Administration Guide

Access and Time Biometric Terminals

COPYRIGHT© 2016-2023 IDEMIA

Osny, France

WARNING

COPYRIGHT© 2016-2023 IDEMIA All rights reserved.

Information in this document is subject to change without notice and do not represent a commitment on the part of IDEMIA. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of IDEMIA.

This legend is applicable to all pages of this document.

This manual makes reference to names and products that are trademarks of their respective owners.

PROPRIETARY RIGHTS

This document contains information of a proprietary nature to IDEMIA 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 within document 2017_2000025464.

Version	Date	Description
01	April 2017	First version MorphoAccess® SIGMA Family Series Administration Guide Created from: 2014_0000002196_v11- MA SIGMA - Administration Guide 2015_2000010196_v8 - MorphoAccess® SIGMA Lite Series Administrator Guide
02	June 2017	OSDP support added Seos card support added Limited User Database added USB enable/disable feature added. Note about partionned usb key that should not be used Note about encoding card with only one finger that is not supported Note about encoded name and first name that are limited to 20 caracters Note about the behavior during second biometric attempt with SIGMA Lite Note about transaction logs that should be erase Replace alphanumeric PIN by numeric PIN in webserver
03	July 2017	New administrator profile for SIGMA Series: Limited database admin (refer to ***Section 5 : MorphoAccess® Terminal Administration Menu***) Update first boot-up for SIGMA LITE terminal in LED – Buzzer Sequence chapter
04	October 2017	Update regarding L1 Legacy mode support added in MorphoAccess® SIGMA Extreme terminal Add ***Plugging a USB Wi-Fi™ or 3G adapter*** paragraph in ***Section 2***
05	October 2017	1. Added description for sending Extended Id to Control Panel through a custom Wiegand format.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

		2. Added description for Cyrillic keyboard support 3. Added description for support of new font .
06	January 2018	Update company name (IDEMIA)
07	July 2018	Update Morpho*Wave*® Compact
08	August 2018	1. Update figure: “Events Monitoring Configuration” with the new events list 2. Update chapter: “List of contactless cards validated” 3. Update chapter: “OSDP Protocol support” 4. Delete chapter: “ Protocol configuration“. The mode change is done via a firmware upgrade instead of a terminal protocol configuration. 5. Update chapter: “ Terminal Firmware Upgrade ” 6. Update chapter: “Information Menu” section “View Firmware Upgrade” 7. Upgrade chapter: “Access Schedule” 8. Upgrade chapter: “Access Request Result Log File” 9. Add “Job Code” Control 10.
09	August 2018	Update Matching strategy products supported table for MorphoWave® Compact
10	September 2018	Update Webserver capability of MorphoWave® Compact
11	January 2019	1. Add “Touch Sound” configuration (section 5) 2. Update chapter : “Dynamic Message”. This feature is available for « Access Granted » & « Access Denied » messages (section 5) 3. Add “Expiry date” configuration (Infinite or Limited duration) (sections 5 & 8) 4. Add “Card Data Encryption” configuration (sections 5 & 8) 5. Add a NOTE about the display duration of a “access control result” message (section 10) 6. Remove all NOTEs about the no support of Mifare Plus. 7. Remove all NOTEs about the unavailability of Access schedules features with 96 quarter hours and “Identified Mode” log format on Morpho*Wave*® Compact terminals
12	April 2019	1. “Hardware Factory Reset” support added (Section 5) 2. “User Access Schedule” Support added (Section 18) 3. Configuration of retrofit port (Section 3) 4. Updated MMI Dynamic message modes (Section 5) 5. Configuration of different threshold values for authentication and identification (Section 5)
13	June 2019	Added QR code capability for Morpho*Wave*® Compact

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

		Document OSDP unsecure commands supported In Enforced Security configuration
14	September 2019	Added User Access Schedule details in Schedule Configuration Section. Update chapter: “Image Settings” for customize Access/Granted logo and customize animations for trigger events. Update “Scope of the document” by removing outdoor reference Update “Templates supported”, adding recommandation Update “Connection methods” with POE+ for MWC Update “Plugging a USB Wi-Fi™ or 3G adapter” removing installation section Update “MorphoAccess® Terminal License Management” removing internal licenses Update “Encode Administrator card” remove limitation about iClass Update “Authentication process” update “List of contactless cards validated” Remove “Selection of user’s contactless card type (MIFARE® and/or DESFire®)” Update “Wiegand Parameters Settings”, remove reference to L& terminal and internal license Replace “Proxy Mode” by “Distant Commands Mode” Update “Sending Interfaces” add reference to “MA5G - Remote Message Specification”

The table below contains the history of changes made within document 2020_2000050320.

Version	Date	Description
01	June 2020	Add a new Access and Time Biometric Terminal : VisionPass terminal • Features not present in comparison with Morpho*Wave*® Compact - BIOPIN - Multi-User identification - Audio/VideoPhone feature - User Face enrolment via Webserver - Animations presence/change on Home screen - QR Code - OSDP BIOMATCH command - Eco-Mode (Disable Sensor in idle mode) • New Features in comparison with Morpho*Wave*® Compact - Time and Attendance per User (instead of optional T&A) - Video play in Home Screen BACKGROUND - Easy User Enrolment (LCD, MorphoManager) - User Guidance (None, MMI icons & Live Feedback) - Intentional mode (camera images management done continuously or on request)

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

02	September 2020	• Added details for Video file resolution for Morpho*Wave*® Compact and VisionPass terminal • Updated Card type compatibility
03	November 2020	• Added details for customized Animations and pictures to replace Access Granted and Denied message in MorphoAccess® SIGMA, SIGMA Extreme and Morpho*Wave*® Compact Terminal • Correction for Elite key configuration section • Add Seos and HID Mobile Credential keys configuration section • Add note about Morpho*Wave* Compact MDPI-M
04	December 2020	Correction to replace MorphoWave MDPI-M by VisionPass MDPI-M
05	February 2021	• Update support of MA_100K_USERS license for Morpho*Wave*® Compact • Update support of newly added template i.e face_v2 and face_v2_light_comp for Vision Pass
06	March 2021	• Add photo taking for VisionPass
07	March 2021	• Add support of VIP_40K_USERS license for VisionPass
08	July 2021	• Information for user capacity for Terminals without a license

09	October 2021	• Additions on OSDP section:
		  ○ Describe answer to OSDP capability request
		  ○ Describe use of OSDP ignore MMI functionality

10	January 2022	Add a new Access and Time Biometric Terminal : MorphoWave SP

11	March 2022	• Additions in the Security Administration section (14)
		  ○ Biometric Technology settings
		  ○ Recommendations for a secure installation
		• Update of User licenses
		• Update of IDEMIA web portal for Biometric Devices and Support Contact details

