is paired with the fingerprint scanner that supports the 64-bit Windows as well.

The 32-bit version of the M2Sys Software will be installed on 32-bit computers that are running the 32-bit version of Windows and paired with the scanner that supports 32-bit Windows.

5.1.2.1 Client Installation

1. Run the applicable M2Sys Client installer.

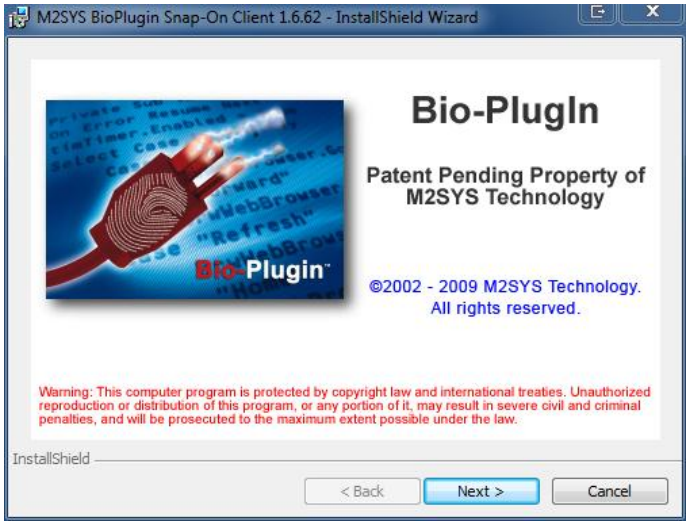

Figure 22 - License Agreement

2. Click Next at the Bio-Plugin Intro Screen.

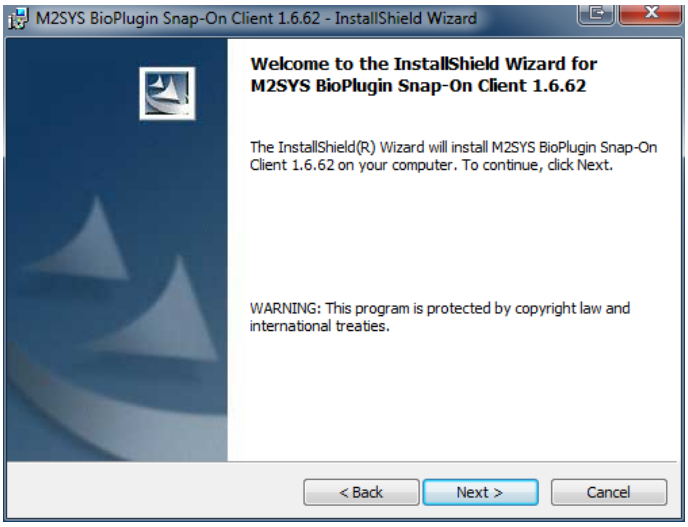

Figure 23 - Welcome Screen

3. Click Next at the Welcome screen.

Figure 24 - License Agreement

4. Accept the license Agreement.
5. Click Next.

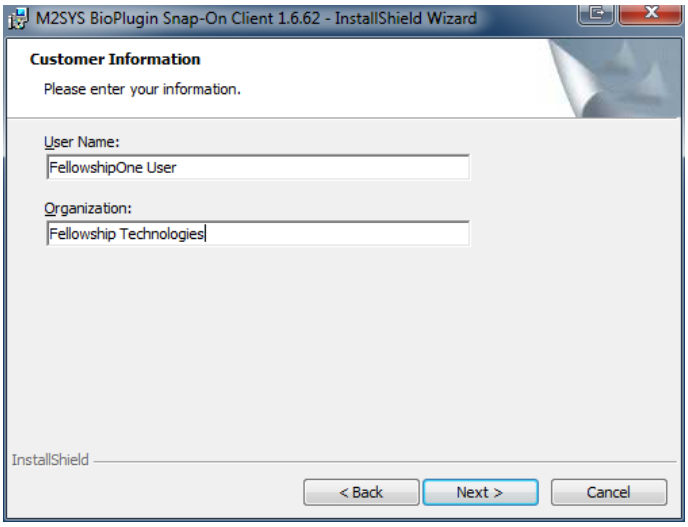

Figure 25 - Customer Information

6. Enter your Name and Organization name.
7. Click Next.

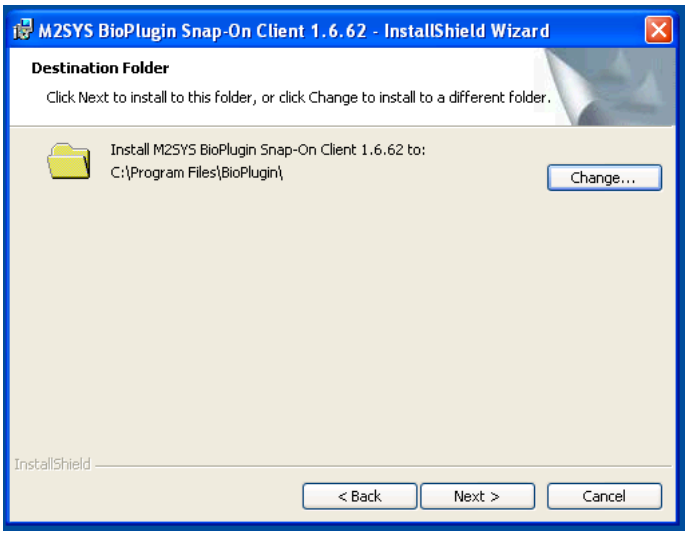

Figure 26 - Driver Install

8. Accept the default location for the client files. You can change it if required by selecting Change.
9. Click Next.

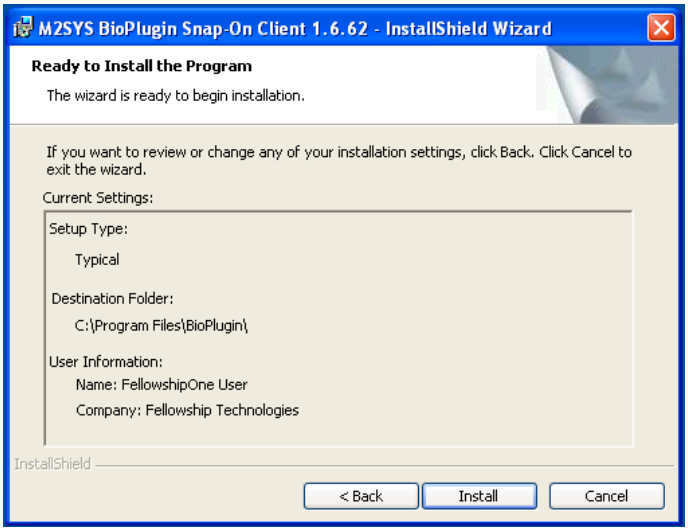

Figure 27 - Ready to Install

10. This window will show the setting that you configured. Click Next.

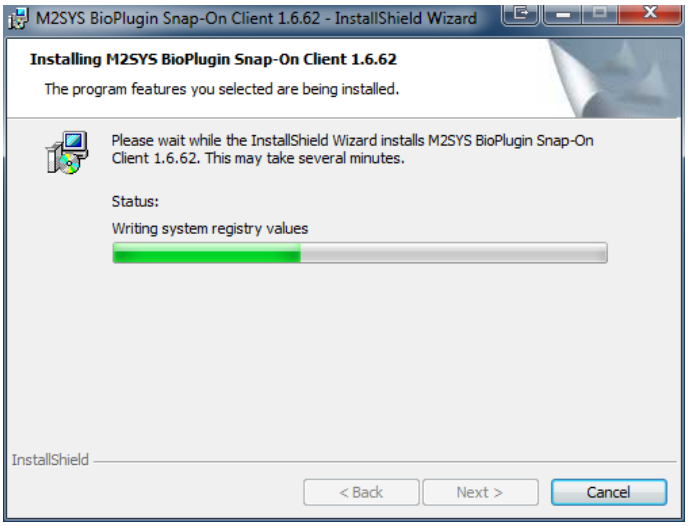

Figure 28 - File Load

11. The client application will begin to install the files.

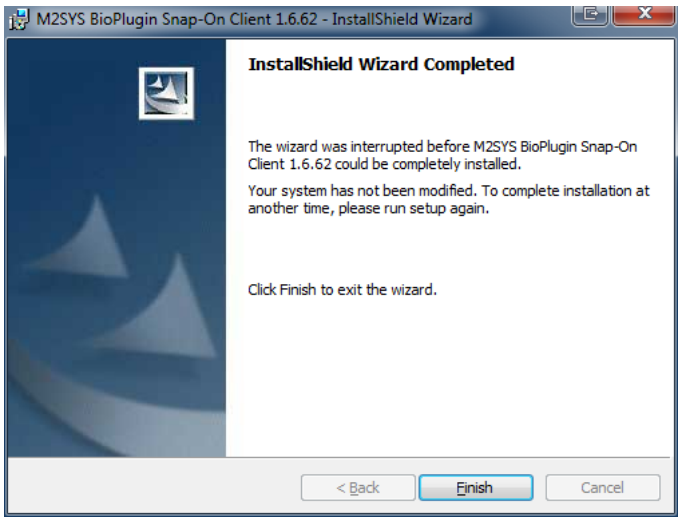

Figure 29 - Install Wizard Complete

12. The M2Sys Client will finish. Click Finish.

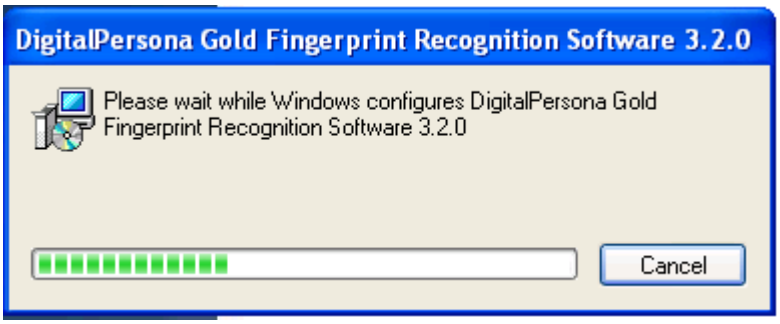

Figure 30 - Finger print recognition software

13. The DigitalPersona Fingerprint Recognition software will install. It is the driver for the fingerprint scanner.

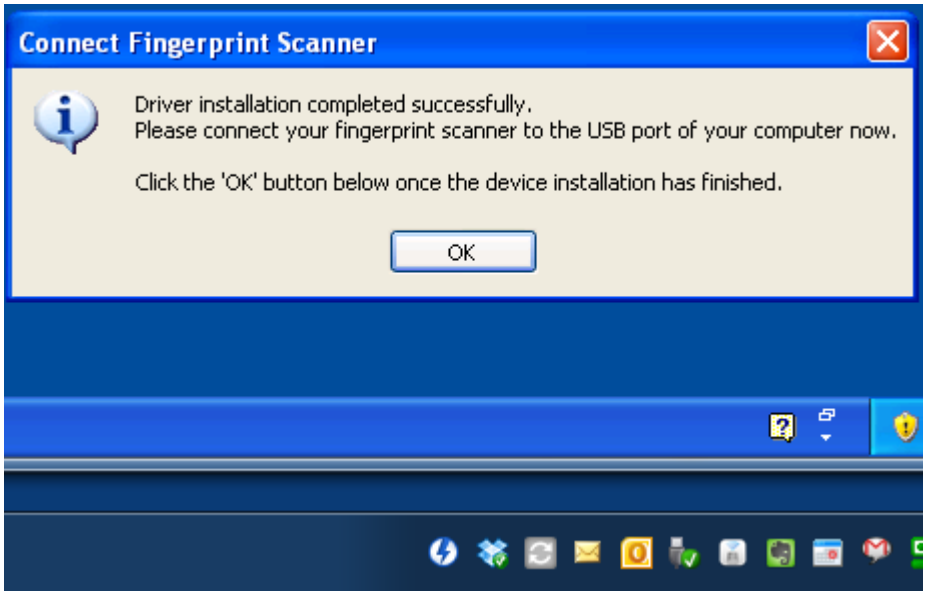

Figure 31 - Fingerprint recognition software complete

14. Once the driver is completed click OK to complete the install. It will be important to configure the Client software before connecting the fingerprint scanner.

5.1.2.2 Client Configuration

Once the client is installed it must be configured to connect to the M2Sys Server even if the Server is located on the same computer or another computer.

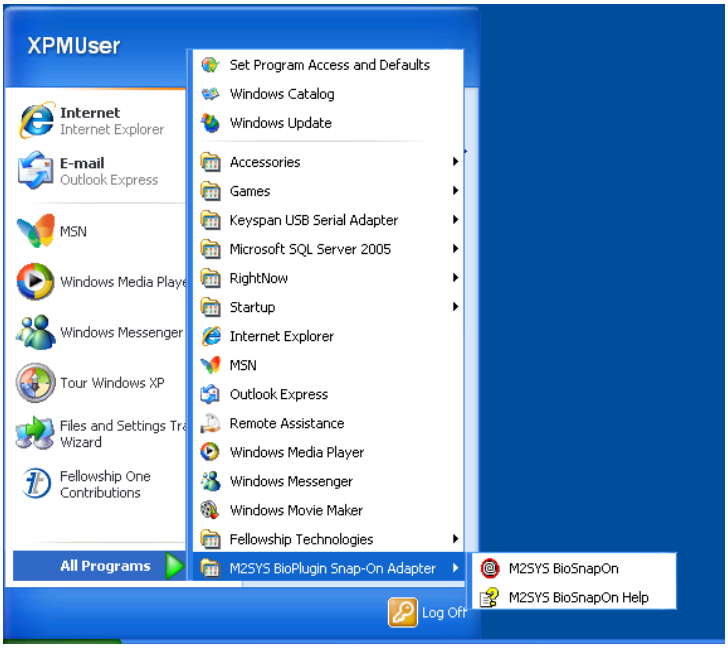

Figure 32 - M2Sys client in Start Menu

1. Once the install is complete the M2Sys client can be started by going to the Start menu |Programs| M2Sys Bioplugin Snap-on Adapter. Click on the M2Sys BioSnapon application.

