PART VIII – INTEGRATION MODULES

Contents

PART VIII – INTEGRATION MODULES 1

CONTENTS 3

INTRODUCTION 5

SAGEM READER USE IN AN IMPRONET SYSTEM 7

General 7

Principle of Operation 7

Hardware Installation of Sagem Readers 8

Electrical Connection of the Sagem Biometric Readers 8

Configuration Notes 10

Configuring the Biometric Enrollment Device 11

Sagem MA100, MA120 or MA500 Internal Parameter Setup Procedure 12

Sagem MA200 or MA300 Internal Parameter Setup Procedure 17

ImproNet Configuration of Sagem Biometric Readers 20

HANDKEY® CR USE IN AN IMPRONET SYSTEM 33

General 33

Principle of Operation 33

Hardware Installation of HandKey® CR Readers 34

Electrical Connection of the HandKey® CR Readers 35

Configuring the Biometric Device 38

B-SHO FINGERPRINT TERMINALS USE IN AN IMPRONET SYSTEM 43

General 43

Principle of Operation 43

Hardware Installation of B-SHO Fingerprint Terminals 44

Electrical Connection of the B-SHO Fingerprint Terminal 45

Configuring the Biometric Device 46

Introduction

This section describes integration of the following third-party systems with ImproNet:

- Various **Sagem** Fingerprint and Registration Readers, integrated with ImproNet via the Biometric Server Software.
- The **HandKey®** CR Reader, integrated with ImproNet via the Biometric Server Software.
- **B-SHO** Fingerprint Terminals, integrated direct to the Access Module.

The introduction of biometric access control greatly increases the access control capabilities of ImproNet Systems where you need extra security measures.

Some Biometric Readers are not supported by the Biometric Server Software. Table 1 below gives Biometric Reader support information.

Biometric Reader	Biometric Server Software Support	Number of Users	Firmware Supported	Approved Terminals	Enrollment
MorphoAccess™ MA100	**YES**	500	2.07.09	See Note 3	Access
MorphoAccess™ MA120	**YES**	500 (see Note 1)	2.07.09	See Note 3	Access (see Note 4)
MA200 Fingerprint Reader	**YES**	800	5.53	See Note 3	Access
MA220 Fingerprint Reader	**YES**	800 (see Note 1)	5.53	See Note 3	Access (see Note 4)
MA300 Fingerprint Reader	**YES**	48 000 (see Note 2)	5.53	See Note 3	Access
MA500 Fingerprint Reader	**YES**	3 000 to 50 000	2.07.09	See Note 3	Access
MA520 Fingerprint Reader	**YES**	3 000 to 50 000 (see Note 1)	2.07.09	See Note 3	Access (see Note 4)
HandKey® CR	**YES**	31 000	TBA	TBA	Access
Schlage HandKey 2	No				
B-SHO Fingerprint Terminal	No	TBA	TBA	TBA	Access
B-SHO Registration Reader	No	TBA	TBA	TBA	Access

Table 1 – Biometric Readers Supported by the Biometric Server Software

Note 1—Limited by the number of Tags supported by the Controller.
Note 2—Limited to 3 000 users per Database, with a maximum of 16 Databases supported.
Note 3—The ImproX PT, ImproX TA, ImproX TRT and ImproX MfT each offer a Third-party Port approved for use with the Biometric Reader.
Note 4—Enrollment is carried out in Access, using a MIFARE® Registration Reader and Tags.

The Biometric Server Module lets the System Administrator configure various third-party Biometric Readers for use with ImproNet. The Module also allows for the direct enrollment (registration) of Tagholders and related biometric data at those Biometric Readers from within the ImproNet Software.

Sagem Reader Use in an ImproNet System

General

This section guides you step by step through the process of setting up Sagem Biometric Readers to work with the ImproNet System. The requirements for the integration are as follows:

- IXP400 Access Control System.
- ImproNet V7.60 Installed.

There are five steps in configuring the Biometric Readers to work with ImproNet. These are:

1. Hardware installation of the Biometric Readers.
2. Software setup of the Biometric Readers using the Biometric Server Software.
3. Detection of the Biometric Readers on the TCP/IP bus.
4. Setting up the Enrollment Reader.
5. Enrolling users on the System.

Sagem enrollment is not yet supported when using the Windows® Vista (Business or Ultimate) operating system.

Sagem Documentation

Sagem documentation for these units can be found on the supplied ImproNet Installation CD. This information references the Sagem documentation where necessary.

Principle of Operation

Figure 1 shows the data flow when using a Sagem Reader with ImproNet.

Figure 1 – Data Flow when using a Sagem Reader with ImproNet

Hardware Installation of Sagem Readers

MA100, MA120, MA200, MA300, MA500 and MA520 Connections

Each Sagem Reader must connect to the LAN to send and receive templates from the ImproNet Database. The Sagem Reader must also connect to an associated ImproX Terminal (such as the ImproX PT, TA, TRT or the MfT) thus facilitating communication with the Controller. Please install the Sagem Readers as outlined in the associated Sagem Hardware Installation Manual.

Electrical Connection of the Sagem Biometric Readers

Connection to the ImproX TRT

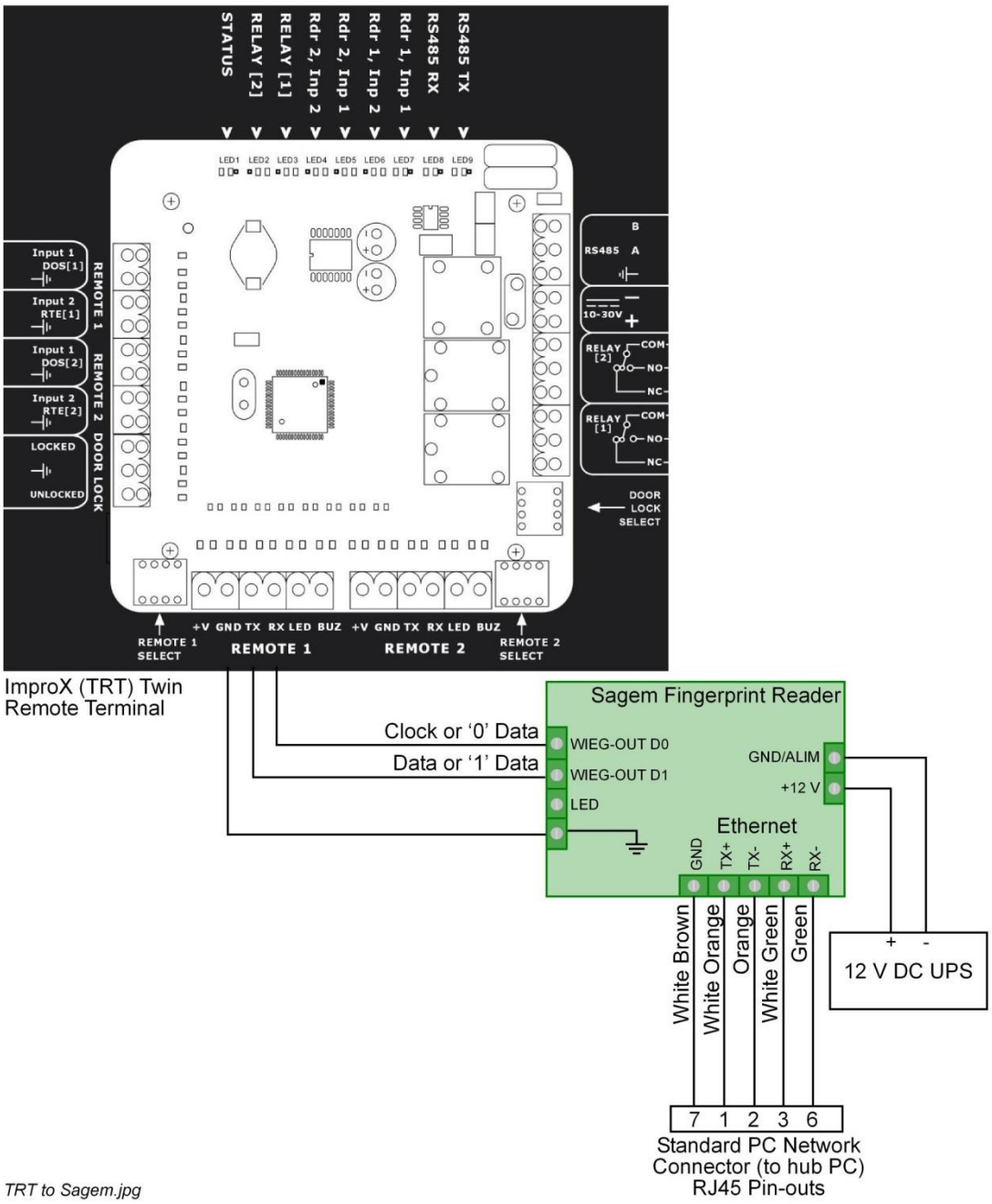
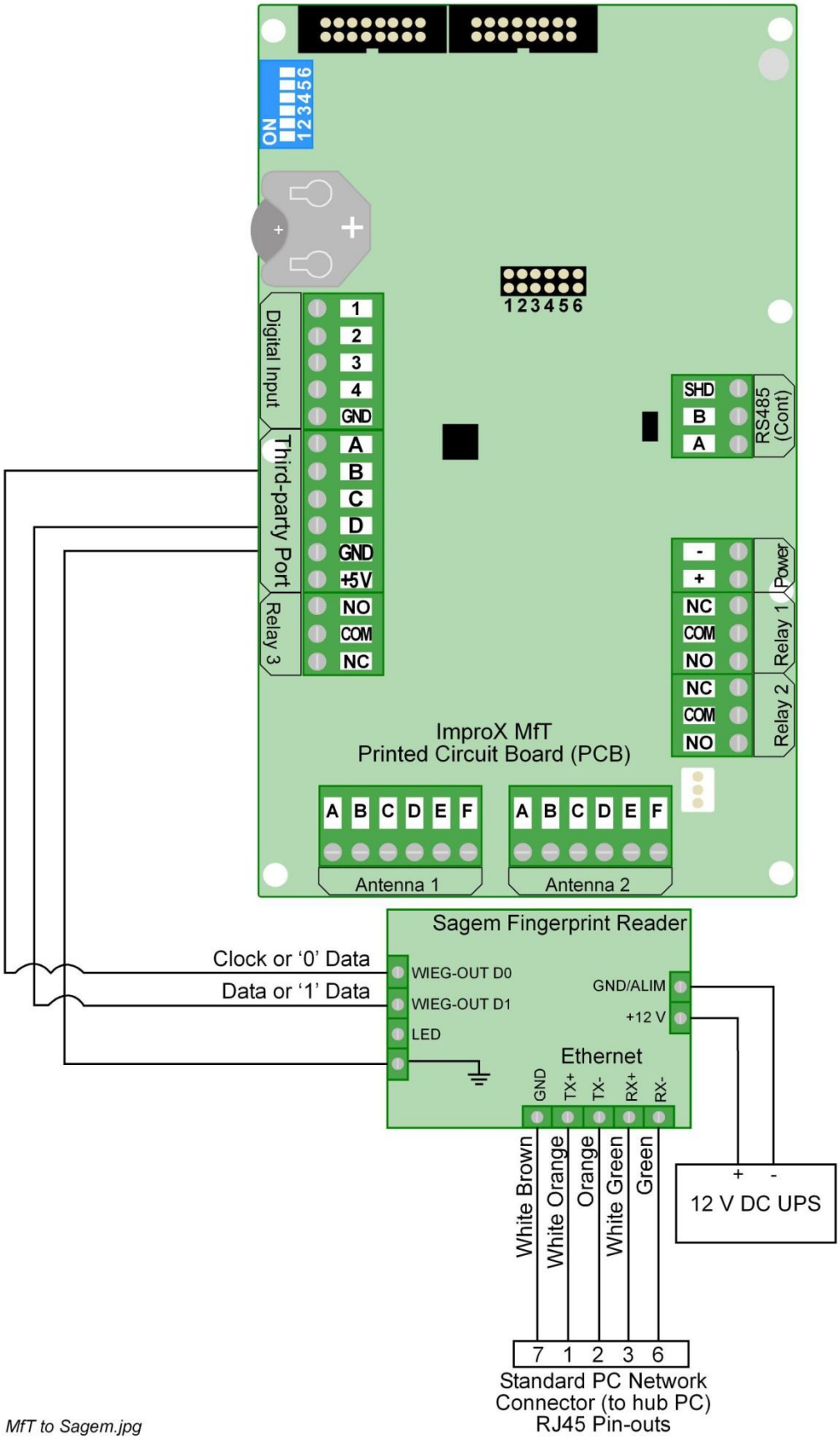


Figure 2 – Sagem Reader [MA100, MA200, MA300, MA500 or MA520] Connected to the ImproX TRT and LAN

Connection to the ImproX MfT



MfT to Sagem.jpg

Figure 3 – Sagem Reader [MA100, MA200, MA300, MA500 or MA520] Connection to the ImproX MfT and LAN

Connection to the ImproX PT or ImproX TA

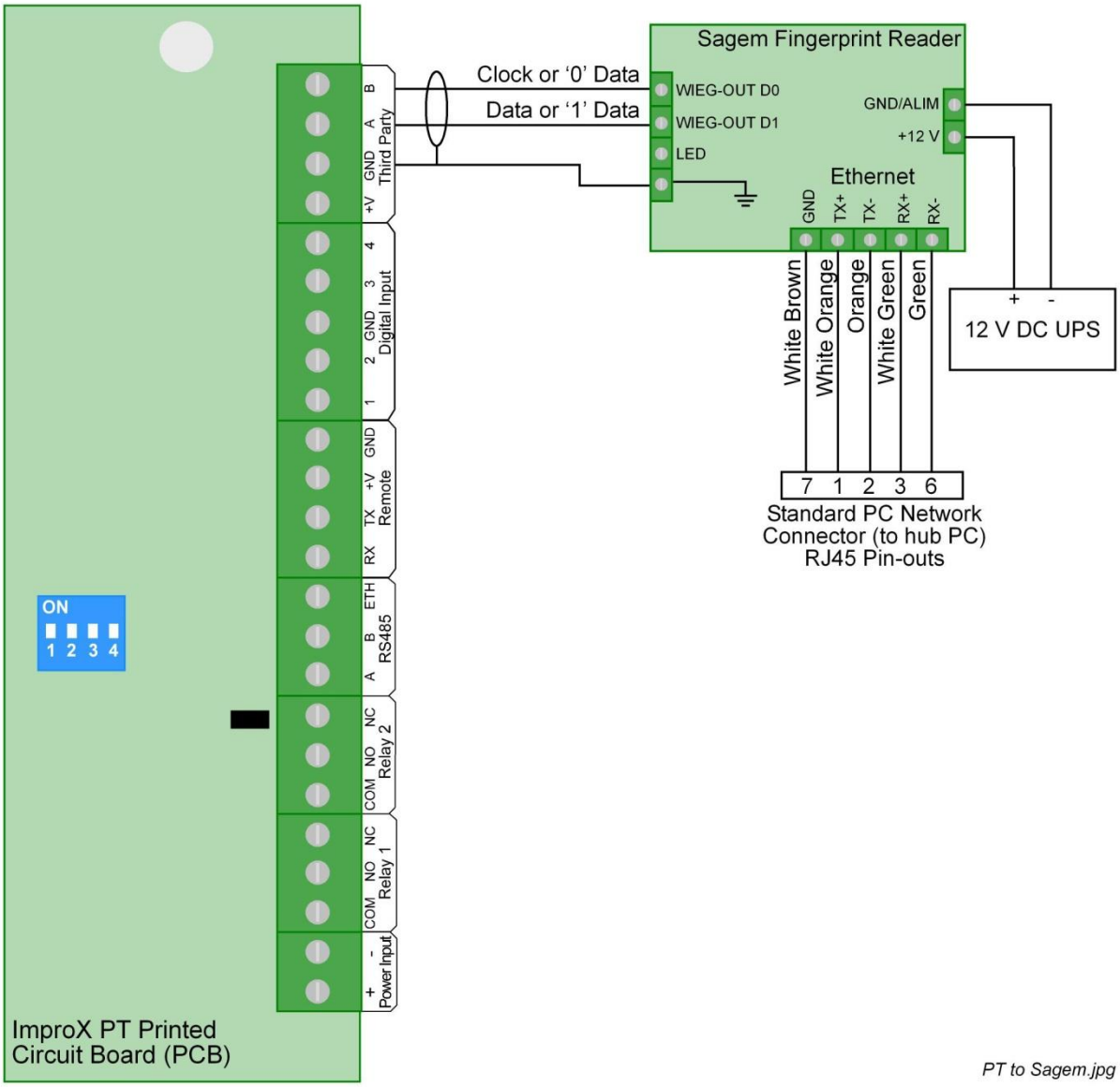


Figure 4 – Sagem Reader [MA100, MA200, MA300, MA500 or MA520] Connected to the ImproX PT or ImproX TA and LAN

Configuration Notes

Before configuration into an ImproNet System, internally configure each Sagem Reader as described here.