12	September 2022	• Add SEOS to supported Contactless card
		• Complete Transaction logs description
		• Modify HID configuration card procedure
		• Add the secure mode
		  ○ Add every warning about webserver not available
		  ○ Add multiple restriction due to secure mode
		• Complete information about OSDP_LSTATR management
		• Provide template data size

13	April 2023	• Available licenses Update • Complete osdp_BUSY answer description • Add OSDP icon
14	December 2023	• Available licenses Update • Add a new Access and Time Biometric Terminal : VisionPass SP
15	February 2024	• New formulation fore reset factory • Add description of the functionality PIN over OSDP • Add description of the functionality multiple fingerprint templates in OSDP_BIOMATCH command

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

16	July 2024	• Add license BT_DESFIRE_SEC • Describe OSDP command for user rejection event • Remove QR code limitation for MorphoWave SP
17	December 2024	• Add Sigma terminals support PIN over OSDP functionality • Add 20k users license to Sigma Lite • Add 50k users license to VisionPass SP • Add DESFire EV2 to Sigma series • Update date and time store management • Add recommendation and limitation for OSDP • Complete upgrade using Thrift commands • Add webserver default password section
18	August 2025	• Add notes to HID configuration card procedure • Add Mobile credential • Remove Wi-Fi • Introduce MorphoWave XP2 • Remove Webserver for MorphoWave XP2, MorphoWave SP and VisionPass SP • Add Fingerscan section • Replace Multi by MD for Sigma family • Update terminals table • Add SSCP section
19	February 2026	• Complete the Fingerscan section • Document the already matched use case in identification section • Add 100K users licence for VisionPass SP • Add SSCP Identify command • Complete SSCP Verify command • Support of OSDP v2.2.2

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Table of Contents

WARNING **2**
REVISION HISTORY **3**
TABLE OF CONTENTS **8**
SECTION 1 : INTRODUCTION **19**
Scope of the document ***20***
Product support notation: *21*
About Biometrics ***22***
About fingerprint biometrics *22*
Finger Templates supported *23*
About face biometrics *24*
Face Templates supported *24*
Templates size *25*
SECTION 2 : CONNECT THE TERMINAL TO A PC **26**
General ***27***
Why would one connect the terminal to a PC? *27*
Connection methods *27*
First connection *27*
Network parameter initialization *28*
Point to Point Ethernet Connection ***29***
Connection through only one Ethernet switch ***30***
Connection through a LAN ***31***
Description *31*
LAN with DNS Server *31*
LAN without DNS Server *32*
Static IP address (DHCP disabled) *32*
Dynamic IP address (DHCP enabled) *32*
SECTION 3 : TERMINAL CONFIGURATION AND ADMINISTRATION **33**
Understanding Terminal Configuration ***34***
Presentation *34*
Modifying the value of a parameter *34*
Backup of customized parameters *35*
Configuring a Networked terminal ***36***

Introduction *36*
Network factory settings *36*
Date/Time settings *37*
SSL Securing *37*
Network Wi-Fi™ configuration *38*
Terminal Database Management ***39***
General *39*
Adding a user to the database *39*
Removing a user from the database *39*
Database Size *39*
Terminal License Management ***41***
User licenses *41*
Communication licenses *41*
DESFire EV2 secure messaging license *42*
802.1x license *42*
SSCP license *42*
User data extraction license *42*
Getting a license for a Access and Time Biometric Terminal *42*
Checking licenses installed in the terminal with license manager application *43*
Installing a new license *45*
Terminal Firmware Upgrade ***46***
How to get latest version of firmware *46*
How to Open/Close the Retrofit port *46*
How to upgrade the firmware *46*
Firmware upgrade using a USB Mass Storage Key *46*
Firmware upgrade tool for expert users *46*
Terminal upgrade using Thrift commands *48*
SECTION 4 : TERMINAL FIRST BOOT ASSISTANT **49**
Assistant Initialization ***50***
Date & Time Configuration ***51***
Trigger Event ***55***
Language Configuration ***57***
Show/Hide Language Icon ***59***
Ethernet Interface Settings ***60***
Password Configuration ***64***
First Boot Assistance At Next Boot Configuration ***66***

Recover Corrupted Components ***68***
SECTION 5 : TERMINAL ADMINISTRATION MENU **70**
Access to Administration Menu ***71***
User Menu ***74***
User Enrollment in Database *75*
User Enrolment in Card *93*
User Enrolment in Card & Database *96*
Update User Information *98*
Authenticate User (SIGMA Ranges only) *101*
Delete User *102*
Card Manager *108*
Multimedia menu ***145***
Audio Settings *146*
Video Settings *149*
Images Settings *152*
System Menu ***156***
Terminal Settings *157*
Network Time Protocol Server (NTP Server) *161*
Transaction Log *180*
Miscellaneous Settings *185*
Touch Sound *189*
Web Server *190*
Error Log Settings *191*
Sensor Log Configuration *193*
Communication menu ***196***
Security recommendation *197*
Ethernet Network Configuration *197*
Wi-Fi™ Network Configuration *199*
Mobile Network Configuration *199*
Configure Hostname *203*
Serial Parameters *203*
Security Menu ***207***
User Control Settings *208*
Anti-Tamper Switch For Terminal Security *224*
Network & Communication Security Settings *228*

Multi User Settings *243*
Change the LCD Login Password *246*
Additional User Control Settings *248*
USB Menu ***254***
Enable or Disable USB port *255*
Initialize USB Mass Storage device *256*
Format USB Mass Storage device *258*
Import Data into Terminal *259*
How to Import User Database *261*
How to Import Contactless key *264*
How to Import Language *266*
Export Data in USB Mass Storage Device *268*
How to Export & View Transaction Logs *269*
How to Export Error Log *272*
How to Export User Database *274*
How to Export Contactless key *276*
Information Menu ***278***
View Device Details *279*
View Firmware Information *281*
View Sensor Revision Information *283*
View Communication Parameters *284*
View Memory Status *287*
View User Status *287*
View Transaction Log Status *289*
Reboot Terminal ***290***
SECTION 6 : TERMINAL VIDEOPHONE /AUDIOPHONE FACILITY **292**
Introduction to Videophone ***293***
Configure Video Phone / Audio Phone Server ***295***
Viewing Video/Audio Phone Server Details ***298***
Delete Video/Audio Phone Server ***299***
How User can make Video/Audio Call ***301***
SECTION 7 : TERMINAL MENU FOR SIGMA LITE+ SERIES **304**
SIGMA Lite+ Series terminal Screens ***305***
Terminal Home Screen *305*
Terminal Information Menu *305*

