PART 8 – INTEGRATION MODULES

Contents

PART 8 – INTEGRATION MODULES 1

CONTENTS 3

INTRODUCTION 6

MORPHO (SAGEM) READER USE IN AN IXP220 SYSTEM 8

General 8

Principle of Operation 8

Hardware Installation 9

Installation and Setup of the MSO300 Enrollment Reader and Verification Dongle 17

Morpho MA100, MA120, MA500 or J-Series Internal Parameter Setup..... 20

Morpho MA200 or MA300 Internal Parameter Setup 26

Configuration of Morpho Readers into the IXP220 System 29

Configuration of MIFARE® Encoders into the IXP220 System 36

IMPROX B-SHO FINGERPRINT TERMINALS USE IN AN IXP220 SYSTEM.....41

General 41

Principle of Operation 41

Hardware Installation of ImproX B-SHO Fingerprint Terminals 42

Configuring the Biometric Device..... 45

Troubleshooting 56

NITGEN FINGERPRINT TERMINALS USE IN AN IXP220 SYSTEM 58

General 58

Principle of Operation 58

Hardware Installation of NITGEN Fingerprint Terminals..... 59

NITGEN Fingerprint Terminal Internal Parameter Setup 67

Using NITGEN Terminals within the IXP220 System..... 67

Introduction

This section describes integration of the following third-party systems with the IXP220 Software:

- Various **Morpho** Fingerprint and Registration Readers, integrated via the Biometric Server Software.
- ImproX **B-SHO** Fingerprint Terminals, integrated direct to the IXP220 Base Application.
- **NITGEN** Fingerprint Terminals, integrated via the Biometric Server Software.

The introduction of biometric access control greatly increases the access control capabilities of IXP220 Systems where you need extra security measures. Some Biometric Readers are not supported by the Biometric Server Software. Table 1 gives Reader support information.

Biometric Reader	**Biometric Server Software Support**	**Number of Users**	**Firmware Supported**	**Approved Terminals**	**Enrollment Support at Reader**
MorphoAccess™ MA100	**YES**	500	2.13.4	iTRT, MfT, TA and IXP220 Controller	No
MorphoAccess™ MA120	**YES**	500	2.13.4	iTRT, MfT, TA and IXP220 Controller	No
MorphoAccess™ J-Bio	**YES**	500 standard, upgradeable to 3 000	2.13.4	iTRT, MfT, TA and IXP220 Controller	No
MorphoAccess™ J-Dual	**YES**	500 standard, upgradeable to 3 000	2.13.4	iTRT, MfT, TA and IXP220 Controller	No
MA200 Fingerprint Reader	**YES**	800	5.53	iTRT, MfT, TA and IXP220 Controller	No
MA220 Fingerprint Reader	**YES**	800	5.53	iTRT, MfT, TA and IXP220 Controller	No
MA300 Fingerprint Reader	**YES**	48 000	5.53	iTRT, MfT, TA and IXP220 Controller	No
MA500 Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT, TA and IXP220 Controller	No
MA500+ Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT, TA and IXP220 Controller	No
MA520 Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT, TA and IXP220 Controller	No
MA520+ Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT, TA and IXP220 Controller	No
OMA520 Fingerprint Reader	**YES**	3 000 standard, upgradeable to 50 000	2.13.4	iTRT, MfT, TA and IXP220 Controller	No
MorphoSmart™ MSO300 Registration Reader	**YES**	NA	TBA	TBA	Yes

Biometric Reader	Biometric Server Software Support	Number of Users	Firmware Supported	Approved Terminals	Enrollment Support at Reader
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
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

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 the IXP220 Software. The Module also allows for the direct enrollment (registration) of Tagholders and related biometric data at those Biometric Readers from within the IXP220 Software.

Morpho (Sagem) Reader Use in an IXP220 System

General

This section guides you step by step through the process of setting up Morpho Biometric Readers to work with the IXP220 System. The requirements for the integration are as follows:

- IXP220 Access Control System
- IXP220 System Software Installed
- Latest Morpho Integration Patch

There are five steps in configuring the Biometric Readers in the IXP220 System. 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.

*Ensure that you unlock your Registration Interface (**Impro-Touch License**) and source your **Unlock Token** and **Verification Dongle** before using Morpho equipment with the IXP220 Software. The Impro-Touch License allows for a maximum of 1 seat.*

Principle of Operation

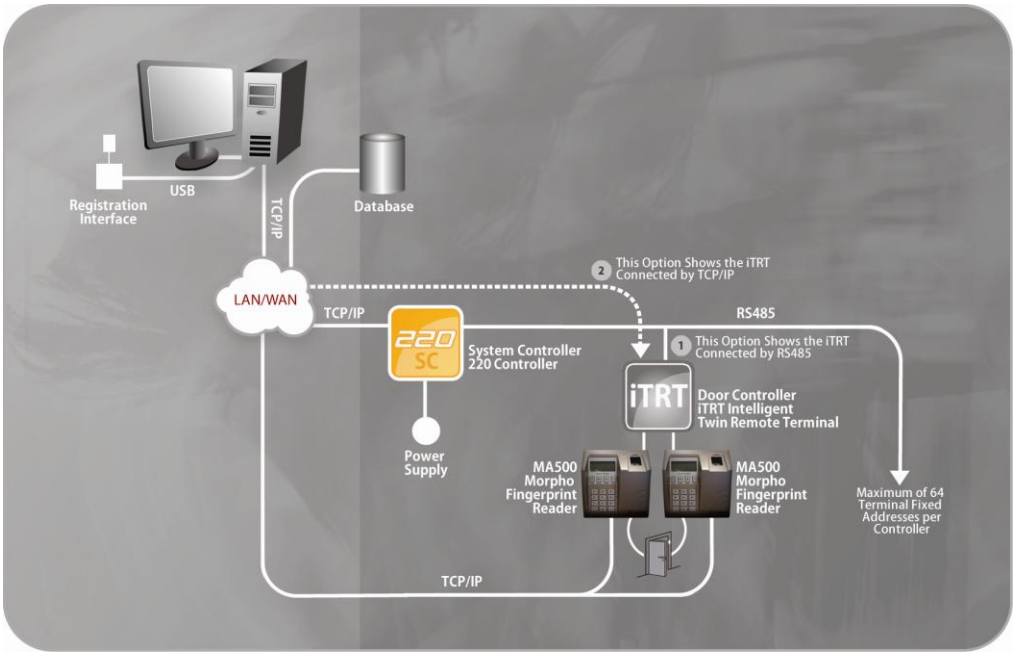


Figure 1 – Using Morpho Fingerprint Readers within an IXP220 System

Hardware Installation

Each Morpho Reader must connect to the LAN to send and receive templates from the IXP220 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. 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 IXP220 Controller

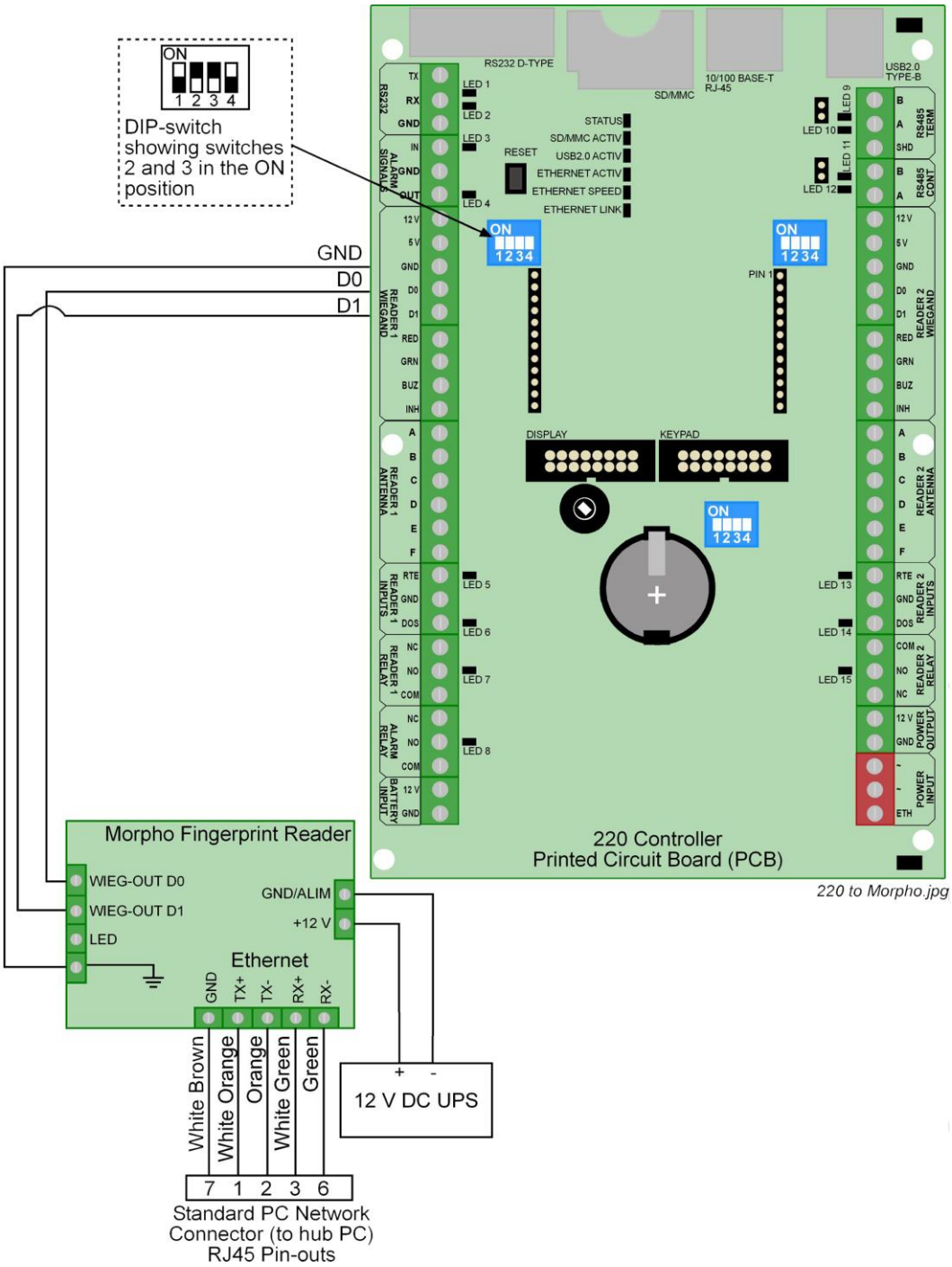
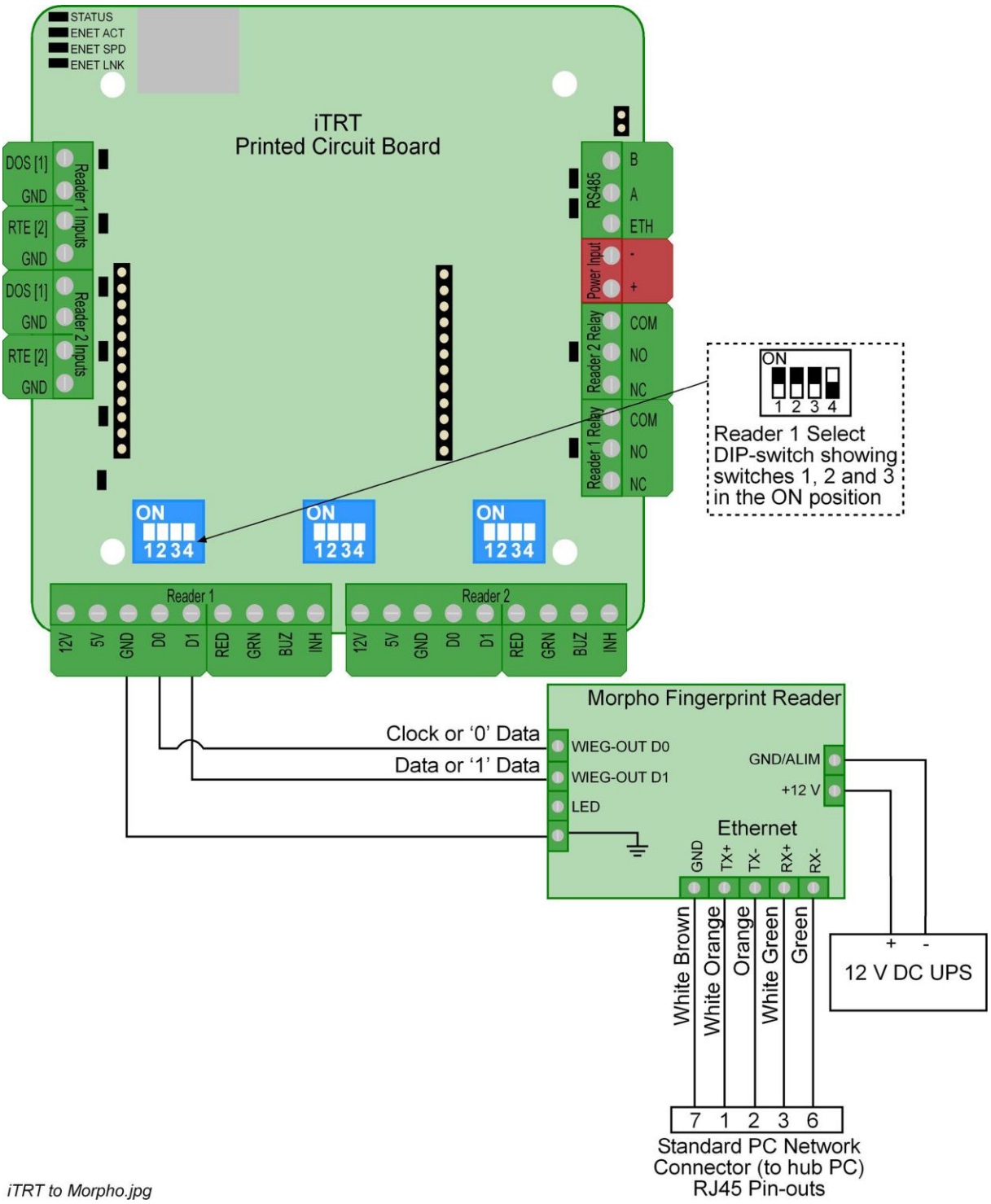


Figure 2 – Morpho Reader (MA100, MA120, MA200, MA300, MA500 or MA520) Connected to the IXP220 Controller and LAN

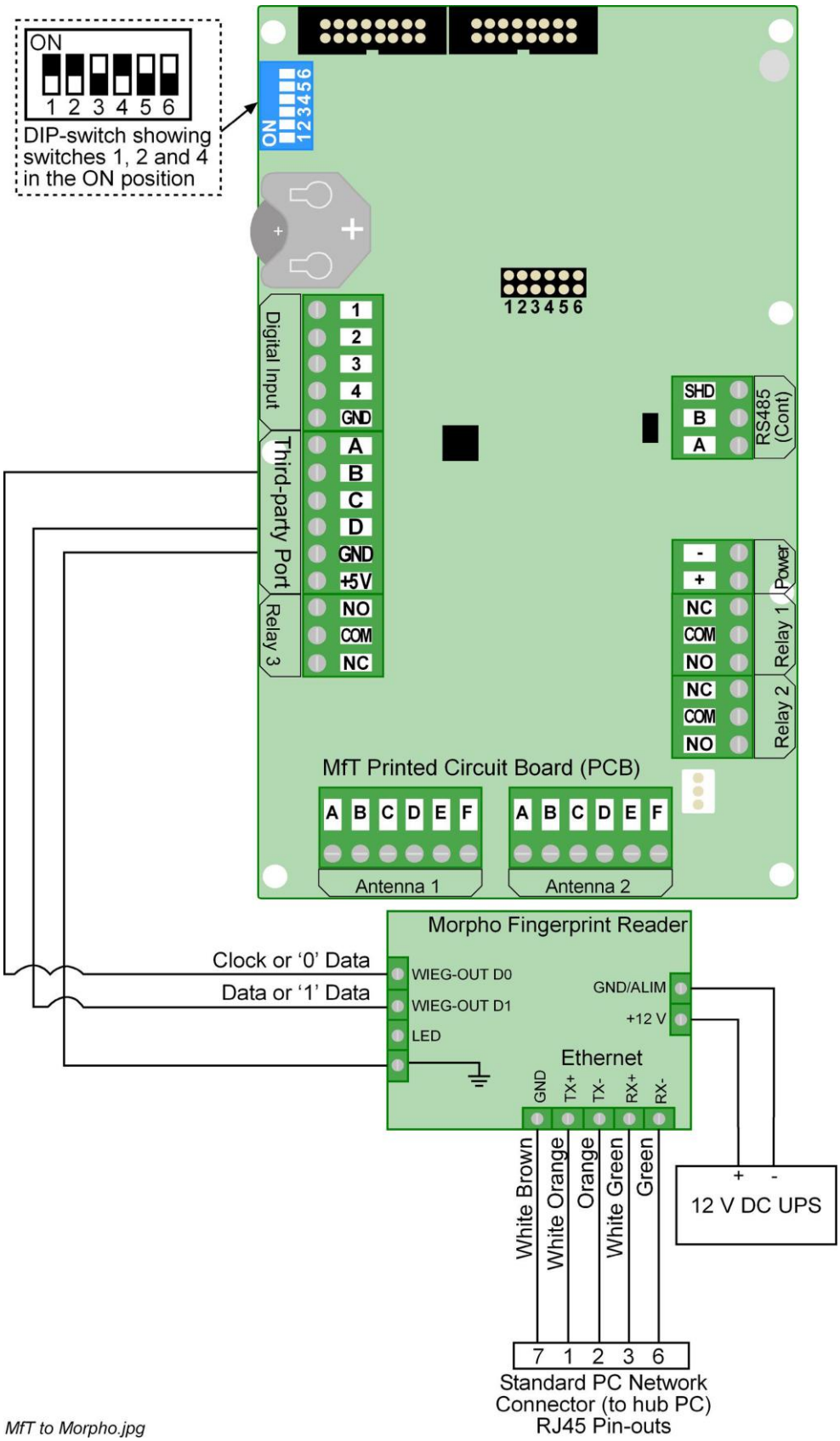
Connection to the MA100, MA120, MA200, MA300, MA500 or MA520 to the ImproX iTRT



iTRT to Morpho.jpg

Figure 3 – 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 ImproX MfT



MfT to Morpho.jpg

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

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

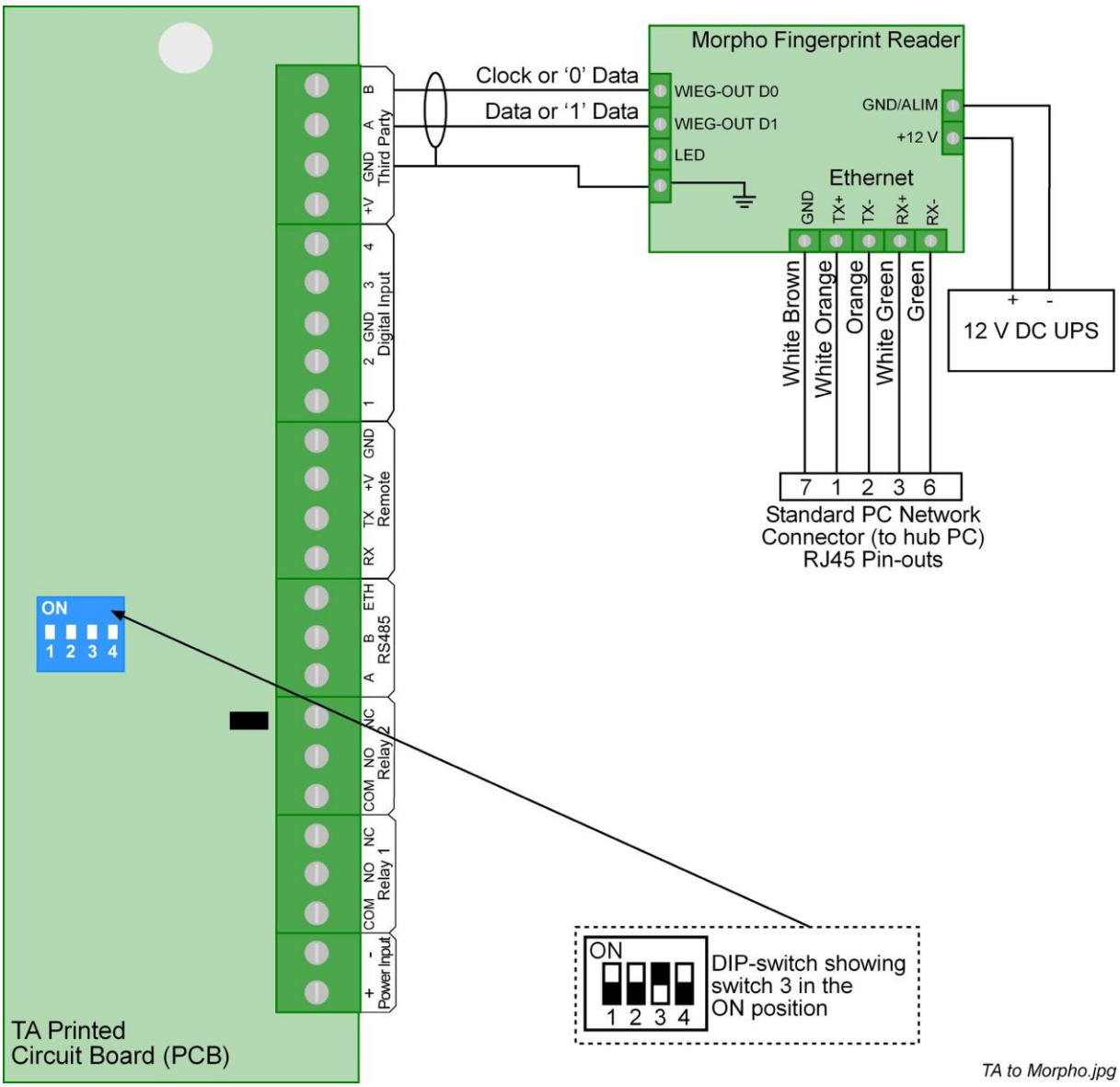


Figure 5 – Morpho Reader (MA100, MA120, MA200, MA300, MA500 or MA520) Connected to the ImproX TA and LAN

