System Galaxy Quick Guide
CONFIGURATION AND OPERATION

SAGEM MA110 Biometric Integration
Authentication (1:1) HID iClass 16x16k Card Encoding,
Identification (1:N | Finger-Only) and Other Modes

GALAXY
CONTROL SYSTEMS

System Galaxy Biometric Guide

for Sagem MA110 & HID iClass Cards

Configuring SG to encode HID iClass Cards for use with Sagem MA110 Readers

first edition

Galaxy Control Systems

3 North Main Street

Walkersville MD 21793

301-845-6600

www.galaxysys.com

This document describes setup of System Galaxy to interface with Sagem Biometric MorphoAccess™ Terminals (MA110) using human fingerprint data and HID iClass Contactless Cards.

Information in this document is subject to change without notice. No claims are made, express or implied, as to the completeness or accuracy of this document.

Galaxy Control Systems supports installing and using the enrollment devices described herein on workstations running Windows XP Pro, or Vista Ultimate/Business. Windows Server operating systems are not supported for this enrollment interface.

This document does not intend to supersede any installation or operating requirements for products not manufactured by Galaxy Control Systems.

No claims are made, express or implied, about operating system compatibility or system requirements for 3rd party applications or devices.

Technical illustrations are creations of the technical author.

Revision 1.11 | 3-6-2009

Table of Contents

List of Tables and Figures

Preface

This manual describes the following;

GETTING STARTED

- System **Overview, Capabilities and Requirements**

- how to **plan your system** for MA110 and iClass contactless cards (13.56 MHz)

- how to **create a *single-card solution*** for Sagem MA110 and HID iClass readers, or other readers.

- how to **order iClass cards and enrollment equipment**

- how to **upgrade existing biometric customers**

- how to **import FGR templates** into SG8.2.4

HOW TO INSTALL and CONFIGURE MA110 and ENROLLMENT DEVICES

- how to **register System Galaxy** (SG) **for Biometrics**

- how to **install MA110 with Galaxy Hardware**

- how to **install enrollment devices and drivers**

HOW TO SET UP ADMINISTRATOR OPTIONS SYSTEM GALAXY

- how to **manage operator privileges** for biometric options

- how to **configure *card data format* and *card mode*** (behavior)

- how to **make the iClass card compatible*** **with HID iClass readers**

HOW TO CREATE CREDENTIALS IN SYSTEM GALAXY

- how to **enroll fingerprints** in System Galaxy

- how to **encode iClass cards** in System Galaxy

HOW TO CONFIGURE SAGEM READERS

- how to **set *recognition modes*** for the MA110

- how to **set output format and HID Conversion** option for the MA110

HOW TO MANAGE YOUR READER BASES AND USERS

- how to **load fingerprints** and cardholder data to the MA110

- how to **manage your Sagem reader BASES** using the GCS MALoader Utility

NOTE: See *Chapter 1* to order single-card or dual-card technology to support mixed readers along with the Sagem MA110.

NOTICES

IMPORTANT: It is important to understanding how credentials and modes work before setting up your system. The *Introduction* and *System Planning* chapters are designed to guide you through the following:

- overview of capabilities & requirements of using iClass cards with Sagem MA110
- determining which credentials you want to make (finger-only, iClass –prints on card, iClass prints in reader, iClass ID Only, pass-through, etc.)
- determining which reader *recognition modes* you want to use and how the credentials will behave in those modes (identification mode, card mode, prints in card, prints in reader, multifactor mode, etc.)

IMPORTANT! CARD TECHNOLOGY – 16k read/write iClass smart cards are compatible with the Sagem MA110. See ordering information in Chapter 1.

For customers who that have mixed readers and want a single-card solution, single-technology or dual-technology cards are available. The cards must be ordered with the correct information to support.

IMPORTANT! READER TECHNOLOGY – Sagem MA110 reader is compatible with iClass cards and reads the data encoded by System Galaxy on the application sector of the card.

In addition, the MA110 can be configured to use **HID Conversion** if the customer also uses HID iClass Readers. The iClass card must be programmed/encoded with the HID Compatible ID and site code to work with both readers at the same site.

IMPORTANT! CONFIGURING CARD MODES - The cards must be properly encoded with the correct card mode. It is important to determine your intended use of biometric credentials **before** you start making cards. *It is possible to encode cards in a way that is not compatible with a reader 'recognition mode', thus resulting in undesired behavior.*

IMPORTANT! CONFIGURING READER MODES - The MA110 *Recognition Mode* must be set properly to work with your credentials. *It is possible to configure the 'recognition mode' in a way that results in undesired behavior.*

WARNING! It is possible to customize your reader's *recognition mode*. Doing this can change how your credentials work and can result in undesired behavior. If your credentials work differently or stop working, you need to correct the reader settings to work with your credentials.

This manual describes the configurations that Galaxy considers the most logical solution. *Some combinations may conflict and thus may not be valid.*

IMPORTANT: Galaxy Control Systems supports installing and using the enrollment devices described herein on workstations running Windows XP Pro, or Vista Ultimate and Business. Windows Server operating systems are not supported for this enrollment interface. No claims are made, express or implied, about operating system compatibility or system requirements for 3rd party applications and devices

List of System Galaxy Manuals

System Galaxy manuals are found on disk2 of the Galaxy Software Installation CD and the Galaxy website (dealer password is required).

SG Hardware Manuals:

600-series Hardware Install Manual - covers installation and configuration of 600-series controllers.

600-series Configuration Tool Guide - covers installation / operation of the hardware programming tool.

508i-series Hardware Addendum - covers installation and configuration of 600-series controllers.

508i-series Blue Board System Planning - covers CPU install/replacement using 508i Blue CPU's.

SG Software Manuals:

System Galaxy Software Installation Guide - covers installing the SG software from the Galaxy CD.

System Galaxy Software User Manual - covers SG system programming and functionality.

SG Biometric Addendums:

System Galaxy Biometrics Guide for Sagem MA110 using HID iClass Cards

System Galaxy Biometrics Guide for Sagem MA520 using MIFARE Cards (this manual)

NOTE: Sagem manuals are also located on the System Galaxy installation CD.

Galaxy Control Systems promotes *GREEN* documentation practices!

We encourage saving trees by making all manuals available in electronic format. Manuals are designed to be easy to read and use in electronic form. Our PDF manuals provide bookmarks allow users to navigate right to the topic page.

Our manuals are designed to minimize the impact on the environment by reducing the number of pages. Composite illustrations are used to condense several screens and steps into one picture/page. Space-saving typeface and line spaces are used. Dispensable book parts like end-sheets are eliminated. Necessary front matter is condensed. Graphics are designed to look good in low-res color PDF/HTML as well as black/white printers.

Please print responsibly. Use duplex (2-sided) printing and recycle.

---

1 Introduction: Capabilities and Requirements

System Galaxy provides a **single-card solution** for using **HID iClass smart cards** *(13.56 MHz / 16k)* with mixed-reader systems (Sagem/iClass). This means an employee can have one card that will work at both readers (Sagem MA110 Biometric /HID iClass). *Proper programming of cards, access rules, and reader modes is required.*

1.1 Overview of Hardware Interface

SG SOFTWARE: System Galaxy 8.2.4 is compatible with…

- **Sagem MA110 Biometric Reader/Terminal** (indoor) for fingerprint identification and iClass card authentication. (500 users – 1 base)

- **HID iClass read/write contactless cards** – supports reading and encoding card data and fingerprints onto the application sector of the card.

- **Sagem MSO-300 fingerprint enrollment** station.

    See Section 1.2 for part numbers of compatible iClass cards and enrollment devices.

SG HARDWARE: System Galaxy 600-series and 508i-series access control panels are compatible with the System Galaxy 8.2.4. As always, you must operate the panels with the version of S28 flash that comes with the System Galaxy 8.2.4 software CD.

Table 1: System Galaxy Biometric Capabilities Compared

Sagem MA110 90-9110-05	Fingerprint Encoding	Card ID Encoding Contactless Card	PIN Code	BIOPIN (accessibility)
	Yes*	iClass 16k	*no keypad*	*no keypad***

* Supports Identification (1:N) and Authentication (1:1)

** If a person(s) has 'unscanable' prints, you can use an MA520 with MIFARE and BIOPIN or it is possible to use the MA110 in 'Card Determines Mode' and provide specific users with an ID Only iClass card (aka. visitor mode).

Sagem MA520/521	Fingerprint Encoding	Card ID Encoding Contactless Card	PIN Code	BIOPIN (accessibility)
	Yes*	MIFARE	YES	YES
Sagem MA120	Yes*	MIFARE	*no keypad*	*no keypad***

NOTE: *SG 8.2.4 still supports prior capabilities with MA200/300 models, but these readers must be manually programmed, whereas the MALoader is used to program the MA00 and 500 Terminals.*

NOTE: see the _SG Biometric Guide for MA520 & MIFARE_ for information on integrating with MIFARE.

1.2 Overview of System Features & Capabilities

1.2.1   Encode iClass cards to work with Sagem 110 and HID iClass Readers

System Galaxy allows the customer to choose which **card output format** to use.

- System Galaxy encodes an **HID Compatible ID** and **HID Site Code** onto the iClass card, which makes it work at any MA110 and any iClass reader (recommended).

- Galaxy can also encode ABA formats for custom solutions. Contact **Galaxy Control Systems Technical Support** for more information.

1.2.1.1   Ordering ~ Part Numbers for Compatible iClass cards

Table 2: Compatible iClass Cards

IMPORTANT! There are important requirements for ordering HID iClass smart cards. The following Galaxy Control Systems part numbers are provided for ordering iClass Cards that are compatible with Sagem MA110 and HID readers.		
HID iClass Card – for iClass/MA110 readers		(*SG uses 1 application area*)
95-2001-00	iClass 13MHz card	16k with 2 application areas
95-2002-00	iClass 13MHz card	16k with 16 application areas
HID iClass / Prox Card – for iClass/Prox/MA110 readers		
95-2021-00	iClass 13MHz / 125 kHz card	16k with 2 application areas
95-2022-00	iClass 13MHz / 125 kHz card	16k with 16 application areas
Galaxy Customer Service for information ordering cards for other types of reader technologies not listed here.		

1.2.2   Enroll and Encode Fingerprints onto iClass cards

System Galaxy allows customer to choose where **fingerprint templates** are stored.

- Galaxy can encode fingerprint templates onto the iClass card, or can load fingerprint templates into the reader (based on card mode). It is possible to have a mixture of credentials using prints-only, or cards with prints in reader, or prints on cards, or any combination.

- Fingerprint templates are also saved in the System Galaxy database in 8.2.4 (or later). For customers who are upgrading, see the upgrade section in this manual.

1.2.2.1   Ordering ~ Part Numbers for Finger Enrollment and Card Writer devices

Table 3: Compatible Finger Enrollment / Card Writer devices

Fingerprint Enrollment and Encoding devices		
**	MSO 300	Sagem Finger Enrollment station
**	iClass encoder	card read/writer device

Contact **Galaxy Control Systems Technical Support for more information.

1.2.3   Configurable Sagem 'Card Modes' in System Galaxy

System Galaxy encodes **card modes** on iClass cards**.** The *card mode* is read by the Sagem reader. The **card mode** dictates how the credential will be handled based on the *recognition mode* set at the reader.

Card Mode / Behavior

- **ID Only** = prints not on card; prints could be in the MA110 if they are captured and loaded in SG.
- **Biometric** = prints are on the card.

NOTE: *See* more on the *Card Modes* and how they behave in specific recognition modes in Planning Chapter of this manual.

1.2.4   Predefined 'Recognition Modes' for Sagem MA110 in System Galaxy

A **recognition mode** is a specific combination of Sagem *biometric control options* that are configured in the MA110.

Recognition Modes

Pre-defined Recognition modes: Galaxy provides seven pre-defined 'recognition modes'. These are the most commonly needed configurations. The list includes modes for Finger Identification, Card ID Only, Multi-factor mode, Card Mode and Card Pass-through.

Sagem's *Visitor Mode***:** This is supported by the "iClass - Card Determines Mode" (i.e. Card Mode). It allows the MA110 to read both card behaviors at one reader (i.e. the 'biometric cards' and 'ID Only cards') in the case where you will fingerprint employees and not visitors.

Customizing modes: It is possible to manually configure the MA110 to use a combination of options outside the pre-defined list. **WARNING:** Customization beyond the recommended solution could cause undesired results or security risks.

NOTE: *S*ee more on *Recognition Modes* and how each credential/card is treated in the Planning Chapter of this manual.