Terminal Details *306*
Communication Details *307*
Steps to Setup Wallpaper ***308***
Recover Corrupted Components ***309***
Display Screens and Actions ***310***
SECTION 8 : TERMINAL CONFIGURATION THROUGH WEBSERVER **314**
Access to Administration Menu through Webserver ***315***
Login to Webserver *316*
User Enrollment in Database *318*
User Enrolment in Card *324*
User Enrolment in Card & Database *325*
Update User Information *326*
Delete User *328*
Card Manager *329*
SECTION 9 : USB SCRIPTS **342**
USB Scripts ***343***
SECTION 10 : ACCESS CONTROL **344**
Access control presentation ***345***
Typical architecture of an access control system *345*
Typical access control process *346*
Preliminary: adding a biometric template in local database ***347***
Access and Time Biometric Terminal operating modes ***348***
Standalone mode or Slave mode *348*
Standalone mode: Identification and/or Authentication *348*
Access Control Process in Identification Mode *350*
Access Control Process in Authentication Mode *351*
Access Control Process for VIP Users *351*
Access Control Result ***353***
Information for the User *353*
Information for the Administrator *353*
Integration in an Access Control System *353*
Access Granted *354*
Access Denied *354*
SECTION 11 : ACCESS CONTROL BY IDENTIFICATION **355**
Identification Mode Description ***356***
Identification Process *356*

Access Control by Identification *356*
Result of the access control request *356*
User's Data required in the terminal *356*
Identification Modes (database extension licences) *356*
Compatibility with Access Control Systems *357*
User Interface *358*
SECTION 12 : ACCESS CONTROL BY AUTHENTICATION **359**
Authentication Process ***360***
Introduction *360*
Authentication process *360*
Access control by authentication *360*
Contactless Smartcard *361*
List of contactless cards validated *362*
Authentication Process Options *362*
Manual bypass of biometric control *362*
Automatic bypass of biometric control *362*
Result of access control check *363*
Compatibility with Access Control Systems *363*
Biometric check, biometric data on user's card ***364***
Description *364*
User's data required in the terminal *364*
User's data required on the user's card *364*
Activation key *364*
User Interface *364*
PIN verification - PIN stored on card ***366***
Description *366*
User's data required in the terminal *366*
User's data required on the user's card *366*
Activation key *367*
User Interface *368*
BIOPIN verification - BIOPIN stored on card ***369***
Description *369*
User's data required in the terminal *369*
User's data required on the user's card *369*
Activation key *369*

User Interface *370*
Biometric check and biometric data in local database ***371***
Description *371*
User's data required in the terminal *371*
User's data required on the user's card *371*
Activation key *372*
User interface *372*
Authentication with local database: User ID entered from keyboard ***373***
Description *373*
Activation key *373*
Authentication with local database: ID input from Wiegand or Clock & Data ***374***
Description *374*
Activation key *374*
Wiegand Frame Configuration *376*
Site-code Propagation *377*
Wiegand frame example (26 bits) *377*
No biometric check, no User ID check ***378***
Description *378*
User's data required in the terminal *378*
User's data required on the user's card *378*
Activation key *379*
User Interface *379*
No biometric check, User Identifier in the database ***380***
Description *380*
User's data required in the terminal *380*
Activation key *380*
User Interface *381*
Authentication process specified by User's card ***382***
Description *382*
User's data required in the terminal *382*
User's data required on the user's card *382*
Activation key *383*
User Interface *383*
Allowed format for User's identifier ***385***
TLV structured data *385*

Binary Data *387*
SECTION 13 : FINGERSCAN ACCESSORY **390**
Functionality ***391***
Identification *391*
Authentication *391*
Dual biometric control *391*
Fingerscan parameters *392*
SECTION 14 : MULTIFACTOR ACCESS CONTROL MODE **393**
Multi-factor Mode ***394***
Description *394*
User Interface *394*
User's data required in the terminal *394*
User's data required on the user's card *394*
Activation keys *395*
SECTION 15 : SECURITY ADMINISTRATION **396**
Tamper Setting ***397***
Biometric technology Settings ***398***
Recommendations for a Secure Installation ***399***
SECTION 16 : WIEGAND CONFIGURATIONS **400**
Wiegand Parameters Settings ***401***
Wiegand Parameters Configuration through Webserver *402*
SECTION 17 : THREAT LEVEL CONFIGURATIONS **405**
Threat Level Configuration ***406***
Threat Level Configuration through Webserver *406*
SECTION 18 : TIME AND ATTENDANCE CONFIGURATIONS **408**
T&A Synoptic ***409***
T&A Mode in SIGMA Lite+ Series *411*
T&A Normal Mode for all other Access and Time Biometric Terminals *411*
T&A Extended Mode for all other Access and Time biometric Terminals *413*
T&A Mode Mandatory or Optional Scenarios *414*
T&A request on VisionPass Range terminals *415*
T&A configuration through Webserver *416*
T&A - Mandatory Mode Work Flow Diagram *418*
T&A - Non Mandatory Mode Work Flow Diagram *419*
SECTION 19 : SCHEDULES CONFIGURATION **420**

Schedules Configuration **421**
Define Access Schedule 421
Define User Access Schedule 424
Define Holiday Schedule 426
SECTION 20 : CONTROLLER FEEDBACK **430**
Controller Feedback **431**
SECTION 21 : OSDP PROTOCOL SUPPORT **434**
Description **435**
Terminal Configuration **436**
OSDP Commands and Responses **438**
About the osdp_BIOMATCH command 439
osdp_BIOMATCH command with multiple fingerprint templates 440
About the osdp_POLL command 440
About the osdp_COMSET command 441
About the osdp_CAP command 441
About OSDP secure channel 442
Demonstration of osdp_LED and osdp_TEXT command for SIGMA terminal 442
Demonstration of osdp_LED and osdp_TEXT command for SIGMA Lite+ terminal 444
Demonstration of osdp_LED command for SIGMA Lite terminal 445
How to ignore MMI OSDP commands and play Idemia MMI **446**
OSDP.ignore_MMI set to 1 446
OSDP.ignore_MMI set to 3 446
PIN over OSDP **448**
Report user rejection event with OSDP **449**
Recommendation and limitation for OSDP integration 451
SECTION 22 : SSCP **452**
Description **453**
Terminal Configuration **454**
SSCP Commands and Responses **456**
About the Verify command 457
About the OutputRGB command 457
SECTION 23 : USER CONTROL CONFIGURATIONS **458**
User Control Configurations **459**
SECTION 24 : EVENT CONFIGURATIONS **464**
Event Configurations **465**
SECTION 25 : MMI (MAN-MACHINE INTERFACE) CONFIGURATIONS **468**

