System Galaxy Quick Guide

System Galaxy 10.5.6 Biometric Integration

with MorphoManager v9.4.5

SigmaPROX & SigmaBIO in MA5G Mode

Also see BioBridge Conversion Guide & Sigma Reader Cfg Guide

2024 | SG 11.8.6

This document covers…

1. **Software & Hardware Requirements** for enrolling biometric credentials using the BioBridge module and MorphoManager Client with SIGMA MA5G Readers.
   - » Description of **System Galaxy Event Communications** for this Sigma interface
2. **Instructions include …**
   - » **Connecting and Configuring Hardware**:
     - ▪ SIGMA Reader configuration of Mode and IP Address, etc.
     - ▪ SIGMA reader wiring to the Galaxy 635-Controller
     - ▪ SIGMA LED-1 wiring to allow Galaxy panel to control SIGMA Reader's access response – i.e. wait for panel decision at an invalid access point. (optional)
   - » **Registering & Configuring System Galaxy** for Biometric Support, reader count, and the "MorphoManager/BioBridge" interface setting.
   - » Installing the **MorphoManager Server/Client** (BioBridge & Morpho Database).
   - » Creating a **Client Login** for MorphoManager ADO/NET Connection.
   - » Installing the **MSO-300** Enrollment device**.**
   - » Configuring the **BioBridge Connection Settings** in MorphoManager.
   - » Adding the **SIGMA MA5G Readers** and **Device Profiles** into MorphoManager.
   - » Adding **User Policy*, Distribution Groups, Authentication Types**, **Wiegand Profiles, Clients,** and **Multifactor Modes**, etc. in MorphoManager. (*must use "Per User")
   - » Enrolling **Biometric Credentials from System Galaxy** cardholder screen using the integrated BioBridge Enrollment module.

This guide covers enrolling the following Authentication Types …

- ● Biometric Credentials (Finger-Only)
- ● Proximity + Biometric Credentials (Card + Finger)

NOTICE: Sigma-Multi Readers are only supported if they are placed in a multifactor mode that is supported; either ***finger only*** or ***prox card+finger***. Using encoded cards with a Sigma-multi reader is not currently supported in the SG 9.4.5 release.

IMPORTANT: A credential's ***Authentication Type*** at the time the finger was captured must match the SIGMA Reader's ***Multifactor Mode*** (i.e. a credential made for a ***Proximity Card+Finger*** will not work at a reader that is configured for ***Biometric-Only*** multifactor mode; and visa-versa).

System Galaxy

Sigma MA5G and MorphoManager/BioBridge

Guide

Integrating System Galaxy with
SIGMA PROX & SIGMA BIO
using Galaxy 635 PANELS

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

This document describes how to connect and configure the SIGMA Reader with the 635 Control Panel, as well as how to configure the reader using the MorphoManager, and how to enroll credentials from System Galaxy using the BioBridge Client middleware. This guide does not supersede the manufacturer's documentation for products not manufactured by Galaxy Control Systems.

10th Edition

Galaxy Control Systems

3 North Main Street
Walkersville MD 21793

301-845-6600

www.galaxysys.com

Table of Contents

Table of Figures

DOCUMENT HISTORY

DATE	HISTORY
FEB 2015	1st Edition published with SG 10.4.1 using MorphoManager/BioBridge 6.2.0.
MAY 2015	2ND Edition includes: • Updates to instructions and wiring diagrams to show LED1 wiring, which allows the signal from the ***Galaxy Control Panel*** to control the SIGMA Reader's Access Granted response message to the user. Affects sections for Requirements, Hardware Installation and Wiring, Configuring Device Profile, • Updates to the System Upgrade instructions to MorphoManager. • Updates to the System Upgrade instructions to System Galaxy. • Improve instructions concerning User Not Found (BioBridge tab) and cardholder enrollment instructions where related to Authentication Types. • Additions to the trouble-shooting section. • Other general edits and adjustments to pagination.
JUNE 2015	3rd Edition includes: • Added an Enrollment Requirements table and section to chapter 7. • Added Access Card Enrollment Infographic to Ch7 Cardholder Screen. • Added Biometric Credential Enrollment Infographic to Ch7. • Added some additional notes to Chapter 7.
MAR 2016	**4TH Edition includes the following:** *NOTE: this edition is a major rewrite of the entire document. If you are upgrading from MM V6.2 please carefully read this document. The new functionality impacts all chapters and heavily impacts the programming in the MorphoManager Client.* • All MorphoManager Client instructions and screen shots have been updated/replaced. • Updated requirements: MM v9 requires Sigma firmware v1.4.1 and System Galaxy 10.4.9 (min). • Added Sigma Reader installation diagrams & instructions to include using DRM Relay-2 to control the Sigma LED-1 ("wait for panel decision" function). This is a way of wiring the Sigma LED-1 that ensures the Sigma reader will get the constant low voltage needed to sustain the Sigma 'delay for panel decision' before denying access in the cases of an expired or invalid credential. • Added cautions in appropriate sections do not power a Sigma Reader from the Galaxy DRM board or the Galaxy control panel's power supply. • **MM v9 no longer uses *User Groups*** – the functionality provided by User Groups is divided between other entities (such as User Policy, User Distribution Groups, etc.). The enrollment and creation of credentials and any features that were dependent on User Groups have all been affected. All instructions, descriptions, and references to these functions have been updated. • The ***user not found*** *option* has moved and is not called the deleted user management option. • The *Authentication Type* has been moved is and now called ***Authentication Mode***. However, the Sigma's **Multi-Factor Mode** must still be compatible with the credential's **Authentication Mode.** • Updated instructions related to the *pre-selection screen* of the ***BioBridge enrollment module.*** The User Distribution Group must be mapped. Also the operator must select which User Policy (finger only vs. prox+finger) if multiple reader types are used. • Added a new feature to BioBridge enrollment module that allows operator to select which ***Legacy MA reader base*** a finger template will be stored. MA Readers could have multiple bases (memory segments).
APR 2016	**5TH Edition has minor updates** including a notice on cover page to clarify that a Sigma Multi reader must be placed in a supported multifactor mode before using it. The Sigma Multi with encoded cards is not currently supported in this edition. Also a specific setup in Morpho Manager was also updated.
AUG 2016	**Inserted some tech notes to help installers and other minor updates.**
AUG 2017	Added information about importing.

1 Introduction & Requirements

This guide covers instructions for integrating System Galaxy v10.4.9 (or higher) with MorphoManager v.9.4.5 for use with MSO300 Enrollment Station v10.00.g and SIGMA Readers v1.4.1 (min. version) operating in MA5G Mode.

1.1 INTRODUCTION

System Galaxy (SG) supports enrolling biometric credentials from the Cardholder screen using ***BioBridge Enrollment Module*** /***MorphoManager Client software.***

1.1.1 SUPPORTED CREDENTIAL TYPES vs. READER MODES

Galaxy supports **MA SIGMA readers (SigmaBIO, SigmaPROX) operating in MA5G Mode**.
Galaxy supports enrolling two types of credentials (**authentication modes**) which are set up in MorphoManager Client.

Figure 1 – TABLE: Supported Readers, Modes, and Credentials (Enrolled through SG)

READER MODEL(1)	Firmware Version	Reader Mode	Reader Multi-Factor Mode Configured in Device Profile in MMC.	&	User Authentication Mode(2) Based on MMC User Policy
SigmaPROX	v1.4.1 (min)	MA5G	“Proximity Card”	=	Contactless + Biometric (in MM 10.4.16 this may be set differently)
SigmaBIO (note PROX can be downgraded to Biometric)	v1.4.1 (min)	MA5G	“Biometric”	=	Biometric Only

(1) MA500/100 readers can be used with the Sigma MA5G using BioBridge module.
(2) Smart card encoding is not supported in this release. Call tech support for future versions.

If using multiple *Authentication Types* for the same User, the SG Operator must enroll separate credentials.

The **Authentication Type** is assigned to a credential at enrollment and must match the Multifactor Mode assigned to the Reader. Incompatible credentials result in an ‘Invalid Access’. Create a new cardholder record for the credential.

1.1.2 VERSIONS & COMPATIBILITY

System Galaxy version 10.4.9 (or higher) supports the **Sigma-Prox** & **Sigma-Bio** models in MA5G mode. Any Sigma MA5G model configured for “Biometric” multifactor mode (Finger-only) – **see Section 1.1.3 for more**.

- System Galaxy software v10.4.9 (or higher)
- 635 Panels running Flash v10.4.15 (or higher – must match the released version)
- MorphoManager client/server software v 9.4.5
- Morpho MSO300 Enrollment Station v10.00.g
- SIGMA Firmware v1.4.1 for the SigmaPROX or SigmaBIO Reader
  (+12v/1A dedicated power for the SIGMA reader to avoid improper reader operation)
- Sigma LED-1 must be wired to the DRM Relay-2 to use the Sigma’s “wait for panel decision” feature.

*For integrating SIGMA Readers using Morpho Legacy mode, see the **Galaxy SIGMA Legacy Guide**. Legacy mode uses the traditional fingerprint capture and does not require MorphoManager/BioBridge software.*

For complete list of requirements, see the Requirements section of this guide.

1.1.3 How Credentials are Handled During Enrollment

Overview of how data and credentials are handled during enrollment.

1. The ***Cardholder/User*** is created in System Galaxy Cardholder screen**.**
   - The Biometric (finger) enrollment is launched from the SG Cardholder screen.
   - When the enrollment is launched, the BioBridge Enrollment Client will open and allow the SG Operator to capture the biometric data.

2. All ***Cardholder Data*** is stored in the System Galaxy database;
   - (i.e. including the User Name, Card Code, and Access Privileges)

3. During enrollment, System Galaxy passes User data to the BioBridge Enrollment Client;
   - (i.e. including First & Last Name, Card ID, and Access Group Name)

4. When enrollment is completed, the Biometric Data is stored in the MorphoManager database;
   - (i.e. along with the User First & Last Name and Card ID)

5. When enrollment is completed, the Biometric Data and Card ID are stored in the appropriate SIGMA Reader;
   - (provided Reader's Multifactor Mode matches the Authentication Mode associated with the credential)

6. When enrollment is completed, System Galaxy sets a Biometric Indicator in the System Galaxy database in the Cardholder table and in the Card table for the specific card record that enrolled biometric data.

   - a **Fingerprint Icon** appears on the Cardholder screen if a biometric data has been enrolled.
   - a **Fingerprint Icon** also appears on the specific Card Record that enrolled biometric data.

7. When a biometric card (or the Cardholder) is deleted from the System Galaxy database, the User and biometric data is likewise removed from the SIGMA Reader;
   - and User is deleted in MorphoManager database if the BioBridge User Not Found is set to "Delete".
   - or User is disabled in MorphoManager database if the BioBridge User Not Found is set to "Disable".

Important: Galaxy Control Systems does not recommend deleting the card or cardholder records from System Galaxy if you need to keep the card activity history intact.

FOOTNOTES

(1) System Galaxy must be registered for Biometric Support and the System Settings must be set to use MorphoManager as the enrollment system.

(2) MorphoManager v9.x supports 1 authentication type per User, therefore System Galaxy supports 1 Biometric Credential per Cardholder. If you need multiple credentials for different authentication types, you must make separate cardholder records.

(3) MorphoManager integration supports one User Distribution Group.

1.2 ADDITIONAL DOCUMENTATION

System Galaxy Online Guides	www.galaxysys.com/sghelp go to Documentation Menu > Current PDFs
SG v10 System Specification Guide	System specifications for the database, software, hardware, operating system; system architecture guidelines, and 3rd Party integrations;
SG v10 Software User Guide	Describes how to configure and operate System Galaxy software;
635-series Hardware Guide	Describes how to install and configure the hardware panels ;
SG BioBridge Conversion Addendum	How to convert biometric credentials from a legacy Sagem system
SG Sigma MA5G Config Addendum	How to configure SigmaMA5G with Morpho Config Tool

1.3 TERMS & DEFINITIONS – BY SYSTEM

SYSTEM GALAXY (SG) – Access Control System	
ACP & ACS [SG]	[acronyms] ACP =Access Control Panel & ACS =Access Control System.
Access Group [SG]	The entity in SG database that contains the access rules/privileges to doors (time schedules, days, holidays). At least one Access Group must be assigned to a biometric credential.
Access Card; or Card	The ***physical access credential*** that is given to a Cardholder (User) and enrolled into the System Galaxy cardholder screen. The access card is assigned access privileges and can have biometric prints associated with it during enrollment process.
Biometric Credential	A biometric credential includes biometric (fingerprint) data and must be given a valid card ID, even if a physical access card is not issued. Galaxy supports two types of Biometric Credentials with the MorphoManager - - they are Finger Only and Card + Finger. The credential is only valid at a reader that is in the correct multi-factor mode.
Cardholder [SG]	A person (or person's record) who is added to the System Galaxy database and has enrolled with an access card(s) or biometric credentials. Also called a User in the MorphoManager software.
Card Technology [SG]	The type and format of the access card – i.e. Wiegand 26bit, HID Corporate 1000, etc.; which is equivalent to the MorphoManager's Wiegand Profile.
DRM	635-series ***Dual Reader Module*** (circuit board) in the Galaxy Access Control Panel (ACP); a DRM supports two readers per board.
MORPHO MANAGER CLIENT (MMC) & BIOBRIDGE ENROLLMENT MODULE	
Authentication Type	The Auth type is the ***kind of biometric authentication*** that is assigned to a credential during enrollment (such as finger only or card+finger). This is accomplished during enrollment when the operator assigns a User Policy.
Biometric Device	A device that reads biometric credentials – i.e. a SIGMA reader for example.
Biometric Device Profile	The **device profile** defines which Wiegand Format and Multi-factor Mode the reader will use (as well as several other settings). The device profile is assigned to the reader in the MMC.
BioBridge Module	The BioBridge module is the ***fingerprint capture module*** that opens during Galaxy's biometric enrollment process. (the module can be opened independently for diagnostic purposes, but you must enroll all biometric credentials thru System Galaxy or they will not have access to the doors).
MA5G	Sigma Reader Operation Mode that is compatible with the MorphoManager/BioBridge integration.
MMC	[acronym] MorphoManager Client software.
Multi-Factor Mode	The Multi-Factor Mode is the ***reader recognition mode*** that is assigned to a biometric reader via the Biometric Device Profile. The multi-factor mode dictates which type of credential is recognized (finger only vs card-finger).
User	A person/credential that is added to a SIGMA Reader/MorphoManager database. Equivalent to SG Cardholder. Users are enrolled through SG.
User Distribution Group	The **User Distribution Group** defines the access group mapping to the readers.
User Policy (Per User)	The **User Policy** defines the ***Access Mode and Authentication Type*** (i.e. biometric only, proximity + biometric). The User Policy is assigned to the device (reader) and also must be assigned to a *biometric credential* during enrollment. A "rule triggered mismatch" indicates the credential Auth Type is not compatible with the reader's multifactor mode. ALSO NOTE: as of MM 9.4.5 the only supported ***Access Mode*** for User Policy is "Per User".
Wait for Panel Decision	Sigma feature that allows the reader to wait on the panel decision before responding as valid or invalid access. Sigma LED-1 must be wired to the DRM; and DRM Relay-2 wiring and configuration must be done.
Wiegand Profile	The **Wiegand Profile** defines the Wiegand format and its facility code/company code. It is equivalent to the 'Card Technology' in SG Cardholder enrollment screen.

1.4 INTEGRATION REQUIREMENTS

This section provides a **consolidated list of *Requirements*** for integration with MorphoManager and Sigma MA5G readers.

FOR Requirements outside the scope of this guide, see the ***Galaxy System Specification Guide***, the ***Galaxy Hardware Installation Guide,*** *or the appropriate* ***other Integration Guide*** – or contact Galaxy Technical Support. 3rd Party requirements not found in this guide, may also be found in the manufacturer's documentation.

TECH NOTE: familiarize yourself with these Requirements BEFORE proceeding to the instructions.

NOTICE: This consolidated list of requirements that must be satisfied to support this integration. Use these requirements as part of your prep checklist or as a trouble-shooting resource. ***These are not intended to replace following instructions.*** The install instructions *begin at Chapter 2 (or the appropriate section thereafter).*

1.4.1 REQUIREMENTS LIST FOR GALAXY HARDWARE

1. Galaxy supports **Standard 26b Wiegand** and **HID Corp 1000 formats** with the SIGMA Prox readers.
2. VERSION REQUIREMENT: 635 Control Panel: 635 CPU must be flashed to v10.4.15 (or higher)
3. VERSION REQUIREMENT: 635 DRM boards must be flashed to the same as the CPU

CAUTION: DO NOT INTERRUPT POWER DURING THE FLASHING PROCESS - to the controller unit, the CPU, or to any daughter boards. Interrupting power can damage the board boot and require a factory reset.

Note that a factory reset can be performed in the field using a 635-CPU. The Factory Test Guide is available from Galaxy Technical Support and may also be included on the SG software disks.

ALSO SEE: See the ***Galaxy 600-635 Hardware Guide*** for detailed flashing instructions.

4. SIGMA Data 0 must be wired to Data 0 on the DRM Reader port.
5. SIGMA Data 1 must be wired to Data 1 on the DRM Reader port.
6. (optional) SIGMA LED-1 can be wired to Relay-2 on the DRM Reader board in order to get reader response that consistently matches the Galaxy panel response for invalid or expired credentials.

If you do not wire the LED-1, the SIGMA reader can return a "valid access" response when the panel denies access (this is due to card expiration). The panel is always correct. Wiring LED-1 to Relay-2 allows the SIGMA Reader to wait for the panel response. **THE GALAXY PANEL WILL ONLY PERMIT ACCESS WHEN A CREDENTIAL IS VALID – REGARDLESS OF WHAT THE SIGMA INDICATES.** The Sigma cannot track expired and disabled cards. The panel responds based on the card active/expire date, which is stored in the panel, not the reader. SEE THE APPROPRIATE SECTION FOR WIRING TO RELAY-2.

7. **SIGMA Readers require their own dedicated power supply.**

IMPORTANT: DO NOT POWER A SIGMA READER FROM THE PANEL – a SIGMA reader may operate incorrectly or inconsistently if it is powered from the Galaxy DRM or the panel's power supply.

1.4.2 REQUIREMENTS LIST FOR SIGMA PROX READER:

TECH NOTE: familiarize yourself with these Requirements BEFORE proceeding to the instructions.

NOTICE: This consolidated list of install & configuration requirements must be satisfied to support this integration.
Use these requirements as part of your prep, install/setup checklist, or trouble-shooting resource. These are not the install instructions and are not intended to replace instructions, or be used as a shortcut.
The instructions for Installing & Configuring components begin at Chapter 2 (or the appropriate section thereafter).

1. VERSION REQUIREMENT: Firmware v1.4.1 (min) must be installed on each SIGMA Reader.
2. **Galaxy supports Standard 26b Wiegand and HID Corp 1000 formats with the SIGMA Prox readers.**
3. **You must install a separate, dedicated power supply for each SIGMA reader.** *The same is true for legacy readers***.**
4. **Input power is rated at +12V / 1A** (according to the markings on the reader – i.e. orange warning sticker). SIGMA readers require their own dedicated power supply. They will not operate properly if you power them from the DRM or panel power supply. *One symptom of incorrect voltage is flakey behavior when credentials are presented*.
5. **The Sagem install guide recommends 20-24 AWG non-stranded wiring for the data and power input.** *Galaxy recommends using shielded cable for data connections.*
6. **NOTICE: SIGMA Power/Data Connectors** use a "push-in/push-pin release" type connector to land the wires. This is explained on the instructions inside the reader packaging. To insert a wire simply push the non-stranded wire into the hole and the contacts will grab the wire. To remove a wire, you must release the contacts by inserting a pin-tool into the hole next to the contact – this will open the contacts and release the wire.
7. **NOTICE: SIGMA Wiring Pin-out Stickers** are affixed to the rear-side of the reader.

CAUTION: Avoid damaging the reader - pay close attention to how you insert the power wires. ***Inverting the power input wires will cause damage according to MorphoTrak documentation***.

8. **Reader Set-up** is done using the "**First Boot Config Assistant**", which is a Configuration Wizard that auto-launches when the unit is first powered-up.

RECOMMENDED: After the set-up is completed, the reader configuration should be made "permanent" so that the reader will always return to operational mode after a power failures. (If you do not save the setup as permanent, the reader will automatically launch *First Boot Assistant* whenever a power failure happens.)

9. Each SIGMA Reader must be given a **unique IP Address** on the network.
10. **NOTE:** You do not need to change the **Site Code** or **Facility Code** during installation of the reader. The SIGMA Reader gets it ***Site Code*** or ***Facility Code*** from the MorphoManager Client Software. The site code is configured in the Wiegand Profile and linked to the reader through complex configuration steps that are covered in the instructions. The site code/fac code will be downloaded to the SIGMA Reader once the reader has been correctly added to the MorphoManager Client (MMC).

Also see the MorphoManager Software Requirements section of this guide.

1.4.3 REQUIREMENTS LIST FOR GALAXY SOFTWARE

TECH NOTE: familiarize yourself with these Requirements BEFORE proceeding to the instructions.

NOTICE: This consolidated list of install & configuration requirements must be satisfied to support this integration.
Use these requirements as part of your prep, install/setup checklist, or trouble-shooting resource. These are not the install instructions and are not intended to replace instructions, or be used as a shortcut.
The instructions for Installing & Configuring components begin at Chapter 2 (or the appropriate section thereafter).

1. VERSION REQUIREMENT: **System Galaxy v10.4.9** (or higher) is required

2. VERSION REQUIREMENT: **MorphoManager v9.4.5** (with BioBridge Enrollment and Synchronization Module).

3. **System Galaxy must be Properly Registered with a current, valid maintenance agreement …**
   a) A valid **License Key** must be entered into the System Registration screen, if the system is a new install.
      - All remaining options must be correctly configured all the according to the purchase agreement.
      - The correct **Registration Code** must be entered into the System Registration screen & Workstation Registration. The system has a 14-day registration grace period.

   b) The number of **Total Readers** must be set to a value that includes the correct number of both biometric and non-biometric readers. You must set the number of Biometric Readers to a value that supports all biometric readers, and this must include any wall reader used for enrollment. This does not need to include an MSO-MorphoSmart Optical device. (See MMC Reqs. for using a reader as enrollment finger-capture device.)

   c) **Biometric Support** must be enabled in the System Registration screen. If your system is not currently registered for Biometric Support, contact your authorized Galaxy Dealer for customer support.

4. **System Settings screen**: System Galaxy must be configured to use "MorphoManager/BioBridge" in order for enrollment to work correctly. *This feature depends on Biometric Support being enabled in system registration*.

5. **Reader Properties screen**: The **Technology Type** must be set to "Wiegand Standard" for each Sigma Reader.

6. **(optional) Reader Properties screen**: if you want to take advantage of the Sigma's Voice Command will "wait for panel decision", you must configure the **DRM Relay 2** to pull the **Sigma LED-1** low.

   in System Galaxy Reader Properties screen ...

   a) Set **Relay-2** = **Timed Mode**
   b) Configure the relay to **Energize for 1 - 3 seconds**.
   c) check/enable the **Valid Unlock option**.

   This depends upon the LED-1 being correctly wired to the Relay-2. The Sigma will 'wait for panel decision' and display the appropriate grant or deny access. If you do not wish to take advantage of this feature and do not wire Sigma LED-1 to Relay-2, then the reader may respond with a valid access before the panel decision. If the panel decision is deny access, the panel will not unlock/open the door regardless of what the reader said. This typically affects expired credentials, where they are still in the reader. The panel decision is always correct.

7. (FYI) **Cardholder Enrollment screen**: if you have both SigmaPROX and SigmaBIO readers at the same site, you must make separate credentials for the Prox+finger and the Biometric only authentication modes. The same credential will not work at both multifactor modes. **DO NOT PUT THE CREDENTIALS ON THE SAME CARDHOLDER RECORD. MAKE SEPARATE CARDHOLDERS.**

1.4.4 REQUIREMENTS LIST FOR MORPHOMANAGER SOFTWARE

TECH NOTE: familiarize yourself with these Requirements BEFORE proceeding to the instructions. This list of install and configuration requirements must be satisfied to support this integration.

NOTICE: These are not the install instructions and are not intended to replace following instructions. Use these requirements as part of your prep, install/setup checklist, or trouble-shooting resource.

WARNING: if you are upgrading your MorphoManager system, you must back up your MorphoManager database.

1) See manufacturer's specifications for server and OS requirements.

2) **MorphoManager Server Requirements and Stipulations**:

   a) The ***MorphoManager Server.exe*** must be installed on only one computer.

   b) The computer hosting the MorphoManager Server (service) must be running and able to connect to the server/PC that runs the System Galaxy database instance. *See the appropriate section for install instructions*.

   c) You must provide a **valid SQL Server Instance name** and a **valid SA admin-level database login** during the Install process. The installer only checks whether the login credentials are present in the test connection step. It does not check whether the credentials are admin-level - - therefore the program will fail to complete the install.

WARNING: **The SQL Server Login must have "sa" <u>administrative-level</u> database permissions**. Failure to provide a login with correct permissions will result in a *catastrophic failure* when trying to install the MorphoManager database. Recovery will include doing a complete uninstall and reinstall.
SEE the Troubleshooting & Exceptions section in this guide for correct recovery methods.

CAUTION: DO NOT DROP AN EXISTING DATABASE SCHEMA IF YOU DO NOT WANT TO LOSE DATA IN IT OR INTEND TO CONTINUE USING THE EXISTING DATA.

3) The **MorphoManager Server Configuration Tool:**

   After installing the MM Server, you must run the *MorphoManager Server Configuration Tool* to configure the ADO.NET connection string (*before you install and configure the MorphoManager Client)*.

4) The ***MorphoManager Client.exe*** must be installed on <u>every</u> PC/workstation where a biometric enrollment will occur.

5) The **MorphoManager Client Configuration Tool:**

   After installing the MM Client software, you must run the *MorphoManager Client Configuration Tool* on every workstation where the MM Client is installed, **to** configure the following …

   a) (recommended) If you want the *MM Client* to manually detect the *MM Server*, the HostName/IP Address of the *MM Server must be configured*.

   b) (optional) If you want the *MM Client* to automatically detect the *MM Server*, the user can invoke the Tool to search for the server.

   c) (optional) **<u>Automatic Client Login parameters</u>** for the BioBridge Enrollment Module can be configured into the MMC Advanced Configuration Tool. This auto login option allows Galaxy to automatically log into BioBridge for every enrollment. If no login parameters are provided, the Galaxy operator will have to re-login each time an enrollment is performed in the Galaxy cardholder screen (i.e. login between every credential). Unique Operator logins can be created for each MM Client in the MorphoManager Client software.

- Requirements continue on next page. -

6) **The MorphoManager Client** must be configured with the correct settings ….

a) One **User Group** must be configured to use the specific Wiegand Profile/Card Technology that will enrolled through Galaxy (i.e. either 26bit Wiegand or Corp 1000); This type chosen for the User Group must match the system setting that is configured in the BioBridge tab (Requirement below).

b) The **System Configuration/BioBridge tab** must be configured correctly

- The Access Control System must be set to "Galaxy"
- ***ODBC client login parameters*** must be configured for thee *System Galaxy connection* (this allows the MorphoManager client to pull in the *Access Group Names.* This is a system-wide setting for BioBridge synchronization.)
- The specific ***Wiegand Profile/Card Technology*** must be configured for enrollment and synchronization from the Access Control System (i.e. either 26bit Wiegand or Corp 1000); All biometric credentials must be enrolled from System Galaxy using this card type. BioBridge will not update card types that are different from the card type configured in this tab.

NOTE: The BioBridge Client supports enrolling one Card Type. This is a requirement imposed by MorphoManager.

c) The **System Configuration/BioBridge tab** must have the *User Group Mapping* set correctly …

- MANUAL is recommended. If you use AUTOMATIC, the User Group name must be "Biometric Access" (case sensitive).

NOTE: The BioBridge Client supports one User Group/Access Group per User/Credential. This is a requirement imposed by MorphoManager. The SIGMA READER will verify the biometric credential matches the card code presented. System Galaxy will control granting and denying access to doors via the 635 control panel, based on schedules and access groups.

d) The correct Facility Code or Site Code must be configured for the appropriate **Wiegand Profile**.

e) A **Biometric Device Profile** must be created/configured with the appropriate settings:

- The Access Control System must be set to "Integrated".
- the desired Multi-factor Mode must be set to support the type of credentials to be allowed at the associated Reader (i.e. the credential's *Authentication Type* must be compatible with the Sigma Reader's *Multifactor Mode* - - i.e. Biometric (Finger Only) or Proximity Card (Prox + Biometric).

f) User Policy must be configured correctly, including the Access Mode must be set to "Per User".

g) In the Clients screen you can configure the fingerprint capture device…

- The default setting is "MorphoSmart", which is the USB MSO* 300 capture device.
- Optionally you can set it to "MorphoAccess" and click [Search] to select a reader that is already online. You can enroll from a wall-mounted SIGMA Reader. See MorphoManager documentation as needed.

  * NOTICE: the MSO firmware must be current to be compatible with MorphoManager/BioBridge.

1.4.5 REQUIREMENTS LIST for ENROLLMENT STATION (MorphoSmart "MSO300")

1) The **MSO300 Device Driver** must be installed on each enrollment workstation/pc.

> NOTE: the MSO Device Driver is installed during the *MorphoManager Client* install (MorphoManagerClient.exe).

2) The **MSO300 Enrollment Station** running firmware v 10.00.g (minimum)

> NOTE: The firmware can be upgraded with the **MSO_V10_00_g.exe** – this utility is included in the Sagem\MorphoManager folder on Disk-2 of the Galaxy Install Suite. Run the file on each workstation where the MSO needs to be upgraded.

3) The **MSO300 Enrollment Station** must be connected (USB) and indicating ready/idle state.

> NOTE: The **MSO300 Enrollment Station's LEDs** emits "Green blinking" state when MSO300 is connected and idle/ready. The finger sensor will remain "OFF" until a capture request is issued by the BioBridge Client.
>
> NOTE: The **MSO300 Enrollment Station's LEDs** emits "RED solid/on" state when MSO300 is not properly connected.

2 OVERVIEW OF EVENT COMMUNICATION

This chapter covers fundamental access control event communication and decisions.

2.1.1 Understanding Events at the System Galaxy Panel

For monitoring and audit purposes, it is helpful to understand the event transmission between each component in the two systems.

Ultimately, it is the Galaxy Access Panel that makes the final decision whether to grant or deny access.

The SIGMA reader is designed to issue a verbal and visual “access granted” when a credential and the biometric template is found and matches within the SIGMA Reader. This does not guarantee access to the door or entry point from the Galaxy system. This is because the SIGMA is not designed to understand which access privileges or which schedules are applied to the Cardholder/Credential in System Galaxy.

2.1.2 Chart of Events at System Galaxy Panel

The following chart shows the various status/conditions the user/credential can be in, and the result at the reader, panel, and what event will occur in System Galaxy.

USER / CREDENTIAL STATUS	SIGMA READER RESPONSE	PANEL RESPONSE	EVENT AT SG
User presents wrong finger	SIGMA will DENY – Biometric Mismatch	Panel will deny access	NOT IN SYSTEM 🔒
User presents correct finger at a reader that is set to a Multifactor Mode that does not match the authentication type on the credential	SIGMA will DENY – Rule Triggered Biometric Mismatch (ex: Credential enrolled as *Biometric* Auth Type presented at reader using *Prox Mode*)	Panel will deny access	NOT IN SYSTEM 🔒
User is expired or disabled in SG	SIGMA may prompt VALID ACCESS*	Panel will deny access	NOT IN SYSTEM
User is deleted from SG	SIGMA Access Denied (User Not Found)	Panel will deny access	NOT IN SYSTEM 🔒
User does not have access at door	SIGMA may prompt VALID ACCESS *	Panel will deny access	**INVALID ACCESS**
User is not within scheduled access	SIGMA may prompt VALID ACCESS *	Panel will deny access	**INVALID ACCESS**
User presents correct finger	**SIGMA will GRANT credential**	**Panel will grant access**	**VALID ACCESS**

*** MATCH PANEL RESPONSE: if the Sigma Reader is set up for “Wait for Panel Response”, the Sigma will display “Access Denied” whenever the Galaxy Panel denies access. To make the reader wait for panel, the Sigma LED1 must be wired to Relay-2 of Galaxy DRM board, the Sigma will wait for the Panel Response and will match the panel decision.**

NOTE: if the SIGMA does not identify the user (user not found), the reader will issue “access denied” and send the card code with a ‘0’ site code to the Galaxy Panel. This will result in a NOT IN SYSTEM in System Galaxy. Right-clicking the incoming card code will not discover an existing cardholder record it normally would from another reader since the SIGMA passes a ‘0’ site code. However you can right-click the incoming card code to discover the card ID and then search for it in your system database.

2.1.3 System Galaxy Events Explained

The following list shows the events that come from the Galaxy Access Panel and the various reasons/conditions that cause the event to occur.

Ultimately, it is the Galaxy Access Panel that makes the final decision whether to grant or deny access.

The SIGMA reader is designed to issue a verbal and visual "access granted" when a credential and the biometric template is found and matches within the SIGMA Reader. This does not guarantee access to the door or entry point from the Galaxy system. This is because the SIGMA is not designed to understand which access privileges or which schedules are applied to the Cardholder/Credential in System Galaxy.

NOTE: if the SIGMA does not identify the user (user not found), the reader will issue "access denied" and send the card code with a '0' site code to the Galaxy Panel. This will result in a NOT IN SYSTEM in System Galaxy. Right-clicking the incoming card code will not discover an existing cardholder record it normally would from another reader since the SIGMA passes a '0' site code. However you can right-click the incoming card code to discover the card ID and then search for it in your system database.

"VALID ACCESS": the Galaxy panel sends a VALID ACCESS event for the following reasons

- the card ID is in the panel, and the assigned access group /time schedule that is permitted access at the time the card is presented (and the user presented a valid finger at the SIGMA).

