Sagem Défense Sécurité
SAFRAN Group

MorphoAccess™ 100 Series

User Guide

Produced by SAGEM Défense Sécurité

www.sagem.com

Table of content

INTRODUCTION

Congratulations for choosing the SAGEM MorphoAccess™ 1XX Automatic Fingerprint Recognition Terminal.

MorphoAccess™ 1XX series provides an innovative and effective solution for access control applications using Fingerprint Verification or/ and Identification.

Among a range of alternative biometric techniques, the use of finger imaging has significant advantages: each finger constitutes an unalterable physical signature which develops before birth and is preserved until death. Unlike DNA, a finger image is unique to each individual - even identical twins.

The MorphoAccess™ terminal integrates SAGEM image processing and feature matching algorithms. This technology is based on lessons learned during 20 years of experience in the field of biometric identification and the creation of literally millions of individual fingerprint identification records.

We believe you will find the SAGEM MorphoAccess™ fast, accurate, easy to use and suitable for physical access control or time and attendance.

To ensure the most effective use of your SAGEM MorphoAccess™, we recommend that you read this User Guide totally.

INTERFACES PRESENTATION

Man-machine interface

The MorphoAccess™ 1XX offers a simple and ergonomic man-machine interface dedicated to access control based on fingerprint recognition:

- A high quality optical scanner to capture fingerprints (1).
- A multicolor led (8 colors) (2).
- A multi-toned buzzer (3).
- A Mifare™ contactless reader on MA12X, to read reference templates from a contactless card (4).

Electrical interfaces

The terminal offers multiple interfaces dedicated to administration and control information:

- A multiplexed Wiegand / Dataclock / RS485 output (5).
- Two LED IN inputs to improve integration in an access control system (6).
- A relay to directly command an access (7).
- A tamper switch (8).
- An Ethernet interface (LAN 10/100 Mbps), allowing remote management through TCP and sending control result through UDP (9).
- A USB Host port dedicated to local configuration (10).

The *MA1XX Installation Guide* describes precisely each interface and connection procedure.

SETTING UP THE TERMINAL IP ADDRESS

The MorphoAccess™ can run in stand alone mode but a TCP/IP connection is required to download records in the terminal and to configure its recognition mode.

It is possible to specify standard TCP parameters: terminal network address, network gateway and mask.

These parameters can be set using a USB *mass storage* key.

The complete procedure is described in section Configuring a “standalone” MA1XX.

Once connected on the network, the MorphoAccess™ can be configured using (for example) the.*Configuration Tool.*

Identification - authentication

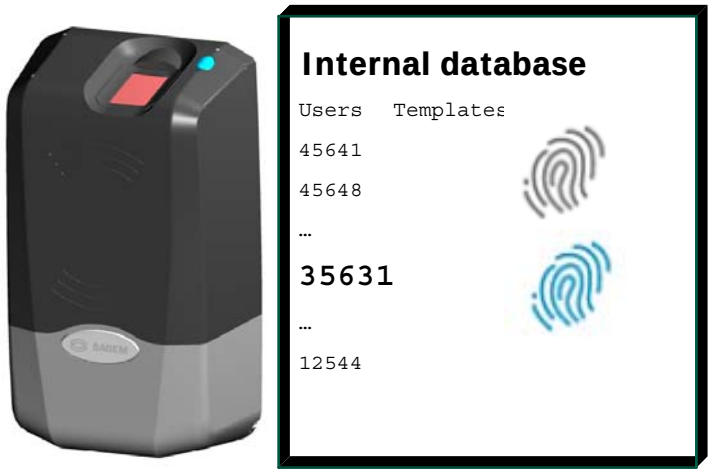
The MorphoAccess™ works according two biometric recognition modes: identification or authentication. Both identification and authentication can be activated (fusion mode).

Identification

The captured fingerprint is matched against a database – 1 vs. N.

Minutiae are stored in terminal local database. The terminal can store 500 users (2 fingers per user) in its local database.

In this mode the sensor will be always switched on, waiting for a finger. The captured fingerprint is matched against the whole database.



If the user is matched access is granted.

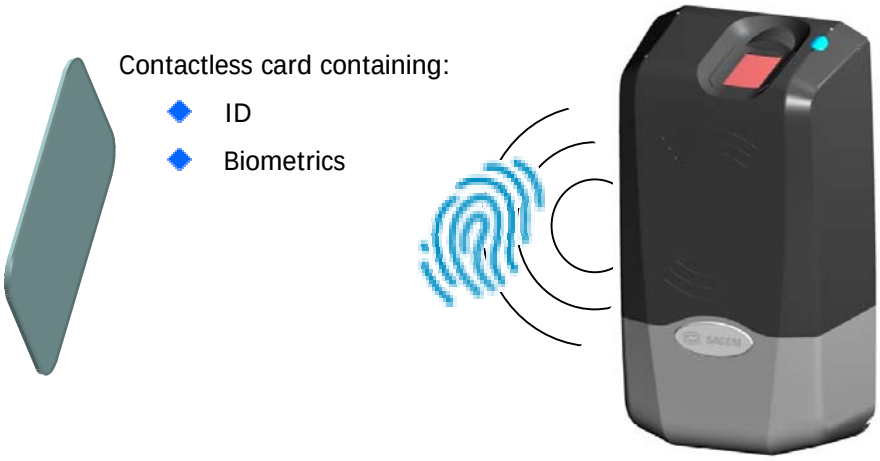
If the user is not recognized access is refused.

See section Access Control By Identification.

Authentication

The captured fingerprint is matched against a reference template – 1 vs. 1.

In authentication, user minutiae can be stored on a contactless card. It is also possible to store minutiae in terminal local database.



If the user is matched access is granted.

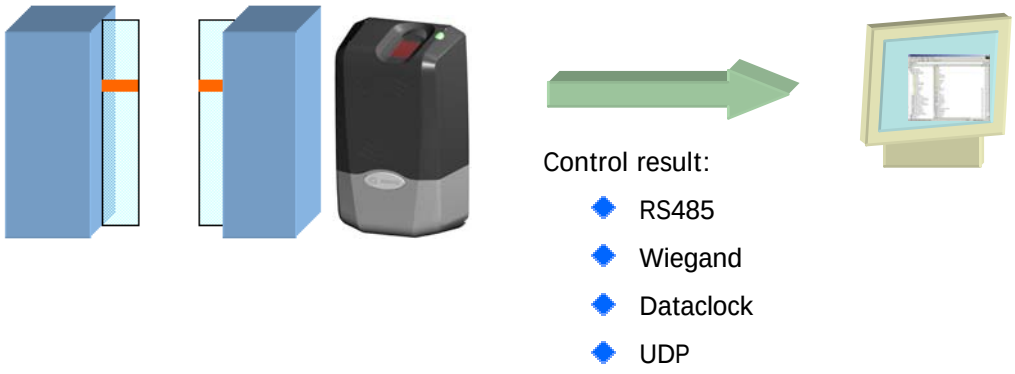
If the user is not recognized access is refused.

See section Access Control By Authentication.

“Hit or No Hit” result communication

If access is granted (the user has been recognized) the led lights green and the buzzer emits a high-pitched “beep”.

If access is denied (the user has *not* been recognized) the led lights red and the buzzer emits a low-pitched “beep”.



Various messages or interfaces can be activated to send the control result:

Relay

After a successful control the MorphoAccess™ relay may be activated during a given period.

Wiegand Id Emission

The ID of the recognized user can be sent though the Wiegand output. The format of the frame may be user defined.

Dataclock Id Emission

The ID of the recognized user can be sent though the Dataclock output.

Udp Id Emission

The ID of the recognized user can be sent though the Ethernet link using UDP. The administrator may set the port.

RS485

Control information can be sent through RS485.

Local Diary (log)

A local file will store biometric logs.

“Proxy” mode

Proxy Mode is not strictly speaking a recognition mode. In this mode, the MorphoAccess™ works as “a slave” waiting for external orders such as:

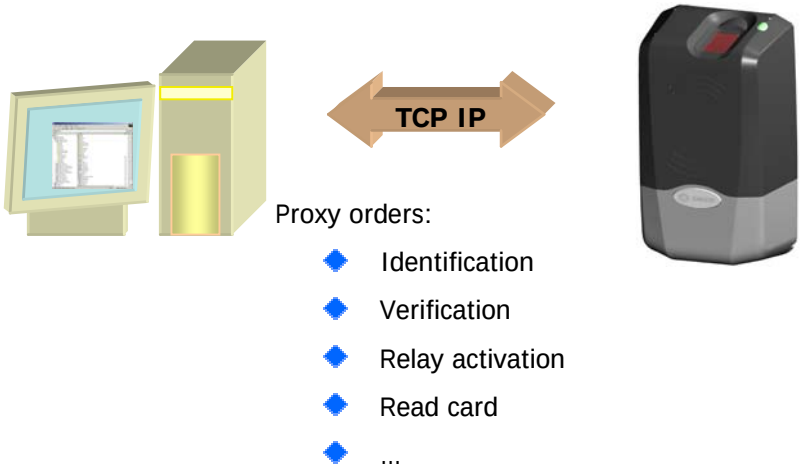
Identification

Verification

Relay activation

Read data on a contactless card.

…



Section Remote Management gives more information about remote management.

Please refer to *MA100 Series Host System Interface* for a complete description of TCP orders possibilites.

CONFIGURING A "CONNECTED" MORPHOACCESS

Introduction

A PC (typically a station with MEMS^{TM}) connected to a MorphoAccess™ can manage the terminal. Available remote operations are:

Biometric template addition,

Control settings modification,

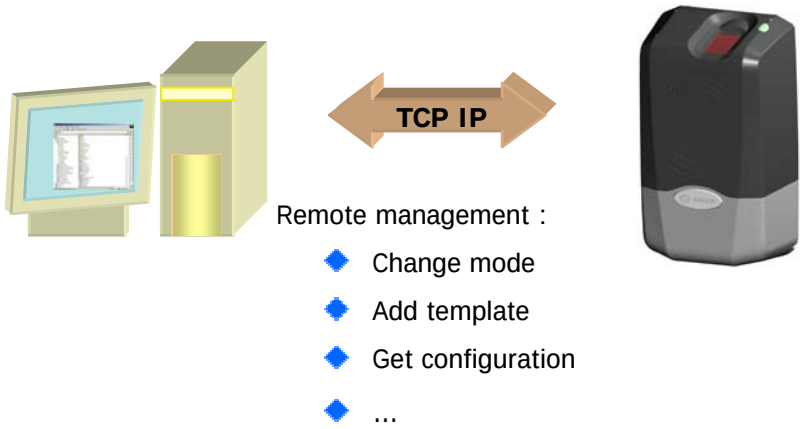
Configuration reading,

Local database deletion,

Record deletion,

Control diary downloading,

Firmware upgrade.



The MorphoAccess™ works as a server waiting for PC request.

The PC will send biometric templates to the terminal and manage the local database.

Please refer to *MA100 Series Host System Interface* for a complete description of TCP administration. This document explains how to create a database and store biometric records in this base.

Network factory settings

By default the terminal IP address is *134.1.32.214*. This address can be changed through Ethernet or with a USB mass storage key.

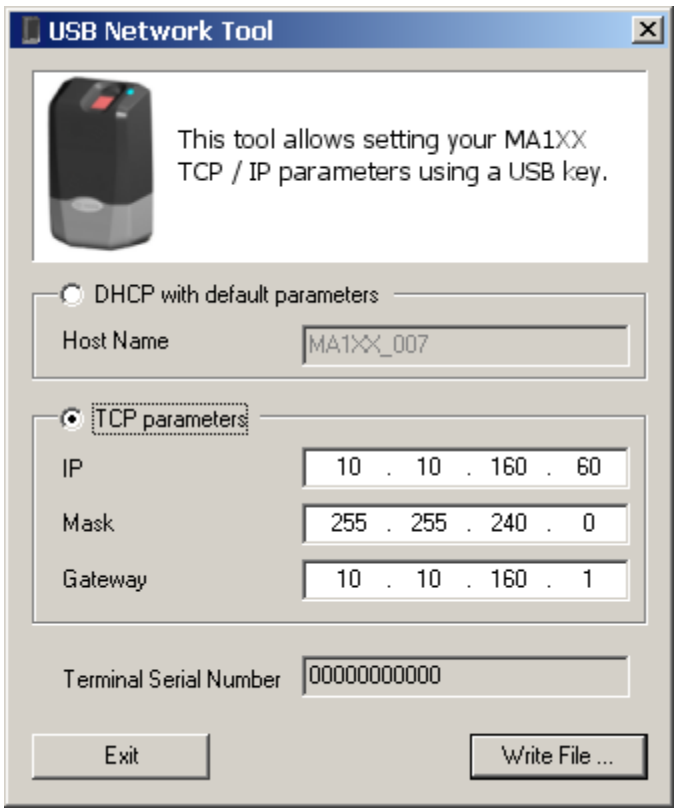
The default server port is 11010.

CONFIGURING A STANDALONE MORPHOACCESS

“USB” key administration

MA100 series have no keyboard, no screen. However it is possible to change TCP/IP parameters without connecting the terminal on a network. This operation only requires a standard USB Mass Storage Key (FAT16).

A dedicated PC application, *USB Network Configuration Tool*, allows writing these new parameters on the key.



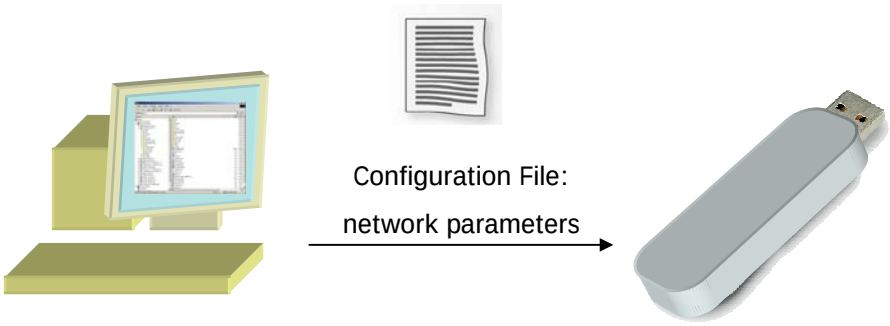
Please refer to *MA100 Series USB Network Tool User Guide*.

Principle

This feature is available to change network parameters (IP address, mask and gateway).

Store a file on a USB Key

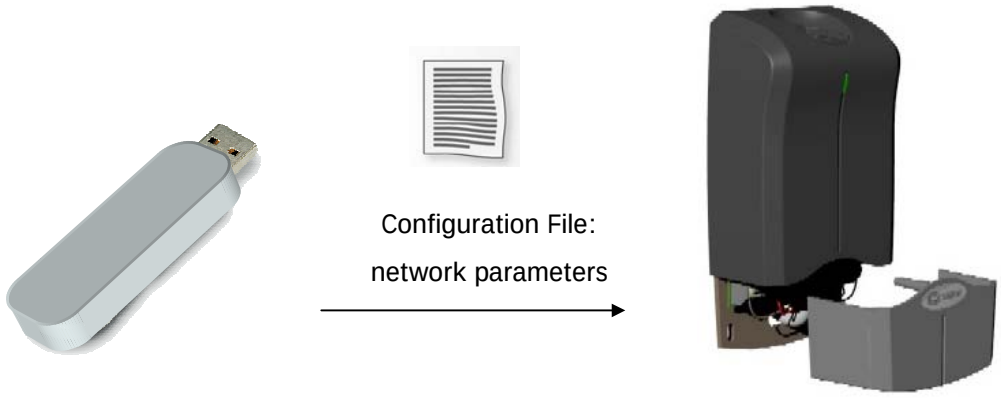
The administrator creates a *configuration file* on a PC using the *USB Network Configuration Tool*. This *configuration file* contains new network parameters. This file must be stored on a USB Mass Storage Key.



Apply changes on a “stand alone” MorphoAccess

The lower protection of the MorphoAccess must be removed to give access to the USB Host Interface of the terminal. The terminal must be powered on.

When the USB key is inserted in the MorphoAccess USB interface, the *configuration file* is read: Ethernet parameters are applied.



At the end of the process a low-pitched “beep” indicates that the key can be removed.

Please refer to *USB Network Configuration Tool User Guide* for more information about this procedure.

CHANGING A PARAMETER

Configuration interface

Terminal parameters are stored in files. These files can be retrieved and modified through TCP/IP using ILV commands. For more information about remote management please refer to *MA100 Series Host System Interface.*

Configuration organization

The terminal contains four files:

- app.cfg.
- adm.cfg.
- bio.cfg.
- net.cfg

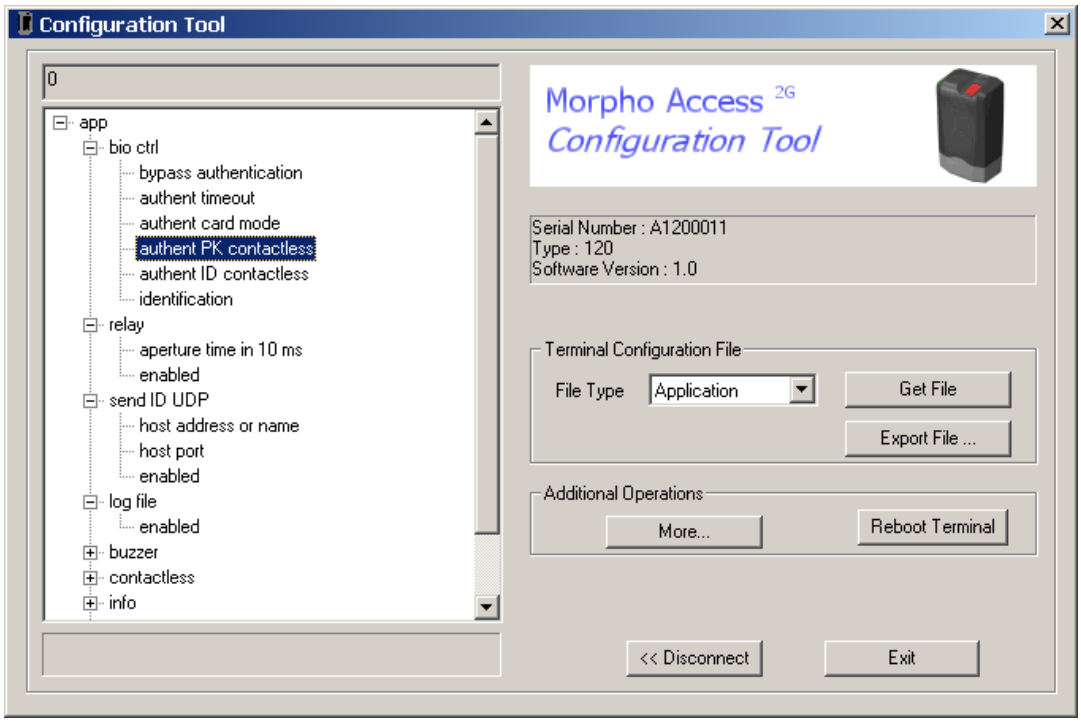
The *app.cfg* file contains the application settings, *adm.cfg* contains administration parameters, *bio.cfg* the biometric sensor settings and *net.cfg* Ethernet parameters.

Parameter path has the following structure *file_name/section/parameter*.

For example the relay activation is driven by the *app/relay/enabled* parameter.

“Configuration tool”

The *Configuration Tool* allows changing these parameters. This program is an illustration of utilization of the TCP API. Please refer to *Configuration Tool User Guide* for more information about this program.



UPGRADING THE FIRMWARE

It is possible to upgrade your MorphoAccess™ firmware. Two packages type are available. One dedicated to terminal system, another one dedicated to biometric library.

Use the MA1XX Downloader to upgrade your terminal system.

Use the MA1XX BioLoader to upgrade your terminal biometric library.

Please refer to the *MA100 Series Upgrade Tools User Guide* for more information about upgrade procedures.

ACCESS CONTROL BY IDENTIFICATION

Access control by identification	
app/bio ctrl/identification	1

To configure MorphoAccess™ terminal in this mode, set the parameter *app/bio ctrl/identification* at 1.

After starting the MorphoAccess™ terminal waits for fingerprint detection in identification mode.

If the identification is successful, the terminal triggers the access or returns the corresponding ID to central security controller. The ID can be sent through various interfaces. Please refer to *MA100 Series Remote Messages Specification* for a complete description of "*hit*" and "*no hit*" messages.

A relay can also be activated.

Once the person's identification is done, the terminal automatically loops back and waits for a new finger.

At least one fingerprint must be stored in the local database. The terminal can store 500 users with 2 fingerprints each.

If the terminal is running in identification mode with an empty database, the sensor is off and the led flashes "yellow".

Set *app/bio ctrl/identification* at 0 to disable the sensor (Proxy Mode).

ACCESS CONTROL BY AUTHENTICATION (MA120 / MA110 ONLY)

Various recognition modes can be applied depending on the templates localization, the required security level.

These modes can be combined with a local identification (fusion mode).

Following modes are available:

Contactless authentication with templates on card:

Captured fingerprints are matched against templates *read on the card (PK)*. **Identifier** and **fingerprints** must be stored on the card.

Contactless authentication with templates on local database:

Captured fingerprints are matched against templates *read from the local database*. Only the **identifier** is required on the card.

Contactless authentication based on card mode:

Depending on the **card mode** either templates are read on the card or the control can be bypassed (visitor mode). The **"card mode"** tag must be stored on the card.

Please refer to *MA100 Series Contactless Card Specification* for a complete description of card structure and access mode.

It is also possible to skip the biometric control: in this case the terminal acts as a badge reader.

Contactless authentication with templates on a contactless card

Contactless authentication with templates (PK) on card	
app/bio ctrl/authent PK contactless	1

MorphoAccess™ 110 or 120 can work in *contactless authentication mode*: the user presents its card, the terminal reads the reference biometric templates (PK) on the card and launches a biometric control based on the read templates.

In this case the card will contain the user identifier and biometric templates: no local database is required.

To change the parameter value use the *Set Registry Key* ILV command, or directly the *Configuration Tool*.

To enable this mode set *app/bio ctrl/authent PK contactless* to 1.

To disable this mode set *app/bio ctrl/authent PK contactless* to 0.

Required tags on card

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent PK contactless	Yes	No	Yes	Yes	No	No

Card structure is described in *MA100 Series Contactless Card Specification*.

Contactless authentication with templates on local database

Contactless authentication with templates on local database	
app/bio ctrl/authent ID contactless	1

The user identifier can be used as an index in the local database of the MorphoAccess™: in this case the reference biometric templates are stored in the local database.

The content of the “ID” tag must match with the user identifier in the terminal database.

To enable this mode set *app/bio ctrl/authent ID contactless* to 1.

To disable this mode set *app/bio ctrl/authent ID contactless* to 0.

Required tags on card

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent ID contactless	Yes	No	No	No	No	No

Card structure is described in *MA100 Series Contactless Card Specification*.

Contactless authentication based on card mode

Contactless authentication with card mode	
app/bio ctrl/authent card mode	1

In this mode the card “decides” on the control progress.

The “CARD MODE” tag is required. This tag can take two values:

- PKS [0x02]: user identifier, template 1 and template 2 are required on the card. Biometric authentication is triggered with biometric templates.
- ID_ONLY [0x01]: only the user identifier is required. There is **no biometric** control, the control is immediately positive. This feature is usefull for visitor requiring an access without enrollment. But it is still possible to store templates on the card.

To enable this mode set *app/bio ctrl/authent card mode* to 1.

To disable this mode set *app/bio ctrl/authent card mode* to 0.

Required tags on card

If CARD MODE tag value is ID_ONLY.

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent card mode (ID_ONLY)	Yes	Yes	No	No	No	No

If CARD MODE tag value is PKS.

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
authent card mode (PKS)	Yes	Yes	Yes	Yes	No	No

Card structure is described in *MA100 Series Contactless Card Specification*.

Bypassing the biometric control in authentication

In this mode only the user id is required on the card. This flag must be combined with an authentication mode. Activating this flag means that the biometric verification is bypassed.

When combined “authent ID contactless” the MorphoAccess™ verifies that the identifier read on the card is present on the local database before granting the access.

Disabling biometric control, but ID must be present in the local database	
app/bio ctrl/bypass authentication	**1**
app/bio ctrl/authent ID contactless	1

When combined “authent PK contactless” the MorphoAccess™ allways authorizes the access: the MorphoAccess™ works as a “simple” Mifare™ or *iCLASS*™ card reader.

Disabling biometric control, access is allways granted	
app/bio ctrl/bypass authentication	**1**
app/bio ctrl/authent PK contactless	1

To bypass biometric control set *app/bio ctrl/bypass authentication* to 1.

To enable biometric control set *app/bio ctrl/bypass authentication* to 0.

Required tags on card

	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
bypass authentication	Yes	No	No	No	No	No

Merged mode

This mode is the fusion of identification mode and contactless authentication without database mode.

So this mode allows:

Running an identification if user places his finger (operation identical to identification mode),

Running a contactless authentication if user places his contactless card (operation identical to contactless authentication without database mode).

If there is no database contactless card presentation is still possible.

This mode is activated by enabling one contactless mode and identification.

Merged mode	
app/bio ctrl/identification	1
And	
app/bio ctrl/authent PK contactless	0 or 1
app/bio ctrl/authent card mode	0 or 1

Required tag on card depends on the authentication mode.

MorphoAccess 220 320 compatibility

These tables present parameter equivalence between MA320/220 family and MA120 family.

Merged mode (*/cfg/Maccess/Admin/mode 5* on 220 and 320) is activated when *app/bio ctrl/identification* is set to 1.

MA 220 320	MA 120
Contactless authentication with ID on card, template in local database	
/cfg/Maccess/Admin/mode 4	*app/bio ctrl/authent ID contactless 1*
Contactless authentication: Card mode	
/cfg/Maccess/Contactless/without DB mode 0 */cfg/Maccess/Admin/mode 3 or*	*app/bio ctrl/authent card mode 1*
/cfg/Maccess/Admin/mode 5 *(merged mode)*	*app/bio ctrl/identification 1*
Contactless authentication: Biometric verification	
/cfg/Maccess/Contactless/without DB mode 2 */cfg/Maccess/Admin/mode 3 or*	*app/bio ctrl/authent PK contactless 1*
/cfg/Maccess/Admin/mode 5 *(merged mode)*	*app/bio ctrl/identification 1*
Contactless authentication: ID “only”, no biometric verification	
/cfg/Maccess/Contactless/without DB mode 1 */cfg/Maccess/Admin/mode 3 or*	*app/bio ctrl/authent PK contactless 1* *app/bio ctrl/bypass authentication 1*
/cfg/Maccess/Admin/mode 5 *(merged mode)*	*app/bio ctrl/identification 1*

PROXY MODE

This mode allows controlling the MorphoAccess™ remotely (the link is Ethernet) using a set of biometric and databasing management function interface access commands.

Identification and authentication must be disabled. It means that all control must be turned off: the terminal becomes a “slave”.

Proxy mode	
app/bio ctrl/identification	**0**
app/bio ctrl/authent PK contactless	**0**
app/bio ctrl/authent ID contactless	**0**
app/bio ctrl/authent card mode	**0**

Please refer to refer to *MA100 Series Host System Interface*: this document explains how to manage a terminal on a TCP network.

RECOGNITION MODE SYNTHESIS

The MA100 series operating mode is driven by:

- The authentication or identification mode required: Card Only, Card + Biometric, Biometric only
- Who defined the operating mode: Card or Terminal

	Mode defined by Card *app/bio ctrl/authent card mode 1*	**Mode defined by Terminal** *app/bio ctrl/authent card mode 0*
Operating mode		
Authentication **Card only** (MA120/MA110)	**ID in card** Card Mode Tag = ID_ONLY	**ID in card** bypass authentication 1 authent ID contactless 1 ***Check ID on terminal***
		ID in card bypass authentication 1 authent PK contactless 1 ***No ID check on terminal***
Authentication **Card** **+ Biometric** (MA120/MA110)	**ID and BIO in Card** Card Mode Tag = PKS	**ID and BIO in card** bypass authentication 0 authent PK contactless 1
		ID on card and BIO in terminal bypass authentication 0 authent ID contactless 1
Identification **Biometric only** (MA1xx)		**ID and BIO in termina** identification 1

SETTING UP RECOGNITION MODE

Two attempts mode

If the recognition fails, it is possible to give a “second chance” to the user.

In identification mode if a bad finger is presented the user has 5 seconds to present a finger again. The result is sent if this period expires or if the user presents a finger again.

In authentication mode, if the user presents a bad finger, he can replace his finger without presenting his card again. The result is sent only after this second attempt.

It is possible to set the finger presentation timeout and to deactivate this “two attempts mode”.

Parameters

This mode can be configured using the *Configuration Tool* for example.

By default the two attempts mode is activated.

Setting up the number of attempts	
app/bio ctrl/nb attempts	1 (only one attempts) 2 (two attempts mode)

The period between two attempts in identification (two attempts mode) can be modified.

Setting up the identification timeout	
app/bio ctrl/identification timeout	5 (1-60)

In authentication mode a finger presentation period can be defined.

Setting up the authentication timeout	
app/bio ctrl/authent timeout	(1-60)

SETTING UP MATCHING PARAMETERS

Setting up matching threshold	
bio/bio ctrl/matching th	1-10

The performances of a biometric system are characterized by two quantities, the False Non Match Rate - FNMR - (Also called False Reject Rate) and the False Match Rate - FMR - (Also called False Acceptance Rate). Different trade-off are possible between FNMR and FMR depending on the security level targeted by the access control system. When convenience is the most important factor the FNMR must be low and conversely if security is more important then the FMR has to be minimized.

Different tuning are proposed in the MorphoAccess terminal depending on the security level targeted by the system. The table below details the different possibilities.

This parameter can be set to values from 1 to 10. This parameter specifies how tight the matching threshold is. Threshold scoring values are identified hereafter

1	Very few persons rejected	FAR < 1%
2		FAR < 0.3%
3	Recommended value (default value)	FAR < 0.1%
4		FAR < 0.03%
5	Intermediate threshold	FAR < 0.01%
6		FAR < 0.001%
7		FAR < 0.0001%
8		FAR < 0.00001%
9	Very high threshold (few false acceptances) Secure application	FAR < 0.0000001%
10	High threshold for test purpose only	There are very few false recognitions, and many rejections

RELAY ACTIVATION

If the control is successful, a relay may be activated to directly control a door. This installation type offers a low security level.

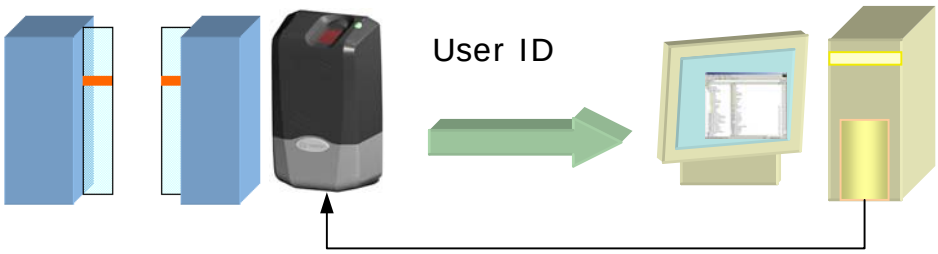
Relay activation	
app/relay/enabled	1

The relay aperture time can be defined and is set by default to 3 seconds (i.e. 300).

Relay aperture time in 10 ms	
app/relay/aperture time in 10 ms	300 (50 to 60000)

LED IN ACTIVATION

Use this signal to wait a controller “ACK” before granting the access.



LED1 to GND: Access authorized.

LED2 to GND: Access refused.

1- If the user is recognized the MA1XX sends the user identifier to the controller.

2 - The MA1XX waits for a **GND** signal on LED1 or LED2. A timeout can be defined.

3 - The controller checks the user rights.

4 - The controller sets LED1 to **GND** to authorize the access or sets LED2 to **GND** to forbid the access.

5 – The control restarts only when LED1 and LED2 are set to “1” again.

This feature improves integration in an access control system (ACS). The ACS through LED IN signals validates result of biometric matching.

LED IN mode activation	
app/led IN/enabled	1

When the ACS validates the control a timeout must be specified: it defines the time during which the MorphoAccess™ will wait for an acknowledgement signal from the ACS through LED IN signals

LED IN “acknowledgement timeout” in 10 ms	
app/led IN/controller ack timeout	0 to 268435455

During the time LED1 or LED2 is set to GND the control DOES NOT RESTART.

LOG FILE

MorphoAccess™ is logging its activities	
app/log file/enabled	1

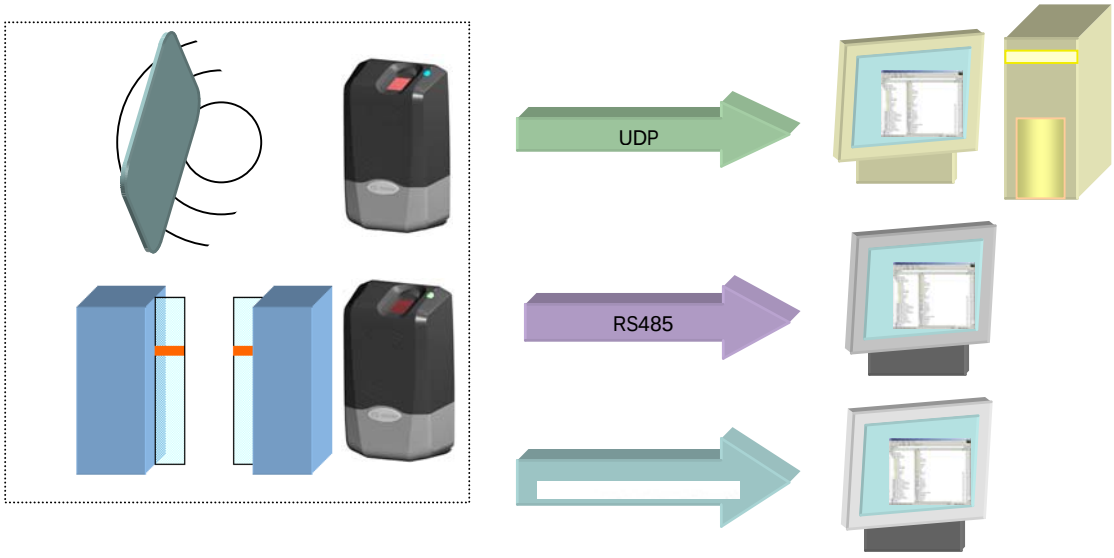
The MorphoAccess™ can log its biometric activities. It stores the result of the command, the date and time, the matching mark, the execution time, and the ID of the user.

It is possible to download the diary file. For more information on this feature, refer to the *MA100 Series Host System Interface*.

REMOTE MESSAGES

Presentation

The MorphoAccess™ terminal can send status messages in real time to a controller by different means and through different protocols. This information, called *Remote Messages* can be used, for instance to display on an external screen the result of a biometric operation, the name or the ID of the person identified…depending on the role of the controller in the system.



The *MA100 Series Remote Messages Specification* describes the different solutions offered by the MorphoAccess™ to dialog with a controller, and how to make use of them.

Supported Protocols

The terminal can send messages about the biometric operations performed by the MorphoAccess™ to a controller through the following protocols:

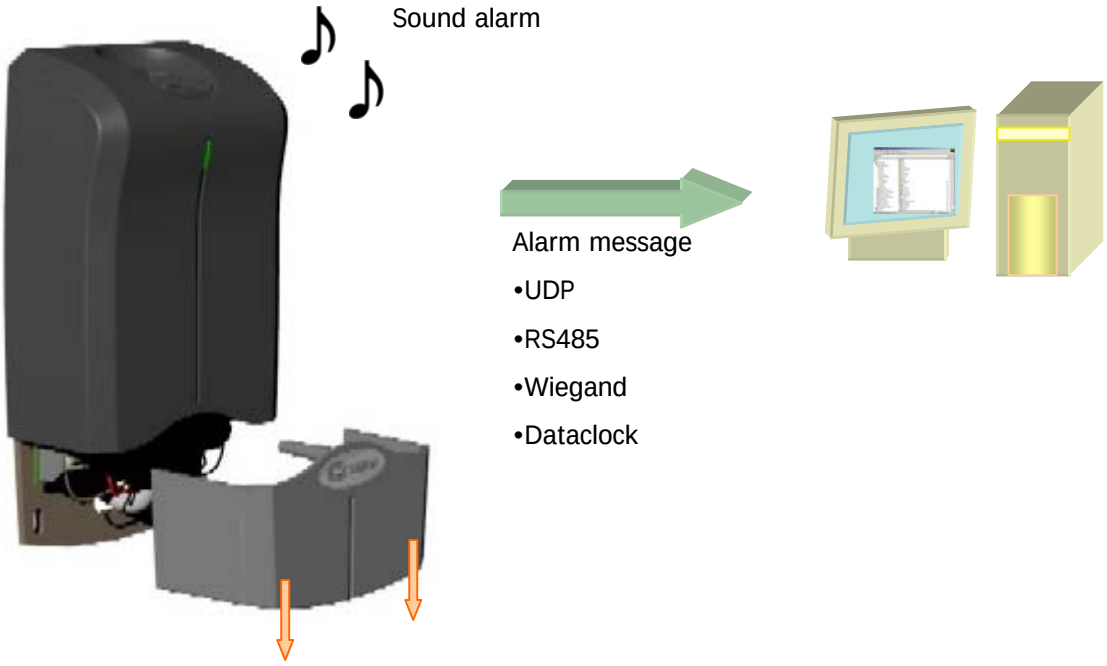
- Wiegand
- Dataclock
- RS485
- Ethernet (UDP)

TAMPER SWITCH MANAGEMENT

Alarm activation

The MorphoAccess™ can detect that the back cover has been removed.

The device can send an alarm to the central controller in case of intrusion. It can also play a sound alarm whilst sending the alarm.



To send an alarm on an output (UDP, Wiegand, Dataclock or RS485), the corresponding interface must be activated otherwise no alarm will be sent.

Because Wiegand, Dataclock, and RS485 are multiplexed on the same lines, only one of these protocols shall be enabled at one time, else priority is given to *Wiegand,* then *Dataclock*, then *RS485*.

These keys are:

app/send ID wiegand/enabled

app/send ID dataclock/enabled

app/send ID RS485/enabled

app/send ID UDP/enabled

Tamper switch management feature is configured by setting the key *app/tamper alarm/level* to an appropriate value.

Tamper Alarm Level	
app/tamper alarm/level	0 - 2
0 No Alarm.	
1 Send Alarm (No Sound Alarm).	
2 Send Alarm and Activates Buzzer (Sound Alarm)	

The key *app/failure ID/alarm ID* defines the value of the alarm ID to send in Wiegand or Dataclock. This ID permits to distinguish between an user ID and a error ID. To be validated , key *app/failure ID/enabled* must be set to 1.

Tamper Alarm ID	
app/failure ID/alarm ID	0 - 65535
app/failure ID/enabled	1

In Wiegand and Dataclock the alarm ID is sent like other Failure IDs, see the documentation *MA100 Series Remote Messages Specification* for a description of the packet format in UDP and RS-485.

Examples

Example 1: Send an alarm ID (62221) in Wiegand, and play sound warning, in case of intrusion detection.

To send an alarm in Wiegand, the key *app/send ID wiegand/enabled* must be set to 1.and the key *app/tamper alarm/level* must be set to 2 (alarm and buzzer.)

The key *app/failure ID/alarm ID* must be set to 62221 to link the intrusion event to this identifier.

Example 2: Send an alarm in UDP quietly in case of intrusion detection.

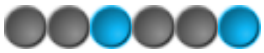
To send an alarm in UDP, the key *app/send ID UDP/enabled* must be set to 1.

Then the key *app/tamper alarm/level* must be set to 1 (quiet alarm.)

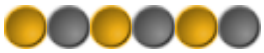
MAN MACHINE INTERFACE

Convention

Intermittent "Pulse": led is 1 second OFF, 0.05 second ON. For example:

Intermittent blue "Pulse" 

Fast "Pulse": led flashes quickly. The rhythm is the same than when a hard drive works.

Fast orange "Pulse" 

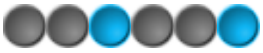
Slow intermittent "Pulse". led is 1 second OFF, 1 second ON. For example:

Slow intermittent red "Pulse". 

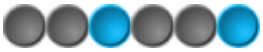
Identification – waiting for a finger

Sensor	ON	
Led	OFF	

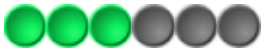
Authentication – waiting for a badge

Sensor	OFF	
Led	Intermittent blue "Pulse"	

Fusion - waiting for a finger or a badge

Sensor	ON	
Led	Intermittent blue “Pulse”	

Control OK

Sensor	ON	
Led	Green 1 second	
Buzzer	ON 0.1 second - High-pitched	

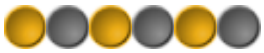
Control failed

Sensor	ON	
Led	Red 1second	
Buzzer	ON 0.7 second - Low-pitched	

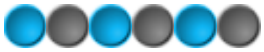
No database or empty database

Sensor	OFF	
Led	Slow intermittent orange “Pulse”.	

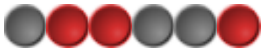
Biometric acquisition, bad placement

Sensor	ON	
Led	Fast intermittent orange “Pulse”.	

USB key can be removed

Sensor	-	-
Led	Fast intermittent blue “Pulse”.	
Buzzer	ON 0.7 second - Low-pitched	

Sensor failed

Sensor	OFF	
Led	Slow intermittent red “Pulse”.	

NETWORK PARAMETERS

These parameters can be changed using the *Configuration Tool* or by implementing ILV commands.

Network parameters are stored in a file named “net.cfg”.

A change is applied after rebooting the terminal.

Section [boot proto]

DHCP activated

0 NO

1 YES

Section [parameters]

host name

“MA-1234567890”

network address

“134.1.32.214” by default, static address.

network mask

“255.255.240.0“by default.

default gateway

“134.1.6.20“ by default.

These parameters can be changed using the *Configuration Tool* or by implementing ILV commands.

The “app.cfg” file contains information about your terminal configuration.

Section [info] (read only)

Type

120: MorphoAccess™ with local database and Mifare™ contactless reader

110: MorphoAccess™ with local database and ICLASS™ contactless reader

100: MorphoAccess™ with local database.

Minor

Software revision (minor)

Major

Software revision (major)

Release

Release version.

ADMINISTRATION PARAMETERS

The “app.cfg” file contains advanced parameter to modify the host port and the connection mode. This parameter **must not** be changed.

Section [remote management TCP]

Inactivity timeout

Must be set to 0.

Port

11010 by default, defines the socket server port.

Section [terminal]

Group

Must be set to 255.

ANNEX: CONTACTLESS MODES TABLE

Operation	*Authent card mode*	*Authent PK contactless*	*Authent ID contactless*	*Bypass authentication*
Authentication with templates in database Read ID on contactless card. Retrieve corresponding templates in database. Biometric authentication using these templates. Send ID if authentication is successfull.	0	0	1	0
Authentication with templates on card Read ID and templates on contactless card. Biometric authentication using these templates. Send ID if authentication is successfull.	0	1	0	0
Card mode authentication Read card mode, ID, templates (if required by card mode) on contactless card. If card mode is « ID only », send ID. If card mode is « Authentication with templates on card », biometric authentication using templates read on card, then send ID if authentication is successfull.	1	0	0	0
Authentication with templates in database – biometric control disabled Read ID on contactless card. Check corresponding templates presence in database. Send ID if templates are present.	0	0	1	1
Authentication with templates on card – biometric control disabled Read ID on contactless card. Send ID.	0	1	0	1
Card mode authentication – biometric control disabled Read card mode, ID, templates (if required by card mode) on contactless card. Whatever card mode, send ID.	1	0	0	1

ANNEX: REQUIRED TAGS ON CONTACTLESS CARD

Operation	ID	CARD MODE	PK1	PK2	PIN	BIOPIN
Authentication with templates in database	Yes	No	No	No	No	No
Authentication with templates on card	Yes	No	Yes	Yes	No	No
Card mode authentication (ID_ONLY)	Yes	Yes	No	No	No	No
Card mode authentication (PKS)	Yes	Yes	Yes	Yes	No	No
Authentication with templates in database – biometric control disabled	Yes	No	No	No	No	No
Authentication with templates on card – biometric control disabled	Yes	No	No	No	No	No
Card mode authentication (ID_ONLY) – biometric control disabled	Yes	Yes	No	No	No	No
Card mode authentication (PKS) – biometric control disabled	Yes	Yes	Yes	Yes	No	No

FAQ

Terminal IP address is unknown or terminal is not reachable

Use *USB Network Configuration Tool* to set a valid network address in your terminal. See section Configuring a standalone MorphoAccess.

Sensor is off

Verify that the base contents at least one record.

Check that identification is enabled.

Terminal returns erratic answers to ping requests

Check the subnet mask. Ask to your administrator the right value.

BIBLIOGRAPHY

MA100 Series Installation Guide

This document describes terminal electrical interfaces and connection procedures.

MA100 Series Standard Host Interface Specification

A complete description of remote management commands.

MA100 Series Remote Messages Specification

A description of the MA1XX communication interfaces.

MA100 Series Contactless Card Specification

This document describes the MA12X Contactless card feature.

MA100 Series Configuration Tool User Guide

Configuration Tool user guide , via Ethernet

MA100 Series USB Network Tool User Guide

Configuration Tool user guide , via USB key

MA100 Series Upgrade Tools User Guide

Upgrade Tool user guide about firmware upgrading procedures.

MA100 Series Configuration Guide

The complete description of terminal configuration files.

Siège social : Le Ponant de Paris
27, rue Leblanc - 75512 PARIS CEDEX 15 - FRANCE