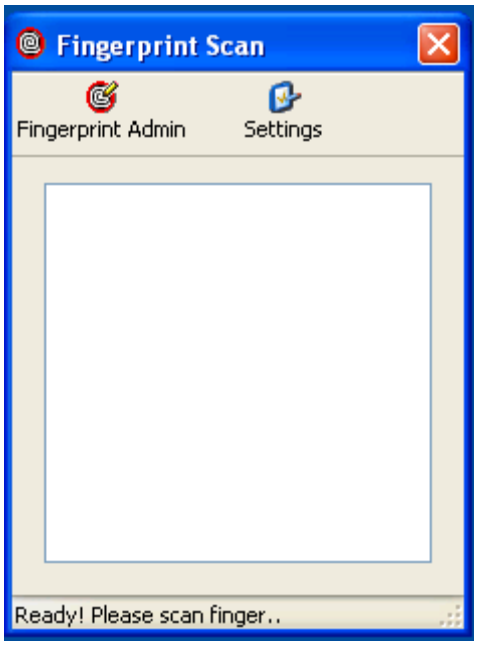

Figure 33 - Fingerprint Scan Application

2. The Fingerprint Scan application will start.
3. Click on Settings.

Figure 34 - Fingerprint Scan Administrator Password

4. Enter the Administrator Password. The default is “admin”.

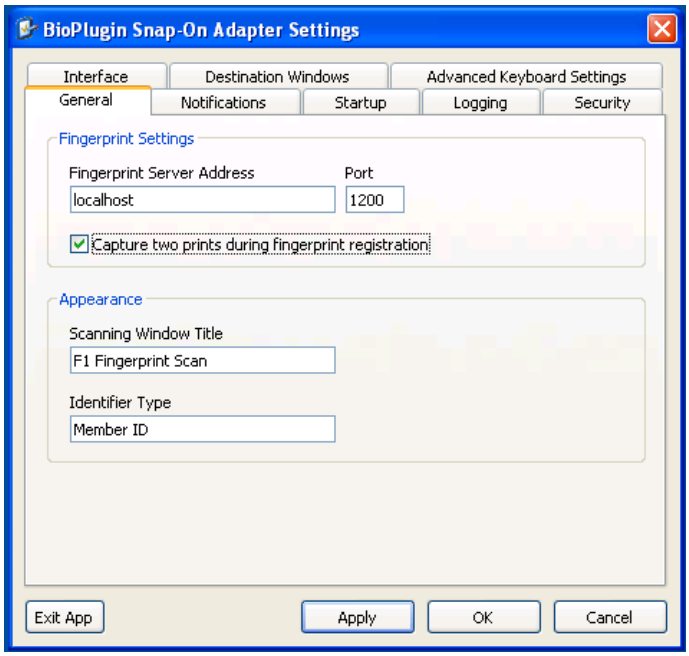

Figure 35 - Fingerprint Scan General Tab – Local Server

5. The General tab has several important settings:
    a. Fingerprint Server Address – If the M2Sys Client is installed on the same computer as the M2Sys Server then localhost is the correct setting. The Port only needs to change if the Port was changed in the Server configuration.
        i. If the Server is installed on a different computer than the client then the TCP/IP address of the Server computer needs to be entered here.
    b. Be sure to check "Capture two prints during fingerprint registration". It changes the option when two fingers are selected on the Server settings for capture to have the client get the fingers scans from two hands instead of 1. It makes the fingerprint capture process easier to understand.
    c. The Appearance section provides the ability to change the names of the Scanning Window that appears on the screen and the name of the Identifier used on the screen when capturing the fingerprints.

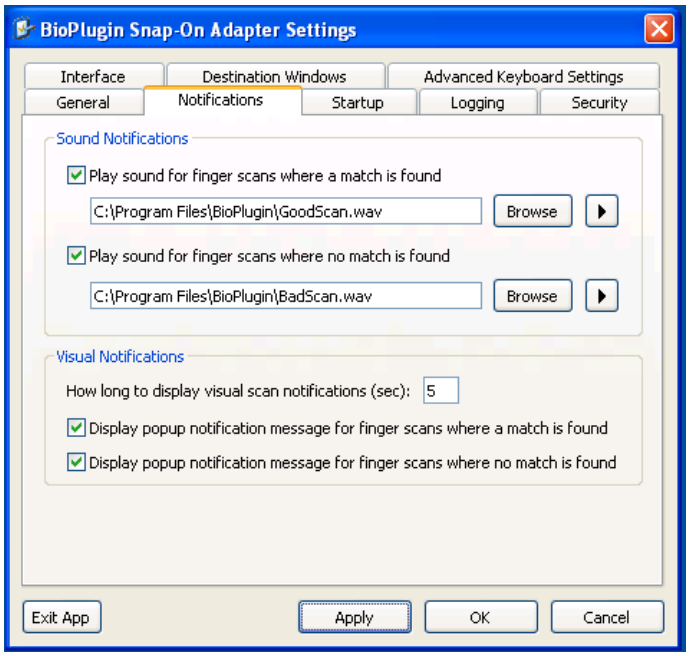

Figure 36 - Fingerprint Scan Notification Tab

6. The Notification tab provides the ability to have both audio and visual verifications when a fingerprint is captured and passed to Check-in.
7. These settings are best determined by the organization. The defaults are recommended.

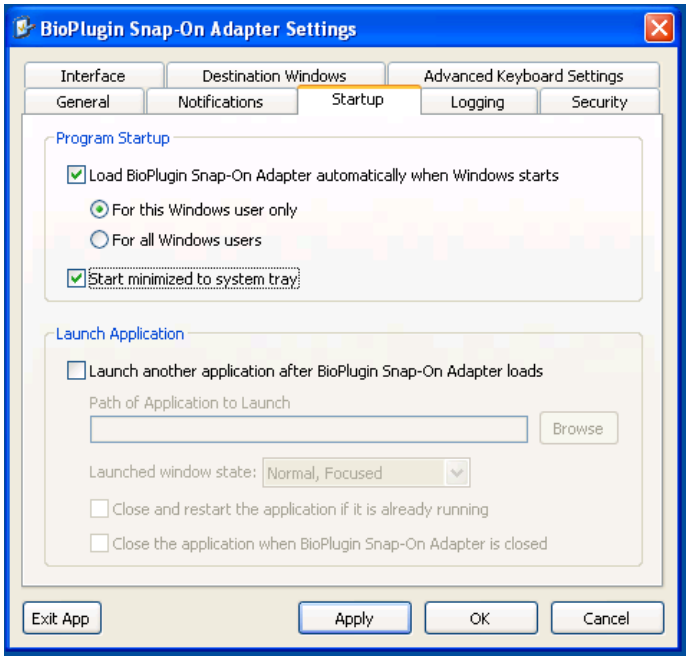

Figure 37 - Fingerprint Scan Startup Tab

8. The Startup tab is used to configure how the M2Sys BioPlugin client starts.

d. By checking “Load BioPlugin Snap-On Adapter automatically when Windows starts” the BioPlugin client will automatically start whenever Windows starts.
e. The option “For this Windows user only” is the default and works best.
f. Check “Start minimized to System tray” to prevent the BioPlugin Client from showing up on the screen when it starts. It will still run in the background and will not need to be seen to run with Check-in.
g. The Launch Application is not needed for Check-in.