1.2.5   Manage Sagem Bases and Recognition Modes from System Galaxy

The Galaxy **GCS MA Loader** **utility** allows a customer to manage the Sagem readers individually.

Managing the bases and users/finger templates:

- User can **create and delete the MA110 base.**
- User can **delete all fingers** and **load fingerprint templates**

Managing the reader configuration:

- user can **set the *HID Conversion* option** at the reader (checked = on/enabled).
- user can **configure output format** at the MA110 (i.e. Wiegand, etc.)
- user can **set the *Recognition Mode*** of the MA110. Seven predefined recognition modes are provided (see the Planning chapter for more details).

1.3 System Overview & Diagram of Credentialing

1.3.1 Overview of Creating and Using Biometric Credentials

1. **Cardholder is enrolled** at the System Galaxy client workstation. Fingerprints are captured and associated with a card ID. The card is encoded.

2. **Cardholder data is sent/loaded to MA110** over an Ethernet connection. This is done when the credentials are saved* in System Galaxy or when loaded via the GCS MALoader utility.

3. **Cardholder presents credentials (finger/card).** Card and human finger are matched to the fingerprint template and the associated with the card ID**. User is identified/authenticated.

4. **MA110 outputs data to the Galaxy controller** for an access control decision. The cardholder is granted or denied access based on the programming of access rules/schedules at the panel.

5. **Access Control Event is logged** to the System Galaxy database and Event monitoring screen.

* The *Load Morpho* option must be checked and the *Loop and Access Privileges* must be assigned in order for the credentials to be sent to the MA110 when the cardholder record is saved.

** A valid card ID is created in SG even when cards are not issued (i.e. Fingerprint Identification mode). This is required so that access privileges can be controlled for the enrollee.

Figure 1 - System Galaxy Biometrics Interface – Enrollment & Access Control:
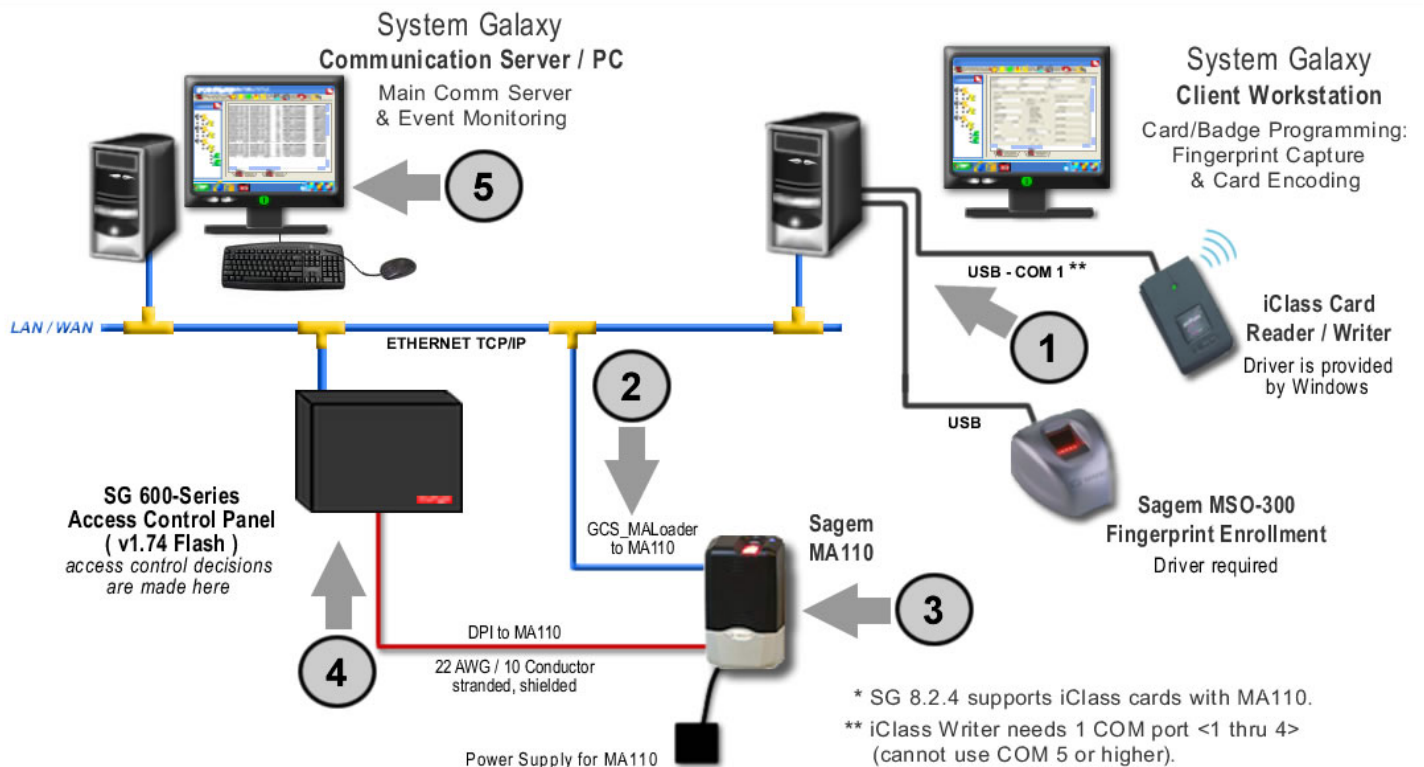
1.4 Requirements

1.4.1   System Galaxy Installation Requirements

1. System Galaxy software Installation/Upgrade must be completed (i.e. the main communication server, database, and client workstation(s)).

   For new installs:
   ‣ Programming of Loops, Schedules, & Access Rules should be completed before attempting cardholder enrollment. Refer to the installation instructions found on the install CD.

   For upgrades:
   ‣ **Always back-up .FGR files to a safe location <u>before</u> upgrading System Galaxy software.**
   ‣ If you must transfer .FGR files into the SysGal database. This is done using the GCS MALoader **after** the System Galaxy database and software upgrades are properly completed.
   ‣ A valid maintenance agreement is required to upgrade. See upgrading in Chapter 4.

2. System Galaxy must be registered for biometrics. SG must be restarted after registration.

1.4.2   Biometric Device Installation Requirements

1. The Sagem MA110 Reader must be installed and configured properly.
   ‣ The MA110 must be wired to the Dual Reader board (DPI) using 22 AWG, 10-conductor wiring, and stranded shielded cable.
   ‣ The MA110 must use a separate power supply.
   ‣ The MA110 must have a TCP/IP (LAN) connection to perform configuration and load the credentials (cardholders/fingerprints).
   ‣ The MA110 must have an IP address. A static IP address is recommended. Basic configuration is needed to get reader up and running.
   ‣ An initial hardware connection test should be done
   ‣ The *GCS MALoader utility* can be used to set up the card format and recognition mode, create bases, load fingerprints, etc.
   ‣ You must create bases before you can load finger data.
   ‣ You will need a USB thumb drive to set up the Network addressing on the MA110. Initial configuration is done using the *Sagem Configuration tool,* found on disk2 of the Galaxy CD.

2. You **must** uninstall the MSO100 driver. The MSO100 is not compatible with SG 8.2.4 since it is not currently supported by the Sagem SDK used to create the new interface.

3. The MSO-300 Fingerprint Capture device must be installed, including the driver, if the customer will be capturing fingerprints. See section 3.2 for details.

4. The Card Writer device must be installed, if the customer will be encoding iClass cards. The Card Writer uses a Windows default driver. See important details in section 3.3.

> **IMPORTANT:** Galaxy Control Systems supports installing and using the enrollment devices described herein on workstations running Windows XP Pro, or Vista Ultimate and Business. Windows Server operating systems are not supported for this enrollment interface.

1.4.3   Card Encoding Requirements and Recommendations

1. CARD TECHNOLOGY MA110 is compatible with HID iClass 16k contactless cards (13.56 MHz).

IMPORTANT: You must set the MA110's *Recognition Mode* to be compatible with the way you are encoding and using the cards. See **Table 5** in section 2.4.

IMPORTANT: You must set the MA110 *Output Format* to match the *Card Code Format* you use on the card (i.e. 26-bit Wiegand or Data-Clock/ABA)

2. CARD ENCODING: You should configure the Administrative Setup Options for Capture/Encoding to ensure cards are created correctly and consistently. See Chapter 4.

3. If you want fingerprints on the card, you should choose Card Behavior = "**Biometric**" or "**Pin Code + Biometric**" before you [write data to card] in the Capture/Encode Card screen.

4. If you do not want fingerprints on the card, you should choose Card Behavior = "**ID Only**" or "**Pin Code**" before you [write data to card] in the Capture/Encode Card screen and do not capture fingerprints.

5. If you want to use the HID Compatible ID and Site Code, you must do the following:
  - In the Setup Options screen, choose Card Format = "Wiegand" and How Card ID is Generated = "Use HID Compatible value". (See chapter 2 for other formats)
  - You set the HID Conversion option to "1" and format to Wiegand in the MA110.

6. LOADING USERS: Users must be loaded into the MA110 based on how you are using the cards.

NOTE: users are sent to readers when cardholder data is saved in System Galaxy, only if the loop/access privileges are assigned and the 'Load Morpho' option is checked when the [Apply] button is clicked. Also, you can send users to the Sagem readers via the MALoader Utility.

7. <u>**Two unique fingerprints**</u> **must be captured for every cardholder * who needs access at a** <u>**Sagem reader**</u>**. Sagem readers require 2 unique prints to load users into their bases.**

* There are two exceptions to this rule.
1- If the card is ID Only (visitor) card that will be used at a reader set for *Card Determines Mode*
2- if the card is ID Only card to be used at a reader set for *Card Pass-Through* mode, and this card will not need access at other reader / recognition modes.

8. If using *Finger-only Identification* (not issuing cards), you must create a unique Card ID in System Galaxy, but simply do not encode a card. This way the Galaxy controller can identify the access rules associated with the finger.

9. If using *Card Pass-through*, you do not need to capture prints and you do not need to load data to the MA110. You must set the MA110 for pass-through mode via the MALoader.

10. To take advantage of **Sagem's Visitor Mode**: make 'ID Only' cards for visitors without capturing prints. Visitor's cards are recognized/work at readers that are set to Card Determines Mode. ID Only cards are also recognized at readers set for Pass-Through. Door Access is denied by the controller IF cards are not given 'access privileges' to the loop or door.

2 System Planning

The MA110 handles credentials differently depending on the *"recognition mode"* at the reader. Also the **type of credential** and its **encoded "behavior"** can affect whether it is accepted in a given recognition mode.

Thus, how you intend to use biometric features will dictate how you create credentials, which enrollment devices you need, and which recognition mode you set at the MA110.

This chapter leads you through planning steps and basic concerns you will encounter.

Quick Start List of Basic System considerations to be determined:

1	**Accessibility and Visitor Mode:** Will you need an accessibility solution?	Step-1 p. 14
2	**Card Output/Format:** Which card output/format will you choose?	Step-2 p. 15
3	**Type of Credentials:** What type of credentials will you be creating?	Step-3 p. 16
4	**Recognition Mode:** Which *recognition mode* must be configured at the MA110 to be compatible with credentials you will use?	Step-4 p. 17
5	**Administrator Setup Options:** How do you need to configure the setup options to support your credentialing process?	Step-5 p. 25
6	**Understanding Operator Privileges** as they pertain to enrollment	Step-6 p. 27
7	**Flow diagrams of the biometric credentials at the MA110**	Step-7 p. 28

2.1 Planning Step 1 – Accessibility and Visitor Mode

Your site may need a credentialing solution for cardholders who cannot be fingerprinted.

System Galaxy supports the BIOPIN feature with the Sagem 520/521 models. See the SG manual for the Sagem MA520 with MIFARE as needed.

Be aware that Sagem uses an option known as Visitor Mode. This is supported by the "Card Determines Mode" (a.k.a. Card Mode). It allows the MA110 to read both card modes at one reader (i.e. the 'biometric cards' and 'ID Only cards') in the situation where you fingerprint employees but not visitors. Employees will be given a 'biometric card' that has prints in the card, whereas the visitor will be given an ID Only card that will not have prints in the card or in the reader. Both cards are accepted at the reader. The employee's biometric card will require a fingerprint to be authenticated. The visitor's ID Only card would not authenticate a fingerprint and would be accepted by the reader. Both cards will still be subject to access control rules at the controller.

2.2 Planning Step 2 - Choose the Card Output Format

System Galaxy requires a valid ID code for every access credential. The code must be transmitted in a compatible format such as 26-bit Wiegand or Data/Clock(ABA).

