PART VIII – INTEGRATION MODULES

Contents

PART VIII – INTEGRATION MODULES **1**

CONTENTS **3**

INTRODUCTION **5**

Biometric Readers 5

The Biometric Server Module 5

SAGEM READER USE IN AN NEXUS220 SYSTEM **6**

General 6

Principle of Operation 6

Hardware Installation of Sagem Readers 7

Electrical Connection of the Sagem Biometric Readers 7

Configuration Notes 7

Configuring the Biometric Enrollment Device 8

Sagem MA100, MA120 or MA500 Internal Parameter Setup Procedure 9

Sagem MA200 or MA300 Internal Parameter Setup Procedure 14

Nexus220 Configuration of Sagem Biometric Readers 17

Introduction

This part of the manual describes the Integration of other software/hardware systems with the Nexus 220 Software. These systems currently include various Sagem Fingerprint Readers, integrated with the Nexus 220 Software via the Biometric Server Software.

Biometric Readers

The introduction of biometric access control greatly increases the access control capabilities of Nexus 220 Systems where you need extra security measures. The Software supports several types of third-party supplied Biometric Readers (refer to Table 1 for details of these Readers). Biometric Readers not listed in Table 1 are not yet supported by the Biometric Server Software.

Biometric Reader	Biometric Server Software Support	Number of Users	Firmware Supported	Approved Terminals	Enrollment
MorphoAccess™ MA100	**YES**	500	2.07.09	See Note 3	Nexus 220
MorphoAccess™ MA120	**YES**	500 (see Note 1)	2.07.09	See Note 3	Nexus 220 (see Note 4)
MA200 Fingerprint Reader	**YES**	800	5.53	See Note 3	Nexus 220
MA220 Fingerprint Reader	**YES**	800 (see Note 1)	5.53	See Note 3	Nexus 220 (see Note 4)
MA300 Fingerprint Reader	**YES**	48 000 (see Note 2)	5.53	See Note 3	Nexus 220
MA500 Fingerprint Reader	**YES**	3 000 to 50 000	2.07.09	See Note 3	Nexus 220
MA520 Fingerprint Reader	**YES**	3 000 to 50 000 (see Note 1)	2.07.09	See Note 3	Nexus 220 (see Note 4)

Table 1 – Biometric Readers Supported by the Biometric Server Software

Note 1—Limited by the number of Tags supported by the Controller.
Note 2—Limited to 3 000 users per Database, with a maximum of 16 Databases supported.
Note 3—The Amano PT, Amano TA, Amano TRT and Amano MfT each offer a Third-party Port approved for use with the Biometric Reader.
Note 4—Enrollment is carried out in the Nexus 220 Base Application, using a MIFARE® Registration Reader and Tags.

The Biometric Server Module

This Module lets the System Administrator configure various third-party Biometric Readers for use with the Nexus 220 Software. The Module also allows for the direct enrollment (registration) of Tagholders and related biometric data at those Biometric Readers from within the Nexus 220 Software.

Sagem Reader Use in a Nexus 220 System

General

This section guides you step by step through the process of setting up Sagem Biometric Readers to work with the Nexus 220 System. The requirements for the integration are as follows:

- Nexus 220 Access Control System
- Nexus 220 System Software Installed
- Latest Sagem Integration Patch

There are five steps in configuring the Biometric Readers to work with the Nexus 220 System. These are:

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

Sagem enrollment is not supported when using the Windows® Vista operating system.

Sagem Documentation

Sagem documentation for these units can be found on the supplied Nexus 220 Installation CD. This information references the Sagem documentation where necessary.

Principle of Operation

Figure 1 shows the data flow when using a Sagem Reader with the Nexus 220 Software.

Figure 1 – Data Flow when using a Sagem Reader with the Nexus 220 Software

Hardware Installation of Sagem Readers

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

Each Sagem Reader must connect to the LAN to send and receive templates from the Nexus 220 Database. The Sagem Reader must also connect to an associated Nexus220 controller. Please install the Sagem Readers as outlined in the associated Sagem Hardware Installation Manual.