The setup procedures for each of the named Biometric Readers differ slightly from Reader to Reader.

Configuring the Biometric Enrollment Device

Sagem MA100, MA200 and MA300 Biometric IP Address Configuration

Change IP Address as follows. The default address is **0.0.0.0.**

1. In Windows®, click **Start**>**Programs**>**ImproNet**>**Access**.
2. From the Menu Bar, select **Configuration**>**Biometric Addresses**.

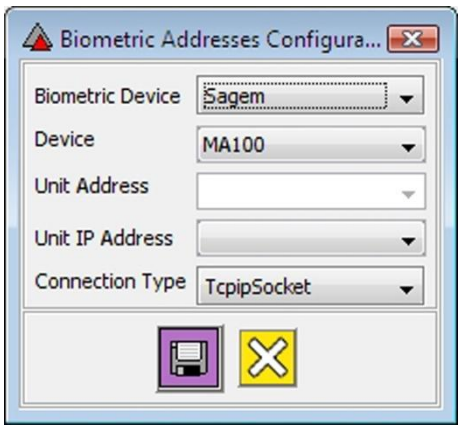


Figure 5 – Biometric Addresses Configuration Dialog

If this option appears greyed purchase a Biometric Unlock Code from your Impro distributor.

3. From the **Biometric Device** drop-down list. Select **Sagem**.

In future versions of this Software, this list will detail other biometric devices that can be integrated with ImproNet, and will allow you to set up the enrollment units for each biometric device.

4. From the **Device** drop-down list, select the type of Sagem unit on which you wish to enroll Tagholders.

*The default is the **MorphoSmart™ MSO300** using the licensed verification dongle. If you are not using the verification dongle for enrollment, then select the type of unit you are going to use. If you select the **MSO300** option, a dialog pops up asking for the Com Port and Baud Rate. Keep the Baud Rate set at **115200** but change the Com Port to the Com Port you connected the MorphoSmart™ to.*

The Unit Address field appears greyed out for Sagem, as it refers to addresses of units on the RS485 bus, Sagem does not currently support RS485.

5. In the **Unit IP Address** field, enter the **IP Address** of the Sagem Enrollment Reader **only** if you are using an MA100, MA120, MA200 or MA300.

The MSO300 has no IP Address.

6. Click on the button.
7. Click on the button.

You may set up a separate Enrollment Reader for each PC on the system running Access. For each of these PCs repeat steps 1 to 7 above.

For MA100, MA120 or MA500 Biometric Readers, go to the section titled Sagem MA100, MA120 or MA500 Internal Parameter Setup Procedure see page 12.

For MA200 or MA300 Biometric Readers, go to the section titled Sagem MA200 or MA300 Internal Parameter Setup Procedure see page 17.

Sagem MA100, MA120 or MA500 Internal Parameter Setup Procedure

USB Flash Disk Setup

Using a **USB Flash Disk** that is smaller than **512 MB**:

1. Format the Flash Disk in **FAT16**.
2. Assign the Flash Disk a **name** of no more than **12 characters**.
3. Browse to **C:\Impronet\Driver\Tools\Sagem\USB Network Tools**.
4. Double-click on the **USBNetworkTool.exe** file.

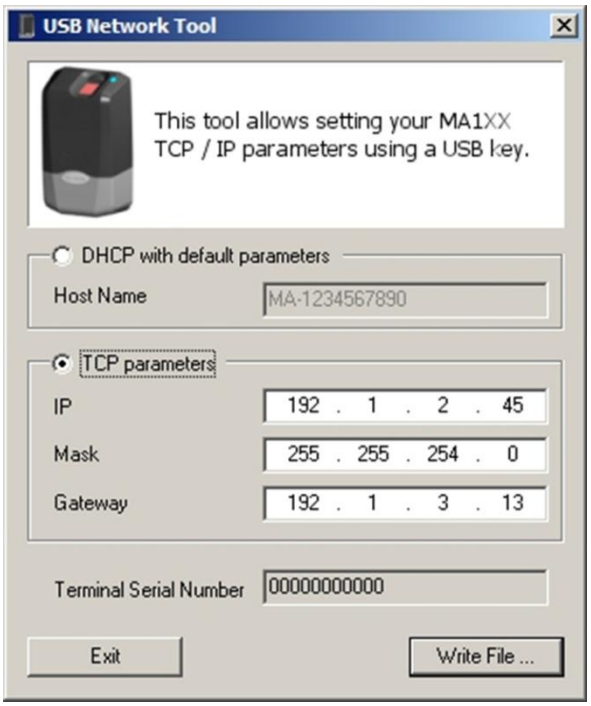


Figure 6 – USB Network Tool Dialog

5. In the USB Network Tool dialog, under TCP Parameters complete the following details:
   - In the **IP** field, assign an available **IP Address** for your network
   - In the **Mask** field, give details for the **Subnet mask**
   - In the **Gateway** field, give details for the **Default Gateway**

If you are in any doubt as to where to source this information, please contact your network administrator for assistance.

*You cannot at this time edit the **Terminal Serial Number** field.*

6. Click the **Write File** button.
7. In the Save As dialog, from the **Save In** drop-down list, select your pre-formatted **USB Flash Disk**.
8. In the **File Name** field, give the file a name.

*The file saves as a ***.reg** file.*

9. Plug the USB Flash Disk into the front of your MA100.

During the file download process the MA100's Buzzer beeps and the LED changes colour.

Do NOT remove the USB Flash Disk until the downloads complete. *On completing the download, the MA100's Buzzer emits a deep tone and the LED slowly flashes Blue.*

Setting up the Wiegand Configuration on an MA100 or MA500

1. Browse to **C:\Impronet\Driver\Tools\Sagem\Configuration Tool**.
2. Double-click on the **ConfigurationTool.exe** file.

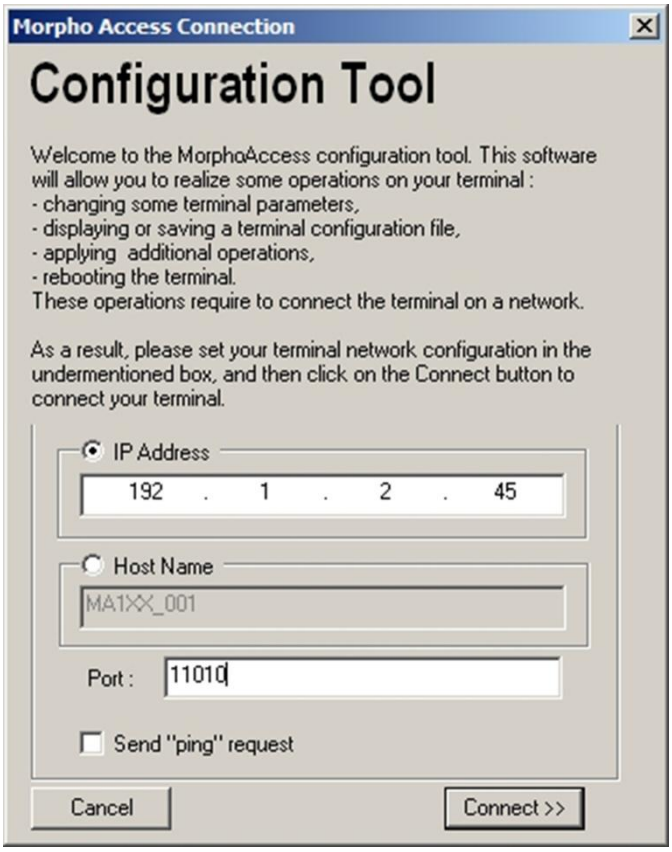


Figure 7 – Configuration Tool Dialog

3. In the Morpho Access Connection dialog, ensure that the **IP Address** field reflects the same IP Address details as used in point 5 on page 12.

4. Click the **Connect >>** button.

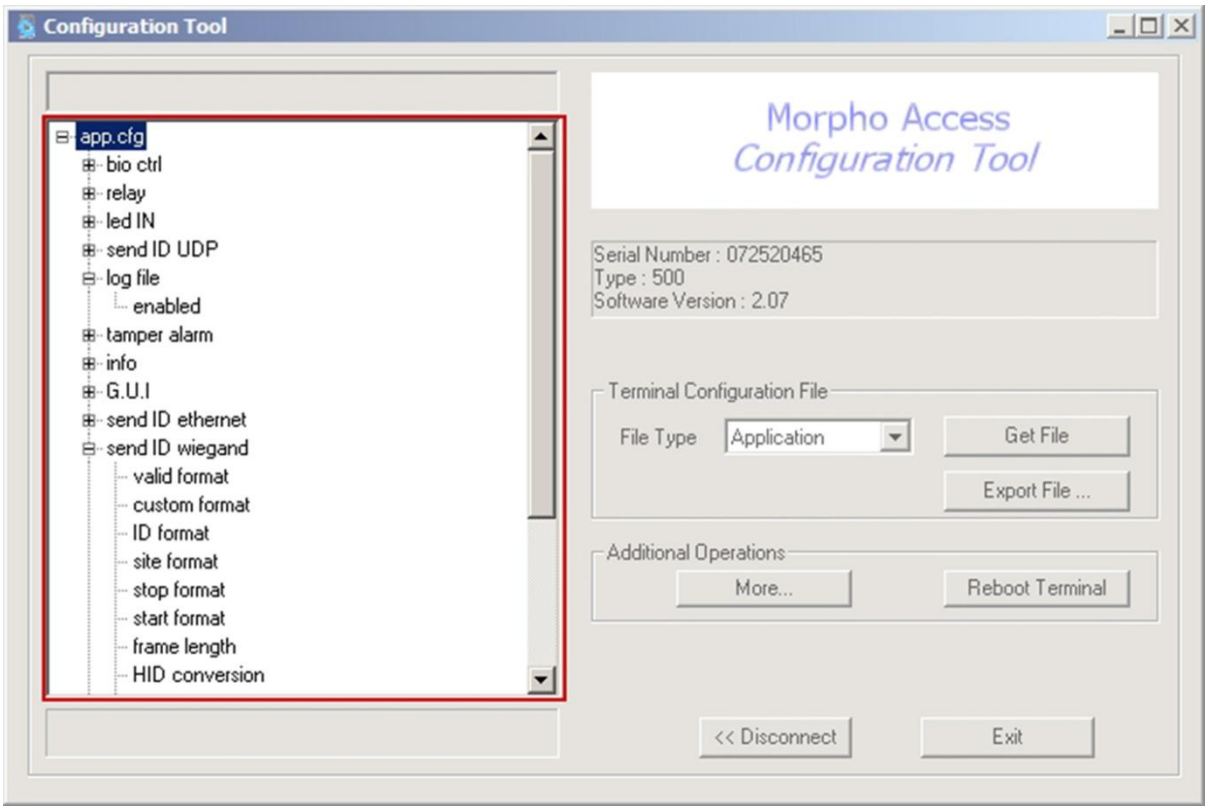


Figure 8 – Configuration Tool Dialog

5. In the Configuration Tool dialog, click the **Get File** button.

*The setting referred to in point 6 (only available on sites using MA100 and MA500 Sagem Readers) is required for the functionality of the **Sagem Identify Report**. In Installations without installed MA100 and MA500 Sagem Readers, skip direct to point 8.*

6. From the Directory Tree, double-click the **Log File** setting.
7. Double-click on the **Enabled** setting and adjust the value to **1**.
8. From the Directory Tree, double-click the **send ID wiegand** setting.
9. Double-click on the following settings to adjust their values:
   - valid format—**1**
   - custom Format—**0.0**
   - ID format—**1.24**
   - site Format—**0.0**
   - stop Format—**3.12**
   - start Format—**2.12**
   - frame length—**26**
   - HID Conversion—**0**
   - site code—**0**
   - enabled—**1**
10. Apply the settings by **rebooting the Terminal**.

Problems and Solutions

1. ***Problem***—*Wiegand Code not sent through.*
   Solution—Swap your Data 1 and Data 0.

2. ***Problem***—*Wiegand Code not sent through.*
   Solution—Check each setting in the **App** file according to the following list:

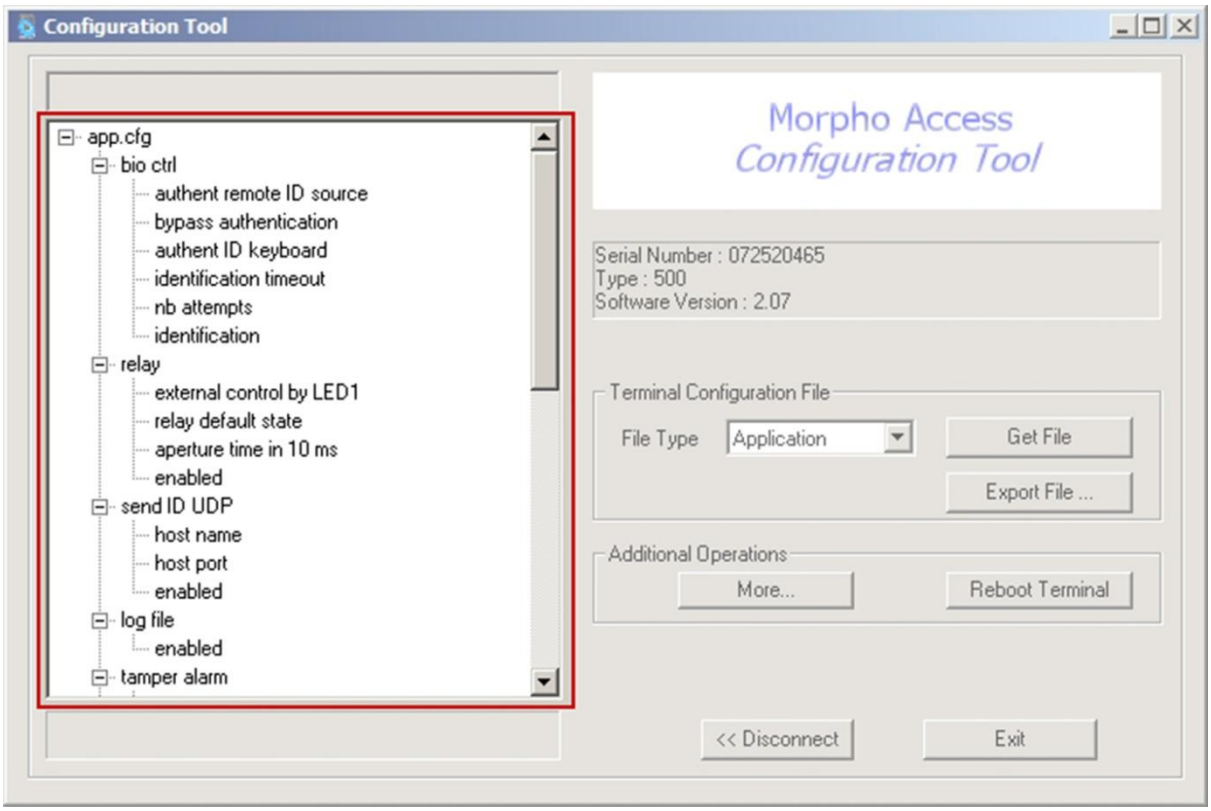


Figure 9 – Configuration Tool Dialog

- **bio ctrl**
  - authent remote ID source—**5**
  - bypass authentication—**0**
  - authent ID keyboard—**0**
  - identification timeout—**5**
  - nb attempts—**2**
  - identification—**1**
- **relay**
  - external control by LED—**0**
  - relay default state—**0**
  - aperture time in 10 ms—**300**
  - enabled—**1**
- **send ID UDP**
  - host name—**134.1.2.189**
  - host port—**11020**
  - enabled—**0**
- **log file**
  - enabled—**1**