Connection to the MorphoAccess™ J-Bio or J-Dual to the IXP220 Controller

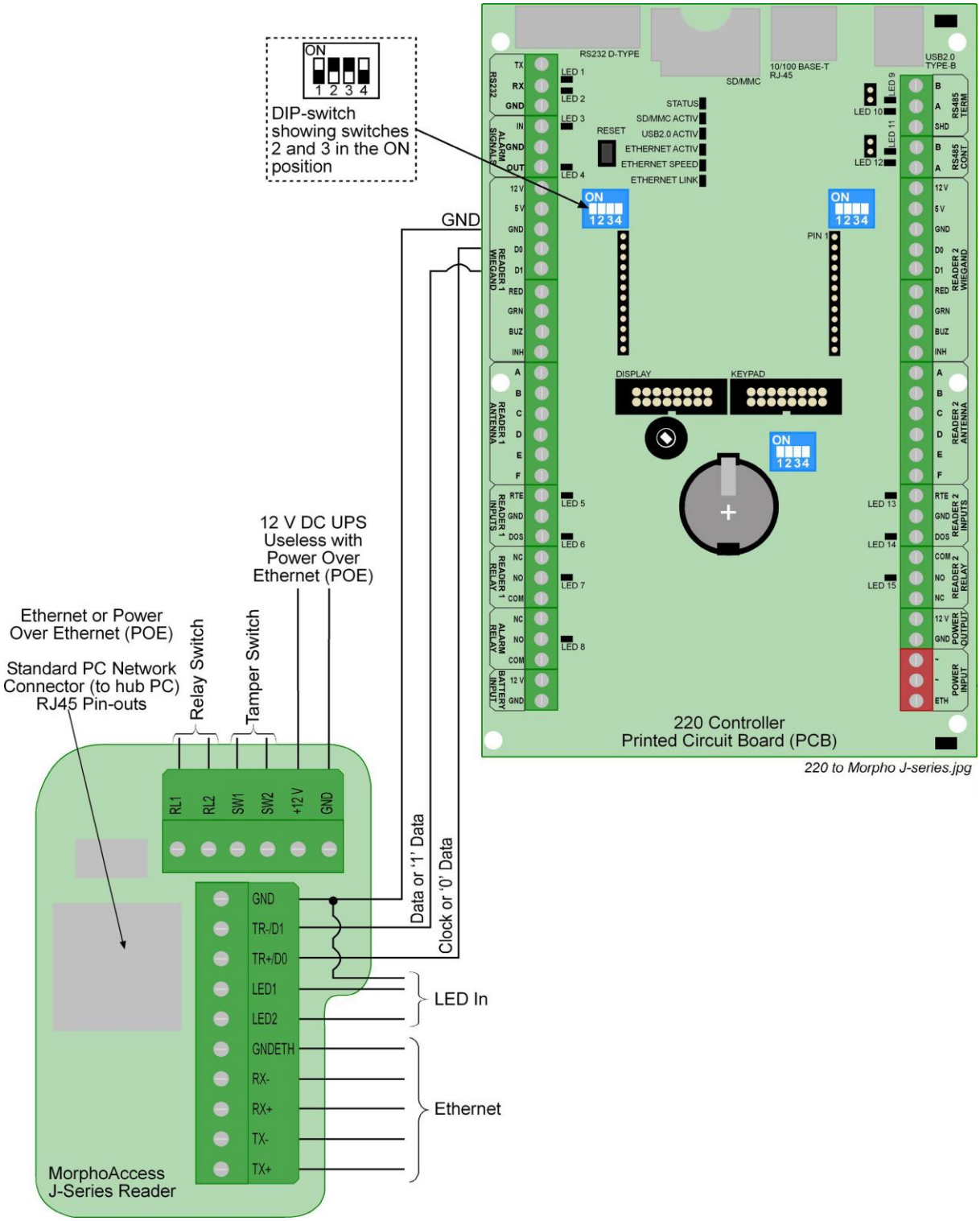


Figure 6 – MorphoAccess™ J-Bio or J-Dual Connected to the IXP220 Controller and LAN

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

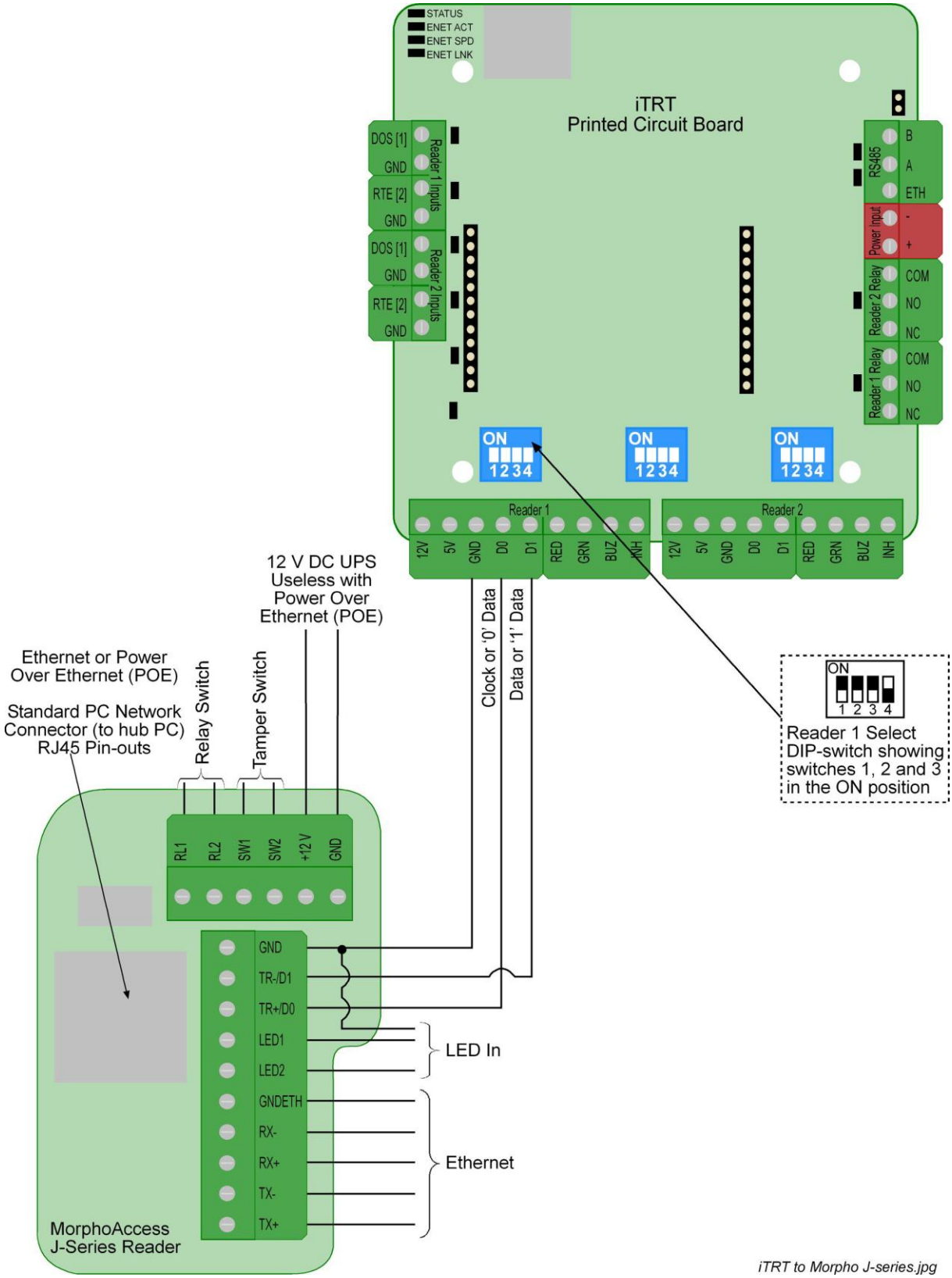


Figure 7 – MorphoAccess™ J-Bio or J-Dual Connected to the ImproX iTRT and LAN

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

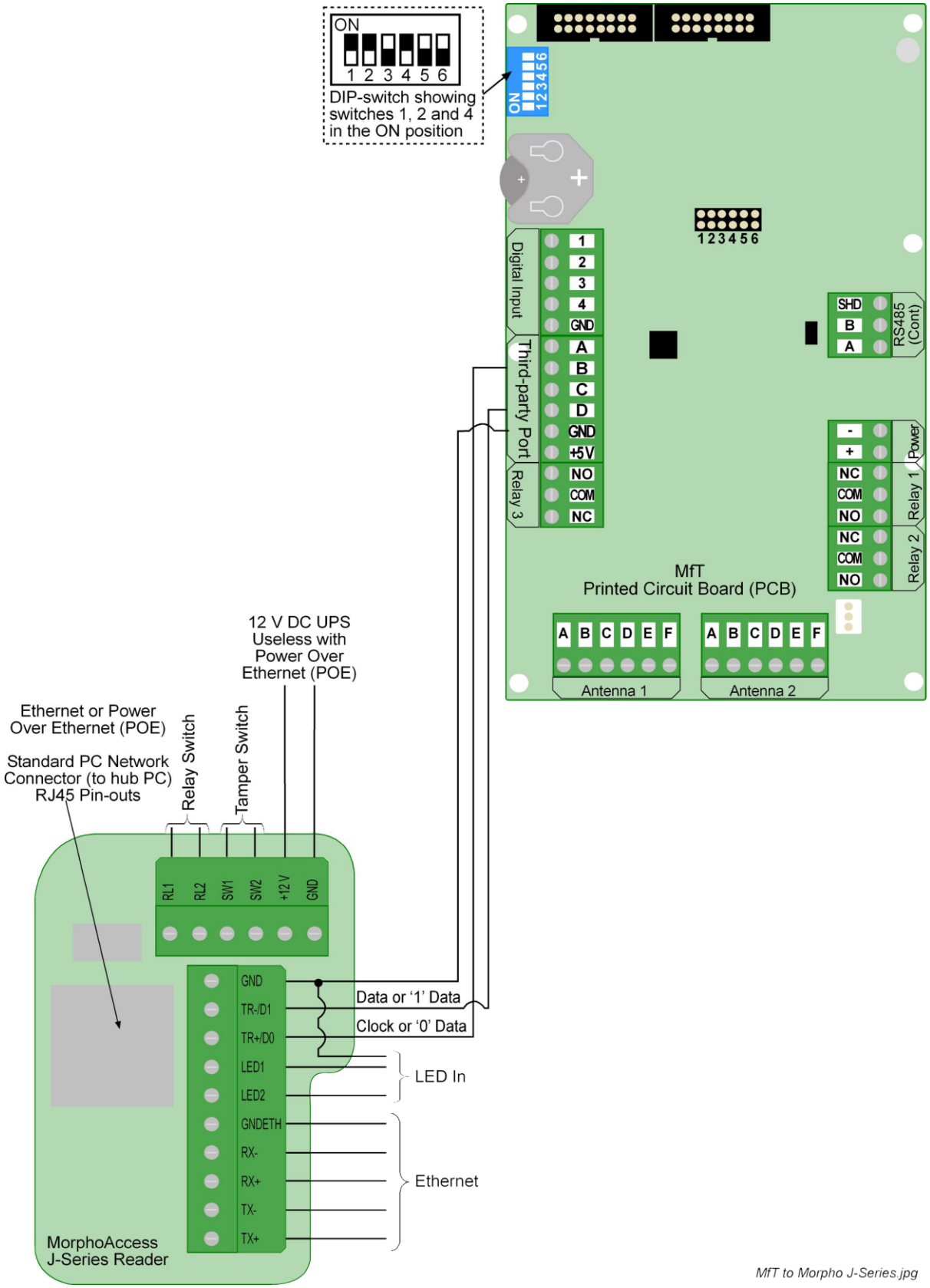
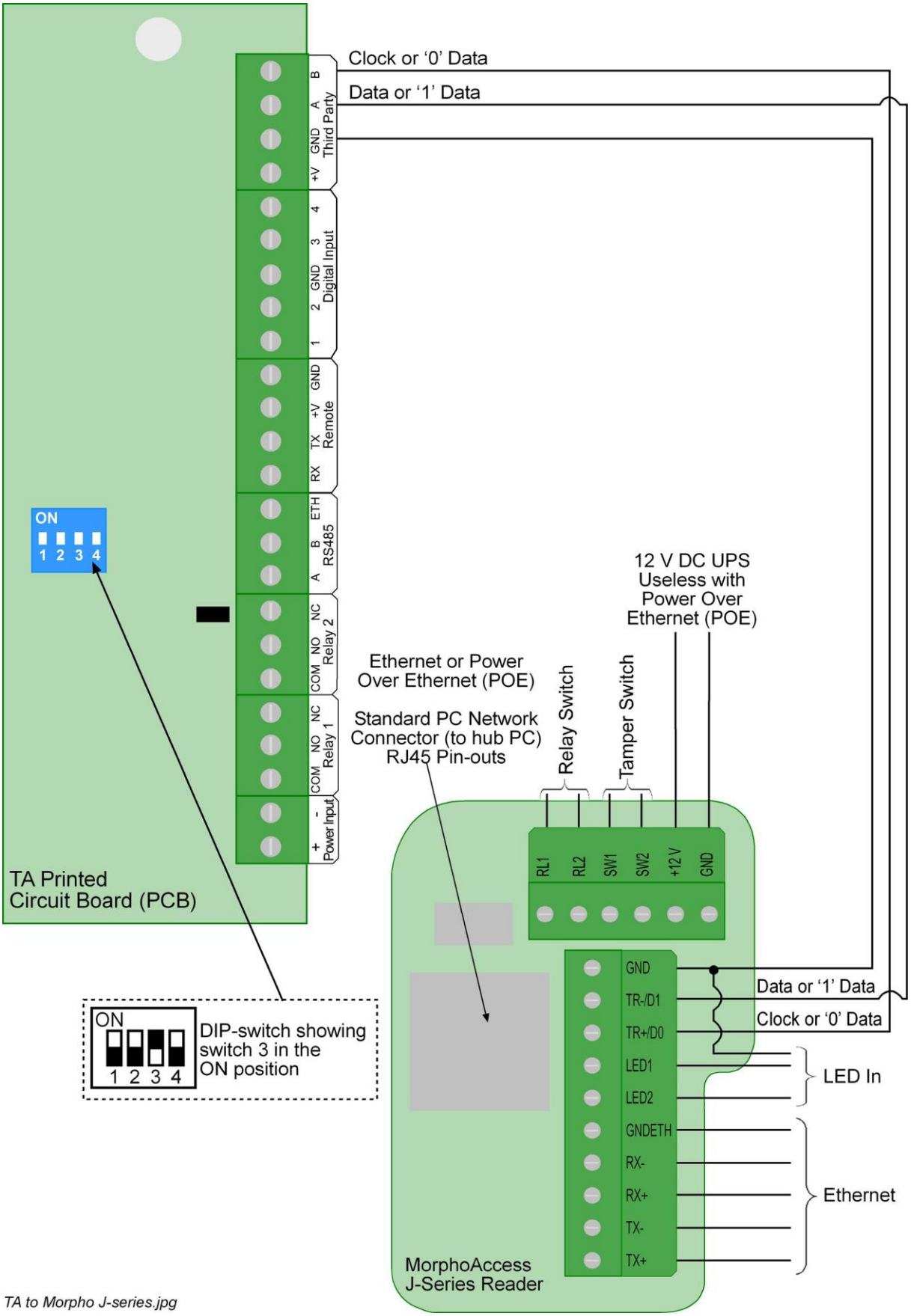


Figure 8 – MorphoAccess™ J-Bio or J-Dual Connected to the ImproX MfT and LAN

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



TA to Morpho J-series.jpg

Figure 9 – 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 (Impro-Touch License) before proceeding further. This license allows for a maximum of 1 seat.

.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 and reboot the PC.

1. If running a **32-bit** operating system, continue as follows:
   - Browse to **C:\IXP220\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:\IXP220\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 and reboot the PC.

SafeNet Dongle

1. Browse to **C:\IXP220\driver\SafeNetDongle**.
2. Double-click the **SentinelProtectionInstaller.7.4.0.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:\IXP220driver\Morpho Dongle\x86.**
2. Alternatively, if running a **64-bit** operating system, browse to **C:\IXP220\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 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:\IXP220\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:\IXP220\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. In the Performance options dialog, select the **Data Execution Prevention** tab.
6. Select the **Turn On DEP for all Programs and Services Except Those I Select** radio button.
7. Click the **Add...** button.
8. Navigate to the installation directory at **C:\Program Files\Sagem Securite\Licence Protection**.
9. Double-click on the following executable files:
   - **SagemSecurite_Licence_Protection.exe**
   - **SagemSecurite_Licence_Manager.exe**
10. Click the **OK** button.
11. At the System Properties dialog, click the **OK** button.
12. Click the button.

Morpho MSO300 Biometric Configuration

1. In Windows®, click **Start**>**All Programs**>**IXP220**>**IXP220**.
2. Select the Page Tab.
3. Open an existing Tagholder record for editing.
4. In the Tagholder dialog, select the **Tag** Tab.
5. Click one of the assigned Tag buttons (that is **Tag 1**, **Tag 2**, **Tag 3** *or* **Tag 4**).
6. From the **Configuration Level** group, select the **Advanced Configuration** radio button.