You must create an *ID code* and choose **card output format** even if you are not encoding and assigning a physical card. Fingerprint-only identification mode is an example of a credential that does not get a card (ref. Table 5) but still needs a code and format. The Galaxy controller uses the code to determine whether to allow or deny access (Figure 1).

System Galaxy can encode the *HID iClass cards* in the following formats:

1. **26-bit Wiegand / HID Compatible (recommended)** encodes the card's true facility code and generates/encodes an HID compatible value. This means that the customer is not limited to one facility code or block of cards. *The facility code in the MA110 is ignored.*

   NOTE: the MA110 will use the facility code on the card.

   NOTE: MA110 must have option 'HID Conversion = 1' and be configured for 26-bit wiegand output.

2. **26-bit Wiegand / Numeric ID** [1]**:** Galaxy encodes a unique ID set by the enrollment operator.

   ▪ Uses the facility code from the Sagem MA110 terminal (7 default).

   IMPORTANT: This card will not work at other HID/Prox readers.

   NOTE: the MA110 must have option 'HID Conversion = 0' and be set for 26-bit wiegand output.

3. **Data/Clock(ABA) / Card Serial Number**[2]**:** Galaxy encodes the unique ID using the Card Serial Number. Serial Numer is automatically read out when you click [Write Data to Card].

   NOTE: the MA110 must be configured for clock/data output.

4. **Data/Clock(ABA)** / **Numeric ID** [1] [2]**:** Galaxy encodes the unique ID entered by the enrollment operator. The software provides a [Next Number] button in the Card/Badge Settings tab that auto-assigns the next number (after the highest number already used).

   NOTE: the MA110 must be configured for clock/data output.

---

(1) If you are doing fingerprint-only (no card/mode in **Table 5**), you can use Numeric ID in either 26-bit wiegand or Data/Clock formats as the card code. You must set the MA110 to use the same output format you have applied in system galaxy.

(2) SG panel stores up to 48 bits binary (max. 12 digit number). If the number is larger than 12 digits, you must turn on the data-folding checkbox option in Loop properties.

2.3 Planning Step 3 - Determine the Type of Credentials

The types of credentials that work at the MA110 are fingerprints and 16K iClass Contactless Cards. These can be used individually or in various combinations depending on your site needs.

HID iClass cards can be used as follows:

Biometric Card   ▪ Card + Fingerprint (prints are in the card)

ID Only Card
  ▪ Card (prints not in SG/not loaded to 110)
  ▪ Card + Print if using *Prints in Reader* recognition mode (prints in SG & loaded to 110)

Fingerprint Only Identification   ▪ Fingerprint – two prints are in SG and loaded to 110

Table 4: Types of Credentials with compatible MA110 Recognition Modes

Type of Credentials	Behavior	Compatible MA110 Recognition Modes [1]	Output Format
iClass cards w/ prints (prints on the card)	Biometric	iClass - Card Determines Mode iClass - prints in card iClass - card or Identification (Multifactor)	**26-bit Wiegand** ◆ HID Compatible[2] ◆ Numeric ID **Data/Clock**
iClass cards w/o prints (prints not in card)	ID Only *	iClass - Card Determines Mode (visitor*) iClass - prints in the reader	
iClass cards only (prints not in card)	ID Only	No Fingerprints – Card Only	◆ Serial number** ◆ Numeric ID
Card Pass-Through	ANY *	Card Pass-Through	
Fingerprints only	Card not created	iClass or Identification (Multifactor) Identification mode	**26-bit Wiegand** ◆ Numeric ID **Data/Clock** ◆ Numeric ID
* ID Only cardholders are not required to enroll/capture fingerprints ONLY IF they are Visitor Cards needing access at readers set for Card Determines mode, or needing access for readers set for Pass-Through. ** Serial Number uses 48-bit binary, which means you must enable data folding if the ID is larger than 12 digits. (1) see **Section 2.4** for a **Table 5: MA110 Recognition Modes and the Accepted Credentials** (2) HID Compatible (recommended) is a 26-bit Wiegand value that will work at the MA110 and HID iClass readers.			

2.4   Planning Step 4 - Determine the Recognition Mode

You must decide which *recognition mode* you will use at each MA110. The mode you choose **must** be compatible with the *card mode/behavior* you are using. Use both **Table 4** (*Section 2.3*) and **Table 5** (*below*) to determine which MA110 Mode supports the credentials you want to use.

> **IMPORTANT:** the initial configuration of the MA110 is done using the Sagem Configuration tools. These tools and their manuals are on disk 2 of the System Galaxy Install CD.

> **NOTE:** The *GCS MALoader Utility* is used to set the recognition mode at the MA110. The MALoader utility is found in the System Galaxy folder after the SG Installation is completed.

Table 5: MA110 Recognition Modes and the Accepted Credentials

MA110 Recognition Modes	MA110 Sensor	Credentials Encoded / Accepted (card mode behavior)	Devices Needed
1 iClass – the card determines mode (1:1)	OFF until card is presented	• iClass cards **with** fingerprints (Biometric) • iClass cards **without** fingerprints (ID Only) (**visitor mode**) The card determines where the MA110 looks for print (i.e. on the card or in the MA110 Base).　Notes A, B, and C apply.	MSO-300 Card Writer iClass cards
2 iClass – prints in the card (1:1)	OFF until card is presented	• iClass cards **with** fingerprints (Biometric). Notes A, and C apply.	MSO-300 Card Writer iClass cards
3 iClass – prints in the MA110 (1:1)	OFF until card is presented	• iClass cards **without** fingerprints (ID Only) Notes A, B, and C apply.	MSO-300 Card Writer iClass cards
4 iClass or Identification mode (1:1 or 1:N) (**Multifactor**)	ON - card or finger can be presented	• iClass cards **with** fingerprints (Biometric). • Fingerprints enrolled and card not issued (SG requires a valid card code to be assigned for access control) Notes B, and C apply.	MSO-300 Card Writer iClass cards
5 Identification mode (1:N)	ON - only finger is presented	• Fingerprints enrolled and card not issued (Note that SG requires a valid card code to be assigned for access control). **Cards are not encoded.** Fingerprints must be loaded to MA110.	MSO-300
6 No fingerprints – Card only	OFF	• iClass cards **without** fingerprints (ID Only) fingerprints must be captured, but are not authenticated at the reader	MSO-300 Card Writer iClass cards
7 No fingerprints – passthrough	OFF	• iClass cards **without** fingerprints (ID Only) Card ID is not in the MA110, fingerprints do not need to be captured.	Card Writer iClass cards
a) A card must be presented at the reader before a fingerprint is scanned/authenticated. **b)** Fingerprints that are not on the card must be loaded to the MA110. **c)** The finger that is presented must match the print that is associated with the card. Wrong fingers or unidentified cards are not forwarded to the Galaxy controller for access decisioning.			
NOTE: prints must be captured for a cardholder unless you are using Sagem's Visitor Mode (ID Only card for reader set to card determines mode), or if you are using Pass-through mode. Pass-through mode reads a card ID and passes it to ACP.			

2.4.1   Sagem MA110 Recognition Modes described

2.4.1.1   Card Determines Mode

iClass –Card Determines Mode (1:1) – in this mode the Sagem Reader determines how to handle the card based on which Card Mode is on the card. Biometric iClass cards and ID-Only iClass cards with (or without prints/visitor) are accepted/recognized at the same reader/door when using this mode. If a print is on the card (biometric) it is authenticated. IF the card is ID Only, the card is passed-through to the Galaxy control panel even if there are prints in the reader for that cardholder.

This mode is also known as the Sagem *Visitor Mode*. An example scenario: employees might be required to enroll fingerprints, while visitors would be given an ID Only card that can be given access without capturing or authenticating prints.

IMPORTANT: Care should be taken as to whether "visitor access" is appropriate for the intended area. Visitor cards should have the appropriate limitations such as an expire date or limited number of uses. These options are set in the Card / Badge settings tab of the cardholder programming screen.

Which cards will work and how…

Card Mode Behavior	What's encoded	How it works at reader	Galaxy access control panel (ACP)
Biometric	ID + PRINTS	Reader recognizes card and prompts for finger > sends data to ACP	▪ Access is granted or denied based on access rules from Galaxy. ▪ A bad or incorrect finger will be logged as Invalid Access Attempt – not recognized ID" ▪ An invalid or rejected card will not create a logged event in galaxy because the reader does not forward it to the panel. Access to the door will not be granted.
ID Only	ID (no prints captured – visitor)	Card is passed-through to ACP	
ID Only	ID (prints in reader, not on card)	Card is passed-through to ACP without authenticating fingerprint	

2.4.1.2 Prints in Card Mode

Prints in Card Mode (1:1) – in this mode, the user presents the card to the Sagem Reader, which reads the prints from the card, then prompts user to provide a fingerprint (scanner turns on). When user provides the correct print, the reader forwards the card data to the access control panel for access decisioning.

Cards are created by.enrolling prints in SG, selecting BIOMETRIC, creating a card ID and writing data to the card.

NOTE: Prints are not required to be loaded the reader, since comparison is made to the prints that were encoded in the card.

NOTE: ID ONLY cards are not recognized / accepted in the mode, even if prints were captured / enrolled.

Which cards will work and how…

Card Mode Behavior	What's encoded	How it works at reader	Galaxy access control panel (ACP)
Biometric	ID + PRINTS	Reader reads card and sends data to ACP	• Access is granted or denied based on access rules from Galaxy. • A bad or incorrect finger will be logged as Invalid Access Attempt – not recognized ID"
ID Only	ID (no prints captured)		
ID Only	ID (prints capture in System Galaxy)		

2.4.1.3   Prints in Reader Mode

Prints in Reader Mode (1:1) – in this mode, the user presents the card to the Sagem Reader, which looks up the print from the Sagem reader base that is assigned to that card ID, then prompts user to provide a fingerprint (scanner turns on).

Card is created by enrolling fingerprints in System Galaxy, then select ID Only, create a card ID and write data to the card.

NOTE: prints must be loaded to the reader.

Which cards will work and how…

Card Mode Behavior	What's encoded	How it works at reader	Galaxy access control panel (ACP)
Biometric	ID + PRINTS	▪ Card accepted if user is loaded to the reader ▪ Card is rejected if user is **not** loaded to the reader	▪ A rejected card will not create a logged event in galaxy because the reader does not forward it to the panel. Access to the door will not be granted.
ID Only	ID (no prints captured)	Card is rejected – User not found in base.	
ID Only	ID (prints capture in System Galaxy and loaded to reader)	Reader recognizes card and prompts for finger > sends data to ACP	▪ Access is granted or denied based on access rules from Galaxy. ▪ A bad or incorrect finger will be logged as Invalid Access Attempt – not recognized ID"

2.4.1.4   Card or Identification Mode (Multifactor)

Card or Identification Mode (Multifactor) – in this mode, the reader will accept two kinds of credentials, fingerprint identification and biometric cards. This mode is a combination of identification and 'prints in card' modes also know to Sagem as Multifactor or Merged mode. The scanner is on all the time in this mode.

Card is created by enrolling fingerprints in System Galaxy, then select Biometric behavior, create a card ID and write data to the card. (prints are on the card) User presents the card to the Sagem Reader, which gets the print from the card, then user to provides a fingerprint (scanner is on).

Fingerprint-only credential is created by enrolling fingerprints in System Galaxy, creating a card ID. You do not write data to a card for Identification mode credential. User presents the fingerprint (scanner is on). Card is not issued to the finger-only user.

NOTE: prints must be loaded to the reader for the biometric card and the finger-only credential.

Which cards will work and how…

Card Mode Behavior	What's encoded	How it works at reader	Galaxy access control panel (ACP)
Biometric	ID + PRINTS	Reader recognizes card and prompts for finger > sends data to ACP	▪ Access is granted or denied based on access rules from Galaxy. ▪ A bad or incorrect finger will be logged as Invalid Access Attempt – not recognized ID"
Finger-only credential	Fingers are enrolled, but card is not created	Reader searches it base for a matching print	
ID Only	ID (no prints captured)	Card is rejected	▪ A rejected card will not create a logged event in galaxy because the reader does not forward it to the panel. Access to the door will not be granted.
ID Only	ID (prints capture in System Galaxy)	Card is rejected	

2.4.1.1   Identification Mode

Identification Mode – in this mode, the reader accepts finger-only credentials. This is the same mode all older readers use.

Fingerprint-only credential is created by enrolling fingerprints in System Galaxy, creating a card ID. You do not write data to a card for Identification mode credential. User presents the fingerprint (scanner is on). Card is not issued to the finger-only user.

NOTE: prints must be loaded to the reader for finger-only credential.

