MorphoAccess® SIGMA Lite Series

Administration Guide

Osny, France

WARNING

PROPRIETARY RIGHTS

This document contains information of a proprietary nature to Morpho and is submitted in confidence for a specific purpose. The recipient assumes custody and control and agrees that this document will not be copied or reproduced in whole or in part, nor its contents revealed in any manner or to any person except to meet the purpose for which it was delivered.

This caveat is applicable to all the pages of this document.

Revision History

The table below contains the history of changes made to the present document.

Version	Date	Description
01	October 2015	First Version

Table of Contents

This document and the information therein are the property of Morpho. They must not be copied or communicated to a third party without the prior authorization of Morpho

This document and the information therein are the property of Morpho. They must not be copied or communicated to a third party without the prior authorization of Morpho

This document and the information therein are the property of Morpho. They must not be copied or communicated to a third party without the prior authorization of Morpho

Table of Figures

Section 1 : **Introduction**

MorphoAccess® SIGMA Lite Series Terminal

Congratulations for choosing a MorphoAccess® SIGMA Lite Series Automatic Fingerprint Recognition Terminal.

MorphoAccess® SIGMA Lite Series provides an innovative and effective solution for access control applications using Fingerprint Verification or/and Identification.

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

The MorphoAccess® SIGMA Lite Series terminals integrate Morpho image processing and feature matching algorithms. This technology is based on lessons learned during 25 years of experience in the field of biometric identification and the creation of literally millions of individual fingerprint identification records.

Designed for physical access control applications, MorphoAccess® SIGMA Lite Series terminals feature a compact, attractive design, coupled with high reliability and security. These 5thgeneration terminals are both robust and easy to use for a variety of applications, including office, headquarters and administrative building security, as well as protection of external access points.

To ensure the most effective use of MorphoAccess® SIGMA Lite Series terminal, an administrator should read this User Guide completely.

Scope of the document

This document is intended to guide administrators on how to use MorphoAccess® SIGMA Lite Series Terminal.

Terminal Series	Terminal Name	Biometrics	Contactless smartcard reader		
			iCLASS® iCLASS® SE iCLASS® SEOS	MIFARE® DESFire® NFC®	Prox®
MorphoAccess® SIGMA Lite Series	MorphoAccess® SIGMA Lite MorphoAccess® SIGMA Lite+	✓			
	MorphoAccess® SIGMA Lite iCLASS® MorphoAccess® SIGMA Lite + iCLASS®	✓	✓		
	MorphoAccess® SIGMA Lite Multi MorphoAccess® SIGMA Lite + Multi	✓		✓	
	MorphoAccess® SIGMA Lite Prox MorphoAccess® SIGMA Lite + Prox	✓			✓

The document discusses about the MorphoAccess® SIGMA Lite terminal capabilities, and all the configurations done in the terminal. MorphoAccess® SIGMA Lite terminal is using LED display. MorphoAccess® SIGMA Lite+ terminal is using LCD Touchscreen.

An administrator can learn about Access Control Processes, Compatibility with access control systems, Time & Attendance mode and how terminal is configurable from Webserver, refer Access to Administration Menu through Webserver

In order to perform all operations with the best efficiency, it is recommended to read this guide.

About Biometrics

About fingerprint biometrics

Fingerprints are permanent and unique. They are formed before birth and last throughout one's life. Classification and systematic matching of fingerprints for different purposes have been in use since the late 19th century.

The skin on the underside of fingers is different from the skin on other areas of an administrator body. This skin has raised lines called Ridges.

These ridges do not run continuously from one side to the other, rather they may curve, end, or divide into two or more ridges (Bifurcation and Endings). Barring accidental or intentional mutilation, the ridge arrangement is permanent.

Fingerprints can be divided into major ridge pattern type such as Whorls, Loops and Arches etc. Unique characteristics known as Minutiae identify those points of a fingerprint where the ridges become bifurcation or endings, as illustrated in Figure 1. These minutiae are the unique features, which form the basis of any system using fingerprint comparison techniques for identification and verification purposes.

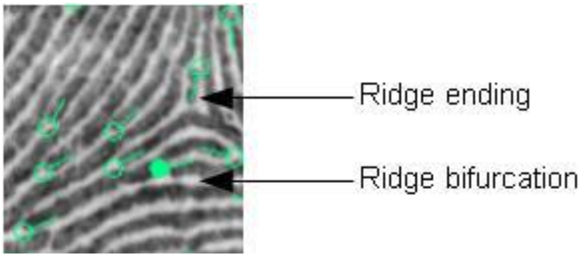


Figure 1: Minutiae are classified in two categories i.e. ridge ending and bifurcation

Fingerprint is a mature biometrics, in use for various applications based on individual’s authentication or identification, as it offers an excellent trade-off between criteria such as user acceptance, easiness of use, performance, stability, cost effectiveness and interoperability.

Since the early eighties, Morpho has studied fingerprint characteristics and continually refined its expertise in fingerprint identification technology, developing first AFIS systems (Automated Fingerprint Identification Systems) and then applying its unique know-how and worldwide leading position to markets such as physical access control (premises), logical access control (computers and networks), secure payment transactions and OEM applications.

Section 2 : **Connecting the Terminal to a PC**

General

Why would one connect the terminal to a PC?

The MorphoAccess® SIGMA Lite Series terminal is designed to be able to run in standalone mode, it means without any connection to a master system. But sometimes, a connection with a PC is useful to perform tasks like:

terminal configuration,

terminal maintenance: firmware upgrade, add a license (to unlock an optional feature),

database management: add, modify or remove a user,

log file management: get or delete log file,

Wi-Fi™ connection configuration before use.

Connection methods

The MorphoAccess® SIGMA Lite Series terminal can be connected to a PC by an Ethernet cable, either directly or through a LAN. The LAN can be reduced to only one Ethernet switch.

Once physically connected, the MorphoAccess® SIGMA Lite Series terminal can be configured using an application such as Morpho Bio Toolbox.

A POE (Power over Ethernet) current injector is mandatory if the MorphoAccess® SIGMA Lite Series terminal is not powered by the +12VDC/GND wires block.

Network parameter initialization

The network parameters of the MorphoAccess® SIGMA Lite Series terminal are:

IP address Mode	Parameter	Factory value
Dynamic (DHCP - Default)	Terminal IP address	192.168.1.1
	Gateway IP address	255.255.255.0
	Sub network mask	0.0.0.0
	Host name	MAsigma-lite MAsigma-lite-plus

MorphoAccess® SIGMA Lite Series provides the quickest method to configure these values.

Point to Point Ethernet Connection

The MorphoAccess® SIGMA Lite Series terminal can be connected directly to a PC by an Ethernet cable.

But there are some limits described in the next paragraphs.

If the PC Ethernet port doesn't support the Auto-MDIX feature, then a crossover Ethernet cable is mandatory. If no crossover Ethernet cable is available, then a switch can be used (please refer to next section).

If the PC to be used is already connected to a LAN, then it must be either disconnected from the LAN, or equipped with a 2nd network interface board, which will be dedicated to the connection with the terminal. It could be mandatory to modify the network parameter of the PC: please contact an administrator LAN administrator to define the best solution.

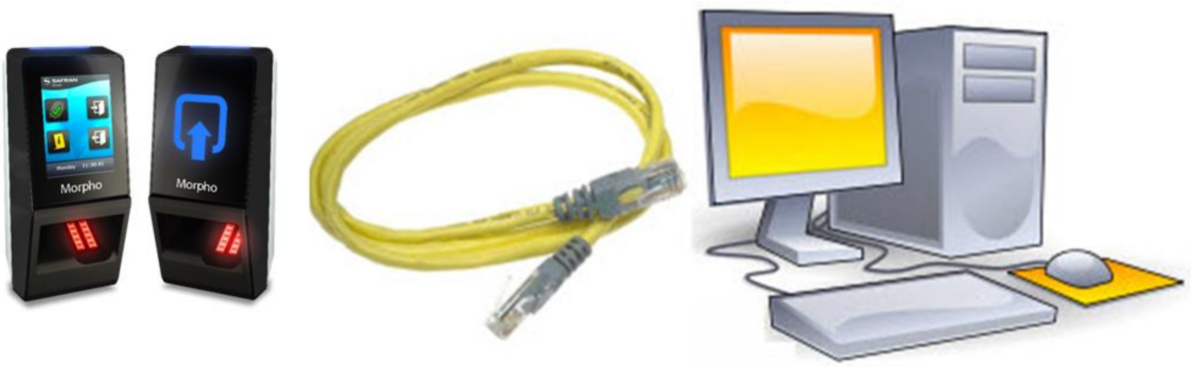


Figure 2: Direct Point to Point Ethernet Connection

Connection through Network Switch

The MorphoAccess® SIGMA Lite Series terminal can be connected to a PC through an Network switch. This is useful when no crossover cable is available, but instead, one Network switch and two Ethernet standard cables are required.

WARNING: an Ethernet HUB doesn't allow a connection between two of its ports. An Network switch is really mandatory.

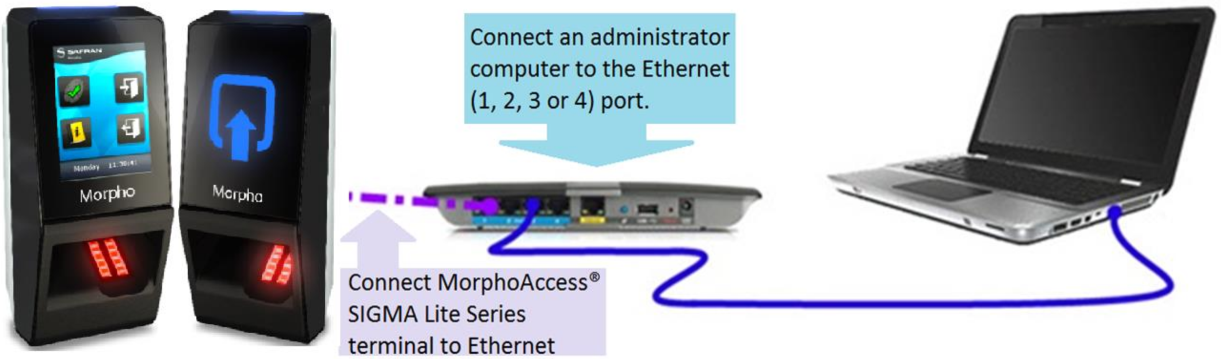

Connect an administrator computer to the Ethernet (1, 2, 3 or 4) port.
Connect MorphoAccess® SIGMA Lite Series terminal to Ethernet
Morpho
Morpho

Figure 3: Connection through an Ethernet switch

Connection through a LAN

Description

The MorphoAccess® SIGMA Lite Series terminal can be connected to a PC through a Local Area Network (LAN).

The MorphoAccess® SIGMA Lite Series terminal required for a connection is specified by its IP address or by its host name, if it can be added to the DNS Server database. The IP address is either static, or dynamically assigned by the DHCP server of the network.

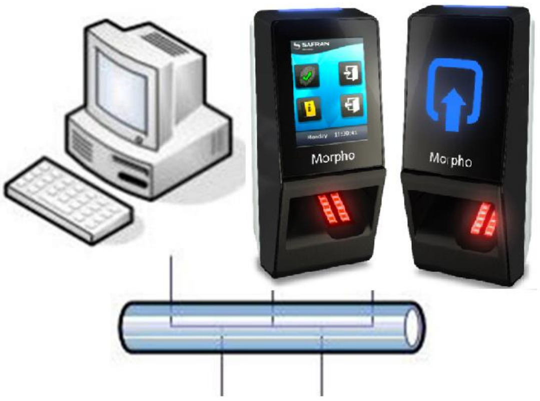


Figure 4: Connection through LAN

It is recommended to connect MorphoAccess® SIGMA Lite Series terminals on a dedicated network to reduce possible fraudulent accesses to terminal configuration. Please contact network administrator for more information about LAN security strategies.

Before connecting the MorphoAccess® SIGMA Lite Series terminal to a LAN, it is necessary to specify the LAN parameters to the terminal. The values of these parameters are to be provided and/or approved by the administrator of the network.

LAN with DNS Server

When a DNS server is available in the LAN, the PC can request the connection to the MorphoAccess® SIGMA Lite Series terminal by using its host name instead of its IP address.

But the network administrator must add the MorphoAccess® SIGMA Lite Series terminal host name to the DNS server database. Otherwise, a TCP open session request, using the terminal's hostname, will fail. Please contact local network administrator to execute this operation in the DNS server.

It is useful to specify the MorphoAccess® SIGMA Lite Series terminal by its host name, when the DHCP mode is enabled, as the IP address of the terminal can change after a power up.

LAN without DNS Server

This section is about LAN without DNS Server, or with DNS Server but the MorphoAccess® SIGMA Lite Series terminal host name cannot be added to the DNS Server base.

In that case the PC is not able to establish a connection with a terminal using its host name. An IP address of the MorphoAccess® SIGMA Lite Series terminal is the only way to specify the terminal.

For standard use (excluding unscheduled maintenance operations), it is not recommended to enable DHCP mode in the terminal; when this mode is enabled, the IP address for the terminal can change each time it is switched on.

Static IP address (DHCP disabled)

This is the easiest way to connect a MorphoAccess® SIGMA Lite Series terminal to a LAN: the IP address of the terminal remains the same after each restart and the Host System need only to know this IP address to establish a connection with the terminal.

The IP address of the MorphoAccess® SIGMA Lite Series terminal must be reserved in the router by the network administrator. The network administrator must also provide and/or approve the network parameter values for the terminal, i.e.:

The MorphoAccess® SIGMA Lite Series terminal IP address,

Gateway IP address,

Local subnet masks value.

WARNING: If the MorphoAccess® SIGMA Lite Series terminal uses an IP address already assigned in the network, the connection to the terminal will be instable.

Dynamic IP address (DHCP enabled)

When the DHCP mode is activated in the terminal, at each power up the MorphoAccess® SIGMA Lite Series terminal requires an IP address to the network router. This address could be different after each start-up: it depends on the DHCP strategy defined for the LAN.

Please contact the network administrator to know if the LAN supports DHCP mode, and if yes, which dynamic IP address assignation is used.

Wi-Fi™ Network configuration

Requirements

Wi-Fi™ connection is available under the following mandatory conditions:

- A Morpho Wi-Fi™ USB adapter must be plugged in the rear USB port of the terminal (please refer to MorphoAccess® SIGMA Lite Series Quick User Guide).
- A Wi-Fi™ license (dedicated to this terminal) must be present in the terminal (as described in Communication licenses
- The terminal is not connected to a network with an Ethernet cable: Wi-Fi™ connection and Ethernet cable connection are mutually exclusive,

After Wi-Fi™ license downloading and Wi-Fi™ USB adapter installation, make sure to reboot the terminal.

NOTE: Both Wi-Fi™ USB adapter and license can be ordered under the reference "MA WI-FI™ PACK".

Configuration

The Wi-Fi™ network configuration is described in subsequent section Wi-Fi™ Configuration

Troubleshooting

If the terminal is configured to use the Wi-Fi™ connection with the Wi-Fi™ USB adapter plugged in and if there is no WI-FI™ license present, the MorphoAccess® SIGMA Lite Series terminal will emit a short-low tone.

To solve this issue, unplug the Wi-Fi™ USB adapter and restart the terminal.

The Wi-Fi™ configuration parameters are described in the **MorphoAccess® SIGMA Lite Series terminals Parameters Guide document**.

Section 3 : **Terminal Configuration and Administration**

Understanding MorphoAccess® Configuration

Presentation

MorphoAccess® SIGMA Lite Series terminal has factory default settings for all the functionalities supported. An administrator can configure the terminal as per requirement. The terminal can be configured using one of the methods described below:

Webserver Application: Webserver can be called a remote configuration panel of MorphoAccess® SIGMA Lite Series terminal. It enables an administrator to configure any parameter of terminal connected remotely. Webserver is accessible through Ethernet or Wi-Fi network connected to the terminal. Only an administrator can login to Webserver. Refer "Access to Administration Menu through Webserver

" in this document.

Webserver application also has a module called "Complete Configuration" which is used for setting parameter keys of MorphoAccess® SIGMA Lite Series terminal. For detailed description of all the parameters, please refer to **MorphoAccess SIGMA and SIGMA Lite Series Parameters Guide**.

Modifying the value of a parameter

There are two ways to modify the value of a terminal parameter:

- Remotely through Ethernet or Wi-Fi™, with a client application/interface running on the Host System (such as MorphoBioToolbox or a web browser connected to the embedded Webserver),
- With a USB mass storage key, which contains a script prepared on a PC using MorphoBioToolBox.

Notation

In this manual a parameter is presented using this format:

Parameter name	Value	Description
_	_	_

For example to allow additional attempt for biometric authentication:

Parameter name	Value	Description
auth_param.additional_bio_check_nb_attempt	1 or 2	A value of “2” means that after a first incorrect identification or authentication a second chance is given to place finger on the biometric sensor. Set this parameter to “1” to offer only one attempt to place finger.

Configuring a Networked MorphoAccess®

Introduction

A MorphoAccess® SIGMA Lite Series terminal can be managed by a PC connected to the terminal, using an application such as Webserver or Morpho Bio Toolbox (in case terminal is in legacy Morpho mode).

The remote operations available are mainly:

Time and Attendance configuration,

read the value of parameters,

modify the value of parameters,

create access schedules,

network configuration,

Tamper settings, etc.

The terminal works as a TCP/IP server, which waits for a request from the Host System application, which acts as a TCP/IP client.

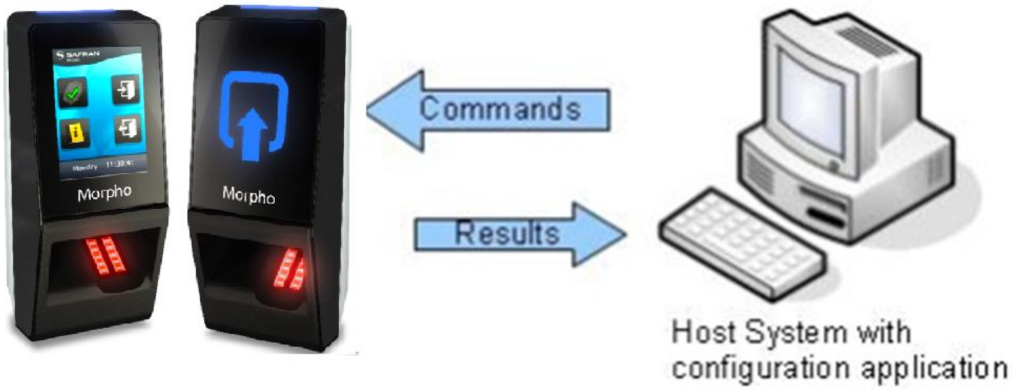


Figure 5: Configuration of a MorphoAccess® SIGMA Lite Series terminal by a Host System

The commands supported by the MorphoAccess® SIGMA Lite Series terminal are described in the **MorphoAccess® SIGMA Lite Series Host System Interface Specification** document.

Refer to “Access to Administration Menu through Webserver

” section in this document, for details on actions that can be performed from Webserver.

Network factory settings

By default the terminal IP address is 192.168.1.1. This address can be changed by a distant system connected through an IP link or with a USB flash drive (USB Network Tool).

The default server port is 11010.

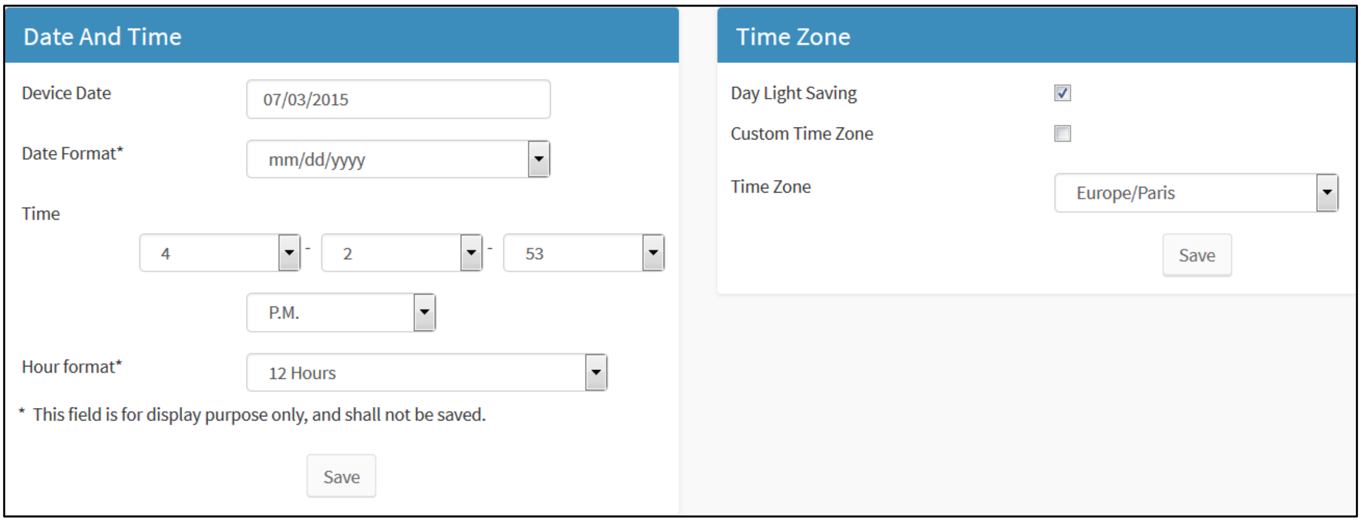
Date/Time settings

The date/time of the terminal can be initialized by a distant system or through Webserver.

Access Path

Webserver > Terminal Settings > Date Time

Screens & Steps



Date And Time

Device Date	07/03/2015
Date Format*	mm/dd/yyyy
Time	4 - 2 - 53
	P.M.
Hour format*	12 Hours

* This field is for display purpose only, and shall not be saved.

Time Zone

Day Light Saving	☑
Custom Time Zone	□
Time Zone	Europe/Paris

Figure 6: Date and Time setting of Terminal from Webserver

SSL Securing

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are cryptographic protocol designed to provide communication security over Ethernet or Wi-Fi™ channels.

These protocols are used to protect the communication between the MorphoAccess® SIGMA Lite Series terminal and a distant system, such as a central access controller or a terminal configuration station.

References

Refer to “SSL Configuration” in this guide, to enable and configure SSL communication port.

Network Wi-Fi™ configuration

Through applications like Webserver and Morpho Bio Toolbox, an administrator can configure Wi-Fi™ parameters. Wi-Fi™ connection is available under the following conditions:

A Morpho WI-FI™ USB adapter, ref. 189930722, must be plugged in the rear USB port of the terminal. Installation procedure is described in the MorphoAccess® SIGMA Lite Series Installation Guide,

A MorphoAccess® WI-FI™ License is loaded in the terminal (cf. NOTE 2 "Downloading a license"),

There are two ways to configure Wi-Fi™.

One of the way is to connect to a network with an Ethernet cable, connect the terminal through Wi-Fi™. Once the terminal is connected over Wi-Fi™, unplug the Ethernet cable.

Other way is using USB script which can be create from MBTB.

WI-FI™ connection and Ethernet cable connection are not mutually exclusive.

NOTE: A DHCP server and a DNS server are mandatory when the Wi-Fi™ interface is configured in DHCP mode.

The DHCP server automatically attributes an IP address to the MorphoAccess® SIGMA Lite Series terminal.

The DNS server links the terminal hostname to its real IP address.

It is also important that the DNS server is updated each time the DHCP server attributes another IP address to a terminal.

NOTE: A MorphoAccess® WI-FI™ License is mandatory.

If WI-FI™ USB adapter is plugged in and if there is no license present; then on configuring WLAN, the terminal will display an error message: "license not present".

See WI-FI™ parameters description in paragraph Wi-Fi™ Configuration

using Webserver.

This document and the information therein are the property of Morpho. They must not be copied or communicated to a third party without the prior authorization of Morpho

MorphoAccess® Terminal Database Management

General

The management of the MorphoAccess® SIGMA Lite Series terminal can be done through Webserver application connected to terminal.

Adding a user to the database

Adding a user means to create a record with the biometric data of two fingers of the user, and a unique identifier. Users stored in database are of following types:

Normal Users are the ones to whom access is granted or rejected based on access rights check.

Authorized Users List are the ones, that the centralize access controller checks before granting access.

VIP listed Users are allowed access without performing biometric/PIN check by the terminal. Read more about VIP users under “Access Control Process for VIP Users”.

The user’s enrolment is directly done on the MorphoAccess® SIGMA Lite Series terminal without managing a database on the PC.

Removing a user from the database

Removing a user means deleting the user’s record from the database of the MorphoAccess® SIGMA Lite Series terminal.

The user can be removed directly from the MorphoAccess® SIGMA Lite Series terminal without managing a database on the PC.

Database Size

The MorphoAccess® SIGMA Lite Series terminal database can store as below:

Basic capacity of terminal users’ database is 3,000 users (and administrators).

Maximum Authorized User List Capacity, indicates the maximum number of users can be added to authorized user list, which is 250,000 users by default.

Maximum VIP user capacity, indicates the maximum capacity of the users can be enrolled as VIP users, that is 100 users by default.

By default, terminal can store up to 100,000 transaction.

The database size can be increased by installing licenses. E.g. the user record storage size can be increased up to 10,000 user records with a MA_10K_USERS license. For each user, the terminal stores the biometric data of two or three fingers. For MorphoAccess® Terminal License Management, refer subsequent section for more details.

MorphoAccess® Terminal License Management

The installation of a license in the terminal, unlocks one or several optional features of the MorphoAccess® SIGMA Lite Series terminal.

The MorphoAccess® SIGMA Lite Series terminal supports below types of licenses:

MA_10K_USERS

MA_1M_LOGS (extend database maximum size)

MA_PAC

MA_TA (MorphoAccess® SIGMA Lite+)

MA_WI-FI™ (allows Wi-Fi™ connection)

MIMA (Internal Default License)

VERIF (Internal Default License)

BCL (Internal Default License)

The function of each license is described in detail in the following sections.

User licenses

By default, the maximum size of a MorphoAccess® SIGMA Lite Series terminal database is limited to 3,000 user records (with two or three fingers per user record). User licenses can be installed for extending this maximum database limit. Following types User licenses are available:

The **MA_10K_USERS** license extends the maximum size of the database to 10,000 user records (With two fingers per user record. In case, duress finger is enabled, it can have three fingers per user record).

Logs licenses

By default, MorphoAccess® SIGMA Lite Series Terminal can store up to 100,000 logs. By installing Logs licenses, the storage capacity of the logs can be increased. Below are the types of Logs Licenses:

The **MA_1M_LOGS** license extends the maximum size of the database to store 1,000,000 (1 million) logs.

Communication licenses

MorphoAccess® SIGMA Lite Series terminal supports communication to distant system through Ethernet Connection. There are other networks such as Wi-Fi™ which can be used for connecting terminal with distant systems. To enable these network communication, it is required to install licenses.

Following types of communication licenses are available:

MA_WI-FI

The MA_WI-FI license enables the Wi-Fi™ network (WLAN) which replaces the standard Ethernet connection. The terminal can communicate with distant systems through WLAN.

NOTE: The license alone is not enough, a USB Wi-Fi™ adapter compatible with MorphoAccess® SIGMA Lite Series terminals is mandatory. The adaptor and license can both be ordered under reference "MA WI-FI PACK".

Access Control license

MA_PAC

The MA_PAC license (available by default) enables following functionalities of the MorphoAccess® SIGMA Lite Series terminal:

Single Door Access Control (SDAC)

Wiegand output

Clock & data output

IP output

Serial output

Time and Attendance (T&A) license

MA_TA

The MA_TA license is required to be loaded on terminal, in order to enable Time & Attendance (T&A) feature. Only if the license is loaded, an administrator can configure Time & Attendance parameters and perform T&A actions.

Note: Time and Attendance (T&A) license is supported, by default, on MorphoAccess® SIGMA Lite+ Series Terminals only.

Basic Licenses

MIMA/VERIF/BCL are sensor related licenses, without which it is not possible to get the sensor work.

Getting a license for a MorphoAccess® SIGMA Lite Series terminal

Morpho Online License Generator allows ordering any type of license for any kind of Morpho biometric product. The file containing the license is automatically sent by email.

The access to the Online License Generator requires an account in our biometric terminals support website, and an account in the License Generator sub website.

www.biometric-terminals.com (see “License Generator" section)

If an administrator does not have an account, please contact our customer support service:

hotline.biometrics@morpho.com

The license is delivered in a file dedicated to only one terminal. Each license file is generated for a unique serial number, and this is checked by the license installation tool, when the license is added to the terminal. The file must not be modified.

Checking licenses installed in the terminal with license manager application

The Terminal Info page of the Webserver or the Information Menu of the terminal (MorphoAccess® SIGMA Lite+) allows to check installed licenses: please refer to **Information Menu > Device section**. Otherwise, to view installed licenses and to add a license from a PC, an Ethernet (or Wi-Fi™) connection and the License Manager application are needed. The application can be downloaded from our biometric terminals website (www.biometric-terminals.com).

Screens & Steps

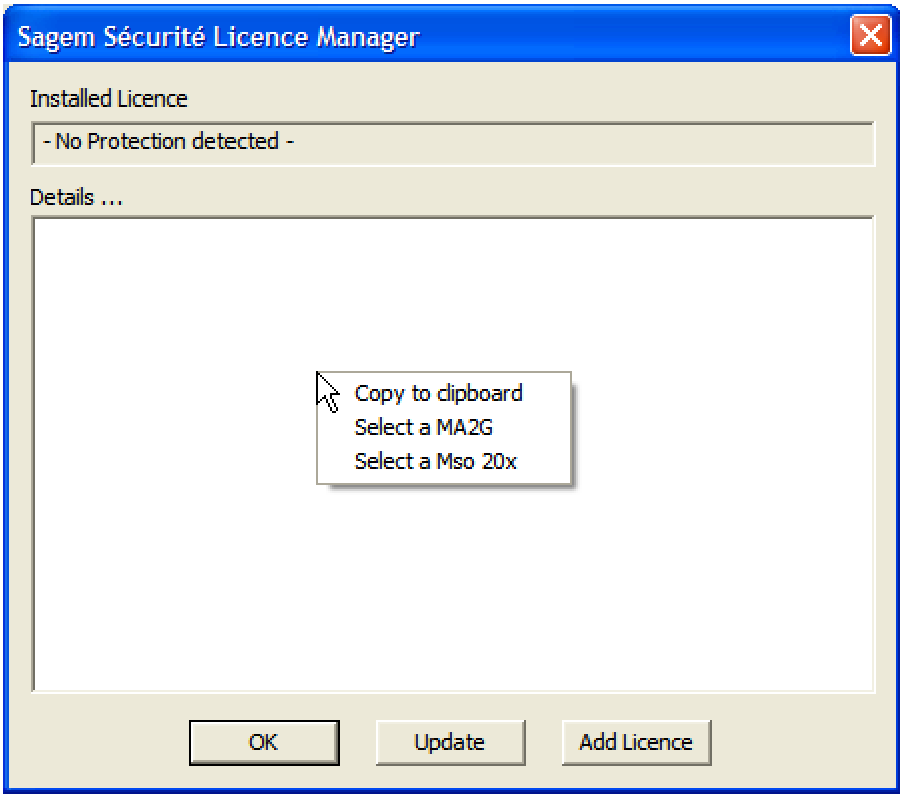


Figure 7: License Manager, adding a MorphoAccess® SIGMA Lite Seriesterminal

1. Launch the License Manager application, right click in the main window and select the “Select a MA2G” operation.

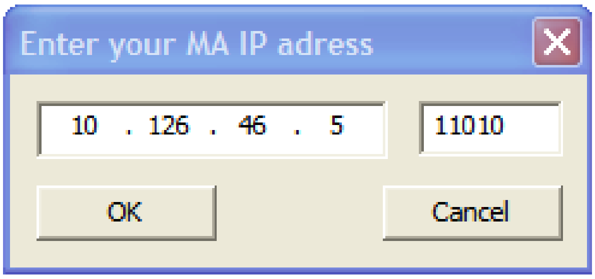
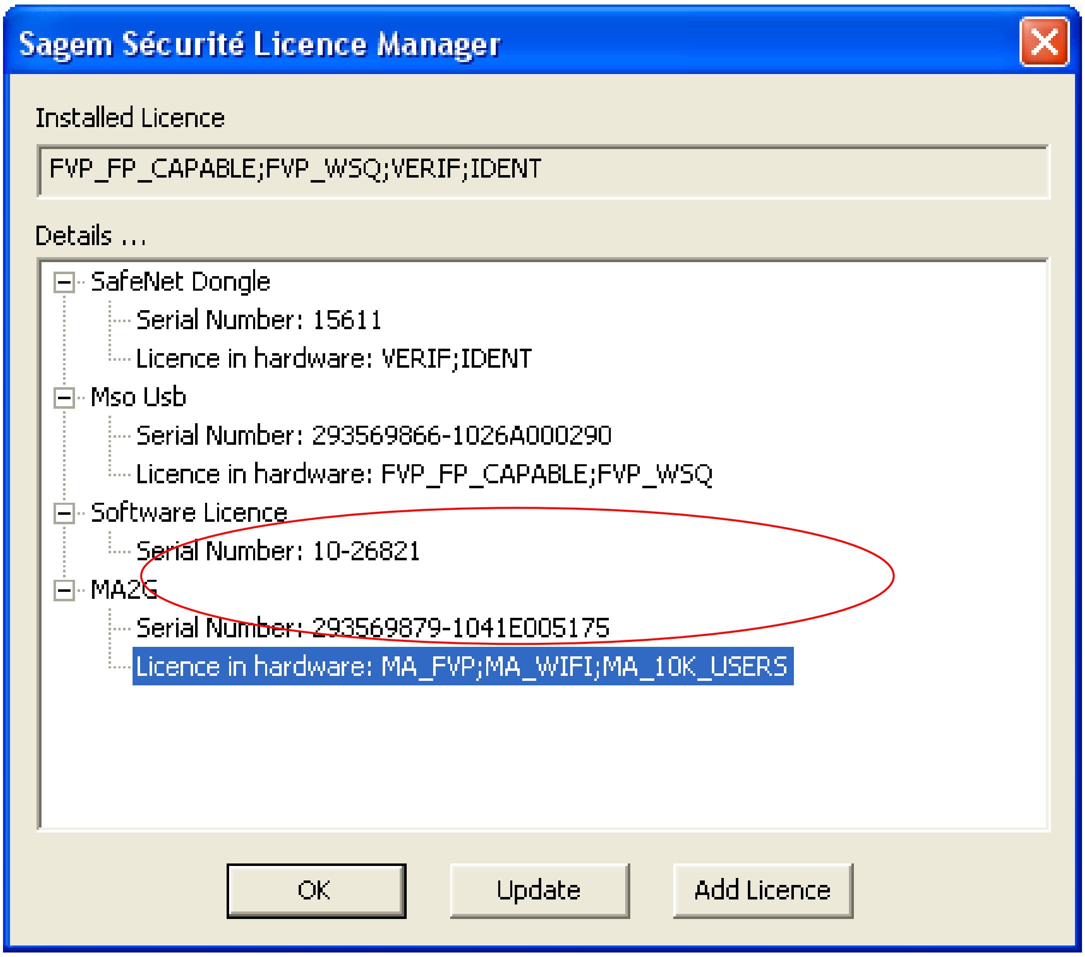


Figure 8: License Manager, entering an IP address for a MorphoAccess® SIGMA Lite Series terminal

2. Enter the IP address of the MorphoAccess® SIGMA Lite Series terminal in the window that opens.



Sagem Sécurité Licence Manager

Installed Licence

FVP_FP_CAPABLE;FVP_WSQ;VERIF;IDENT

Details ...

- SafeNet Dongle
  - Serial Number: 15611
  - Licence in hardware: VERIF;IDENT
- Mso Usb
  - Serial Number: 293569866-1026A000290
  - Licence in hardware: FVP_FP_CAPABLE;FVP_WSQ
- Software Licence
  - Serial Number: 10-26821
- MA2G
  - Serial Number: 293569879-1041E005175
  - Licence in hardware: MA_FVP;MA_WIFI;MA_10K_USERS

Figure 9: Licenses installed in a MorphoAccess® SIGMA Lite Series terminal

3. The licenses on the MorphoAccess® SIGMA Lite Series terminal are listed in the “license in hardware" line in the main window.

For further information concerning the license management tool (License Manager PC tool), please see the document MorphoAccess® SIGMA Lite **Terminal License Management**.

Installing a new license

Proceed as follows to install a new license:

Copy the received license file (.lic extension) on the PC

launch the "License Manager" application then add the MorphoAccess® SIGMA Lite Series terminal IP address as specified in the previous section,

click “Add license”, then “Browse…” to select the license file (.LIC),

a specific window will open to indicate whether or not the license has been loaded successfully,

The main window will then indicate the presence of the new license.

The terminal must be restarted to activate the different functions unlocked by the new license.

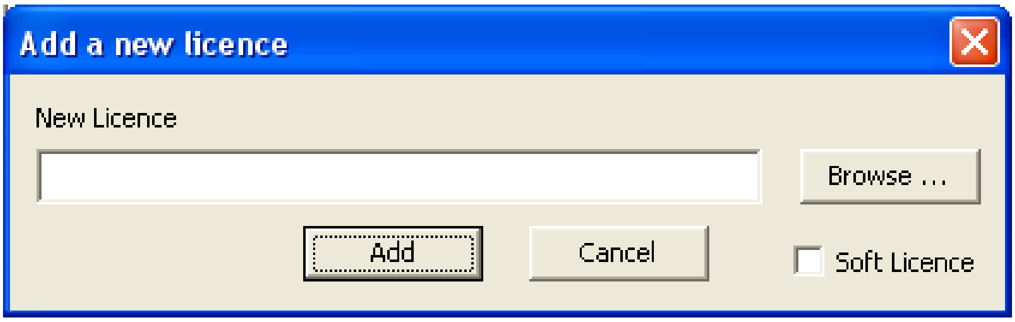


Figure 10: Adding a license in a MorphoAccess® SIGMA Lite Seriesterminal

For further information about the license management tool (License Manager PC tool), please see the **MorphoAccess® SIGMA Lite Series License Management** document.

Terminal Firmware Upgrade

How to get latest version of firmware

The last MorphoAccess® SIGMA Lite Series terminal firmware can be obtained on a CD/ROM package from the customer service, or can be downloaded from Morpho Website dedicated to biometric terminals:

http://www.biometric-terminals.com/

A login name and a password are required to access to the private part which contains the firmware. If you have not yet your login information, please ask for it to our customer service using the mail address below:

hotline.biometrics@morpho.com

How to upgrade the firmware

When required, the MorphoAccess® SIGMA Lite Series terminal firmware can be upgraded from a PC, through an IP link (either Ethernet or Wi-Fi™).

The easiest way to update the firmware is to use MorphoBioToolBox software application.

Find "terminal firmware update" proposed by the interface of the software application, select the file with the new firmware and validate.

Note: Terminal must not be switched off during firmware update. Before starting firmware upgrade please insure that the power supply of terminal will not be interrupted. Otherwise instability can occurs.

Firmware upgrade using a USB Mass Storage Key

It is possible to update the firmware, using a USB mass storage key. This feature is available in the 3 different modes by using MorphoBioToolBox.

Firmware upgrade tool for expert users

MorphoAccess® SIGMA Lite Series Upgrade Tool

A software application is available for expert users. This tool allows expert users to upgrade directly the firmware of a specified MorphoAccess® SIGMA Lite Series terminal.

This tool has no graphic interface: only a command-line interface.

Syntax of the command-line

[-h] [-v] -f *path_to_file* -e *IP_address* [-t *timeout*] [-p *port_number*]

Options	Description
-h	Displays help (this message) and returns without upgrading firmware.
-v	Verbose mode. Optional.
-f path	Path to the binary file used for upgrade. Mandatory.
-e IP_address	IP address of the terminal to upgrade. Mandatory.
-t timeout	Timeout of the connection (in ms). Optional, default and min value is 10s.
-p port_number	TCP port number to use to start upgrade. Optional, default is 11001.

Samples:

Upgrades firmware of terminal at address 192.168.1.2 using file new_firmware.bin

```
-f new_firmware.bin -e 192.168.1.2
```

Upgrades firmware of terminal at address 192.168.1.2 using file new_firmware.bin, with a 15 seconds timeout

```
-f new_firmware.bin -e 192.168.1.2 -t 15000
```

Upgrades firmware of terminal at address 192.168.1.2 using file new_firmware.bin using verbose mode

```
-v -f new_firmware.bin -e 192.168.1.2.
```

Note: If the Ethernet connection is broken during the firmware upgrade process, user can re-plugin the Ethernet cable and re-launch Retrofit Tool with the same command line. The firmware upgrade is restarted and is entirely executed, with restarting of the terminal.

MorphoAccess® SIGMA Lite Series Modes

MorphoAccess® SIGMA Lite Series (also referred as MA5G) terminals are standalone biometric access control terminals which offers advance features for access rights check of the users. MorphoAccess® SIGMA Lite Series terminals are equipped with a facility to emulate (partially) either MorphoAccess® terminal previous generation, or L-1 Bioscrypt 4G Series terminals.

When MorphoAccess® SIGMA Lite Series is set in any of the legacy modes; it supports the database structures and configurations of the selected legacy terminal. Administrator can select the required mode of functioning by selecting it and rebooting the terminal.

MorphoAccess® 500 or J Series legacy mode

MorphoAccess® SIGMA Lite Series terminal can be operated in MA500 mode (also referred as Legacy Morpho). In this mode, the terminal will support configurations and operations of MA500 terminals. Terminal can authenticate users enrolled in the MA500 terminals, using biometric check as well as contactless card. New users can also be enrolled in MA500 mode.

Access Path

USB Script > Legacy Morpho

L-1 Bioscrypt 4G Series legacy mode

MorphoAccess® SIGMA Lite Series terminal can be operated in Bioscrypt 4G mode (also referred as Legacy L1). In this mode, the terminal will support limited operations and configurations that are done using SecureAdmin™ application. The terminal in L1 mode is able to authenticate the users enrolled on 4G terminals and contactless cards. However **User Enrolment** in legacy L1 mode on MorphoAccess® SIGMA Lite Series terminal is possible only when Secure Admin station is equipped with a MorphoSmart™ MSO biometric sensor.

In case, users are enrolled in MA5G mode, the user data cannot be exported when terminal is in L1 mode. There are certain other limitations, when MorphoAccess® SIGMA Lite Series terminal is run in L1 Legacy mode. For details about these limitations, refer to MorphoAccess® SIGMA and Lite Series - L1 Legacy Mode limitations document.

Access Path

USB Script > Legacy L1

MorphoAccess® SIGMA Lite Series native mode

MorphoAccess® SIGMA Lite Series terminal is by default in native mode; this native mode is designed by MA5G, which means MorphoAccess® 5th generation. This mode supports new features and a remote management application called Webserver.

This guide details entire operations that can be performed from Webserver connected to MorphoAccess® SIGMA Lite Series terminal.

Access Path

USB Script > Standard

NOTE: When terminal mode is switched from MA5G to any of the legacy modes, the entire configuration and all databases are erased, except communication links.

The terminal is rebooted on mode change and factory settings are applicable.

Date & Time Configuration

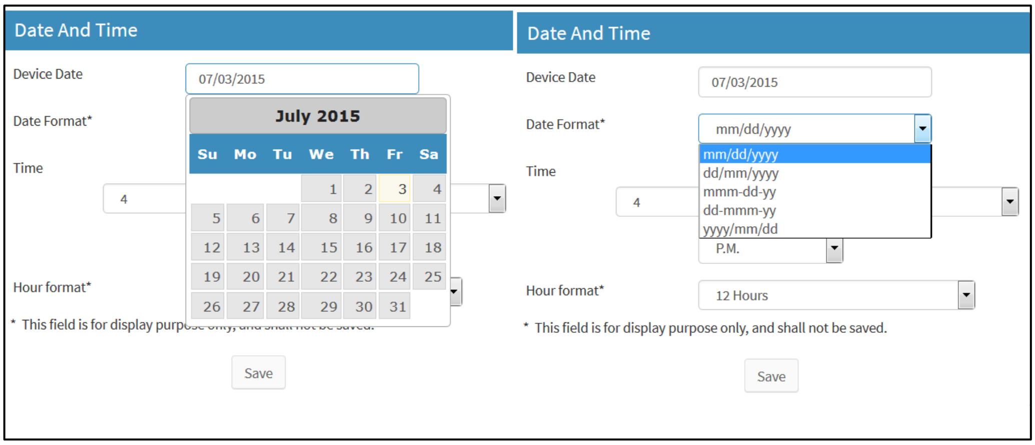
After first bootup of the terminal it is mandatory to set the current date, time and time zone in the terminal.

NOTE: The time stored in the product is not lost if power supply is removed for up to 48 hours.

Access Path

Webserver > Terminal Settings > Date Time Screens & Steps

1. Select **Date Configuration**



Date And Time

Device Date: 07/03/2015

Date Format*

Time: 4

Hour format*

* This field is for display purpose only, and shall not be saved.

Save

July 2015

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Date And Time

Device Date: 07/03/2015

Date Format*: mm/dd/yyyy

Time: 4 P.M.

Hour format*: 12 Hours

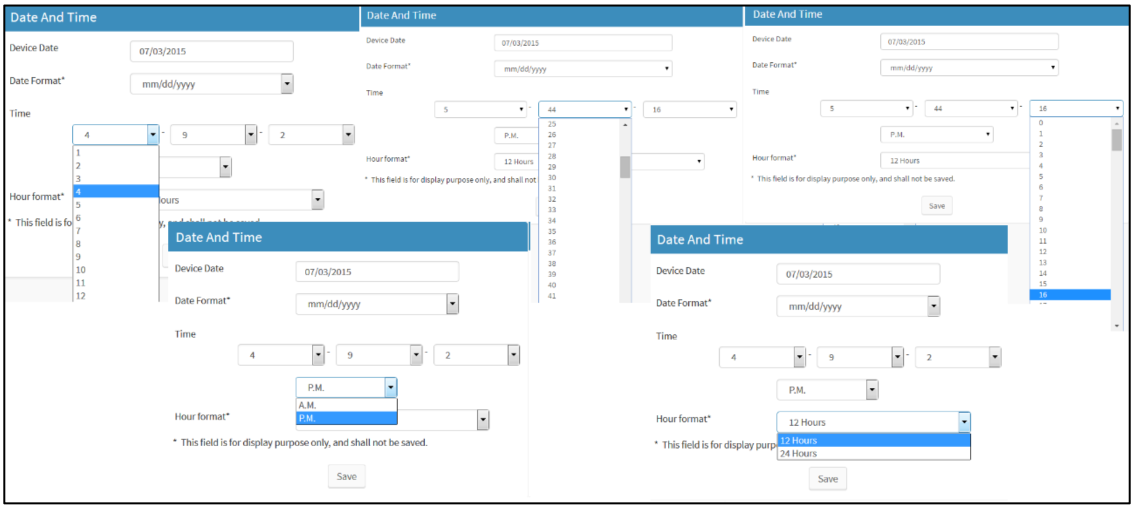
* This field is for display purpose only, and shall not be saved.

Save

Figure 11: Configuring Current Date

2. Select the date to be set on the terminal from the calendar displayed
3. Select **Date Format** in which, the date should be displayed. The available formats are:
    a. MM/DD/YYYY
    b. DD/MM/YYYY
    c. MMM-DD-YY
    d. DD-MMM-YY
    e. YYYY/MM/DD (this format is not available, if terminal is set in L1 mode)
4. Use Check button **SAVE** to save the setting

5. Select **Time Configuration**



Date And Time

Device Date 07/03/2015

Date Format* mm/dd/yyyy

Time 4 : 9 : 2

P.M.

Hour format* 12 Hours

* This field is for display purpose only, and shall not be saved.

Save

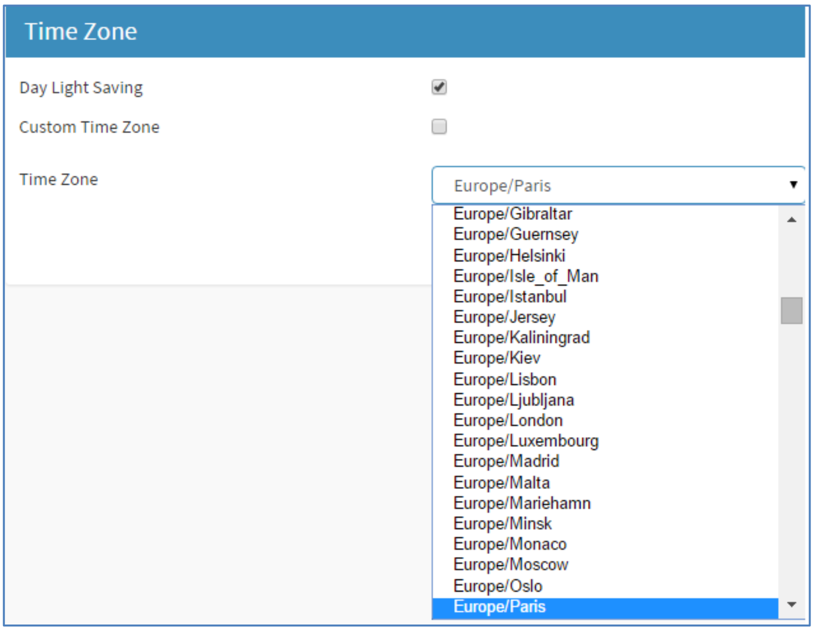
Figure 12: Configuring Current Time

6. Select the current **Hour**, **Minute**, and **Second** from the drop down menu

7. Set **Hour Format** as analogue i.e. ‘12 Hour’ or digital i.e. ‘24 hour’

8. Use Check button **SAVE** to save the setting

9. Select **Time Zone Configuration**



Time Zone

Day Light Saving ☑

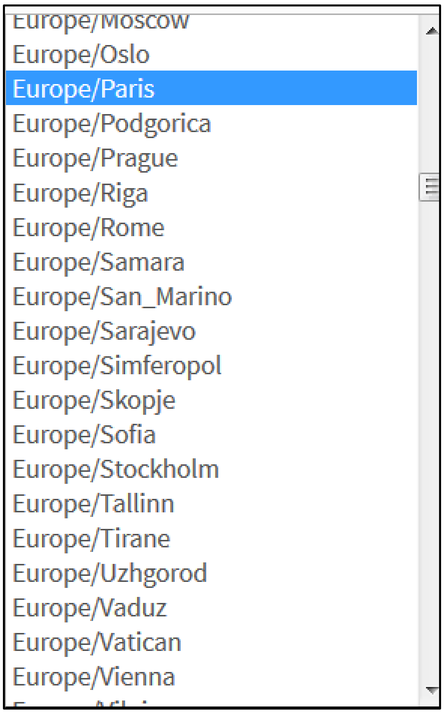
Custom Time Zone ☐

Time Zone Europe/Paris

Figure 13: Configuring Time Zone

10. Select **Observe Daylight Saving** as ‘On’, if an administrator requires to auto-schedule the time during Daylight Saving months. In day light saving mode, the terminal time is auto set to 1 hour ahead of the actual time. E.g. if the current time is 10 am, in day light saving the time is auto-set to 11 am.

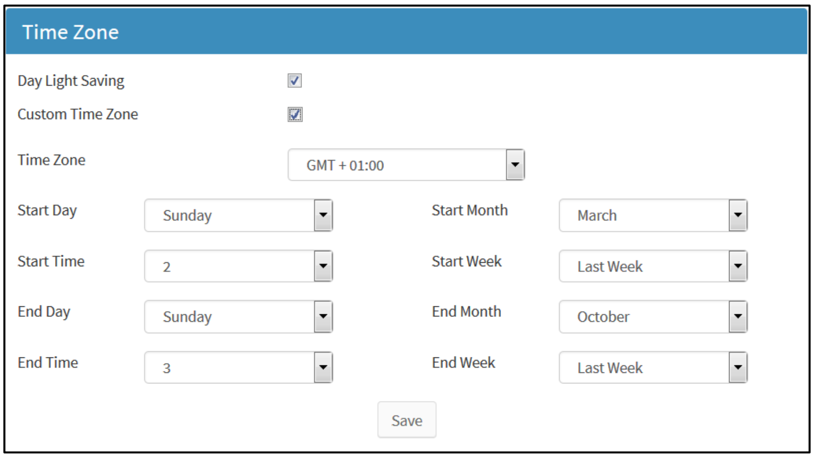
11. Select **Time Zone Type** as 'Predefined' or 'Custom'. If an administrator selects Predefined, the list of Predefined time zones of entire world will be available to select from. And if an administrator select Custom, an administrator can set a customized time zone
12. Use Check button **SAVE** to save the setting
13. Based on the **Time Zone Type**, Time Zone selection parameters are displayed next



Europe/Moscow
Europe/Oslo
Europe/Paris
Europe/Podgorica
Europe/Prague
Europe/Riga
Europe/Rome
Europe/Samara
Europe/San_Marino
Europe/Sarajevo
Europe/Simferopol
Europe/Skopje
Europe/Sofia
Europe/Stockholm
Europe/Tallinn
Europe/Tirane
Europe/Uzhgorod
Europe/Vaduz
Europe/Vatican
Europe/Vienna

Figure 14: List of Predefined Time Zones of World

14. The list of Predefined Time Zones of entire world is displayed
15. Scroll up or down to select required **Time Zone** from the list
16. Use Check button **SAVE** to save the setting



Time Zone

Day Light Saving ☑

Custom Time Zone ☑

Time Zone: GMT + 01:00

Start Day	Sunday	Start Month	March
Start Time	2	Start Week	Last Week
End Day	Sunday	End Month	October
End Time	3	End Week	Last Week

Figure 15: Custom Time Zone Setting

17. If an administrator Select **Time Zone Type** as ‘Custom’, then an administrator need to define below time zone parameters:
18. Select **Time Zone, Start Month**, **Start Week**, **Start Day**, **Start Time**, **End Month**, **End Week**, **End Day** and **End**
19. Use Check button **SAVE** to save the setting

NOTE: While setting custom time zone, make sure the GMT offset to be set is the 'Standard GMT Offset' of the region.

Trigger Event

MorphoAccess® SIGMA Lite Series terminal is able to start access rights check when a specific trigger event occurs on terminal. Using this configuration an administrator can set on which events the terminal should perform operations. Below is the list of events available:

Biometric, a finger is detected on the biometric sensor (which starts biometric identification process)

Contactless card, a contactless card is detected, which starts authentication process using user's data found on a contactless card

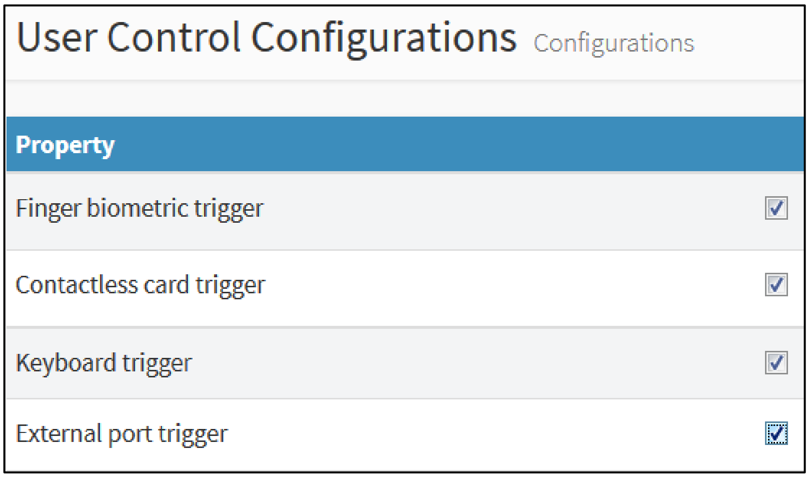
Keypad, a User ID is entered with the keypad

External Port, a User ID is received on Wiegand or Clock and Data input port

Access Path

Webserver > Control Configuration > User Control

Screens & Steps



User Control Configurations Configurations

Property	
Finger biometric trigger	☑
Contactless card trigger	☑
Keyboard trigger	☑
External port trigger	☑

Figure 16: Selecting the event(s) that starts access control rights check process

20. Select the above stated events as ON or OFF
21. Use Check button **SAVE** to save settings

Ethernet Interface Settings

MorphoAccess® SIGMA Lite Series terminal can be connected to management and/or enrolment stations and door panels via **Ethernet channel.** Using Ethernet connection, the terminal can make access request to the access controller and receive result message.

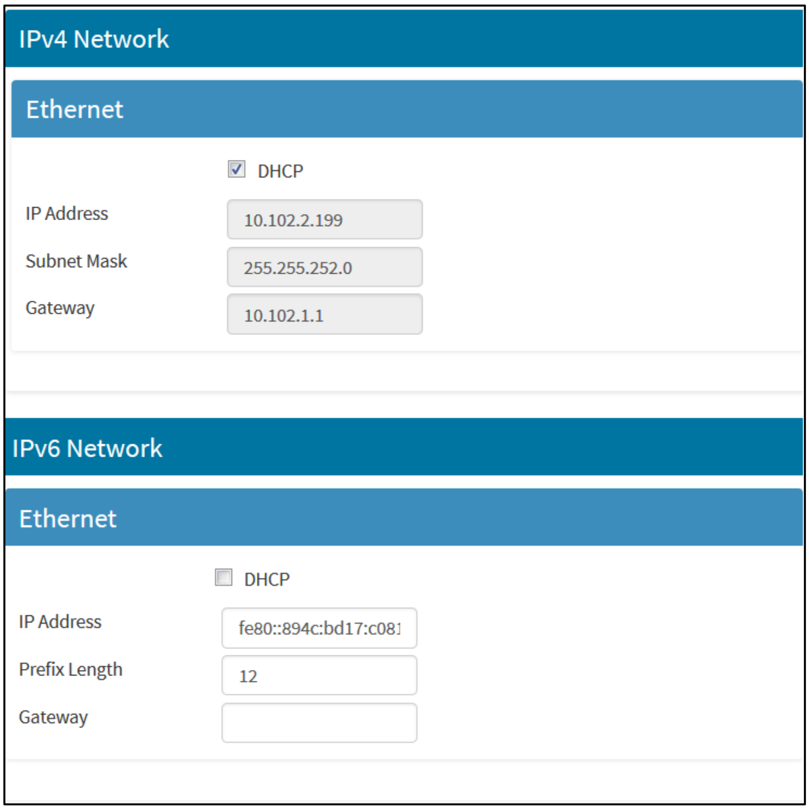
After the First Bootup of the terminal, an administrator can configure the terminal to communicate through Ethernet channel. An administrator can set the IP attribution protocol as DHCP or Static, which is used to assign an IP address to the terminal.

When IP mode is **Static**, the IP Address of the terminal is allocated manually

When IP mode is **DHCP** (Dynamic), the IP Address of the terminal is automatically set and is changed. By default, IP Mode is selected as DHCP

Access Path

Webserver > Terminal Settings > Communication Screens & Steps



IPv4 Network

Ethernet

☑ DHCP

IP Address: 10.102.2.199

Subnet Mask: 255.255.252.0

Gateway: 10.102.1.1

IPv6 Network

Ethernet

☐ DHCP

IP Address: fe80::894c:bd17:c081

Prefix Length: 12

Gateway:

Figure 17: Ethernet Configuration

1. Under Ethernet, an administrator can select **IPV4** or **IPV6**
2. An administrator can select **IP Mode** as ‘Static’ or ‘DHCP’
3. Use **Save** button to save the setting

USB Scripts

MorphoAccess® SIGMA Lite Series terminal can be configured using USB scripts. These scripts can be created from MBTB.

From MBTB, user can create script for:

- Get/Set IP Configuration
- Get/Set Wi-Fi Configuration
- Firmware Upgrade
- Error Log Configuration
- Retrieve Error Log
- Reset Configuration
- SSL Configuration
- Protocol Switch

Access Path

Login to MBTB > Device Settings > USB Scripts

Pre-requisites

USB Drive

Wi-Fi™ Configuration

MorphoAccess® SIGMA Lite Series terminal can be connected to other servers and door panels via **WLAN (Wi-Fi™ network).** Using Wi-Fi™ connection, the terminal can make access request to the access controller and receive result message.

Automatic: The available networks are listed automatically. An administrator can select the network and connect by entering encryption key

Manual: The manual configuration is useful to connect with a hidden Wi-Fi™ network. An administrator can manually configure the WLAN, by entering SSID, Encryption Mode and Encryption Key.

Access Path

Webserver > Terminal Settings > Communication

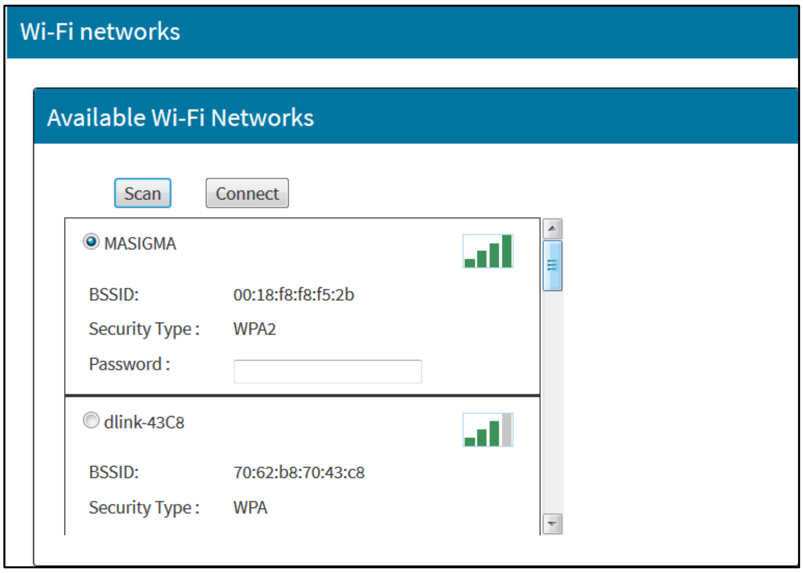
Pre-requisites

Wi-Fi™ USB dongle should be plugged

MA_WI-FI™ license should be installed on terminal

Screens & Steps

Automatic Configuration



Wi-Fi networks

Available Wi-Fi Networks

● MASIGMA

BSSID: 00:18:f8:f8:f5:2b

Security Type : WPA2

Password :

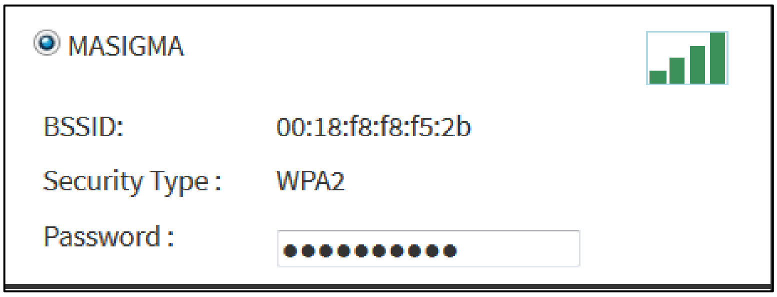
○ dlink-43C8

BSSID: 70:62:b8:70:43:c8

Security Type : WPA

Figure 18: Selecting available Wi-Fi™ network

1. Select from the list of scanned Wi-Fi™ networks



○ MASIGMA

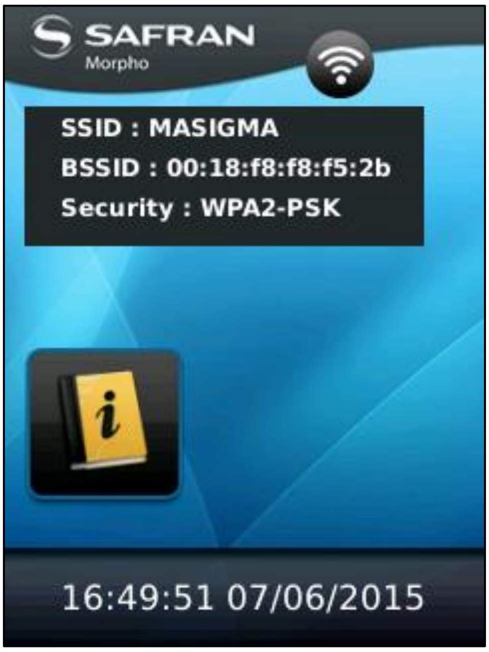
BSSID: 00:18:f8:f8:f5:2b

Security Type : WPA2

Password : ●●●●●●●●●●

Figure 19: Enter Encryption Key

2. Enter an **Encryption Key** to connect to the selected Wi-Fi™ network



SSID : MASIGMA

BSSID : 00:18:f8:f8:f5:2b

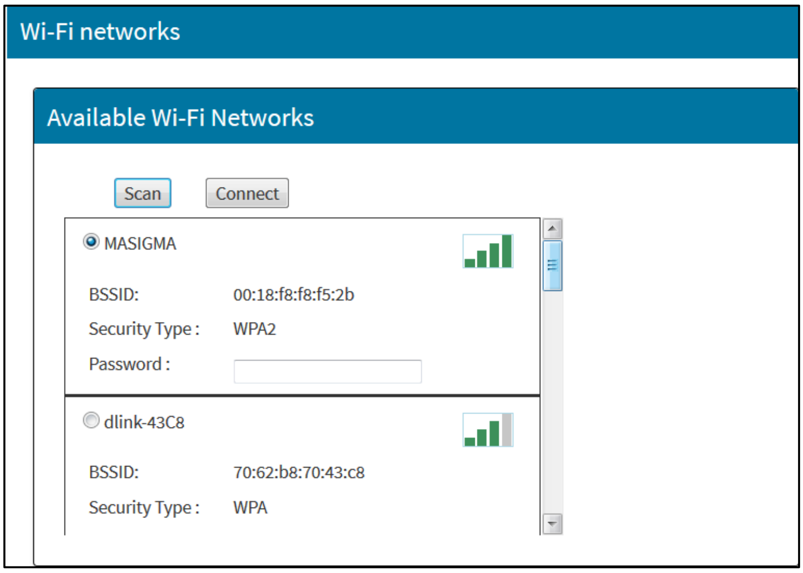
Security : WPA2-PSK

16:49:51 07/06/2015

Figure 20: Connected to Wi-Fi™ network

Manual Configuration

1. Select **WLAN Configuration** to set up Wi-Fi™ Network



Wi-Fi networks

Available Wi-Fi Networks

● MASIGMA

BSSID: 00:18:f8:f8:f5:2b

Security Type : WPA2

Password :

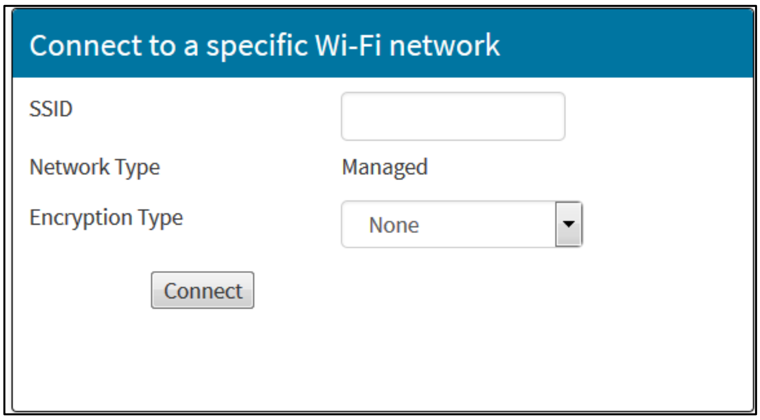
○ dlink-43C8

BSSID: 70:62:b8:70:43:c8

Security Type : WPA

Figure 21: Selecting Other Network to set up Wi-Fi™ network manually

2. The list of available Wi-Fi™ networks will be displayed. Select **Other Network** to set up Wi-Fi™ network manually



Connect to a specific Wi-Fi network

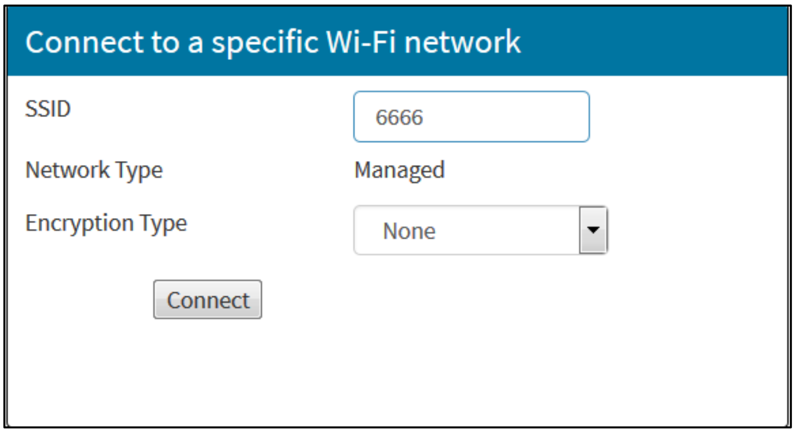
SSID

Network Type Managed

Encryption Type None

Figure 22: WLAN Parameter Configuration

3. Under WLAN configuration, an administrator need to configure **SSID**, **Encryption Mode** and **Encryption Key** provided by the Wi-Fi™ network provider



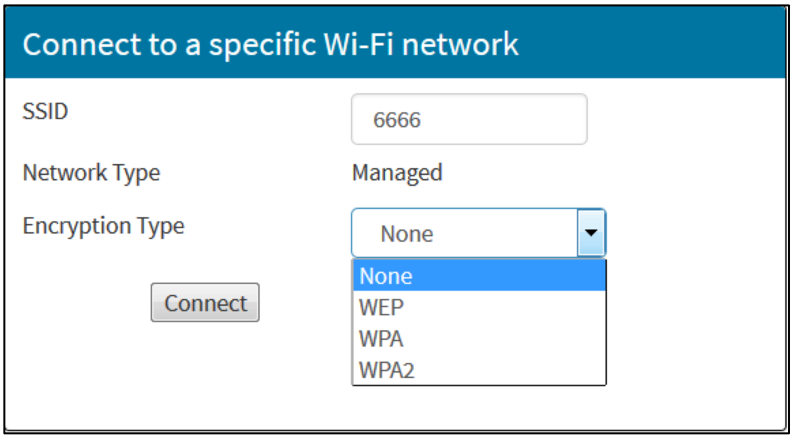
Connect to a specific Wi-Fi network

SSID: 6666

Network Type: Managed

Encryption Type: None

Figure 23: Setting SSID



Connect to a specific Wi-Fi network

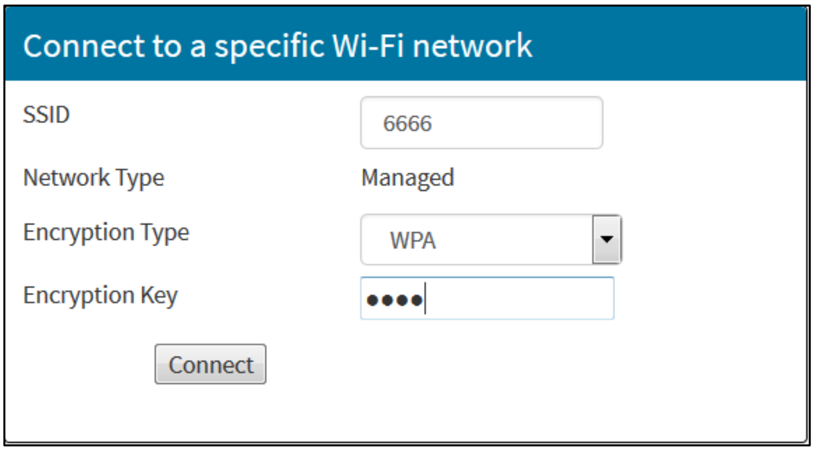
SSID: 6666

Network Type: Managed

Encryption Type: None

Figure 24: Selecting Encryption Mode

4. Select the **Encryption Mode**, as supported by an administrator Wi-Fi™ Router. Encryption mode is selected for Wi-Fi™ security, to prevent from unauthorized access. The available Encryption modes are:
    a. Open (no encryption)
    b. WEP
    c. WPA
    d. WPA2

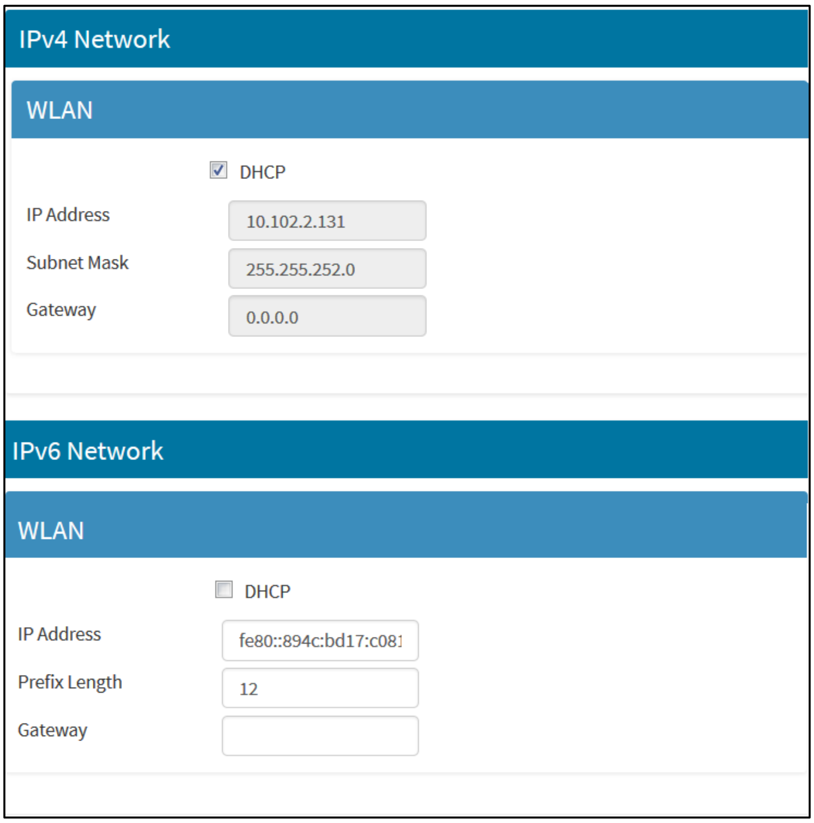


Connect to a specific Wi-Fi network

SSID	6666
Network Type	Managed
Encryption Type	WPA
Encryption Key	●●●●

Figure 25: Define Encryption Key

5. Enter Encryption Key to connect to Wi-Fi™. Only by entering Encryption Key, the Wi-Fi™ network can be accessed
6. Use Check button **CONNECT** to connect to the Wi- Fi™ and click on save button to save the setting



IPv4 Network

WLAN

☑ DHCP

IP Address	10.102.2.131
Subnet Mask	255.255.252.0
Gateway	0.0.0.0

IPv6 Network

WLAN

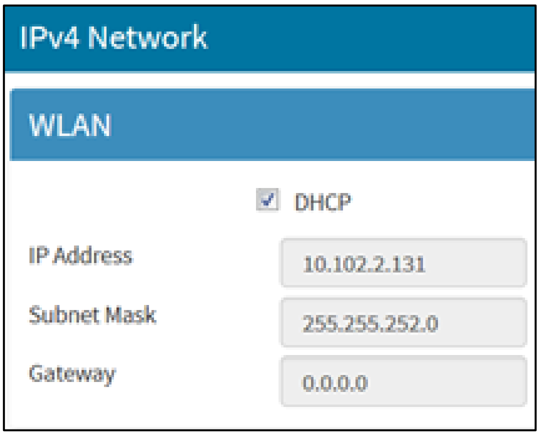
☐ DHCP

IP Address	fe80::894c:bd17:c081
Prefix Length	12
Gateway	

Figure 26: Entering in WLAN – IP Configuration

7. On WLAN screen select “IP Configuration” to set up the server IP which is required to be connected through WLAN

8. Select **IPV 4** or **IPV 6**



IPv4 Network

WLAN

☑ DHCP

IP Address 10.102.2.131

Subnet Mask 255.255.252.0

Gateway 0.0.0.0

Figure 27: WLAN – IP Configuration

9. An administrator can select **IP Mode** as ‘Static’ or ‘DHCP’
    a. If IP Mode is ‘Static’, then enter parameters such as IP Address, Subnet Mask, Gateway Address, Preferred DNS Address and Alternate DNS Address
    b. If IP Mode is ‘DHCP’, then IP address is allocated automatically to the terminal
10. Use **Save** button to save the setting

Protocol Configuration

Using Protocol Configuration an administrator can set terminal mode as

Legacy L1 i.e. Bioscrypt 4G Series Legacy Mode terminals

Legacy Morpho i.e. MorphoAccess® 500 or J Series legacy mode

MA5G i.e. MorphoAccess® SIGMA Lite Series native mode

If an administrator set terminals in legacy mode, it will support the legacy terminal's features and database.

Refer to MorphoAccess® Sigma Lite Series Modes for detailed explanation on supported modes.

Access Path

USB Script > Protocol Configuration

Steps & Results

The required Protocol script is copied to the USB and connected to the terminal through the USB connector. Once the script is run, the protocol selected is saved. The terminal will be required to reboot, in order to use the terminal in any of the legacy modes. When one protocol is switched to another, MorphoAccess® SIGMA Lite Series terminal will erase entire configuration and user database; except communication links.

Password Configuration

This function is used to modify terminal's default login password. An administrator can use the password to access web-server and perform required configuration & operations. In order to prevent any unauthorized access to the web-server, it is recommended to change the default login password of web-server.

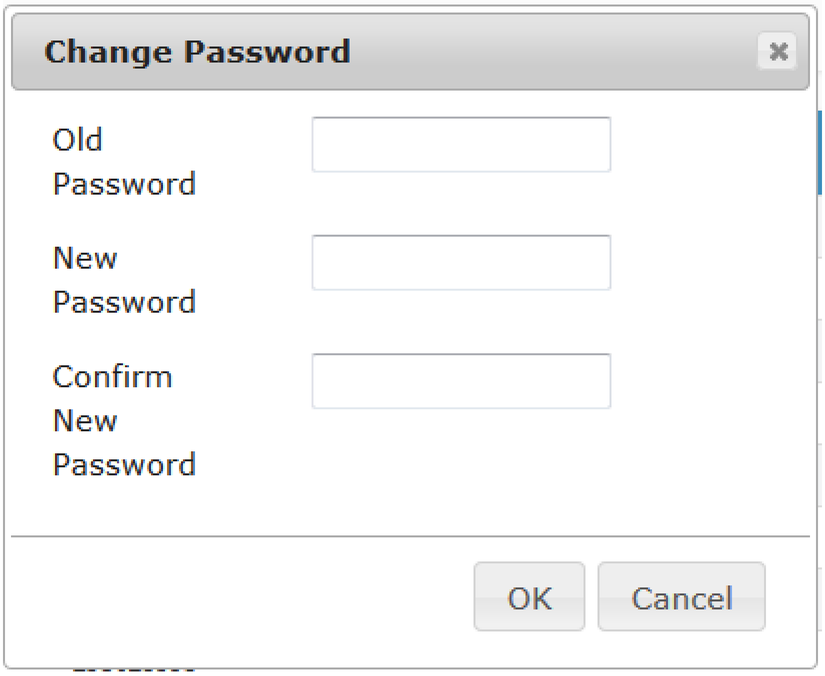
The login password should be changed periodically to ensure better security. The administrator can change password anytime from "Web Server".

The password is a numeric value with 4 digits minimum and 8 digits maximum.

Access Path

Welcome Admin > Change Password

Screens & Steps



Change Password

Old Password

New Password

Confirm New Password

Figure 28: Change Device Password

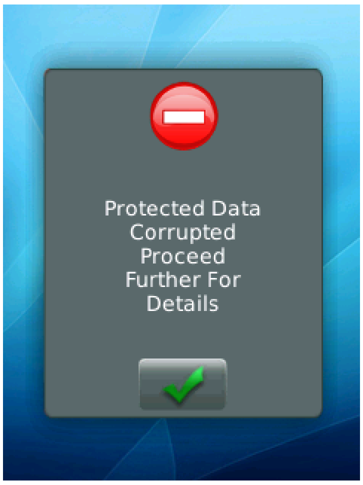
1. Enter **Old Password, New Password and Confirm New Password.**
    a. Default password is set as "12345"
2. Click on **OK** to change.

Results

The terminal administration menu is accessible only using a valid new password.

Recover Corrupted Components

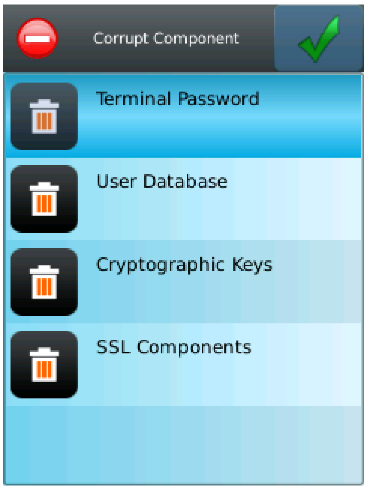
There is a system within the terminal to recover corrupted secure container components like Smartcard Keys, Terminal Password, SSL Certificate and User Database. Due to problem in power failure or interrupt in operation causes the corruption. When booting up device if there is any corruption found in secure container component, terminal will display following screen in MorphoAccess® SIGMA Lite Series terminal.



Protected Data Corrupted Proceed Further For Details

Figure 29: Protected Data Corrupted Error

And on clicking on "✓" terminal lists all corrupted component as below.



Corrupt Component

Terminal Password

User Database

Cryptographic Keys

SSL Components

Figure 30: List Of Corrupted Components

Once user selects "✓", corrupted component recovers to default state after terminal Reboot.

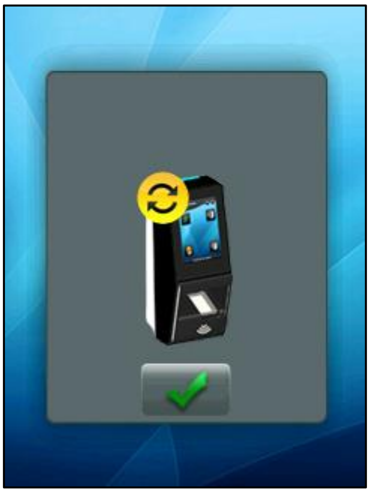


Figure 31: Reboot Terminal

Section 4 : **Administration Menu through Webserver**

Access to Administration Menu through Webserver

An administrator can login to MorphoAccess® SIGMA Lite Series terminal through Webserver using the default password. The Webserver allows user to perform various actions and configurations on terminal, through below listed menus:

User Management Menu: For enrolling and managing users

Terminal Info Menu: Used for viewing information of terminal

Reboot Product: Allows an administrator to reboot terminal

Logs Menu: Used for retrieving transaction logs, configure transaction and debug logs

Schedules Menu: Used to add/edit/delete user defined Access Schedules, Holiday Schedules and Door Open Schedules

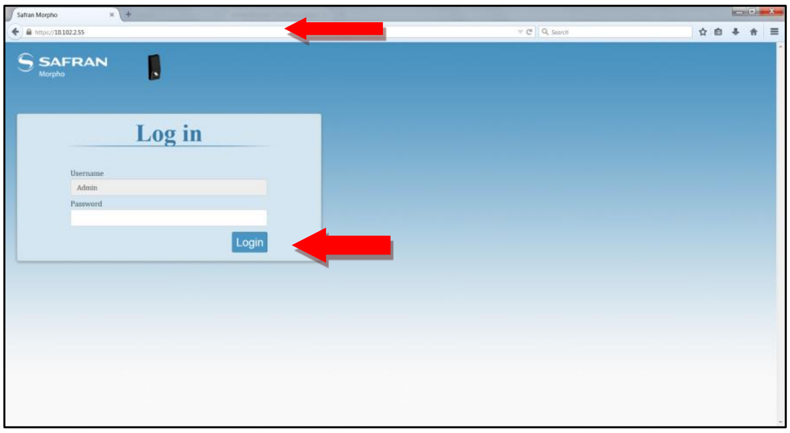
Control Configuration Menu: Used to configure the Controller (Panel) Feedback, User Control Parameters, Events and Contactless Card parameters

Terminal Settings Menu: Used to configure the Biometric, Communication, Wiegand, Threat Level, GPIO, SDAC and Terminal Date and Time

Reset Default Menu: Used to reset all/any parameter to factory default values

Complete Configuration Menu: Used to configure any parameter to access the terminal

Screens & Steps



Username
Admin
Password

Figure 32: Logging in Webserver

1. Enter the password

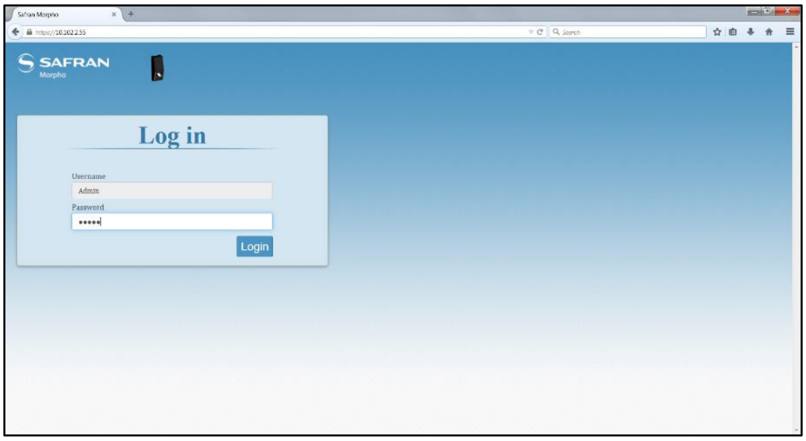
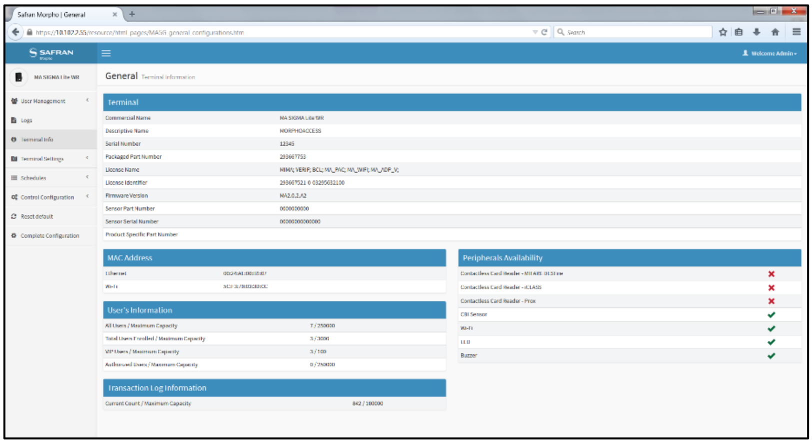


Figure 33: Entering Password

2. Enter **Password** and Press on **Login** to save password



Terminal	
Commercial Name	MA SIGMA Lite WR
Descriptive Name	MORPHOACCESS
Serial Number	12345
Packaged Part Number	293667753
License Name	MIMA; VERIF; BCL; MA_PAC; MA_WIFI; MA_ADP_V;
License Identifier	293667521 0 03295632100
Firmware Version	MA2.0.2.A2
Sensor Part Number	0000000000
Sensor Serial Number	00000000000000
Product Specific Part Number	

MAC Address	
Ethernet	[illegible]
Wi-Fi	[illegible]

User's Information	
All Users / Maximum Capacity	7 / 250000
Total Users Enrolled / Maximum Capacity	3 / 3000
VIP Users / Maximum Capacity	3 / 100
Authorised Users / Maximum Capacity	0 / 250000

Transaction Log Information	
Current Count / Maximum Capacity	842 / 100000

Peripherals Availability	
Contactless Card Reader - MIFARE DESFire	✗
Contactless Card Reader - iCLASS	✗
Contactless Card Reader - Prox	✗
CBI Sensor	✓
Wi-Fi	✓
LED	✓
Buzzer	✓

Figure 34: Administrator Menu

3. On successful login, an administrator menu is displayed, with various menus

User Menu

User menu offers all functions related to the end users. An administrator can enroll new user in the system, edit user information, delete users from the terminal database, and reset user information from contactless smart cards.

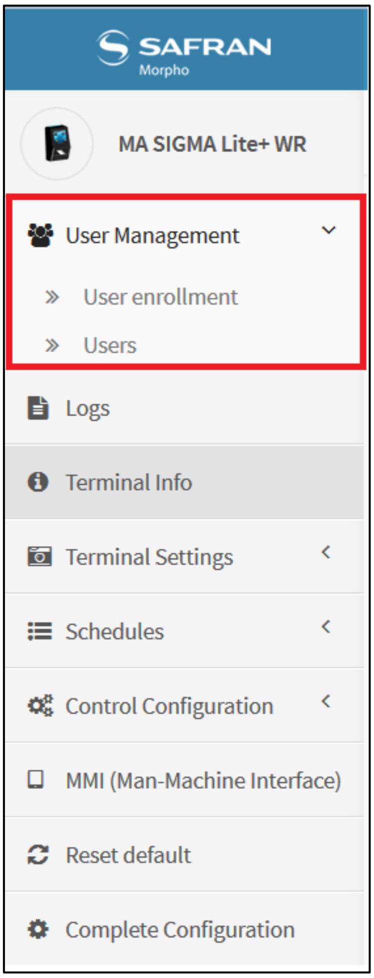


Figure 35: User Management Menu – Webserver

User Enrollment in Database

This feature of MorphoAccess® SIGMA Lite Series terminal allows an administrator to enroll new users in the terminal. The user information such as name, biometric data (i.e. fingerprint); User ID and PIN, access rights, etc. are entered and stored in the terminal database.

Terminal will allow access to the user by comparing the data provided by the user at access request, against the data provided by the user at the time of enrollment.

Access Path

User Management > User Enrollment > Enrollment mode > DB Only

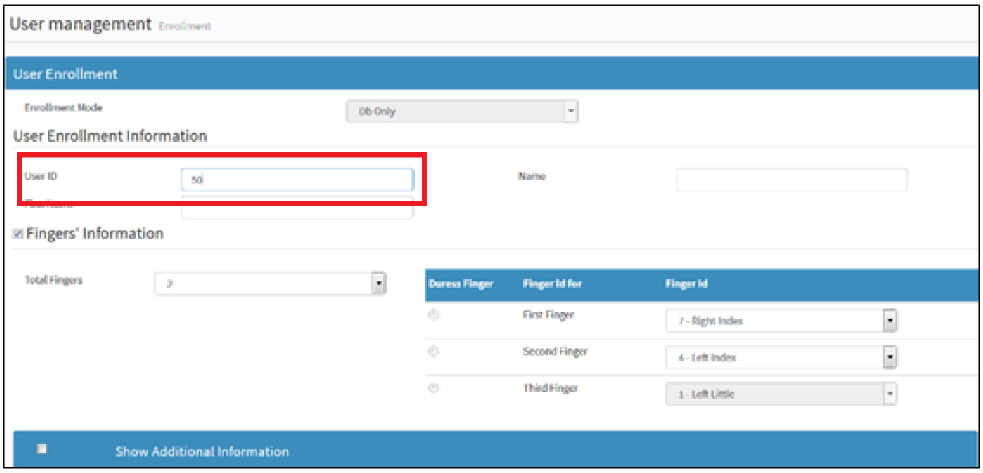
Pre-requisites

An Administrator can enroll new users

If terminal is in Legacy L1 mode, then enrolment of users can be done only if Secure Admin station is equipped with a MorphoSmart™ MSO biometric sensor

The data of the users enrolled in MA5G mode cannot be exported in L1 systems

Screens & Steps



User management Enrollment

User Enrollment

Enrollment Mode: Db Only

User Enrollment Information

User ID: 50

Name:

☑ Fingers' Information

Total Fingers: 2

Duress Finger	Finger Id for	Finger Id
○	First Finger	7 - Right Index
○	Second Finger	4 - Left Index
○	Third Finger	1 - Left Little

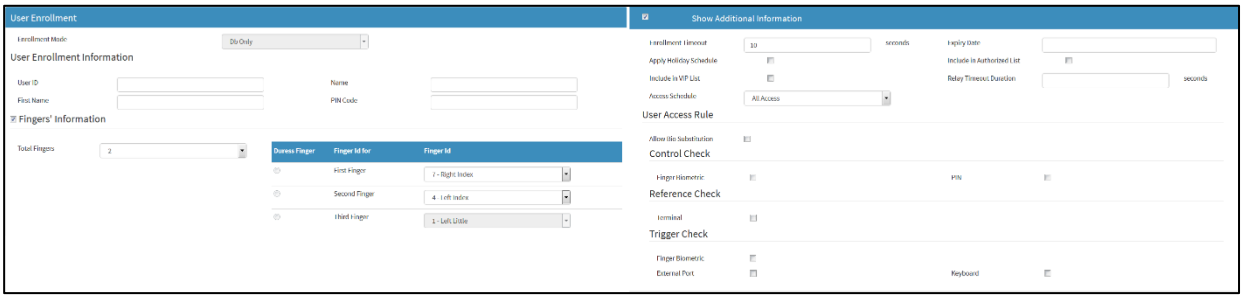
□ Show Additional Information

Figure 36: Entering User Identifier

1. Enter **User Identifier (User ID)**. Numeric value up to 24 digits.

NOTE: Wiegand protocol for User ID doesn't support special characters such as "*" and "#", then is not recommended to insert these characters in the User ID value.

NOTE: There is a configuration key, **misc.user_id_edit**, to make user ID field read only. With this parameter, the user id can be extracted from the Smartcard and restrict user to edit this field. **misc.user_id_edit** is accessible from PC application or Web Server**.**



User Enrollment

Enrollment Mode: Db Only

User Enrollment Information

User ID:

Name:

First Name:

PIN Code:

☑ Fingers' Information

Total Fingers: 2

Duress Finger	Finger Id for	Finger Id
○	First Finger	7 - Right Index
○	Second Finger	4 - Left Index
○	Third Finger	1 - Left Little

☑ Show Additional Information

Enrollment Timeout: 10 seconds

Expiry Date:

Apply Holiday Schedule: □

Include in Authorized List: □

Include in VIP List: □

Relay Timeout Duration: seconds

Access Schedule: All Access

User Access Rule

Allow Bio Substitution: □

Control Check

Finger Biometric: □ PIN: □

Reference Check

Terminal: □

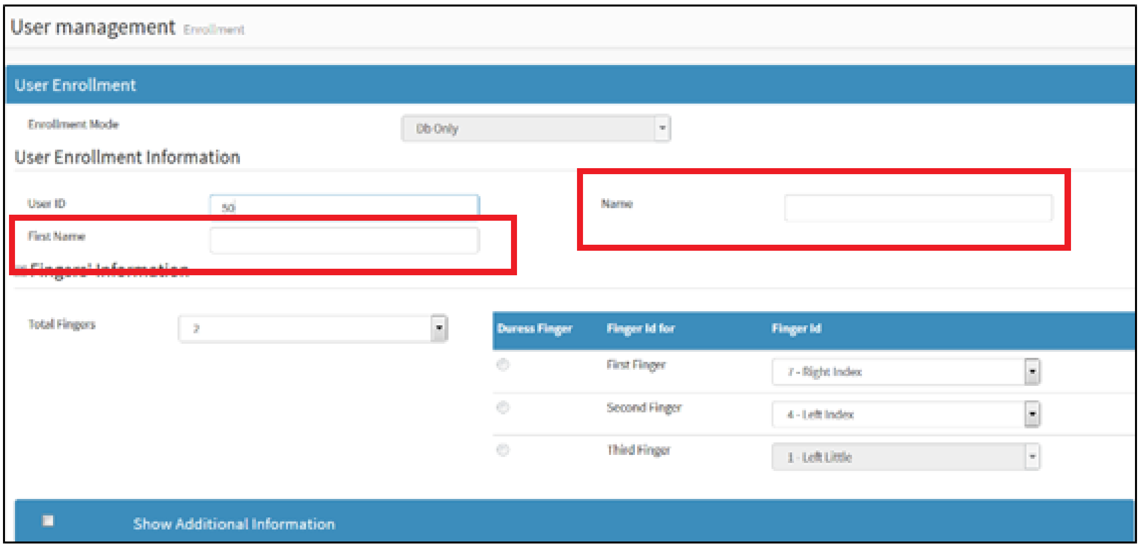
Trigger Check

Finger Biometric: □

External Port: □ Keyboard: □

Figure 37: Adding user information

2. Under **Enrolment Information** screen, an administrator need to enter several parameters:



User management Enrollment

User Enrollment

Enrollment Mode: Db Only

User Enrollment Information

User ID: 50

Name:

First Name:

Fingers' Information

Total Fingers: 2

Duress Finger	Finger Id for	Finger Id
○	First Finger	7 - Right Index
○	Second Finger	4 - Left Index
○	Third Finger	1 - Left Little

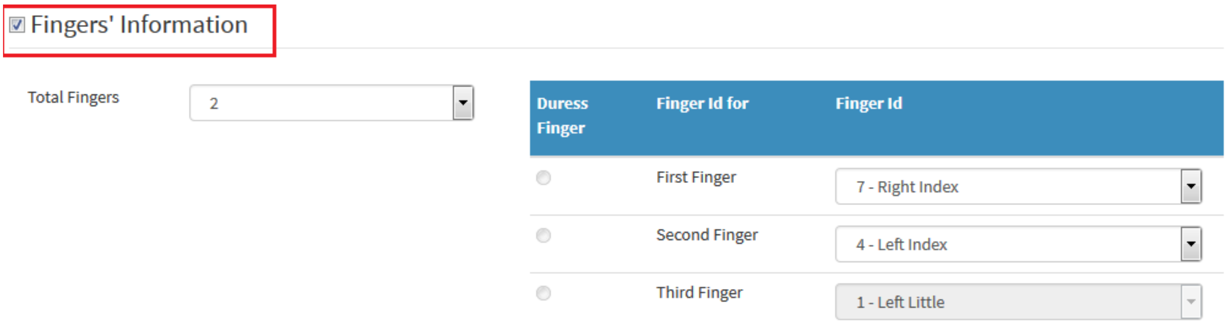
□ Show Additional Information

Figure 38: Enter First Name of User

3. Enter the **First Name** of user

4. Similarly, Enter **Last Name** of user

5. Select the Finger Index of First and Second Finger to enroll fingerprints of the user



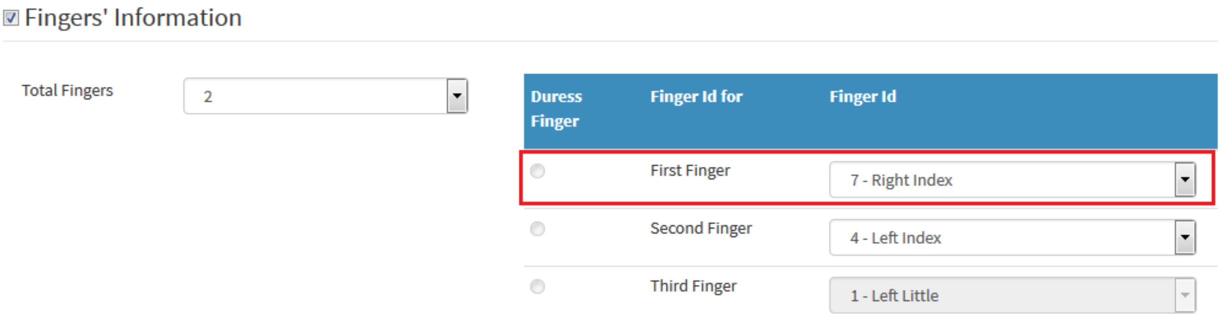
☑ Fingers' Information

Total Fingers: 2

Duress Finger	Finger Id for	Finger Id
○	First Finger	7 - Right Index
○	Second Finger	4 - Left Index
○	Third Finger	1 - Left Little

Figure 39: Enrolling Finger Index

6. A user is required to provide the biometric data of at least two different fingers. Select first finger for biometric data capture



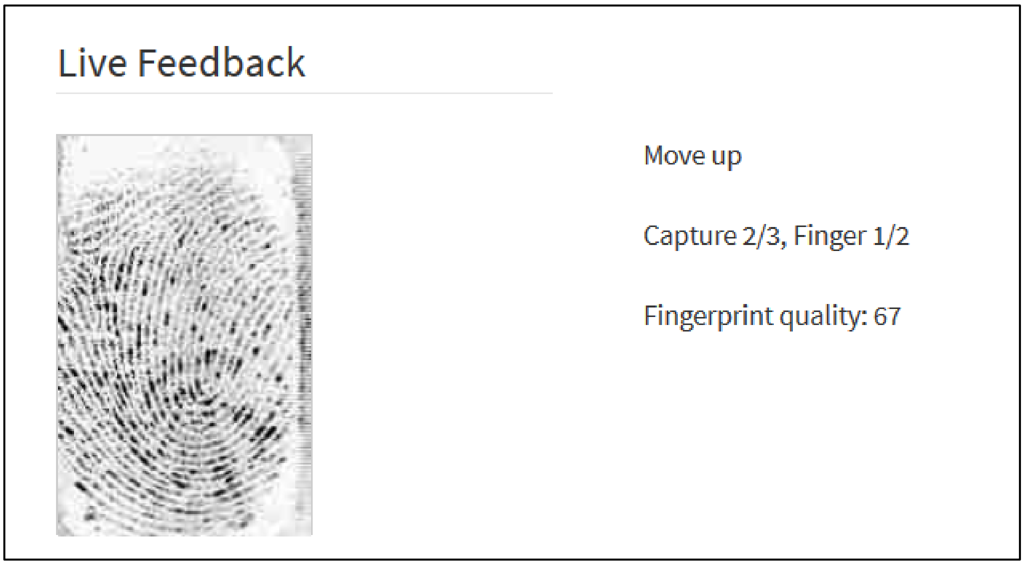
☑ Fingers' Information

Total Fingers: 2

Duress Finger	Finger Id for	Finger Id
○	First Finger	7 - Right Index
○	Second Finger	4 - Left Index
○	Third Finger	1 - Left Little

Figure 40: Select first finger to capture

7. Select second finger for biometric data capture



Live Feedback

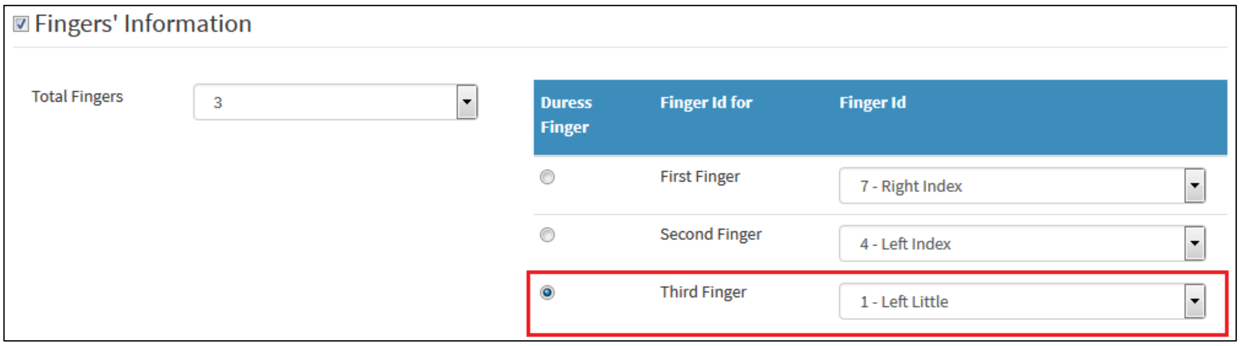
Move up

Capture 2/3, Finger 1/2

Fingerprint quality: 67

Figure 41: Biometric data capture

8. Place the finger on **biometric Sensor**. If the finger is not placed properly or within the time limit, an error message is displayed. Refer to "*Finger Placement Recommendation*" section to know the correct position of finger.
9. Three Fingerprints are captured of the same user and the best quality image is auto-selected by the terminal
10. Once one fingerprint is stored, the administrator will need to capture the user's second fingerprint. Repeat steps 8 and 9 for enrolling finger 2



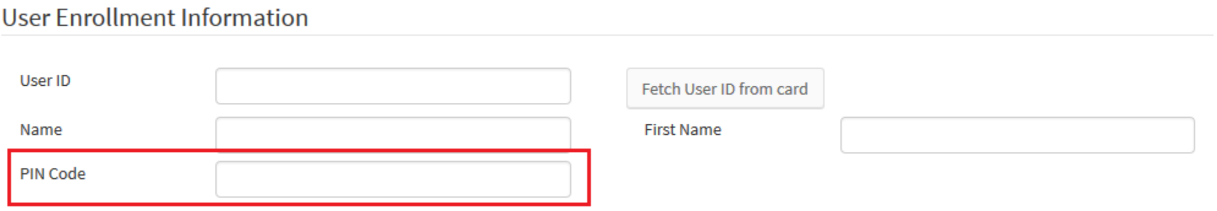
☑ Fingers' Information

Total Fingers: 3

Duress Finger	Finger Id for	Finger Id
○	First Finger	7 - Right Index
○	Second Finger	4 - Left Index
●	Third Finger	1 - Left Little

Figure 42: Set Duress Finger as ON

11. If the administrator wants to capture Duress Finger, the Total Fingers to enroll should be set as '3'
12. Repeat steps 8 and 9 to enroll the duress finger.



User Enrollment Information

User ID

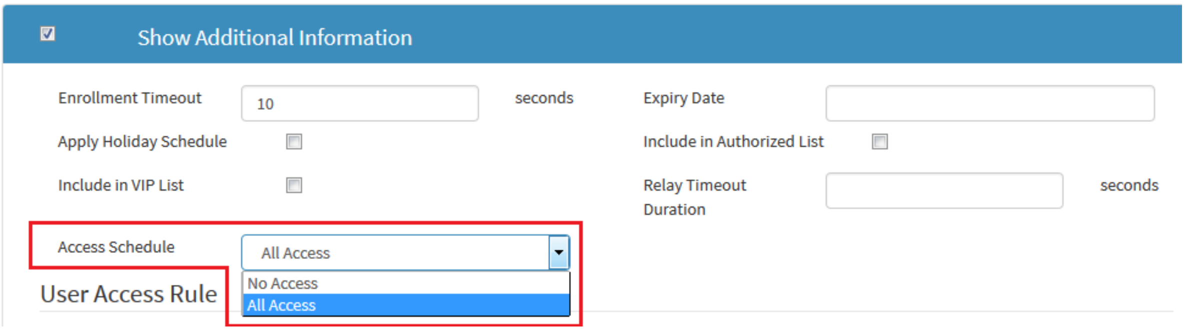
Name

PIN Code

First Name

Figure 43: Enter User PIN

13. Enter **User PIN** which should be of up to 15 digits alphanumeric. This PIN can be used by user, when PIN based authentication mode is enabled. The user will be required to enter PIN, for authentication.



☑ Show Additional Information

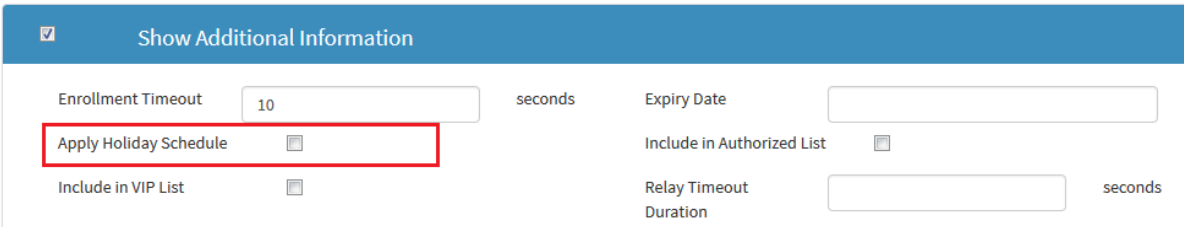
Enrollment Timeout: 10 seconds
Expiry Date:
Apply Holiday Schedule: □
Include in Authorized List: □
Include in VIP List: □
Relay Timeout Duration: seconds
Access Schedule: All Access
No Access
All Access

User Access Rule

Figure 44: Assigning Access Schedule

14. Select an **Access Schedule**, if the access is allowed within particular hours of the day. By default, the access schedule is selected as Schedule 63 that means access allowed at any time of the day.

    NOTE: Refer to *Define Access Schedule* under Configuration through Webserver section to know more about access schedule.



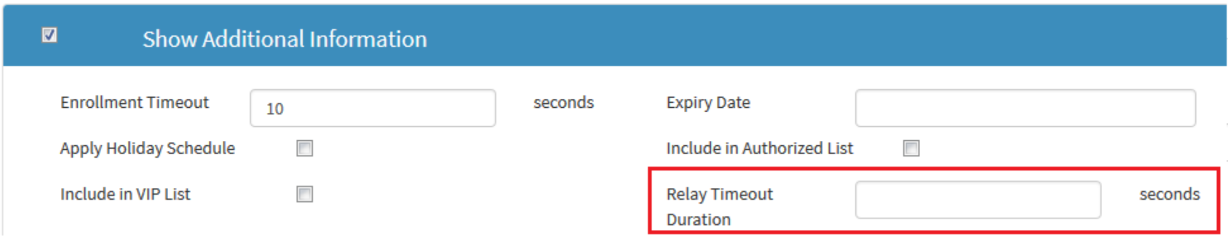
☑ Show Additional Information

Enrollment Timeout: 10 seconds
Expiry Date:
Apply Holiday Schedule: □
Include in Authorized List: □
Include in VIP List: □
Relay Timeout Duration: seconds

Figure 45: Enrolment Information Screen – Configuring parameters

15. Configure **Observe Holiday Schedule** by enabling or disabling. If this parameter is enabled, then access on holiday will be provided as per defined holiday schedule. If this parameter is disabled, then authentication is done without any check on holiday schedule.

    NOTE: Refer to *Define Holiday Schedule* under Configuration through Webserver section to know more about access schedule.

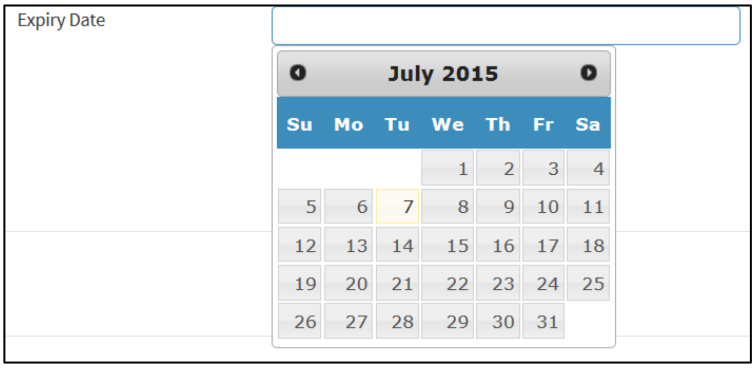


☑ Show Additional Information

Enrollment Timeout: 10 seconds
Expiry Date:
Apply Holiday Schedule: □
Include in Authorized List: □
Include in VIP List: □
Relay Timeout Duration: seconds

Figure 46: Configuring Door Open Time Out

16. Configure **Relay Timeout Duration** in seconds. The door stays open for the time duration defined here for the particular user.



Expiry Date

July 2015

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Figure 47: Configure User Expiry Date

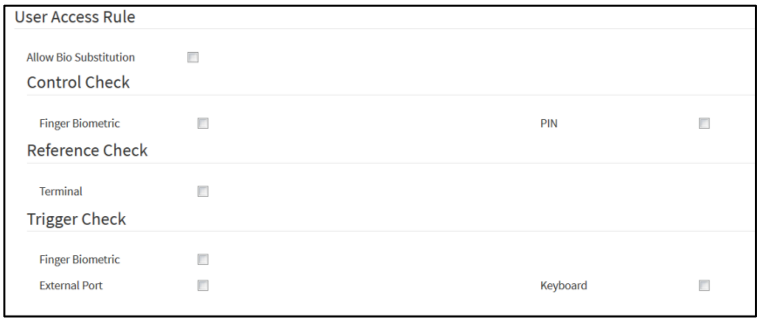
17. This parameter indicates whether user account is active for specific duration or will be active forever
    a. If Expiry Date parameter is Blank, then the user expiry is considered as infinite.
    b. If any Expiry Date is set, then the user record shall expire by the end of the set date.
18. Configure Include in **Authorized List** as ON or OFF. Only if the user is in Authorized list, access will be granted. By default, this parameter is set as OFF.

NOTE: The authorized list parameter will be effective only if the parameter "Authorized List Check Mode" is ON, under Control Configuration > User Control.

19. Configure Include in **VIP List** as ON or OFF. If user is enrolled as VIP user, then at the time of authentication, terminal will not ask for biometric or PIN or BIOPIN.

NOTE: The VIP list parameter will be effective only if the parameter "Allow VIP authentication bypass" is ON, under Control Configuration > User Control.

20. Configure **User Access Rule**. This configuration panel allows an administrator to modify the general authentication rule applied to all users, to user specific settings.



User Access Rule

Allow Bio Substitution □

Control Check

Finger Biometric □ PIN □

Reference Check

Terminal □

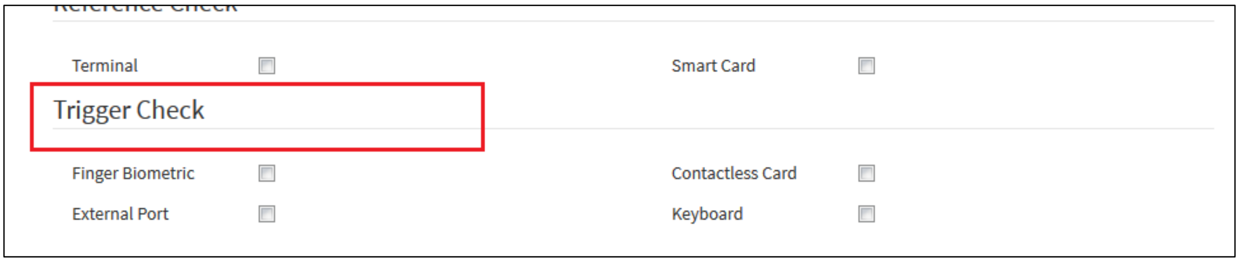
Trigger Check

Finger Biometric □

External Port □ Keyboard □

Figure 48: Defining User Rule

21. The User Rule settings includes below parameters:



Reference Check

Terminal □ Smart Card □

Trigger Check

Finger Biometric □ Contactless Card □

External Port □ Keyboard □

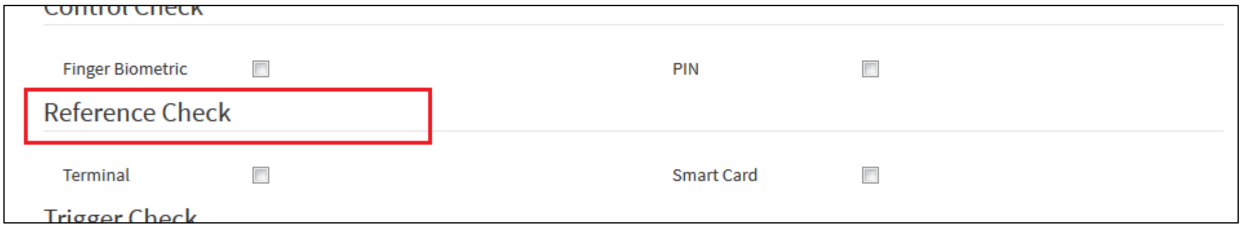
Figure 49: Defining User Rule – Trigger Check

22. Under **Trigger Check**, an administrator can configure the mediums through which user can trigger request for access
    a. Set **Biometric** as ON, if an administrator wants to allow user to access by fingerprint identification. If trigger event through biometric is OFF, then user cannot initiate the access rights check using fingerprint. And Biometric Check will be bypass for the particular user.

    NOTE: In case the MorphoAccess® SIGMA Lite Series terminal is used in Legacy L1 mode, a generic user rule is required to be set as authentication using Card Only. Which can be set from access path Biometric Security > Trigger event.

    And biometric check of the users, except the ones whose biometric check is bypass, is required to be enabled using specific user rule configuration.

    b. Set **Contactless Card** as ON, if an administrator wants to allow user to request access by presenting card authentication
    c. Set **Keypad** as ON (applicable for *MorphoAccess® SIGMA Lite+ Series* only), if an administrator wants to allow user to request access by entering User ID using keypad. The authentication is done by matching the User ID of the stored user in the database.
    d. Set **External Port** as ON, if an administrator allows a user to request access by providing his User ID through External port



Control Check

Finger Biometric □ PIN □

Reference Check

Terminal □ Smart Card □

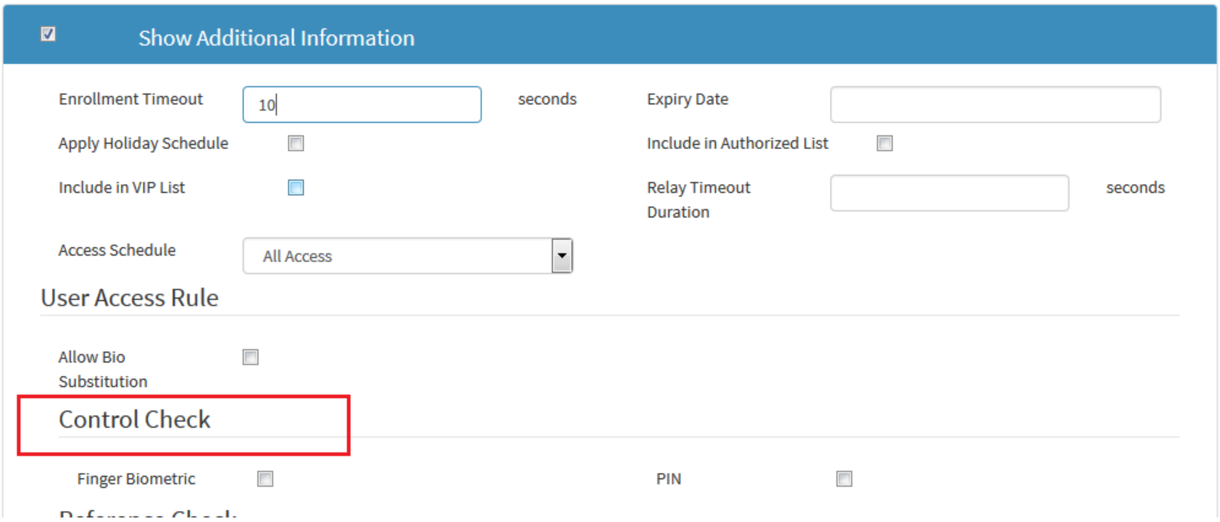
Trigger Check

Figure 50: Defining User Rule –Reference Check

23. Under **Reference Check**, an administrator can configure whether user's information should be referred from Terminal database or/and Smart Card

a. Set **Terminal** as ON, if terminal should refer to user's profile in database

b. Set **Smart Card** as ON, if terminal should refer to user's profile in smart card



☑ Show Additional Information

Enrollment Timeout: 10 seconds

Expiry Date:

Apply Holiday Schedule □

Include in Authorized List □

Include in VIP List □

Relay Timeout Duration: seconds

Access Schedule: All Access

User Access Rule

Allow Bio Substitution □

Control Check

Finger Biometric □

PIN □

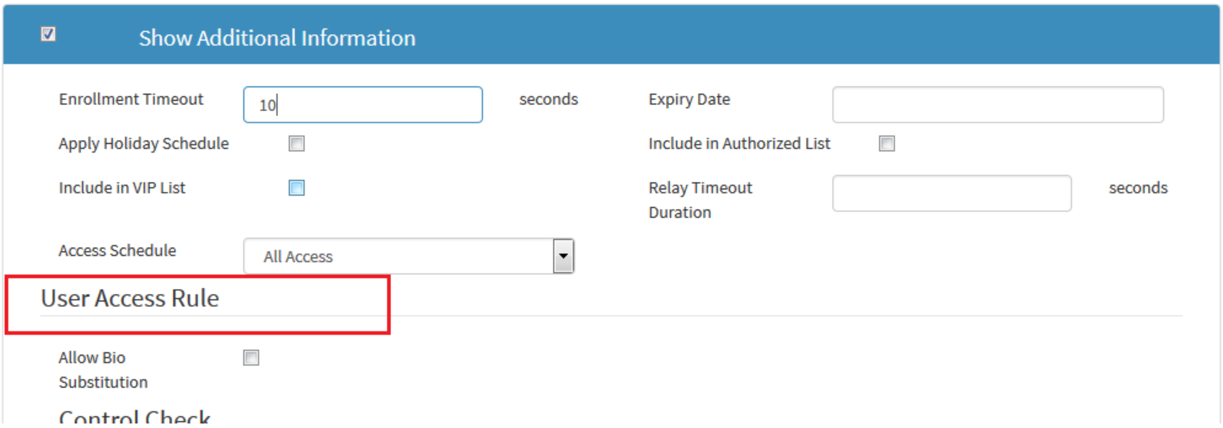
Reference Check

Figure 51: Defining User Rule – Control Check

24. Under Control Check, an administrator can set:

    a. **PIN** mode as ON, if PIN based authentication is required (For *MorphoAccess® SIGMA Lite+ Series* terminal only)

    b. **Biometric** as ON, if Biometric authentication is required



☑ Show Additional Information

Enrollment Timeout: 10 seconds

Expiry Date:

Apply Holiday Schedule □

Include in Authorized List □

Include in VIP List □

Relay Timeout Duration: seconds

Access Schedule: All Access

User Access Rule

Allow Bio Substitution □

Control Check

Figure 52: Defining User Rule

25. **Allow Bio Substitution** parameter can be set as ON. It indicates that instead of Biometric, the user can be authenticated through a substitute such as BIO-PIN or PIN (For *MorphoAccess® SIGMA Lite+ Series* terminal only)

26. Press on **Enroll User** to **Enroll** the user with the details inputted.

Results

A confirmation message is displayed showing User is enrolled successfully. The user information is stored in the database.

Whenever user tries to access by providing fingerprint, terminal will match the fingerprint with the records stored in the database and allow access on successful identification.

Recommendation: In case of authentication failed due to bad biometric, the user can be re-enrolled. In case of L1 mode, the re-enrolment can be done using Secure Admin station is equipped with a MorphoSmart™ MSO biometric sensor only.

User Enrolment in Card

Using this functionality, an administrator can encode a contactless smartcard for a user. The user's data are saved only on the card, and not in the terminal database. It means, that the authentication of the user is done by checking the user's data stored in the card. For example, when user place finger on biometric sensor, the terminal will check the biometric provided by the user with the biometric stored in the users card.

Access Path

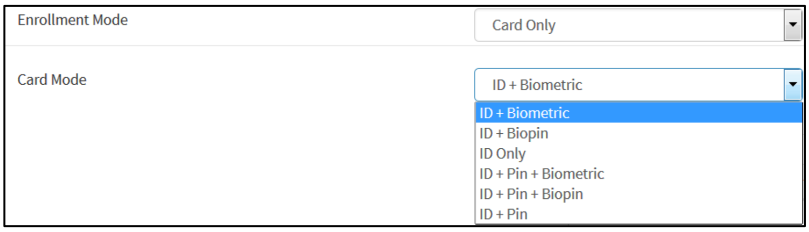
Webserver > User Management > User Enrollment > Enrollment Mode > Card Only

Pre-requisites

If terminal is in Legacy L1 mode, then enrolment of users can be done only if the biometric sensor is a MorphoSmart™ MSO terminal

The data of the users enrolled in MA5G mode cannot be exported in L1 systems

Screens & Steps

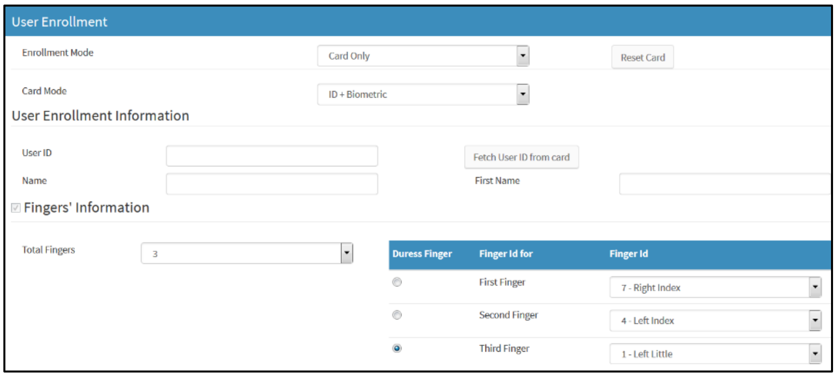


Enrollment Mode: Card Only

Card Mode: ID + Biometric

Figure 53: Select Card Data Format

1. Card Data Format allows an administrator to select the data that will be used for user authentication. Below options are available:
   a. **ID + Template:** This format indicates that the user authentication is done by verifying the User ID and biometric template (i.e. fingerprint registered by user) Three biometric templates can be stored for a user including two mandatory biometric templates (fingerprints) and one duress finger



User Enrollment

Enrollment Mode: Card Only

Card Mode: ID + Biometric

User Enrollment Information

User ID:

Name:

First Name:

☑ Fingers' Information

Total Fingers: 3

Duress Finger	Finger Id for	Finger Id
○	First Finger	7 - Right Index
○	Second Finger	4 - Left Index
●	Third Finger	1 - Left Little

Figure 54: Enrollment Finger Index in Card

b. **ID + BIOPIN:** This format indicates that the user authentication is done by verifying the User ID and BIOPIN (i.e. PIN that is used in place of biometric data)

c. **ID Only:** This format indicates that the user authentication is done by verifying the User ID

d. **ID + PIN + Template:** This format indicates that the user authentication is done by verifying the User ID, PIN, and Biometric Template

e. **ID + PIN + BIOPIN:** This format indicates that the user authentication is done by verifying the User ID, PIN, and BIOPIN

f. **ID + PIN:** This format indicates that the user authentication is done by verifying the User ID, and PIN

2. According to the selected Card Data Format, next user's data will be captured and stored in the card. The below steps are for ID + Template format
3. Refer steps 1 to 26 of section *User Enrolment in Database*
4. A message to place card at terminal is displayed.
5. **Place Smart Card** on the card reader. You may have to place card for 1 to 10 seconds, till the success message is displayed showing the user's data is stored in the card

Results

The user is enrolled successfully and user's data is stored in the Card. The user can initiate access request by placing a card at terminal. The terminal will read User ID and ask user to enter required data, i.e. biometric/pin/biopin.

The user's data stored on card are neither editable nor viewable.

User Enrolment in Card & Database

Using this functionality, an administrator can enroll a new user and store the user data in contactless smartcard as well as in database of terminal. It means, that the authentication of the user is done by checking the details stored in the card as well as in terminal database. For example, when user places finger on biometric sensor, the terminal will check the biometric provided by the user against the biometric stored in the users card.

Access Path

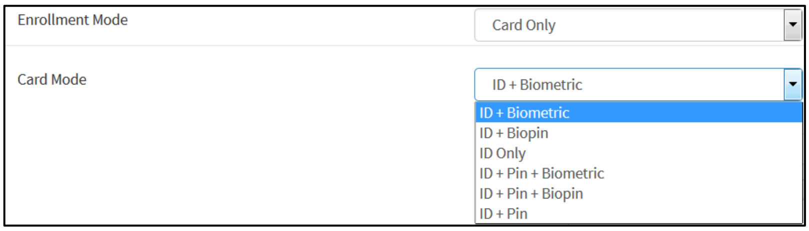
Webserver > User Management > User Enrollment > Enrollment Mode > DB + Card

Pre-requisites

If terminal is in Legacy L1 mode, then enrolment of users can be done only if Secure Admin station is equipped with a MorphoSmart™ MSO biometric sensor

The data of the users enrolled in MA5G mode cannot be exported in L1 systems

Screens & Steps



Enrollment Mode: Card Only

Card Mode: ID + Biometric

Figure 55: Select Card Data Format

1. Card Data Format allows an administrator to select the user's data required for access rights check, and then required to be written on user's card. Please refer to step # 1 of *User Enrolment in Card* section for various available options
2. Please refer to *User Enrolment in Database* section step # 1 to 26
3. A message to place card at terminal is displayed.

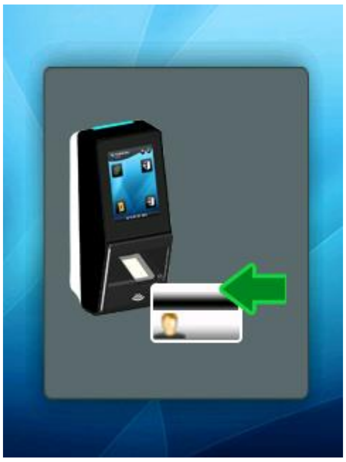


Figure 56: Place Card

4. On placing card, the user's data is stored in the card and the terminal asks user to remove the card.

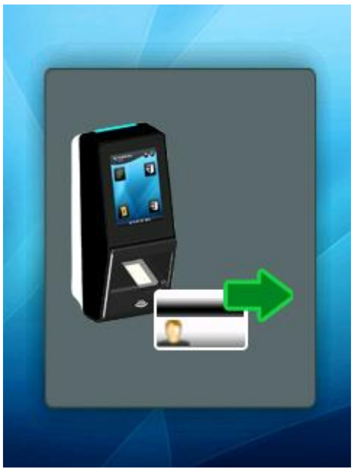


Figure 57: Remove Card

Results

The user is enrolled successfully and user's data are stored in the terminal database and smartcard. The user can initiate access request by placing a card at terminal. The terminal will read User ID and ask user to enter required data, i.e. biometric/pin/biopin. The authentication of user’s details is done based on **Record Reference Source** selected in User Rule.

The user's data stored on card are not editable or viewable.

Recommendation: In case of authentication failed due to bad biometric, the user can be re-enrolled. In case of L1 mode, the re-enrolment can be done using Secure Admin station equipped with a MorphoSmart™ MSO biometric sensor only.

Update User Information

Using this functionality, an administrator can edit the user information stored in database. It is not possible to edit the information of the user stored on the Card but it is possible to erase and rewrite the user's card with new data.

Access Path

Webserver > User Management > Users

Screens & Steps

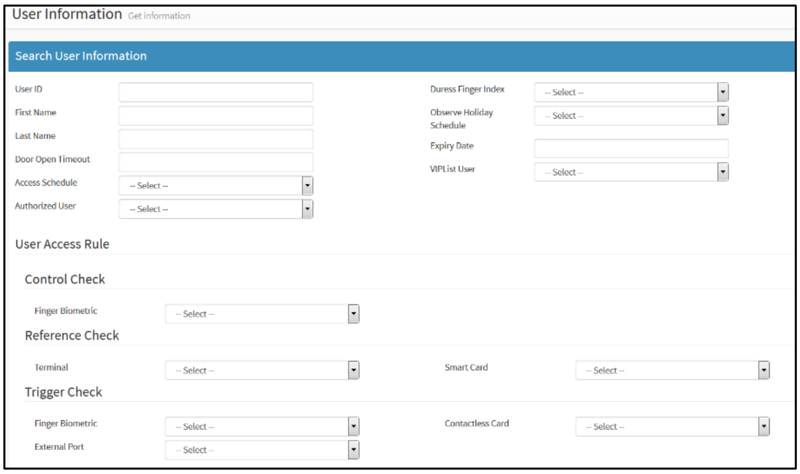
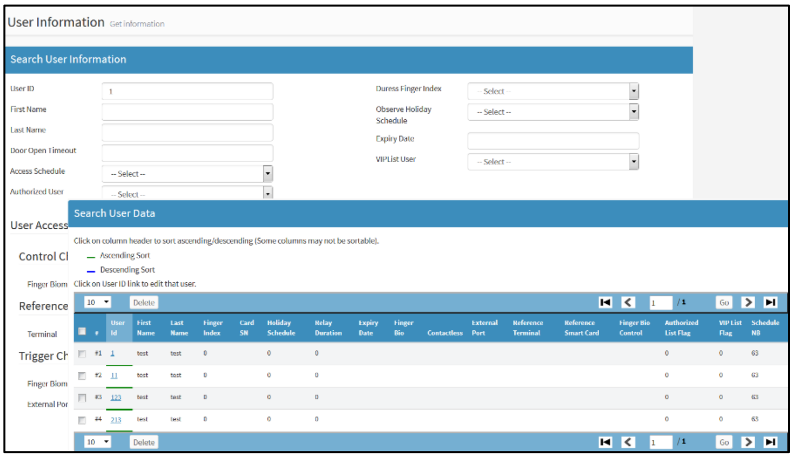


Figure 58: Selecting Search Criteria

1. Select Search User by **ID**, **First Name** or **Last Name**
2. Press on **Search** button to Search the users enrolled
3. Enter the **User ID** of the user account which is required to be edited
4. Press on **Search** button to get the user details enrolled with the entered User ID



User Information Get information

Search User Information

User ID: 1
First Name:
Last Name:
Door Open Timeout:
Access Schedule: -- Select --
Authorized User: -- Select --
Duress Finger Index: -- Select --
Observe Holiday Schedule: -- Select --
Expiry Date:
VIPList User: -- Select --

Search User Data

Click on column header to sort ascending/descending (Some columns may not be sortable).

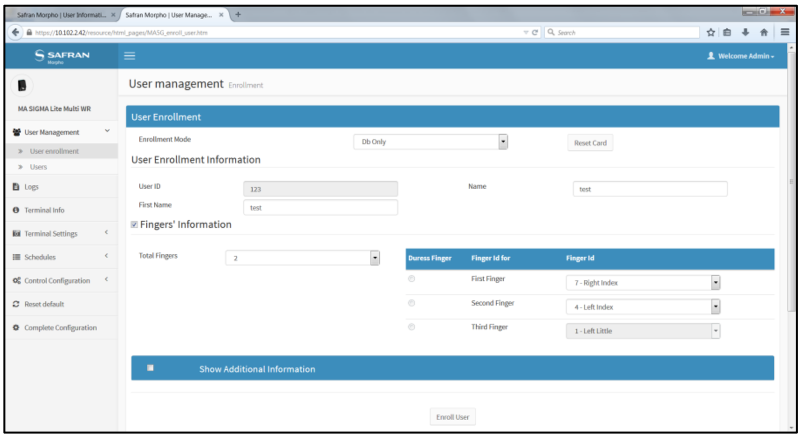
— Ascending Sort
— Descending Sort

Click on User ID link to edit that user.

□	#	User Id	First Name	Last Name	Finger Index	Card SN	Holiday Schedule	Relay Duration	Expiry Date	Finger Bio	Contactless	External Port	Reference Terminal	Reference Smart Card	Finger Bio Control	Authorized List Flag	VIP List Flag	Schedule NB
□	#1	1	test	test	0		0	0								0	0	63
□	#2	11	test	test	0		0	0								0	0	63
□	#3	123	test	test	0		0	0								0	0	63
□	#4	213	test	test	0		0	0								0	0	63

Figure 59: Selecting User ID

5. The list of User IDs with the entered ID placed anywhere in the user ID will be displayed. **Select User ID** from the list and click on the User ID to get the details entered during enrollment.



https://10.102.2.42/resource/html_pages/MA5G_enroll_user.htm

User management Enrollment

User Enrollment

Enrollment Mode: Db Only

User Enrollment Information

User ID: 123
Name: test
First Name: test

☑ Fingers' Information

Total Fingers: 2

Duress Finger	Finger Id for	Finger Id
○	First Finger	7 - Right Index
○	Second Finger	4 - Left Index
○	Third Finger	1 - Left Little

□ Show Additional Information

Figure 60: Enrolment Information screen is displayed for editing

6. Enrolment Information screen is displayed. An administrator can update below information:
   a. First Name and Last Name of the user
   b. Capture Fingerprints
   c. Update User Pin
   d. Configure Access Schedule
   e. Set Observe Holiday Schedule
   f. Set Door Open Timeout
   g. Set Infinite Expiry Date
   h. Configure Authorized list
   i. Configure VIP User

   j. Configure User Rules

7. Press on **Enroll User** to **Save** user information

Results

The user information is updated and stored in database. When user tries to access, the updated information is used for verification.

Note: The list of User ID's retrieved upon search are displayed in the string format and not in the serial order.

Delete User

Using this functionality, an administrator can delete user information. There are several options for deleting users:

Delete a User

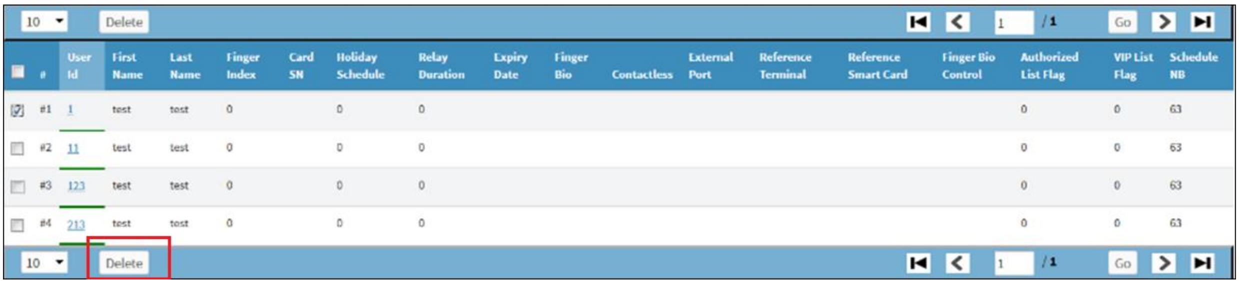
Delete All Users

Delete a User

Access Path

Webserver > User Management > Users

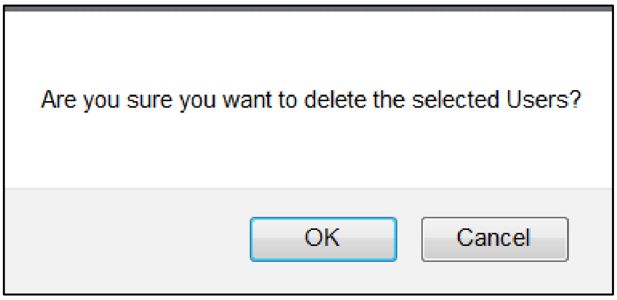
Screens & Steps



□	#	User Id	First Name	Last Name	Finger Index	Card SN	Holiday Schedule	Relay Duration	Expiry Date	Finger Bio	Contactless	External Port	Reference Terminal	Reference Smart Card	Finger Bio Control	Authorized List Flag	VIP List Flag	Schedule NB
☑	#1	1	test	test	0		0	0								0	0	63
□	#2	11	test	test	0		0	0								0	0	63
□	#3	123	test	test	0		0	0								0	0	63
□	#4	213	test	test	0		0	0								0	0	63

Figure 61: Deleting User

1. Get the list of Users enrolled in the terminal
2. Select the **User ID** that the administrator need to delete
3. Press on **Delete** button to delete the user



Are you sure you want to delete the selected Users?

Figure 62: A confirmation message pop up for delete

4. A confirmation message is displayed, asking to confirm the action
5. Press on **OK** to confirm delete action

Results

The User ID is deleted successfully. The terminal will deny access to the deleted user upon user control.

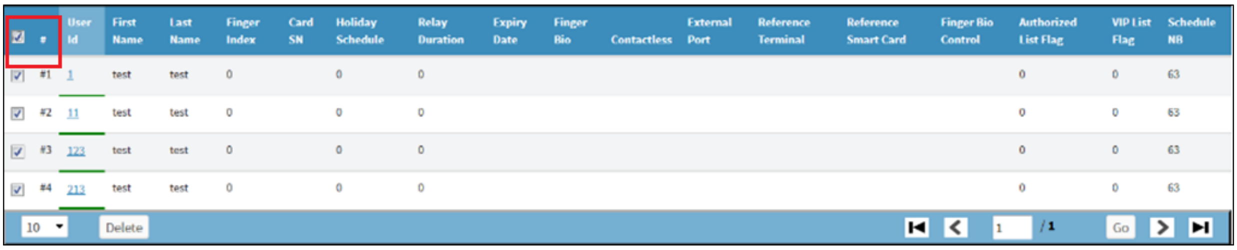
Delete All User ID

This functionality will delete all the users stored in terminal database.

Access Path

Webserver > User Management > Users

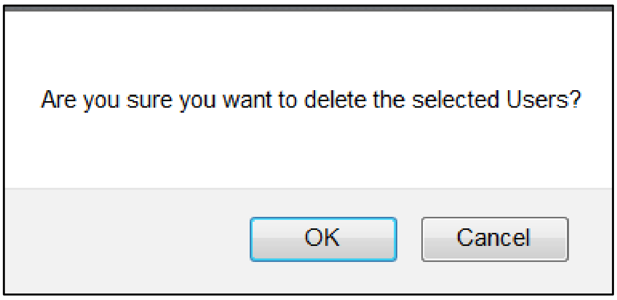
Screens & Steps



☑	#	User Id	First Name	Last Name	Finger Index	Card SN	Holiday Schedule	Relay Duration	Expiry Date	Finger Bio	Contactless	External Port	Reference Terminal	Reference Smart Card	Finger Bio Control	Authorized List Flag	VIP List Flag	Schedule NB
☑	#1	1	test	test	0		0	0								0	0	63
☑	#2	11	test	test	0		0	0								0	0	63
☑	#3	123	test	test	0		0	0								0	0	63
☑	#4	213	test	test	0		0	0								0	0	63

Figure 63: Select Delete All Users action

1. Select **Delete All Users** to delete all the user in the database



Are you sure you want to delete the selected Users?

Figure 64: Confirm All User Deletion

2. A confirmation message is displayed, asking to confirm the action
3. Press on **OK** to confirm delete all users action

Card Manager

MorphoAccess® SIGMA Lite Series terminals allows user enrolment and authentication using contactless smart cards. When a user is enrolled on smart card, the User Identifier, Fingerprint Template and PIN/BIOPIN are stored in the card. Terminal can check this information on card for authenticating a user.

Using Card Manager Menu, an administrator can configure the contactless smart card parameters, which are supported by MorphoAccess® SIGMA Lite Series terminals.

Access Path

User Menu > Card Manager

Screens & Steps

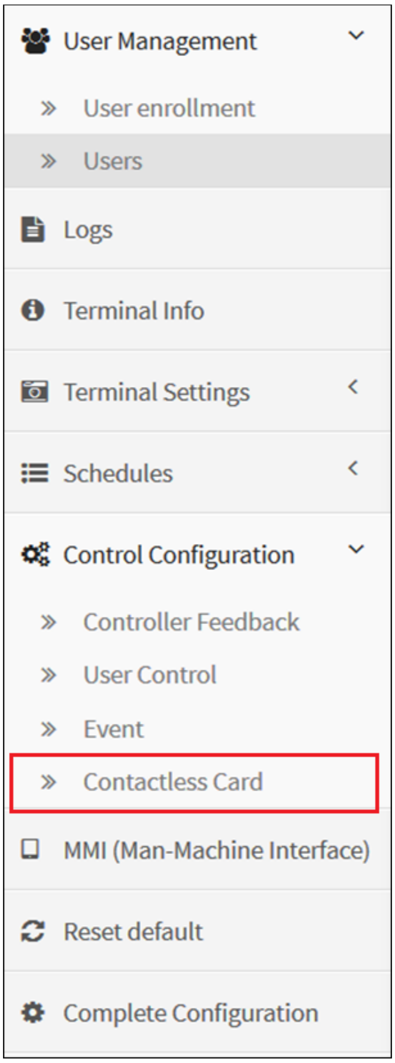


Figure 65: Contactless Card Configuration – Webserver

The card manager has certain parameters that are required to be configured, for required behavior of the system. These parameters are explained subsequently.

Renewal of User Card

A smart card has a default expiry date. Once the smart card is expired it is not useful for verification. Using Renewal of User Card functionality, an administrator can renew a contactless card that is expired, with the same user data such as User ID, fingerprint, PIN and BIOPIN; stored in it. By renewing user card, the expiry of the card is reset and card can be used for verification.

This feature is also useful when a user lose his card. In that case, it is recommended to add the lost card to the Banned list, in order to avoid fraudulent use of the lost card.

Access Path

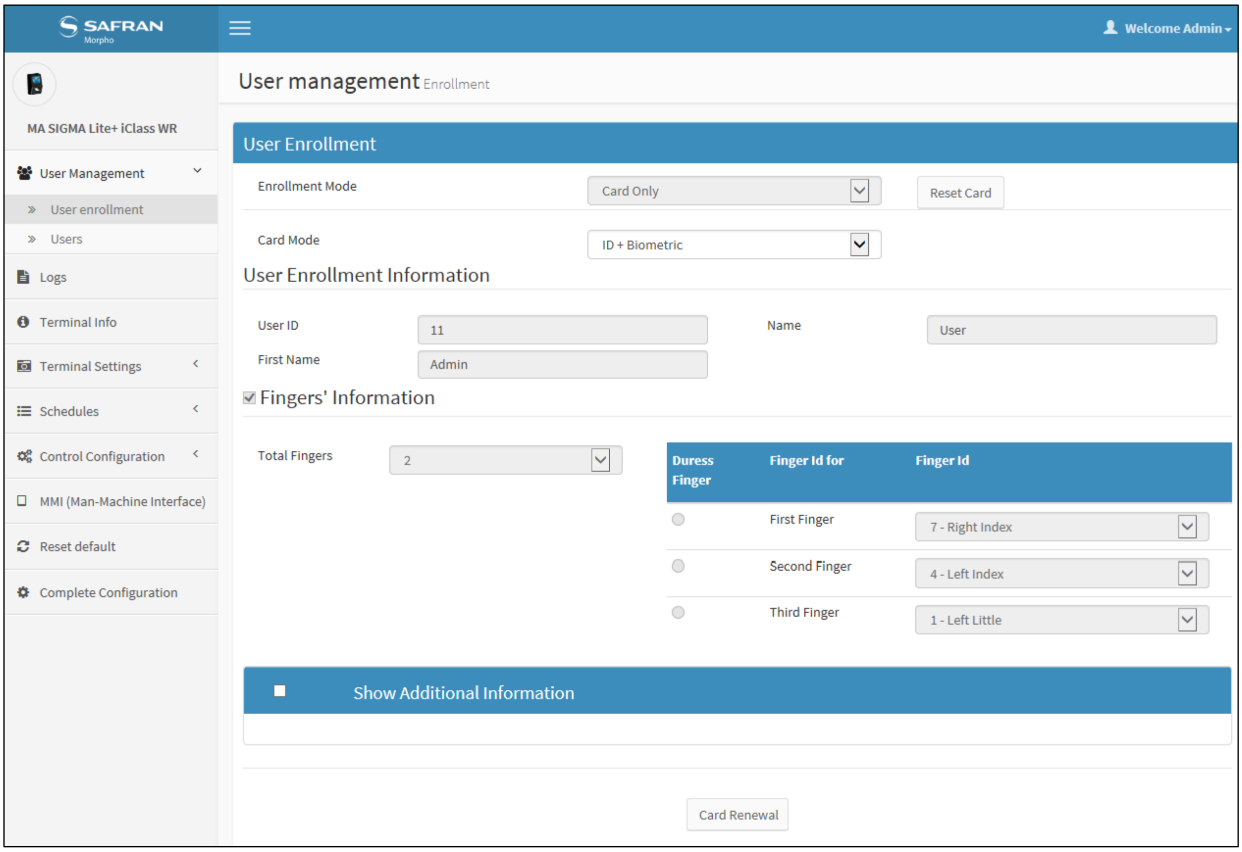
Webserver > User Management > Users

Pre-requisites

User data stored must be available in terminal database, the same data is written on card on renewal.

Card is secured with the same key as on terminal.

Screens & Steps



User management Enrollment

User Enrollment

Enrollment Mode: Card Only

Card Mode: ID + Biometric

User Enrollment Information

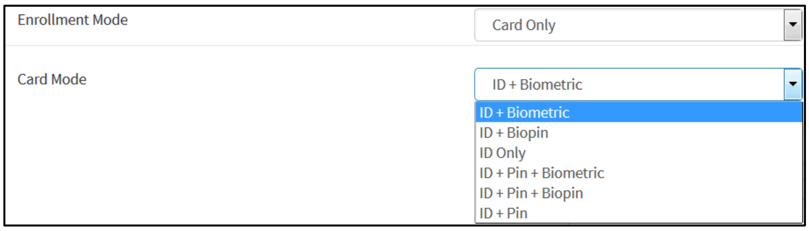
User ID: 11
Name: User
First Name: Admin

☑ Fingers' Information

Total Fingers: 2

Duress Finger	Finger Id for	Finger Id
○	First Finger	7 - Right Index
○	Second Finger	4 - Left Index
○	Third Finger	1 - Left Little

Figure 66: Renewal of User Card



Enrollment Mode: Card Only

Card Mode: ID + Biometric

Figure 67: Select Card Data Format

1. Go to Users and Search the user
2. Click on user and Terminal will open a new window “Edit Type”
3. Select Card Only to Renew the Card.
4. Now terminal open a new page to renew the card for the user.
5. Select the card data format from available options as below:
    a. ID + Template (fingerprint)
    b. ID + BIOPIN
    c. ID Only
    d. ID + PIN + Biometric

   e. ID + PIN + BIOPIN
   f. ID + PIN

6. Enter the details required
7. Click on **Card Renewal** to renew the card
8. Terminal will ask to place the card on card reader. **Place card**

Results

User’s data stored in terminal database are copied on the card. The card is renewed with new expiry date. Now user can use this card for authentication.

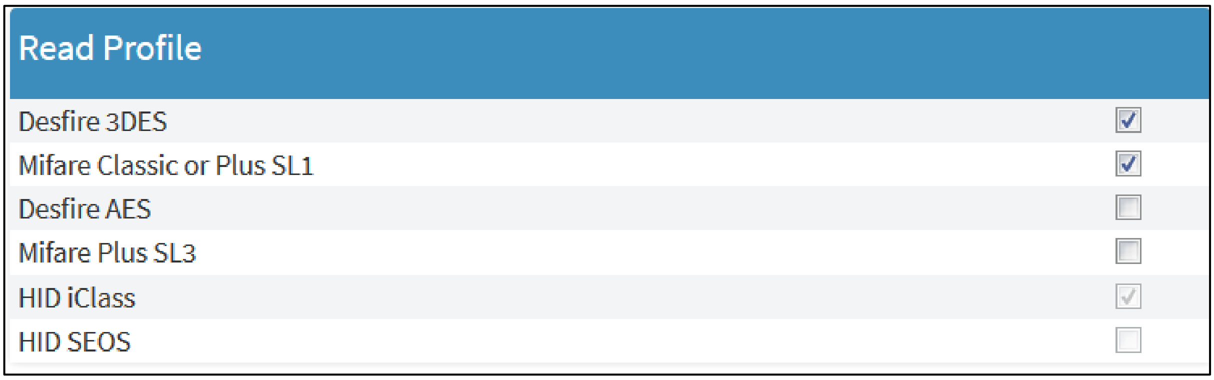
Smart Card Read Profile

Using this functionality, an administrator can set the type of card that MorphoAccess® SIGMA Lite Series terminal will be able to read. It means these cards can be used for authentication purpose only. The data on the card cannot be changed.

Access Path

Webserver > Control Configuration > Contactless Card > General Configurations > Read Profile

Screens & Steps

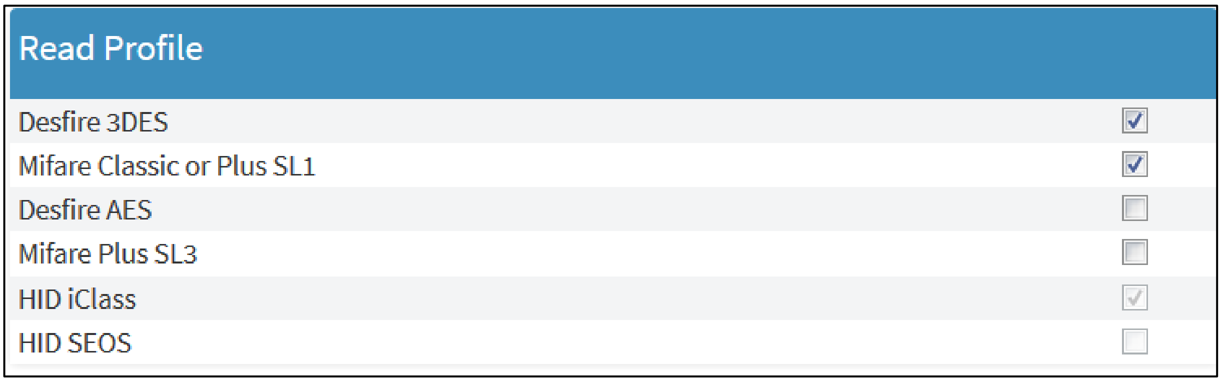


Read Profile

Desfire 3DES	☑
Mifare Classic or Plus SL1	☑
Desfire AES	□
Mifare Plus SL3	□
HID iClass	☑
HID SEOS	□

Figure 68: Smartcard Read Profile

1. Select **Smartcard Read Profile**
    a. *In case of Multi product.*

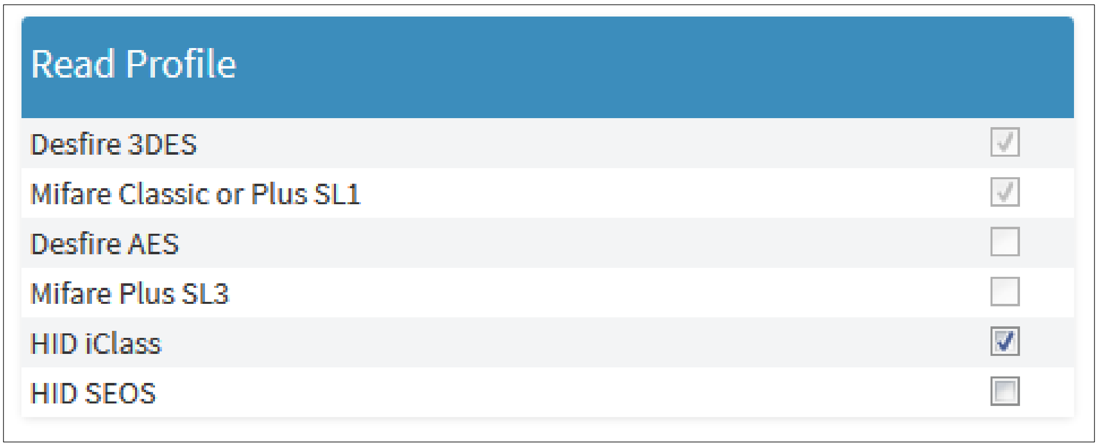


Read Profile

Desfire 3DES	☑
Mifare Classic or Plus SL1	☑
Desfire AES	□
Mifare Plus SL3	□
HID iClass	☑
HID SEOS	□

Figure 69: Smartcard Read Profile_Multi

    b. *In case of iClass product.*



Read Profile

Desfire 3DES	☑
Mifare Classic or Plus SL1	☑
Desfire AES	□
Mifare Plus SL3	□
HID iClass	☑
HID SEOS	□

Figure 70: Smartcard Read Profile_iClass

2. Set the following cards read profile as ON, if an administrator require terminal to read them:

   ➔ In case of Multi Product

   a. MIFARE® Classic or Plus SL1
   b. MIFARE® Plus SL3
   c. MIFARE® DESFire® 3DES
   d. MIFARE® DESFire® AES

   ➔ In case of iClass Product

   a. HID IClass
   b. HID SEOS

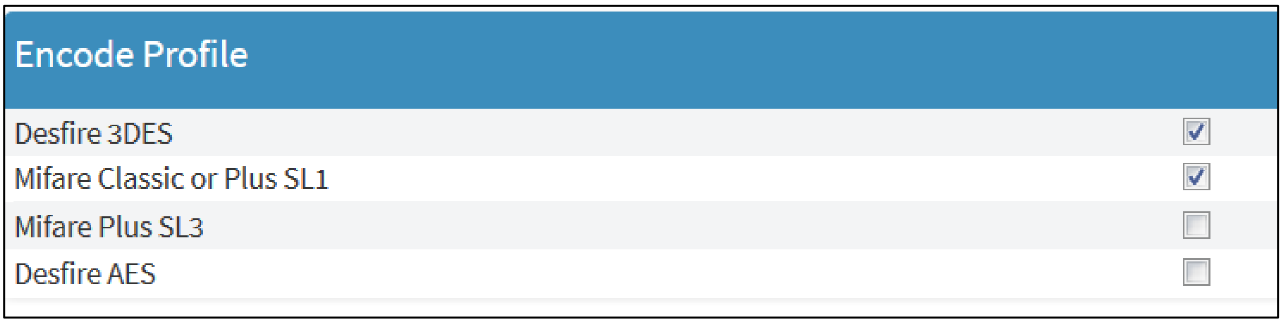
3. Press on **Save** button to save configuration

Smart Card Encode Profile

Using this functionality, an administrator can set the type of card that MorphoAccess® SIGMA Lite Series terminal will be able to encode. It means these cards can be used to store user's profile and used for user authentication. It is possible to update/reset card's data.

Access Path

Webserver > Control Configuration > Contactless Card > General Configurations > Encode Profile Screens & Steps



Encode Profile

Desfire 3DES	☑
Mifare Classic or Plus SL1	☑
Mifare Plus SL3	☐
Desfire AES	☐

Figure 71: Smartcard Encode Profile

1. Select Smart card encode profile
2. Set the following smartcards encode profile as ON, if an administrator require terminal to encode them:
   a. MIFARE® Classic or Plus SL1
   b. MIFARE® Plus SL3
   c. DESFire® 3DES
   d. DESFire® AES

NOTE: It is not possible to encode several type of MIFARE (Plus and Classic) or DESFire (3DES and AES) cards at the same time. And for HID iClass, Encode profile is not applicable as there is only one type HID iClass card for encode.

3. Press on **Save** button to save configuration

No. of Blocks and Start Block for MIFARE® Cards

It is possible to define the location of the access control data on the contactless card, by specifying the number of the first block and total number of blocks to read on the card. By default, the 1st block to read is block # 4 and total number of blocks is #31.

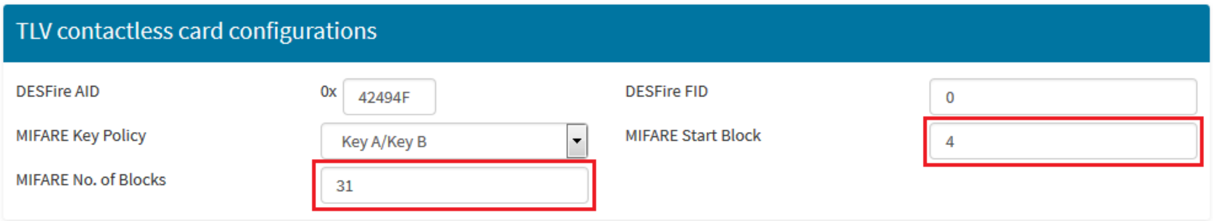
NOTE 1: The value specified for the start block and number of blocks, also applies to the administrator cards, then ensure that administrator data is stored from the same block number as user data on user cards and on given number of blocks.

NOTE 2: In case of 1 K MIFARE®, an administrator can set start block no. 4 to block 48. In case of 4 K MIFARE®, an administrator can set start block no. 4 to block 216.

Access Path

Webserver > Control Configuration > Contactless Card > TLV contactless card configurations > MIFARE Start Block

Screens & Steps



TLV contactless card configurations

DESFire AID 0x 42494F
DESFire FID 0
MIFARE Key Policy Key A/Key B
MIFARE Start Block 4
MIFARE No. of Blocks 31

Figure 72: Setting No. of Block & Start Block

1. Select **No. Of Block** & **Start Block**
2. Press on **Save** button to save changes

Select Keyset for Reading MIFARE® Cards

Using this functionality, an administrator can select a key set that is used by terminal for authentication and reading MIFARE® cards. The below key set values can be configured:

Key A

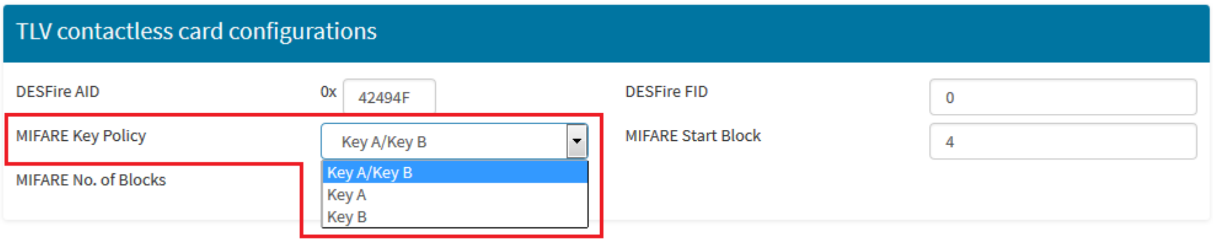
Key B

Key A and Key B

Access Path

Webserver > Control Configuration > Contactless Card > TLV contactless card configurations > MIFARE Key Policy

Screens & Steps



TLV contactless card configurations

DESFire AID 0x 42494F

DESFire FID 0

MIFARE Key Policy Key A/Key B

MIFARE Start Block 4

MIFARE No. of Blocks

Figure 73: Keyset configuration

1. Select a **keyset**
2. Press on **Save** button to save changes

Select Enroll ID Format

Using this functionality, an administrator can set the User ID format to be encoded on card.

Access Path

Webserver > Control Configuration > Contactless Card > General configurations > Enroll User ID

Screens & Steps

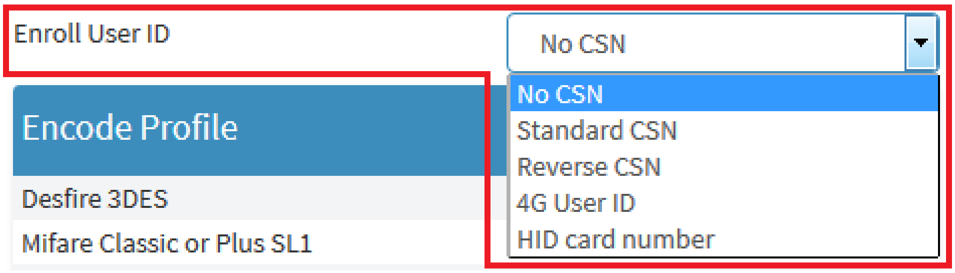


Figure 74: Selecting Enroll User ID Format

1. Select **Enroll User ID Format**
2. Select User ID format used for enrolling users on card:
   a. **No CSN**: this value indicates that contactless card serial number will not be used as User ID
   b. **Standard CSN**: If this option is selected, the contactless card serial number is considered as User ID at the time of enrolment and authentication
   c. **Reverse CSN**: If this option is selected, the contactless card serial number read in reverse byte order, is considered as User ID at the time of enrolment and authentication
   d. **4G User ID**: If this option is selected, the read contactless card serial number is manipulated as per 4G terminal. Manipulation is as per given below.

e.g.

Step 1: *CSN read from the card.*

```
            If (ICLASS)
            {
                  //Reverse all the bytes in case iclass card
            }
            Else
            {
                //Do not reverse
        }
Step 2:
        If (MIFARE)     // 4 Byte CSN card
        {
                //generate decimal from 4 Byte CSN.
        }
        Else if (DESFire) // OR any 7 BYTE CSN card
        {
                //Add 0 in beginning of CSN
                //reverse the first 4-bytes and reverse the next 4-bytes.
                //reverse the whole 8-byte after above manipulation
                //generate decimal from the manipulated HEX

        }
        Else //ICLASS CARD
        {
                //reverse the first 4-bytes and reverse the next 4-bytes.
                //reverse the whole 8-byte after above manipulation
                //generate decimal from the manipulated HEX
        }
```

e. **HID card number:** if this option is selected, terminal read the HID card number from the iClass card.

NOTE: This option only available in iClass product.

3. Press on **Save** button to save changes

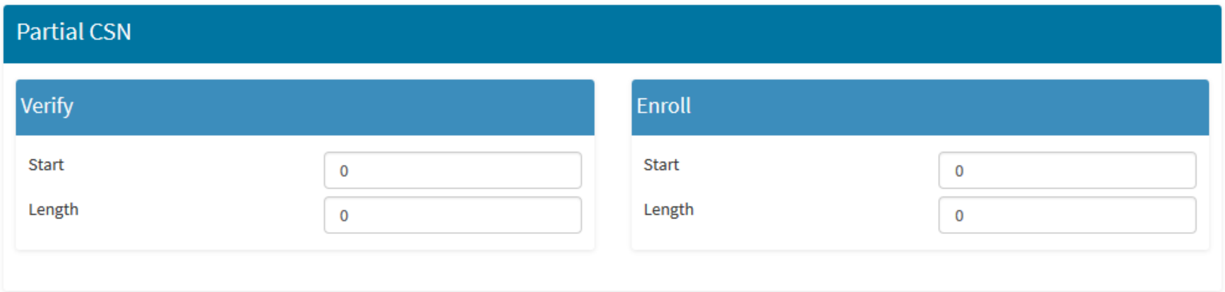
Configure Partial CSN

Using this functionality, an administrator can set the value of start bit and length of bit i.e. total number of bit, to be used for Enroll and Verify.

Access Path

Webserver > Control Configuration > Contactless Card > Partial CSN

Screens & Steps



Verify
Start 0
Length 0

Enroll
Start 0
Length 0

Figure 75: Configure Partial CSN for Enroll and Verify

1. Select **Start** & **Length** for **Enroll** and **Verify.**
   a. Default value of **Start** and **Length** is **0**
   b. **Start** can be configured in range **0 to 79**
   c. **Length** can be configured in range **0 to 80**
2. Press on **Save** button to save changes

Note: These keys are only used when the keys "Enroll" or "Verify" are set to "ReverseCSN" or "StandardCSN".

Example
CSN card: 0xE012FFFB012D89FF
CSN Decimal value: 16146249067598285311
CSN Binary value:
1110000000010010111111111111101100000001001011011000100111111111
Truncated value, using interface we propose, with programmed start bit to 11 and length to 53
CSN Binary value: 10010111111111111101100000001001011011000100111111111
ID Decimal value: 5348003102427647

Defining Application ID and File ID for DESFIRE® Cards

Using this functionality, an administrator can specify the value of Application ID and File ID for reading DESFire® cards. When the DESFire® card is presented to the reader during authentication, the application ID is read from the configured location from where the active File ID is fetched which further contains the user data.

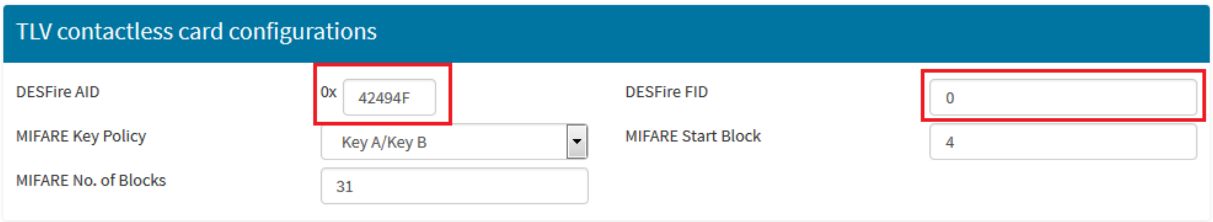
Access Path

Webserver > Control Configuration > Contactless Card > TLV contactless card configurations > DESFire AID

And

Webserver > Control Configuration > Contactless Card > TLV contactless card configurations > DESFire FID

Screens & Steps



TLV contactless card configurations

DESFire AID	0x 42494F	DESFire FID	0
MIFARE Key Policy	Key A/Key B	MIFARE Start Block	4
MIFARE No. of Blocks	31		

Figure 76: Configuring Application ID and File ID

1. Select **Application ID**
   a. Configure Application ID in range of 0x000001-0xFFFFFF.
   b. Default Application ID 0x42494F
2. Now select **File ID**
   a. Configure File ID in range of 0 – 31.
   b. Default File ID is 0
3. Press on **Save** button to save changes

Defining Offset for Reading iCLASS® Cards

Using this functionality an administrator can configure the offset to read the data from 2APP iCLASS® cards. When the iCLASS® card is presented to the reader, the application area 2 is read after the card is authenticated with the key 2.

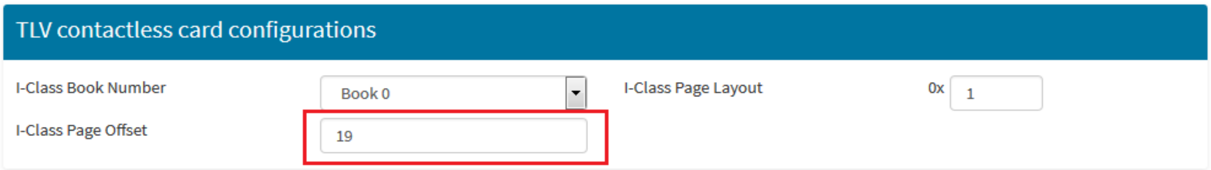
Access Path

Webserver > TLV contactless card configurations > I-Class Page Offset

Pre-requisites

MorphoAccess® SIGMA Lite Series iCLASS® terminal required to configure Offset for reading iCLASS® card

Screens & Steps



TLV contactless card configurations

I-Class Book Number: Book 0

I-Class Page Layout: 0x 1

I-Class Page Offset: 19

Figure 77: Set Key Offset for iCLASS® cards

1. Select **i-Class Page Offset**
   a. Configure **Page Offset** in range of 0-255.
   b. Default **Page Offset** is 19
2. Use “ Save ” button to save the Offset value

Defining Active Pages for Reading iCLASS® Cards

Using this functionality an administrator can configure the active page for reading data from 16APP iCLASS® cards. When the iCLASS® card is presented to the reader, the application area 2 is read after the card is authenticated with the key 2. Depending on the template and size of data stored, the number of pages shall be used in case the card is 16App iCLASS®.

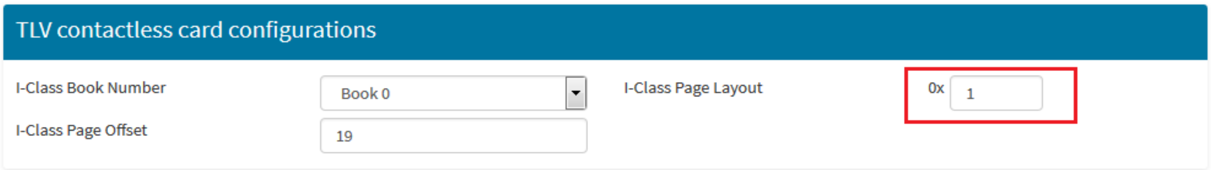
Access Path

Webserver > Control Configuration > Contactless Card > TLV contactless card configurations > I-Class Page Layout

Pre-requisites

MorphoAccess® SIGMA Lite Series iCLASS® terminal required to configure Active for reading iCLASS® card

Screens & Steps



TLV contactless card configurations

I-Class Book Number: Book 0
I-Class Page Offset: 19
I-Class Page Layout: 0x 1

Figure 78: Configure Active Pages for iCLASS® cards

1. Select **i-Class Page Layout.**
   a. Configure **Page Layout** in range of 0-5.
   b. Default **Page Layout** is 1
2. Select “ Save ” button to save

Reset Card

Using this functionality an administrator can reset a contactless card. The user data stored in the card is erased. Terminal will also overwrite the current site key on the card with default.

Access Path

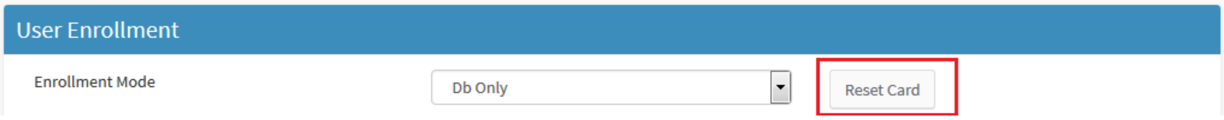
Webserver > User Management > User Enrollment

Pre-requisites

A smart card has user details stored

Card is secured with the same key as on terminal

Screens & Steps



User Enrollment

Enrollment Mode: Db Only

Figure 79: Reset card

1. Click on **Reset Card**
2. Terminal will ask to **Place Card** at card reader.
3. Once an administrator places card, terminal will read and reset card by erasing data stored. And will set card key to default key.

Results

Card is reset successfully. Now a new user can be enrolled on this card.

Terminal Information Menu (Webserver)

MorphoAccess® SIGMA Lite Series terminal administration interface has Information Menu, which enables an administrator to view important data from single panel. Data such as:

Information related to Terminal commercial name and license

Sensor Information

Firmware version

Network settings done in terminal, includes Ethernet and Wi-Fi™

User Status, showing count of enrolled, authorized listed and VIP users. Also shows maximum capacity of users supported in terminal

Transaction Log Status shows count of current logs and maximum supports logs records in terminal

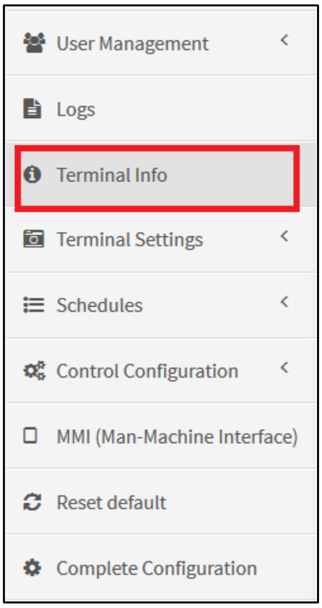


Figure 80: Information Menu – Webserver

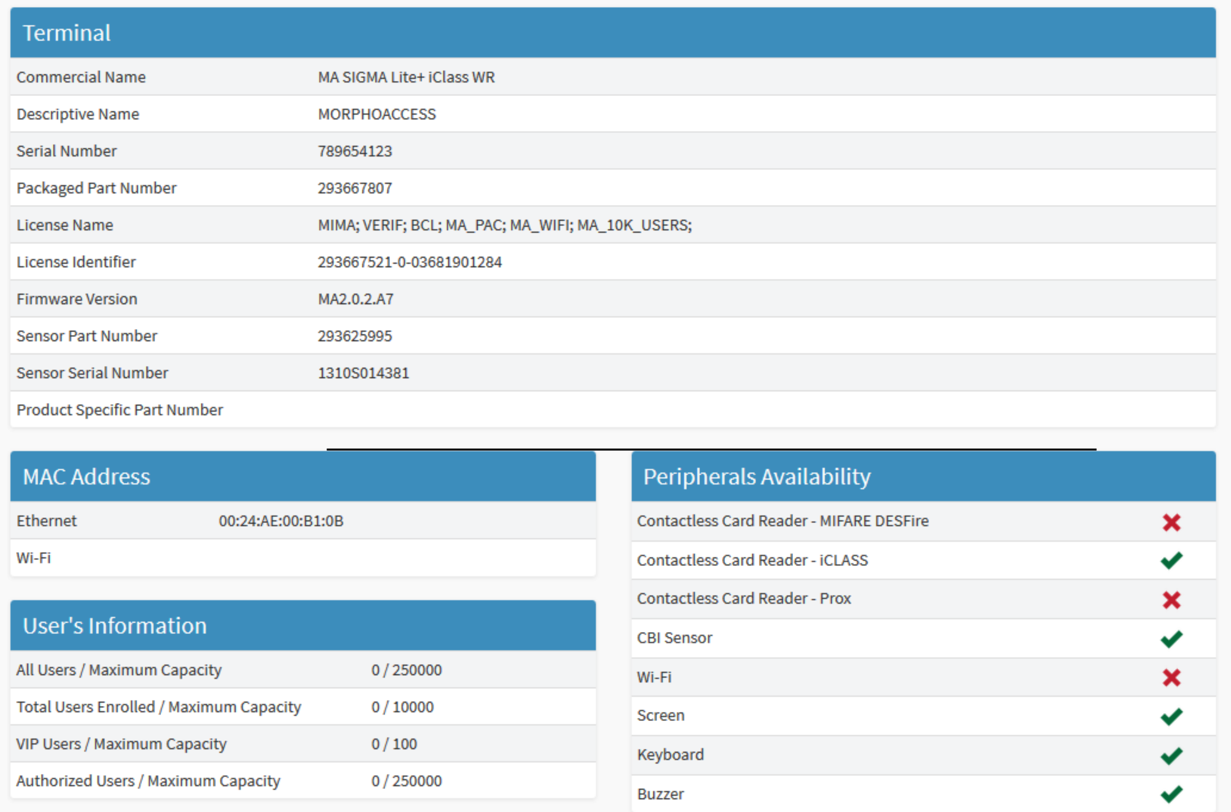
View Terminal Details

Using this functionality, an administrator can view the information related to the MorphoAccess® SIGMA Lite Series Terminal.

Access Path

Webserver > Terminal Info OR Terminal Home screen (For *MorphoAccess® SIGMA Lite+ Series*)

Screens & Steps



Terminal

Commercial Name	MA SIGMA Lite+ iClass WR
Descriptive Name	MORPHOACCESS
Serial Number	789654123
Packaged Part Number	293667807
License Name	MIMA; VERIF; BCL; MA_PAC; MA_WIFI; MA_10K_USERS;
License Identifier	293667521-0-03681901284
Firmware Version	MA2.0.2.A7
Sensor Part Number	293625995
Sensor Serial Number	1310S014381
Product Specific Part Number	

MAC Address

Ethernet	00:24:AE:00:B1:0B
Wi-Fi	

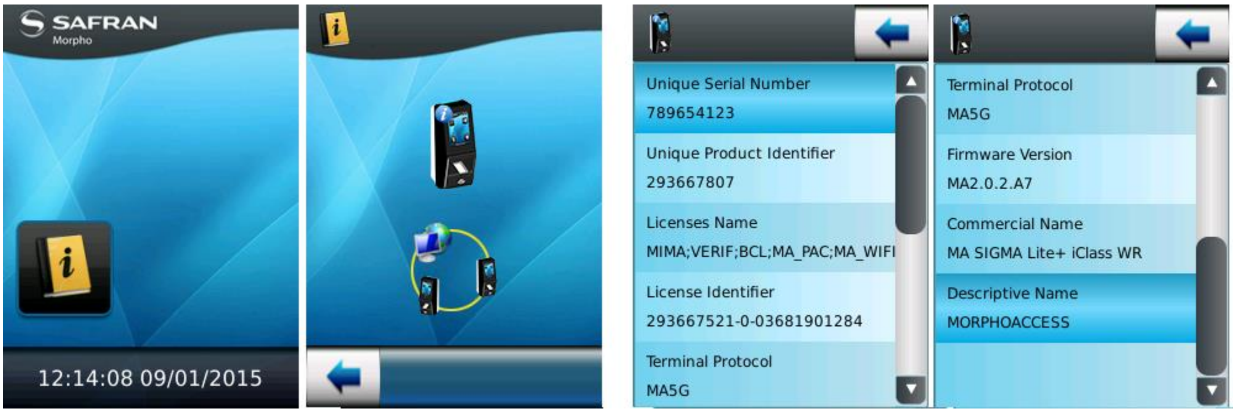
User's Information

All Users / Maximum Capacity	0 / 250000
Total Users Enrolled / Maximum Capacity	0 / 10000
VIP Users / Maximum Capacity	0 / 100
Authorized Users / Maximum Capacity	0 / 250000

Peripherals Availability

Contactless Card Reader - MIFARE DESFire	✗
Contactless Card Reader - iCLASS	✓
Contactless Card Reader - Prox	✗
CBI Sensor	✓
Wi-Fi	✗
Screen	✓
Keyboard	✓
Buzzer	✓

Figure 81: View Device Information – Webserver



Unique Serial Number
789654123
Unique Product Identifier
293667807
Licenses Name
MIMA;VERIF;BCL;MA_PAC;MA_WIFI
License Identifier
293667521-0-03681901284
Terminal Protocol
MA5G

Terminal Protocol
MA5G
Firmware Version
MA2.0.2.A7
Commercial Name
MA SIGMA Lite+ iClass WR
Descriptive Name
MORPHOACCESS

Figure 82: View Device Information – Terminal

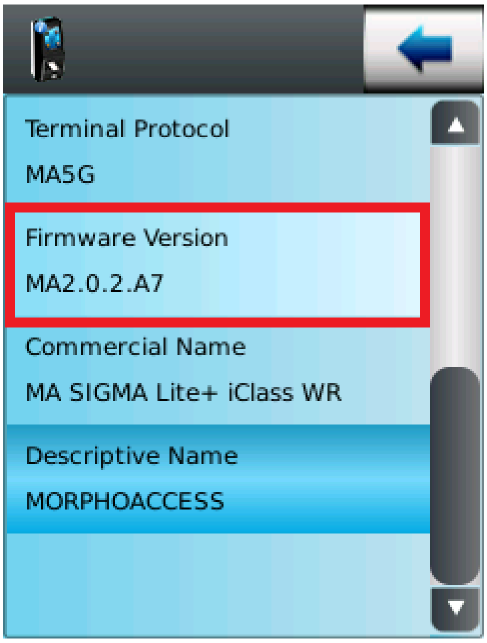
View Firmware Information

Using this functionality, an administrator can view information regarding the current Terminal firmware version. The firmware version is upgradeable and this functionality provides an administrator the information of current firmware of the terminal.

Access Path

Information Menu > Terminal Info > Firmware

Screens & Steps



Terminal Protocol
MA5G

Firmware Version
MA2.0.2.A7

Commercial Name
MA SIGMA Lite+ iClass WR

Descriptive Name
MORPHOACCESS

Figure 83: MorphoAccess® SIGMA Lite Series Terminal Firmware Version information

1. The current terminal firmware version information is displayed

This document and the information therein are the property of Morpho. They must not be copied or communicated to a third party without the prior authorization of Morpho

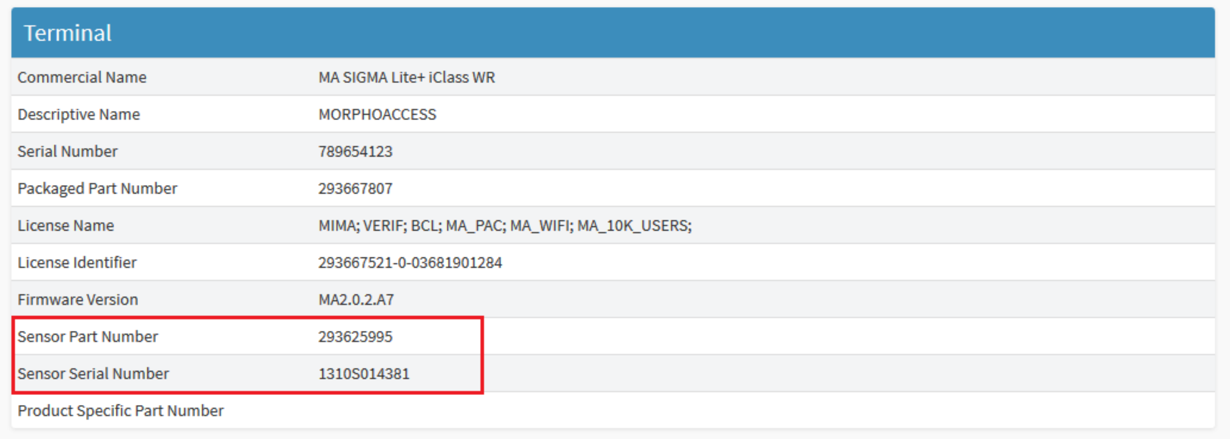
View Sensor Information

Using this functionality, an administrator can view the information related to the biometric sensor.

Access Path

Webserver > Terminal Info > Terminal

Screens & Steps



Terminal

Commercial Name	MA SIGMA Lite+ iClass WR
Descriptive Name	MORPHOACCESS
Serial Number	789654123
Packaged Part Number	293667807
License Name	MIMA; VERIF; BCL; MA_PAC; MA_WIFI; MA_10K_USERS;
License Identifier	293667521-0-03681901284
Firmware Version	MA2.0.2.A7
Sensor Part Number	293625995
Sensor Serial Number	1310S014381
Product Specific Part Number	

Figure 84: Biometric Sensor data

1. **Sensor Part Number**
2. **Sensor Serial Number** is displayed

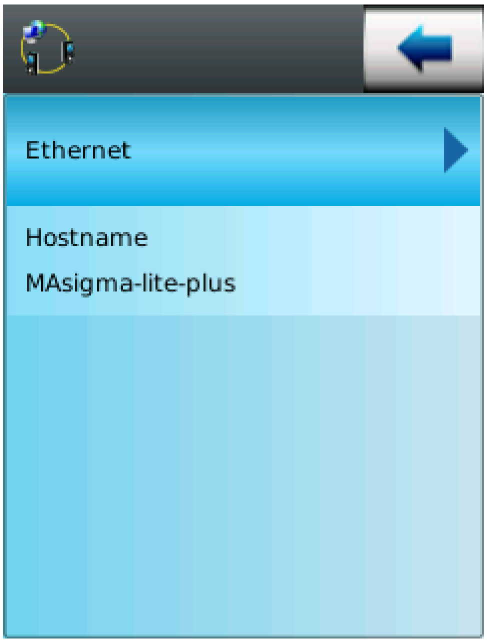
View Communication Parameters

Under Communication, an administrator can view the information of various networks, through which the terminal is connected with distant systems.

Access Path

Information > Communication

Screens & Steps



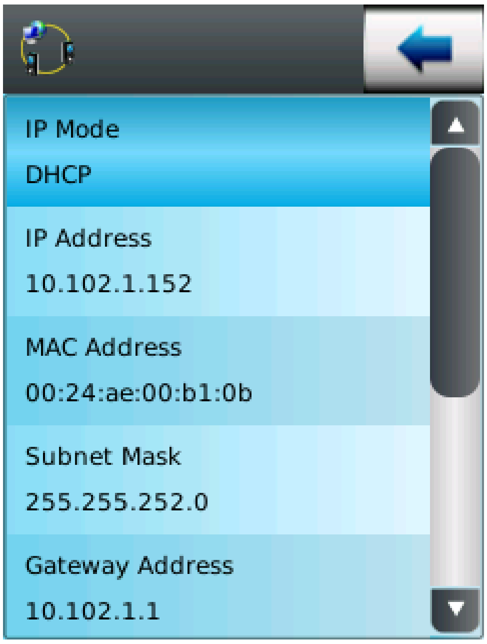
Ethernet

Hostname

MAsigma-lite-plus

Figure 85: Selecting communication network

1. Select the type of communication network from following options :
    a. Ethernet
    b. WLAN
    c. Hostname



IP Mode
DHCP

IP Address
10.102.1.152

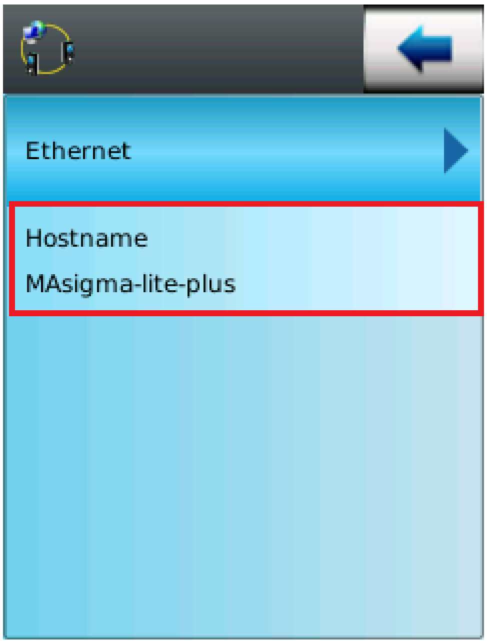
MAC Address
00:24:ae:00:b1:0b

Subnet Mask
255.255.252.0

Gateway Address
10.102.1.1

Figure 86: Viewing information of Ethernet network

2. Under Ethernet, select **IPV4** or **IPV6**
3. Following information is displayed, of an IP connection :
    a. **IP Mode** i.e. Static or DHCP
    b. **IP Address** of the terminal
    c. **MAC Address** of the terminal
    d. **Subnet Mask**
    e. **Gateway Address**
    f. **Preferred DNS Address**
    g. **Alternate DNS Address**



Ethernet

Hostname
MAsigma-lite-plus

Figure 87: View Hostname of the terminal

4. **Hostname** of the terminal is displayed

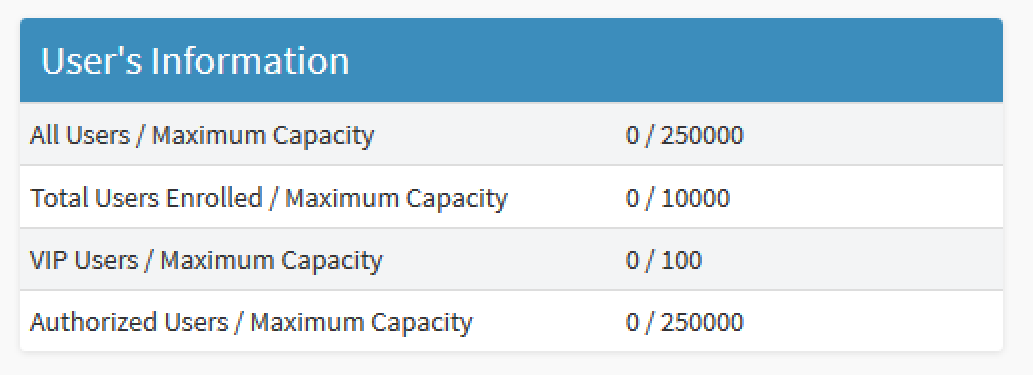
View User Status

User Status gives to an administrator the summary of number of enrolled users, number of authorized listed users and number of VIP users.

Access Path

Webserver > Terminal Info > User's Information

Screens & Steps



User's Information

All Users / Maximum Capacity	0 / 250000
Total Users Enrolled / Maximum Capacity	0 / 10000
VIP Users / Maximum Capacity	0 / 100
Authorized Users / Maximum Capacity	0 / 250000

Figure 88: View User Status

Under User Status information section, following information is displayed:

1. **Number of Users Enrolled** in the terminal is displayed
2. **Maximum enrolled user capacity** indicates the maximum number of users can be enrolled. Basic capacity of terminal is to store 3,000 users' database. This capacity can be increased up to 10,000 user's records, by implementing users' license. Refer to *User licenses* for more information.
3. **Number of Authorized List Users**, the users enrolled as Authorized listed users
4. **Maximum Authorized List User Capacity**, indicates the maximum number of users that can be added in authorized list, which is 250,000 users by default
5. **Number of VIP users**, the users enrolled as VIP users. Read more on "Access Control Process for VIP Users"
6. **Maximum VIP user capacity,** indicates the maximum capacity of the users that can be enrolled as VIP users, that is 100 users by default

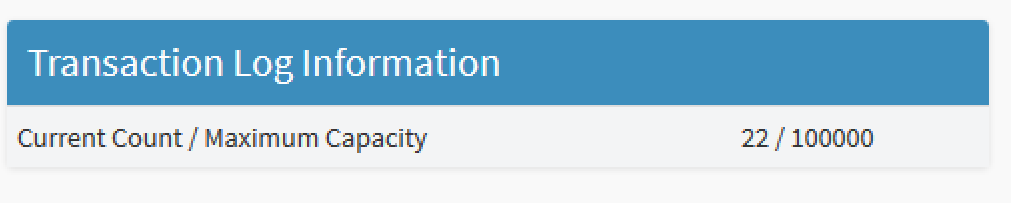
View Transaction Log Status

Transaction log status shows the number of current logs recorded in terminal database. Also the maximum capacity of logs that can be stored in terminal is displayed.

Access Path

Webserver > Terminal Info > Transaction Log Information

Screens & Steps



Transaction Log Information

Current Count / Maximum Capacity	22 / 100000

Figure 89: Transaction Log Status is displayed

1. **Current Log Count** stored in terminal is displayed
2. **Maximum Log Capacity**, the maximum number of transaction logs that can be stored in terminal is displayed

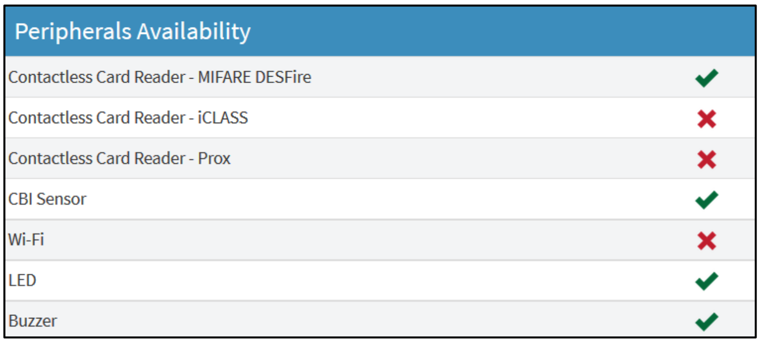
View Peripherals Availability

Peripherals availability shows the available peripherals to the terminal.

Access Path

Webserver > Terminal Info > Peripherals Availability

Screens & Steps



Peripherals Availability	
Contactless Card Reader - MIFARE DESFire	✓
Contactless Card Reader - iCLASS	✗
Contactless Card Reader - Prox	✗
CBI Sensor	✓
Wi-Fi	✗
LED	✓
Buzzer	✓

Figure 90: Available Peripherals to the terminal is displayed

1. All the available peripherals to the terminal are displayed with a “✓” symbol
2. All the peripherals unavailable but can be configured to the terminal are displayed with a “✗” symbol

Reboot Terminal Menu

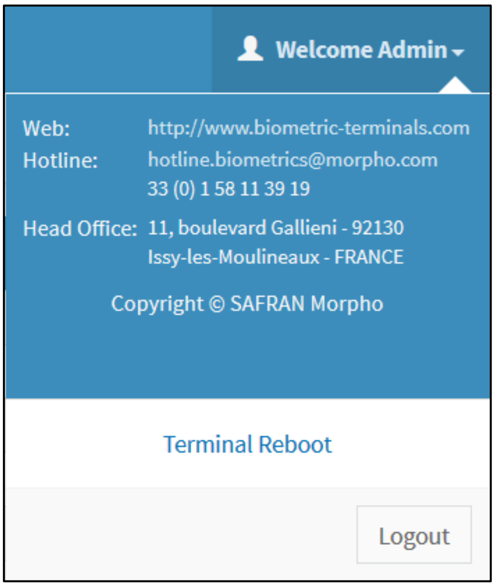
Reboot of Terminal is performed to restart the terminal (soft restart). Reboot is required in following scenarios:

On firmware upgrade

Connection of Wi-Fi™ USB Adapter

When terminal protocol is changed to ‘Legacy L1’ or ‘Legacy Morpho’ or ‘MA5G’

After installation of a new license which upgrade terminal features



Web: http://www.biometric-terminals.com
Hotline: hotline.biometrics@morpho.com
33 (0) 1 58 11 39 19
Head Office: 11, boulevard Gallieni - 92130
Issy-les-Moulineaux - FRANCE
Copyright © SAFRAN Morpho

Figure 91: Reboot Device

After reboot all the settings are kept. To reset the terminal to default factory settings please use the corresponding function Set Factory Defaults.

Log Menu

The MorphoAccess® SIGMA Lite Series terminal records each event taken place on a terminal. The logs that has both action triggered and result given by terminal are called transaction logs. The events that can be logged are:

- Access granted to the user
- Access denied to the user
- Time and Attendance actions
- Error occurred
- Etc…

NOTE: The events that user has cancelled are not logged

All events are recorded in a local file. The log created has various information fields, such as User ID, Name of User, Time of action triggered, Biometric Matching Score, Action Status, Action etc.

The MorphoAccess® SIGMA Lite Series terminal can store up to 100,000 transaction logs in the database, by default. However, the capacity of storing logs in terminal database can be increased by installing *Logs licenses*.

In order to view transaction logs, an administrator requires to retrieve transaction logs through Webserver.

In subsequent sections of Logs Menu, the parameters that can be configured by Administrator are explained.

Configure Transaction Logging Mode

Using this functionality an administrator can select which event has to be logged:

No Log: An administrator can set Transaction Logging to ‘No Log’ mode. This indicates that no actions will be recorded and stored on terminal

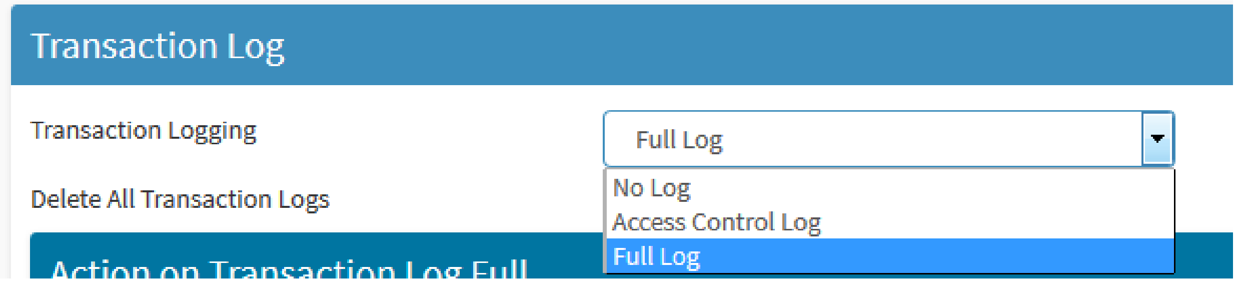
Access Control Log: This mode indicates that only user access request (successful and failed user control) should be recorded and stored

Full Log: This mode indicates that all the events taken place on terminal including configurations done, time and attendance actions, errors, etc. are captured and stored in terminal.

Access Path

Webserver > Logs

Screens & Steps



Transaction Log

Transaction Logging: Full Log

Figure 92: Selecting Transaction Logging Mode

1. Select **Transaction Logging** as ‘No Log’, ‘Access Control Log’ or ‘Full Log’
2. Press on **Save** button to save settings

Results

As per the selected mode of logging, transaction logs are created by terminal. In case terminal fails to store log parameter, an error message is displayed.

Action on Transaction Log Full

Using this functionality an administrator can select the action to perform when there is no room for a new log record:

Delete Partial Logs

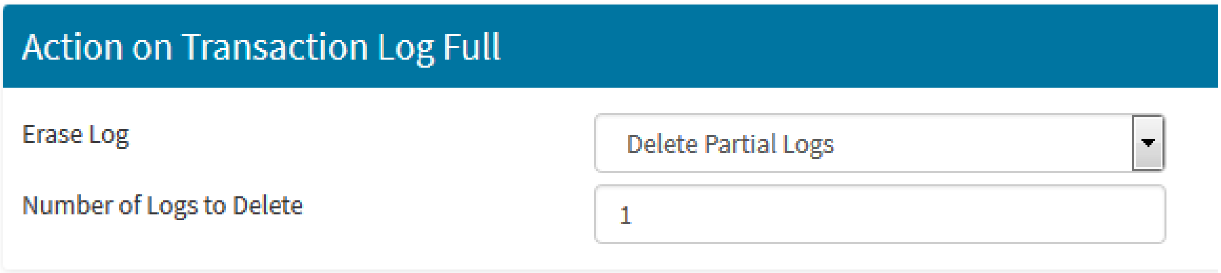
Delete Full Logs

Based on this configuration, terminal will delete logs entirely or partially, when log full event occurs.

Access Path

Webserver > Logs > Action on Transaction Log Full > Erase Log

Screens & Steps



Action on Transaction Log Full

Erase Log	Delete Partial Logs
Number of Logs to Delete	1

Figure 93: Setting Erase Log Status

1. Select Erase **Log Status** as:
   a. **Delete Partial Logs**, if specific number of logs should be deleted when transaction log file is full. With this terminal allow to configure **Number of Logs to Delete** when transaction log is full
   b. **Delete All Logs**, if all logs stored in database should be deleted when transaction log file is full
2. Press on **Save** button to save settings

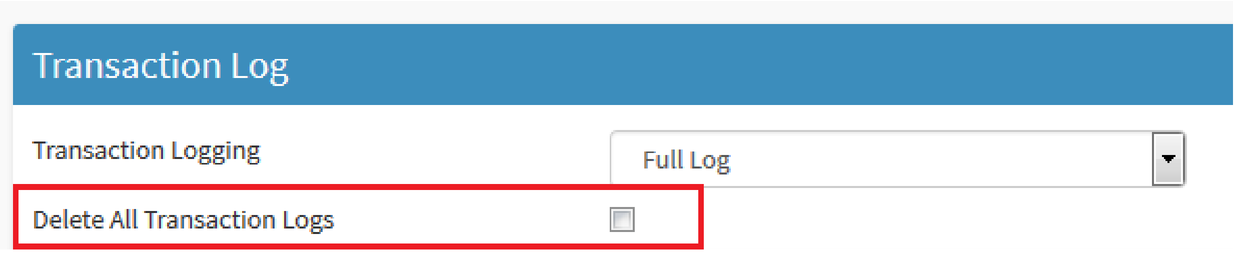
Delete Transaction Logs

Using this functionality, an administrator can delete all transaction logs recorded and stored in terminal database.

Access Path

Webserver > Logs > Transaction Log > Delete All Transaction Logs

Screens & Steps



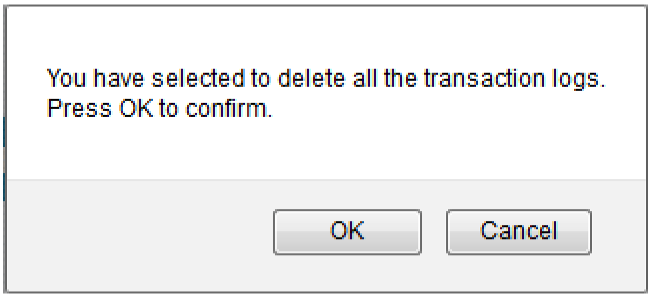
Transaction Log

Transaction Logging: Full Log

Delete All Transaction Logs □

Figure 94: Delete All Transaction logs

1. Select **Delete All Transaction Logs and press on Save button**
2. A confirmation message will pop-up to confirm an action to delete all transaction logs



You have selected to delete all the transaction logs.
Press OK to confirm.

Figure 95: Confirmation Message to Delete All Logs

3. Press on **OK** button to delete. An administrator can Press on **Cancel** button to cancel

Results

A success message is displayed. All Transaction Logs are deleted from the database.

Error Log Configuration

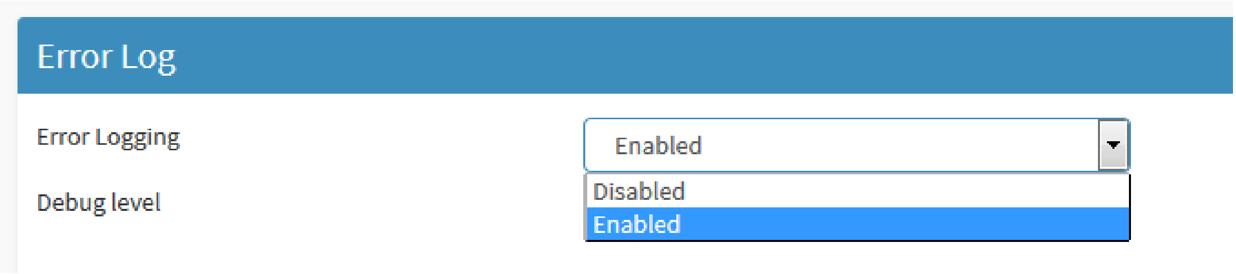
MorphoAccess® SIGMA Lite Series terminal is capable of capturing logs of all the events performed on the terminal.

Using Error log configuration feature, an administrator can enable/disable error logging, and configure related parameters.

Access Path

Webserver > Logs > Error Log > Error Logging

Screens & Steps



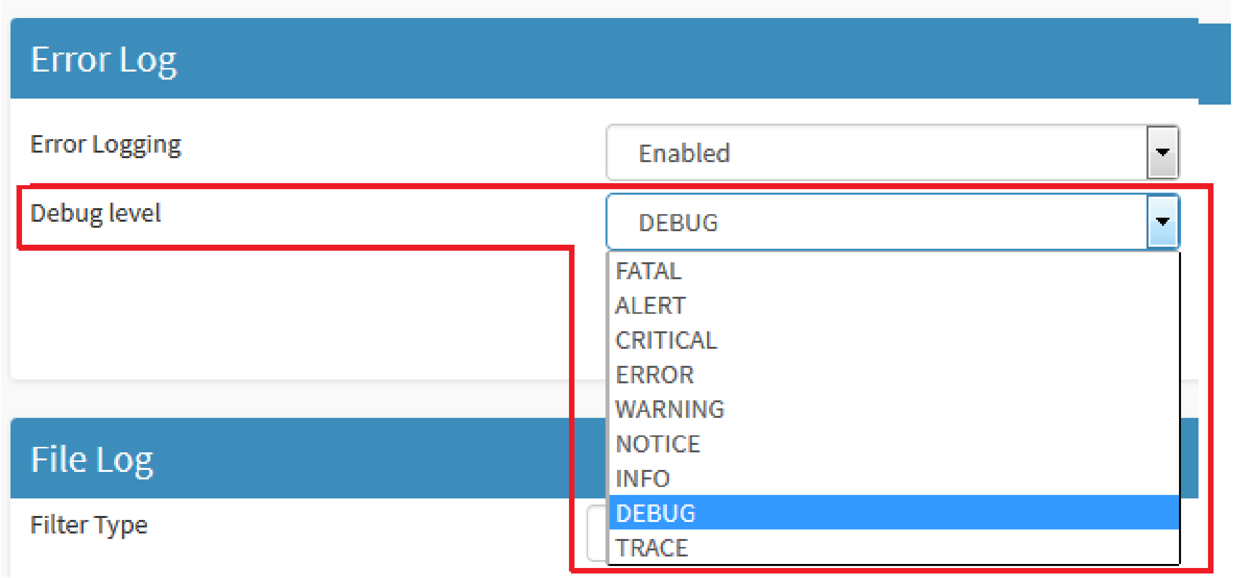
Error Log

Error Logging: Enabled

Debug level

Figure 96: Error Log Configuration (Enabled/Disabled)

1. Select **Error Log Configuration**
2. Select **Error Log** as ON, to enable error logging.



Error Log

Error Logging: Enabled

Debug level: DEBUG

Figure 97: Setting Error Log Debug Level

3. Select **Debug Level** from the available list

a. Fatal
b. Alert
c. Critical
d. Error
e. WARNING
f. Notice
g. Info
h. Debug
i. Trace

NOTE: The selected debug level error logs as well as the error logs that fall into previous levels will also be included in the Error Log File. For example, if an administrator selected the debug level as 'Debug', then the Error Log file will consist the logs of debug level as well as the logs of previous levels such as Fatal, Alert, Critical, Error, WARNING, Notice and Info.

4. Press on **SAVE** button to save settings

Results

Error logs are captured and stored in terminal in encrypted format.

View Transaction Logs

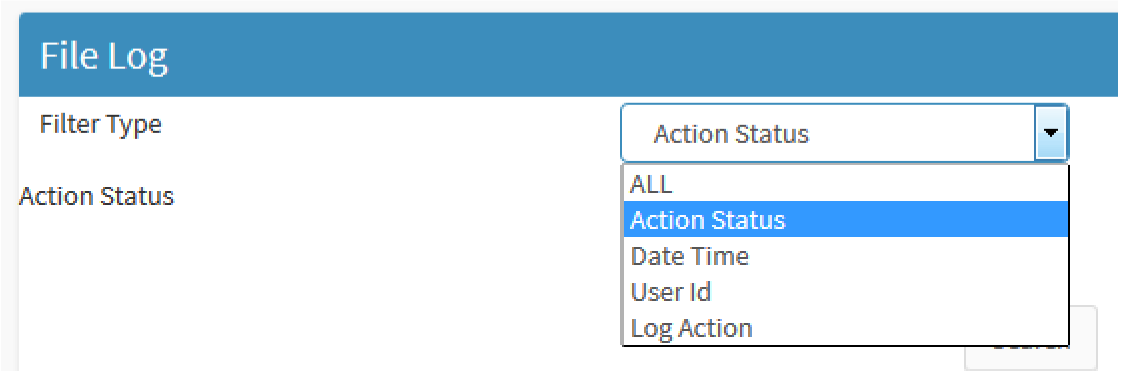
Access Path

Webserver > Logs > File Log

Pre-requisites

Transaction Logging Mode must be enabled, then only transaction logs are recorded in terminal

Screens & Steps



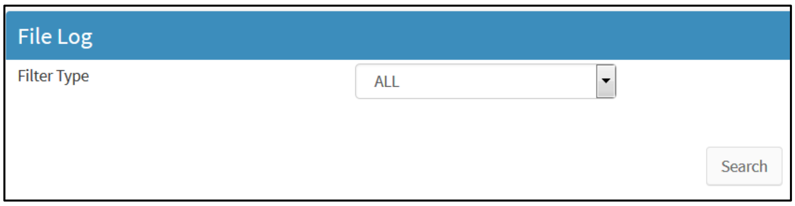
File Log

Filter Type: Action Status

Action Status

Figure 98: Retrieve Transaction Log

1. Select the filter type that an administrator requires to view the transaction logs

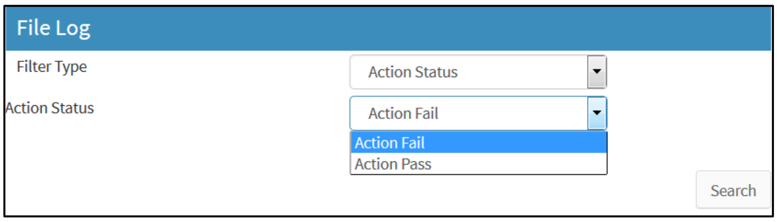


File Log

Filter Type: ALL

Figure 99: Retrieve Logs with Filter Type - ALL

2. Select the Filter Type as ALL to retrieve all the transaction logs.



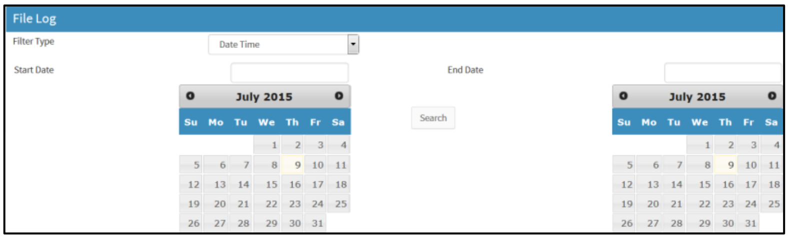
File Log

Filter Type: Action Status

Action Status: Action Fail

Figure 100: Retrieve Logs with Filter Type – Action Status

3. Select the Filter Type as Action Status. Select the Action Status as Action Fail/Pass to retrieve the transaction logs with the corresponding Action Type



File Log

Filter Type: Date Time

Start Date

End Date

July 2015

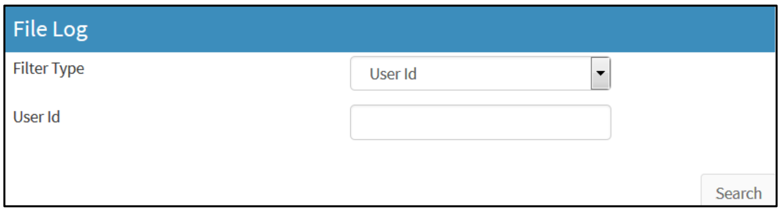
Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

July 2015

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Figure 101: Retrieve Logs with Filter Type – Date Time

4. Select the Filter Type as Date Time to select the time period range of the logs to be retrieved



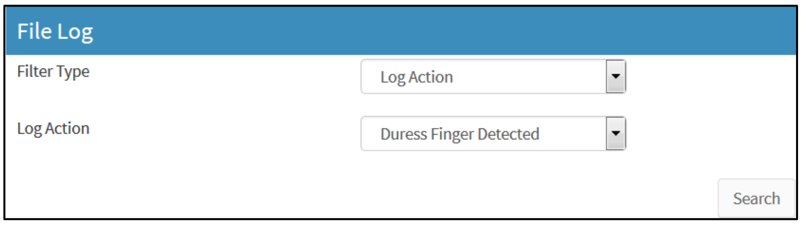
File Log

Filter Type: User Id

User Id

Figure 102: Retrieve Logs with Filter Type – User ID

5. Select the Filter Type as User Id to retrieve the transaction logs of a particular User ID only.



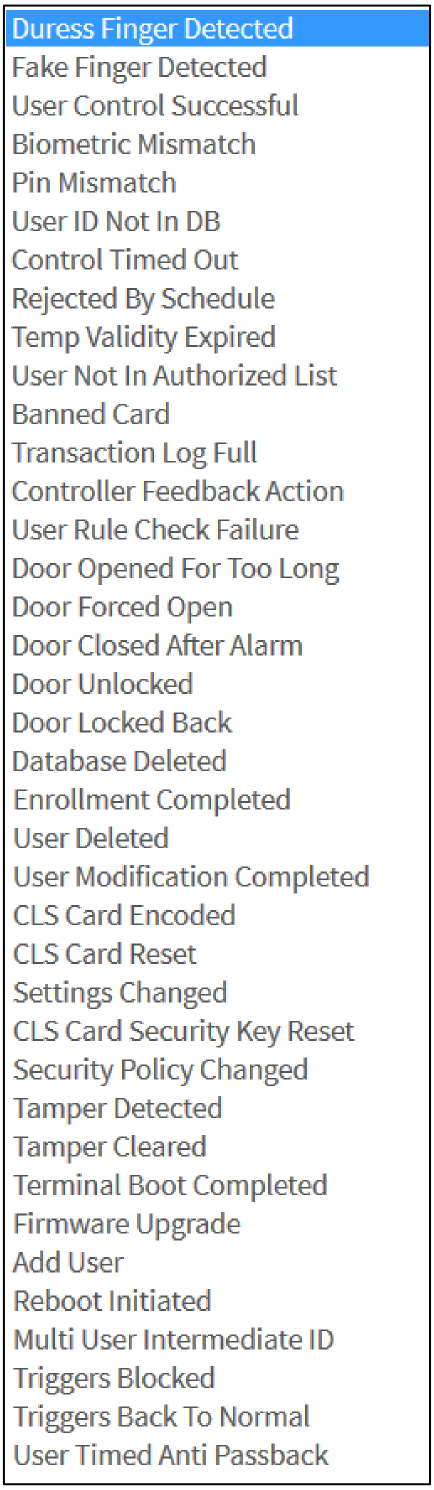
File Log

Filter Type: Log Action

Log Action: Duress Finger Detected

Figure 103: Retrieve Logs with Filter Type – Log Action

6. Select the Filter Type as Log Action to retrieve the transaction logs with a particular Action only.



- Duress Finger Detected
- Fake Finger Detected
- User Control Successful
- Biometric Mismatch
- Pin Mismatch
- User ID Not In DB
- Control Timed Out
- Rejected By Schedule
- Temp Validity Expired
- User Not In Authorized List
- Banned Card
- Transaction Log Full
- Controller Feedback Action
- User Rule Check Failure
- Door Opened For Too Long
- Door Forced Open
- Door Closed After Alarm
- Door Unlocked
- Door Locked Back
- Database Deleted
- Enrollment Completed
- User Deleted
- User Modification Completed
- CLS Card Encoded
- CLS Card Reset
- Settings Changed
- CLS Card Security Key Reset
- Security Policy Changed
- Tamper Detected
- Tamper Cleared
- Terminal Boot Completed
- Firmware Upgrade
- Add User
- Reboot Initiated
- Multi User Intermediate ID
- Triggers Blocked
- Triggers Back To Normal
- User Timed Anti Passback

Figure 104: List of Various Log Action

This document and the information therein are the property of Morpho. They must not be copied or communicated to a third party without the prior authorization of Morpho

Terminal Settings Menu

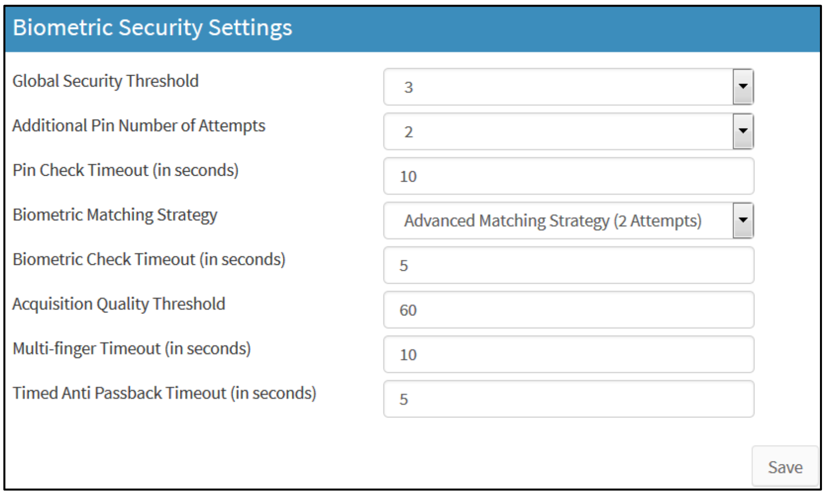
Biometric Security Settings

Biometric Security parameters can be configured from Webserver. Using these parameters an administrator can control the level of security of biometric comparison to prevent from false rejection of authentic users.

Access Path

Webserver > Terminal Settings > Biometric

Screens & Steps



Biometric Security Settings

Global Security Threshold: 3

Additional Pin Number of Attempts: 2

Pin Check Timeout (in seconds): 10

Biometric Matching Strategy: Advanced Matching Strategy (2 Attempts)

Biometric Check Timeout (in seconds): 5

Acquisition Quality Threshold: 60

Multi-finger Timeout (in seconds): 10

Timed Anti Passback Timeout (in seconds): 5

Figure 105: Biometric Security Settings

1. Select the Global Security Threshold Level for matching biometric data. This parameter allows controlling the false rejection rate and false acceptance rates. An administrator can set threshold level between level 0 to level 10. Refer to *Setting-up Matching Security Threshold*
2. for False Acceptance Ratio at each level.
3. **Addition Pin Number of Attempts:** This allows the number of attempts allowed to a user to enter the Pin
4. **PIN check Timeout**: The duration within which user have to enter the PIN
5. **Biometric Matching Strategy:** It can be selected with multiple options.
6. **Biometric check Timeout**: The duration within which user has to place finger on biometric sensor
7. **Acquisition Quality Threshold**: It is the Parameter to set quality threshold used during a user enrolment.

This document and the information therein are the property of Morpho. They must not be copied or communicated to a third party without the prior authorization of Morpho

8. **Multi Finger Timeout**: The duration within which the second user has to complete authentication when Additional User Authentication is required.
9. **Timed Anti Passback Timeout**: The duration within which a user cannot perform successful user control repeatedly on a terminal.
10. Click on **Save** to save settings

Communication Settings

MorphoAccess® SIGMA Lite Series terminals are standalone terminals, it means the configuration and operations are performed without any connection to a host application. However, MorphoAccess® SIGMA Lite Series Terminal is required to communicate with distant applications such as door controller, access controller or hosted application like Webserver. Communication with distant systems can be done to perform:

Require the conclusion of access rights check to a Central Access Controller, to grant or deny access to user

terminal configuration

terminal maintenance: firmware upgrade, add a license (to unlock an optional feature)

database management: add, modify or remove a user

log file management: get or delete log file

Wi-Fi™ connection configuration

There are several communication channels which can be used to connect with distant systems like through Ethernet channel, Wi-Fi™ network, 3G/GPRS network or Serial channel. Refer section *Connecting the Terminal to a PC* to understand in detail.

Using Communication Menu, an administrator can configure network parameters to enable communication with distant systems. Only an administrator with Full Admin Rights can access this menu.

An administrator can set the network parameters which are used for communication of MorphoAccess® SIGMA Lite Series terminals with distant systems such as external access controller. Network parameters of Serial Channel, Ethernet and WLAN connections are configurable from Webserver.

An administrator can also set the network security parameters which will restrict the access to terminal from specific IP or IP Range. Apart from the defined IP, none other IP can access/communicate with terminal.

Security recommendation

To avoid security break, it is recommended to disable unused communication channels. But be sure to let at least one way to configure the terminal.

Ethernet Network Configuration

MorphoAccess® SIGMA Lite Series terminal can be connected to devices (such as central access controller, and door controller) via Ethernet. Under Ethernet configuration, an administrator can configure an IP Mode, which can be static or DHCP (dynamic).

When IP mode is DHCP, an IP address of the terminal is set and updated automatically. While in Static mode an IP Address and related settings are done manually.

NOTE: Terminal can support connection through Ethernet and Wi-Fi™ both simultaneously.

Access Path

Webserver > Terminal Settings > Communication

Pre-requisites

For Wi-Fi™ Network connection:

Wi-Fi™ USB dongle should be plugged

MA_WI-FI license should be installed on terminal

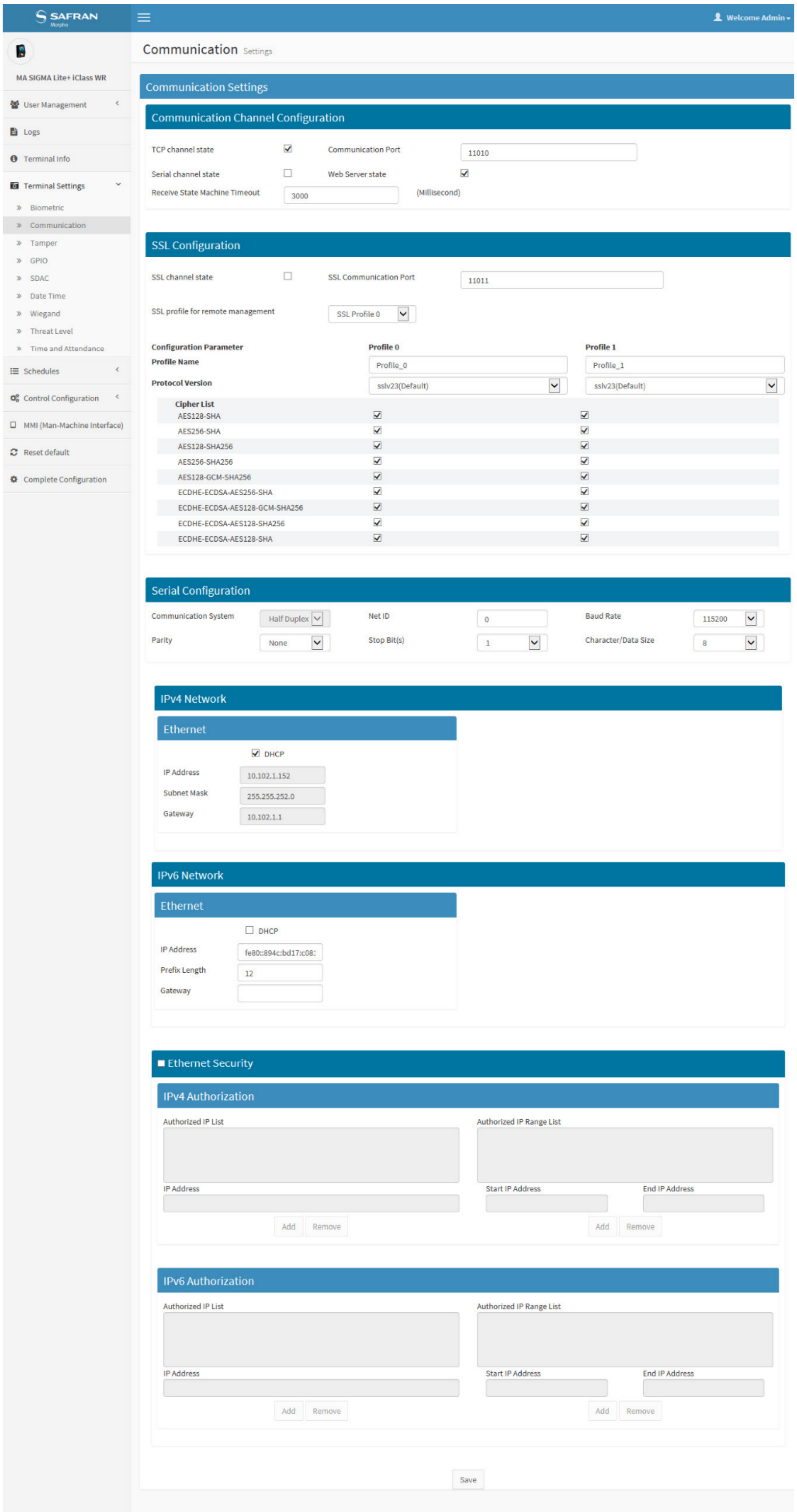
Steps to Configure an Ethernet Network

1. Select **IPv4 or IPv6 Network**
2. Under IPv4 or IPv6, an administrator can select **Ethernet**
3. The default IP Mode is selected as DHCP for IPv4 and Static for IPv6.
4. An administrator can select **IP Mode** as ‘Static’ or ‘DHCP’
5. Click on **SAVE** to save the settings Under Static IP Mode.
6. An administrator can manually configure ‘IP Address’ of the terminal, ‘Subnet Mask’, 'Network Mask', 'Gateway Address' and 'DNS Servers’

Results

Once the Ethernet Configuration is done, the terminal is connected to a distant server. An administrator can also set the IP restriction for preventing terminal from unauthorized access. These settings can be done from Security menu, refer below section.

Screens & Steps



Communication Settings

Communication Settings

Communication Channel Configuration

TCP channel state ☑ Communication Port 11010

Serial channel state ☐ Web Server state ☑

Receive State Machine Timeout 3000 (Millisecond)

SSL Configuration

SSL channel state ☐ SSL Communication Port 11011

SSL profile for remote management SSL Profile 0

Configuration Parameter	Profile 0	Profile 1
Profile Name	Profile_0	Profile_1
Protocol Version	sslv23(Default)	sslv23(Default)
Cipher List		
AES128-SHA	☑	☑
AES256-SHA	☑	☑
AES128-SHA256	☑	☑
AES256-SHA256	☑	☑
AES128-GCM-SHA256	☑	☑
ECDHE-ECDSA-AES256-SHA	☑	☑
ECDHE-ECDSA-AES128-GCM-SHA256	☑	☑
ECDHE-ECDSA-AES128-SHA256	☑	☑
ECDHE-ECDSA-AES128-SHA	☑	☑

Serial Configuration

Communication System Half Duplex Net ID 0 Baud Rate 115200

Parity None Stop Bit(s) 1 Character/Data Size 8

IPv4 Network

Ethernet

☑ DHCP

IP Address 10.102.1.152

Subnet Mask 255.255.252.0

Gateway 10.102.1.1

IPv6 Network

Ethernet

☐ DHCP

IP Address fe80::894c:bd17:c08:

Prefix Length 12

Gateway

■ Ethernet Security

IPv4 Authorization

Authorized IP List

IP Address

Add Remove

Authorized IP Range List

Start IP Address End IP Address

Add Remove

IPv6 Authorization

Authorized IP List

IP Address

Add Remove

Authorized IP Range List

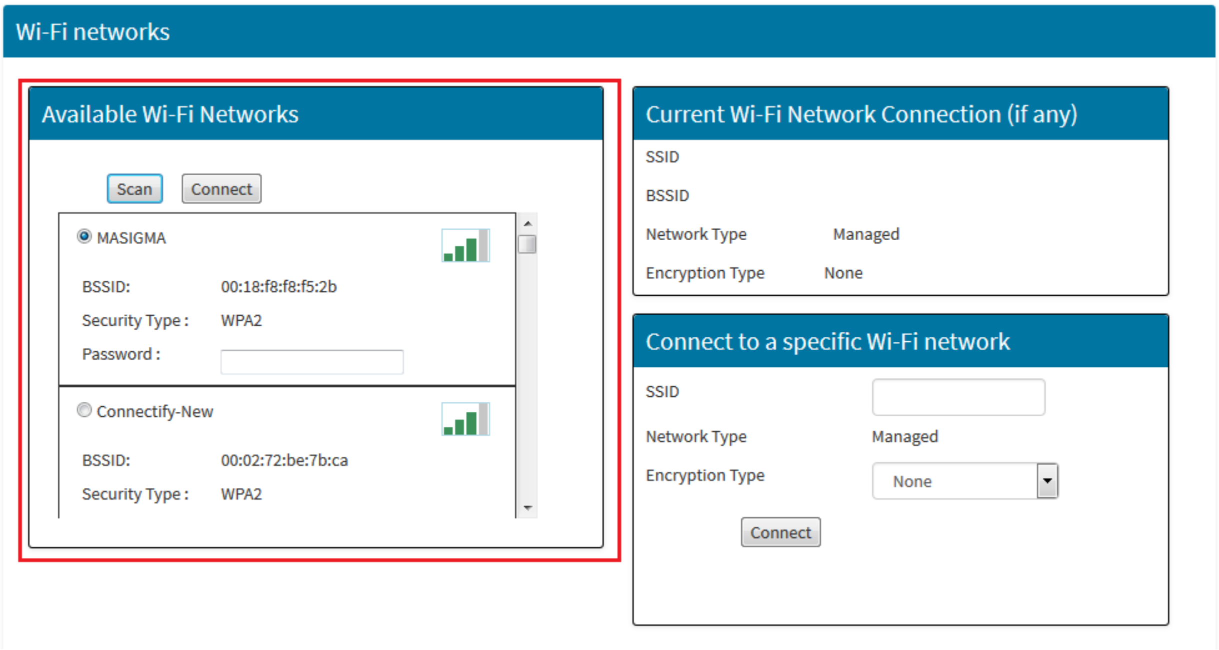
Start IP Address End IP Address

Add Remove

Save

Figure 106: Network parameters settings through Webserver

1. **Serial Configuration**: When terminal is connected to distant systems, through Serial Port
    a. **Communication System:** Select Half Duplex
    b. **Net ID:** Enter Net ID
    c. **Protocol Baud Rate:** Select one of the preset values (such as 115200 Bd)
    d. **Parity:** An administrator can select 'None', 'ODD' or 'Even'. Parity bit is used for checking whether the data is sent from one terminal to other is same. If an administrator selects ODD, then parity is on ODD number
    e. **Stop Bit(s):** Set stop bit length. Default value is set as 1
    f. **Character/Data Size:** An administrator can set character size as 7 or 8 bits
2. **Ethernet Configuration**: When terminal is connected through Ethernet Cable
    a. Enter parameters for IPv4 or IPv6 protocol
    b. Select **IP Mode** as DHCP. If an administrator do not select DHCP, then by default the IP mode will be static and an administrator must enter the IP address manually
    c. **IP Address**, **Subnet Mask** and **Gateway** is displayed automatically when DHCP mode is enabled
3. **Wi-Fi™ Configuration (WLAN):** When terminal is connected through Wi-Fi™ Network. The "Available Wi-Fi networks" area provides a scan command for available Wi-Fi™ networks, and a connect command to an available Wi-Fi™ networks (found by scan command). Wi-Fi™ adaptor must be plugged to the terminal and MA_WIFI license installed in the terminal.
    a. Enter parameters for IPv4 or IPv6 protocol
    b. Select **IP Mode** as DHCP. If an administrator does not select DHCP, then by default the IP mode will be static and the administrator needs to enter the IP address manually
    c. **IP Address**, **Subnet Mask** and **Gateway** is displayed automatically
4. Setting **Ethernet Security** by setting IP Authorization for IPv4 or IPv6
    a. For authorizing an IP address, enter IP Address in the field and click on **Add**
    b. For authorizing IP addresses range, enter Start IP Address and End IP Address in the fields and click on **Add**


Wi-Fi networks
Available Wi-Fi Networks
Scan
Connect
Current Wi-Fi Network Connection (if any)
Connect to a specific Wi-Fi network
Connect

● MASIGMA

BSSID: 00:18:f8:f8:f5:2b

Security Type : WPA2

Password :

○ Connectify-New

BSSID: 00:02:72:be:7b:ca

Security Type : WPA2

SSID

BSSID

Network Type Managed

Encryption Type None

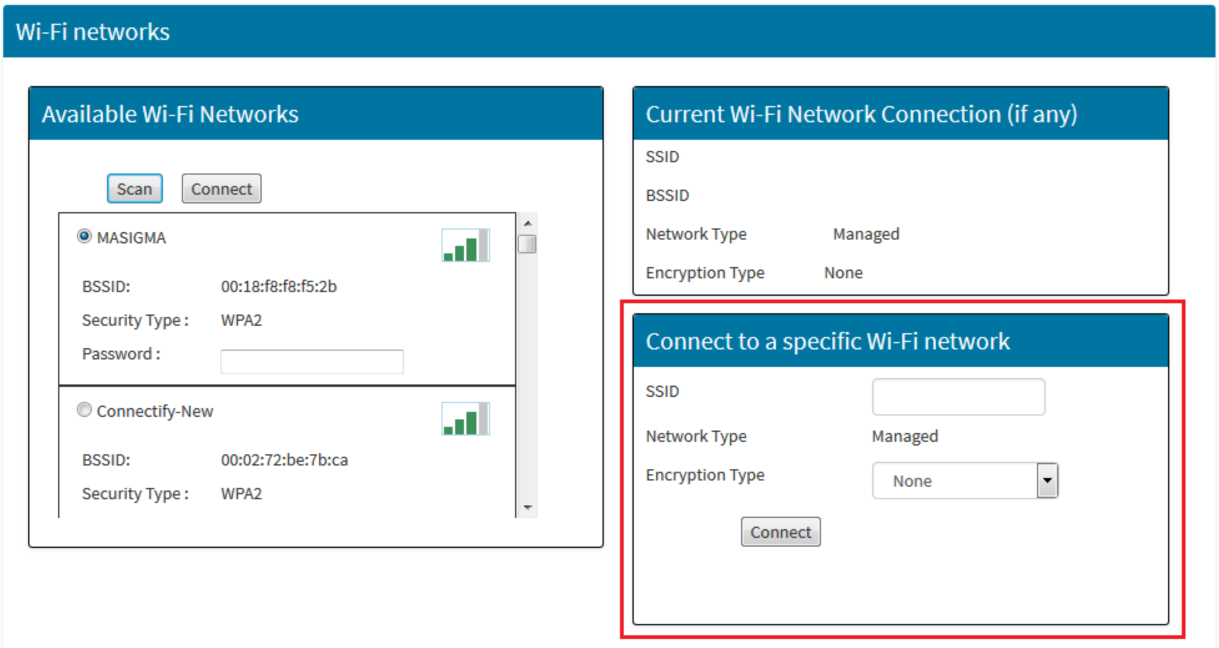
SSID

Network Type Managed

Encryption Type None

Figure 107: Configuring Wi-Fi™ Network

5. **Scan and connect to Wi-Fi™ Network**
   a. Click on **Scan**, the available network is displayed
   b. Enter the **Password**
   c. Click on **Connect**


Wi-Fi networks
Available Wi-Fi Networks
Scan
Connect
Current Wi-Fi Network Connection (if any)
Connect to a specific Wi-Fi network
Connect

● MASIGMA

BSSID: 00:18:f8:f8:f5:2b

Security Type : WPA2

Password :

○ Connectify-New

BSSID: 00:02:72:be:7b:ca

Security Type : WPA2

SSID

BSSID

Network Type Managed

Encryption Type None

SSID

Network Type Managed

Encryption Type None

Figure 108: Configuring Wi-Fi™ Network manually

6. Use **Connect to a specific Wi-Fi™ Network** to manually set up a hidden Wi-Fi™ network
    a. Enter **SSID**
    b. **Network Type** is displayed as Managed or Ad hoc,
        i. **Managed** network indicates that the Wi-Fi™ network is connected through a centralized access point
        ii. **Ad hoc** network allows wireless devices to directly communicate with each other without any need to connect to centralized access point or a router
    c. Select **Encryption Type** as Open, WEP, WPA, WPA2; used for Wi-Fi™ network security to prevent unauthorized access to Wi-Fi™ network
    d. Enter **Encryption Key**
    e. Click on **Connect**
7. Click on **Save**

SSL Configuration

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are cryptographic protocol designed to provide communication security over Ethernet or Wi-Fi™ channels.

These protocols are used to protect the communication between the MorphoAccess® SIGMA Lite Series terminal and a distant system, such as a central access controller or a terminal configuration station.

The cryptographic protocols supported by the terminal are listed below:

SSLv3

SSLv23

TLS 1.0

TLS 1.1

TLS 1.2

The terminal supports the algorithms listed below for communication security:

AES128-SHA OpenSSL cipher suite

AES256-SHA OpenSSL cipher suite

AES128-SHA256 OpenSSL cipher suite

AES256-SHA256 OpenSSL cipher suite

AES128-GCM-SHA256 OpenSSL cipher suite

ECDHE-ECDSA-AES256-SHA OpenSSL cipher suite

ECDHE-ECDSA-AES128-GCM-SHA256 OpenSSL cipher suite

ECDHE-ECDSA-AES128-SHA256 OpenSSL cipher suite

ECDHE-ECDSA-AES128-SHA OpenSSL cipher suite

NOTE: The communication security is automatically configured during negotiation between the client and the server. The client specifies the security level requested, and the server accepts or proposes a lower level. The client accepts it or cancels its request. The final configuration corresponds to the higher security level common with the client and the server.

Compatibility of cipher algorithms with SSL protocol versions

Cipher Algorithm List	Protocol Version				
	sslv2.3	sslv3	tlsv1	tlsv1.1	tlsv1.2
AES128-SHA	Y	Y	Y	Y	Y
AES256-SHA	Y	Y	Y	Y	Y
AES128-SHA256	N	N	N	N	Y
AES256-SHA256	N	N	N	N	Y
AES128-GCM-SHA256	N	N	N	N	Y
ECDHE-ECDSA-AES256-SHA:ECDH-ECDSA-AES256-SHA	Y	Y	Y	Y	Y
ECDHE-ECDSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256	N	N	N	N	Y
ECDHE-ECDSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256	N	N	N	N	Y
ECDHE-ECDSA-AES128-SHA:ECDH-ECDSA-AES128-SHA	Y	Y	Y	Y	Y

NOTE: Cipher algorithm that ends with ‘SHA256’ supports only SSL protocol version tlsv1.2.

SSL Protocol Versions support for communication

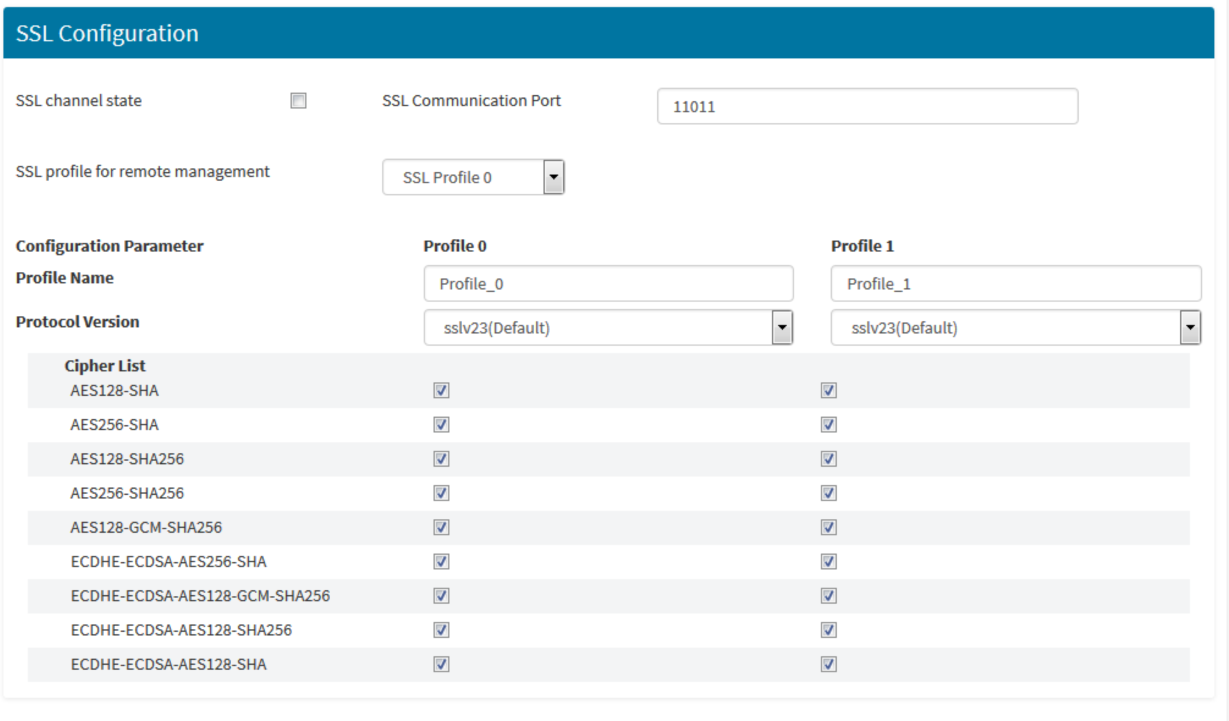
		Client side (from PC application)				
		sslv2.3	sslv3	tlsv1	tlsv1.1	tlsv1.2
On Terminal	sslv2.3	Y	Y	Y	Y	Y
	sslv3	Y	Y	N	N	N
	tlsv1	Y	N	Y	N	N
	tlsv1.1	Y	N	N	Y	N
	tlsv1.2	N	N	N	N	Y

The above table describes the protocol versions supported by client side application, when communication is started by terminal using specific protocol. E.g. If terminal starts communication using sslv2.3 protocol, then client side application will be able to communicate using all the protocol versions. While if communication is initiated using sslv3 protocol, then client application will only support sslv2.3 and sslv3 protocol versions for communication.

Access Path

Webserver > Terminal Settings > Communication > SSL Configuration

Screens & Steps



SSL Configuration

SSL channel state □

SSL Communication Port: 11011

SSL profile for remote management: SSL Profile 0

Configuration Parameter	Profile 0	Profile 1
Profile Name	Profile_0	Profile_1
Protocol Version	sslv23(Default)	sslv23(Default)
Cipher List		
AES128-SHA	☑	☑
AES256-SHA	☑	☑
AES128-SHA256	☑	☑
AES256-SHA256	☑	☑
AES128-GCM-SHA256	☑	☑
ECDHE-ECDSA-AES256-SHA	☑	☑
ECDHE-ECDSA-AES128-GCM-SHA256	☑	☑
ECDHE-ECDSA-AES128-SHA256	☑	☑
ECDHE-ECDSA-AES128-SHA	☑	☑

Figure 109: SSL Configuration

1. Select SSL Configuration
2. Select **Input Channel**
3. Select **SSL Mode** as ON or OFF. Only if the SSL Mode is ON, the SSL protocol is used
4. Enter **Secure Communication Port**: port that will be used for TLS or SSL protocol
5. Use “ Save ” button to save the settings

Serial Channel Communication

Serial Channel is used for transmission of the input/output messages between the MorphoAccess® SIGMA Lite Series terminal and distant systems, such as external controllers, connected through RS485.

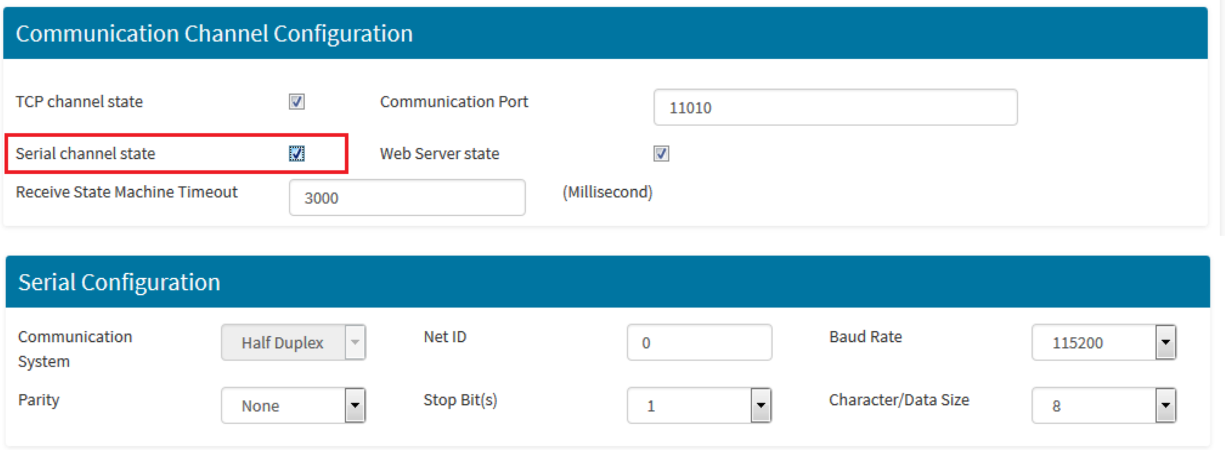
By default, Serial Channel is enabled. If this parameter is disabled, the terminal will not be able to communicate (i.e. input/output messages) with distant systems using Serial channel.

NOTE: Configuration of parameters is not possible in Webserver through Serial Channel.

Access Path

Webserver > Terminal Settings > Communication > Serial Configuration

Screens & Steps



Communication Channel Configuration

TCP channel state ☑

Communication Port 11010

Serial channel state ☑

Web Server state ☑

Receive State Machine Timeout 3000 (Millisecond)

Serial Configuration

Communication System Half Duplex

Net ID 0

Baud Rate 115200

Parity None

Stop Bit(s) 1

Character/Data Size 8

Figure 110: Enabling/Disabling RS485 Serial Chanel

1. Select the **Serial Channel** as ON or OFF
2. Use “ Save ” to Save

Setting-up Matching Security Threshold

The performances of a biometric system are mainly characterized by two values:

- **False Reject Rate (FRR):** number of wrongly rejected authorized users, divided by the number of access requests,
- **False Acceptance Rate (FAR):** number of wrongly admitted unauthorized users, divided by the number of access requests.

With the MorphoAccess® SIGMA Lite Series terminal, the FAR value can be set according to customer request. However the value of these two characteristics is inversely related: when one value is tuned in one direction the other value will change in the other direction.

When user's convenience is the most important factor, the FAR value must be set to a high value (which reduces the FRR value), and conversely if security is more important, then the FAR must be set to a low value (which increases the FRR).

Different tunings are proposed in the MorphoAccess® SIGMA Lite terminal depending on the security level targeted.

Parameter Configuration

The False Acceptance Rate is tuned by a parameter value, i.e. the highest the parameter value is, the lower the FAR value is.

Parameter name	Value	Description
bio_security_settings.matching_threshold	0 to 10	Using this parameter, an administrator can set the threshold for matching the biometric data provided by the user, with the biometric data stored in terminal in user profile.

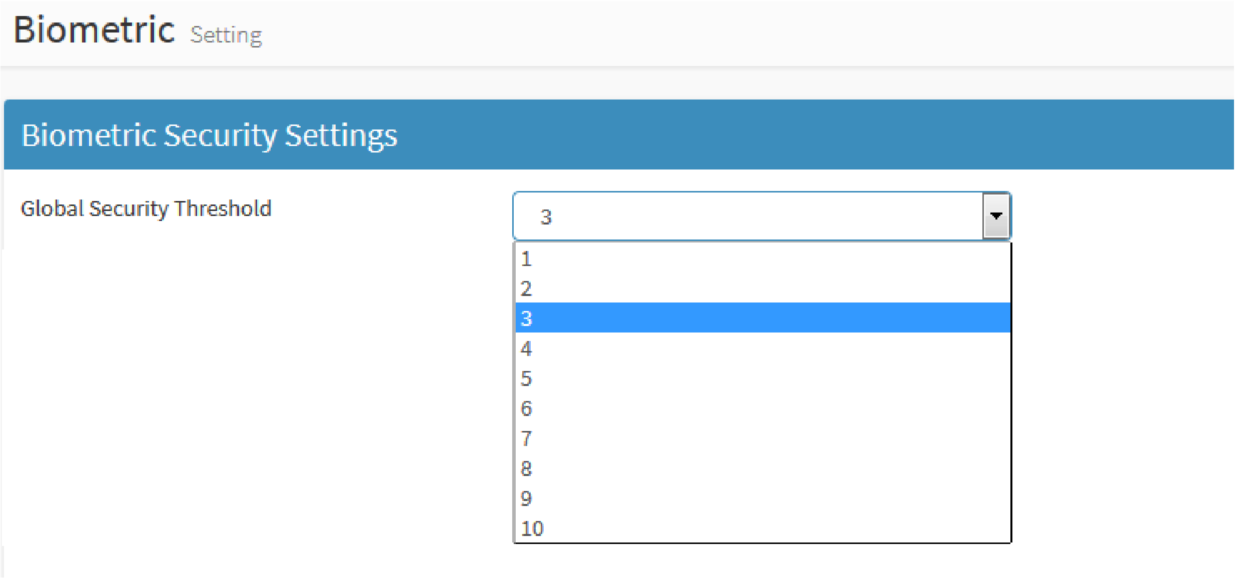
Matching threshold values are detailed in the table below:

Value	Description
0	Lowest threshold value: the number of false rejects is very low, but the number of false acceptances is too high for a secure usage. It is strongly advised not to use this value, because the terminal becomes too tolerant.
1	FAR < 1 %
2	FAR < 0.5 %
3	FAR < 0.1% (Default value) Recommended value for physical access control applications using identification.
4	FAR < 0.05 %
5	FAR < 0.01 %
6	FAR < 0.001 %
7	FAR < 0.0001 %
8	FAR < 0.00001 %
9	FAR < 0.0000001 %
10	Highest threshold value: the number of false acceptance is very low, but the number of false rejections is too high for the comfort of users. It is strongly advised not to use this value, because the terminal becomes too restrictive.

Access Path

Webserver > Terminal Settings > Biometric

Screens & Steps



Biometric Setting

Biometric Security Settings

Global Security Threshold: 3

Figure 111: Setting Security Threshold

1. Select **Global Security Threshold** from values 0 to 10
2. Click on Save to **Save** settings

Results

Terminal performs biometric comparison and uses this threshold to determine the result: match or no match.

Tamper Setting for Terminal Security

MorphoAccess® SIGMA Lite Series terminal can detect two intrusion attempt types:

Someone tries to steal the complete terminal,

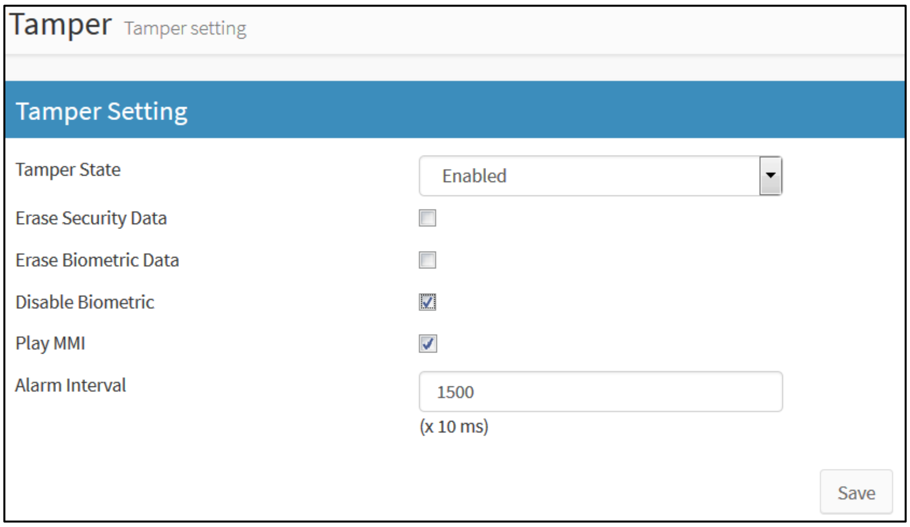
Someone tries to open the terminal

At such intrusions, Tamper switch is triggered on terminal and Tamper alarm is played on terminal. Terminal can also transmit an alarm indication to the central controller using a Wiegand output. For that purpose, contact connections are provided on I/O board (open circuit equals detection).

Access Path

Webserver > Terminal Settings > Tamper

Screens & Steps



Tamper Tamper setting

Tamper Setting

Tamper State: Enabled

Erase Security Data □

Erase Biometric Data □

Disable Biometric ☑

Play MMI ☑

Alarm Interval: 1500 (x 10 ms)

Figure 112: Tamper Settings through Webserver

1. Select **Tamper State** as Disable or Enable. Tamper status is monitored only when tamper state is set to **Enable**.
2. Once an administrator enables Tamper State, it is required to configure below parameters:
    a. **Erase Security Data**: When this parameter is enabled, security data i.e. terminal certificates and contactless card keys, will be deleted from terminal on Tamper detection
    b. **Erase Template Database**: When this parameter is enabled, then on tamper detection, all the templates enrolled and save in the MorphoAccess® SIGMA Lite Series terminal will be deleted

c. **Disable Biometric**: If this parameter is enabled, then under Tamper state user will not be able to do biometric check on the terminal

d. **Play MMI** can be enabled if an administrator requires playing a sound alarm on terminal on tamper detection. The buzzer in the terminal will play

3. Click on **Save**

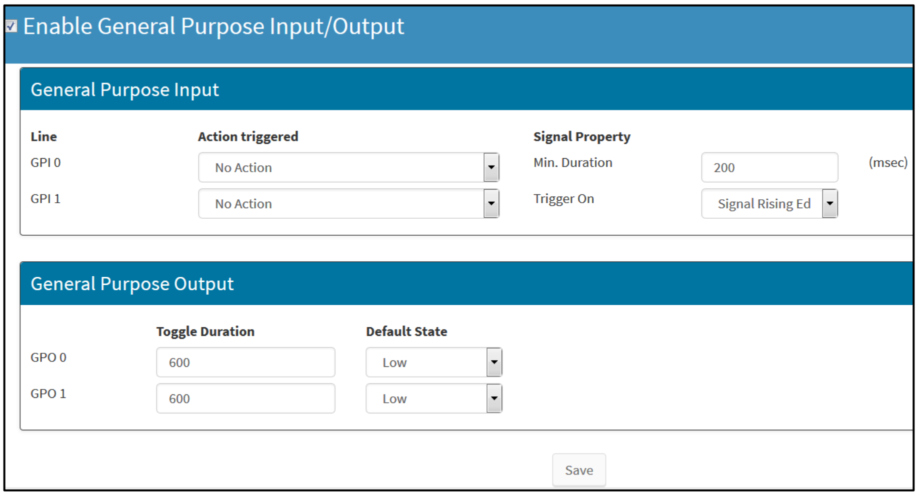
General Purpose Input Output Configuration

General Purpose Input Output (GPIO) mode is used for passing multiple signals to door panel through input-output lines on action triggered on terminal. By default, GPIO Mode is enabled. For More detail please refer *Single Door Controller (SDC) Configuration* section

Access Path

Webserver > Terminal Settings > GPIO

Screens & Steps



☑ Enable General Purpose Input/Output

General Purpose Input

Line	Action triggered	Signal Property		
GPI 0	No Action	Min. Duration	200	(msec)
GPI 1	No Action	Trigger On	Signal Rising Ed	

General Purpose Output

	Toggle Duration	Default State
GPO 0	600	Low
GPO 1	600	Low

Figure 113: GPIO Settings through Webserver

1. Select check box to **Enable General Purpose Input / Output**
2. Actions to be triggered on GPI lines are available for selection. The options are **Delete Template**, **Reboot Terminal** and **Alarm**. Select actions for GPI line 0, 1
3. Enter **Signal Property** as below
    a. Set **Minimum Duration** for action triggering on each line, in msec. By default the value of the duration is 200 msec
    b. Select **Trigger On** “Signal Falling Edge” or “Signal Rising Edge”
4. Under **General Purpose Output** an administrator can configure below for lines 0, 1:
    a. **Toggle Duration**
    b. **Default state** as Low or High
5. Click on **Save**

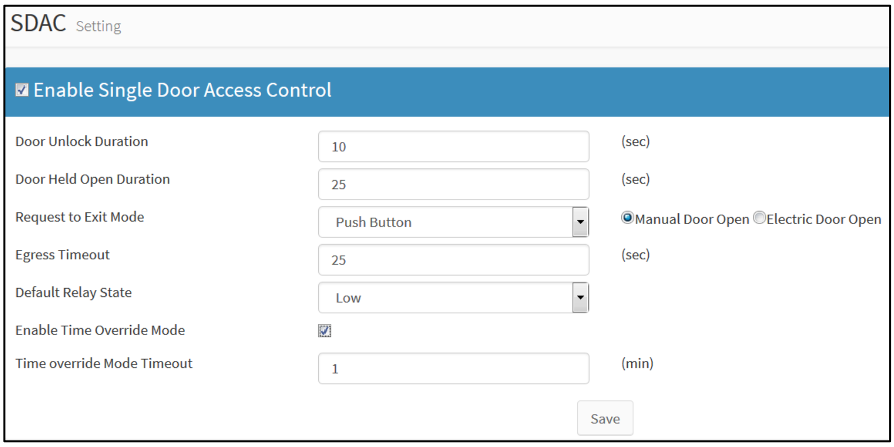
Single Door Access Control Settings

Single Door Controller (SDC) mode is used for controlling access through single door. Several parameters such as door unlock duration, alarm when door held open, and time over mode can be configured. When SDC mode is enabled, GPIO mode is disabled.

Access Path

Webserver > Terminal Settings > SDAC

Screens & Steps



SDAC Setting

☑ Enable Single Door Access Control

Door Unlock Duration	10	(sec)
Door Held Open Duration	25	(sec)
Request to Exit Mode	Push Button	● Manual Door Open ○ Electric Door Open
Egress Timeout	25	(sec)
Default Relay State	Low	
Enable Time Override Mode	☑	
Time override Mode Timeout	1	(min)

Figure 114: SDAC Settings on Webserver

Once an administrator selects **Enable SDC Mode**, an administrator needs to configure the parameters listed below:

1. In **Door Unlock Time** field set duration (in Seconds only) for which the door should be unlocked after access is granted. E.g. if 25 seconds is the Door Unlock Time, then the door will be unlocked for 25 seconds and after that the door will be locked automatically
2. In **Door Held Open Duration** field set the duration (in Seconds only) within which door must be closed. Once Door Unlock Time is exceeded and door is not closed; the terminal will start counting Door Held Open Duration. If user is not closing the door within this duration, an auto-alert "Door Opened For Too Long" will be generated on terminal.
3. Select **Exit Mode** as 'None' or 'Push button'
    a. **Push button exit mode** is selected when a push button is located at exit gate and users are allowed push the exit button to open the exit door.
        i. If an administrator selects Push Button as Request to Exit mode, then an administrator can select **Manual Door Open** or **Electric Door Open** actions

   b. When Exit Mode is in ‘Push Button-Manual Door Open’, then an administrator needs to set **Egress Time Out**. Within the Egress Time, the user will need to open the door and on timeout it will lock automatically

4. Select **Default Relay** state as High or Low. Here an administrator can set a default state of the internal relay, which is powered or unpowered.
   a. Select “0” for Low. It indicates that by default the internal relay will be unpowered and on access granted the internal relay state will change to high (it will be powered).
   b. Select “1” for High. It indicates that by default the internal relay will be powered and on access granted the internal relay state will change to low (it will be powered off).
5. Enable **Time Override Mode (TOM)**, it allows an administrator to temporarily suspend the need for verification of users for a specific time period on a terminal. Whenever TOM is triggered on terminal then door gets unlock and user can open Door without any authentication till TOM remains active.
   a. **For example**, during lunch hours most of the employees head towards cafeteria. Suppose an administrator set TOM for 90 minutes, then during this period the door will be opened and employees will not require to verify for opening door.
6. Enter the number of minutes TOM will be active into the **Time Override Mode Timeout** field
7. Click on **Save**

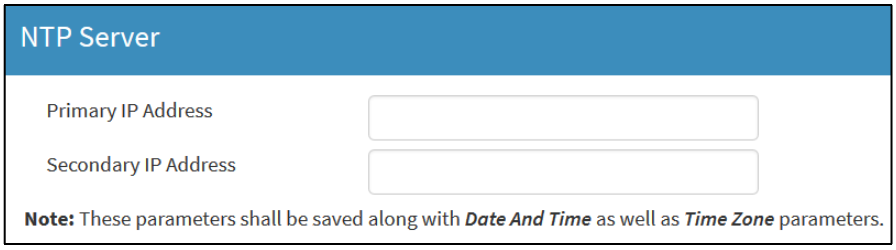
Network Time Protocol Server (NTP Server)

This functionality is used to synchronize the terminal date and time with external server using SNTP/NTP protocol, to update the terminal date and time automatically with the NTP server time.

Access Path

Webserver > Terminal Settings > Date Time

Screens & Steps



NTP Server

Primary IP Address	
Secondary IP Address	

Note: These parameters shall be saved along with ***Date And Time*** as well as ***Time Zone*** parameters.

Figure 115: NTP Server Configuration

1. Enter the computer’s IP address on which NTP server is configured as Primary IP Address
2. Click on Save
3. Leave the terminal idle for 5 to 10 minutes
4. The date and time on the terminal synchronizes with the date and time set on the computer

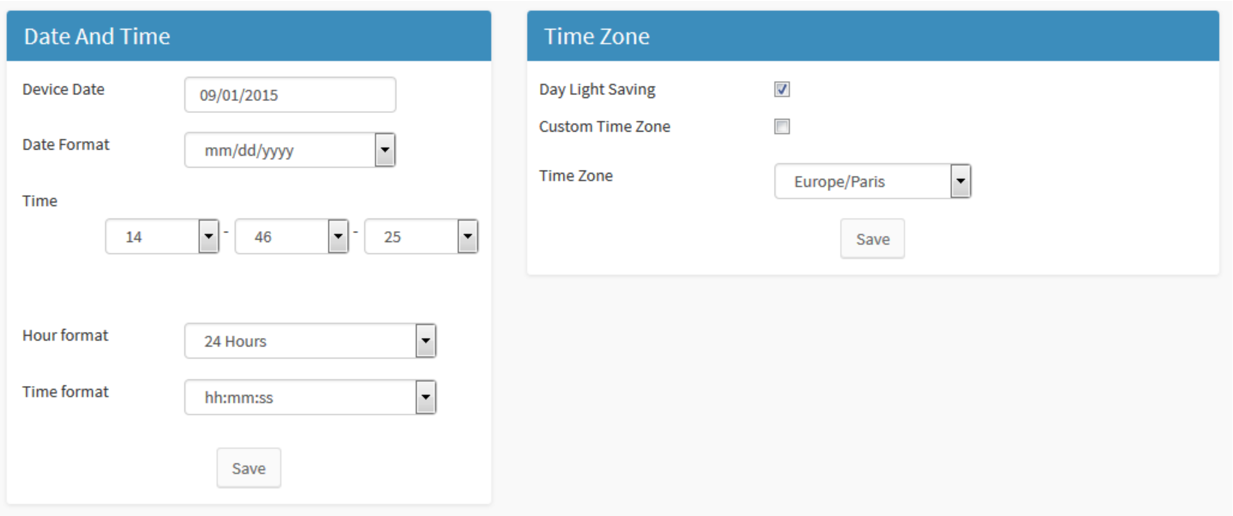
Date and Time Settings

This functionality allows an administrator to set time zone, current date and time of MorphoAccess® SIGMA Lite Series terminal. There are also options to set the format of date and time. These parameters are basic and required to be set at first boot of the terminal.

Access Path

Webserver > Terminal Settings > Date Time

Screens & Steps



Date And Time

Device Date: 09/01/2015

Date Format: mm/dd/yyyy

Time: 14 - 46 - 25

Hour format: 24 Hours

Time format: hh:mm:ss

Time Zone

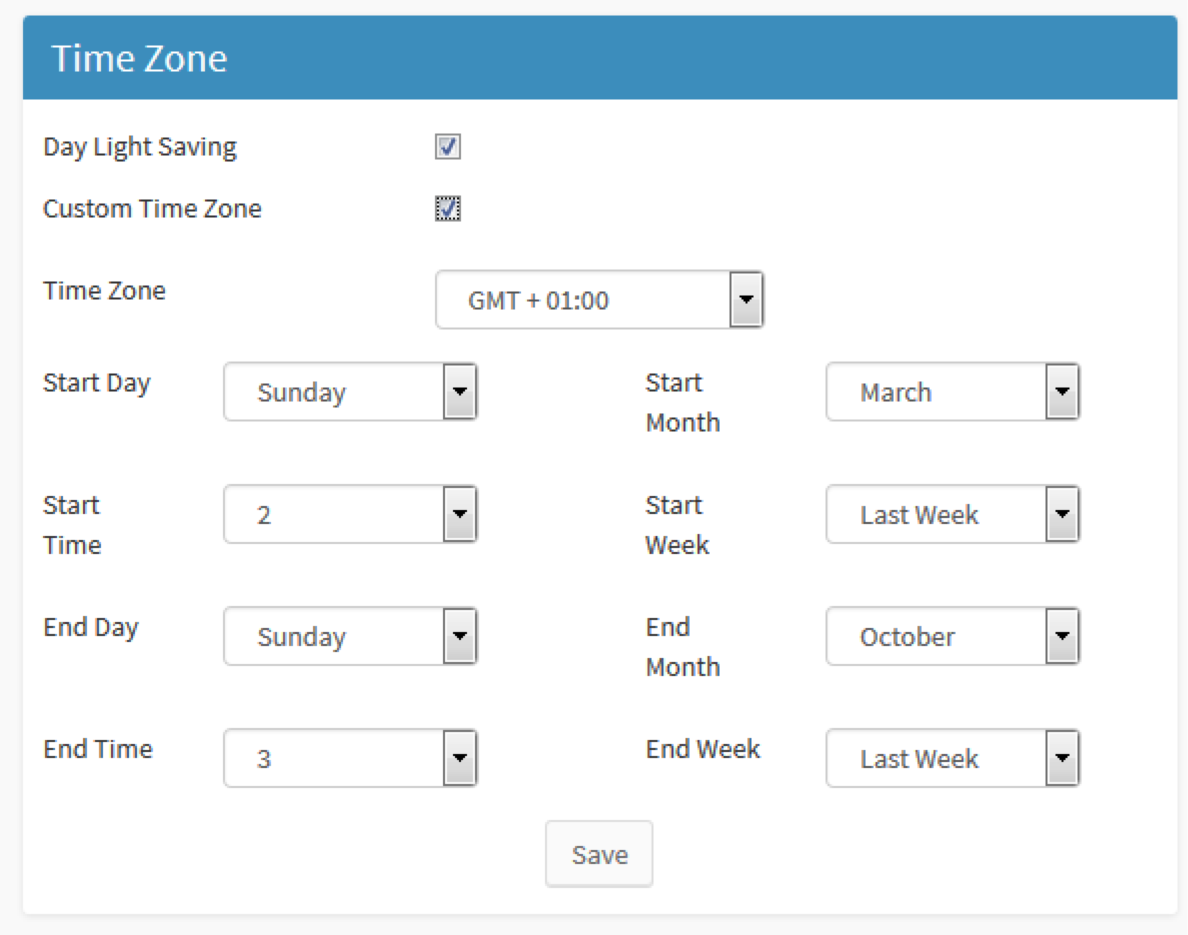
Day Light Saving ☑

Custom Time Zone □

Time Zone: Europe/Paris

Figure 116: Configuring Date and Time of Terminal

1. Enter current **Device Date**
2. Select **Date Format** as mm/dd/yyyy, dd/mm/yyyy, mmm-dd-yy, dd-mmm-yy, or yyyy/mm/dd (Applicable for *MorphoAccess® SIGMA Lite+ Series* only)
3. Select current **Time**
4. Select **Hour Format** as ‘12 hour’ or ‘24 hour’
5. Select **Time Format** as ‘hh:mm:ss’ or ‘hh.mm.ss’ (Applicable for *MorphoAccess® SIGMA Lite+ Series* only)
6. Select **Time Zone** from the available dropdown menu
7. Select **Day Light Saving**, if an administrator requires the time of the terminal to be auto-set when day light saving starts/ends
8. If an administrator require to customize Time Zone, then click on **Custom Time Zone** option, and enter below parameters:



Time Zone

Day Light Saving ☑

Custom Time Zone ☑

Time Zone: GMT + 01:00

Start Day: Sunday

Start Month: March

Start Time: 2

Start Week: Last Week

End Day: Sunday

End Month: October

End Time: 3

End Week: Last Week

Figure 117: Setting Custom Time Zone

a. Select **Time Zone**

> **NOTE:** While setting custom time zone, make sure the GMT offset value is to the 'Standard GMT Offset' of the region.

b. If **Day Light Saving** is enabled then enter below customer fields to set day light saving:

   i. Select Start Day, Start Month, Start Week and Start Time

   ii. Select End Day, End Month, End Week and End Time

9. Click on **Save**

Results

The date and time of the terminal will be set as per configuration done in Webserver.

Wiegand Parameters Settings

MorphoAccess® SIGMA Lite Series terminals can communicate with distant systems, using Wiegand interface. The protocol used for communicating on Wiegand channel is called Wiegand protocol. It is required to configure Wiegand input and output string format that is understood by terminal and distant system

Several Wiegand formats are preloaded on MorphoAccess® SIGMA Lite Series terminals and are designated as a Standard type in the table below. They contain an ID of 32 bits or less. All MorphoAccess® SIGMA Lite Series terminals support these formats. Using Webserver an administrator can configure the desired Wiegand format for both input and output. "Standard 26-bits" is the default format.

Format	Type	Site Code Range	Template ID Number Range	Extended ID Number Range
Standard 26-bit (default)	Standard	0 - 255	1 - 65535	N/A
Apollo 44-bit	Standard	0 - 16383	1 - 65535	N/A
Northern 34-bit	Standard	0 - 65535	1 - 65535	N/A
Northern 34-bit [no parity]	Standard	0 - 65535	1 - 65535	N/A
HID Corporate [35-bit]	Standard	0 - 4095	1 - 1048575	N/A
Ademco 34-bit (without RCM code)	Standard	0 - 4095	1 - 1048575	N/A
HID 37-bit	Standard	0 - 2047	1 - 16777215	N/A

Table 1 : Wiegand Format and Associated Values

Refer to "*Authentication with local database: ID input from Wiegand or Clock & Data*" to learn more about authentication process when initiated through Wiegand or Clock & Data.

Access Path

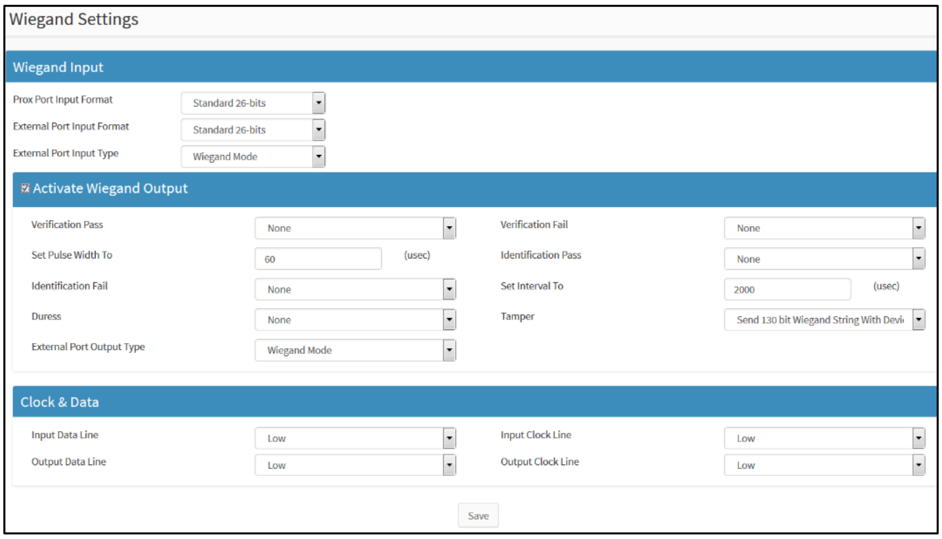
Webserver > Terminal Settings > Wiegand

Pre-requisites

MA_PAC license should be uploaded on terminal

Terminal has factory default settings

Screens & Steps



Wiegand Settings

Wiegand Input

Prox Port Input Format: Standard 26-bits
External Port Input Format: Standard 26-bits
External Port Input Type: Wiegand Mode

☑ Activate Wiegand Output

Verification Pass: None
Set Pulse Width To: 60 (usec)
Identification Fail: None
Duress: None
External Port Output Type: Wiegand Mode
Verification Fail: None
Identification Pass: None
Set Interval To: 2000 (usec)
Tamper: Send 130 bit Wiegand String With Devi

Clock & Data

Input Data Line: Low
Output Data Line: Low
Input Clock Line: Low
Output Clock Line: Low

Figure 118: Wiegand Settings through Webserver

1. Configure below Wiegand Input parameters, for action triggered through Wiegand to terminal:
   a. Select **Prox Port Format** from available format list, as mentioned under *Wiegand Format and Associated Values*
   b. Select **External Port Format** from available format list, as mentioned *Wiegand Format and Associated Values*
   c. Select **External Port Input Type** as Wiegand Mode or Clock & Data mode.
      i. If Wiegand mode is selected then Wiegand channel is used for sending input on terminal. By default Wiegand mode is selected
      ii. If Clock & Data mode is selected then Clock & Data channel is used for sending input on terminal. The Clock & Data settings will be applicable if this mode is activated.

2. **Activate Wiegand Output**: This parameter is enabled to allow the Wigand data to be sent using Wiegand Output Port. If this parameter is disabled then the terminal never tries to send any data frame through Wiegand port. Configure the Wiegand Output parameters listed below, for each event which must be communicate through Wiegand from the terminal:
   a. Select **Verification Pass** format from available format list, as mentioned under *Wiegand Format and Associated Values*
   b. Select **Verification Fail** format from available format list, as mentioned under *Wiegand Format and Associated Values*

c. Select **Identification Pass** format from available format list, as mentioned under *Wiegand Format and Associated Values*

d. Select **Identification Fail** format from available format list, as mentioned under *Wiegand Format and Associated Values*

e. Select **Duress Finger** detection format as ‘None’ or ‘Reverse Wiegand Output’. When duress finger is detected and verification is successful, terminal will send Wiegand output in selected form, to access controller. A controller will further respond by opening door

f. Select **Tamper** detection format as ‘None’ or ‘Send 130 bit Wiegand string with terminal serial number’. It is a pre-requisite to enable Tamper settings in the terminal. When tamper event is detected, terminal will send terminal serial number in a Wiegand string format to access controller, for alerting controller about the Tamper detection.

g. Select **External Port Output Type** as ‘Wiegand Mode’ or ‘Clock & Data mode’. If you select Clock & Data mode, then respective format will be used for sending data over Wiegand port.

h. **Set Pulse Width To** in terms of microseconds

i. **Set Pulse Interval To** in terms of microseconds

3. If External Port Input Type and Output Type is selected as Clock & Data, then configure Clock & Data parameters:
    a. Select **Input Data Line** as Low or High
    b. Select **Output Data Line** as Low or High
    c. Select **Input Clock Line** as Low or High
    d. Select **Output Clock Line** as Low or High
4. Click on **Save**

Threat Level Configuration

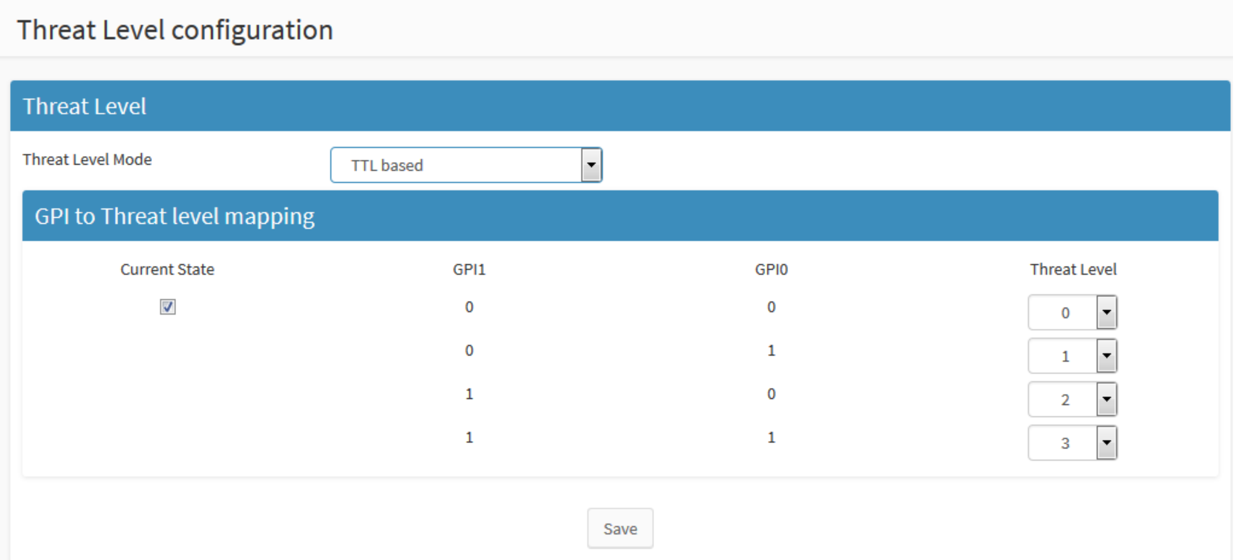
This feature allows an administrator to set threat levels using the TTL input lines. When enabled, the TTL signals can define the level of security and also can be used to compel users to use a specific authentication method. The available choices are Card Only and Card + Biometrics. For example, if Threat level 1 is set to Card + Biometrics and the TTL input for GPI0 is triggered, a successful verification requires presenting a smart card and a finger to the terminal.

If TTL is not active (both lines are 0), the verification follows command based inputs.

Access Path

Webserver > Terminal Settings > Threat Level

Screens & Steps



Threat Level configuration

Threat Level

Threat Level Mode: TTL based

GPI to Threat level mapping

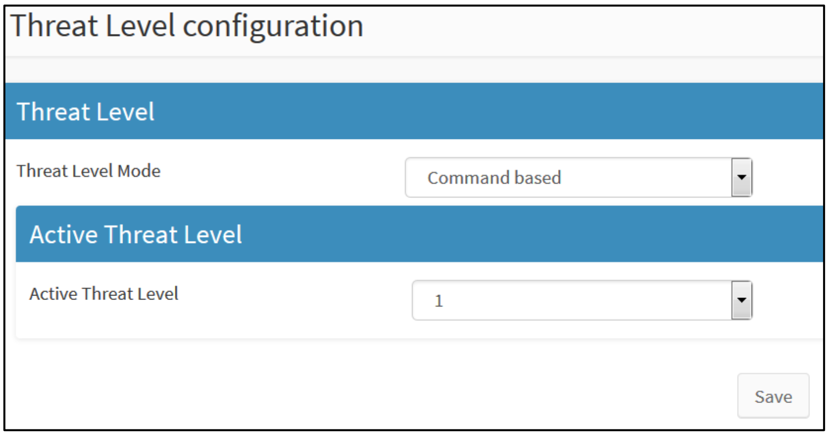
Current State	GPI1	GPI0	Threat Level
☑	0	0	0
	0	1	1
	1	0	2
	1	1	3

Figure 119: Configuring TTL Based Threat Level

1. Select **Threat Level Mode** as “TTL based”. In this mode, Active Threat Level will be determined by the current TTL line status and its mapping as per GPI to Threat Level Mapping. For example, to activate Threat Level 2, GPI1 line should be triggered. GPI to Threat Level Mapping allows an administrator to configure active threat level as per the GPI line.

10. User can change the default settings of **GPI to Threat Level Mapping**. Select the threat level corresponding to GPI line 1 and GPI line 0

11. Click on **Save**



Threat Level configuration

Threat Level

Threat Level Mode: Command based

Active Threat Level

Active Threat Level: 1

Figure 120: Configuring Command Based Threat Level

12. Select **Threat Level Mode** as ‘Command based’. If Threat Level is set to Command Based, the active threat level from the drop-down box has to be set. With Command Based threat level, the terminal does not refer to TTL lines inputs.
13. Command based threat level can also be modified using threat level parameters under Webserver > Complete Configuration and also distant commands.
14. Select **Active Threat Level** from dropdown menu

Time and Attendance Mode Configuration

MorphoAccess® SIGMA Lite Series terminal can be set in Time and Attendance (T&A) Mode. Under this mode, the user has to provide T&A data by using function keys before presenting fingerprint. The basic purpose of this mode is to log attendance information such as in time, lunch time, out time, etc.

E.g. T&A is configured as below:

Function key # 1 (In)

Function key # 2 (Out)

A user has to press respective In/Out key, for an action. If user is entering in office, then user is required to first press _In Key_ on the touch screen and then place finger for biometric authentication.

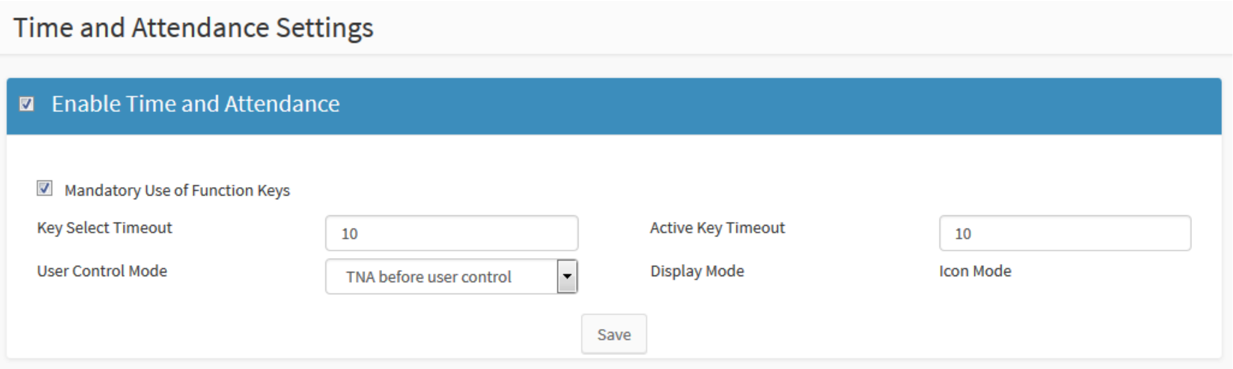
A transaction log is created, which contains items such as in time, Out time and break timings of a user. Using this records, productive working hours of an employee can be analyzed.

Using Webserver interface an administrator can configure the Time and Attendance parameters of the terminal. Below screens and steps shows an administrator how an administrator can configure T&A parameters.

Access Path

Webserver > Terminal Settings > Time and Attendance

Screens & Steps



Time and Attendance Settings

☑ Enable Time and Attendance

☑ Mandatory Use of Function Keys

Key Select Timeout	10	Active Key Timeout	10
User Control Mode	TNA before user control	Display Mode	Icon Mode

Save

Figure 121: Normal Time and Attendance mode

1. Click on **Enable Time and Attendance**, for enabling this mode
2. Click on **Mandatory Use of Function Keys**. On enabling this, terminal will pop up T&A screen every time after user presents fingerprint. If mandatory is not selected, then user can select T& A option before

3. **Key Select Timeout:** An administrator can define the duration for which F-key selection option will be displayed. If user does not input the key, then access is denied (in case T&A is mandatory). Valid range of timeout is 3 to 60 seconds.
4. **Active Key Timeout:** Within this duration the key should be pressed. Valid range of timeout is 3 to 60 seconds.
5. Select **User Control Mode** as “TNA before user control”, it means user have to first select a T&A action before user control; or “TNA after user control”, it means user have to select TNA action after user control (such as entering biometric/pin data).
6. Click on **Save** once required configurations done

Once T&A mode is enabled, the user interface of the terminal has a T&A button. See below screens:

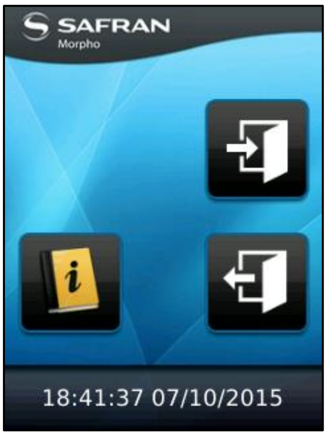


Figure 122: User Interface on Terminal

Results

Once T&A parameters are configured, T&A icon is displayed on the home screen of the MorphoAccess® SIGMA Lite Series terminal. When user presents his fingerprint, on successful authentication, terminal will ask user to select functional key on T&A screen. If T&A is not mandatory, user can select the T&A icon before presenting the fingerprints, if required.

Schedules Menu

Define Access Schedule

Access Schedules is used to define a time slot, during which access is allowed, for example during working hours of working days. Before and after the selected timings, the access is denied to the user, even if authenticated successfully.

Access schedule enables to define time slots for entire week. A time slot is defined by selecting a start time and end time in hours and minutes. An Access Schedule can have up to two time slots per day.

Maximum 64 access schedules can be created, where by

By default, Schedule no. 0 is defined as access denied at whichever time the access is requested

By default, Schedule no. 63 is defined as FULL access time slot. On user enrolment, Access Schedule 63 is assigned by default.

Schedule no. 59 to Schedule no. 62 is reserved for internal use and cannot be assigned to any user.

On user enrolment, administrator can select the required access schedule and associate it with the user details. E.g. Access Schedule 1 is created and has access rights in time slot from 10:00 am 13:00 pm and then from 14:00 pm to 20:00 pm (with interval being from 13:00 pm to 14:00 pm). User is granted access only from 10:00 to 13:00 and from 14:00 to 20:00.

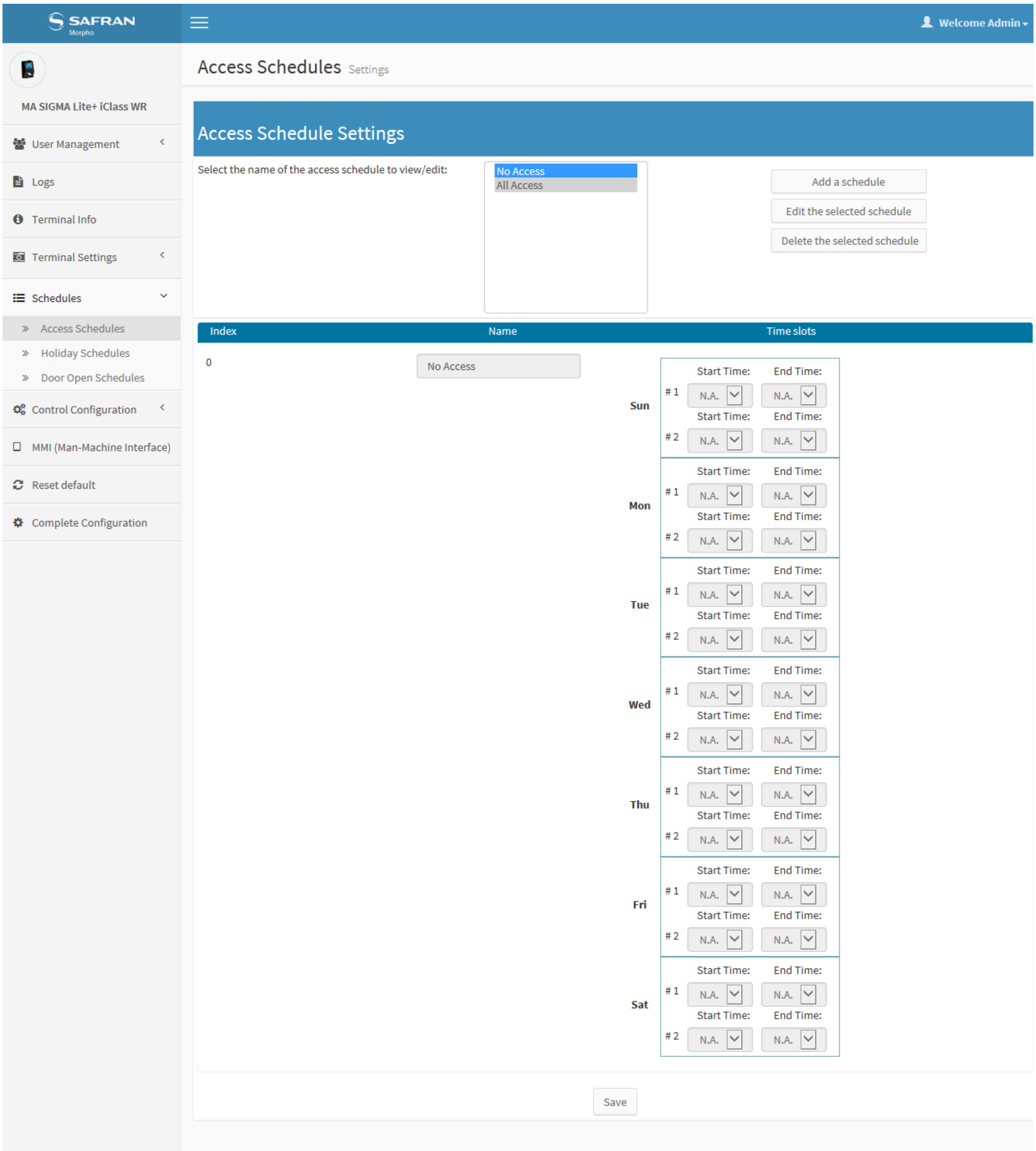
Every time on successful authentication of the user, the terminal will also check access schedule selected for the user and will allow access according to the defined schedule.

Using Webserver, an administrator can configure Access Schedule, for MorphoAccess® SIGMA Lite Series terminals.

Access Path

Webserver > Schedules > Access Schedules

Screens & Steps



Access Schedules Settings

Access Schedule Settings

Select the name of the access schedule to view/edit:

No Access
All Access

Index	Name	Day	Slot	Start Time:	End Time:
0	No Access	Sun	# 1	N.A.	N.A.
			# 2	N.A.	N.A.
		Mon	# 1	N.A.	N.A.
			# 2	N.A.	N.A.
		Tue	# 1	N.A.	N.A.
			# 2	N.A.	N.A.
		Wed	# 1	N.A.	N.A.
			# 2	N.A.	N.A.
		Thu	# 1	N.A.	N.A.
			# 2	N.A.	N.A.
		Fri	# 1	N.A.	N.A.
			# 2	N.A.	N.A.
		Sat	# 1	N.A.	N.A.
			# 2	N.A.	N.A.

Figure 123: Adding Access Schedule

Adding a New Access Schedule

1. The list of default access schedules is displayed. No Access and All Access are by default created and not editable. An administrator can add new schedules as per requirement
2. Click on **Add a Schedule** to create a new access schedule

3. Enter **Name** of the schedule
4. Define **Time Slots** for each day, by selecting Start Time (hh:mm) and End Time (hh:mm). During the selected time slot, access is granted to user.
   a. **N.A.** indicates there is no time slot defined. Access is denied on the days when N.A. is selected.
5. Click on **Apply**

NOTE:

- *In MA5G mode, two time slots per day can be defined with one interval in between*

- *If terminal is in L1 Legacy mode, then Access Schedule can be configured from Secure Admin. Where an administrator can also define "Schedule Tolerance" duration that allows user access early/late than the scheduled access time.*

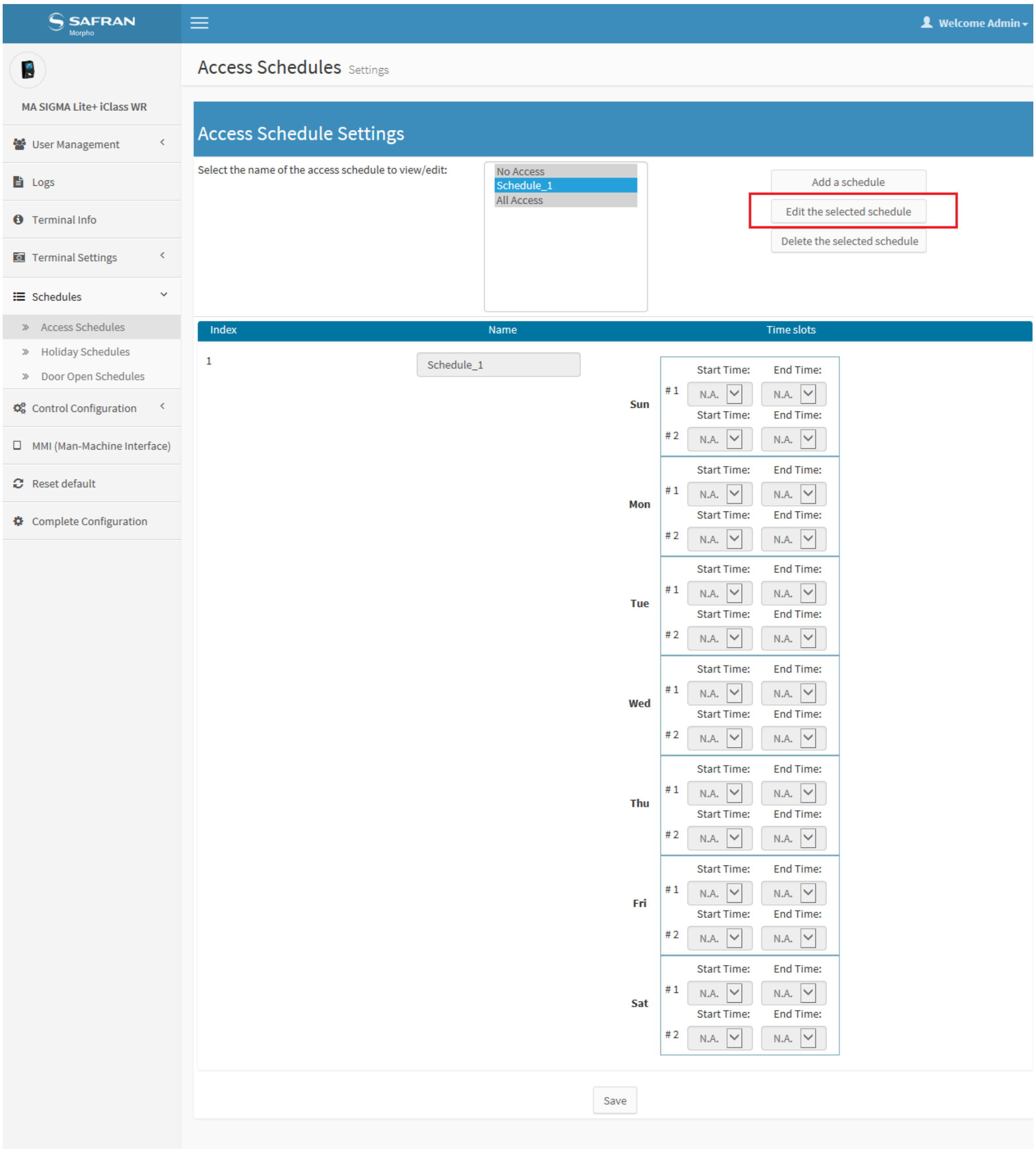
- *Moreover, in L1 Legacy mode, an administrator can set two intervals in a day.*

- *If terminal is in Legacy Morpho mode, then access schedule can be configured, using Time Mask feature in MorphoBioToolBox (MBTB) application.*

Results

An Access Schedule is created from 08:00 am to 13:00 pm and 14:00 pm to 20:00 pm and it is available for assignment to users at the time of user enrolment. User is allowed to access only during the access time scheduled. If user tries to access at another time, then MorphoAccess® SIGMA Lite Series terminal will deny access to the user.

Editing Access Schedule



Access Schedule Settings

Select the name of the access schedule to view/edit:

- No Access
- Schedule_1
- All Access

Index	Name	Time slots			
1	Schedule_1	Sun	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Mon	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Tue	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Wed	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Thu	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Fri	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Sat	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.

Figure 124: Editing Access Schedule

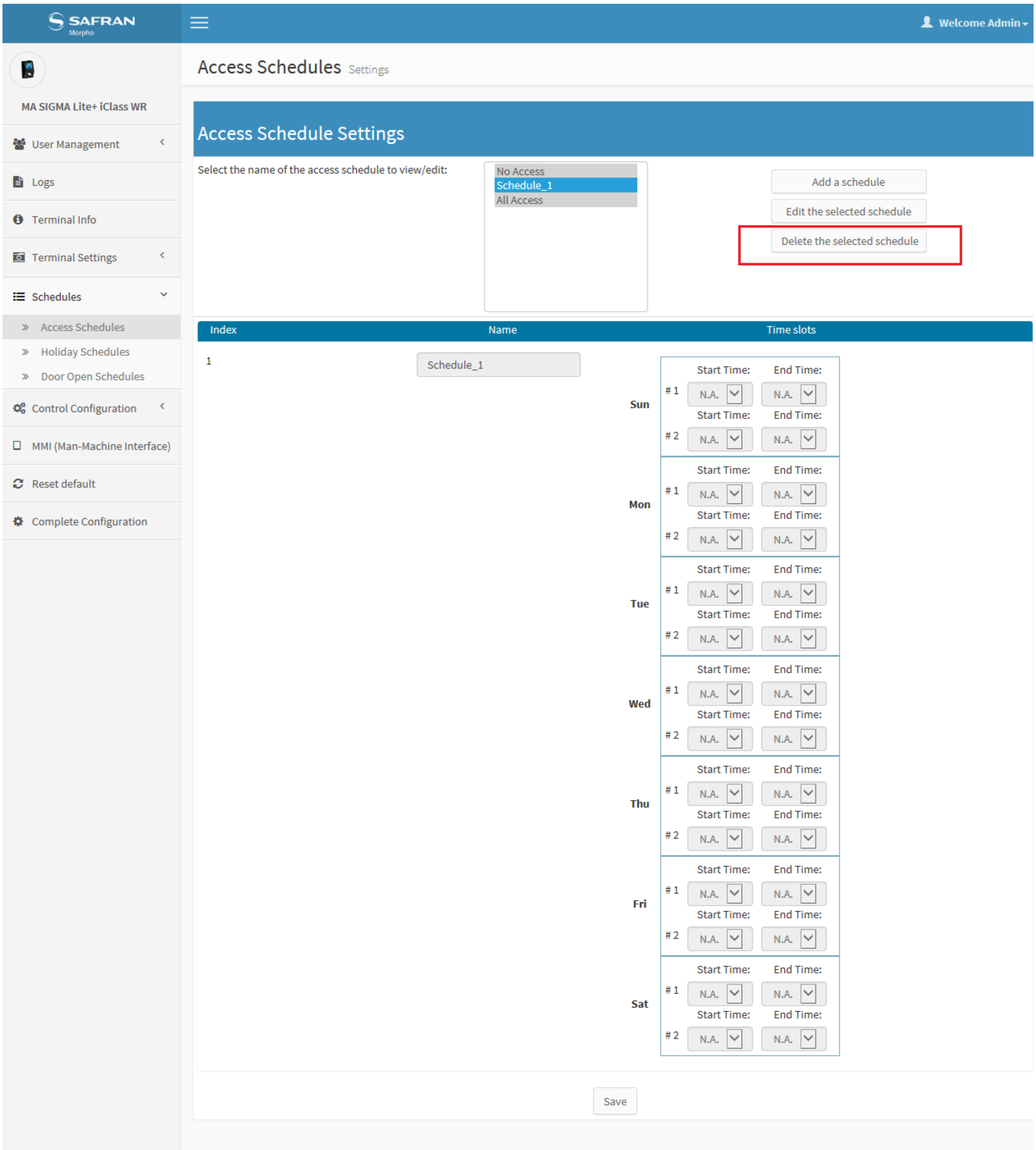
1. Select an access schedule from the list
2. Click on **Edit the Selected Schedule** tab

NOTE: The default access schedules cannot be modified.

3. An administrator can edit **Access Schedule Name** and **Time Slots**
4. Once required information is updated, click on **Apply**

5. The Access Schedule is updated and then click on Save to save the updated Access Schedule.

Delete Access Schedule



Access Schedule Settings

Select the name of the access schedule to view/edit:

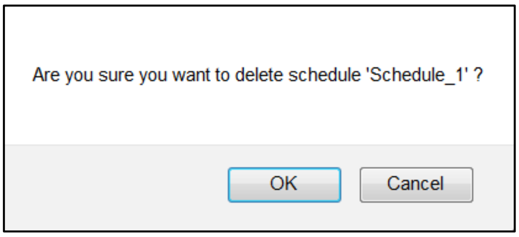
- No Access
- Schedule_1
- All Access

Index	Name	Time slots			
1	Schedule_1	Sun	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Mon	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Tue	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Wed	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Thu	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Fri	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.
		Sat	# 1	Start Time: N.A.	End Time: N.A.
			# 2	Start Time: N.A.	End Time: N.A.

Figure 125: Deleting an Access Schedule

1. Select an **Access Schedule** from the list
2. Click on **Delete the Selected Schedule**

NOTE: The default access schedules cannot be deleted.



Are you sure you want to delete schedule 'Schedule_1' ?

Figure 126: Deleting an Access Schedule

3. A confirmation message pops up, to confirm delete action. Click on Ok to delete Access Schedule

Results

An access schedule is deleted. It is no longer available for selection on user enrolment.

Define Holiday Schedule

Using holiday schedule, an administrator can control access of users on holidays. Holiday Schedule can be defined for the public holidays of entire Year. When user tries to access, terminal will authenticate user and on successful authentication, terminal will check if Holiday Schedule is to be considered. Even if the user is authenticated, the access is denied on the holiday, if the user observes holiday.

MorphoAccess® SIGMA Lite Series terminal can support up to 46 holiday schedules.

Access Path

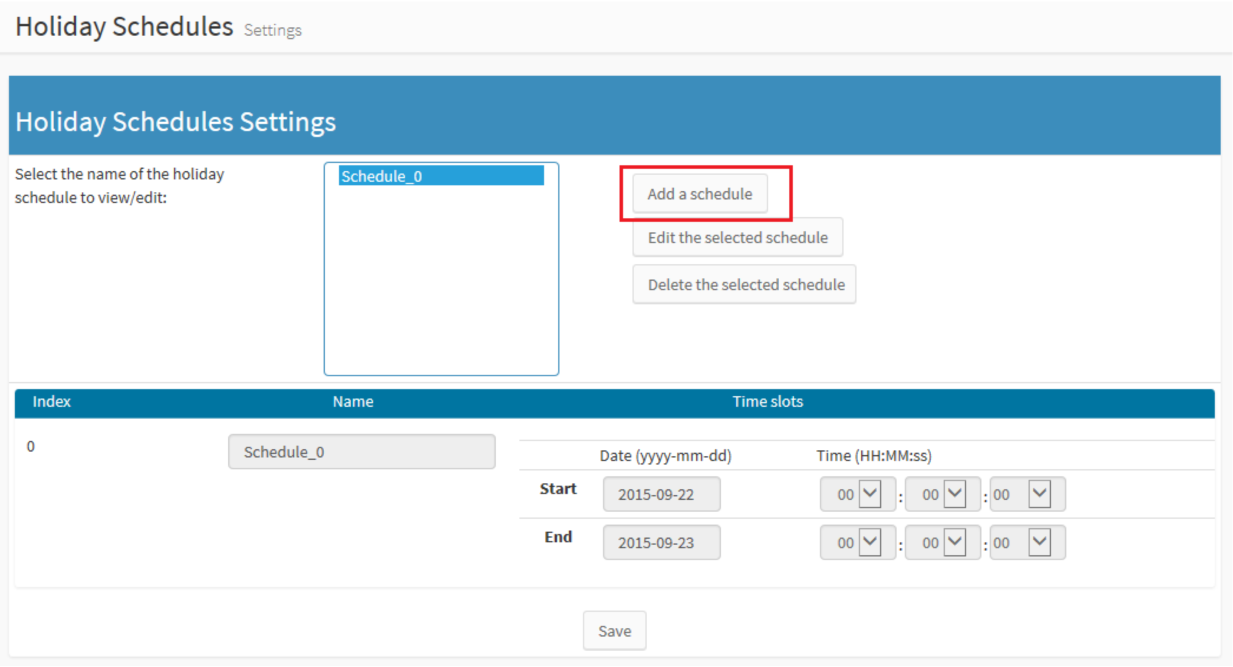
Webserver > Schedules >Holiday Schedules

Pre-requisites

Observe Holiday parameter should be enabled for individual user, at the time of User Enrolment

Screens & Steps

Add a Holiday Schedule



Holiday Schedules Settings

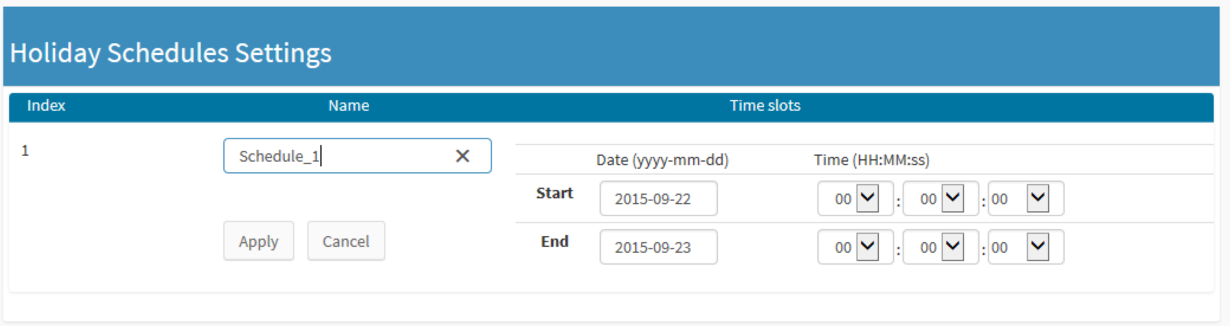
Holiday Schedules Settings

Select the name of the holiday schedule to view/edit: Schedule_0

Index	Name	Time slots		
			Date (yyyy-mm-dd)	Time (HH:MM:ss)
0	Schedule_0	Start	2015-09-22	00 : 00 : 00
		End	2015-09-23	00 : 00 : 00

Figure 127: Creating a Holiday Schedule

1. The list of Holiday Schedules is displayed, an administrator can view a holiday schedule showing date and time slot
2. Click on **Add a Schedule**



Holiday Schedules Settings

Index	Name	Time slots		
			Date (yyyy-mm-dd)	Time (HH:MM:ss)
1	Schedule_1	Start	2015-09-22	00 : 00 : 00
	Apply Cancel	End	2015-09-23	00 : 00 : 00

Figure 128: Creating a Holiday Schedule

3. Enter Schedule Name, usually the name of the holiday (such as "Christmas")
4. Enter **Schedule Name**, usually the name of the holiday (such as "Christmas")
5. Select **Start Date** and **End Date** of the holiday, by default the date format is YYYY-MM-DD. One schedule allows to specify several consecutive days
6. Select **Start Time** and **End Time**, applicable on selected dates. By default the date format is HH:MM:ss. During this time slab, access is not granted.

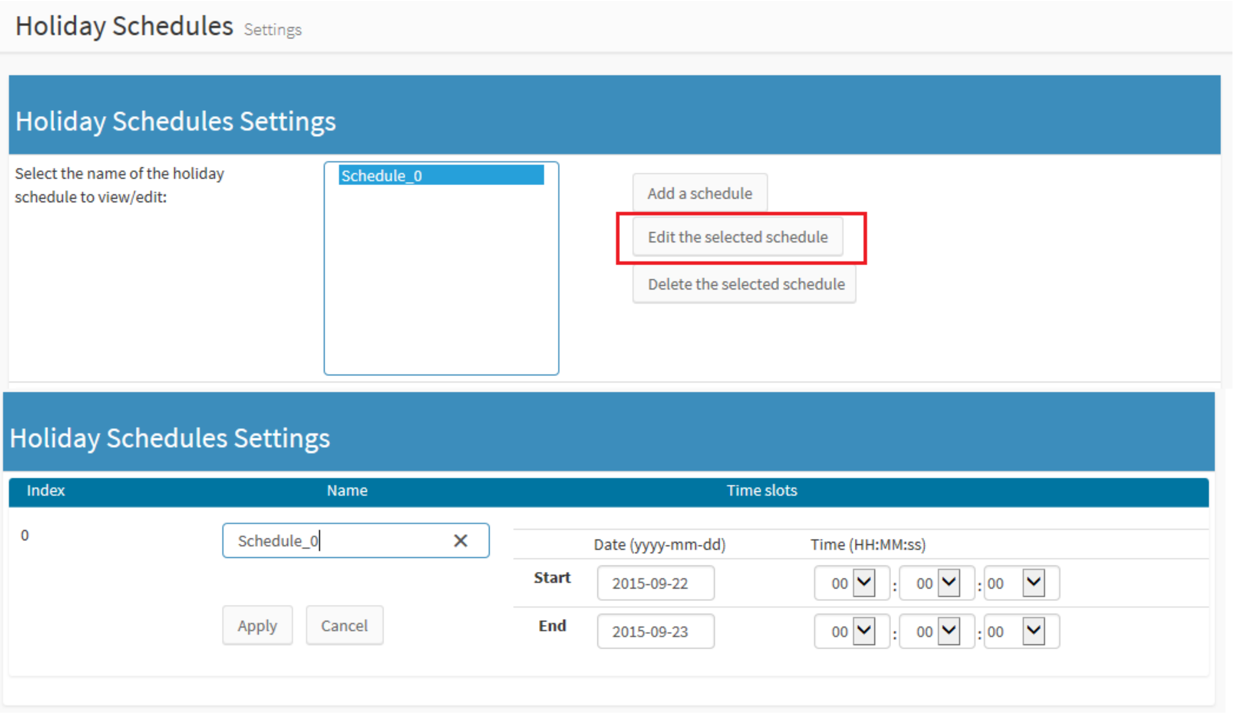
NOTE: *If terminal is in L1 Legacy mode, then Holiday schedule is defined using Secure Admin. The Time slot with maximum interval can be set.*

7. Click on **Apply**

Results

A Holiday Schedule is created. An administrator can define holidays of entire year (one holiday schedule per holiday). When Observe Holiday parameter is enabled in user template, then during the defined holidays user is not allowed access. Terminal will deny access to the user.

Edit Holiday Schedule



Holiday Schedules Settings

Holiday Schedules Settings

Select the name of the holiday schedule to view/edit: Schedule_0

Holiday Schedules Settings

Index	Name	Time slots		
			Date (yyyy-mm-dd)	Time (HH:MM:ss)
0	Schedule_0	Start	2015-09-22	00 : 00 : 00
		End	2015-09-23	00 : 00 : 00

Figure 129: Editing Holiday Schedule

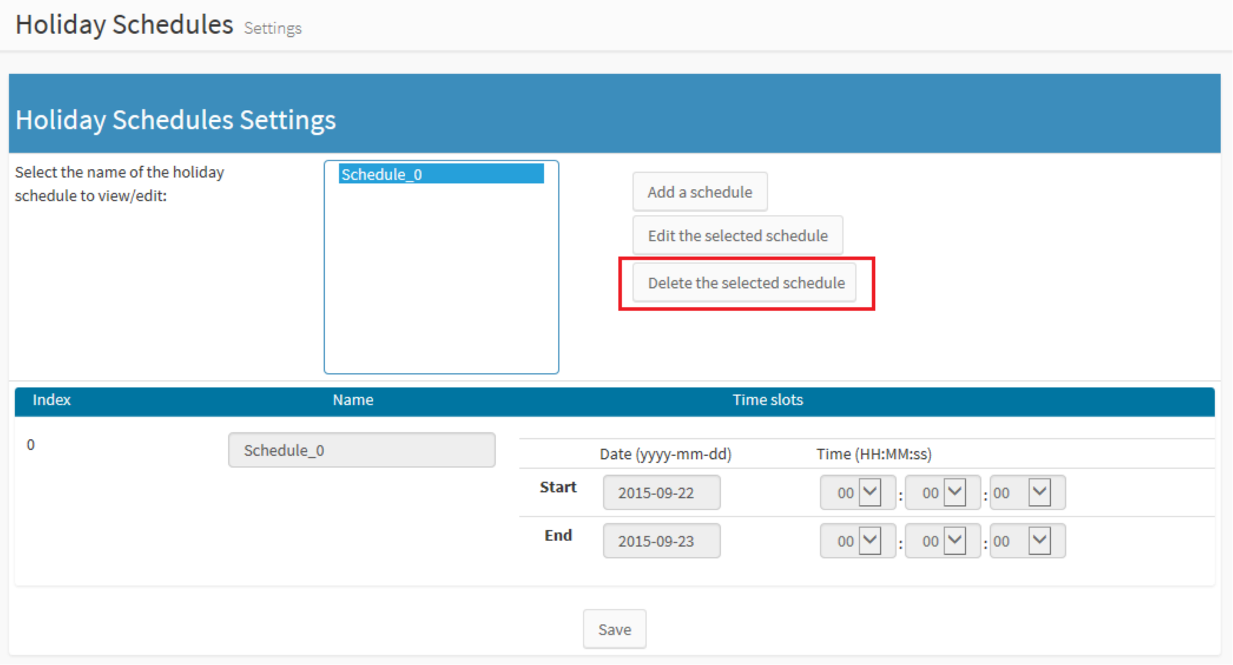
1. Select a Holiday Schedule that an administrator require to update
2. Click on **Edit the Selected Schedule**
3. Update necessary information in Name of holiday schedule, Date and Time slots
4. Click on **Apply**

Results

The Holiday schedule is updated successfully. The access requests are controlled based on the updated date/time slot.

Delete a Holiday Schedule

Using this feature an administrator can delete holiday schedules from the terminal. The holiday schedules that are expired are recommended to be deleted.


Holiday Schedules Settings
Holiday Schedules Settings
Select the name of the holiday schedule to view/edit:
Schedule_0
Add a schedule
Edit the selected schedule
Delete the selected schedule
Save

Index	Name	Time slots		
			Date (yyyy-mm-dd)	Time (HH:MM:ss)
0	Schedule_0	Start	2015-09-22	00 : 00 : 00
		End	2015-09-23	00 : 00 : 00

Figure 130: Deleting a Holiday Schedule

1. Select a name of the Holiday Schedule from the list
2. Click on **Delete the Selected Schedule**
3. A confirmation message pops up, to confirm delete action. Click on Ok to delete Holiday Schedule

Results

A holiday schedule is deleted. It is no longer considered for granting access to the user.

Door Open Schedule Configuration

The **Door Open Schedule** option allows terminal to keep the Door Unlocked for a specific period of time. Using Webserver interface, the Door Open Schedule can be defined. During this period, access is granted without access rights check. That is users can access without biometric authentication.

In a real life scenario, this feature can be implemented during lunch hours, when all employees need to go out or come in for a lunch break. Hence the door open schedule can be configured if no biometric check is required during specific interval.

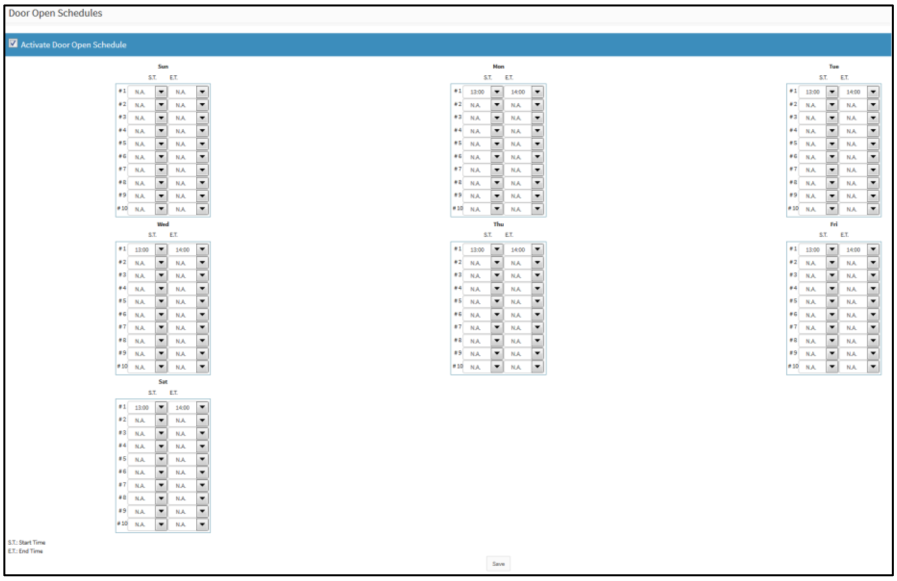
Access Path

Webserver > Schedules > Door Open Schedules

Pre-requisites

SDAC must be activated

Screens & Steps



Door Open Schedules

☑ Activate Door Open Schedule

	Sun		Mon		Tue		Wed		Thu		Fri		Sat	
	S.T.	E.T.	S.T.	E.T.	S.T.	E.T.	S.T.	E.T.	S.T.	E.T.	S.T.	E.T.	S.T.	E.T.
#1	N.A.	N.A.	13:00	14:00	13:00	14:00	13:00	14:00	13:00	14:00	13:00	14:00	13:00	14:00
#2	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
#3	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
#4	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
#5	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
#6	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
#7	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
#8	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
#9	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.
#10	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.	N.A.

S.T.: Start Time
E.T.: End Time

Figure 131: Door Open Schedule Configuration

1. Set **Start Time** and **End Time** for each day of the week
2. Click on **Save**

Results

As per the Door Open Schedule, terminal will send signal to door control panel to open the door at a start time of the schedule. The door is opened (or unlocked) till the end time of the schedule. On end time terminal will send signal to door panel to close (or lock) the door.

Control Configurations

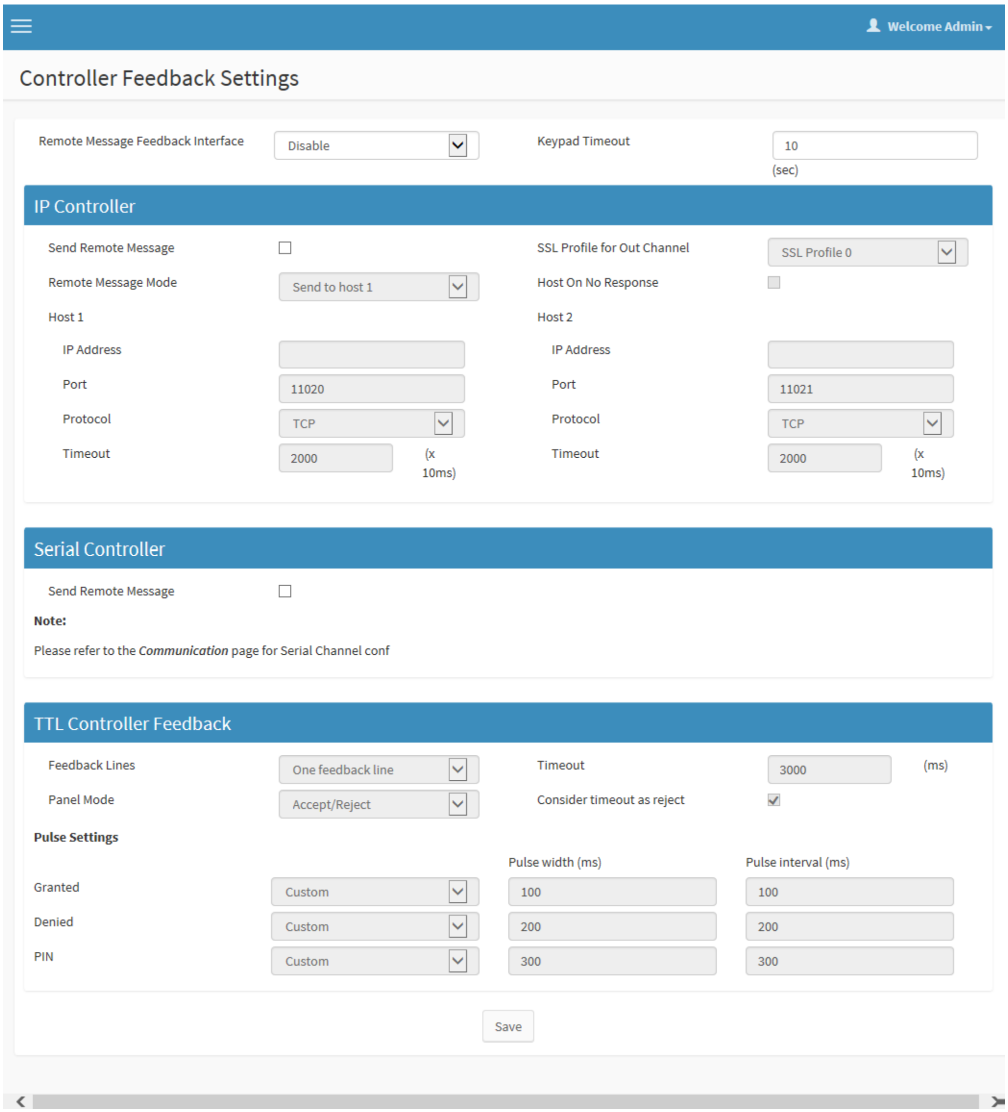
Controller Feedback

This configuration screen allows an administrator to set parameters that enable the Access Controller to send feedback messages on every event reported by the terminal.

Access Path

Webserver > Control Configuration > Controller Feedback

Screens & Steps



Controller Feedback Settings

Remote Message Feedback Interface: Disable
Keypad Timeout: 10 (sec)

IP Controller

Send Remote Message ☐
SSL Profile for Out Channel: SSL Profile 0
Remote Message Mode: Send to host 1
Host On No Response ☐

Host 1		Host 2	
IP Address		IP Address	
Port	11020	Port	11021
Protocol	TCP	Protocol	TCP
Timeout	2000 (x 10ms)	Timeout	2000 (x 10ms)

Serial Controller

Send Remote Message ☐

Note:

Please refer to the ***Communication*** page for Serial Channel conf

TTL Controller Feedback

Feedback Lines: One feedback line
Timeout: 3000 (ms)
Panel Mode: Accept/Reject
Consider timeout as reject ☑

Pulse Settings

		Pulse width (ms)	Pulse interval (ms)
Granted	Custom	100	100
Denied	Custom	200	200
PIN	Custom	300	300

Figure 132: Controller Feedback Settings

1. Select Remote Message Feedback Interface as:
    a. **Disable:** If an administrator do not require to expect Controller Feedback, then an administrator can set interface as Disabled
    b. **Feedback over IP:** Select Feedback over IP, if controller feedback is to be received on IP channel
    c. **Feedback over TTL:** Select Feedback over TTL, if controller feedback is to be received on TTL.
2. Only if TTL channel is used, you need to configure below parameters:
    a. Select **Feedback Lines**, it means the number of lines in which access controller will send feedback to terminal. An administrator can select “One feedback line” or “Two feedback line”
    b. Select **Panel Mode** as
        a. **Accept/Reject:** This mode indicates that access controller will only send Accepted (Access Granted) or Rejected (Access Denied) feedback messages to terminal
        b. **Accept/Reject/PIN:** Access Controller feedback consist Accepted (Access Granted), Rejected (Access Denied) and PIN (Asks user to enter PIN). This mode is not applicable if Two Feedback Line is selected in previous step
    c. Enter **Timeout** within which the feedback is sent by controller to the terminal
3. If Feedback Line is set as “One feedback line”, then each feedback message i.e. **Granted**, **Denied**, and **PIN** can have different pulse width and pulse interval. An administrator can define the same as below:
    a. **High**: If an administrator select High, then Pulse Width and Pulse Interval of the feedback message will be as per system default value for high pulse
    b. **Low**: If an administrator select Low, then Pulse Width and Pulse Interval of the feedback message will be as per system default value for low pulse
    c. **Custom**: If an administrator select Custom, then the field for editing Pulse Width and Pulse Interval is enabled and an administrator can customize the pulse as below:
        i. The **Pulse Width** can vary between 50 to 1000 milliseconds, 0 or 1
        ii. The **Pulse Interval** can vary between 50 to 1000 milliseconds, value 0 or 1.
    d. **None:** This option is available for Access Denied feedback only. It indicates that on no response from controller feedback, for Access Denied, the terminal can show timeout or access denied message. You can configure whether to consider timeout as reject. Refer step 4.

e. **Default value for custom fields is as below:**

    i. For **Access Granted** – 100 pulse width and interval

    ii. For **Access Denied** – 200 pulse width and interval

    iii. For **PIN** – 300 pulse width and interval

4. **Consider Timeout as Reject:** This function is valid for Access Denied feedback only. If it is enabled, then on timeout the access will be denied due to Controller Feedback Rejected. If 'Consider timeout as Reject' is unchecked, then on timeout the access will be denied due to Controller Feedback Timeout.
5. Enter **Keypad Timeout**, for user to enter the PIN. This is used when panel mode is set as Accept/Reject/PIN and controller panel contains PIN (asks user to enter PIN).
6. Click on **Save**

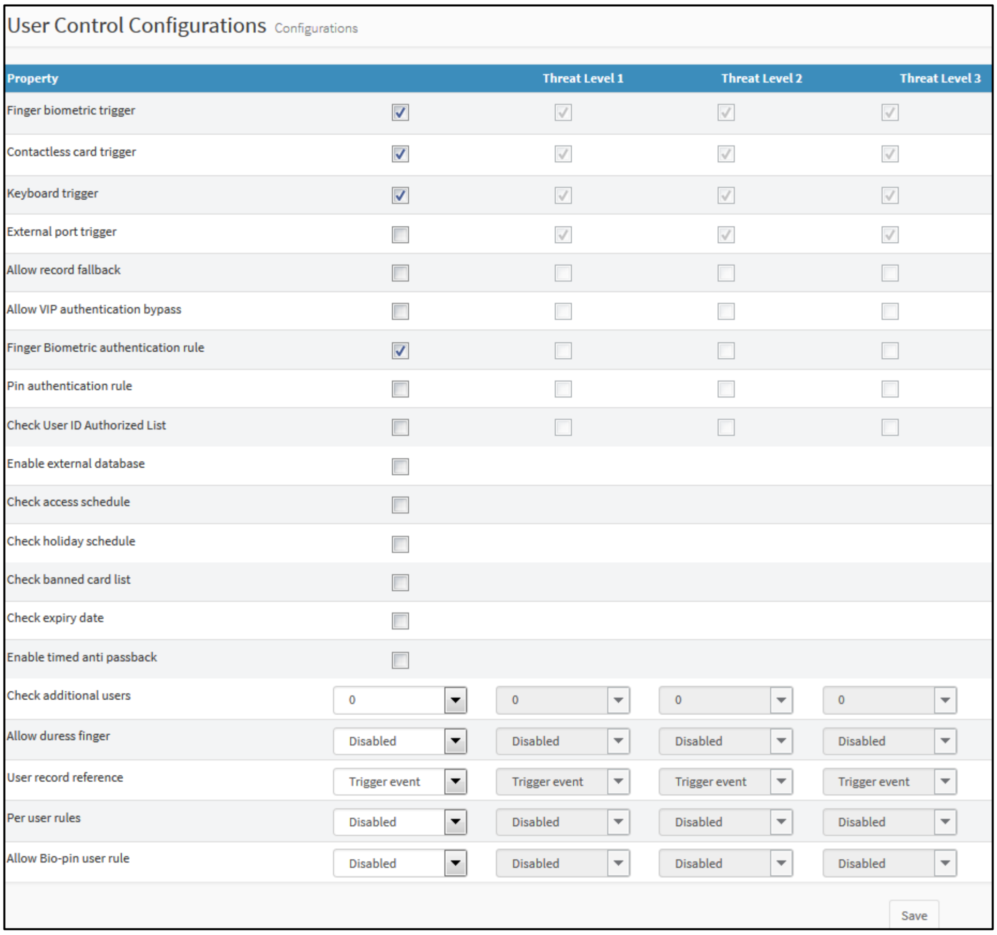
User Control Configurations

User Control configurations consists the list of parameters which terminal should check for authenticating and granting access to the user. An administrator can enable or disable these parameters.

Access Path

Webserver > Control Configuration > User Control

Screens & Steps



User Control Configurations Configurations

Property		Threat Level 1	Threat Level 2	Threat Level 3
Finger biometric trigger	☑	☑	☑	☑
Contactless card trigger	☑	☑	☑	☑
Keyboard trigger	☑	☑	☑	☑
External port trigger	□	☑	☑	☑
Allow record fallback	□	□	□	□
Allow VIP authentication bypass	□	□	□	□
Finger Biometric authentication rule	☑	□	□	□
Pin authentication rule	□	□	□	□
Check User ID Authorized List	□	□	□	□
Enable external database	□			
Check access schedule	□			
Check holiday schedule	□			
Check banned card list	□			
Check expiry date	□			
Enable timed anti passback	□			
Check additional users	0	0	0	0
Allow duress finger	Disabled	Disabled	Disabled	Disabled
User record reference	Trigger event	Trigger event	Trigger event	Trigger event
Per user rules	Disabled	Disabled	Disabled	Disabled
Allow Bio-pin user rule	Disabled	Disabled	Disabled	Disabled

Figure 133: User Control Configurations from Webserver

For enabling the actions, check on the checkbox corresponding to the listed parameters as below:

1. **Finger Biometric Trigger:** A user control operation can be triggered by placing finger on the biometric sensor. An administrator can enable or disable Biometric trigger using this parameter.

Note: *Access request using biometric will be triggered only if the user's biometric data is stored in the terminal's local database.*

2. **Contactless Card Trigger:** If this parameter is enabled, terminal starts access rights check, using authentication process, when a user card is detected by embedded contactless card reader. This parameter can be enabled or disabled for terminals having internal Smartcard reader or internal Prox card reader.
3. **Keyboard Trigger:** This parameter can be enabled to start access rights check, using authentication process, when a user ID is entered through terminal keyboard. This is applicable for MorphoAccess® SIGMA Lite+ Series only.
4. **External Port Trigger:** This parameter can be enabled to start access control check, using authentication process, when a data is received from an external device (such a swipe card reader) by Wiegand or Clock & Data protocol.
5. **Allow Record Fallback:** To allow terminal to use references from database, if references from smartcard are not present. E.g. for smartcard trigged authentication, if BIO check is enabled and BIO data is not found on smartcard, and if this parameter is enabled, terminal will use biometric data corresponding to the user stored in the terminal database to perform BIO check. The user with the same User ID needs to be available on both the contactless card and the terminal.
6. **Allow VIP Authentication Bypass:** If this parameter is enabled then users in the VIP list are exempted from authentication checks (finger bio, pin), only if the trigger event comes from a trusted source i.e. Biometric or Contactless Card (but not Keyboard or External trigger source). Only the controls intended to validate a user's identity are suppressed.
7. **Finger Biometric Authentication Rule:** This parameter indicates whether terminal should check biometric of the user as a part of user control workflow.
8. **Pin Authentication Rule:** This parameter indicates whether terminal should check PIN of the user as a part of user control workflow. This is applicable for MorphoAccess® SIGMA Lite+ Series only.
9. **Check User ID Authorized list:** This parameter controls authorized list check during user control workflow. If enabled, the terminal will check whether user is authorize listed or not.
10. **Enable external database:** If enabled, the terminal polling mode will be activated, and check the user's data with the data stored in external database. Refer "*Polling Mode*" for understanding polling mode.
11. **Check access schedule:** This indicates whether terminal should check the access schedule before granting access to the user
12. **Check holiday schedule:** This indicates whether terminal should check the holiday schedule before granting access to the user

13. **Check banned card list:** If this parameter is enabled, terminal searches for users card in banned card list before starting user's authentication. The user's presented contactless card serial number is checked against the contactless card serial numbers stored in the banned card list of the terminal.
14. **Check expiry date:** If this parameter is enabled terminal will check the expiry date of user account.
15. **Enable timed anti passback:** If this parameter is enabled then the repeated access control for a user till anti passback timeout is not allowed on the terminal.
16. **Check additional users:** Specifies the number of additional users to check before granting the access. Set this parameter value to either 0 (no additional users required) or 1 (one additional user required). If a single user is successfully identified multiple times, the duplicates are ignored and the terminal again prompts for the additional user, until the workflow times out. If one of the users fails the workflow is interrupted.
17. **Allow duress finger:** This parameter indicates whether to allow duress finger detection or not. An administrator can select "Alarm only" to allow duress finger. If set to Alarm only, the standard workflow applies, but an additional "duress finger detected" event is raised before the eventual user control result.
18. **User record reference:** This parameter defines where the references for control are taken from. Possible values are "Trigger event" or "Terminal". If set to "Trigger Event" then reference source is based on trigger event i.e. reference is smartcard for smartcard trigger source and terminal for other trigger source. If set to "Terminal" then reference is terminal for all trigger source.
19. **Per user rules:** Defines additional rules reference (i.e. rules that add to terminal defined rules). Possible values are "Disabled", "Trigger Event" and "Terminal".
    a. If set to "Disabled", then only terminal configuration defined controls are performed,
    b. If set to "Trigger Event", then user rules are retrieved based on user control trigger source i.e. user rule retrieved from smartcard for smartcard triggered user control operation and user rule retrieved from terminal database for other trigger source.
    c. If set to "Terminal", then user rule is retrieved from terminal database for all trigger source.

Note: *If no user rules are specified for a given user because the field is missing on the card or in the terminal database, only the controls specified for all users in the terminal configuration will be performed.*

20. **Allow Bio-pin user rule:** This parameter can be enabled to allow terminal to substitute BIO check by a PIN check or BIOPIN check. For this substitution to work, "**ucc.per_user_rules**" parameter shall also be enabled, which allows only users with defined user rule (from DB or CARD) that allows BIO substitution. Possible values are "Disabled", "Use Bio-PIN" or "Use PIN".
    a. If set to "Disabled" then BIO check substitution is not allowed.
    b. If set to "Use Bio-PIN" then BIO check is substituted by BIOPIN check. BIOPIN data is only stored on smartcard. If substitution by BIOPIN is allowed and PIN control is also enabled, then BIOPIN is requested separately from PIN.
    c. If Set to "User PIN" then BIO check is substituted by PIN check. If substitution by PIN is allowed and PIN control is also enabled, then only one PIN check is performed
21. Click on **Save**

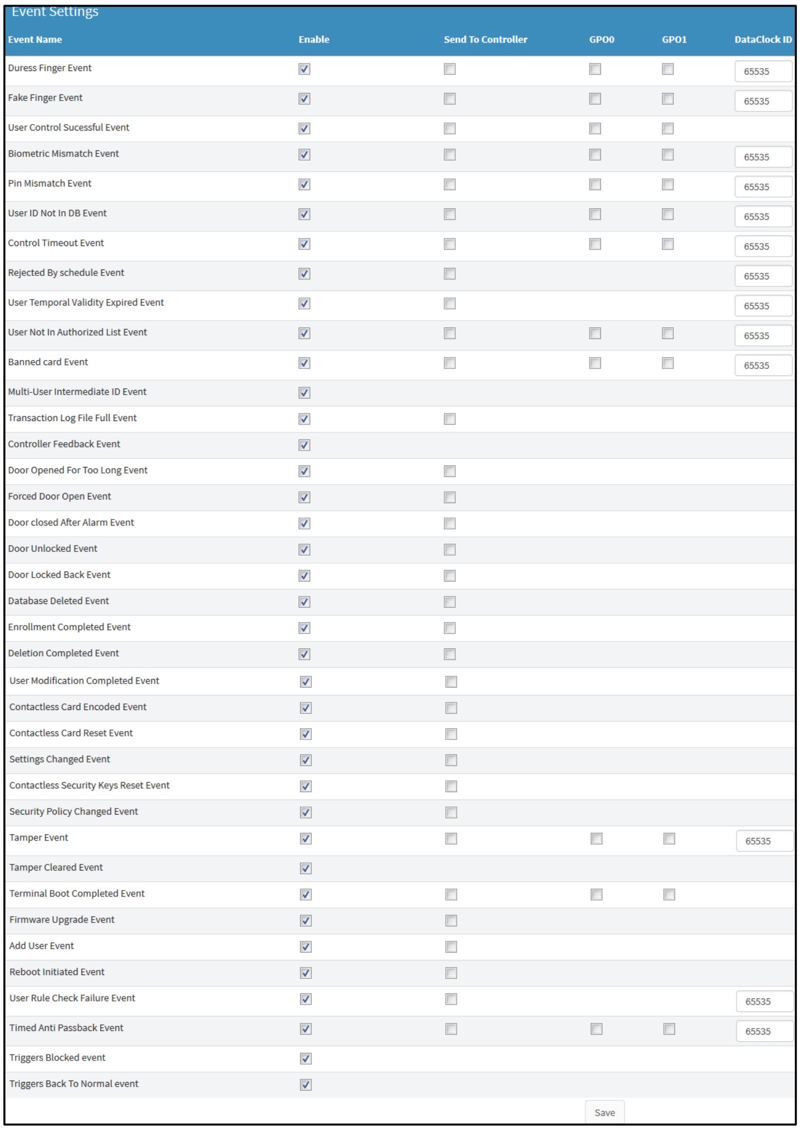
Event Configurations

Events which can be monitored in MorphoAccess® SIGMA Lite Series terminal are listed in event configuration screen of Webserver. An administrator can enable or disable the monitoring and reporting events that can be triggered on terminal. An administrator can also configure which events to be sent to access controller, GPO TTL lines and its data clock id.

Access Path

Webserver > Control Configuration > Event

Screens & Steps



Event Settings

Event Name	Enable	Send To Controller	GPO0	GPO1	DataClock ID
Duress Finger Event	☑	□	□	□	65535
Fake Finger Event	☑	□	□	□	65535
User Control Sucessful Event	☑	□	□	□	
Biometric Mismatch Event	☑	□	□	□	65535
Pin Mismatch Event	☑	□	□	□	65535
User ID Not In DB Event	☑	□	□	□	65535
Control Timeout Event	☑	□	□	□	65535
Rejected By schedule Event	☑	□			65535
User Temporal Validity Expired Event	☑	□			65535
User Not In Authorized List Event	☑	□	□	□	65535
Banned card Event	☑	□	□	□	65535
Multi-User Intermediate ID Event	☑				
Transaction Log File Full Event	☑	□			
Controller Feedback Event	☑				
Door Opened For Too Long Event	☑	□			
Forced Door Open Event	☑	□			
Door closed After Alarm Event	☑	□			
Door Unlocked Event	☑	□			
Door Locked Back Event	☑	□			
Database Deleted Event	☑	□			
Enrollment Completed Event	☑	□			
Deletion Completed Event	☑	□			
User Modification Completed Event	☑	□			
Contactless Card Encoded Event	☑	□			
Contactless Card Reset Event	☑	□			
Settings Changed Event	☑	□			
Contactless Security Keys Reset Event	☑	□			
Security Policy Changed Event	☑	□			
Tamper Event	☑	□	□	□	65535
Tamper Cleared Event	☑				
Terminal Boot Completed Event	☑	□	□	□	
Firmware Upgrade Event	☑	□			
Add User Event	☑	□			
Reboot Initiated Event	☑	□			
User Rule Check Failure Event	☑	□			65535
Timed Anti Passback Event	☑	□	□	□	65535
Triggers Blocked event	☑				
Triggers Back To Normal event	☑				

Figure 134: Events Monitoring Configuration

1. Enable the monitoring of **Events** by selecting the checkboxes corresponding the event
2. An administrator can also select the events which are required to be **Reported to Controller**
3. Select the **GPO lines** using which events are passed to controller
4. Enter **Clock & Data ID**, corresponding to event that is passed to controller through Clock & Data protocol

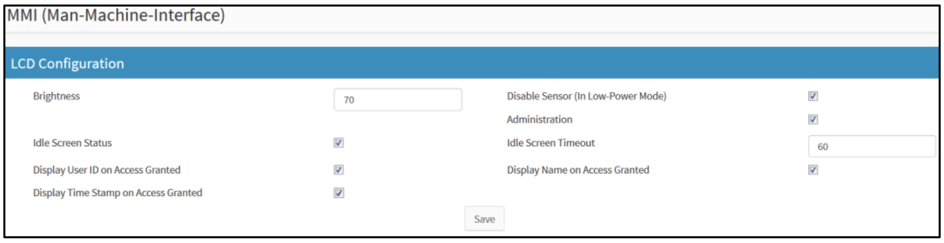
MMI (Man-Machine Interface) Menu

This section of the webserver provides various configurations that an administrator can make to the terminal LCD. This is applicable only to MorphoAccess® SIGMA Lite+ Series terminals only.

Access Path

Webserver > MMI (Man-Machine Interface)

Screens & Steps



MMI (Man-Machine-Interface)

LCD Configuration

Brightness	70	Disable Sensor (In Low-Power Mode)	☑
		Administration	☑
Idle Screen Status	☑	Idle Screen Timeout	60
Display User ID on Access Granted	☑	Display Name on Access Granted	☑
Display Time Stamp on Access Granted	☑		

Figure 135: Man-Machine Interface Menu

1. **Brightness:** The administrator can set the terminal brightness. The range of this parameter is 5-100.
2. **Idle Screen Status:** The administrator can configure the terminal to idle status by enabling/disabling this parameter.
3. **Display User ID on Access Granted:** If this parameter is enabled, upon successful user access control, the User ID shall be displayed on the terminal LCD.
4. **Display Time Stamp on Access Granted:** If this parameter is enabled, upon successful user access control, the Time of the access control result shall be displayed on the terminal LCD.
5. **Disable Sensor (In Low-Power Mode):** If this parameter is disabled then when the terminal should allow user to perform biometric operation (identification) when in Low Consumption mode.
6. **Administration:** If this parameter is enabled, the information menu on the terminal shall be displayed.
7. **Idle Screen Timeout:** The administrator can configure the duration after which the terminal shall switch to Low Consumption Mode. The range of this parameter is 1-3600 seconds.
8. **Display Name on Access Granted:** If this parameter is enabled, upon successful user access control, the User Name shall be displayed on the terminal LCD.

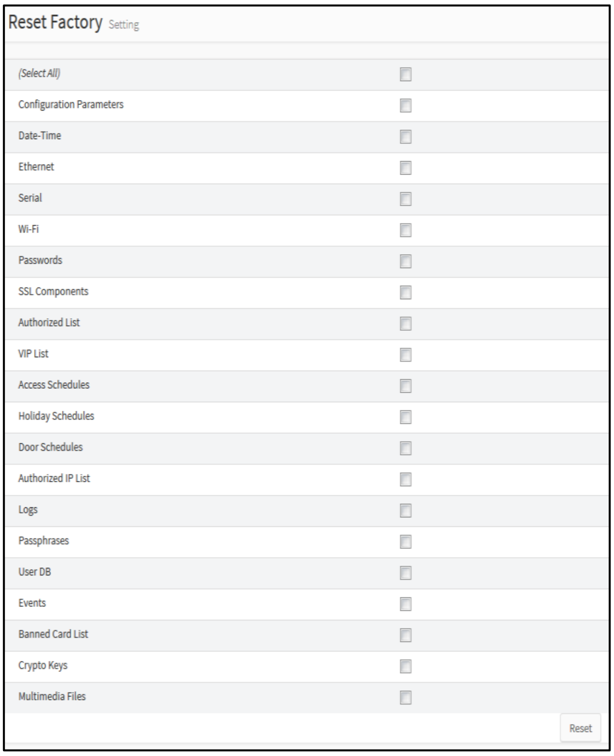
Reset Factory Settings

This screen displays all the parameters that can be reset from the Webserver to Factory Default Settings.

Access Path:

Webserver > Reset Default

Screens & Steps



Reset Factory Setting

(Select All)	□
Configuration Parameters	□
Date-Time	□
Ethernet	□
Serial	□
Wi-Fi	□
Passwords	□
SSL Components	□
Authorized List	□
VIP List	□
Access Schedules	□
Holiday Schedules	□
Door Schedules	□
Authorized IP List	□
Logs	□
Passphrases	□
User DB	□
Events	□
Banned Card List	□
Crypto Keys	□
Multimedia Files	□

Reset

Figure 136: Reset Factory Settings Screen

1. The list of all the parameters are displayed which can be reset to factory default values.
2. To reset any parameter, select the checkbox next to the corresponding parameter name
3. Click on Reset
4. The corresponding parameter values are reset to the factory default settings.

Complete Configuration

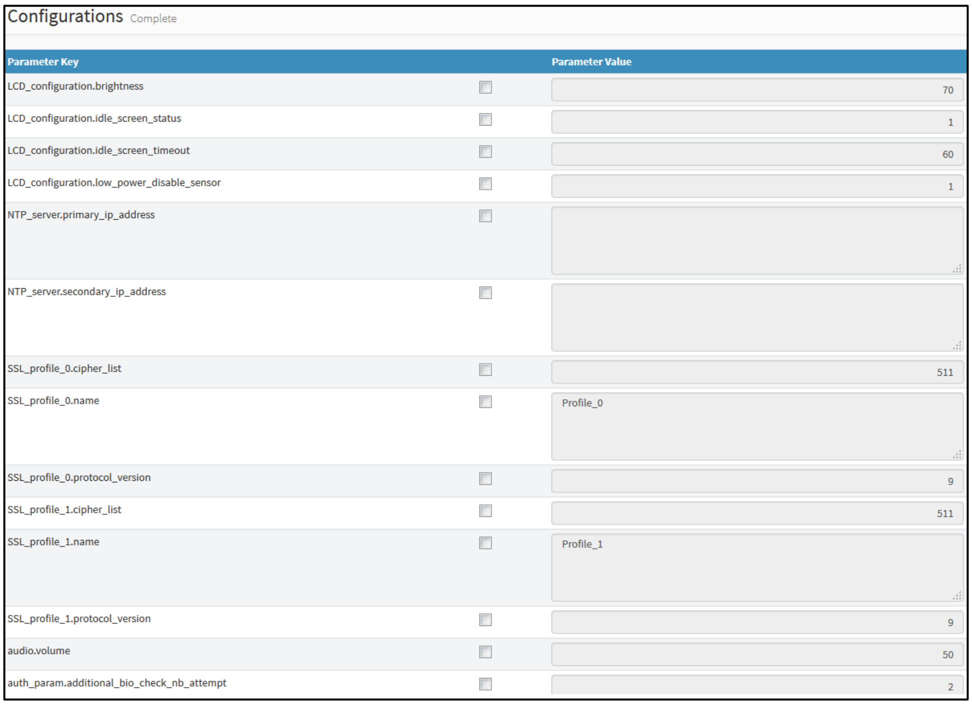
Complete Configuration (Advanced users only)

This configuration screen displays all the parameters of the terminal in only one screen. Then, it is reserved to experimented administrator, who wants to change the value of several parameters related to different features.

Access Path

Webserver > Complete Configuration

Screens & Steps



Configurations Complete

Parameter Key		Parameter Value
LCD_configuration.brightness	☐	70
LCD_configuration.idle_screen_status	☐	1
LCD_configuration.idle_screen_timeout	☐	60
LCD_configuration.low_power_disable_sensor	☐	1
NTP_server.primary_ip_address	☐	
NTP_server.secondary_ip_address	☐	
SSL_profile_0.cipher_list	☐	511
SSL_profile_0.name	☐	Profile_0
SSL_profile_0.protocol_version	☐	9
SSL_profile_1.cipher_list	☐	511
SSL_profile_1.name	☐	Profile_1
SSL_profile_1.protocol_version	☐	9
audio.volume	☐	50
auth_param.additional_bio_check_nb_attempt	☐	2

Figure 137: Complete Configuration Screen

1. The list of all the parameters is displayed with default parameter value
2. For changing the parameter value, select the checkbox corresponding to relevant parameter key
3. The parameter value field will be active. Make necessary changes
4. Click on **Save**

Reference

Refer to **MorphoAccess SIGMA and SIGMA Lite Series Parameters Guide** for detailed understanding.

Section 5 : **Access Control**

Access control presentation

Typical architecture of an access control system

Typical access control system architecture includes:

One MorphoAccess® terminal per area to protect,

A user management or administration menu

A Central Security Controller: for area access final check and physical access command (open the door).

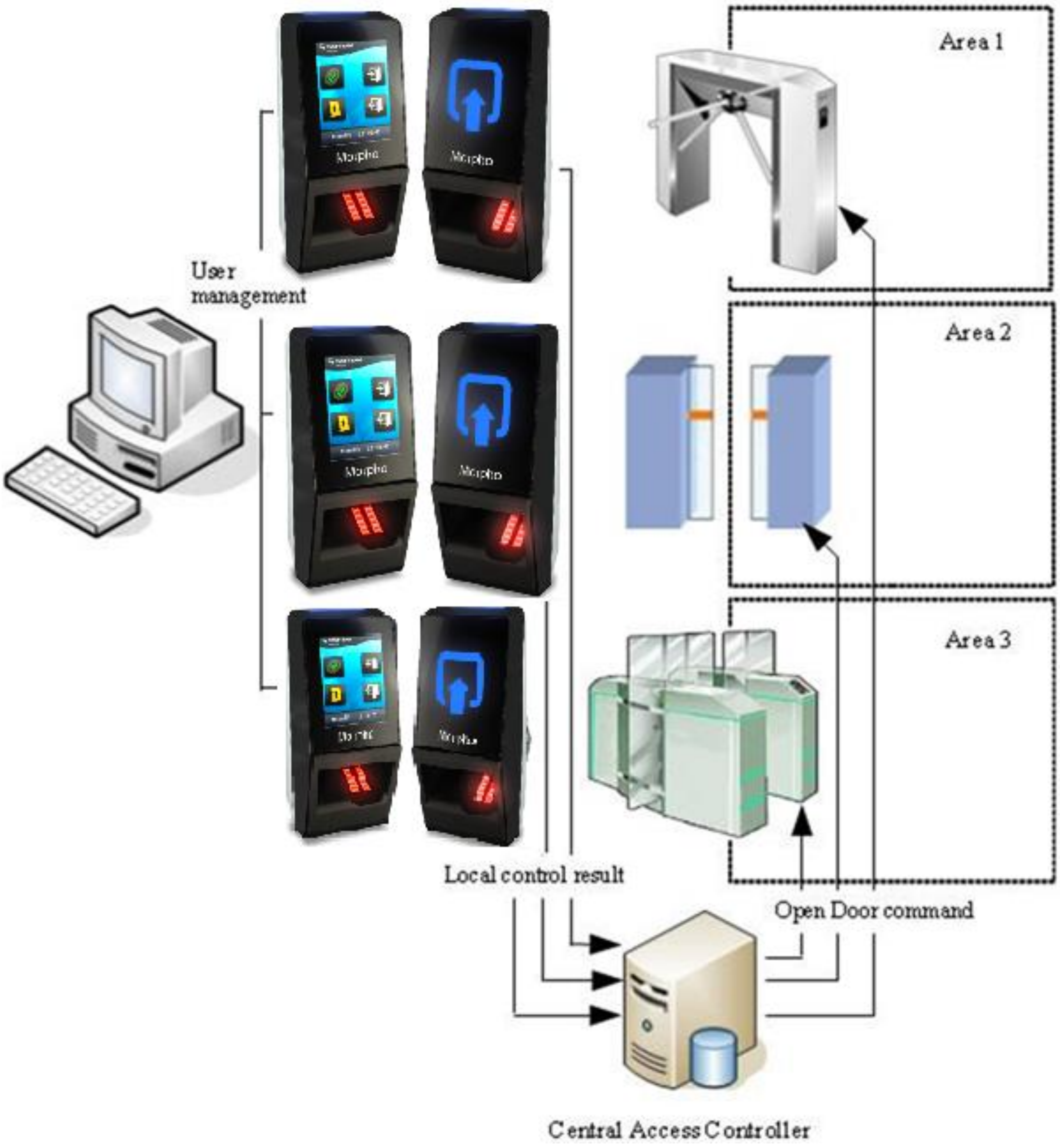


Figure 138: Typical access control system architecture

Typical access control process

1. All authorized users must be enrolled. This means that a record is created for each user, containing a unique identifier and biometric data for two of his fingers.
2. When a user requests the access to the area, the terminal checks user's access rights using a biometric check.
3. If the result of the check is successful (access granted), a message is sent to the Central Security Controller for additional access rights check.
4. If the user is allowed to access to the protected zone, the central access controller returns status access granted to the terminal and an "open" command to the gate controller.

Preliminary: adding a biometric template in local database

The management of internal biometric database can be done externally (through the Webserver) in MorphoAccess® SIGMA Lite Series terminals.

User enrolment can be done by administrator from User Management Menu of the Webserver.

Contactless cards containing user templates can be generated from User Management Menu of the Webserver.

A message can be sent to a distant host to inform that changes were made on the MorphoAccess® SIGMA Lite Series terminal internal biometric database. Then changes can be exported to the host centralized database.

Please refer to "*User Enrollment in Database*" section in this document for a complete description of how a user can be enrolled.

MorphoAccess® terminal operating modes

Standalone mode or Slave mode

The terminal supports two exclusive operating modes:

- **Standalone mode**, where the terminal runs an access control program that can make the access decision alone, or with final authorization from a central access controller. This mode is described in detail in next section below,
- **Proxy mode (slave)**, where a distant system runs an access control application that uses the terminal's high-level functions. This mode is described in detail in the Proxy Mode section.

Standalone mode: Identification and/or Authentication

When in standalone mode, the MorphoAccess® SIGMA Lite Series terminal supports two main different access control processes that can be used separately or together:

- The identification process, which starts when the user places his finger on the biometric sensor. This process is described in the "Identification" section,
- The authentication process, which starts with the communication of the User ID of user, for example by the presentation of a user's contactless card. Next step is the placement of user's finger on the biometric sensor. The terminal allows several authentication processes depending on the location of the reference biometric data, and on the level of security required. These processes are described in the "*Access Control by Authentication*" section.

Identification and authentication processes can also be activated at the same time, as described in "*Multifactor Access Control Mode*" section.

Access Control Process in Identification Mode

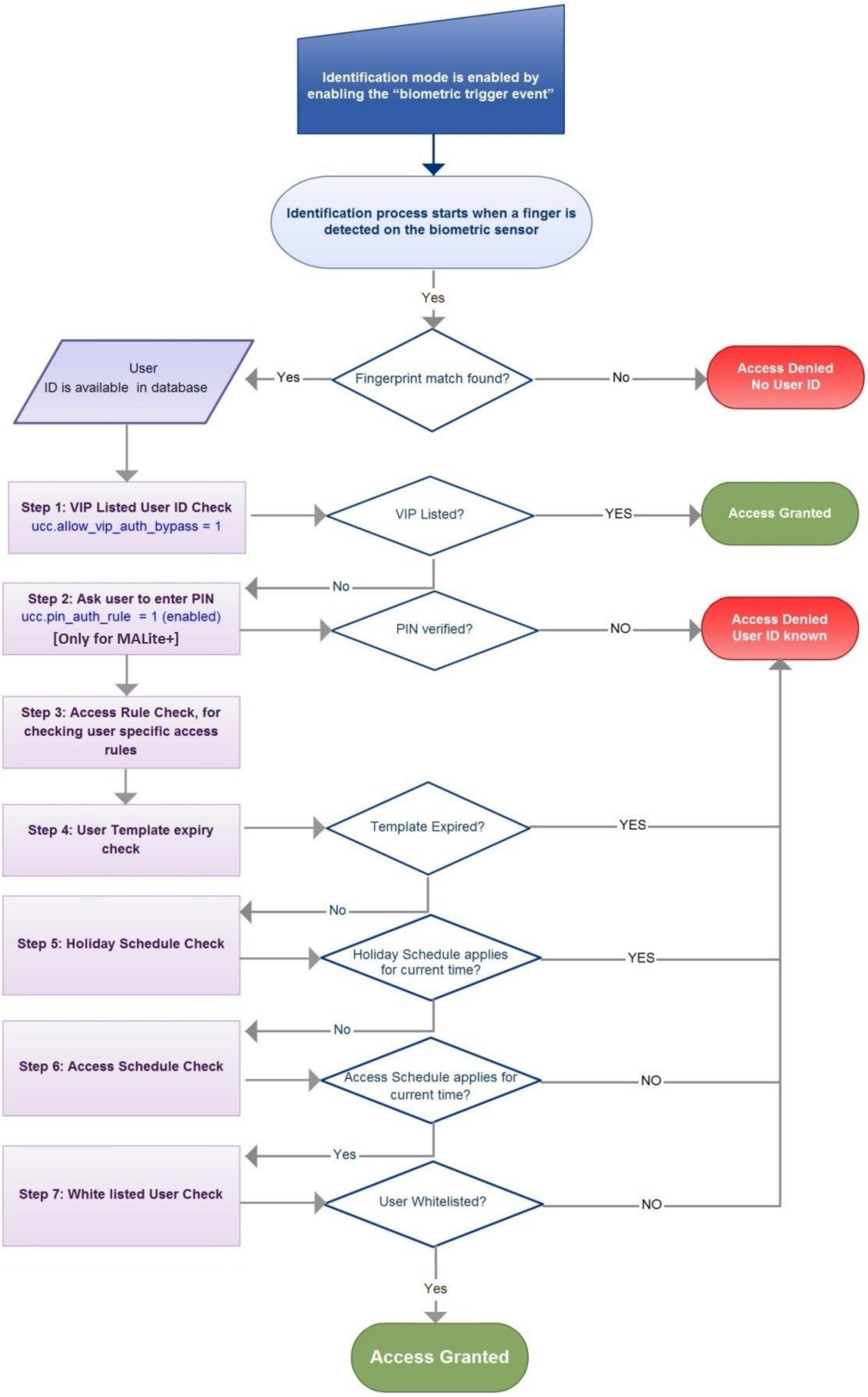

Identification mode is enabled by enabling the "biometric trigger event"
Identification process starts when a finger is detected on the biometric sensor
Yes
Fingerprint match found?
No
Access Denied No User ID
Yes
User ID is available in database
Step 1: VIP Listed User ID Check
ucc.allow_vip_auth_bypass = 1
VIP Listed?
YES
Access Granted
No
Step 2: Ask user to enter PIN
ucc.pin_auth_rule = 1 (enabled)
[Only for MALite+]
PIN verified?
NO
Access Denied User ID known
Step 3: Access Rule Check, for checking user specific access rules
Step 4: User Template expiry check
Template Expired?
YES
No
Step 5: Holiday Schedule Check
Holiday Schedule applies for current time?
YES
No
Step 6: Access Schedule Check
Access Schedule applies for current time?
NO
Yes
Step 7: White listed User Check
User Whitelisted?
NO
Yes
Access Granted

Figure 139: Identification Process Workflow

Access Control Process in Authentication Mode

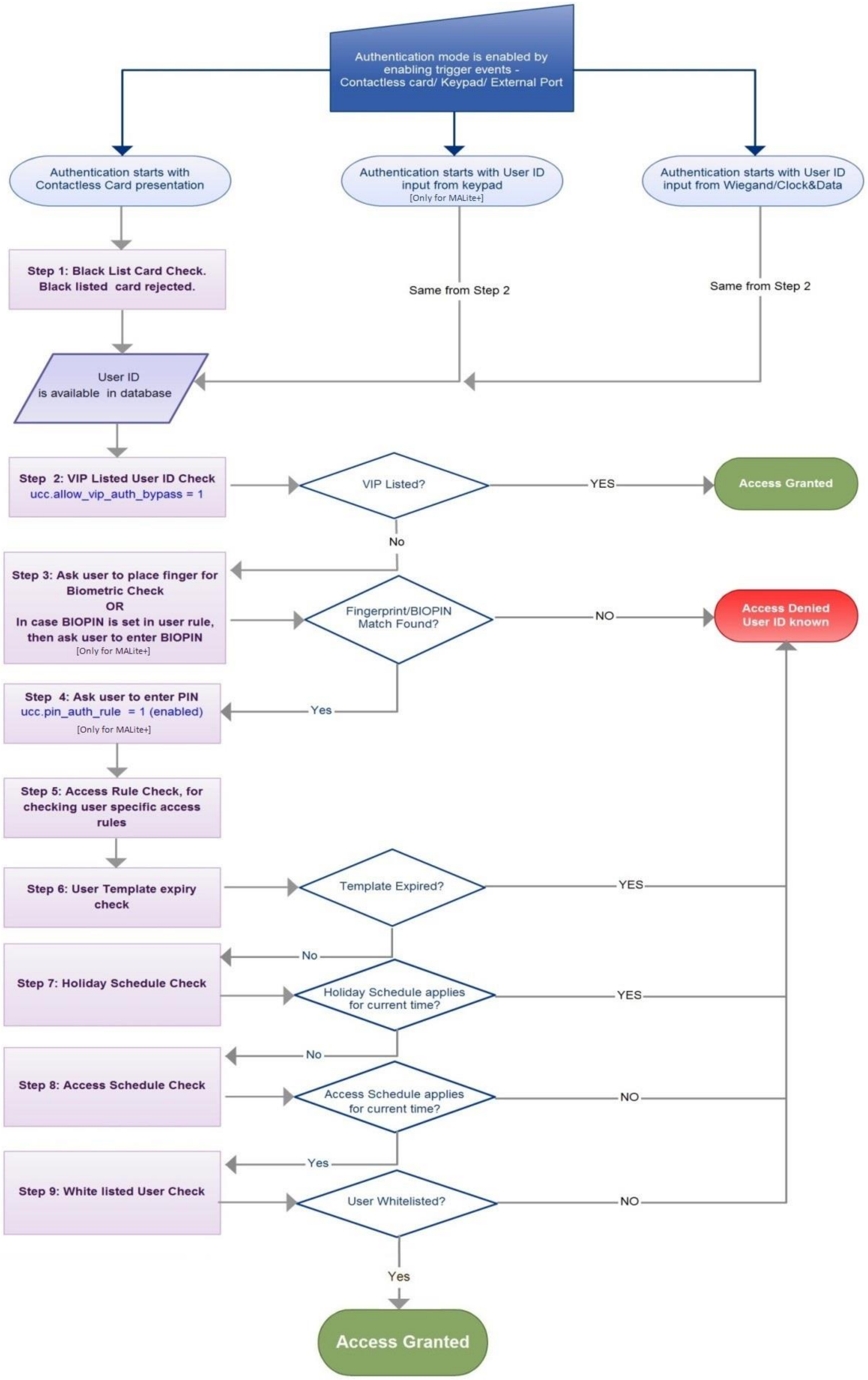

Authentication mode is enabled by enabling trigger events - Contactless card/ Keypad/ External Port
Authentication starts with Contactless Card presentation
Authentication starts with User ID input from keypad [Only for MALite+]
Authentication starts with User ID input from Wiegand/Clock&Data
Step 1: Black List Card Check. Black listed card rejected.
Same from Step 2
Same from Step 2
User ID is available in database
Step 2: VIP Listed User ID Check ucc.allow_vip_auth_bypass = 1
VIP Listed?
YES
Access Granted
No
Step 3: Ask user to place finger for Biometric Check OR In case BIOPIN is set in user rule, then ask user to enter BIOPIN [Only for MALite+]
Fingerprint/BIOPIN Match Found?
NO
Access Denied User ID known
Yes
Step 4: Ask user to enter PIN ucc.pin_auth_rule = 1 (enabled) [Only for MALite+]
Step 5: Access Rule Check, for checking user specific access rules
Step 6: User Template expiry check
Template Expired?
YES
No
Step 7: Holiday Schedule Check
Holiday Schedule applies for current time?
YES
No
Step 8: Access Schedule Check
Access Schedule applies for current time?
NO
Yes
Step 9: White listed User Check
User Whitelisted?
NO
Yes
Access Granted

Figure 140: Access Control Flow Diagram in Authentication Mode

Access Control Process for VIP Users

If the user is listed as VIP, then access control flow will differ from the general access control flows. When a user is enrolled as VIP and the VIP bypass is enabled, then the VIP listed user is exempted from authentication using biometric data, PIN, or BIOPIN.

The Access Control Process for VIP listed users has following steps:

1. A user can initiate access request by placing card or finger
2. One identified as VIP listed user terminal will not ask for any biometric data
3. Other checks such as such as access schedule, holiday schedule, banned card, authorized list, expiry date, trigger event check, etc. are done as per the authentication process, refer from Step 5 in *Access Control Flow Diagram in Authentication Mode*
4. On successful authentication, access is granted to VIP listed user

Note: If the access request is triggered from keyboard or external source like Wiegand string, then the user authentication process will be conducted using biometric/PIN check.

Configuration Key

Parameter Name	Parameter Value	Description
ucc.allow_vip_auth_bypass	0 or 1	Using this parameter an administrator can enable or disable VIP user authentication bypass for threat level 0. If this parameter is set to “0”, VIP user authentication bypass is not allowed. Users have to input fingerprint and access is granted only on successful authentication. If this parameter is set to “1”, VIP user authentication bypass is allowed. A VIP user is granted access without authentication checks.

Access Control Result

Information for the User

The MorphoAccess® SIGMA Lite Series terminal communicates the result of the access right check by a local audible and visible signal. These signals are described in the "*Man Machine Interface*" section.

For example:

when the access is granted, the terminal emits a low pitched note,

When the access is denied, the terminal emits a high pitched note.

Information for the Administrator

The MorphoAccess® SIGMA Lite Series terminal creates a record for each access request, in an internal log file. Each record contains the date and the time, the user's identifier (if available), and the result of the local access control check.

This feature is described in the "*Access Request Result Log File*" section.

Integration in an Access Control System

At the end of the access rights control, the MorphoAccess® SIGMA Lite Series terminal is able to:

- Send a message, with data related to the access request. This feature is described in the Sending the access control result message section,
- Activate an internal relay (if the access is granted to the user), as described in "*Internal Relay activation on Access Granted result*" section.

The format of the messages (which include the user's identifier) sent to the distant system is described in the **MorphoAccess® terminals Remote Messages Specifications** document.

Access Granted

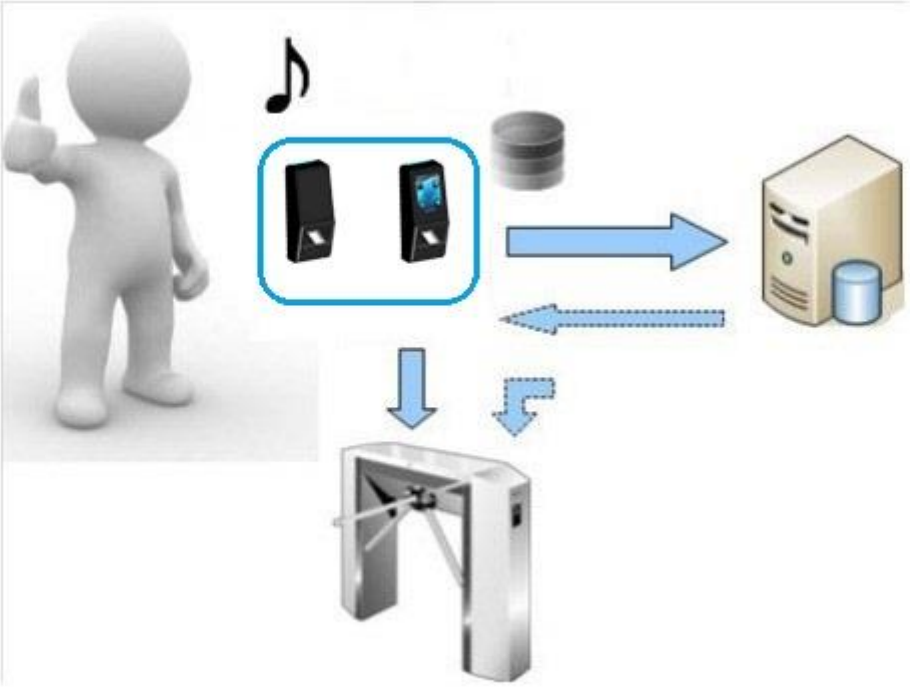


Figure 141: Access Granted Diagram

Access Denied

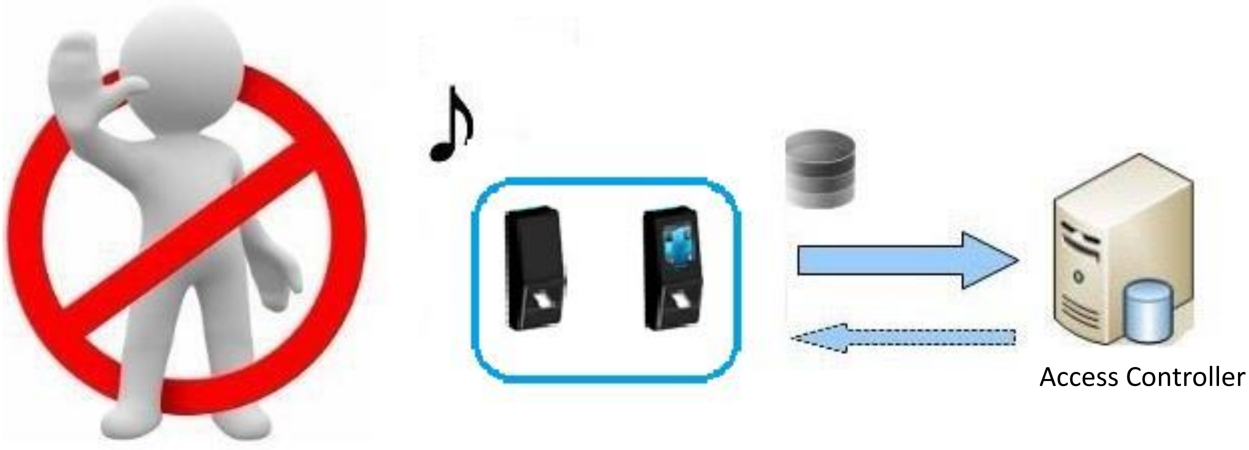


Figure 142: Access Denied diagram

Section 6 : Access Control by Identification

Identification Mode Description

Identification Process

The identification process consists in retrieving the identity of an unknown person, by comparison of a personal data with a base which contains the same type of personal data of known persons. At the end of the process, the person is either identified (identity found), or still unknown.

Access Control by Identification

The Identification process of the MorphoAccess® SIGMA Lite Series terminal proceeds by comparison of the biometric data of the finger placed on the biometric sensor, with the biometric data of all the fingers stored in the database.

It means that the biometric data of the allowed users must be stored in the internal database before they can request the access on the terminal. This biometric data is acquired directly on the terminal (using the Administrator interface), using the biometric sensor.

The access control by identification process is started when a finger is detected on the biometric sensor

When the user requests the access, his identity is unknown, and it is the terminal that searches for his identity. The terminal grants the access if a match is found (the user is identified); otherwise the access is denied (the user remains unknown).

Result of the access control request

The result of the access right control is indicated by an audible and visible signal emitted by the terminal itself. These signals are described in the **Access request result** section under Terminal Sound Interface.

User’s Data required in the terminal

This mode requires that all authorized users must be enrolled in the internal database of the terminal. It means that there is one record per user: each user record contains a unique identifier and the biometric data of two or three different fingers of the user.

The management of the internal database is described in the *MorphoAccess® Terminal Database Management* section.

Identification Modes (Database extension licenses)

Identification process relay on the database, in which user's data are stored at the time of enrolment. By default, MorphoAccess® SIGMA Lite Series terminals database can store up to 3,000 user's records, with the biometric data of 2 or 3 fingers per record. The database extension licenses are available for storing more records, licenses available are listed below:

MA_10K_USERS

Refer to *User licenses* section for more details about licenses.

Compatibility with Access Control Systems

When the identification mode is activated, the MorphoAccess® SIGMA Lite Series terminal supports the optional features listed below:

internal relay activation when the access is granted, as described in "*Internal Relay activation on Access Granted result*" section,

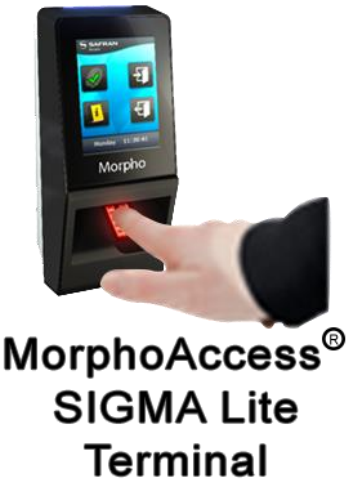
external activation of the internal relay, as described in "*External activation of the internal relay*" section,

send access control result message to a remote system, as described in "*Sending an Access Control Result Message*" section

User Interface

In this mode, the MorphoAccess® SIGMA Lite Series terminal waits for the placement of a finger on the biometric sensor. This state is displayed to the user by a specific signal, as described in Terminal State.

To request the access, the user places his finger on the biometric sensor: this action starts the identification process.



Place finger on
biometric sensor

Figure 143: Identification Mode

The biometric data of the finger is captured, and then compared to all the biometric data stored in the local database of the terminal:

if a match is found, then the user is identified (the terminal has its identifier) and access is granted to the user,

Otherwise, if no match found, the user remains unknown (the user's identifier is unavailable), and the access is denied.

The result of the identification process is notified to the user by a specific signal, as described in Terminal States section.

Section 7 : Access Control by Authentication

Authentication Process

Introduction

The MorphoAccess® SIGMA Lite Series terminal offers an authentication mode designed to work with contactless smart cards used as personal cards.

Then this section relates only to terminals equipped with a contactless smartcard reader (see section *Scope of the document*).

In the whole document the word “card” means “contactless smart card”.

Authentication process

Unlike the "identification" mode, the User Identity must be known in order to execute the authentication process.

Indeed, authentication is an identity verification process: the user provides his identity and the terminal checks it with the relevant process.

This mode doesn’t compare the user’s data to the data of several users: it compares the data provided by the user with the reference data provided by the same user during enrolment phase.

Access control by authentication

To provide his identity, the user presents his personal identity card, which contains his identifier. This action starts the authentication process.

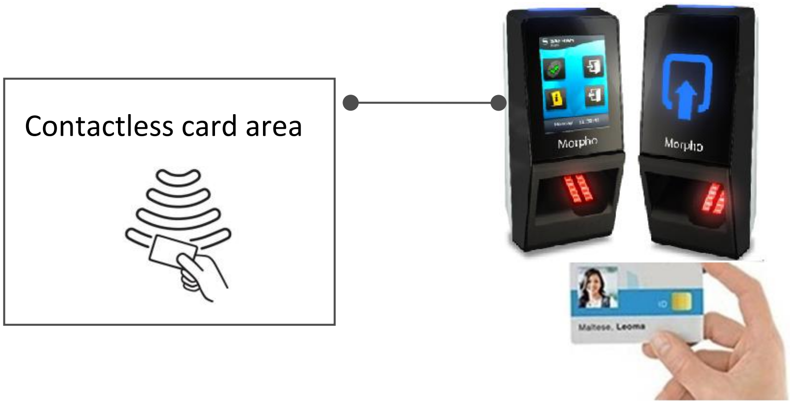


Figure 144: Users trigger the authentication process by showing their card

The user’s card must contain the user’s identifier and optionally his biometric data.

The terminal performs the required identity checks using the data read on the user's card, and if required, data stored in the internal database.

When it is required, the biometric check compares the biometric data of the finger placed on the sensor with the reference biometric data of two fingers of the user, acquired during enrolment process.

If a match is found, the result of the biometric check is positive: user's identity is confirmed. Otherwise, the result of the biometric check is negative: user's identity is not confirmed.

The access is granted only to authenticated users (user's identity confirmed).

The MorphoAccess® SIGMA Lite Series terminal authorizes simultaneous activation of Identification mode and an authentication mode, as specified in "*Multifactor Access Control Mode*" section.

Contactless Smart Card

The terminal ignores contactless cards encrypted with unknown "Card-terminal" authentication keys. Only access requests made with the encoded cards with the same "card-terminal" authentication keys as those for the terminal will be taken into account.

The terminal rejects user's cards without the data required by the authentication process selected.

All authentication modes require the presence of the user's identifier value. The other data and the format of all the data required depends on the authentication mode selected.

All non-mandatory data found on the user's card is ignored.

Please refer to the **MorphoAccess® terminals Contactless Card Specification** document for more information about contactless smartcard logical structure.

Authentication Process Options

The MorphoAccess® SIGMA Lite Series terminal offers several authentication processes, depending on the user's reference biometric data location, and the security level required.

The user's reference biometric data can be located:

either on his personal card, as described in "*Biometric check, biometric data on user's card*" section,

or in a record of the internal database, as described in "Biometric check and biometric data in local database" section

In addition, the biometric check can be disabled as specified in the sections "*Manual bypass of biometric control*" and "*Automatic bypass of biometric control*".

Manual bypass of biometric control

Biometric control is required by default but it can be disabled by the terminal administrator. An administrator can define a user rule for particular users. In this rule, the trigger event through biometric can be disabled and trigger event through Card only is required to be enabled.

For per user rule configuration, refer to "*User Enrollment in Database*" section.

Bypass Biometric Check Rule set for terminal in L1 Legacy mode:-

In L1 Legacy mode, user access rule works along with terminal setting with logical AND operation.

For example,

If User rule is "Keypad + BIO" but biometric check is disabled then for that user BIO check is not performed.

If biometric check is enabled but user rule is "Keypad" only then for that user BIO check is not performed.

Whereas in MA5G mode, user rule is a combination of terminal settings and user rule settings.

For example,

If User rule is "Keypad + BIO" for a particular user and biometric check is disabled on the terminal, then also for that user BIO check is performed (Logical OR operation).

If User rule is “Keypad only” for a particular user and biometric check is enabled on the terminal, then also for that user BIO check is performed (Logical OR operation).

Because of above change in access rule workflow, to achieve L1 use case of disabling BIO check for certain user, follow below procedure

Disabled terminal biometric check

Enable BIO check in user rule for all the user

Disable BIO check for user for whom BIO check needs to be bypassed

Above workflow is achieved in L1 terminal by just disabling BIO check for users for whom BIO checks needs to be bypassed and for all other users keep user rule to default.

When Bypass Biometric Check is enabled in a user profile, terminal will behave as below:

The terminal doesn’t require the user to place a finger on the biometric sensor. The access is granted without biometric check.

According to the authentication process selected, the terminal:

doesn’t perform any check on the user’s identifier, as described in section “No biometric check, no User ID check”

The terminal checks that the user’s identifier is in the terminal database, as specified in the section “*Biometric check and biometric data in local database*”

Automatic bypass of biometric control

The MorphoAccess® SIGMA Lite Series terminal offers an authentication mode which depends on the user's card content.

The terminal searches the user card for data indicating whether biometric control is mandatory or inhibited.

This authentication mode is described in section "*Authentication process specified by User's card*".

Result of access control check

The result of the access control check is signified to the user by local audible and visible signals, as described in the "*Terminal User Interface*".

Compatibility with Access Control Systems

When the identification mode is activated, the MorphoAccess® SIGMA Lite Seriesterminal supports the optional features listed below:

internal relay activation when the access is granted, as described in "*Internal Relay activation on Access Granted result*" section,

external activation of the internal relay, as described in "*External activation of the internal relay*" section,

send access control result message to a remote system, as described in "*Sending an Access Control Result Message*" section

Selection of user's contactless card type (MIFARE®/DESFire®)

Contactless Card type

As MorphoAccess® SIGMA Lite Series terminals are equipped with a contactless smartcard reader compatible with MIFARE® and DESFire® cards, it is possible to specify the type of card to be supported by the terminal:

- MIFARE® cards only,
- or DESFire® 3DES cards only,
- or DESFire® AES cards only,
- or MIFARE® and DESFire® 3DES cards,
- or MIFARE® and DESFire® AES cards,
- or MIFARE® and DESFire® AES and 3DES cards.

The MorphoAccess® SIGMA Lite Series terminals are able to read both DESFire® and DESFire® EV1 smartcards.

The AES cipher is only supported on DESFire® EV1 cards.

The 3DES cipher used on DESFire® EV1 cards is the same as the one used on DESFire® cards (i.e. it is the backward compatibility mode, not the new 3DES cipher of the DESFire® EV1 cards).

Parameter Configuration

The type of contactless smartcard enabled by the access control application is defined by the following parameter value:

Parameter Name	Parameter Value	Contactless Card Type to be Encoded
sc.encode_profile	1	DESFire® 3DES
	2	MIFARE® Classic
	3	Both DESFire® 3DES and MIFARE® Classic at the same time (auto recognition of the card type)
	4	MIFARE® Plus
	5	DESFire® 3DES and MIFARE® Plus at the same time (auto recognition of the card type)
	8	DESFire® AES
	10	Both DESFire® AES and MIFARE® Classic at the same time (auto recognition of the card type)
	12	Both DESFire® AES and MIFARE® Plus at the same time (auto recognition of the card type)

Compatibility with “Authentication” modes

Using a binary value read on the card as user’s identifier is allowed only with MIFARE® smart cards, and when the “sc.encode_profile” configuration key is set to 0 (zero).

All other values of this configuration keys requires TLV formatted data, as described in the **MorphoAccess® terminals Contactless Card Specification** document.

Biometric check, biometric data on user's card

Description

In this mode, each user's card contains an identifier and the biometric data of two or three different fingers of the user. The terminal compares the biometric data of the finger placed on the biometric sensor, with the reference biometric data of the two user's fingers read on the card. If a match is found, the access is granted, otherwise the access is denied.

This authentication mode doesn’t use the internal database of the terminal.

If required, the biometric check can be disabled, as described in the “*No biometric check, no User ID check*” section.

User’s data required in the terminal

This authentication mode doesn’t use the internal database of the MorphoAccess® SIGMA Lite Series terminal. None of the user’s personal data is required in the terminal.

User’s data required on the user’s card

To be compatible with this authentication mode, the user’s card must contain:

the user’s identifier (User ID),

The biometric data of two or three reference fingers of the user.

All other data are ignored.

The data on the card must comply with the TLV format, as described in the **MorphoAccess® terminals Contactless Card Specification** document.

Activation key

Card Type selected at the time of User Enrolment should be at least User ID + Biometric

Using Webserver, the User Record Reference parameter value must be set to Card (Trigger Event) for authentication using smart card. Refer to *User Control Configurations* under Webserver

User Interface

The authentication process starts when the user presents his contactless card in front of the terminal (where the antenna of the contactless card reader is located). If it is compatible (same authentication keys, and mandatory data present on card), the user will be invited to place his finger on the biometric sensor, for biometric authentication.

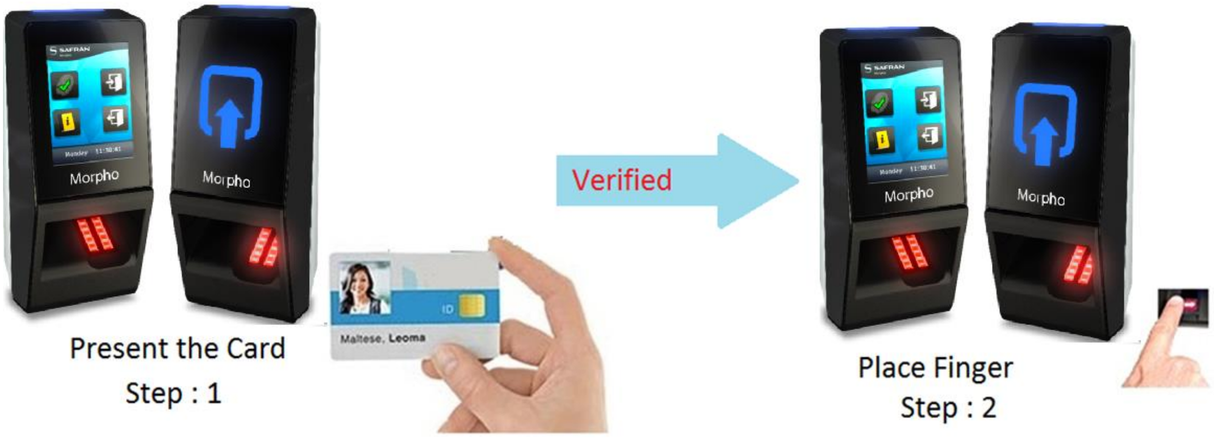


Figure 145: Authentication with user's fingerprints on contactless card

The terminal compares the biometric data of the finger placed on the sensor, with the reference biometric data of the two reference fingers read on user's card.

The authentication process is successful (identity confirmed) if the captured finger data matches with one of the two references finger data. Otherwise, if no match is found, the authentication process fails (identity not confirmed).

The result of the authentication process is notified to the user by a specific signal, as described in Terminal states section.

When the authentication process is completed, whatever is the result (identity confirmed or not), the terminal automatically restarts to the initial state: wait for another user’s card presentation.

PIN verification - PIN stored on card

Description

In this mode, each user's card contains an identifier, PIN Code and the biometric data of two different fingers of the user. The terminal compares the entered PIN Code with the corresponding code in the user's card. If PIN is verified successfully and biometric check is mandatory, then terminal will compare the biometric data of the finger placed on the biometric sensor, with the reference biometric data of the two user's fingers read on the card. If a match is found, the access is granted, otherwise the access is denied.

This authentication mode doesn't use the internal database of the terminal.

If required, the biometric check can be disabled, as described in the "*No biometric check, no User ID check*" section.

Note: This section is applicable for MorphoAccess® SIGMA Lite+ Series terminal only.

User's data required in the terminal

This authentication mode doesn't use the internal database of the MorphoAccess® SIGMA Lite Series terminal. None of the user's personal data is required in the terminal.

User's data required on the user's card

To be compatible with this authentication mode, the user's card must contain:

the user's identifier (User ID),

the PIN code of user

the biometric data of two reference fingers of the user.

All other data are ignored.

The data on the card must comply with the TLV format, as described in the **MorphoAccess®terminals Contactless Card Specification** document.

Activation key

Card Type selected at the time of User Enrolment should be at least "User ID + PIN" or "User ID + Biometric + PIN"

Using Webserver, the User Record Reference parameter value must be set to Card (Trigger Event) for authentication using smart card. Refer to *User Control Configurations* under Webserver

User Interface

The authentication process starts when the user presents his contactless card in front of the terminal (where the antenna of the contactless card reader is located). If it is compatible (same authentication keys, and mandatory data present on card), the user is invited to enter their PIN, for PIN Verification.

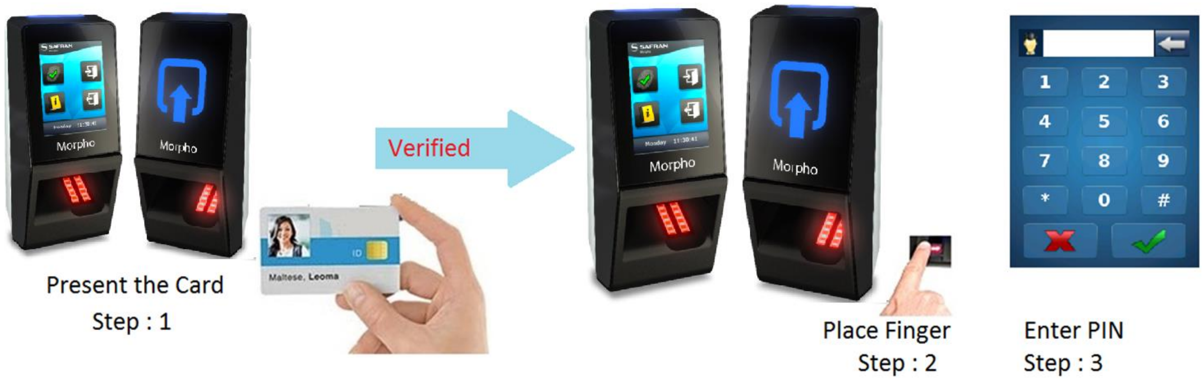


Figure 146: Authentication with user's PIN Code and fingerprints on contactless card

Once the PIN is verified, and biometric check is enabled, then the user is invited to place his finger on the biometric sensor, for biometric authentication. The terminal compares the biometric data of the finger placed on the sensor, with the reference biometric data of the two or three reference fingers read on user's card.

The authentication process is successful (identity confirmed) if the PIN is verified and captured finger data matches with one of the two or three reference finger data. Otherwise, if no match is found, the authentication process fails (identity not confirmed).

The result of the authentication process is notified to the user by a specific signal, as described in

BIOPIN verification - BIOPIN stored on card

Description

In this mode the card should contain a Biometric PIN (BIOPIN). The goal of this code is to replace fingerprints authentication by BIOPIN verification when the fingerprints of the user are not available for verification for any reason. Each user's card contains an identifier and BIOPIN. Authentication process starts when user presents card at terminal card reader and enters BIOPIN. Entered BIOPIN is matched with the BIOPIN stored in card, and then access is granted. This authentication mode doesn't use the database of the terminal.

This feature enables to support two kind of users in the same access control system: normal user with fingerprints (biometric check), and special user without fingerprints but with a BIOPIN code (BIOPIN check instead of biometric check).

Note: This section is applicable for MorphoAccess® SIGMA Lite+ Series terminal only.

User's data required in the terminal

This authentication mode doesn't use the internal database of the MorphoAccess® SIGMA Lite Series terminal. None of the user's personal data is required in the terminal.

User's data required on the user's card

To be compatible with this authentication mode, the user's card must contain:

the user's identifier (User ID),

the BIOPIN code of user

All other data are ignored.

The data on the card must comply with the TLV format, as described in the **MorphoAccess® terminals Contactless Card Specification** document.

Activation key

Card Type selected at the time of User Enrolment should be at least User ID + BIOPIN

Using Webserver, the User Record Reference parameter value must be set to Card (Trigger Event) for authentication using smart card. Refer to *User Control Configurations* under Webserver

A configuration key allows the administrator to enable or disable BIOPIN check.

Parameter Name	Parameter Value	Description
ucc.allow_biopin_user_rule	0 or 1	Set this parameter to “0”, to disable BIOPIN check Set this parameter to “1”, to enable BIOPIN check (Use BIOPIN) Set this parameter to “2”, to set PIN check instead of BIOPIN check (Use PIN)

User Interface

The authentication process starts when the user presents his contactless card in front of the terminal (where the antenna of the contactless card reader is located). If it is compatible (same authentication keys, and mandatory data present on card), the user is asked to enter Biometric PIN (BIOPIN) using keypad, instead of requested to place his finger on the biometric sensor.

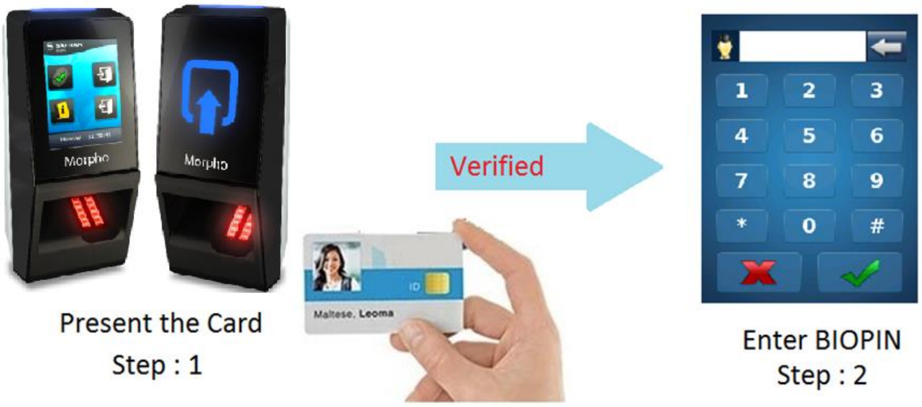


Figure 147: Authentication with user's BIOPIN on contactless card

The terminal compares the BIOPIN entered, with the BIOPIN read from user's card.

The authentication process is successful (identity confirmed) if the entered BIOPIN is matched with the BIOPIN stored on user’s card.

The result of the authentication process is notified to the user by a specific signal, as described in Terminal States section.

Biometric check and biometric data in local database

Description

In this mode, the identifier of the user is the only one data read on user's card. The biometric data of two or three different fingers of the user are stored in the internal database, with the same user’s identifier as the one on the user’s card.

The terminal compares the biometric data of the finger placed on the biometric sensor, with the user’s biometric data found in the database (in user's record). If a match is found, the access is granted, otherwise (no match found) the access is denied.

User’s data required in the terminal

This mode requires the use of the terminal’s internal database and the presence of a record for each authorized user. Each record contains:

the same user’s identifier value as the one stored on user’s card,

the biometric data of two or three fingers of a user.

If the user’s identifier, read on the user’s card, is not found in the database, then the access is denied.

The size and the management of the internal database are described in *MorphoAccess® Terminal Database Management* section.

User’s data required on the user’s card

The only data required on the user’s card is the user’s identifier. All other data is ignored.

The terminal is able to read the user’s identifier either stored in a TLV structure or to be read directly at a given offset on the card (binary format) (MIFARE® card only).

The TLV format is described in the **MorphoAccess® SIGMA Lite Series terminals Contactless Card Specification** document.

Activation key

Card Type selected at the time of User Enrolment should be User ID.

Trigger event "Card" must be ON.

Using Webserver, the User Record Reference parameter value must be set to Card (Trigger Event) for authentication using terminal database. Refer to *User Control Configurations* under Webserver.

User interface

The authentication process starts when the user presents his contactless card in front of the terminal (where the antenna of the contactless card reader is located). If the user's identifier read on the card is found on the terminal's internal database, then the user will be invited to place his finger on the biometric sensor, for biometric authentication.

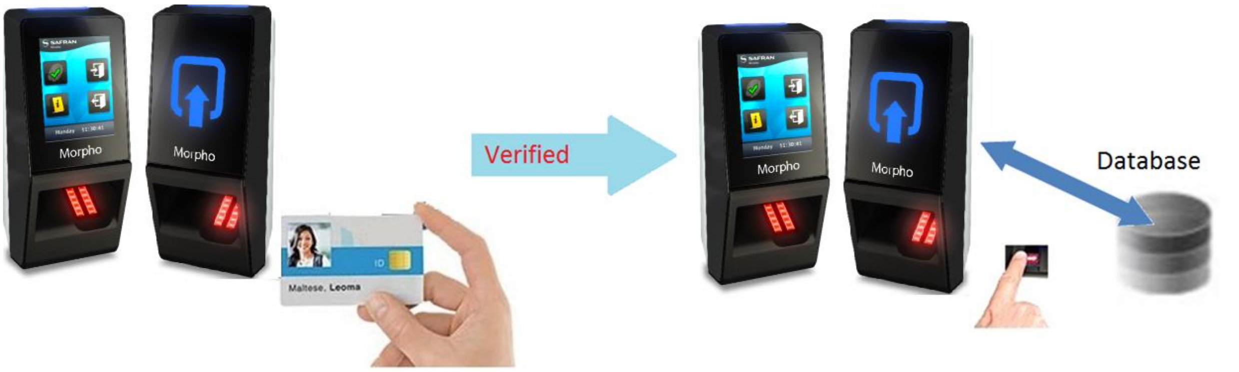


Figure 148: Authentication with biometric check, reference in database

The terminal then compares the biometric data of the finger on the sensor with the reference biometric data found in the database record.

The authentication process is successful (identity confirmed) if the captured finger data matches with one of the two references finger data. Otherwise (no match found) the authentication process fails (identity not confirmed).

The result of the authentication process is notified to the user by an audio signal, as described in Terminal states section.

When the authentication process is completed (whatever is the result), the terminal automatically returns to the initial state: wait for another user's card presentation.

When there is no user stored in the database, this authentication process is disabled. No user is able to grant the access by this way. The terminal notifies this invalid state to the user, as described in Terminal State.

Authentication with local database: User ID entered from keyboard

Description

In this mode, the User ID of the user is entered using the MorphoAccess® SIGMA Lite Series terminal keyboard. If the User ID exists in the database, the terminal performs an authentication using the biometric templates associated to this User ID.

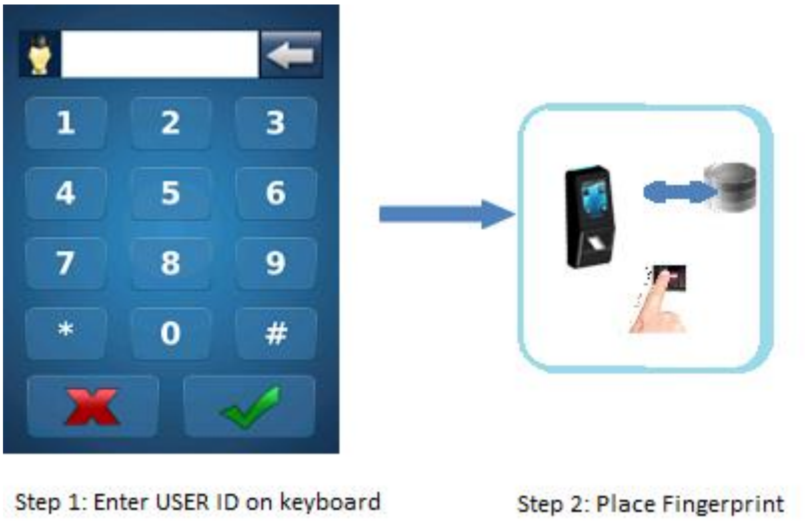


Figure 149: Authentication with User ID entered from Keyboard and biometric check

The authentication process starts when the user enters User ID, using keyboard on terminal. If the user's identifier is found on the terminal's internal database, then the user will be invited to place his finger on the biometric sensor, for biometric authentication.

The terminal then compares the biometric data of the finger on the sensor with the reference biometric data found in the database record. The authentication process is successful (identity confirmed) if the captured finger data matches with one of the two references finger data. Otherwise (no match found) the authentication process fails (identity not confirmed).

Note: This section is applicable for MorphoAccess® SIGMA Lite+ Series terminal only.

Activation key

Trigger event "Keypad" must be ON

Using Webserver, the User Record Reference parameter value must be set to Keyboard (Trigger Event) for authentication using terminal database. Refer to *User Control Configurations* under Webserver.

Authentication with local database: ID input from Wiegand or Clock & Data

Description

This mode requires an external card reader that will send the user's ID to authenticate to the MorphoAccess® SIGMA Lite Series terminal through Wiegand or Clock & Data input.

The default screen invites the user to pass his badge so the external reader sends the User ID to the terminal's Wiegand or Clock & Data input. If the ID exists in the database, the terminal performs an authentication using the biometric templates associated to this ID.

If the authentication is successful, the terminal triggers the access or returns the User ID to the Central Access Controller.

Once the user authentication is done, terminal will automatically loops back and waits for a new input ID. If the identifier sent by the reader is not present in the local database, authentication is not launched.

Activation key

The activation of this mode is controlled by following parameter:

Parameter name	Value	Description
ucc.trigger_event	1 to 15	Use this parameter to enable finger, contactless, keypad and external port trigger. Only when external port trigger is enabled, the terminal would receive trigger from Wiegand or Clock & Data. • Set '8' to enable External Port Note: *Trigger Event* through Terminal and *Event Configurations* through Webserver.
wiegand.external_port_input_type	0 or 1	Storing current external port input type as: • Set '0' for Wiegand format input (default) • Set '1' for Clock & Data format input
wiegand.external_port_output_status	0, -1 or 1	To enable/disable Wiegand output functionality.

Parameter name	Value	Description
		• Set '0' to never send data using Wiegand Port • Set '1' to always send data using Wiegand Port (default) • Set '-1' to send data only when verification is initiated from Wiegand source
wiegand.external_port_output_type	0 or 1	Storing current external port output type as: • Set '0' for Wiegand format output • Set '1' for Clock & Data format output

References

- Wiegand Parameters are configurable from Webserver; refer to *Wiegand Parameters Settings* in this guide.
- You can also refer to MorphoAccess SIGMA and SIGMA Lite Series Parameters Guide for complete list of Wiegand parameters.
- If the MorphoAccess® SIGMA Lite Series terminal is in L1 legacy mode, then Wiegand parameters can be configured from SecureAdmin^{TM} application

Wiegand Frame Configuration

When set up to communicate with Wiegand protocol, the MorphoAccess® SIGMA Lite Series terminal can handle several data formats for reading Wiegand string; refer to *Wiegand Format and Associated Values*.

The default format of Wiegand string is Standard 26 Bits. An authentication is initiated through User ID input from Wiegand string, which consists below information:

- **Total Bits**: The number of Wiegand bits in the Wiegand string (maximum 512 bits length)
- **ID Start Bit**: the start bit of the ID Field (where the first bit is Bit 0)
- **Total ID Bits**: the number of bits in the ID Field (must be contiguous bits).

Using these parameters, when a card is presented to the terminal, it attempts to decode the ID Field and uses that information as the User Identifier (User ID of a template). All Site codes, Parity, and any other data are ignored.

Using the decoded ID, the terminal will verify corresponding User IDs stored in the database.

If the ID is not found in the terminal database, the verification attempt fails and Wiegand output string is set to the Wiegand Port in the configured format. There is no communication with central access controller.

If the ID is valid and a successful verification is performed, the Wiegand Output String is sent to Wiegand port in the configured format.

Note: For sending Wiegand Output, it is required to enable ‘Activate Wiegand Output’ parameter from Webserver. If this parameter is disabled, then no Wiegand output is sent by terminal on verification fail or pass.

Wiegand frame example (26 bits)

For Standard 26 bit - [(26, 9, 16) (1, 8, 10) P1 = (0, Even, 1-12) P2 = (25, Odd, 13-24)],

Wiegand string sent from Terminal 1 to terminal2 will be as below:

0	1	2	3	…	8	9	10	11	12	…	23	24	25
Parity 1	SITE					ID							Parity 2
0	8 bits					16 bits							1

Here,

(26,9,16): consists ID total length, ID start bit, ID length

(1,8,10): consists Site code start bit, length, value

Parity1 (P1): Even parity calculated on 0 bit from 1 to 12 bit. Parity Bit is a check whether the data sent from one device to other is same.

Parity2 (P2): Odd parity is calculated on 25 bit from 13 to 24 bit

No biometric check, no User ID check

Description

This authentication mode is the version of the "*Biometric check, biometric data on user's card*" authentication mode with biometric check disabled.

The terminal searched only for the user's identifier on the user's card. No other check is performed: the user's identifier is not searched in the local database, and there is no biometric check.

A user's card which disables the biometric control is useful when the biometric data capture is not required (for example, for a short period visitor), or impossible (physically or legally). This kind of cards can be realized without user's presence and the same card used for different visitors.

The internal database of the terminal is not used. The MorphoAccess® SIGMA Lite Series terminal acts as a simple contactless card reader.

The access is granted only if the user's card is encrypted with the authentication keys stored in the terminal, and if the terminal is able to read a user's identifier. Otherwise, the card is ignored and the access denied.

User's data required in the terminal

In this authentication mode, the terminal's internal database is not used. No user data is required.

User's data required on the user's card

To be compatible with this authentication mode, the user's card must contain a User Identifier (User ID). It can be in a TLV structured data, or a Binary data to be read on the card (MIFARE® card only).

All other data is ignored.

The TLV format is described in the **MorphoAccess® terminals Contactless Card Specification** document.

The MorphoAccess® SIGMA Lite Series terminal doesn't perform any check on the value of the user's identifier.

Activation key

Card Type selected at the time of User Enrolment should be User ID only.

Using Webserver an administrator can set **User Record Reference** parameter as Card for authentication using smart card, refer *User Control Configurations*.

If no PIN code check and no biometric check are required for the user, then the best is to provide him a Visitor card.

User Interface

The authentication process starts when the user presents his contactless card to terminal. As shown below:

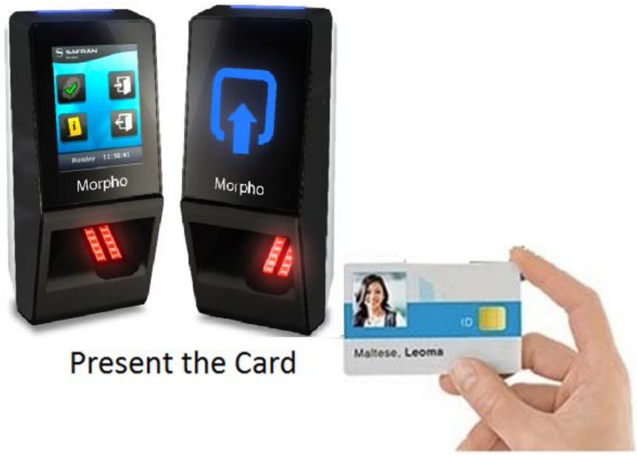


Figure 150: Authentication without biometric check and with User ID check in card

The authentication process succeeds if the user's identifier is found. Otherwise, the authentication process fails.

The result of the authentication process is notified to the user by an audio signal, as described in Terminal states section.

When the authentication process is completed (whatever is the result), the terminal automatically returns to the initial state: wait for another user's card presentation.

No biometric check, User Identifier in the database

Description

This authentication mode is the version of the "*Biometric check and biometric data in local database*" authentication mode, when biometric check is disabled.

The user's identifier is the only data read on user's card. The terminal checks if the user's identifier exists in the database, but doesn't perform any biometric check.

The access is granted if the user's identifier read on the user's card is found in the internal database. Otherwise (user's identifier not found in the database), the access is denied.

User's data required in the terminal

This mode requires a local database, and a record must be created for each allowed user. Each record contains:

the same identifier as the one on the user's card,

the reference biometric data of two fingers of the user (not used, but required)

If the terminal doesn't find a record with the user's identifier read on the card, the access is denied.

The size and the management of the internal database are described in **MorphoAccess® Terminal Database management** section.

User's data required on the user's card

In order to be compatible with this authentication mode, the user's card must contain a User ID. It can be in a TLV structured data, or a Binary data to be read on the card (MIFARE® card only).

All other data are ignored.

The TLV format is described in the **MorphoAccess® terminals Contactless Card Specification** document.

Activation key

- Card Type selected at the time of User Enrolment should be User ID only.
- Using Webserver an administrator can set **User Record Reference** parameter as Terminal for authentication using terminal database, refer *User Control Configurations*.
- Following parameter is required to be configured:

Parameter Name	Parameter Value	Description
ucc.allow_vip_auth_bypass	0 or 1	Using this parameter an administrator can enable or disable VIP user authentication bypass. If this parameter is set to “0”, VIP user authentication bypass is not allowed. Users have to provide fingerprint and access is granted only on successful authentication. If this parameter is set to “**1**”, VIP user authentication bypass is allowed. A VIP user is allowed access without user's identity checks (without finger bio, pin) during user control operation.

User Interface

The authentication process starts when the user presents his contactless card in front of the terminal (where the antenna of the contactless smartcard reader is located).

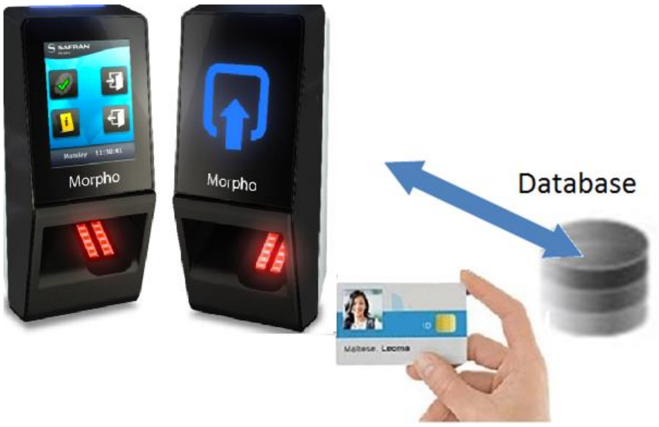


Figure 151: Authentication without biometric check, reference in database

The user's identifier is read on the user's card and searched in the local database.

The authentication process succeeds if the user's identifier is found in the local database. Otherwise, the authentication process fails.

The result of the authentication process is notified to the user by an audio signal as described in Terminal states section. Once the authentication process is completed (regardless of the result), the terminal automatically loops back and waits for another user's card presentation.

Authentication process specified by User's card

Description

When this mode is enabled, the access rights check to perform is specified by a dedicated data on user’s card. It means that the same terminal can execute a different process according to the data found on the user’s card:

the biometric check is performed with the reference biometric data found on user’s card,

the PIN check is performed with the reference PIN data found on user’s card,

the PIN + biometric check is performed with the reference PIN + biometric data found on user’s card,

The biometric check is disabled, and only the presence of the user’s identifier on the user’s card is checked.

A user’s card which disables the biometric control is useful when the biometric data capture is not required (for example, for a short period visitor), or impossible (physically or legally). These kind of cards can be realized without user’s presence and the same card used for different visitors. The internal database of the terminal is not used in such case.

Note: PIN check is applicable to MorphoAccess® SIGMA Lite+ Series terminals only.

User’s data required in the terminal

This authentication mode doesn’t use the internal database of the MorphoAccess® SIGMA Lite Series terminal. There is no personal data stored in the terminal.

User’s data required on the user’s card

To be compatible with this authentication mode, the user’s card must contain at least the user’s identifier and the process selector data.

If the biometric check is requested, the biometric data of two or three fingers of the user must be present on the user’s card.

If PIN check is required, the user's PIN must be on user's card.

All other data is ignored.

The required data must be stored according to TLV format. The user's card format (and the TLV format) is described in the **MorphoAccess® terminals Contactless Card Specification** document.

Activation key

Card Type selected at the time of User Enrolment should be "User ID only", "User ID + PIN", "User ID + Template" or "User ID + PIN + Template" as required

Using Webserver an administrator can set **User Record Reference** parameter as Card for authentication using Card data, refer *User Control Configurations*

If no PIN code check and no biometric check are required for the user, then the best is to provide him a Visitor card.

User Interface

Start

The authentication process starts when the user presents his contactless card at card reader of terminal.

The terminal searches on the user's card, for the data that indicates which kind of check is mandatory or enabled. If this data is found, the terminal executes the required process (with or without PIN code check, and with/without biometric data check).

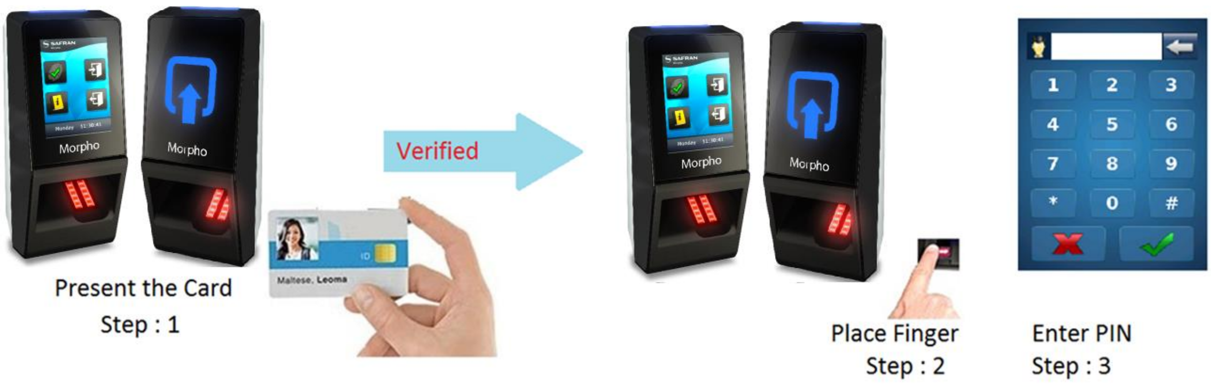


Figure 152: Authentication process specified by user's card

The result of the authentication process is notified to the user by an audio signal as described in Terminal states section.

Once the authentication process is completed (regardless of the result), the terminal automatically loops back and waits for another user's card presentation.

PIN check disabled, Biometric check mandatory

The terminal requires the user to place a finger on the biometric sensor. Then it executes a comparison of the biometric data of the finger placed on the sensor and the reference biometric data read on user's card.

The process is identical to the one described in "*Biometric check, biometric data on user's card*" section.

PIN check disabled, Biometric check disabled

The result of the authentication process is positive (identity confirmed), if the user's identifier is found on the user's card.

The terminal doesn't require the user to place a finger on the biometric sensor, and doesn't perform any biometric check.

The process executed in identical to the one described in "*No biometric check, no User ID check*".

PIN check mandatory, Biometric check mandatory

On User ID verification, the terminal requires user to enter a PIN code. The PIN entered by user is matched with the PIN stored on Card.

On successful verification of PIN, the user is asked to place the finger on the biometric sensor. Then it executes a comparison of the biometric data of the finger placed on the sensor and the reference biometric data read on user's card.

The process is identical to the one described in "*PIN verification - PIN stored on card*" section.

PIN check mandatory, Biometric check disabled

On User ID verification, the terminal requires user to enter a PIN code. The PIN entered by user is matched with the PIN stored on Card.

The process is identical to the one described in "*PIN verification - PIN stored on card*" section.

Allowed format for User's identifier

TLV structured data

The user’s identifier is stored in ASCII characters within a TLV structure.

This is the default configuration of the MorphoAccess® SIGMA Lite Series terminal: the related parameters are listed in the table below for each type of card:

Parameter Name	Parameter Value	Description
sc_tlv_desfire.aid	0 to 16777215 (0x000000 to 0xFFFFFF) (0x42494F - Default)	Sets DESFire® application ID to read/write data on TLV card.
sc_tlv_desfire.fid	0 to 31 (0x00 to 0x1F) (0x00 - Default)	Sets DESFire® file ID to read/write data on TLV card.
sc_tlv_iclass.book_number	0 - 1 (0 - Default)	Sets iCLASS® card book number for 32K for TLV card.
sc_tlv_iclass.page_layout	1 - 5 (1 - Default)	Sets iCLASS® card page layout for 16APP for TLV card.
sc_tlv_iclass.page_offset	0 - 255 (19 - Default)	Sets iCLASS® card Page offset for 2APP for TLV card.
sc_tlv_mifare.key_policy	1, 2 or 3	Sets key policy to read MIFARE® card for TLV mode. Set “1” - Try to read card first with Key A then Key B (Default) Set “2” - Try to read card with Key A Set “3” - Try to read card with Key B
sc_tlv_mifare.num_block	4 - 215 (31 - Default)	Sets number of blocks to read MIFARE® card for TLV mode.

Parameter Name	Parameter Value	Description
sc_tlv_mifare_plus.key_policy	1, 2 or 3	Sets key policy to read MIFARE® Plus card for TLV mode. Set "1" - Try to read card first with Key A then Key B (Default) Set "2" - Try to read card with Key A Set "3" - Try to read card with Key B
sc_tlv_mifare_plus.start_block	4 - 215 (4 - Default)	Sets start block number to read MIFARE® plus card for TLV mode.
sc_tlv_mifare.start_block	4 - 215 (4 - Default)	Sets start block number to read MIFARE® card for TLV mode.
sc_tlv_iclass.num_block	0 to 255 (128 – Default)	Sets number of blocks to read from iCLASS® card for TLV mode.

The contactless smartcard logical structure is described in a dedicated document: **MorphoAccess® terminals Contactless Card Specification**.

Binary Data

Description

The MorphoAccess® SIGMA Lite Series terminal is able to use a binary value to read on specific location on user's card, as user's identifier. The terminal in legacy modes can also write smart card in binary data format.

As a sample of binary value, the serial number of the card can be used, as explained in the "*Example: MIFARE® card Serial Number*" in this section subsequently.

The MorphoAccess® SIGMA Lite Series terminal is able to read a binary value which is not aligned on complete bytes. This ability is useful to extract the user's identifier from a Wiegand frame written on the user's card. A sample is described in "*Example: 32 bits user's identifier within a 37-bits Wiegand frame*" section.

No TLV structure is required on user's card: the MorphoAccess® SIGMA Lite Series terminal is able to proceed with user's cards written by other systems.

Card type compatibility

This feature can only be used when the "MIFARE® card only" mode is set (User ID in binary or TLV format). Then the related configuration key must be set to zero.

Type of contactless smartcard enabled	
sc.encode_profile = 2	MIFARE® card only (identifier of the user is a binary value).

Configuration keys

The binary data to be read is defined by:

the first block containing the data,

the offset of the first byte and first bit of the data, inside the sector. This value must not exceed 15 bytes. The terminal can read data that doesn't start on a full byte,

the length in bytes and additional data bits; this must not exceed 8 bytes. The terminal can read data where the length is not a multiple of 8 bits,

the read direction: MSB or LSB.

User Identifier to be read in binary format	
sc_tlv_MIFARE®.start_block	[4-215] First block to read on card
sc_binary_read.data_length_num_bytes	[0-4294967295] Number of bytes of binary data to read.
sc_binary_read.data_offset_num_bytes	[0-4294967295] Binary reading starting position in bytes from start block.
sc_binary_read.data_type_direction	Set data type direction to read binary data: • 0 - Binary identifier read in LSB • 1 - Binary identifier read in MSB

Example: MIFARE® card Serial Number

In this sample the terminal read the first four bytes, in MSB direction, of the first sector of the MIFARE® card which contains the serial number of the card.

If bytes to read are F4 E1 65 34, then the User Identifier value is "4108412212" (ASCII).

Activation of identification mode	
sc_binary_read.data_type_direction = 1	Binary MSB format
sc_binary_read.data_length_num_bytes = 4	Size = 4 bytes, no additional bit
sc_binary_read.data_offset_num_bytes = 0	First byte of the block
sc_tlv_MIFARE®.start_block = 1	First block of the card

Example: 32 bits user's identifier within a 37-bits Wiegand frame

The user's card contains, at the first block of sector 15 a full 37 bits Wiegand frame (which includes start and stop bits, the site code of the sender, and user's identifier). The first block in sector 15 is block 46.

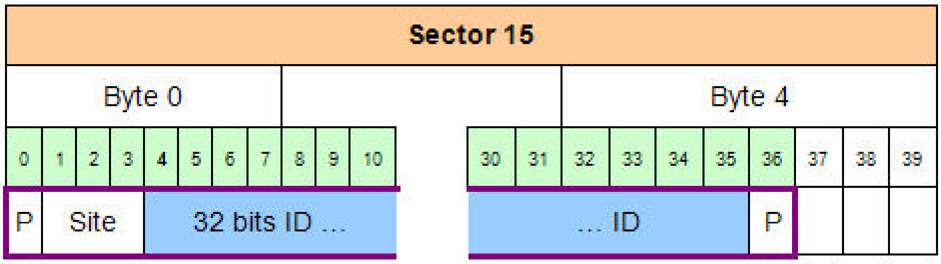


Figure 153: Using a Wiegand frame as User ID

The 32 bits identifier begins at bit four. It is located after the start bit (bit0) and the site code (bit1-2-3), and is followed by the end of frame bit.

Acquisition of a 32 bits user's identifier inside a 37 bits Wiegand frame.	
sc_binary_read.data_type_direction = 1	Binary identifier, MSB format
sc_binary_read.data_length_num_bytes = 4	Size = 4 bytes
sc_binary_read.data_offset_num_bytes = 4	User's identifier begins at bit 4 of the first byte of the block specified below
sc_tlv_MIFARE®.start_block = 46	Read from first block of sector 15 (i.e. block 46)

When the user's identifier must be sent to a distant system using Wiegand protocol, it is possible to configure the terminal to add automatically the start and stop bits to the Wiegand output frame.

Section 8 : **Multifactor Access Control Mode**

Multi-factor Mode

Description

The MorphoAccess® SIGMA Lite Series terminal authorizes simultaneous activation of the access control mode by identification and one of the access control modes by authentication.

This is the first user action which automatically selects the access right control process to be executed.

User Interface

In this mode the terminal is waiting for the placement of a finger on the biometric sensor, or for the presentation of a user's card. It will run:

the identification process if the user places his finger on the biometric sensor first,

Or the authentication process if the user shows his card first.

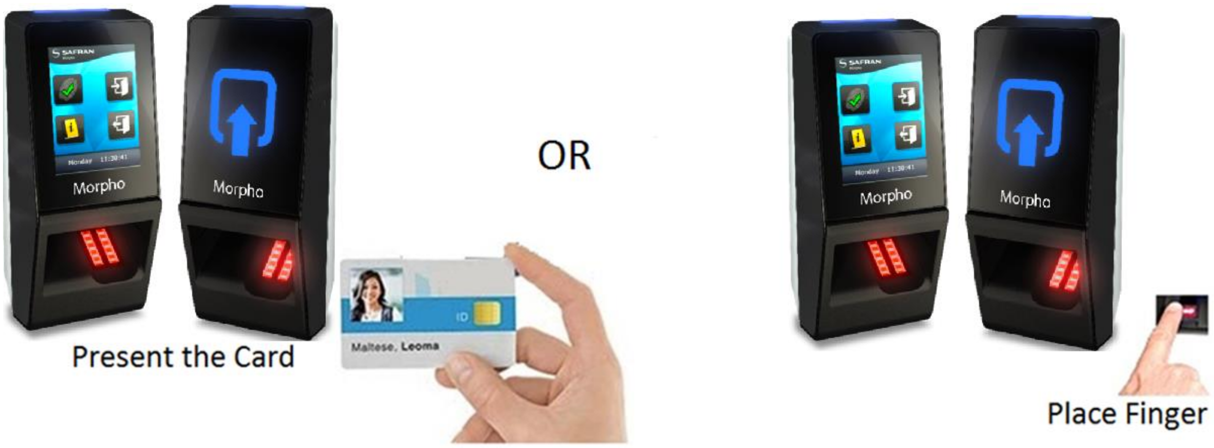


Figure 154: Multi-factor mode (identification or authentication)

When there is no database, the identification mode (with finger) is automatically disabled, but the authentication mode is still available (by showing the card).

User's data required in the terminal

These are the same data as those required by the "*Identification Mode Description*".

These are also the same data as those required by the "*Authentication Process*". Please see corresponding section.

User’s data required on the user’s card

The items required on the user’s card depend on the activated authentication mode(s). Please refer to the appropriate section for further details.

Activation keys

Trigger event through Biometric, Contactless Card, Keypad and External Database should be enabled.

Section 9 : **Time and Attendance Mode**

Time and Attendance Synoptic

MorphoAccess® SIGMA Lite Series terminals can be configured to work in Time and Attendance (T&A) mode. When T&A mode is enabled, each terminal event logged would have some attendance information (such as entry time, exit time, etc.).

When the time and attendance feature is activated, the home screen of the terminal displays certain function keys or a bitmap file. For example, LCD Displays below keys as T& A action:

F1 = IN

F2 = OUT

Instead of texts, icons can be selected to be displayed to the user. Along with biometric presentation, use is also required to select applicable function key (F Key). Suppose, user is entering office in the morning, than F key displaying 'IN' must be pressed. Similarly on every exit and entry the appropriate option must be selected.

T&A action inputs are logged by the terminal. This information is used to track the attendance of an employee, analyze employee productivity and overall organization productivity. Thus Time and Attendance mode becomes a crucial feature for human resource management.

Note: This section is applicable for MorphoAccess® SIGMA Lite+ Series terminal only.

Time and Attendance can be configured as below:

There are 2 function keys that can be associated with T&A action and displayed to the user. When T&A data is required from the user, the terminal displays the Time and Attendance screen below:

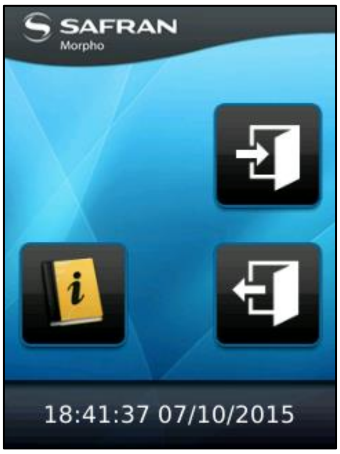


Figure 155: Time and Attendance Screen

In the above sample screen, the IN function is associated to F1 key, OUT function is associated to F2 key. A user can select any of the Function Keys to input required T&A action.

An administrator can configure the Time & Attendance mode by configuring relevant parameters using Web server interface.

Parameter Configuration

Time and Attendance Mode Activation	
time_and_attendance.tna_mode	If an administrator selects parameter value as 0, the T&A mode is disabled. If an administrator selects parameter value as 1, the T&A mode is enabled. When T&A is enabled, it will show 2 F-keys.

T&A Mode Mandatory or Optional Scenarios

Mandatory: An administrator can set T&A Mode as Mandatory. It means it is mandatory for the user to input T&A action by selecting function key, in order to get access. There are three scenarios when T&A is normal mandatory mode and user initiates access request,

T&A before User Control with F Key Selection Initially: It means user first selects a T&A action, then terminal will ask user to place his finger on the sensor or present his card. Then, after user's data acquisition, the terminal checks access rights and display the result for the user.

T&A before User Control without F Key Selection Initially: In this scenario, user will place his finger on the sensor or present his card. Instead of access rights check, terminal will first prompt user to enter a T&A action. Once function key is selected, user access rights check will begin and terminal will display access result

T&A after User Control without F Key: In this scenario, user will place his finger on the sensor or present his card. Terminal will first authenticate the user. On access granted result, terminal will prompt user to enter a T&A action. Once function key selected, terminal will allow access

Optional: If T&A Mode is not mandatory, then user has a choice to whether input the function key or not. The terminal will initiate access rights check without T&A input. However, the transaction logs generated has the records, provided user has input the F key.

Parameter Configuration

Time and Attendance Mandatory/Normal Mode Selection	
time_and_attendance.tna_mandatory_mode	If an administrator selects parameter value as 0, the mandatory mode is disabled. If an administrator selects parameter value as 1, the mandatory mode is enabled.

Refer to *Time and Attendance Mode Configuration* to know more on how to configure T&A parameters using Webserver interface.

T&A - Mandatory Mode Work Flow Diagram

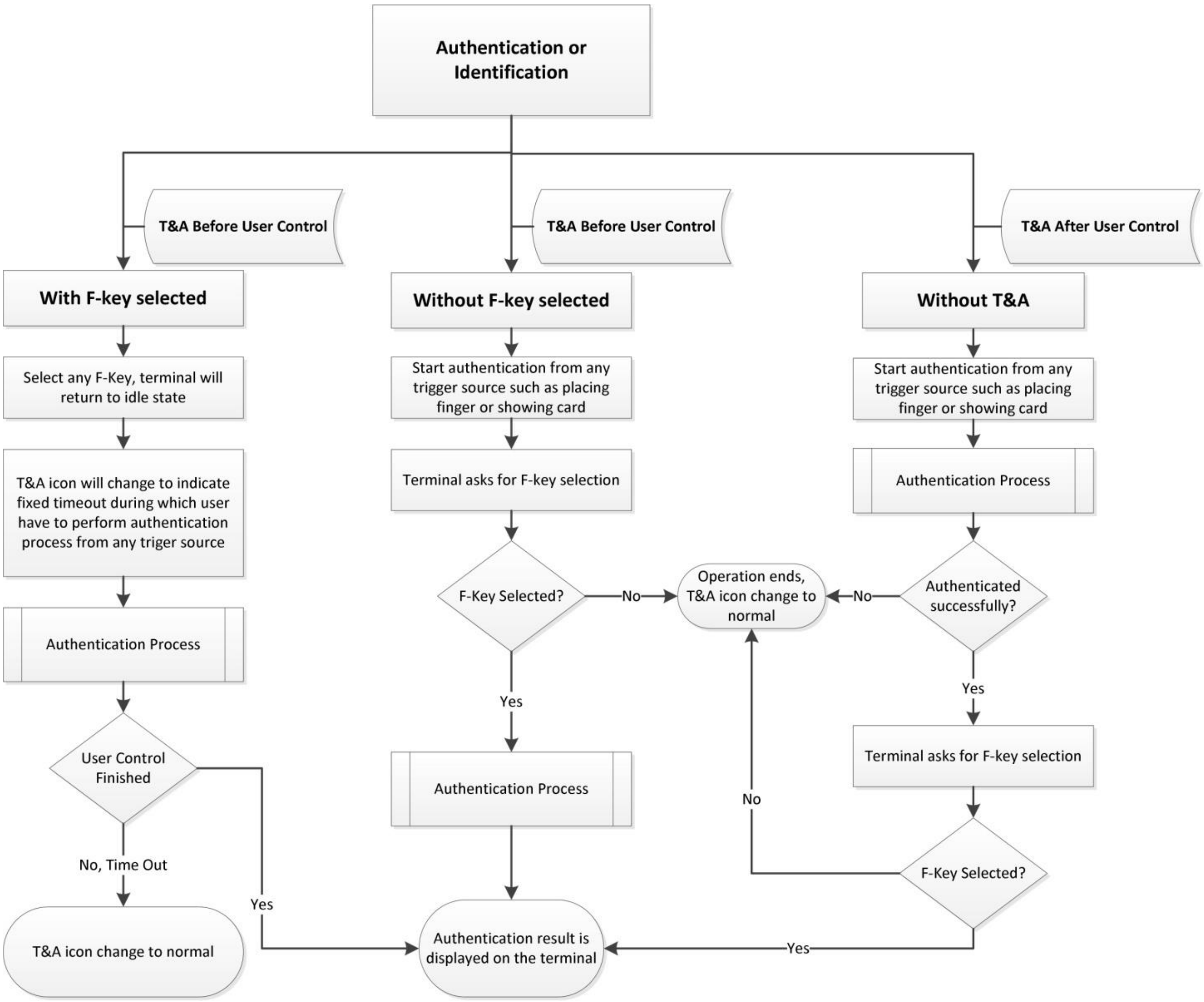

Authentication or Identification
T&A Before User Control
T&A Before User Control
T&A After User Control
With F-key selected
Without F-key selected
Without T&A
Select any F-Key, terminal will return to idle state
Start authentication from any trigger source such as placing finger or showing card
Start authentication from any trigger source such as placing finger or showing card
T&A icon will change to indicate fixed timeout during which user have to perform authentication process from any triger source
Terminal asks for F-key selection
Authentication Process
Authentication Process
F-Key Selected?
No
Operation ends, T&A icon change to normal
No
Authenticated successfully?
Yes
Yes
User Control Finished
Authentication Process
Terminal asks for F-key selection
No
No, Time Out
Yes
F-Key Selected?
T&A icon change to normal
Authentication result is displayed on the terminal
Yes

Figure 156: Time and Attendance in Mandatory Mode Workflow Diagram

T&A - Non Mandatory Mode Work Flow Diagram

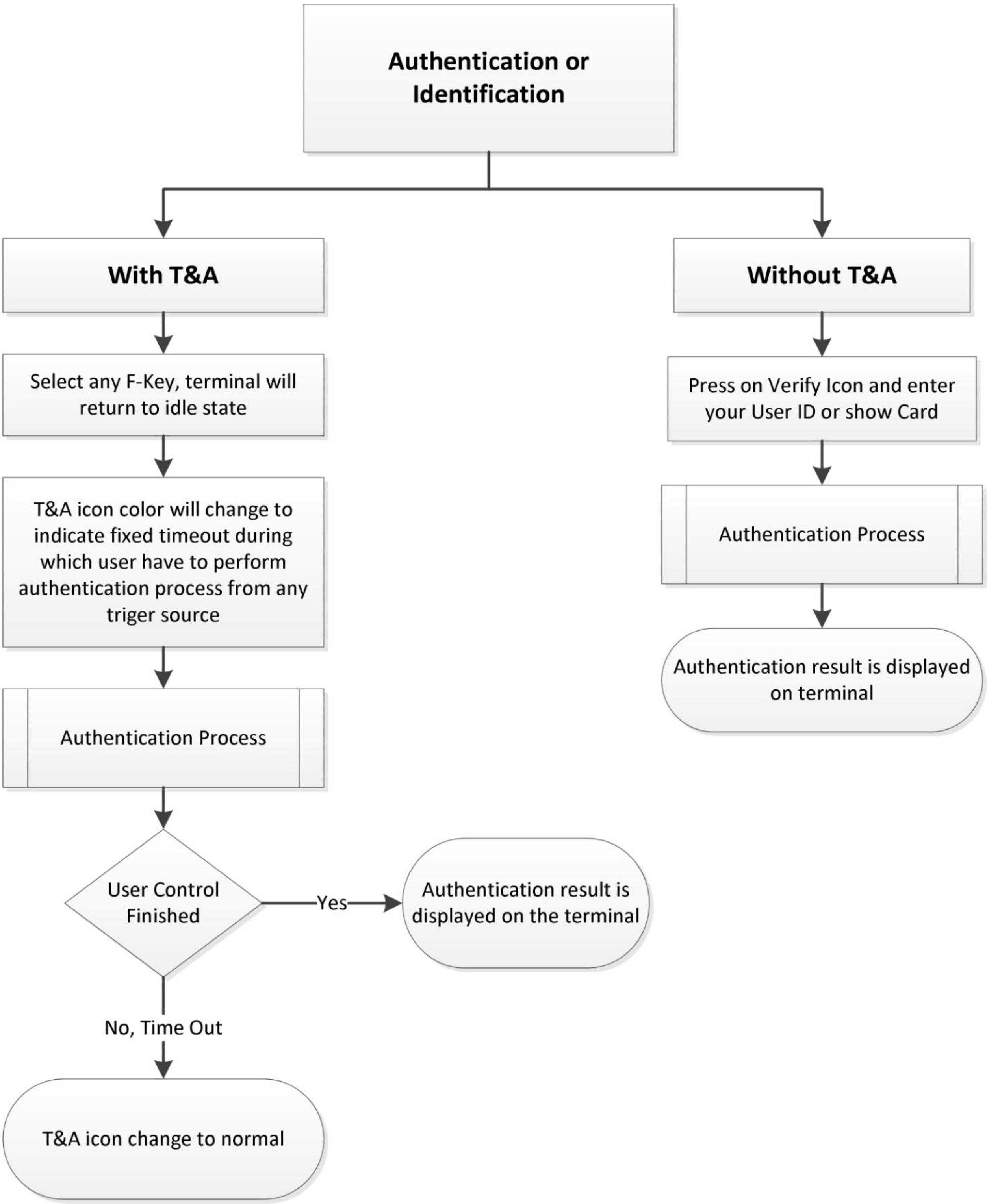

Authentication or Identification
With T&A
Without T&A
Select any F-Key, terminal will return to idle state
T&A icon color will change to indicate fixed timeout during which user have to perform authentication process from any triger source
Authentication Process
User Control Finished
Yes
Authentication result is displayed on the terminal
No, Time Out
T&A icon change to normal
Press on Verify Icon and enter your User ID or show Card
Authentication Process
Authentication result is displayed on terminal

Figure 157: Time and Attendance in Non-Mandatory Mode Workflow Diagram

Note on Terminal Clock Deviation

The terminal clock has a +/- 4 sec per day typical time deviation at +25°C. At 50°C, the time deviation may be up to -8 sec per day.

For application requiring time precision (such as SSL, DESFire®), MorphoAccess® SIGMA Lite Series terminal clock must be synchronized regularly with an external reliable clock.

Section 10 : **Proxy Mode**

Presentation of Proxy (or slave) mode

Process

This operating mode allows to control the MorphoAccess® SIGMA Lite Series terminal remotely (the link is IP or RS422) using a set of biometric and databases management commands.

In Proxy mode the access control is performed remotely by the Host System: the MorphoAccess® SIGMA Lite Series terminal works as a slave waiting for external commands such as:

- ✓ user identification,
- ✓ user verification,
- ✓ relay activation,
- ✓ read data on a contactless smart card,
- ✓ Biometric database management,
- ✓ terminal configuration changes,
- ✓ read an entry from the keyboard,
- ✓ display a message,
- ✓ read a contactless smart card.

The MorphoAccess® SIGMA Lite Series terminal is driven through an Ethernet (or Wi-Fi™) link using TCP or SSL protocol.

The terminal acts as a server: it is either waiting for a command or executing a command.

Please refer to **MorphoAccess 5G Series - Host System Interface**: this document explains how to remotely manage a terminal.

Local signals

When the terminal is waiting for a command from the distant system, there is no local signal (biometric sensor backlight off, status light off).

But when a command is in progress the terminal emits the signals related to the function.

It means, for example, that:

when the Identify command is in progress, the terminal displays the same signals as the standalone Identification mode, when the terminal receives the "access granted" command from the distant system, it emits the "access granted" signal as described in the *Access Request Result*

The local signals are described in the "*Terminal User Interface*" section.

Proxy mode use sample

When terminal is in proxy mode, then using distant commands an administrator can control several functions of the terminal. For example, realize the backup of terminal database, an administrator can activate proxy mode of the terminal, do a backup of database in the remote server, and deactivate the proxy mode.

Within proxy mode, none of the actions can be performed using terminal LCD touch screen.

The sample below describes a typical exchange between the terminal and the distant system for a basic access control by identification driven by the distant system.

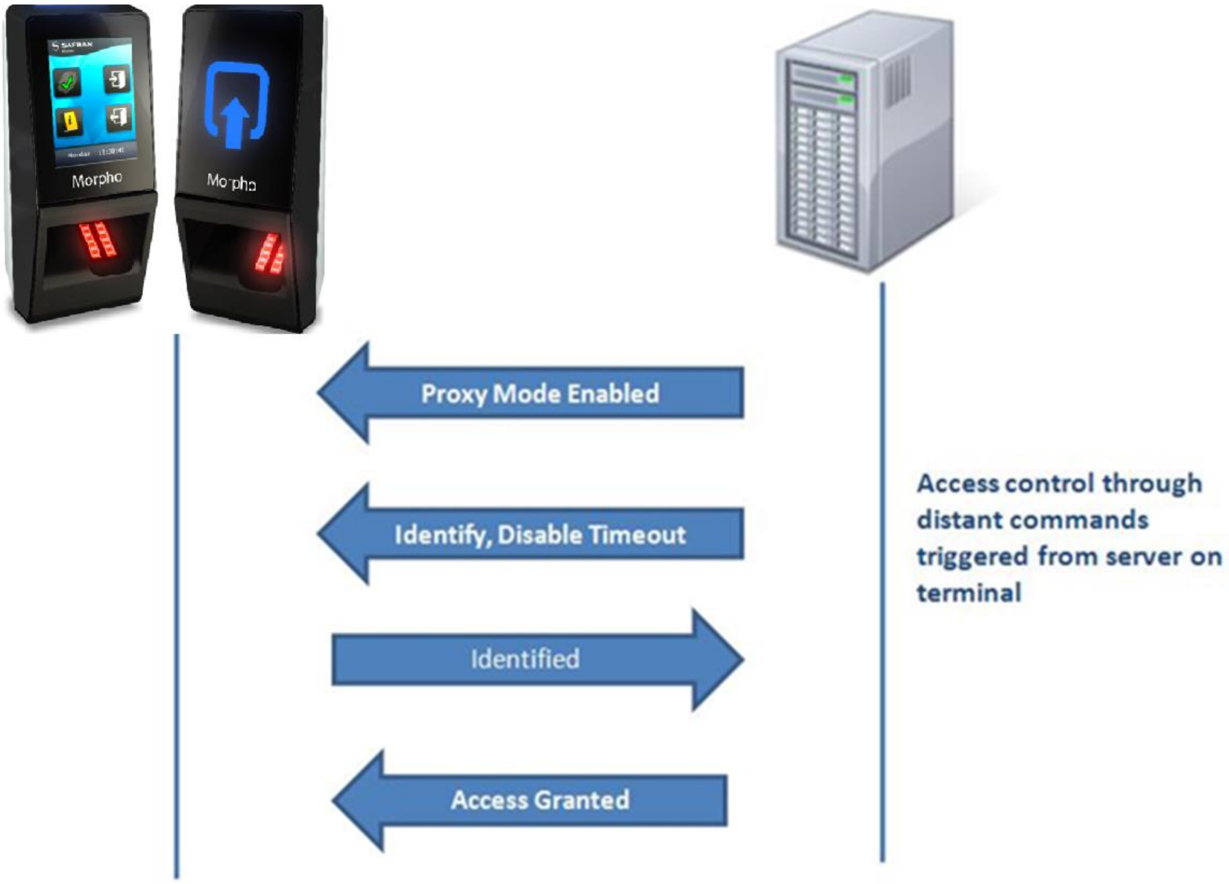

Proxy Mode Enabled
Identify, Disable Timeout
Identified
Access Granted
Access control through distant commands triggered from server on terminal

Figure 158: PROXY sample with a remote Identification process

Proxy mode activation

Proxy mode can be enabled using distant command through a server connected to terminal using serial channel, or Ethernet, or Wi-Fi™.

Please refer to **MorphoAccess 5G Series - Host System Interface**: this document explains how to remotely manage a terminal using distant commands.

Section 11 : **Polling Mode**

Presentation of Polling mode

When polling mode is activated, the MorphoAccess® SIGMA Lite Series terminal does not verify user template in its local database. This mode is useful when the user templates are stored in external database.

When authentication is initiated on the terminal, the terminal will expose the User ID to external controller via polling buffer; the terminal accepts distant commands that provide a reference, overriding the reference specified in parameter ucc.user_record_reference, the ucc.allow_fallback_rule and the user ref_check rule.

If **ucc.per_user_rules** = Trigger Event with trigger as smartcard then user rule from smartcard will be used and NOT from one provided by distant command.

If **ucc.per_user_rules** = Terminal then user rule provided by distant command will be used.

If **ucc.per_user_rules** = Disabled then user rule check is disabled.

Process

Polling using buffer:

The user’s input ID will be queued in the terminal’s queue, which is polled by external application.

External application waits for the User ID by polling the buffer. After getting an ID, it will search the template in database and send template to terminal for further authentication.

The user is authenticated by the external terminal and granted access accordingly.

MorphoAccess® SIGMA Lite Series terminal also has distant commands to retrieve polling buffer status and polling buffer data. Refer to **MorphoAccess 5G Series - Host System Interface** guide.

Polling mode activation

Polling mode can be activated through Webserver > Complete Configuration, by setting "**ucc.enable_external_database**" parameter value as '1'. Only an administrator can activate polling mode. An administrator can refer to **MorphoAccess SIGMA and SIGMA Lite Series Parameters Guide** to know how to set this parameter.

NOTE: When terminal is in L1 legacy mode, then polling mode can be configured using Secure Admin application.

Section 12 : **Messages Sending**

Message Sending

Principle

When specific events occurred during the MorphoAccess® SIGMA Lite Series terminal access control application’s working, some messages can be generated and sent to another physical entity.

The events that produce messages sending are:

Result of access rights check (after access request by a user),

Internal log file full,

Tamper detected,

Time and Attendance actions,

Duress Finger detected.

Please refer to **MorphoAccess® SIGMA Lite Series Remote Messages Specification** for details about the messages content.

Events

MorphoAccess® SIGMA Lite Series terminal allows an administrator to select several events on which messages can be sent to external controller. An administrator can enable or disable events using Webserver or distant command.

Refer to *Event Configurations* under Webserver section in this document, to learn more on various events that can be selected.

Sending Interfaces

The terminal allows choosing the number of interfaces that will be available for the messages sending process.

By default, no interface is available. Set below parameter for activating remote message sending:

Number of available interfaces	
Remote_msg_conf.send_ethernet_state	This parameter can be set as "1" to enable message sending over Ethernet/IP Channel
Remote_msg_conf.send_serial_state	This parameter can be set as "1" to enable message sending over Serial (RS485)

For each interface available, the following parameters are customizable:

- Communication layer
- Protocol used
- Parameters depending on the layer and the protocol used.

There is TCP protocol on the IP layer that is available. In that case, the parameters available are for host 1 are as below:

TCP parameters	
remote_msg_ip_conf.host_1_ip	The distant IP address to contact
remote_msg_ip_conf.host_1_port	The distant port to connect to
remote_msg_ip_conf.host_1_protocol	Protocol Type used for communication through TCP channel
remote_msg_ip_conf.host_1_timeout	Timeframe within which terminal is required to connect with host 1 remote controller and read/write the commands

The same parameter is configurable for host 2, in case terminal is not able to connect to host 1 server, and then it will attempt to send message on host 2. Please refer to MorphoAccess SIGMA and SIGMA Lite Series Parameters Guide for further details about the interfaces configuration.

Section 13 : Compatibility with an Access Control System

Internal Relay activation on Access Granted result

Description

If the result of the access rights check is successful, the internal relay may be optionally activated, for example, to directly trigger a door switch.

The duration of the activation of the internal relay can be modified by a specific configuration key.

Access control installation using internal relay offers a lower security level, than an installation with a central access controller which is the only one allowed opening the door.

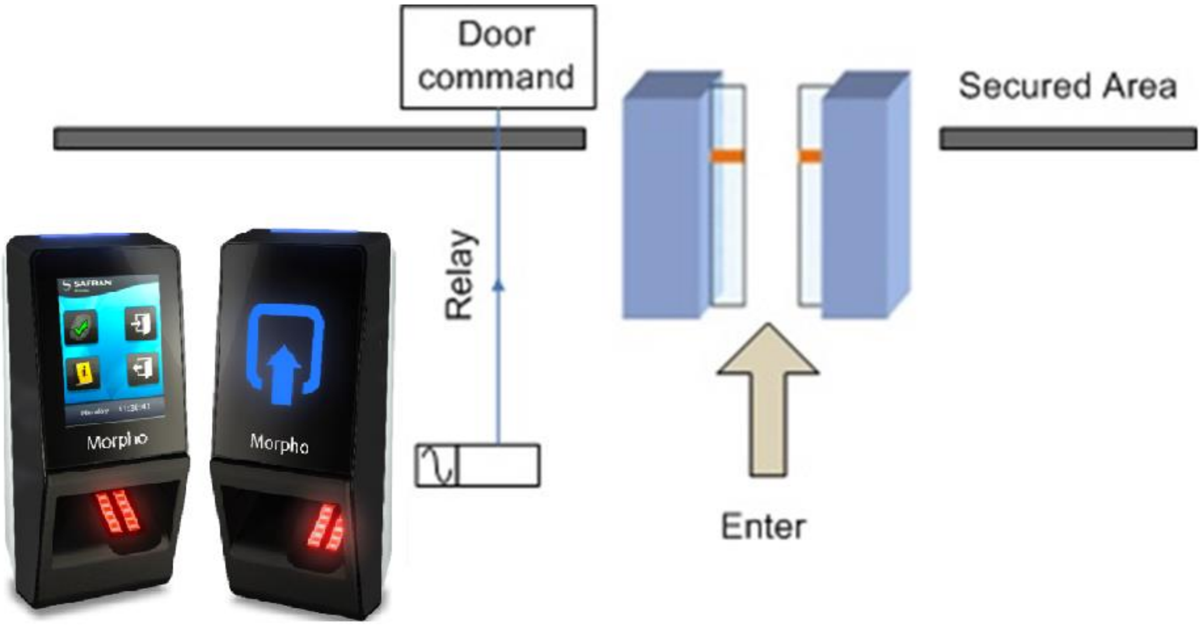


Figure 159: Using the internal relay on the MorphoAccess® SIGMA Lite Series terminal

Activation key

Configuration key enables internal relay activation on access granted is:

Parameter name	Value	Description
gpio.sdac_relay_default_state	0 or 1	Using this parameter, an administrator can set a default state of the internal relay, which is powered or unpowered. Select "0" for Low. It indicates that by default the internal relay will be unpowered and on access granted the internal relay state will change to high (it will be powered). Select "1" for High. It indicates that by default the internal relay will be powered and on access granted the internal relay state will change to low (it will be powered off).

Configuration key

Parameter name	Value	Description
gpio.sdac_door_unlock_dur	2 - 60 sec. (10-Default)	Configuration for duration for which SDAC door should be opened after access is granted. This parameter can be set only when gpio.func_mode is set as "2" (SDAC).

External activation of the internal relay

Description

This function allows the activation of the terminal internal relay via a push button connected between the LED1 and the GND wires. Then the internal relay is activated in two cases: when the terminal authorizes the access after access rights check, and when a contact is closed between the LED1 and GND terminals.

A typical application of this feature is to open the door from inside an area protected by a MorphoAccess® SIGMA Lite Series terminal (as described in figure below):

to enter in the protected area the user must be successfully recognized by the MorphoAccess® SIGMA Lite Series terminal,

to exit from the protected area, the user presses a simple push-button connected between the LED1 and GND wires of the MorphoAccess® SIGMA Lite Series terminal.

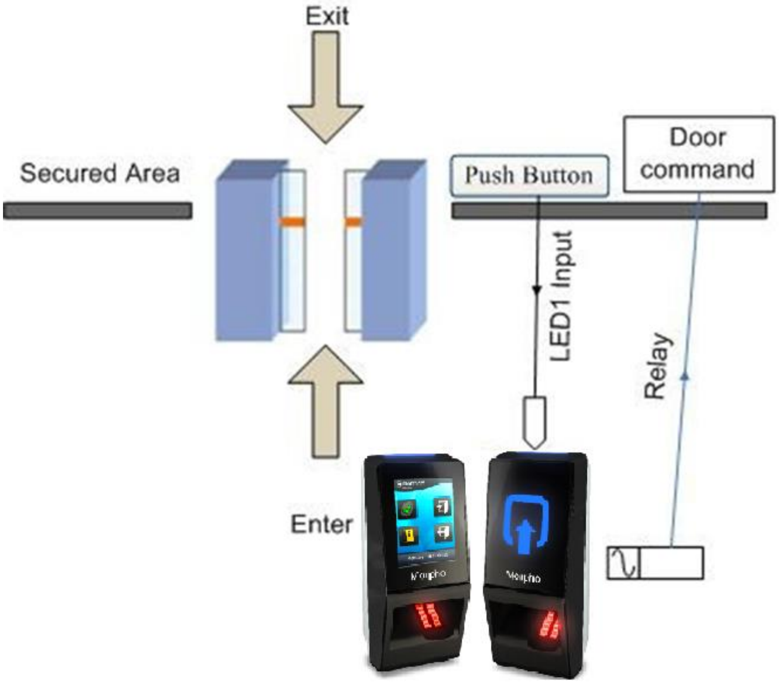


Figure 160: Internal relay activated by LED 1 signal

Activation key

A specific configuration key enables this feature.

Parameter name	Value	Description
gpio.sdac_rte_mode	0, 1	Using this parameter, an administrator can set an exit mode in SDAC. Following parameter values can be configured: • Parameter value "0" means None • Parameter value "1" means Push Button. Push button exit mode is selected when a push button is located at exit gate and users are allowed push the exit button to open the exit door.

Configuration key

Parameter name	Value	Description
gpio.sdac_rte_egress_timeout	1 to 300 Seconds	Using this parameter, an administrator can define an egress time, the duration for which door will be opened on Request to Exit (Push Button – Manual) and on timeout door is closed automatically.

Access Request Result Log File

Description

When enabled, the terminal creates a record for each access request in a local log file. Each record includes:

the date and the time of record creation (when access control result is known),

the user’s identifier (if available),

the access control process executed (Identification, Authentication with biometric check, etc.),

the result of the access control: granted or denied, and if denied for which reason, (user not recognized, outside authorized time slot, etc.),

and other data used for statistical reasons.

The format of a log record is described in the MorphoAccess 5G Series - Host System Interface document.

Log File management

Three commands are available for log file management:

a command which returns the current status of the log feature (enabled/disabled, number of records),

a command which returns the content of the log file,

a command that deletes the log file.

For more information about these commands, refer to MorphoAccess 5G Series - Host System Interface document.

Log File size

The capacity of the internal log file is customizable up to 1,000,000 records by installing *Logs licenses* (default value is 100,000).

When the file is full, the log will initiate to delete the old logs and log the new logs and, depending on the terminal settings, a WARNING message may be sent to a remote system.

The format of the “Log File Full Warning” message is described in the **MorphoAccess® terminals Remote Messages Specification** document.

Activation key

The creation of a record for each access request is enabled (and disabled), by only one configuration key.

Parameter name	Value	Description
transaction_log.logging	0, 1 or 2	This parameter allows an administrator to set transaction log logging status, as below: Set parameter value “0”, to disable transaction logging Set parameter value “1”, to enable access control logging. It means only user access accepted and rejected, along with timings and profile details are logged. Set parameter value “2”, to enable full logging. Full logs include record of each action performed on terminal.

Sending an Access Control Result Message

Presentation

After access control rights check, the MorphoAccess® SIGMA Lite Series terminal can send a message which contains the result of the control, to a distant terminal. The MorphoAccess® SIGMA Lite Series terminal is able to use different channels and different protocols, to send this message.

This message can be used for different actions, depending on the role of the receiver in the access control system: simple logging of access requests (no response expected), or performing additional checks on access rights (expected response: access authorized or denied).

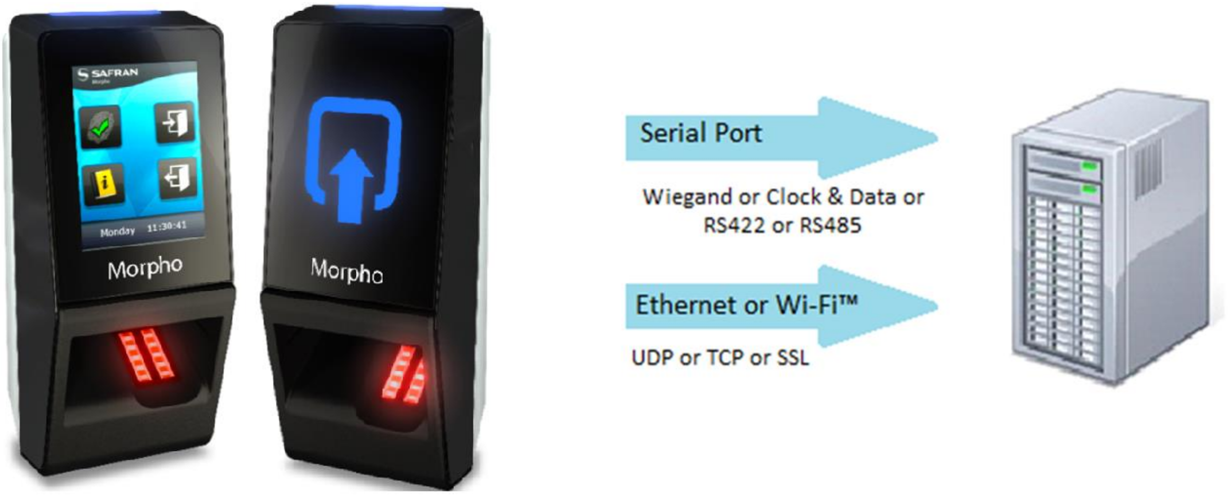


Figure 161: Sending access control result message to a distant system

Ports and protocols

The MorphoAccess® SIGMA Lite Series terminal is able to send the access control result messages to a distant system, using the following ports and protocols:

Serial Port : Wiegand or Clock & Data or RS485 or RS422,

Ethernet or Wi-Fi™ link: UDP or TCP or SSL.

This is detailed in the next sections.

Please refer to **MorphoAccess® terminals Remote Messages Specification** for more information about the format and the protocol of the access control result messages.

Serial Port (Output only)

Protocol selection

MorphoAccess® SIGMA Lite Series terminal has two serial ports:

One for Wiegand or Clock & Data protocols

One port for RS485 or RS422 protocols

Wiegand protocol

The Wiegand frame includes only the User Identifier (which must be a numeric value).

By default, the message is sent only when the local access control result is positive (access authorized). But this message can also be sent when the result is negative (access denied). In this case, the User Identifier is replaced by an error code indicating the reason for access denial.

The activation and format of the outgoing Wiegand frame can be configured by the user through Webserver. Refer to *Wiegand Parameters Settings* under Webserver.

An administrator can also configure using below parameter:

Parameter name	Value	Description
wiegand.external_port_output_type	0 or 1	This parameter allows an administrator to set an external port output type. Below are parameter values that can be selected: If an administrator set "0", it indicates external port type is Wiegand.

Clock & Data protocol

The description provided for Wiegand protocol (see previous section) applies also to Clock & Data protocol.

The sending of the message is conditioned to only one configuration key:

Parameter name	Value	Description
wiegand.external_port_output_type	0 or 1	This parameter allows an administrator to set an external port output type. Below are parameter values that can be selected: If an administrator set "1", it indicates external port type is clock & data.

RS485 protocol

The message is sent whatever the control result is, and it contains more information than the Wiegand and the Clock & Data frames:

date and time,

User Identifier (if available),

result from the local access right (authorized, denied, reason for deny).

The sending of the message is conditioned to the following configuration keys:

Parameter name	Value	Description
remote_msg_conf.send_serial_state	0 or 1	Using this parameter, an administrator can select remote message sending state over Serial channel. Select parameter value as "0", to disable message sending on serial port. Select parameter value as "1", to enable message sending on serial port.

Ethernet port

Protocol selection

The protocol used to send the message through the Ethernet link, must be only one of these protocols: UDP or TCP or TLS/SSL.

MorphoAccess® SIGMA Lite Series terminal is able to send message to two different distant systems: one preferred (host # 1) and one alternate (host #2).

Parameter name	Value	Description
remote_msg_ip_conf.host_1_protocol or remote_msg_ip_conf.host_2_protocol	0, 1 or 2	Using this parameter, an administrator can set a protocol type that will be used for communicating with remote controller host 1. Below are the values: Set "0", for using TCP protocol for communication Set "1", for using UDP protocol for communication Set "2", for using TLS/SSL over TCP for communication

For details on more parameters for sending remote message to access controller, refer to MorphoAccess SIGMA and SIGMA Lite Series Parameters Guide.

Wi-Fi™ Channel

Instead of Ethernet connection, the terminal can be connected using a wireless Wi-Fi™ b/g connection. Please refer to *Wi-Fi™ Configuration*

section for more information.

The message format and the protocols supported are the same as the Ethernet channel: UDP, or TCP or SSL.

WARNING: It is not possible for a terminal to be connected through Ethernet and through Wi-Fi™ at the same time.

Note about Terminal Clock Deviation

The message sent through IP and RS485 protocols includes the date/time of access control result.

The terminal clock has a +/- 4 sec per day typical time deviation at +25°C.

At 50°C, the time deviation may be up to -8 sec per day.

For features requiring time precision (such as SSL protocol or DESFire® contactless card), the internal clock/calendar of the MorphoAccess® SIGMA Lite Series terminal must be synchronized regularly with an external terminal (using the appropriated ILV command).

Section 14 : Terminal User Interface

Man Machine Interface

Audible signal

The volume of the audible signal can be tuned by a specific configuration key:

Parameter name	Value	Description
audio.volume	0 to 100	Using this parameter, an administrator can set global audio volume that will be played on specific events. (default value is 50)

Terminal States

Identification, Authentication or Multi-factor mode: waiting for a finger or a card

In identification mode, the terminal is waiting for a finger to be placed on the biometric sensor.

In Authentication mode, the terminal is waiting for a user's card close to the embedded contactless smartcard reader.

In multi-factor mode, the identification mode and one of the authentication modes are activated. Then the terminal is expecting a finger on the biometric sensor or a card close to the smartcard reader.

Authentication mode, after presentation of a card, waiting for a finger or biometric data acquisition of the finger is in progress

After reading a user's card, the terminal emits this signal while waiting for a finger or when the acquisition of the biometric data of the finger placed on the sensor is in process. Do not remove the finger while this signal is emitted.

Identification: Finger detected, Acquisition of biometric data of the finger is in process

After detection of a finger on the biometric sensor, the terminal emits this signal during the whole biometric data acquisition (of the finger on the sensor) process. Do not remove the finger while this signal is emitted.

Identification or Authentication: database blank or absent

This signal is emitted when the activated mode requires a database (identification mode, or authentication mode with biometric data in the database) and it isn't created or is empty.

Proxy mode - waiting for distant system command

When the proxy mode is enabled and when the terminal is expecting for a command from the distant system, there is no local signal.

Incorrect finger position

The terminal emits this signal when the position of the finger on the biometric sensor is not good enough. Remove the finger from the biometric sensor and follow the recommendations detailed in "*Finger Placement Recommendation*" section.

Biometric Sensor start up error

The terminal fails to start the biometric sensor. If the trouble persists after several terminal start-ups, please contact our customer service.

Maintenance: terminal configuration in process

This signal indicates that a configuration operation is in process, whether by TCP or by USB mass storage key. The current operation can be one of the following: management of the biometric database, modification of a configuration key, management of the log file, etc.

In this state, the terminal ignores all access requests by users.

Maintenance: USB mass storage key can be removed

This signal is emitted when the USB Mass Storage key, used to configure the terminal, can be removed from the USB port. The USB Mass Storage key must be removed to complete the maintenance process.

Maintenance: Biometric Sensor firmware update

This signal is emitted when the biometric Sensor firmware update is in progress or whenever the terminal boots up. This update occurs at first startup of the terminal after terminal firmware update or during every terminal reboot.

Change Key OK

This signal is emitted when the Card is encoded and it is detected as an Admin Card and the corresponding keys on the card are written correctly.

Change Key Not OK

This signal is emitted when the Card is encoded and it is detected as an Admin Card. However, the corresponding keys on the card are incorrectly written.

Anti-tamper alarm

This signal is optionally emitted when the terminal has detected opening of the terminal (except lateral USB port cover), or separation from the wall support.

Access Emergency

This signal is optionally emitted when the terminal has detected opening of the door forcefully of door not closed properly.

Time Override Mode

This signal is emitted when the Time Override is enabled. The buzzer beeps only during the beginning on the last 1 minute of TOM and plays continuously during the last 30 seconds.

Access Request Result

Identification or Authentication - Access granted

The user is recognized and the access is allowed.

Identification or Authentication - Access denied

The user is not recognized, or some data is missing, or the access is not allowed to this user (by Time Mask feature or by the Central Access Controller).

Authentication - Timeout while waiting for finger on the sensor

Time-out occurs during the wait for a finger/PIN on the sensor.

Finger removed too early

The terminal emits this signal when the finger is removed before the end of biometric data acquisition (while the finger biometric data acquisition is still in progress).

Enrolment

Waiting for a finger

The enrolment sequence is launched and the terminal is waiting for a user to place a finger on the biometric sensor.

Acquisition in process

The user has placed a finger on the biometric sensor and is awaiting completion of the acquisition process (notified by the Acquisition complete event).

Current positioning - Acquisition complete (but not enrolment sequence)

The current acquisition is complete and the user may remove their finger from the terminal.

Current capture complete – Remove finger from terminal to proceed with next finger

The current capture is complete and the user is invited to remove the finger from the terminal. The next capture will not start until the finger has been removed from the terminal.

Current finger – Acquisition complete (but not enrolment sequence)

The current finger acquisition has completed with success and the user has just removed their finger from the terminal. If acquisition of another finger is required, the terminal will emit the Waiting for finger signal.

Enrolment complete

The enrolment sequence has completed successfully. Depending on how long the biometric data registration process has taken, the terminal may emit the signal Enrolment complete – Registration of biometric data in process.

Enrolment complete – Registration of biometric data in process

The enrolment sequence is complete and registration of biometric data is in process. When a user is enrolled and only Finger Biometric Trigger is enabled.

Enrolment Error

The enrolment sequence has not completed successfully. Depending on how long the biometric data registration process has taken, the terminal may emit the signal Enrolment Failed.

LED – Buzzer Sequence

Below table describes LED and Buzzer sequence for different action of MorphoAccess® SIGMA Lite Series.

Action	LED						Buzzer
	🔴	🟢	🔵	🟡	🟣	●	
	Red	Green	Blue	Yellow	Purple	Cyan	
Default MMI when Database is Empty and only Biometric Trigger is Enabled				√			
Default MMI when Database is Empty and Trigger is not Biometric			√				
Default MMI when Database is not empty and only Biometric Trigger is Enabled							
Default MMI when limited to 3,000 user records not empty and Trigger is not Biometric			√				
Distant Session is Open					√		
Distant Command Cancelled	√						
USB Key Detected							√
USB Script In Progress					√		
USB Script Successful		√					√
USB Script Error	√						√
First Boot up	√	√	√	√	√	√	
Change Key OK		√					√
Change Key Not OK	√						√
Alarm (15 times)	√						√
Access Emergency	√						√
TOM		√					√
Access Granted		√					√
Access Denied	√						√
Access Timeout	√						√
Place Finger				√			
Change Finger		√					
End of Acquisition							√
Enrolment Complete		√					√
Enrolment Failed	√						√
Missing Data from Card	√						√

Screens Displayed

This section indicate various Actions (Applicable on MorphoAccess® SIGMA Lite+ Series terminals only).

Terminal Home Screen

During the power up, the Morpho Logo and boot up animation will be displayed. Once product booted, the LCD will display wallpaper (can be logo of company e.g. Morpho logo by default).

Idle screen will display wallpaper, date and time with different icons.

There will be four icons.

- Information icon – To shows basic information about terminal.
- Authentication icon – To initiate authentication from touch screen.
- T & A icons - If Time & Attendance feature is enabled on the terminal then two icons (IN and OUT) for T & A shall be displayed.

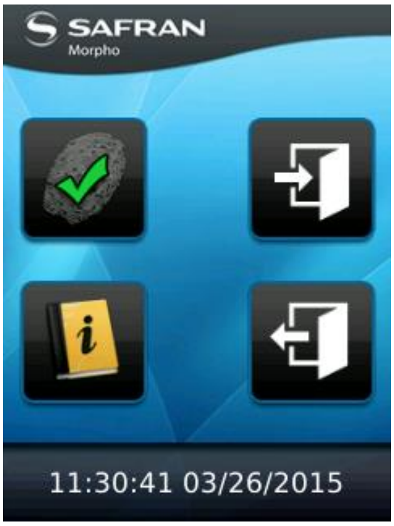


Figure 162: Terminal Home Screen

Terminal Information Menu

When Information button "i" is pressed for entering in Menu, below screen is displayed.

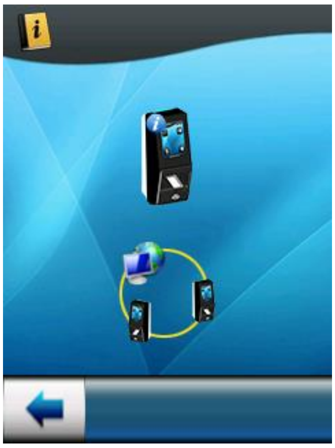
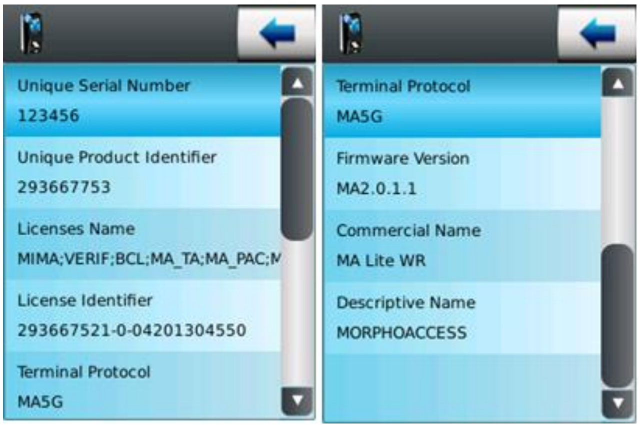


Figure 163: Information Menu

Terminal Details



Unique Serial Number
123456

Unique Product Identifier
293667753

Licenses Name
MIMA;VERIF;BCL;MA_TA;MA_PAC;M

License Identifier
293667521-0-04201304550

Terminal Protocol
MA5G

Terminal Protocol
MA5G

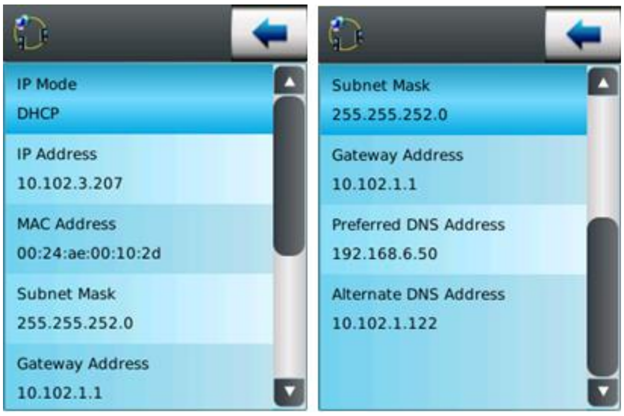
Firmware Version
MA2.0.1.1

Commercial Name
MA Lite WR

Descriptive Name
MORPHOACCESS

Figure 164: Terminal Details

Communication Details



IP Mode
DHCP

IP Address
10.102.3.207

MAC Address
00:24:ae:00:10:2d

Subnet Mask
255.255.252.0

Gateway Address
10.102.1.1

Subnet Mask
255.255.252.0

Gateway Address
10.102.1.1

Preferred DNS Address
192.168.6.50

Alternate DNS Address
10.102.1.122

Figure 165: Communication Details

Keypad Authentication

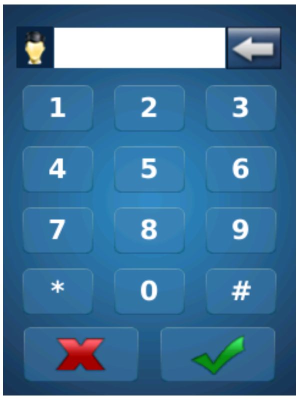


Figure 166: Keypad Authentication

Keypad Authentication for second user (In case of Multi User Mode)

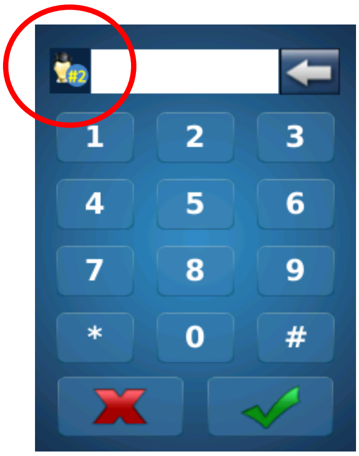
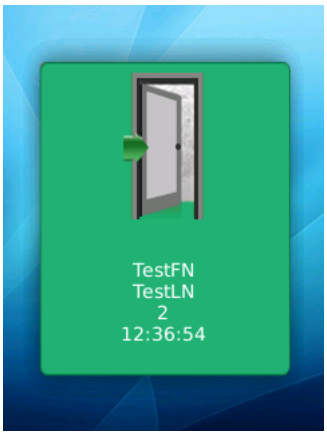


Figure 167: Keypad Authentication for Second User

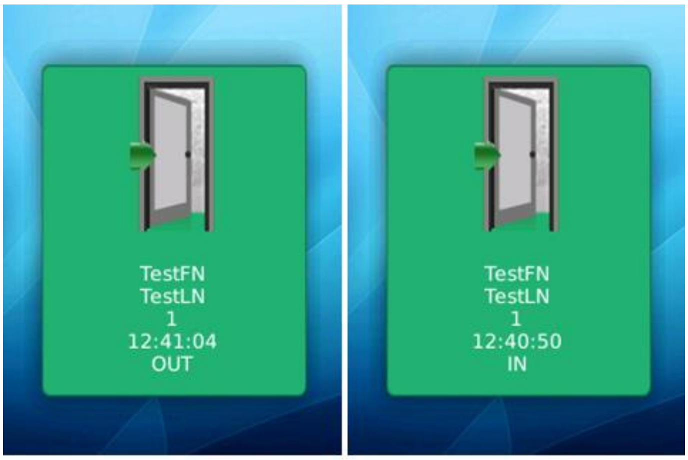
Access Granted



TestFN
TestLN
2
12:36:54

Figure 168: Access Granted

Access Granted (with F-Key)



TestFN
TestLN
1
12:41:04
OUT

TestFN
TestLN
1
12:40:50
IN

Figure 169: Access Granted with F-Key

Access Denied

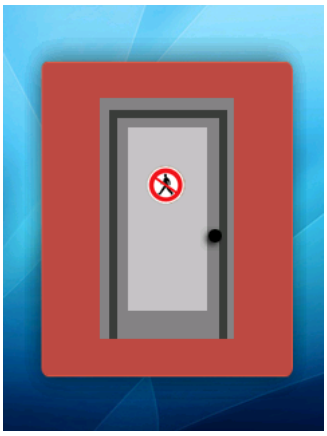


Figure 170: Access Denied

USB Information

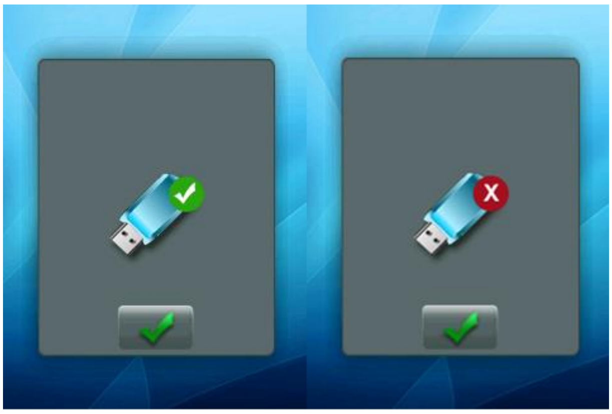


Figure 171: USB Connected/Not Detected

Live Finger Feedback with Animation

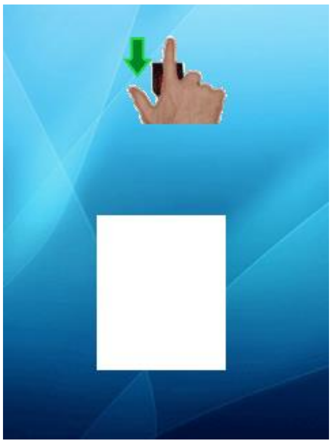


Figure 172: Live Fingerprint Feedback

Pin Entry Request

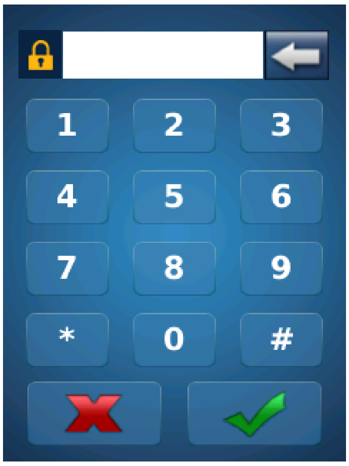


Figure 173: PIN Prompt

BIOPIN Entry Request

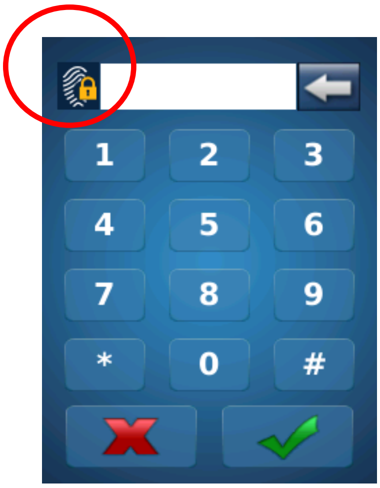


Figure 174: BIOPIN Prompt

Bootup Animation Screen

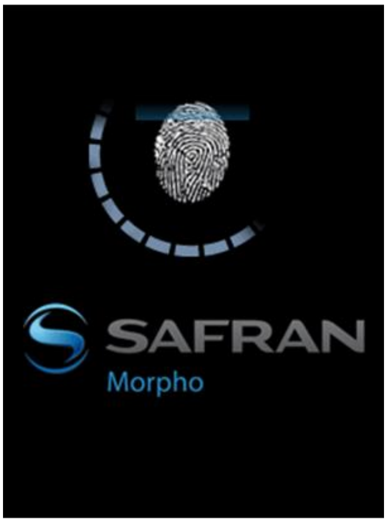


Figure 175: Bootup Screen

Please Wait…Action in Progress

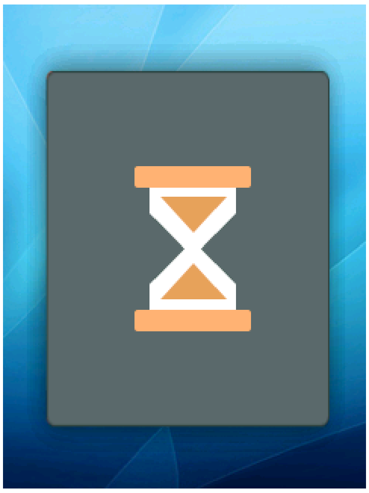


Figure 176: Configuration in Progress

Tamper Detected

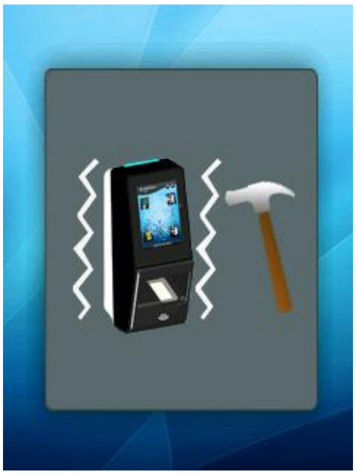


Figure 177: Tamper Detected

Distant Session Is Opened

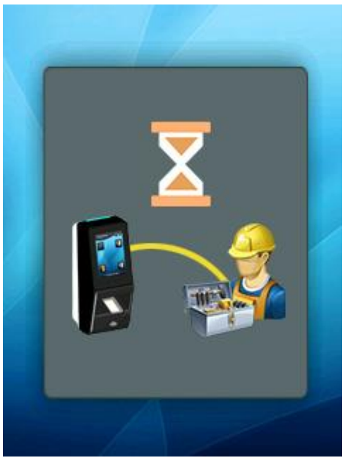


Figure 178: Distant Session Open

Controller Feedback

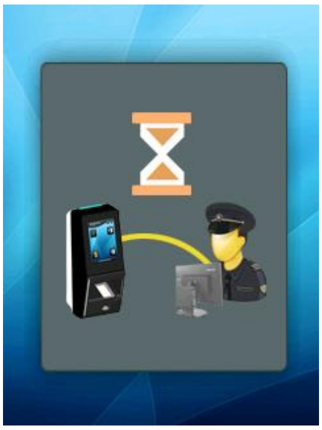


Figure 179: Waiting for Controller Feedback

Animation with Door Open

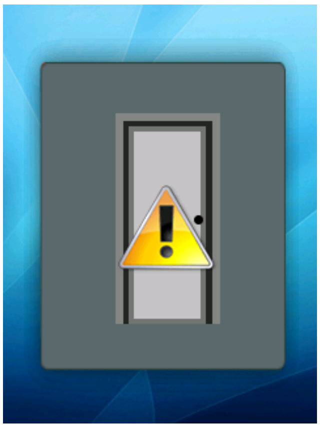


Figure 180: Force Door Open/Door Held Open

Configuration Failed for Device

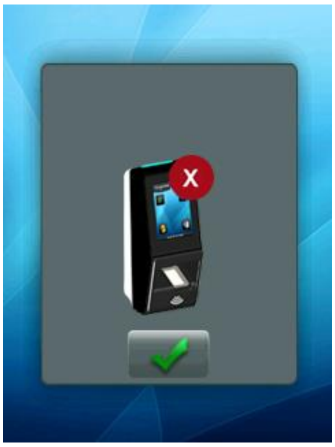


Figure 181: Configuration Failed for Device

Configuration Failed for Communication

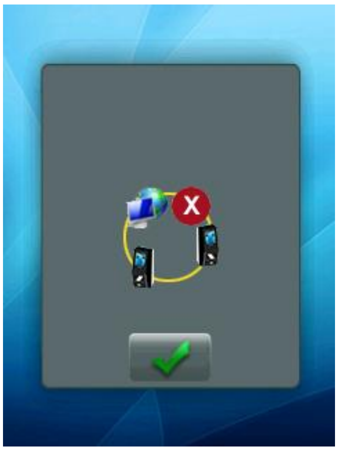


Figure 182: Configuration Failed for Communication

Place Card

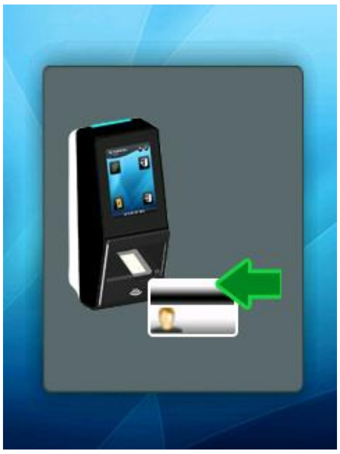


Figure 183: Place Card

Remove Card

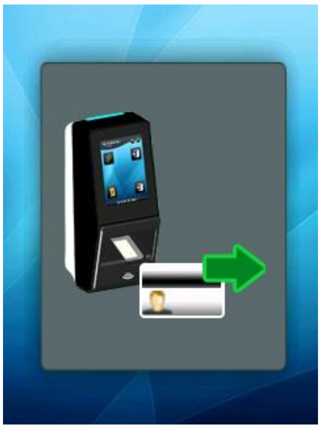


Figure 184: Remove Card

Prompt for second attempt

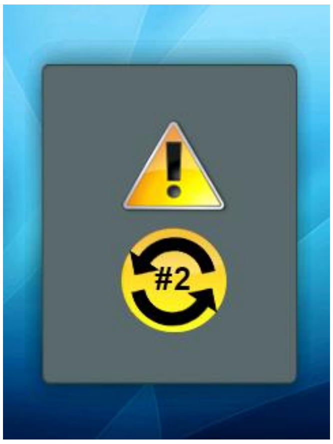


Figure 185: First Attempt Failed, Second Attempt

Admin Card Detected

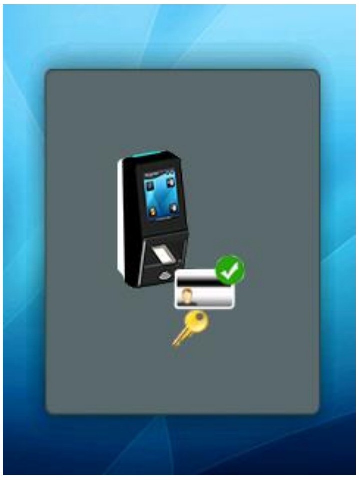


Figure 186: Admin Card Detected

Firmware Upgrade Started

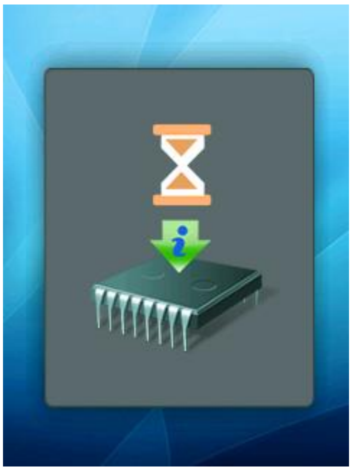


Figure 187: Firmware Upgrade Started

Remove Finger

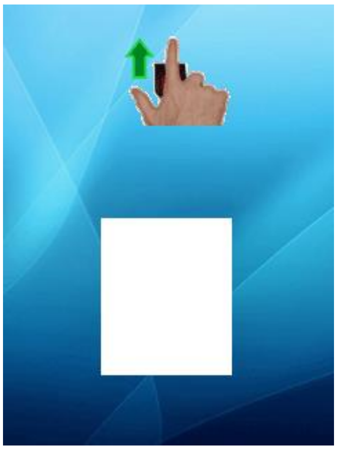


Figure 188: Remove Finger

Invalid Input

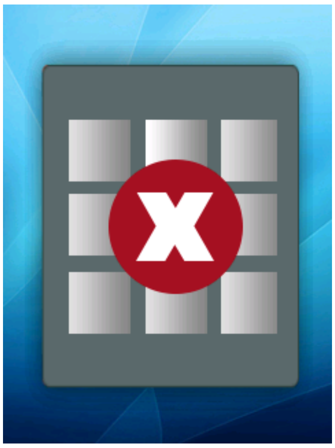
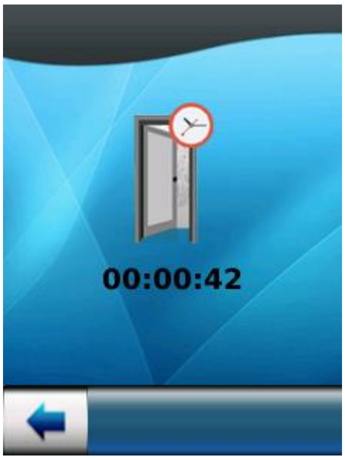


Figure 189: Invalid Input

Time Override Mode – Active



00:00:42

Figure 190: TOM Active

Sensor DB Upgrade

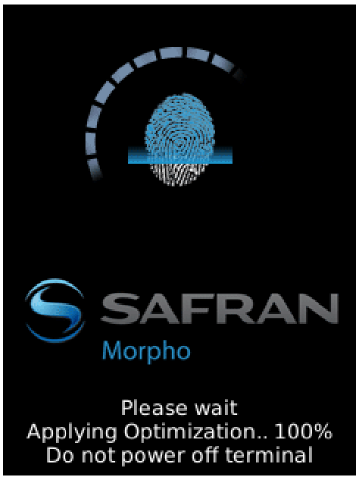

Please wait
Applying Optimization.. 100%
Do not power off terminal

Figure 191: Sensor DB Upgrade

Terminal Blocked

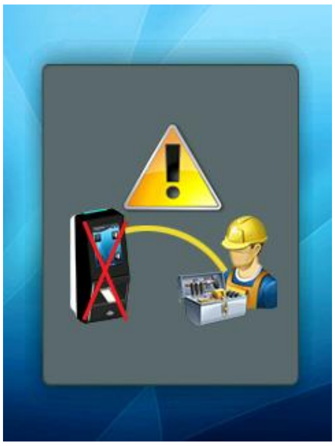


Figure 192: Terminal Blocked

Section 15 : **Compatibility Accessories, Software Licenses and Software Applications**

Compatible Accessories & Software Licenses

The following items can be ordered directly to Morpho or to an official distributor, so as to enjoy all the features of an administrator MorphoAccess® SIGMA Lite Series terminal:

Power supply units,

Contactless smartcards: MIFARE® 4K; DESFire® 2K, 4K or 8K, HID iCLASS®, Prox®,

User database size licenses (MA_10K_USERS): enabling database size upgrade from 3,000 to 10,000 users' capacity (2 or 3 fingers per record) at creation of the database,

Log size licenses (MA_1M_LOGS): enabling logs size upgrade from 100,000 to 1,000,000.

Compatible software applications

MorphoAccess® SIGMA Lite Series terminals are fully compatible with:

The low level protocol using thrift commands, for more information refer to MorphoAccess 5G Series - Host System Interface document.

Morpho Integrator's Kit (MIK) software development kit (version 6.1 or later).

Using Legacy Morpho mode, MorphoAccess® SIGMA Lite Series is also compatible with:

MEMS,

MIK 5 or later.

With the following limitations:

Refer to MorphoAccess SIGMA and Lite Series - Morpho Legacy Mode limitations document

Using Legacy L1 mode, MorphoAccess® SIGMA Lite Series is also compatible with:

SecureAdmin^{TM}(version v4.1.20.0.1.0.0 or later).

With the following limitations:

Refer to MorphoAccess® SIGMA and Lite Series - L1 Legacy Mode limitation document

Section 16 : **Recommendations**

Warning

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

General precautions

Do not attempt to repair the MorphoAccess® SIGMA Lite 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 an administrator warranty.

Do not expose the terminal to extreme temperature

Only use the terminal with its original accessories. Attempts to use unapproved accessories with an administrator terminal will void an administrator warranty.

Due to electrostatic discharge, and depending on the environment, synthetic carpeting should be avoided in areas where the MorphoAccess® SIGMA Lite Series terminal has been installed.

Areas containing combustibles

It is strongly recommended that you do not install your MorphoAccess® SIGMA Lite Series terminal in the vicinity of gas stations, petroleum processing facilities or any other facility containing flammable or combustible gases or materials.

Specific precautions for terminals fitted with a contactless smartcard reader

It is recommended to install MorphoAccess® SIGMA Lite Series terminals equipped with a contactless smartcard reader at a certain distance (> 30cm) from metallic elements such as iron fixations or lift gates. Performances in terms of contactless badge reading distance will decrease when metallic elements are closer.

Ethernet connection

It is recommended to use a category 5 shielding cable (120 Ohms). It is also strongly recommended to insert a repeater unit every 90m.

Extreme care must be taken while connecting Ethernet wire to the MorphoAccess® SIGMA Lite Series terminal block board since low quality connection may strongly impact Ethernet signal sensibility.

It is recommended to connect Rx+ and Rx- with the same twisted-pair wire (and to do the same with Tx+/Tx- and the other twisted-pair wire).

Date / Time synchronization

If you want to use the MorphoAccess® SIGMA Lite Series terminal for application requiring high time precision, we recommend synchronizing regularly your MorphoAccess® SIGMA Lite Series terminal time with an external clock.

The MorphoAccess® SIGMA Lite Series terminal clock has a +/-10 ppm typical time deviation at +25°C (roughly less than +/- 1 sec per day).

Cleaning precautions

A dry cloth should be used to clean the terminal, especially the biometric sensor.

The use of acid liquids, alcohol or abrasive materials is prohibited.

Annex 1 : **Finger Placement Recommendation**

Most Useful Areas for Biometric Data

The terminal is designed to capture the area containing the most useful biometric data. In fingerprints, this is usually at the center of the first phalanx.

This is illustrated in the figure below:

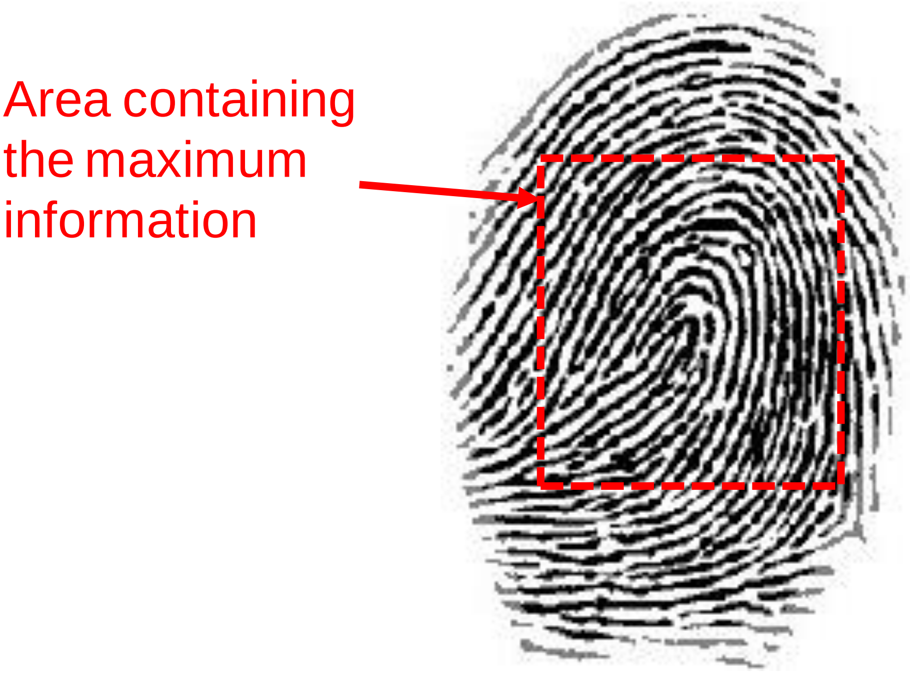


Figure 193: Most Relevant Biometric Data in a Fingerprint

The sensor is designed so that when the fingertip is in contact with the rounded hollow guide, the central zone of the first phalanx is aligned with that of the section dedicated to fingerprint capture.

Position of Finger

Finger Height

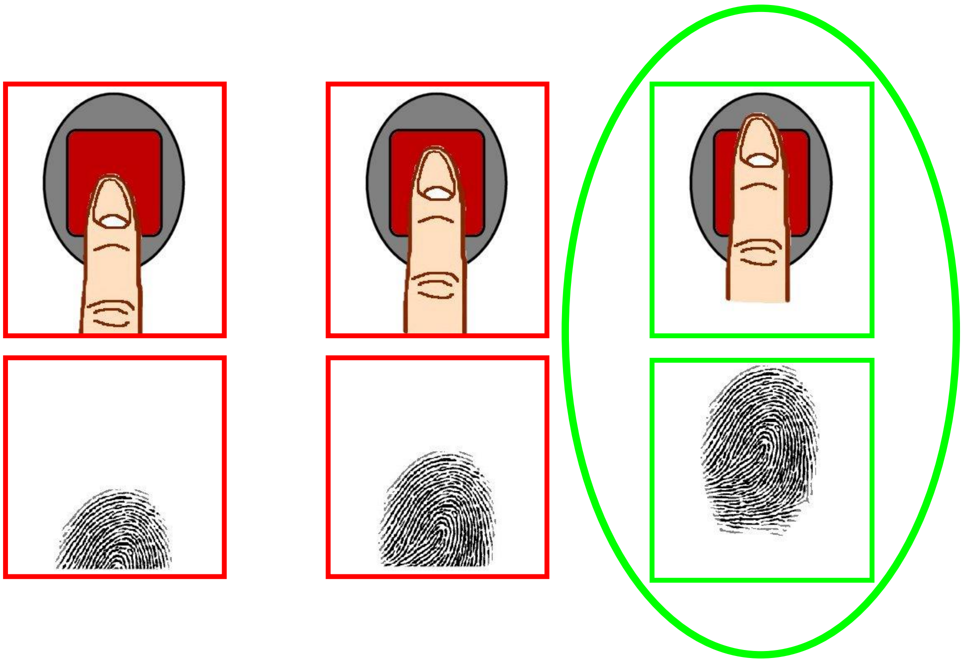


Figure 194: Finger Height

Incorrect Position:

Do not place the finger tip on the top of the fingertip guide.

Do not place the finger tip on the surface of the sensor

Correct Position:

Align center of 1st phalanx with sensor center

Finger Angle

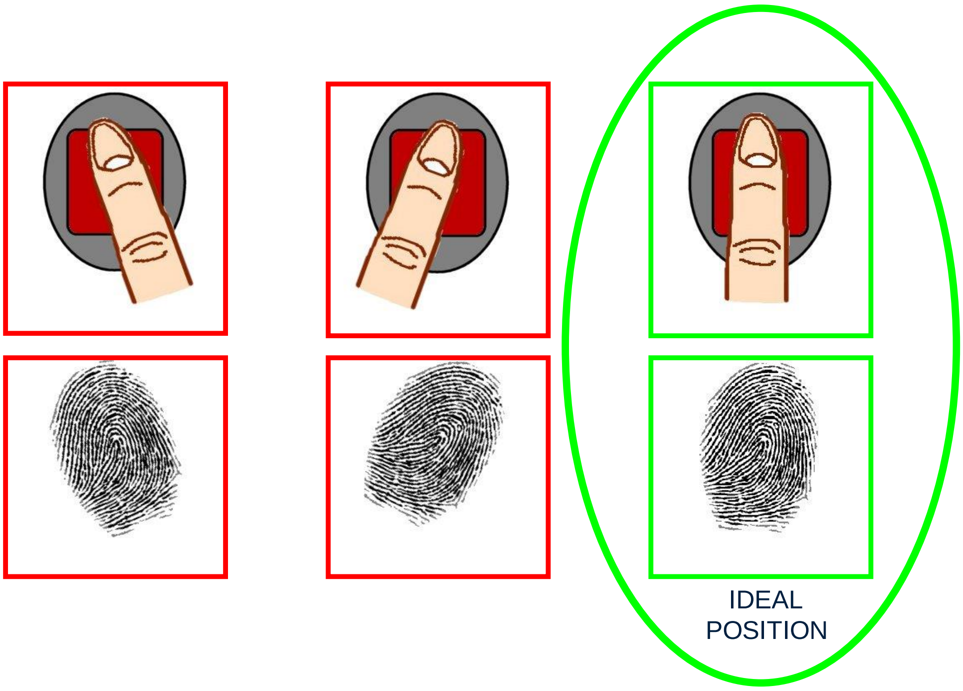


Figure 195: Finger Angle

Incorrect Position:

Do not tilt the finger on right or left side of the sensor

Correct Position:

The finger must be parallel to sensor sides

Finger Inclination

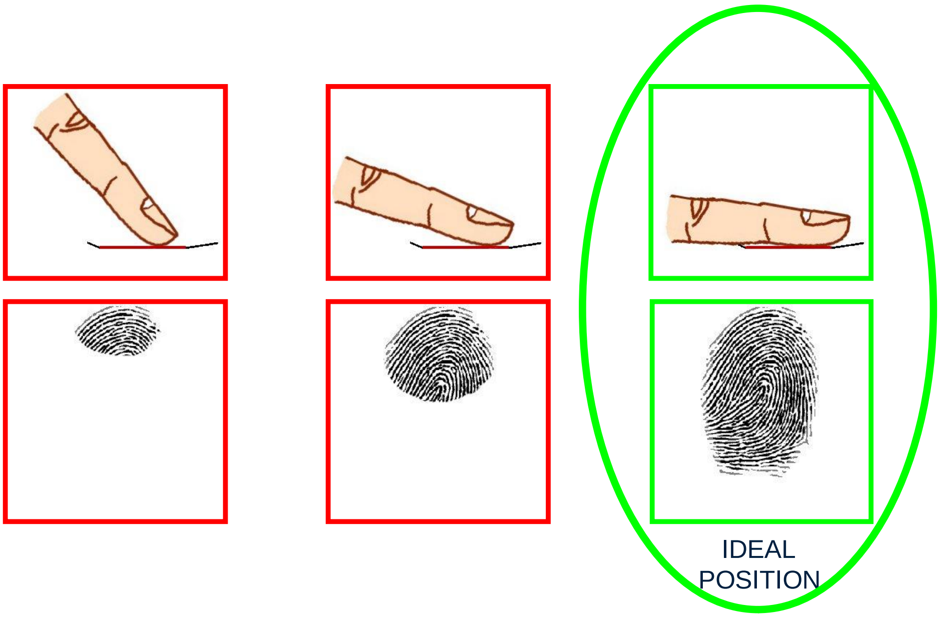


Figure 196: Finger Inclination

Incorrect Position:

Do not leave the finger in the air

Do not bend finger upward or downward

Correct Position:

Finger must be parallel to the sensor surface

Finger rotation

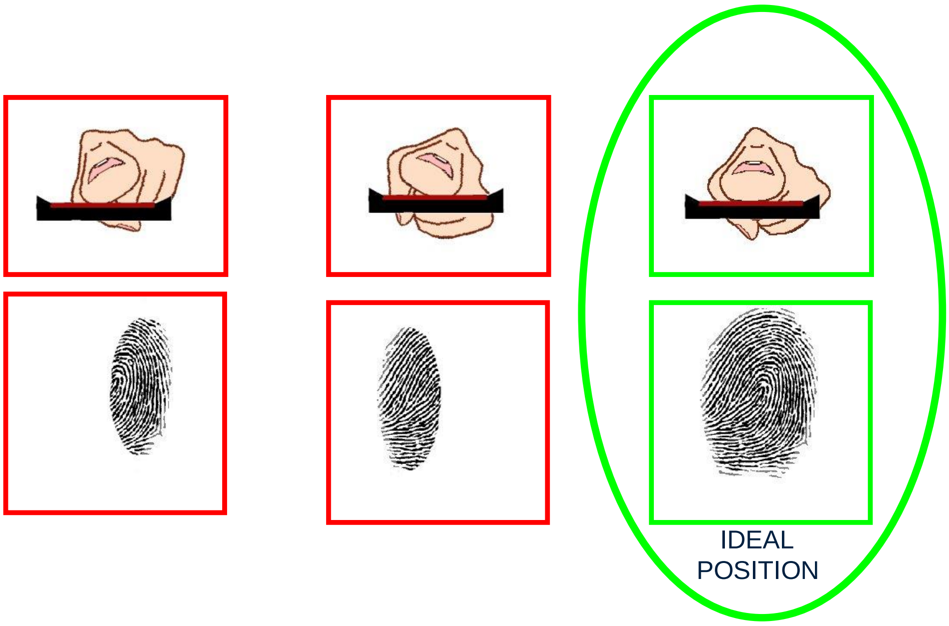


Figure 197: Finger Rotation

Incorrect Position:

Do not roll finger

Correct Position:

Finger must be parallel to the sensor surface

Finger Condition

When finger biometric data acquisition is difficult, please follow the recommendations listed below:

The finger is cold

Solution : warm up the finger

The finger is wet

Solution : wipe the finger

The finger is dry

Solution : warm up the finger and/or add a little bit of humidity

The finger is dirty

Solution: wash hands

Remove bandages or adhesive tapes from the fingerprint area.

Do not press or tense finger to avoid blood vessels constriction.

Annex 2 : **Comparison of Authentication mode with Contactless Card**

Contactless Modes Table

Operation	Actions Performed by Terminal
Authentication with biometric templates in database	Read ID on contactless card. Retrieve corresponding templates in database. Biometric authentication using these templates. Send ID if authentication is successful.
Authentication with biometric templates on card	Read ID and templates on contactless card. Biometric authentication using these templates. Send ID if authentication is successful.
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 successful.
Authentication with biometric templates in database – biometric control disabled	Read ID on contactless card. Check corresponding templates presence in database. Send ID if templates are present.
Authentication with biometric templates on card – biometric control disabled	Read ID on contactless card. Send ID.
Card mode authentication – biometric control disabled	Read card mode, ID, templates (if required by card mode) on contactless card. Whatever card mode, send ID.

Required Tags on Contactless Card

Operation	ID	CARD MODE	Template 1	Template 2	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) – no PIN code check, no biometric check	Yes	Yes	No	No	No	No
Card mode authentication (PKS) – no PIN code check, with biometric check	Yes	Yes	Yes	Yes	No	No
Authentication by BIOPIN code check only	Yes	No	No	No	No	Yes
Authentication by PIN code check only	Yes	No	No	No	Yes	No

With:

- ID_ONLY : no PIN code check, no biometric check,
- PKS : no PIN code check, with biometric check.

Annex 3 : **Bibliography**

How to get latest version of the documents

The last version of the documents is available on a CD/ROM package from our factory, or can be downloaded from our web site at the address below:

www.biometric-terminals.com

(Login and password required).

To request a login, please send us an email to the address below:

hotline.biometrics@morpho.com

Documents concerning the MorphoAccess® terminal

Document about installing the terminal

MorphoAccess® SIGMA Lite Series Installation Guide,

ref. 2015_2000007248 - MA SIGMA Lite - Installation Guide

This document describes terminal physical mounting procedure, electrical interfaces and connection procedures. This document is in English.

Documents about administrating/using the terminal

MorphoAccess® SIGMA Lite Series Administration Guide,

ref. 2015_2000010196 - MorphoAccess® SIGMA Lite Series Administration Guide

This document describes the different functions available on the terminal and procedures for configuring the terminal. This document is in English.

MorphoAccess® SIGMA Lite Series – Morpho Legacy Mode Limitations,

ref. 2015_2000012402 - MorphoAccess® SIGMA and Lite Series - Morpho Legacy Mode limitations

This document describes the limitations of MorphoAccess® SIGMA Lite Series terminal operating in Legacy Morpho mode. This document is in English.

MorphoAccess® SIGMA Lite Series – Morpho L-1 Bioscrypt Legacy Mode Limitations,

ref. 2015_2000012403 - MorphoAccess® SIGMA and Lite Series - L1 Legacy Mode limitations

This document describes the limitations of MorphoAccess® SIGMA Lite Series terminal operating in L-1 Bioscrypt Legacy mode. This document is in English.

MorphoAccess® SIGMA Lite Series Quick User Guide,

ref. 2015_2000005700 - MA SIGMA Lite - Quick User Guide

This document is a short summarized guide that is used for learning the basic steps for initializing the terminal operations. This document is in English.

Documents for Developer

MorphoAccess® SIGMA Lite Series Parameters Guide,

ref. 2015_2000010197 - MorphoAccess SIGMA and SIGMA Lite Series Parameters Guide

This document contains the full description of all the configuration parameters for the terminal. This document is in English.

MorphoAccess® SIGMA Lite Series Host System Interface Specifications,

ref. 2015_2000012335 - MorphoAccess 5G Series - Host System Interface

This document describes all the commands supported by a MorphoAccess® SIGMA Lite Series terminal.

MA5G_distant_commands,

ref. 2015_2000012323 - MA-SIGMA-Lite_FW_Distant commands Guide

This document describes thrift commands supported by a MorphoAccess® SIGMA Lite Series terminal.

MorphoAccess® terminal Serial Command Manual

ref. 2015_2000012655 - MA-LITE-SW_SecureSDK_Serial_Command_Manual

This document details all the distant commands supported by MorphoAccess® 4G terminals and MorphoAccess® SIGMA Lite Series terminals in L1 legacy mode.

MorphoAccess® terminal Command Support Matrix

ref. 2015_2000012654 - MA-LITE-SW_SecureSDK_Command_Support_Matrix

This document has command support matrix for all MorphoAccess® 4G terminals and MorphoAccess® SIGMA Lite Series terminals in L1 legacy mode.

MorphoAccess® SIGMA Lite Series Contactless Card Specifications,

ref. 2014_0000001408 - MA SIGMA - Contactless Cards Specification

This document describes the contactless cards supported by a MorphoAccess® SIGMA Lite Series terminal. It also describes the format of the data on the contactless card.

MorphoAccess® SIGMA Lite Series Remote Messages Specification,

ref. SSE-0000101111-02 - MA SIGMA - Remote Message Specification

This document describes the protocols, and the format of the data, supported by a MorphoAccess® SIGMA Lite Series terminal.

Configurations tools user's guide

MorphoAccess® SIGMA Lite Series Terminal License Management

ref. SSE- 0000072605-01 - License Management

This document explains how to use the License manager application. This tool enables to read and to load software licenses in a MorphoAccess® SIGMA Lite Series terminal.

Release Note

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, etc.

Annex 4 : **Glossary, Acronyms and Abbreviation**

GLOSSARY

Access Controller/Controller: This term is used for centralized access controller. Terminal communicates with controller for granting or denying access to the user.

Terminal: This term is used for MorphoAccess® SIGMA Lite Series terminal

Device: This term is used for an external device attached to MorphoAccess® SIGMA Lite Series terminal, such as USB Mass Storage device.

Admin/Administrator: A user who is authorized to manage the settings and user information of a fingerprint reader. Administrators can enroll or delete users and change terminal settings.

Capacitive Sensor: A device that detects the voltage differences between the sensing surface and individual fingerprint ridges. MorphoAccess® SIGMA Lite Series terminal supports only Optical Sensor for better biometric performance.

Core: A term used to describe an area of the finger-scan characterized by ridgelines with the tightest curvature and most unique content. Although the entire finger-scan has significant data, the "core" is the most data-intensive area and thus is extremely important to the algorithm. Normally, the core is located in the middle of the fingerprint.

Duress Mode: A mode that offers users a way of indicating a duress situation (such as being forced to open a door). The user verifies with a specially designated finger resulting in an inverted Wiegand output that is detectable on certain Access Control Panels.

Finger Print Capture: The process of extracting features of a fingerprint image obtained from a fingerprint sensor, and saving them into the internal memory of a device. The fingerprint data is called a fingerprint template.

User Enrolment: creation of a record in a database with personal data of a unique user, or creation of a card with personal data of a user

Firmware: The set of programs contained permanently in a hardware device (as read-only memory) that controls the unit.

Host Mode: The normal mode of operation when the device is waiting for a card to be presented to the terminal.

Optical Sensor: A device that detects that detects the intensity or brightness of light. Morpho biometric sensors are used to create graphical representations of fingerprints.

Single Door Access Control (SDAC): The capability of controlling/monitoring all functions related to a single entry/exit point.

Software The set of programs associated with a computer system.

Template: A term used to describe the data that is stored during the enrolment process. The data is a mathematical representation of the ridge pattern of the enrolled finger scan.

Primary Template: This is the template that resides in the first template slot on the smart card. When verification is initiated, this primary template is the first template that is used in that verification process.

Secondary Template: This is an optional second template stored on the smart card that is also used in the verification process if the primary template verification fails.

Users: The individuals that use a hardware system.

User Groups: The sets of users grouped together in a system (usually by the similarity of the functions they perform).

1:1 Mode: In 1:1 mode, a user enters his or her User ID first. Then the user is requested to provide a personal data such as place a finger on a sensor or enter a PIN. Then the acquired data is matched against the reference data linked to user ID (example: fingerprint found on users' card which provides the User ID at beginning of the process).

1: N Mode: In 1: N mode, a user places his or her finger on the device without entering an ID. The terminal compares the user's scanned finger with the many enrolled fingers in its internal database.

Identification (Searching or 1:N): The operation of Identifying a user by comparing a live finger scan against all stored finger-scan records in a database to determine a match. Identification uses the finger scan only - no cards or PINs. Identification is only available on devices that are in 1:N mode.

Authentication (1:1): The operation of confirming a user is who he claims to be by comparing a live finger scan image against a stored fingerprint template. The result (pass or fail) that is returned is based on whether the score is above a pre-defined threshold value. Some type of credential (PIN, Prox card, smart card, etc.) is necessary to initiate the biometric verification.

Webserver: Webserver is a web-based application embedded in the MorphoAccess® SIGMA Lite Series terminal. Webserver enables the management of the settings of the terminal from any computer (desktop, laptop, tablet …) equipped with a compatible Internet browser and connected to the same network as the terminal.

SecureAdmin™: Client software for managing terminal configuration for MorphoAccess® SIGMA Lite Series terminal running in L-1 Bioscrypt Legacy mode

Acronyms and Abbreviations

AUX: Auxiliary

LCD: Liquid Crystal Display

LED: Light Emitting Diode

MAC (address): Media Access Control, a unique identifier assigned to network interfaces for communications on the physical network segment

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6 - IPv6 is intended to replace IPv4, which still carries the large majority of Internet traffic (2013).

DNS: Domain Name Server. It provides naming for all systems, computers, terminals in a network

DHCP: Dynamic Host Configuration Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

SSL: Secure Sockets Layer

VIP: Very Important Person. The users in the system can be enrolled under VIP list.

PIN: Personal Identification Number

BIOPIN: Biometric Personal Identification Number. The BIOPIN is used for authentication when biometric authentication is not required

F Key: Function Key

MA: MorphoAccess®, a generic name of the physical access control terminals by Morpho.

T&A: Time and Attendance Mode

MMI: Man Machine Interface

SDAC: Single Door Access Control

GPIO: General Purpose Input Output

Annex 5 : **Support**

Troubleshooting

Customer service

Morpho

SAV Terminaux Biométriques

Boulevard Lénine - BP428

76805 Saint Etienne du Rouvray

FRANCE

Phone: +33 2 35 64 53 52

Hotline

Morpho

Support Terminaux Biométriques

18, Chaussée Jules César

95520 Osny

FRANCE

hotline.biometrics@morpho.com

Phone: + 33 1 58 11 39 19

(9H00am to 6H00pm French Time, Monday to Friday)

http://www.biometric-terminals.com/

A login and password are required to access the full site content. If an administrator doesn't have one, please send us an email to the address above to request one.

Contact by email is preferred.

October 2015

SAFRAN
Morpho

Registered Office:

Morpho

11, boulevard Gallieni

92130 Issy-les-Moulineaux – France
www.morpho.com