PART 9 – INTEGRATION MODULES

Contents

PART 9 – INTEGRATION MODULES 1

CONTENTS 3

INTRODUCTION 5

MORPHO (SAGEM) READER USE IN AN IMPRONET SYSTEM 7

General 7

Principle of Operation 7

Hardware Installation 8

Installation and Setup of the MSO300 Enrollment Reader and Verification Dongle 14

Morpho MA100, MA120, MA500 or J-Series Internal Parameter Setup..... 17

Morpho MA200 or MA300 Internal Parameter Setup 24

Configuration of Morpho Readers into the ImproNet System 26

Configuration of MIFARE® Encoders into the ImproNet System 34

HANDKEY® CR USE IN AN IMPRONET SYSTEM 39

General 39

Principle of Operation 39

Hardware Installation of HandKey® CR Readers 40

Configuring the Biometric Device..... 43

IMPROX B-SHO FINGERPRINT TERMINALS USE IN AN IMPRONET SYSTEM 47

General 47

Principle of Operation 47

Hardware Installation of ImproX B-SHO Fingerprint Terminals 48

Configuring the Biometric Device..... 51

NITGEN FINGERPRINT TERMINALS USE IN AN IMPRONET SYSTEM 57

General 57

Principle of Operation 57

Hardware Installation of NITGEN Fingerprint Terminals 58
NITGEN Fingerprint Terminal Internal Parameter Setup 61
Using NITGEN Terminals within the ImproNet System 61

Introduction

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

- Various **Morpho** 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 Reader support information.

Biometric Reader	**Biometric Server Software Support**	**Users**	**Firmware Supported**	**Approved Terminals**	**Enrollment Support**
MorphoAccess™ MA100	**YES**	500	2.13.4	iTRT, MfT and TA	No
MorphoAccess™ MA120	**YES**	500	2.13.4	iTRT, MfT and TA	No
MorphoAccess™ J-Bio	**YES**	500	2.13.4	iTRT, MfT and TA	No
MorphoAccess™ J-Dual	**YES**	500	2.13.4	iTRT, MfT and TA	No
MA200 Fingerprint Reader	**YES**	800	5.53	iTRT, MfT and TA	No
MA220 Fingerprint Reader	**YES**	800	5.53	iTRT, MfT and TA	No
MA300 Fingerprint Reader	**YES**	48 000	5.53	iTRT, MfT and TA	No
MA500 Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT and TA	No
MA500+ Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT and TA	No
MA520 Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT and TA	No
MA520+ Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT and TA	No
OMA520 Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT and TA	No
MorphoSmart™ MSO300 Registration Reader	**YES**	NA	TBA	iTRT, MfT and TA	Yes
ImproX B-SHO Fingerprint Terminal	No	TBA	1.22	TBA	No
ImproX B-SHO USB Fingerprint Enrollment Reader	No	TBA	1.04	TBA	Yes
ImproX B-SHO BioMini USB Fingerprint Enrollment Reader	No	TBA	TBA	TBA	Yes
NITGEN Fingkey Hamster II™	**YES**	TBA	TBA	TBA	Yes

Biometric Reader	Biometric Server Software Support	Users	Firmware Supported	Approved Terminals	Enrollment Support
NITGEN Fingkey Access Terminal	**YES**	TBA	TBA	TBA	No
NITGEN NAC-2500 Plus Terminal	**YES**	TBA	TBA	TBA	No
NITGEN NAC-5000 Terminal	**YES**	TBA	TBA	TBA	No
HandKey® CR	**YES**	31 000	TBA	iTRT, MfT and TA	TBA
Schlage HandKey 2	No	TBA	TBA	TBA	TBA

Table 1 – Biometric Reader Support Information

Number of users supported by the MA120, MA220 and MA520 limited by the number of Tags supported by the Controller.

MA200 and MA300 limited to 3 000 users per Database, with a maximum of 16 Databases supported. MA5XX series, limited to 5 Databases of 10 000 users each.

The ImproX TA, ImproX iTRT and ImproX MfT each offer a Third-party Port approved for use with the Biometric Reader.

The MorphoAccess™ J-Bio and MorphoAccess™ J-Dual support 500 users (with 2 templates each) or 3 000 users (with 2 templates each) with a license.

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.

Morpho (Sagem) Reader Use in an ImproNet System

General

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

- IXP400 Access Control System.
- ImproNet V7.60 and Service Pack 3 (or higher) installed.

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

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

Documentation

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

Principle of Operation

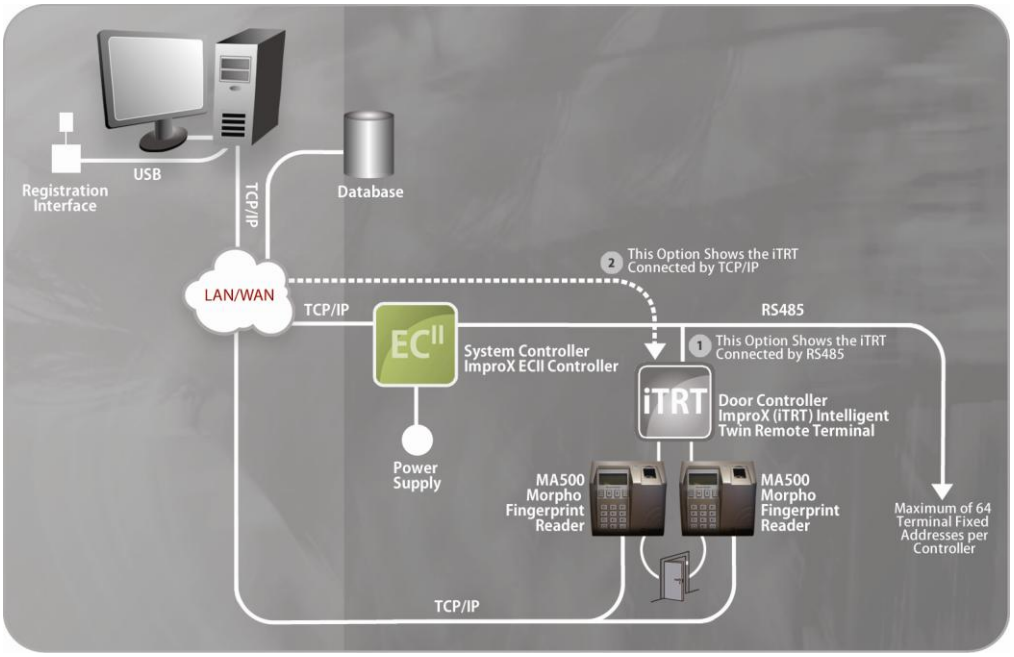
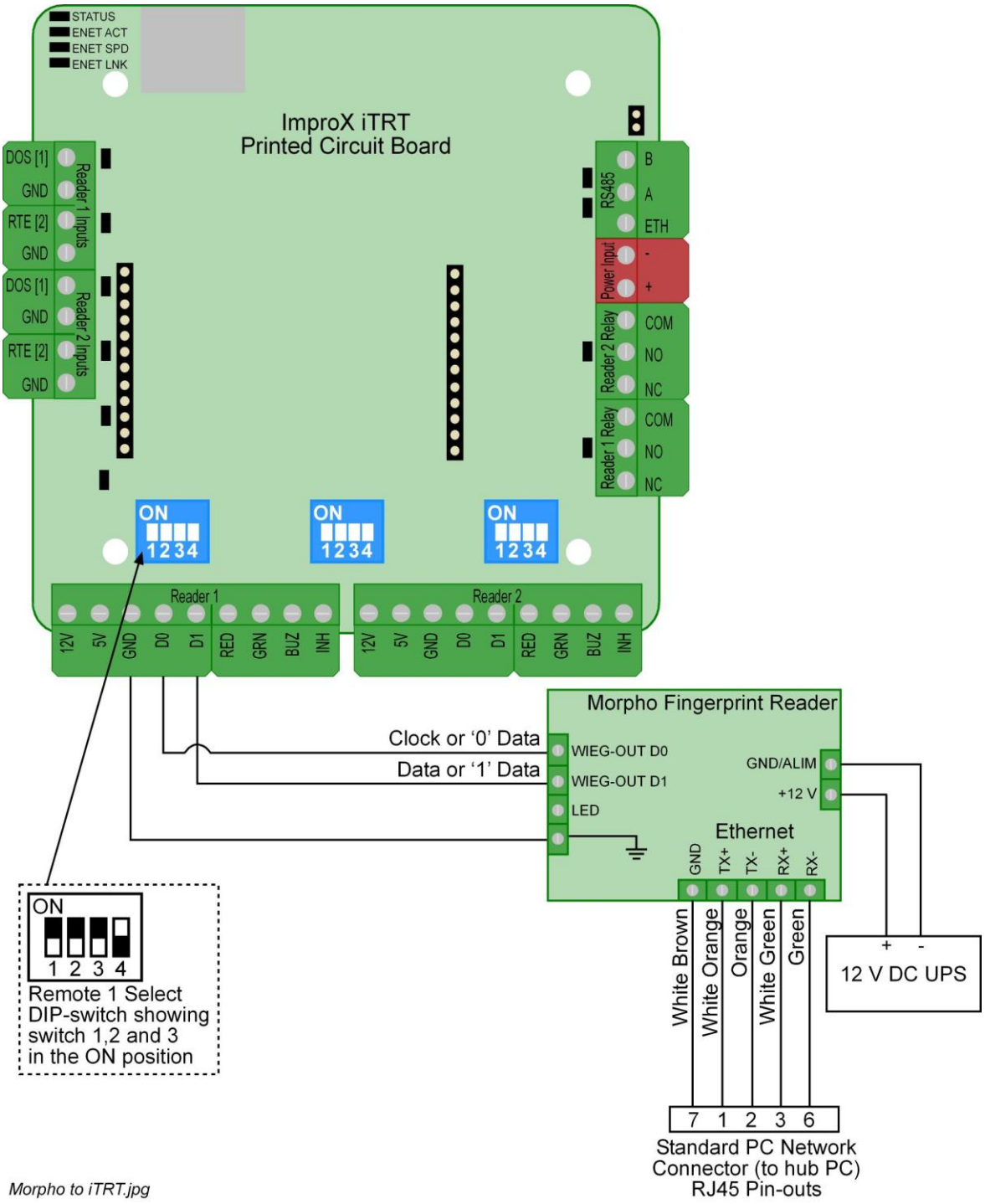


Figure 1 – Using Morpho Fingerprint Readers within an ImproNet System

Hardware Installation

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

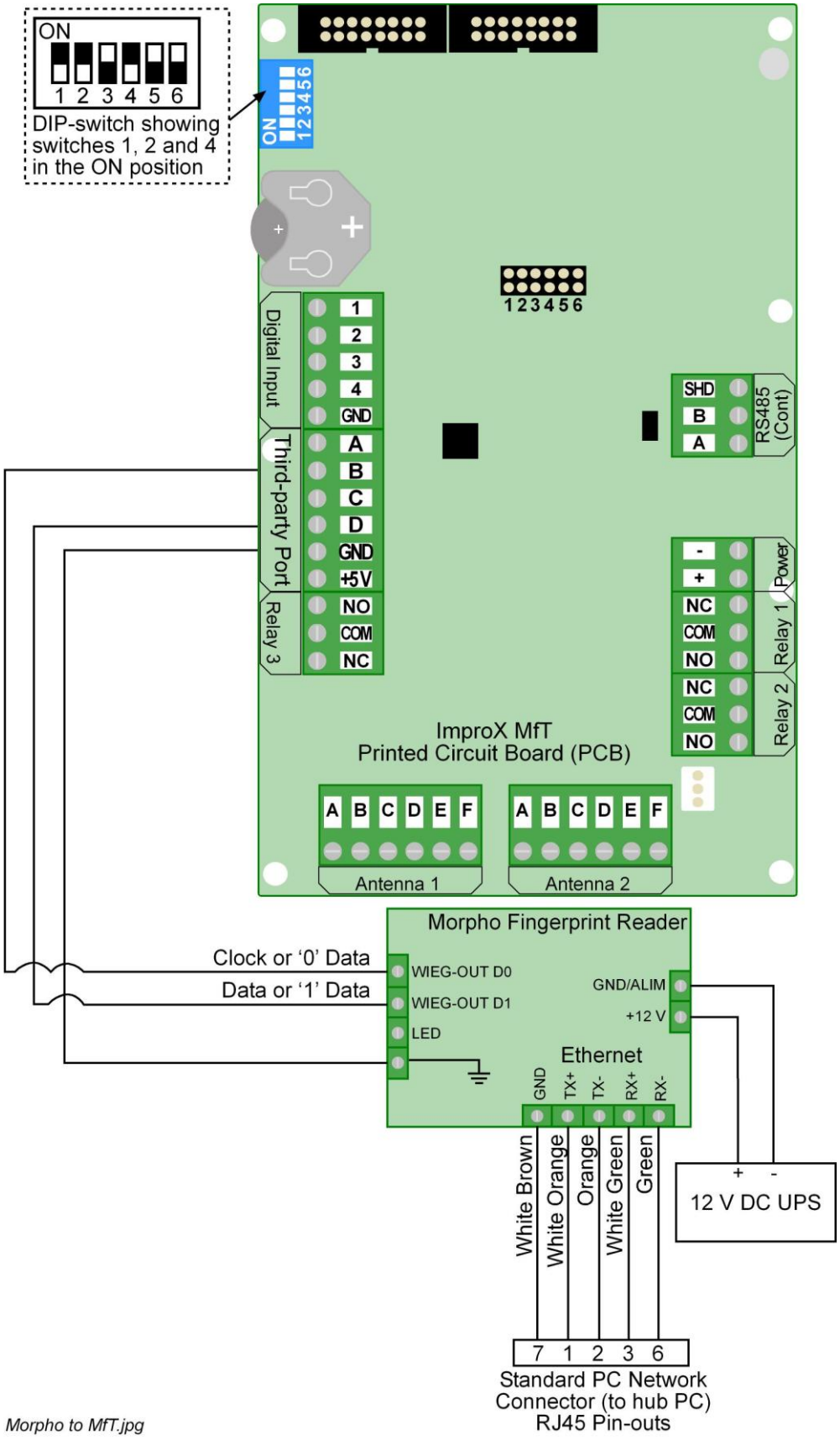
Connection to the MA100, MA120, MA200, MA300, MA500 or MA520 to the iTRT



Morpho to iTRT.jpg

Figure 2 – Morpho Reader (MA100, MA120, MA200, MA300, MA500 or MA520) Connected to the ImproX iTRT and LAN

Connection to the MA100, MA120, MA200, MA300, MA500 or MA520 to the MfT



Morpho to MfT.jpg

Figure 3 – Morpho Reader (MA100, MA120, MA200, MA300, MA500 or MA520) Connection to the ImproX MfT and LAN

Connection to the MA100, MA120, MA200, MA300, MA500 or MA520 to the TA

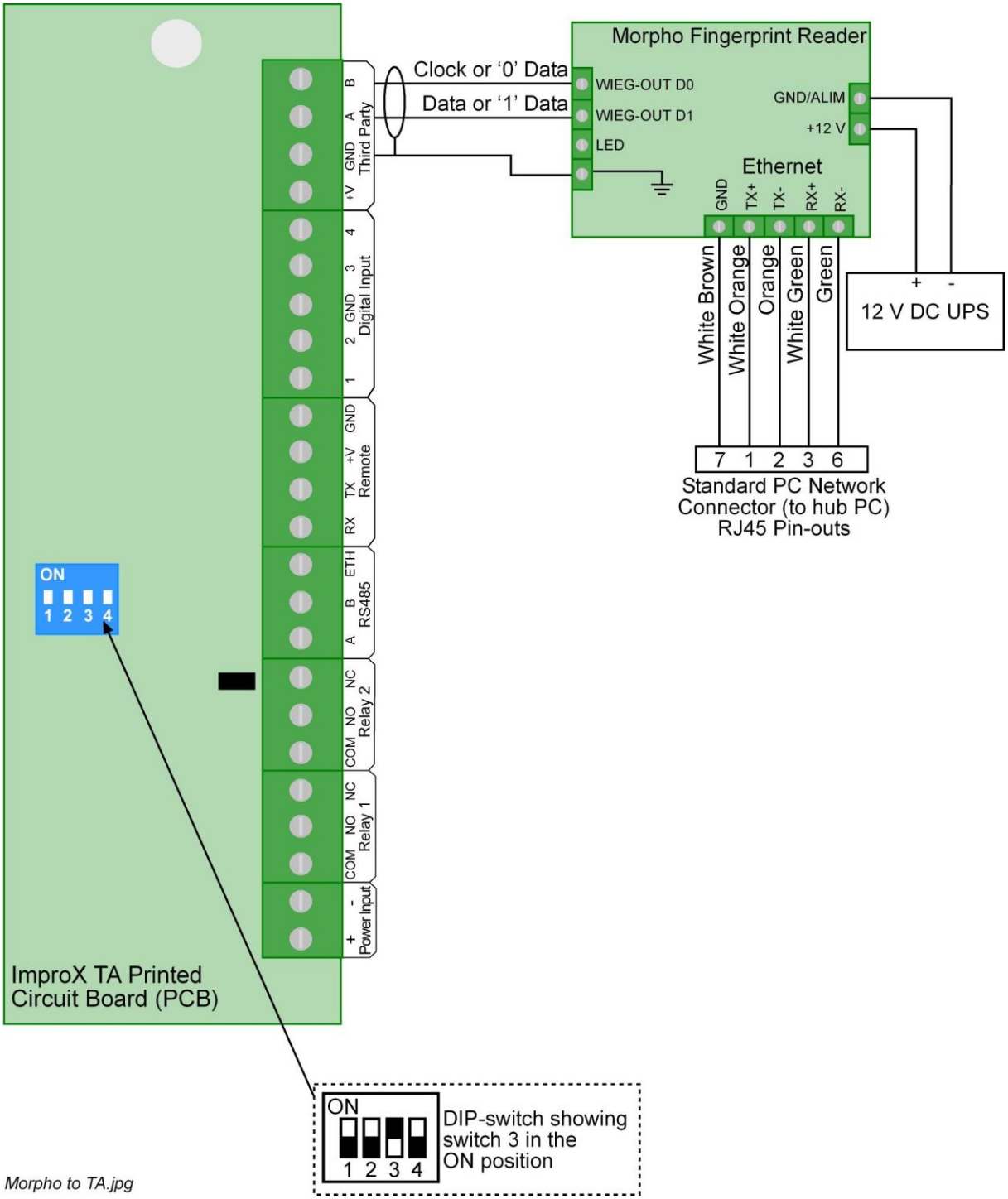


Figure 4 – Morpho Reader (MA100, MA120, MA200, MA300, MA500 or MA520) Connected to the ImproX TA and LAN