Which credentials will work and how…

Card Mode Behavior	What's encoded	How it works at reader	Galaxy access control panel (ACP)
Finger-only credential	Fingers are enrolled, but card is not created	Reader searches it base for a matching print	▪ Access is granted or denied based on access rules from Galaxy.
Biometric	ID + PRINTS	Card is rejected	▪ A rejected card will not create a logged event in galaxy because the reader does not forward it to the panel. Access to the door will not be granted.
ID Only	ID	Card is rejected	

2.4.1.2   No Fingerprints – Card Only Mode

No Fingerprints – Card Only Mode – in this mode, the reader accepts ID-only cards. Fingerprints must be captured, but are not authenticated.

Card is made by capturing fingers and selecting ID Only, creating an ID and writing data to the card. Prints are not in the card.

NOTE: prints must be loaded to the reader for this credential.

Which cards will work and how…

Card Mode Behavior	What's encoded	How it works at reader	Galaxy access control panel (ACP)
Biometric	ID + PRINTS	Card is rejected	A rejected card will not create a logged event in galaxy because the reader does not forward it to the panel. Access to the door will not be granted.
ID Only	ID (prints not captured)	Card is rejected	
ID Only	ID (prints captured)	Reader recognizes card	▪ Access is granted or denied based on access rules from Galaxy.

2.4.1.3   No Fingerprints – Card Pass-Through Mode

No Fingerprints – Card Pass-through Mode – in this mode, the reader accepts and passes-through all valid cards. Fingerprints are not captured/loaded for a pass-through mode unless they are needed for access at a different reader in the same system. To work be captured, but are not authenticated.

Card is made by ID Only, creating an ID and writing data to the card. Prints are not in the card and do not have to be captured.

Which cards will work and how…

Card Mode Behavior	What's encoded	How it works at reader	Galaxy access control panel (ACP)
Biometric	ID + PRINTS	Card is rejected	A rejected card will not create a logged event in galaxy because the reader does not forward it to the panel. Access to the door will not be granted.
ID Only	ID (no prints)	Reader recognizes card and ID is passed-through	▪ Access is granted or denied based on access rules from Galaxy.

2.5   Planning Step 5 – Administrator Setup Options

You should determine how the Cardholder Enrollment workstation will be configured. The enrollment options can be pre-configured in the Administrator Setup Options screen by a master operator.

System Galaxy allows you to …

1. **Pre-set the certain fields in the Capture/Enrollment screen:** This helps the operator capture fingerprints and encode cards the same way each time.

2. **Lock certain fields in the Capture/Enrollment screen:** This ensures the operator doesn't accidentally disrupt the feature that is locked.

   NOTE: Only a Master Operator can open the Administrator Setup Options screen.

   IMPORTANT: Some options can only be changed by a Master Operator. Some options can be configured by Enrollment Operators as long as the feature is unlocked by the Master Operator.

Table 6: Administrator Setup / Enrollment Options

Capture/Encoding Feature	Options	Presetable	To Lock Feature in Setup Options screen
Fingerprint Consolidation (triple-scan)	on/off	- -	Check the 'Always requrie Consolidation (triple-scan)' option.
Acquire 1st Fingerprint	- -	- -	- -
Acquire 2nd Fingerprint	- -	- -	- -
Compare Fingerprints	- -	- -	- -
Default Card Writer type droplist	Choices are ♦ iClass ♦ Mifare	YES	Uncheck the 'Allow Non-Master to select different writers'
Default Card Behavior droplist	Choices are ♦ Biometric ♦ ID Only	YES	Uncheck the 'Allow Non-Master to select card behavior
Card ID format * droplist	Choices are ♦ 26-bit Wieg. ♦ Data/Clock	YES	*Locked by default.* *Only a master operator can change this.*
How Card ID is Generated* droplist	Choices are ♦ HID Compat. ♦ Numeric ID ♦ Card S/N	YES	*Locked by default.* *Only a master operator can change this.*
* see Section 2.2 for description of valid Output/Formats			

2.5.1   Setting fingerprint triple-scan option:

If you are capturing fingerprints, you must set the Use Consolidation (triple-scan) option in the Capture/Encoding Screen. This option requires you capture the finger 3 times. Checked means you will capture every print 3 times.

NOTE: you can require triple-scan on all cardholders by enabling the 'Always require the triple-scan' option in the *Setup Options screen.* Checked means triple-scan enabled/required.

2.5.2   Setting the default Card Writer:

You can set the default card writer to always be iClass. You can also lock this field from being changed by non-master operators. iClass and MIFARE are the current options available.

NOTE: you can lock this *card writer field* so the operator can only uses the default writer. Checked means unlock field for non-master operators. Unchecked means locked.

2.5.3   Setting the default Card Behavior:

You can set the default card behavior to and also lock the card behavior field.

- **Biometric** means you will encode the fingerprint on the card.
- **ID Only** means fingerprint data will not be encoded on the card. Only the card ID will be encoded. If you are capturing prints when using ID Only, fingerprint data will be saved in the System Galaxy database and can be loaded to the MA110 reader.

NOTE: you can lock the Card Behavior field so that the operator only used the defaulted behavior. Checked means unlock field for non-master operators. Unchecked means locked.

IMPORTANT: If you are using *'iClass Card determines mode'*, you should not lock the Card Behavior field.

2.6   Planning Step 6 – Understanding Operator Privileges

You should create Operator logins for each operator.   Logins and passwords should not be shared. Operator priviliges are set up in the System Operator screen (see Chap. 10 - SG 8.2 software manual).

SG operator privileges do not apply to the MALoader utility.

MASTER OPERATOR:

At least one Master Operator should be created for the system. A master operator will have full privileges to view and edit all fields in any screen in System Galaxy.

Master Operator Privileges for *CAPTURE/ENCODING* and *SETUP* screens:
- Always able to capture prints and encode cards.
- Always able to edit fields that are locked for non-master operators.
- Always required to perform a triple-scan on fingerprint capture in the *Capture/Encoding screen ONLY IF* the [Always require triple-scan] option is checked (ON) in the *Setup Options screen.*
- Must use the defaulted card format and ID numbering scheme in the *Card/Encoding screen*.
- Always able to change the card format and ID numbering scheme in the *Setup Options screen.*
- Always able to see the [Setup Options] button or open the *Setup Options screen*.
- Always able to open the *Setup Options screen* and see/change the setup options (including locking or unlocking *card writer field* and *card behavoir field*).

ENROLLMENT OPERATOR:

An Enrollment Operator should not be given master operator rights. The enrollment operator should have the correct privileges (viewing/editing Cardholder-programming, Loops, Access Groups, etc.)..

Enrollment Operator Privileges for *CAPTURE/ENCODING* screen:
- Always able to capture prints and encode cards
- Only able to edit fields that are unlocked for non-master operators
- Always required to perform a triple-scan on fingerprint capture in the *Capture/Encoding screen* ONLY IF the [Always require triple-scan] option is checked (ON) in the *Setup Options screen*
- Must use the defaulted card format and ID numbering scheme in the *Card/Encoding screen*.
- Never able to change the format and ID numbering scheme in the *Setup Options screen.*
- Never able to see the [Setup Options] button or open the *Setup Options screen*.
- Never able to see/change the setup options, including locking or unl*ocking card writer field* and *card behavoir field*.

2.7 Flow Diagrams of credentials at the MA110

As explained in prior sections, the MA110 Terminal/reader has several ***recognition modes***. This section provides a visual example of how each type of credential (by behavior/card mode) will be handled at the MA110.
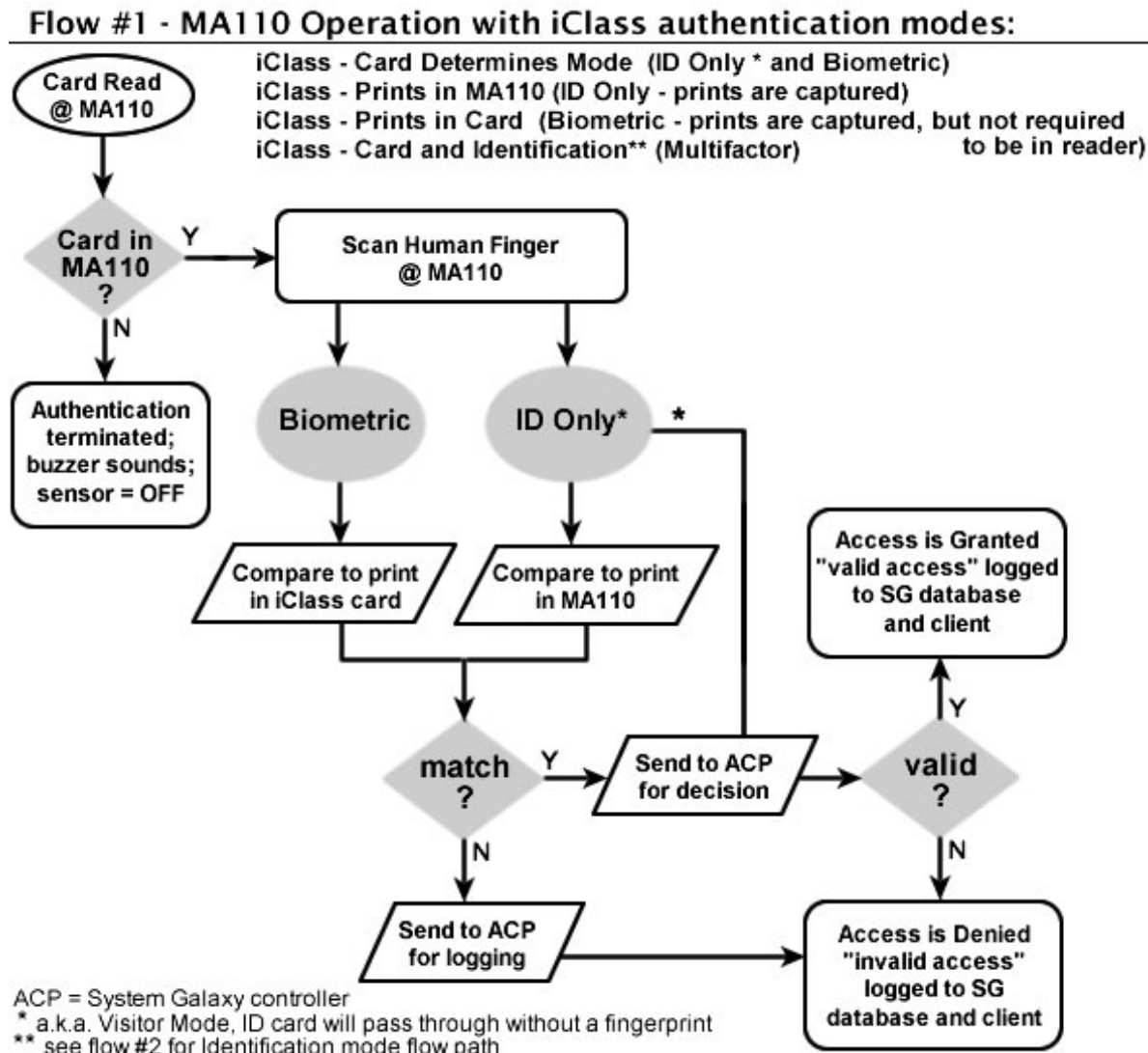
2.7.1   MA110 Authentication Modes (1:1)

All authentication modes using iClass cards (Wiegand or ABA) require fingerprints. You must use the mode that is compatible with the card behavior (i.e. Biometric or ID Only).

Four modes use authentication for iClass card and fingerprints:

- iClass – Card determines mode (ID Only and Biometric)
- iClass – Prints in MA110 (ID Only) prints are enrolled in SG and must be loaded in reader
- iClass – Prints in Card (Biometric) – prints are not required in reader.
- iClass –Card and Identification (Multifactor) – mix of prints in card mode and identification mode.

Figure 2 – Flow-chart of MA110 Authentication (1:1) using iClass cards and fingerprints:

Flow #1 - MA110 Operation with iClass authentication modes:

iClass - Card Determines Mode (ID Only * and Biometric)
iClass - Prints in MA110 (ID Only - prints are captured)
iClass - Prints in Card (Biometric - prints are captured, but not required to be in reader)
iClass - Card and Identification** (Multifactor)

ACP = System Galaxy controller
* a.k.a. Visitor Mode, ID card will pass through without a fingerprint
** see flow #2 for Identification mode flow path

2.7.2   MA110 Identification Modes (1:N)

All Identification modes require using fingerprints. In Identification modes, the finger credentials are compared to the prints stored in the MA110.