Configure the Biometric Reader

1. From the **Miscellaneous** group, select the **Configure Biometric Reader** button.

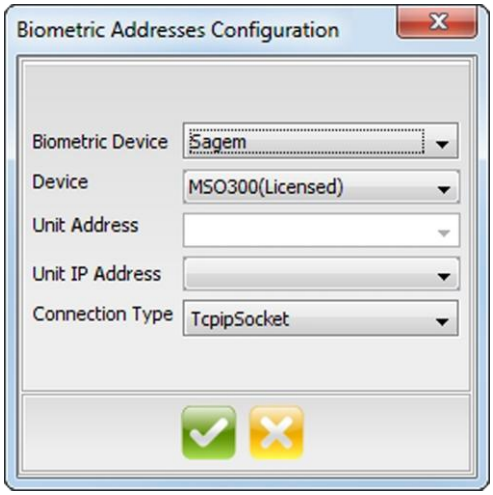


Figure 10 – Biometric Addresses Configuration Dialog

2. In the **Biometric Address Configuration** dialog, 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 the IXP220 Software, and will allow you to set up the enrollment units for each biometric device.
3. From the **Device** drop-down list, select the MSO300 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.*

4. From the **Connection Type** drop-down list, make your selection.
5. Click on the button.
6. Click on the button.
7. Click the button.
8. Click the button.

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**, acceptable Flash Disk sizes include **128 MB**, **256 MB** or **512 MB** (maximum usable size):

1. Format the Flash Disk in **FAT16**.
2. Assign the Flash Disk a name of no more than **12 characters**.
3. Browse to **C:\IXP220\Driver\Tools\Sagem\USB Network Tools**.
4. Double-click on the **USBNetworkTool.exe** file.

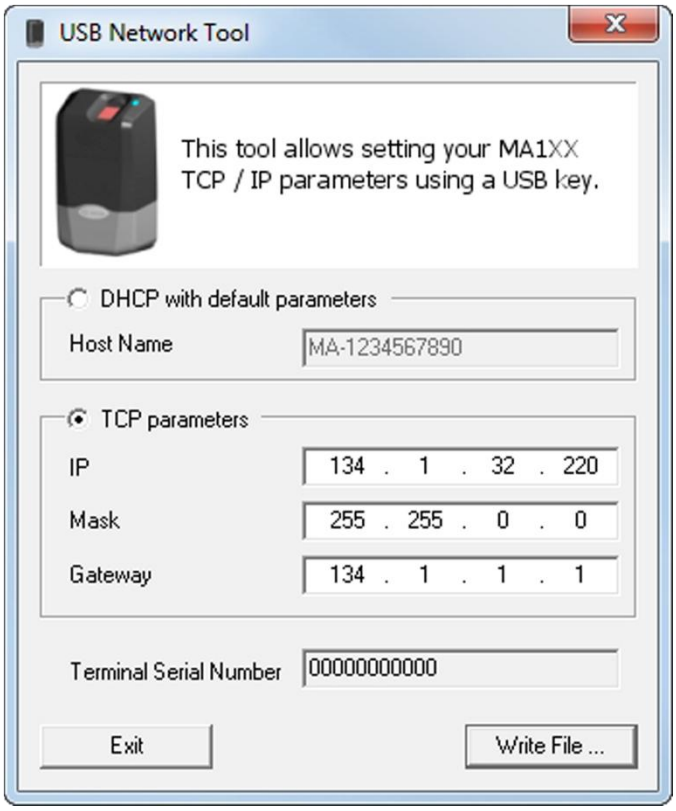


Figure 11 – USB Network Tool Dialog

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 download is 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, MA500 or J-Series

1. Browse to **C:\IXP220\Driver\Tools\Sagem\Configuration Tool**.
2. Double-click on the **ConfigurationTool.exe** file.

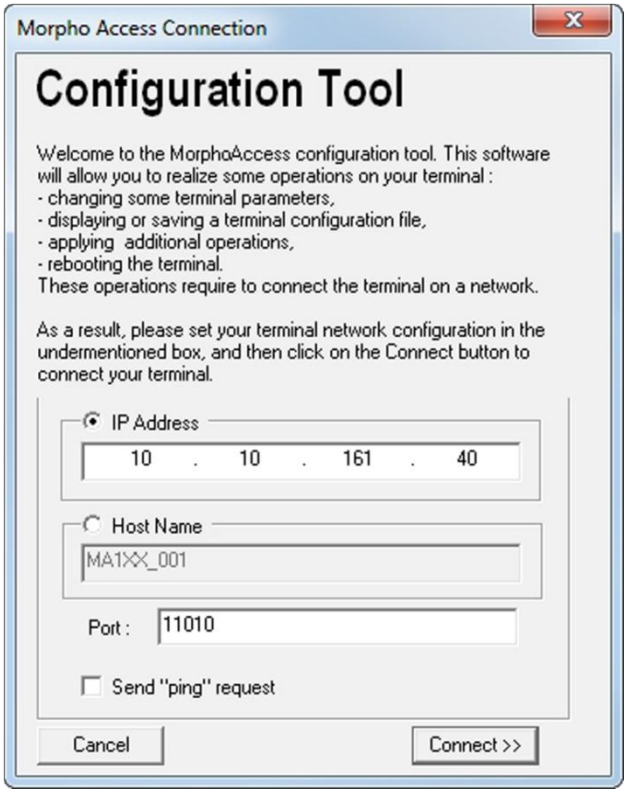


Figure 12 – Configuration Tool Dialog

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 21.
4. Click the **Connect >>** button.

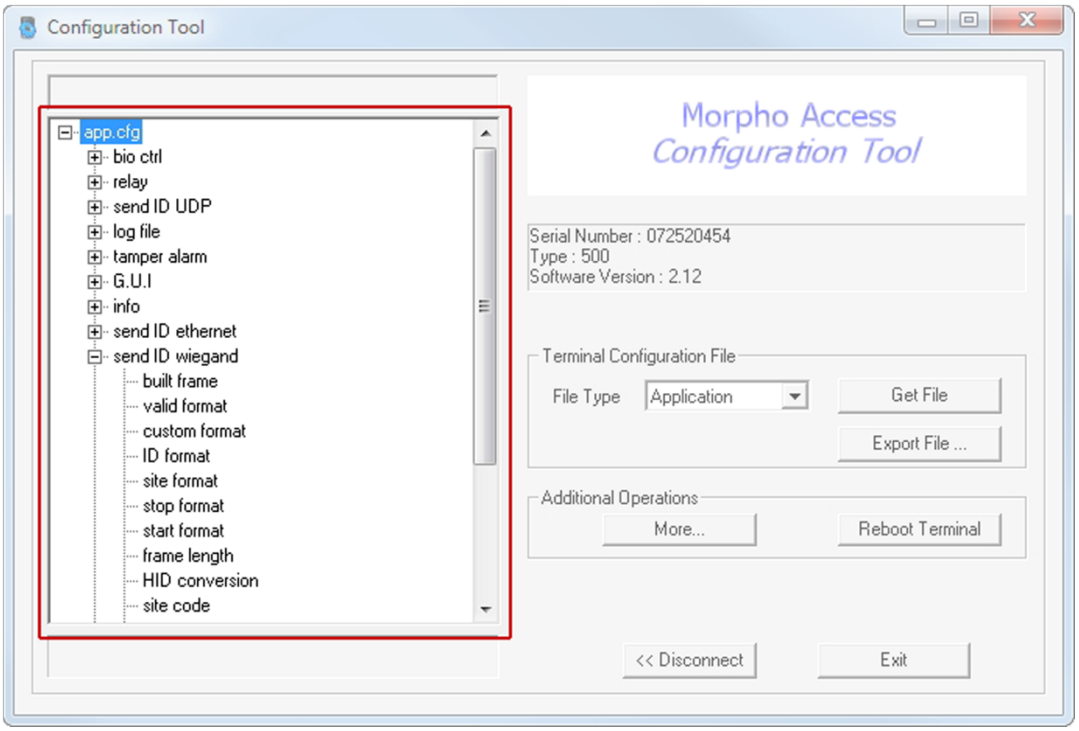


Figure 13 – Configuration Tool Dialog

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:
   - build frame—
   - 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**—*Software fails to report denied transactions on sites with installed Sagem 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 the Controller's DIP-switch settings.

   Solution 3—Check each setting in the **App** file according to the following list:

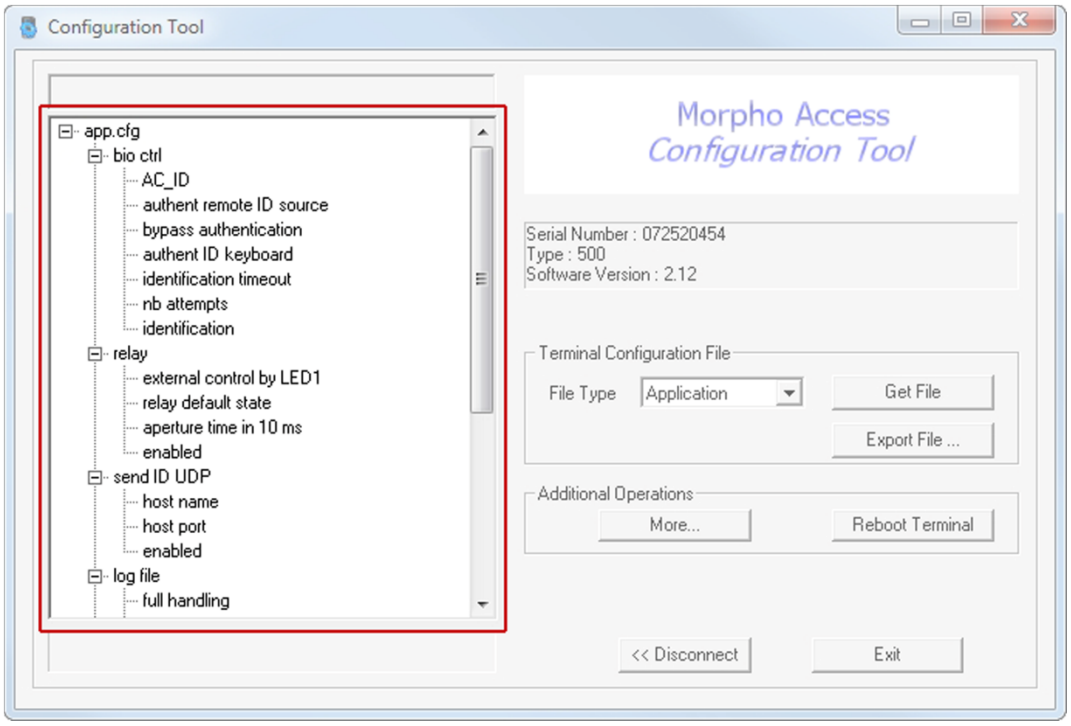


Figure 14 – Configuration Tool Dialog

- **bio ctrl**
  - AC_ID—**FINGER;CARDDATA;KBD;WGDTCLK;**
  - authent remote ID source—**0**
  - bypass authentication—**0**
  - authent ID keyboard—**0**
  - identification timeout—**5**
  - nb attempts—**2**
  - identification—**1**
- **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**
  - Time and attendance icons—**1**
  - 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—**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**
  - terminal identifier—**178**
  - priority—**0**
  - stopbits—**1**
  - databits—**8**
  - speed—**11520**
  - mode—**485**
  - 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**
  - 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 the IXP220 Software, and which does not.

Internal Morpho Configuration Steps

The internal configuration steps of the MA200 or MA300 into the IXP220 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-IXP220 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 will refer you to the STEP in which this information is 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 3, Figure 4 and Figure 5 in this manual.
	Terminal Block Board	Background Information.
	Power Supply Cable	See Figure 3, Figure 4 and Figure 5 in this manual.
	Ethernet Wiring	See Figure 3, Figure 4 and Figure 5 in this manual.
	Wiegand Output Wiring	See Figure 3, Figure 4 and Figure 5 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 IXP220	**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.

STEP DESCRIPTION	MORPHO MANUAL HEADING	PROCEDURE OR COMMENTS
	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 IXP220 Integration.*

Configuration of Morpho Readers into the IXP220 System

Once you've connected the Morpho Readers and configured them internally as described in the previous paragraphs, configure the Readers into the IXP220 System. This section applies to the supported Morpho Fingerprint Readers, the MA100, MA120, MA200, MA300, MA500, MA520 and J-Series.

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 31.

The configuration of these Readers within IXP220 is done using the Biometric Server Software, as follows: From the IXP220 Software, select **File**>**Biometric Server**.

Detecting Morpho Readers on the TCP/IP Bus

1. From the Main Menu, select **Configuration**>**Sagem**>**Sagem Devices**.

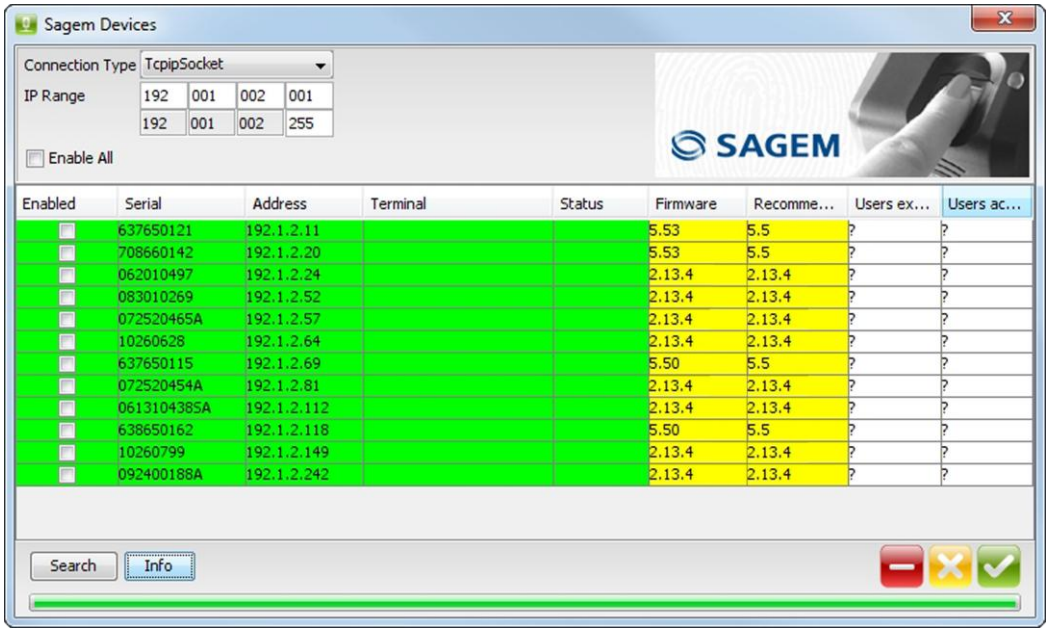


Figure 15 – Sagem Devices Dialog

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.

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. While the **Enable 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. After setting up the units, do a **Full Upload** to create fresh databases on the units.
6. 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.

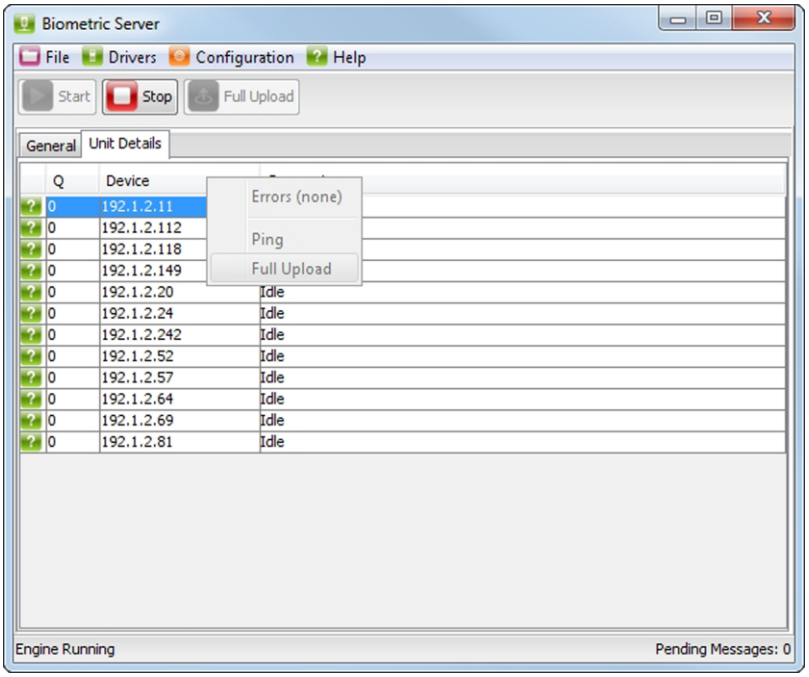


Figure 16 – Unit Details Tab

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 popup, select the **Full Upload** option.

Duplicate Search (1:N Matching)

Using the IXP220 Software, 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 29).
2. From the menu bar, select **Configuration**>**Sagem**>**Matcher**.

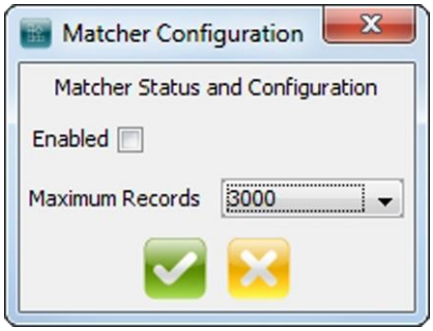


Figure 17 – Matcher Configuration Dialog

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 decompresses 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 33.

1. In the Biometric Enrollment dialog, click the **Advanced** button.
2. Select the **Enable Duplicate Check** checkbox.
3. Click the button.
4. Restart the IXP220 Base Application 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 record is 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

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 IXP220, with central enrollment taking place in the IXP220 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.

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

1. Using the IXP220 Main Menu, select **File**>**Biometric Server**.
2. In the Licence Info dialog, click the **Unlock** button.
3. Place your **Unlock Token** in position in the Tag Registration Reader.
4. In the Sagem Device Unlock dialog, click on the **Read** button.
5. Click on the **OK** button.

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

Enrolling Users on the System

From Windows® select **Start**>**All Programs**>**IXP220**>**IXP220**.

Preference Setup

1. From the Main Menu, select **File**>**Preference**.
2. Select the **Enrollment** Tab.
3. From the **Tag Code Truncation** group, from the **3rd Party Other** drop-down list, select **24 bits**.
4. Click the button.

Enrollment in the IXP220 Software

1. Select the Page Tab.
2. Open a new or existing Tagholder record for editing.
3. In the Tagholder dialog, select the **Tag** Tab.
4. Click one of the assigned **Tag** buttons (that is **Tag 1**, **Tag 2**, **Tag 3** *or* **Tag 4**) or select one of the **Create New Tag** buttons.
5. From the **Configuration Level** group, select the **Advanced Configuration** radio button.
6. Have the Tagholder place his/her Tag on the Enrollment Reader.
7. Click **Read Tag**.
8. Set the **Access Rights** group options as you require.
9. Click the button.
10. Click on the **Biometric Enrollment** button.

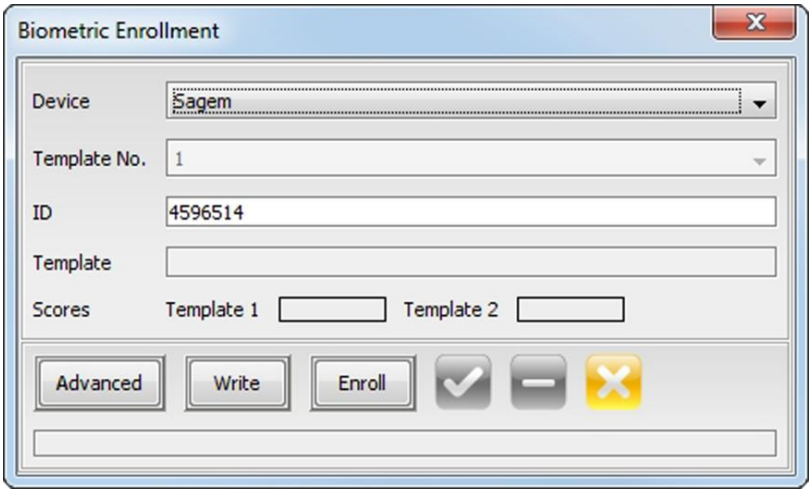


Figure 18 – Biometric Enrollment Dialog

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 **Sagem**.

*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.*

12. 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 rang**e 0** t**o 255**. For best results, we recommend a score above o**f 200**.
- **Enable Duplicate Check**—when enabled, after template capture, the IXP220 Software searches for matches in the Matcher Database (located in the Biometric Server Software).

Restart the Base Application 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 31 for more information.

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

Fingerprint Placement Rules

Figure 19 shows the area of the fingerprint that contains the most information. Therefore, when enrolling Tagholders, ensure they place their fingers as shown in Figure 20.

Finger_Placemnt_01.jpg

Figure 19 – Area of the Fingerprint Containing the most Information

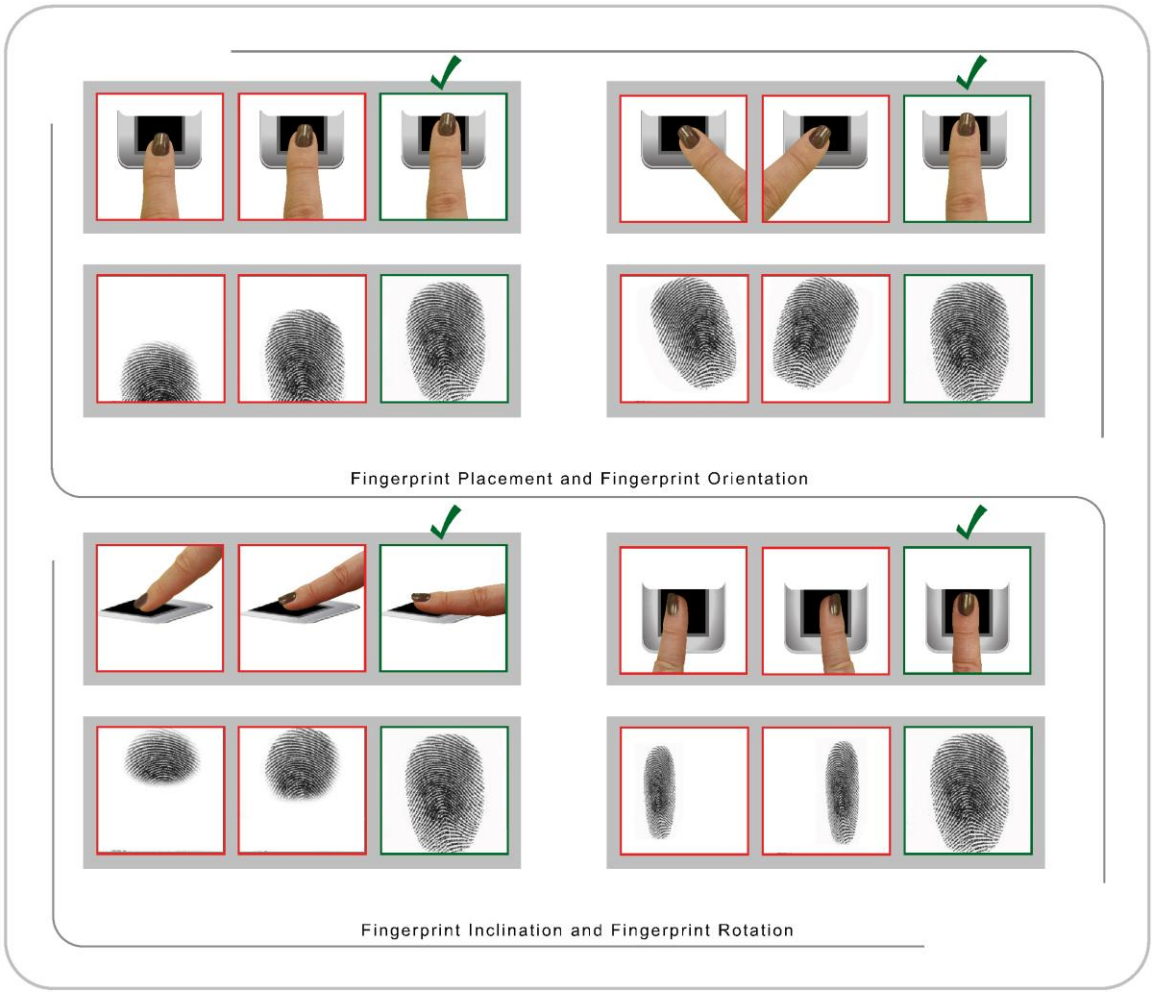


Figure 20 – Fingerprint Placement Rules (Generic Enrollment Reader, Fingerprint Sensor Shown)

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.

1. Click the button.
2. 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 IXP220 System

In instances where you cannot store fingerprint templates in the IXP220 Database, you may write templates direct to the MIFARE® Tag. Reasons for this action could include: cost, Reader limits, laws of the country or just general safety concerns.

By making use of MIFARE® Encoder support, templates do not upload to the Biometric Readers. Instead templates write direct to the MIFARE® Tag. Thus when you present the MIFARE® Tag to the Biometric Reader, the template on the Tag is read. Presenting your finger to the Reader then confirms 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 you wish, there are no limits imposed.

IXP220 offers MIFARE® Encoder support on the following 32-bit and 64-bit Operating Systems: Windows XP, Windows Vista and Windows 7.

*IXP220 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:\IXP220\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:\IXP220\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 IXP220 installation.

1. Browse to **C:\IXP220\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:\IXP220\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:\IXP220\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 **IXP220\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 **IXP220\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 **IXP220\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 **C:\IXP220\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

1. From Windows® select **Start**>**All Programs**>**IXP220**>**IXP220**.
2. From the Main Menu, select **File**>**Preference**.
3. Select the **Enrollment** Tab.
4. From the **Tag Code Truncation** group, from the **3rd Party Other** drop-down list, select **24 bits**.
5. Click the button.

Tagholder Setup

1. Select the Page Tab.
2. Open a new or existing Tagholder record for editing.
3. In the Tagholder dialog, select the **Tag** Tab.
4. Click one of the assigned **Tag** buttons (that is **Tag 1**, **Tag 2**, **Tag 3** *or* **Tag 4**) or select one of the **Create New Tag** buttons.
5. From the **Configuration Level** group, select the **Advanced Configuration** radio button.
6. Have the Tagholder place his/her Tag on the Enrollment Reader.
7. Click **Read Tag**.
8. Set the **Access Rights** group options as you require.
9. Click the button.
10. Click on the **Biometric Enrollment** button.

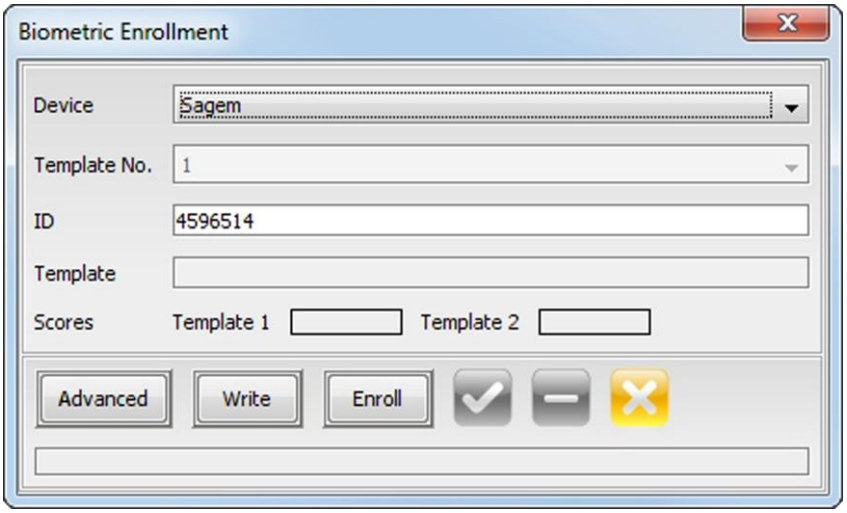


Figure 21 – Biometric Enrollment Dialog

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 **Sagem**.
12. Place your MIFARE® Tag on the SDI010 Contact or Contactless Reader.
13. Click on the **Enroll** button, thereby initiating the enrollment.
14. 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 Sagem 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 enrollment is 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.
11. Click the button.

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

ImproX B-SHO Fingerprint Terminals Use in an IXP220 System

General

This section guides you step by step through the process of setting up ImproX B-SHO Fingerprint Terminals to work with the IXP220 System. The requirements for the integration are as follows:

- IXP220 Access Control System.
- IXP220 V1.80 (and Service Pack 1) or later Installed.

There are four steps in configuring the Fingerprint Terminals to work with IXP220. 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

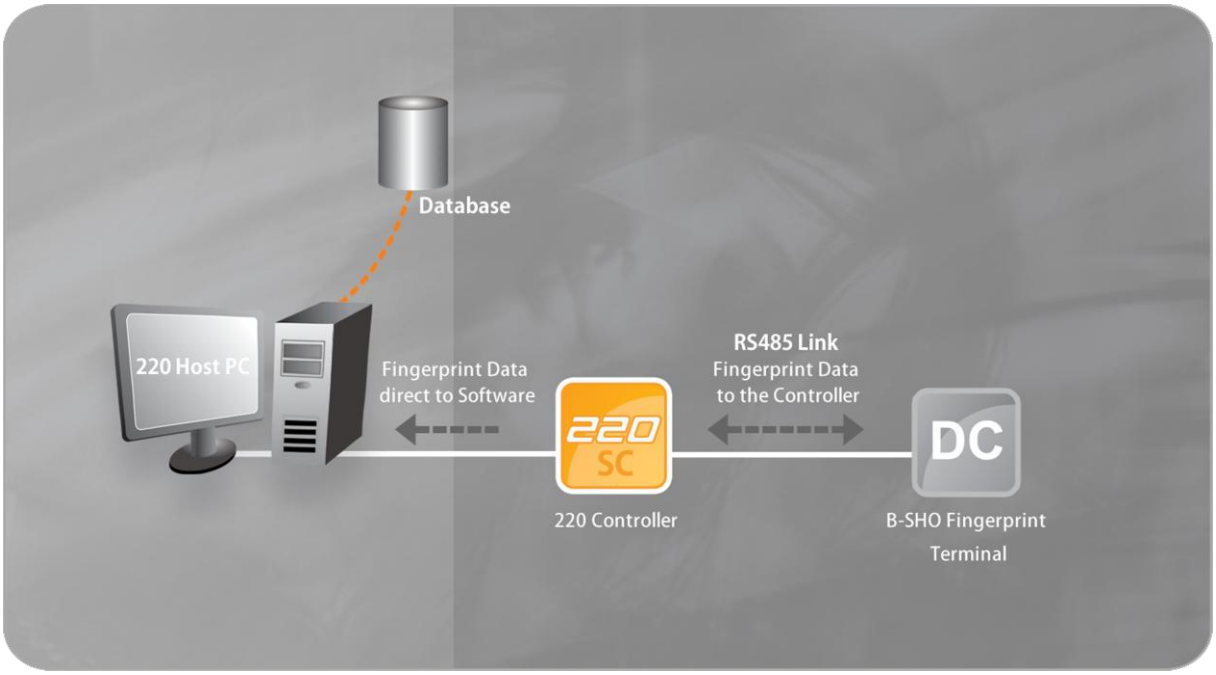


Figure 22 – Tag and Template data flow when using a B-SHO Fingerprint Terminal with IXP220

Hardware Installation of ImproX B-SHO Fingerprint Terminals

The IXP220 System recognizes these Fingerprint Terminals in the same fashion as our ImproX Terminals. Therefore, connect these Terminals to the IXP220 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 IXP220 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.

***Fall-back communications** is NOT supported on sites using ImproX B-SHO Fingerprint Terminals.*

Figure 23, Figure 25 and Figure 24 show connections to the ImproX B-SHO Fingerprint Terminal, these connections remain the same for the ImproX B-SHO Keypad Fingerprint Terminal.

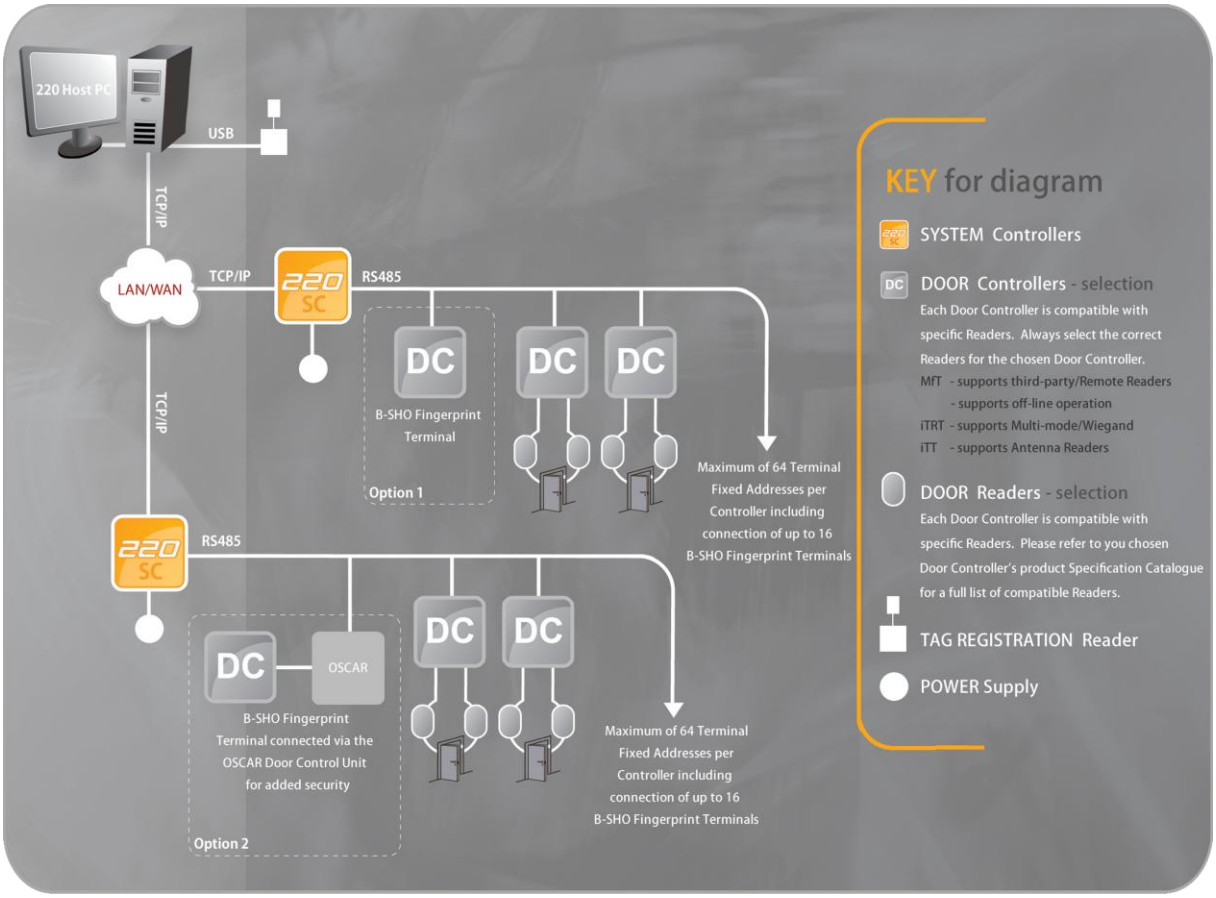
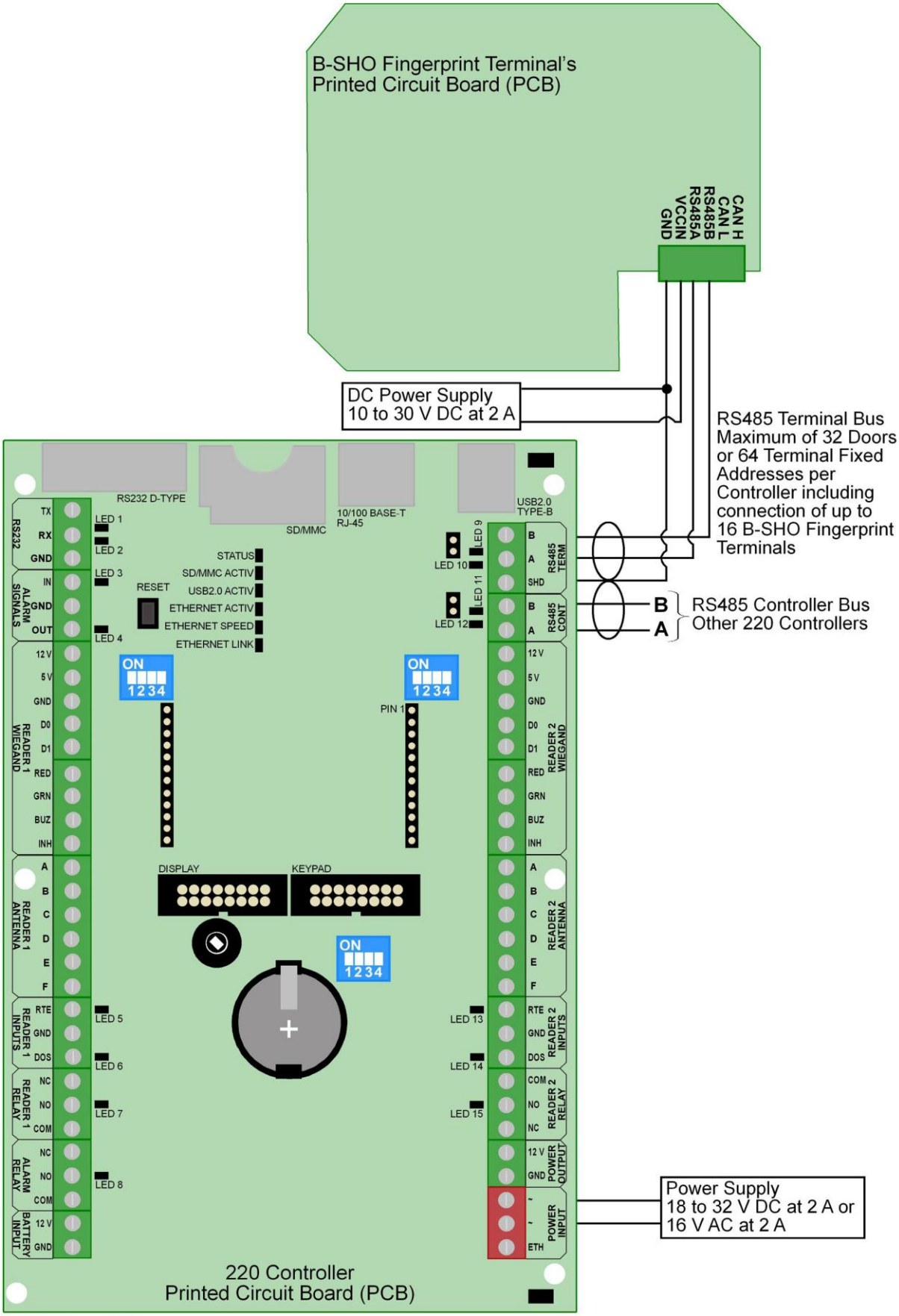


Figure 23 - Fingerprint Terminals Relationship with the Rest of the ImproX Product Range



BSHO_Conn_03.jpg

Figure 24 – ImproX B-SHO Fingerprint Terminal Connected to the Controller via the Terminal Bus

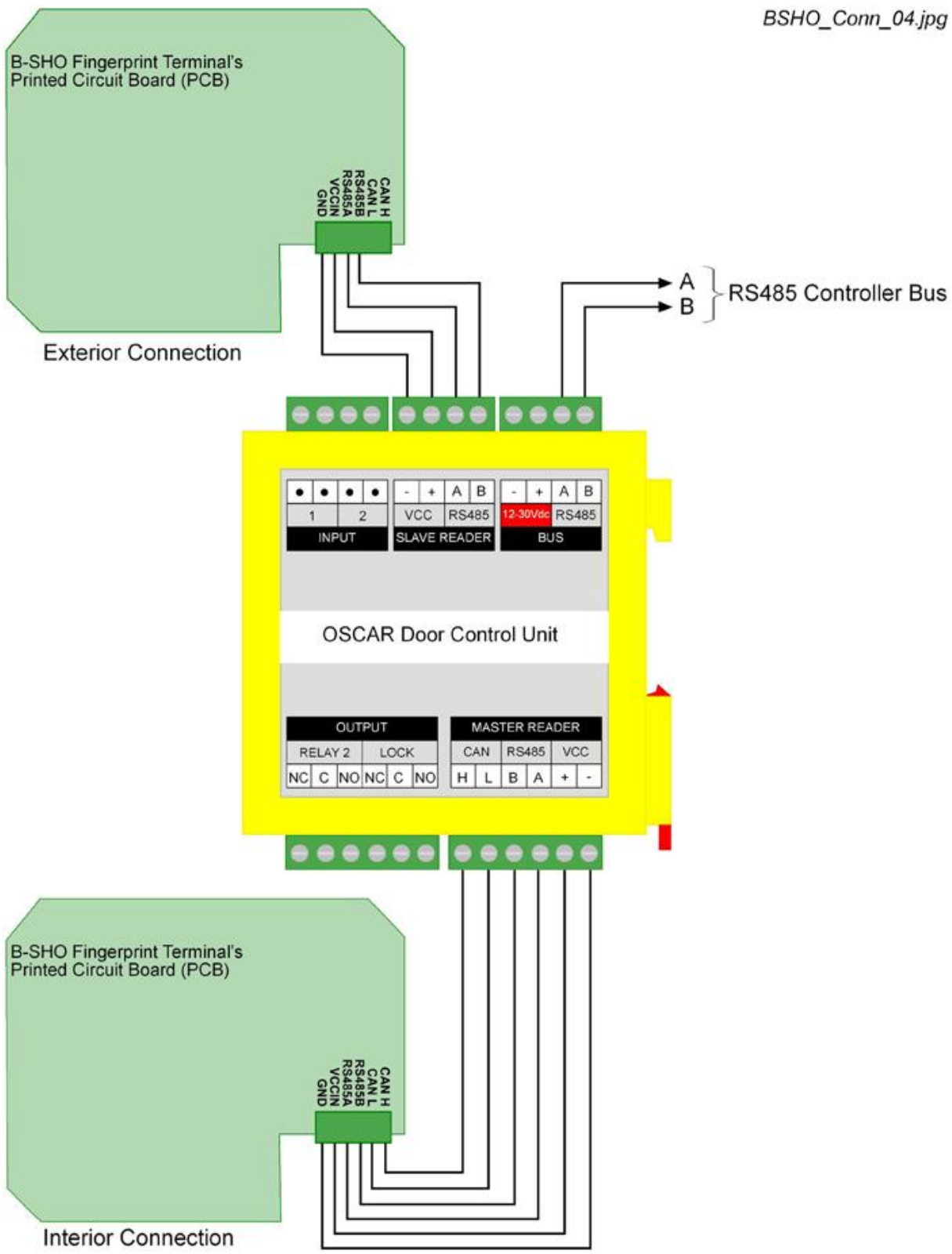


Figure 25 – ImproX B-SHO Fingerprint Terminal Connected Via the ImproX OSCAR Door Control Unit

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 IXP220 System:

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

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

To open the IXP220 Base Application, proceed as follows:

1. In Windows®, click **Start**>**All Programs**>**IXP220**>**IXP220**.
2. Enter your **Username** (**SYSDBA**) and **Password** (**masterkey**).
3. From the **Security Device Search** drop-down list, select from the following choices:

*On first time installation of the IXP220 Software, the **I do not have one** choice is by default selected. If the site has an ImproX RS connected that's unlocked for a System 3 or System 4 then the IXP220 Software starts up as a **System 1**. This means, no search is performed for the ImproX RS.*

   – **Automatically Search**
   – **Enter the COM Port Name**
   – **I do not have one**
4. Click the button.

After completing the login action, the **Automatic Database Upgrade Utility** checks the database version. If the Utility confirms the Database is older than that needed by the Software, perform the upgrade as follows:

1. At the Warning dialog, click the **OK** button.
2. In the Database Updater dialog, click the **Upgrade** button.
3. At the Message dialog, click the **OK** button.

The Auto-ID process differs across the different communication mediums; therefore continue with one of the following:

Controller Connected to Host PC using RS485 (ImproX RS)

1. From the Main Menu, select **Hardware**>**Auto ID Units**.
2. At the **Confirm Auto-ID** dialog, click the **OK** button.
3. From the Auto ID Communications Configuration dialog, select the appropriate **Com Port** record.
4. From the list of devices displayed, in the **Auto-ID Channel** column, make your selection.
5. Click the button.
6. At the Firmware Revision dialog, click the button.

Controller Connected to the Host PC using TCP/IP

1. From the Main Menu, select **Hardware**>**Auto ID Units**.
2. At the **Confirm Auto-ID** dialog, click the **OK** button.
3. If your Controller does NOT appear in the **Auto ID Communications Configuration** dialog continue as follows:

When using IP Terminals, do not use the button. Instead, make use of the button.

a. Click the button.
b. In the **Channel** column, replace the default IP Address details with the IP Address of your Controller.
c. Press **Enter**.

Or alternatively continue as follows:

a. Click the button.
b. In the Input dialog, enter the **Subnet Mask** details for your Network.
c. Click the button.

*The **IP Door Controllers (Advanced)** tab provides a list if the IP Terminals in the System as well as the IP Address of the Controllers they connect to. When using IP Terminals over a WAN, change the Controller IP Address to the IP Address of the Router to ensure that the IP Terminal communicates correctly. To do this, continue as follows:*

1. *On the Auto-ID Channel tab, click the button.*
2. *In the Input dialog, enter the **Subnet Mask** details for your network.*
3. *Click the button.*
4. *Select the **IP Door Controllers (Advanced)** tab.*
5. *In the **Address** column, enter the Public Static IP Address of the Router the Controller will use to communicate with the Terminal.*
6. *In the **Respond To Address** column, enter the Public Static IP Address of the Router the Terminal will use to communicate with the Controller.*
7. *If necessary, edit the **Additional Timeout (0.1s)** value.*
8. *Continue with Auto-ID as normal. (See step 4 below).*

4. From the list of devices displayed, in the **Auto-ID Channel** column, make your selection.
5. Click the button.
6. At the Firmware Revision dialog, click the button.

Controller Connected over a Wide Area Network (WAN)

Controllers connected using a GSM Module do NOT support IP Terminals.

1. At the **Auto-ID is Recommended for New Sites** dialog, click the **Yes** button.
2. At the **Confirm Auto-ID** dialog, click the **OK** button.
3. In the Auto ID Communications Configuration dialog, click the **Import Channels** button.
4. Select the **Discovery.txt** file (originally exported from the Discovery Utility).
5. Click the **Open** button.

*The **IP Door Controllers (Advanced)** tab provides a list of the IP Terminals in the System as well as the IP Address of the Controllers they connect to. When using IP Terminals over a WAN, change the Controller IP Address to the IP Address of the Router to ensure that the IP Terminal communicates correctly. To do this, continue as follows:*

1. *On the Auto-ID Channel tab, click the **Import Channels** button.*
2. *Select te **Discovery.txt** file (originally exported from the Discovery Utility).*
3. *Click the **Open** button.*
4. *Select the **IP Door Controllers (Advanced)** tab.*
5. *In the **Address** column, enter the Public Static IP Address of the Router the Controller will use to communicate with the Terminal.*
6. *In the **Respond To Address** column, enter the Public Static IP Address of the Router the Terminal will use to communicate with the Controller.*
7. *If necessary, edit the **Additional Timeout (0.1s)** value.*
8. *Continue with Auto-ID as normal. (See step 6 below).*

6. From the list of devices displayed, in the **Auto-ID Channel** column, make your selection.
7. Click the button.
8. At the Firmware Revision dialog, click the button.

When hardware units are detected, they are added to the IXP220 Database and become available in the IXP220 Software. 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. Select the Page Tab. Within the previously selected Door Tab, you will notice a new set of Tabs activate. These newly activated Tabs include a new **Door** Tab, an **Entry** Tab and an **Exit** Tab.
2. Click the button.
3. In the **Door Name** textbox, assign the Door a suitable name. This Door Name textbox has a 16 character limit.
4. From the **Configuration Level** group, select one of the following radio buttons:
   - **Standard Configuration**—activates only the basic Access Control features.
   - **Advanced Configuration**—activates extra advanced features, for sites that need Daily Door Mode Patterns, Zones, Door Entry Codes and Alarm Arming.
5. In the **Reader Configuration** group, alongside the **Entry Reader** textbox, click the **Select** button.
6. In the **Unassigned Readers** dialog, from the list of displayed records, select a Reader (for example the ImproX B-SHO Fingerprint Terminal).

In the Unassigned Readers dialog, reduce the number of Readers displayed by selecting a specific Controller from the Controller Filter drop-down list.

7. Click the button.
8. Alongside the **Exit Reader** textbox, click the **Select** button.
9. In the **Unassigned Readers** dialog, from the list of displayed records, select a Reader (for example the ImproX B-SHO Fingerprint Terminal).
10. Click the button.

Entry or Exit Reader Configuration

1. Select the **Entry** or **Exit** Tab.

The settings displayed on the Entry or Exit Tabs depend on the type of Terminal connected. Ignore references made to fields that do not display.

2. From the **Configuration Level** group, select one of the following radio buttons:
   - **Standard Configuration**
   - **Advanced Configuration**
3. From the **Miscellaneous** group, from the **RTE Mode** drop-down list, make your selection from the following:
   - **Normally Open**
   - **Normally Closed**
4. From the **Reader Function** drop-down list, make your selection from the following:
   - **Access Control**
   - **Access Control + Time & Attendance**
5. From the **Message Display Supervisor** drop-down list, make your selection.
6. From the **Enable Off-line Validation** drop-down list, make your selection from the following:
   - **Disabled**—disables off-line validation.
   - **Enabled**—enables off-line validation.

ImproX iTT and ImproX iTRT units connected by IP will always run in Full Off-line Validation Mode. ImproX iTT and ImproX iTRT units connected by RS485 will run in Full Off-line Validation Mode when there are 1 000 Tags or less in the System. Once this threshold is exceeded, it will switch over to Cached Off-line Validation Mode. Cached Off-line Validation Mode relies on transactions in the ImproX iTT and ImproX iTRT Transaction Buffer to make access control decisions.

7. From the **DOS Mode** group, from the DOS Mode drop-down list, make your selection from the following:
   - **Normally Closed**
   - **Normally Open**
8. From the **DOS Usage** drop-down list, make your selection from the following:
   - **Normal**
   - **Terminate Strike**
   - **Inhibit**
9. Edit the **Strike Duration (0.1s)** textbox, the default value is **40** (0.1s). Setting the Strike Duration to **55555** toggles the Relay.
10. Edit the **Open Duration(s)** textbox. By default, the Open Duration is set to **0**, disabling the Door Open Sensor (DOS).

It is possible to drive a single Relay or use a single Door Open Sensor (DOS) for both entry and exit Readers, removing the need to wire up both Relays or both Door Open Sensors for a single door. To do this, set the Strike Duration or Open Duration to 0 on one Reader. The associated Reader is then able to use the Relay or DOS from the opposite Door. When using an ImproX MDTA, the Open Duration and Strike Duration default to 0. Therefore, setting the Strike Duration and Open Duration on the associated Reader allows the MDTA to use the opposite Reader's Relay or DOS.

A practical example would be:
A Terminal, used for a reception entry and exit, only requires one Relay to open. The entry Reader (Reader 1) has the Strike Duration set accordingly. Instead of bridging the Relay for the exit Reader (Reader 2), set the Strike Duration to 0. This allows both the entry and exit Readers to drive Relay 1 when someone presents an allowed Tag to either of the Readers. The same theory applies to the Door Open Sensor.

11. Enable End-of-line Sensing by selecting the **Enable End-of-line Sensing** checkbox.

End-of-line Sensing lets the System raise an alarm when somebody bypasses the Door Open Sensor. That is, the System distinguishes between tampering on the circuit and closure of the Door Open Sensor. End-of-line sensing on the IXP220 Controller, ImproX iTT (input 1 and 3 only) and iTRT (input 1 and 3 only) is only possible if Door Open Sensing is configured. Set End-of-line Sensing per Door.

12. From the **ON VALID Tag** group, from the **LED Action** drop-down list, select the required LED colour state and Duration.
13. From the **Buzzer Volume** drop-down list, select the Buzzer volume and Duration.
14. From the **ON INVALID Tag** group, from the **LED Action** drop-down list, select the required LED colour state and Duration.
15. From the **Buzzer Volume** drop-down list, select the Buzzer volume and Duration.
16. Click the button.

Add a Zone

1. On the Configuration Pane, select the **Zone** Tab.
2. Click the button.
3. In the Create Zone dialog, select a Controller from the **Select Controller** drop-down list.
4. In the **Zone Name** textbox, assign the Zone a suitable name.
5. Select one of the **APB Mode** (Anti-passback Mode) radio buttons:
   - **Off**
   - **Relaxed**
   - **Strict**
6. Click the button.

Add Door Mode Patterns

The IXP220 Software supports a maximum of 8 Door Mode Patterns at each Door.

1. On the Configuration Pane, select the **Door Mode Pattern** Tab.
2. Click the button.
3. In the **Pattern Name** textbox, assign your Door Mode Pattern a suitable name.
4. Click the button.
5. From the records displayed on the left-hand side of the Configuration Pane, select the newly created Door Mode Pattern record.
6. Edit the following settings for the selected record:
   - **Start Time**
   - **End Time**
   - **Mode**
   - **Finger (B-SHO)**—make a selection from the choices presented.

Finger (B-SHO) setting examples include: No, "+Entry", "+Exit", "+Both", "or Entry", "or Exit", "or Both", "Finger only Entry", "Finger only Exit" or "Finger only Both". These are explained as follows:

- *Selecting "+Entry", "+Exit" or "+Both", calls for Tagholders to present their Tag (MIFARE® or DESFIRE®) and their fingerprint at the ImproX B-SHO Fingerprint Terminal.*
- *Selecting "or Entry", "or Exit" or "or Both", calls for Tagholders to present either their Tag or fingerprint at the ImproX B-SHO Fingerprint Terminal.*

- *For the following options, "Finger only Entry", "Finger only Exit" or "Finger only Both", only fingerprint presentation is allowed (the tag reader is disabled).*

  - **+PIN**
  - **+Reason**
  - **+Dual Tag**
  - **Record**
  - **Denied Alarm**
  - **LED**

7. Click the button.
8. Select the **Advanced Configuration** radio button.
9. On the Configuration Pane, select the **Door** Tab.
10. In the **Daily Door Mode Patterns** group**,** make your selections from the Day's Door Mode Pattern drop-down lists.
11. In the **Zone** group, select a Zone from the drop-down list.
12. Click the button.

Add a Tagholder

To add a Tagholder, proceed as follows:

1. Select the Page Tab.
2. Click the button.
3. In the Tagholder dialog, select the **General** Tab.
4. Enter the Tagholder's **First Name**.
5. Enter the Tagholder's **Last Name**.
6. From the **Configuration Level** group, select from the following radio buttons:
   - **Standard Configuration**
   - **Advanced Configuration**

The instructions below continue as for an Advanced Configuration.

7. In the **PIN Used with Tag** textbox, enter a PIN-code of up to 4 digits. (PIN-codes range from **2 to 65534**).
8. From the **Department** drop-down list, select a department name.

*Add extra **Departments** as follows:*

1. *Click the **Department** button.*
2. *Click the button.*
3. *In the **Department** textbox, enter a suitable name for the Department.*
4. *Click the button.*
5. *Click the button.*

Click the button to edit a Department or the button to delete a Department.

*The **Send E-Mail** button lets you send Tagholder details to interested parties. The **To** textbox is mandatory, thus requiring data entry for successful e-mail transmission. For e-mail setup information please refer to the section Preference Configuration (System Notification Tab) in Part 3 – General Configuration.*

9. From the **Type** drop-down list make your selection.
10. Complete other personal information as necessary.

*Add a Tagholder **Image** as follows:*

1. *Click the button.*
2. *At the Open dialog, select the image file. Image formats supported include: jpg, jpeg, gif, tif and tiff. The recommended resolution is 640 x 480 pixels.*
3. *Click the **Open** button.*

For more information on the Live Video Image Capture feature ( ) please see Part 5 – Advanced Configuration.

Clicking the button opens the Edit dialog, allowing image cropping, rotation, resizing and use of an image mirror effect.

11. Use the **Note** text area when entering further information about the Tagholder.
12. Click the button.

Assign Tags to Tagholders

A Tagholder can have up to 4 Tags assigned to them. To assign Tags to a Tagholder, proceed as follows:

1. In the Tagholder dialog, select the **Tag** Tab.
2. Click any of the **Create New Tag** buttons.

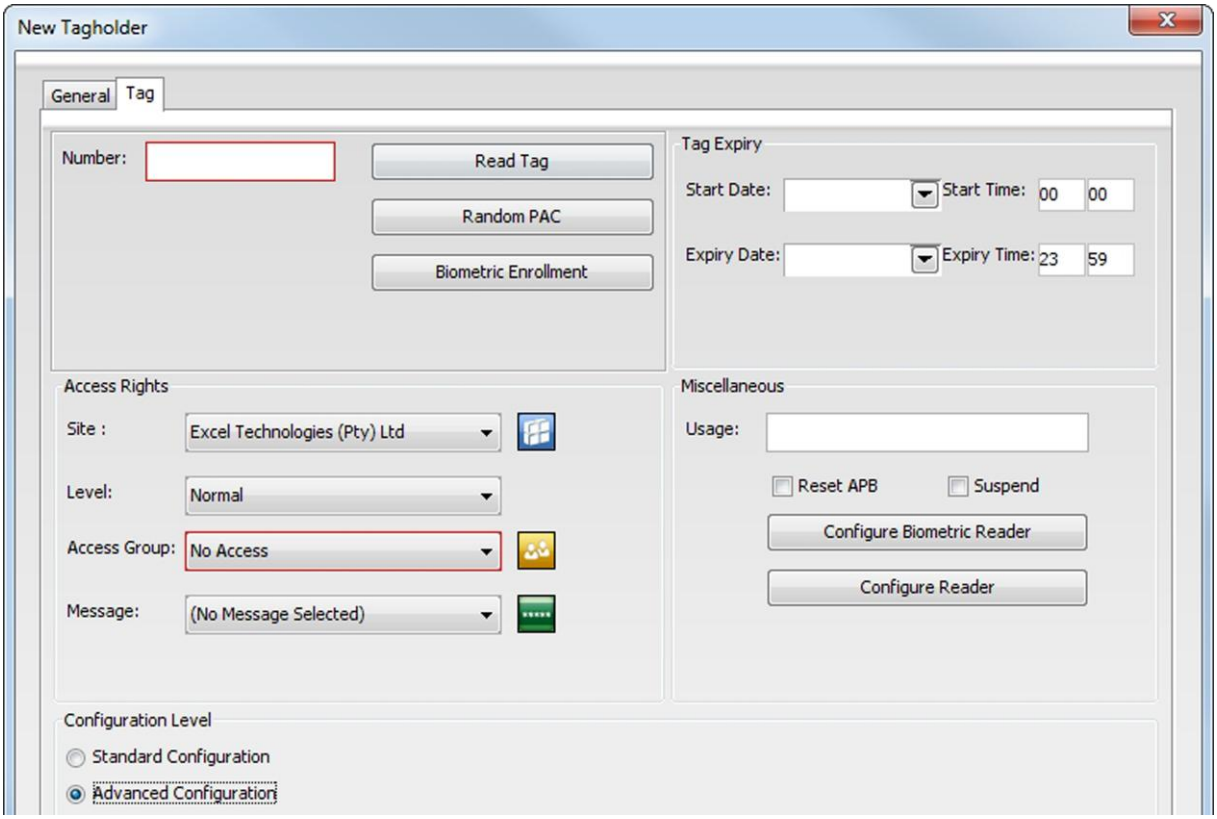


Figure 26 – Tagholder Dialog (Showing the Tag Tab)

3. From the **Configuration Level** group, select one of the following radio buttons:
   - **Standard Configuration**—disables advanced configuration options.
   - **Advanced Configuration**—enables advanced configuration options.

The instructions that follow continue as for an Advanced Configuration. For a Standard Configuration ignore references made to fields that appear greyed out.

4. Select from the following tasks in order to complete the Tag assignment process:

   Selecting a Registration Reader

   a. From the **Miscellaneous** group, select the **Configure Reader** button.
   b. In the **Configure Tag Reader** dialog, from the Use Registration Reader radio buttons, select one of the following:
      - **Yes**
      - **No**
   c. Click the button.

5. Click the button.

Biometric Enrollment

1. From the **Configuration Level** group, select the **Advanced Configuration** radio button.
2. In the **Number** textbox, enter a number.

*This number later links to the **ID** field (shown in Figure 27) this is the number under which the user's data is saved when his or her fingerprints are enrolled in the units.*

3. Click on the **Biometric Enrollment** button.

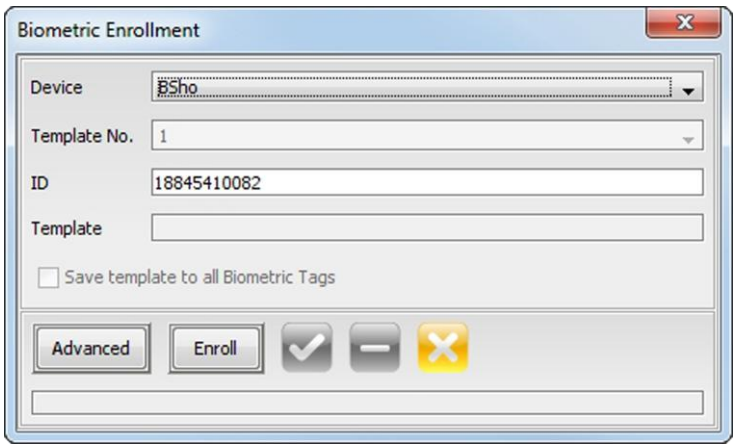


Figure 27 – Biometric Enrollment Dialog

4. 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 B-SHO units. The **ID** field is the ID derived from the Tag Code (Number field) 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 enrollment is 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 **Enrollment Device** drop-down list, select either Suprema BioMini or B-Sho Editor.
4. Click the button.

*The **Query Templates** button collects information from the B-Sho Readers, around the site, to see how many templates are on the Readers.*

Fingerprint Placement Rules

Figure 28 shows the area of the fingerprint that contains the most information. Therefore, when enrolling Tagholders, ensure they place their fingers as shown in Figure 29.

Finger_Placemnt_01.jpg

Figure 28 – Area of the Fingerprint Containing the most Information

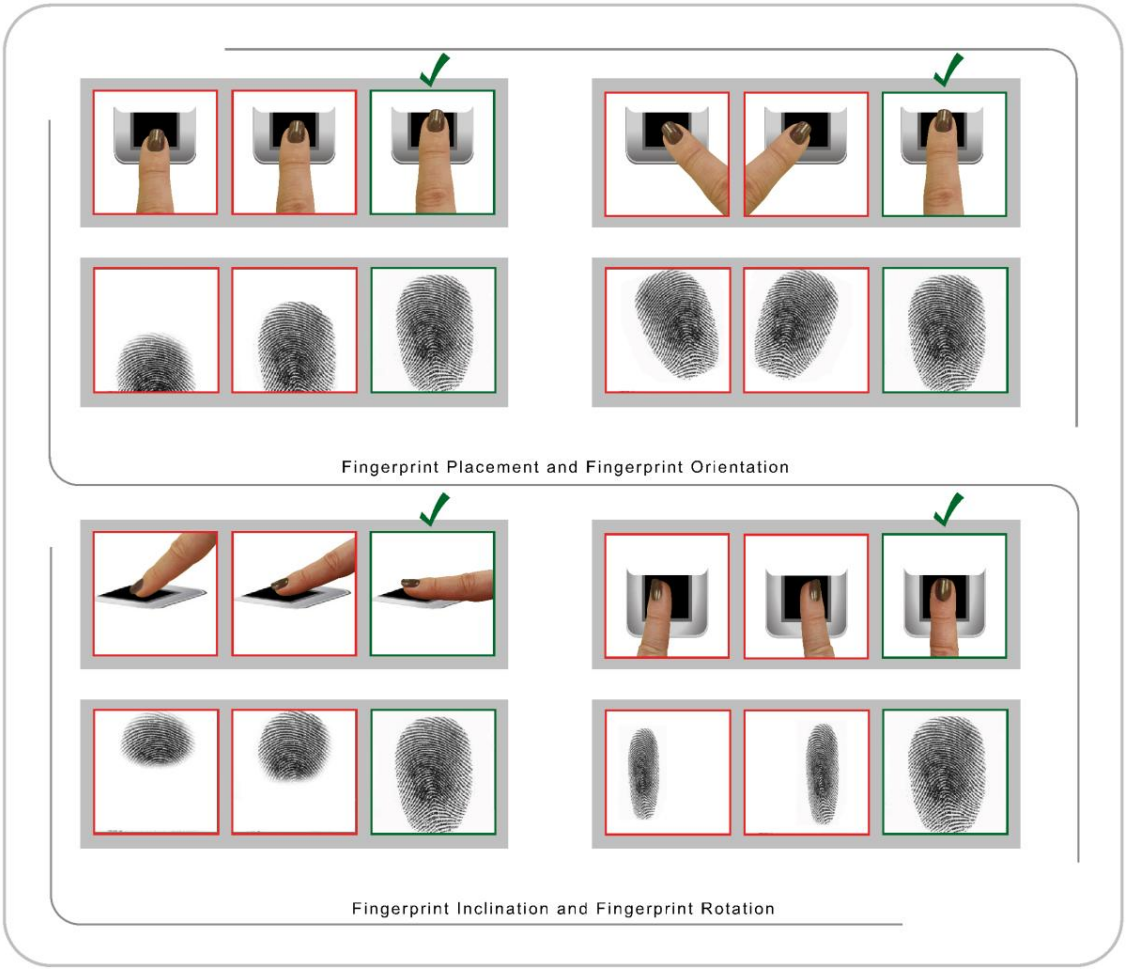


Figure 29 – Fingerprint Placement Rules (Generic Enrollment Reader, Fingerprint Sensor Shown)

After enrollment, ensure that Tagholders use the Fingerprint Placement Rules shown in Figure 29 each time they present their finger to the ImproX B-SHO Fingerprint Terminal.

Enrollment procedure at the ImproX B-SHO BioMini USB Fingerprint Enrollment Reader

1. Click on the **Enroll** button, thereby initiating the enrollment.
2. Enroll **Finger 1** as follows:
   a. At the Acquisition Window dialog, place Finger 1 (fingerprint down) on the Enrollment Reader's fingerprint Sensor.
   b. Remove Finger 1 from the Sensor.
   c. At the Template Captured dialog, click the **Yes** button thus accepting the template.
   d. Place Finger 1 on the Sensor a second time.
   e. Again, remove Finger 1 from the Sensor.
   f. At the Template Captured dialog, click the **Yes** button thus accepting the template.
   g. At the Acquisition Window dialog, place Finger 1 on the Sensor for matching purposes.
3. Enroll **Finger 2** as follows:
   a. Place Finger 2 (fingerprint down) on the Enrollment Reader's fingerprint Sensor.
   b. Remove Finger 2 from the Sensor.
   c. At the Template Captured dialog, click the **Yes** button thus accepting the template.
   d. Place Finger 2 on the Sensor a second time.
   e. Again, remove Finger 2 from the Sensor.
   f. At the Template Captured dialog, click the **Yes** button thus accepting the template.
   g. At the Acquisition Window dialog, place Finger 2 on the Sensor for matching purposes.

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

Access Rights Configuration

1. From the **Site** drop-down list, select the Site name.

Alternatively, click the button to select the Access Group for the Tagholder across all Sites.

2. From the **Level** drop-down list make your selection from the following choices:
   - **Visitor**
   - **Normal**
   - **Supervisor**
   - **Administrator**
3. From the **Access Group** drop-down list, make a selection.

Alternatively, click the button to create a new Access Group.

You must assign a Tagholder Access Group for the Tag to have any access rights.

Tag Expiry Configuration

For temporary Tagholders, proceed as follows:

1. From the **Start Date** drop-down list, select a suitable start date.
2. In the **Start Time** textboxes, enter a suitable start time.
3. From the **Expiry Date** drop-down list, select a suitable expiry date.
4. In the **Expiry Time** textboxes, enter a suitable expiry time.

Message Configuration

*For information on adding Messages, refer to the **Messages** section in Part 3 – General Configuration.*

From the Message drop-down list, select a Message for display.

Alternatively, click the button to create a new Message.

Miscellaneous Configuration

- **Reset APB**—resets the Anti-passback (APB) status for an individual Tagholder.
- **Suspend**—suspends the Tag in the event the Tag is lost or no longer required.
- **Usage**—stores a description of the Tag's usage.
- **Configure Reader**—lets you select the Reader for use as the Registration Reader for the site.
- **Configure Biometric Reader**—opens the Tagholder biometric configuration and enrollment settings.

General Details

1. Click the button.
2. Click the button.

If necessary, repeat the **Assign Tags to Tagholders** procedure for any extra Tagholders.

Upload Fingerprint Templates

B-SHO templates upload as added. If however, you modified Site Configuration information, or you want to add a batch of templates at once, use the **BSHO Full Upload (Current Site)** option.

After performing a Full Upload, there is a time of adjustment needed by the ImproX B-SHO Fingerprint Terminal. During this time the Terminal learns the best template read process, afterwards giving Tagholders improved fingerprint read times.

Use this option as follows:

1. From the Main Menu, select **Configuration**>**BSHO Full Upload (Current Site)**.

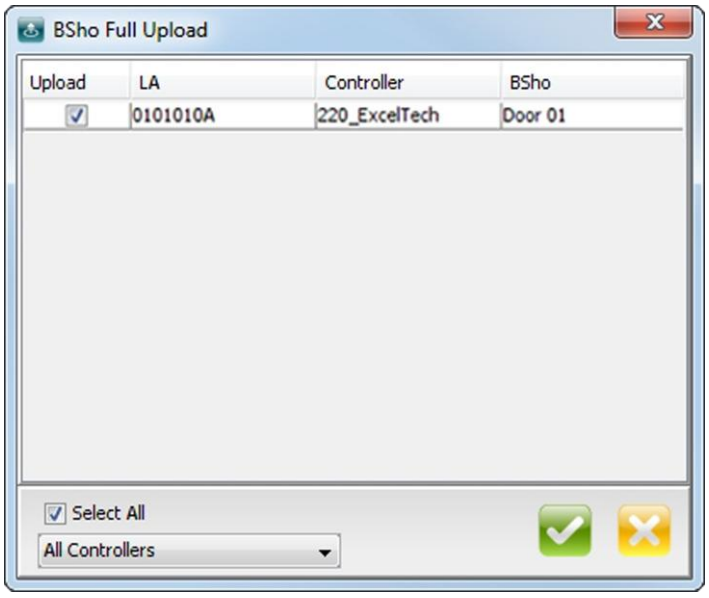


Figure 30 – B-SHO Full Upload Dialog

2. Select the records for upload.
3. Click the button.

Troubleshooting

1. Clicking the **Enroll** button (accessed from the Biometric Enrollment dialog – see Figure 27) displays an Error dialog with the message **"Enrollment failed**!". Possible solutions to this problem include: Check and make sure the ImproX B-SHO Enrollment Reader is plugged into the PC. Alternatively, if the ImproX B-SHO Enrollment Reader is plugged in, restart the IXP220 Base Application.

2. At the Acquisition dialog, while enrolling fingerprints, the IXP220 Software asks the user to "**Please Remove Finger**". The System fails to detect that the **finger is NOT positioned on the Enrollment Reader**. As a solution to this, ensure the Enrollment Reader's Sensor area is clean.
3. At the Acquisition dialog, while enrolling fingerprints, the IXP220 Software asks the user to "**Please Place Your First (or Second) Finger**". The System fails to detect the finger is already in position on the Enrollment Reader. Scanning can only take place when the Sensor area's red LED lights up. When this problem occurs, remove the finger from the sensor area, place the finger back on the sensor area only when the Sensor's red LED lights up.
4. When told by the IXP220 Software that the **fingerprint quality is below threshold**. Follow finger placement rules to achieve a higher finger threshold percentage. If you do not notice an improvement, drop the threshold to a lower value.

NITGEN Fingerprint Terminals Use in an IXP220 System

General

This section guides you step by step through the process of setting up NITGEN Fingerprint Terminals to work with the IXP220 System. The requirements for the integration are as follows:

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

- IXP220 Access Control System.
- IXP220 V1.86 or later installed.

There are five steps in configuring the Fingerprint Terminals to work with IXP220. 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

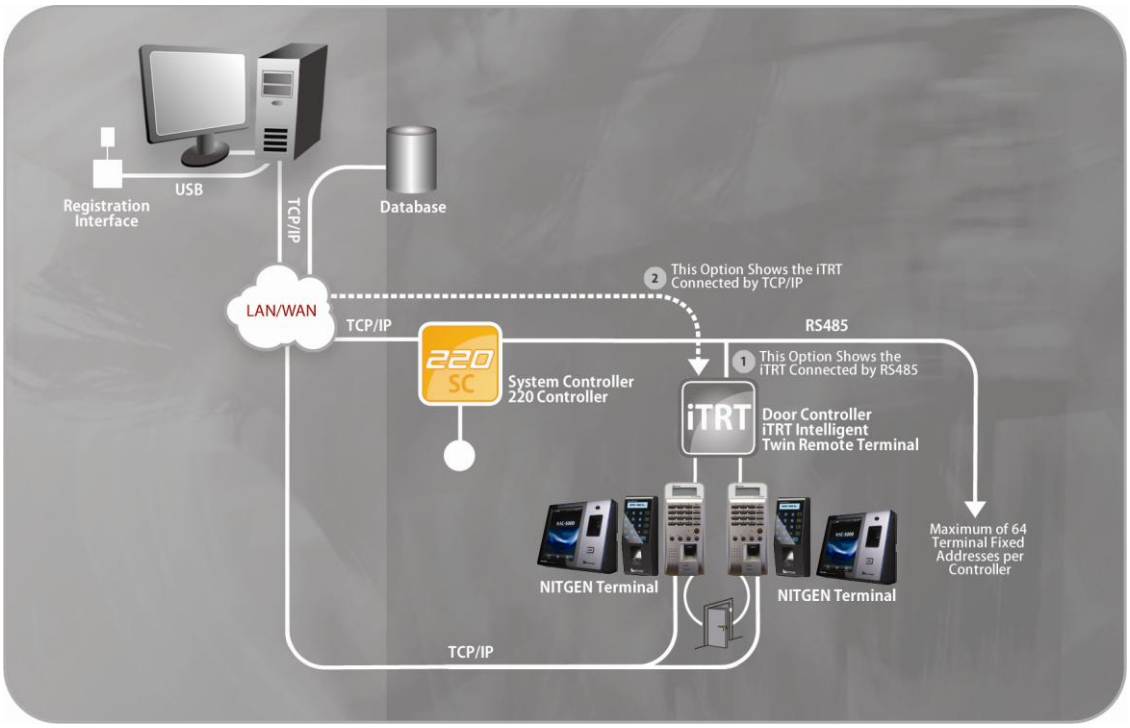


Figure 31 – Using NITGEN Fingerprint Terminals within the IXP220 System

Hardware Installation of NITGEN Fingerprint Terminals

Each NITGEN Terminal must connect to the LAN to send and receive templates from the IXP220 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:

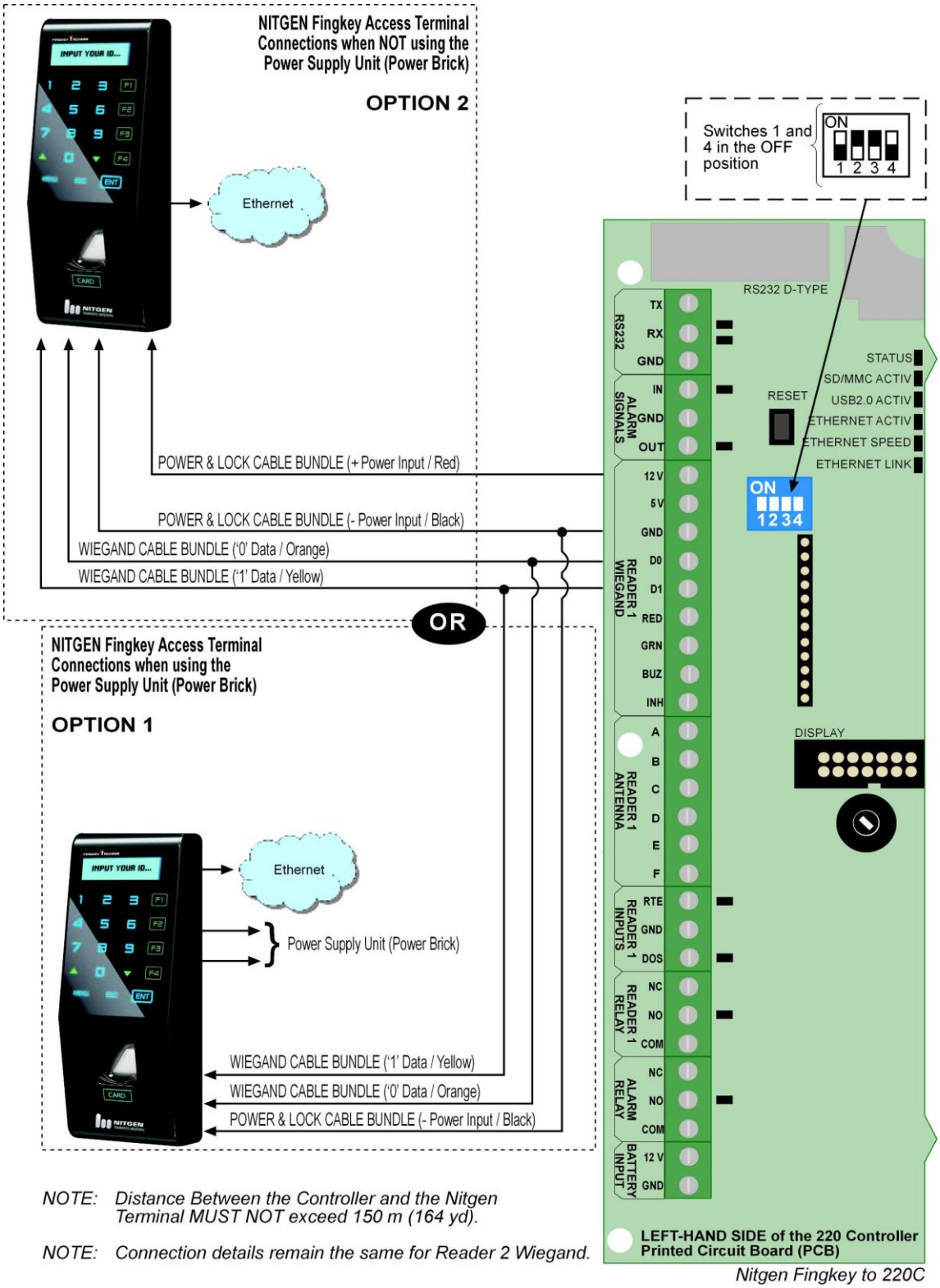


Figure 32 – NITGEN Fingkey Terminal Connected to the IXP220 Controller

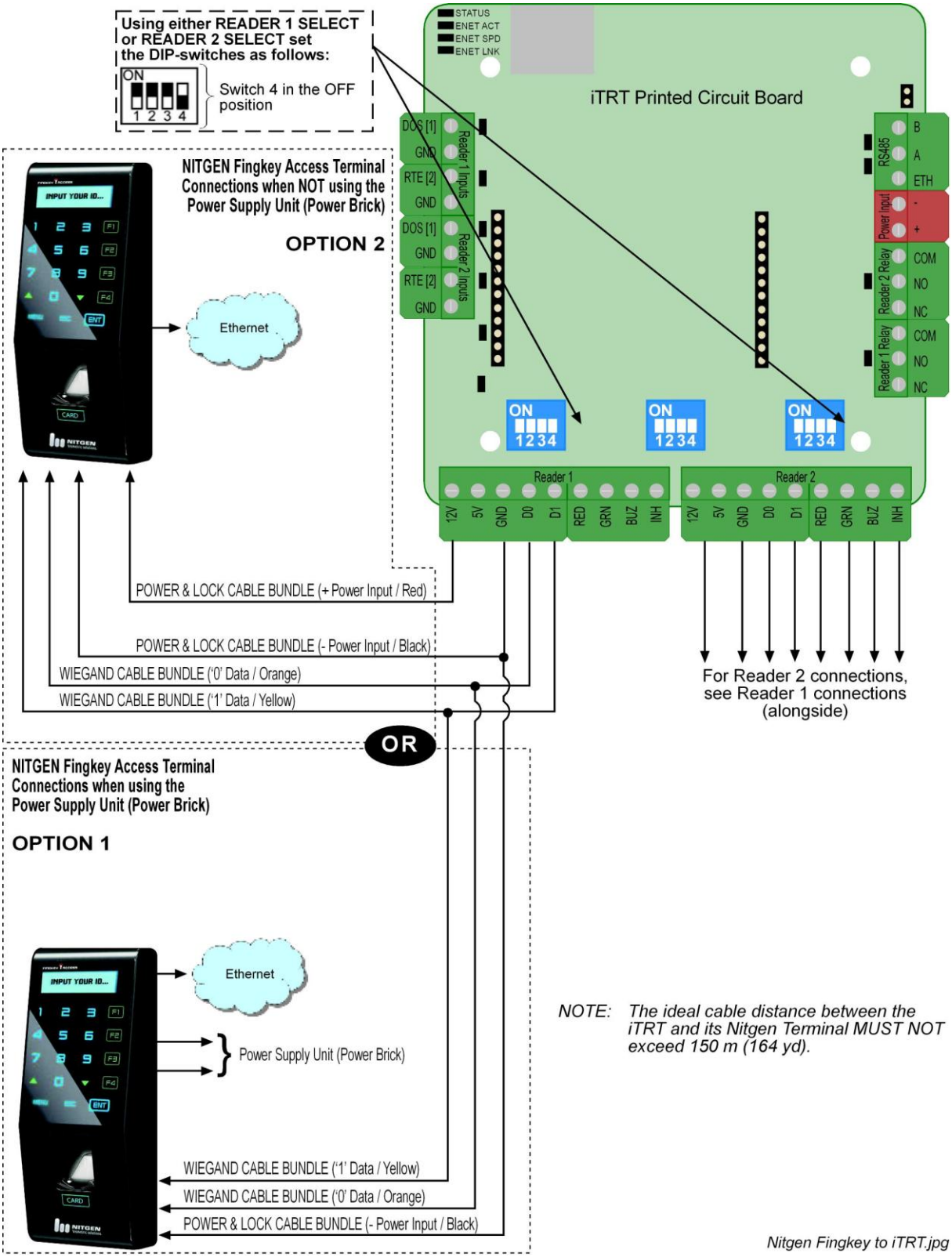


Figure 33 – NITGEN Fingkey Terminal Connected to the ImproX iTRT Terminal

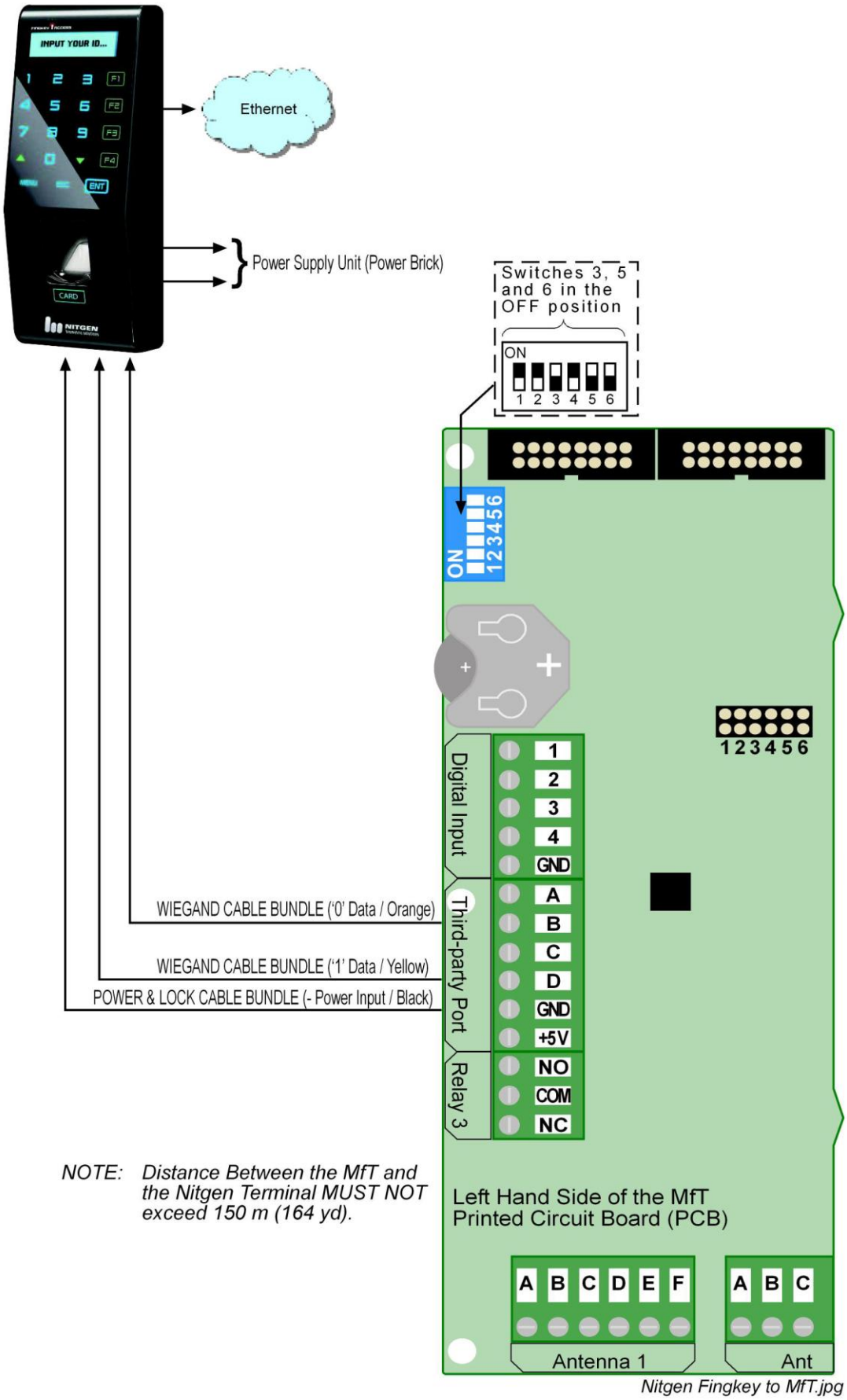
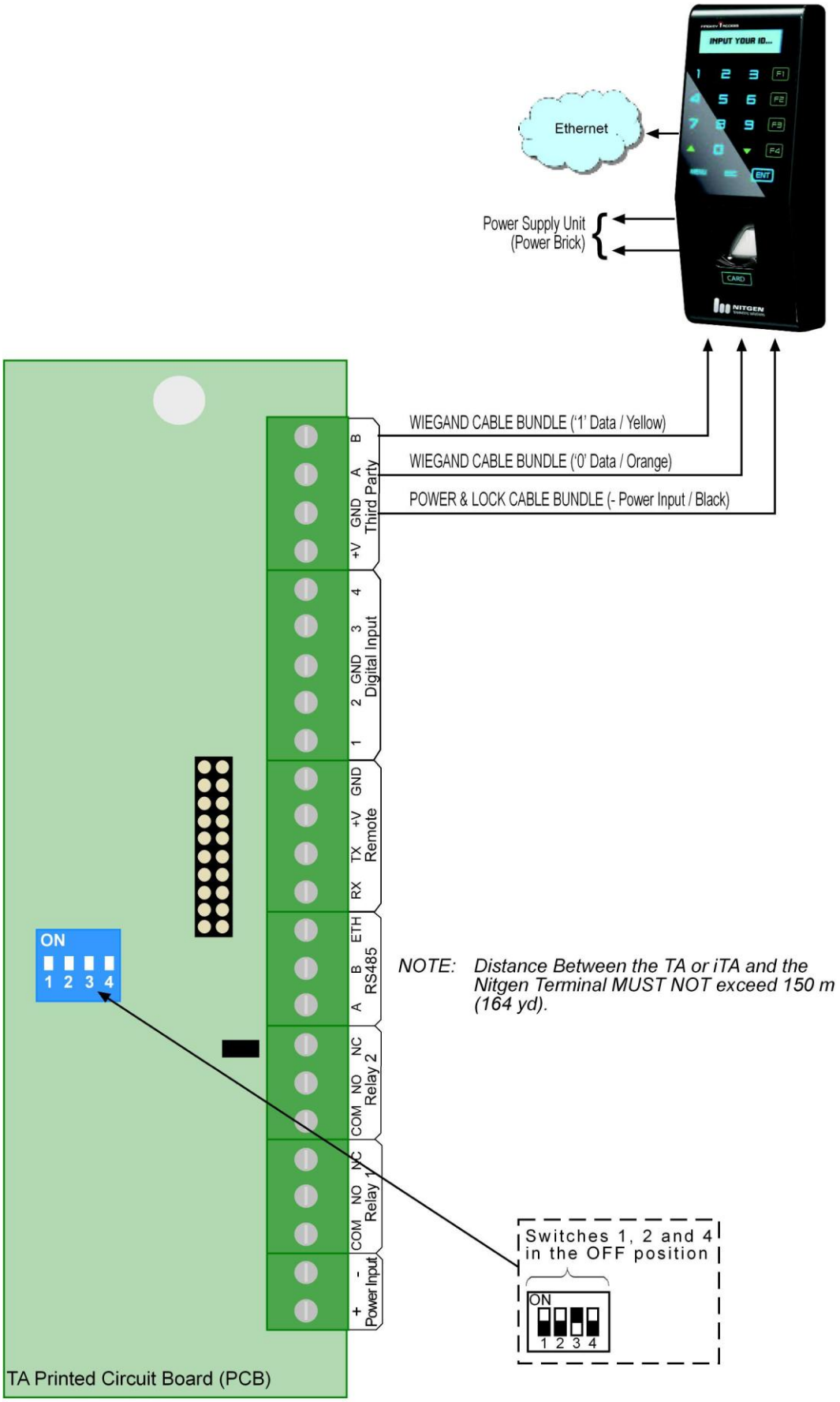
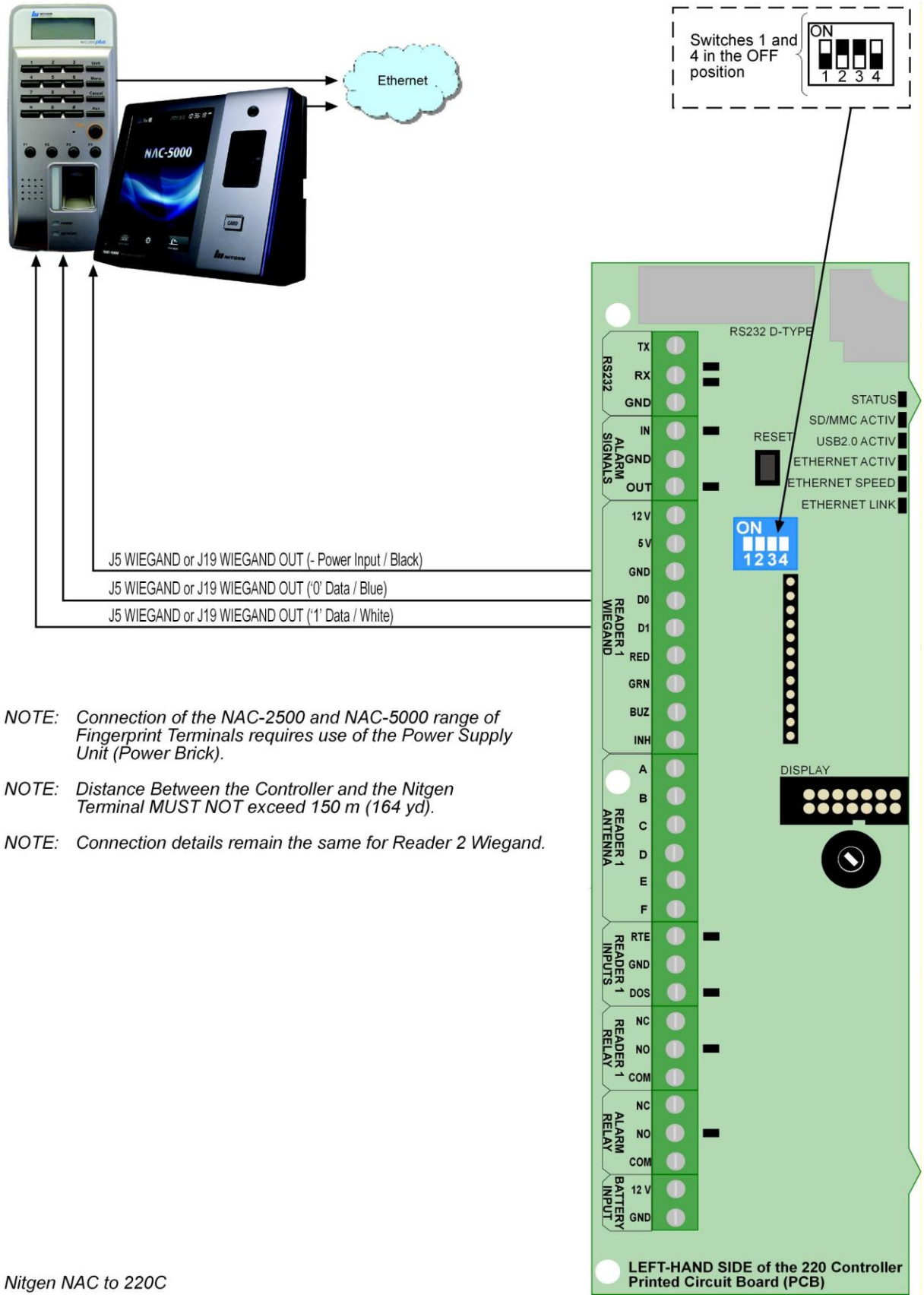


Figure 34 – NITGEN Fingkey Terminal Connected to the ImproX MfT Terminal



Nitgen Fingkey to TA.jpg

Figure 35 – NITGEN Fingkey Terminal Connected to the ImproX TA Terminal



NOTE: Connection of the NAC-2500 and NAC-5000 range of Fingerprint Terminals requires use of the Power Supply Unit (Power Brick).

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

NOTE: Connection details remain the same for Reader 2 Wiegand.

Nitgen NAC to 220C

Figure 36 – NITGEN NAC-2500 or NAC-5000 Terminal Connected to the IXP220 Controller

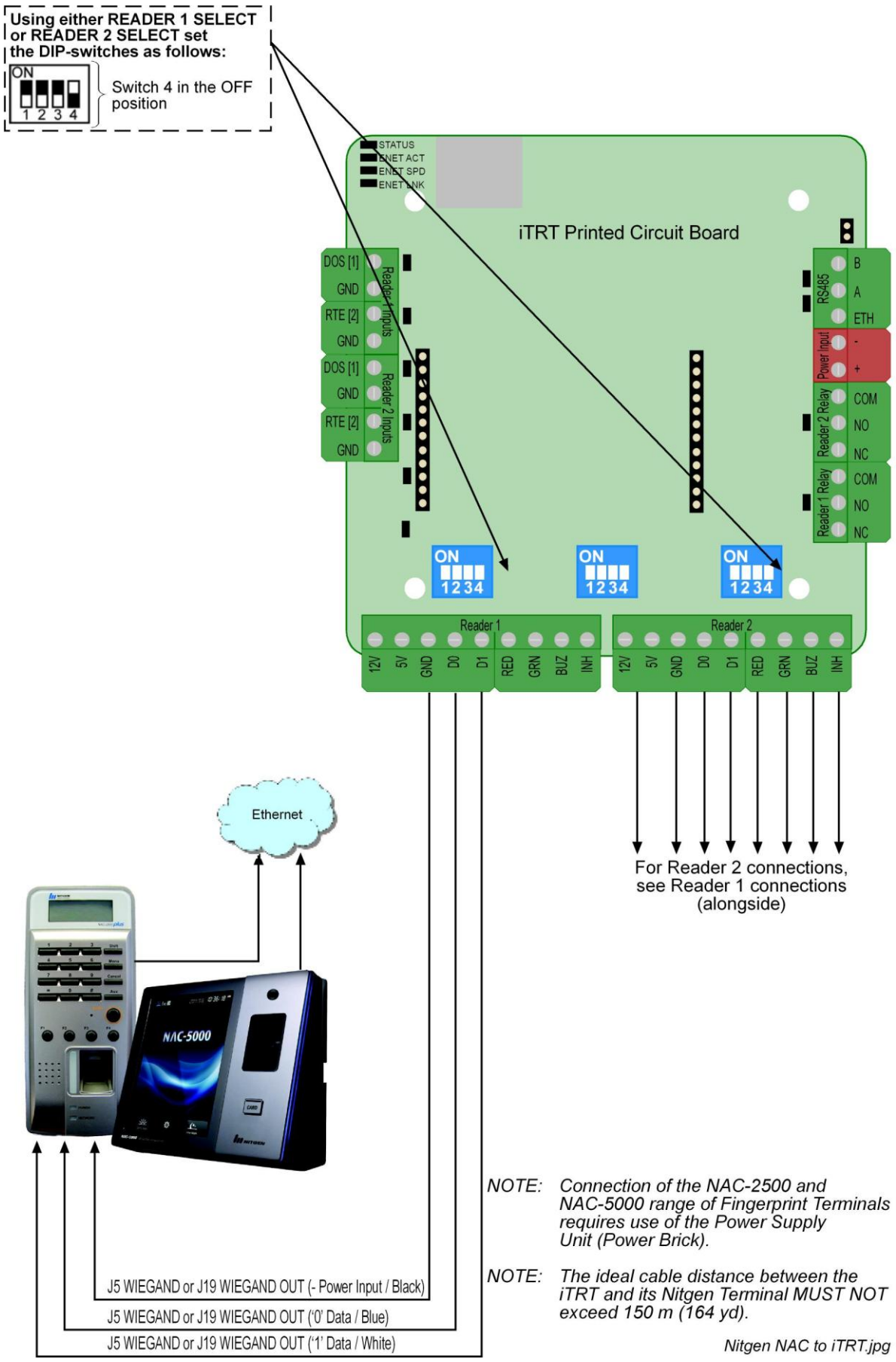


Figure 37 – NITGEN NAC-2500 or NAC-5000 Terminal Connected to the ImproX iTRT Terminal

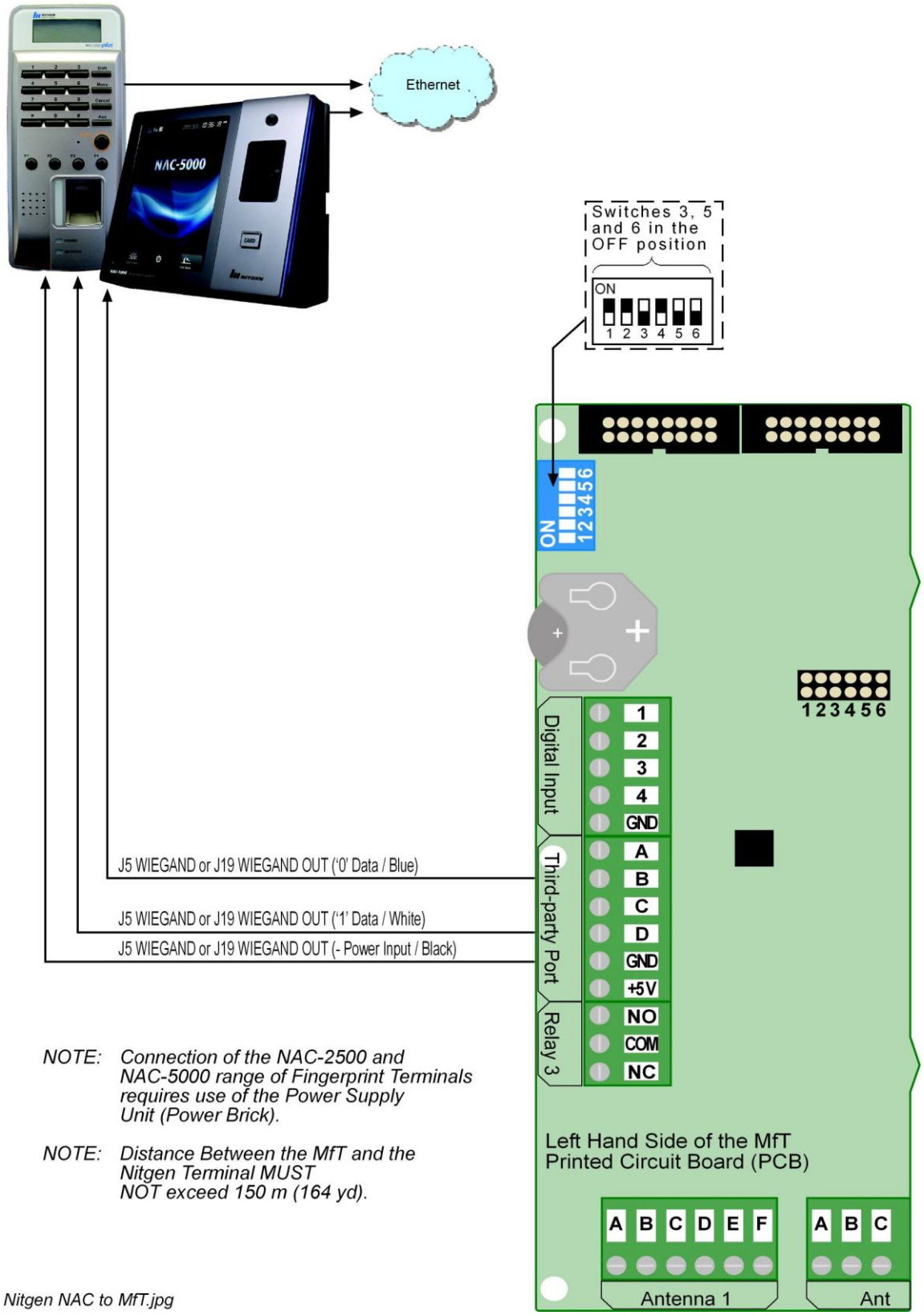


Figure 38 – NITGEN NAC-2500 or NAC-5000 Terminal Connected to the ImproX MfT Terminal

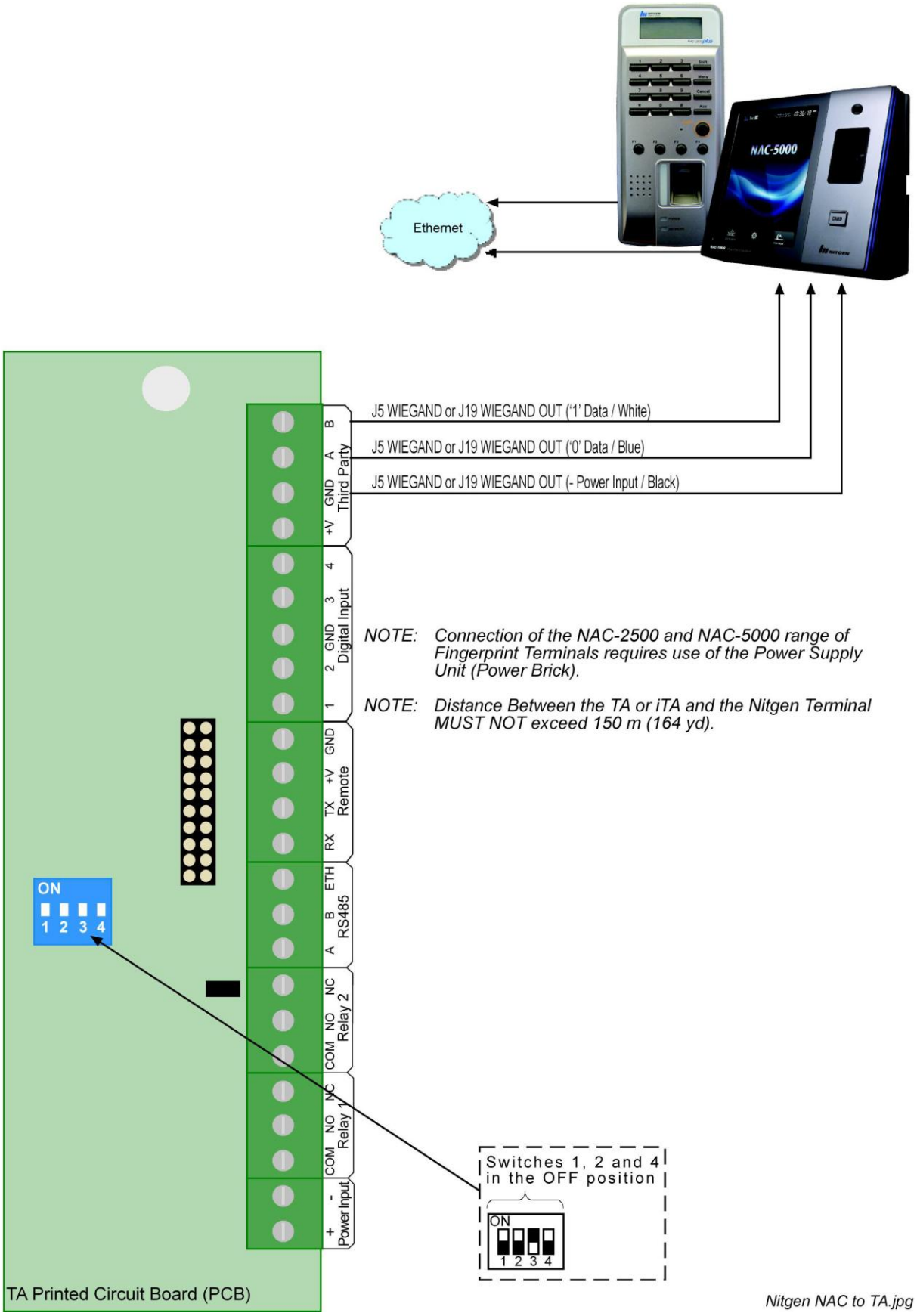


Figure 39 – NITGEN NAC-2500 or NAC-5000 Terminal Connected to the ImproX TA Terminal

Connecting the NITGEN Fingerprint Enrollment Reader

1. Browse to **C:\IXP220\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 Install Shield 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. Press the **ENT** (**Enter**) button.
8. Set the **IP Address** by selecting menu option **2**.
9. Press the **ENT** (**Enter**) button.
10. Within the **TCP/IP** menu, select option **1** to **Use DHCP**.
11. Select the **ON** option.
12. Press the **ENT** (**Enter**) button.
13. Select option **5** to set the **Server IP**.
14. Press the **ENT** (**Enter**) button.
15. Enter the **IP Address** of the Host PC (running the Biometric Server Software).
16. Press the **ENT** (**Enter**) button.
17. Press the **ESC (Escape)** button.
18. 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 **Drivers** menu, select **Nitgen**. Thereafter on the **Configuration** menu, select **Nitgen**>**Properties** to change the **Port Number**.*

Using NITGEN Terminals within the IXP220 System

Once you've connected the NITGEN Terminals and configured them internally as described in the previous paragraphs, use the Terminals within the IXP220 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 70.

The configuration of these Terminals within IXP220 is done using the Biometric Server Software, as follows:

1. From Windows® select **Start**>**Programs**>**IXP220**>**IXP220**
2. Enter your **Username** (**SYSDBA**) and **Password** (**masterkey**).
3. From the **File** menu, select **Biometric Server**.

Detecting NITGEN Terminals on the TCP/IP Bus

1. From the **Drivers** 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. Close the IXP220 Software, by clicking the button.
9. From Windows® select **Start**>**Programs**>**IXP220**>**IXP220**.
10. Enter your **Username** (**SYSDBA**) and **Password** (**masterkey**).
11. From the **File** menu, select **Biometric Server**.
12. On the **Configuration** menu, select **Nitgen**>**Devices**.
13. 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**.*

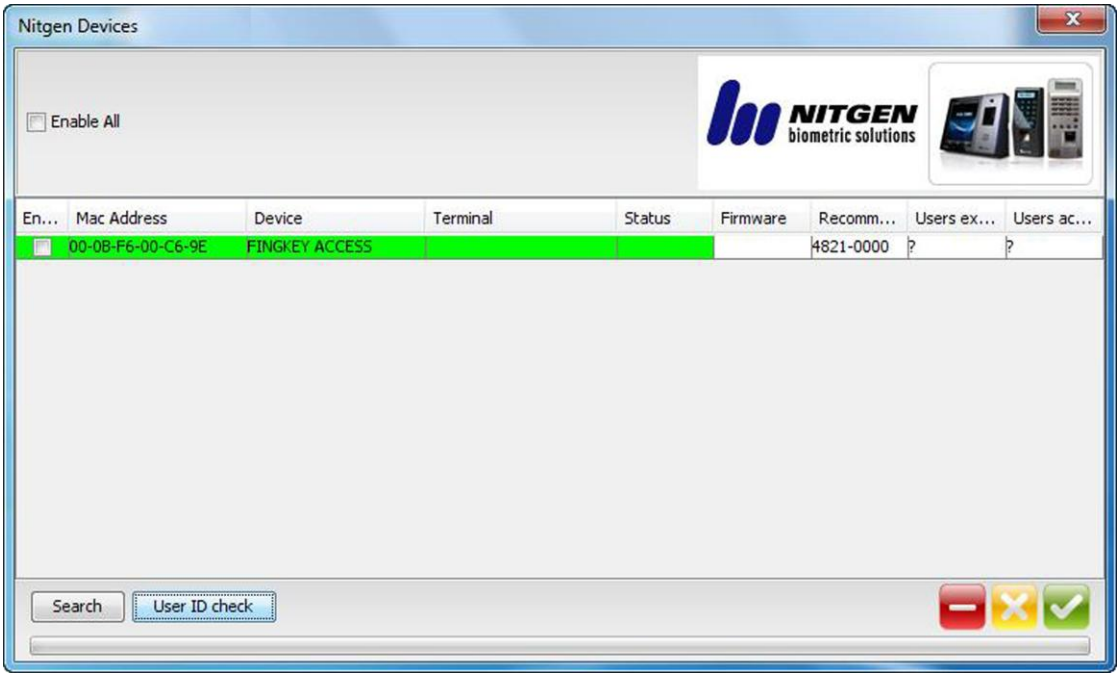


Figure 40 – NITGEN Devices Dialog

*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 the 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.*

14. Enable the NITGEN Fingerprint Terminals as required by selecting the associated Fingerprint Terminal's **Enabled** checkbox.
15. Click the button.
16. 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.

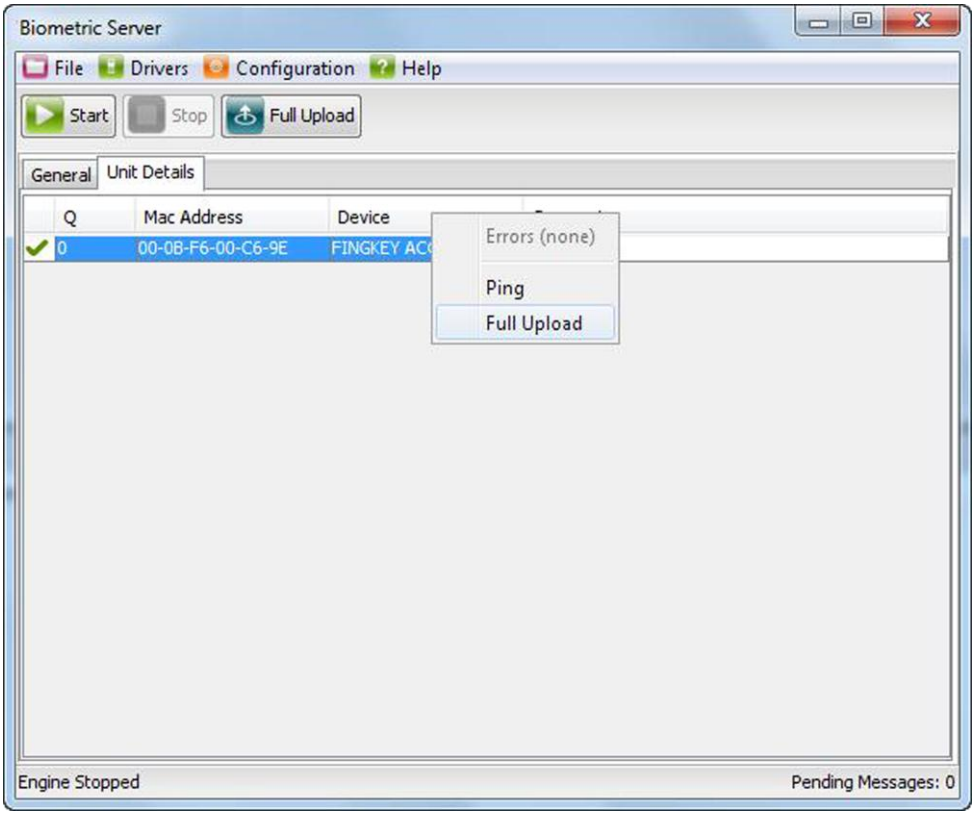


Figure 41 – Unit Details Tab

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 IXP220, with central enrollment taking place in the IXP220s 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**>**IXP220**>**IXP220**.
2. From the Main Menu, select **File**>**Preference**.
3. Select the **Enrollment** tab.
4. Alongside the **3rd Party (Other)** option, click the **Truncation** button.
5. From the **Tag Format** drop-down list, select the **Standard 16-bit** option.
6. Click the button.
7. Close the Preference Configuration dialog by clicking the button.

Tagholder Setup

1. Select the Page Tab.
2. Open a new or existing Tagholder record for editing.
3. In the Tagholder dialog, select the **Tag** Tab.
4. Click one of the assigned **Tag** buttons (that is **Tag 1**, **Tag 2**, **Tag 3** *or* **Tag 4**) or select one of the **Create New Tag** buttons.
5. From the **Configuration Level** group, select the **Advanced Configuration** radio button.
6. Have the Tagholder place their Tag on the Enrollment Reader.
7. Click the **Read Tag** button (or just enter a number of 7 digits or less in the Number field).
8. Set the **Access Rights** group options as you require.
9. Click the button.
10. Click on the **Biometric Enrollment** but

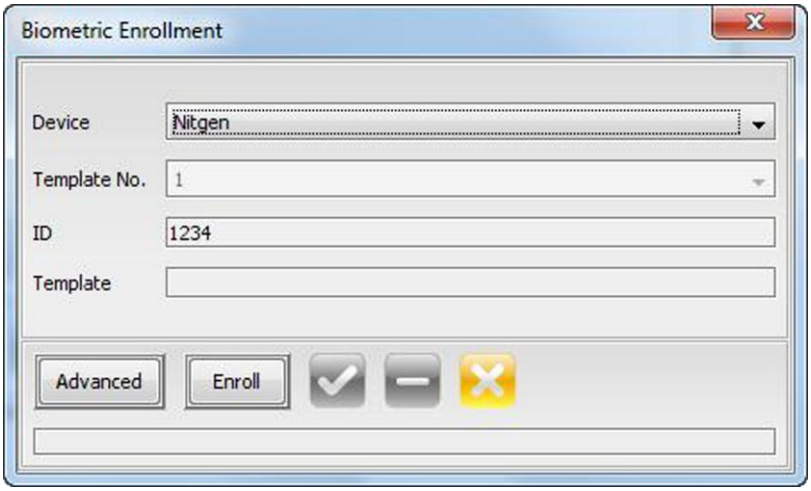


Figure 42 – Biometric Enrollment Dialog

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 **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.*

12. 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.

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

Fingerprint Placement Rules

Figure 43 shows the area of the fingerprint that contains the most information. Therefore, when enrolling Tagholders, ensure they place their fingers as shown in Figure 44.

Figure 43 – Area of the Fingerprint Containing the most Information

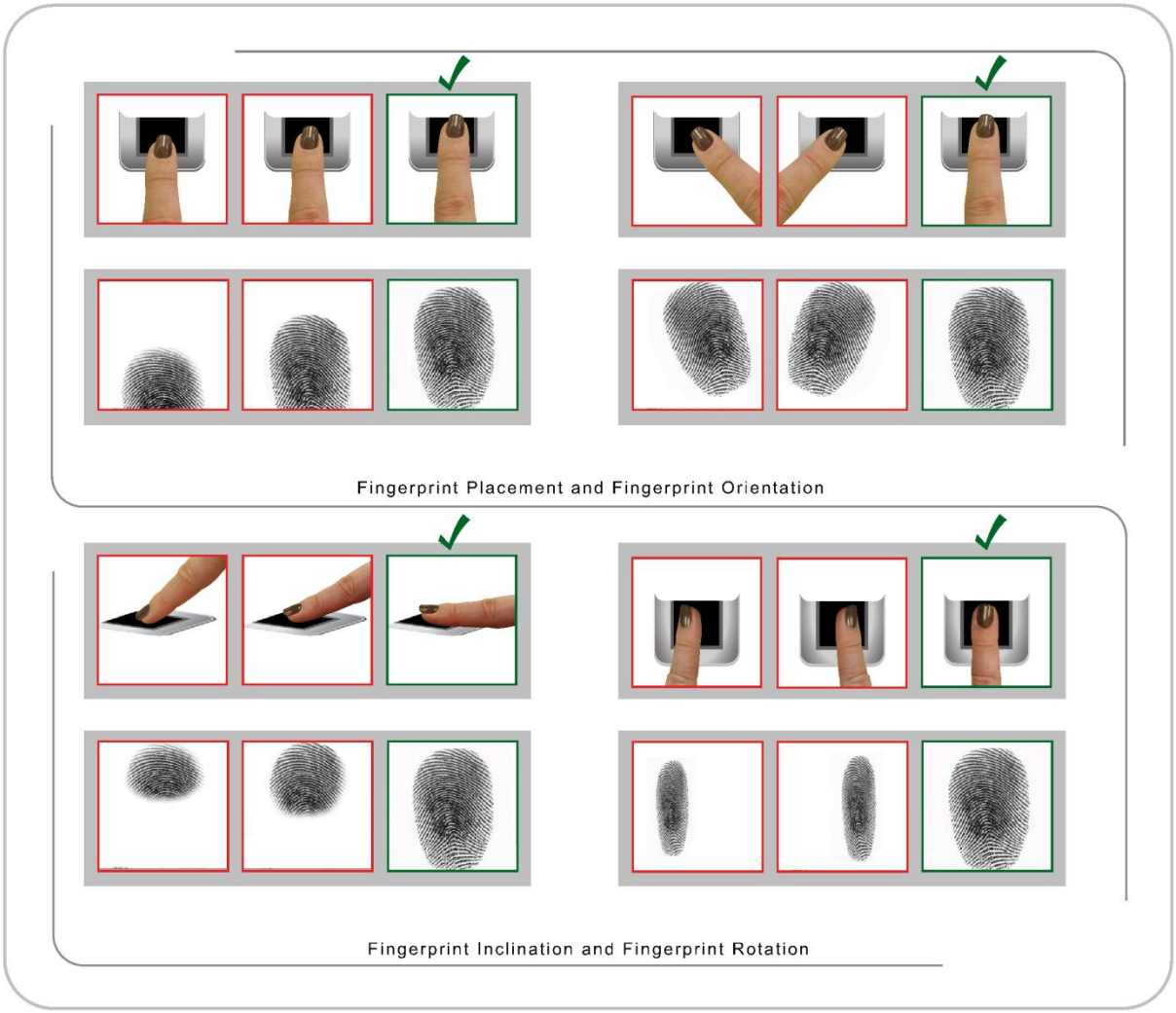


Figure 44 – Fingerprint Placement Rules (Generic Enrollment Reader, Fingerprint Sensor Shown)

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