Connection to the MorphoAccess™ J-Bio or J-Dual to the iTRT

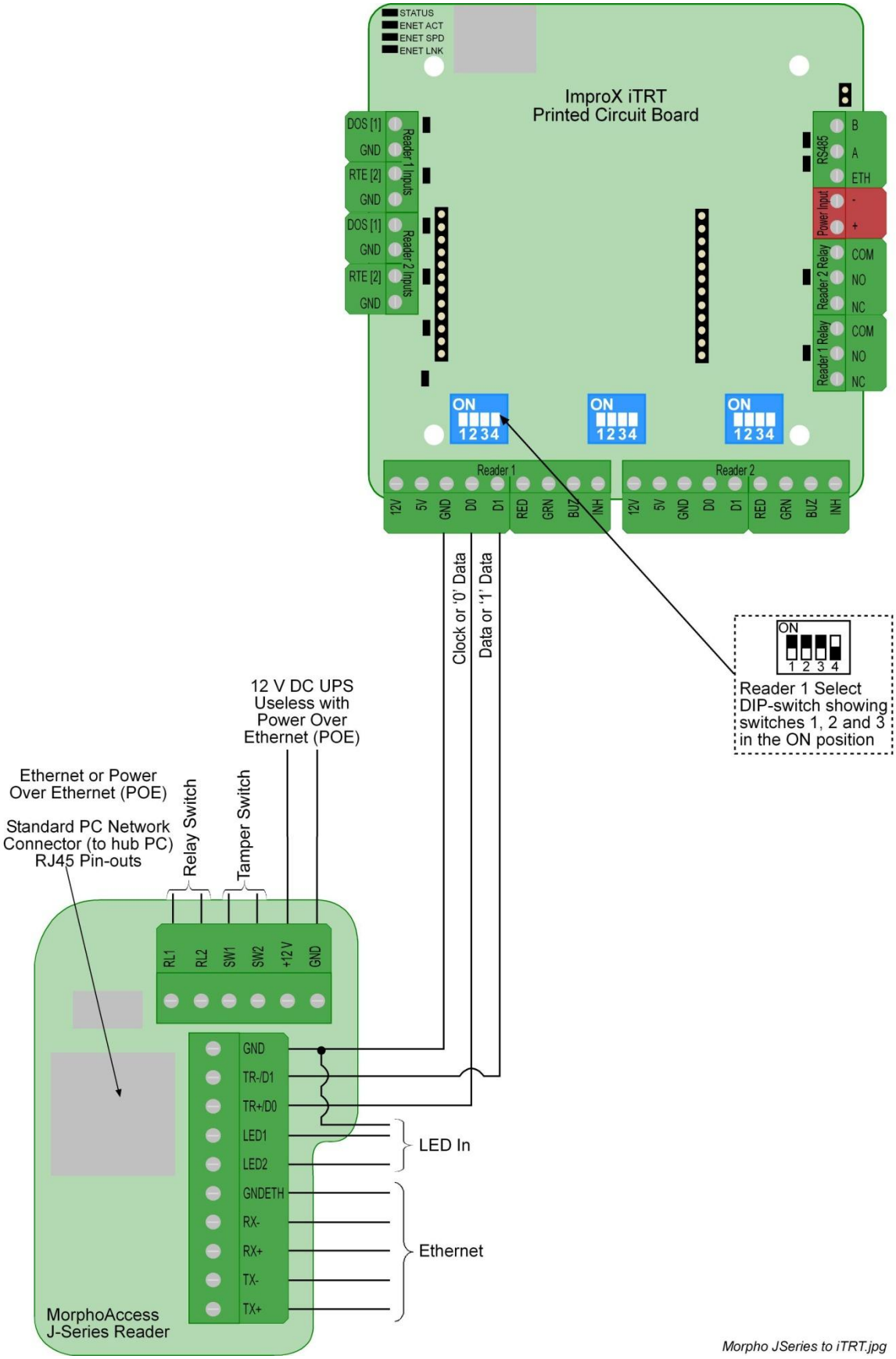


Figure 5 – MorphoAccess™ J-Bio or J-Dual Connected to the ImproX iTRT and LAN

Connection to the MorphoAccess™ J-Bio or J-Dual to the MfT

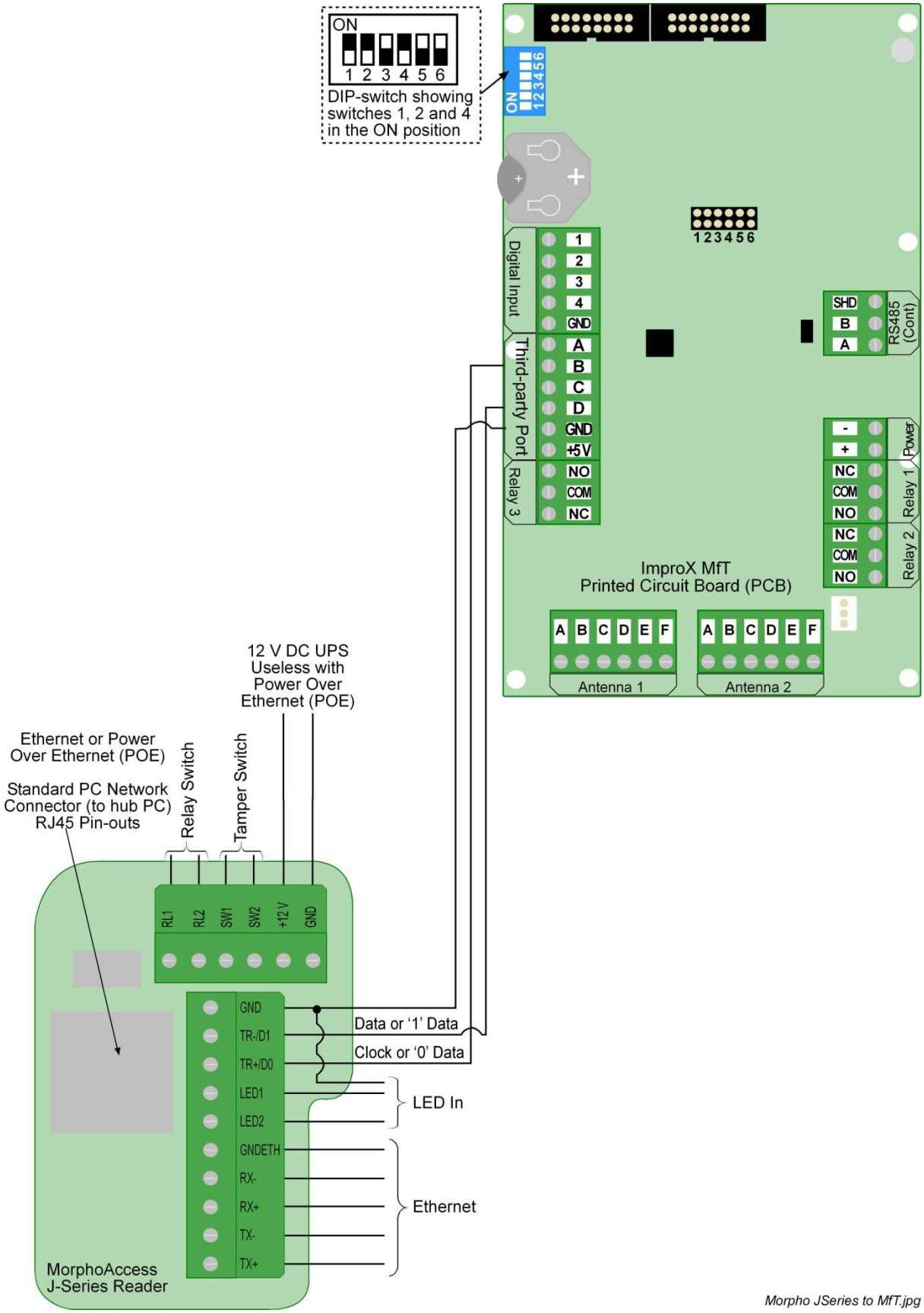


Figure 6 – MorphoAccess™ J-Bio or J-Dual Connected to the ImproX MfT and LAN

Connection to the MorphoAccess™ J-Bio or J-Dual to the TA

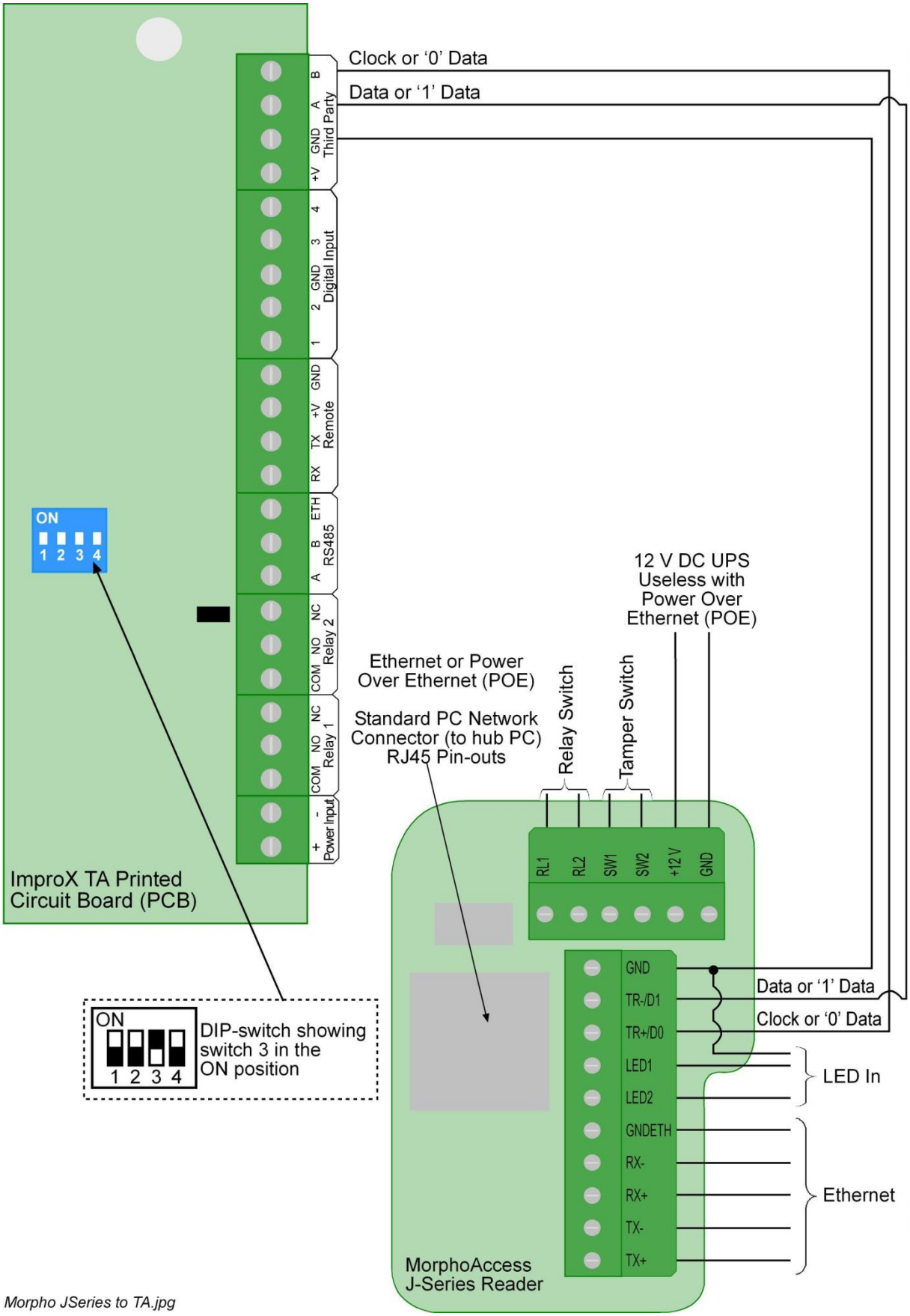


Figure 7 – MorphoAccess™ J-Bio or J-Dual Connected to the ImproX TA and LAN

Installation and Setup of the MSO300 Enrollment Reader and Verification Dongle

Ensure that you unlock your Registration Interface (by purchasing a Biometric Unlock Code) before proceeding further.

.NET Framework Installation

If the .Net Framework is NOT already installed, download the update as follows: From **http://www.microsoft.com/downloads**, download the **.NET Framework Version 2.0** update.

*Alternatively download the update from **http://www.impro.net/site/downloads/listing/10/Other**. From the list of displayed files, select **Files for Sagem Enrolment**. This package includes the .NET Framework installation files.*

MSO300 Enrollment Device Driver Installation

Install the drivers, before you plug in the MSO300.
If connected, disconnect the MSO300 Enrollment Reader from the PC.

1. If running a **32-bit** operating system, continue as follows:
   - Browse to **C:\ImproNet\driver\Sagem MorphoSmart USB 32 bits Driver**.
   - Double-click on the **Sagem MorphoSmart USB Drivers.msi** file.
2. Alternatively, if running a **64-bit** operating system, continue as follows:
   - Browse to **C:\ImproNet\driver\Sagem MorphoSmart USB 64 bits Driver**.
   - Double-click on the **Sagem MorphoSmart USB 64 bits Drivers.msi** file.
3. At the Welcome screen, click the **Next** button.
4. Click the **Next** button to install in the default directory.
5. Click the **Install** button.
6. Click the **Finish** button.

Verification Dongle Device Driver Installation

Install the drivers, before you plug in the Verification Dongle.
If connected, disconnect the Verification Dongle from the PC.

SafeNet Dongle

1. Browse to **C:\ImproNet\driver\SafeNetDongle**.
2. Double-click the **SentinelProtectionInstaller.7.4.0(DriversOnly).exe** file.
3. At the Welcome screen, click the **Next** button.
4. Select the **I Accept the Terms in the License Agreement** radio button.
5. Click the **Next** button.
6. Under Setup Type, select either the **Complete** or **Custom** radio button.
7. Click the **Next** button.
8. Click the **Install** button.
9. At the Windows Firewall Detected screen, click the **Yes** button.
10. Click the **Finish** button.

Morpho Dongle (MSO-EVerif)

1. If running a **32-bit** operating system, browse to **C:\ImproNet\driver\Morpho Dongle\x86.**
2. Alternatively, if running a **64-bit** operating system, browse to **C:\ImproNet\driver\Morpho Dongle\x64**.
3. Double-click on the ACR38U_PCSC_Driver-1.1.6.1.msi file.
4. At the Welcome screen, click the **Next** button.
5. Click the **Next** button to install in the default directory.
6. Click the **Install** button.
7. Click the **Finish** button.

MSO300 Installation

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 Securite\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.

MSO300 Firmware Upgrade Procedure

1. Browse to **C:\ImproNet\driver\Sagem MorphoSmart Firmware Update**.
2. Double-click on the **Firmware_MSO.exe** file.
3. At the Welcome screen, click the **Next** button.
4. Select the method by which you want to upgrade your MSO300 Enrollment Reader.
   - **A Serial Connection**
   - **A USB Connection**
5. Click the **Next** button.
6. Once the result shows Upgrade Successful, click the **Finish** button.

Verification Dongle Installation

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.

Morphokit Licensing Service Installation

The Morphokit Licensing Service runs continuously after installation. If you do not see evidence of the SagemSecurite_Licence_Protection.exe file running in the Windows Task Manager, install the software as follows.

1. Browse to **C:\ImproNet\driver**.
2. Double-click on the **SagemSecurite_Licence_Protection_Installer.exe** file.

3. At the Welcome screen, click the **Next** button.
4. Click the **Next** button to install in the default directory.
5. Click the **Next** button.
6. Click the **Close** button.

Creating a Data Execution Prevention Exception for Sagem Securite Licence Manager

1. From the **Control Panel**, select the **System** option.
2. Select the **Remote Settings** option.
3. In the System Properties dialog, select the **Advanced** tab.
4. In the Performance group, click the **Settings...** button.
5. Select the **Turn On DEP for all Programs and Services Except Those I Select** radio button.
6. Click the **Add...** button.
7. Navigate to the installation directory at **C:\Program Files\Sagem Securite\Licence Protection**.
8. Double-click on the following executable files:
   - **SagemSecurite_Licence_Protection.exe**
   - **SagemSecurite_Licence_Manager.exe**
9. Click the **OK** button.
10. At the System Properties dialog, click the **OK** button.
11. Click the button.

MSO300 Biometric Address Configuration

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

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

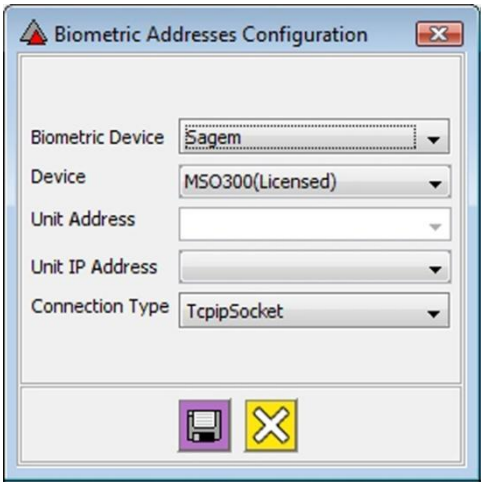


Figure 8 – Biometric Addresses Configuration Dialog

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 **MSO300(Licensed)** option.

*The Unit Address field appears greyed out for Sagem, as it refers to addresses of units on the RS485 bus, Morpho (Sagem) does not currently support RS485. The **Unit IP Address** field is reserved for future use.*

5. Click on the button.
6. Click on the button.

Repeat steps 1 to 6 above to setup separate Enrollment Readers for each System PC running Access.

Morpho MA100, MA120, MA500 or J-Series Internal Parameter Setup

*The Morpho MA1XX, MA5XX and J-Series biometric devices have the following default IP Address: **134.1.32.214**.*

USB Flash Disk Setup

Using a **USB Flash Disk** (refer to the unit's Installation Manual for acceptable Flash Disk sizes) continue as follows:

1. Format the Flash Disk as indicated in the unit's Installation Manual.
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.

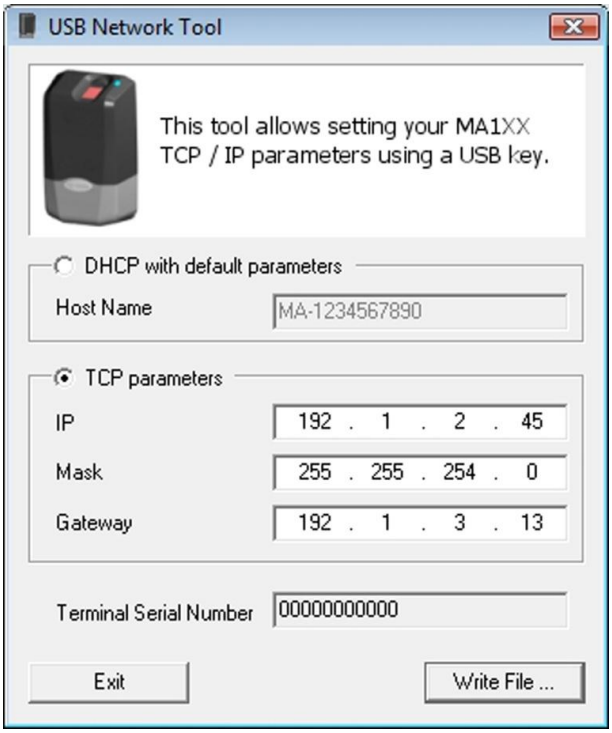


Figure 9 – USB Network Tool Dialog

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. With the MA100 powered up, 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.