Two modes use fingerprint-only identification:

- iClass – Card and Identification (Multifactor)
- Fingerprint Identification mode (Finger only)

NOTICE: Multifactor mode accepts both Fingerprint-only credentials and iClass cards at the same reader. The flowchart (Figure 3 below) shows the Fingerprint-only behavior for mixed mode. The previous flow-chart (Figure 2) shows the iClass card behavior for mixed mode.

Remember that Table 5 lists all the modes of operation with the compatible credentials.

Figure 3 - Flow-chart of MA110 Identification mode (1:N) using fingerprints:

Flow #2 - MA110 Operation Finger Identification modes:
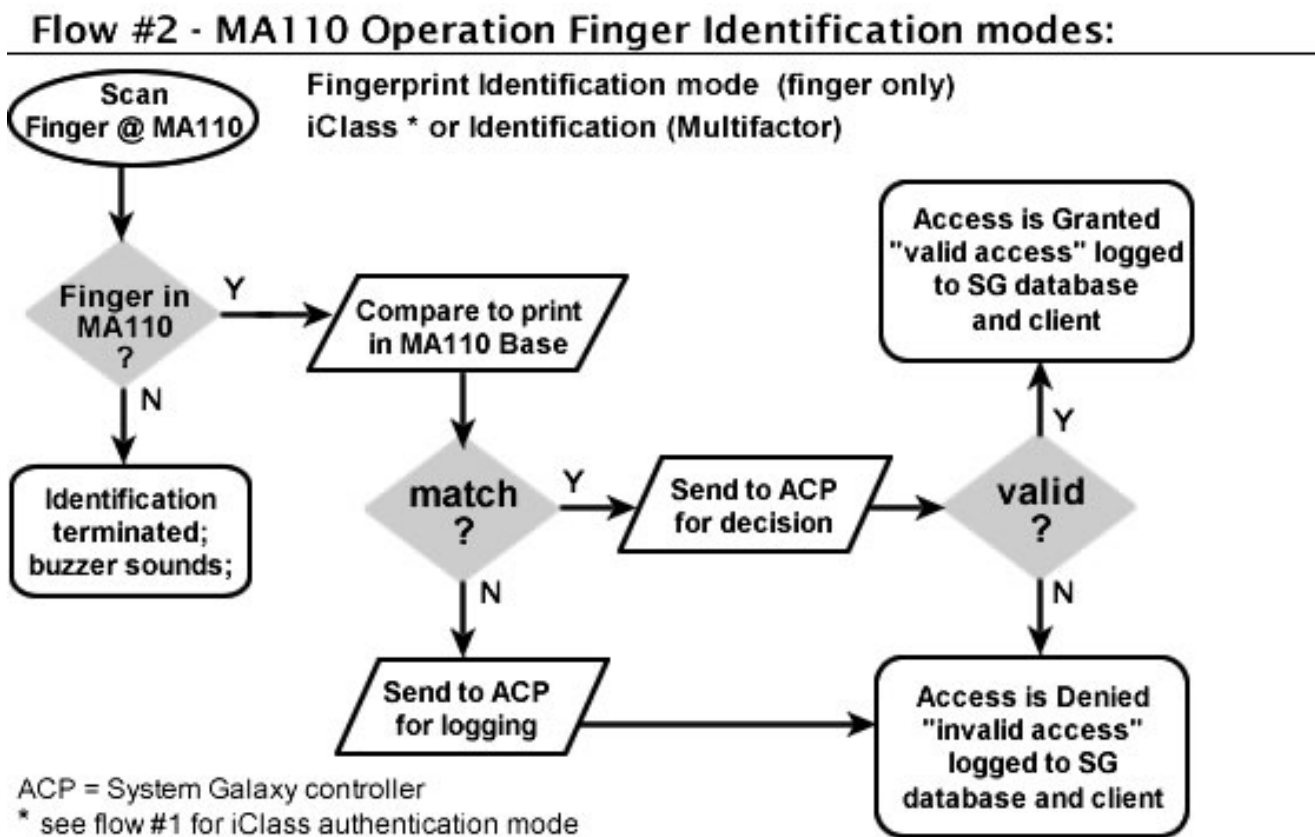
2.7.3 MA110 Card Only Modes

All "Card-only" or "No Finger" modes do not use fingerprints. These modes allow the MA110 identify cards or work as a pass-through reader.

In the No Finger mode, the Card ID is stored in the MA110 terminal base. Only the cards that are in the MA110 base are forwarded to the SG controller for access decisions.

In the Card Pass-through mode, the MA110 does not store any card IDs in its base. It simply reads the card and passes the ID to the SG controller for access validation.
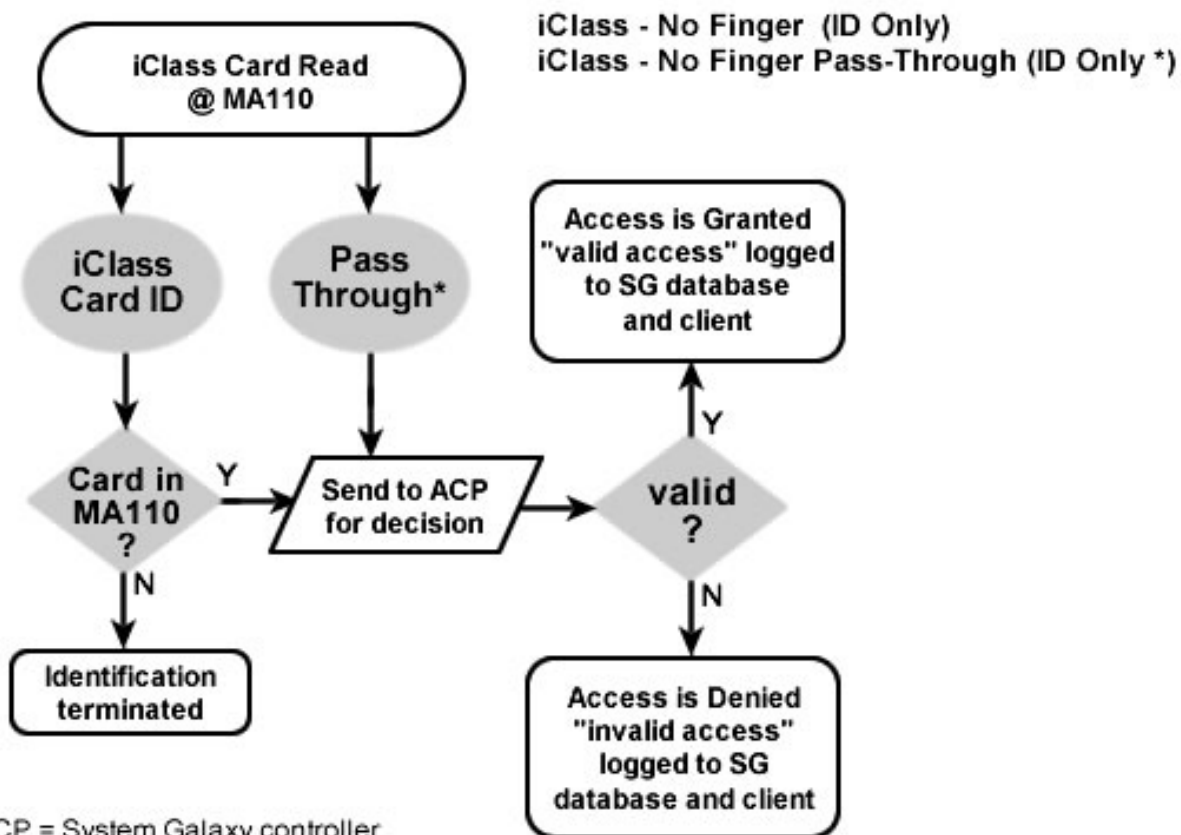
Two modes use Card-only credentials:

- No Finger (ID Only)
- No Finger - pass-through (ID Only)

Remember that Table 5 lists all the modes of operation with the compatible credentials.

Figure 4 - Flow-chart of MA110 Card-Only mode:

3 Installing Biometric Equipment

This chapter covers installing the biometric readers and biometric enrollment devices.

3.1 Installing the Sagem MA110 Reader

You will install and set up the MA110 Terminal/Reader according to the Sagem manufacturer's directions. The following must be done before you can interface with System Galaxy.

- Do not power Sagem reader off the Galaxy access control panel's power-supply. Sagem readers should be powered separately

- Also do not power door locks off the Galaxy access control panel power supply.

- Once the MA110 is installed, you will connect to the Dual Reader Module (DPI) Board in the System Galaxy access control panel, according to the instructions in the Hardware Manual.

- The MA110 will need to be given and IP Address that is valid for the customer's network. The IP Address must be added using a USB memory thumb drive.

- Once the MA110 has a valid IP Address you can connect to it using the Sagem Configuration tool (found on disk2 of the CD in the Sagem folder) to do the initial configuration.

- After configuration is done you should test the reader to ensure it is working.

- Once this is done, you can use the Galaxy **GCS MALoader** to do the following:

  1. create bases in the MA110

  2. configure the output format (26-bit Wiegand, Data/Clock ABA)

  3. turn on (or off) the **HID Conversion option** and set the reader **recognition mode**

IMPORTANT: If using *HID Conversion* (recommended*) to be compatible with the iClass readers, you must do the following:

- cards must also be encoded using 26-bit Wiegand output format
- MA110 must also be configured for 26-bit Wiegand output format
- cards must be encoded with the **HID Compatible ID** and **Card Site Code**.
- MA110 default site code (7) will be ignored since the reader will use the site code on the cards.

* Turning off HID Conversion means the cards must have the MA110's site code encoded into them. Thus using **HID Conversion is recommended** even if you don't use iClass readers so that you will avoid problems with duplicate card IDs or cards not working at this reader or other readers due to incompatible site codes.

NOTE: using HID Conversion does not interfere with interfacing to Prox readers since they depend on the dual-technology 125kHz chip. You can order the 125 chip to match the 13.56 MHz chip.

3.2 Installing the MSO-300 Fingerprint Enrollment device

If your site is capturing fingerprints as a part of your credentialing, you will need to install the fingerprint enrollment device. System Galaxy 8.2.4 is compatible with the MSO-300 Enrollment device. The MSO-100 will not work.

NOTICE: you can install the MSO-300 after you install the System Galaxy software if you desire since testing the device will require you to get to the Cardholder screen. Installing the software is covered briefly in the following chapter, and in great detail in the SG Software Installation manual or the Galaxy Install CD help screens.

The MSO-300 MorphoAccess USB Driver must be installed.

  ▪ The driver can be installed from disk1 of the Galaxy Install CD at Installers\ Drivers\ Sagem\ Sagem MorphoSmart USB Driver.

  ▪ Double click "setup" file to install driver.

  ▪ The enrollment device requires a USB port (2.0) to connect to the Client Workstation PC

Once the installation of these components is properly completed, you should be able to capture fingerprints in the System Galaxy Capture/Encoding screen.

  ▪ Open the Cardholder programming screen at the bottom of the Card/Badge Settings tab.
  ▪ Click the [Scan Fingers] button to open the Capture/Encoding window.

NOTE: In order to scan fingers, the Biometric Interface Support option must be enabled when System Registration is performed.

3.3 Installing the Card Writer (encoding) device

If you are encoding cards as a part of your credentialing, you will need to install the Card Writer device. Contact Galaxy Control Systems Customer or Technical Support for a valid part number.

NOTICE: you can install the card writer after you install the System Galaxy software if you desire since testing the device will require you to get to the Cardholder screen. Installing the software is covered briefly in the following chapter, and in great detail in the SG Software Installation manual or the Galaxy Install CD help screens.

The Card Writer uses a Windows default driver.
> ‣ The driver should already be present as a part of the Windows system components.
> ‣ Simply plug the card writer into a com/USB port and allow windows to detect the device and associate it with the driver.

The Writer must be assigned to use COM port 4 or below.

> ‣ Set this in the Windows Hardware Device Manager.
> ‣ COM Port 5 or above are invalid and will cause the writer to fail to work.

You must set the same COM Port value in System Galaxy software.

> ‣ Sign in as a Master Operator
> ‣ Open System Galaxy Cardholder screen and click the [Edit] button to edit a cardholder
> ‣ Click the [Scan Fingers] button on the bottom of the Card / Badge Settings tab
> ‣ Click the [Configure Writer] button on the Capture/Encode Card screen
> ‣ Set the COM port field to match what you set in the device manager screen.
> ‣ Click [OK] and [Apply] to save your settings
> ‣ To test the writer, place an iClass card onto the card writer and click the [Read card] button. System Galaxy should pop up a dialog box with the card data shown. If the card is blank, you can enter an ID number into the *ID field* and set the *Behavior field* to ID Only. Then write the ID onto the card and read it back.