MMI (Man-Machine Interface) Menu ***469***
SECTION 26 : DISTANT COMMANDS MODE **471**
Presentation of Distant Commands mode ***472***
Process *472*
Distant Commands mode use sample *473*
SECTION 27 : POLLING MODE **474**
Presentation of Polling mode ***475***
Process *475*
Polling mode activation *476*
SECTION 28 : MESSAGES SENDING **477**
Principle ***478***
Events ***479***
Sending Interfaces ***480***
SECTION 29 : COMPATIBILITY WITH AN ACCESS CONTROL SYSTEM **481**
Internal Relay activation on Access Granted result ***482***
Description *482*
Activation key *483*
Configuration key *484*
External activation of the internal relay ***485***
Description *485*
Activation key *486*
Configuration key *486*
Access Request Result Log File ***487***
Description *487*
Log File format *487*
Log File management *488*
Log File size *488*
Activation key *488*
Sending an Access Control Result Message ***490***
Presentation *490*
Ports and protocols *490*
Serial Port (Output only) *491*
Ethernet port *493*
Wi-Fi™ Channel *493*
Note about Terminal Clock Deviation *493*
SECTION 30 : TERMINAL USER INTERFACE **495**

Audio Man Machine Interface ***496***
Audible signal *496*
Terminal States *497*
Enrolment *500*
LED – Buzzer Sequence *501*
SECTION 31 : COMPATIBILITY SOFTWARE APPLICATIONS **505**
Compatible software applications ***506***
SECTION 32 : RECOMMENDATIONS **507**
Warning ***508***
General precautions *508*
Areas containing combustibles *508*
Specific precautions for terminals fitted with a contactless smartcard reader *508*
Ethernet connection *509*
Date / Time synchronization *509*
Cleaning precautions *509*
Recommended Conditions for Face Detection *509*
Technical Support and Hotline *527*

ANNEX 1 : SIGMA RANGE SERIES FINGER PLACEMENT RECOMMENDATION **510**
ANNEX 2 : COMPARISON OF AUTHENTICATION MODE WITH CONTACTLESS CARD **517**
ANNEX 3 : BIBLIOGRAPHY **520**
ANNEX 4 : GLOSSARY, ACRONYMS AND ABBREVIATION **522**
ANNEX 5 : SUPPORT **526**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 1 : **Introduction**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Scope of the document

This document is intended to guide administrators on 'How to setup and use' the Access and Time Biometric Terminals. It also talks about capabilities, and the possible configurations that can be done along with detailed steps and snapshots. On top of this an administrator can learn about access control processes, compatibility with access control systems, Time & Attendance mode and how terminal is configurable through Webserver.

In order to setup and use the Access and Time Biometric Terminal in the most efficient way, it is recommended for the Administrator to thoroughly read this guide.

NOTE: In this document, all references to VisionPass MDPI terminals are applicable to VisionPass MDPI-M terminal too, all references to Morpho*Wave®* SP MDPI terminals are applicable to Morpho*Wave®* SP MDPI-M terminal too

Terminal Series	Terminal Name	Contactless smartcard reader			QR Code		Mobile Credential	
		iCLASS® SEOS®	MIFARE® DESFire®	Prox®	Paper	Phone	HID Mobile Access	HID Apple Wallet
SIGMA Wide Series	SIGMA Wide iCLASS®	✓						
	SIGMA Wide MD		✓					
	SIGMA Lite							
	SIGMA Lite iCLASS® SIGMA Lite + iCLASS®	✓						
	SIGMA Lite MD SIGMA Lite + MD		✓					
	SIGMA Lite Prox SIGMA Lite + Prox			✓				
SIGMA Extreme Series	SIGMA Extreme iCLASS®	✓						
	SIGMA Extreme MD		✓					
	SIGMA Extreme Prox			✓				
Morpho*Wave®* Compact	Morpho*Wave®* Compact MDPI	✓	✓	✓	✓			

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

	Morpho*Wave*® Compact MDPI-M	✓	✓	✓	✓		✓	
	Morpho*Wave*® Compact MD		✓		✓			
MorphoWave® XP2	MorphoWave® XP2 MD		✓		✓			
MorphoWave® XP2	MorphoWave® XP2 MDI-M	✓	✓		✓		✓	✓
Morpho*Wave*® SP	Morpho*Wave*® SP MDPI	✓	✓	✓	✓			
	Morpho*Wave*® SP MDPI-M	✓	✓	✓	✓		✓	
	Morpho*Wave*® SP MD		✓		✓			
VisionPass	VisionPass MDPI	✓	✓	✓	✓	✓		
	VisionPass MDPI-M	✓	✓	✓	✓	✓	✓	
	VisionPass MD		✓		✓	✓		
VisionPass SP	VisionPass SP MDI	✓	✓		✓	✓	✓	✓
	VisionPass SP MD		✓		✓	✓		

Product support notation:

In this document, the term “SIGMA Range Series” is considered either “SIGMA Wide” or “SIGMA Lite” or “SIGMA Extreme” Series terminal, unless it is explicitly mentioned. The term “SIGMA Lite” is also considered “SIGMA Lite+” Series terminal, unless it is explicitly mentioned. The term “MorphoWave® Range Series” is considered either “MorphoWave® Compact” or “MorphoWave® XP2” or “MorphoWave® SP” Series terminal. The term “VisionPass Range Series” is considered either “VisionPass” or “VisionPass SP” Series terminal.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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 a human 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 three major ridge patterns such as Whorls, Loops and Arches. Unique characteristics known as Minutiae identify those points of a fingerprint wherein the ridges become either 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.

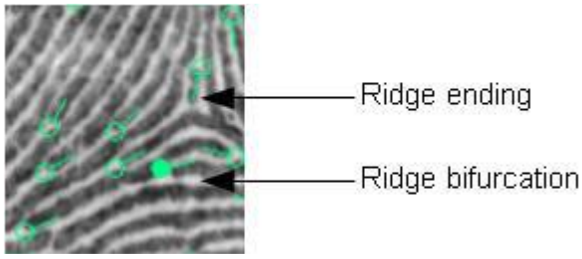


Figure 1: Minutiae are classified in two categories i.e. ridge ending and bifurcation

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, IDEMIA has carried an extensive research in the field of studying fingerprints and continually refined its expertise in the domain of fingerprint based recognition systems. It has lead the market in 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),

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

logical access control (computers and networks), secure payment transactions and OEM applications.

Finger Templates supported

Idemia Finger Terminals are able to manage external templates.

Following is the list of supported templates.