- **tamper alarm**
  - interval—**1500**
  - level—**0**
- **G.U.I**
  - display hour—**0**
  - LED out signal—**0**
  - Time and attendance icons—**1**
  - database conversion—**500**
  - display user info—**2**
  - default language—**0**
  - volume—**5**
- **info**
  - type—**500**
  - release—**9**
  - minor—**7**
  - major—**2**
- **send ID ethernet**
  - connect timeout—**2000**
  - profile ID—**0**
  - SSL enabled—**0**
  - controller on no responce—**1**
  - timeout back to controller 1—**3600**
  - controller 2 timeout—**2000**
  - controller 2 port—**11020**
  - controller 2 IP—**134.1.2.189**
  - controller 1 timeout—**2000**
  - controller 1 port—**11020**
  - controller 1 IP—**134.1.2.189**
  - mode—**0**
- **send ID wiegand**
  - valid format—**1**
  - custom format—**0.0**
  - ID format—**1.24**
  - site format—**0.0**
  - stop format—**3.12**
  - start format—**2.12**
  - frame length—**26**
  - HID conversion—**0**
  - site code—**0**
  - enabled—**1**
- **send ID dataclock**
  - card present signal—**0**
  - data inverted—**0**
  - clock inverted—**0**
  - enabled—**0**
- **send ID serial**
  - display duration—**3**
  - reply timeout—**5**
  - wait reply—**0**

  - mode—**485**
  - terminal identifier—**178**
  - priority—**0**
  - stopbits—**1**
  - databits—**8**
  - speed—**11520**
  - enabled—**0**
- **failure ID**
  - send ID mask—**255**
  - not on time ID—**65535**
  - generic error ID—**65535**
  - timeout ID—**65535**
  - not in DB ID—**65535**
  - not recognized ID—**65535**
  - alarm ID—**65535**
  - enabled—**0**
- **wiegand in**
  - custom format—**0.0**
  - ID format—**9.16**
  - site format—**1.8**
  - stop format—**2.12**
  - frame length—**26**
  - check site code—**1**
  - site code—**7**
- **data clock in**
  - data inverted—**0**
  - clock inverted—**0**
- **led IN**
  - controller ack timeout—**300**
  - enabled—**0**
- **modes**
  - time mask—**0**
  - time and attendance—**0**

Sagem MA200 or MA300 Internal Parameter Setup Procedure

General

Set up the internal parameters for MA200 and MA300 Biometric Readers using the built-in Display and Keypad. In order to carry out this procedure, please refer to: Sagem MA200/300 MorphoAccess Installation Guide, SK-0000011145-03 – January 2004.

Notes on Set-up for Sagem MA200 or MA300

The information that follows takes you through the Sagem Manual, indicating which information applies to the use of the Biometric Reader with ImproNet, and which does not.

Internal Sagem Configuration Steps

The internal configuration steps of the MA200 or MA300 into the ImproNet System include:

1. Configure the **Switches** on the motherboard.
2. Configure the **Software Administration Interface**.
3. Perform **Sagem System Set-up Actions** (biometric management operations).
4. Configure the Biometric Reader using the **Sagem CONFIG Menu**.

Table 2 lists all headings in the Sagem manual, and indicates whether, and how, this information relates to the Sagem-ImproNet integration process.

*The Sagem MA200 or MA300 Manual headings are listed **sequentially** in Table 2 as a guide to the use of the Sagem manual in this application. However, in some cases the most convenient order for the integration process is different. In these cases the PROCEDURE or COMMENTS column will refer you to the STEP in which this information is used.*

STEP DESCRIPTION	SAGEM MANUAL HEADING	PROCEDURE OR COMMENTS
1. PHYSICAL INSTALLATION	INSTALLATION PROCEDURE	Follow the Sagem Manual procedures.
2. ELECTRICAL CONNECTION	ELECTRICAL INTERFACE	The Sagem Interfaces used in this application are J1, J3 and J4 (Refer to the Sagem Manual). See Figure 2, Figure 3 and Figure 4 in this manual.
	Terminal Block Board	Background Information
	Power Supply Cable	See Figure 2, Figure 3 and Figure 4 in this manual.
	Ethernet Wiring	See Figure 2, Figure 3 and Figure 4 in this manual.
	Wiegand Output Wiring	See Figure 2, Figure 3 and Figure 4 in this manual.
	Output Relays and Tamper Switch	Optional, depends on user requirements. Follow the instructions in the Sagem Manual if required.
	CONFIGURING THE MORPHOACCESS™	
	Motherboard Configuration	Refer to the Sagem Manual. Configure the Switches as follows: Set SW1 and SW2 for Wiegand Mode. Set SW3 and SW4 as indicated in the Sagem Manual. Set SW7 and SW8 for Wiegand Mode.
	MORPHOACCESS™ SOFTWARE	Refer to step 5 of this Table.

STEP DESCRIPTION	SAGEM MANUAL HEADING	PROCEDURE OR COMMENTS
3. INTERNAL SETUP OF THE READER BEFORE INTEGRATION AND USE WITH IMPRONET	BIOMETRIC MANAGEMENT OPERATIONS	Refer to the Sagem Manual, "Access the Set up Functions of the System", but ignore the following headings: • Biometric Management in Stand Alone • Insert Template/ID in Database • Remove Template/ID from Database
	THE CONFIG MENU	Refer to the Sagem Manual.
	SETTING UP NETWORK PARAMETERS	Refer to the Sagem Manual.
	SETTING UP THE SYSTEM ADMINISTRATOR PIN	Refer to the Sagem Manual. This PIN provides access to the SYSTEM Menus in the Sagem Software for administration of the Reader.
	SETTING UP THE MORPHOACCESS™ ADMINISTRATOR PIN	Refer to the Sagem Manual. This PIN provides access to the MACCESS Menus in the Sagem Software for administration of the external management.
	Setting Up Host Communication	Refer to the Sagem Manual. Set the Host Com value to 3.
	Setting Up User Interface	Refer to the Sagem Manual.
	Setting Up Wiegand or Dataclock Output	Refer to the Sagem Manual.
	Setting Up Wiegand Interface	Refer to the Sagem Manual. The default format is 26-Bit.
	Frame Definition	Refer to the Sagem Manual.
	Configuration Keys	Refer to the Sagem Manual. Set Section is OUT. Set Length is 26.
	Setting Up Etherlink Parameters	Refer to the Sagem Manual. Set Etherlink Send is 1. Set IP Address as required.
	Setting Up Time Attendance	Refer to the Sagem Manual.
4. OPTIONAL SETUP AND BACKGROUND INFORMATION	THE VERSION MENU	Refer to the Sagem Manual.
	THE SERIAL NUMBER MENU	Refer to the Sagem Manual.
	THE SETTING MENU	Refer to the Sagem Manual.
	COMMUNICATION PROTOCOL	Background Information.
	MORPHOACCESS™ TECHNICAL CHARACTERISTICS	Background Information.
	Recommendations	Background Information.
	Ethernet Colour Standard	Background Information.
	Appendix 2	Background Information.
	Appendix 4	Background Information.
	APPENDIX 5 – FINGERPRINT PLACEMENT RULES	Refer to step 6 of this Table.

STEP DESCRIPTION	SAGEM MANUAL HEADING	PROCEDURE OR COMMENTS
5. USER INTERFACE SETUP	MORPHOACCESS™ SOFTWARE USER INTERFACE	Refer to the Sagem Manual.
	Access Control by Identification (MA200)	Refer to the Sagem Manual. The Mode is 0.
	Access Control by Identification (MA300)	Refer to the Sagem Manual. The Mode is 0.
	Access Control by Identification (MA200 and MA300)	Optional – use if authentication is used by presentation of Tag to an external Reader.
6. OPERATIONAL INFORMATION	APPENDIX 5 – FINGERPRINT PLACEMENT RULES	Important operational information. Follow the instructions in the Sagem Manual. Ensure that all users are aware of these rules.

Table 2 – Internal Configuration of the Sagem Fingerprint Readers

*For easy reference we listed the Sagem Manual Headings in Table 2 in the order in which they appear in the Sagem Manual. Sections not listed in Table 2 are **NOT** required for ImproNet Integration.*

ImproNet Configuration of Sagem Biometric Readers

Once you've connected the Sagem Readers and configured them internally as described in the previous paragraphs, configure the Readers into the ImproNet System. This section applies to the supported Sagem Fingerprint Readers, the MA100, MA120, MA200, MA300, MA500 and MA520.

Each Sagem Reader used in the Biometric Server requires its own Unlock Token. For details of the unlocking procedure refer to the section titled Sagem Dongle Protection using the Unlock Token on page 25.

The configuration of these Readers within ImproNet is done using the ImproNet Biometric Server Software, as follows:

1. From Windows® select **Start**>**Programs**>**ImproNet**>**Biometric Server**.
2. Enter your **Username** and **Password**.

Figure 10 – Logon Dialog

*The default username is **SYSDBA**. The default password is **masterkey**.*

*When you upgrade an existing ImproNet System to V7.40, you need to tell the new Software what Readers are installed. In this case, a **Unit Not Detected** dialog (see Figure 8) displays. For the units **NOT** detected, specify the unit **Type**.*

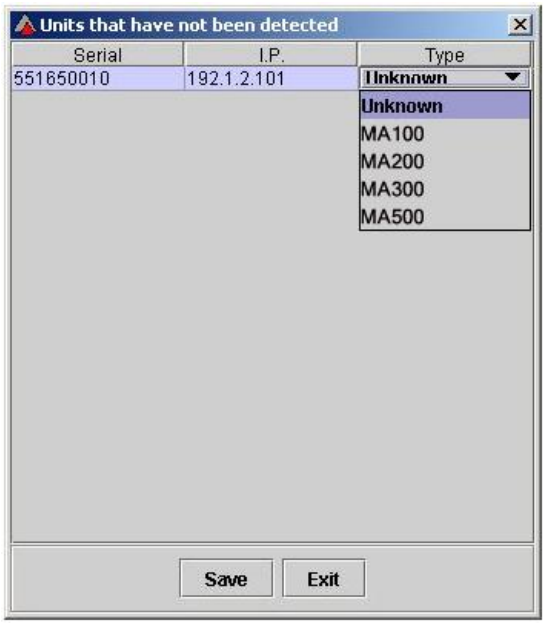


Figure 11 – Units that have not been Detected Dialog

Detecting Sagem Readers on the TCP/IP Bus

This procedure is the same for the MA100, MA120, MA200, MA300, MA500 and MA520.

1. On the **Configuration** menu, select **Sagem**>**Sagem Devices**.

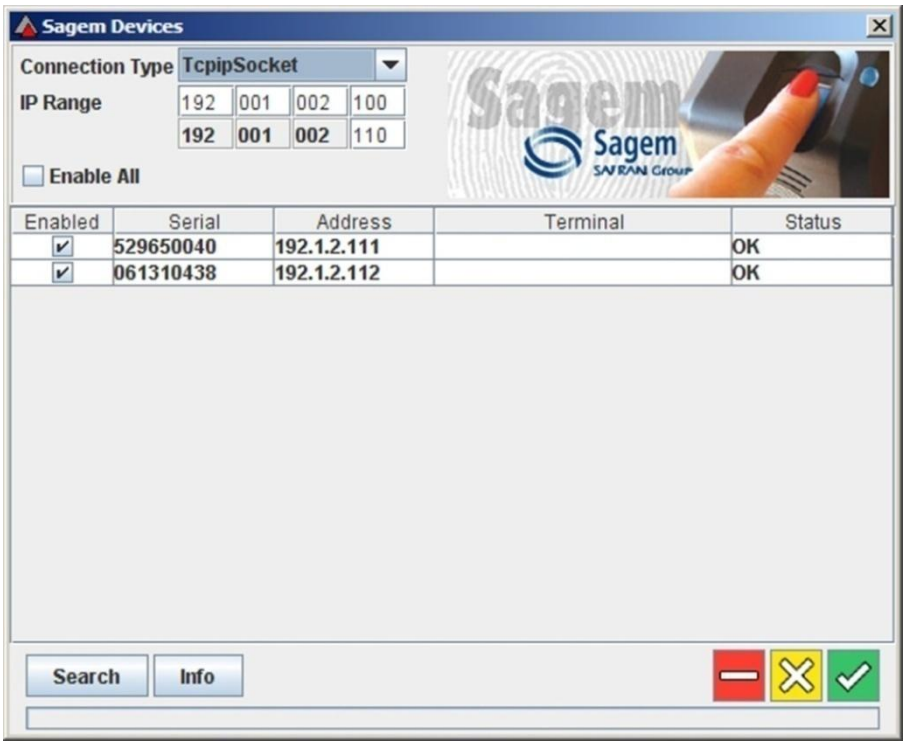


Figure 12 – Sagem Devices Dialog

At the top of the **Sagem Devices** dialog you will see the **Connection Type** drop-down list with **TcpipSocket** selected. This is the only option at this stage (ImproNet V7.40).

2. In the **IP Range** field enter the start and end IP Addresses for the range of Addresses that the Biometric Server must search for.
3. Click the **Search** button.

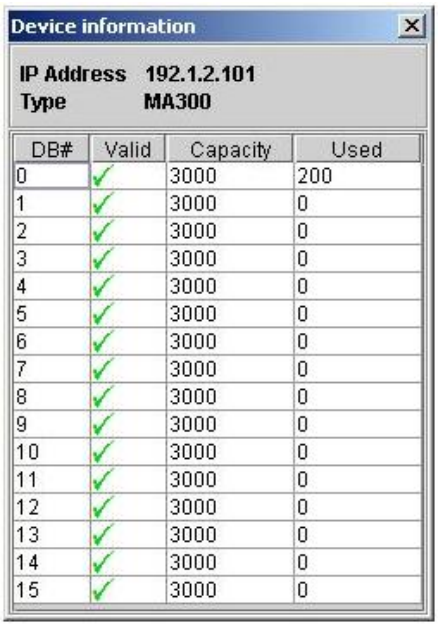
*The **Search** may take some time, depending on how busy the network is. After the Search finds the Sagem units, they appear as records in the table with their Serial Numbers, IP Addresses and their current Status.*

*The **Enabled** checkbox enables or disables each individual Sagem unit on the network. This means that you can carry out repairs on a unit without affecting the rest.*
*The **Enable / Disable All** checkbox enables or disables all the Sagem units on the network.*
The Server will not attempt communication with a disabled Sagem unit.

You will also notice a button in the dialog. This button allows manual deletion of Sagem Readers from the database. Note however, reintroduction of the Sagem Reader requires use of the Unlock Token.