NOTE: In order to set COM port in System Galaxy, the Biometric Interface Support option must be enabled when System Registration is performed.

NOTE: Any key files associated with this writer will automatically be installed as a part of the software CD install process. Registration of biometric support will enable you to see the key files.

---

4 Setting up System Galaxy for Biometrics

This chapter covers the following:

- Brief notes on installing and registering System Galaxy

- Upgrading an existing biometric systems to SG 8.2.4

- Importing existing FGR files into the SysGal database

- Programming the biometric readers in System Galaxy

- Setting up the Card Encoding options in the Administrator Setup screen

IMPORTANT: you must be logged in as a master operator to program the software.

4.1 Installing New System Galaxy Software

System Galaxy 8.2.4 or later supports the biometric features described in this manual.

IMPORTANT: If you are upgrading please perform all backups before you upgrade and see important information in the next section.

For new installs, run all three parts of the Install (1-Prerequisites, 2-Database, and 3-Software) on every Server and Client Workstation.

The details of doing the software install is documented in the *System Galaxy Software Installation Manual* and also in the Installation CD Help screens which run in a windows browser (IE-6 or later).

4.2 Upgrading an Existing Sagem Site

In the SG 8.2.4, the fingerprint templates are stored in the SysGal database.

IMPORTANT: <u>Always back up your databases and any support files</u> you must continue to use after the upgrade (custom/saved reports, badge design templates, photo, graphics, icons, and .fgr files). All system assets should be backed up on a separate drive. *See Chapter 22 in the main Software Manual for details and charts on databases.*

- ▪ If your site does <u>not</u> have existing fingerprints, see Section 4.2.1.
- ▪ If your site does have existing biometrics (FGR files), do the standard upgrade in Section 4.2.1 and then see Section 4.2.2 .

4.2.1   Performing the standard system upgrade

The SG 8.2.4 Install CD allows you to do the normal database and software upgrades. You will run the Install (1-Prerequisites, 2-Database, and Software upgrade). If you have existing Sagem equipment, see the following section.

See the System Galaxy Software Installation Manual and in the Install Help screens for details. Coordinate large systems or systems with a lot of cardholders with the technical support department.

NOTE: If the site you are upgrading does not already use Sagem readers, then you will not have fingerprint templates to import. You will simply perform the system upgrade and advance to the next section.

IMPORTANT: Remember to back up your databases and all system assets (badge designs, graphics, icons, photos, reports and .FGR files) to a separate drive.

4.2.2   Importing fingerprint templates via GCS MA Loader

Once the standard system upgrade is finished, you can import your fingerprint templates into the SysGal database.

In previous versions of SG, the fingerprint templates were stored in the Sagem folder under the System Galaxy directory. This is typically found in c:\Program Files\System Galaxy.

When the software installation / upgrade was completed, the GCS MA Loader utility was installed in the System Galaxy folder. It is recommended you use the MA Loader from the PC that is normally responsible for connecting to the Sagem readers. Do not move the MA Loader to a different location. You can make a desktop shortcut to point to the MA Loader in the System Galaxy folder.

IMPORTANT: If the customer is keeping existing Sagem 200 / 300-series MA Terminals, **they MUST recreate their bases and reload fingers** (see below for details)**.**

4.2.3   Quick Steps to Upgrading to SG 8.2.4

1	Back-up your FGR files to a separate drive.	See section 4.2.4.1
2	Upgrade your entire system to SG 8.2.4	See section 4.2.4.2
3	Flash your hardware panels to the current S28 code.	See section 4.2.4.2
4 - 5	Import FGR files into SysGal database.	See section 4.2.4.3
6	Recreate Bases and Load any existing Sagem 200/300 readers and load finger data. (also applies to MA100/500)	See section 4.2.4.4
7	Create Bases, Load, and Configure newly installed Sagem readers.	See section 4.2.4.5
8	Integration with other reader types.	See section 4.2.4.6
9	Configure System Galaxy for the MA110 readers according to instructions in this manual.	See section 4.2.4.7

4.2.4 Detailed Instructions to Upgrading to SG 8.2.4

4.2.4.1 Backing up you Sagem FGR files before upgrading SG

1. **Copy / Back-up your SagemMA folder that stores the FGR files to a separate drive before you upgrade your System Galaxy Software and database!** Leave your FGR files in their SagemMA subdirectories and do not uninstall your System Galaxy software.

4.2.4.2 Upgrading your System to SG 8.2.4

NOTE: A valid maintenance / registration is required to upgrade. Contact Galaxy Customer Service or Technical Support for assistance.

2. Use the Galaxy Installation CD to **upgrade your SG databases and System Galaxy software** at all servers and client workstations. Follow the installation procedures found on the CD.

3. **Flash all your control panels** to the proper flash (600-series uses v2.10c and 508i-series uses 8.10a in SG 8.2.4). Instructions for flashing panels are found in the Galaxy Hardware manual.

4.2.4.3 Import existing FGR files into the SysGal Database

4. Start/**Run the GCS MALoader** from the same PC/workstation that the customer used in the previous version to load fingerprints to Sagem readers.

    a. **Click the [Applications Settings] button** on the main MALoader screen. The MALoader should already be pointed to the data source for the SysGal database and correct *SagemMA* directory that stored the FGR templates.

    b. **Test the data source connection** by clicking the [Test Connection] button. A dialog message should display "Connection Successful". .

    c. **Verify the path to SagemMA** in the MALoader. For typical installs, this path should be **C:\Program Files\System Galaxy\SagemMA**   Although the finger files are stored in subfolders, you must point to the SagemMA folder.

5. From the **MALoader** main screen, select the File menu and "**Import Finger Files into Database**". The MALoader searches the SysGal database for indicators for employees that have fingerprints on file, and then writes the fingerprint files into the SysGal database.

    a. When MALoader is finished, a message displays showing how many records were updated.

    b. If MALoader cannot locate any FGR files, the message "0 finger files imported" displays.

    IMPORTANT: you should randomly spot-check (compare) fingerprints for several users to verify the prints imported correctly. This is done in the Galaxy Cardholder screen.

    NOTE: You should keep a backup of your SagemMA directory and .FGR files until you are sure your imported files are correctly stored and credentials are working.

4.2.4.4 Recreate Bases and Load existing Sagem 200/300 readers

6. **If the customer is keeping existing Sagem 200/300-series readers,** the bases must be recreated – do the following steps: (also applies to MA100/500)

    a. Execute "delete all bases" and then "get all DB configuration" to verify "0" bases exist.

    b. Execute "create all bases", then "get all DB configuration" to verify bases are recreated.

    c. Execute "load finger data", then choose "get all DB configuration" to verify users are loaded.

    NOTE: Sagem 200/300 readers do not use iClass or Prox cards. These readers only support fingerprint identification mode. Thus, information that applies to card modes and recognition modes at MA110 does not apply. MA 200/300 readers can be operated in Fingerprint Identification Mode without conflicting with the single-card solution at other readers.   MA110 *recognition modes* and card modes should not adversely affect the system integration with older readers.

    NOTE: If external readers exist on the MA 200/300 readers, then you may be able to purchase *dual-technology cards* in order to continue providing a *single-card solution*. Or you may need to upgrade the reader technology to a more current solution.

4.2.4.5 Create Bases and Load newly installed MA110 readers

7. **If the customer is adding MA110 readers to the system,** the MA110 must be properly installed according to Sagem documentation and must be configured into System Galaxy according to the instructions in this addendum. Note wiring to the Galaxy panel is covered in Hardware Manuals

4.2.4.6 Integration with other reader types

8. **If the customer is keeping or adding other technology, such as iClass or Prox readers, etc., you must do the following:**

    a. Determine which cards will be ordered, (single- or dual-technology cards) and properly order the configuration of the card chip.

    b. If iClass readers are used, the MA110 should be set up for HID compatibility and the iClass cards should be encoded with the HID compatible ID and Site Code.

    c. If Prox or other type readers are used, the site can order dual-technology cards. The dealer must order the 125kHz chip to be programmed for the type of reader being used. Contact Galaxy Customer Service for assistance.

4.2.4.7 Register and Configure SG for Sagem interface

9. Once these steps are completed, you should be able to register and configure System Galaxy according to the instructions in this manual.

4.3 Registering for Biometrics

System Galaxy must be registered for biometric support. This option is found in the System Registration screen.

- **To start System Galaxy 8,** d**ouble-click the** *System Galaxy icon* (located on the PC's desktop)

- If this is the first time you have started the system, you must choose your product level, create a master operator login, and then sign into the system with it.

- If this is the first time you have logged into the system, the Loop Wizard opens up. You can close this wizard and go ahead to the registration. Then return to the wizard later.

- **Open the Registration Wizard from the following menu selections:** *Configure >> Options >> Registration >> Wizard*
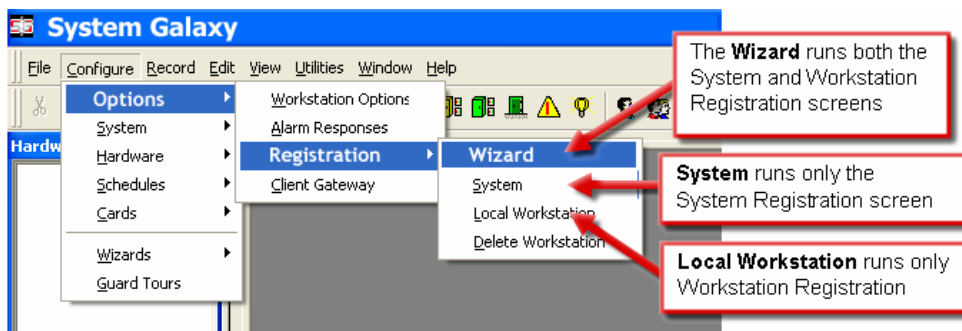
CAUTION about proceeding with registration: **The ability to use the** *Card Import Utility* **to setup users/cardholders could be impacted by system registration – see items below:**

1. Card Import Utility will not be available after completing system registration if the site will be registering for 'Professional' Product Level.

2. Card Import Utility will not be available after completing system registration if the site is Corporate or Enterprise, but WILL NOT BE purchasing the Card Import/ Export feature.

 Note: that the Card Import is available during the 14-day grace period as a courtesy for upgrades.

IMPORTANT: Card Import and Batch Loading cards is separate from importing FGR files and you will want to do the batch load or card import first. See Chapter 12 in the SG Software manual.

- The System registration screen must be properly filled out. Dealer online registration system is available from the Galaxy Control System's website at www.galaxysys.com and through Customer Service department.

- The Workstation registration screen must be properly filled out. Dealer online registration system is available from the Galaxy Control System's website at www.galaxysys.com and through Customer Service department.

4.4 About Operator Privileges

You must be signed in as a master operator to perform the programming and setup for the Sagem options. You must be signed in as a master operator to create an enrollment operator (in system operator programming).

When you create a system operator to do the cardholder enrollment, you will need to make sure you allow the operator to have access to edit the cardholder programming screens, loop and access control, etc.

See Chapter 2 in this manual for information that applies to operators concerning the Sagem programming screens. See Chapter 10 in the main SG Software manual for detailed instructions about all the filters and privileges in the Operator Programming screens.