"INVALID ACCESS" ATTEMPT: the Galaxy panel returns an INVALID ACCESS event for the following reasons:

- the card ID is in the panel, but it is assigned to a schedule that does not have access at the time the card was presented.
- the card ID is in the panel, but it is not assigned to any Access Group.
- the card ID is in the panel, but it is expired or disabled.

"NOT IN SYSTEM" EVENT: the Galaxy panel returns a NOT IN SYSTEM event for the following reasons:

- the card ID is not in the panel - because the card does not have access to any door at the panel (the card ID may be in other panels if it has been assigned access;
- the card ID is not in the panel - because the card has not been enrolled or has been deleted;
- the card ID is not in the panel – because the card was not loaded due to a network disconnect between the controller and the SG software at the time the card was added in SG.
- Not In System events are also caused when the **Sigma reader passes a 0 site code or facility code** – and this happens when …
  - the user/card is not loaded to the Sigma reader (check the User Group is configured for All Readers or the credential is correctly associated User Group that is assigned to the Reader.
  - the user/card was deleted from the SG system – and removed from the reader.
  - the user/card was deleted from the MorphoManager software (not recommended).
  - the card technology did not match the Wiegand profile chosen MorphoManager User Group/Device Profile.
  - the card's site code did not match the Wiegand profile .
  - the Device Profile was not configured to connect to the reader in question.
  - the user presented the wrong finger and received a biometric mismatch.
  - the wrong person is trying to use the card and gets a biometric mismatch.

2.2 ON-LINE EVENTS EXPLAINED

To Galaxy, “Online events” means the Galaxy access control panel is able to communicate with the System Galaxy database and communication server.

2.2.1 ACCESS DECISIONS AT THE PANEL

The panel always makes the access control decisions based on access privileges and cardholder programming that is stored in the memory of the panel, regardless of whether the server/database is online or not.

When the panel is online with the Server and Database, it immediately transmits the access decision (granted or denied) to the Software monitoring screen where the SG operator can monitor the event as well as logging the event the database for system reporting.

2.2.2 UNINTERRUPTED EVENT LOGGING

Since SG uses true background services, Operators can sign in & out of SG software, or sign in & out of PC user account, without interrupting the event communication between the panels and the SG Database. The core GCS services continue operation as long as the PC is powered on. Therefore, events that occur while the SG software is logged out/shut down, or while the user is logged out of the PC OS, will be available from System Reports based on the logging to the database.

2.3 OFF-LINE EVENTS EXPLAINED

“Offline events” means the Galaxy panel is unable to communicate with the System Galaxy database.

The Galaxy 600 panel is designed to remain fully operational during an ‘off-line’ condition and continues to provide uninterrupted access control decisions. Events are stored at the panel until the connection to the database is restored; at which time the panel retransmits all buffered events to the database.

» This can occur if the Communication/Database Server, database engine, or core GCS Services are down.

» Access decisions are based on the rules stored in the panel’s memory.

» Offline events are available in SG Activity History Reports after the event buffer has been transmitted.

3 Configuring Hardware

This chapter covers how to install the SIGMA Reader on the 635 Galaxy Panel.

3.1 ABOUT INSTALLING THE 635-SERIES HARDWARE

Properly install the Controller, the CPU board and DSI board according to the instructions in the Galaxy Hardware Manual.

3.1.1 The Galaxy Hardware Panel & CPU

1. **GALAXY Controller (access control panel)**
    - **635 CPU Board** - with v10.4.15 S28 flash code (or higher)
    - **635 DRM Board** - with v10.4.15 flash (or higher)

2. **When you install the Galaxy access control panel, you must configure the 635 CPU.**
   You can configure it using the 635 Web Configuration Tool (see the Web Config Tool Guide).
   Basically you can launch Web Config the tool on a PC/Laptop that is running on the same network segment as the access panel. The Web Tool with pick up all 635 CPUs on the network by their MAC Address and display them by their serial number. Once you select the correct serial number of the CPU you need to configure, you can program the network address and other settings. Then you can simply enter the new IP Address of the CPU into the browser search bar and pull back the Panel Programming screen and also see all the boards that are connected to the CPU. Boards can be updated/flashed, configured and tested via the Web interface.

ALSO SEE: the ***Galaxy 600-635 Hardware Guide*** for installation and flashing instructions in more detail.

The main **635 Hardware Installation manual** provides hardware & flash requirements, and installation instructions for the 600-series hardware, CPU and its daughter boards.

These step-by-step instructions cover installing and configuring the boards, flashing, and how to wire the field devices (readers, relays, inputs, outputs, etc.).

- You can find the manual on the Software Install CD (disk-2).
- You can also the manuals them on the Galaxy website www.galaxysys.com. Click on the **Support** link on the left side menu, then click **Technical Support**; then locate **Documentation** at the bottom of the Tech Support page.

3.2 ABOUT INSTALLING THE SIGMA HARDWARE

Consult the MorphoTrak Install Guide to physically mount the reader to the wall.
The reader flips forward to allow access to the connectors.

3.2.1 Wiring the MA SIGMA Reader at Galaxy Controllers

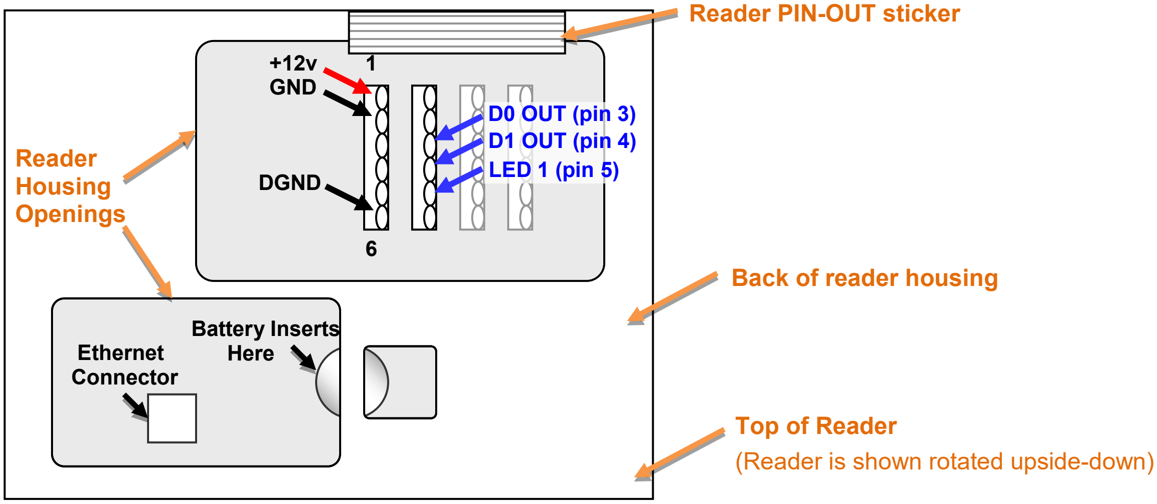
The SIGMA reader supports the reader wiring and is compatible with the 635 DRM Board. The Sagem install guide recommends 20-24AWG, non-stranded wiring. Galaxy recommends 22 AWG shielded cable.

1. Turn the reader to the back side where you can see the connectors. Rotate the reader upside-down so that the ***wiring pin-out stickers*** are upright/readable.
2. Locate the first two connectors (from the left) that are used for **power input** and **data wiring**.
3. On the second connector, insert the Data-0 (D0out) into pin-3, & Data-1 (D1out) into pin-4 .
4. On the first connector, insert the Data-GND Wire (DGND) into pin-6.
5. Wire the Data 0 of the SIGMA to Data-0 of the 635 DRM board.
6. Wire the Data 1 of the SIGMA to Data-1 of the 635 DRM board.
7. (OPTIONAL) Wire the LED-1 of the SIGMA to LED-1 of the 635 DRM board (this allows the valid access from the Galaxy access control panel to control the Valid Access Prompt at the Sigma Reader.
8. Wire the Data GND at the correct terminals of the 635-DRM Board Ground the drain-wire of the reader cable shielding to ground at the Galaxy DRM reader terminal.
9. Wire power to the reader from an **adequate power adapter (+12Vdc/1A) being careful to observe polarity**.
   a. Insert **+12V power input wire** into **pin-1** of the first connector
   b. Insert the **ground wire** into **pin-2** of the first connector.

WARNING: Observe polarity. Before applying power to the Sigma reader, be sure to reference the PIN-OUT STICKER on the back of reader. Correctly match the wiring according to the reader markings.

10. Install (insert) the 3v battery into the battery slot.
11. Connect Ethernet cable to RJ45 jack.
12. Once you test the reader for correct card/biometric recognition, you can permanently mount the reader to the wall using the Sagem mounting instructions that came with the reader packaging.

Figure 2 – SIGMA READER (BACK / INVERTED VIEW)



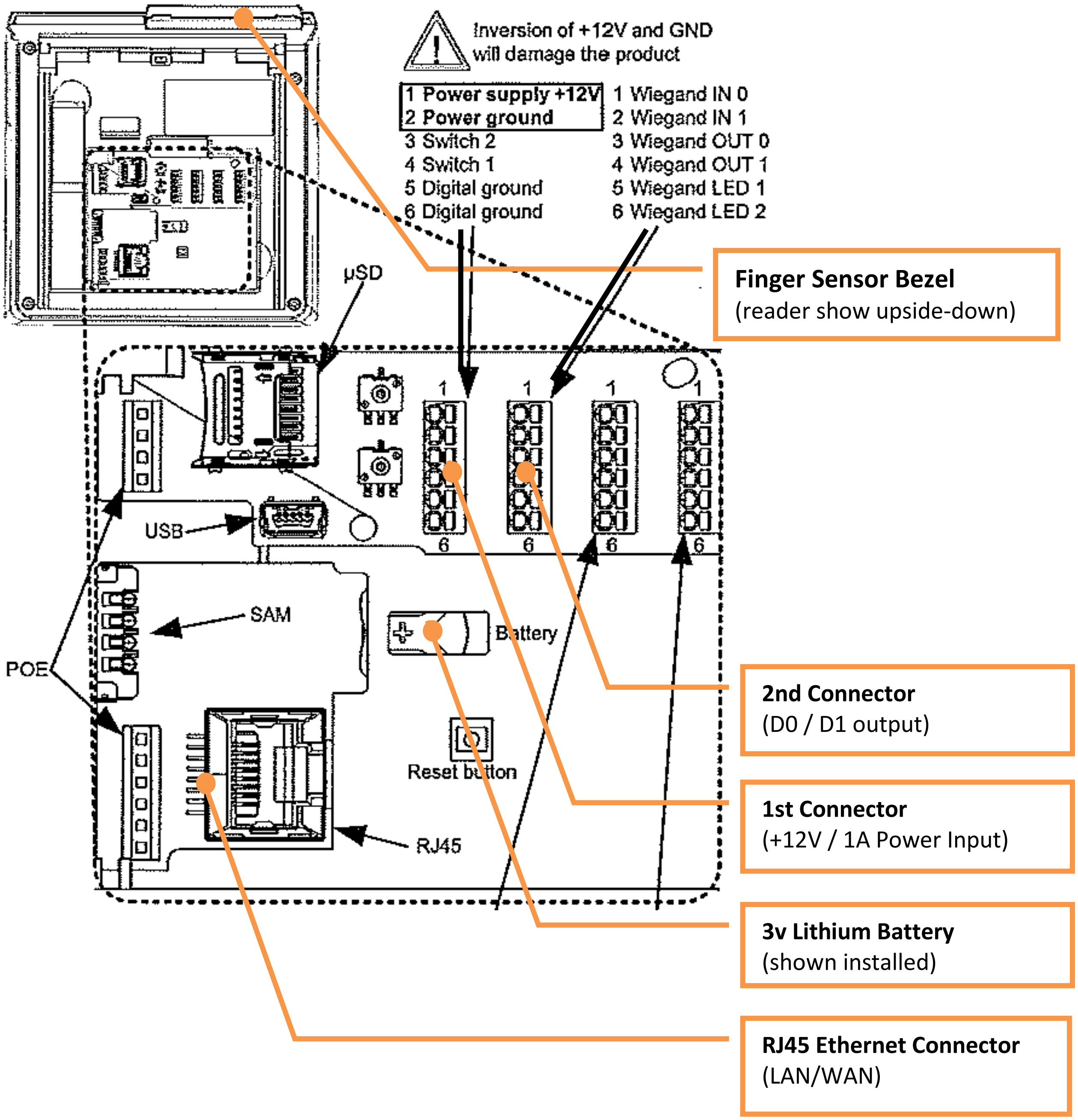
You may need to turn the reader upside-down to read the pin-out sticker.

3.2.2 From the Morpho Installation Quick Guide

The SIGMA Reader comes with a pictogram (no words) installation sheet.

On the front page (top right corner), is the ***pin-out diagram*** *of the Sigma reader as viewed from the back with the reader turned upside-down.*

Figure 3 – SIGMA READER DIAGRAM FROM (BACK/ INVERTED VIEW)



Inversion of +12V and GND will damage the product

1 Power supply +12V	1 Wiegand IN 0
2 Power ground	2 Wiegand IN 1
3 Switch 2	3 Wiegand OUT 0
4 Switch 1	4 Wiegand OUT 1
5 Digital ground	5 Wiegand LED 1
6 Digital ground	6 Wiegand LED 2

Finger Sensor Bezel
(reader show upside-down)

2nd Connector
(D0 / D1 output)

1st Connector
(+12V / 1A Power Input)

3v Lithium Battery
(shown installed)

RJ45 Ethernet Connector
(LAN/WAN)

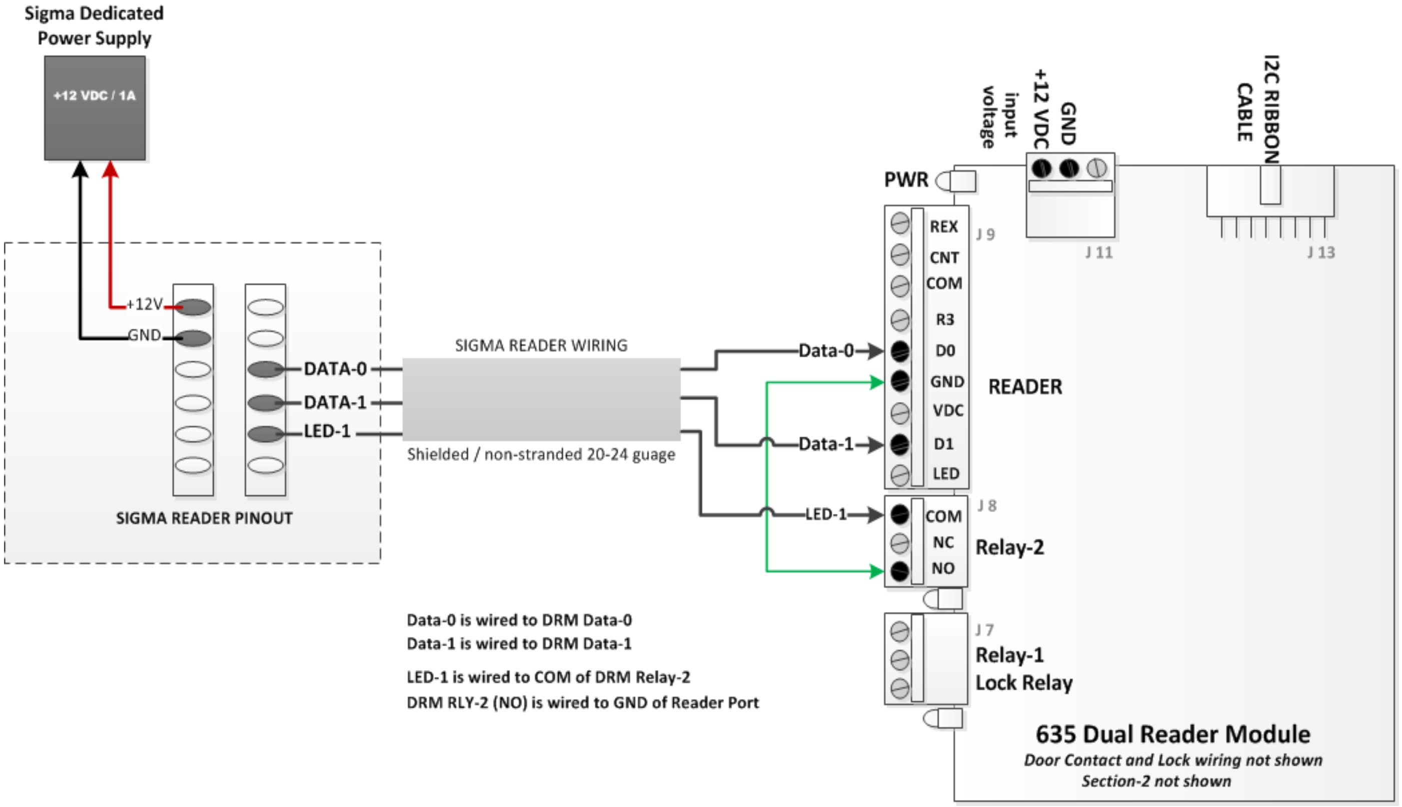
3.2.3 Wiring the SIGMA to the Galaxy Panel (DRM Board)

The SIGMA Reader can use the "wait for panel decision" function by wiring LED-1 to Relay-2. The diagram below shows how to wire the SIGMA to use Relay-2 to pull the LED-1 signal to ground.

1. Wire Sigma Data-0 to the Data-0 contact on the DRM Reader Section
2. Wire Sigma Data-1 to the Data-1 contact on the DRM Reader Section
3. Wire Sigma LED-1 to the COM Contact on the DRM Relay-2
4. Wire DRM Relay-2 (NO) contact to the GND contact on the DRM Reader Section

5. The Sigma Reader must have a separate power supply. Do not power a Sigma reader from the DRM board or from the Galaxy controller's power supply.

Figure 4 – WIRING A SIGMA READER TO THE PANEL (635-DRM BOARD)



Data-0 is wired to DRM Data-0
Data-1 is wired to DRM Data-1

LED-1 is wired to COM of DRM Relay-2
DRM RLY-2 (NO) is wired to GND of Reader Port

3.3 PROGRAMMING THE SIGMA READER

The Sigma reader programming is basically the same as the 500-series in that you can manually edit the biometric control settings, network parameters, card formatting, etc.

1. Power ON the reader. The 'Boot Assistant' app will open automatically.

2. Enter the password when prompted (factory default = 12345).

3. Set up the Network Configuration as follows:

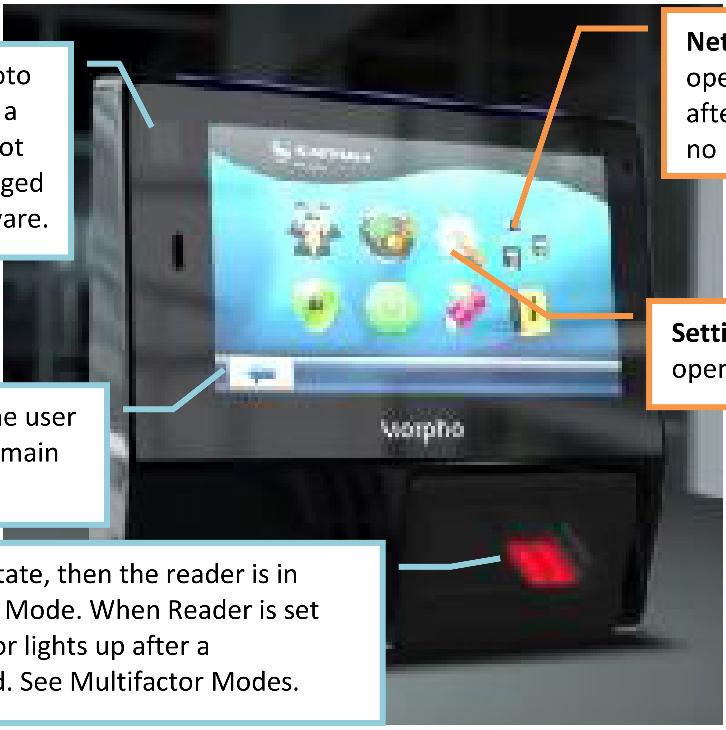
   - **Choose "Ethernet"** and **"IPv4"**
   - **Static Mode:** Enter IP, Subnet, and Gateway addresses (recommended; DNS 'OFF/disabled').
   - **Protocol Config:** choose "**MA5G**"
   - **Create a new password** (recommended)
   - **First Boot Config Storage:** (recommended) choose "**permanent**" to prevent the Boot Assistant from launching in the event of future power failures, and needing to reconfigure reader.

   > Once the **storage mode** is set to "permanent", user can open the 'Config. Assistant' by pressing the [lock icon], located on the reader's home screen. Enter the password to access settings.

4. **Exit the Boot Assistant** by pressing the back arrows to return to the home screen.

5. **The remainder of the configuration is done through the MorphoManager Client software.**

Figure 5 – SIGMA READER (FRONT VIEW)



Reader Camera – takes a photo of person at the reader when a biometric mismatch or user not found occurs. Pictures are logged in the MorphoManager Software.

Network Config. Icon – (tap) opens to Network Configuration after the 1st Boot Assistant is no longer in use.

Settings Config. Icon – (tap) opens to Reader Settings.

Menu Back Button – takes the user back to previous screen or to main screen.

Finger Sensor – if lit in Idle state, then the reader is in 'Biometric Only' (Finger Only) Mode. When Reader is set for Proximity Mode, the sensor lights up after a valid/known card is presented. See Multifactor Modes.

4 CONFIGURING SYSTEM GALAXY SOFTWARE

WARNING (!) FOR UPGRADING SYSTEMS: BEFORE YOU RUN the System Galaxy Upgrade , YOU MUST BACK UP your existing databases and all loose assets such as finger template files, reports, photos, badge templates, icons, symbols, sound files, video files, etc. Place your back-ups in a safe folder that is not on the Galaxy PC.

4.1 ABOUT UPGRADING SYSTEM GALAXY SERVER

This section covers information and warnings about upgrading.

WARNING: if you are upgrading an existing System Galaxy system, you must back up your SysGal and SysGalArc database BEFORE you proceed with your upgrade.

WARNING: Back up all assets, including finger templates and other System Galaxy assets also. In older versions of System Galaxy, the finger templates were stored either in the finger templates folder under System Galaxy folder on the Main Communication Server or other specified location. More recent versions of System Galaxy stored fingerprint templates in the SysGal database.

WARNING: FAILURE TO PROPERLY PERFORM BACK-UPS OF DATABASES AND OTHER ASSETS COULD LEAD TO LOSS OF DATA THAT CANNOT BE RECOVERED IF ANYTHING GOES WRONG DURING THE UPGRADE PROCESS.

4.1.1 Backing up Databases on SQL Server

1. Open your ***SQL Server Management Studio Tool*** and log in with administrator-level permission.
2. Expand the “Databases” branch and select your database name.
3. Right-click and select **‘Tasks > Back Up…’** from the context menu.
4. Perform the necessary steps and click OK to create the backup file.
5. Copy all backed-up databases and other assets to a separate server/secure location.

4.1.2 Backing up all assets on Servers & Clients

Always perform back-ups of all assets at each server and all clients before running any upgrades or installations.

NOTE: System Galaxy assets can include the SysGal & SysGalArc databases, cardholder photos (main & alternate), digital signatures, dossiers, badges/templates, logos & graphics used for badges & dossiers, time punches, biometric finger templates, custom report templates, custom SQL scripts, system logs, system-generated reports, graphic symbols for devices, alarm sound files, floor plans, (etc.). Copy all backed-up assets to a separate/secure server.

4.2 QUICK STEPS FOR INSTALLING SYSTEM GALAXY SERVER & DATABASE

These are abbreviated instructions for installing System Galaxy.

PREREQUISITES:

- This part must be performed by an Authorized Dealer.
- After backing up any assets and your SG databases, you are ready for upgrading.
- Installer must use an administrator-level OS login and use "run as administrator" when installing.

A. **INSTALLING the SG Database server…**
This is typically a different computer than the main communication server.

Part 1. Install the Prerequisites: (required)
This installs the .NET 4.5 Framework and other required components.

Part 2. Install/Upgrade the Database:
This installs the MSSQL Database Engine, MSSQL Management Studio and the System Galaxy databases (or upgrades the existing databases) depending on the choices made.
SG 10.4.9. installs SQL 2014 64Bit; but remains compatible with SQL 2008/2008-R2 32b/64b for upgrades.

Part 3. (optional) Install the SG Software – supported for diagnostic and administrative:

- You can install option B, which only lays down the SG Software (no active services).
- Or if you do want to run your services on the same computer as the database, you can install option A, which will install all the services with the core operating services enabled to start /run automatically.

Keep in mind that launching SG at this server will temporarily usurp one client seat - therefore if you did not purchase a client seat specifically for this computer, one of your other clients cannot be running while this client is logged into the database. You can add (purchase) a client seat for this server and thereby avoid interrupting other clients while this one is in use.

NOTICE: Galaxy does not support 3rd party integrations on a MS-Server Operating Systems (i.e. biometric enrollment or other integrations). Galaxy has no control over whether 3rd party software or drivers are compatible on a server platform.

B. **INSTALLING the main SG Communication Server separately form the main server …**

Part 1. Install Prerequisites: (required)
This installs the .NET 4.5 Framework and other required components.

Part 2. Install MS-SQL ODBC Client Components: (required)
This installs the ODBC Client Components.

Part 3. Install SG Software Components:
Choose option A which lays down all the GCS Services and installs the SG Software. The core GCS Services are installed to run automatically. Services that support peripheral interfaces must be configured to start automatically by the installing technician or administrator.

C. **INSTALLING the SG Client (such as an Enrollment or Monitoring Workstation)…**

Part 4. Install Prerequisites: (required)
This installs the .NET 4.5 Framework and other required components.

Part 5. Install MS-SQL ODBC Client Components: (required)
This installs the MS-SQL ODBC Client Components (Required on all servers and clients).

Part 6. Install SG Software Components:
Choose option B which only lays down the SG Software (no active services).

4.3 CONFIGURING THE SYSTEM GALAXY SOFTWARE

The **System Galaxy** software must be …

1. registered for biometric support and the number of biometric readers that will be installed.

2. configured to use the BioBridge integration

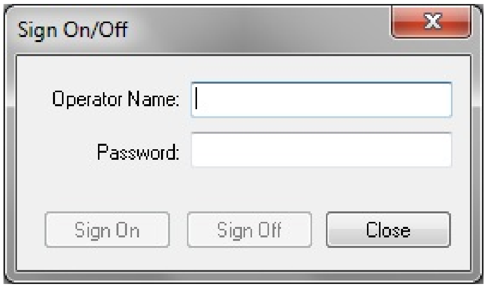
3. and SIGMA reader properties must be programmed.

4.3.1 Signing-in to the System Galaxy Software

Launch System Galaxy software and sign-in as a master operator.

1) Double-click the **SG icon** on the desktop of the Communication server.
2) Supply the **operator name** and **password** for a **Master-level operator**.
3) Click [Sign On] button.

Figure 6 – System Galaxy: Logging into System Galaxy



4.3.2 Configuring System Registration

All product-levels support the registration/licensing of biometric readers.

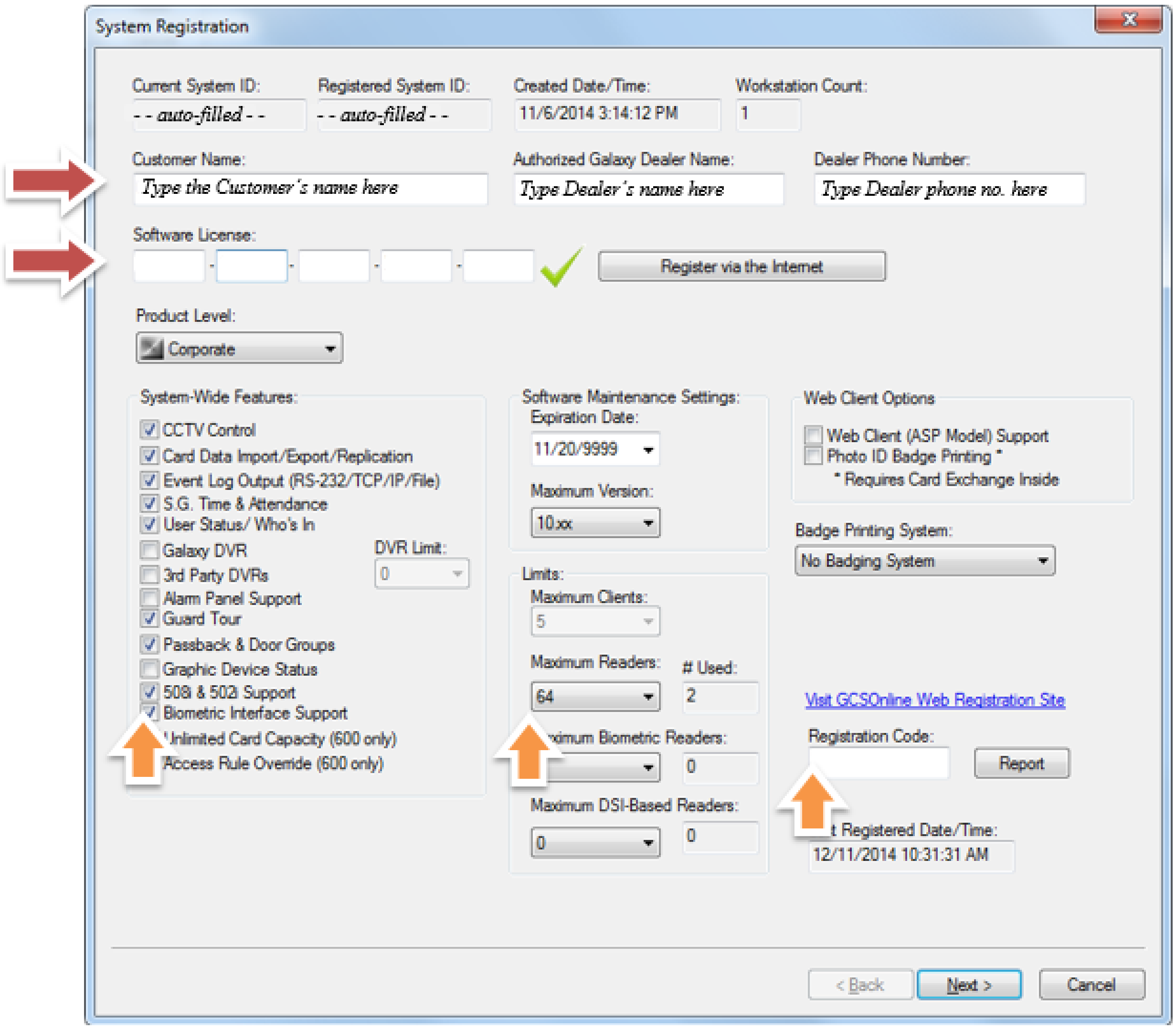
PREREQUISITES:

- Dealer must be signed-in as a master operator to open the System Registration screen.
- Registration must be performed by an Authorized Dealer in contact with Galaxy Dealer Support or the Galaxy Registration Website.

Open the Registration Screen from SG menu: select ***Configure > Options > Registration > System***

1. Enter the Customer Name, Dealer Name and Phone.
2. Enter the valid License Key (came with your purchase order)
3. Click the [Register via Internet] button – to open a dialog box and fill out all the fields as appropriate. *NOTE: the Biometric Support, readers, and Registration Code should be auto-filled appropriately.*
4. Click [Apply or NEXT] in SG to save System Registration and complete the workstation registration.

Figure 7 – System Galaxy: System Registration Screen



System Registration

Current System ID: -- *auto-filled* --

Registered System ID: -- *auto-filled* --

Created Date/Time: 11/6/2014 3:14:12 PM

Workstation Count: 1

Customer Name: *Type the Customer's name here*

Authorized Galaxy Dealer Name: *Type Dealer's name here*

Dealer Phone Number: *Type Dealer phone no. here*

Software License: - - - - ✓ [Register via the Internet]

Product Level: Corporate

System-Wide Features:

☑ CCTV Control
☑ Card Data Import/Export/Replication
☑ Event Log Output (RS-232/TCP/IP/File)
☑ S.G. Time & Attendance
☑ User Status/ Who's In
☐ Galaxy DVR
☐ 3rd Party DVRs
☐ Alarm Panel Support
☑ Guard Tour
☑ Passback & Door Groups
☐ Graphic Device Status
☑ 508i & 502i Support
☑ Biometric Interface Support
'Inlimited Card Capacity (600 only)
Access Rule Override (600 only)

DVR Limit: 0

Software Maintenance Settings:
Expiration Date: 11/20/9999
Maximum Version: 10.xx

Limits:
Maximum Clients: 5
Maximum Readers: 64 # Used: 2
ximum Biometric Readers: 0
Maximum DSI-Based Readers: 0 0

Web Client Options
☐ Web Client (ASP Model) Support
☐ Photo ID Badge Printing *
* Requires Card Exchange Inside

Badge Printing System: No Badging System

Visit GCSOnline Web Registration Site

Registration Code: [Report]

t Registered Date/Time: 12/11/2014 10:31:31 AM

4.3.3 Configuring System Settings in SG

The system must be configured for the correct Biometric System integration.