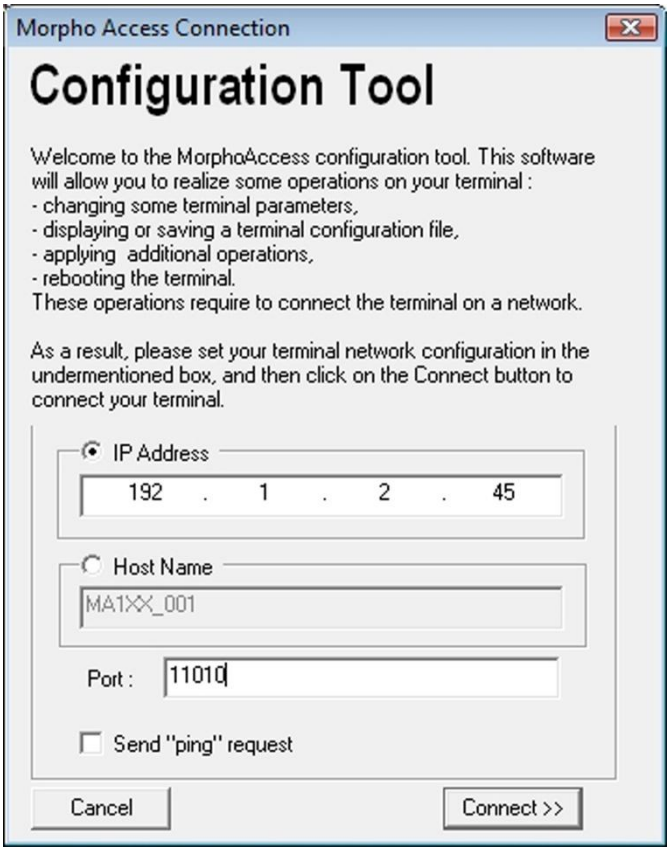


Figure 10 – Configuration Tool Dialog

3. In the Morpho Access Connection dialog, ensure that the **IP Address** field reflects the same IP Address details as used in point 0 on page 18.
4. Click the **Connect >>** button.

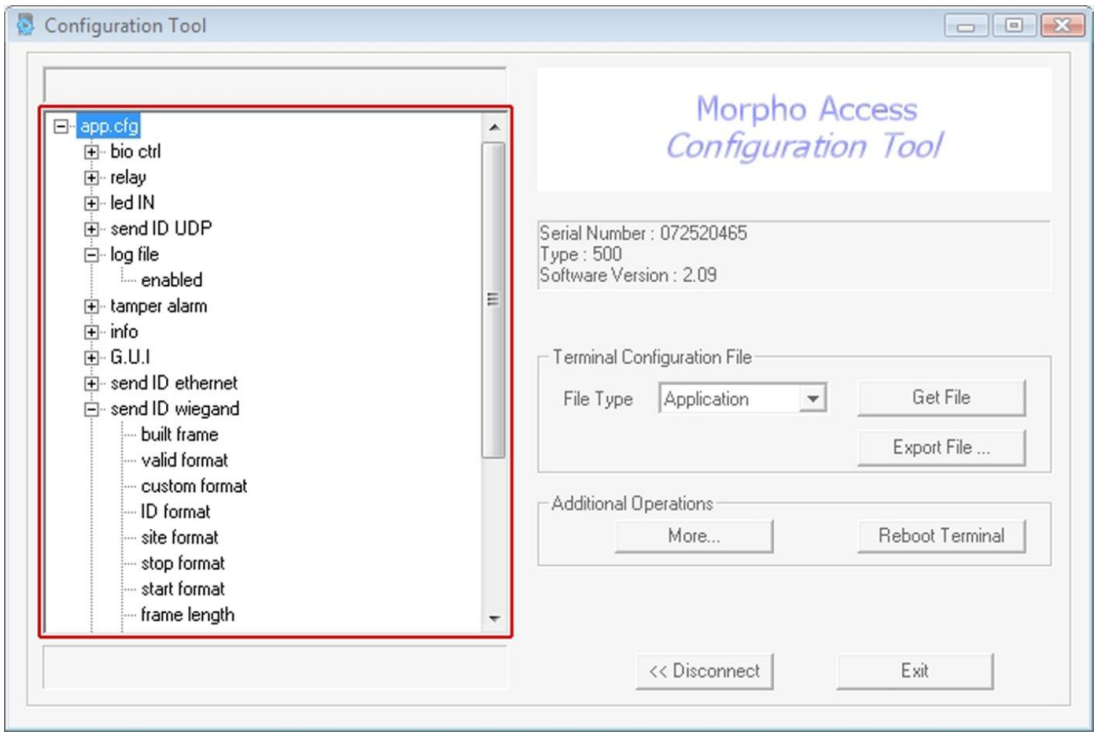


Figure 11 – Configuration Tool Dialog

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

*The **Log File** setting referred to in point 6 (only available on sites using MA100 and MA500 Morpho Readers) is required for the functionality of the **Sagem Identify Report**. In Installations without installed MA100 and MA500 Morpho 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:
   - built frame
   - valid format—**1**
   - custom format—**0.0**
   - ID format—**0.40**
   - site format—**0.0**
   - stop format—**4.0**
   - start format—**4.0**
   - frame length—**40**
   - HID conversion—**0**
   - site code—**0**
   - enabled—**1**
10. Apply the settings by **rebooting the Terminal**.

Problems and Solutions

1. **Problem**—Software fails to report denied transactions on sites with installed Morpho J-Series Readers.
   Solution—Adjust the following settings under **Failure ID**:
   - not recognized ID—**0**
   - enabled—**1**
2. ***Problem**—Wiegand Code not sent through.*
   Solution 1—Swap your Data 1 and Data 0.
   Solution 2—Check each setting in the **App** file according to the following list:

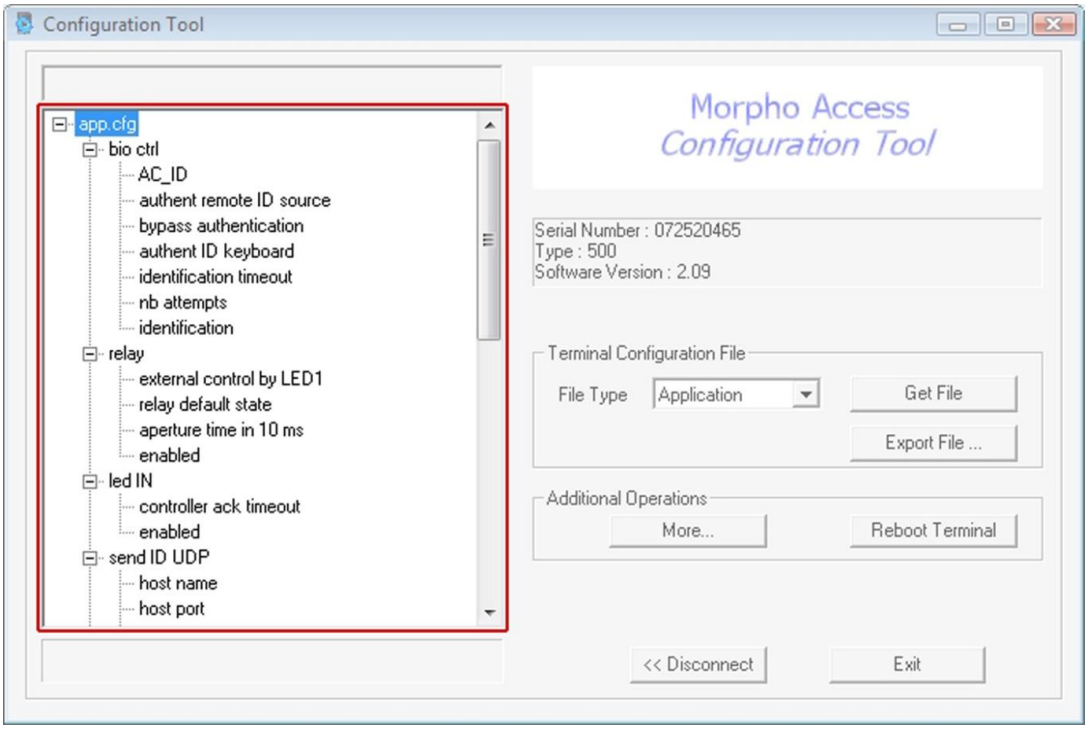


Figure 12 – Configuration Tool Dialog

- **bio ctrl**
  - AC_ID—**FINGER;CARDDATA;KBD;WGDTCLK;**
  - bypass authentication—**0**
  - authent timeout—**10**
  - authent card mode—**1**
  - authent PK contactless—**1**
  - authent ID contactless—**0**
  - authent remote ID source—**0**
  - authent ID keyboard—**0**
  - identification timeout—**5**
  - nb attempts—**2**
  - identificaton—**1**
- **contactless**
  - desfire params—**2**
  - enabled profiles—**0**
  - data type—**0.1**
  - data offset—**0**
  - data length—**0**
  - C—**1**
  - B—**4**
  - event on—**2**
  - data format—**0**
- **relay**
  - external control by LED1—**0**
  - relay default state—**0**
  - aperture time in 10 ms—**300**
  - enabled—**1**
- **led IN**

  - controller ack timeout—**300**
  - enabled—**0**
- **send ID UDP**
  - host name—**134.1.2.189**
  - host port—**11020**
  - enabled—**0**
- **log file**
  - enabled—**1**
- **tamper alarm**
  - interval—**1500**
  - level—**0**
- **info**
  - release—**15**
  - minor—**9**
  - major—**2**
  - type—**500**
- **G.U.I**
  - display hour—**0**
  - led out signal—**0**
  - database conversion—**500**
  - display user info—**2**
  - time and attendance icons—**1**
  - default language—**0**
  - volume—**5**
- **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 port—**11020**
  - controller 2 IP—**134.1.2.189**
  - controller 1 port—**11020**
  - controller 1 IP—**134.1.2.189**
  - mode—**0**
- **send ID wiegand**
  - built frame
  - valid format—**1**
  - custom format—**0.0**
  - ID format—**0.40**
  - site format—**0.0**
  - stop format—**4.0**
  - start format—**4.0**
  - frame length—**40**
  - 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**
  - terminal identifier—**178**
  - parity—**0**
  - stopbits—**1**
  - databits—**8**
  - speed—**11520**
  - mode—**485**
  - enabled—**0**
- **failure ID** (used for diagnostic purposes)

*In this mode, set the ImproX iTRT to **Wiegand Open Mode** (that is on the DIP-switch, 123 OFF and 4 ON)*

  - 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—**1**
- **wiegand in**
  - custom format—**0.0**
  - ID format—**9.16**
  - site format—**1.8**
  - stop format—**2.12**
  - start format—**2.12**
  - frame length—**26**
  - check site code—**1**
  - site code—**7**
- **data clock in**
  - data inverted—**0**
  - clock inverted—**0**
- **modes**
  - idle timeout—**0**
  - idle peripherals—**3**
  - T&A operation timeout—**20**
  - time mask—**0**
  - time and attendance—**0**

Morpho MA200 or MA300 Internal Parameter Setup

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: Morpho MA200/300 MorphoAccess Installation Guide, SK-0000011145-03 – January 2004.

Notes on Set-up for Morpho MA200 or MA300

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

Internal Morpho 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 Morpho manual, and indicates whether, and how, this information relates to the Morpho-ImproNet integration process. The Morpho MA200 or MA300 Manual headings are listed **sequentially** in Table 2 as a guide to the use of the Morpho 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 refers you to the STEP where this information's used.*

STEP DESCRIPTION	MORPHO MANUAL HEADING	PROCEDURE OR COMMENTS
1. PHYSICAL INSTALLATION	**INSTALLATION PROCEDURE**	Follow the Morpho Manual procedures.
2. ELECTRICAL CONNECTION	**ELECTRICAL INTERFACE**	The Morpho Interfaces used in this application are J1, J3 and J4 (Refer to the Morpho 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 Morpho Manual if required.
	CONFIGURING THE MORPHOACCESS™	
	Motherboard Configuration	Refer to the Morpho Manual. Configure the Switches as follows: Set SW1 and SW2 for Wiegand Mode. Set SW3 and SW4 as indicated in the Morpho Manual. Set SW7 and SW8 for Wiegand Mode.
	MORPHOACCESS™ SOFTWARE	Refer to step 5 of this Table.

STEP DESCRIPTION	MORPHO MANUAL HEADING	PROCEDURE OR COMMENTS
3. INTERNAL SETUP OF THE READER BEFORE INTEGRATION AND USE WITH IMPRONET	**BIOMETRIC MANAGEMENT OPERATIONS**	Refer to the Morpho 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 Morpho Manual.
	SETTING UP NETWORK PARAMETERS	Refer to the Morpho Manual.
	SETTING UP THE SYSTEM ADMINISTRATOR PIN	Refer to the Morpho Manual. This PIN provides access to the SYSTEM Menus in the Morpho Software for administration of the Reader.
	SETTING UP THE MORPHOACCESS™ ADMINISTRATOR PIN	Refer to the Morpho Manual. This PIN provides access to the MACCESS Menus in the Morpho Software for administration of the external management.
	Setting Up Host Communication	Refer to the Morpho Manual. Set the Host Com value to 3.
	Setting Up User Interface	Refer to the Morpho Manual.
	Setting Up Wiegand or Dataclock Output	Refer to the Morpho Manual.
	Setting Up Wiegand Interface	Refer to the Morpho Manual. The default format is 26-Bit.
	Frame Definition	Refer to the Morpho Manual.
	Configuration Keys	Refer to the Morpho Manual.. Set Section is OUT. Set Length is 26.
	Setting Up Etherlink Parameters	Refer to the Morpho Manual. Set Etherlink Send is 1. Set IP Address as required.
	Setting Up Time Attendance	Refer to the Morpho Manual.
4. OPTIONAL SETUP AND BACKGROUND INFORMATION	**THE VERSION MENU**	Refer to the Morpho Manual.
	THE SERIAL NUMBER MENU	Refer to the Morpho Manual.
	THE SETTING MENU	Refer to the Morpho 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.
5. USER INTERFACE SETUP	**MORPHOACCESS™ SOFTWARE USER INTERFACE**	Refer to the Morpho Manual.
	Access Control by Identification (MA200)	Refer to the Morpho Manual. The Mode is 0.
	Access Control by Identification (MA300)	Refer to the Morpho 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 Morpho Manual. Ensure that all users are aware of these rules.

Table 2 – Internal Configuration of the Morpho Fingerprint Readers

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

Configuration of Morpho Readers into the ImproNet System

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

Each Morpho Reader used in the Biometric Server requires its own Unlock Token. For details of the unlocking procedure refer to the section titled Morpho Dongle Protection using the Unlock Token on page 29.

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** (**SYSDBA**) and **Password** (**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 displays. For the units **NOT** detected, specify the unit **Type**.

Detecting Morpho 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**.

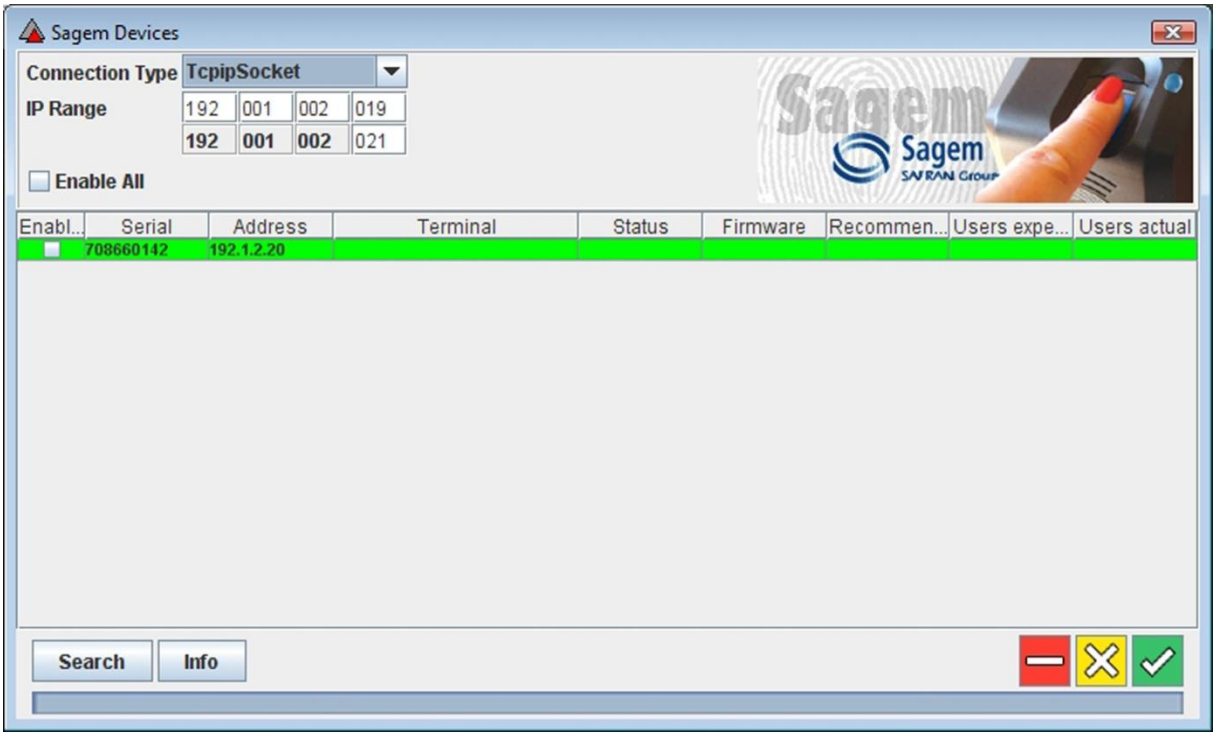


Figure 13 – Sagem Devices Dialog

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 Morpho units, they appear as records in the table with their Serial Numbers, IP Addresses and their current Status. The displayed units appear as follows:*

- *All newly discovered units highlight in **Green**.*
- *All units with changed IP Addresses highlight in **Orange**.*
- *All units that are in the Database but have been found to be off-line or missing highlight in **Red**.*

*The **Enabled** checkbox enables or disables each individual Morpho 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 Morpho units on the network.*
The Server will not attempt communication with a disabled Morpho unit.

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

*On enabled Morpho 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 Morpho Reader and the unused capacity.*

4. When you are finished using the **Sagem Devices** dialog, click the button.
5. Click the button.
6. After setting up the units, do a **Full Upload** to create fresh databases on the units.
7. 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 Morpho 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.