4.5 About System Programming

Schedules, access groups, controllers, boards, etc. are covered in detail in the main SG Software manual (esp. Chapters 7, 8, and 9). This section covers information that is directly related to programming the Sagem options for readers and cardholders.
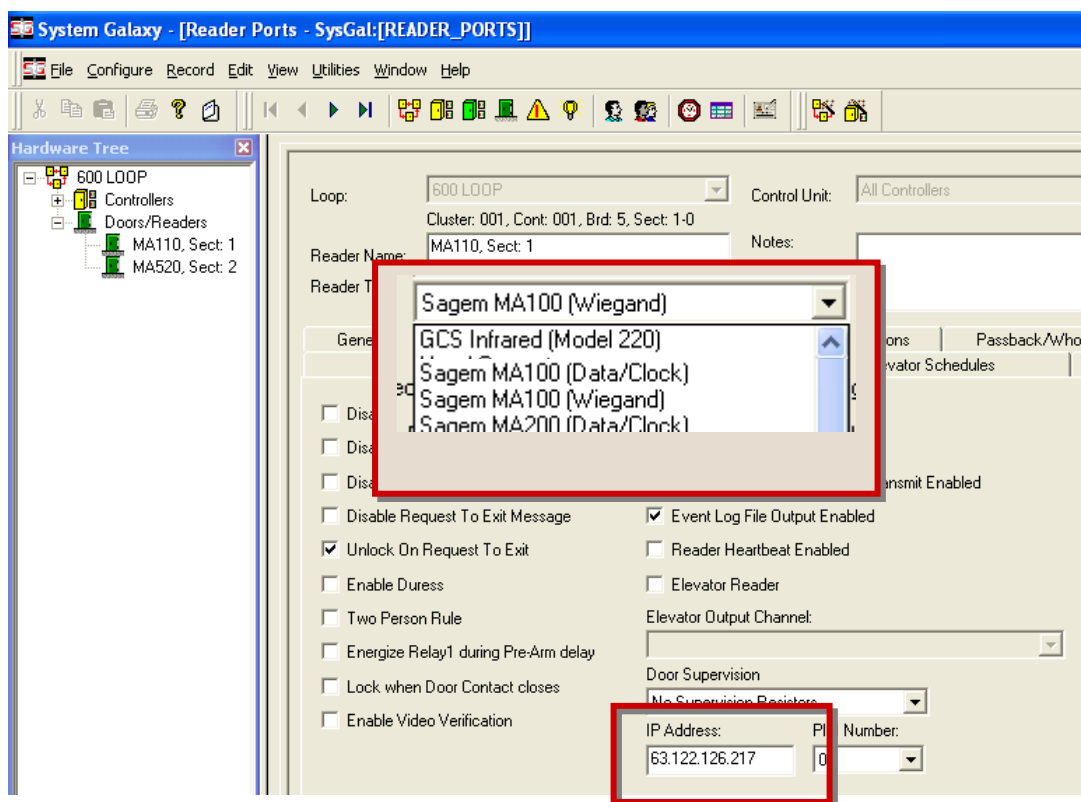

Assumptions:
- You have properly installed or upgraded all servers and workstations in your system (database and software). *See instructions in this manual and in the SG software manual.*
- GCS core services are running on the main communication server. *Services are covered in detail in Chapter 11 in the SG8.2 Software manual.*
- You have installed your Galaxy Hardware. *See SG Hardware manuals.*
- You have installed your Sagem readers and finished programming the IP Addresses and basic reader options. And the readers are online / on the network. *See instructions in this manual as well as the Sagem manuals main and SG hardware manual.*
- You have completed programming your hardware loop/clusters, controllers and boards. *Also see to Chapters 8 and 9 of the SG 8.2 Software manual for instructions.*
- You have completed programming your necessary schedules, days, access groups or profiles. *See Chapter 7 of the* SG *8.2 Software manual for instructions*
- You properly imported, or batch loaded, cards and cardholder data as is appropriated for your system. If this is a new install and you do not have employee or cardholder data from a prior or external system, then you will be enrolling your cardholders from scratch. *Also see to Chapters 6, 12 and 13 of the SG 8.2 Software manual for general instructions.*
- You have imported your FGR files according to the upgrade instructions in this manual. This does not apply to sites that are not upgrading existing Sagem readers.
- You have registered your system for biometric support according to instructions in this manual.
- You have installed your MSO-300 and card writer and their drivers (see this manual).

4.6 Configuring Reader Properties

To set up the Reader Properties for a Sagem reader, you need to do the following:

- Program the Loops and controllers and add the DPI – Dual Reader Modules as required.

- Open the Reader Properties screen and select the General tab. To configure a Reader Port, open the Reader Port window. Follow the menu **selections Configure > Hardware > Reader Ports**, or click the **Doors/Readers button** on the toolbar.

- Give the reader a unique name that you can correctly identify from the MA Loader utility. Example could be "Lobby 110", which tells you that the reader is the 110 in the lobby. The galaxy screen will always display the system default name, which shows which controller, and board the reader is on. You can leave this as part of the reader name if you like.

- Set the *reader technology* as appropriate for the type of reader and output format. This means that if you are going to use the Wiegand format, you must choose MA100 Wiegand option. And if you are using the ABA format, you will choose MA100 Data/clock option.

- Then enter the reader's IP address in the IP field at the bottom of the screen.

- Click APPLY to save your settings. Once this is done, the GCS MA Loader should be able to connect to the reader.

Figure 5 – Setting Sagem options in the Reader Properties screen:

4.7 Configuring Biometric Options in SG

This section covers information specific to setting up the biometric options directly related to enrolling biometric cardholders.

Assumptions:

- You must be signed in as a master operator.

- The Card Writer and MSO-300 should already be installed according to instructions in this manual.

- To set up the Biometric Options for the cardholder enrollment, you will need to have covered the planning information in Chapter 2 of this manual regarding output format, card modes/behavior, and the fingerprint enrollment options. You should have an understanding of which recognition modes you plan to use so that you can setup the card mode options correctly (also covered in Chapter 2).
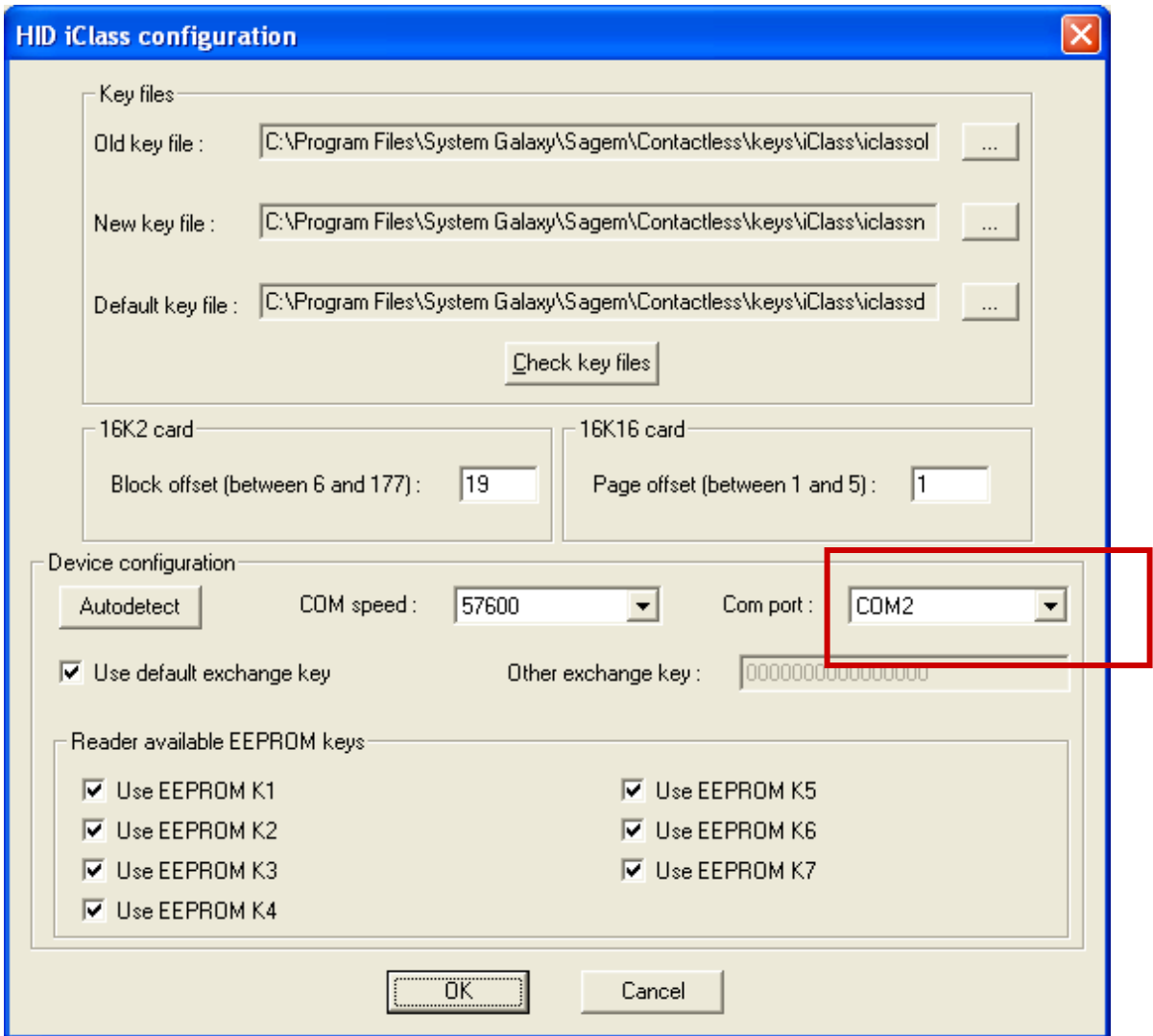
4.7.1   Configure the Card Writer COM Port in SG

To configure the Card Writer options do the following:

- Open the cardholder programming screen by following the menu selections

    Configure > Cards > Cardholders or clicking the Cardholder button on the toolbar

- Click ADD NEW to start a cardholder record (you will use this to get the setup screen).

- Choose the **Card / Badge Settings tab** and click **the [Scan Fingers**] button at the bottom of the screen. This opens the **Capture / Encode Card screen**.

- Click the **[Administrator Setup Options]** button. If you cannot see this button you are not signed in as a master operator.

- Click the **[Configure Writer]** button. This opens the Writer Configuration screen. The options in this screen will be setup according to the install.

- Set the COM Port field to match what you set for the Writer in the PC's Hardware Device Manager. BE AWARE – the writer will not work if this field does not match the hardware device manager. ALSO BE AWARE – if the PC is powerfailed or looses power for any reason it could cause the device manager to change the COM port number. Card writer will stop working until this is corrected. Value must be 4 or less and must match.

- Click OK to save and go ahead to the section to setup the encoding options (next section).

Screen shot of the Writer Configuration screen on next page.

Figure 6 – Setting Card Writer COM Port in SG:

4.7.2   Configure the Setup Options for Encoding Cards in SG

To configure the Encoding Options do the following:

- Open the cardholder programming screen by following the menu selections

     Configure > Cards > Cardholders or clicking the Cardholder button on the toolbar

- Click **ADD NEW** to start a cardholder record (you will use this to get the setup screen).

- Choose the **Card / Badge Settings tab** and click **the [Scan Fingers]** button at the bottom of the screen. This opens the **Capture / Encode Card screen**.

- Click the **[Administrator Setup Options]** button. If you cannot see this button you are not signed in as a master operator.

Figure 7 – Setting Administrator Options in SG:

- Check the **[Triple Scan]** option if you want the enrollment operator to always perform a triple scan when fingerprints are captured for each print (optional setting).

<<instructions continue on next page>>

▪ Set the **Default Card Writer** field to the type of cards you are encoding – the choices are "iClass" and "Mifare".

▪ Set the *allow non-master operators to choose a different writer* option. Checked will let the enrollment operator switch writers (not typical). Unchecked will lock this field in the Encoding Screen.

▪ Set the **Default Card Behavior** to the type of credentials (card mode) you have planned to make. Planning information about card modes is covered in Chapter 2.

▪ Set the *allow non-master operators to change behavior / card mode option.* Checked will allow the operator switch between card modes in the Encoding screen. You should check this option if you are making Visitor Mode cards that will work without prints in the reader's Card Determines Mode. If you do not check this option the default value will be the only card mode the operator can encode. Unchecked locks the field to the operator in the Encoding screen.

  The behavior / card modes are …

    Biometric = prints are required and will be encoded on the card.

    ID Only = prints may or may not be capture but will NOT be encoded on the card. If prints are captured, they can be loaded to the reader for use in the "Prints in Reader" recognition mode.

▪ Set the **Card ID format** for the Encoding screen. If you are using HID Conversion for iClass reader compatibility, you will choose Wiegand.

▪ Set the **how card ID is generated** field to the desired value. Remember Chapter 2 covers these options.

  The choices are …

    Use HID Compatible value = SG will generate a unique value that makes the iClass card compatible at both the MA110 and the iClass readers. HID Conversion must be on at the MA110.

    User determines number = means that the SG operator will manually set the ID value to a valid and unique number in the system. If you are using the ABA format, you can use the NEXT NUMBER option back in the Card/badge Settings tab to generate the next consecutive number in the system.

    Use card serial number = means that card serial number will automatically be read out and encoded on the card in the Encoding screen. This is recommended for ABA Data/Clock formats. Keep in mind that data folding may need to be turned on in the controller programming screen– see Requirements in this manual.

▪ Set the **create files when reading data from card** option as desired (diagnostic purpose). Checking this option will cause system galaxy software to create a text file of the card contents when the card is read in the Encoding screen. Every time you read a card, the file is overwritten. The file is placed in the current working directory – this is typically My Documents.

▪ Click OK to save these settings.