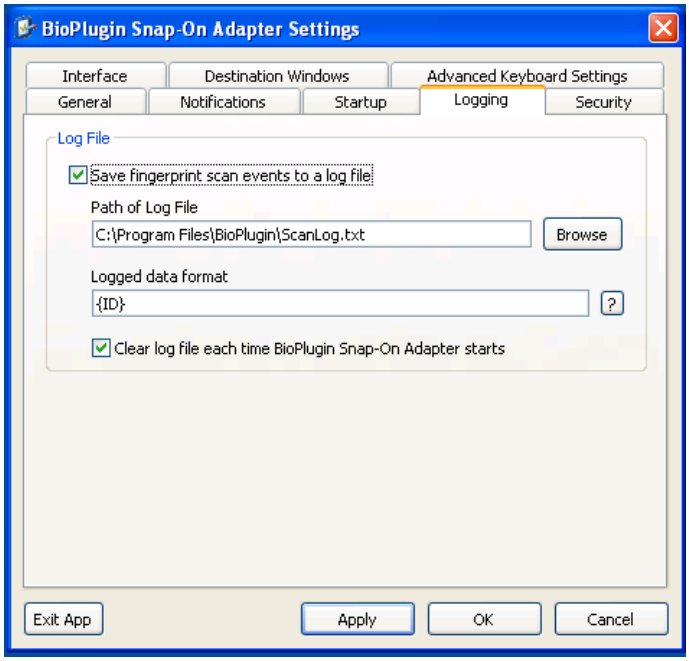

Figure 38 - Fingerprint Scan Logging Tab

9. The Logging tab is useful especially for troubleshooting. Logging can be left on at all times, but can also be turned on only when troubleshooting is needed. (This is recommended)
    h. Check “Save fingerprint scan events to a log file” to turn on logging.
    i. The default path of the log file and the logged data format don’t need to be changed.
    j. Be sure to check “Clear log file each time BioPlugin Snap-On Adapter starts” to insure that the client log doesn’t grow too large. For troubleshooting it may be useful to uncheck the box if longer term monitoring is required.

Figure 39 - Fingerprint Scan Security Tab

10. The Security tab allows for changing the default Administrator Password from "admin" to something more secure.
    k. The "Require password for access to settings and application exit" normally should be checked for security of the client settings.
    l. Require password for access to fingerprint administration can be turned off when fingerprints are being captured to the BioScan database.
    m. Neither of the check boxes affects the operation of the BioPugin client when capturing fingerprints for Check-in. These are only affecting administrative functions.
    n. The Current Password, New Password, and Confirm New Password are used for changing the Administrator Password.

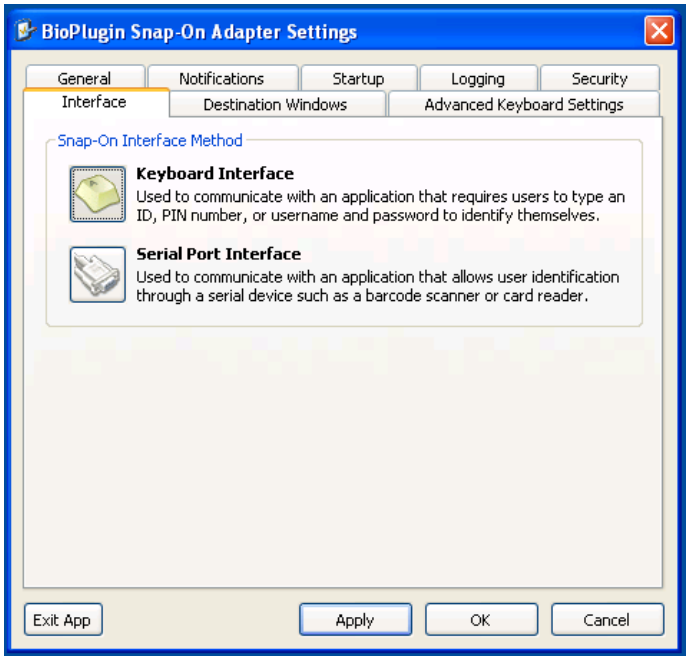

Figure 40 - Fingerprint Scan Interface Tab

11. The Keyboard Interface is what needs to be selected. It insures that the BioPlugin client feeds the ID from the BioScan database as if it were being entered on a keyboard.

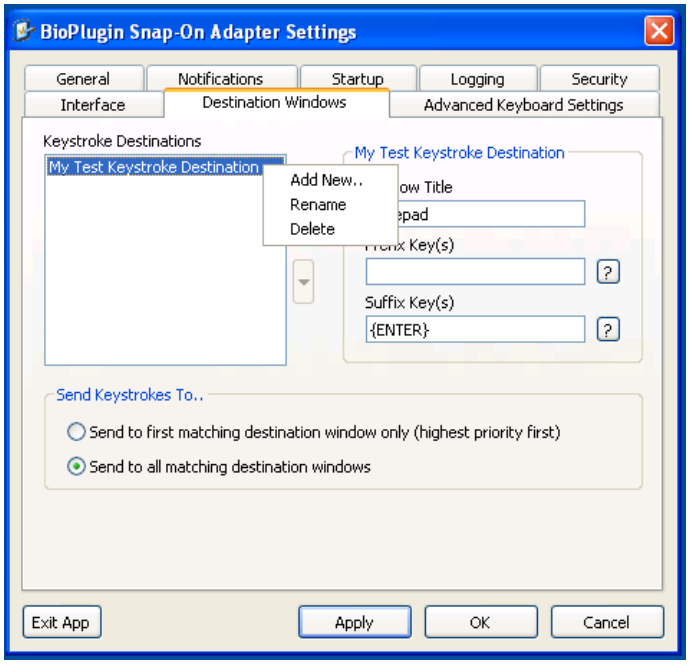

Figure 41 - Fingerprint Scan Destination Windows Tab

12. The BioPlugin client is a Snap-on application. In other words it Snaps-on to Check-in and doesn't directly interface to Check-in. The way that it does this is by sending the ID to

Check-in by acting as a keyboard and sending the keyboard data (the ID) to the Check-in application as if it is selecting the Check-in Application Window and typing the ID.

13. To set up the Windows that are used by Check-in for both Self Check-in and Assisted Check-in the Keystroke Destinations are configured.
14. Begin by deleting the default “My Test Keystroke Destination” by right-clicking on it and selecting Delete.

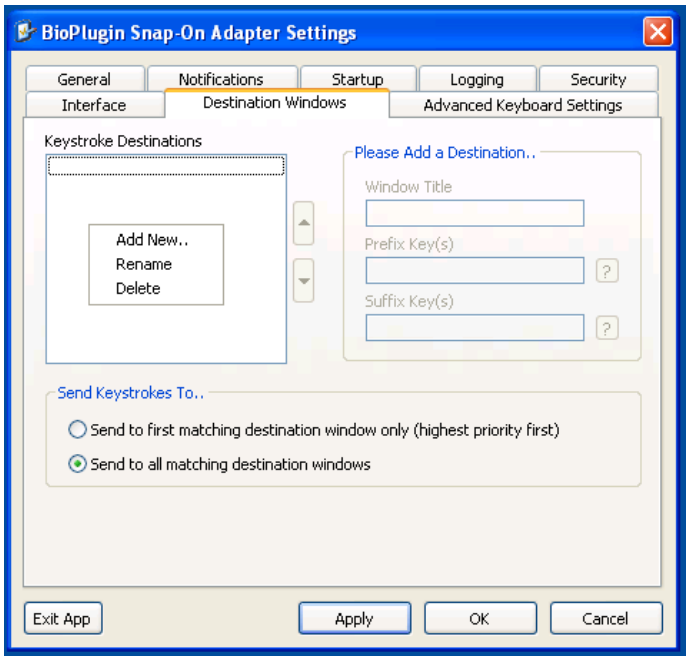

Figure 42 –Bioplugin Destination Add

15. Right on the blank “Keystroke Destinations” area and click Add New.

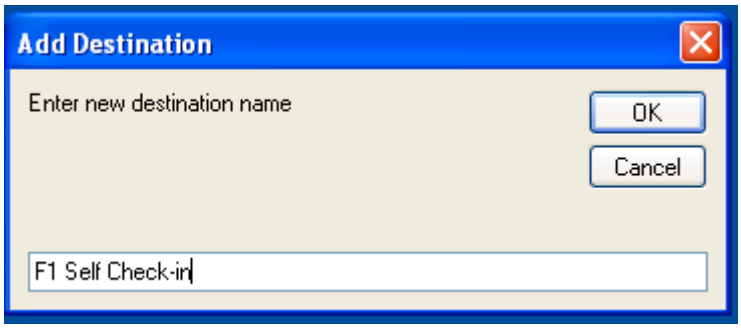

Figure 43 - Bioplugin Destination Entry

16. Enter “F1 Self Check-in” then Click OK.

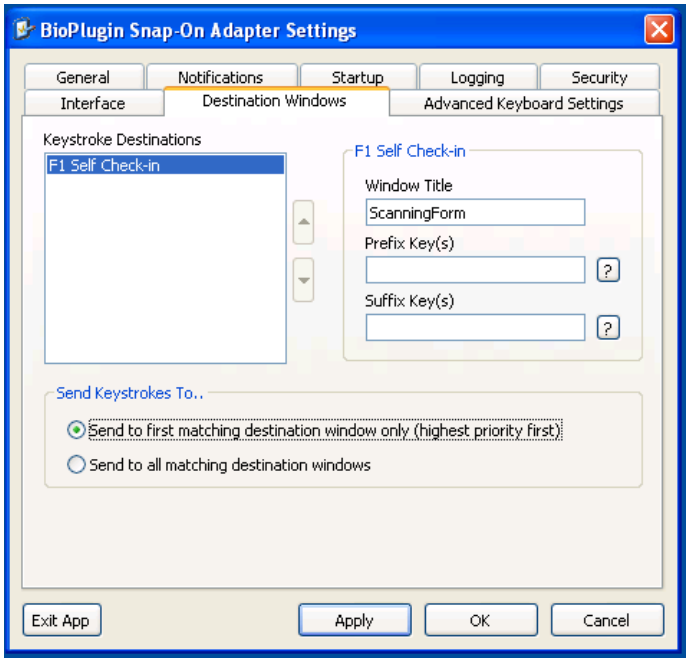

Figure 44 - Bioplugin Destination Add

17. Set the Window Title field to be “ScanningForm”. The case and spacing are important.
18. Prefix Key(s) and Suffix Key(s) remain blank.
19. “Send to first matching destination window only (highest priority first) “should be selected.
20. Click Apply.

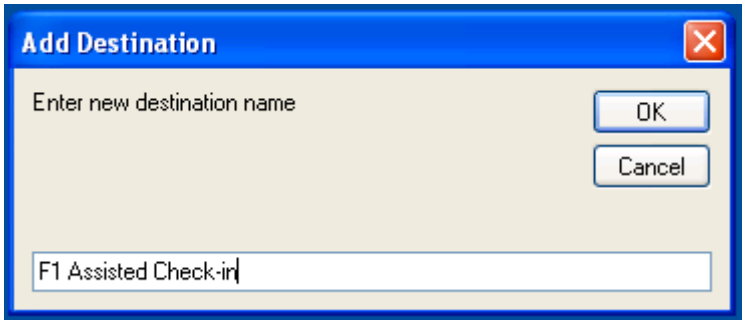

Figure 45 - Bioplugin Destination Entry

21. Right-click in an empty space in the Keystrokes Destination box and select “Add New”
22. Enter “F1 Assisted Check-in” and click OK.

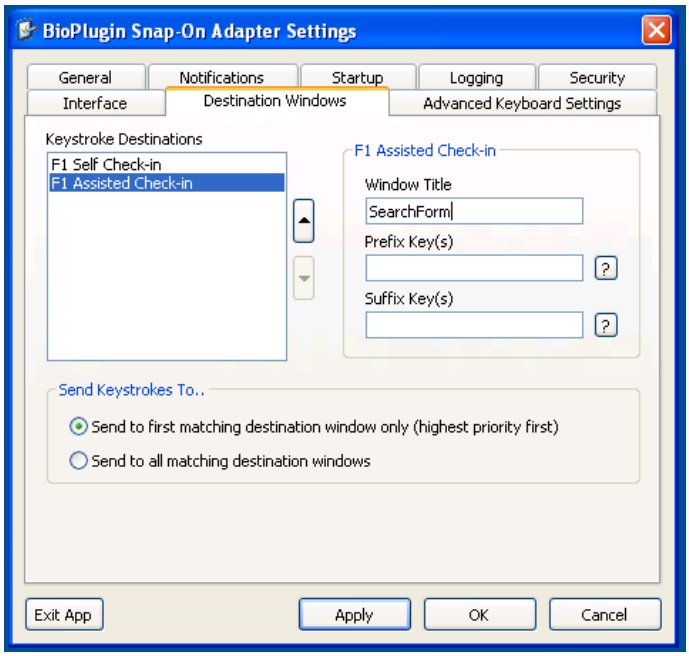

Figure 46 - Bioplugin Destination Configuration

23. Set the Window Title field to be "SearchForm". The case and spacing are important.
24. Prefix Key(s) and Suffix Key(s) remain blank.
25. "Send to first matching destination window only (highest priority first) "should be selected.
26. Click Apply.

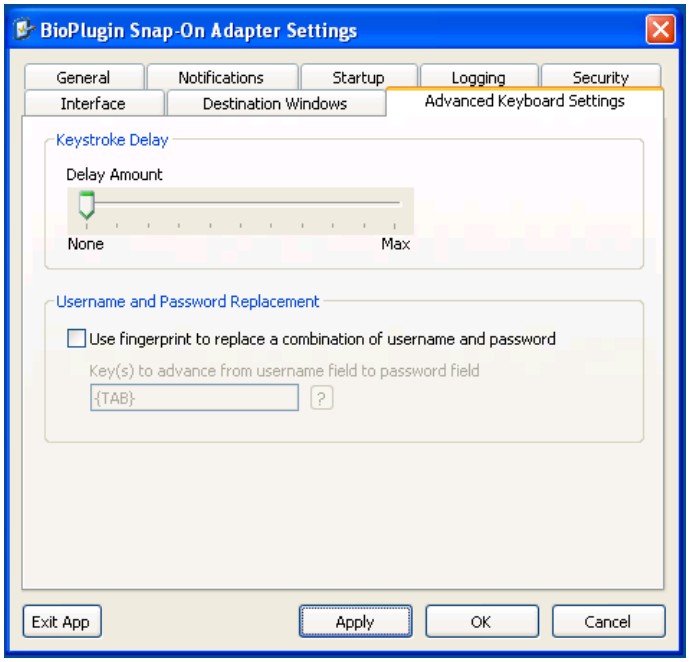

Figure 47 - Fingerprint Scan Advanced Keyboard Settings Tab

27. The defaults shown above are the recommended settings for the Advanced Keyboard Settings tab.
28. Once all setting are set click Apply then click OK.

5.2 HARDWARE INSTALLATION

The hardware installs very simple. After the Software is installed then simply finding a USB port and plugging in the fingerprint scanning device is all that's needed. The software will find the device automatically.

Figure 48 - Basic Check-in Setup with Scanner

5.2.1.1 Fingerprint Capture Process

There is a process that needs to occur to match the IDs used for the fingerprints and the Bar Code field in the Individual record in Fellowship One. Normally the ID that is assigned is from a Bar Code. The Barcode field is the field that is used in Check-in to ID the person checking in.

The ID that is used can be the person's cell phone number or can be a barcode which would allow them to Check-in using a Barcode tag or their fingerprint. Either way it is best to determine a standard that will be used.

The Bar Code/ID will be setup in the M2Sys System and then configured and/or verified in Fellowship One.

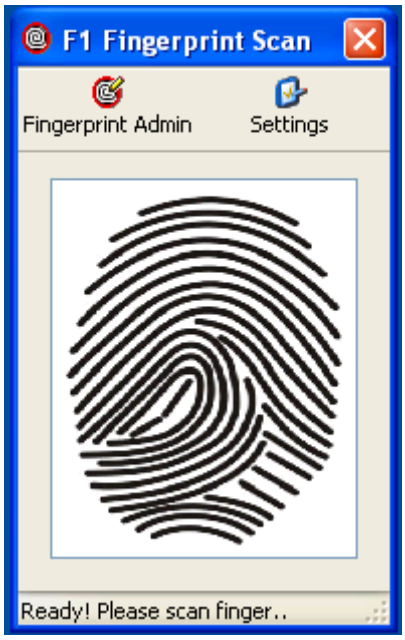

Figure 49 - Fingerprint Scan Client Application

1. To begin the process click on Fingerprint Admin in the Client Application.

Figure 50 - Fingerprint Administrator Password

2. Enter the Administrator Password then click OK.

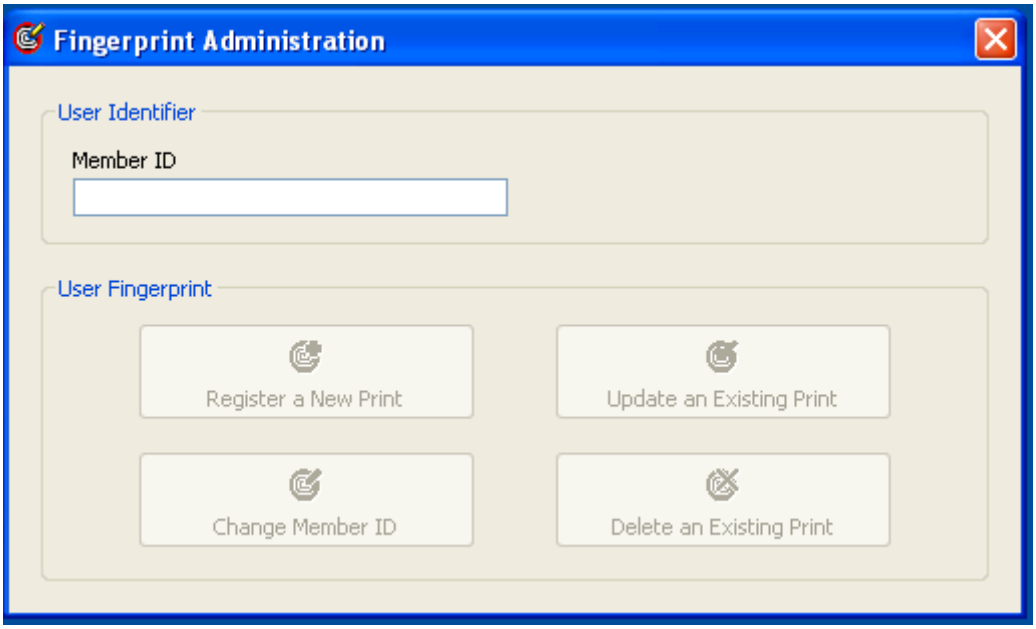

Figure 51 - Fingerprint Administrator

3. The Fingerprint Administrator screen begins with deciding what the Member ID will be If it's a bar code then if the Barcode reader is attached it can be scanned.

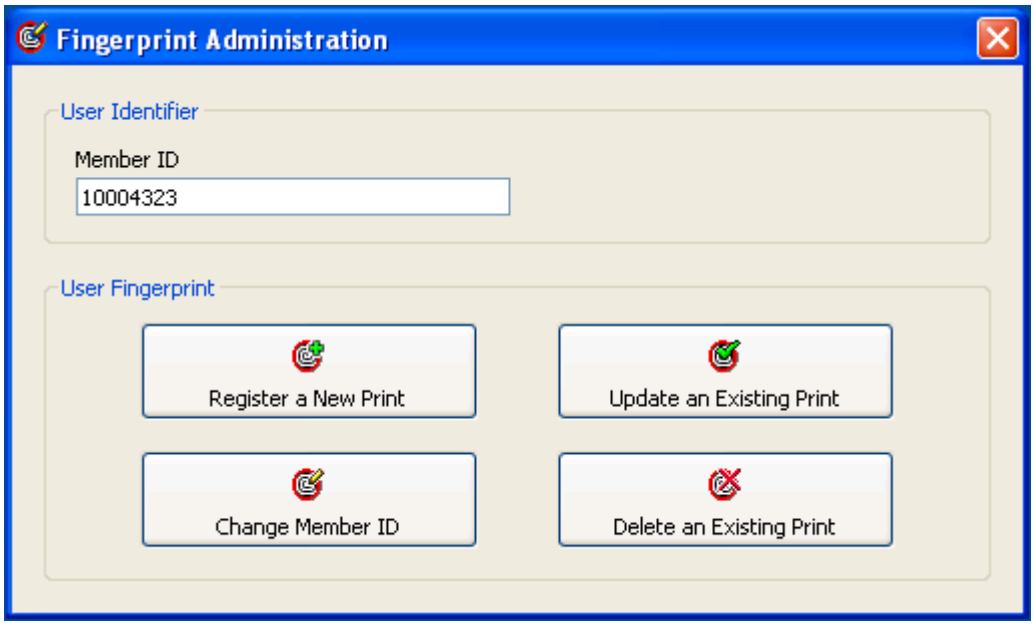

Figure 52 - Fingerprint Administrator Member ID

4. Once the ID is entered click the "Register a New Print" button. It can be entered manually or the Barcode scanner can be used to scan a barcode.

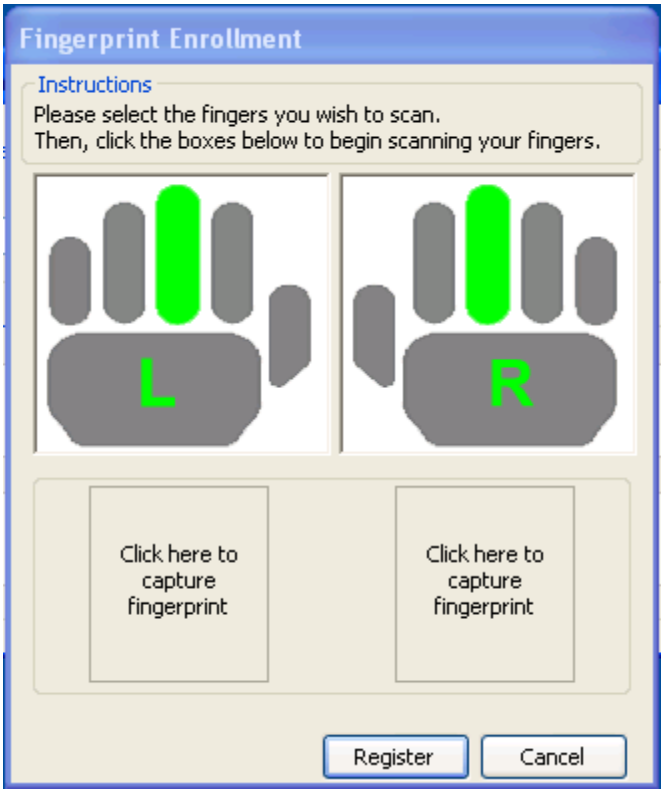

Figure 53 - Fingerprint Enrollment – Two Hands

5. Depending on the selections made in the configuration on the Advanced tab in the Server configuration there are two options for the capture window.
6. When "Compare against both "left" and "right" fingers per person" is select the two hand option like the above figure will be shown.

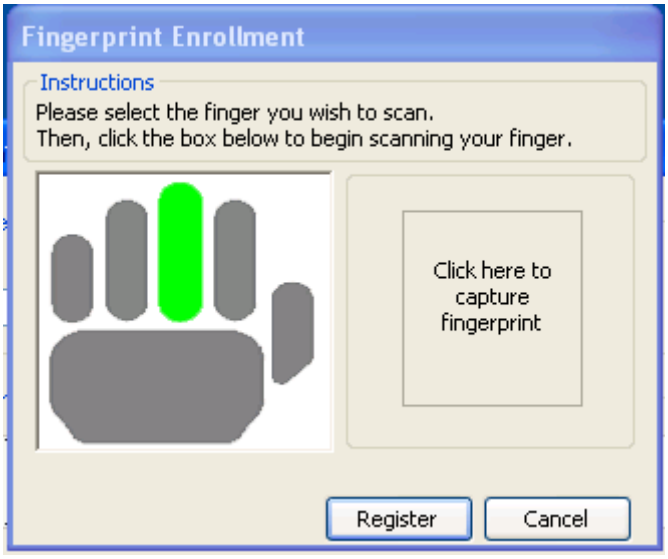

Figure 54 - Fingerprint Enrollment – One Hand

7. When “Compare against only single finger (“Left”) per person” is selected in the Server configuration then the Single hand window is shown.
8. In either window option the Fingers are captured one at a time.
9. The default finger is the middle finger, but any finger can be used by clicking on it.
10. To begin capturing the fingerprint, click the “Click here to capture fingerprint” area.

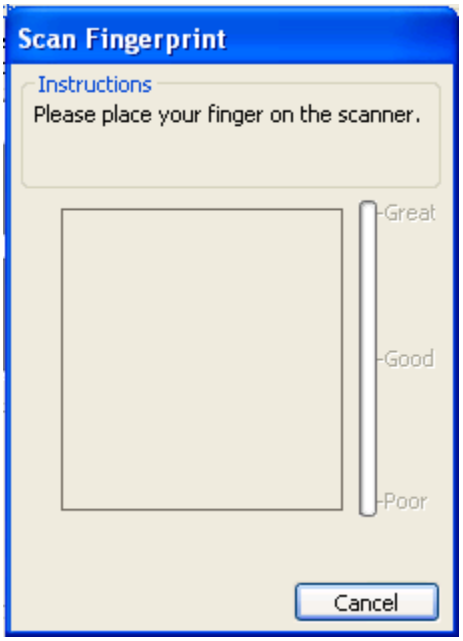

Figure 55 - Scan Fingerprint Window

11. The Scan Fingerprint window will appear with the instructions to place the finger on the scanner.
12. The finger will be scanned three times.

Figure 56 - Scan Fingerprint Second Time

13. The instructions will be given to lift the finger and place it on the scanner a second time.

Figure 57 - Scan Fingerprint Third Time

14. The instructions will then be given to lift the finger and place it on the scanner again.

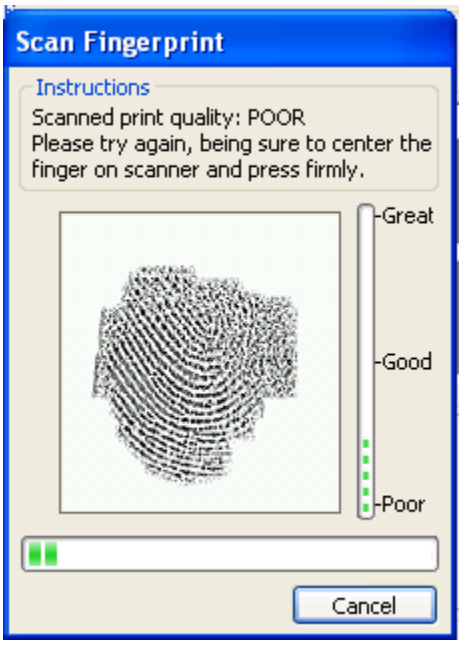

Figure 58 - Scan Fingerprint Poor/Fail

15. If at any point the scanner cannot capture the fingerprint with a good quality scan then the message will change to show that the scan was Poor quality and the user will be asked to lift their finger and place it on the scanner again.

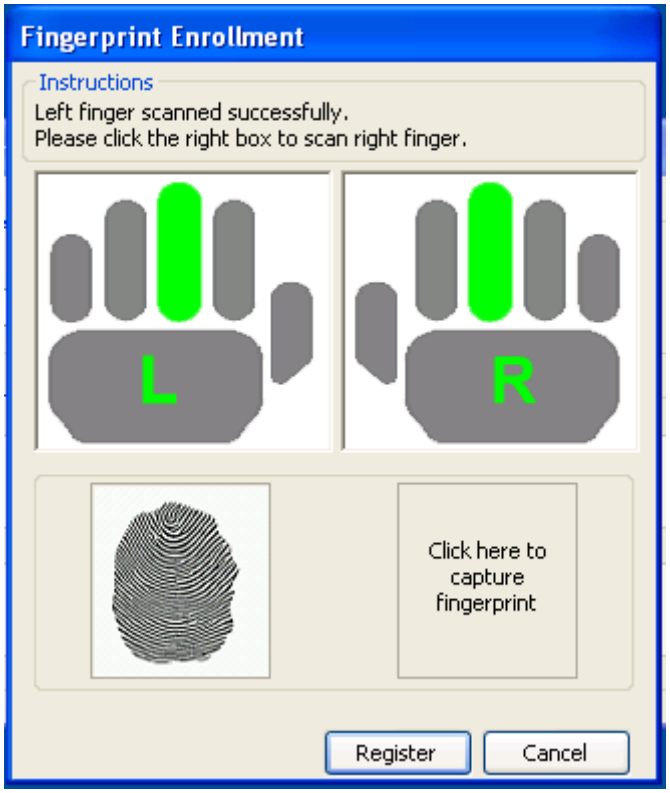

Figure 59 - Fingerprint Enrollment First Hand

16. Once the scans are completed the third time successfully, then the user will be taken back to the Fingerprint Enrollment window and will show that the first finger has been scanned.
17. If the one finger option is selected in the Server configuration then the window will show only one hand and the Register button can be clicked.
18. If the two hand option is selected then the process for the second had can begin by clicking on the second “Click here to capture fingerprint” area.
19. The second hand can be the person’s second hand or the hand can be the hand of a second parent or guardian.

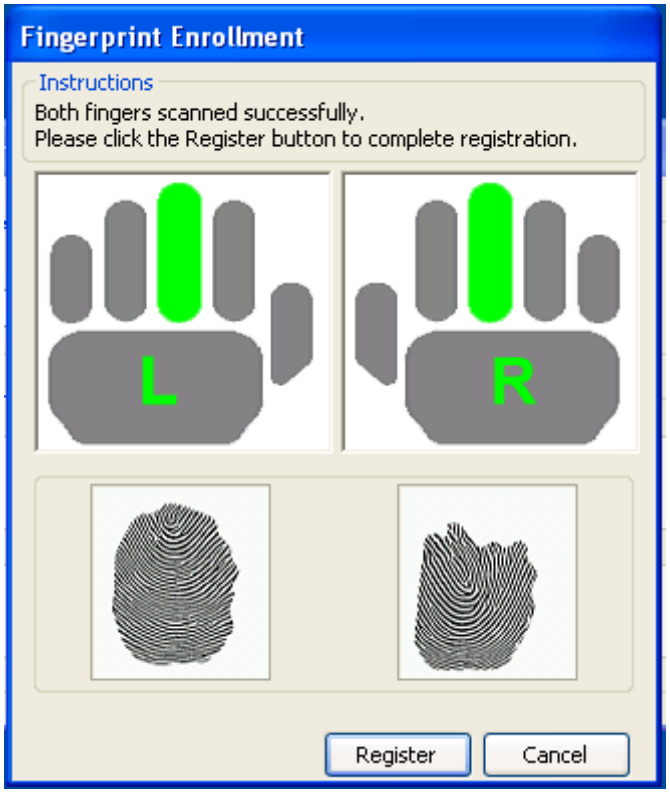

Figure 60 - Fingerprint Enrollment Second Hand

20. Once the fingerprint scans are completed then the process is completed by clicking the Register button.

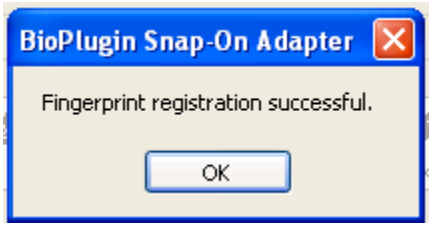

Figure 61 - Fingerprint Enrollment Success

21. The success of the registration will be shown.

Figure 62 - Fingerprint Enrollment Failure/Duplicate

22. If the fingerprints have already been registered then the registration will show as being a failure. This process is covered in 5.2.1.2 FingerPrint Failure/Deletion

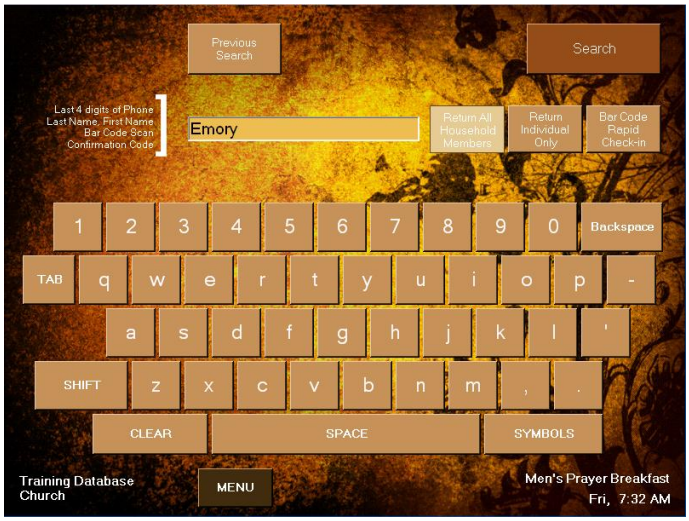

Figure 63 - Assisted Check-in Search

23. Next the Member ID has to be entered into the Individuals record in Fellowship One.
24. In Assisted Check-in enter the Individuals info to search for their record.

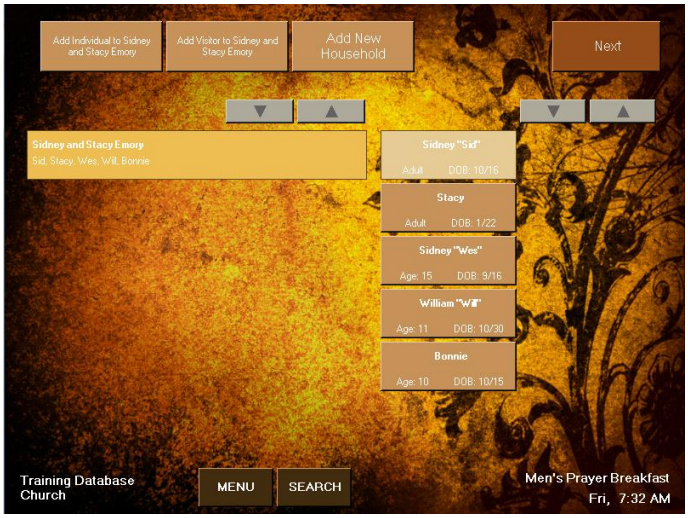

Figure 64 - Check-in Member Select

25. Select the Individual that will be updated.

Figure 65 - Member Activity

26. At the top of the screen select Edit to edit the individual's record.

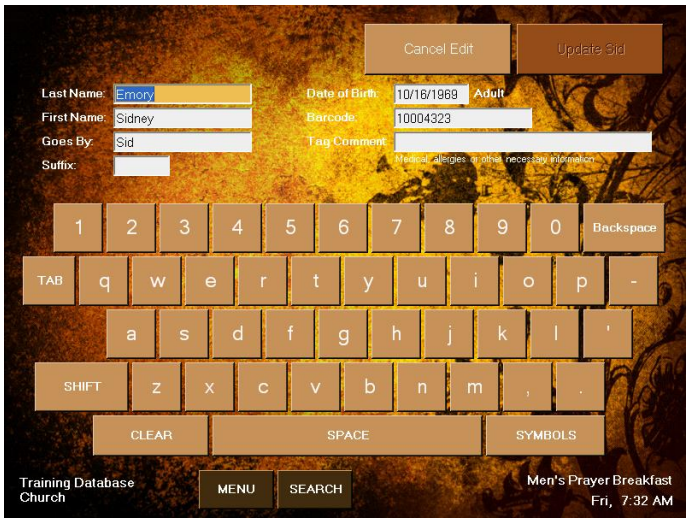

Figure 66 - Member Information

27. It is here that the individual's Barcode can be entered. This may be a Barcode number or another number.

5.2.1.2 Palm Vein Capture Process

There is a process that needs to occur to match the IDs used for Palm Veins and the Bar Code field in the Individual record in Fellowship One. Normally the ID that is assigned is from a Bar Code. The Barcode field is the field that is used in Check-in to ID the person checking in.

The ID that is used can be the person's cell phone number or can be a barcode which would allow them to Check-in using a Barcode tag or their fingerprint. Either way it is best to determine a standard that will be used.

The Bar Code/ID will be setup in the M2Sys System and then configured and/or verified in Fellowship One.

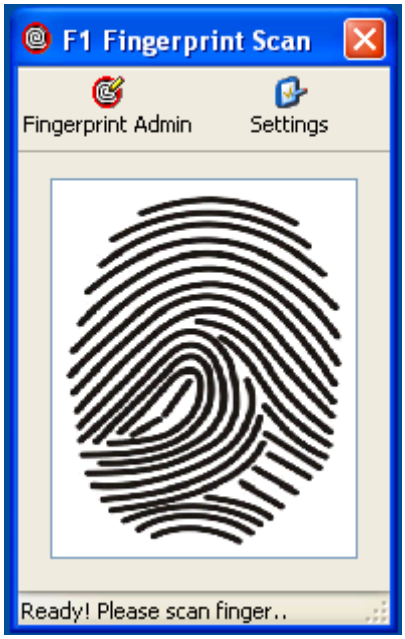

Figure 67 - Fingerprint Scan Client Application

1. To begin the process click on Fingerprint Admin in the Client Application.

Figure 68 - Fingerprint Administrator Password

2. Enter the Administrator Password then click OK.

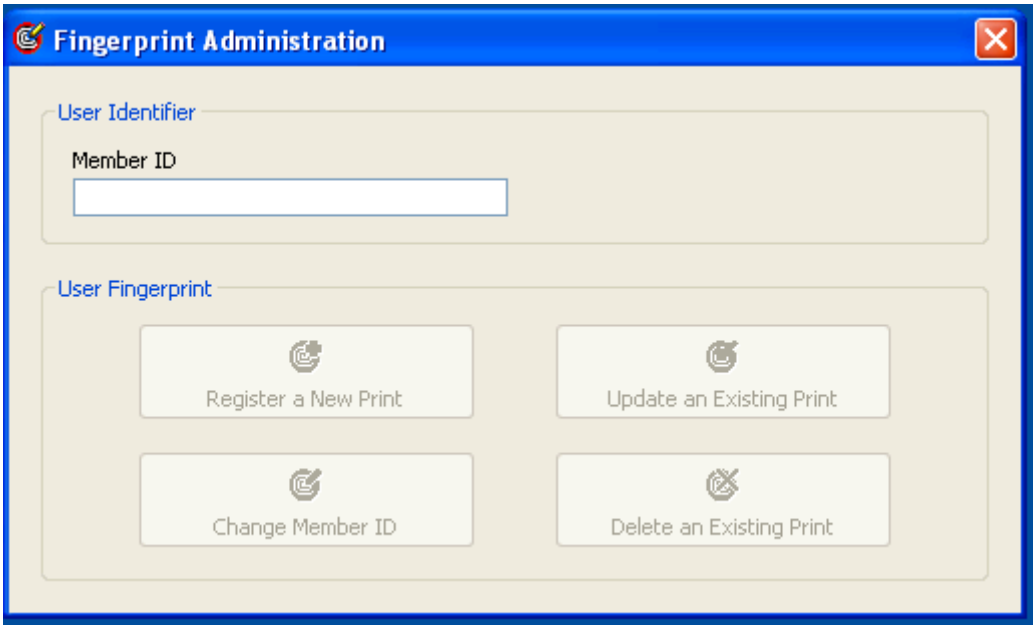

Figure 69 - Fingerprint Administrator

3. The Fingerprint Administrator screen begins with deciding what the Member ID will be If it's a bar code then if the Barcode reader is attached it can be scanned.

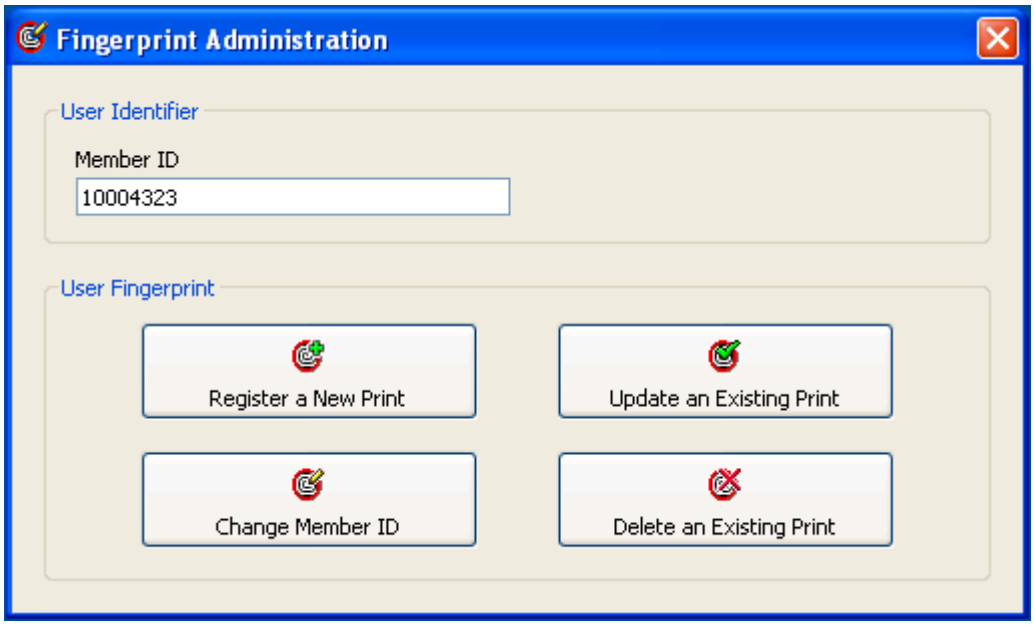

Figure 70 - Fingerprint Administrator Member ID

4. Once the ID is entered click the "Register a New Print" button. It can be entered manually or the Barcode scanner can be used to scan a barcode.

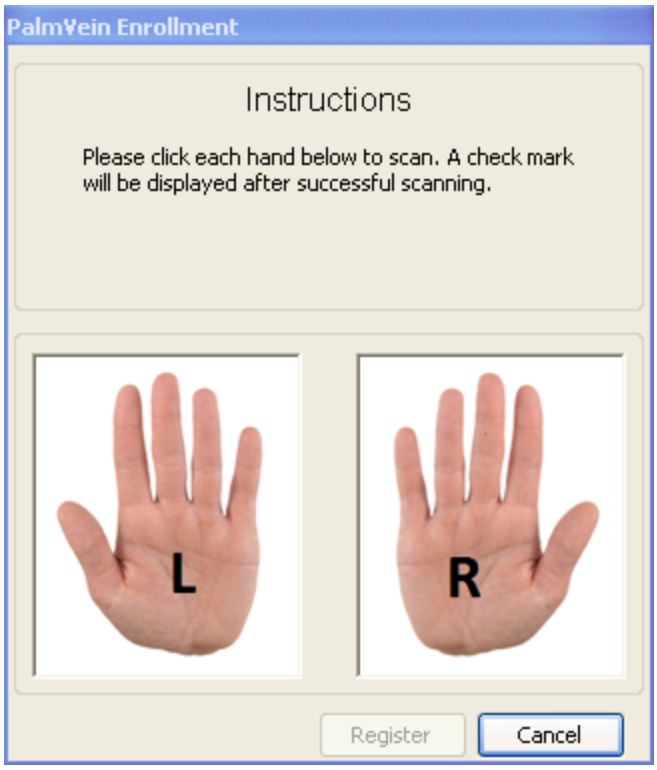

Figure 71 – Palm Vein Enrollment – Two Hands

5. The Scanning instructions will be given like the window above. To begin capturing the Palm Vein, click the Right Hand.

Figure 72 - Capture Vein Pattern Window

6. The Capture Vein Pattern window will appear with the instructions to place the hand on the scanner.
7. The hand will be scanned three times.

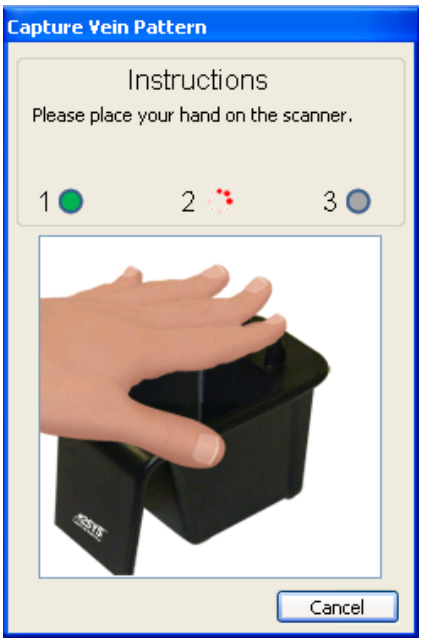

Figure 73 - Capture Vein Pattern Second Time

8. The instructions will be given to lift the hand and place it on the scanner a second time.

Figure 74 - Capture Vein Pattern Third Time

9. The instructions will then be given to lift the hand and place it on the scanner again.
10. If at any point the scanner cannot capture the hand with a good quality scan then the message will change to show that the scan was Poor quality and the user will be asked to lift their hand and place it on the scanner again.

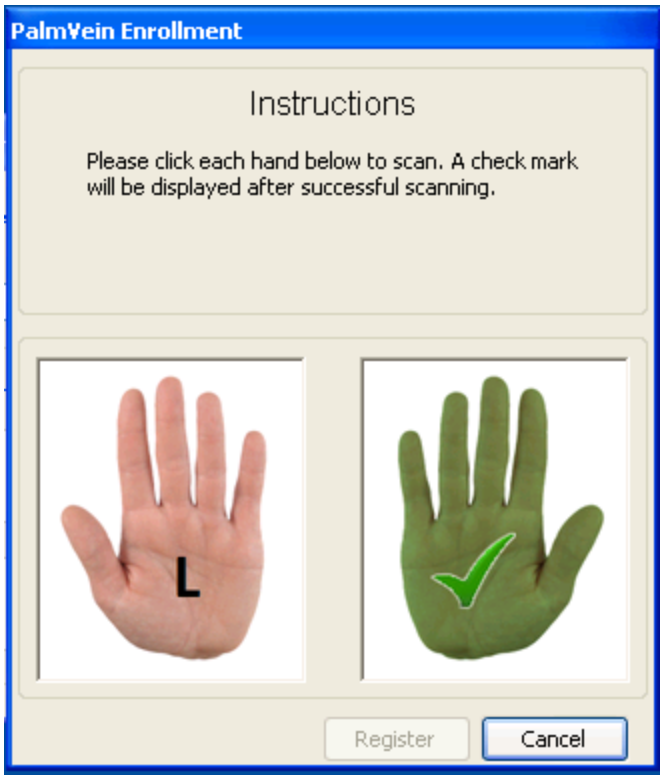

Figure 75 – PalmVein Enrollment First Hand

11. Once the scans are completed the third time successfully, then the user will be taken back to the PalmVein Enrollment window and will show that the first finger has been scanned.
12. The second hand can be the person's second hand or the hand can be the hand of a second parent or guardian.

Figure 76 - PalmVein Enrollment Second Hand

13. Once the fingerprint scans are completed then the process is completed by clicking the Register button.

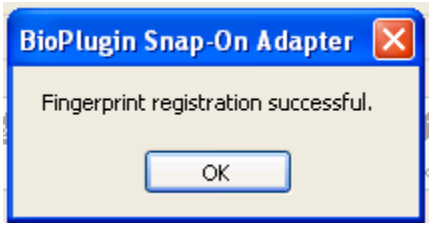

Figure 77 - Fingerprint Enrollment Success

14. The success of the registration will be shown.

Figure 78 - Fingerprint Enrollment Failure/Duplicate

15. If the fingerprints have already been registered then the registration will show as being a failure. This process is covered in 5.2.1.2 FingerPrint Failure/Deletion

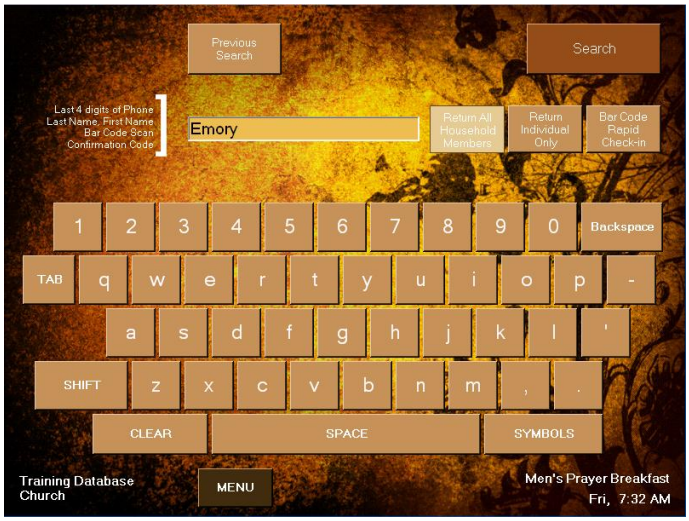

Figure 79 - Assisted Check-in Search

16. Next the Member ID has to be entered into the Individuals record in Fellowship One.
17. In Assisted Check-in enter the Individuals info to search for their record.

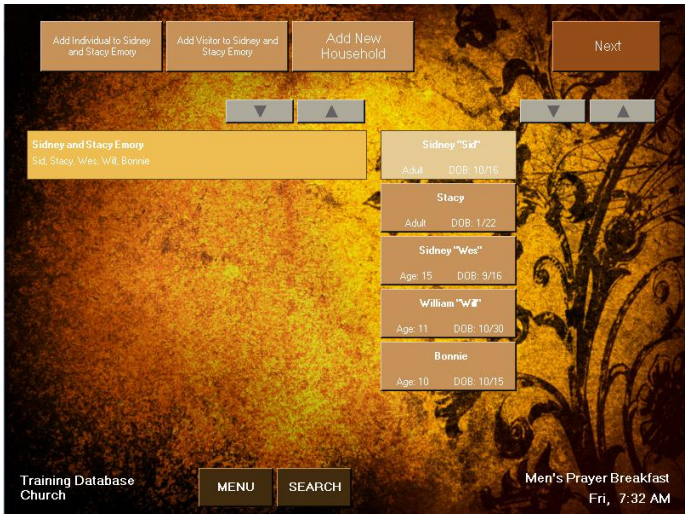

Figure 80 - Check-in Member Select

18. Select the Individual that will be updated.

Figure 81 - Member Activity

19. At the top of the screen select Edit to edit the individual's record.

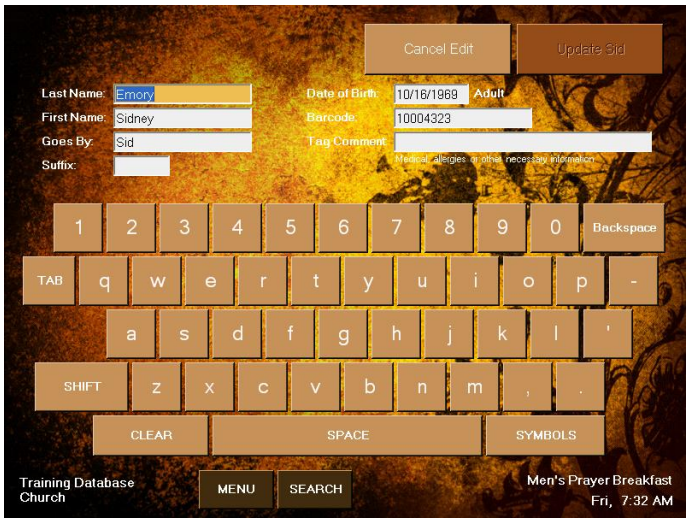

Figure 82 - Member Information

20. It is here that the individual's Barcode can be entered. This may be a Barcode number or another number.

5.2.1.3 Fingerprint Capture Failure/Deletion

If fingerprints for an individual has already be captured and the ID that it's associated with is unknown then the easiest way to determine the ID that is assigned to the individuals fingerprint is to enter into Assisted Check-in.

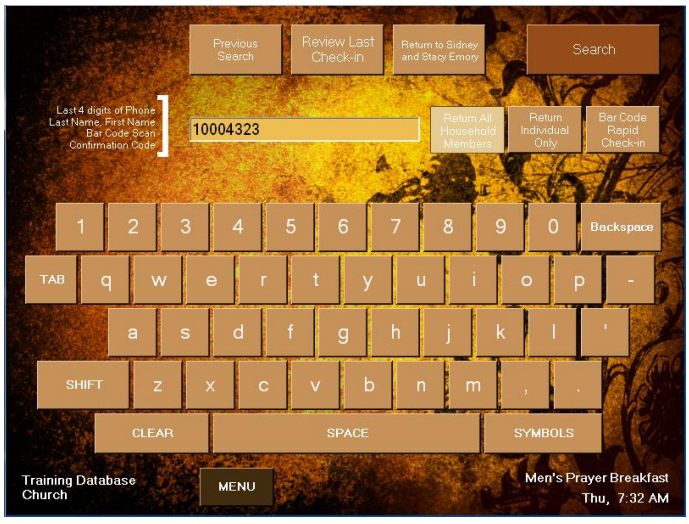

Figure 83 - Assisted Check-in Search Window

1. Have the Individual scan their fingerprint. The ID will show in the Search box.

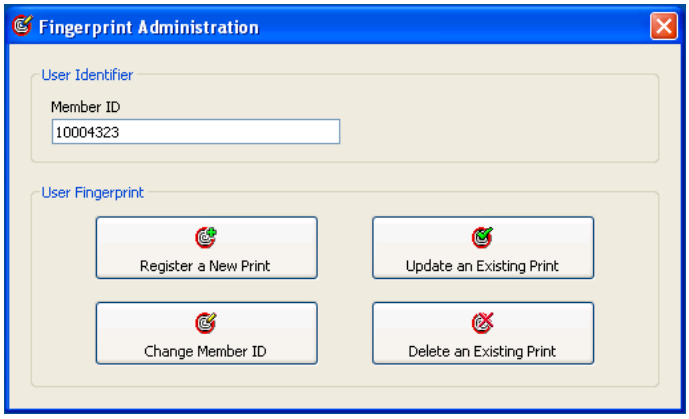

Figure 84 - Fingerprint Administration

2. Once the ID is know the Fingerprints can be updated or Member ID changed.
3. It's also possible to delete the fingerprint by selecting "Delete and Existing Print"

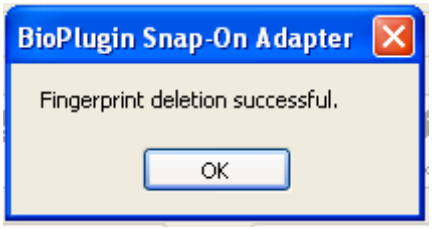

Figure 85 - Fingerprint Deletion Successful

4. If the fingerprint is deleted the above is the confirmation message that will be received.
5. If the fingerprint is deleted and another is created with another Member ID then be sure to update the person(s) individual record in Fellowship One

5.2.1.4 Check-in Configuration and Using Fingerprint Scanning

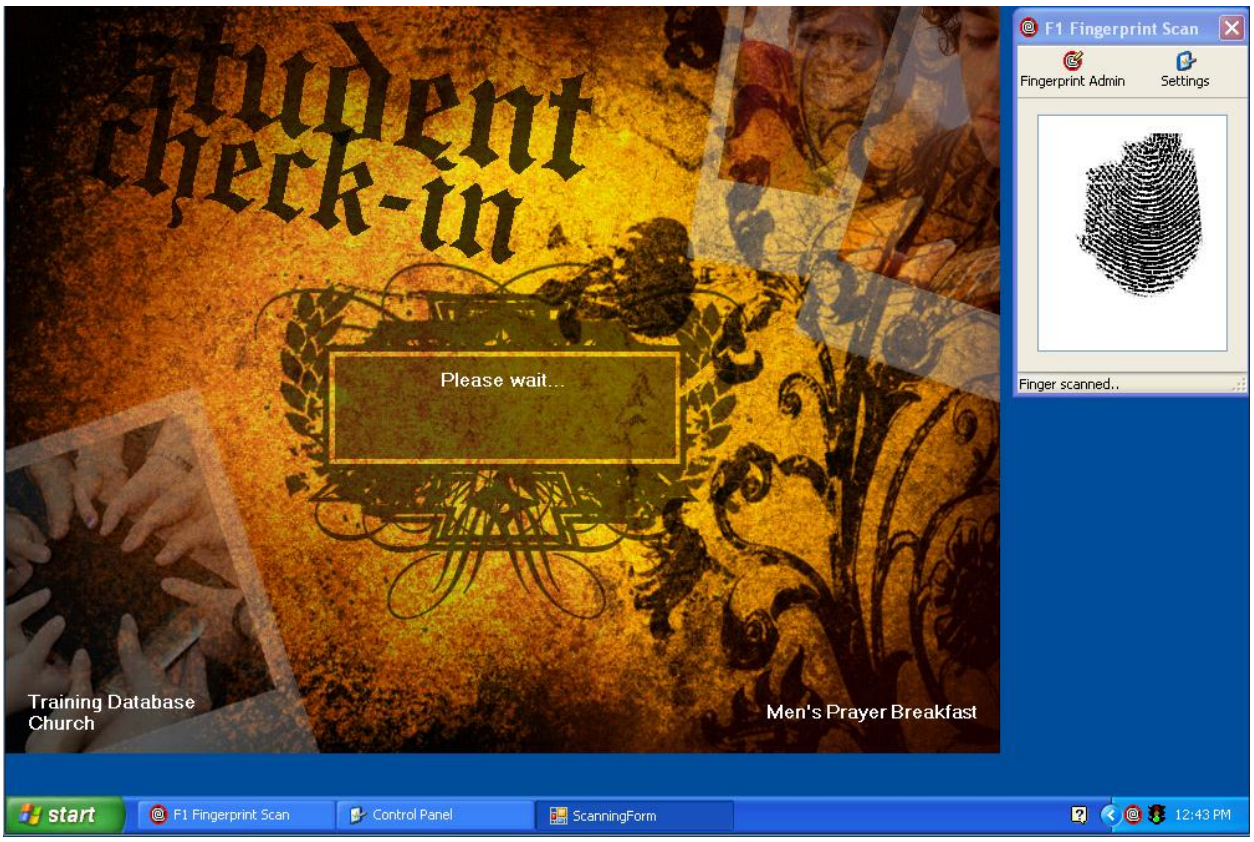

Figure 86 - Fingerprint Scan and Check-in on one Window

1. The standard 800x600 can work with fingerprint scanning since the M2Sys scanning software runs in the back ground.
2. It is also possible to change the screen resolution to 1024X768 and have both Check-in and the Fingerprint Scanner on the screen.

Figure 87 - Basic Check-in Station with Scanner

3. A member will approach the Fingerprint Scanning Check-in station.

Figure 88 - M2Sys Scanner Ready to Use

4. When the Scanner is live and ready to scan the blue backlight will be lit.

Figure 89 - Fingerprint Scan

5. When the individual is ready they will place their finger that they were setup with on to the window.

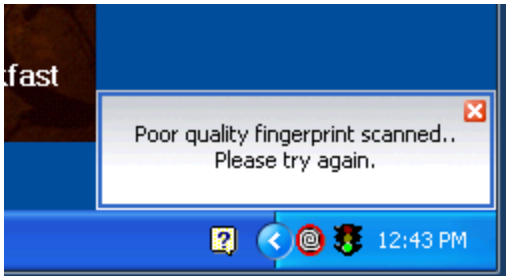

Figure 90 - Fingerprint Scan – Poor Scan

6. If the scan is poor then the above message will be displayed and they will not be checked-in.

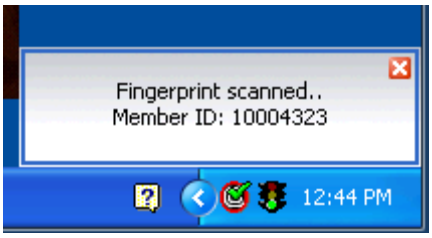

Figure 91 - Fingerprint Scan success

7. If they scan their finger and it is successful then the above message will appear and their tag will print.