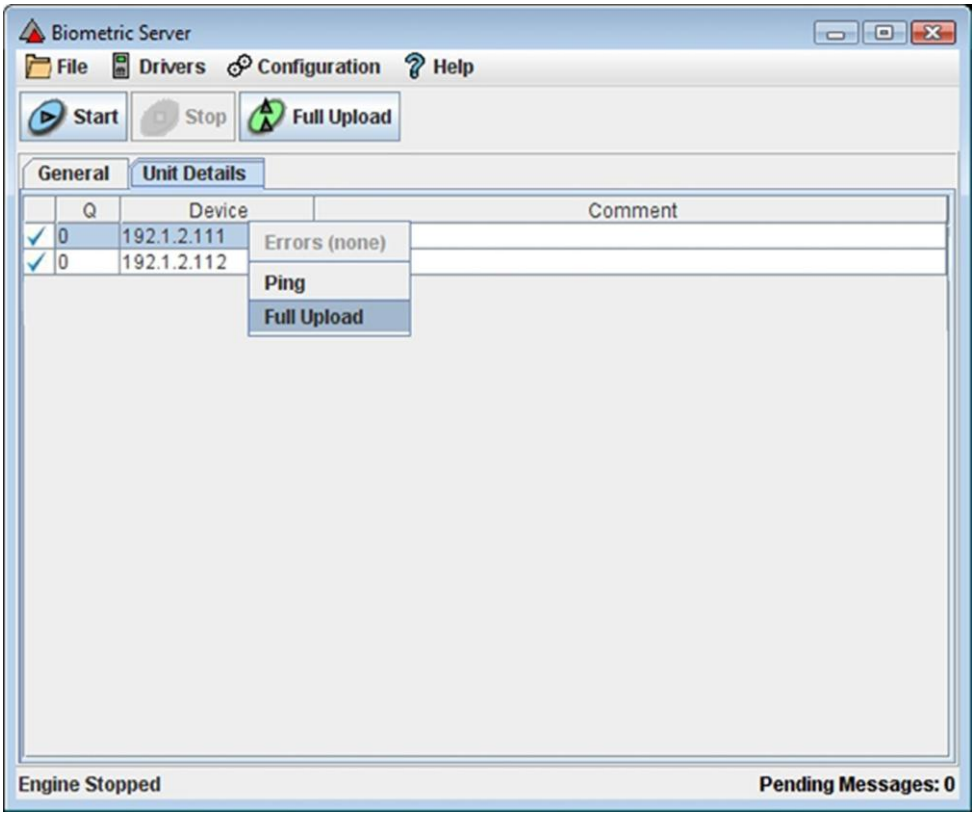


Figure 14 – Unit Details Tab

The queue processes automatically during normal operation (that is after you press the **Start** button). You may perform a full upload on a specific Morpho 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. This communication structure enables duplicate search functionality. To use this feature, ensure that you have a MorphoSmart™ MSO300 Registration Reader and one of the following licences: an **IDENT LITE** (5 000 templates), an **IDENT** (10 000 templates) or an **IDENT PLUS** (20 000 templates).

Usually installed on a USB Flash Disk, the IDENT licence connects direct to the Biometric Server. You may, however, purchase an IDENT licence that resides direct on the MSO300, for use in a stand-alone PC environment.

Enabling Matcher in the Biometric Server Software

1. Start the Biometric Server Software (for more information, see page 26).
2. From the menu bar, select **Configuration**>**Sagem**>**Matcher**.

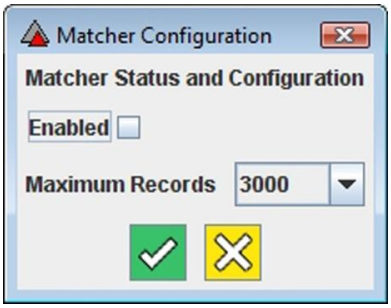


Figure 15 – Matcher Configuration Dialog

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, IDENT 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 runs upon starting the Biometric Server.

Enabling Duplicate Search at an Enrollment Station

For detailed steps on arriving at the Biometric Enrollment dialog, refer to page 30.

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.

Morpho 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 Morpho Reader of the same type. That is, any MA100 Unlock Token unlocks any MA100 Morpho Reader, any MA200/300 Token unlocks any MA200, MA300 or MA500 Morpho Reader and any J-Series Token unlocks any J-Bio or J-Dual Reader. However, once an Unlock Token is used with a specific Morpho 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 Morpho 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 Morpho Readers enabled in the Biometric Server, continue as follows:

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

Enrolling Users on the System

Setting Truncation for Enrollment

1. From Windows® select **Start**>**Programs**>**ImproNet**>**Access**.
2. From the Main Menu, select **File**>**Preferences**.
3. Select the **Enrollment** tab.
4. Alongside the **Ascii, Biomentric, Magstripe** option, click the **Truncation** button.
5. From the **Tag Format** drop-down list, select the **26-bit Normal** option.
6. Click the button
7. Close the Preference Configuration dialog by clicking the button

Tagholder Setup

1. In the Navigator Pane, select the **Tagholder** icon.
2. Open the **Edit Tagholder** or **Add Tagholder** dialog.
3. Select **New Tag** to enter the **Tag** dialog.
4. Have the Tagholder place their Tag on the Enrollment Reader.
5. Click **Read Tag** (or just enter a number of 7 digits or less in the **Tag Code** field).
6. From the **Tag Type** drop-down list, select **ASCII, Biometric, Magstripe**.

7. Set the Access Groups in the usual way.
8. Click on the button.
9. Click on the **Biometric Enrollment** button.

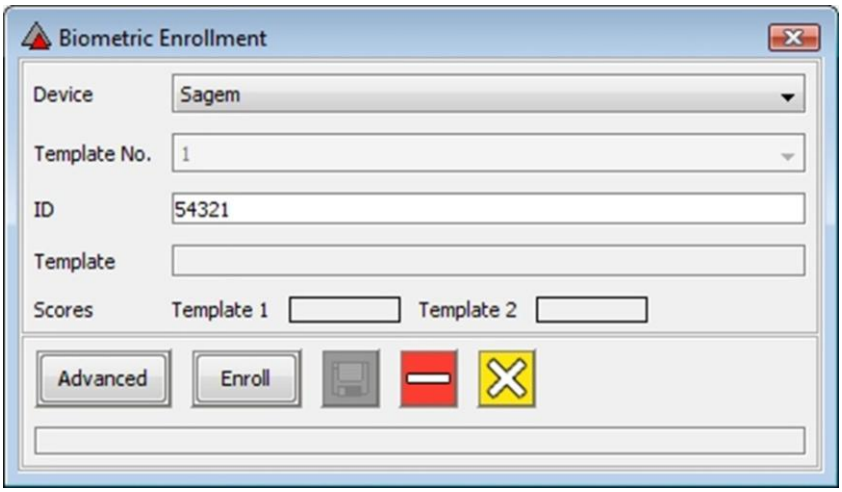


Figure 16 – Biometric Enrollment Dialog

10. 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 Morpho units. Other Biometric Devices allow you to enroll multiple templates per user. Morpho 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.*

11. 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. Changing the default Database to a number greater than **0** may result in fingerprint templates not uploading to the MA100, MA120, MA200 and J-Series Readers.
- **DB for this User**—the default MA300 or MA500 database to which this users templates are stored. Changing the default Database to a number greater than **0** may result in fingerprint templates not uploading to the MA100, MA120, MA200 and J-Series Readers.
- **Quality Threshold**—determines the minimum quality score for each template. A higher threshold, leads to a better quality template. Make your selection from the range **0** to **255**. For best results, we recommend a score of above **200**.

- **Use Consolidation**—allows you to capture the fingerprint **3** times. The Software then saves the best capture. If disabled, the Software only captures the fingerprint once.
- **Enable Matching**
- **Matching Threshold**—determines the minimum accepted matching threshold during the verification stage of each template capture. For full functionality, ensure that you have a Morpho Dongle or Verification Dongle installed and plugged in. Make your selection from the range **0** to **255**. For best results we recommend a score of above **200**.
- **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 and that you have a MorphoSmart™ MSO300 Registration Reader and either an **IDENT LITE** (5 000 templates), an **IDENT** (10 000 templates) or an **IDENT PLUS** (20 000 templates) licence**.** Refer to the section Duplicate Search (1:N Matching) on page 28 for more information.

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

Fingerprint Placement Rules

Figure 17 shows the area of the fingerprint that contains the most information. Therefore, when enrolling Tagholders, ensure they place their fingers as shown in Figure 18.

Figure 17 – Area of the Fingerprint Containing the most Information

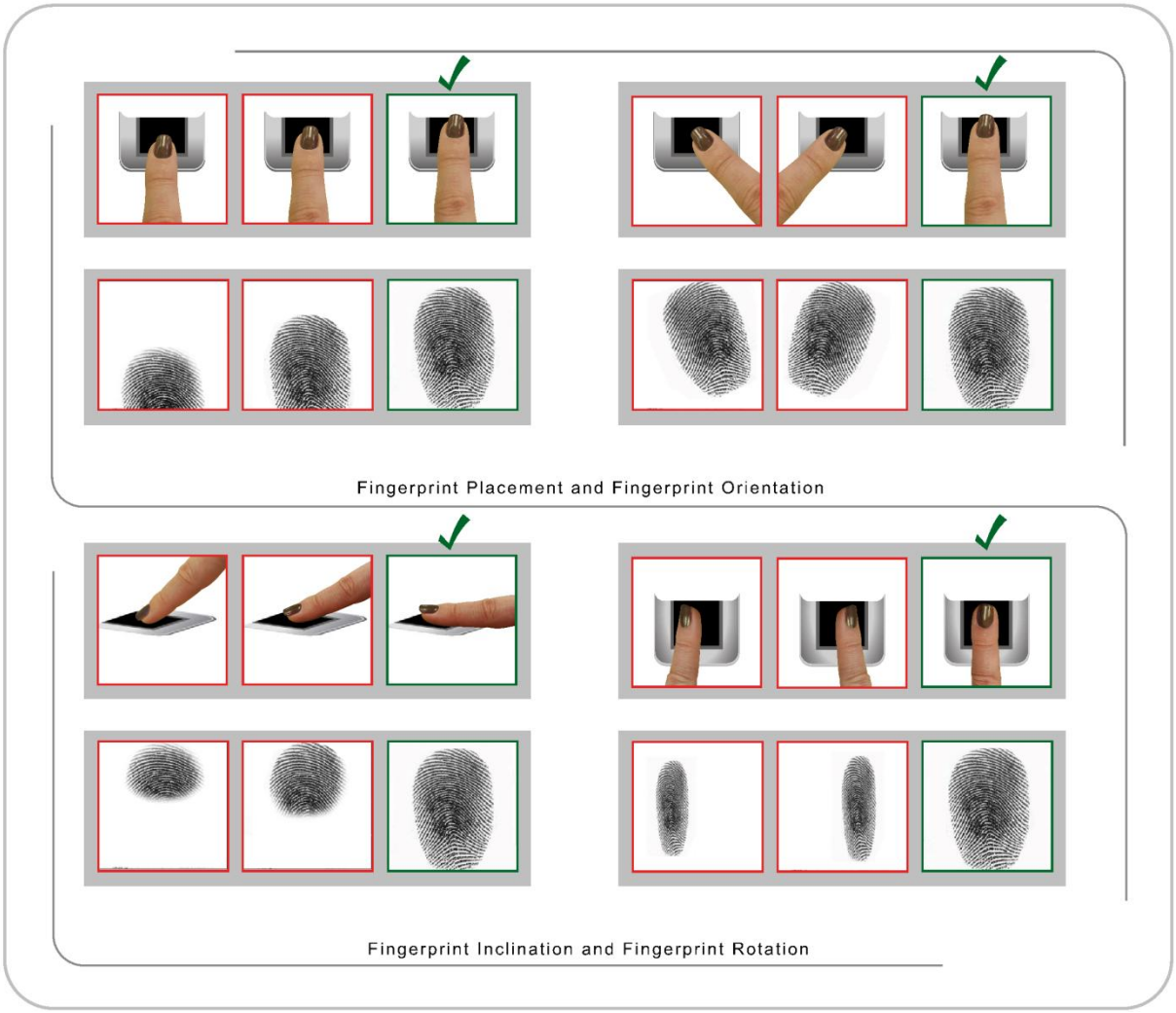


Figure 18 – Fingerprint Placement Rules (Generic Enrollment Reader, Fingerprint Sensor Shown)

Enrollment procedure at the Morpho 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 Morpho Readers.

Configuration of MIFARE® Encoders into the ImproNet System

In instances where you cannot store fingerprint templates in the ImproNet Database, you may write templates direct to the MIFARE® Tag. Reasons for this could include: cost, Reader limits, laws of the country or just general safety concerns.

Using MIFARE® Encoder support, templates do not upload to the Biometric Readers. Instead templates are written directly to the MIFARE® Tag. Thus when you present the MIFARE® Tag to the Biometric Reader, it reads the template information from the Tag. When presenting your finger to the Reader, the Reader performs a 1:1 authentication of the template information stored on the MIFARE® Tag.

The MIFARE® Encoder is only supported when using the Morpho MA120, MA520 and the J-Dual.

You may have as many MIFARE® Tags with templates written to them as supported by your System. That is, up to 8 000 in an IXP300 System, up to 160 000 in an IXP400 System and up to 300 000 in an IXP400i System. You are therefore, not limited by the number of templates supported by the Biometric Reader.

ImproNet offers MIFARE® Encoder support on the following 32-bit and 64-bit Operating Systems: Windows XP, Windows Vista and Windows 7.

*ImproNet supports **1 K** and **4 K** MIFARE® Tags used with the **SDI010 Contact or Contactless Reader** (MIFARE® Encoder).*

MIFARE® Encoder Driver Installation

*On a **32-bit** Operating System, ensure you use Driver version **V4.36**.*

*On a **64-bit** Operating System, use Driver version **V5.18**. V5.18 is however a legacy Windows XP Driver and therefore installation must take place from a PC running Windows XP.*

1. Plug the **SDI010 Contact or Contactless Reader** into an unused USB Port on the PC.
2. From the Found New Hardware dialog, click the **Cancel** button.
3. From the **Control Panel**, select the **Device Manger** option.

SDI010 Contact (Smart) Card Reader Driver

1. From the displayed tree, select the **Other Devices** node.
2. From the displayed list, select the **SDI010 Smart Card Reader** option.
3. Select the **Update Driver Software...** option.
4. Select the **Browse My Computer for Driver Software** option.
5. Browse to **C:\ImproNet\driver\Mifare Encoder**.
6. Click the **OK** button.
7. Select the **Include Subfolders** checkbox.
8. Click the **Next** button.
9. At the **Found New Hardware** dialog, click the **Cancel** button.
10. At the Update Driver Software – SDI010 Smart Card Reader dialog, click the **Close** button.

SDI010 Contactless Reader Driver

1. From the displayed tree, select the **Other Devices** node.
2. From the displayed list, select the **SDI010 Contactless Reader** option.
3. Select the **Update Driver Software...** option.
4. Select the **Browse My Computer for Driver Software** option.
5. Browse to **C:\ImproNet\driver\Mifare Encoder**.
6. Click the **OK** button.
7. Select the **Include Subfolders** checkbox.
8. Click the **Next** button.
9. At the Update Driver Software – SDI010 Contactless Reader dialog, click the **Close** button.
10. At the **Device Manager** dialog, click the button.

MIFARE® Encoder Firmware Installation

V6.32 is the supported Firmware version and is included in the ImproNet installation.

1. Browse to **C:\ImproNet\driver\Mifare Encoder\SDI010_fw6.32**.
2. Run the file **FwUpdate.exe**.
3. Follow the prompts as they appear thus completing the Firmware installation.

MIFARE® Encoder Configuration and Testing

Ensure the SDI010 Contact or Contactless Reader is plugged in and that a MIFARE® Tag is in position on the MIFARE® Encoder.

1. Browse to **C:\ImproNet\test.exe**.
2. In the Card Writer Test dialog, from the **Select Writer** drop-down list, select the **Mifare SCM** option.
3. At the Contactless Card error message, click the **OK** button.
4. On the Left-hand-side of the Card Writer Test dialog, click the **Configure** button.
5. From the Device Name drop-down list, select the **SCM Microsystems Inc. SDI010 Contactless Reader 0** option.
6. In the Mifare Contactless Card Writer Configuration dialog, click the **Autodetect** button.
7. At the Information dialog, click the **OK** button.
8. In the Mifare Contactless Card Writer Configuration dialog, click the **OK** button.
9. In the Card Writer Test dialog, from the Basic Operations group, click the **Autodetect** button.
10. From the Basic Operations group, click the **Read File Keys** button.
11. At the Test dialog, click the **OK** button.
12. From the Basic Operations group, click the **Load Keys** button.
13. At the Test dialog, click the **OK** button.
14. From the Basic Operations group, click the **Write** button.
15. At the Test dialog, click the **Yes** button.
16. Click the **Quit** button.

Key File Configuration

The steps that follow are optional for Contact (Smart) Card users. By following this procedure a unique to site security code writes to the Contact (Smart) Card. This unique security code prevents users gaining entry to site using unencrypted MIFARE® Tags.

1. Browse to **C:\ImproNet\test.exe**.
2. In the Card Writer Test dialog, from the **Select Writer** drop-down list, select the **Mifare SCM** option.
3. On the Left-hand-side of the Card Writer Test dialog, click the **Configure** button.
4. From the Key Files group, alongside the **Old Key File** textbox, click the button.
5. Browse to **ImproNet\keys\4K**.
6. Select the **oldkeys_Philips.ini** file.
7. Click the **Open** button.
8. Alongside the **New Key File** textbox, click the button.
9. Browse to **ImproNet\keys\4K**.
10. Select the **newkeys_Philips.ini** file.
11. Click the **Open** button.
12. Alongside the **Default Key File** textbox, click the button.
13. Browse to **ImproNet\keys\4K**.
14. Select the **defaultkeys_Philips.ini** file.
15. Click the **Open** button.
16. Click the **Check Key Files** button.

17. At the Information dialog, click the **OK** button.
18. Click the **Quit** button.

Writing Templates to the MIFARE® Tag

Editing the Biometric.properties File

1. Browse to **ImproNet\Biometric.properties**.
2. Set the **server.drivers.Sagem.enroll.writeToTag=false** property to **True**.
3. From the drop-down menu, select **File**>**Save**.
4. Click the button.

Setting Truncation for Enrollment

***Setup Truncation on ASCII Tag Types**, thus ensuring matching of Tags and generation of the Allowed Event. Enrolling a MIFARE® Tag at a MIFARE® Registration Reader or tagging at a MIFARE® Reader **requires truncation on the MIFARE® Tag type**.*

1. From Windows® select **Start>Programs>ImproNet>Access**.
2. From the Main Menu, select **File**>**Preferences**.
3. Select the **Enrollment** tab.
4. Alongside the **Ascii, Biomentric, Magstripe** option, click the **Truncation** button.
5. From the **Tag Format** drop-down list, select the **26-bit Normal** option.
6. Click the button.
7. Close the Preference Configuration dialog by clicking the button.

Tagholder Setup

1. In the Navigator Pane, select the **Tagholder** icon.
2. Open the **Edit Tagholder** or **Add Tagholder** dialog.
3. Select **New Tag** to enter the **Tag** dialog.
4. Have the Tagholder place their Tag on the Enrollment Reader.
5. Click **Read Tag** (or just enter a number of 7 digits or less in the **Tag Code** field).
6. From the Tag Type drop-down list, select **ASCII, Biometric, Magstripe**.
7. Set the **Access Groups** in the usual way.
8. Click on the button.
9. Click on the **Biometric Enrollment** button.