Template	Descritption	Use case	SIGMA Range Series	MorphoWave® Range Series
pkcompv2	Idemia private fingerprint template	Template on card	Y	Y
pkmat	Idemia private fingerprint template	Legacy installations	Y	Y
ansi378_2004	Public fingerprint template Finger Minutiae Record	Legacy installations	Y	Y
iso19794_2_fmc_cs	Public fingerprint template Finger Minutiae Card Record Compact Size	Legacy installations	Y	Y
iso19794_2_fmc_ns	Public fingerprint template Finger Minutiae Card Record Compact Size	Legacy installations	Y	Y
iso19794_2_fmr	Public fingerprint template Finger Minutiae Record	Legacy installations	Y	Y
iso19794_2_fmc_cs_aa	Public fingerprint template Finger Minutiae Card Record Compact Size, minutiae ordered by Ascending Angle	Legacy installations	Y	N
minex_a	fingerprint template format	Legacy installations	Y	N
din_v66400_cs	Compact Size fingerprint template format (minutiae)	Legacy installations	Y	N
din_v66400_cs_aa	Compact Size fingerprint template format (minutiae ordered by Ascending Angle)	Legacy installations	Y	N
PK_PV multimodal (fingerprint part only)	Idemia private multimodal template	Legacy installations	Y	Y
pklite	Idemia private fingerprint template	Template on device	Y	Y
ansi378_2009	Public fingerprint template Finger Minutiae Record	Legacy installations	N	Y
iso19794_2_fmr_2011	Public fingerprint template Finger Minutiae Record	Legacy installations	N	Y

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

TEM from 4G	L-1 Bioscrypt private fingerprint template (pattern) (only used for 1/1 matching)	Legacy installations	Y	N
VUR from 4G	L-1 Bioscrypt private fingerprint template (pattern) (only used for 1/1 matching)	Legacy installations	Y	N
BUR from 4G	L-1 Bioscrypt private fingerprint template (pattern and minutiae) (used for 1/1 and 1/N matching)	Legacy installations	Y	N

About face biometrics

The face biometric data for VisionPass terminal are based on 3 images.

These 3 images are obtained by 3 cameras :

- RGB camera to capture visible light picture
- NIR camera to capture infrared light picture
- 3D camera to capture 3D picture

These 3 pictures allow to create a face biometric template.

The face biometric data for VisionPass SP terminal is based on an image that is obtained by RGB camera to capture visible light picture.

Face Templates supported

Idemia Terminals are not able to manage external face templates.

Following is the list of supported templates.

Template	Descritption	Use case	VisionPass	VisionPass SP
face_v2	Idemia private face template based on RGB, NIR and 3D images	Template on device	Y	Y
face_v2_comp_light	Idemia private face template based on RGB, NIR images to reduce the template size	Template on card	Y	Y
Face_v3	Idemia private face template based on RGB	Template on card or device	N	Y

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Templates size

To store biometric templates in an external data base or in a contactless card, it is frequently necessary to know memory size needed. Here the biometric template sizes:

Template	Use case	Max Size
pklite MorphoAccess® SIGMA Range Series	To store in an external data base (for example MorphoManager)	1553 bytes
Pklite MorphoWave® Range Series	To store in an external data base (for example MorphoManager)	1699 bytes
pkcompv2 (when generate using MorphoKit and optimized parameter case MorphoManager)	To store in a contactless card or to execute a biometric verification operation using distant command (example osdp_BIOMATCH)	170 bytes
face_v2	To store in an external data base (for example MorphoManager)	2426 bytes
face_v2_comp_light	To store in a contactless card or to execute a biometric verification operation using distant command (example osdp_BIOMATCH)	1046 bytes
Face_v3	To store in an external data base (for example MorphoManager) or in a contactless card	726 bytes

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

General

Why would one connect the terminal to a PC?

The Access and Time Biometric Terminals are designed to be able to run in standalone mode, it means without any connection to a master system. But, a connection with a PC is useful to perform tasks like:

- Configuring the terminal.
- Maintaining terminal: firmware upgrade, add a license (to unlock an optional feature)
- Managing the database, i.e., adding or deleting or modifying the user data.
- Managing log files, i.e., get or delete the log files.
- Configuring the Wi-Fi™ connection.

Connection methods

The Access and Time Biometric Terminals 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 Access and Time Biometric Terminal can be configured using an application such as **MorphoBioToolBox**.

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

A POE+ current injector is mandatory if the Morpho*Wave®* Range Series terminal is not powered by the +12VDC/GND wires block.

A POE+ current injector is mandatory if the VisionPass SP terminal is not powered by the +12VDC/GND wires block.

VisionPass terminal should be powered by the +12VDC/GND wires block.

First connection

All access and time biometrics terminals are delivered in Enforced Security configuration. This includes a TLS default certificate. By consequence, first connection should be done using Idemia software, like MorphoBioToolBox or MorphoManager.

Please refer to our website knowledge base https://biometricdevices.idemia.com to know more about the installation procedure.

Main consequence of secure mode are:

- Connection using plain TCP is not authorized : only TLS connection is available

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

- Webserver is not available
- USB scripts are not available
- Local administration menu is restricted, depending of user right
- Thrift commands are not available using USB port or Serial Link

Customer could unlock the Enforced Security configuration and switch to the On-Demand security mode, using MorphoBioToolBox, to access to these functionalities.

Network parameter initialization

The 'default' network parameters of the Access and Time Biometric Terminals are:

IP address Mode	Parameter	Factory value
Static	Terminal IP address	192.168.1.10
	Gateway IP address	192.168.1.254
	Sub network mask	255.255.254.0
	Host name	MAsigma/MAsigma-lite/MAsigma-lite-plus/MAextreme/Morpho*Wave*-Compact/ Morpho*Wave*-SP/VisionPass/ VisionPassSP/MorphoWaveXP2

If the terminal's default network parameter values cannot be used, it is recommended to refer to the "*Communication menu*" to change these values.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Point to Point Ethernet Connection

The Access and Time Biometric Terminals can be connected directly to a PC by an Ethernet cable.

The administrator needs to consider the points mentioned below prior to connecting the terminal directly to a PC via an Ethernet cable.

If the Ethernet port of the PC does not 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 "*Connection through only one Ethernet switch*").

If the PC that the administrator uses is already connected to a LAN, then it must be either disconnected from the LAN, or equipped with a 2nd network interface board. This 2nd network board will be dedicated to the connection with the terminal. The administrator may need to modify the network parameters of the PC, in that case a Network or LAN administrator should be contacted for seeking the best solution.

Figure 2: Direct Point to Point Ethernet Connection

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Connection through only one Ethernet switch

The Access and Time Biometric Terminals can be connected to a PC through an Ethernet switch. This is useful when no crossover cable is available, in that case the administrator can use one Ethernet switch and two Ethernet standard cables.

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

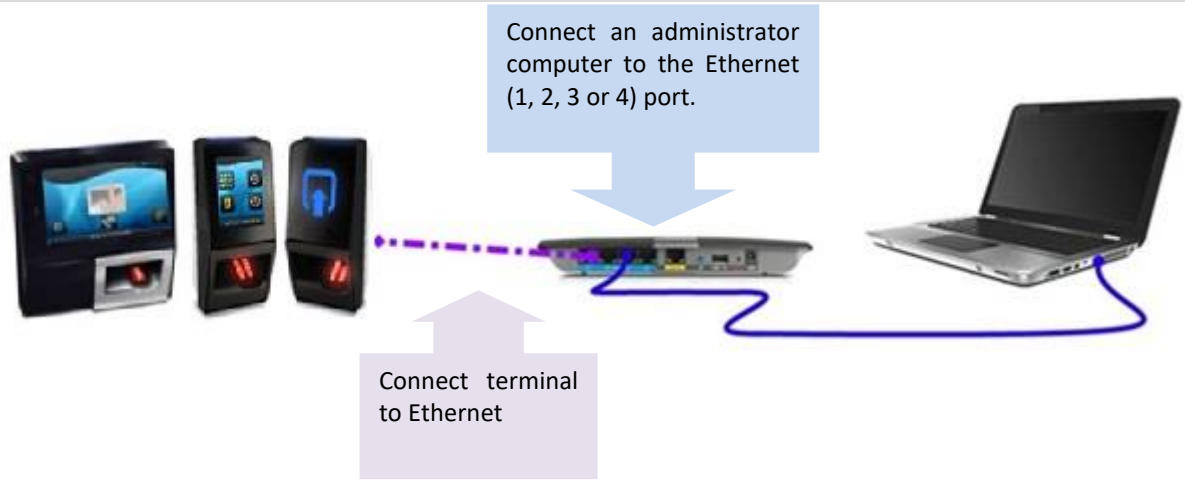


Figure 3: Connection through an Ethernet switch

Connection through a LAN

Description

The administrator can also connect the Access and Time Biometric Terminals to a PC via Local Area Network (LAN) by specifying a unique IP address or host name.

The IP address could be static or dynamically assigned by the DHCP server in the network. If the administrator chooses to specify the host name of the terminal as its unique identifier, then in that case the 'terminal name' must be added to the DNS server database by the network administrator.

Figure 4: Connection through LAN

The administrator is recommended to connect Access and Time Biometric Terminals on a dedicated network in order to reduce possibilities of fraudulent access to the configuration of the terminal. It is advised to contact the network administrator for more information on LAN security strategies.

Before the administrator connects the Access and Time Biometric Terminals to a LAN, it is necessary to configure the LAN parameters into the terminal. The values of these parameters are to be provided and/or approved by the network administrator.

LAN with DNS Server

When a DNS server is available in the LAN, the PC can request the connection to the Access and Time Biometric Terminal by using its host name instead of its IP address.

The network administrator must add the Access and Time Biometric Terminal host name to the DNS server database, otherwise a TCP open session request using the terminal's hostname will fail.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

It is useful to specify the Access and Time Biometric 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 helps the administrator in connecting the Access and Time Biometric Terminal to a LAN that does not have a DNS server or when host name cannot be added to the DNS Server database.

The PC is not able to establish a connection with a terminal using its host name. An IP address of the Access and Time Biometric Terminal is the only way to specify the terminal.

For standard use (excluding unscheduled maintenance operations), it is recommended that the administrator should not enable DHCP mode in this case. This is because in the DHCP mode the IP address for the terminal can change each time it is restarted.

Static IP address (DHCP disabled)

This is the easiest way for an administrator to connect a Access and Time Biometric Terminal to a LAN. In this case, the IP address of the terminal remains the same after each reboot and the Host System needs to know only this IP address in order to establish a connection with the terminal.

The IP address of the Access and Time Biometric 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 Access and Time Biometric Terminal IP address,
- Gateway IP address,
- Local subnet masks value.

WARNING: If the Access and Time Biometric Terminal uses an IP address already assigned in the network, the connection to the terminal will be unstable.

Dynamic IP address (DHCP enabled)

When the administrator enables the DHCP mode in the terminal, the terminal IP address and other networking parameters are assigned automatically from the DHCP Server (network routers). This address could be different after each start-up as it depends on the DHCP strategy defined for the LAN.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 3 : **Terminal Configuration and Administration**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Understanding Terminal Configuration

Presentation

Access and Time Biometric Terminals have factory default settings or reset values for all the supported functionalities. The administrator can configure the terminal depending on the desired level of security using these methods:

- **Terminal Administration Menu (except for SIGMA Lite and Morpho*Wave*® SP Series)**
- **Webserver Application**
- **Distant system Application**
- **USB Scripts**
- **MorphoBioToolBox**

Terminal Administration Menu: The administrator can login to terminal and access several functionalities under administration menu. This allows administrator to perform configuration, add users, upload multimedia, download logs, etc. The complete menus are covered in the subsequent sections of this document.

Webserver Application: Webserver can be termed as a remote configuration panel of terminal. Using Webserver, the administrator can configure any parameter of the terminal while connected remotely. Webserver is connected to the terminal through Ethernet or Wi-Fi™ network. Only an administrator with full administrative rights can login to Webserver. Webserver also has a 'Complete Configuration' tab from which the administrator can configure all possible parameters. For detailed description of all the parameters, please refer to **Parameters Guide** document.

NOTE: Webserver Application and USB scripts are no more available In Enforced Security configuration. Please refer to our website knowledge base https://biometricdevices.idemia.com to unlock the Enforced Security configuration and switch to the On-Demand security mode, if needed.

NOTE: the Webserver is no more available for "MorphoWave® XP2" "MorphoWave® SP" and "VisionPass SP".

Modifying the value of a parameter

There are two ways an administrator can 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),

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

- With a USB mass storage key, which contains a script prepared on a PC using **MorphoBioToolBox**. This requires to switch to the On-Demand security mode.

Backup of customized parameters

It is strongly recommended to backup the new values on a physical support such as paper (stored in a safe place) or a digital file (saved in a software safe).

Do not note it on visible or easily accessible supports (keyboard, datebook, pad...). If necessary, store them in a ciphered file.

According to the wished security level, the backup location can be a simple drawer, or a shielded and fireproofed cupboard.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Configuring a Networked terminal

Introduction

The administrator can manage an Access and Time Biometric Terminal by a PC connected to the terminal, by using an application such as a web browser connected to the embedded Webserver or **MorphoBioToolBox**.

The remote operations available are mainly:

- Time and Attendance configuration
- Read and Modify parameter values
- Manage access schedules
- Manage network configuration
- User Management
- Log Management
- Tamper settings, etc.

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

Figure 5: Configuration of a SIGMA Range terminal by a Host System

To know more on the commands supported by the Access and Time Biometric Terminal, the administrator needs to refer to **Access and Time Distant Commands Guide** document.

Network factory settings

By default, the IP address of the Access and Time Biometric Terminal is 192.168.1.10. The default server port is 11010.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Date/Time settings

The administrator can update the date/time of the terminal by a distant system, by the local Administrator Menu or Webserver.

SSL Securing

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

These protocols are used to protect the communication between the Access and Time Biometric Terminals and a distant system, such as a central access controller or a terminal configuration station.

References

Refer to "*SSL Configuration*" under Security Menu section in this guide, to enable and configure SSL communication port

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Network Wi-Fi™ configuration

Administrator can configure Wi-Fi™ parameters, Wi-Fi™ connection is available under the following conditions:

The administrator has plugged in a Wi-Fi™ USB adapter. Details of the installation procedure are described in the **Installation Guide** document associated to each terminal type.

The administrator had loaded WI-FI™ License in the terminal.

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 Access and Time Biometric 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 Wi-Fi™ License is mandatory (except for VisionPass Range terminals, this feature is available without license)

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 “*Wi-Fi™ Network Configuration*” section.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Terminal Database Management

General

The administrator can manage the database of the Access and Time Biometric Terminal by using administration menu of the terminal (except for SIGMA Lite and Morpho*Wave*® SP Series) or through Webserver application connected to terminal.

Adding a user to the database

Adding a user means to create a record of the user that contains at least a unique identifier. Users stored in the database are of following types:

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

Limited Database Administrators are allowed access to the administration menu of the terminal, to consult the device information and to add users to the data database. There are not authorized to remove or modify already existing user records.

Database Administrators are allowed access to the administration menu of the terminal, to consult the device information and to manage the users database.

Full Administrators are allowed access to the administration menu of the terminal, to consult the device information, to perform configurations and to manage the users database.

The user's enrolment can be directly done on the Access and Time Biometric Terminals without managing a database on the PC.

NOTE: In Enforced Security configuration, access to database management menu requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Removing a user from the database

Removing a user means deleting the user's record from the database of the Access and Time Biometric Terminals.

The user can be removed directly from the Access and Time Biometric Terminals without managing a database on the PC.

Database Size

The Access and Time Biometric Terminal database storage is as follows:

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Database Limits	SIGMA Series SIGMA Extreme Series	SIGMA Lite Series	Morpho*Wave*® Compact / XP2	Morpho*Wave* ® SP	VisionPass	VisionPass SP
Maximum User (Including Administrator)	5,000	500	Based on Database license (see below)	10,000	Based on Database license (see below)	Based on Database license (see below)
Maximum Authorized User	250,000	250,000	1,000,000	1,000,000	250,000	250,000
Maximum VIP User	100	100	100	100	100	100

Maximum User indicates the basic capacity of terminal users' database including administrators.

Maximum Authorized User List Capacity indicates the maximum number of users which can be added to authorize user list.

Maximum VIP User capacity, indicates the maximum capacity of the users which can be enrolled as VIP users.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Terminal License Management

The administrator can install one or more licenses in the terminal in order to unlock one or several optional features of the Access and Time Biometric Terminal.

User licenses

Administrator can install user licenses to extend the maximum database limit.

- For SIGMA Range terminals, user data are stored with two fingers per user record (three fingers per user record in case duress finger is enabled).
- For Morpho*Wave*® Range terminals, user data are stored with eight fingers per user record.
- For VisionPass Range terminals, user data are stored with one face template.

Depending on the terminal, the following user licenses are available for procurement:

License	SIGMA Wide Series	SIGMA Extreme Series	SIGMA Lite Series	Morpho*Wave*® Compact / XP2	Morpho *Wave*® SP	VisionPass	VisionPass SP
MA_3K_USERS	✗	✗	✓	✗	✗	✗	✗
MA_10K_USERS	✓	✓	✓	✗	✓	✗	✓
MA_20K_USERS	✗	✗	✓	✗	✗	✓	✗
MA_40K_USERS	✗	✗	✗	✓	✗	✓	✗
MA_50K_USERS	✓	✓	✗	✗	✗	✗	✓
MA_100K_USERS	✓	✓	✗	✓	✗	✓	✓

Communication licenses

Access and Time Biometric terminals support communication to distant system through Ethernet Connection. There are other networks such as Wi-Fi™ and 3G which can be used for connecting terminal with distant systems. The administrator needs to install license(s) in order to enable communication between the terminal and the distant system. Following is an overview of the types of licenses available.

- 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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

NOTE: The license alone is not enough, a USB Wi-Fi™ adapter compatible with Access and Time Biometric Terminals is mandatory. The adaptor and license can both be ordered under reference "MA WI-FI PACK" (except for VisionPass Range terminals, this feature is available without license)

- The administrator needs to install the MA_3G license in order to enable the 3G network (GPRS/GSM/3G) which replaces the standard Ethernet connection. The terminal can communicate with distant systems through 3G/GPRS/GSM network. This license is applicable to Access and Time Biometric Terminal only.

NOTE: MA_WI-FI license and MA_3G license are no more available

DESFire EV2 secure messaging license

SIGMA range terminals, Morpho*Wave®* SP, Morpho*Wave®* XP2 and VisionPass SP terminals support DESFire EV2 secure messaging. The administrator needs to install license BT_DESFIRE_SEC in order to enable it.

802.1x license

Morpho*Wave®* SP, Morpho*Wave®* XP2 and VisionPass SP terminals support 802.1x protocol. The administrator needs to install license BT_802_1X in order to enable it.

SSCP license

Morpho*Wave®* SP, Morpho*Wave®* XP2 and VisionPass SP terminals support SSCP protocol from the SPAC Alliance. The administrator needs to install license BT_SSCP in order to enable it.

User data extraction license

Morpho*Wave®* SP, Morpho*Wave®* XP2 and VisionPass SP terminals need license to extract user data. The administrator needs to install license BT_EXPORT_USERS to use function that requires extracting data from the terminal.

Getting a license for a Access and Time Biometric Terminal

In case you would need one (or more) license(s) for your terminal(s), please liaise with your IDEMIA Sales Representative, who will advise you the best way to purchase, depending on your use case (license type, number, etc.).

In any case, each purchased license will be delivered as a file.

The license is delivered in a file dedicated to only one terminal.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Checking licenses installed in the terminal with license manager application

The Terminal Info page of the Webserver on SIGMA Lite or the Information Menu of the terminal (on SIGMA Wide, SIGMA Extreme, SIGMA Lite+, Morpho*Wave*® Compact, VisionPass) allows to check the installed licenses: please refer to **Administration Menu > Information Menu > Device > License Name**. If the administrator wants to view the installed licenses or add licenses from a PC, an Ethernet or Wi-Fi™ connection and License Manager Application are needed. The application can be downloaded from our biometric terminals website (www.biometric-terminals.com).

NOTE: Checking or installing license requires to open the dedicated port, that is closed by default. The configuration key comm_channels_state.upgrade_firmware must be set to 1 . It is not possible for Morpho*Wave* SP, but no commercial license is available for this terminal.