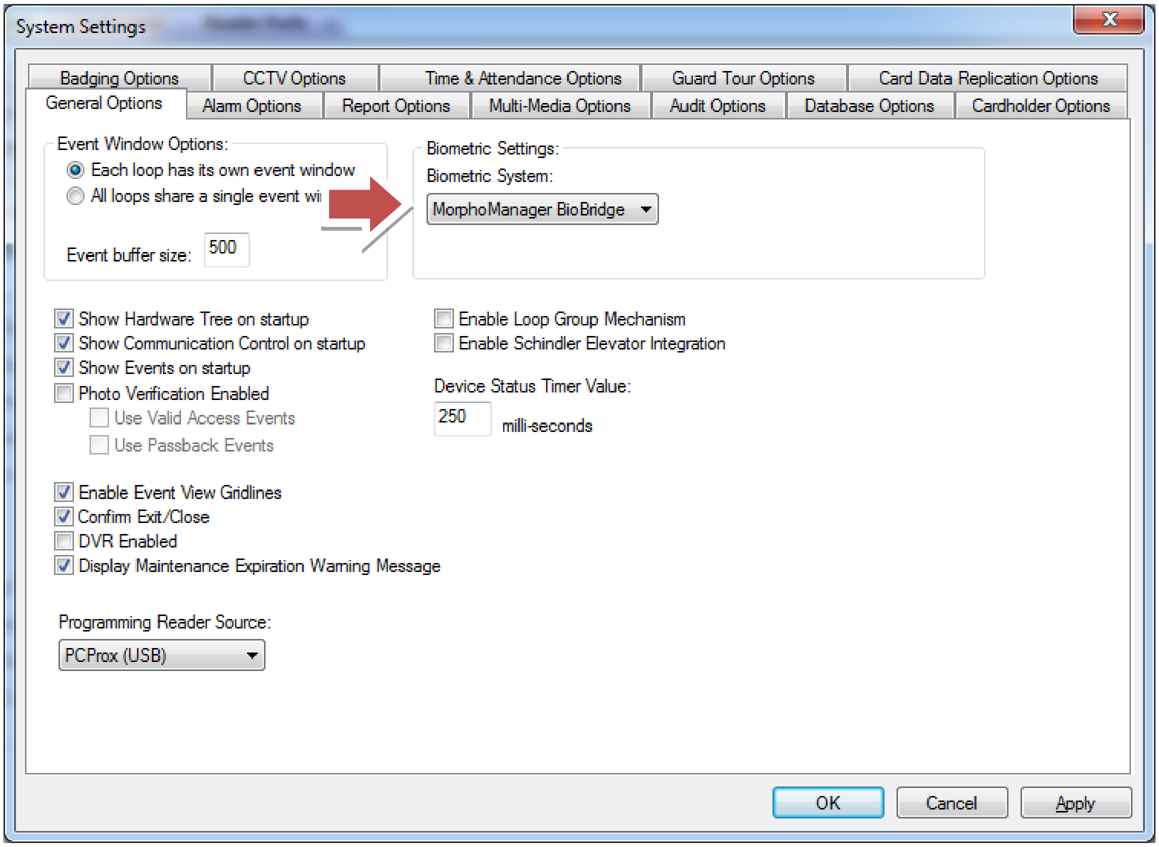
PREREQUISITES:

- To open the System Settings screen, you must be signed in as a master operator.
- The system must be registered for biometric support.

Open the Registration Screen: select *Configure > Options > System Settings*

1. Select the *General Options* tab
2. Choose the "**MorphoManager BioBridge**" option in the Biometric System droplist.
3. Click [Apply] to save changes.
4. **IMPORTANT! Restart the SG Software** to initialize all registration and system settings.

Figure 8 – System Galaxy: Biometric System Setting



Event Window Options:
● Each loop has its own event window
○ All loops share a single event wi

Event buffer size: 500

Biometric Settings:
Biometric System: MorphoManager BioBridge

☑ Show Hardware Tree on startup
☑ Show Communication Control on startup
☑ Show Events on startup
□ Photo Verification Enabled
□ Use Valid Access Events
□ Use Passback Events

☑ Enable Event View Gridlines
☑ Confirm Exit/Close
□ DVR Enabled
☑ Display Maintenance Expiration Warning Message

Programming Reader Source: PCProx (USB)

□ Enable Loop Group Mechanism
□ Enable Schindler Elevator Integration

Device Status Timer Value: 250 milli-seconds

4.4 CONFIGURING READER PROPERTIES IN SYSTEM GALAXY

This section only covers reader options that are specifically related to integrating Sigma Readers when using the MorphoManager interface as you configured in the Galaxy *System Settings screen*. (This guide does not apply to *Sigma Legacy Mode* or to integrating with traditional *Sagem Biometric* or legacy versions that supported MA520/MA100/110 Readers for traditional biometric enrollment.)

Reader/Door properties must be configured in System Galaxy for the Galaxy panel to integrate with a Sigma reader.

PREREQUISITES:

- The reader type must be set to Wiegand Standard
- Relay-2 must be configured if the Sigma Reader is using LED-1 to "wait for panel decision"*.

See the ***System Galaxy Software User Guide*** for reader properties that are outside the scope of this guide.

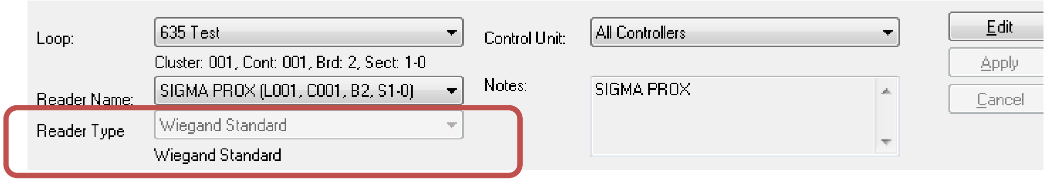
4.4.1 Setting Reader Properties in System Galaxy

Open the Reader Properties screen: click on the Door button on the SG toolbar **…**

{Or from the menu, select ***Configure > Hardware > Reader Ports}***

1. Select the correct **loop** name and **control unit** name that your Sigma reader is connected to.
2. Select the specific **Reader (by Name)** you are setting up.
3. Click the Edit button.
4. (recommended) **change the Reader Name** (up to 65 characters) to something that better identifies the reader (i.e. Room 101; supply closet). The system mapping is still displayed above the reader name field.
5. **(required) Set the Reader Type field to "Wiegand Standard".**
6. (recommended) Click the Relay-2 Options tab – to configure the Sigma for "follow panel decision"
7. Select "**Timed Mode**"
8. Set the [**Energize For**] field to **"1" or "2" seconds**.
9. Check **Valid Unlock*** (causes Relay-2 to energize when an Access Credential is presented). The SIGMA Reader will 'wait for the panel decision' before it displays/voices "Valid Access" or "Access Denied" (as appropriate). *Remember that the Sigma LED1 must be properly wired to Relay-2, as shown in prior section*.
10. **Click APPLY to save.**

Figure 9 – System Galaxy: Reader Properties for a SIGMA Reader (with LED-1 follows panel decision)



Loop: 635 Test

Cluster: 001, Cont: 001, Brd: 2, Sect: 1-0

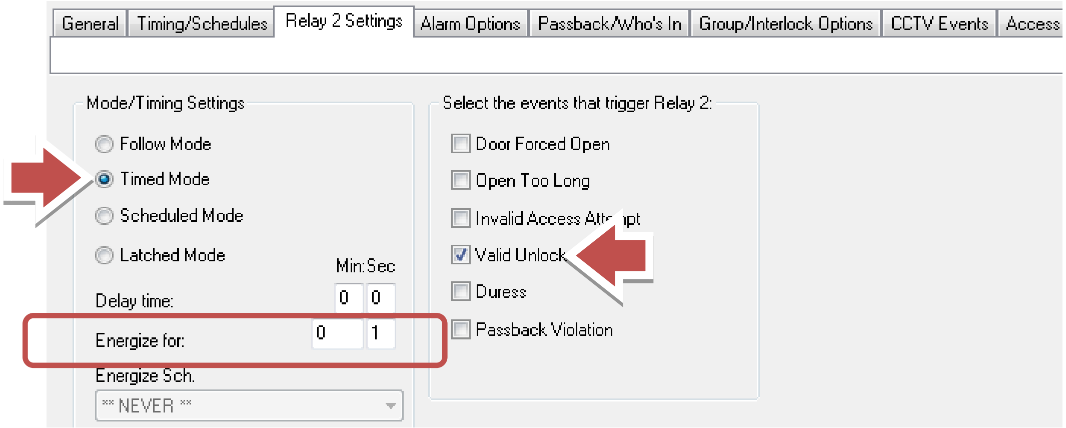
Reader Name: SIGMA PROX (L001, C001, B2, S1-0)

Reader Type: Wiegand Standard

Wiegand Standard

Control Unit: All Controllers

Notes: SIGMA PROX



Mode/Timing Settings

○ Follow Mode
● Timed Mode
○ Scheduled Mode
○ Latched Mode

Min:Sec

Delay time: 0 0

Energize for: 0 1

Energize Sch. ** NEVER **

Select the events that trigger Relay 2:

□ Door Forced Open
□ Open Too Long
□ Invalid Access Att pt
☑ Valid Unlock
□ Duress
□ Passback Violation

4.5 SYSTEM GALAXY ACCESS PRIVILEGES

This section covers how access groups are used and are mapped to the User Distribution Group from a System Galaxy perspective.

SG 10.4.9 (or later) provides one *Access Group Name* called "Biometric Access". It will appear in the MorphoManager Client Software in the *System Configuration > BioBridge setup screen*, and must be mapped to the User Distribution Group. The User Distribution Group is explained in a later section in the MorphoManager configuration.

4.5.1 Importing the Access Group Name (Biometric Access) into MorphoManager

MorphoManager must auto-import the "Biometric Access" ***access group name into the BioBridge configuration screen.***

- The name is automatically imported into MorphoManager when the SG database connection is configured in the BioBridge tab of MorphoManager Client.
- Notice: the default name "Biometric Access" cannot be changed.
- After the "Biometric Access" is imported, it must be mapped to the desired User Distribution Group.

Currently, the MorphoManager integration supports only one User Distribution Group per user.

See section 6.7 CONFIGURING A USER DISTRIBUTION GROUP in this guide for instructions about configuring and mapping the User Distribution Group in the MorphoManager Software Configuration.

4.5.2 About Assigning Access Privileges to a System Galaxy Cardholder

During the initial cardholder/card enrollment, you must assign at least one ***active access group*** to the card before you can enroll any fingers. However, the BioBridge Enrollment module queries the associated User Group (based on mapping to the Access Group Name in MMC). This is how the BioBridge determines which Authentication Types are available for enrollment.

It does not matter whether you use Access Profiles, Access Groups, or Personal Doors as long as you have selected at least one ***active access group***.

The operator cannot enroll biometrics if all Access Groups are set to "NO ACCESS" in Cardholder.

See the **System Galaxy User Guide** for instructions on how to preconfigure time schedules, access groups, and access profiles. Personal doors are assigned at the Cardholder screen.

5 Installing the MorphoManager /BioBridge Software

WARNING (!): **DO NOT DROP YOUR SCHEMA until you have backed up the database! Dropping your schema will delete your existing MorphoManager database and all your data!** Contact Morpho for technical support relating to upgrading your system.

5.1 ABOUT UPGRADING MORPHO MANAGER SERVER

This section covers information and warnings about upgrading an existing MorphoManager server/database.

UPGRADE WARNING: ALWAYS BACK UP the MorphoManager database BEFORE you proceed with the running the MorphoManager upgrade.exe. Failure to back up databases risks losing data that may not be recoverable.

UPGRADE WARNING: Back up all assets, including finger templates and System Galaxy databases also. System Galaxy, the finger templates were stored either in the finger templates folder under System Galaxy folder on the Main Communication Server or other specified location. More recent versions of System Galaxy also stored fingerprint templates in the SysGal database.

WARNING: FAILURE TO PROPERLY PERFORM BACK-UPS OF DATABASES AND OTHER ASSETS CAN LEAD TO LOSS OF DATA THAT CANNOT BE RECOVERED IF A CATASTROPHIC FAILURE HAPPENS DURING THE UPGRADE.

5.1.1 General Info on Backing up Databases on SQL Server

1. Open your ***SQL Server Management Studio Tool*** and log in with administrative-level permission.
2. Expand the **"Databases" branch** and select the MorphoManager database name.
3. Right-click and select **'Tasks > Back Up…'** from the context menu.
4. Perform the necessary steps and click OK to create the backup file.
5. Also back up the ***SysGal & SysGalArc Databases***, as needed – for example, if you are also upgrading System Galaxy or you do not have a current back-up copy of the Galaxy databases. (NOTICE: in prior versions of SG, fingerprints are stored in the Galaxy database and/or also as discrete files, depending on version of SG. SG-9x and older stored configuration.)
6. Copy of all backed up databases and assets to a separate, secure server/location.

5.1.2 Backing up all assets on Communication Servers & Clients

Always perform back-ups of all assets at each server and all clients before running any upgrades or installations. MorphoManager Database, Error logs, and camera snapshots, reports, etc. should be backed up on a secure server. Also, reader biometric profiles can be exported to a separate file if desired – see Morpho documentation for details.

NOTE: System Galaxy assets can include the SysGal & SysGalArc databases, cardholder photos (main & alternate), digital signatures, dossiers, badges/templates, logos & graphics used for badges & dossiers, time punches, biometric finger templates, custom report templates, custom SQL scripts, system logs, system-generated reports, graphic symbols for devices, alarm sound files, floor plans, (etc.). Copy all backed-up assets to a separate/secure server.

5.2 INSTALLING MORPHO MANAGER SERVER

The following file must be executed to install the Sagem MorphoManager Software.

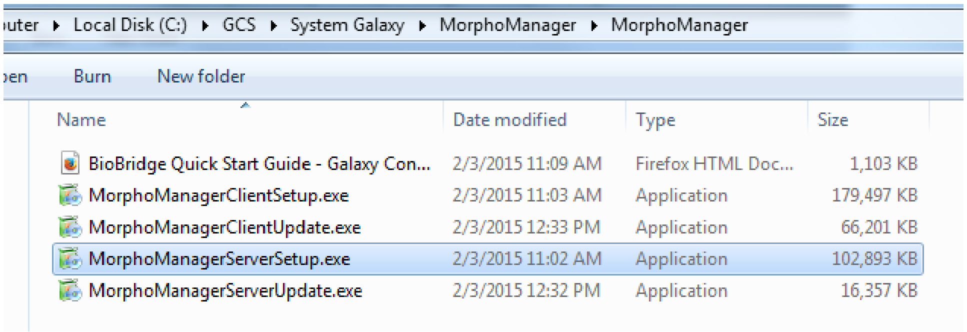
TECH NOTE: information in this guide is subject to change after publication. The location of 3rd Party installer files and drivers is also subject to change.

TIP: If the file location has changed, you can use *Windows File Explorer* to search for the file name. Be aware that you can also find 3rd Party install files on either Disk-1 in the installer's folder, or on the supplemental disk (Disk 2) for your product.

Contact Technical Support if you have any unresolved questions about file locations.

5.2.1 Installing the MorphoManager Server

1. Locate the **MorpphoManagerServerSetup.exe**. (the file is either laid down on the hard drive of the Galaxy comm server, or found on the Galaxy installation disk set: try Disk-2 *Sagem>MorphoManager* folder).

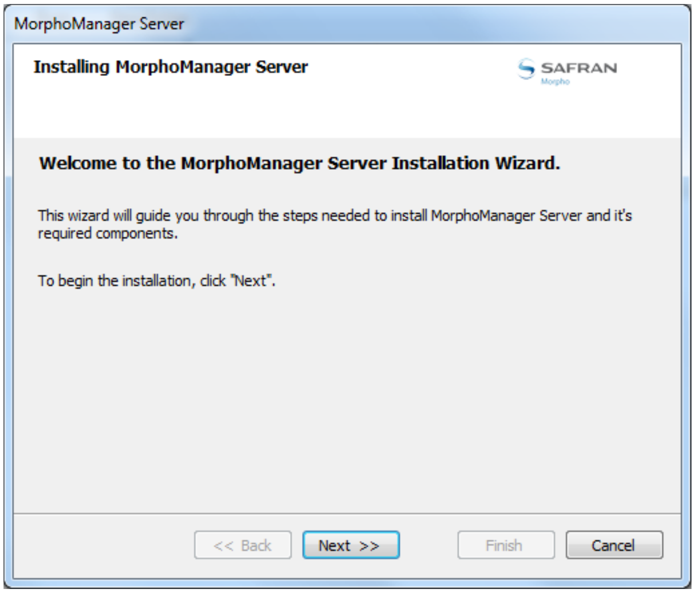


ıuter ▸ Local Disk (C:) ▸ GCS ▸ System Galaxy ▸ MorphoManager ▸ MorphoManager

Name	Date modified	Type	Size
BioBridge Quick Start Guide - Galaxy Con...	2/3/2015 11:09 AM	Firefox HTML Doc...	1,103 KB
MorphoManagerClientSetup.exe	2/3/2015 11:03 AM	Application	179,497 KB
MorphoManagerClientUpdate.exe	2/3/2015 12:33 PM	Application	66,201 KB
MorphoManagerServerSetup.exe	2/3/2015 11:02 AM	Application	102,893 KB
MorphoManagerServerUpdate.exe	2/3/2015 12:32 PM	Application	16,357 KB

2. Right-click filename MorphoManagerServerSetup.exe and choose 'Run as administrator'.

3. Click the [Next >>] button when the Installation Wizard launches.



MorphoManager Server

Installing MorphoManager Server

Welcome to the MorphoManager Server Installation Wizard.

This wizard will guide you through the steps needed to install MorphoManager Server and it's required components.

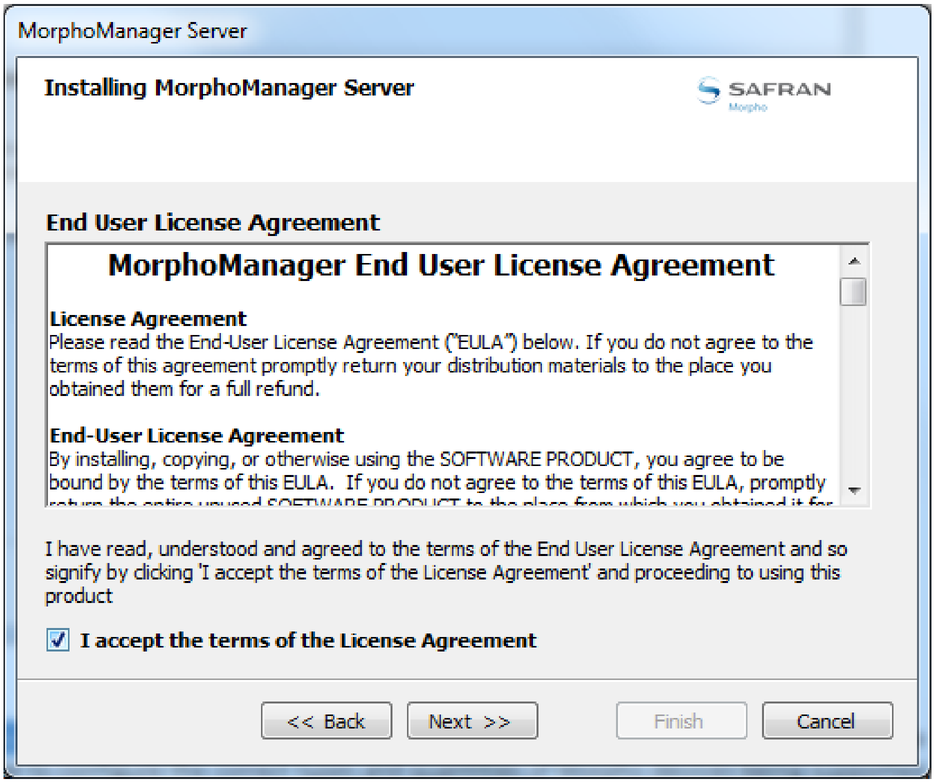
To begin the installation, click "Next".

INSTRUCTIONS CONTINUE ON NEXT PAGE

5.2.2 Accepting the MorphoManager License

4. Enable(check) the 'Accept License Agreement' option.

5. Click the [Next >>] button.



Installing MorphoManager Server

End User License Agreement

MorphoManager End User License Agreement

License Agreement
Please read the End-User License Agreement ("EULA") below. If you do not agree to the terms of this agreement promptly return your distribution materials to the place you obtained them for a full refund.

End-User License Agreement
By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, promptly return the entire unused SOFTWARE PRODUCT to the place from which you obtained it for

I have read, understood and agreed to the terms of the End User License Agreement and so signify by clicking 'I accept the terms of the License Agreement' and proceeding to using this product

☑ I accept the terms of the License Agreement

INSTRUCTIONS CONTINUE ON NEXT PAGE

5.2.3 Configuring the Database Provider/Usage Requirements

After Accepting the License Agreement, the following screen will appear:

6. Configure the quantity of devices and users based upon your system requirements.

   a) Enter the **number of Sigma readers** to be installed.

   b) *Enter the quantity of 2G and 3D devices to be installed, if any*.

7. Enter the **number of users** to be biometrically enrolled (default = 300).

> The Wizard automatically sets the 'Recommended Database Provider', based on the usage requirements. Galaxy will require you to override the database provider if it does not set to SQL 2005 automatically.

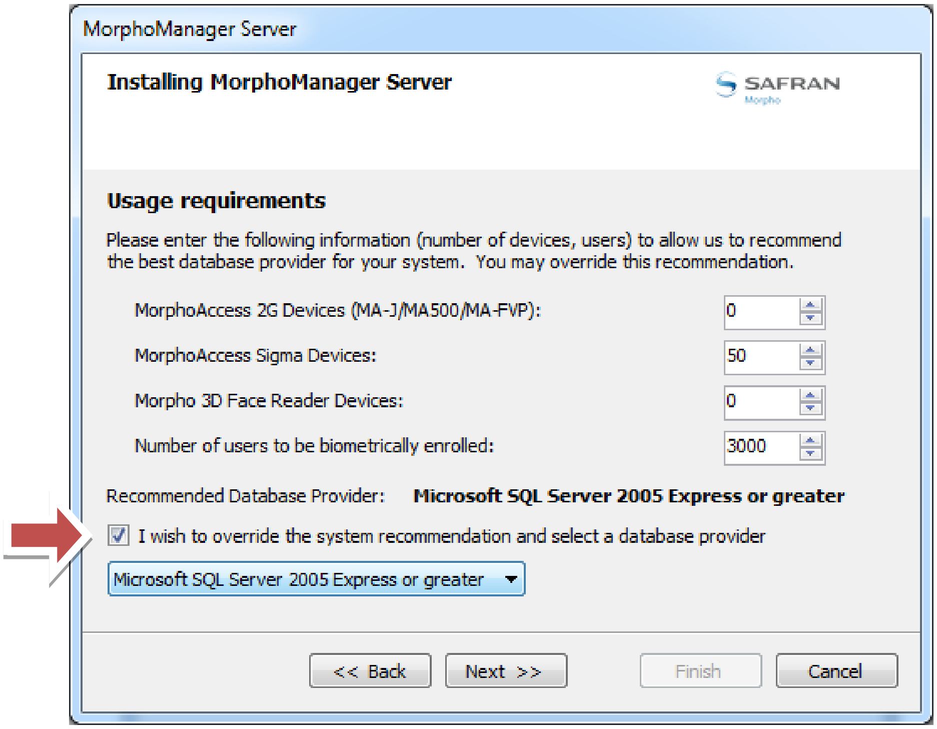
8. Configure the **Database Provider** to be "Microsoft SQL Server 2005 or greater"

   a) Galaxy Integration must use the SQL Server Database. If the screen did not auto-pick SQL Server 2005 edition, you must override and manually select it.

   b) Enable (check) the [I wish to Override system recommendation…] option, and then select "Microsoft SQL Server 2005" from the provider droplist.

9. Click the [Next >>] button to continue.

Figure 10 – MORPHOMANAGER INSTALL: Max Users & SQL Database Override



MorphoManager Server

Installing MorphoManager Server

Usage requirements

Please enter the following information (number of devices, users) to allow us to recommend the best database provider for your system. You may override this recommendation.

MorphoAccess 2G Devices (MA-J/MA500/MA-FVP): 0

MorphoAccess Sigma Devices: 50

Morpho 3D Face Reader Devices: 0

Number of users to be biometrically enrolled: 3000

Recommended Database Provider: **Microsoft SQL Server 2005 Express or greater**

☑ I wish to override the system recommendation and select a database provider

Microsoft SQL Server 2005 Express or greater

INSTRUCTIONS CONTINUE ON NEXT PAGE

5.2.4 Configuring & Testing your SQL Server Connection Parameters

You must provide a true admin-level login. By default, Galaxy provides a sys admin (sa) level login. You can use that login or you can go to the SQL Managagement Studio and create an sa-level login.

10. Enter the correct SQL Server Instance path (machine_name\GCSSQLEXPRESS).

> GCSSQLEXPRESS is the default database instance name. Enter your actual instance name.

11. Disable (uncheck) the **Login using [Integrated Security]** option.

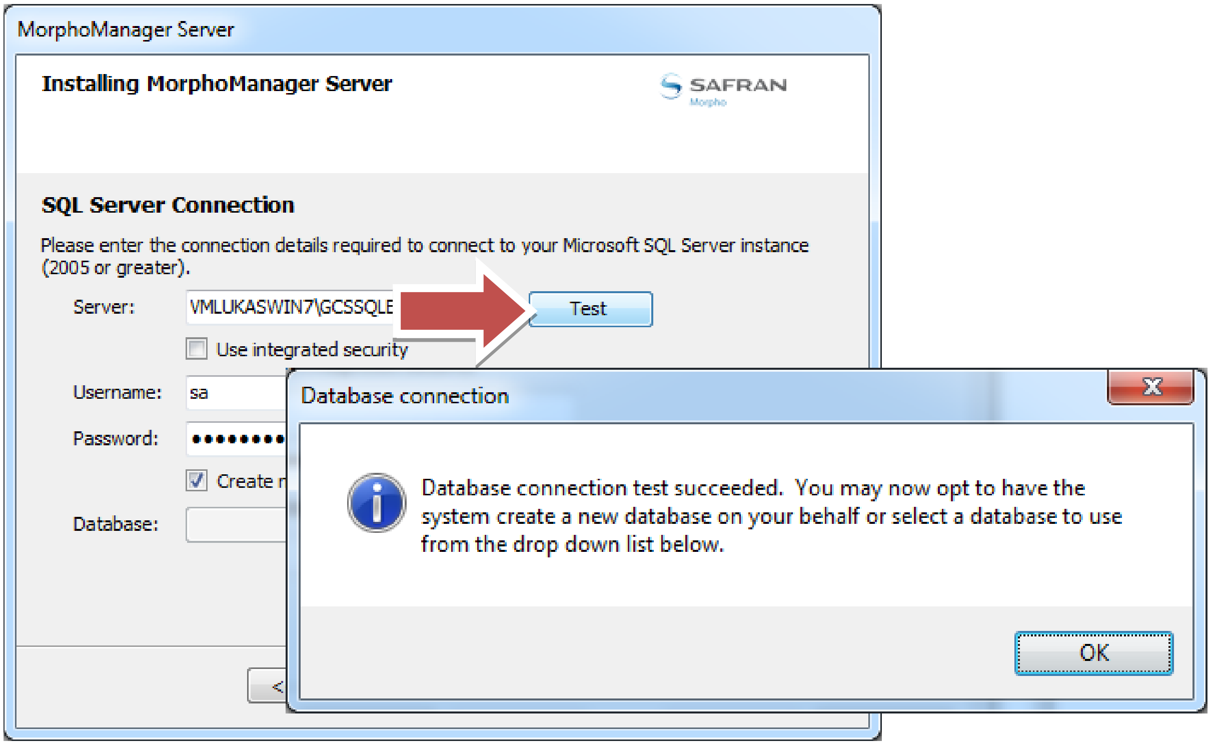
12. Enter the System Galaxy "sa" **login** and **password** ("sa" admin-level permissions required).

> **WARNING**: **The SQL Server Login must have administrative-level database permissions**. Failure to use a login with the correct permissions could result in a catastrophic failure in the MorphoManager Installation program that cannot be recovered except by uninstalling and reinstalling. If for any reason you experience this undesired result, consult the Troubleshooting & Exceptions section in this guide for possible recovery methods.

13. Click the [Test] button to ensure you can connect.
A Database Connection confirmation message should display.

> **WARNING**: **be aware that a successful connection test does not ensure you have the proper "sa" admin privileges.** It is possible to get a successful connection test and still fail to install the Database. The database components fail to install and the server install must be redone.

Figure 11 – MORPHOMANAGER INSTALL: SQL Server Connection



Installing MorphoManager Server

SQL Server Connection

Please enter the connection details required to connect to your Microsoft SQL Server instance (2005 or greater).

Server: VMLUKASWIN7\GCSSQLE

□ Use integrated security

Username: sa

Password: ••••••••

☑ Create r

Database:

Database connection test succeeded. You may now opt to have the system create a new database on your behalf or select a database to use from the drop down list below.

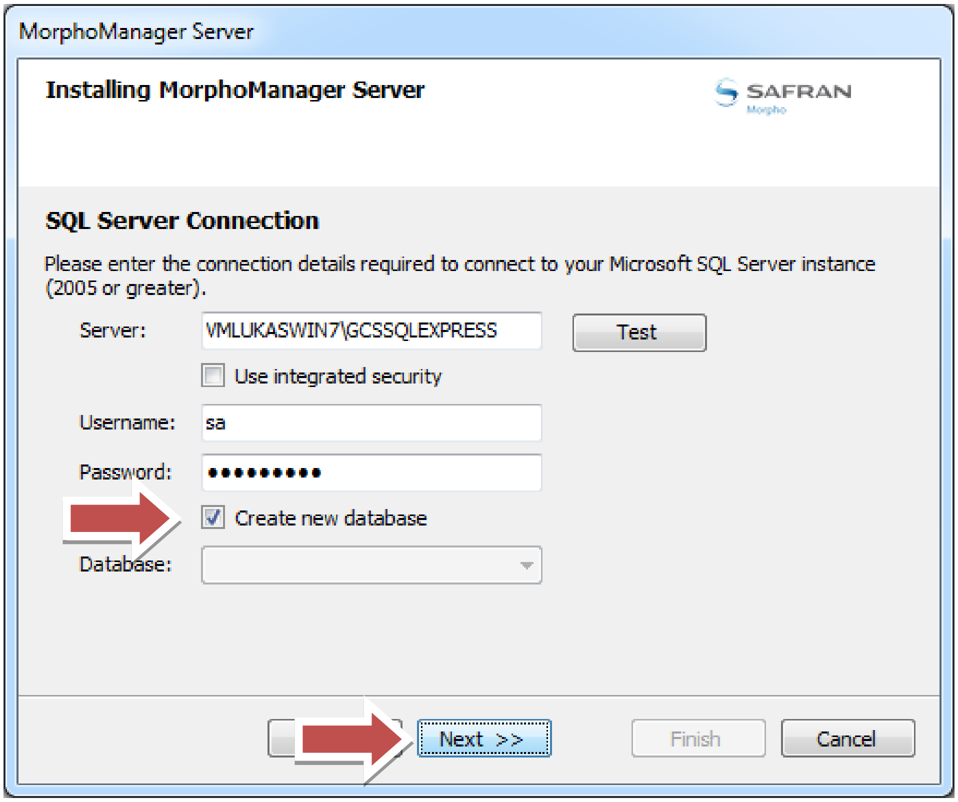
INSTRUCTIONS CONTINUE ON NEXT PAGE

5.2.5 Creating the New Database and Completing the Server Installation

After testing the Database Connections, do the following:

1. After testing the connection to the database instance, the Database selection fields become enabled.
2. Enable (check) the [Create New Database] option if installing a new MorphoManager Database.
3. Click the [Next >>] button to proceed with the Server and Database installation.

Figure 12 – MORPHOMANAGER INSTALL: SQL Server Login and Creating Database



MorphoManager Server

Installing MorphoManager Server

SQL Server Connection

Please enter the connection details required to connect to your Microsoft SQL Server instance (2005 or greater).

Server: VMLUKASWIN7\GCSSQLEXPRESS

□ Use integrated security

Username: sa

Password: ●●●●●●●●●

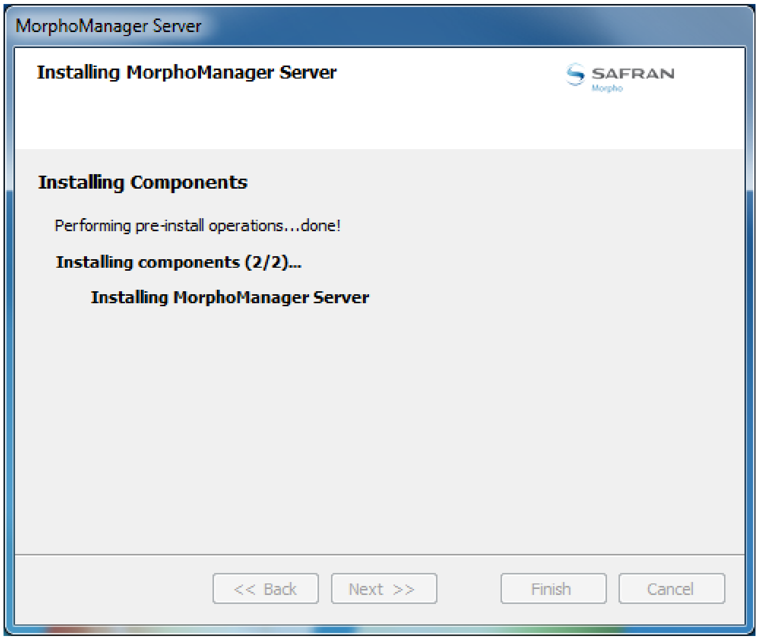
☑ Create new database

Database:

INSTRUCTIONS CONTINUE ON NEXT PAGE

4. Wait for the Installer to install the Server components.

INSTALLING COMPONENTS: During this step the Install Wizard may open a console window to complete the installation of various components Note this is where the install could fail if you didn't provide a correct connection in the



MorphoManager Server

Installing MorphoManager Server

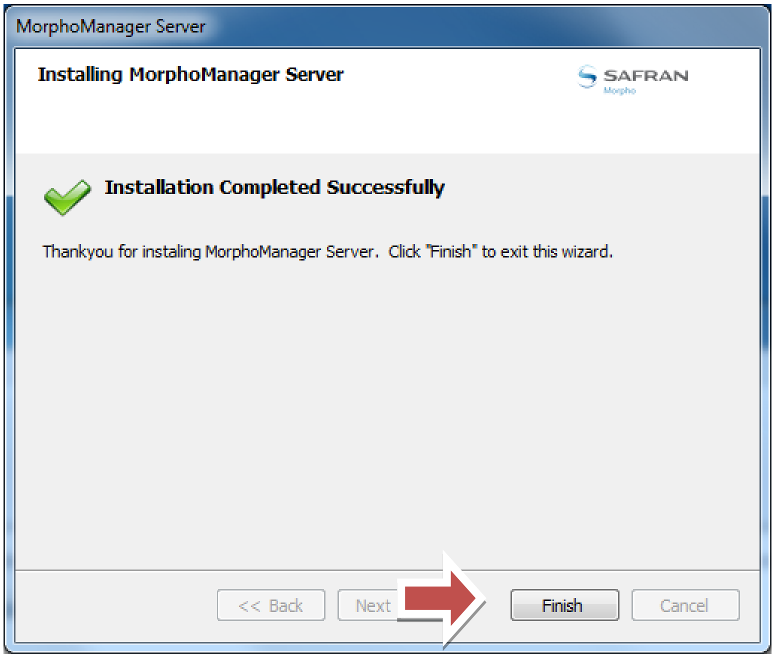
Installing Components

Performing pre-install operations...done!