4. A coloured Key, situated above the buttons, displays the colours used to indicate the status of units:
   - All enabled units are Searched automatically
   - All newly discovered units highlight in **Green**
   - All units whose IP Address has changed highlight in **Orange**
   - All units that are in the Database but have been found to be off-line or missing highlight in **Red**

*On enabled Sagem Readers with their status shown as OK, clicking the Info button displays the **Device Information** dialog. This dialog shows the number of templates uploaded to the Sagem Reader and the unused capacity.*



DB#	Valid	Capacity	Used
0	✓	3000	200
1	✓	3000	0
2	✓	3000	0
3	✓	3000	0
4	✓	3000	0
5	✓	3000	0
6	✓	3000	0
7	✓	3000	0
8	✓	3000	0
9	✓	3000	0
10	✓	3000	0
11	✓	3000	0
12	✓	3000	0
13	✓	3000	0
14	✓	3000	0
15	✓	3000	0

Figure 13 – Device Information Dialog

5. When you are finished using the **Sagem Devices** dialog, click the button.
6. Click the button.
7. After setting up the units, do a **Full Upload** to create fresh databases on the units.
8. Now click on the **Start** button to get the Biometric Server running and ready to upload templates as you enroll users.

Biometric Server Queue

All messages to Sagem devices queue so that each device can be processed independently. The **Unit Details** tab shows the queue status and allows you to upload to each unit individually.

This tab is also useful in identifying units having communication problems.

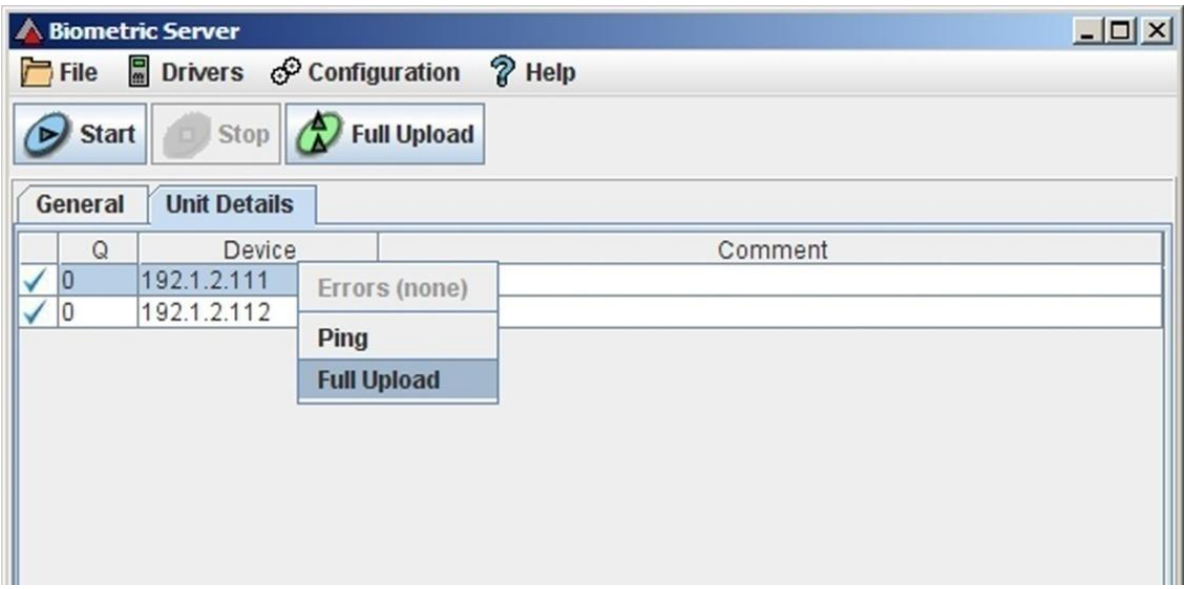


Figure 14 – Unit Details Tab

The queue processes automatically during normal operation (that is after you press the **Start** button). You may perform a full upload on a specific Sagem Reader as follows:

1. Select the unit record for update.
2. From the menu, select the **Full Upload** option.

Duplicate Search (1:N Matching)

From ImproNet V7.60 onwards, the Biometric Server communicates with the Sagem Matcher service. This communication structure enables duplicate search functionality.

To use this service, ensure that you have a MorphoSmart™ MSO300 Registration Reader and either an **IDENT LITE** (3 000 templates) or **IDENT PLUS** (20 000 templates) licence.

Installing the Service

Only install the Sagem Matcher Service on the PC running the Biometric Server Software.

In a default installation (from **C:\ImproNet\Driver)** run the **AddMatcherService.bat** script. After execution, enable the Matcher service using the standard Windows Services dialog.

Enabling the Service

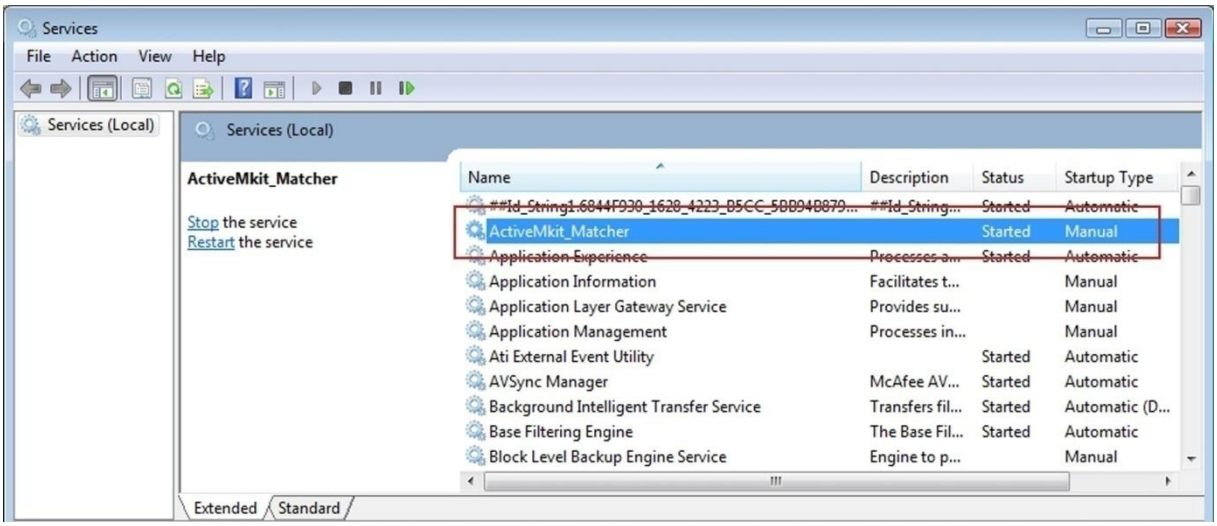


Figure 15 – Services Interface

1. Access the Services dialog using **Windows® XP**, by going to: **Start**>**Control Panel**>**Administrative Tools**>**Services**.
2. From the Services dialog, select the **ActiveMkit_Matcher** service.
3. Right-click over the Service and from the shortcut menu, select **Properties**.
4. On the General tab, from the Startup Type drop-down list, select **Automatic**.

*Start the **ActivMkit_Matcher** service before running the Biometric Server Software.*

5. If the Service is not already started, start the service now, by right-clicking over the Service and from the shortcut menu, select **Start**.

Enabling Matcher in the Biometric Server Software

1. Start the Biometric Server Software (for more information, see page 20.
2. From the menu bar, select **Configuration**>**Sagem**>**Matcher**.

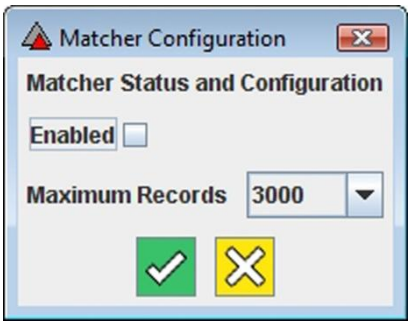


Figure 16 – Matcher Configuration Dialog

3. In the Matcher Configuration dialog, select the **Enabled** checkbox.

4. From the **Maximum Records** drop-down list, select the maximum number of records supported by your IDENT LITE or IDENT PLUS licence.
5. Click the button.
6. Restart the Biometric Server Software for the changes to take effect.

The Biometric Server opens a TCP/IP server on Port 26670 for all Matcher related communications.

For an existing site, with templates already loaded, the Matcher uncompresses all your existing templates into a format easily searched and stored in the Matcher database. This process can take some time to complete but only needs completion once. If you cancel the conversion process at any stage, the process halts and automatically continues from where stopped when you next run the Matcher service. All future templates are stored in the required format at enrollment stage.

Enabling Duplicate Search at an Enrollment Station

For detailed steps on arriving at the Biometric Enrollment dialog, refer to page 27.

1. In the Biometric Enrollment dialog, click the **Advanced** button.
2. Select the **Enable Duplicate Check** checkbox.
3. Click the button
4. Restart the Access Module for this change to take effect.

*Ensure the **Biometric Server Software is running** for checking to take place.*

If the Matcher Service does NOT find a matching record, the records added to the Matcher Database. If the Matcher Service finds a matching record, an Error message gives you the matching records Tag code.

Sagem Dongle Protection using the Unlock Token

*Only ImproNet Software V7.40 (with service packs **ImproNet_ESU_20070620.exe** and **update-ImproNet-7.40-20070620.exe**) upwards supports the use of the Unlock Token.*

Only the ProxMate (any Firmware version) or USB Registration Readers with Firmware V1.14 upwards support the use of the Unlock Token.

On initial use, ANY Unlock Token of the correct type unlocks ANY Sagem Reader of the same type. That is, any MA100 Unlock Token unlocks any MA100 Sagem Reader, and any MA200/300 Token unlocks any MA200, MA300 or MA500 Sagem Reader. However, once an Unlock Token is used with a specific Sagem Reader, the Unlock Token is permanently associated to that Reader. Ensure that you keep your supplied Unlock Tokens labelled and in a safe place.

The Unlock Token supplied with third-party integrated products, shows the products have our full factory level approval. This means the products work seamlessly with ImproNet, with central enrollment taking place in the ImproNet Tagholder Enrollment screen.

The Token allows you access to extra integration features related to the Sagem Readers. These features include:

- Intelligent distribution of templates (uploading of templates only to Readers where the Tagholder has access).
- Sagem Capture Quality Report (implemented in ImproNet V7.60).

To unlock Sagem Readers enabled in the Biometric Server, continue as follows:

1. From Windows® select **Start**>**Programs**>**ImproNet**>**Biometric Server**.
2. Enter your **Username** and **Password** (this is only required on first-time use of the Biometric Server Software).

*The default username is **SYSDBA**. The default password is **masterkey**.*

3. In the **Licence Info** dialog, click the **Unlock** button.
4. Place your **Unlock Token** in position in the Tag Registration Reader.
5. In the **Sagem Device Unlock** dialog, click on the **Read** button.
6. Click on the **OK** button.

On unlock, the Biometric Server Software opens allowing full use of the Software.

Installation of the MSO300 Enrollment Reader and Verification Dongle for ImproNet V7.40 Upwards

These steps are normally, automatically, carried out during the ImproNet installation. However if for any reason you need to install the MSO300 Enrollment Reader and Verification Dongle manually continue as outlined below.

The MSO300 is the preferred dedicated Enrollment Reader for desktop use. You may also configure the MA100, MA200 and MA300 for use as Enrollment Readers, however, remember that using these units could lead to uploading and quality (false rejection or acceptance) problems.

If connected, disconnect the MSO300 Enrollment Reader and the Verification Dongle from the PC.

Install the drivers, before you plug in the MSO300 or Verif Dongle.

Upgrading from Earlier Version of ImproNet

When upgrading to V7.60 from V7.40 or earlier, ensue that you carry out the following steps:

1. Unplug both the MSO300 and the Verif Dongle.
2. Go to **Start**>**Control Panel**.
3. Select **Programs and Features**.
4. Select the **Sentinel Protection Installer Driver**.
5. Click the **Uninstall** button.
6. Select the **Sagem MorphoSmart USB Driver**.
7. Click the **Uninstall** button.

8. Click the button.

MSO Driver

1. Browse to **C:\ImproNet\driver\Sagem MorphoSmart USB Driver**.
2. Double-click the **setup.exe** file.
3. Follow the on-screen prompts.
4. At the end of the installation click the **Finish** button.

Verif Driver

1. Browse to **C:\ImproNet\driver\SafeNetDongle**.
2. Double-click the **SentinelProtectionInstaller.7.4.0(DriversOnly).exe** file.
3. In the Sentinel System Driver Setup dialog, click the **OK** button.

The Installer exits when installation of the Driver's complete.

MSO300 Enrollment Reader

1. Plug in the **MSO300 Enrollment Reader** into an unused USB Port on the PC.

Some PC's proceed with automatic installation of the MSO300, if installation occurs automatically move direct to step 4 below.

2. Follow the on-screen prompts, instead of letting the Installer run automatically, select **Install from a Specific Location**.
3. Browse to **C:\Program Files\SAGEM SA\MorphoSmart Drivers,** this folder contains the drivers for the MSO300.
4. After installation of the Drivers, the LED on the MSO300 blinks Green once a second.

Verification Dongle

1. Now plug in the **Verification Dongle** into an unused USB Port on the PC.
2. The installer runs discreetly and when fully installed, the Verification Dongles Green LED remains permanently on.

With the drivers installed, you can begin enrolling Fingerprint templates into the Database.

Enrolling Users on the System

This information assumes that you are using a Sagem MSO300 as the Registration Reader.

Enrollment in ImproNet

1. From Windows® select **Start**>**Programs**>**ImproNet**>**Access**.
2. In the Navigator Pane, select the **Tagholder** icon.
3. Open the **Edit Tagholder** or **Add Tagholder** dialog.
4. Select **New Tag** to enter the **Tag** dialog.
5. Have the Tagholder place his/her Tag on the Enrollment Reader.
6. Click **Read Tag** (or just enter a number of 7 digits or less in the **Tag Code** field).
7. Click the **Tag Type** drop-down list and select **ASCII, Biometric, Magstripe** from the list.
8. When the dialog pops up, select option **3**, which is **Convert Code to 26 bit Wiegand without Site Code (24 bits)** (ringed in Figure 17).

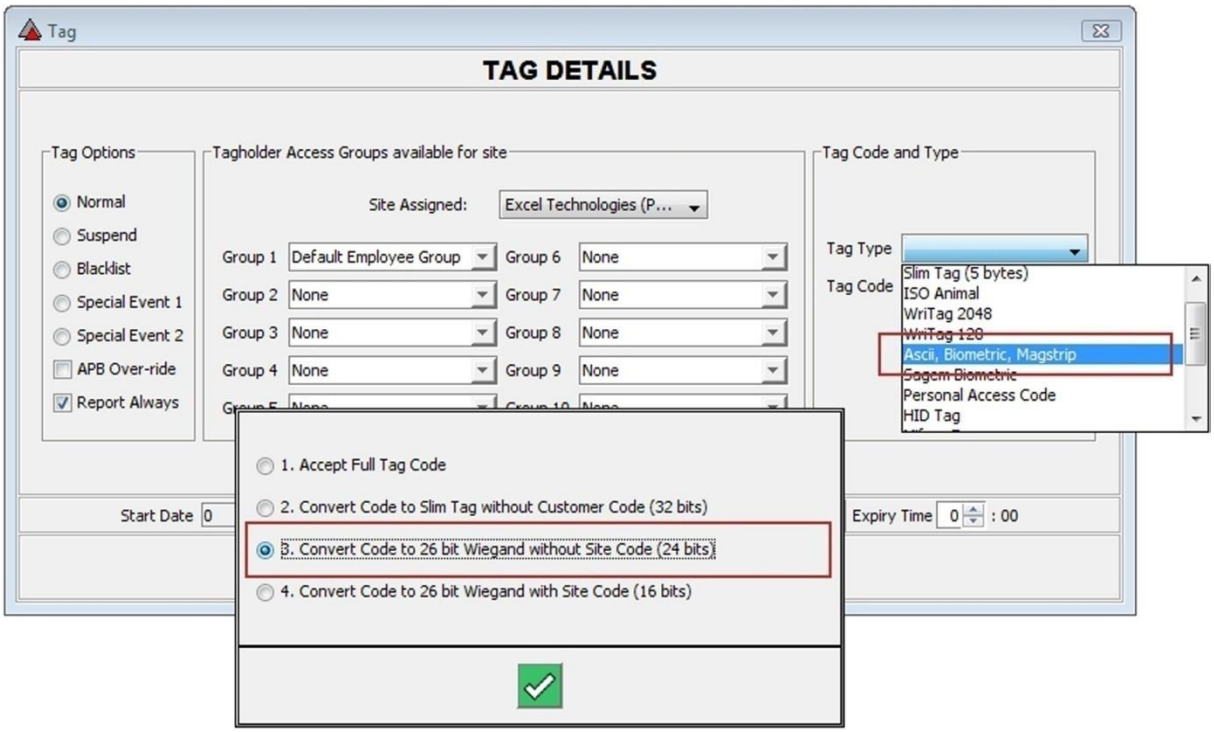


Figure 17 – ASCII, Biometric, Magstripe

9. Set the Access Groups in the usual way.
10. Click on the button.
11. Click on the **Biometric Enrollment** button (see Figure 18).