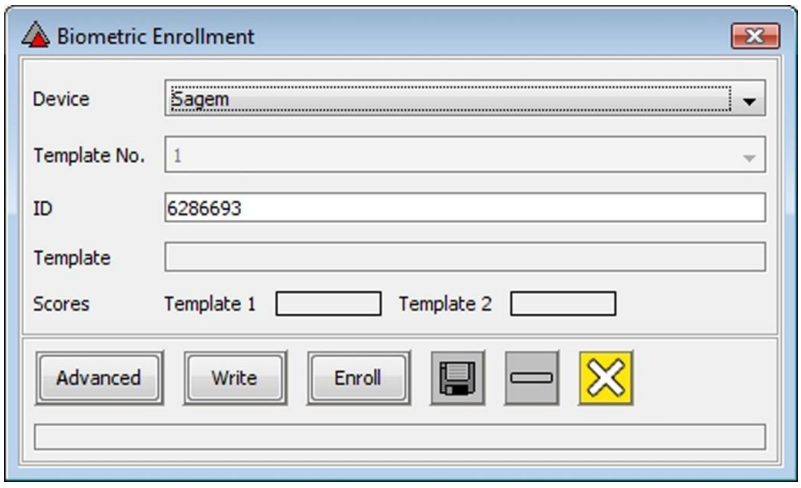


Figure 19 – Biometric Enrollment Dialog

10. 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**.
11. Place your MIFARE® Tag on the SDI010 Contact or Contactless Reader.
12. In the instance that this is a first-time enrollment, click on the **Enroll** button.
13. If you enrolled your template previously, and therefore wish to write an existing template to the MIFARE® Tag, click on the **Write** button. Otherwise, continue with the enrollment procedure as outlined under Enrollment procedure at the Morpho MSO300 (below).

Enrollment procedure at the Morpho MSO300

The number of times you present your finger depends on whether you have duplicate checking enabled.

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 **Write** button.
10. Click the button.

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

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 (and Service Pack 3) or later 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

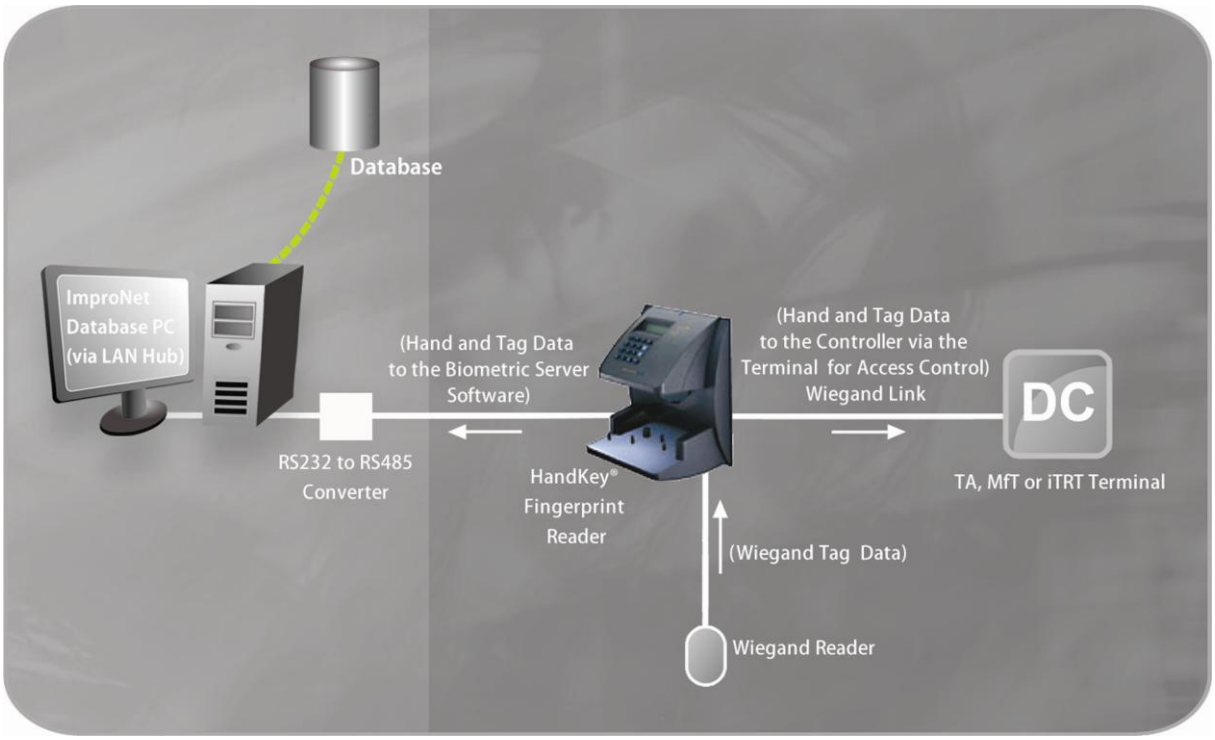


Figure 20 – Data Flow when using a HandKey® Reader with the ImproNet Software

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 TA, iTRT 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.

Connection to the ImproX iTRT

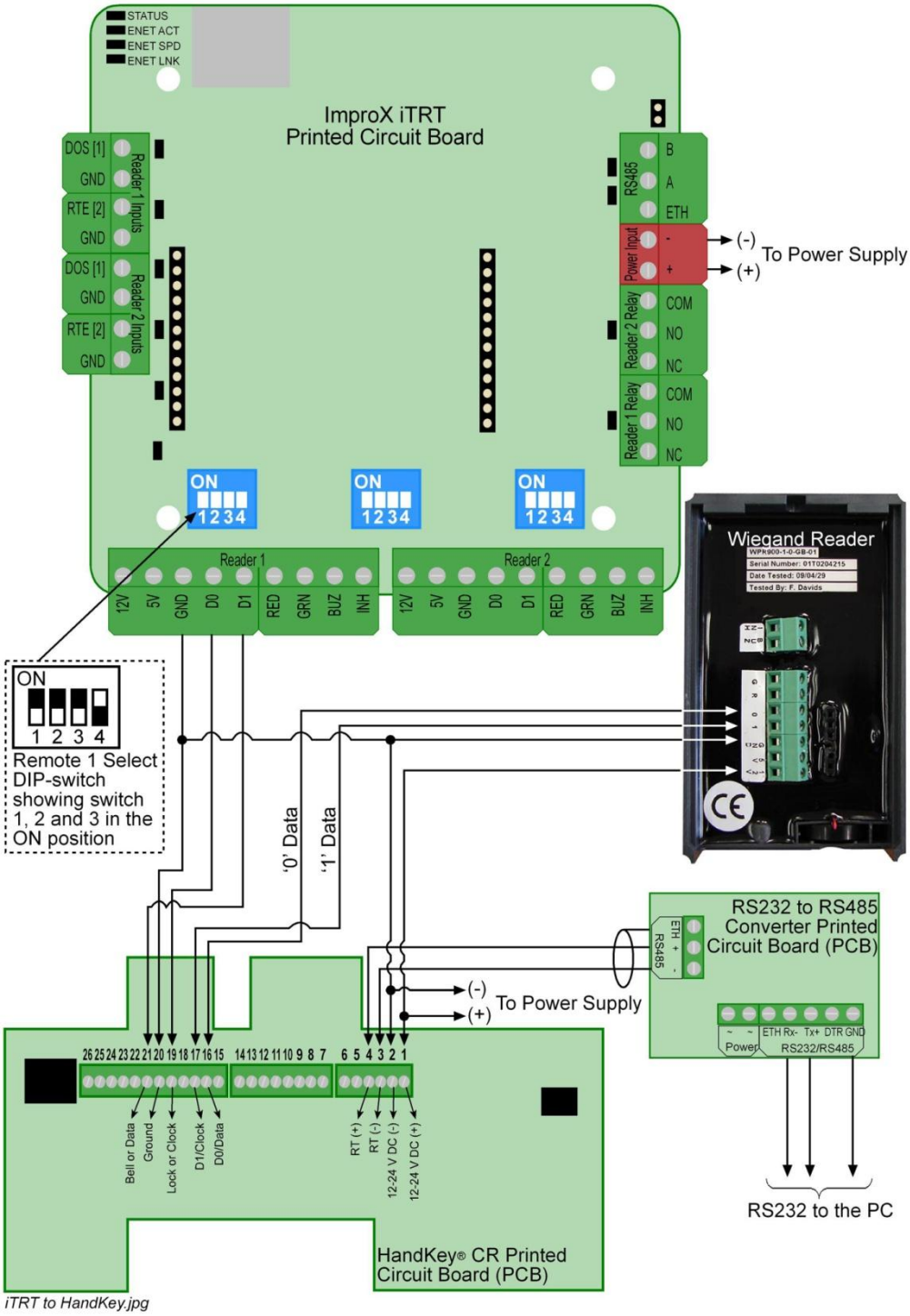


Figure 21 – HandKey® CR Reader Connected to the ImproX iTRT and LAN

Connection to the ImproX MfT

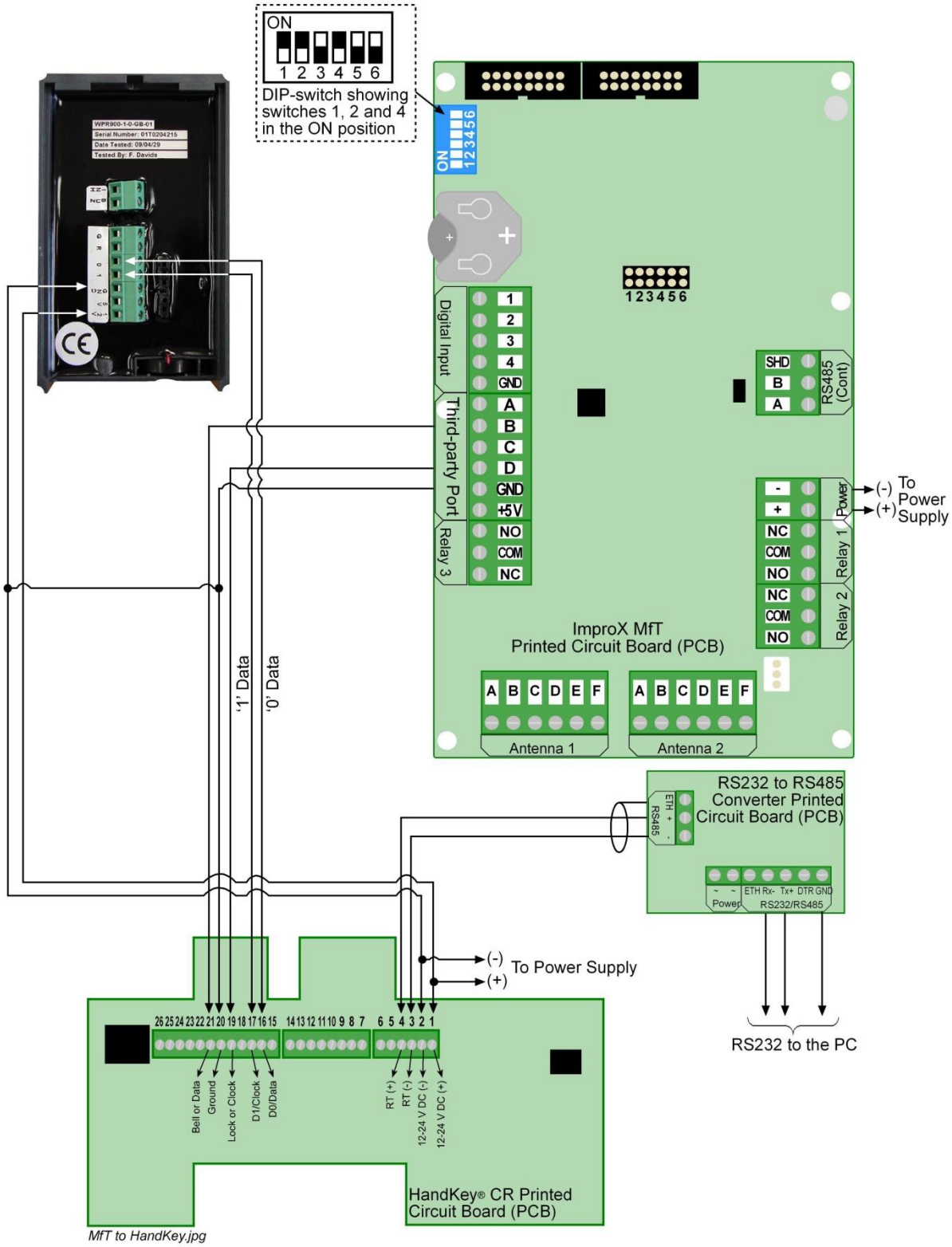


Figure 22 – HandKey® CR Reader Connected to the ImproX MfT and LAN

Connection to the ImproX TA

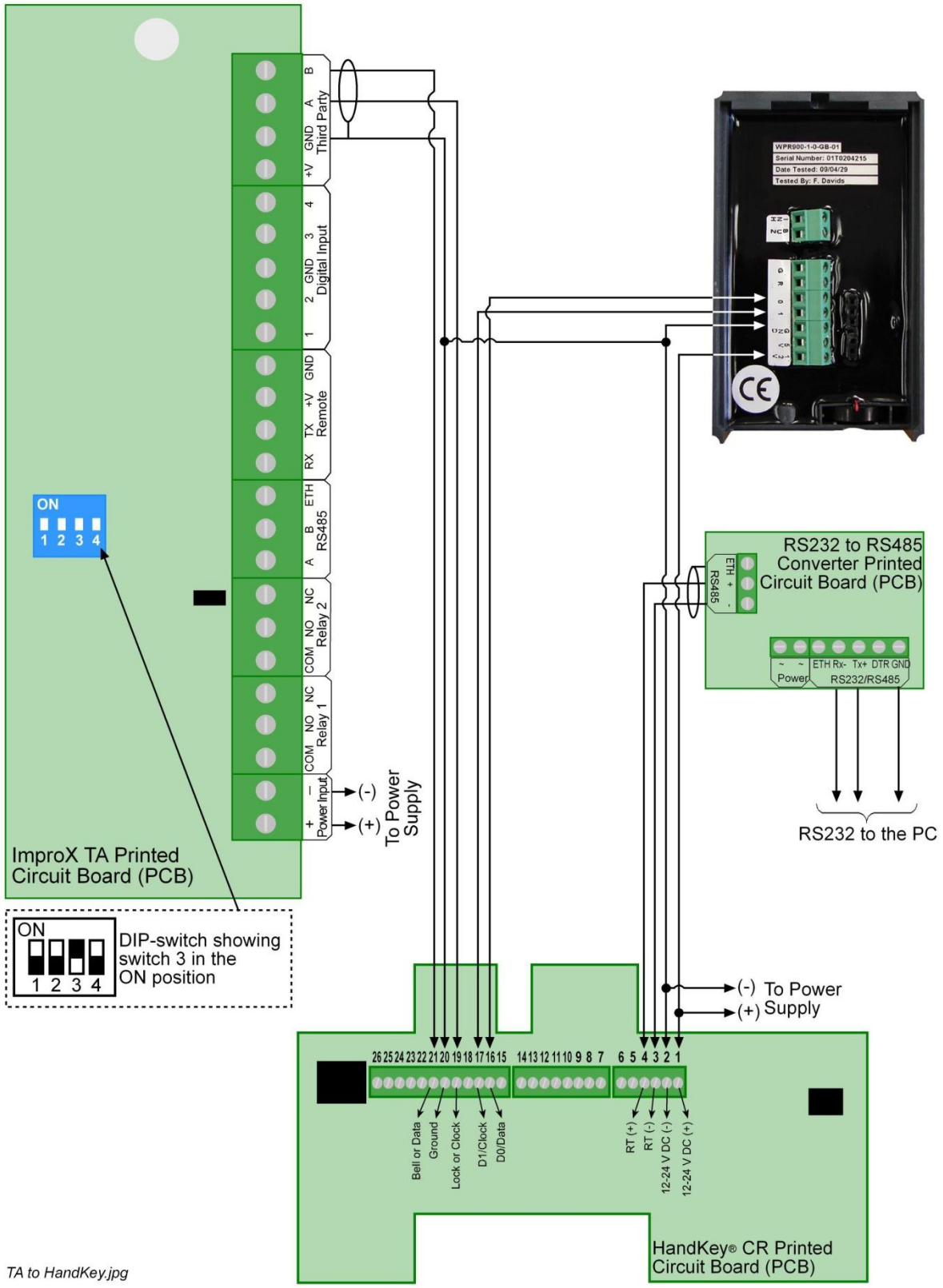


Figure 23 – HandKey® CR Reader Connected to the ImproX TA and LAN

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 21, Figure 22 or Figure 23.
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

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 TCPIP Socket.

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.

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.
4. In the Biometric Server Software, click the **Start** button.

Enrolling Users on the System

Setting Truncation for Enrollment

1. From Windows® select **Start**>**Programs**>**ImproNet**>**Access**.
2. From the Main Menu, select **File**>**Preferences**.
3. Select the **Enrollment** tab.
4. Alongside the **Ascii, Biomentric, Magstripe** option, click the **Truncation** button.
5. From the **Tag Format** drop-down list, select the **26-bit Normal** option.
6. Click the button
7. Close the Preference Configuration dialog by clicking the button

Biometric Address Configuration

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.

1. From the Menu Bar, select the **Configuration** drop-down list.
2. Select **Biometric Addresses**.

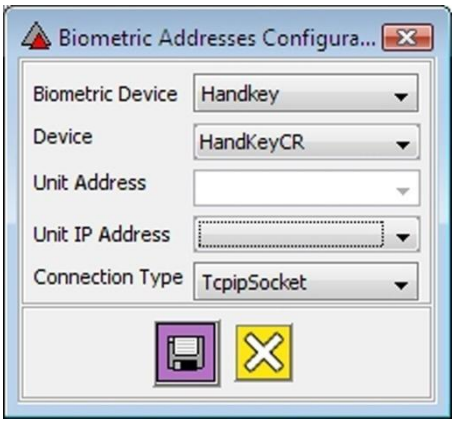


Figure 24 – Biometric Addresses Configuration Dialog

3. From the **Biometric Device** drop-down list, select the **HandKey** option.
4. From the **Device** drop-down list, select the **HandKeyCR** option.

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

Tagholder Setup

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

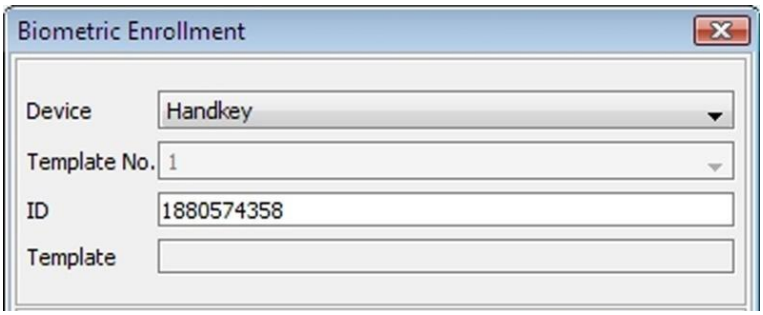


Figure 25 – Biometric Enrollment Dialog

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.

ImproX B-SHO Fingerprint Terminals Use in an ImproNet System

General

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

- IXP400i Access Control System.
- ImproNet V7.60 (and Service Pack 3) or later Installed.

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

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

Principle of Operation

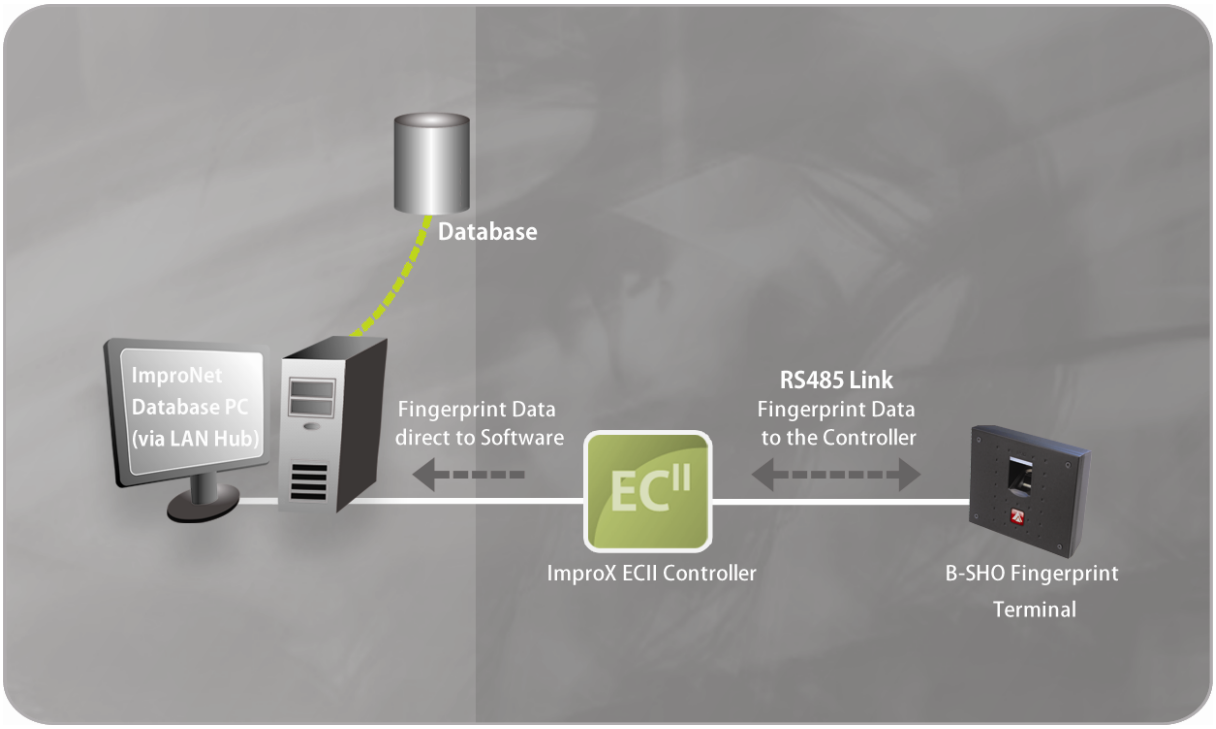


Figure 26 – Data Flow when using an ImproX B-SHO Fingerprint Terminal with ImproNet

Hardware Installation of ImproX B-SHO Fingerprint Terminals

The ImproNet System recognizes these Fingerprint Terminals in the same fashion as other ImproX Terminals. Therefore, connect these Terminals to the ImproX EC^{II} Controller's **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 Terminals per EC^{II} Controller.

In situations that require heightened security, we recommend that you connect the ImproX B-SHO Fingerprint Terminal via an associated ImproX OSCAR Door Control Unit. In all other instances multi-drop the Fingerprint Terminals direct from the Terminal Bus.

Figure 27, Figure 28 and Figure 29 show connections to the ImproX B-SHO Fingerprint Terminal, these connections remain the same for the ImproX B-SHO Keypad Fingerprint Terminal.

Use B-SHO Fingerprint Terminals with ImproX ECII Controllers, where the Controllers connect by Ethernet.

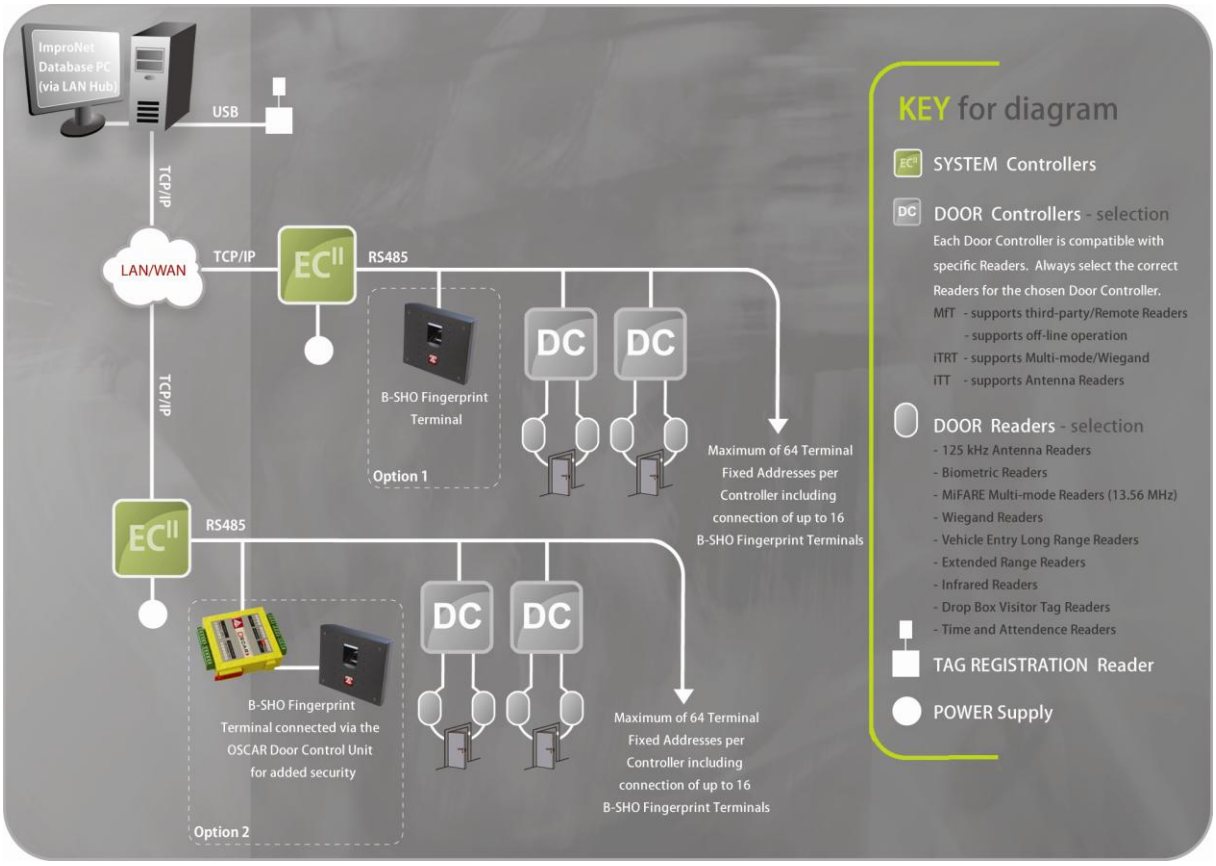


Figure 27 – Fingerprint Terminals Relationship with the Rest of the ImproX Product Range

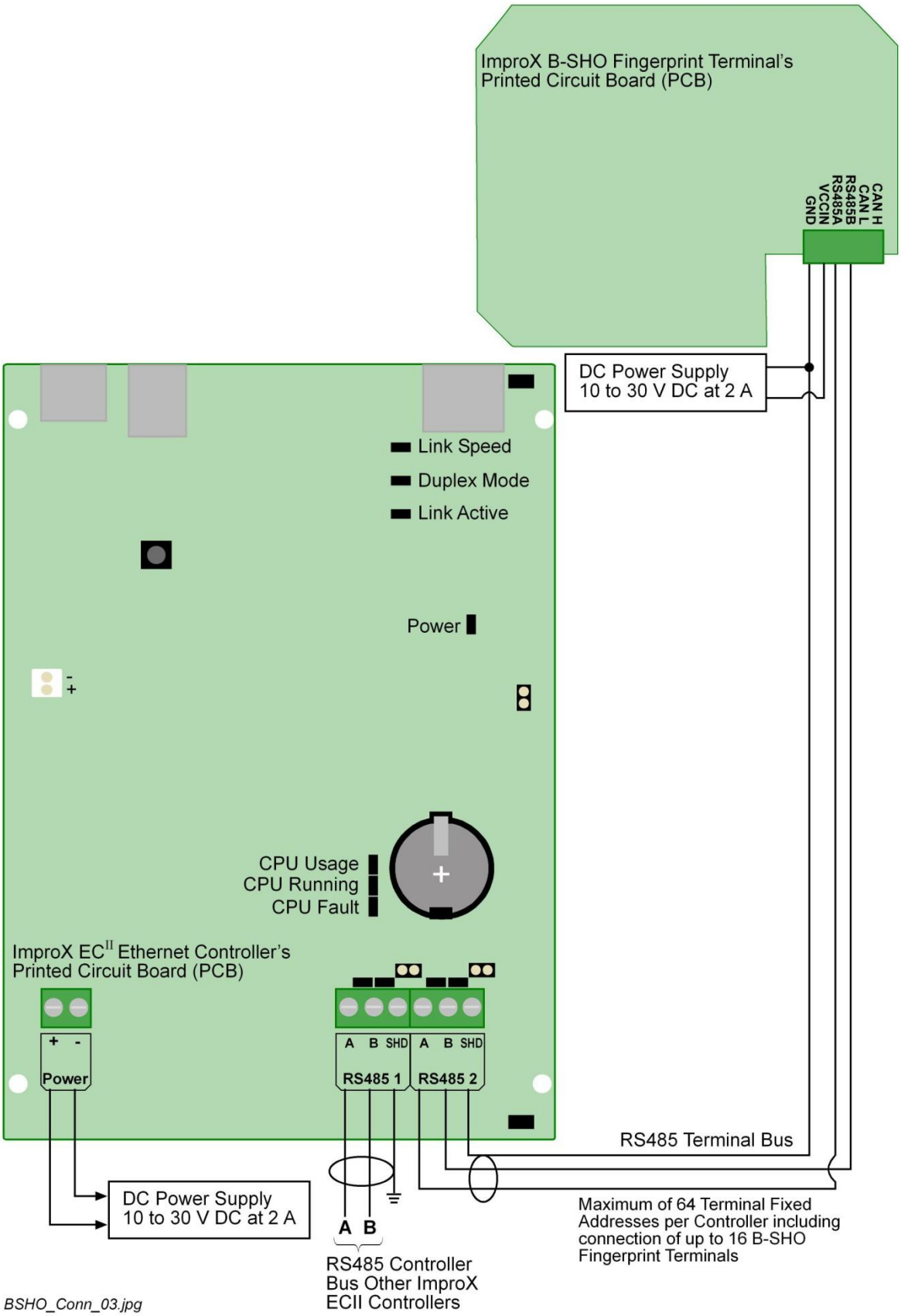


Figure 28 – ImproX B-SHO Fingerprint Terminal Connected to the ImproX EC^{II} using the Terminal Bus

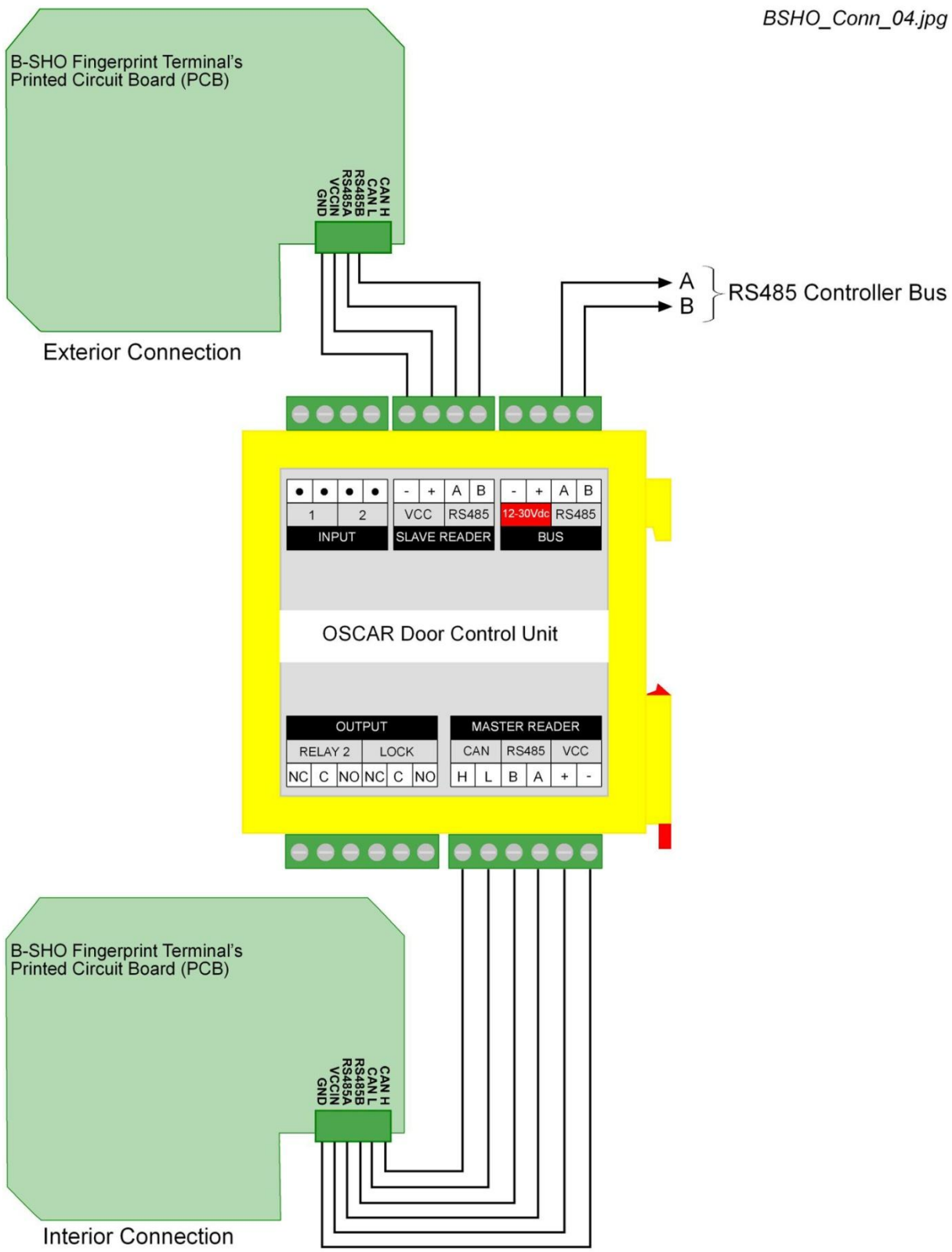


Figure 29 – ImproX B-SHO Fingerprint Terminal Connected Via the ImproX OSCAR Door Control Unit

Connecting the ImproX B-SHO USB Fingerprint Enrollment Reader

1. Plug the **ImproX B-SHO USB Fingerprint Enrollment Reader or ImproX B-SHO BioMini USB Fingerprint Enrollment Reader** into an unused USB Port on the PC.
2. Follow the on-screen prompts for installation of the Enrollment Reader.

Configuring the Biometric Device

Continue as follows for configuration into an ImproNet System:

Run Auto-ID to Detect your Fingerprint Terminals

Before you can use your 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 2 – 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 on the Access Hierarchical 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 30 – Unassigned Terminals

2. Double-click the icon to expand the Unassigned Terminals node.
3. Drag-and-drop unassigned Fingerprint Terminals 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 Fingerprint Terminal and set-up its Actions, Inputs, and Outputs. The Terminal Settings are the same as those mentioned in **Part 3 – General Configuration**. Refer to the section titled **Terminals** for more information.

Terminal Modes

Select the 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 ImproX B-SHO Terminal Modes

Enrolling Users on the System

Tagholder Setup

*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.*

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 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. From the **Tag Type** drop-down list, select **ASCII, Biometric, Magstripe**.
8. Set the Access Groups in the usual way.
9. Click on the button.
10. Click on the **Biometric Enrollment** button.

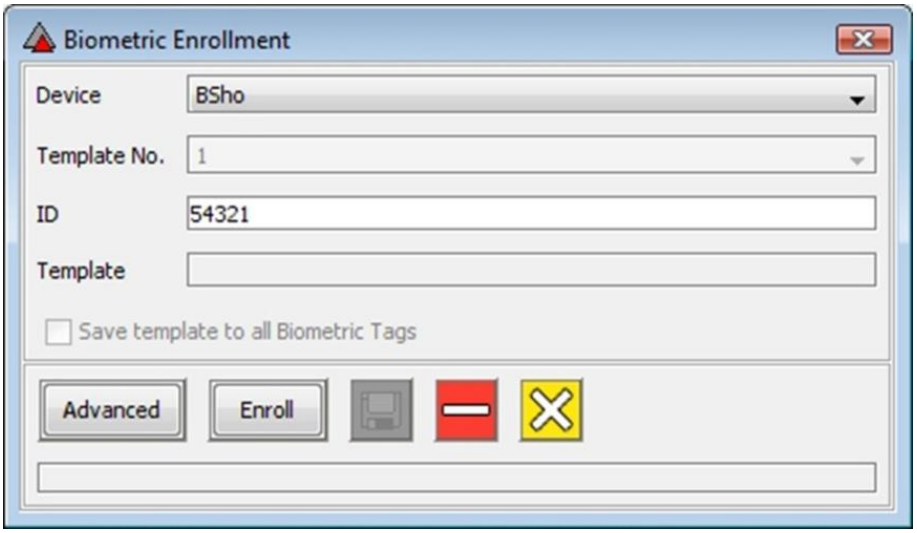


Figure 31 – Biometric Enrollment Dialog

11. 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. Click the button.

Fingerprint Placement Rules

Figure 32 shows the area of the fingerprint that contains the most information.

Finger_Placemnt_01.jpg

Figure 32 – Area of the Fingerprint Containing the most Information

When enrolling Tagholders, ensure enrollees place their fingers as shown in the green (checked) blocks below:

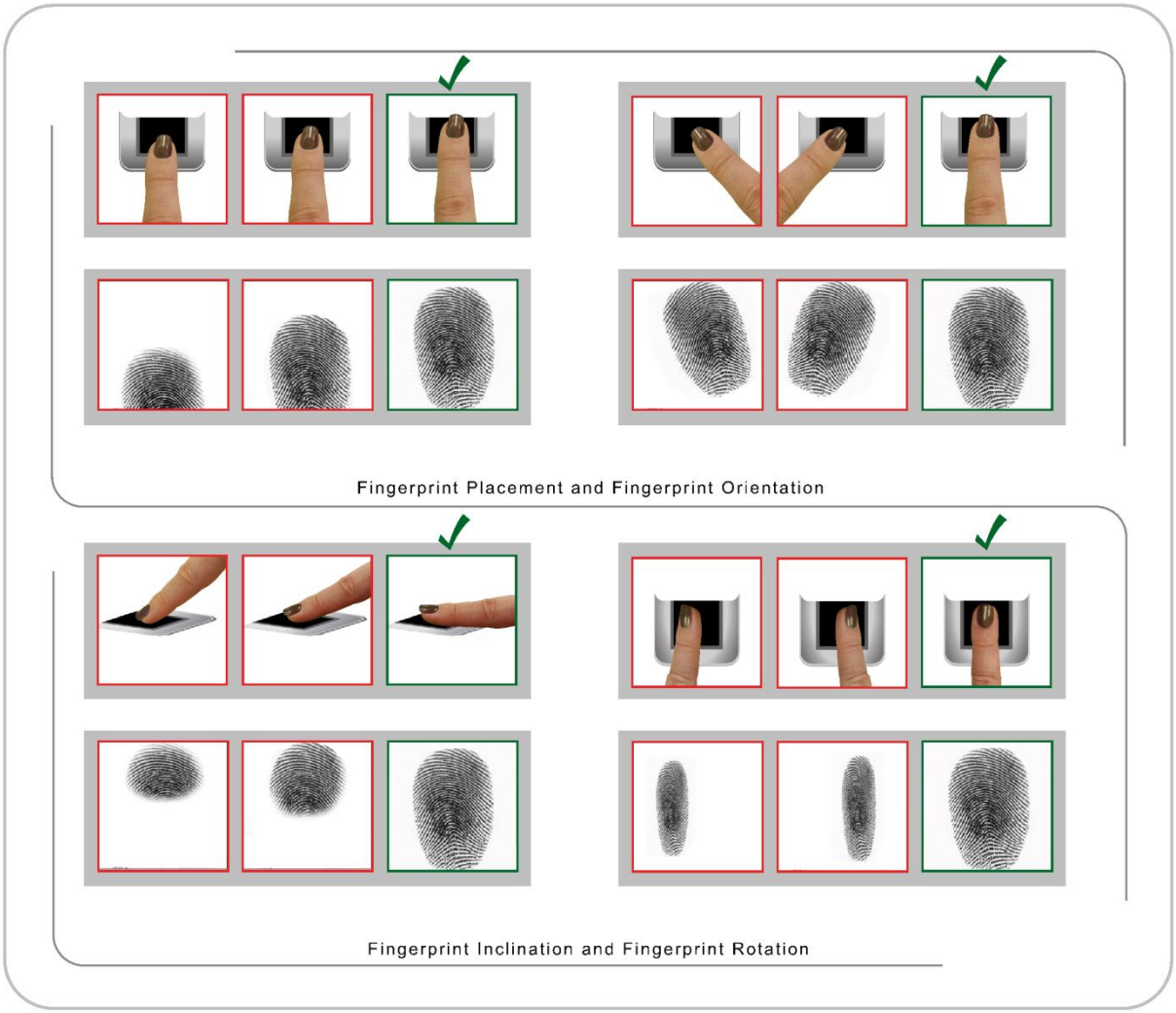


Figure 33 – Fingerprint Placement Rules

After enrollment, ensure that Tagholders use the Fingerprint Placement Rules shown in Figure 33 each time they present their finger to the ImproX B-SHO Fingerprint Terminal.

Enrollment procedure at the ImproX B-SHO USB Fingerprint 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 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. For verification, place Finger 1 on the Sensor a third time.
7. Again, remove Finger 1 from the Sensor.
8. At the Message dialog, click the **OK** button.
9. Place **Finger 2** (fingerprint down) on the Enrollment Reader's fingerprint Sensor.
10. Remove Finger 2 from the Sensor.
11. Place Finger 2 on the Sensor a second time.
12. Again, remove Finger 2 from the Sensor.
13. For verification, place Finger 2 on the Sensor a third time.
14. Again, remove Finger 2 from the Sensor.
15. 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.

16. Click the button.
17. Click the button.
18. At the Tag dialog, click the button.
19. Click the button.

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

NITGEN Fingerprint Terminals Use in an ImproNet System

General

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

Ensure that you unlock your Registration Interface (by purchasing a Biometric Unlock Code).

- IXP400i Access Control System.
- ImproNet V7.67 or later installed.

There are five steps in configuring the Fingerprint Terminals to work with ImproNet. These are:

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

Principle of Operation

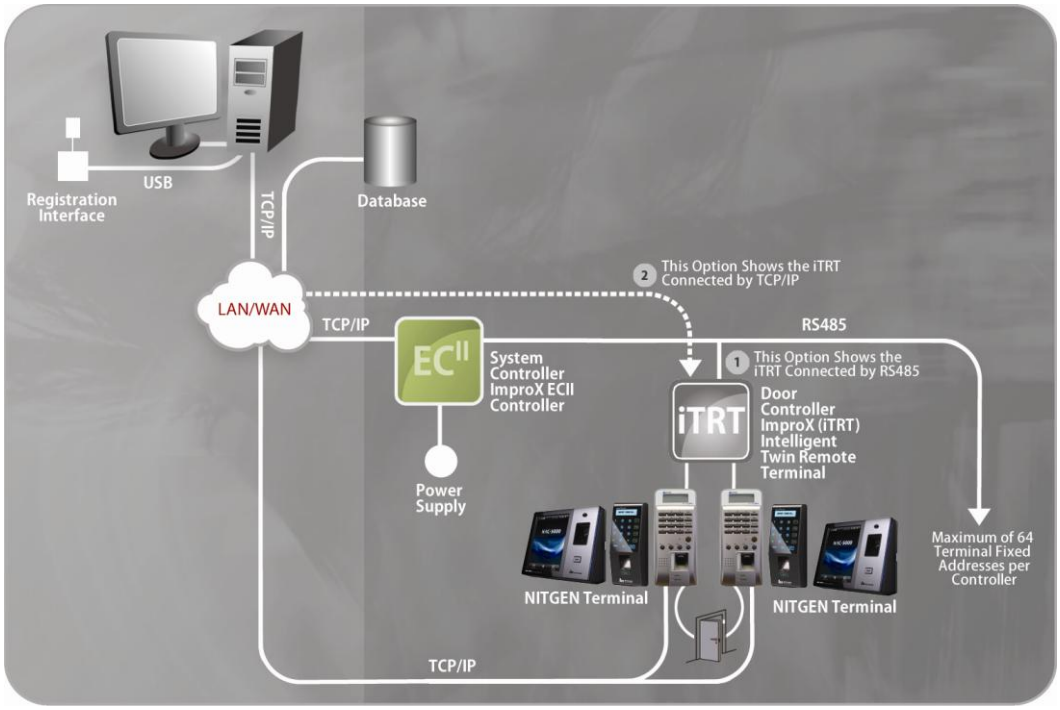


Figure 34 – Data Flow when using a NITGEN Fingerprint Terminal with ImproNet

Hardware Installation of NITGEN Fingerprint Terminals

Each NITGEN Terminal must connect to the LAN to send and receive templates from the ImproNet Database. The NITGEN Terminal must also connect to an associated ImproX Terminal (such as the ImproX TA, iTRT or the MfT) thus facilitating communication with the Controller. Please install the NITGEN Terminals as follows:

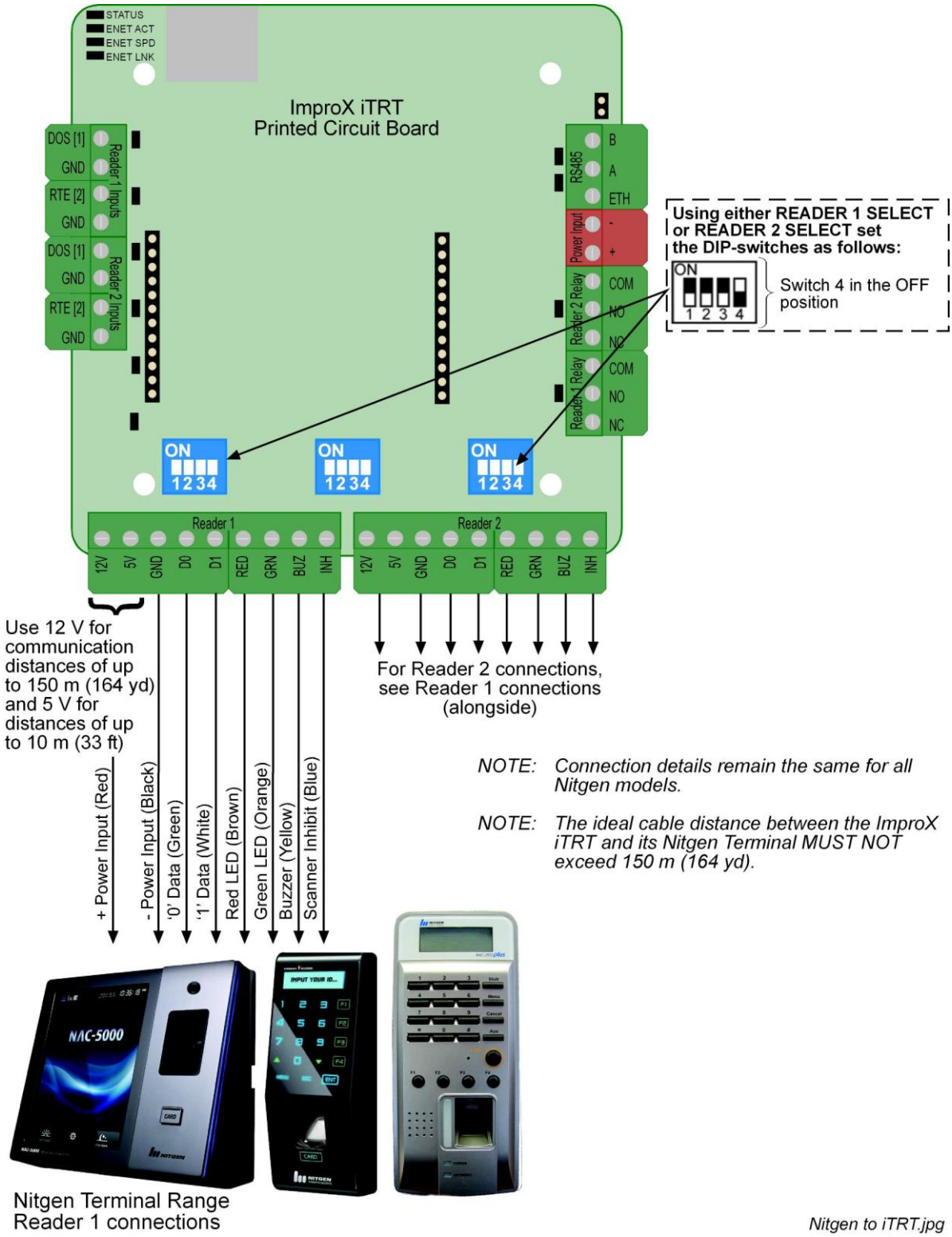
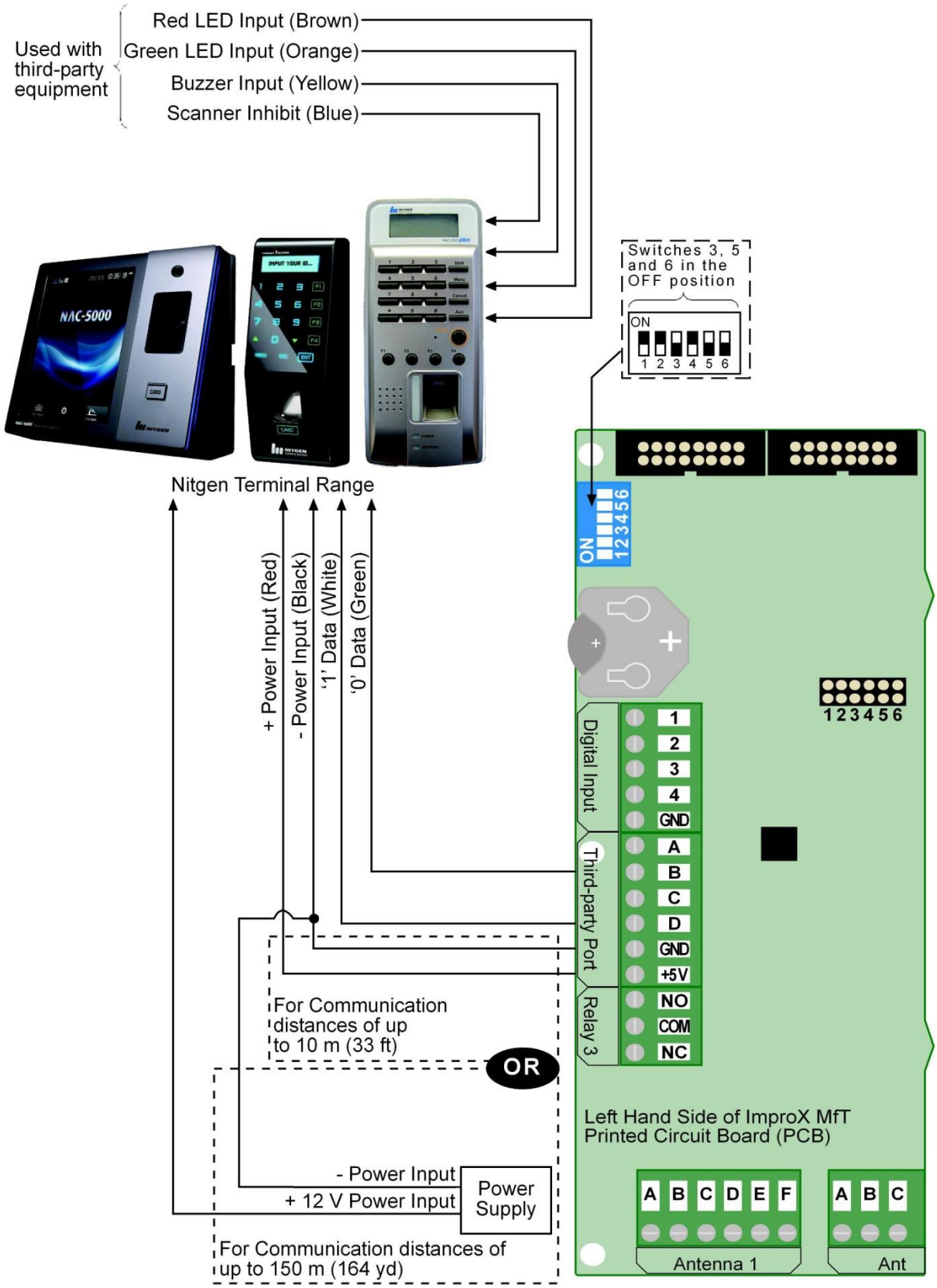


Figure 35 – NITGEN Biometric Terminal Range Connected to the ImproX iTRT Terminal



NOTE: Connection details remain the same for all Nitgen models.

NOTE: Distance Between the ImproX MfT and the Nitgen Terminal MUST NOT exceed 150 m (164 yd).

Nitgen to MfT.jpg

Figure 36 – NITGEN Biometric Terminal Range Connected to the ImproX MfT Terminal

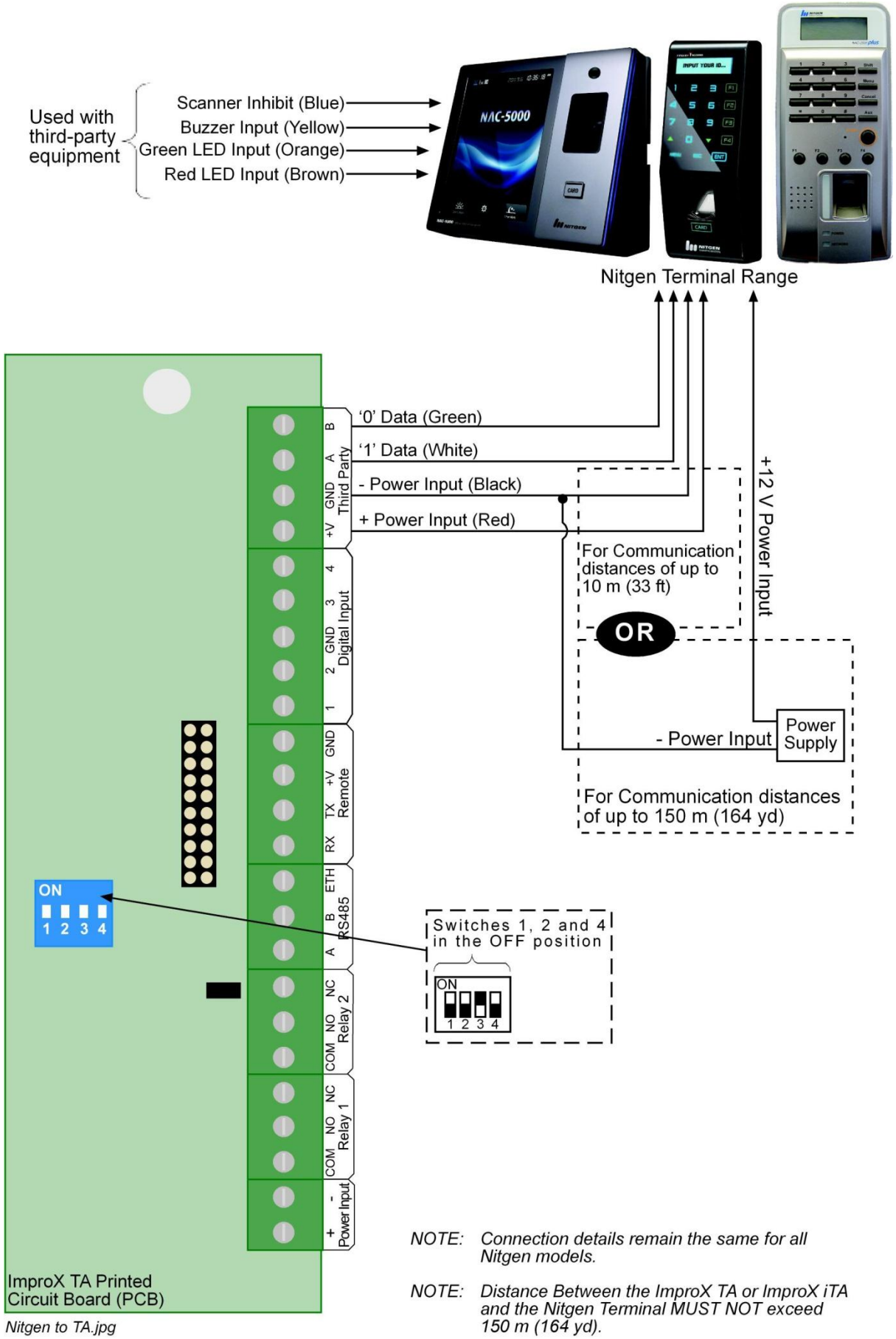


Figure 37 – NITGEN Biometric Terminal Range Connected to the ImproX TA Terminal

Connecting the NITGEN Fingerprint Enrollment Reader

1. Browse to **C:\ImproNet\driver\NITGEN\Hamster II_III**.
2. Run the **Setup.exe** file.
3. At the Welcome screen click the **Next** button.
4. At the Windows Security dialog, select the **Install This Driver Software Anyway** option.
5. At the Device Status screen, plug the NITGEN Fingerprint Enrollment Reader into an unused USB Port on the PC.
6. At the InstallShield Wizard Complete screen, select the **Device Diagnostic Tool** checkbox.
7. Click the **Finish** button.

NITGEN Fingerprint Terminal Internal Parameter Setup

*Navigate within the Fingerprint Terminals internal parameters using either the **Up** and **Down** arrow keys or the numeric keypad. Step back or exit from menu options using the **ESC** or **Cancel** buttons.*

1. On the Fingerprint Reader, press the **Menu** button.
2. Enter the **Network** selection menu by selecting menu option **5**.
3. Press the **ENT** (**Enter**) button.
4. Set the **Terminal ID** by selecting menu option **1**.
5. Press the **ENT** (**Enter**) button.
6. Enter any *UNIQUE* (across all NITGEN Terminals installed) number between **1** and **2 000**.
7. Set the **IP Address** by selecting menu option **2**.
8. Press the **ENT** (**Enter**) button.
9. Within the **TCP/IP** menu, select option **1** to **Use DHCP**.
10. Select the **ON** option.
11. Press the **ENT** (**Enter**) button.
12. Select option **5** to set the **Server IP**.
13. Press the **ENT** (**Enter**) button.
14. Enter the **IP Address** of the Host PC (running the Biometric Server Software).
15. Press the **ENT** (**Enter**) button.
16. Leave the **Port Number** (menu option 4) set at the default of **7332**.

*When changing the Port Number from the default, ensure that you change the Port Number setting in the Biometric Server Software. On the **Configuration** menu, select **Nitgen**>**Properties** to change the **Port Number**.*

Using NITGEN Terminals within the ImproNet System

Once you've connected the NITGEN Terminals and configured them internally as described in the previous paragraphs, use the Terminals within the ImproNet System. This section applies to the following supported NITGEN Fingerprint Terminals: the NITGEN Fingkey Access Terminal, the NITGEN NAC-2500 Plus Terminal and the NITGEN NAC-5000 Terminal.

Each NITGEN Terminal used in the Biometric Server requires its own Unlock. For details of the unlocking procedure refer to the section titled NITGEN Unlock Protection on page 64.

The configuration of these Terminals 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** (**SYSDBA**) and **Password** (**masterkey**).

Detecting NITGEN Terminals on the TCP/IP Bus

1. From the Devices menu, select **Nitgen**.
2. At the Message dialog, click the **OK** button.
3. On the **Configuration** menu, select **Nitgen**>**Properties**.
4. Confirm that the **Server Port** and Server **IP Address** appear as specified under the section NITGEN Fingerprint Terminal Internal Parameter Setup.

*By default the **Master ID** is set at **00000**.*

5. Enter a **Password** (from between **1** and **8** digits in length. By default this password is set at **00000**).
6. Click the **Apply** button.
7. Close the Biometric Server, by clicking the button.
8. From Windows® select **Start**>**Programs**>**ImproNet**>**Biometric Server**.
9. Enter your **Username** (**SYSDBA**) and **Password** (**masterkey**).
10. On the **Configuration** menu, select **Nitgen**>**Devices**.
11. Click the **Search** button.

*The **Search** may take some time, depending on how busy the network is. After the Search finds the NITGEN units, they appear as records in the table. The displayed units appear as follows:*

- *All newly discovered units highlight in **Green**.*
- *All units with changed IP Addresses highlight in **Orange**.*
- *All units that are in the Database but have been found to be off-line or missing highlight in **Red**.*

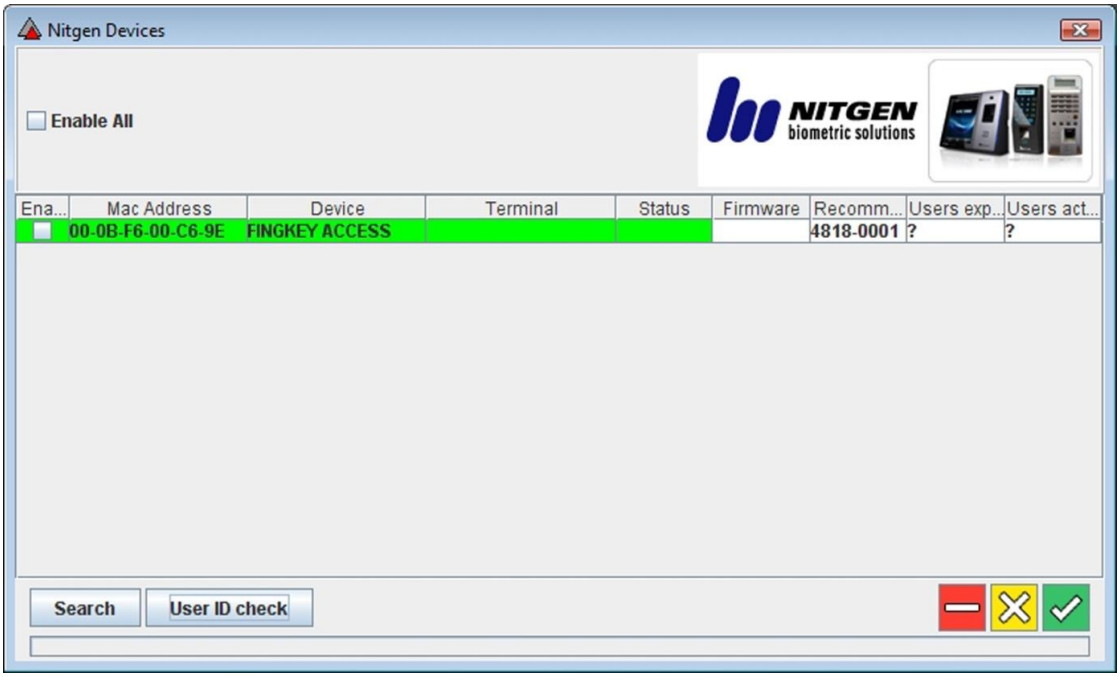


Figure 38 – NITGEN Devices Dialog

*The **Enabled** checkbox enables or disables each individual NITGEN 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 NITGEN units on the network.*
The Server will not attempt communication with a disabled NITGEN unit.

You will also notice a button in the dialog. This button allows manual deletion of NITGEN Terminals from the database. Note however, reintroduction of the NITGEN Terminal requires use of the unlock.

*Enabled NITGEN Terminals display with their status shown as OK. Clicking the **User ID Check** button displays the **Template Comparison** dialog. This dialog shows the first 50 missing User IDs per Database. You may export the full list of missing User IDs.*

12. Enable the NITGEN Fingerprint Teminals as required by selecting the associated Fingerprint Terminal's **Enabled** checkbox.
13. Click the button.
14. 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 NITGEN 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.

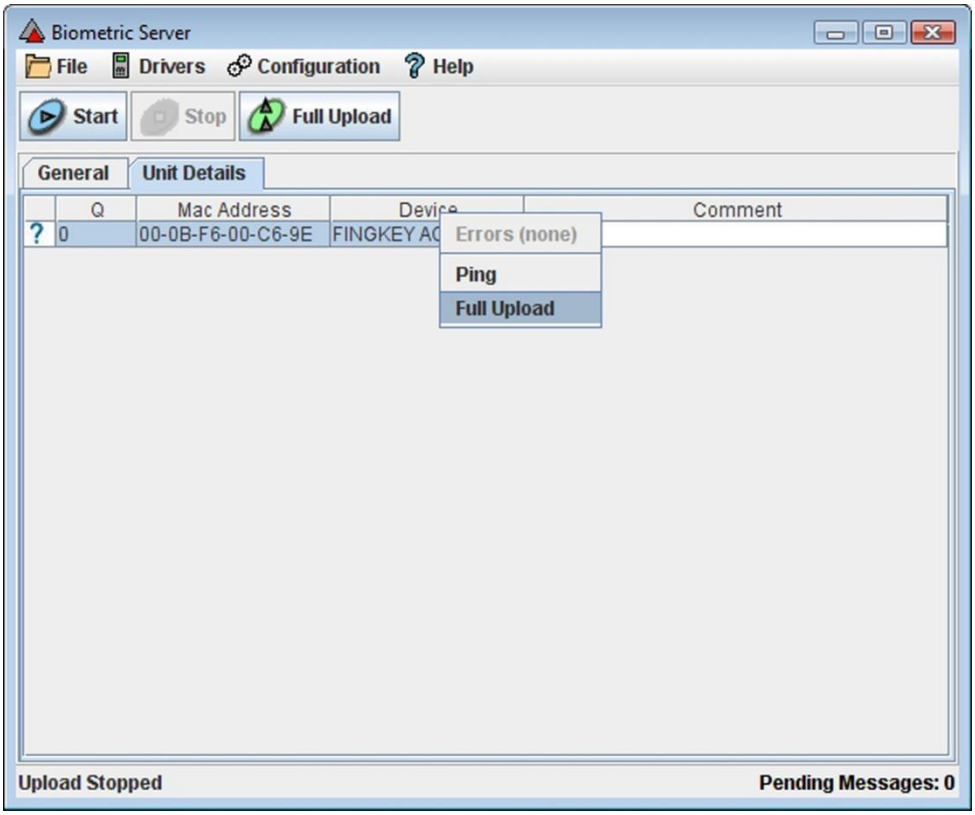


Figure 39 – Unit Details Tab

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

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

NITGEN Unlock Protection

The Unlock 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 Unlock allows intelligent distribution of templates (uploading of templates only to Terminals where the Tagholder has access).

In instances where NITGEN Terminals are purchased from Impro, the Factory unlocks the Terminal prior to shipment. In instances where the Terminal does not come from the Impro Factory, please unlock NITGEN Terminals as follows:

1. At the License Information dialog, click the **Unlock** button.
2. At the Device Unlock dialog, click the **Import** button.
3. Select the **Unlock.xml** file for import (contact Impro's Support team for further information on sourcing this file).
4. Click the **Open** button.
5. At the Message dialog, click the **OK** button.
6. At the Device Unlock dialog, click the **OK** button.

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

Enrolling Users on the System

Setting Truncation for Enrollment

1. From Windows® select **Start**>**Programs**>**ImproNet**>**Access**.
2. From the Main Menu, select **File**>**Preferences**.
3. Select the **Enrollment** tab.
4. Alongside the **Ascii, Biomentric, Magstripe** option, click the **Truncation** button.
5. From the **Tag Format** drop-down list, select the **16-bit Normal** option.
6. Click the button.
7. Close the Preference Configuration dialog by clicking the button.

Tagholder Setup

1. In the Navigator Pane, select the **Tagholder** icon.
2. Open the **Edit Tagholder** or **Add Tagholder** dialog.
3. Select **New Tag** to enter the **Tag** dialog.
4. Have the Tagholder place their Tag on the Enrollment Reader.
5. Click **Read Tag** (or enter any number between 1 and 65535 in the **Tag Code** field).
6. Set the Access Groups in the usual way.
7. Click on the button.
8. Click on the **Biometric Enrollment** button.

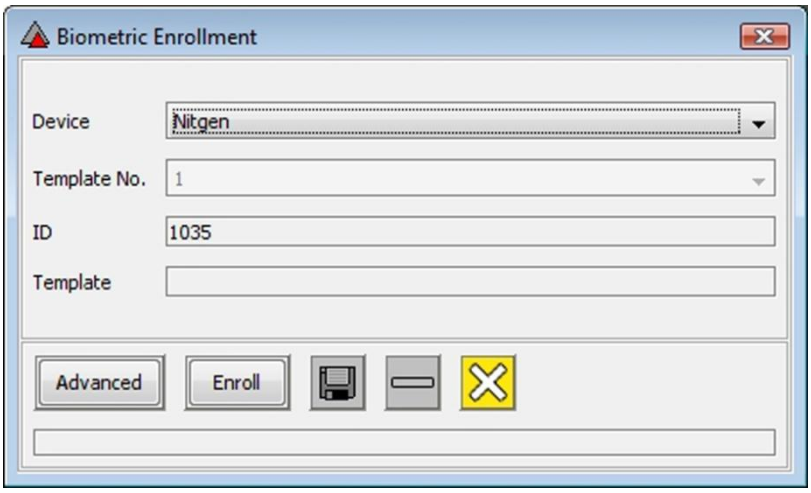


Figure 40 – Biometric Enrollment Dialog

9. 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 **Nitgen**.

*The **Template No** field will be greyed out as it does not apply to NITGEN units. Other Biometric Devices allow you to enroll multiple templates per user. NITGEN 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.*

10. Click on the **Advanced** button.

Advanced Settings

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

- **Enroll Image Quality**—this is the quality setting that will be applied during the enrollment of the fingerprint. By default the Enrollment Image Quality is set to **50**. Reducing this figure will result in a poorer quality fingerprint image. Increasing this figure ensures a higher quality fingerprint image.
- **Verify Image Quality**—quality level of the fingerprint image for verification. The value range is from 0 to 100. The default value is **30**.
- **Security Level**—select from one of the following options: Lowest, Lower, Low, Below Normal, Normal, Above Normal, High, Higher, Highest. By default the Security Level is set at **Normal**. If the level is set to a low setting, the False Acceptance Rate (FAR) increases and False Rejection Rate (FRR) decreases. If set to a high setting, False Acceptance Rate (FAR) decreases and False Rejection Rate (FRR) increases.

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

Fingerprint Placement Rules

Figure 17 shows the area of the fingerprint that contains the most information. Therefore, when enrolling Tagholders, ensure they place their fingers as shown in Figure 18.

Figure 41 – Area of the Fingerprint Containing the most Information

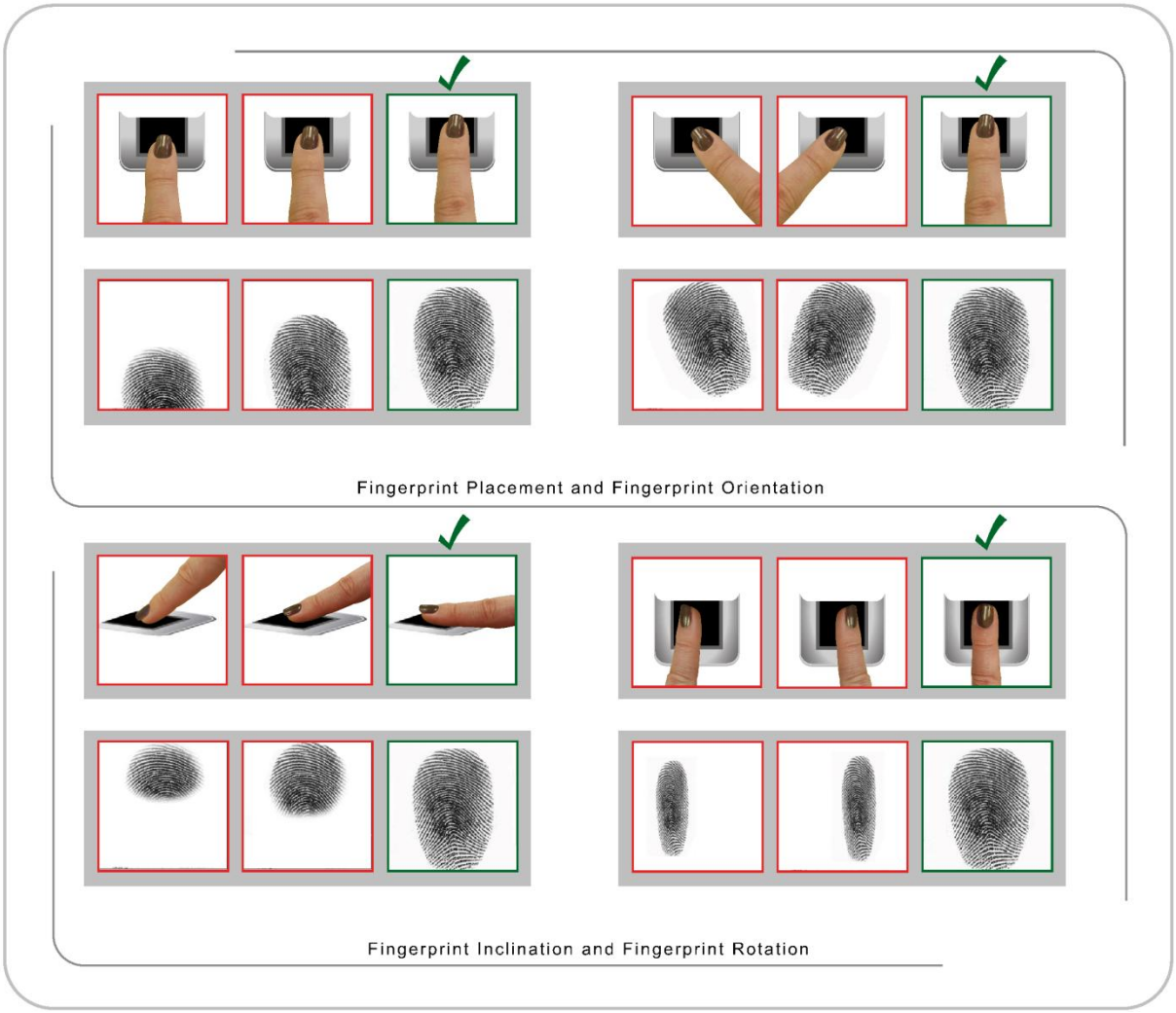


Figure 42 – Fingerprint Placement Rules (Generic Enrollment Reader, Fingerprint Sensor Shown)

Enrollment procedure at the NITGEN Fingkey Hamster II™

Enrollment can take place using either a single finger or multiple fingers per user. Regardless of the number of fingers enrolled, configure the Biometric Server to upload either one or two templates per user. By default two templates upload.

1. At the NITGEN Biometric Solutions dialog, click the **Next** button.
2. Select **Finger 1** for use during enrollment, by clicking on the corresponding dot above the fingertip.
3. Place the corresponding Finger (fingerprint down) on the NITGEN Fingkey Hamster II™ fingerprint Sensor.
4. Remove the Finger from the Sensor.
5. Place the Finger on the Sensor a second time.
6. Again, remove the Finger from the Sensor.
7. Select **Finger 2** for use during enrollment, by clicking on the corresponding dot above the fingertip.
8. Place the corresponding Finger (fingerprint down) on the NITGEN Fingkey Hamster II™ fingerprint Sensor.
9. Remove the Finger from the Sensor.
10. Place the Finger on the Sensor a second time.
11. Again, remove the Finger from the Sensor.
12. Click the **Next** button to end the enrollment process.
13. Click the **Finish** button.

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

14. Click the button.
15. 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 NITGEN Terminals.

USER NOTES