Installing components (2/2)...

Installing MorphoManager Server

5. Click FINISH when installation is complete.



MorphoManager Server

Installing MorphoManager Server

Installation Completed Successfully

Thankyou for instaling MorphoManager Server. Click "Finish" to exit this wizard.

INSTRUCTIONS FINISHED

5.3 INSTALLING THE MORPHOMANAGER CLIENT SOFTWARE

This section covers installing the MorphoManager Client Software. The client software can be installed on the same computer as the server component for administrative purposes. The MorphoManager Client Software must be installed on each (remote) PCs where credentials will be enrolled; thus every badging station.

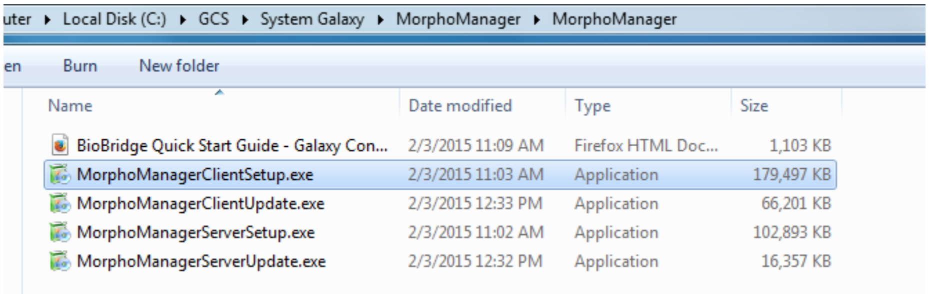
TECH NOTE: information in this guide is subject to change after publication. The location of 3rd Party installer files and drivers is also subject to change.

TIP: If the file location has changed, you can use *Windows File Explorer* to search for the file name. Be aware that you can also find 3rd Party install files on either Disk-1 in the installer's folder, or on the supplemental disk (Disk 2) for your product.

Contact Technical Support if you have any unresolved questions about file locations.

1. The following file must be executed to install the Sagem Morpho Manager Software.

   - **MorphoManagerClientSetup.exe** *is either laid down on the hard drive of the Galaxy comm server or found on the Galaxy installation disk set. Try Disk-2* ***Sagem>MorphoManager*** *folder.*



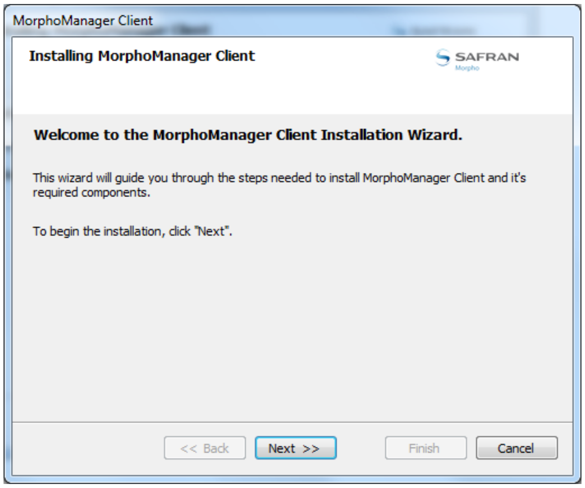
uter ▸ Local Disk (C:) ▸ GCS ▸ System Galaxy ▸ MorphoManager ▸ MorphoManager
en
Burn
New folder

Name	Date modified	Type	Size
BioBridge Quick Start Guide - Galaxy Con...	2/3/2015 11:09 AM	Firefox HTML Doc...	1,103 KB
MorphoManagerClientSetup.exe	2/3/2015 11:03 AM	Application	179,497 KB
MorphoManagerClientUpdate.exe	2/3/2015 12:33 PM	Application	66,201 KB
MorphoManagerServerSetup.exe	2/3/2015 11:02 AM	Application	102,893 KB
MorphoManagerServerUpdate.exe	2/3/2015 12:32 PM	Application	16,357 KB

5.3.1 Installing the MorphoManager Client Software

1. Right-click filename MorpphoManagerClientSetup.exe and choose 'Run as administrator'.

2. When the Installation Wizard launches, click the [Next >>] button.



Installing MorphoManager Client

Welcome to the MorphoManager Client Installation Wizard.

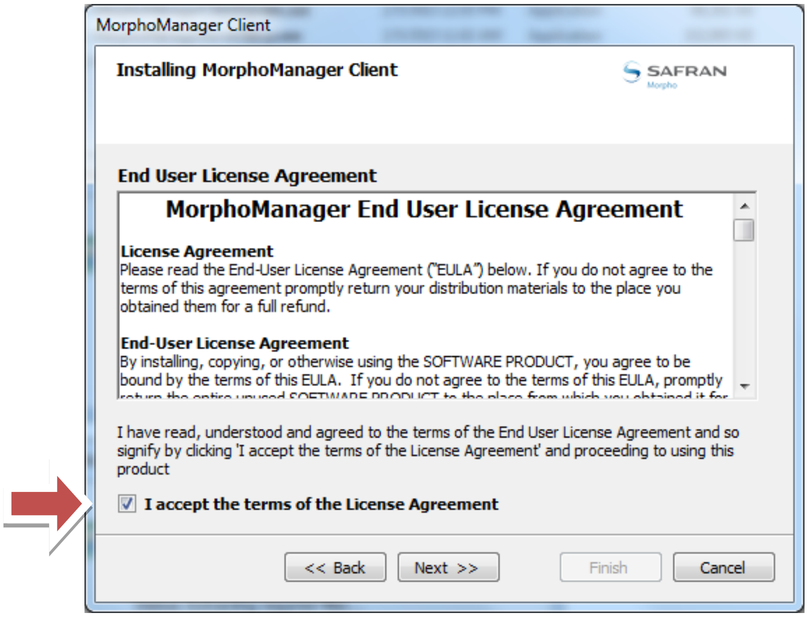
This wizard will guide you through the steps needed to install MorphoManager Client and it's required components.

To begin the installation, click "Next".

INSTRUCTIONS CONTINUE ON NEXT PAGE

5.3.2 Accepting the License and Completing the Client Installation

3. Accept the License Agreement
4. Click the [Next >>] button.



MorphoManager Client

Installing MorphoManager Client

End User License Agreement

MorphoManager End User License Agreement

License Agreement
Please read the End-User License Agreement ("EULA") below. If you do not agree to the terms of this agreement promptly return your distribution materials to the place you obtained them for a full refund.

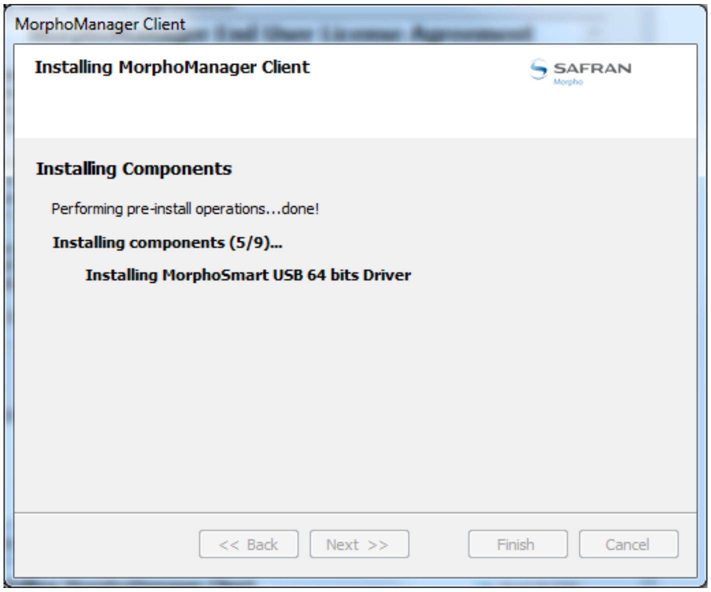
End-User License Agreement
By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, promptly return the entire unused SOFTWARE PRODUCT to the place from which you obtained it for

I have read, understood and agreed to the terms of the End User License Agreement and so signify by clicking 'I accept the terms of the License Agreement' and proceeding to using this product

☑ **I accept the terms of the License Agreement**

5. The client components and drivers will install.

Figure 13 – MORPHOMANAGER INSTALL: Components and Drivers



MorphoManager Client

Installing MorphoManager Client

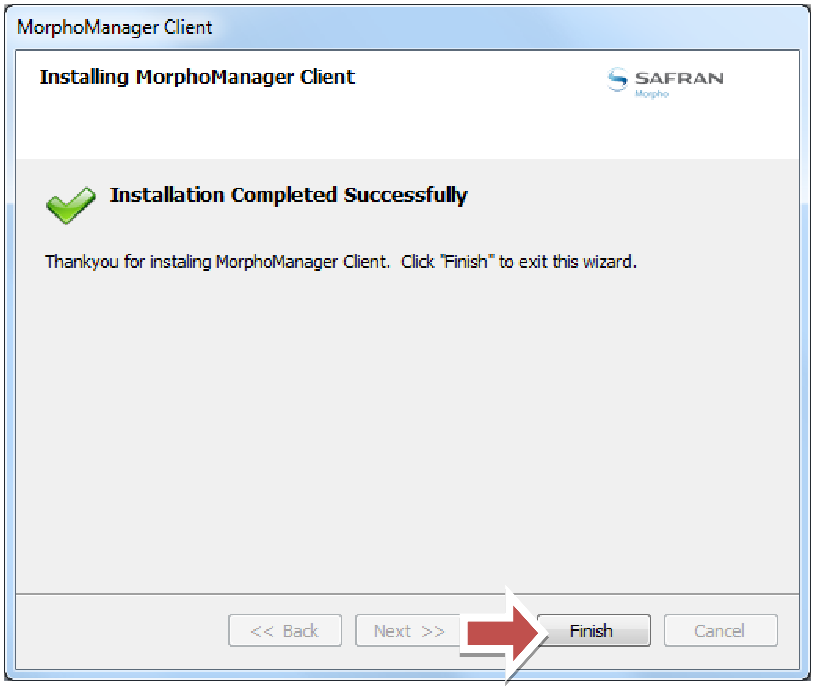
Installing Components

Performing pre-install operations...done!

Installing components (5/9)...

Installing MorphoSmart USB 64 bits Driver

INSTRUCTIONS CONTINUE ON NEXT PAGE


MorphoManager Client

Installing MorphoManager Client

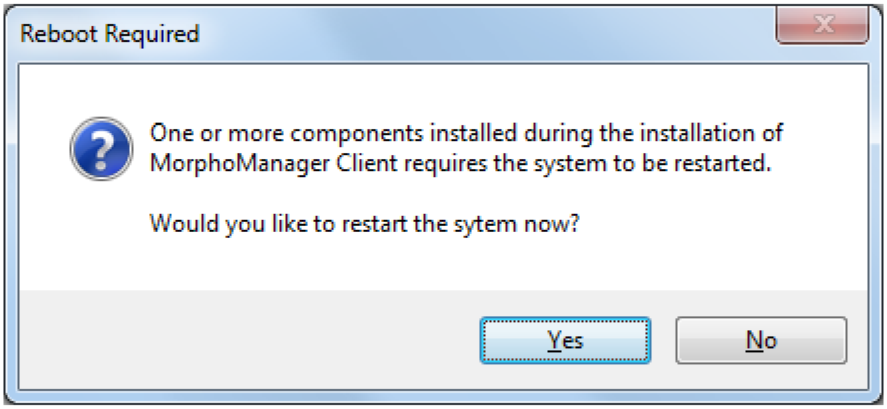
Installation Completed Successfully

Thankyou for instaling MorphoManager Client. Click "Finish" to exit this wizard.

5.3.3 Restarting the Operating System

6. Click [Yes] to restart the Operating System .

CAUTION: Before rebooting your operating system, close and save all work.
NOTICE: after rebooting your system, you may need to manually start the MorphoManager service.


Reboot Required

One or more components installed during the installation of MorphoManager Client requires the system to be restarted.

Would you like to restart the sytem now?

INSTRUCTIONS FINISHED FOR THIS SECTION

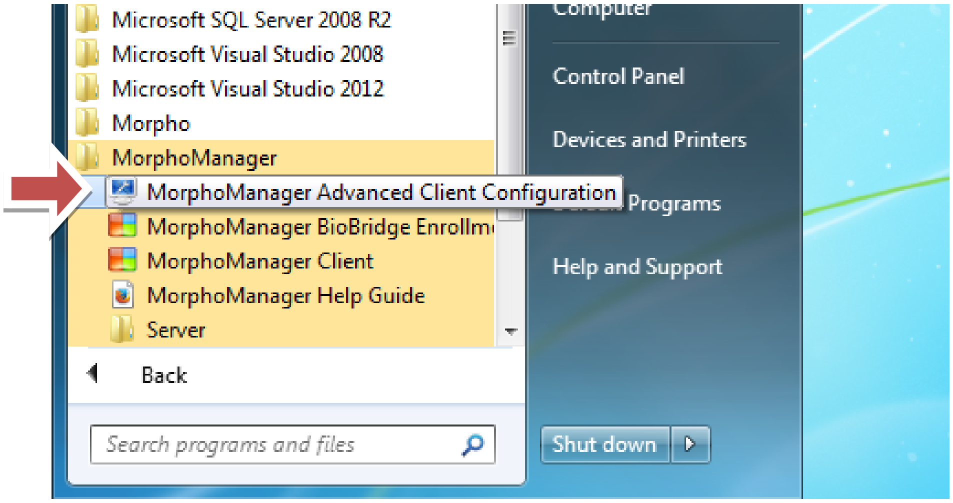
5.4 CONFIGURING THE MORPHOMANAGER CLIENT CONNECTION

The Advanced Client Configuration must be performed at every MorphoManager Client workstation where System Galaxy enrollment occurs.

NOTICE: after rebooting your system, you may need to manually start the MorphoManager service.

5.4.1 Opening the MorphoManager Client Configuration Tool

1. Open the **MorphoManager Advanced Client Configuration** Tool from the Windows Start menu.


Microsoft SQL Server 2008 R2
Microsoft Visual Studio 2008
Microsoft Visual Studio 2012
Morpho
MorphoManager
MorphoManager Advanced Client Configuration
MorphoManager BioBridge Enrollm
MorphoManager Client
MorphoManager Help Guide
Server
Back
Search programs and files
Computer
Control Panel
Devices and Printers
Programs
Help and Support
Shut down

Showing a Windows-7 Start Menu

WINDOWS-10 NOTE: From the ***Windows-10 Start Directory***, you can click the **ALL APPS** option at the bottom of the menu (below the power option); then scroll down to the 'M' and click on the "MorphoManager" folder to expand it. Finally click the ***MorphoManager Advanced Client Configuration*** Tool icon to start the program. Windows-8 should work similarly to Window-10.

TIP: You may wish to temporarily pin an application to the Windows Task Bar to allow you to re-open it during configuration and testing. This is possible to do once you have the application open by right clicking the icon on the task bar and selecting 'PIN to Task Bar'. UNPIN the application when no longer needed.

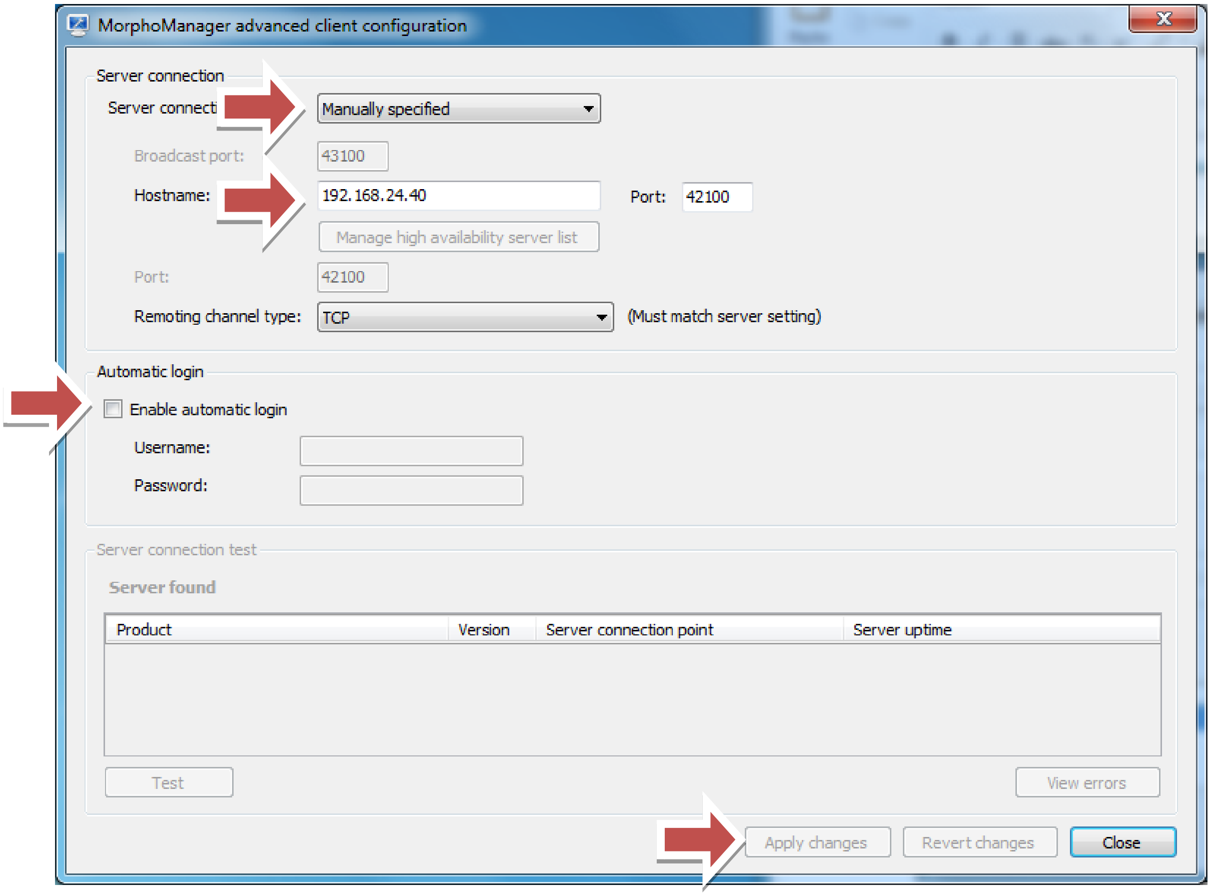
INSTRUCTIONS CONTINUE ON NEXT PAGE

5.4.2 Setting the Server Connection Parameters

System Galaxy recommends using Manual Discovery instead of Automatic Discovery, for remote MorphoManager client/server connections.

2. Set "Manually specified" for the connection type (recommended), to ensure the enrollment clients can connect.
   a) **For *Manual Discovery***: you must enter the **hostname** (or **IP address**) of the Server/PC where you installed the MorphoManager Server component (done is section 5.2).
   b) **For *Automatic Discovery***: you must perform a server connection test (by clicking the TEST button at the bottom of the screen) to allow the client software to perform an automatic discovery. It should pull back the server identity in the "server found" list.
3. (optional) ***Enable Automatic Login*** allows System Galaxy to automatically sign into the MorphoManager database when the BioBridge Client launches. NOTE: If disabled, SG Operators must know and provide the MorphoManager Login every time BioBridge launches to capture fingers (i.e. for each and every biometric credential). NOTE: the initial default login is *administrator* and *password.*
4. Click the **[APPLY CHANGES]** button.
5. Click CLOSE to exit.

Figure 14 – ADVANCED CLIENT CONFIGURATION: Client Connection & Automatic Login



MorphoManager advanced client configuration

Server connection

Server connection: Manually specified

Broadcast port: 43100

Hostname: 192.168.24.40 Port: 42100

Manage high availability server list

Port: 42100

Remoting channel type: TCP (Must match server setting)

Automatic login

☐ Enable automatic login

Username:

Password:

Server connection test

Server found

Product	Version	Server connection point	Server uptime

INSTRUCTIONS FINISHED

6 Configuring the MorphoManager Software

This chapter covers configuring the MorphoManager Client software to integrate with System Galaxy for biometric credential enrollment.

This chapter **only** describes configuring options and that are essential to enrolling of valid credentials for the following reader types:

- SigmaPROX using contactless proximity card + biometric finger prints (Multifactor 1:1)
- SigmaBIO using biometric finger prints (Multifactor 1: many)

SEE the ***MorphoManager User Guide*** for information on options outside the scope of this guide.

***If you see this Morpho Guide symbol in the instructions, you must refer to Morpho User Guide for info*.**

The following are covered for proper configuration:

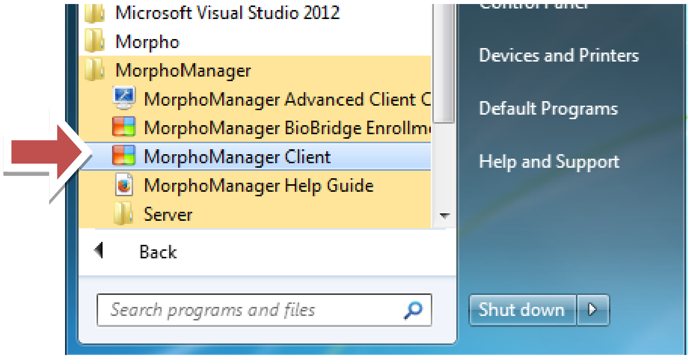
1. Launching the MorphoManager Client - Login.
2. Configuring the **Enrollment Client**.
3. Configuring the **Wiegand Profile** (site code or facility code)
4. Creating and configuring **User Distribution Groups** (used for mapping access groups)
5. Creating **User Policy** (Credential Authentication Mode assigned during enrollment)
6. Configuring the **System Configuration** settings for the BioBridge Module
7. Creating and configuring **Biometric Device Profiles**
8. Adding and configuring **Biometric Devices** (Readers)

6.1 LAUNCHING THE MORPHOMANAGER CLIENT

6.1.1 Launching MorphoManager Client Software

1. Launch the MorphoManager Client from Windows Program menu.

Figure 15 –MORPHOMANAGER: Launching MorphoManager Client



Showing a Windows-7 Start Menu

WINDOWS-10 NOTE: From the ***Windows-10 Start Directory***, you can click the **ALL APPS** option at the bottom of the menu (below the power option); then scroll down to the 'M' and click on the "MorphoManager" folder to expand it. Finally click the ***MorphoManager Advanced Client Configuration*** Tool icon to start the program. Windows-8 should work similarly to Window-10.

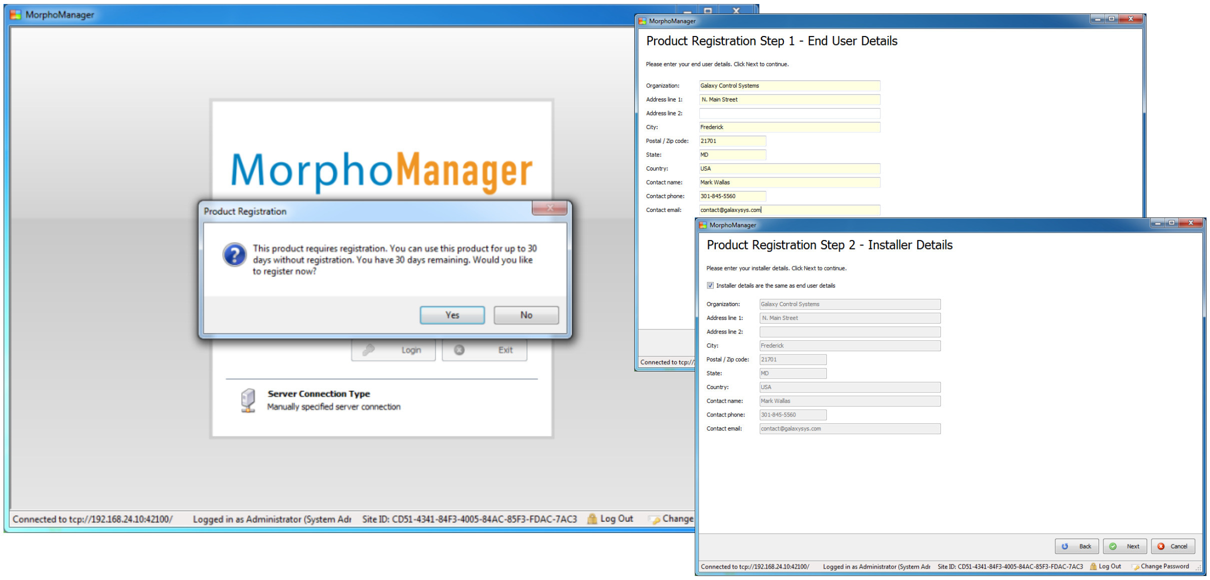
TIP: You may wish to temporarily pin an application to the Windows Task Bar to allow you to re-open it during configuration and testing. This is possible to do once you have the application open by right clicking the icon on the task bar and selecting 'PIN to Task Bar'. UNPIN the application when no longer needed.

6.1.2 MorphoManager Product Registration

The first time you launch the software, you will be prompted to register the MorphoManager system online. The product registration can be easily completed provided you are connected/online.

SEE the *MorphoManager Documentation* for information outside the scope of this guide.

Figure 16 –MORPHOMANAGER: Product Registration



Product Registration

This product requires registration. You can use this product for up to 30 days without registration. You have 30 days remaining. Would you like to register now?

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3 Log Out Change

MorphoManager

Product Registration Step 1 - End User Details

Please enter your end user details. Click Next to continue.

Organization:	Galaxy Control Systems
Address line 1:	N. Main Street
Address line 2:	
City:	Frederick
Postal / Zip code:	21701
State:	MD
Country:	USA
Contact name:	Mark Wallas
Contact phone:	301-845-5560
Contact email:	contact@galaxysys.com

Connected to tcp://

MorphoManager

Product Registration Step 2 - Installer Details

Please enter your installer details. Click Next to continue.

☑ Installer details are the same as end user details

Organization:	Galaxy Control Systems
Address line 1:	N. Main Street
Address line 2:	
City:	Frederick
Postal / Zip code:	21701
State:	MD
Country:	USA
Contact name:	Mark Wallas
Contact phone:	301-845-5560
Contact email:	contact@galaxysys.com

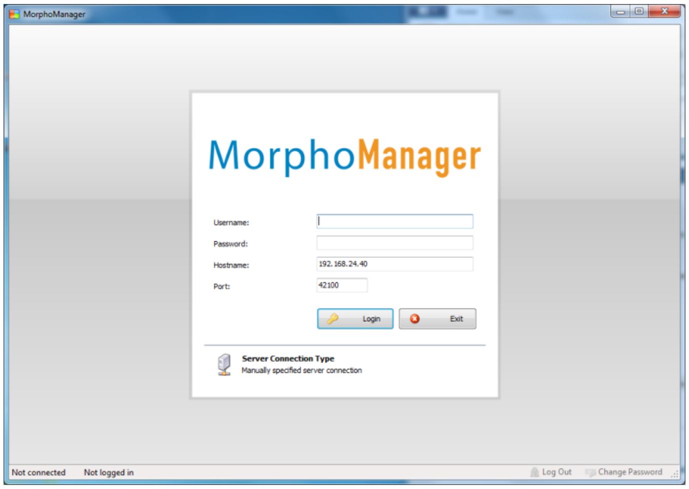
Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3 Log Out Change Password

6.1.3 Logging into MorphoManager Client Software

1. Sign in with the **username** and **password** (see Client Installation section for auto-login options)

2. Click the **Login** button to sign in.

3. Software will show a dialog box that indicates how many days remain on registration grace period.



MorphoManager

MorphoManager

Username:

Password:

Hostname: 192.168.24.40

Port: 42100

Login Exit

Server Connection Type
Manually specified server connection

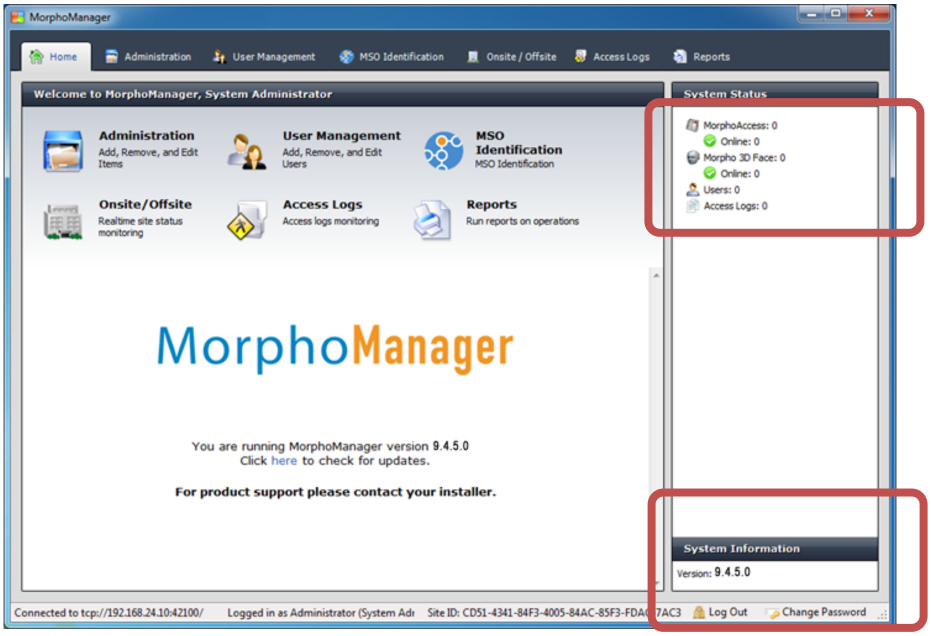
Not connected Not logged in Log Out Change Password

(if the System is configured for Automatic Login, this screen will not display)

4. The MorphoManager Client and the Home screen will display.
   - In this screen you can see the software version in the bottom right corner
   - You can also see any connected readers in the System Status pane.

If this is the first time you are starting, you will not see any readers since you have not added them yet.

Figure 17 – CONFIGURING MORPHOMANAGER: Client Home Screen



MorphoManager

Home | Administration | User Management | MSO Identification | Onsite / Offsite | Access Logs | Reports

Welcome to MorphoManager, System Administrator

Administration Add, Remove, and Edit Items

User Management Add, Remove, and Edit Users

MSO Identification MSO Identification

Onsite/Offsite Realtime site status monitoring

Access Logs Access logs monitoring

Reports Run reports on operations

MorphoManager

You are running MorphoManager version 9.4.5.0
Click here to check for updates.

For product support please contact your installer.

System Status

MorphoAccess: 0
Online: 0
Morpho 3D Face: 0
Online: 0
Users: 0
Access Logs: 0

System Information

Version: 9.4.5.0

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adr Site ID: CD51-4341-84F3-4005-84AC-85F3-FDA(7AC3 Log Out Change Password

6.2 CONFIGURING THE ENROLLMENT CLIENT

You must configure the Enrollment Clients to link the desired enrollment option.

You must configure the client at each workstation.

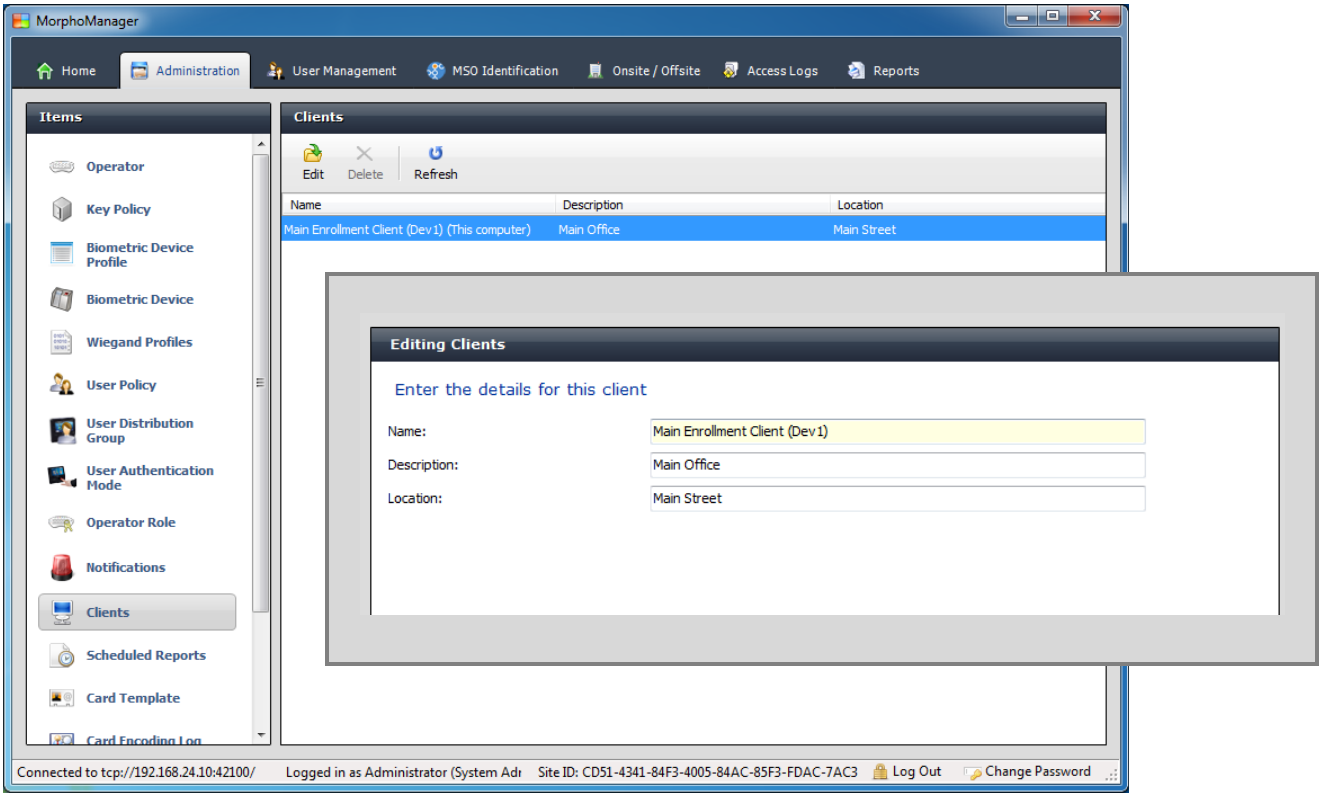
(Configuring a Client is much like configuring any other profile in this software. However Morpho doesn't call it a profile) Basically, you are selecting which readers and which clients are linked.

6.2.1 Naming the Enrollment Client

1. Select the MorphoManager Administration tab (screen).
2. Click **CLIENTS** button on the menu (left panel).
3. Click Edit button as needed.

   (by default, the system uses the machine name as the client name, but you can edit the name).
4. (optional) Edit the default machine name as desired (For example, in the figure below, the client name was edited and left the machine name in parenthesis).
5. Enter a Description that identifies the client
6. Enter the Location of the Client.
7. Click NEXT to advance to the Screen.

Figure 18 – MorphoManager: Assigning a Finger Enrollment Device



Name	Description	Location
Main Enrollment Client (Dev1) (This computer)	Main Office	Main Street

Editing Clients

Enter the details for this client

Name: Main Enrollment Client (Dev1)

Description: Main Office

Location: Main Street

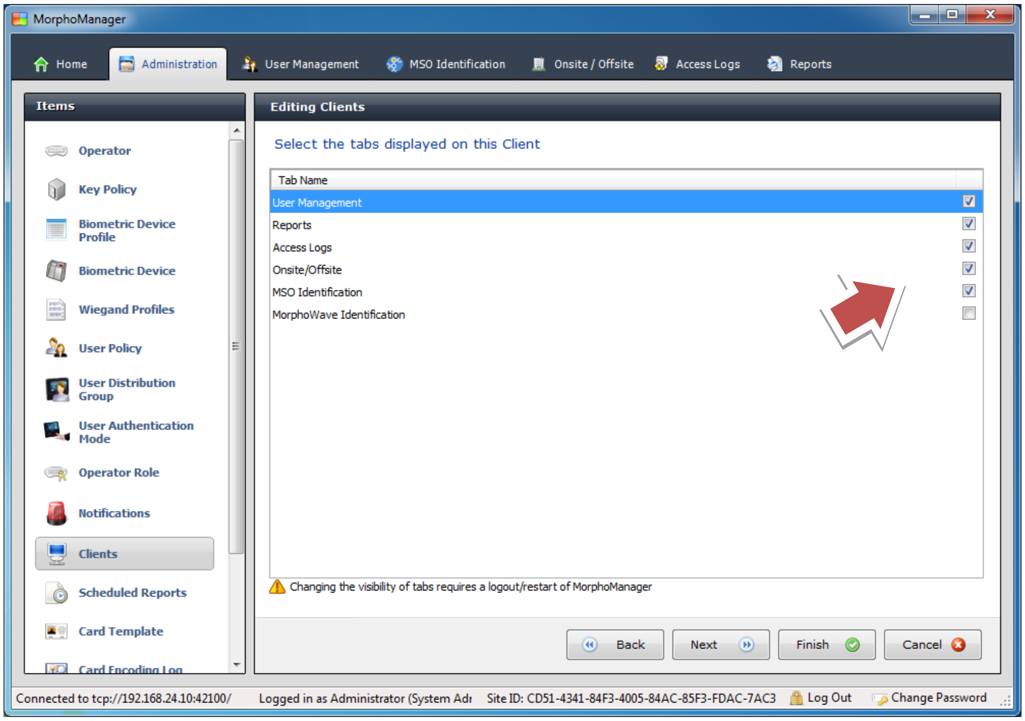
Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

6.2.2 Selecting the Viewable tabs/screens for the Client

In this screen you must select which tabs (screens) are visible at this client.

8. Enable (check) or disable (uncheck) the tabs to be displayed, as needed.
9. Click NEXT to advance to the Screen.

Figure 19 – MorphoManager: Selecting the viewable tabs



Editing Clients

Select the tabs displayed on this Client

Tab Name	
User Management	☑
Reports	☑
Access Logs	☑
Onsite/Offsite	☑
MSO Identification	☑
MorphoWave Identification	☐

⚠ Changing the visibility of tabs requires a logout/restart of MorphoManager

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

6.2.3 Assigning the Finger Enrollment Device

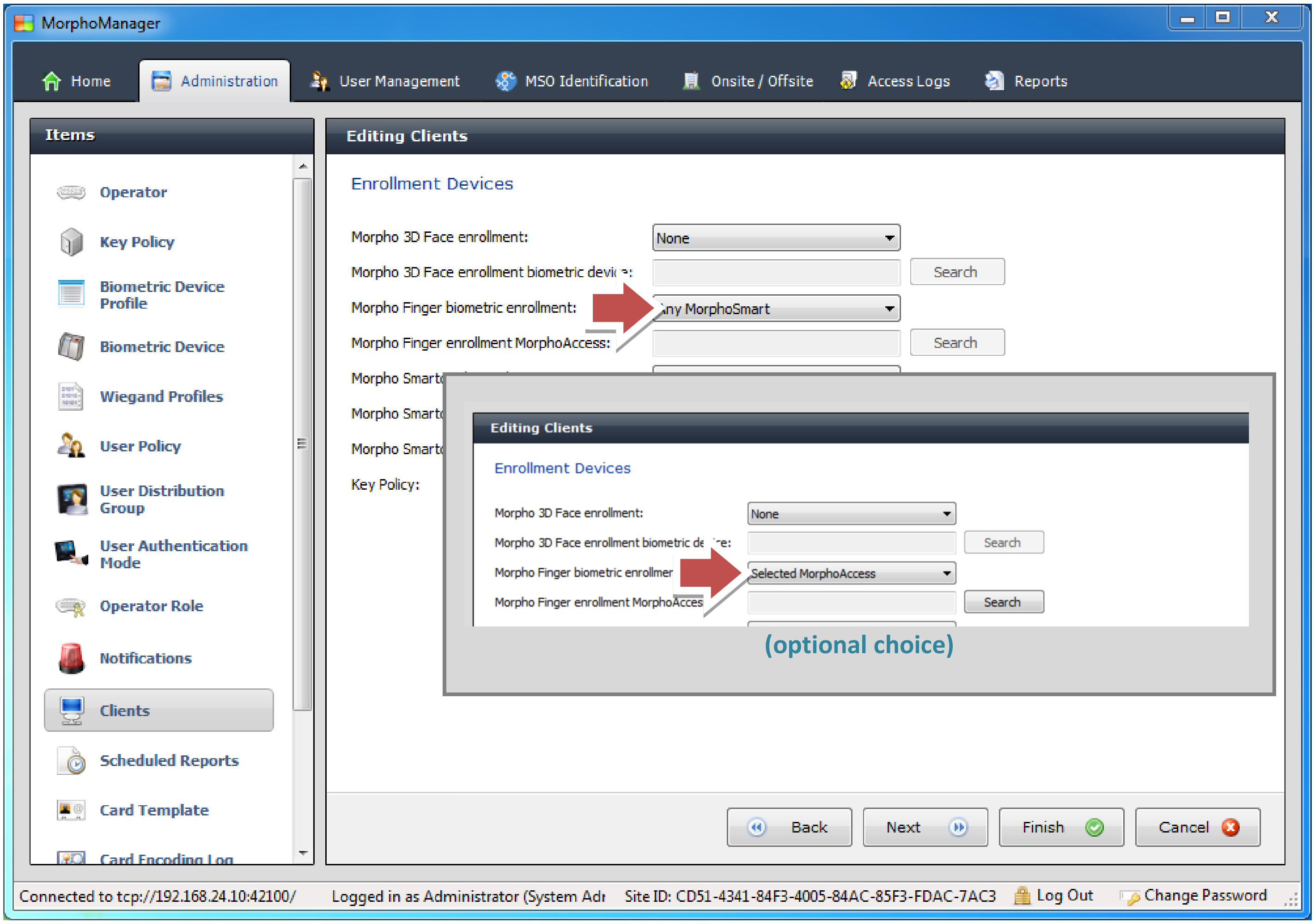
This section skips some intermediate screens and options that do not pertain to enrolling through Galaxy.

10. Click NEXT enough times to advance to the *Enrollment Devices* screen.

11. Set the **[Morpho Finger Biometric Enrollment] droplist** to 'Any MorphoSmart' to use an MSO Enrollment Device. (Optionally) you also could choose the 'Selected MorphoAccess' option , which allows you to search for an MA Reader that can serve as the finger capture device.

12. Click FINISH to save changes.

Figure 20 – MorphoManager: Assigning the Finger Enrollment Device



Editing Clients

Enrollment Devices

Morpho 3D Face enrollment: None

Morpho 3D Face enrollment biometric device:

Morpho Finger biometric enrollment: Any MorphoSmart

Morpho Finger enrollment MorphoAccess:

Morpho Smart

Morpho Smart

Morpho Smart

Key Policy:

Editing Clients

Enrollment Devices

Morpho 3D Face enrollment: None

Morpho 3D Face enrollment biometric device:

Morpho Finger biometric enrollmer Selected MorphoAccess

Morpho Finger enrollment MorphoAcces

(optional choice)

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

SEE the ***MorphoManager User Guide*** for options outside the scope of this guide.

END OF "Clients" CONFIGURATION

6.3 CONFIGURING A WIEGAND PROFILE

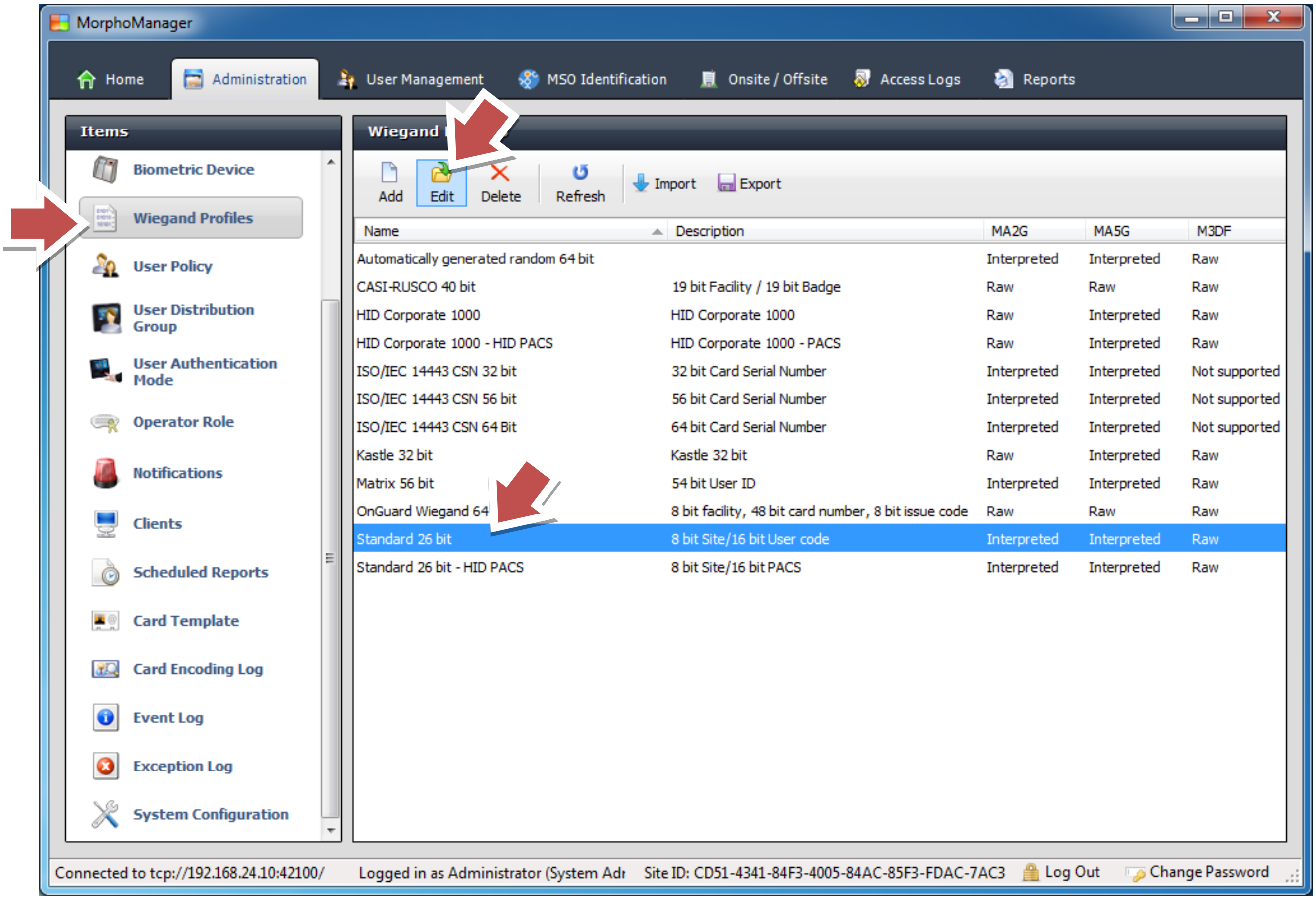
You must add your facility's Site Code to the appropriate Wiegand Profile. You begin by selecting the Wiegand format that matches your physical credentials (26bit or Corp 1000). If you are doing Finger Only (Biometric 1: many) you can simply use Standard 26 Bit Wiegand.

After you have configured the site code to the appropriate Wiegand Profile, you will be assigning the profile to various options that will be configured in other screens (Device Profile, System Configuration, etc.).

6.3.1 Editing the Wiegand Profile

1. From the Administration menu, click **Wiegand Profiles** button (left panel).
2. Highlight the Wiegand Profile you will use (i.e. "HID Corp1000" or "Standard 26bit Wiegand").
3. Click EDIT to open the Wiegand Profile in edit mode.
4. Click NEXT to **advance** to the Screen that accepts the Facility Code or Site Code as appropriate.

Figure 21 – MorphoManager: Editing the Wiegand Profile



Name	Description	MA2G	MA5G	M3DF
Automatically generated random 64 bit		Interpreted	Interpreted	Raw
CASI-RUSCO 40 bit	19 bit Facility / 19 bit Badge	Raw	Raw	Raw
HID Corporate 1000	HID Corporate 1000	Raw	Interpreted	Raw
HID Corporate 1000 - HID PACS	HID Corporate 1000 - PACS	Raw	Interpreted	Raw
ISO/IEC 14443 CSN 32 bit	32 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 56 bit	56 bit Card Serial Number	Interpreted	Interpreted	Not supported
ISO/IEC 14443 CSN 64 Bit	64 bit Card Serial Number	Interpreted	Interpreted	Not supported
Kastle 32 bit	Kastle 32 bit	Raw	Interpreted	Raw
Matrix 56 bit	54 bit User ID	Interpreted	Interpreted	Raw
OnGuard Wiegand 64	8 bit facility, 48 bit card number, 8 bit issue code	Raw	Raw	Raw
Standard 26 bit	8 bit Site/16 bit User code	Interpreted	Interpreted	Raw
Standard 26 bit - HID PACS	8 bit Site/16 bit PACS	Interpreted	Interpreted	Raw

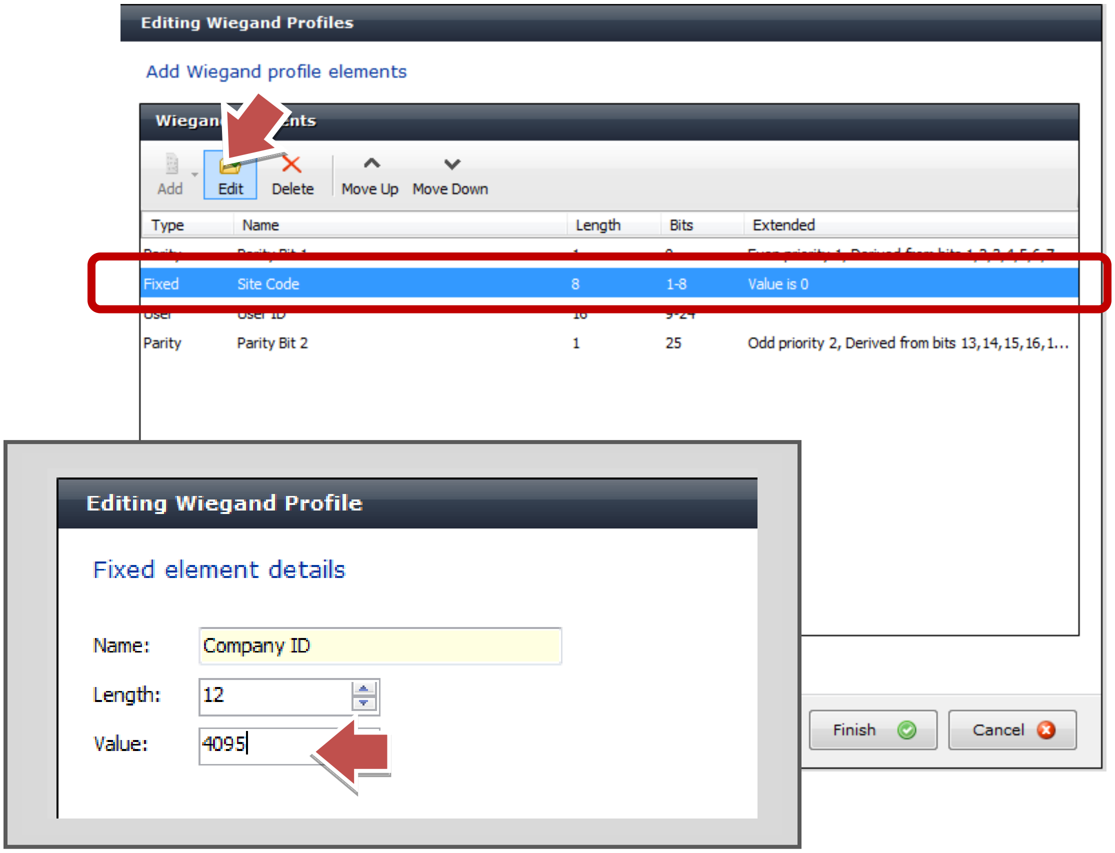
Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

CONTINUE ON NEXT PAGE

Continued from previous page

5. Highlight the ***Site Code*** line
6. Click EDIT again (to open the Fixed element details – see inset).
7. Enter the actual site code in the Value field for your card lot.
8. Click NEXT to accept the value
9. Click FINISH to save your Wiegand Profile.

Figure 22 – MorphoManager: Changing the Site Code/Facility Code



Type	Name	Length	Bits	Extended
Parity	Parity Bit 1	1	0	Even priority 1, Derived from bits 1,2,3,4,5,6,7...
Fixed	Site Code	8	1-8	Value is 0
User	User ID	16	9-24	
Parity	Parity Bit 2	1	25	Odd priority 2, Derived from bits 13,14,15,16,1...

Name: Company ID

Length: 12

Value: 4095

SEE the ***MorphoManager User Guide*** for information on options outside the scope of this guide.

CONFIGURING WIEGAND PROFILE COMPLETED

6.4 CONFIGURING A USER POLICY

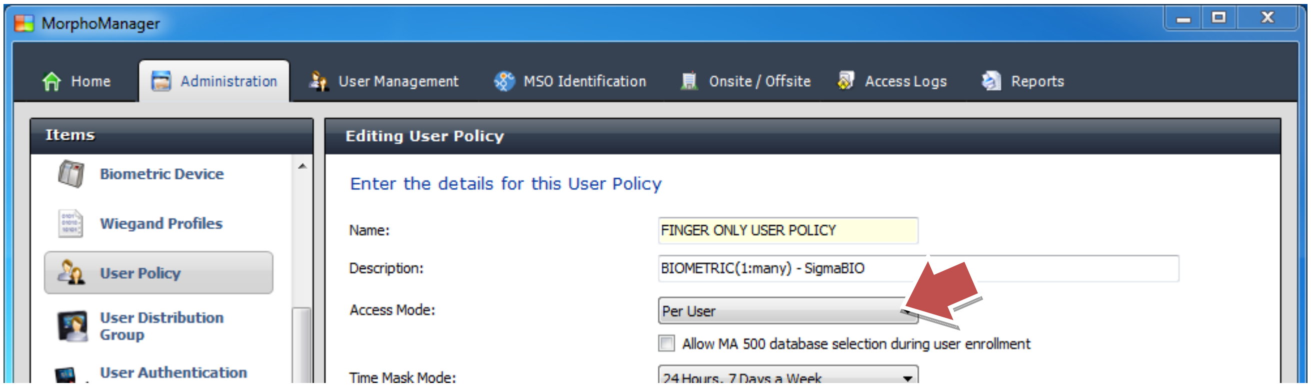
You must have at least one User Policy configured to enroll credentials.
You can have multiple Policies.

There is a “Default” user policy already available when you first install the main client. You can rename it and use it if the Authentication Mode fits your needs. If you need a different Authentication Mode than is configured in the default User Policy, you must create/add a new user policy. See next page.

6.4.1 Configuring the User Policy’s Access Mode

1. Enter a **Name** and **Description** that appropriately identifies the *auth mode* of this policy. If you are using the Default you may want to change the name to indicate the *auth mode*.
2. Set the **Access Mode** to “Per User”
3. The Allow MA 500 CHECKBOX can be checked as needed.

Figure 23 – MorphoManager: User Policy – Setting ACCESS MODE



Enter the details for this User Policy

Name: FINGER ONLY USER POLICY

Description: BIOMETRIC(1:many) - SigmaBIO

Access Mode: Per User

□ Allow MA 500 database selection during user enrollment

Time Mask Mode: 24 Hours, 7 Days a Week

SEE the ***MorphoManager User Guide*** for information on options outside the scope of this guide.

INSTRUCTIONS CONTINUE ON NEXT PAGE

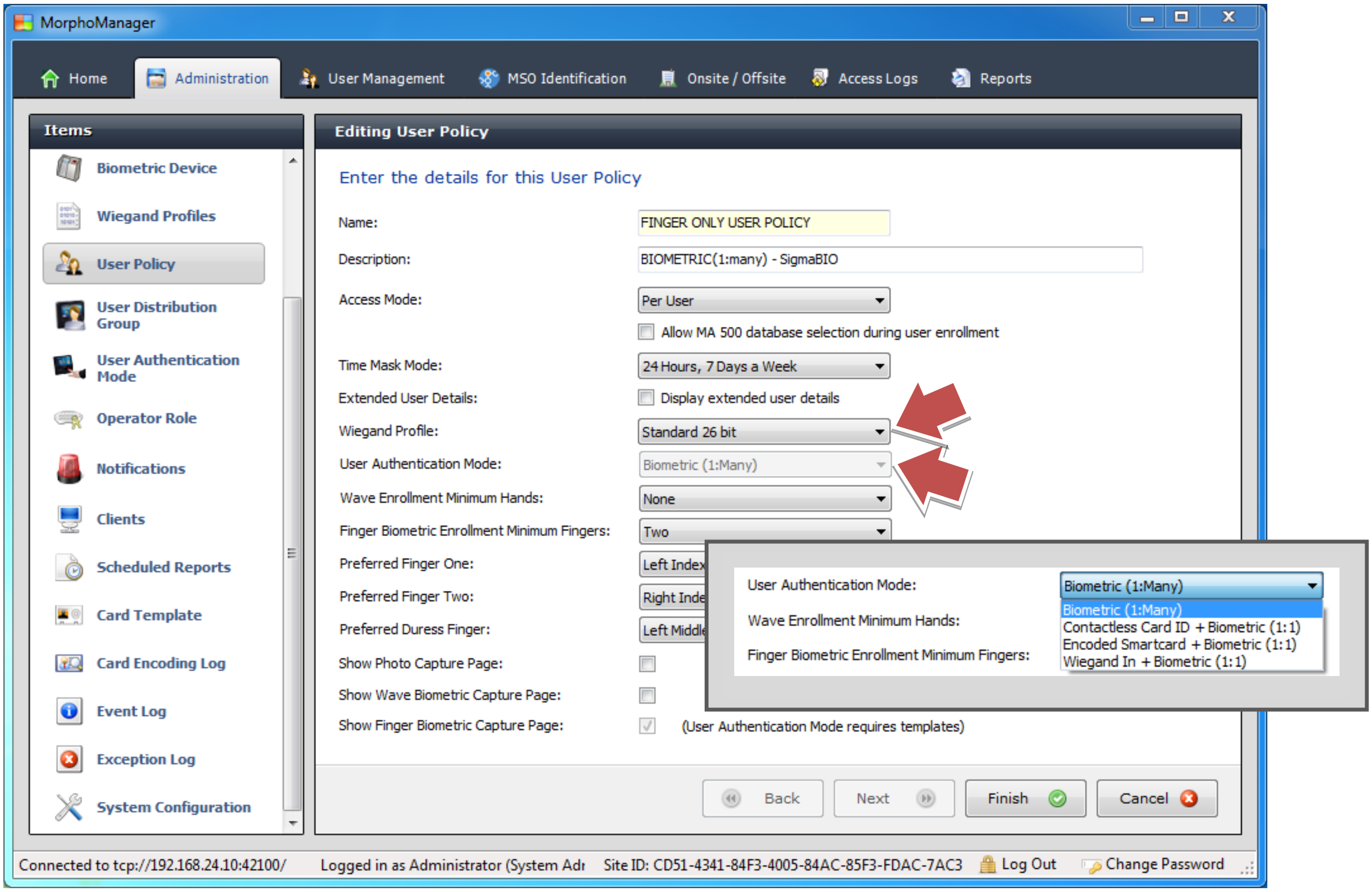
Continued from previous page

6.4.2 Configuring the User Policy's Wiegand Profile and User Authentication Mode

There is a "Default" user policy already available when you first install the main client. You can rename it and use it if the Authentication Mode fits your needs. If you need a different Authentication Mode than is configured in the default User Policy, you must create/add a new user policy. See next page.

4. Set the **Wiegand Profile** to the appropriate type (such as "HID CORP 1000" or "26bit Wiegand) – This must match BioBridge setting (in a future section).
5. Choose the desired **Authentication Mode** for this User Policy.
   (after you save the user policy, this field will be permanently locked)
6. Make sure that the '**Show Finger Capture Page' checkbox is checked.**
   (Also ensure that the Show Photo Capture Page checkbox is unchecked)
7. Click FINISH to save your settings.

Figure 24 – MorphoManager: User Policy – Setting the Wiegand Profile & Authentication Mode



Enter the details for this User Policy

Name: FINGER ONLY USER POLICY

Description: BIOMETRIC(1:many) - SigmaBIO

Access Mode: Per User

□ Allow MA 500 database selection during user enrollment

Time Mask Mode: 24 Hours, 7 Days a Week

Extended User Details: □ Display extended user details

Wiegand Profile: Standard 26 bit

User Authentication Mode: Biometric (1:Many)

Wave Enrollment Minimum Hands: None

Finger Biometric Enrollment Minimum Fingers: Two

Preferred Finger One: Left Index

Preferred Finger Two: Right Inde

Preferred Duress Finger: Left Middl

Show Photo Capture Page: □

Show Wave Biometric Capture Page: □

Show Finger Biometric Capture Page: ☑ (User Authentication Mode requires templates)

User Authentication Mode: Biometric (1:Many)

Wave Enrollment Minimum Hands:

Finger Biometric Enrollment Minimum Fingers:

Biometric (1:Many)
Contactless Card ID + Biometric (1:1)
Encoded Smartcard + Biometric (1:1)
Wiegand In + Biometric (1:1)

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

CONFIGURING USER POLICY IS COMPLETED

6.5 CREATING A DEVICE PROFILE

This guide uses the example of 'Corporate 1000' card type, but remember that the card type chosen must be compatible to the associated SIGMA Reader and must also be associated with the User Group and with the BioBridge Configuration.

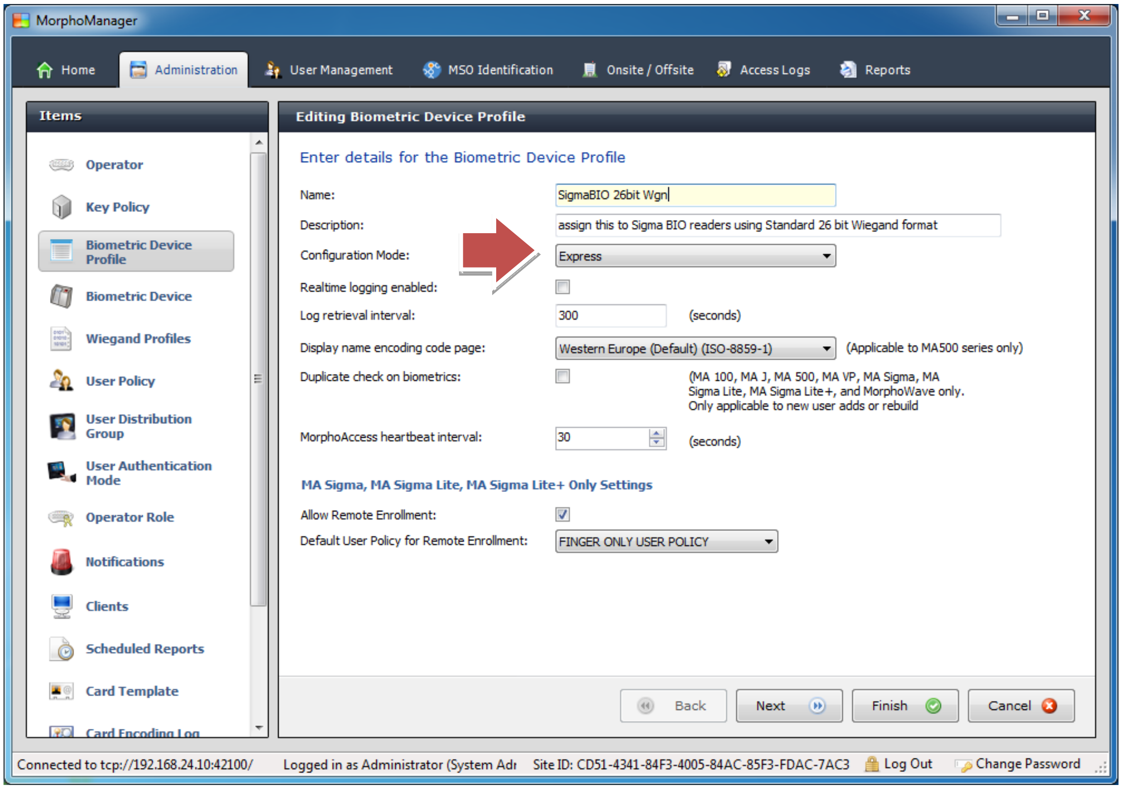
Also see the MorphoManager documentation for extended information about device profiles.

6.5.1 Setting the Wiegand Profile for the Reader

1. From the Administration screen, click the **Biometric Device Profile** button on the menu (left side).
2. Enter a logical Name for your Device Profile and a Description as desired. [TIP: When naming your Device Profile, it is good practice to indicate which Wiegand Format will be assigned (i.e. 26bit Wiegand, Corp 100, etc.). You will appreciate the importance in a future section when you are adding your Biometric Readers.]
3. Set the Configuration Mode to "Express".
4. Set the Default User Policy for Enrollment to the User Policy you desire to have as your default. This means the system will enroll credentials with this User Policy unless the operator picks a different one.
5. Click NEXT to advance to next screen.

SEE the ***MorphoManager User Guide*** for information on options outside the scope of this guide.

Figure 25 – MorphoManager: Biometric Device Profile



Editing Biometric Device Profile

Enter details for the Biometric Device Profile

Name: SigmaBIO 26bit Wgn

Description: assign this to Sigma BIO readers using Standard 26 bit Wiegand format

Configuration Mode: Express

Realtime logging enabled: □

Log retrieval interval: 300 (seconds)

Display name encoding code page: Western Europe (Default) (ISO-8859-1) (Applicable to MA500 series only)

Duplicate check on biometrics: □ (MA 100, MA J, MA 500, MA VP, MA Sigma, MA Sigma Lite, MA Sigma Lite+, and MorphoWave only. Only applicable to new user adds or rebuild

MorphoAccess heartbeat interval: 30 (seconds)

MA Sigma, MA Sigma Lite, MA Sigma Lite+ Only Settings

Allow Remote Enrollment: ☑

Default User Policy for Remote Enrollment: FINGER ONLY USER POLICY

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

INSTRUCTIONS CONTINUE ON NEXT PAGE

Continued from previous page

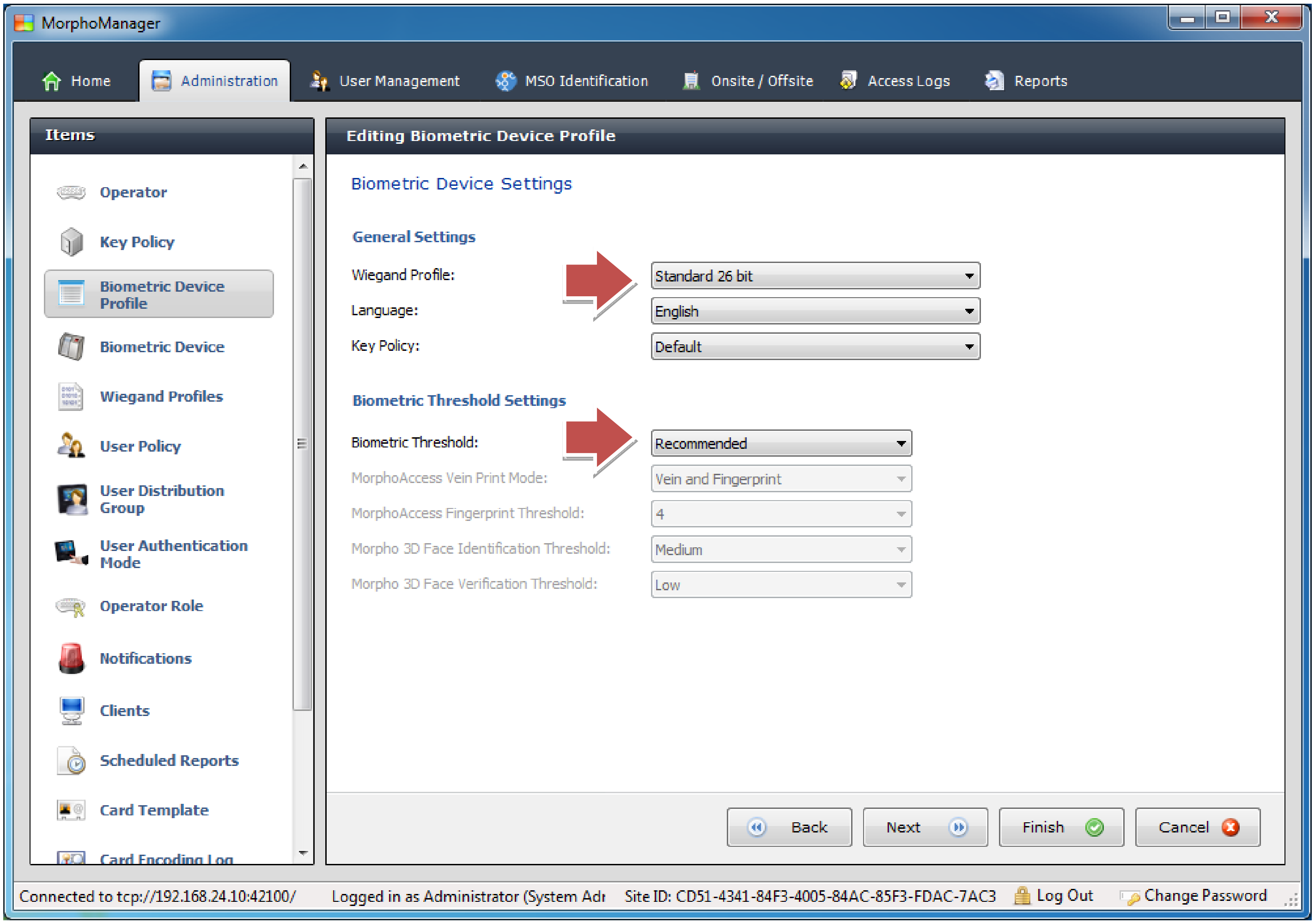
6.5.2 Assigning the Wiegand Profile to the Device Profile

6. Set the Wiegand Profile as desired to format you desire (26b Wiegand or Corp 1000)

7. Accept default settings [Using the "RECOMMENDED" Biometric Threshold is recommended. Consult the MorphoManager documentation for additional information.}

8. Click NEXT to advance to next screen.

Figure 26 – MorphoManager: Biometric Device Profile – Wiegand Profile



Editing Biometric Device Profile

Biometric Device Settings

General Settings

Wiegand Profile: Standard 26 bit

Language: English

Key Policy: Default

Biometric Threshold Settings

Biometric Threshold: Recommended

MorphoAccess Vein Print Mode: Vein and Fingerprint

MorphoAccess Fingerprint Threshold: 4

Morpho 3D Face Identification Threshold: Medium

Morpho 3D Face Verification Threshold: Low

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

INSTRUCTIONS CONTINUE ON NEXT PAGE

Continued from previous page

6.5.3 Setting the Multi-Factor Mode droplist

Read this information carefully to be sure you understand how to match the reader's **Multifactor Mode** with the **Authentication Type** you are assigning to your credentials.

6.5.3.1 ABOUT THE "PROXIMITY CARD" OPTION

When you set the Multifactor Mode to 'Proximity Card', the associated readers will only accept credentials that are enrolled as *Prox+Biometric*. *Which means that " Biometric" (finger-only) credential type will only work at a Reader that is configured to operate in "Biometric" Multifactor Mode.*

- **Notice the Proximity Card checkbox** = **will become checked/enabled** [*This governs the state of the Card Sensor when the Reader is in idle/ready state. In this case the Card Sensor will be "ON" at SIGMA when this profile is assigned to a reader.*]
- **Notice the Biometric checkbox** = **will become unchecked/disabled** [*This governs the state of the Finger Sensor when the Reader is in idle/ready state. In this case the Finger Sensor will be "OFF" at SIGMA when this profile is assigned to a reader. However the Finger Sensor will awake/turn ON after a card is presented.*]

6.5.3.1 ABOUT THE "BIOMETRIC" OPTION

When you set a SIGMA Reader's Multifactor Mode to 'Biometric', the reader will only accept credentials that are enrolled as Biometric (finger-only). *A credential that is enrolled as a Prox+Biometric authentication type will only work at a Reader that is configured to operate in Proximity Card Multifactor Mode.*

- **Notice the Proximity Card checkbox = will uncheck/disable** [This governs the state of the Card Sensor when the Reader is in idle/ready state. In this case the Card Sensor will be "OFF" at SIGMA when this profile is assigned to a reader.]
- **Notice the Biometric checkbox** = **will become checked/enabled** [This governs the state of the finger sensor when the Reader is in idle/ready state. In this case the finger sensor will be "OFF" at SIGMA when this profile is assigned to a reader]

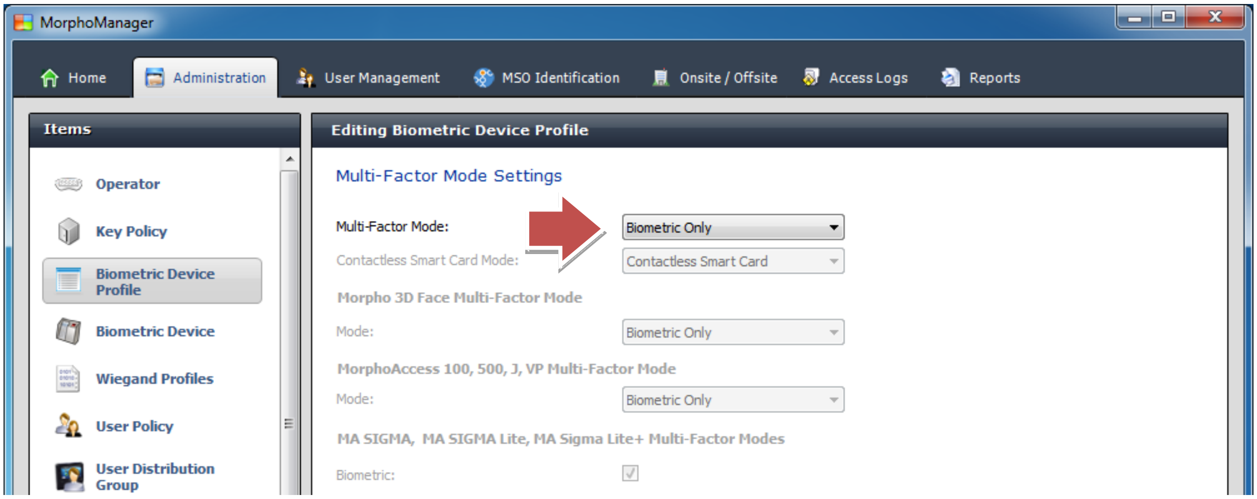
9. Set the **Multi-Factor Mode** (choose one)

   a. Choose **"Proximity Card"** if you are going to assign this Device Profile to **SIGMA-Prox readers**.

   b. Choose **"Biometric"** if you are going to assign this Device Profile to **SIGMA-Bio readers**; or for any SIGMA models you wish to operate in ***Biometric mode (finger-only)***.

10. Click **NEXT** to advance to next screen.

Figure 27 – MorphoManager: Biometric Device Profile – Multifactor Mode



Editing Biometric Device Profile

Multi-Factor Mode Settings

Multi-Factor Mode: Biometric Only

Contactless Smart Card Mode: Contactless Smart Card

Morpho 3D Face Multi-Factor Mode

Mode: Biometric Only

MorphoAccess 100, 500, J, VP Multi-Factor Mode

Mode: Biometric Only

MA SIGMA, MA SIGMA Lite, MA Sigma Lite+ Multi-Factor Modes

Biometric: ☑

INSTRUCTIONS CONTINUE ON NEXT PAGE

Continued from previous page

6.5.4 The Access Control Mode Setting

11. Set the **Access Control Mode** to "INTEGRATED". **IMPORTANT: You must set this to integrated in order to interface with the System Galaxy enrollment**.

12. Set the **Panel Feedback Mode** droplist appropriately:

a. (optional) Set to "LED in" if you are wiring SIGMA's LED-1 pin to LED-1 of the Galaxy Panel – i.e. you are using Galaxy's LED1 to control the Sigma reader's prompts for valid access.

b. Set to "NONE" if you are not wiring LED1 to the Galaxy Panel – i.e. you are not using LED1 to control reader prompts.

13. Set the **Panel Feedback No Response Timeout** option as needed (default 3000 ms = 3 secs):

a. (Only effective if **Panel Feedback** is enabled) if you set the Panel Feedback to "LED in", then set this to the desired amount of milliseconds you want the reader to wait for an access decision. If the reader does not get a Valid Access within the set timeout value, the Sigma reader will deny access.

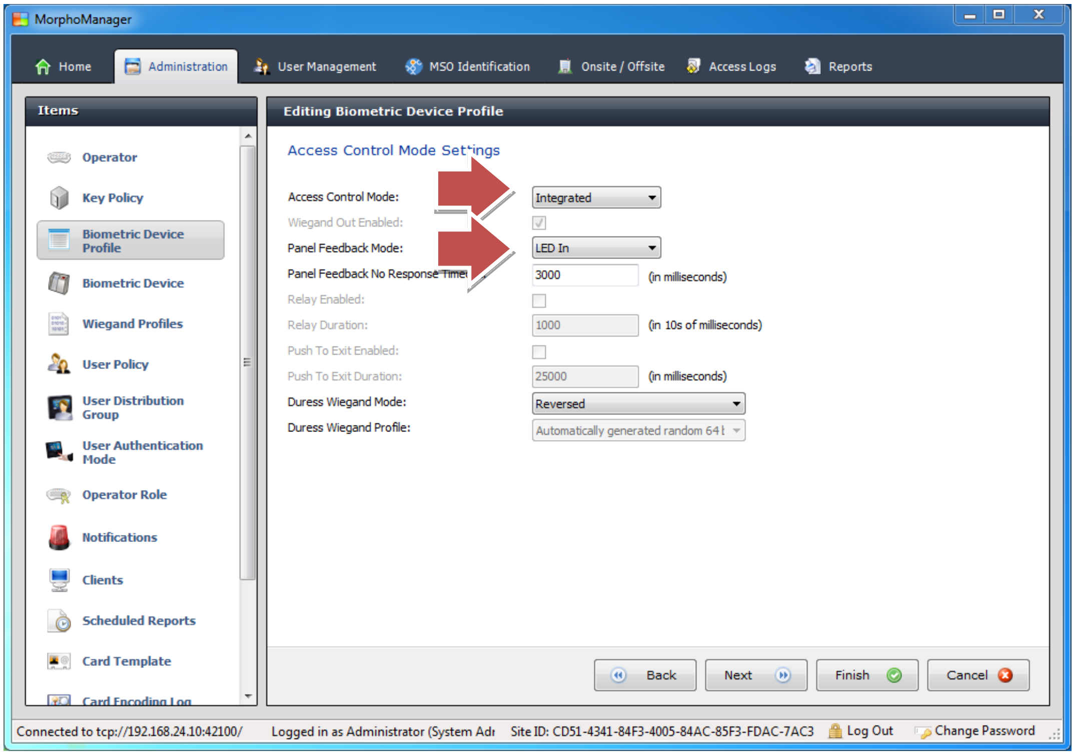
> **IMPORTANT:** you must set this option to a ***high enough value*** that allows the panel enough time to return the valid access. If this value is set too low, valid credentials will not gain access because the reader will time-out too soon.

14. Click **FINISH** to save your Profile.

(or Click NEXT to advance to next screen if you want to see remaining screens.

> **SEE** the ***MorphoManager User Guide*** for information on options outside the scope of this guide.

Figure 28 – MorphoManager: Device Profile – Access Control 'Integrated' Mode



Editing Biometric Device Profile

Access Control Mode Settings

Access Control Mode: Integrated
Wiegand Out Enabled: ☑
Panel Feedback Mode: LED In
Panel Feedback No Response Timeout: 3000 (in milliseconds)
Relay Enabled: □
Relay Duration: 1000 (in 10s of milliseconds)
Push To Exit Enabled: □
Push To Exit Duration: 25000 (in milliseconds)
Duress Wiegand Mode: Reversed
Duress Wiegand Profile: Automatically generated random 64 b

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adr Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

INSTRUCTIONS CONTINUE ON NEXT PAGE

Continued from previous page

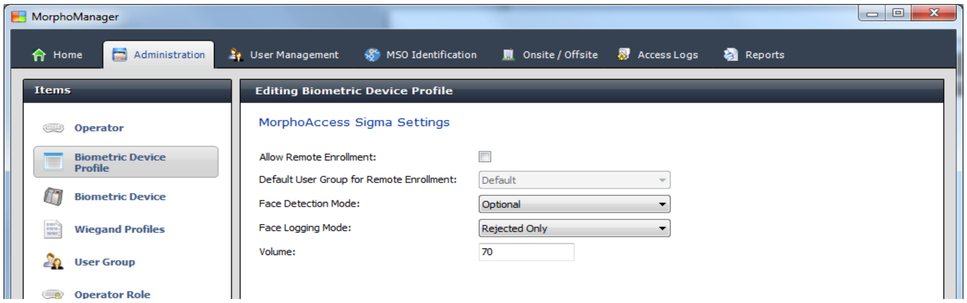
6.5.5 Remainder of Screens - Shown for Info Only

SCREEN 4 THRU 8 – are unused for the purposes of this document. See the MorphoManager User Guide for details.

15. Remote Enrollment is UNCHECKED/DISABLED.

16. (all settings in the default install condition).

17. Click NEXT to advance to next screen.



Editing Biometric Device Profile

MorphoAccess Sigma Settings

Allow Remote Enrollment: ☐

Default User Group for Remote Enrollment: Default

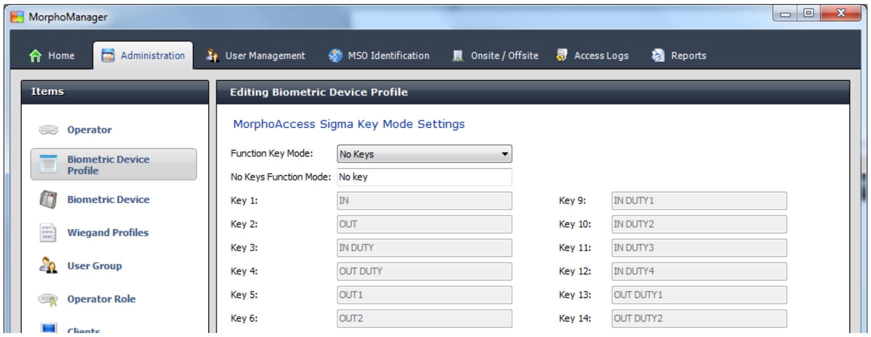
Face Detection Mode: Optional

Face Logging Mode: Rejected Only

Volume: 70

18. Function Key Mode = NO KEYS - DEFAULT INSTALL (all settings in the default install condition).

19. Click NEXT to advance to next screen.



Editing Biometric Device Profile

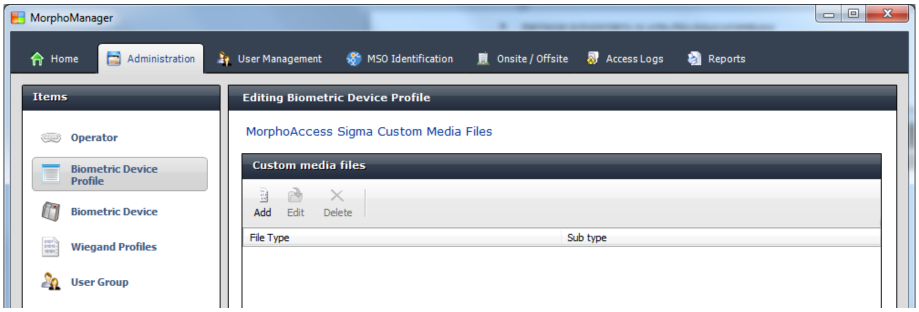
MorphoAccess Sigma Key Mode Settings

Function Key Mode: No Keys

No Keys Function Mode: No key

Key 1:	IN	Key 9:	IN DUTY1
Key 2:	OUT	Key 10:	IN DUTY2
Key 3:	IN DUTY	Key 11:	IN DUTY3
Key 4:	OUT DUTY	Key 12:	IN DUTY4
Key 5:	OUT1	Key 13:	OUT DUTY1
Key 6:	OUT2	Key 14:	OUT DUTY2

20. Click FINISH to save your Profile.



Editing Biometric Device Profile

MorphoAccess Sigma Custom Media Files

Custom media files

File Type	Sub type

See the section on Adding a Biometric Reader to assign the Device Profile to the Reader.

INSTRUCTIONS FINISHED FOR THIS SECTION

6.6 ADDING A BIOMETRIC DEVICE (READER)

This section covers adding and configuring the SIGMA biometric readers.

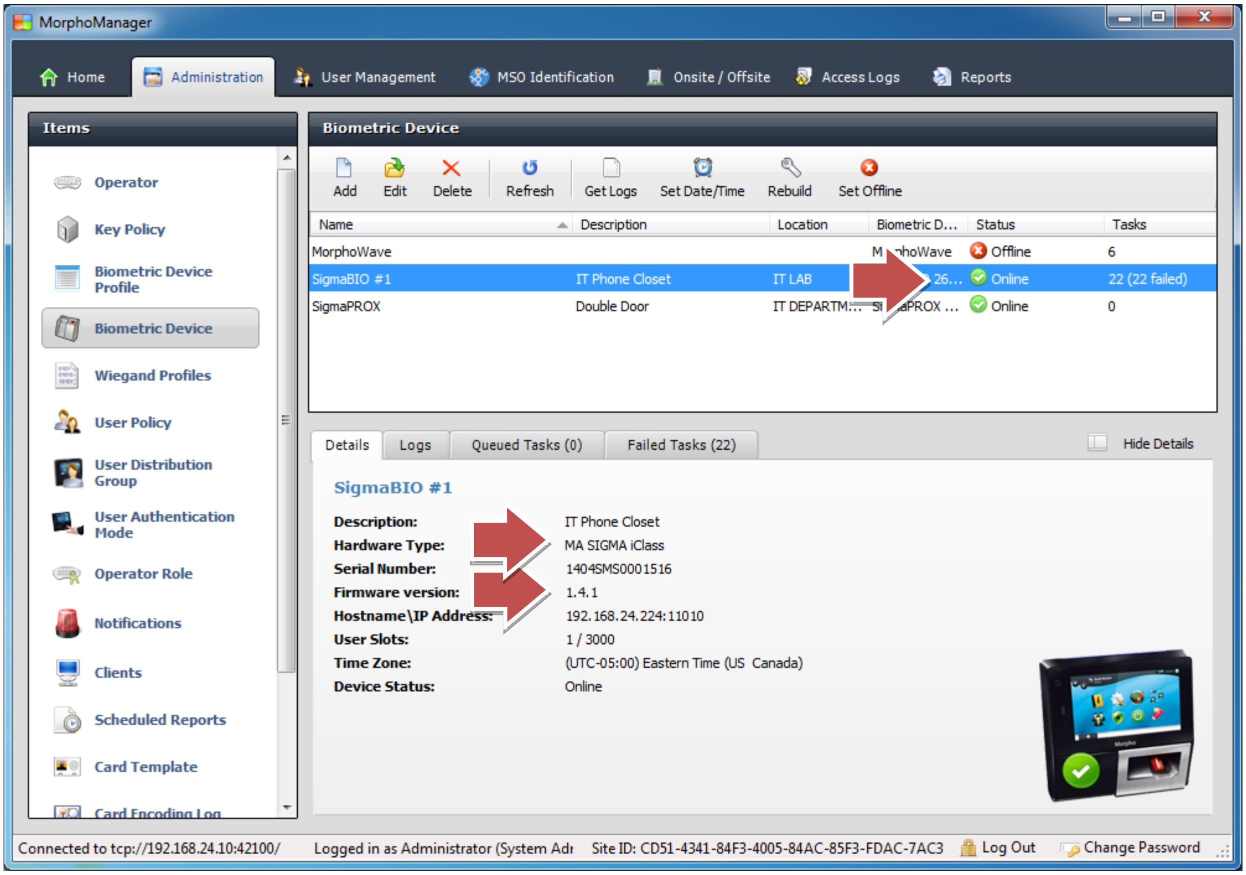
6.6.1 Viewing the List & States of Configured Readers:

When a SIGMA Reader has been added, this is what the screen will look like if the Reader is connected and correctly configured. Note the Screen reports the following:

- Type = **MA SIGMA Prox**
- Firmware Version should show = **1.4.1**
- Device Status = **ONLINE (may take a few minutes for the reader to come online)**
- User Slots: 1/3000 (1 User Record in the reader currently/3000 total available)

1. Click ADD or EDIT button to begin configuring a new or existing reader.

Figure 29 – MorphoManager: Adding a Biometric Device (Sigma Reader)



Name	Description	Location	Biometric D...	Status	Tasks
MorphoWave			M phoWave	Offline	6
SigmaBIO #1	IT Phone Closet	IT LAB	26...	Online	22 (22 failed)
SigmaPROX	Double Door	IT DEPARTM...	Si aPROX ...	Online	0

SigmaBIO #1

Description:	IT Phone Closet
Hardware Type:	MA SIGMA iClass
Serial Number:	1404SMS0001516
Firmware version:	1.4.1
Hostname\IP Address:	192.168.24.224:11010
User Slots:	1 / 3000
Time Zone:	(UTC-05:00) Eastern Time (US Canada)
Device Status:	Online

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

INSTRUCTIONS CONTINUE ON NEXT PAGE

Continued from previous page

6.6.2 Adding a Biometric Reader

1. Enter a Name for the Reader; and it is recommended to add a description and location.

2. Set the Hardware Family to “**MA Sigma”**

3. Enter the **IP Address** of the reader

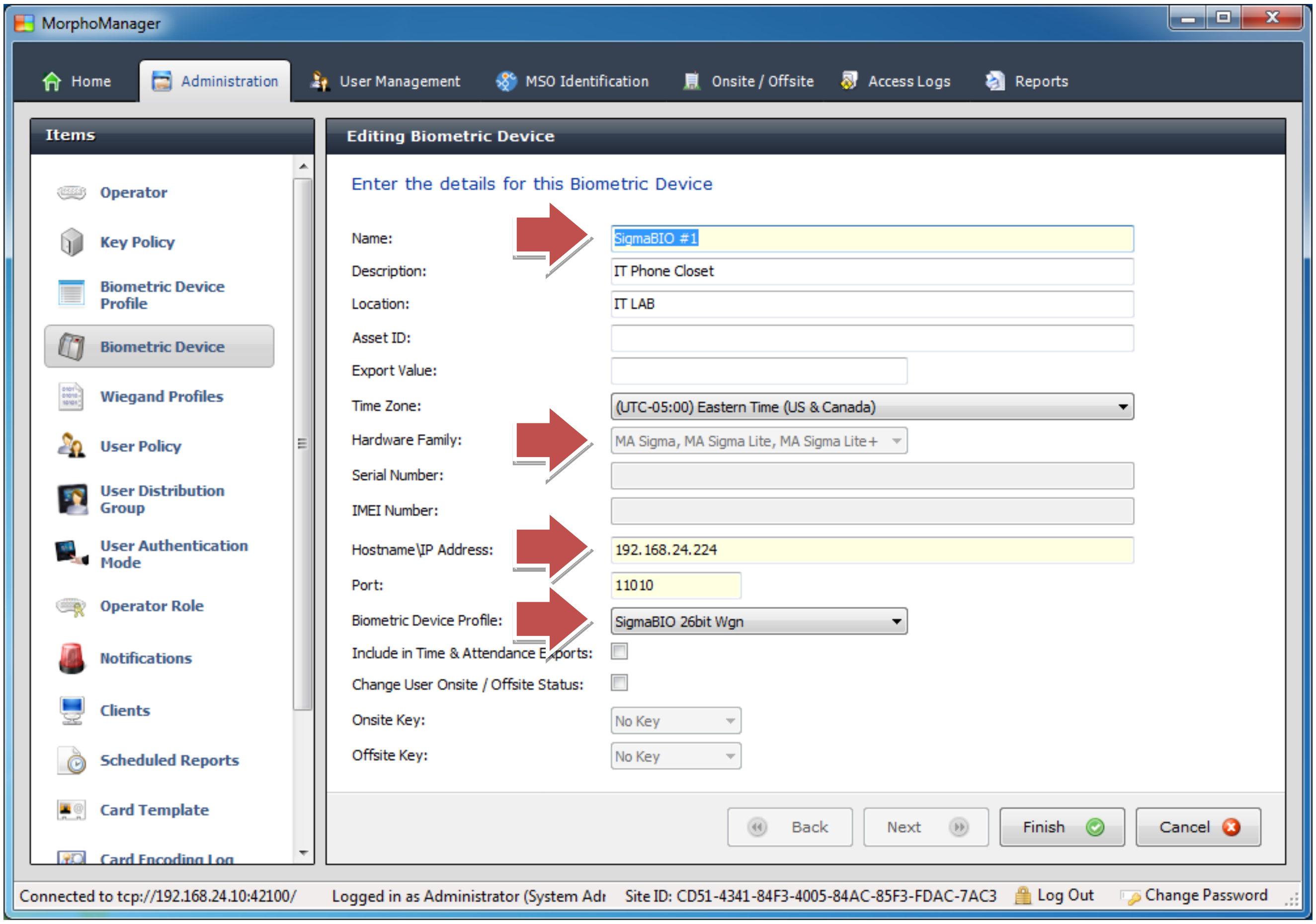
4. Leave the Port default as “11010”

5. Set the [**Biometric Device Profile** droplist] to the desired ***Biometric Device Profile Name*** that you have already created (and have configured to use the Wiegand Profile of your choice). See the previous section on ‘Creating a Biometric Device Profile’ for more info.

> NOTE: in the screenshot below the system was using ***26-bit Wiegand*** and thus named their *Biometric Device Profile Name* to reflect it was using 26-bit Wiegand (you can see why it helps to indicate the Wiegand Profile in the Device Profile Name – because in this step you know which profile to pick).

6. **Click FINISH to save your Reader.**

Figure 30 – MorphoManager: Adding a SIGMA Reader



Editing Biometric Device

Enter the details for this Biometric Device

Name: SigmaBIO #1

Description: IT Phone Closet

Location: IT LAB

Asset ID:

Export Value:

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Hardware Family: MA Sigma, MA Sigma Lite, MA Sigma Lite+

Serial Number:

IMEI Number:

Hostname\IP Address: 192.168.24.224

Port: 11010

Biometric Device Profile: SigmaBIO 26bit Wgn

Include in Time & Attendance Exports: □

Change User Onsite / Offsite Status: □

Onsite Key: No Key

Offsite Key: No Key

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

CONFIGURING BIOMETRIC DEVICE IS COMPLETED

6.7 CONFIGURING A USER DISTRIBUTION GROUP

User Distribution Group will distribute user credentials onto the MA Readers or MorphoManager Clients. In order to be utilized the user must be in a User Policy that has its Access Mode set to “Per User”. Then the User Distribution Groups will be selectable when creating (or editing) a user.

IMPORTANT NOTES

- You must have **one** User Distribution Group configured to enroll credentials.
- It must be mapped to the ‘biometric Access Group’ in the BioBridge tab.

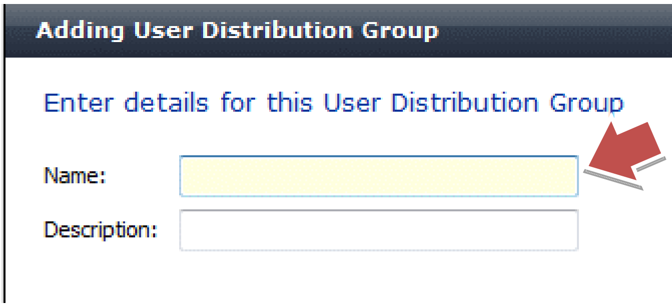
> There may be a “Default” user distribution group already available when you first install the main client. You can rename it or create a different one. You must enable all the readers you have added (checkbox options) or the credentials will not be sent to the reader.

6.7.1 Creating a User Distribution Group

1. Enter a **Name** and **Description** that appropriately identifies the distribution group and it’s purpose. (Galaxy supports only one user distribution group)

2. Click **NEXT** to continue programming.

Figure 31 – MorphoManager: User Distribution Group



Adding User Distribution Group

Enter details for this User Distribution Group

Name:

Description:

INSTRUCTIONS CONTINUE ON NEXT PAGE

Continued from previous page

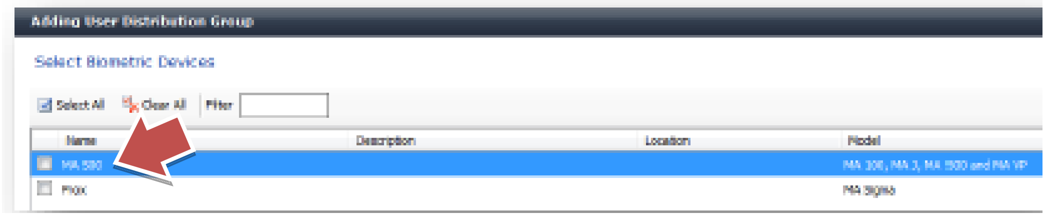
6.7.2 Assigning the Readers

3. Click [**SELECT ALL**] to select all readers or individually click each reader you want in this group.
   Note: The “Clear All” button will remove access to all devices.

4. Click **NEXT** to continue programming.

> If you add READERS later you must come back and check them to include them in the group.

Figure 32 – MorphoManager: User Distribution Group



Adding User Distribution Group

Select Biometric Devices

	Name	Description	Location	Model
☐	MA 500			MA 100, MA 3, MA 500 and MA VP
☐	Prox			MA Sigma

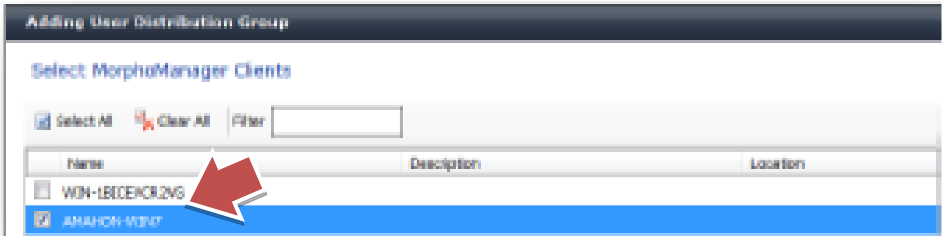
6.7.3 Assigning the Clients

5. Click [**SELECT ALL**] to select all clients ***or individually click each MorphoManager client*** you want in this group. This is required to enable enrolling.

6. Click **FINISH** to save programming.

> If you add CLIENTS later you must come back and check them to include them in the group.

Figure 33 – MorphoManager: User Distribution Group



Adding User Distribution Group

Select MorphoManager Clients

	Name	Description	Location
☐	WIN-1BIDEKCR2VG		
☑	AMAHON-WIN7		

> **SEE** the ***MorphoManager User Guide*** for information on options outside the scope of this guide.

6.8 SYSTEM CONFIGURATION – FOR BIOBRIDGE ENROLLMENT MODULE

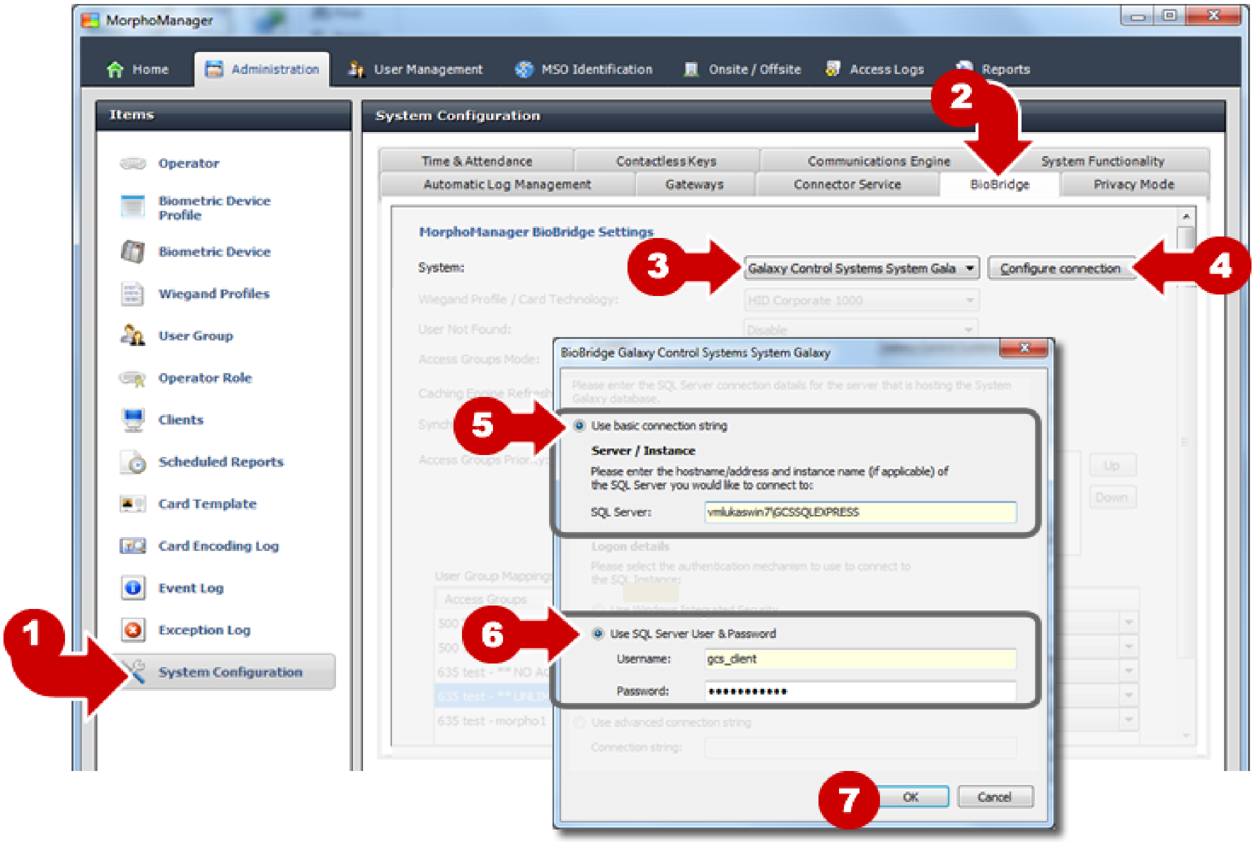
This section covers how to configure the system settings on the BioBridge tab. These settings are used by the BioBridge module to connect and synchronize the Galaxy database for updates. These settings also govern which credentials to import/update, which **user distribution group** to use, and which access group names to import.

6.8.1 BioBridge Tab – System Galaxy Database Connection Parameters:

The System Galaxy database connection settings must be configured.

1. From the Administration screen, click the **System Configuration** button on the menu (left side).
2. Click on the **BioBridge** tab
3. Select "Galaxy Control Systems System Galaxy" for the System droplist.
4. Click the [**Configure Connection**] button.
5. Enter the ***server name*** and ***instance***.
6. Provide the **SQL Server login parameters** for the System Galaxy client.
7. Click **OK**.

Figure 34 – MorphoManager: System Galaxy Database Connection for BioBridge



System: Galaxy Control Systems System Gala

Wiegand Profile / Card Technology: HID Corporate 1000

User Not Found: Disable

BioBridge Galaxy Control Systems System Galaxy

Please enter the SQL Server connection details for the server that is hosting the System Galaxy database.

● Use basic connection string

Server / Instance

Please enter the hostname/address and instance name (if applicable) of the SQL Server you would like to connect to:

SQL Server: vmlukaswin7\GCSSQLEXPRESS

Logon details

Please select the authentication mechanism to use to connect to the SQL Instance:

○ Use Windows Integrated Security

● Use SQL Server User & Password

Username: gcs_client

Password: ●●●●●●●●●●●●

○ Use advanced connection string

Connection string:

INSTRUCTIONS CONTINUE ON NEXT PAGE

Continued from previous page

6.8.2 BioBridge Module – Setting the Wiegand Profile

MorphoManager /BioBridge Module supports only one system-wide site code and Wiegand format.

IMPORTANT > CARD TECHNOLOGY & SITE CODE MUST MATCH SITE-WIDE for ALL BIOMETRIC READERS: When the SG Operator is enrolling biometric credentials, s/he must choose the same *Card Technology* and *Site Code* in System Galaxy Cardholder screen that is specified in the MorphoManager *System Configuration screen* (see Figure 35 below) This applies to both Authentication Types (i.e. Card+finger and finger only). You must use the same card format for a SigmaPROX [card + finger] as you use for a SigmaBIO [finger only].

NOTE > SUPPORT FOR MULTIPLE CARD FORMATS & READER TYPES AT SG (non-biometric): System Galaxy continues to support *multiple card formats and reader types* at the Galaxy system level, but the Morpho specifications supersede for biometric enrollment. **MorphoManager/BioBridge supports only one biometric credential per cardholder record**; however, a Galaxy Cardholder can still have multiple non-biometric credentials with different formats for use at different non-biometric readers. If you are upgrading a legacy system that used Legacy 520/110 Readers you need to contact technical support to determine your best path forward.

8. Set the **Wiegand Profile / Card Technology** droplist to the Card Technology you will enroll and associate with biometric credentials.

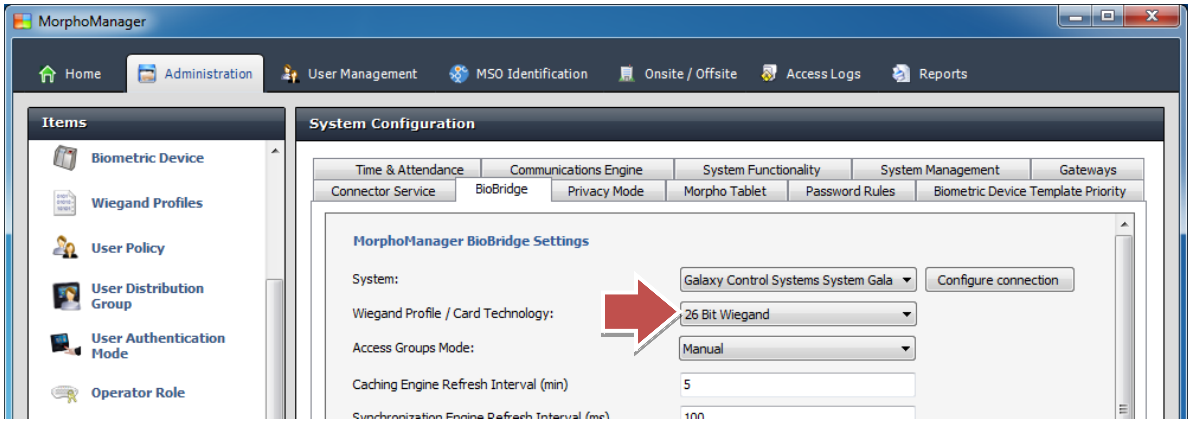
FUNCTIONALITY OF THE WIEGAND PROFILE SETTING:

This setting specifically determines the type of card/credentials that the BioBridge synchronization module will query (filter) from the System Galaxy database when scanning for updates or accepting new enrollments.

The BioBridge synchronization module will ignore/skip records that do not match the designated card type. ***This is a system-wide setting for MorphoManager****, which means that every place in the MorphoManager software that configures the Wiegand Profile must match the same value that is chosen in the System /BioBridge Configuration.*

For example: if you have both SigmaPROX and SigmaBIO readers in the same system, they must all use the same card format and site code.

Figure 35 – MorphoManager: Setting the BioBridge Wiegand Profile



System: Galaxy Control Systems System Gala

Wiegand Profile / Card Technology: 26 Bit Wiegand

Access Groups Mode: Manual

Caching Engine Refresh Interval (min) 5

Synchronization Engine Refresh Interval (ms) 100

6.8.3 BioBridge Module –the User Not Found option (moved)

9. The **User Not Found** setting has been relocated to the *System Management tab*.

(See section of this guide that covers the *BioBridge User Group mapping*.)

INSTRUCTIONS CONTINUE ON NEXT PAGE

Continued from previous page

6.8.4 BioBridge Module – Setting the Access Group Mode

This field determines how the MorphoManager Client will map the imported Access Group Names from the Access control System to the User Distribution Group Names in MorphoManager.

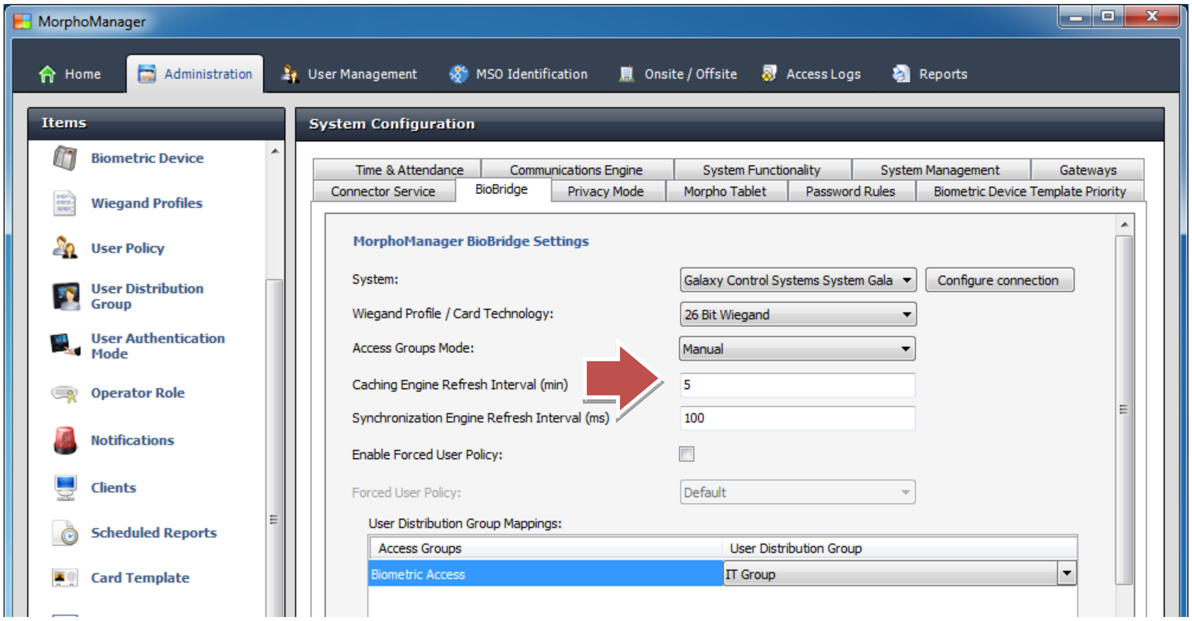
PREREQUISITES:

- The *Access Group Name* must already exist in System Galaxy ("Biometric Access" is default).
- The *User Distribution Group Names* must already exist in the MMC.

10. Set the **Access Group Mode** to "manual".

Manual mode: means the Operator must manually map the *User Distribution Group Name* in MMC to the *Access Group Name(Biometric Access)* imported from System Galaxy.

Figure 36 – MorphoManager: BioBridge Access Group Mode



MorphoManager BioBridge Settings

System: Galaxy Control Systems System Gala

Wiegand Profile / Card Technology: 26 Bit Wiegand

Access Groups Mode: Manual

Caching Engine Refresh Interval (min): 5

Synchronization Engine Refresh Interval (ms): 100

Enable Forced User Policy: □

Forced User Policy: Default

User Distribution Group Mappings:

Access Groups	User Distribution Group
Biometric Access	IT Group

INSTRUCTIONS CONTINUE ON NEXT PAGE

Continued from previous page

6.8.5 BioBridge Client – Mapping User Distribution Group

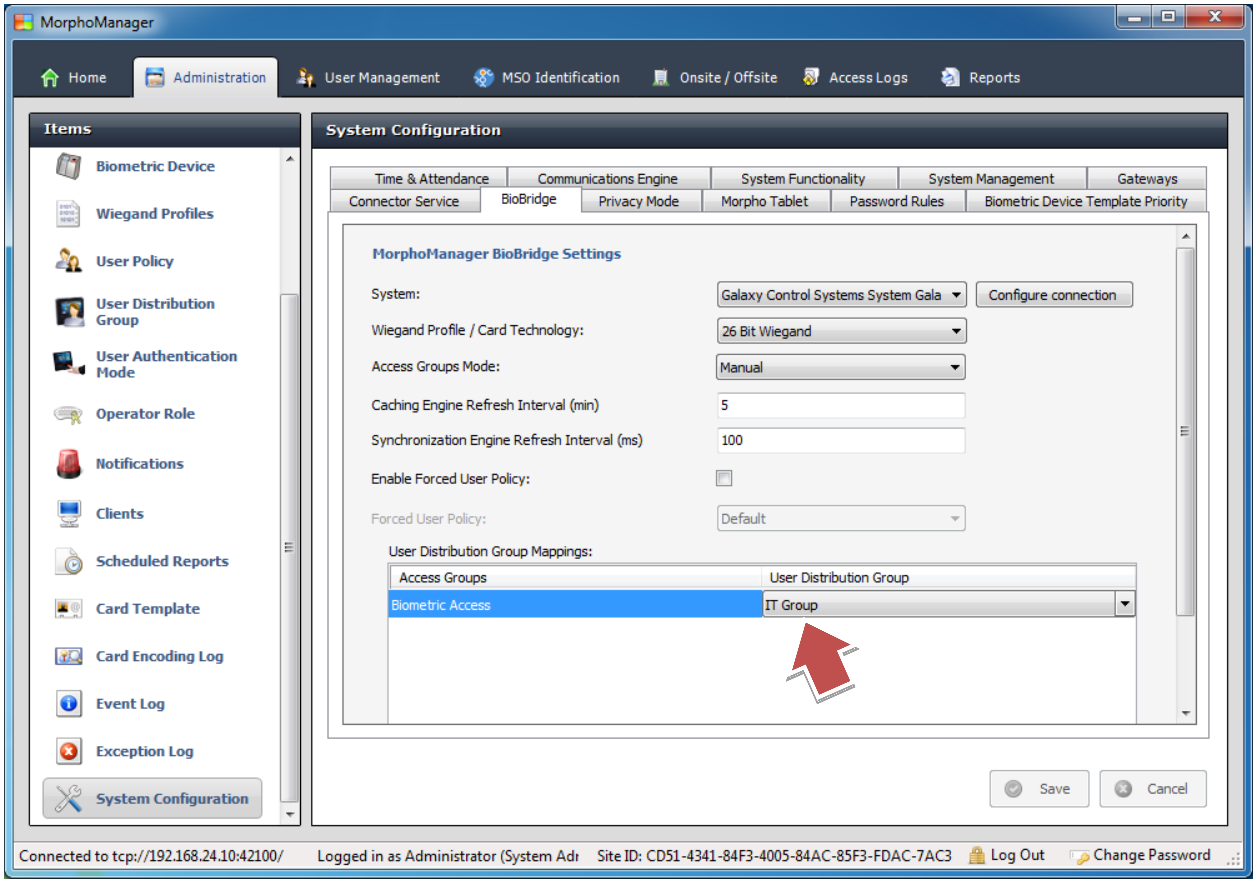
User Distribution Group Name and Access Group Name must be created before you can map this.

11. In the **User Distribution Group** droplist, choose the user distribution group name you configured in the previous section. This officially maps that group to the Access Group from System Galaxy.

12. Click SAVE to save.

MorphoManager v9x supports only one User Distribution Group per User/Credential. Therefore only one Group mapping is supportable for System Galaxy. System Galaxy sets the Access Group Name to "Biometric Access" (see below). Operator can map the Default Access Group to this Access Group name.

Figure 37 – MorphoManager: BioBridge User Distribution Group Mapping



MorphoManager BioBridge Settings

System: Galaxy Control Systems System Gala

Wiegand Profile / Card Technology: 26 Bit Wiegand

Access Groups Mode: Manual

Caching Engine Refresh Interval (min): 5

Synchronization Engine Refresh Interval (ms): 100

Enable Forced User Policy: □

Forced User Policy: Default

User Distribution Group Mappings:

Access Groups	User Distribution Group
Biometric Access	IT Group

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

CONFIGURING BIOBRIDGE TAB IS COMPLETED

6.9 DISABLED USER MANAGEMENT– SYSTEM CONFIGURATION

This section covers how to configure the **Disabled User Management setting (i.e.** USER NOT FOUND) in the System Management tab.

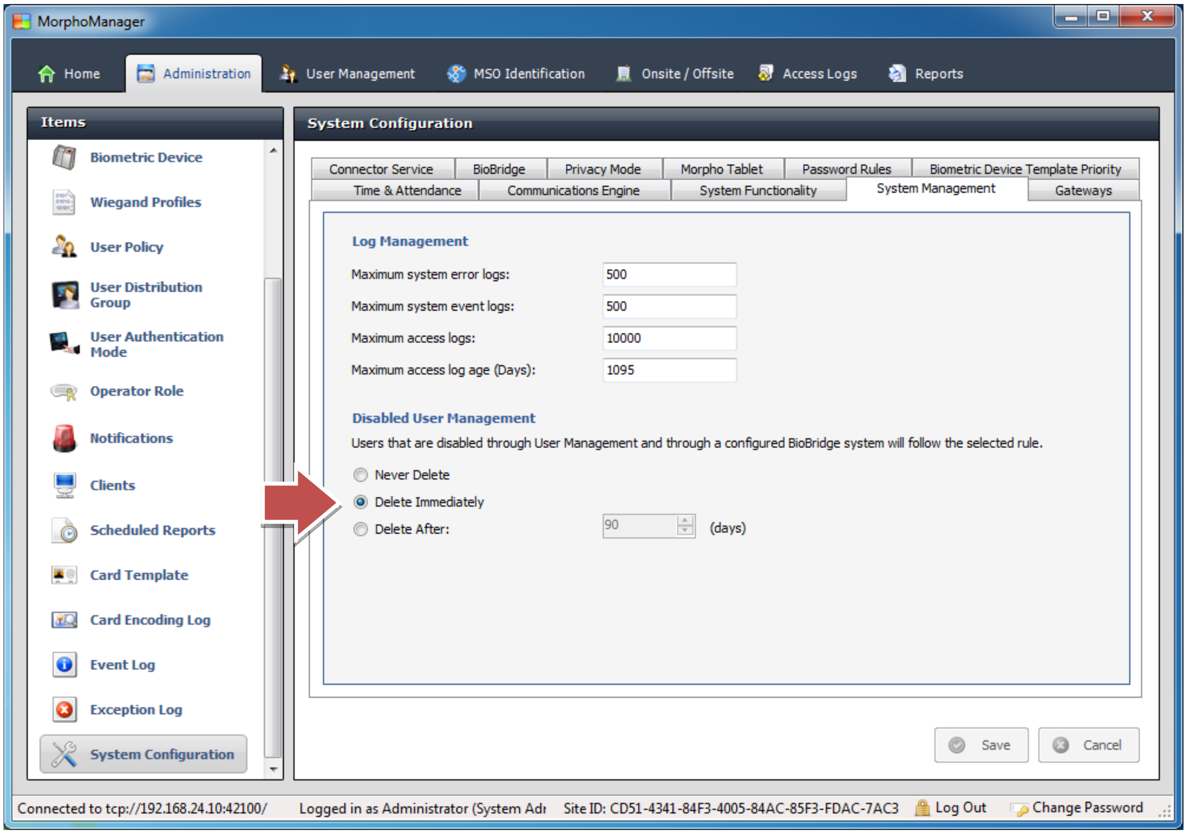
This option determines how a credential is handled when one of the following conditions occur …

a) If the **cardholder is disabled** in System Galaxy (Personnel Tab)
b) the **credential is deleted** from System Galaxy (Card/Badge Settings Tab)

6.9.1 System Management Tab – Handling of Deleted/Disabled Credentials

1. Set the **Disabled User Management** setting to the desired setting …
   - Never Delete (prints / ID remain in Reader)
   - **Delete Immediately** (recommended) - (prints/ID immediately removed from Reader)
   - Delete After XX Days (prints / ID are removed after specified number of days)
2. Click SAVE to save.

Figure 38 – MorphoManager: Disabled User Management Setting



Log Management

Maximum system error logs: 500
Maximum system event logs: 500
Maximum access logs: 10000
Maximum access log age (Days): 1095

Disabled User Management

Users that are disabled through User Management and through a configured BioBridge system will follow the selected rule.

○ Never Delete
● Delete Immediately
○ Delete After: 90 (days)

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adı Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

CONFIGURING USER MANAGEMENT TAB IS COMPLETED

7 Enrolling Biometric Credentials in System Galaxy

This chapter covers how to enroll biometric credentials from System Galaxy.

7.1 REQUIREMENTS FOR ENROLLING BIOMETRIC CREDENTIALS IN SYSTEM GALAXY

The SG Operator must follow specific steps and meet enrollment requirements when enrolling biometric credentials in System Galaxy.

7.1.1 Requirements for Enrolling Biometric Credentials

When creating **Biometric Credentials** be sure to meet the following requirements.

ENROLLMENT REQUIREMENTS - FOR ENROLLING BIOMETRIC CREDENTIALS ON AN ACCESS CARD:

ENROLLMENT REQUIREMENT	SYMPTOM	REMEDY
SG Access Card must be enrolled/saved and include the correct loop and at least one Access Group before the enrollment can successfully proceed.	Enroll button may be disabled in SG. BioBridge will not launch.	**In SG** = Properly add the access card/cardholder
SG Card Technology must match the ***BioBridge Wiegand Profile.***	Card will not work at SIGMA Reader. Reader will not prompt for fingers.	**In SG** = Select the correct Card Type. **In MM** = Configure the correct Wiegand Profile in BioBridge tab.
SG **Site Code/Facility Code** of card must match the Site Code in MorphoMgr ***Wiegand Profile***.	Card will not work at SIGMA Reader. Reader will not prompt for fingers.	**In SG** = Enter the correct Site Code/FAC. **In MM** = Configure the correct site code in the MM *Wiegand Profile* screen.
SG valid Loop/Cluster must be assigned to the card **before** it is saved.	Operator can't enroll fingers. BioBridge Module fails on USER DISTRIBUTION validation.	**In SG** = Assign the correct Loop and **save card**.
SG the card must have **at least one valid access group** assigned **before** it is saved.	Operator can't enroll fingers. BioBridge Module fails on USER DISTRIBUTION GROUP validation.	**In SG** = Assign a valid Access Group and **save card**.
BioBridge module – the operator must choose the correct User Policy (**Authent. Mode)** when the BioBridge Module opens.	Card will not work at SIGMA Reader if the wrong user policy is select, or if the user policy's auth mode doesn't match the reader's multifactor mode. Reader displays "rule triggered mismatch".	**In SG** = if multiple Auth Types are enabled, the SG Operator must select which type to enroll. **In MM** = the User Policy must be configured for the correct Authent Mode.
MM the **User DISTRIBUTION** must be mapped to ***Galaxy Biometric Access*** before enrolling.	Operator can't enroll fingers. BioBridge Module fails on USER DISTRIBUTION GROUP validation.	In MM = map the right User DISTRIBUTION to the Biometric Access Group in the BioBridge tab.
MM the correct **Authentication Mode** must be enabled in the **User Policy** before enrolling.	Credential won't work at SIGMA reader. Operator didn't choose the correct User Policy (**Auth Mode)** during enrollment.	In SG = Assign a valid Access Group / **save card**. Also select the correct User Policy during enroll. In MM = enable the compatible Authent. Mode for the intended reader's Multifactor Mode.

7.1.2 Stipulations for Enrolling Finger-Only Credentials

The same requirements must be met for ***Biometric-only Credentials*** as for ***Card + Biometric Credentials*** – although you may or may not want to issue a physical access card. To enroll biometrics in SG without issuing a physical card, the card code must be a unique ID in the system and must have a valid site code/facility code. This format and site code must the Wiegand format assigned to BioBridge through the MorphoManager Wiegand Profile.

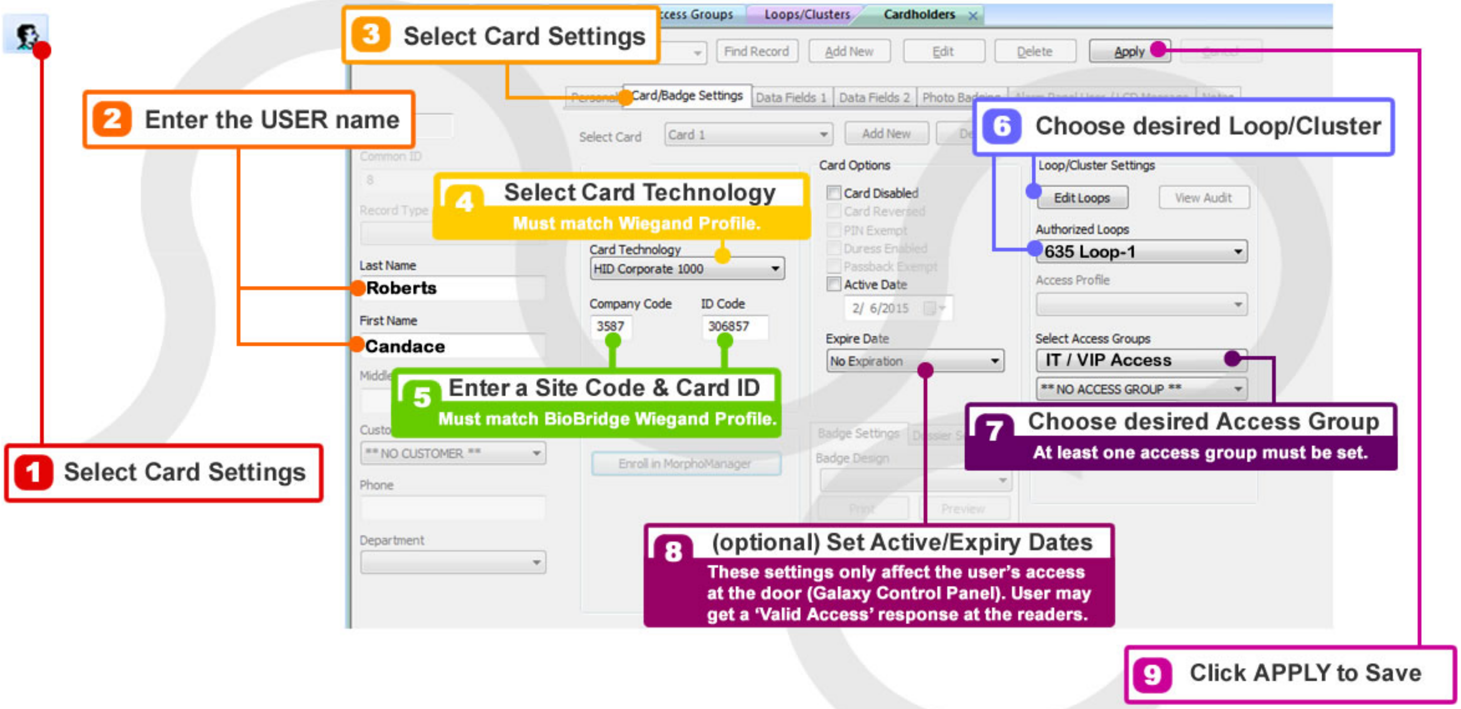
Enrolling Biometric-Only credentials must meet all the requirements listed in the table above.

7.1.3 How to Enroll a Valid Access Card in System Galaxy

In the cardholder screen, the Operator must enroll and save the access card ID before the ***ENROLL button*** will enable to allow biometric enrollment. The following steps and Infographic show the specific settings that must be performed to enroll a valid access card.

1. Click on the 👤 **CARDHOLDER toolbar button** to open the Cardholder screen.
2. Enter a **First** and **Last Name** for the Cardholder (user); and any other data as appropriate.
3. Select the **Card/Badge Settings tab**.
4. Set the **Card Technology** (HID Corporate 1000; or 26bit Wiegand, The Card Type must match the Wiegand Profile type that was configured in the MorphoManager BioBridge tab.)
5. Enter the correct **Site Code** and **Card ID**. (These must match the Wiegand Profile configured in MorphoManager.)
6. Choose any valid **Loop/Clusters** by clicking the EDIT LOOPS button.
7. Select any and all **Access Groups** desired for the user, including Personal Doors.
8. Configure other settings (active/expiry dates*) as needed. *Note: Card Options (active/expiry) do not affect SIGMA response.*
9. **Click APPLY to save the Card/Cardholder.** After the access card is initially saved, SG Operator will Edit the record to enroll the biometric credentials.
    - Only one biometric credential can be added to a Galaxy Cardholder. (*This is a limitation of BioBridge*).
    - If a User needs 2 or more biometric credentials, the SG Operator must make a separate Cardholder Record in System Galaxy for the additional biometric. BioBridge does not support multiple credentials on the same user.
    - The Galaxy Cardholder can have other non-biometric credentials on the same Cardholder Record.

Figure 39 – SYSTEM GALAXY: Enrolling Card & Assigning Access Privileges



1 Select Card Settings

2 Enter the USER name

3 Select Card Settings

4 Select Card Technology
Must match Wiegand Profile.

5 Enter a Site Code & Card ID
Must match BioBridge Wiegand Profile.

6 Choose desired Loop/Cluster

7 Choose desired Access Group
At least one access group must be set.

8 (optional) Set Active/Expiry Dates
These settings only affect the user's access at the door (Galaxy Control Panel). User may get a 'Valid Access' response at the readers.

9 Click APPLY to Save

Last Name: Roberts
First Name: Candace
Customer: ** NO CUSTOMER **
Card Technology: HID Corporate 1000
Company Code: 3587
ID Code: 306857
Active Date: 2/ 6/2015
Expire Date: No Expiration
Authorized Loops: 635 Loop-1
Select Access Groups: IT / VIP Access
** NO ACCESS GROUP **

*NOTICE: See section on wiring Relay-2 to control the Sigma Voice Command to match with panel response for invalid access.

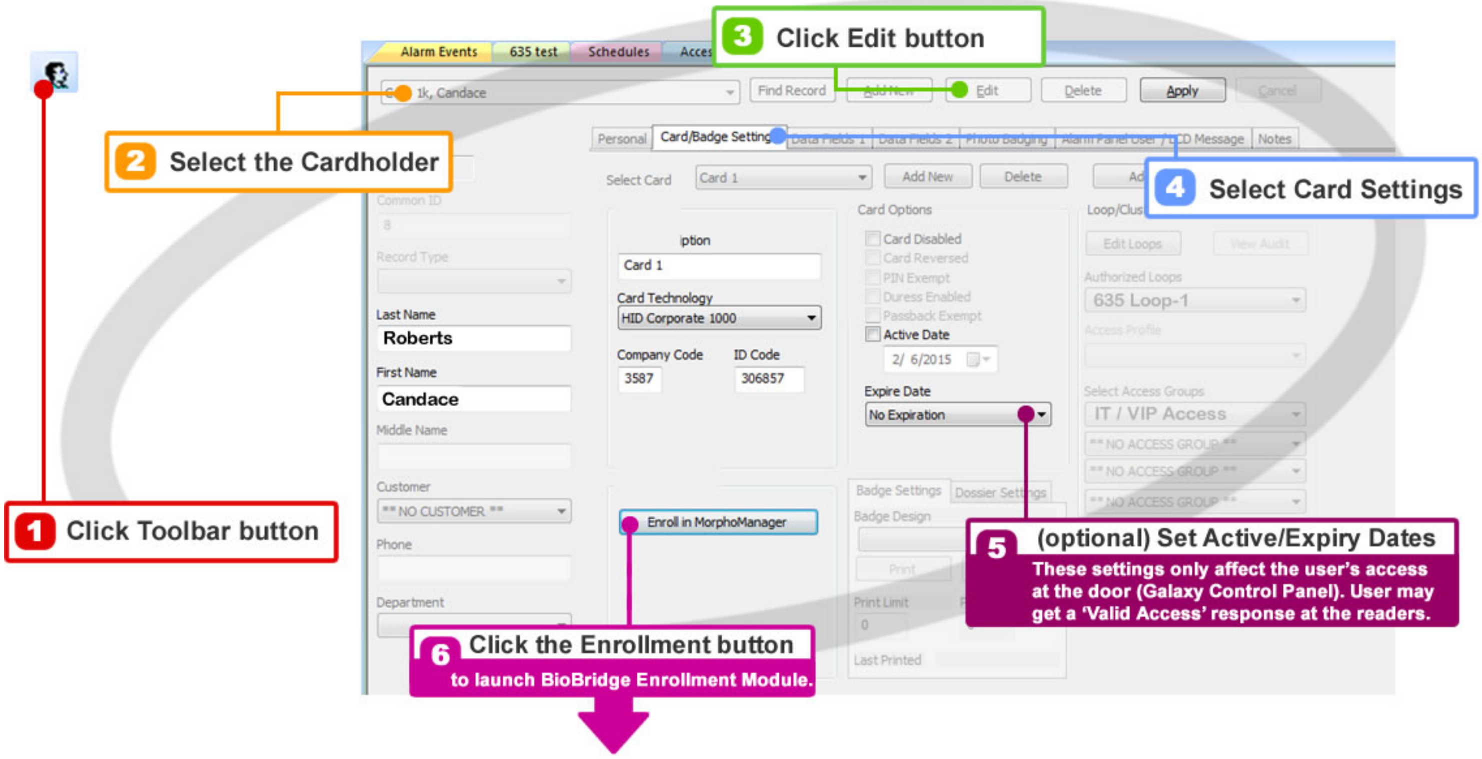
7.1.4 How to Enroll Biometric Credentials on an Access Card

The SG Operator must have already added and saved a **valid** card before *biometric credentials* can be enrolled successfully. All requirements are listed below with the symptom they cause if not met. *See prior section for instructions on Adding Cards.*

1. Click the **Cardholder toolbar button** to open the Cardholder screen.
2. Select the desired **Cardholder Name** from the top droplist**.**
3. Click the Cardholder **EDIT button** to place card in edit mode.
4. Select **Card/Badge Settings** tab.
5. (optional) set any **Active or Expiration dates*** as desired.
6. Click the **[Enroll in MorphoManager] button.** (if this button is disabled, the card has not been saved).

*NOTICE: See section on wiring Relay-2 to control the Sigma Voice Command to match with panel response for invalid access.

Figure 40 – SYSTEM GALAXY: Enrolling Biometric Credentials



1 Click Toolbar button

2 Select the Cardholder

3 Click Edit button

4 Select Card Settings

5 (optional) Set Active/Expiry Dates

These settings only affect the user's access at the door (Galaxy Control Panel). User may get a 'Valid Access' response at the readers.

6 Click the Enrollment button to launch BioBridge Enrollment Module.

Last Name: Roberts

First Name: Candace

Card Technology: HID Corporate 1000

Company Code: 3587

ID Code: 306857

Active Date: 2/ 6/2015

Expire Date: No Expiration

Authorized Loops: 635 Loop-1

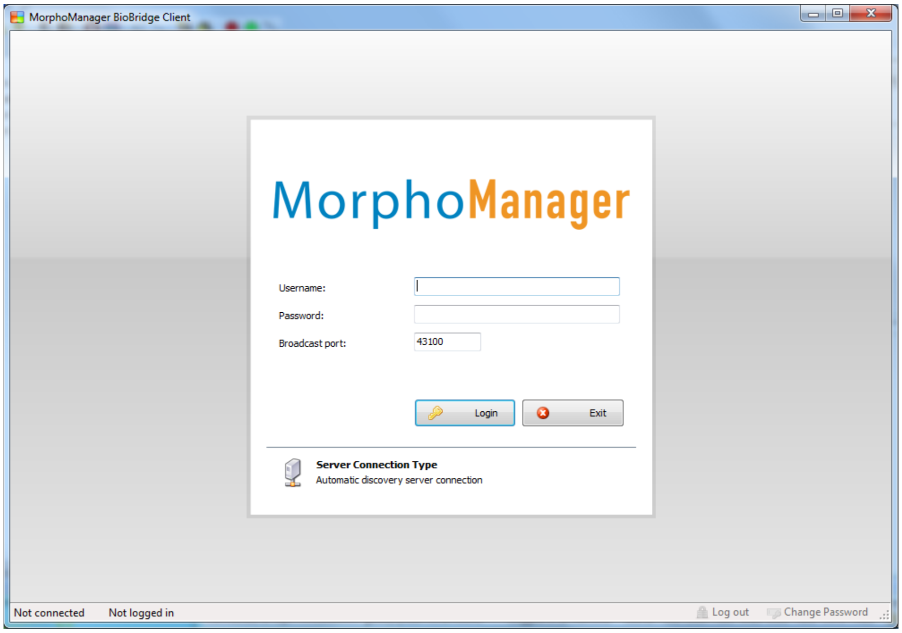
Select Access Groups: IT / VIP Access

INSTRUCTIONS CONTINUE ON NEXT PAGE

7. **The BioBridge client will launch.**

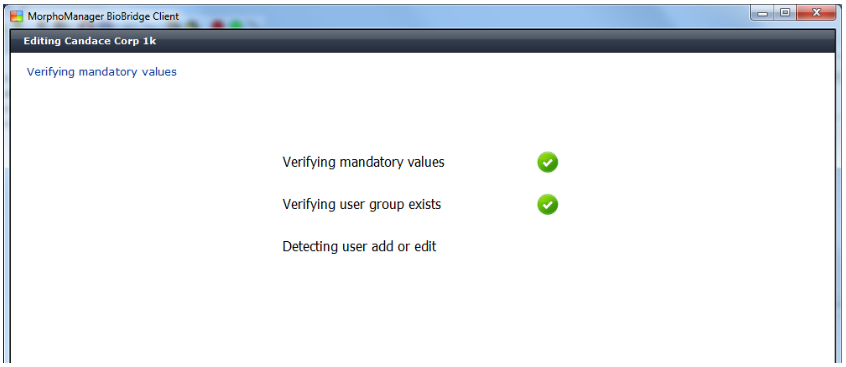
8. The system will automatically log-in only if the operator password is preconfigured in the Client Configuration Tool (recommended). Otherwise, SG Operator must log in manually.

Figure 41 – BIOBRIDGE MODULE: MorphoManager Login screen



9. The BioBridge system will automatically check for the associated **user policy and other mandatory values**.

Figure 42 – BIOBRIDGE MODULE: Detecting User Policy & other mandatory values



Verifying mandatory values ✓

Verifying user group exists ✓

Detecting user add or edit

IMAGE IS CROPPED

NOTE: if any of the mandatory requirements are not met, the BioBridge will fail to open and may return an error message to user.

7.1.5 Choosing the User Policy for the Credential

10. Select on the **User Policy** that you intend to enroll.

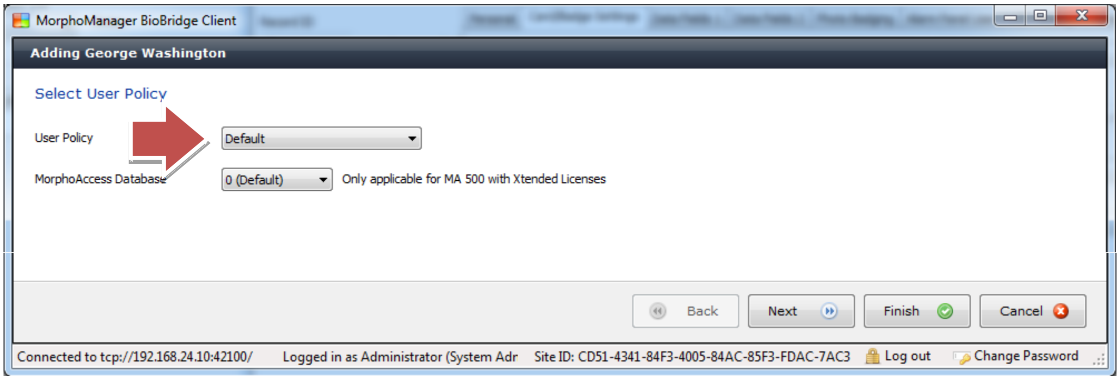
IMPORTANT: If the credential doesn't match, the user will get a "RULE TRIGGERED MISMATCH" at the reader when the credential is presented.

The SG Operator must select a **User Policy (Authentication Mode)** that is compatible with the Reader(s) Multi-Factor mode. Credentials only work at readers that are configured for the matching Multi-Factor Mode.

If you configured only one **User Policy** for the system, then this screen will NOT display.
If you configured more than one User Policy, the operator must choose the appropriate policy for the credential.

- If the credential must work at SigmaBIO readers, the operator must choose the policy that is configured for the "biometric" authentication mode.
- If the credential must work at SigmaPROX readers, the operator must choose the policy that is configured for the "card + biometric" authentication mode.

Figure 43 – BIOBRIDGE MODULE: Choosing the User Policy



MorphoManager BioBridge Client

Adding George Washington

Select User Policy

User Policy: Default

MorphoAccess Database: 0 (Default) Only applicable for MA 500 with Xtended Licenses

Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adr Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3 Log out Change Password

(you must pick the appropriate User Policy to get the correct Mode)

Authentication Mode	&	**Multi-Factor Mode**
Set in the MorphoManager User Policy		Set in the MorphoManager Device Profile
GETS ASSIGNED TO THE CREDENTIAL AT ENROLLMENT		GETS ASSIGNED TO THE READER
Contactless Card + Biometric	=	"Proximity Card"
Biometric Only	=	"Biometric"

INSTRUCTIONS CONTINUE ON NEXT PAGE

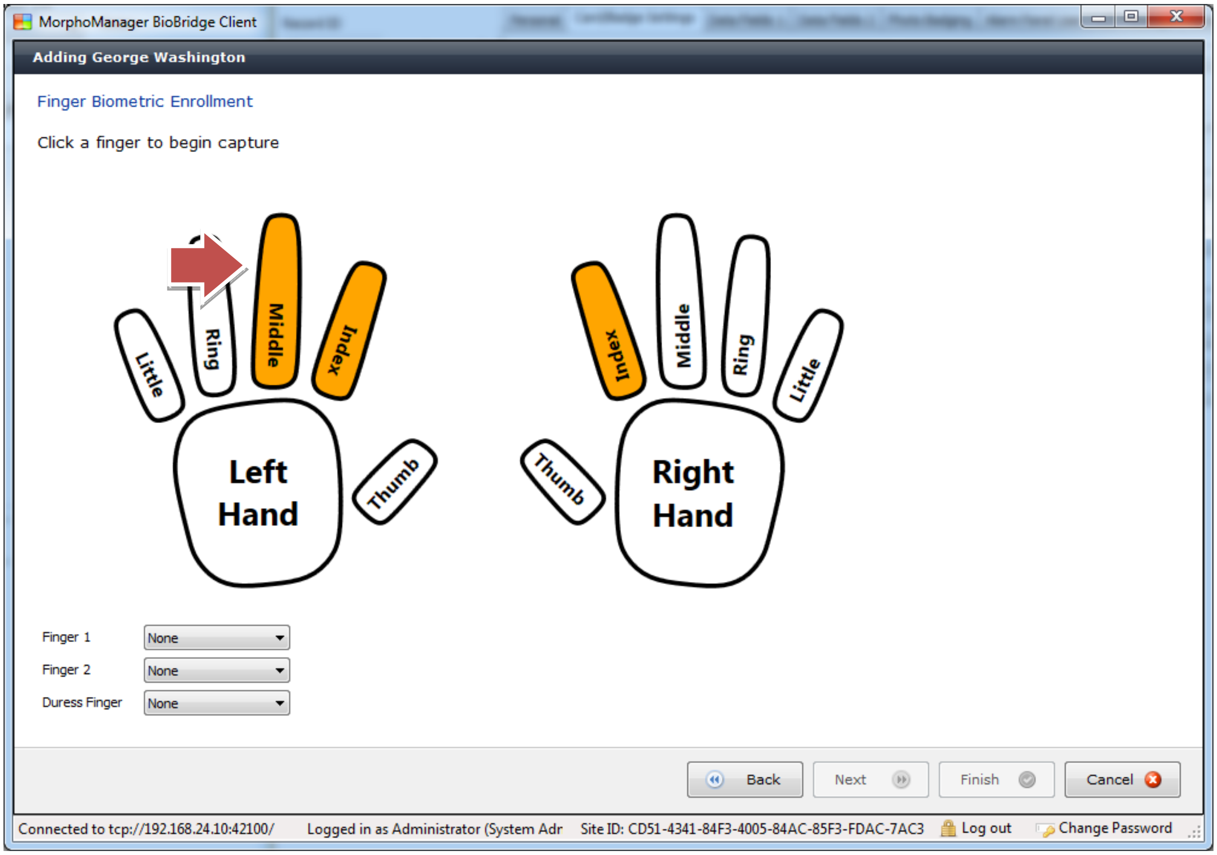
7.1.6 Capturing Fingers for the Biometric Credentials

Position your fingerprint in the middle of the MSO window for best results.

11. Operator will click on each finger as the cardholder is enrolled

12. NOTE that the duress finger will not be used for normal access.

Figure 44 – BIOBRIDGE MODULE: Enrolling Fingers in BioBridge Module


MorphoManager BioBridge Client

Adding George Washington

Finger Biometric Enrollment

Click a finger to begin capture

Finger 1: None

Finger 2: None

Duress Finger: None

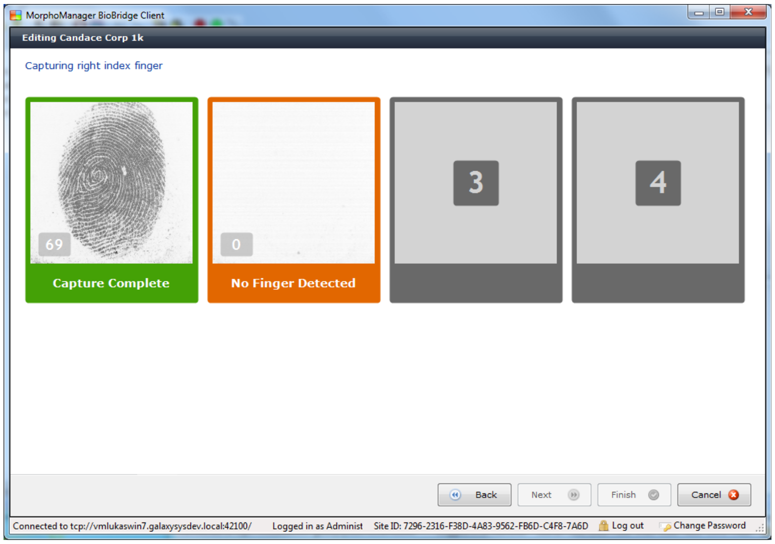
Connected to tcp://192.168.24.10:42100/ Logged in as Administrator (System Adr Site ID: CD51-4341-84F3-4005-84AC-85F3-FDAC-7AC3

INSTRUCTIONS CONTINUE ON NEXT PAGE

13. The system will prompt the Operator to capture the four prints for each finger. Each frame will turn green when the finger capture is successful.

Figure 45 – BIOBRIDGE MODULE: Fingerprint Capture screen

Position your fingerprint in the middle of the window for best results.



MorphoManager BioBridge Client

Editing Candace Corp 1k

Capturing right index finger

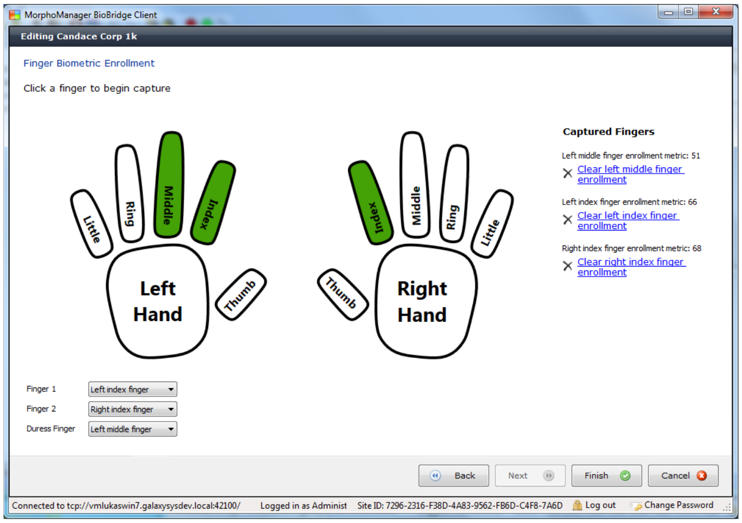
Connected to tcp://vmlukaswin7.galaxysysdev.local:42100/ Logged in as Administ Site ID: 7296-2316-F38D-4A83-9562-FB6D-C4F8-7A6D Log out Change Password

14. The screen returns to the Enrollment Hand screen and Operator must click on the next unenrolled finger and perform the Finger Capture process for each finger.

15. NOTE that the duress finger will not be used for normal access.

16. Click FINISH when all fingers are captured.

Figure 46 – BIOBRIDGE MODULE: Enrolling Fingers screen



MorphoManager BioBridge Client

Editing Candace Corp 1k

Finger Biometric Enrollment

Click a finger to begin capture

Captured Fingers

Left middle finger enrollment metric: 51

× Clear left middle finger enrollment

Left index finger enrollment metric: 66

× Clear left index finger enrollment

Right index finger enrollment metric: 68

× Clear right index finger enrollment

Finger 1: Left index finger

Finger 2: Right index finger

Duress Finger: Left middle finger

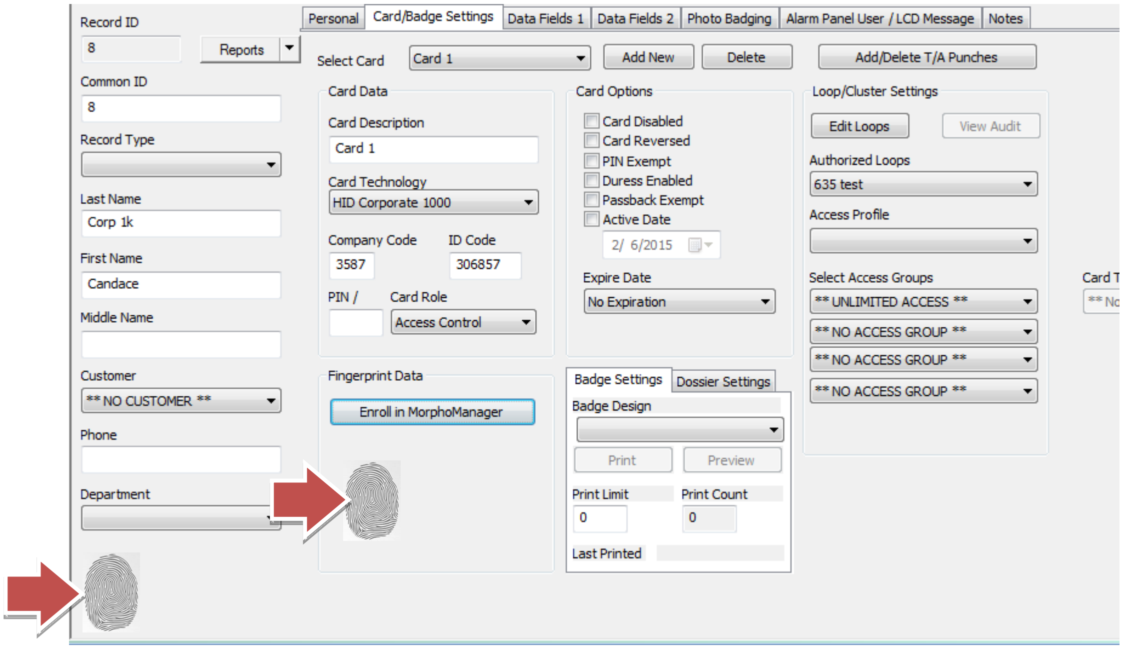
Connected to tcp://vmlukaswin7.galaxysysdev.local:42100/ Logged in as Administ Site ID: 7296-2316-F38D-4A83-9562-FB6D-C4F8-7A6D Log out Change Password

17. Operator will click APPLY in the System Galaxy Cardholder screen.

18. The user should be successfully added . User Card+Biometric record will appear in the MorphoManager User List and will be added to the appropriate SIGMA readers.

> *A biometric icon will appear on the Cardholder record under the [Department] field if the Cardholder has a biometric credential enrolled. A biometric icon will appear on the Card Settings tab under the [Enroll…] button for the specific card that is assigned to biometric credentials.*

Figure 47 – SYSTEM GALAXY: Saving the Biometric Credentials



Record ID: 8

Common ID: 8

Record Type:

Last Name: Corp 1k

First Name: Candace

Middle Name:

Customer: ** NO CUSTOMER **

Phone:

Department:

Select Card: Card 1

Card Description: Card 1

Card Technology: HID Corporate 1000

Company Code: 3587

ID Code: 306857

PIN /

Card Role: Access Control

□ Card Disabled
□ Card Reversed
□ PIN Exempt
□ Duress Enabled
□ Passback Exempt
□ Active Date: 2/ 6/2015

Expire Date: No Expiration

Authorized Loops: 635 test

Access Profile:

Select Access Groups: ** UNLIMITED ACCESS **, ** NO ACCESS GROUP **, ** NO ACCESS GROUP **, ** NO ACCESS GROUP **

Badge Design:

Print Limit: 0

Print Count: 0

Last Printed

7.2 MANAGING EXISTING BIOMETRIC CREDENTIALS FROM SYSTEM GALAXY

7.2.1 Deleting a Card/User Credential from System Galaxy

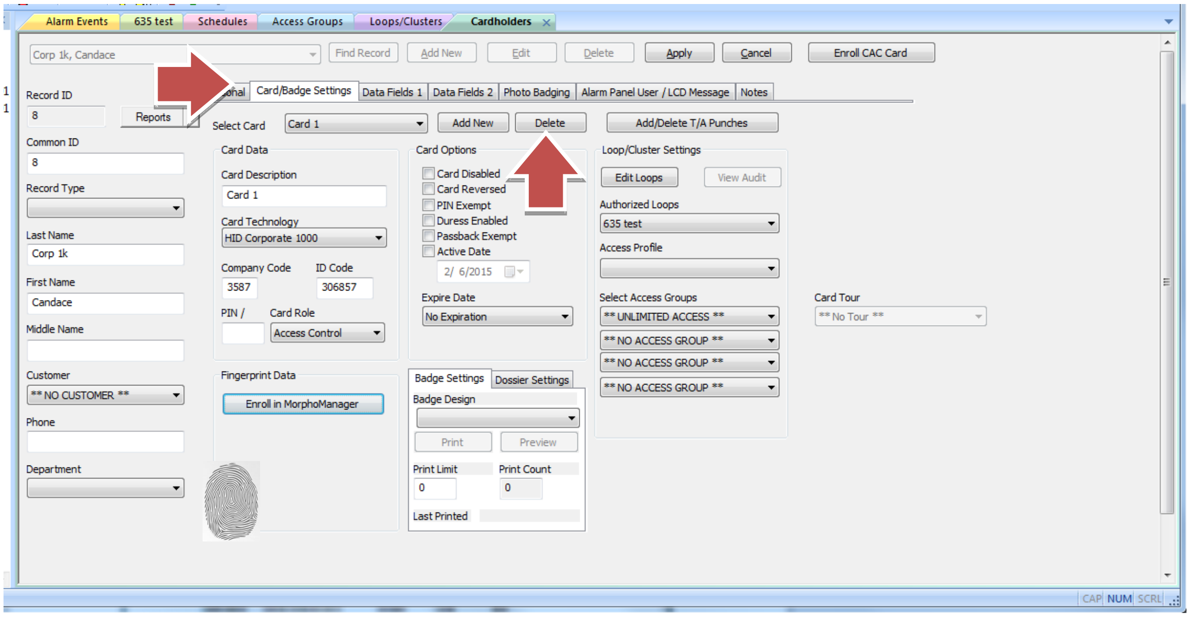
The Operator can delete a card or the entire Cardholder.

> NOTE: Delete the entire cardholder in System Galaxy will remove all the activity history for that user. Be sure you really want to delete a cardholder.

1. Click on the **CARDHOLDER toolbar button** to open the Cardholder screen.
2. Select the desired **cardholder name** from the droplist.
3. Click the **EDIT button**.
4. Click the **Card Settings tab**.
5. **Select the Card** that shows the finger print icon below the ENROLL button.
6. Click the **DELETE button for the Card Record** (not the delete button on the Cardholder)
7. Click **APPLY** to save the Cardholder.
8. The corresponding User should immediately be removed from the MorphoManager User List and from the appropriate SIGMA READER.
9. Operator can click the **refresh button** in the MorphoManager User List to refresh the list if needed.

> If User does not delete from the MorphoManager User List and Sigma reader, the operator may need to delete the User manually from the MorphoManager User List.

Figure 48 – SYSTEM GALAXY: Deleting a Credential



Corp 1k, Candace

Record ID 8

Common ID 8

Last Name Corp 1k

First Name Candace

Customer ** NO CUSTOMER **

Select Card Card 1

Card Description Card 1

Card Technology HID Corporate 1000

Company Code 3587

ID Code 306857

Card Role Access Control

2/ 6/2015

Expire Date No Expiration

Authorized Loops 635 test

Select Access Groups ** UNLIMITED ACCESS **

** NO ACCESS GROUP **

** NO ACCESS GROUP **

** NO ACCESS GROUP **

Card Tour ** No Tour **

Print Limit 0

Print Count 0

7.2.2 Re-Enrolling Biometric Credentials for Existing Cardholder

The Operator can re-enroll a biometric capture for the cardholder for administrative purposes; such as the user has injured or damaged their hand/finger and need to enroll a different finger.

Galaxy recommends the operator deletes the existing credentials from the system.

IMPORTANT: It is not necessary or recommended to delete the entire cardholder in System Galaxy in order to switch or reenroll fingers.

1. Click on the **CARDHOLDER toolbar button** to open the Cardholder screen.
2. Select the desired **cardholder name** from the droplist.
3. Click the **EDIT button**.
4. Click the **Card Settings tab** and **select the card** with the biometric from the Card droplist.
5. Click the **DELETE key** for the Card Record (not the delete key on the Cardholder)
6. Click **APPLY** to save the Cardholder so that the user credentials are removed from the MorphoManager User List and from any SIGMA Readers. Operator can click the refresh button in the MorphoManager User List to refresh the list if needed.
7. To re-enroll fingers, simply put the cardholder in EDIT mode.
8. Click the **ADD NEW button**
9. Select the **Cart Technology**
10. Select the **desired loop** and **access group** privileges.
11. Click **APPLY** to save the settings
12. place the cardholder back in edit mode again.
13. Select the **desired card** and **click the ENROLL BIOMETRIC button** and begin enrolling fingers as appropriate.
14. The enrollment module will be launched – see prior section depicting the enrollment process.

7.2.3 Replacing Lost Card ID

The Operator can simply edit the card ID for an existing cardholder that has a biometric credential without having to re-enroll the fingers. Simply EDIT the cardholder in System Galaxy and change the card ID. After you click the APPLY button to save the change, the BioBridge will detect the change.

You can see the card ID in the User List by editing the User in the MorphoManager. Always change card ID from within Galaxy software. The new card should work immediately at the reader with the original prints.

7.2.4 Changing a Cardholder's First or Last Name

The Operator can simply edit the Cardholder record and change the First or Last Name for an existing cardholder that has a biometric credential without having to re-enroll the fingers. Simply EDIT the cardholder in System Galaxy and change the Name as appropriate. After you click the APPLY button to save the change in System Galaxy, the BioBridge will detect the change.

If the name change is not immediately picked up by MorphoManager/BioBridge, then click the REFRESH button in the . MorphoManager User List. Restarting MorphoManager Client can also trigger a refresh.

7.2.5 Chart of Events at System Galaxy Panel

The following chart shows the various status/conditions the user/credential can be in, and the result at the reader, panel, and what event will occur in System Galaxy.

Ultimately, it is the Galaxy Access Panel that makes the final decision whether to grant or deny access.

The SIGMA reader is designed to issue a verbal and visual "access granted" when a credential and the biometric template is found and matches within the SIGMA Reader. This does not guarantee access to the door or entry point from the Galaxy system. This is because the SIGMA is not designed to understand which access privileges or which schedules are applied to the Cardholder/Credential in System Galaxy.

NOTE: if the SIGMA does not identify the user (user not found), the reader will issue "access denied" and send the card code with a '0' site code to the Galaxy Panel. This will result in a NOT IN SYSTEM in System Galaxy. Right-clicking the incoming card code will not discover an existing cardholder record it normally would from another reader since the SIGMA passes a '0' site code. However you can right-click the incoming card code to discover the card ID and then search for it in your system database.

Figure 49 – SYSTEM GALAXY: Chart of Events

USER / CREDENTIAL STATUS	READER RESPONSE	PANEL RESPONSE	EVENT AT SG
User presents wrong finger	SIGMA will DENY – Biometric Mismatch	Panel will deny access	NOT IN SYSTEM 🔒
User presents correct finger at a reader that is set to a Multifactor Mode that does not match the authentication type on the credential	SIGMA will DENY – Rule Triggered Biometric Mismatch (ex: Credential enrolled as *Biometric* Auth Type presented at reader using *Prox Mode*)	Panel will deny access	NOT IN SYSTEM 🔒
User is expired or disabled in SG	SIGMA will GRANT credential	Panel will deny access	NOT IN SYSTEM
User is deleted from SG	SIGMA will DENY – User Not Found	Panel will deny access	NOT IN SYSTEM 🔒
User does not have access at door	SIGMA will GRANT credential	Panel will deny access	**INVALID ACCESS**
User is not within scheduled access	SIGMA will GRANT credential	Panel will deny access	**INVALID ACCESS**
User presents correct finger	**SIGMA will GRANT credential**	**Panel will grant access**	**VALID ACCESS**

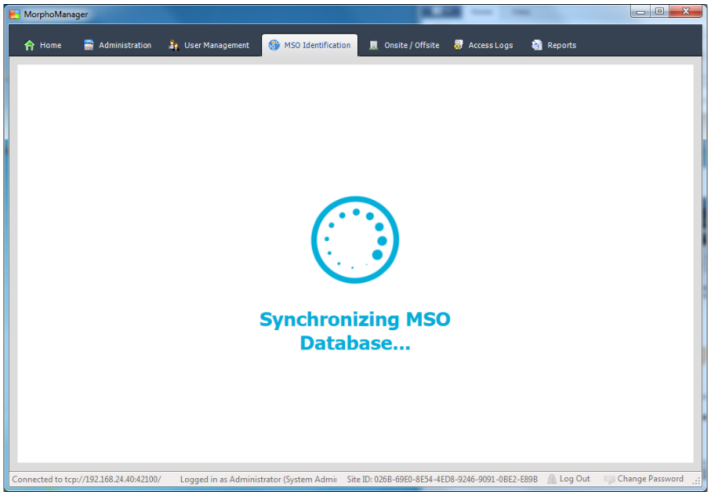
7.3 IDENTIFYING EXISTING BIOMETRIC CREDENTIALS FROM MORPHOMANAGER

7.3.1 Identifying a Credential:

The MSO device drivers are installed with the MorphoManager Client software, so you should be able to connect (plug in) the MSO Enrollment device at this time, if you have not already done so.
1.Plug in (connect) the MSO Enrollment Station to the computer that will enroll the credentials.

2.Select the MSO Identification tab in the MorphoManager Client and this screen will display:

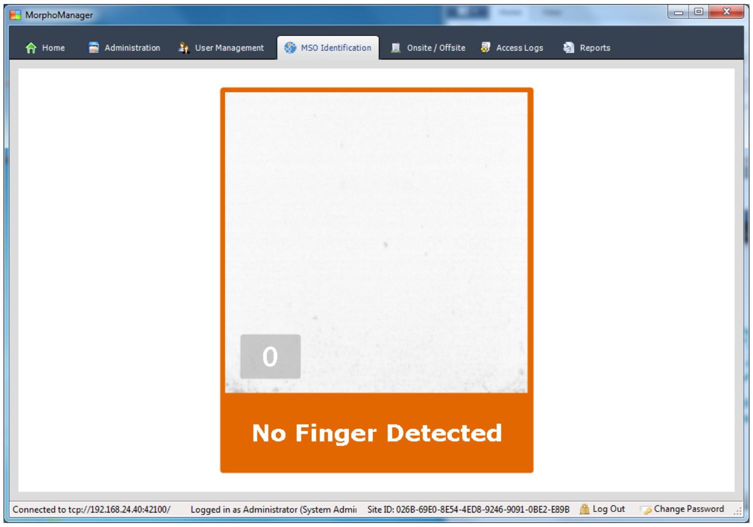
Figure 50 – ENROLLMENT VERIFICATION: MSO Synchronization



Synchronizing MSO Database...

Connected to tcp://192.168.24.40:42100/ Logged in as Administrator (System Admi Site ID: 026B-69E0-8E54-4ED8-9246-9091-0BE2-E89B

3.Screen-2 of MSO Identification – prompting for finger (MSO Sensor is LIT):

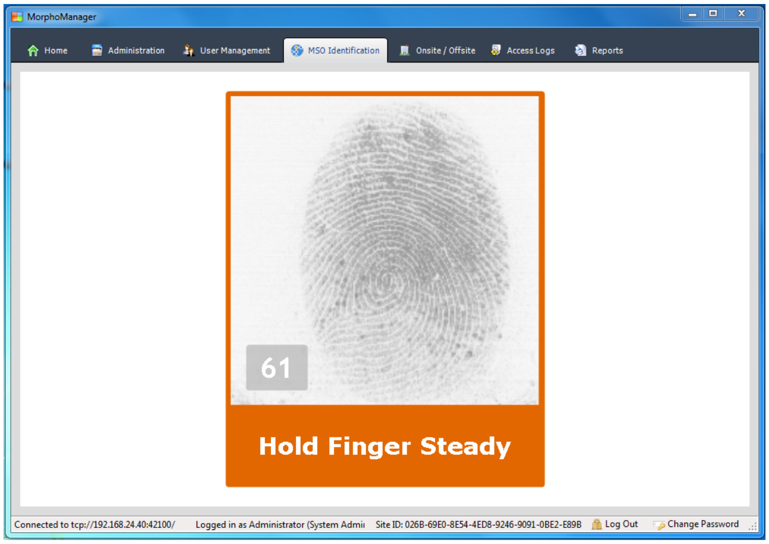


No Finger Detected

Connected to tcp://192.168.24.40:42100/ Logged in as Administrator (System Admi Site ID: 026B-69E0-8E54-4ED8-9246-9091-0BE2-E89B

If there are no fingers in the MorphoManager database, you will not get this prompt/frame display. Instead you will get a message stating that there are no fingers in the system and the MSO sensor will not be lit. *This does not mean the MSO is not connected*. You will verify the MSO connection during the enrollment, which is covered in a later chapter. You must complete the configuration of the MorphoManager software before you can enroll from Galaxy.

4.Place your finger on the MSO Finger Sensor:



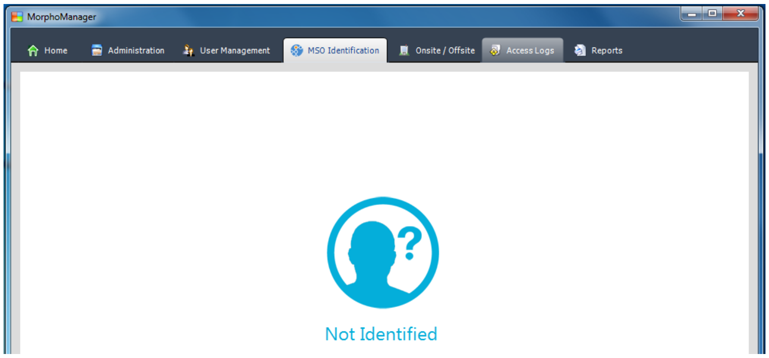
Hold Finger Steady

Connected to tcp://192.168.24.40:42100/ Logged in as Administrator (System Admi Site ID: 026B-69E0-8E54-4ED8-9246-9091-0BE2-E89B

5.The software will return one of three possible screens:

a. MorphoManager returns the name/identity of the person to whom the finger belongs, if the finger has been enrolled.

b. MorphoManager returns “Not Identified” if the finger has not been enrolled, but there are other fingers in the database. (see



Not Identified

INSTRUCTIONS FINISHED FOR THIS SECTION