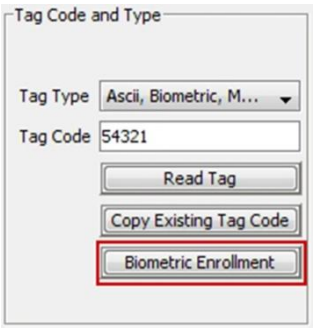


Figure 18 – Extract from Tag Dialog (Ready for Biometric Enrollment)

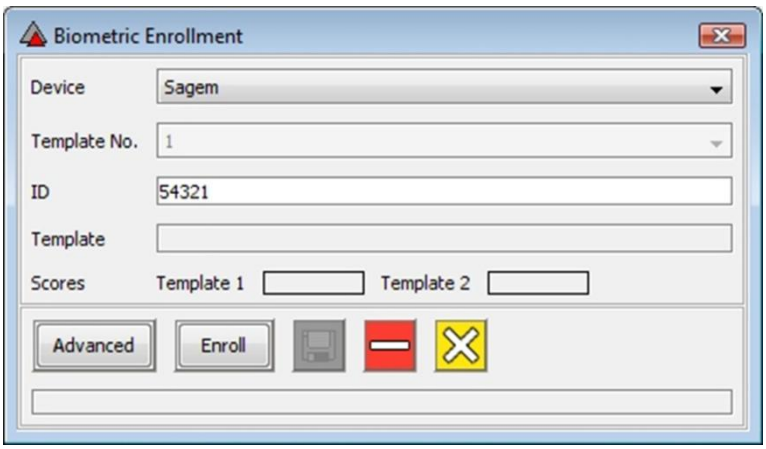


Figure 19 – Biometric Enrollment Dialog

12. In the **Biometric Enrollment** dialog, from the **Device** drop-down list, select the type of device you wish to enroll the user on, in this case **Sagem**.

*The **Template No** field will be greyed out as it does not apply to Sagem units. Other Biometric Devices allow you to enroll multiple templates per user. Sagem units enroll two fingers and store them as one template, not allowing multiple templates per ID.*

*The **ID** field is the ID derived from the Tag Code and is the number under which the user's data is saved when his or her fingerprints are enrolled in the units.*

*The **Template** field remains empty until the enrollments completed.*

13. Click on the **Advanced** button.

Advanced Settings

Clicking the **Advanced** button makes the following settings available for change:

- **Timeout**—this is the time the enrollment unit will wait before declaring the enrollment a failure. The default **30** seconds should serve for most enrollments.
- **Default DB**—the default MA300 or MA500 database to which the Reader assigns fingerprint templates.
- **DB for this User**—the default MA300 or MA500 database to which this users templates are stored.
- **Quality Threshold**—determines the minimum quality score for each template. A higher threshold, leads to a better quality template.
- **Matching Threshold**—determines the minimum accepted marching threshold during the verification stage of each template capture. For standard applications, select 3 000, for secure applications, select 3 500 and for high-security applications, select 4 000.
- **Finger Detection**—when selected, the Acquisition Window dialog automatically detects finger presence, capturing the number of captures defined at each stage. If disabled, you must manually capture each fingerprint.
- **Number of Captures**—the number of automatic fingerprint captures to capture when finger detection is enabled.
- **Enable Duplicate Check**—when enabled, after template capture, the ImproNet Software searches for matches in the Matcher Database (located in the Biometric Server Software). Restart the Access Module for this setting to take effect. For full functionality, ensure that you start the Biometric Server Software. Refer to the section Duplicate Search (1:N Matching) on page 23 for more information.

14. Click on the **Enroll** button, thereby initiating the enrollment.

Fingerprint Placement Rules

Figure 20 shows the area of the fingerprint that contains the most information. Therefore, when enrolling Tagholders, ensure they place their fingers as shown in Figure 21.

Finger_Placemnt_01.jpg

Figure 20 – Area of the Fingerprint Containing the most Information

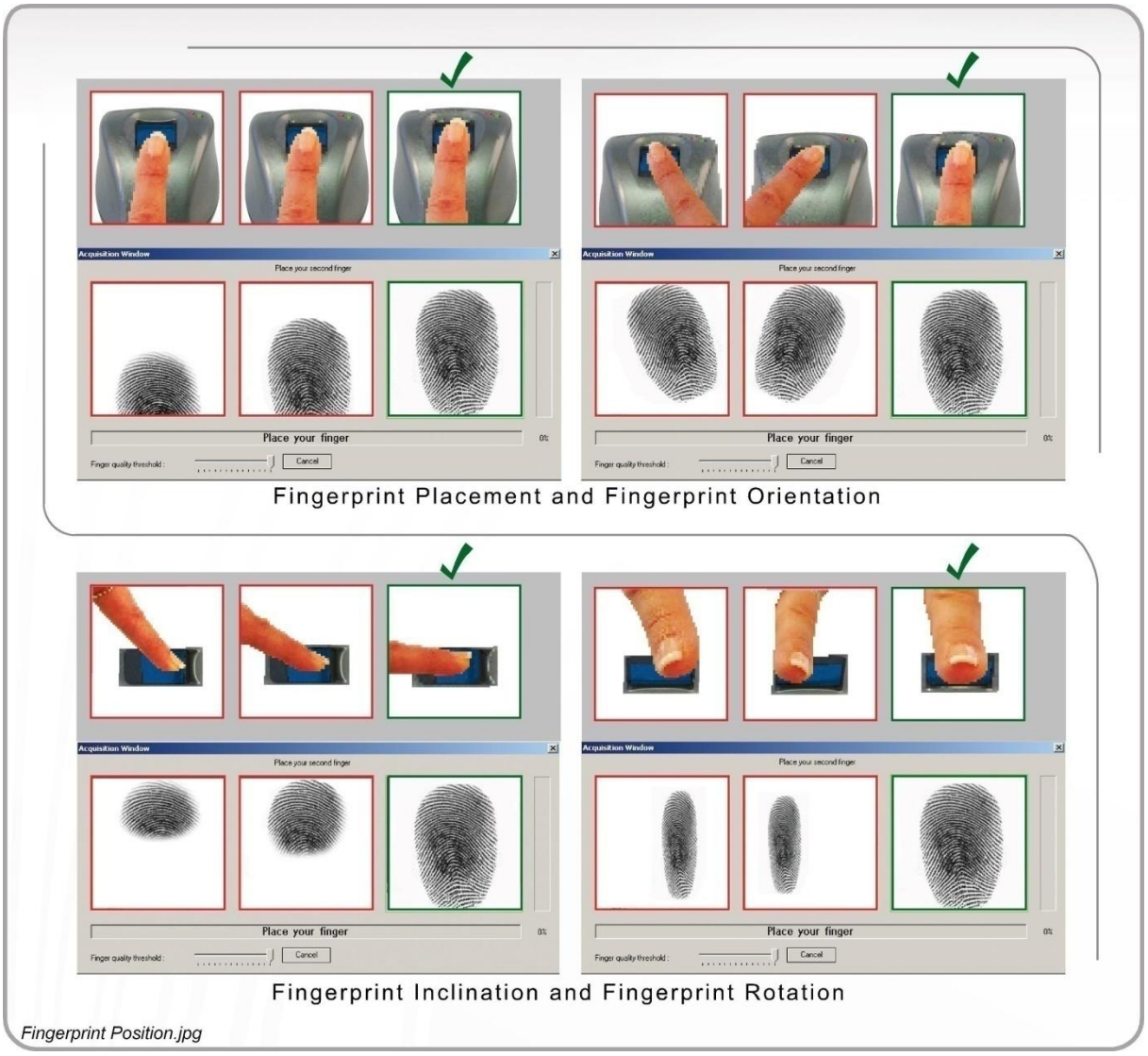


Figure 21 – Fingerprint Placement Rules

Enrollment procedure at the Sagem MSO300

1. Place **Finger 1** (fingerprint down) on the MSO300 Enrollment Reader's fingerprint Sensor.
2. Remove Finger 1 from the Sensor
3. Place Finger 1 on the Sensor a second time.
4. Again, remove Finger 1 from the Sensor.
5. Place **Finger 2** (fingerprint down) on the MSO300 Enrollment Reader's fingerprint Sensor.
6. Remove Finger 2 from the Sensor.
7. Place the Finger 2 on the Sensor a second time.
8. Again, remove Finger 2 from the Sensor.

Once the enrollments complete, the **Template** field displays the Template Number and an **Enrollment Successful** message appears in the Status Bar.

9. Click the button.
10. Click the button.

The enrollment process is now complete. Repeat this process for each Tagholder, as required.

With the Biometric Server running, the Server automatically uploads templates to the Sagem Readers.

HandKey® CR Use in an ImproNet System

General

This section guides you step by step through the process of setting up the HandKey® CR Biometric Reader to work with the ImproNet System. The requirements for the integration are as follows:

- IXP400 Access Control System.
- ImproNet V7.60 Installed.

There are five steps in configuring the Biometric Readers to work with ImproNet. These are:

1. Hardware installation of the Biometric Readers.
2. Software setup of the Biometric Readers using the Biometric Server Software.
3. Detection of the Biometric Readers on the TCP/IP bus.
4. Setting up the Enrollment Reader.
5. Enrolling users on the System.

Principle of Operation

Figure 22 shows the Tag and Template data flow when using a HandKey® CR Reader with ImproNet.

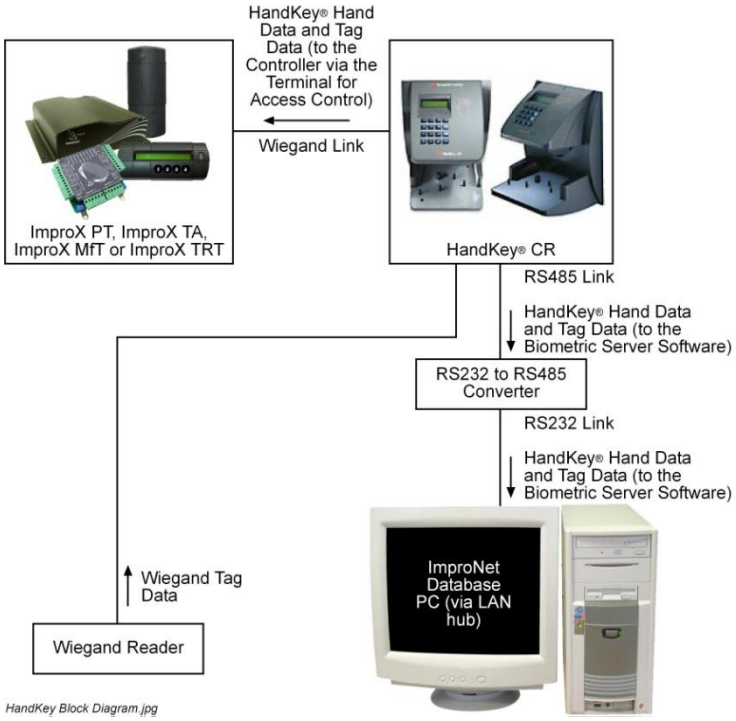


Figure 22 – Data Flow when using a HandKey® Reader with ImproNet

Hardware Installation of HandKey® CR Readers

Each HandKey® CR Reader must connect to the LAN to send and receive templates from the ImproNet Database. The HandKey® Reader must also connect to an associated ImproX Terminal (such as the ImproX PT, TA, TRT or the MfT) thus facilitating communication with the Controller. Please install the HandKey® CR Readers as outlined in the associated HandKey® Readers Hardware Installation Manual.

Note that the following connection diagrams show the HandKey® Reader positioned as shown in Figure 23 below.

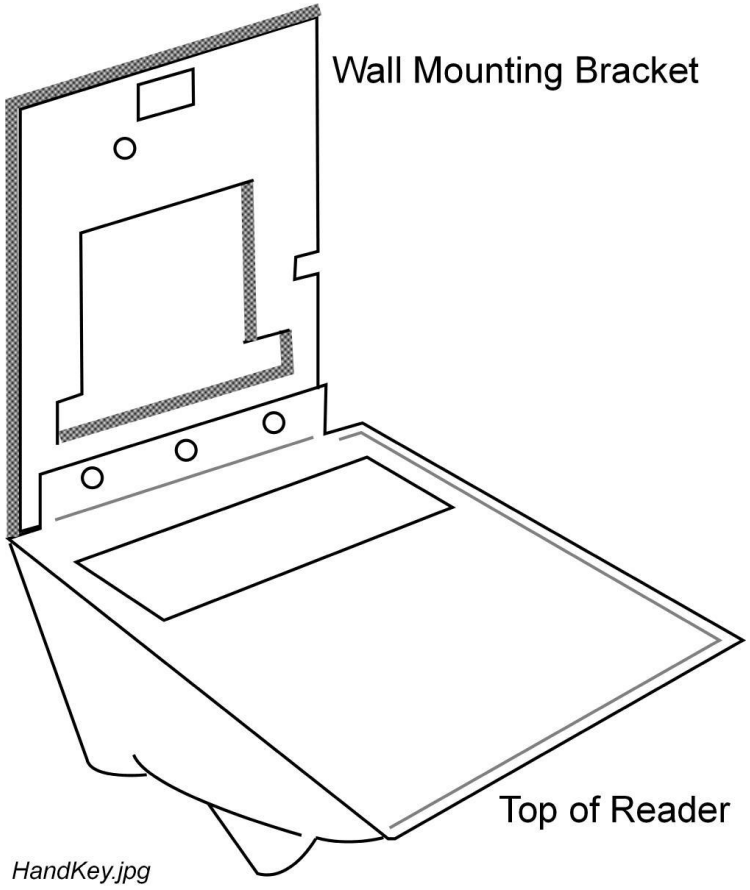
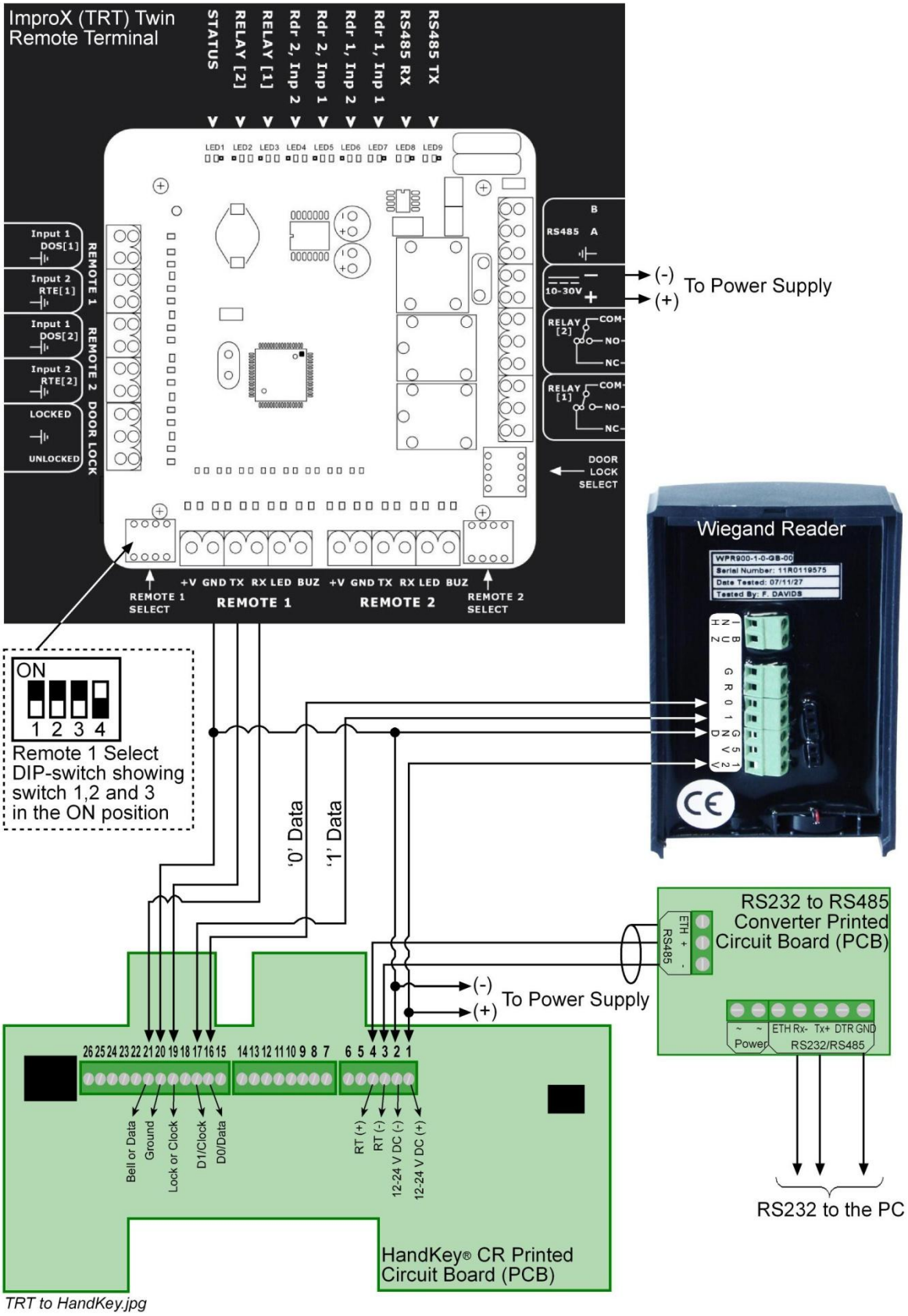


Figure 23 – Position of HandKey® During Connection

Electrical Connection of the HandKey® CR Readers

Connection to the ImproX TRT



TRT to HandKey.jpg

Figure 24 – HandKey® CR Reader Connected to the ImproX TRT and LAN

Connection to the ImproX MfT

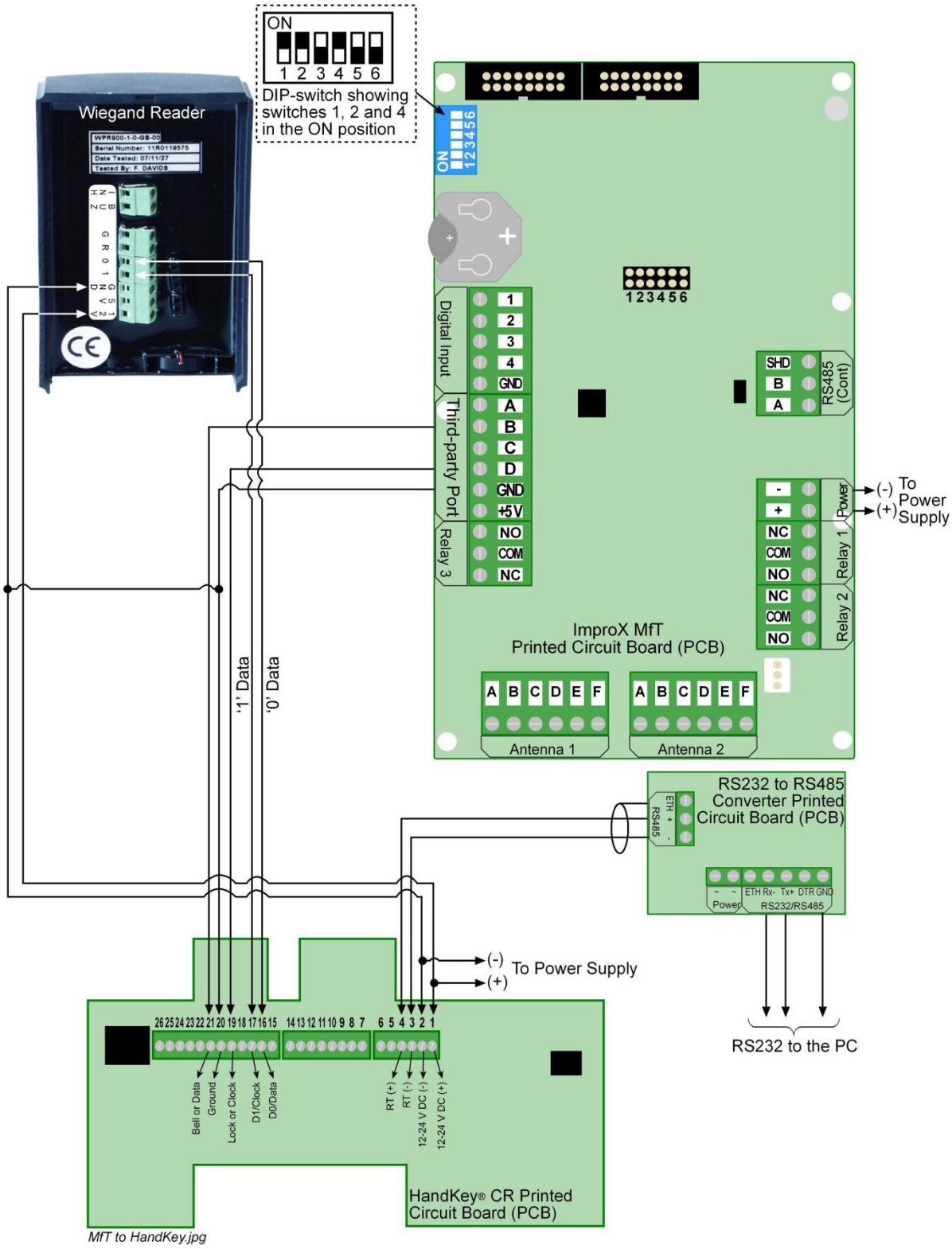


Figure 25 – HandKey® CR Reader Connected to the ImproX MfT and LAN

Connection to the ImproX PT or ImproX TA

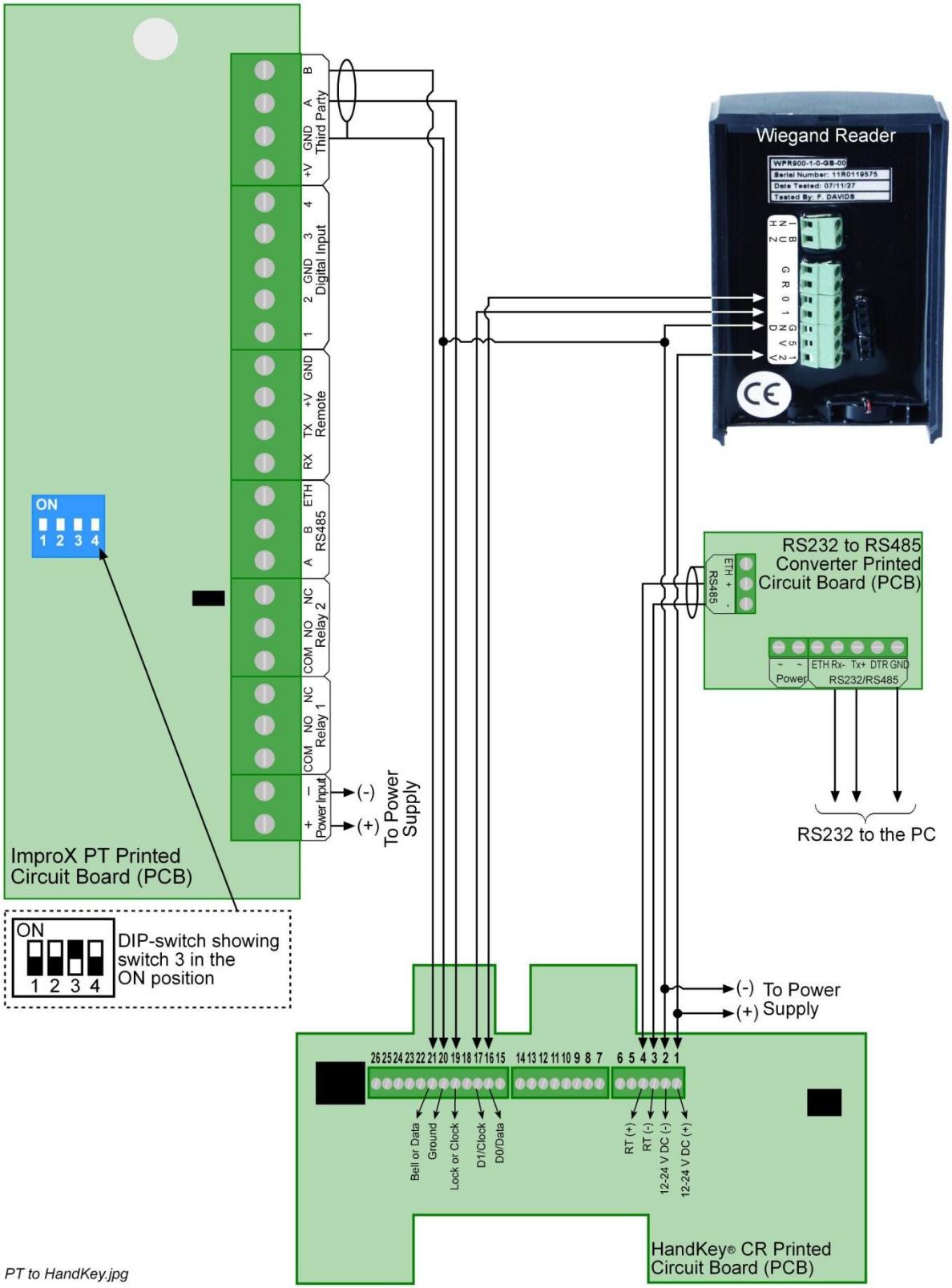


Figure 26 – HandKey® CR Reader Connected to the ImproX PT or ImproX TA and LAN

Configuring the Biometric Device

*Ensure that you unlock BOTH your **Registration Interface** and your **Registration Reader**, for Biometrics, before continuing further.*

Where you intend using a HandKey® CR Reader purely for enrollment, you do NOT require a Wiegand Reader.

Before configuration into an ImproNet System, internally configure each HandKey® Reader (as a stand-alone unit), as follows:

1. Connect the HandKey® Reader as shown in Figure 24, Figure 25 or Figure 26.
2. Internally allocate the HandKey® Reader an address in the range 0 to 255. Refer to the HandKey® CR Installation and Operation Manual supplied with your HandKey® Reader.

Adding a Biometric Driver

The ImproNet Biometric Server Software does not support the Windows® Vista (Business or Ultimate) operating system.

1. From Windows® select **Start**>**Programs**>**ImproNet**>**Biometric Server**.
2. From the Menu Bar, select the **Drivers** drop-down list.
3. Select the **HandKey** radio button.
4. From the Menu Bar, select the **Configuration** drop-down list.
5. Select **HandKey**>**Devices**.
6. In the Search for HandKey Devices dialog, select the **Connection Type**. Your choices include RS232 or TCPIPSocket.

RS232 Configuration (Setting the Address)

1. Apply power to the HandKey® Reader.
2. On the HandKey® Reader's Keypad, simultaneously press the **Clear** and **Enter** buttons.
3. Select menu option **2** and press the **Enter** key.
4. Select the **No** option until you reach the **Set Address** menu option.

"0" Addresses do NOT appear when you set the RS232 Address option.

TCPIP Configuration (Setting the Address)

The settings outlined below set the IP Address, the Gateway and the Host Bit settings.

1. Plug in the Ethernet connection.
2. Apply power to the HandKey® Reader.
3. On the HandKey® Reader's Keypad, simultaneously press the **Clear** and **Enter** buttons.
4. Select menu option **2** and press the **Enter** key.
5. Select the **No** option until you reach the **Set Serial** menu option.

Ensure that all IP Addresses fall under the same subnet.

TCPIP Configuration

*If you change the **Connection Type**, in the Search for HandKey Devices dialog, click the button for the change to take effect.*

*If you carry out an **RS232 search**, the search range automatically runs from 1 to 255. You cannot set the range.*

1. In the **IP Range** textboxes, type in the IP Address for your TCPIP configuration.
2. Click on the **Search** button.

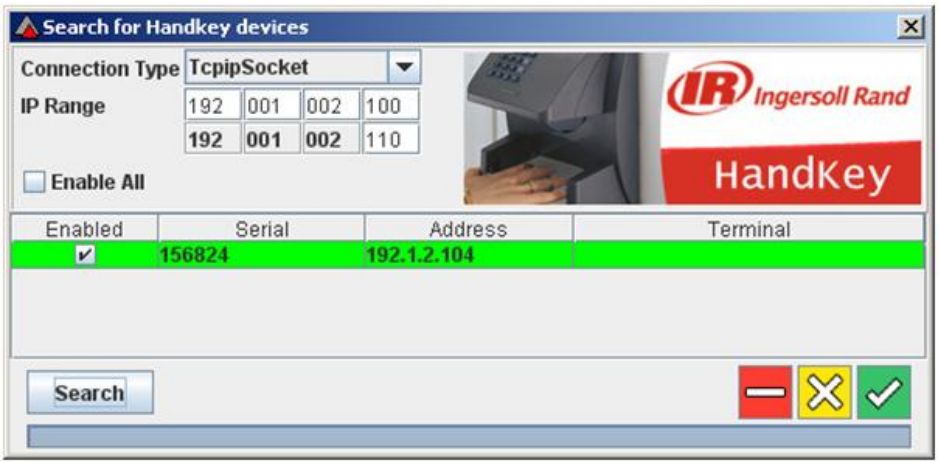


Figure 27 – Search for HandKey Devices Dialog

The search records display highlighted according to the following key. Search Records highlighted in: GREEN represent new HandKey® Readers; RED represent missing HandKey® Readers; ORANGE represents HandKey® Readers that have newly applied setting changes. Records returned without highlighting indicate existing HandKey® Readers without any setting changes.

3. Click the button.

Enrolling a Tagholder

Access Setup

1. In the Biometric Server Software, click the **Start** button.
2. From Windows® select **Start**>**Programs**>**ImproNet**>**Access**.

Ensure that you note each HandKey® Reader's installation location with its serial number on the Site Plan. During this installation phase, you would have appointed one of the HandKey® Readers as the Enrollment Reader for the System. Identify this Enrollment Reader by its serial number.

3. In the Navigator Pane, click the icon.
4. From the Menu Bar, select the **Configuration** drop-down list.
5. Select **Biometric Addresses**.