---

5 Enrolling Cardholder Biometric Data

This chapter covers the following:

- Capturing Fingerprints System Galaxy

- Encoding Cards

- Loading Fingerprints to the Sagem Reader

NOTE 1: the main SG Software Manual covers information that is not covered in this manual.

NOTE 2: It is possible to set up *Card Credentials* without fingerprints, or have the choice of where the fingerprints reside (in the card or at the MA110). The MA110 must be configured to operate.

NOTE 3: The card number is a placeholder in the SG panel/system that associates the credentials with the access rules. Thus, a card number is always required even if the fingerprint is the only credential used at the MA110.

NOTE 4: If you are using finger only, you must create a valid/unique card ID for SG, but you do not need to encode a card. Otherwise, you can encode the Card ID only, or the Card and Finger data.

NOTE 5: that fingerprints are stored in the SG database and will load to the MA110, provided the Load Morpho option is ON/Checked and loop/access privileges are set.

5.1 Capturing Fingerprint Data

1. Open and Edit the **Cardholder screen** and enter the cardholder's information such as Name, Department, Loop privileges, Access groups or profiles.

2. Set up the Card Technology, and get a unique ID number if you are using the "USER SETS NUMBER" option to get an ID. An ID is required always for the System Galaxy hardware.

3. Click the **SCAN FINGERS button** on the Badge Settings tab to open the Encoding screen

4. **Capture two different fingers** for the cardholder in the Encoding screen. You must capture two unique prints unless the person is a Visitor and you are making ID Only Visitor Card to be used at reader set to *Card Determines Mode*. The second exception would be if you are making a pass-through card that will only be used at a pass through reader.
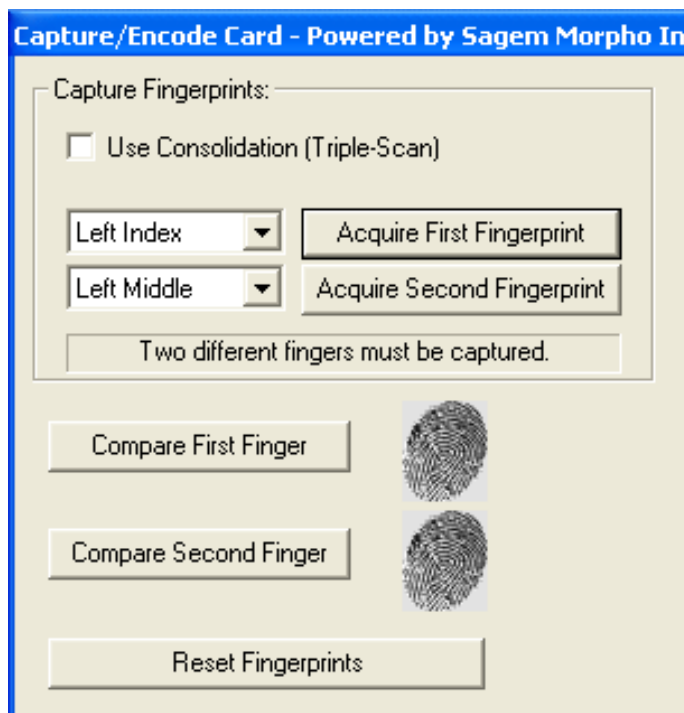
   Note: you can set the finger droplist to indicate which finger you captured.

   Note: that two prints will be encoded on the card if you are using a "biometric" behavior.

   Note: you will see fingerprint icons appear when the fingers are captured**.**

   IMPORTANT: Clicking the RESET button will erase both fingerprints.

Figure 8 – Capturing fingerprints in System Galaxy:

5.2 Encoding the Contactless Card

5. The **card Behavior** should be set by default – change it if needed to the value you desire. Card Modes are described in Chapter 2.

6. **Generate an HID Compatible Card ID** if you are using that feature. If you are not using HID Compatible or Serial Number, then you must create a unique valid ID for this field.

7. **Place the card on the Card Writer** and **click the [Write Data to Card] button**. The system will encode the card in a few seconds. If you are using serial number, the software will automatically read the serial number and write it on the card.

8. You can read the card if you wish to ensure the data was written as expected.

9. **Click OK** to save all data and prints.

10. When you are returned to the Badge Settings tab, the Load Morpho option will be checked. This tells the system to send the prints and card data to the Sagem readers in the assigned loop. You must have assigned loop and access privileges for the fingerprint to load.

11. **Click APPLY** to save record and load fingerprints to Sagem reader.

Figure 9 – Encoding Contactless Card with HID Compatible ID

5.3 Loading Users / Finger Data to the reader

There are two ways to load users to the Sagem reader after the reader has a valid IP Address and is online on the customer's network.

1. When you click Apply in the cardholder screen, the user/finger data is sent to any readers that the cardholder has been given loop/access privileges, provided the Load Morpho option is "checked". The Load Morpho option is at the bottom of the Card / Badge Settings tab in the cardholder screen.

2. When you select a reader and choose to execute a 'Load Finger Data' action from the MALoader. The MALoader sends all users to the selected readers that have been given loop/access privileges, provided the Load Morpho option is "checked". The Load Morpho option is at the bottom of the Card / Badge Settings tab in the cardholder screen.

Once you load finger data you can execute a 'Get DB information' action to see how many users are in your reader base.

See next section for description managing the 'Delete Card Before Loading' option, found in Application Setting screen in the MALoader.

5.4 Managing the Sagem Readers via MALoader

System Galaxy makes managing the Sagem biometric reader very easy from the MALoader utility. The likelihood that a site has more than one Sagem reader and are using different models dictates the capabilities that Galaxy built into the MALOADER.

The MALoader allows the Technician to …
- Manage the base(s) of Sagem readers (create or delete and get the database info.
- Load users / finger data into the readers (see section 5.3).
- Import FGR files (for upgrades – also see Chapter 4).
- Configure the Recognition modes, output format and related options of the readers.

NOTE: You should run the MALoader from the System Galaxy directory on the computer you normally use to connect to the readers. You can make a desktop shortcut to make it easier to open the MALoader from its home directory.

5.4.1.1   Managing Bases

The MALoader allow you to delete bases, which also deletes all users. If you need to get old records out of the bases you will use this option.

Also you can create a single base or all bases for the readers as is appropriate. The **Select Action droplist** contains a list of actions or commands that the MALoader can run when it is connected to the Sagem Reader. Click the EXECUTE ACTION button to send the command to the chosen reader. The actions allow you to delete and create bases, get DB configurations and load finger data to the reader.

- The MA110 has one base that holds 500 users.

- the MA520 has multiple bases that hold up to 1 base with 3,000 users with the standard memory allocation and up to 5 bases with 50,000 users with the extended memory license.

5.4.1.2   Delete Card Before Loading option

In the MALoader has an option to delete card before loading.

To find this option open the MALoader and click on the Applications Settings button. Look for the option at the bottom of the screen.

When checked the option will delete the card being loaded if it existed in the reader already and then load it into the reader. To maintain database integrity it is recommended to use this option. However, be aware that this could slow down large loads and can be unchecked to speed up loading fingers to the reader.

5.4.1.3   Importing FGR files

You only need to import FGR files if you are upgrading from a prior version of System Galaxy such as v 8.2.3 or earlier, and you have captured FGR files that you need to import.

IMPORTANT: You should backup all FGR files before you upgrade your software. The upgrade should not disturb your FGR files, however it is always good practice to backup assets whenever you are upgrading a computer. Upgrading a computer can uncover unexpected hazards that cannot be accounted for in software upgrade processes.

To run the IMPORT of FGR files,

- Open the MALOADER utility and click the FILE menu

- Select the IMPORT option and allow the import to complete.

NOTE: the MALoader must be pointed to the SagemMA folder that is storing the FGR files. FGR files are typically located in a directory structure c:\Program Files\ System Galaxy\SagemMA on the computer performing the finger enrollment. The files are actually in subfolders under the SagemMA folder, but the MALoader must point to the SagemMA folder. The path is set in the Application Settings Setup screen.

Figure 10 – Pointing to FGR files for importing:
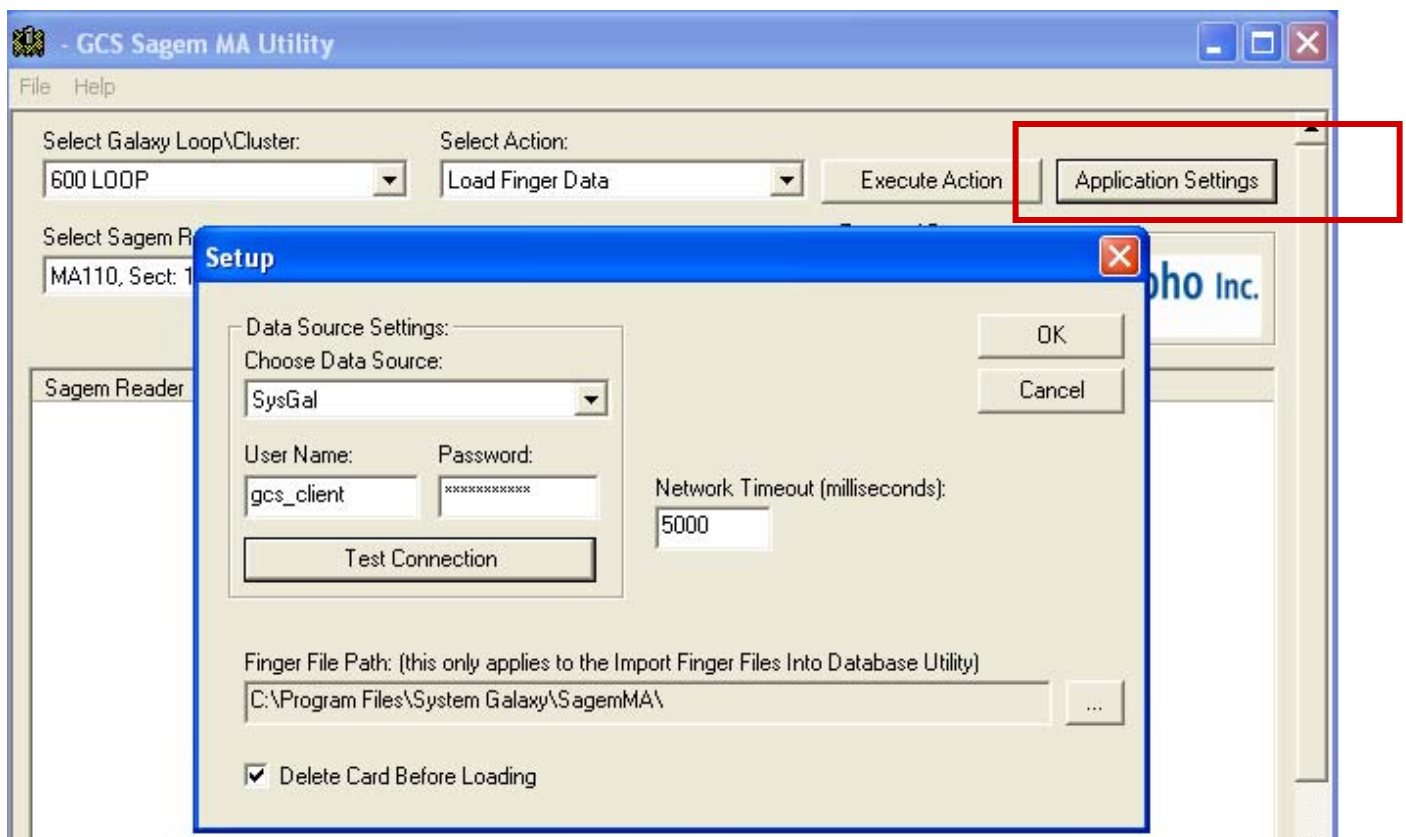
5.4.1.4   Configuring Reader Recognition modes

You can set the recognition mode for the selected reader from the MALoader utility.

- Select the desired reader in the main screen

- Click the CONFIGURE READER button

- Choose the desired recognition mode

- Set the HID Conversion checkbox (0=off, 1=on)

- On the Data Output Format tab you will set the output format and the site code if you are using Wiegand. Note that the reader will use the site code in the card if you choose to enable HID Conversion option.

- Click SEND TO MA TERMINAL button to send the configuration to the reader. The commands will display on the main screen as they are sent to the reader.

- You can set the reader's date and time to match the PC time.

- You can reboot the reader also. It is recommended to reboot the reader after it has loaded a new recognition mode. See chapter 2 for a list of recognition modes and how they work.

Figure 11 – Setting Reader Recognition mode via MALoader: