MorphoAccess® SIGMA Series

Quick User Guide

IDEMIA

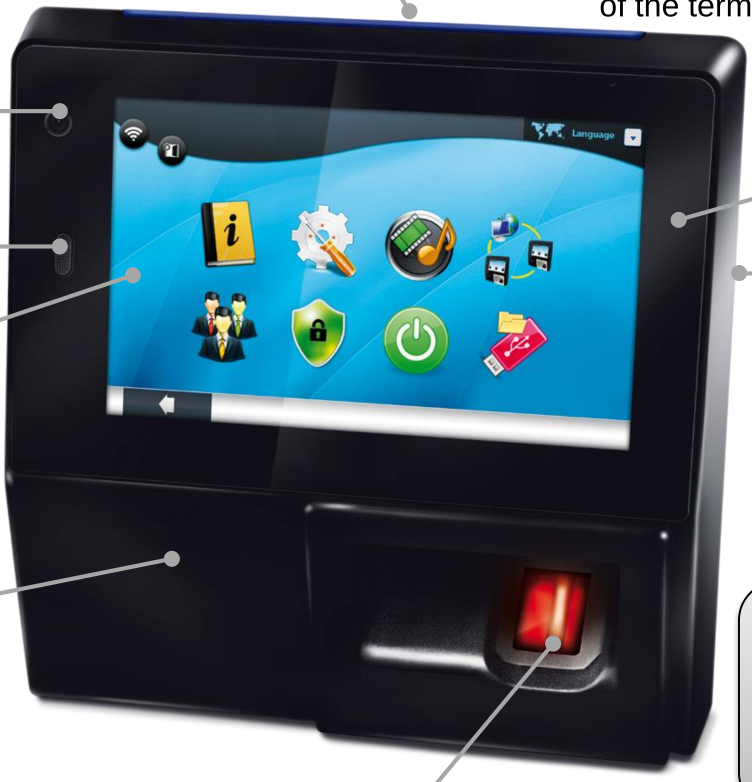
All descriptions illustrations, and specifications in this brochure should be considered approximate and may relate to optional equipment or feature

Table of Contents

Color	Step	Content
■	One	Overview
🟩	Two	Wiring
🟦	Three	Communications
🟥	Four	ACP or SDAC
🟩	Five	Administration
🟨	Six	Software
🟦	Seven	Capture basics

MorphoAccess® SIGMA Overview

The MorphoAccess® SIGMA terminal has a simple and ergonomic man-machine interface designed for access control and Time & Attendance, with fingerprint recognition, contactless card authentication and PIN authentication options.



Status LED

Optional Wi-Fi™ USB adaptor

(plugged at the back of the terminal)

VGA Camera

Microphone

Speaker

USB host port

USB port (for configuration and settings with a USB mass storage key)

5" WVGA touchscreen LCD

Optional Contactless Card reader. Specific logo on cover when available

- HID® iCLASS™ 13,56MHz (SIGMA … ICLASS)
- Or MIFARE™ DESFire ™ 13,56MHz (SIGMA .. MULTI)
- Or HID® Prox ® 125kHz (SIGMA .. PROX)

WR* product comes with a sensor protection cap (not displayed here)

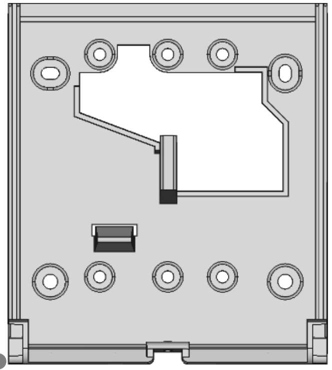
Optical biometrical sensor

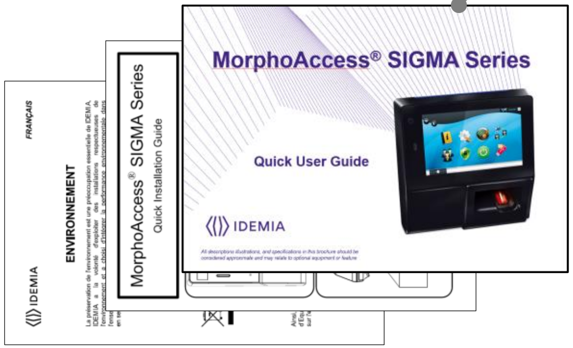
Step one : overview

MorphoAccess® SIGMA Checklist

Product packaging checklist:

QTY	ITEM
1	MorphoAccess® SIGMA terminal
1	Micro SD card installed in the terminal
1	Wall Mount Plate
1	POE module
1	Protection Accessory
1	Connection cable
1	Documentation package





Micro SD card must be installed in the terminal at start up (storage area for internal database and terminal logs)

Micro SD card replacement:

- ➔ Class 10 or higher, 1GB min, 32GB max
- ➔ Formatted by the terminal. Windows® PC may damage the content of the card and make it inoperative.
- ➔ Use only Brand Name cards. No name card may have lower performances or lower life time.

Electronic documentation is provided in Adobe® Acrobat® format (PDF). Adobe® Acrobat® Reader is available at http://www.adobe.com.

MorphoAccess® SIGMA Series

The MorphoAccess® SIGMA Series contains the following product variants:

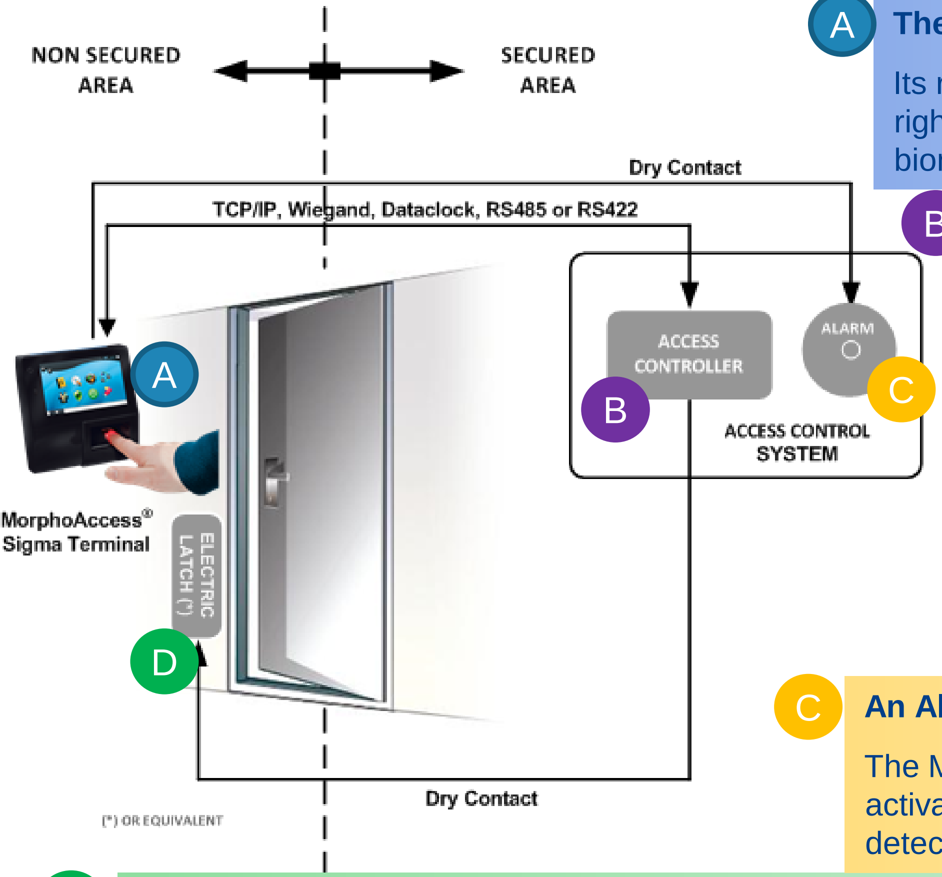
		Contactless Smart card reader			
Product designation	**Biometrics (Fingerprint)**	**iCLASS®**	**MIFARE® DESFire®**	**Prox®**	**Water Resistant (*)**
MorphoAccess® SIGMA	✓				✓
MorphoAccess® SIGMA iClass	✓	✓			✓
MorphoAccess® SIGMA Multi	✓		✓		✓
MorphoAccess® SIGMA Prox	✓			✓	✓

(*) For water resistance, units must be installed according to installation guidelines on *Quick Installation Guide*

Step one : overview

MorphoAccess® SIGMA terminal implementation

To secure an access, IDEMIA recommends installing the MorphoAccess® SIGMA Series terminal as a part of a typical Access Control system, this consists of the components described below.



A The MorphoAccess® SIGMA Series terminal

Its role is to process the access request from the user. It performs access right checks using one-to-many biometric identification or one-to-one biometric verification, and/or RF card authentication, and/or PIN check.

B An Access Controller (3rd party product)

The MorphoAccess® terminal interfaces with an Access Controller (using TCP/IP, Wiegand, Data Clock or RS485 protocol):

- ➔ After user's access rights checks, the MorphoAccess® terminal sends the result to the Access Controller (this message contains at least the User ID)
- ➔ The Access Controller performs additional checks, and returns the final decision (access granted/denied) to the MorphoAccess® terminal (which displays the result to the user), and to the door controller which opens the door (if the access has been granted).

C An Alarm (3rd party product)

The MorphoAccess® terminal sends a message to the Access Controller, to activate the Alarm as soon as a malicious activity such as tamper or pulling, is detected.

D A Door Electric Latch or equivalent such Deadbolt, Door Strike or Magnetic Lock (3rd party product)

The Access Controller sends a command to activate the latch if the access is granted (i.e. if the individual's User ID is listed in the Controller White List). Control of the latch is made through a dry contact..

MorphoAccess® SIGMA Access Control Modes

The terminal can be configured in one of the modes described in the table below

	Identification	Authentication	Multifactor	Proxy
Access control application	Application that runs on the terminal when it starts.	Application that runs on the terminal when it starts.	Application that runs on the terminal when it starts.	Remote application that controls the terminal through network commands
Access control triggering event	A user places a finger on the biometric sensor.	A user places a contactless card in front of the reader (1)	Both Identification and Authentication triggers are enabled.	Triggering events are selected by the remote application
Biometric check (if enabled)	The user's captured fingerprint template is matched against all fingerprint templates in the terminal database (3)	The user's captured fingerprint templated is matched against his reference fingerprint templates (2)	As per Identification or Authentication, depending on the triggering event	Selected by the remote application
Decision to display result signal to user	By Identification standalone application	By Authentication standalone application	By running standalone application	By remote application

(1) or the user enter their Identifier on the keypad, or a Wiegand frame is received from an external device
(2) stored on the contactless card or in the user record in the terminal's local database
(3) There is no fingerprint image stored in the terminal, but only points of interest (minutiae) of each fingerprint

Deployment Environments

Operating temperature	-20° to + 60 ° C (- 4° to 140° F)
Operating humidity	10 % < RH < 80 % (non condensing)
Storage temperature	- 25° to + 70 ° C (-13° to 158° F)
Storage humidity	5% < RH < 95 %
IP code	IP65 rated (once wall-mounted) For UL 294 compliance, the products are rated for indoor use

(*) For water resistance, units must be installed according to installation guidelines on *Quick Installation Guide*

General precautions

- Do not expose the terminal to extreme temperatures.
- When the environment is very dry, avoid synthetic carpeting near the MorphoAccess® SIGMA terminal, to reduce the risk of unwanted electrostatic discharge.

Areas containing combustibles

- Do not install the terminal in the vicinity of gas stations or any other installation containing flammable or combustible gases or materials. The terminal is not designed to be intrinsically safe.

The terminal should be installed in controlled lighting conditions

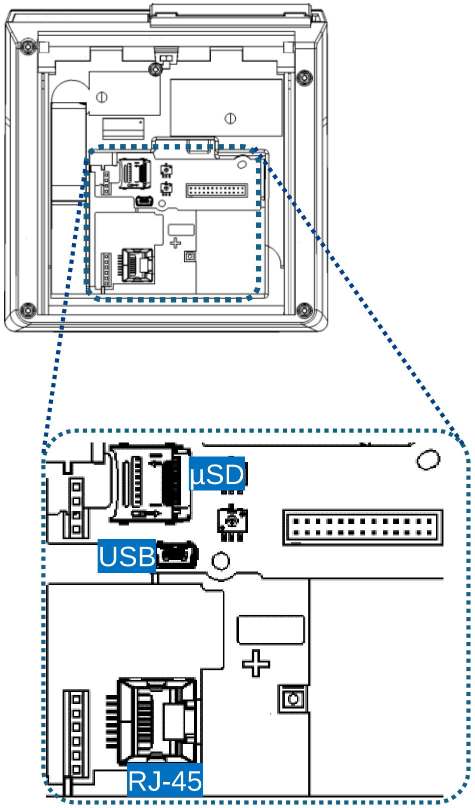
- Avoid biometric sensor exposure to a blinking light
- Avoid direct exposure of the biometric sensor to sunlight or to UV lights.

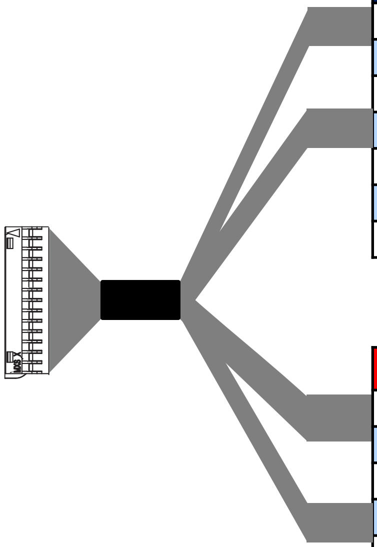
Outdoor installations recommendations

- Outdoor devices shall not encounter extreme weather such as torrential rains, harvest rains, flooding.
- High humidity, direct sun exposure, frequent high temperature, outdoor careless uses may alter the durability of the terminal.
- When the terminal is exposed to such potential extreme conditions, IDEMIA recommends deploying an enclosure to protect the terminal and thus ensure a long-lasting performance in the field.

Step one : overview

Wiring Overview





Wiegand IN & Wiegand OUT		
22	WIEGAND_IN0	Green / Red
23	WIEGAND_IN1	White / Red
20	WIEGAND_GND	Black / Red
24	WIEGAND_OUT0	Green
21	WIEGAND_OUT1	White
25	WIEGAND_LEDOUT1	Blue
26	WIEGAND_LEDOUT2	Blue / Red

RS422 / RS485		
17	RS422_RX+ (A)	Blue / Black
15	RS422_RX- (B)	Blue / White
16	RS422_TX+ / 485_TX/RX+ (Y)	Green / Black
18	RS422_TX- / 485_TX/RX- (Z)	Green / White
19	RS422/485_GND	Black / Red

Power supply, Tamper switch & Relay		
1	Power +12V	Red
2	Power GND	Black
3	SWITCH_PIN1	Light Blue
4	SWITCH_PIN2	Pink
5	RLY_NO	Yellow / White
6	RLY_COM	Grey / White
7	RLY_NC	Orange / White

GP IN & OUT		
8	GPIO_GND	Black / Red
9	GPI0	Orange
11	GPI1	Orange / Red
13	GPI2	Orange / Black
10	GPO0	Yellow
12	GPO1	Yellow / Red
14	GPO2	Yellow / Black

All connections of the terminal are of SELV (Safety Electrical Low Voltage) type.

Power supply from electrical source shall be switched off before starting the installation.

Before proceeding, make sure that the person in charge of installation and connections, is properly connected to earth, in order to prevent Electrostatic Discharges (ESD).

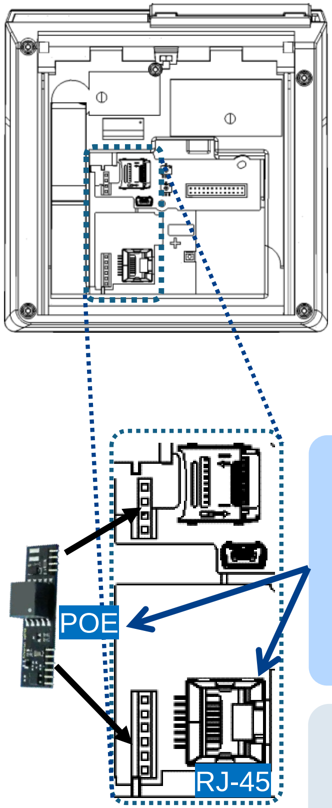
Backup of the Date/Time of the terminal: the volatile settings (such as date/time) of the terminal are protected against power failure, by a dedicated component during a least 24 hours (at 25^{o}C) without external power supply.

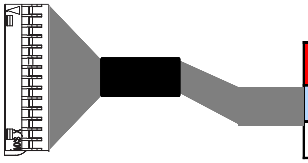
Step two : wiring

Power Wiring

External Power Supply: 12-24 Volts (regulated and filtered) 1 Amp min @12V, CEE/EEC EN60950 standard compliant. A12 Volts power supply compliant with SIA's Wiegand standard will also be suitable. If sharing power between devices, each unit must receive 1A (e.g. two units would require a 12VDC, 2A supply)

A battery backup or uninterrupted power supply (UPS) with built-in surge protection is recommended.





Power supply, Tamper switch & Relay		
1	Power +12V	Red
2	Power GND	Black

Power Over Ethernet (POE): power can be provided through RJ-45 connector using a PSE (Power Sourcing Equipment) IEEE 802.3af or IEEE802.3at type 1 compliant.

This feature requires a specific electronic card plugged at the rear of the product.

Warning: after use, the temperature of the POE module may be high: after power cut off, wait 5mn before working on connectors area.

IDEMIA recommends using a gauge AWG20 for 12V power supply.

The voltage measured on the product block connector of the terminal must be equal to 12V-24V (-15% / +10%).

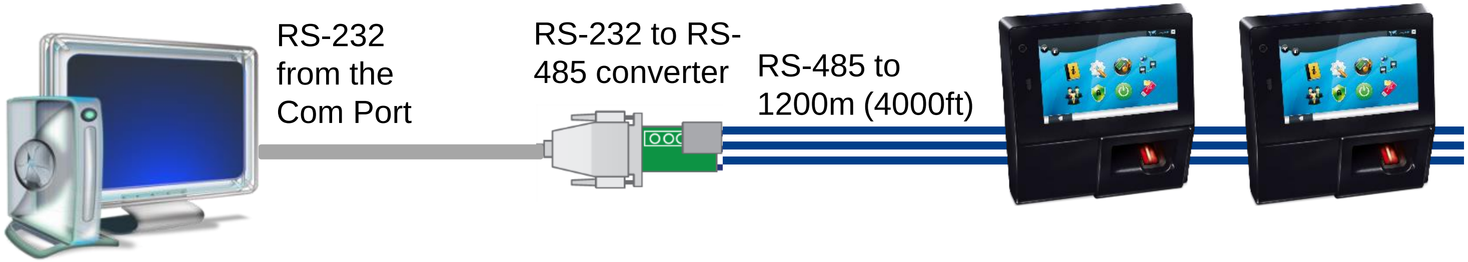
The table at the right, shows the maximum voltage drop between the power source and the terminal, depending on the length of the cable.

Gauge AWG	Diameter (mm)	Maximum voltage drop (V)		
		at 1m	at 5m	at 10m
20	0.81	0.03	0.17	0.33
22	0.64	0.05	0.26	0.53
24	0.51	0.08	0.42	0.84

WARNING: Under powering may cause memory and data corruption; over powering may cause hardware damage. Both of these situations will void the warranty

Step two : wiring

RS-485 Communication



RS-232 from the Com Port

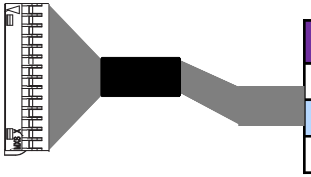
RS-232 to RS-485 converter

RS-485 to 1200m (4000ft)

For RS-485 installations, the cable should be run in a daisy-chain configuration (i.e. converter > position 1 > position 2 > position 3, etc.).

Choose one twisted pair of conductors to use for RS-485 TX/RX+(Y) (Green / Black wire) and RS-485 TX/RX-(Z) (Green / White wire).

Another conductor should be used for Signal Ground (Black / Red Wire) .



RS485		
16	RS422_TX+ / 485_TX/RX+ (Y)	Green / Black
18	RS422_TX- / 485_TX/RX- (Z)	Green / White
19	RS422/485_GND	Black / Red

Use CAT-5 UTP (or better) cable (shielded recommended) with a impedance of 120 Ω. AWG 24 should be the minimum wire gauge used.

Choose a RS-232 to RS-485 converter that supports Sense Data to switch from Send to Receive mode.

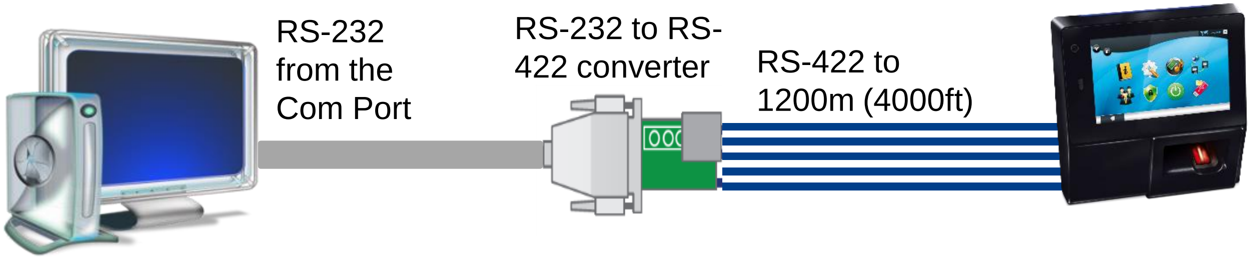
A maximum of 31 devices may be installed on the same line.

The maximum total cable length is 4000 ft. (1200m).

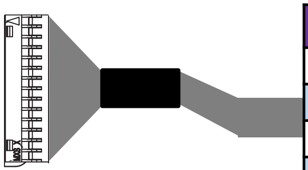
The cable must be dedicated to this installation and not used for any other purpose

Step three : communications

RS-422 Communication



For RS-422 installations, the cable should be run in a point to point configuration (i.e. PC > converter > terminal)



RS422		
17	RS422_RX+ (A)	Blue / Black
15	RS422_RX- (B)	Blue / White
16	RS422_TX+ / 485_TX/RX+ (Y)	Green / Black
18	RS422_TX- / 485_TX/RX- (Z)	Green / White
19	RS422/485_GND	Black / Red

Choose one twisted pair of conductors to use for RS-422 RX+(A) (Blue / Black wire) and RS-422 RX-(B) (Blue / White wire).

Choose one twisted pair of conductors to use for RS-422 TX+(Y) (Green / Black wire) and RS-422 TX-(Z) (Green / White wire).

Another conductor should be used for Signal Ground (Black / Red wire).

Use CAT-5 UTP (or better) cable (shielded recommended) with a impedance of 120 Ω. AWG 24 should be the minimum wire gauge used.

⚠

The maximum total cable length is 4000 ft. (1200m).

The cable must be dedicated to this installation and not used for any other purpose

Ethernet and Wireless LAN

RJ-45 Ethernet connection

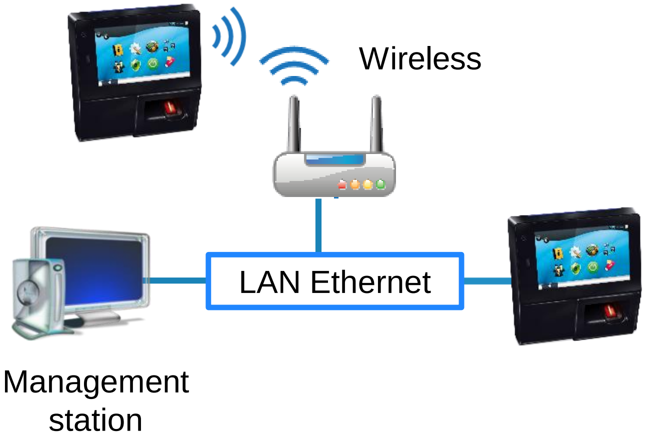
- Ethernet connection to the terminal is made through a standard RJ-45 connector on the back of the terminal.
- Use a category 5 shielding cable (120 Ohms) or better. It is strongly recommended to insert a repeater unit every 90m.
- By default, MorphoAccess® SIGMA Series terminal is configured in Static IP mode.

IP address Mode	Parameter	Factory value
Static	Terminal IP address	192.168.1.10
	Gateway IP address	192.168.1.254
	Sub network mask	255.255.254.0
	Host name	MAsigma

WLAN option

This option is available only with Wi-Fi™ dongle (and adaptation cable) delivered by IDEMIA (kit reference 293658530), and requires the terminal be powered by an external AC/DC 12V to 24V power supply (the POE feature doesn’t provide enough power for the terminal and the dongle).

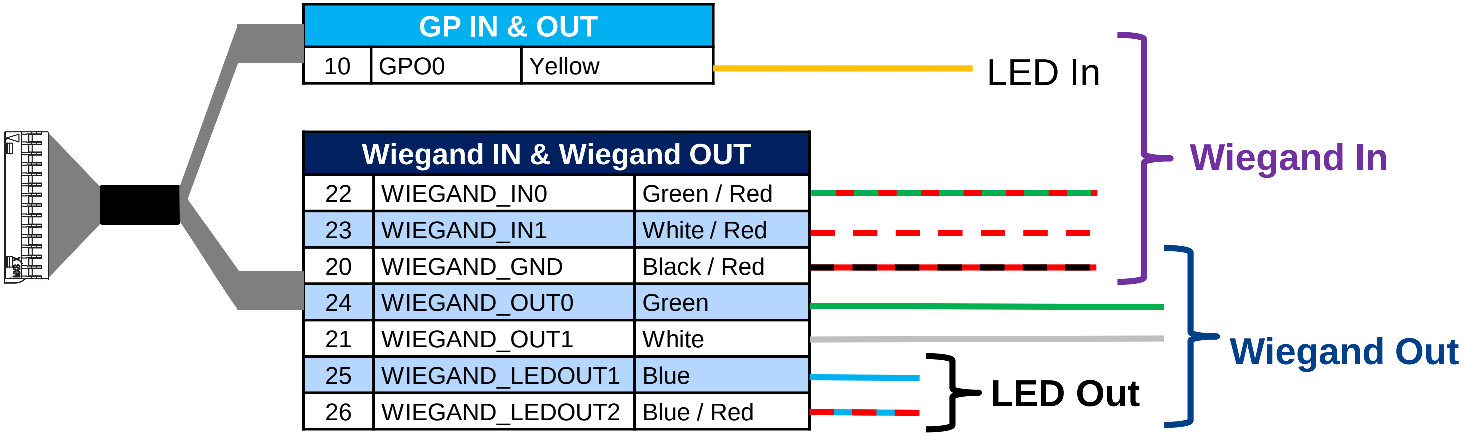
Morpho Wi-Fi™ dongle supports 802.11b and 802.11g standards, WEP Open, WPA and WPA2.



The Wi-Fi™ dongle shall not be exposed to temperatures exceeding 50° C (thermal dissipation).
The Wi-Fi™ dongle shall be installed outside the product (separate area shall be reserved in the wall).

Step three : communications

Wiegand Communication



GP IN & OUT		
10	GPO0	Yellow

Wiegand IN & Wiegand OUT		
22	WIEGAND_IN0	Green / Red
23	WIEGAND_IN1	White / Red
20	WIEGAND_GND	Black / Red
24	WIEGAND_OUT0	Green
21	WIEGAND_OUT1	White
25	WIEGAND_LEDOUT1	Blue
26	WIEGAND_LEDOUT2	Blue / Red

Three-conductor wire (shielded recommended) is required for Data 0, Data 1, and WGND.

Use 18-22 AWG cable in a homerun configuration from each unit to the Access Control Panel (ACP).

- Connect WIEGAND_OUT0 (Green Wire) to ACP Data 0,
- Connect WIEGAND_OUT1 (White Wire) to ACP Data 1,
- Connect WIEGAND_GND (Black / Red Wire) to ACP reader common (0vDC).

For 18 AWG, the maximum cable distance is 500 ft. (150m); for 20 AWG, the maximum is 300 ft. (90m); for 22 AWG, the maximum is 200 ft. (60m).

Electrical interface conforms to the Security Industry Association's Wiegand standard March 1995, and it is 5V TTL compatible.

Wiegand Communication (continued)

Important

By default, the Wiegand output format is not enabled. Wiegand output must be configured before connecting to the ACP.

Note

On installation, the system administrator will be prompted to select either a pre-existing Wiegand frame format or create a custom

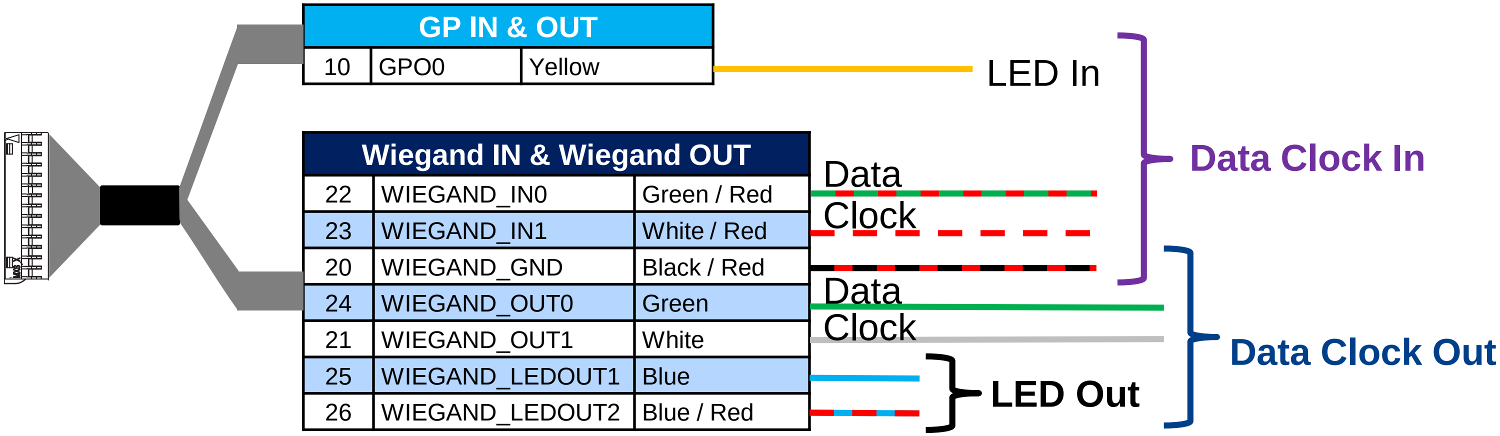
Data Clock

The Wiegand port also supports the Clock & Data protocol. The wiring is described below.

Example Format Information

Type: **Standard 26-bit**

- Alt Site Code and Fail Site Code Range: **0-255**
- Template ID Number Range: **1-65535**
- Extended ID Number Range: **N/A**
- ID Start Bit: 9
- Length of ID: 16
- Site Code Start bit: 1
- Length of Site Code: 8
- Start Bit length : 0



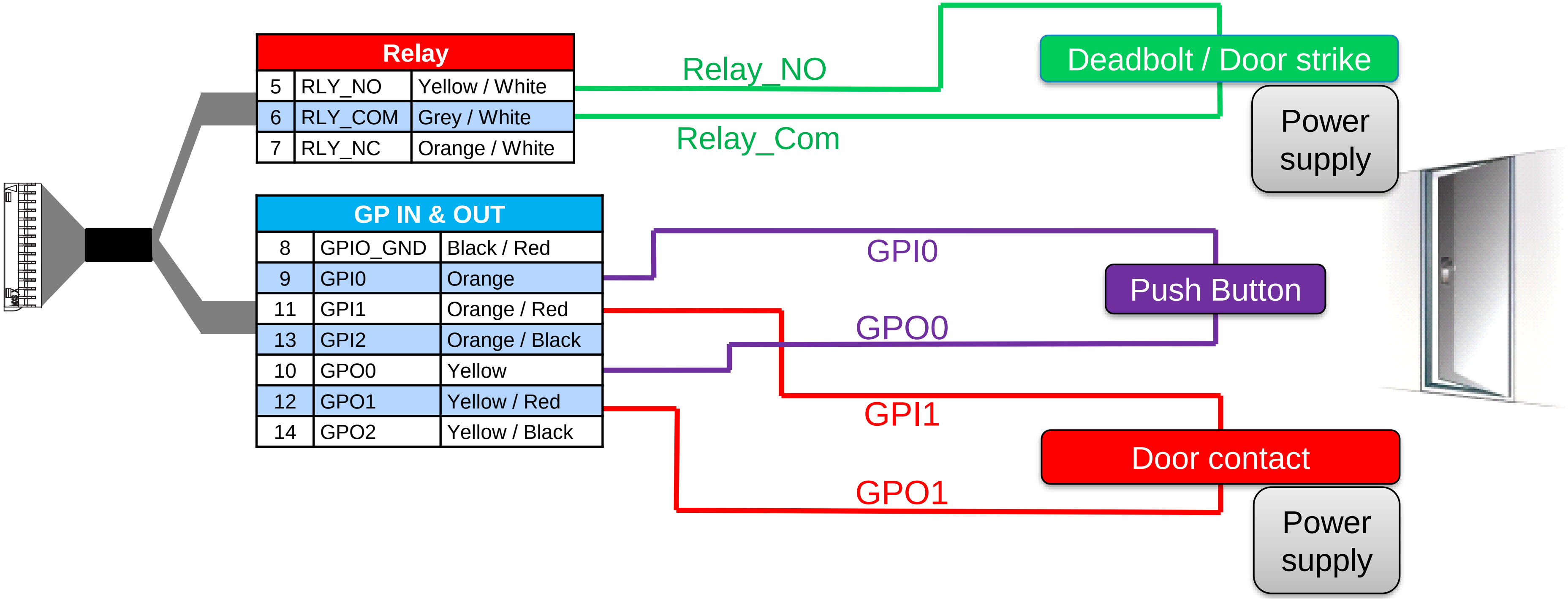
GP IN & OUT		
10	GPO0	Yellow

Wiegand IN & Wiegand OUT		
22	WIEGAND_IN0	Green / Red
23	WIEGAND_IN1	White / Red
20	WIEGAND_GND	Black / Red
24	WIEGAND_OUT0	Green
21	WIEGAND_OUT1	White
25	WIEGAND_LEDOUT1	Blue
26	WIEGAND_LEDOUT2	Blue / Red

Step three : communications

Single Door Access Control (SDAC)

Single Door Access Control (SDAC) wiring sample : with Push Button



Relay		
5	RLY_NO	Yellow / White
6	RLY_COM	Grey / White
7	RLY_NC	Orange / White

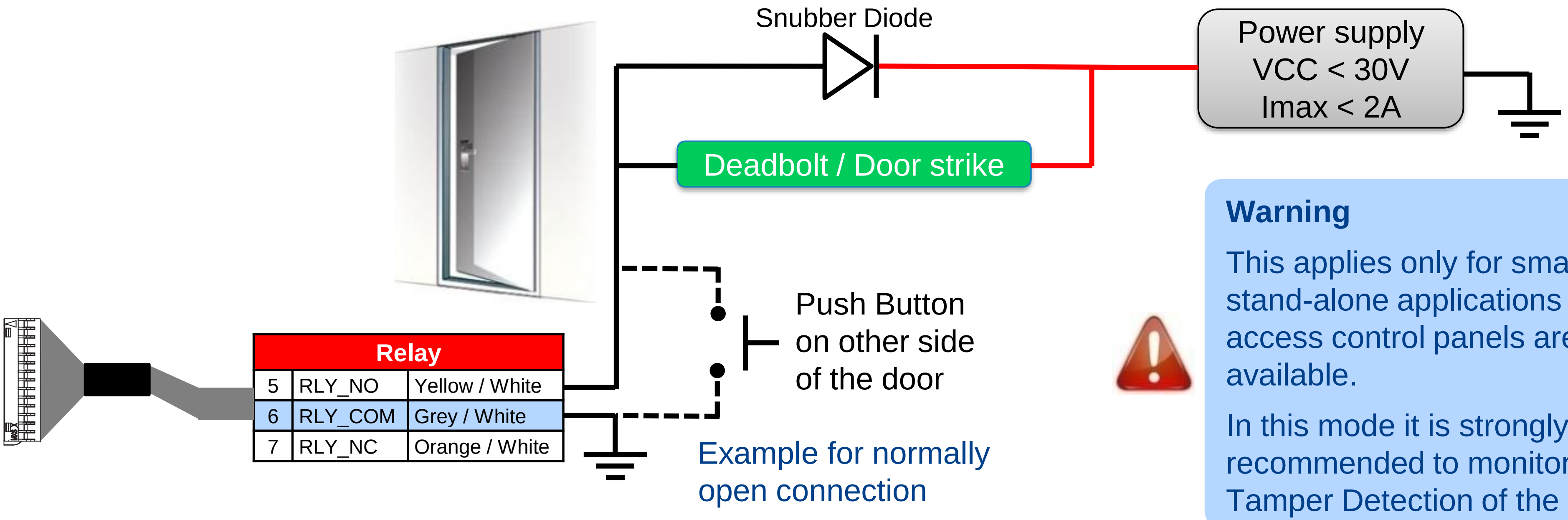
GP IN & OUT		
8	GPIO_GND	Black / Red
9	GPI0	Orange
11	GPI1	Orange / Red
13	GPI2	Orange / Black
10	GPO0	Yellow
12	GPO1	Yellow / Red
14	GPO2	Yellow / Black

Warning

- **Please check next page for important information about internal relay rating**
- **If door contact is not used, GPI1 (Orange / Red wire) and GPO1 (Yellow / Red wire) shall be connected together**
- **Power supply from electrical source shall be switched off before starting the installation.**

Step four: ACP or SDAC

Internal Relay Wiring (Normally open)



Relay		
5	RLY_NO	Yellow / White
6	RLY_COM	Grey / White
7	RLY_NC	Orange / White

Example for normally open connection

Warning

This applies only for small or stand-alone applications where access control panels are not available.

In this mode it is strongly recommended to monitor the Tamper Detection of the device

Relay mode can be changed to “normally close” instead of “normally closed” (default)

Inductive load management requires a parallel diode for a better contact lifetime.

Warning

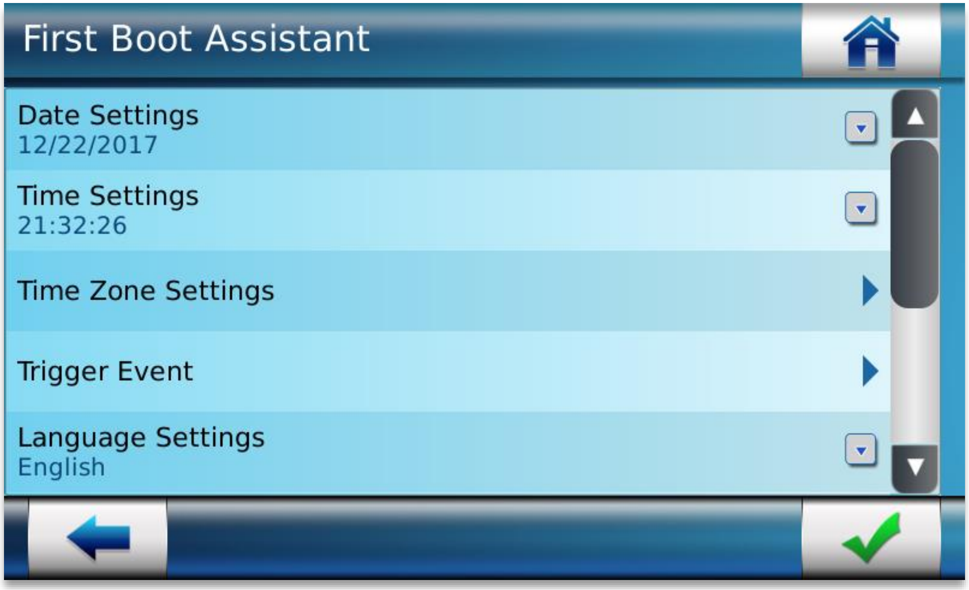
- **The internal relay is limited to a maximum current of 2A @ 30V. If the deadbolt / door strike draws more than 2A, damage to the device may occur. If the deadbolt / door strike load exceeds 2A, an external relay must be used.**
- **The internal relay is designed for 100.000 cycles. If more cycles are needed, an external relay driven by GPO must be used.**

Step four: ACP or SDAC

Local Administration - First Boot Assistant

The First Boot Assistant (FBA) helps the administrator to configure all the devices fundamental settings.

It is automatically launched at first terminal startup, but can also be launched on demand, though administration menu (i.e. to reinitialize terminal main settings)



First Boot Assistant

Date Settings
12/22/2017

Time Settings
21:32:26

Time Zone Settings

Trigger Event

Language Settings
English

Main settings managed by FBA

Date & Time & Time Zone Settings

Trigger Event: select event(s) to be processed as an access request by a user

Language Settings: user interface language selection,

Network Settings: LAN or WLAN parameters

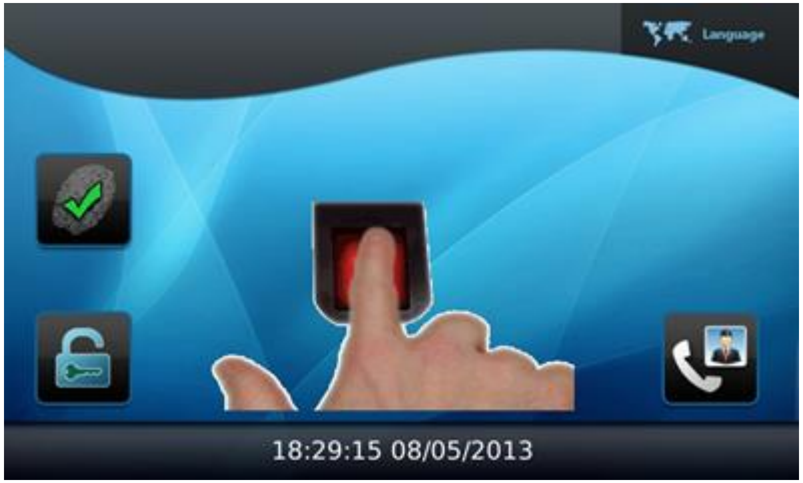
Password Settings: terminal administration password modification

Boot assistant at next boot: Display this screen on next boot.

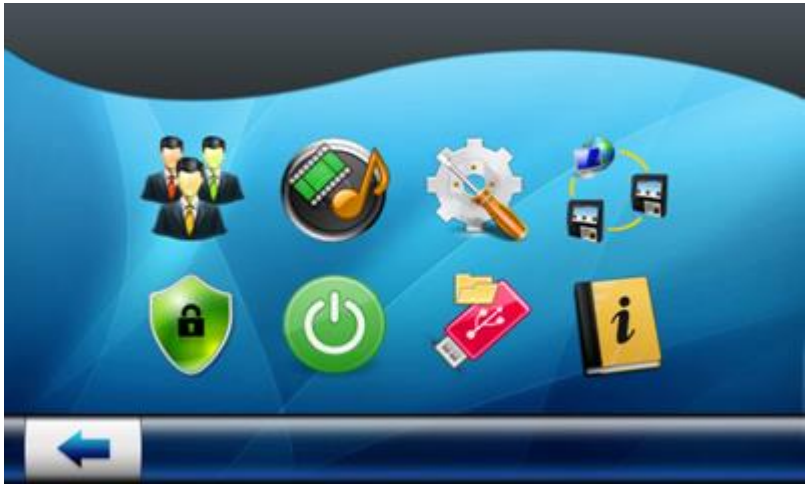
Protocol Settings: select communication protocol : Bioscrypt 4G terminals, MA 500 and J Series (MA2G), or MorphoAccess SIGMA (MA5G)

Step five: administration

Local Administration – Using Touch Screen Menu



🔓 + password (default: 12345)



Frequently used icons

- ⌂ Exit and Go Home
- ✓ Validation or confirmation
- ← Back (and Cancel)
- ✗ Cancel or refuse

⚠ **For security reasons, it is highly recommended to change the devices default password to a custom password.**

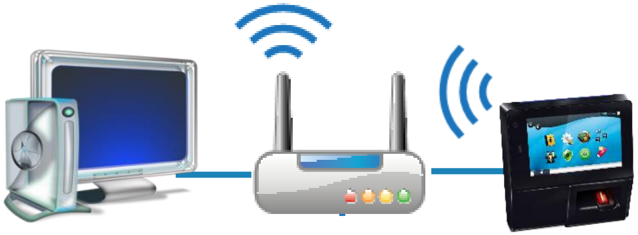
- User management
- Multimedia management
- Terminal settings
- Communication settings
- Security
- Restart Start/Stop
- USB key management
- Information about terminal

Step five: administration

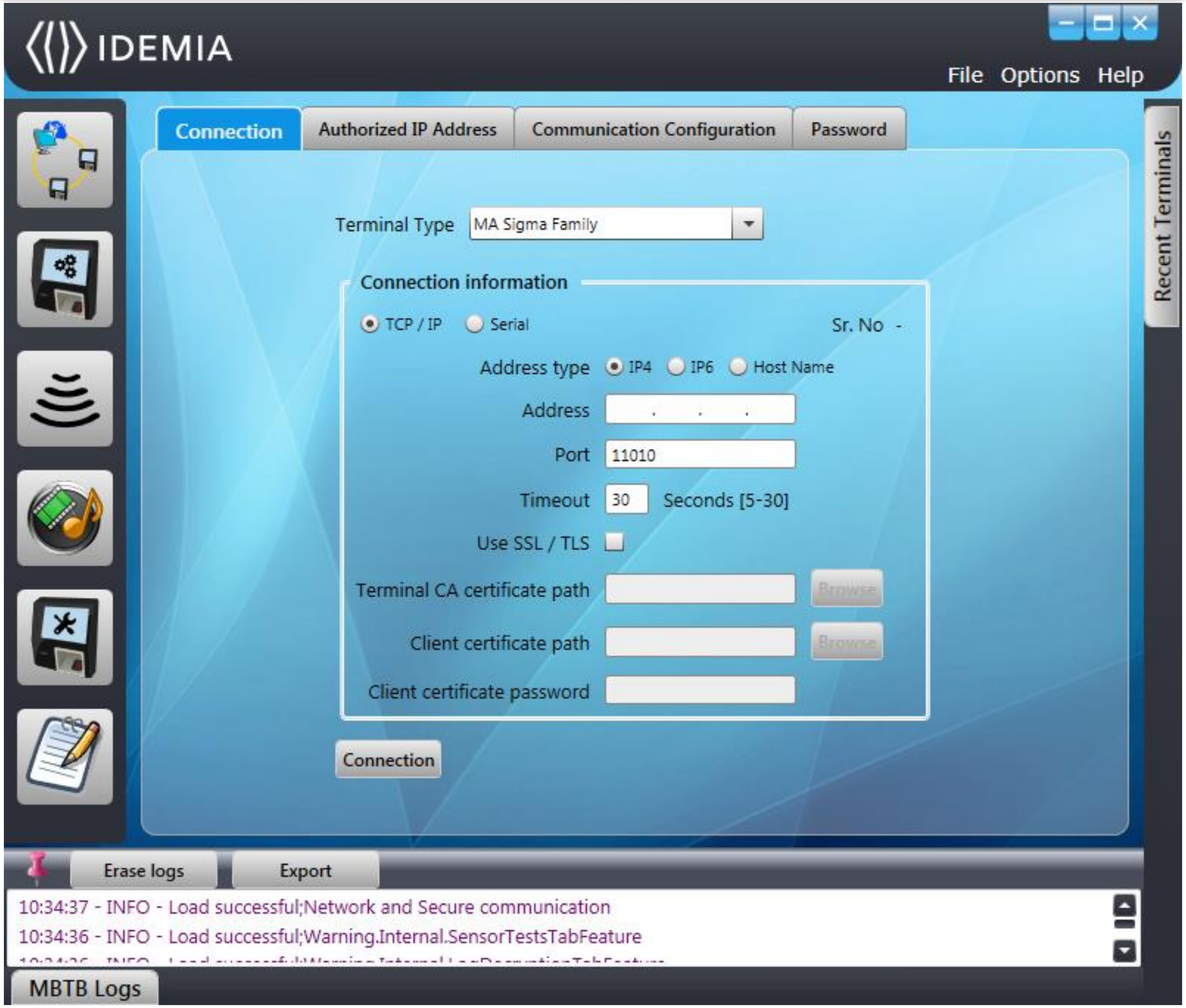
Administration with MorphoBioToolBox application

The MorphoAccess® SIGMA Series terminal can be configured using a dedicated (Windows) application : **MorphoBioToolBox** Please note that this application has an embedded User Guide (Help menu).

North and South America :
E-mail support.bioterminals@idemia.com with your name, phone number, serial number of your MASIGMA and “**Please Send Link for MBTB**” in the subject of your e-mail. A link to download the software will be e-mailed to you.
Other countries : please contact your sales representative.



Terminal administration with MorphoBioToolBox (MBTB) application



Terminal Type: MA Sigma Family

Connection information

● TCP / IP ○ Serial Sr. No -

Address type ● IP4 ○ IP6 ○ Host Name

Address: . . .

Port: 11010

Timeout: 30 Seconds [5-30]

Use SSL / TLS □

Terminal CA certificate path: Browse

Client certificate path: Browse

Client certificate password:

Connection

```
10:34:37 - INFO - Load successful;Network and Secure communication
10:34:36 - INFO - Load successful;Warning.Internal.SensorTestsTabFeature
10:34:36 - INFO - Load successful;Warning.Internal.LogDecryptionTabFeature
```

Step five: administration

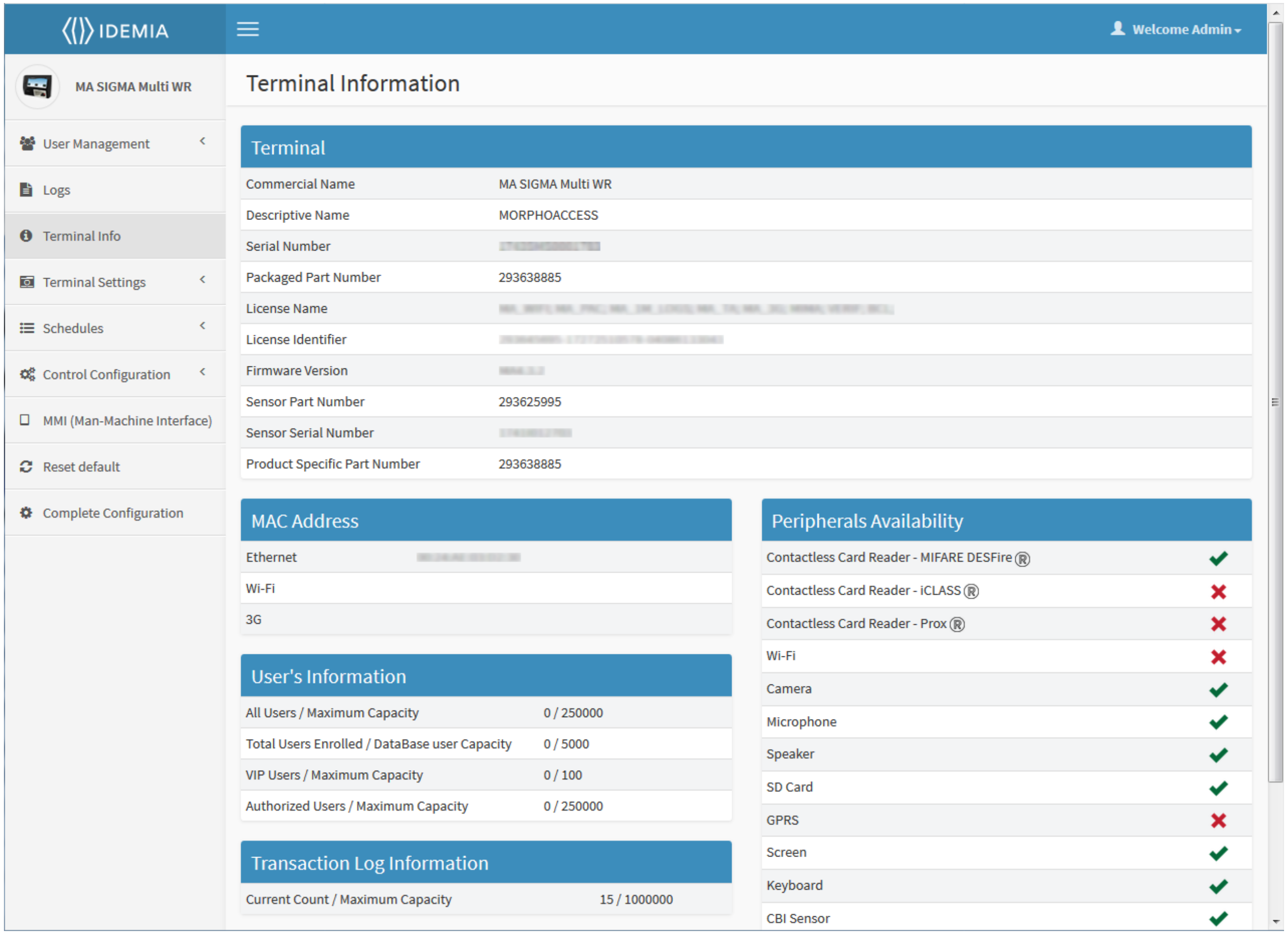
Administration with Embedded Web Server

The terminals embedded Web server enables easy configuration of the devices using a web browser on a Desktop PC, Laptop, Tablet or smart phone.

The connection to the embedded Webserver, through LAN or WLAN, requires the terminals IP address (available with local administration) and terminals password (same as local administration password specified in previous page).

By default, webserver is disabled, then if necessary it must be enabled using local administration before use.

Terminal administration with a standard web browser



Terminal Information

Terminal

Commercial Name	MA SIGMA Multi WR
Descriptive Name	MORPHOACCESS
Serial Number	[redacted]
Packaged Part Number	293638885
License Name	[redacted]
License Identifier	[redacted]
Firmware Version	[redacted]
Sensor Part Number	293625995
Sensor Serial Number	[redacted]
Product Specific Part Number	293638885

MAC Address

Ethernet	[redacted]
Wi-Fi	
3G	

User's Information

All Users / Maximum Capacity	0 / 250000
Total Users Enrolled / DataBase user Capacity	0 / 5000
VIP Users / Maximum Capacity	0 / 100
Authorized Users / Maximum Capacity	0 / 250000

Transaction Log Information

Current Count / Maximum Capacity	15 / 1000000

Peripherals Availability

Contactless Card Reader - MIFARE DESFire®	✓
Contactless Card Reader - iCLASS®	✗
Contactless Card Reader - Prox®	✗
Wi-Fi	✗
Camera	✓
Microphone	✓
Speaker	✓
SD Card	✓
GPRS	✗
Screen	✓
Keyboard	✓
CBI Sensor	✓

Step five: administration

Software for Terminal Remote Administration

➔ MorphoAccess® SIGMA Series terminals are fully compatible with:

- MorphoManager application (version 13.1.5 or later)

➔ When Legacy Morpho mode enabled, the terminal is compatible with:

- MEMS (version 7.3.1 or later),
- The limitations in Morpho Legacy mode are described in the following document:
  - Application Note - Morpho Legacy Mode Limitations

➔ When Legacy L1 mode is enabled, the terminal is compatible with:

- SecureAdmin (version v4.1.19.0.0.a10.0 or later),
- The limitations in L1 Legacy mode are described in the following document:
  - Application Note - L1 Legacy Mode Limitations

Step six : software

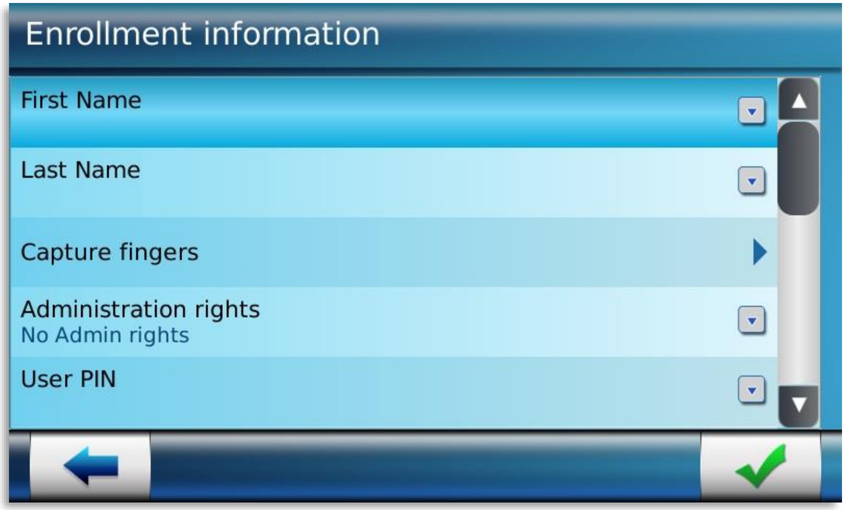
Local Enrolment Process on MorphoAccess® SIGMA

A new user can easily be added by using the administration menu of the MorphoAccess® SIGMA terminal.
This “local enrolment” is recommended only for small or stand alone installations or testing purposes. For professional systems enrollment should be performed remotely with an enrolment station, which is a PC with a dedicated application such as MorphoManager.

This menu allows a user’s record to be added in the local database, with the option of creating a user RF card, with the user’s reference data.

Enrolment gathering user’s data listed below (depending on features enabled in the terminal) :

- User’s first name and last name
- User’s fingerprints (for biometric check)
- User’s administration rights (none, settings, database)
- User’s PIN (for PIN check)
- User’s duress fingerprint
- User’s access schedule and holiday schedule
- User’s dynamic message setting
- User’s record expiry date
- User to include in white list or in VIP list
- User specific access rules definition



Enrollment information

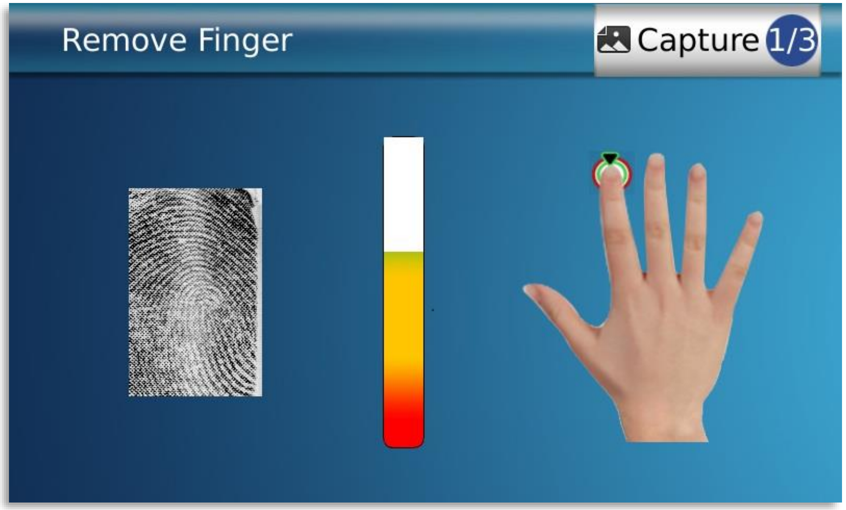
First Name

Last Name

Capture fingers

Administration rights
No Admin rights

User PIN

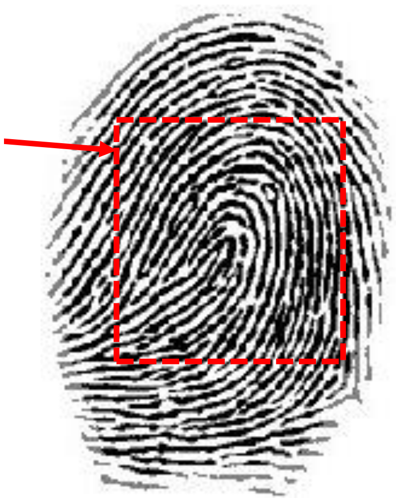
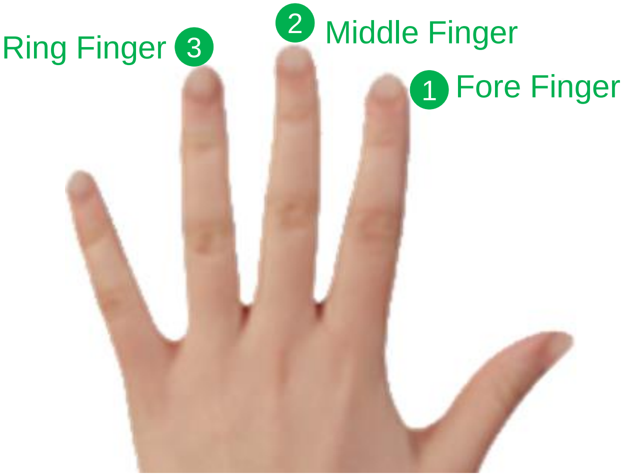


Remove Finger

Capture 1/3

Step seven: capture basics

Fingerprint Capture Basics 1/3

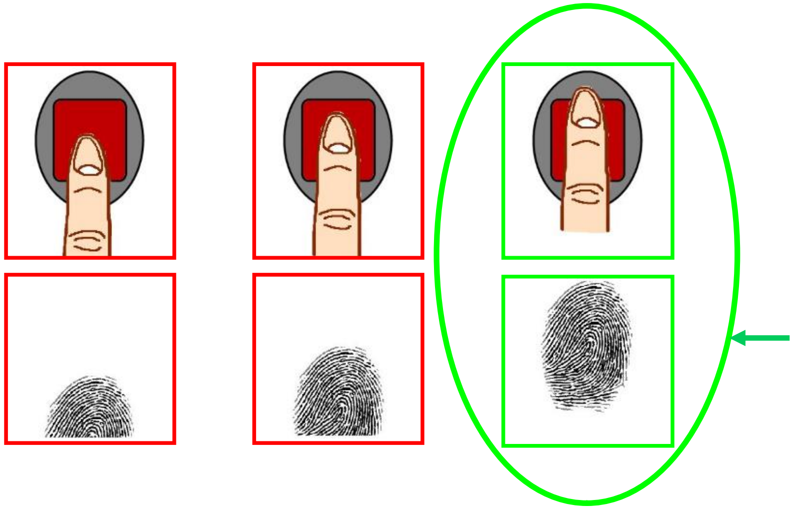
Region of Interest	Recommended Fingers	Acquisition troubleshooting
 The biometric sensor is designed to capture the most useful area of the fingerprint, which is usually at the centre of the finger tip, as shown on the figure above.	 The sensor can capture any finger, but we recommend to : • use Fore finger / Index as 1st choice • use middle finger as 2nd choice • use ring finger as alternative 2nd choice (3rd choice) • avoid little finger (poor fingerprint) • avoid thumb (best accuracy but ergonomically more difficult to use)	**Finger to capture** ➢ the fingerprint area must be free of any occlusion (if not, select another finger to capture, such as the 2nd enrolled finger in case of authentication or identification) ➢ do not press or tense finger to avoid blood vessels constriction. **Fingerprint image too dark :** the finger is probably too moist and/or too dusty ➢ ***too moist** : dry the finger* ➢ ***too dusty**: clean up the finger* **Fingerprint image too light :** the finger is probably too cold and/or too dry ➢ ***too cold** : warm up the finger* ➢ ***too dry** : moisten the finger (i.e. with moistening pad) and /or warm it up.*

For handling large scale enrollments please contact your IDEMIA representative for training and services options

Fingerprint Capture Basics 2/3

Ideal Finger Position

Finger Height



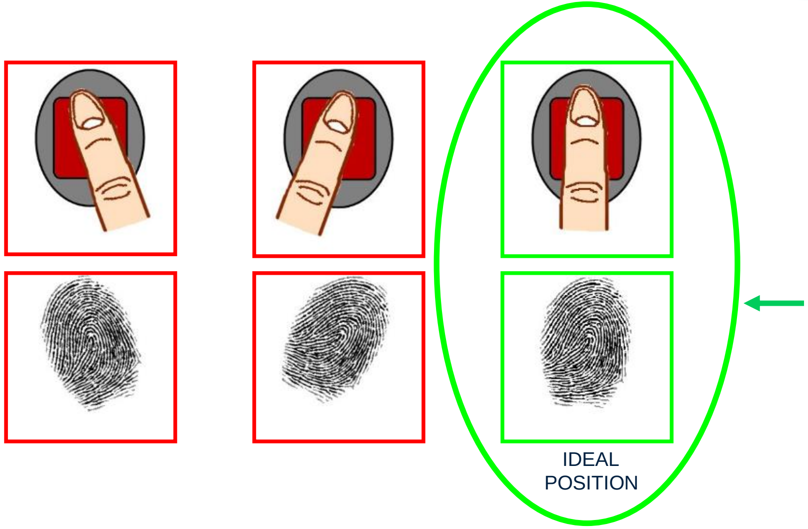
Incorrect Position: ⚠

- Do not place the finger tip :
  - on the bottom of the sensor,
  - or in the middle of the sensor

Correct Position:

- Align centre of finger tip with sensor centre

Finger Angle



Incorrect Position: ⚠

- Do not tilt the finger to the right or left side of the sensor

Correct Position:

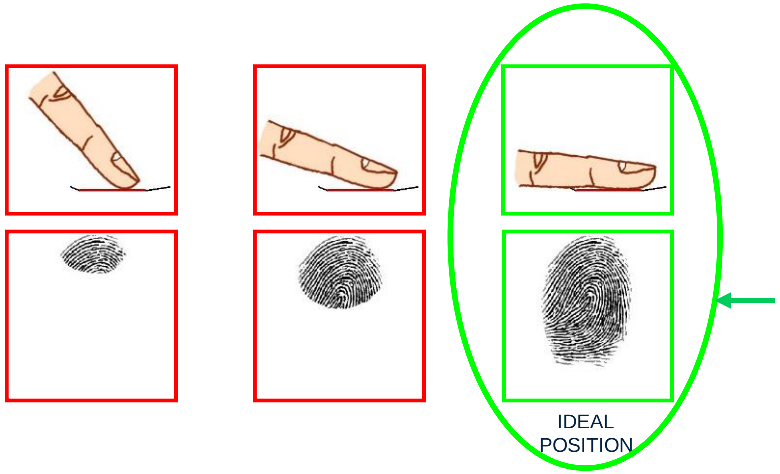
- The finger must be parallel to sensor sides

Step seven: capture basics

Fingerprint Capture Basics 3/3

Ideal Finger Position

Finger Inclination



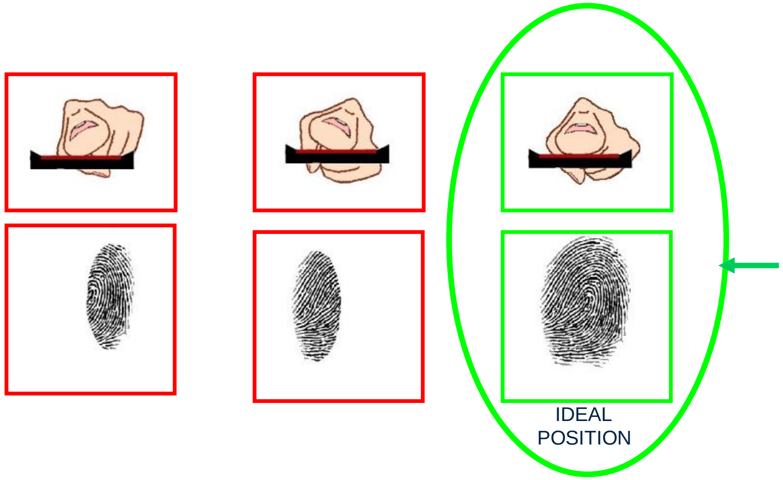
Incorrect Position: ⚠

- Do not leave the finger in the air
- Do not bend finger upward or downward

Correct Position:

- Finger is parallel to sensor surface

Finger rotation



Incorrect Position: ⚠

- Do not roll finger

Correct Position:

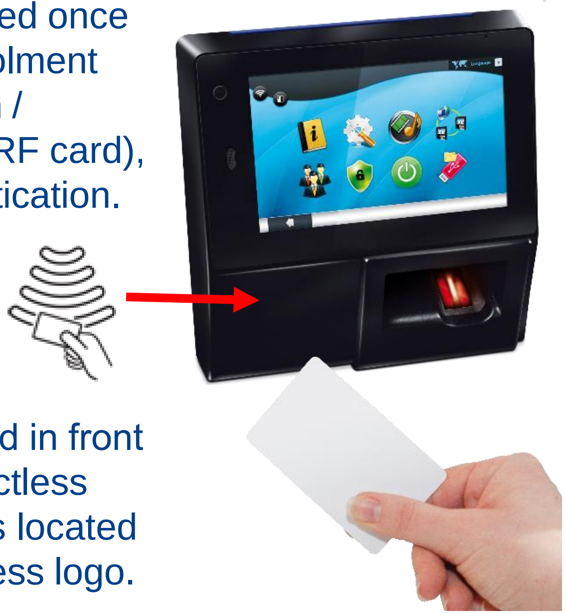
- Finger is parallel to surface sensor

Step seven: capture basics

Contactless Card Position – PIN input

Contactless Card Position

This action is required once during the user enrolment process (generation / encoding of a user RF card), and at each authentication.

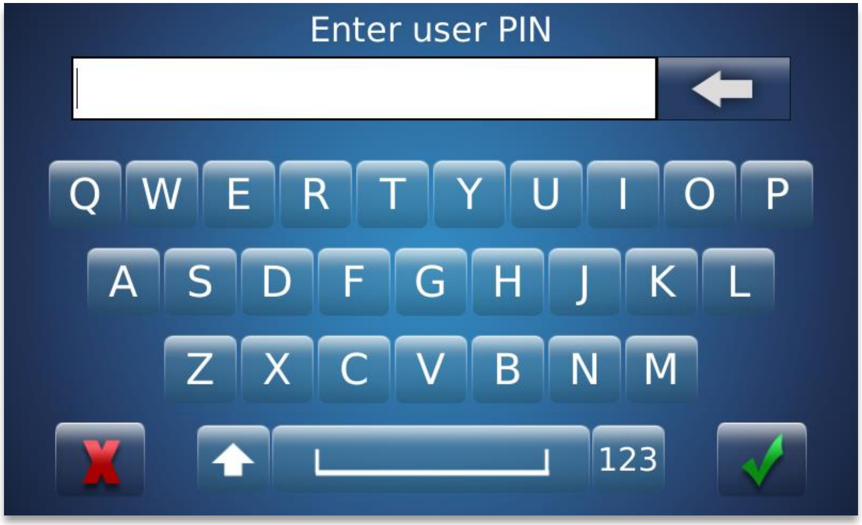


Place user’s RF card in front of embedded contactless card reader which is located behind the contactless logo.

The authentication process is initiated by the detection of a user card by the (optional) contactless card reader.

The terminal reads the user data stored in the card (at least the User ID), and starts the authentication process, as defined by the terminal settings

Input PIN


Enter user PIN

When defined by terminal settings, the user is required to enter his PIN code, once during enrolment process, and at each authentication (in addition or instead of biometric check).

The PIN code is entered using an alphanumeric or a numeric keypad displayed on the LCD touch screen depending on the configuration.

Step seven: capture basics

Recommendations

The manufacturer cannot be held responsible in case of non-compliance with the following recommendations or incorrect use of the terminal.

Repair and Accessories

- Do not attempt to repair the MorphoAccess® SIGMA Series terminal yourself. The manufacturer cannot be held responsible for any damage/accident that may result from attempts to repair components. Any work carried out by non-authorized personnel will void your warranty.
- Only use the terminal with its original accessories. Attempts to use unapproved accessories with your terminal will void your warranty.

Standalone terminals (not connected to a network)

- For terminals used in standalone mode, it is strongly recommended to regularly backup the local database, and at least after significant changes in the database (add, remove or modification of user’s records), on a external support such a mass storage key

Micro SD Card

- The micro SD card is linked to the terminal : it shall not be transferred from one product to another.

Date / Time synchronization

- The MorphoAccess® SIGMA Series terminal clock has a +/- 10 ppm typical time deviation at +25ºC (roughly +/- 3sec per day). At lower and higher temperature, deviation may be greater (maximum : 8sec per day).
- When the terminal is used for applications requiring high time precision, it is strongly recommended to synchronize the terminal with an external clock.

Cleaning & Disinfection precautions

- **To clean the terminal**, a dry cloth is recommended, especially the biometric sensor.
- **To disinfect the terminal**, moisten a non-abrasive wipe with the disinfectant Windex® Multi-Surface (or similar product containing L-Lactic acid) or hydrogen peroxide (<3%) and wipe the device’s surface and leave the surface wet with disinfectant for at least 5 minutes. Any other practices (bleach, chlorine, soda, alcohol, quaternary ammonium etc) permanently damage and/or negatively impact the performances of the device.

Firmware release

- To get the best of our technology, we recommend you to download and install the last firmware release (please refer to last page)

Documentation

Documents about installing the terminal

Quick Installation Guide
This document describes the main step for wall mounting.

Installation Guide
This document describes the terminals physical mounting procedure, electrical interfaces and connection procedures.

Recommendations for Secure Installation
This document describes all actions to secure your installation (physical installation, network, secure protocols etc.).

Documents about administrating / using the terminal

Quick User Guide
This document is the main guide that is used for learning the main steps for initializing the terminal operations.

Administration Guide
This document describes the different functions available on the terminal and the procedures for configuring the terminal.

Parameters Guide
This document contains the full description of all the terminal configuration parameters.

Documents for the developer

Contactless Card Specification
This document describes the contactless cards supported by the terminal and the format of the data on the contactless card.

Host System and Remote Message Interfaces
This document describes the commands, the protocols, and the format of the data supported by the terminal.

Distant Commands Guide
This document describes thrift commands supported by the terminal.

Release notes : for each firmware version, a release note is published describing the new features, the supported products, the potential known issues, the upgrade / downgrade limitations, the recommendations, the potential restrictions…

Notes

Notes

Contacts

Technical Support and Hotline

North America
Mail: support.bioterminals.us@idemia.com
Tel: +1 888 940 7477

South America
Mail: support.bioterminals.us@idemia.com
Tel: +1 714 575 2973

Asia, Pacific:
Mail: support.bioterminals.in@idemia.com
Tel: +91 1800 120 203 020

Europe, Middle-East, Africa:
Mail: support.bioterminals@idemia.com
Tel: +33 1 30 20 30 40

293732943-F

For the latest firmware, software, document releases, and news, please check our website: www.biometric-terminals.com (To get your login and password please contact your sales representative).

www.idemia.com