Electrical Connection of the Sagem Biometric Readers

Connection to the Nexus 220 Controller

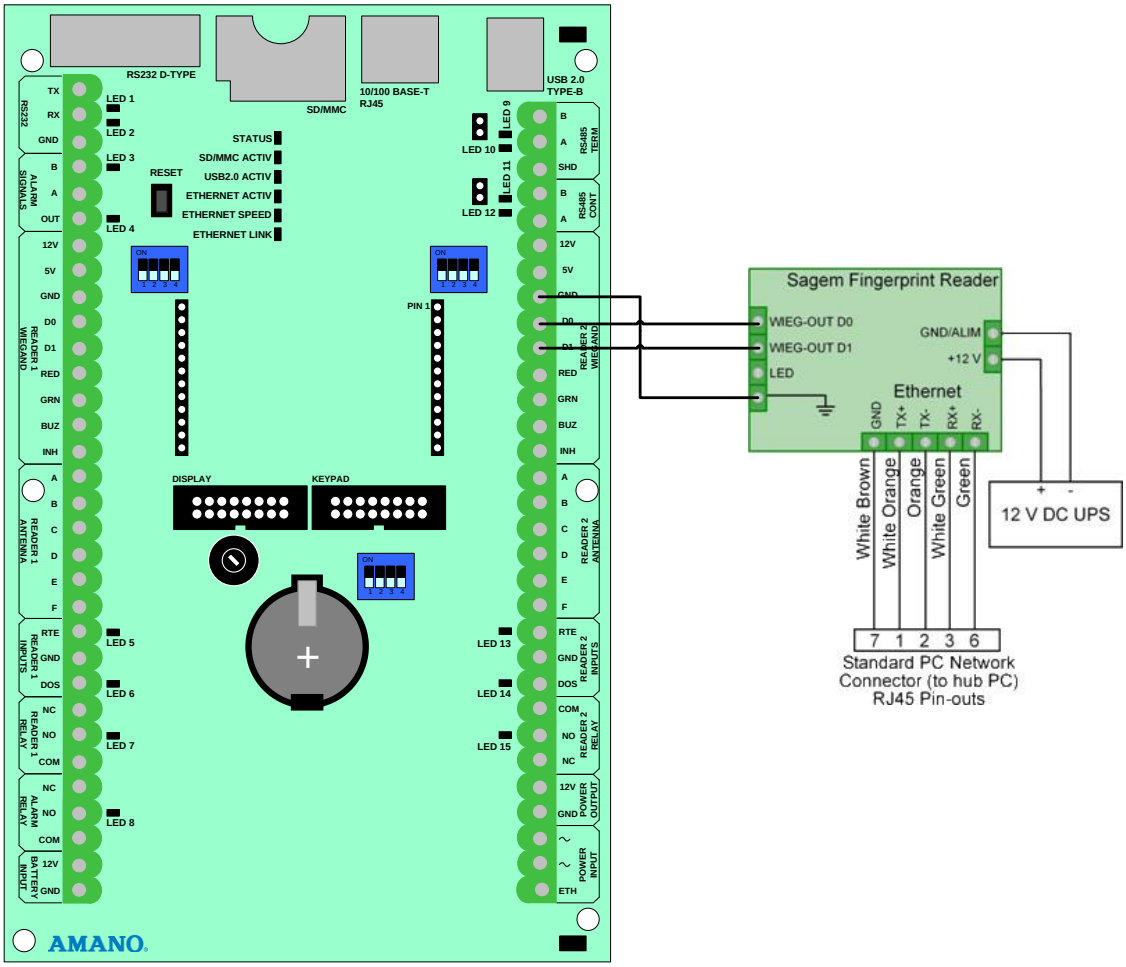


Figure 2 – Sagem Reader [MA100, MA200, MA300, MA500 or MA520] Connected to the Nexus 220 Controller and LAN

Configuration Notes

Before configuration into a Nexus 220 System, internally configure each Sagem Reader as described here.

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

Configuring the Biometric Enrollment Device

Ensure that you unlock your Registration Interface (Amano-Touch License) before proceeding further.

Sagem MA100, MA200, MA300, MA500 and MA520 Biometric IP Address Configuration

1. In Windows®, click **Start**>**All Programs**>**Nexus220**>**Nexus220**.
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 3 – 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 Nexus 220 Software, and will allow you to set up the enrollment units for each biometric device.

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

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

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

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

The MSO300 has no IP Address.

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

Continue with the IP Address configuration:

7. Click the button.
8. Click the button.

For MA100, MA120 or MA500 Biometric Readers, go to the section titled Sagem MA100, MA120 or MA500 Internal Parameter Setup Procedure see page 9.
For MA200 or MA300 Biometric Readers, go to the section titled Sagem MA200 or MA300 Internal Parameter Setup Procedure see page 12.

Sagem MA100, MA120 or MA500 Internal Parameter Setup Procedure

USB Flash Disk Setup

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

1. Format the Flash Disk in **FAT16**.
2. Assign the Flash Disk a name of no more than **12 characters**.
3. Browse to **C:\Nexus‡220\Driver\Tools\Sagem\USB Network Tools**.
4. Double-click on the **USBNetworkTool.exe** file.

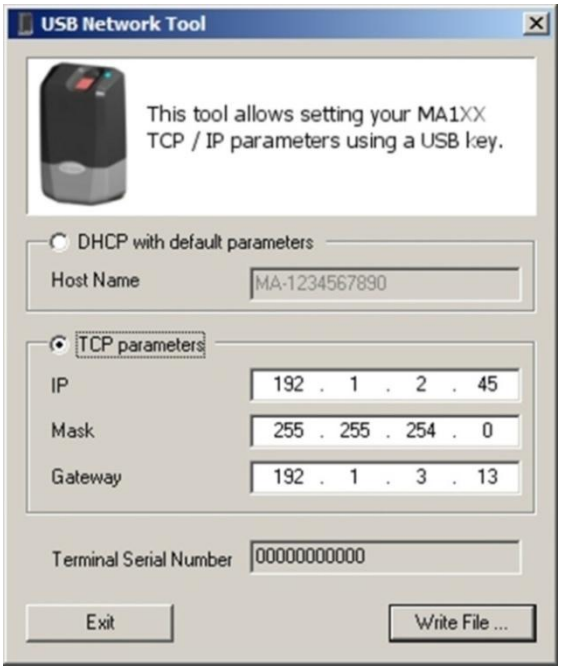


Figure 4 – USB Network Tool Dialog

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

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

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

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

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

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

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

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

Setting up the Wiegand Configuration on an MA100 or MA500

1. Browse to **C:\Nexus220\Driver\Tools\Sagem\Configuration Tool**.
2. Double-click on the **ConfigurationTool.exe** file.

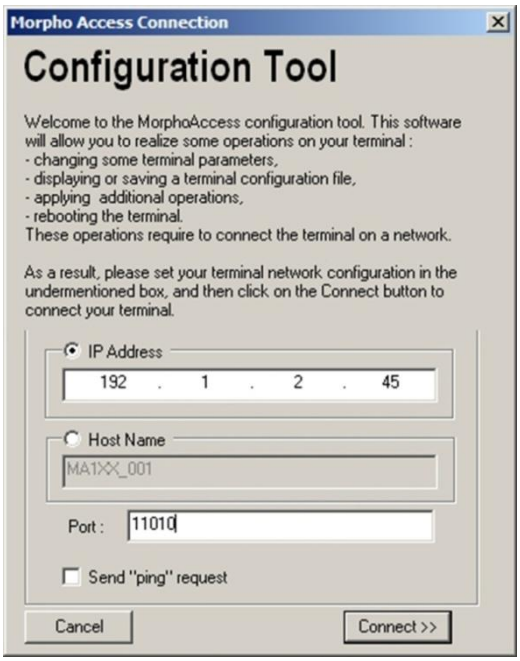


Figure 5 – Configuration Tool Dialog

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 10.
4. Click the **Connect >>** button.

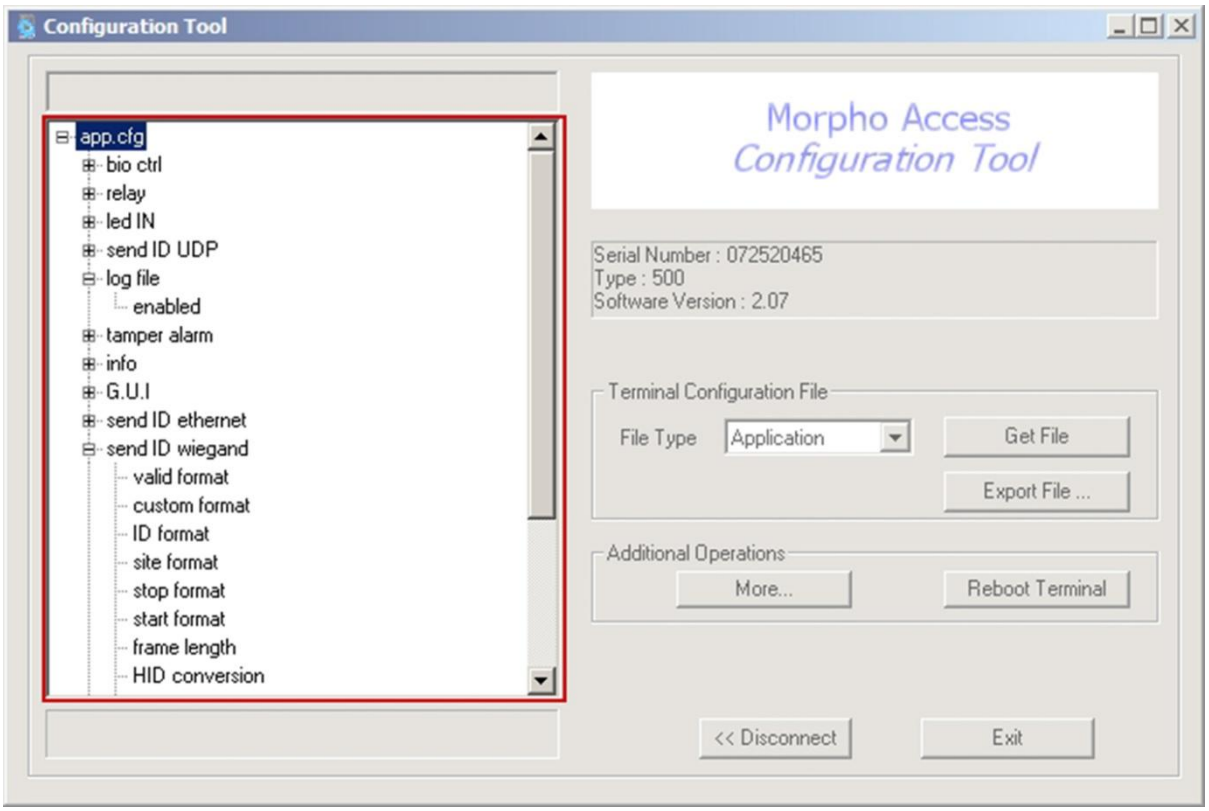


Figure 6 – Configuration Tool Dialog

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

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

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

Problems and Solutions

1. **Problem**—Wiegand Code not sent through.
   Solution 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:

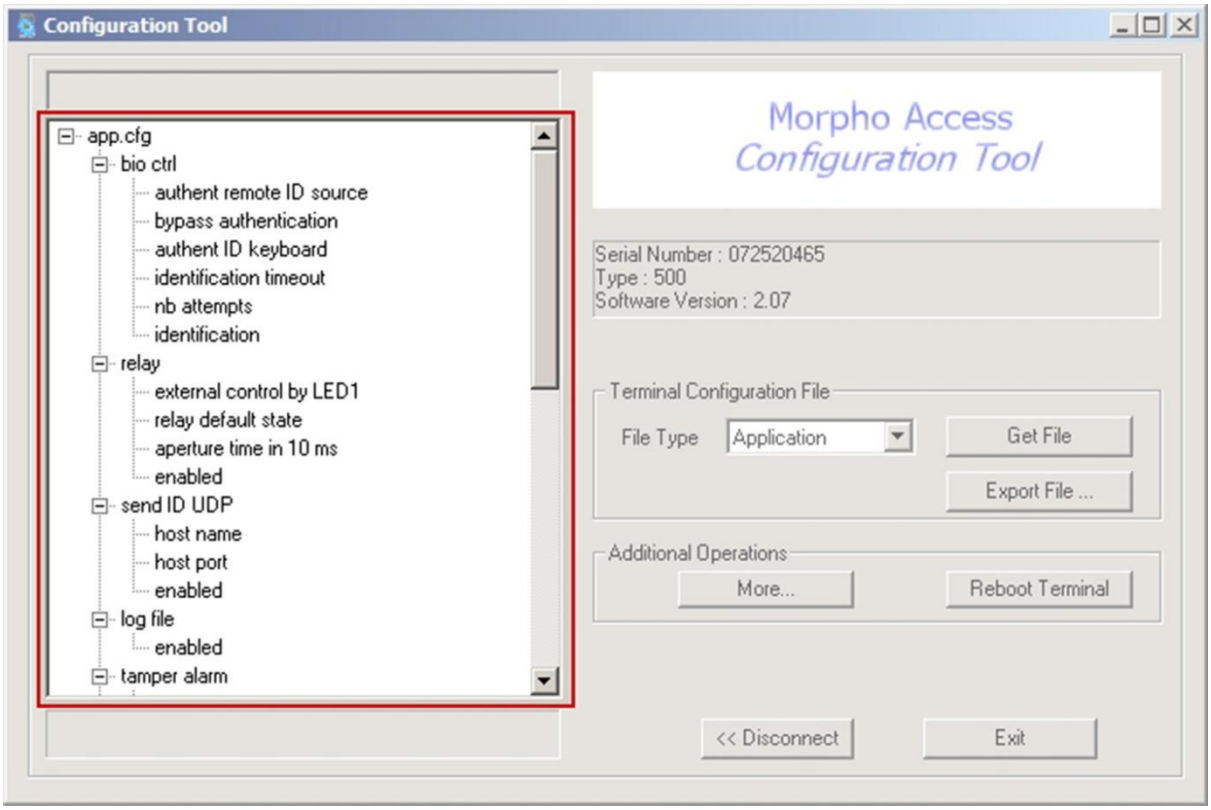


Figure 7 – Configuration Tool Dialog

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

- **tamper alarm**

  - interval—**1500**
  - level—**0**
- **G.U.I**
  - display hour—**0**
  - LED out signal—**0**
  - Time and attendance icons—**1**
  - database conversion—**500**
  - display user info—**2**
  - default language—**0**
  - volume—**5**
- **info**
  - type—**500**
  - release—**9**
  - minor—**7**
  - major—**2**
- **send ID ethernet**
  - connect timeout—**2000**
  - profile ID—**0**
  - SSL enabled—**0**
  - controller on no responce—**1**
  - timeout back to controller 1—**3600**
  - controller 2 timeout—**2000**
  - controller 2 port—**11020**
  - controller 2 IP—**134.1.2.189**
  - controller 1 timeout—**2000**
  - controller 1 port—**11020**
  - controller 1 IP—**134.1.2.189**
  - mode—**0**
- **send ID wiegand**
  - valid format—**1**
  - custom format—**0.0**
  - ID format—**1.24**
  - site format—**0.0**
  - stop format—**3.12**
  - start format—**2.12**
  - frame length—**26**
  - HID conversion—**0**
  - site code—**0**
  - enabled—**1**
- **send ID dataclock**
  - card present signal—**0**
  - data inverted—**0**
  - clock inverted—**0**
  - enabled—**0**
- **send ID serial**
  - display duration—**3**
  - reply timeout—**5**
  - wait reply—**0**
  - mode—**485**

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

Sagem MA200 or MA300 Internal Parameter Setup Procedure

General

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

Notes on Set-up for Sagem MA200 or MA300

The information that follows takes you through the Sagem Manual, indicating which information applies to the use of the Biometric Reader with the Nexus 220 Software, and which does not.

Internal Sagem Configuration Steps

The internal configuration steps of the MA200 or MA300 into the Nexus 220 System include:

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

Table 2 lists all headings in the Sagem manual, and indicates whether, and how, this information relates to the Sagem- Nexus 220 integration process.

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

STEP DESCRIPTION	SAGEM MANUAL HEADING	PROCEDURE OR COMMENTS
1. PHYSICAL INSTALLATION	INSTALLATION PROCEDURE	Follow the Sagem Manual procedures.
2. ELECTRICAL CONNECTION	ELECTRICAL INTERFACE	The Sagem Interfaces used in this application are J1, J3 and J4 (Refer to the Sagem Manual). See Figure 2, **Error! Reference source not found.** and **Error! Reference source not found.** in this manual.
	Terminal Block Board	Background Information
	Power Supply Cable	See Figure 2, **Error! Reference source not found.** and **Error! Reference source not found.** in this manual.
	Ethernet Wiring	See Figure 2, **Error! Reference source not found.** and **Error! Reference source not found.** in this manual.
	Wiegand Output Wiring	See Figure 2, **Error! Reference source not found.** and **Error! Reference source not found.** in this manual.
	Output Relays and Tamper Switch	Optional, depends on user requirements. Follow the instructions in the Sagem Manual if required.
	CONFIGURING THE MORPHOACCESS™	
	Motherboard Configuration	Refer to the Sagem Manual. Configure the Switches as follows: Set SW1 and SW2 for Wiegand Mode. Set SW3 and SW4 as indicated in the Sagem Manual. Set SW7 and SW8 for Wiegand Mode.
	MORPHOACCESS™ SOFTWARE	Refer to step 5 of this Table.

STEP DESCRIPTION	SAGEM MANUAL HEADING	PROCEDURE OR COMMENTS
3. INTERNAL SETUP OF THE READER BEFORE INTEGRATION AND USE WITH NEXUS 220	BIOMETRIC MANAGEMENT OPERATIONS	Refer to the Sagem Manual, "Access the Set up Functions of the System", but ignore the following headings: • Biometric Management in Stand Alone • Insert Template/ID in Database • Remove Template/ID from Database
	THE CONFIG MENU	Refer to the Sagem Manual.
	SETTING UP NETWORK PARAMETERS	Refer to the Sagem Manual.
	SETTING UP THE SYSTEM ADMINISTRATOR PIN	Refer to the Sagem Manual. This PIN provides access to the SYSTEM Menus in the Sagem Software for administration of the Reader.
	SETTING UP THE MORPHOACCESS™ ADMINISTRATOR PIN	Refer to the Sagem Manual. This PIN provides access to the MACCESS Menus in the Sagem Software for administration of the external management.
	Setting Up Host Communication	Refer to the Sagem Manual. Set the Host Com value to 3.
	Setting Up User Interface	Refer to the Sagem Manual.
	Setting Up Wiegand or Dataclock Output	Refer to the Sagem Manual.
	Setting Up Wiegand Interface	Refer to the Sagem Manual. The default format is 26-Bit.
	Frame Definition	Refer to the Sagem Manual.
	Configuration Keys	Refer to the Sagem Manual. Set Section is OUT. Set Length is 26.
	Setting Up Etherlink Parameters	Refer to the Sagem Manual. Set Etherlink Send is 1. Set IP Address as required.
	Setting Up Time Attendance	Refer to the Sagem Manual.
4. OPTIONAL SETUP AND BACKGROUND INFORMATION	THE VERSION MENU	Refer to the Sagem Manual.
	THE SERIAL NUMBER MENU	Refer to the Sagem Manual.
	THE SETTING MENU	Refer to the Sagem Manual.
	COMMUNICATION PROTOCOL	Background Information.
	MORPHOACCESS™ TECHNICAL CHARACTERISTICS	Background Information.
	Recommendations	Background Information.
	Ethernet Colour Standard	Background Information.
	Appendix 2	Background Information.
	Appendix 4	Background Information.
	APPENDIX 5 – FINGERPRINT PLACEMENT RULES	Refer to step 6 of this Table.

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

Table 2 – Internal Configuration of the Sagem Fingerprint Readers

*For easy reference we listed the Sagem Manual Headings in Table 2 in the order in which they appear in the Sagem Manual. Sections not listed in Table 2 are **NOT** required for Nexus 220 Integration.*

Nexus 220 Configuration of Sagem Biometric Readers

Once you've connected the Sagem Readers and configured them internally as described in the previous paragraphs, configure the Readers into the Nexus 220 System. This section applies to the supported Sagem Fingerprint Readers, the MA100, MA120, MA200, MA300, MA500 and MA520.

Each Sagem Reader used in the Biometric Server requires its own Unlock Token. For details of the unlocking procedure refer to the section titled Sagem Dongle Protection using the Unlock Token on page 20.

The configuration of these Readers within Nexus 220 is done using the Biometric Server Software, as follows:

From the Nexus 220 Software, select **File**>**Biometric Server**.

Detecting Sagem Readers on the TCP/IP Bus

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

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

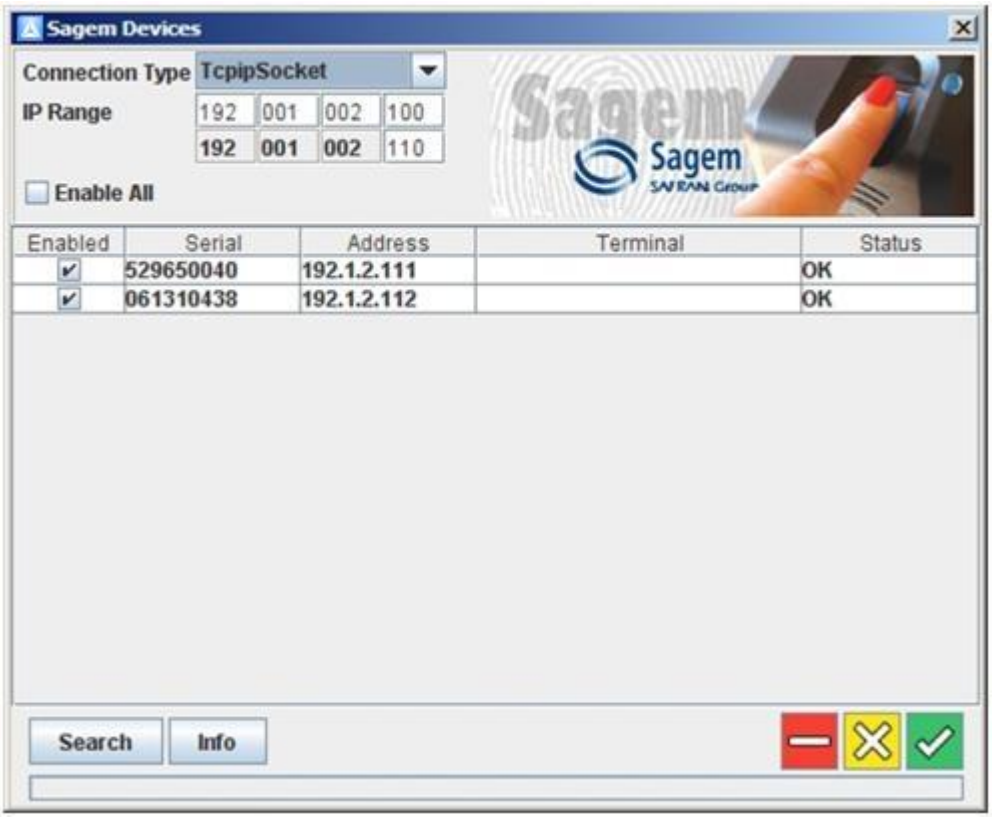


Figure 8 – Sagem Devices Dialog

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

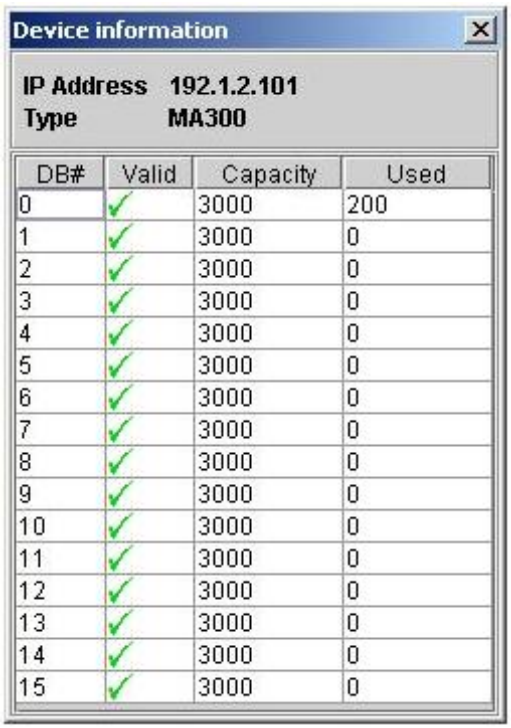
- *All newly discovered units highlight in **Green**.*
- *All units whose IP Address has changed highlight in **Orange**.*
- *All units that are in the Database but have been found to be off-line or missing highlight in **Red**.*

*The **Enabled** checkbox enables or disables each individual Sagem unit on the network. This means that you can carry out repairs on a unit without affecting the rest.*

*The **Enable / Disable All** checkbox enables or disables all the Sagem units on the network. The Server will not attempt communication with a disabled Sagem unit.*

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

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



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

Figure 9 – Device Information Dialog

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

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

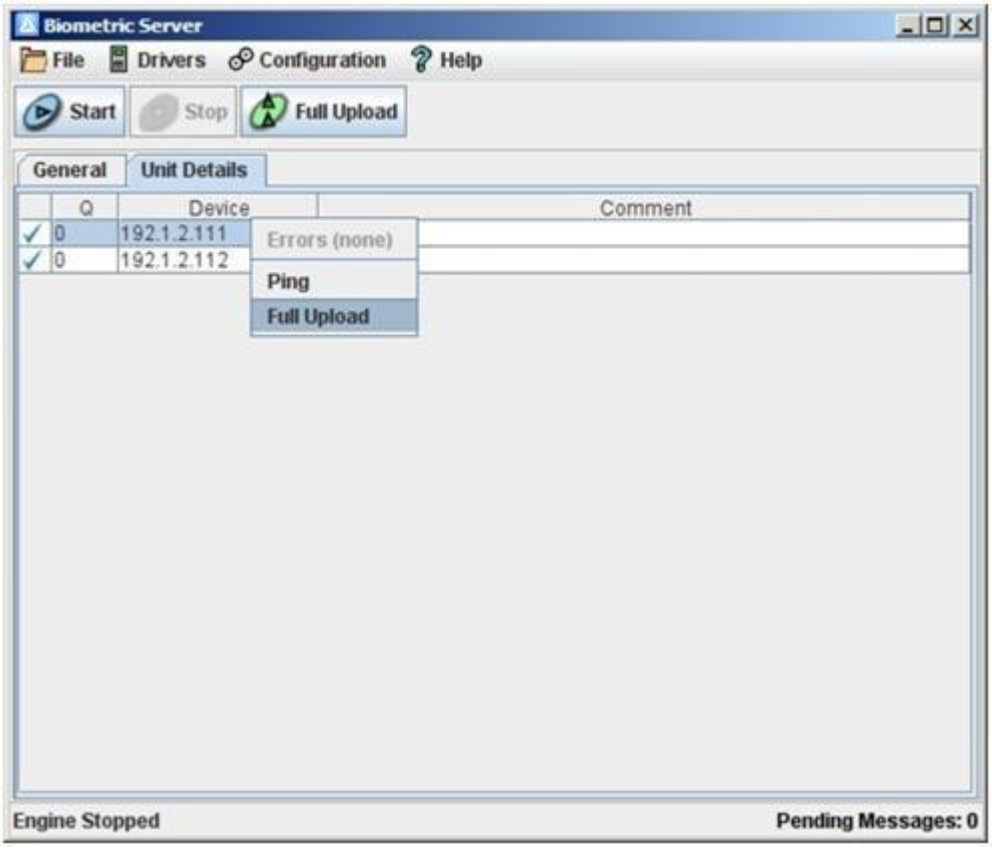


Figure 10 – Unit Details Tab

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

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

Duplicate Search (1:N Matching)

Using the Nexus 220 Software, the Biometric Server communicates with the Sagem Matcher service. This communication structure enables duplicate search functionality.

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

Installing the Service

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

In a default installation (from **C:\Nexus220\Driver)** run the **AddMatcherService.bat** script. After execution, enable the Matcher service using the standard Windows Services dialog.

Enabling the Service

Access the Services dialog using either of the following methods:

- Using **Windows® Vista**, access Services using the **Task Manager**.
- Using Windows® XP, access Services using: **Start**>**Control Panel**>**Administrative Tools**>**Services.**

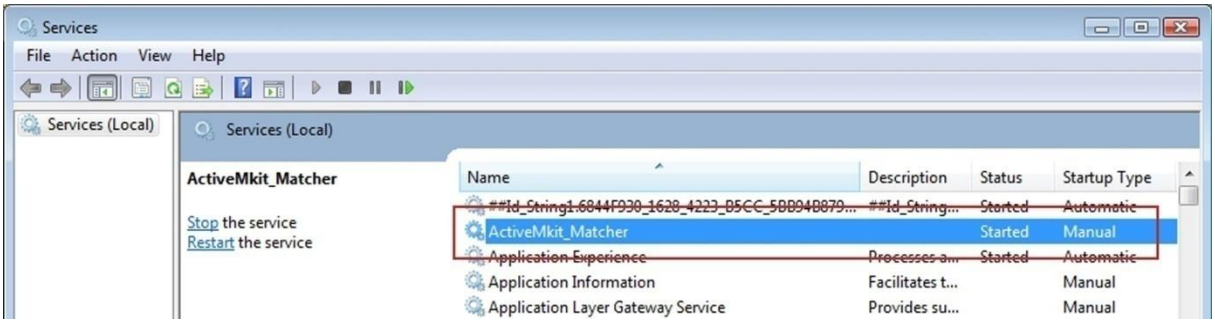


Figure 11 – Services Interface

1. From the Services dialog, select the **ActiveMkit_Matcher** service.
2. Right-click over the Service and from the shortcut menu, select **Properties**.
3. On the General tab, from the Startup Type drop-down list, select **Automatic**.

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

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

Enabling Matcher in the Biometric Server Software

1. Start the Biometric Server Software (for more information, see page 17).
2. From the menu bar, select **Configuration**>**Sagem**>**Matcher**.

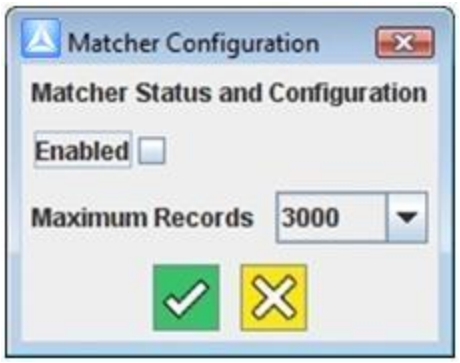


Figure 12 – Matcher Configuration Dialog

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

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

For an existing site, with templates already loaded, the Matcher 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 needs completion once. If you cancel the conversion process at any stage, the process halts and automatically continues from where stopped when you next run the Matcher service. All future templates are stored in the required format at enrollment stage.

Enabling Duplicate Search at an Enrollment Station

For detailed steps on arriving at the Biometric Enrollment dialog, refer to page 24.

1. In the Biometric Enrollment dialog, click the **Advanced** button.
2. Select the **Enable Duplicate Check** checkbox.
3. Click the button.
4. Restart the Nexus 220 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 records added to the Matcher Database. If the Matcher Service finds a matching record, an Error message gives you the matching records Tag code.

Sagem Dongle Protection using the Unlock Token

On initial use, ANY Unlock Token of the correct type unlocks ANY Sagem Reader of the same type. That is, any MA100 Unlock Token unlocks any MA100 Sagem Reader, and any MA200/300 Token unlocks any MA200, MA300, MA500 or MA520 Sagem Reader. However, once an Unlock Token is used with a specific Sagem Reader, the Unlock Token is permanently associated to that Reader. Ensure that you keep your supplied Unlock Tokens labelled and in a safe place.

The Unlock Token supplied with third-party integrated products, shows the products have our full factory level approval. This means the products work seamlessly with Nexus 220, with central enrollment taking place in the Nexus 220 Tagholder Enrollment screen.

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

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

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

1. Using the Nexus 220 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.

Installation of the MSO300 Enrollment Reader and Verification Dongle

These steps are normally, automatically, carried out during the Nexus 220 installation. However if for any reason you need to install the MSO300 Enrollment Reader and Verification Dongle manually continue as outlined on page 23.

The MSO300 is the preferred dedicated Enrollment Reader for desktop use. You may also configure the MA100, MA120, MA200 and MA300 for use as Enrollment Readers, however, remember that using these units could lead to uploading and quality (false rejection or acceptance) problems.

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

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

Upgrading from Earlier Version of Nexus 220 Software

When upgrading from an earlier software version, ensue that you carry out the following steps:

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

MSO Driver

1. Browse to **C:\Nexus220\driver\Sagem MorphoSmart USB Driver**.
2. Double-click the **setup.exe** file.
3. Follow the on-screen prompts.
4. At the end of the installation click the **Finish** button.

Verif Driver

1. Browse to **C:\Nexus220\driver\SafeNetDongle**.
2. Double-click the **SentinelProtectionInstaller.7.4.0(DriversOnly).exe** file.
3. Follow the on-screen prompts.
4. At the end of the installation click the **Finish** button.

Re-start your PC for the settings to take effect.

MSO300 Enrollment Reader

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

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

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

Verification Dongle

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

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

Enrolling Users on the System

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

From Windows® select **Start**>**All Programs**>**Nexus220**>**Nexus220**.

Preference Setup

1. From the Main Menu, select **File**>**Preference**.
2. Select the **Enrollment** Tab.
3. From the 3rd Party Tag and AnyTag, Tag Code Truncation group, select option **3** (**Convert Code to 26 bit Wiegand without Site Code (24 bits)**).
4. Click the button.

Enrollment in the Nexus 220 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.

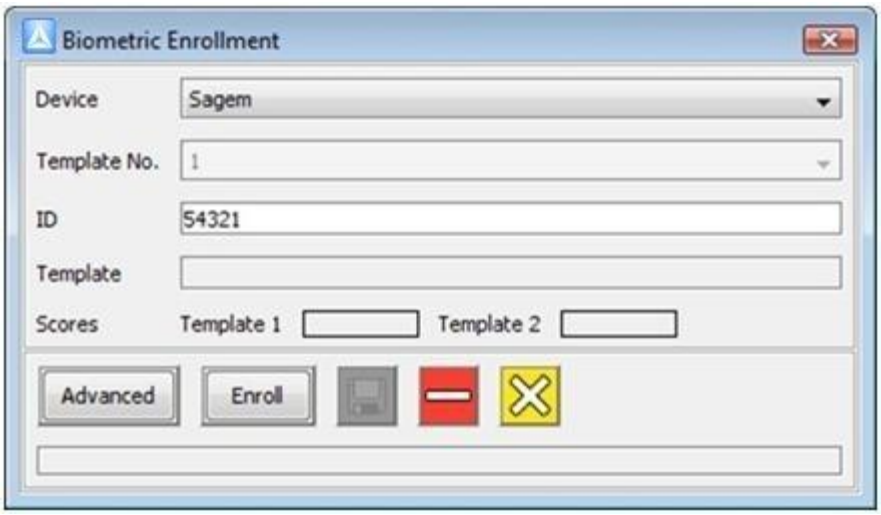


Figure 13 – Biometric Enrollment Dialog

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

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

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

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.
- **DB for this User**—the default MA300 or MA500 database to which this users templates are stored.
- **Quality Threshold**—determines the minimum quality score for each template. A higher threshold, leads to a better quality template.
- **Matching Threshold**—determines the minimum accepted matching threshold during the verification stage of each template capture. For standard applications, select 3 000, for secure applications, select 3 500 and for high-security applications, select 4 000.
- **Finger Detection**—when selected, the Acquisition Window dialog automatically detects finger presence, capturing the number of captures defined at each stage. If disabled, you must manually capture each fingerprint.
- **Number of Captures**—the number of automatic fingerprint captures to capture when finger detection is enabled.

- **Enable Duplicate Check**—when enabled, after template capture, the Nexus 220 Software searches for matches in the Matcher Database (located in the Biometric Server Software). Restart the Nexus 220 Base Application for this setting to take effect. For full functionality, ensure that you start the Biometric Server Software. Refer to the section Duplicate Search (1:N Matching) on page 20 for more information.

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

Fingerprint Placement Rules

Figure 14 shows the area of the fingerprint that contains the most information. Therefore, when enrolling Tagholders, ensure they place their fingers as shown in Figure 15.

Finger_Placemnt_01.jpg

Figure 14 – Area of the Fingerprint Containing the most Information

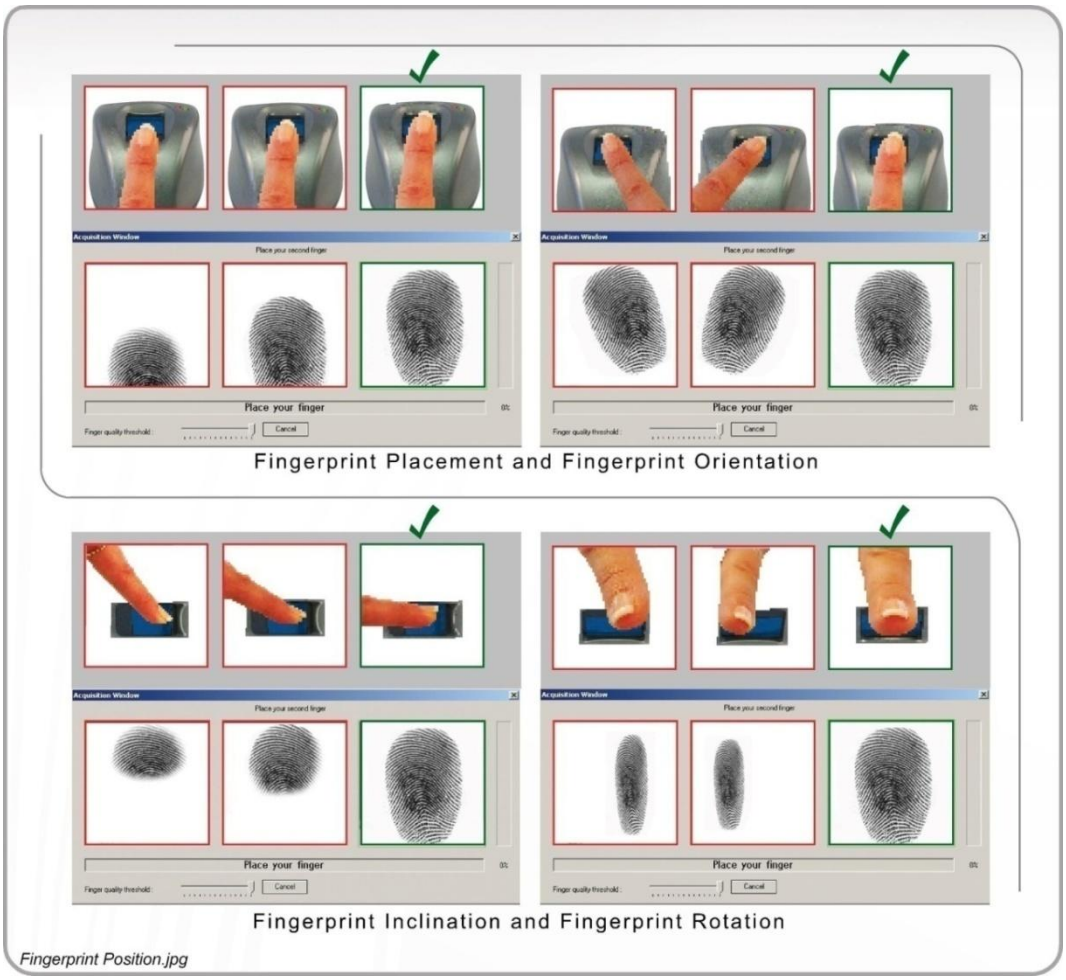


Figure 15 – Fingerprint Placement Rules

Enrollment procedure at the Sagem MSO300

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

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

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 Sagem Readers.

USER NOTES

USER NOTES

ANX102600	Issue 01	February 2009	