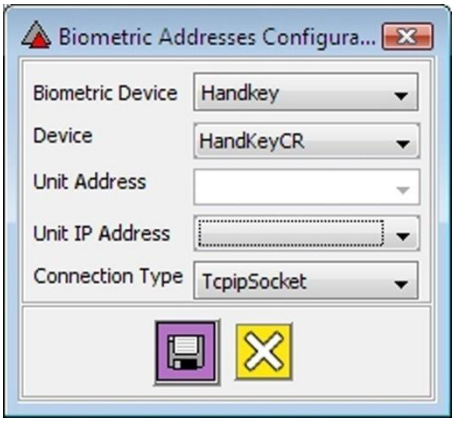


Figure 28 – Biometric Addresses Configuration Dialog

6. From the Biometric Device drop-down list, select the **HandKey** option.
7. From the Device drop-down list, select the **HandKeyCR** option.
8. Check that the **Unit IP Address** reflects the IP Address of your HandKey® Reader.
9. From the **Connection Type** drop-down list, select the connection type in use.
10. Click the button.
11. Click the button.

Tagholder Registration

1. In Access, from the Main Pane, click the button.
2. In the **Add Tagholder** dialog, capture your Tagholders details. Refer to Part III for more information on adding a Tagholder.
3. Click the button.
4. On activation, click the **New Tag** button.
5. From the Tag Type drop-down list, select **Slim Tag (5 Bytes)**.
6. Place your Tag in the Registration Reader.
7. Click the **Read Tag** button.
8. Click the button.
9. From the Tag Type drop-down list, select **ASCII, Biometric, Magstripe**.
10. Select the **Accept Full Tag Code** radio button.
11. Click the button.
12. Click the button.
13. On activation, click the **Biometric Enrollment** button.

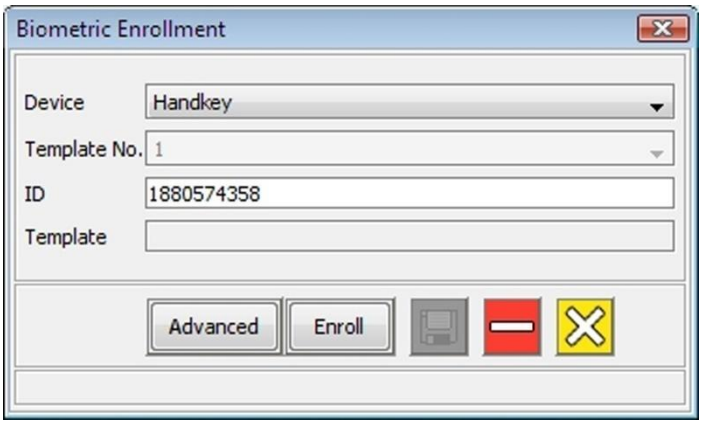


Figure 29 – Biometric Enrollment Dialog

14. From the Device drop-down menu, select the **HandKey** option.

The ID textbox shows the modified Tag Code used by the HandKey® Reader. Note, however, that ImproNet still uses the full unmodified Tag Code in all communications.

*Clicking on the Advanced button lets you set the **Threshold** (optimal at the default setting of **30**), **Authority** (default setting is **0**) and **Special Enroll** settings.*

Settings explained:

- ***Threshold Setting**—the lower the Threshold, the greater the security as you get less false readings. Lowering the Threshold does, however, result in more false rejects.*
- ***Authority Setting**—this setting provides the Tagholder access to the internal HandKey® menus. There are 5 menus, and the digit selected here indicated how many of these menus the Tagholder can access.*
- ***Special Enroll**—selecting this checkbox, allows identification of disabled people (without hands). Enrollment takes place with the Tagholder placing the remainder of the limb on the HandKey® Reader's Registration Plate. Identification of the Tagholder is then only by Tag ID.*

Hand Enrollment

When enrolling the hand template, ensure that you place the Tagholder's hand on the HandKey® Readers Registration Plate, 3 times in quick succession. If enrollment takes too long, the process times out, resulting in a failure to record a template, or the incorrect template being recorded.

At each stage of the Tagholder's hand enrollment the HandKey® Reader displays status messages on the its liquid crystal display (LCD). Take note of these messages and act on them in good time.

1. In the Biometric Enrollment dialog, click the **Enroll** button.
2. Place the Tagholders RIGHT hand on the HandKey® Readers Registration Plate.
3. Remove the Tagholders hand from the HandKey® Readers Registration Plate.
4. Place the Tagholders RIGHT hand on the HandKey® Readers Registration Plate again.
5. Remove the Tagholders hand from the HandKey® Readers Registration Plate.
6. Place the Tagholders RIGHT hand on the HandKey® Readers Registration Plate again.

At the successful enrollment of the Tagholder, *the message "Record added successfully" displays in the Message Panel at the bottom of the Biometric Enrollment dialog.* The Template No. drop-down list is now active.

B-SHO Fingerprint Terminals Use in an ImproNet System

General

This section guides you step by step through the process of setting up B-SHO Fingerprint Terminals to work with the ImproNet System. The requirements for the integration are as follows:

- IXP400 Access Control System.
- ImproNet V7.60 Installed.

There are four steps in configuring the Biometric Terminals to work with ImproNet. These are:

1. Hardware installation of the Biometric Terminals.
2. Detection of the Biometric Readers on the RS485 bus.
3. Setting up the Enrollment Reader.
4. Enrolling users on the System.

Principle of Operation

Figure 30 shows the Tag and Template data flow when using a B-SHO Fingerprint Terminal with ImproNet.

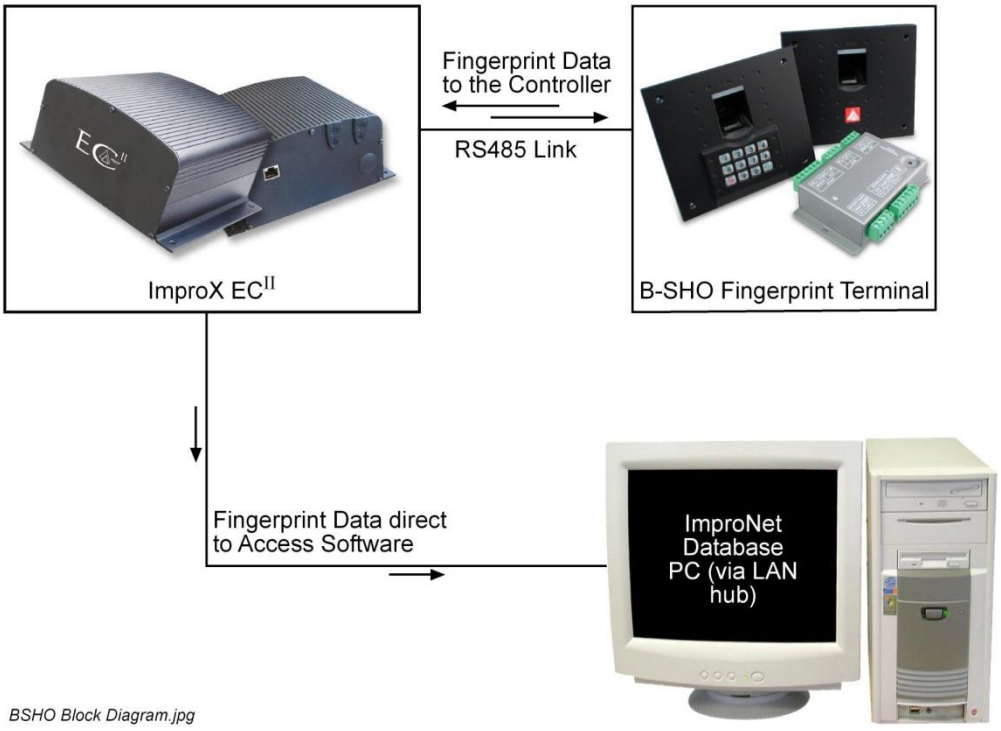


Figure 30 – Data Flow when using a B-SHO Fingerprint Terminal with ImproNet

Hardware Installation of B-SHO Fingerprint Terminals

The ImproNet System recognizes the B-SHO Fingerprint Terminals in the same fashion as our ImproX Terminals. Therefore, connect these Terminals to the ImproX EC^{II} **Terminal Bus** using the **RS485** bus protocol. As when using with associated ImproX Terminals, you may multi-drop up to 64 Terminal Fixed Addresses, including up to **16** B-SHO Fingerprint Terminals per EC^{II} Controller.

The following diagrams show the Fingerprint Terminals relationship with the rest of the ImproX product range.

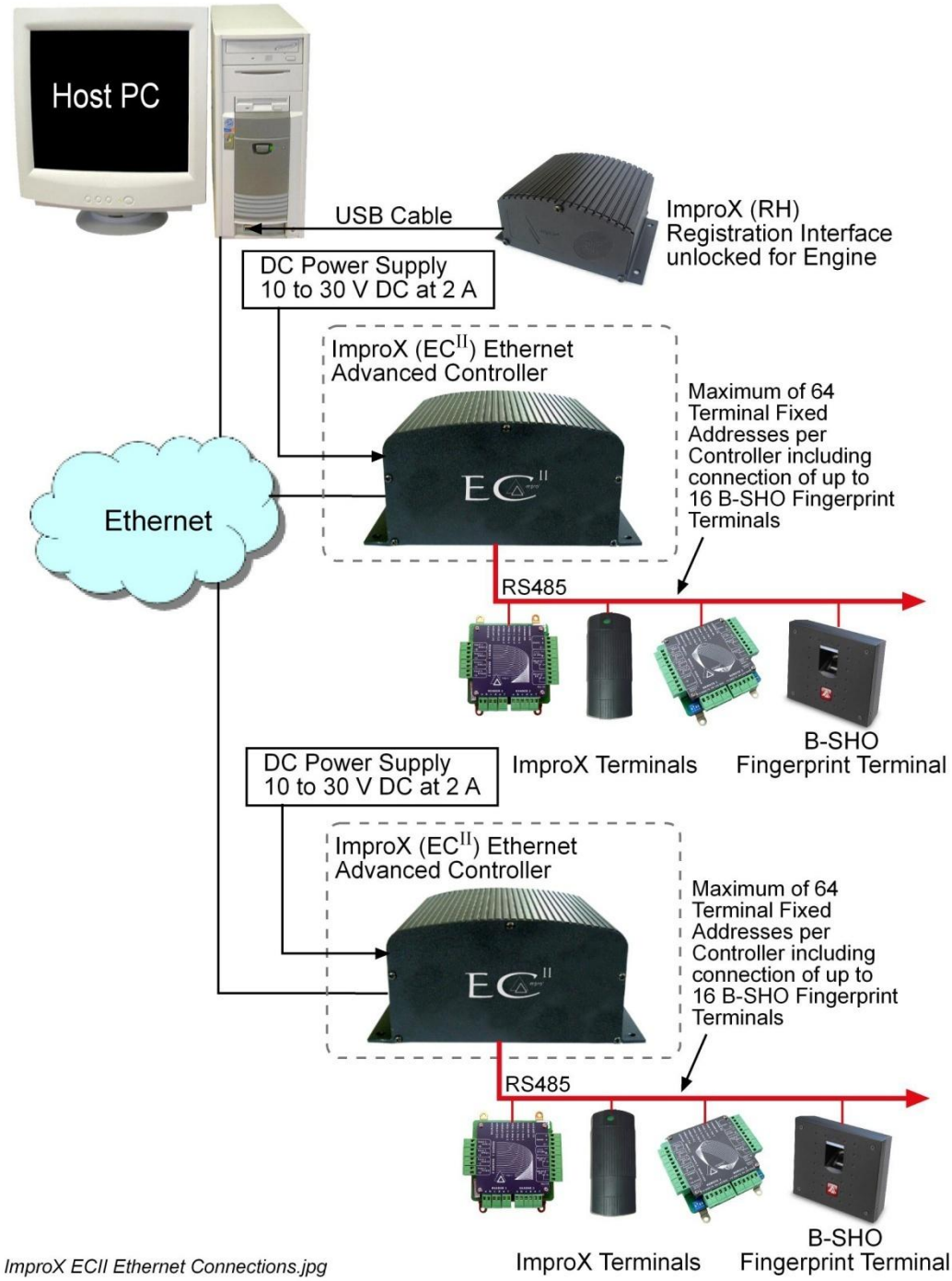


Figure 31: Connection via the Local Area Network (LAN)

Electrical Connection of the B-SHO Fingerprint Terminal

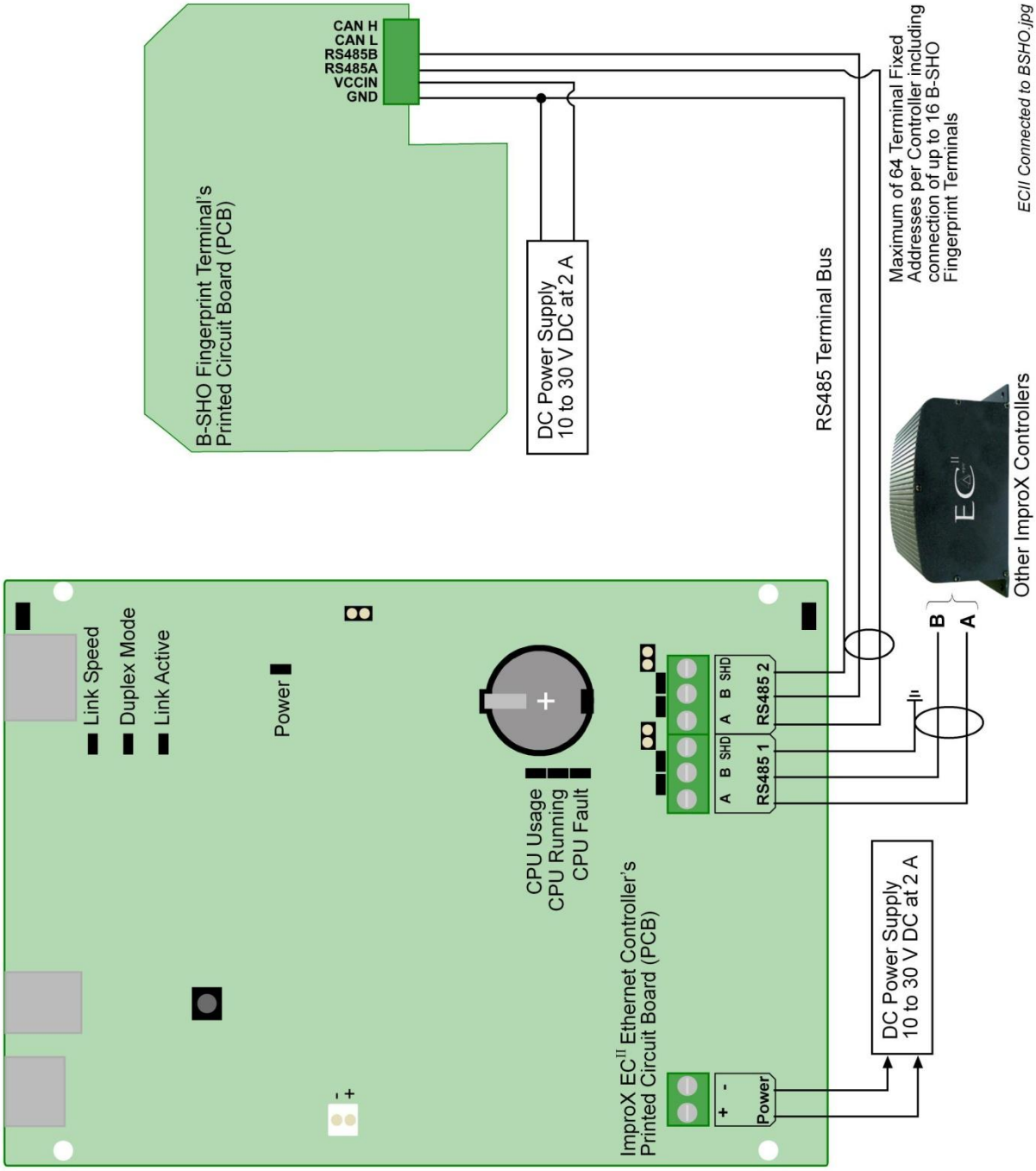


Figure 32 – B-SHO Fingerprint Terminal Connected to the ImproX EC^{II} using the Terminal Bus

Connecting the Enrollment Reader

1. Plug in the **SFR300-D B-SHO Enrollment Reader** into an unused USB Port on the PC.

*Some PC's proceed with automatic installation of the **SFR300-S**, if installation occurs automatically move direct to step 4 above.*

2. Follow the on-screen prompts, instead of letting the Installer run automatically, select **Install from a Specific Location**.

3. In a default installation, browse to **C:\ImproNet\driver\sfr300-s,** this folder contains the drivers for the SFR300-S.
4. After installation of the Drivers, the LED on the SR300-S blinks Green once.

Configuring the Biometric Device

Continue as follows for configuration into an ImproNet System:

Run Auto-ID to Detect your B-SHO Fingerprint Terminals

Before you can use your B-SHO Fingerprint Terminals, you must run the **Auto-ID** function in ImproNet Engine to detect the hardware.

*If ImproNet Engine and ImproNet Access are on different Host PCs, you must change the **Engine.properties** file (refer to Part II – Software for more information).*

To open ImproNet Engine and run Auto-ID, proceed as follows:

1. In Windows®, click **Start**>**Programs**>**ImproNet**>**Engine**.
2. Click the Auto ID button.

When hardware units are detected, they are added to the ImproNet Database and become available in the ImproNet Access tree.

Use your Unit Location Chart to re-name the Fingerprint Terminals.

Assign the Fingerprint Terminals

To assign the Fingerprint Terminals to a Controller, proceed as follows:

1. In the Navigator Pane, select a Controller, an **Unassigned Terminals** node displays.

Figure 33 – Unassigned Terminals

2. Double-click the icon to expand the Unassigned Terminals node.
3. Drag-and-drop unassigned B-SHO Fingerprint Terminal onto a **Controller**. A new **Zone** containing a **Location** is created. **Terminals** display in the Location.

Edit Terminal Parameters

The Terminals screen lets you configure your B-SHO Fingerprint Terminal and set-up its Actions, Inputs, and Outputs. The Terminal Settings are the same as those mentioned in **Part III – General Configuration**. Refer to the section titled **Terminals** for more information.

Terminal Modes

Select the B-SHO Fingerprint Terminal from the Navigator Pane (Hierarchical Tree).

The **Default Terminal Mode** drop-down list situated on the Main Pane, gives you access to the following options:

Mode	Mode Description
Tag or Finger	The Terminal requires a valid Tag OR fingerprint.
Finger	The Terminal requires a valid fingerprint.
Tag + Finger	The Terminal requires a valid Tag code and fingerprint.
“Tag + Finger” + PIN	The Terminal requires a valid Tag code, fingerprint and PIN-code.
“Tag + Finger” + Reason Code	The Terminal requires a valid Tag code, fingerprint and Reason Code.
“Tag + Finger” + PIN + Reason Code	The Terminal requires a valid Tag code, fingerprint and PIN-code and Reason Code.
“Tag or Finger” + PIN	The Terminal requires one of the following combinations: Either a valid Tag code and PIN-code OR a valid fingerprint and PIN-code.
“Tag or Finger” + Reason Code	The Terminal requires one of the following combinations: Either a valid Tag code and Reason Code OR a valid fingerprint and Reason Code.
“Tag or Finger” + PIN + Reason Code	The Terminal requires one of the following combinations: Either a valid Tag code, PIN-code and Reason Code OR a valid fingerprint, PIN-code and Reason Code.
Finger + PIN	The Terminal requires a valid fingerprint and PIN-code.
Finger + Reason Code	The Terminal requires a valid fingerprint and Reason Code.
Finger + PIN + Reason Code	The Terminal requires a valid fingerprint, PIN-code and Reason Code.
Personal Access Code + Finger	The Terminal requires a valid Personal Access Code and fingerprint.
Personal Access Code or Finger	The Terminal requires a valid Personal Access Code OR fingerprint.
“Tag” or “Finger” or “Personal Access Code + Finger”	The Terminal requires one of the following combinations: Either a valid Tag code or fingerprint OR a combination of valid Personal Access Code and fingerprint.

Table 3 – Table of B-SHO Terminal Modes

Support for Reason Code Modes in the B-SHO Terminal Firmware is planned for V1.12.

Enrolling a Tagholder

*For more complex B-SHO installations using ImproNet V7.60 we added the **Copy Existing Tag Code** button and the **Save Template to all Biometric Tags** checkbox.*

*Clicking the **Copy Existing Tag Code** button opens a dialog allowing selection of the Tag Code you want to copy. You may copy the Tag Code of any Tags for that Tagholder (other than ASCII) for creation of a new ASCII Tag. Then connect a fingerprint template to this Tag by going to the Biometric Enrollment dialog of an ASCII Tag already enrolled for that Tagholder and selecting the **Save Template for all Biometric Tags** checkbox.*

Tagholder Settings

1. From Windows® select **Start**>**Programs**>**ImproNet**>**Access**.
2. In the Navigator Pane, select the icon.
3. Open the **Edit Tagholder** or **Add Tagholder** dialog.
4. Select **New Tag** to enter the **Tag** dialog.
5. Have the Tagholder place their Tag on the ImproNet Enrollment Reader.
6. Click **Read Tag** (or just enter a number of 7 digits or less in the **Tag Code** field).
7. Click the **Tag Type** drop-down list and select **ASCII, Biometric, Magstripe** from the list.
8. When the dialog pops up, select option **1**, which is **Accept Full Tag Code** (see below).

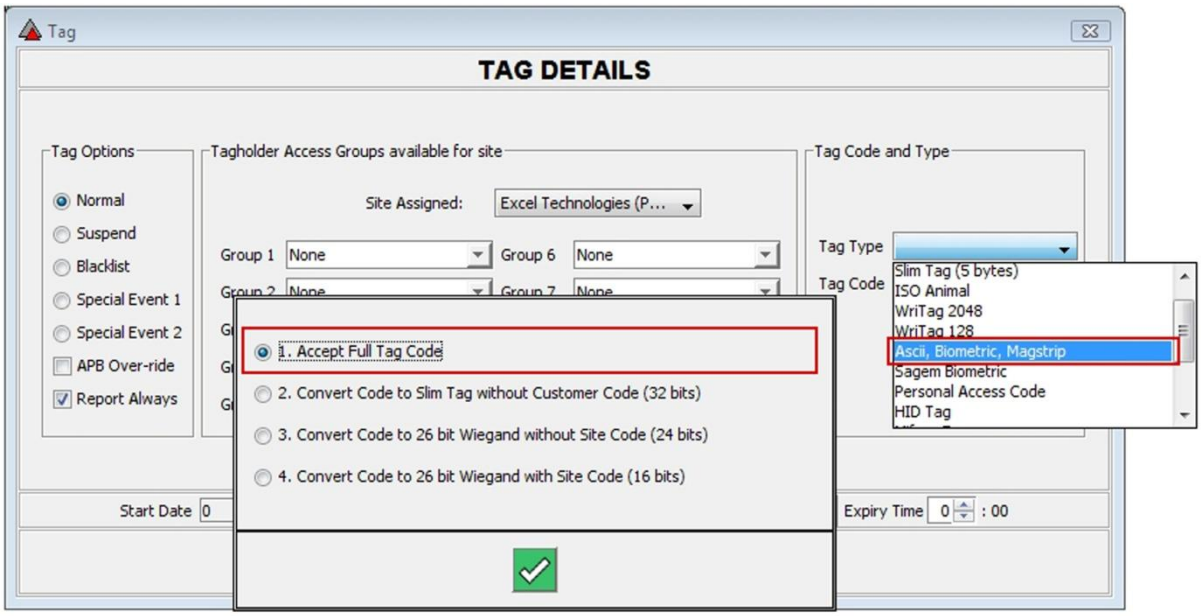


Figure 34 – ASCII, Biometric, Magstripe

9. Set the Access Groups in the usual way.
10. Click on the button.
11. Click on the **Biometric Enrollment** button (see Figure 18).

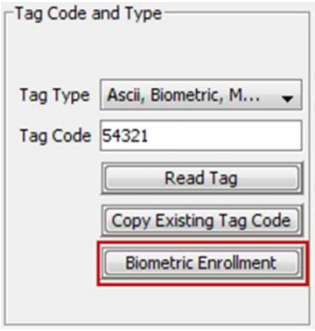


Figure 35 – Extract from Tag Dialog (Ready for Biometric Enrollment)

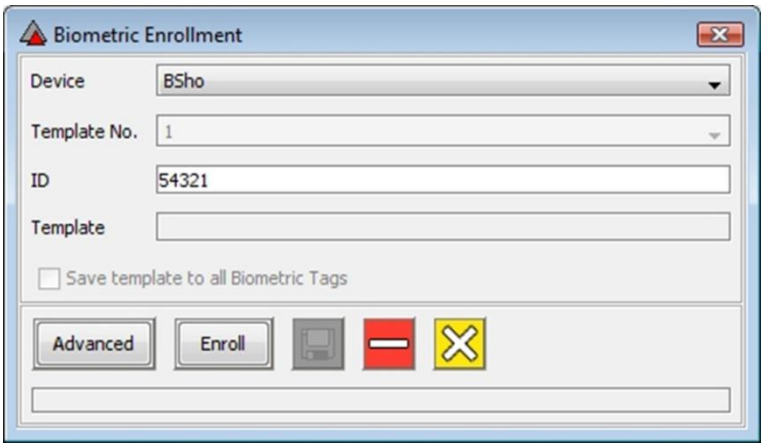


Figure 36 – Biometric Enrollment Dialog

12. In the **Biometric Enrollment** dialog, from the **Device** drop-down list, select the type of device you wish to enroll the user on, in this case **BSho**.

*The **Template No** field appears greyed out as it does not apply to BSHO units.*

*The **ID** field is the ID derived from the Tag Code and is the number under which the user's data is saved when his or her fingerprints are enrolled in the units.*

*The **Template** field remains empty until the enrollments completed.*

Advanced Button Options

1. Click on the **Advanced** Button.

*We recommend that you leave the **Quality Threshold** set at **80**. You may however adjust this setting based on your preferences.*

2. From the **No. Of Enrollments** drop-down list, select **2**. This figure indicates that you intend enrolling 2 fingers.
3. From the **Scans per Finger** drop-down list, select **2**. This figure indicates the number of times you intend scanning each finger.
4. Select the **Verify Templates** checkbox.
5. Click the button.

Fingerprint Placement Rules

Figure 37 shows the area of the fingerprint that contains the most information. Therefore, when enrolling Tagholders, ensure they place their fingers as shown in Figure 38.

Finger_Placemnt_01.jpg

Figure 37 – Area of the Fingerprint Containing the most Information

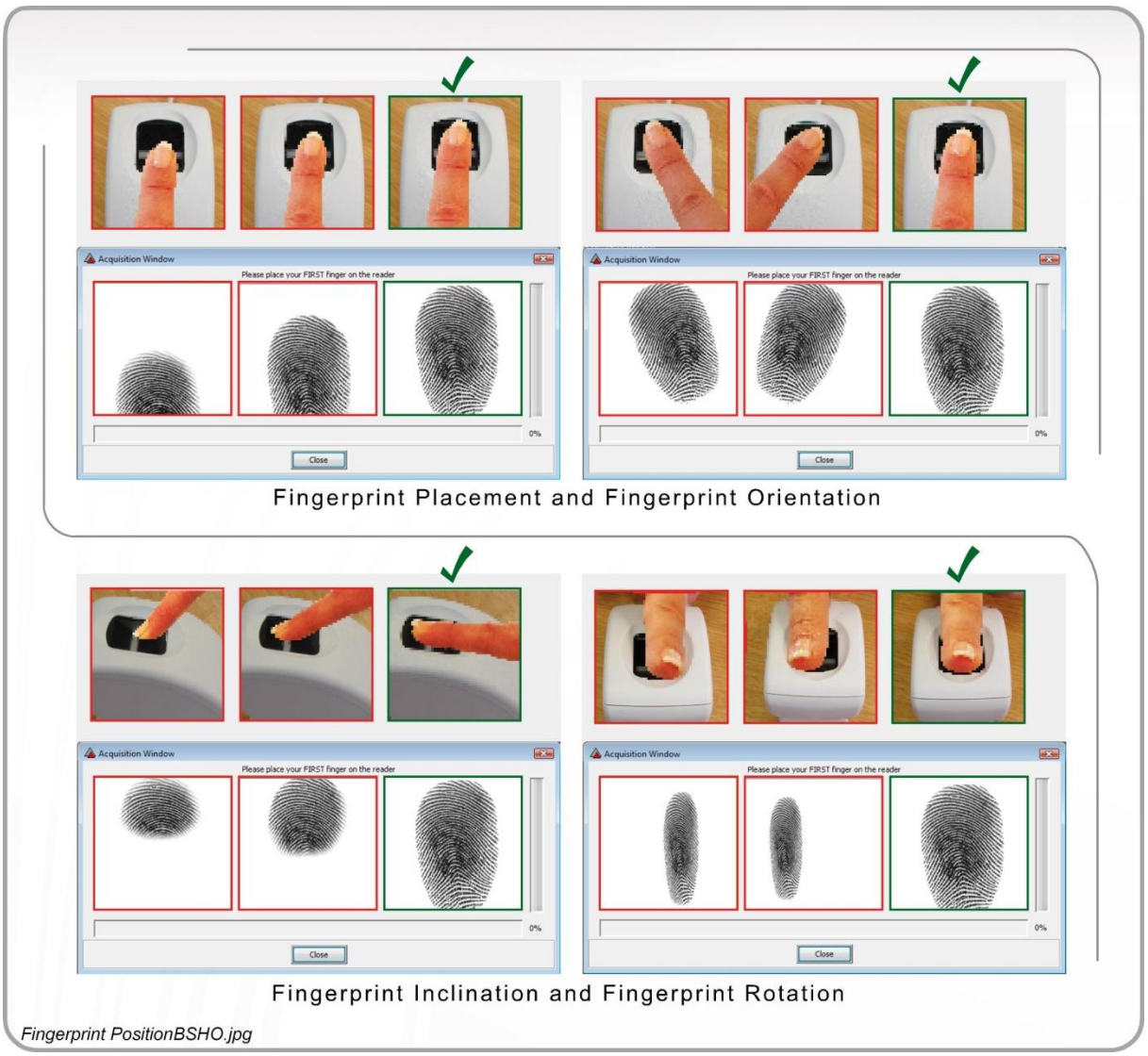


Figure 38 – Fingerprint Placement Rules

After enrollment, ensure that Tagholders use the Fingerprint Placement Rules shown in Figure 38 each time they present their finger to the B-SHO Fingerprint Terminal.

Enrollment procedure at the B-SHO Enrollment Reader

1. Click on the **Enroll** button, thereby initiating the enrollment.
2. At the Acquisition Window dialog, place **Finger 1** (fingerprint down) on the SFR300-S Enrollment Reader's fingerprint Sensor.
3. Remove Finger 1 from the Sensor.
4. Place Finger 1 on the Sensor a second time.
5. Again, remove Finger 1 from the Sensor.
6. At the Message dialog, click the **OK** button.
7. Place **Finger 2** (fingerprint down) on the SFR300-S Enrollment Reader's fingerprint Sensor.
8. Remove Finger 2 from the Sensor.
9. Place the Finger 2 on the Sensor a second time.
10. Again, remove Finger 2 from the Sensor.
11. At the Message dialog, click the **OK** button.

Once the enrollments complete, the **Template** field displays the Template Number and an **Enrollment Successful** message appears in the Status Bar.

12. Click the button.
13. Click the button.
14. At the Tag dialog, click the button.
15. Click the button.

The enrollment process is now complete. Repeat this process for each Tagholder, as required.

You may store up to 1 900 single-finger templates or up to 950 double-finger templates.

USER NOTES

USER NOTES