Screens & Steps

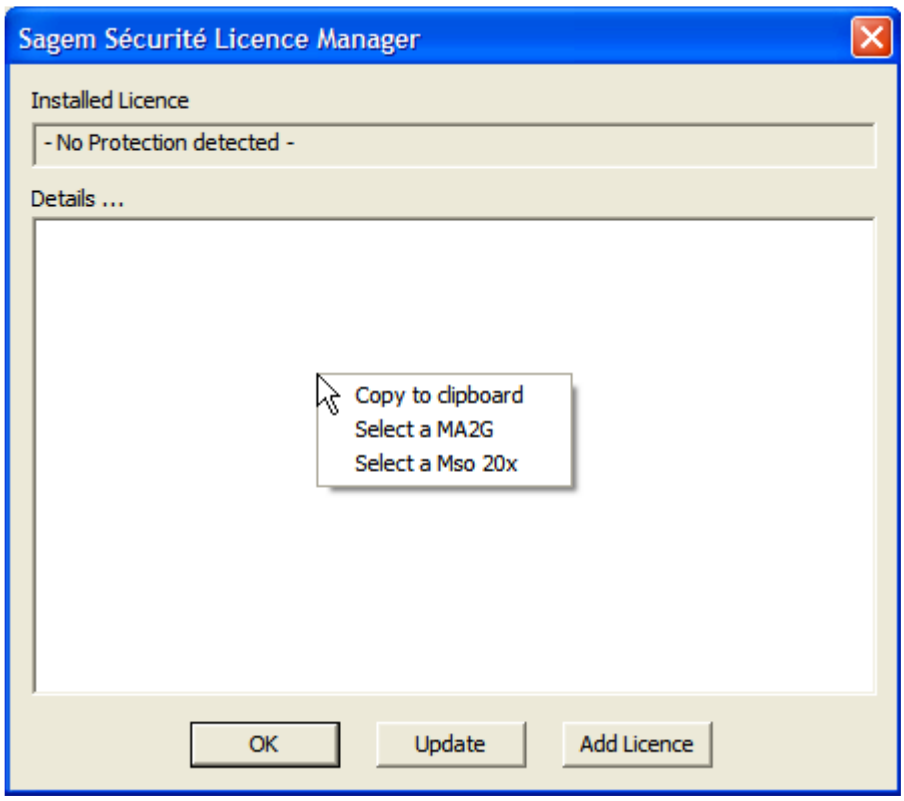


Figure 6: License Manager, adding a Access and Time Biometric Terminals

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

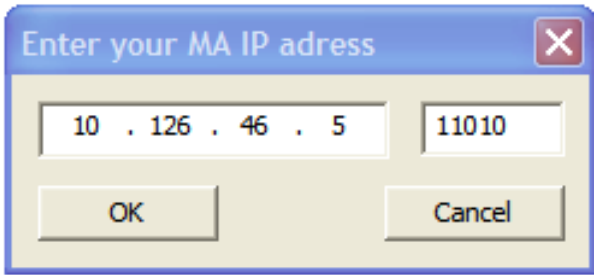


Figure 7: License Manager, enter the IP address

2. Enter the IP address of the Access and Time Biometric Terminal in the window that opens.

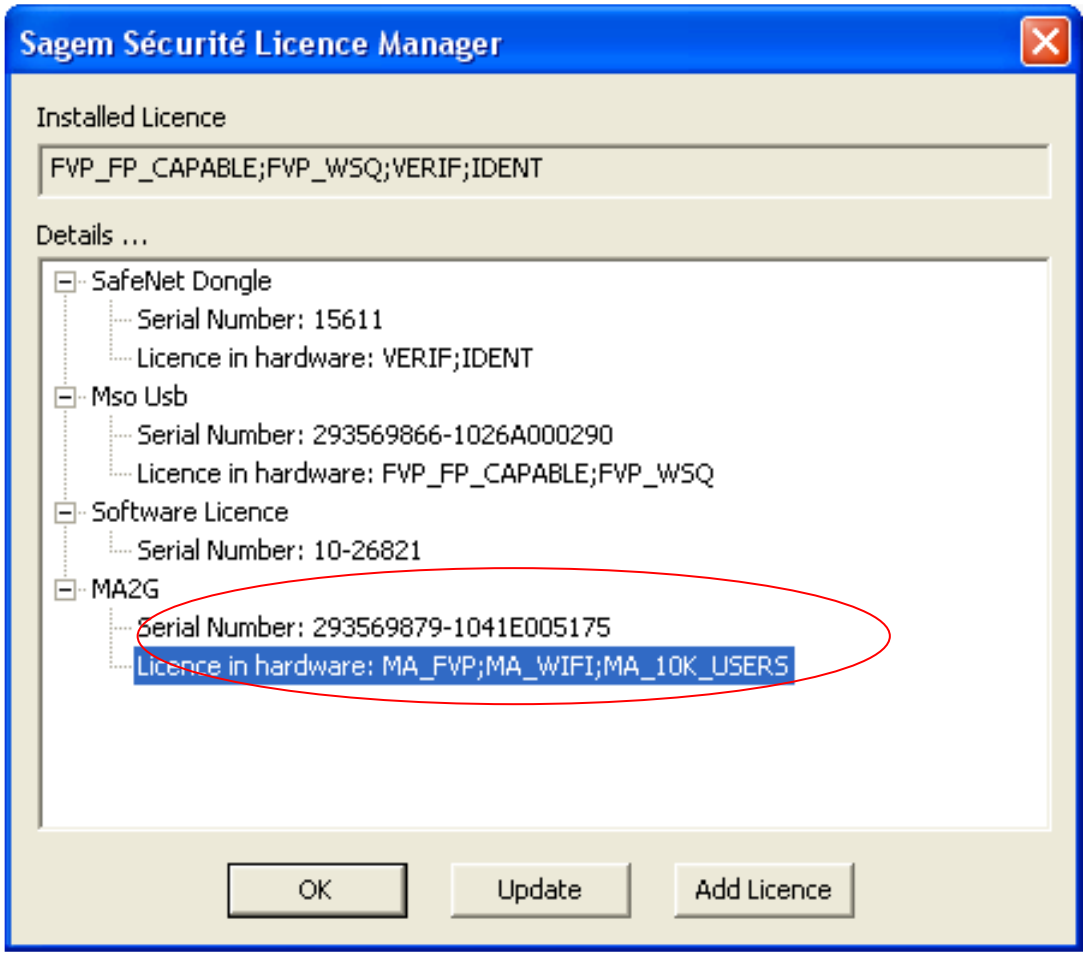


Figure 8: Licenses installed in a Access and Time Biometric Terminals

3. Refer to the screenshot above, the licenses on the Access and Time Biometric Terminals are listed in the “license in hardware" line in the main window.

Installing a new license

To install a new license, the administrator must follow the steps mentioned below:

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

Launch the "License Manager" application then add the Access and Time Biometric Terminals 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.

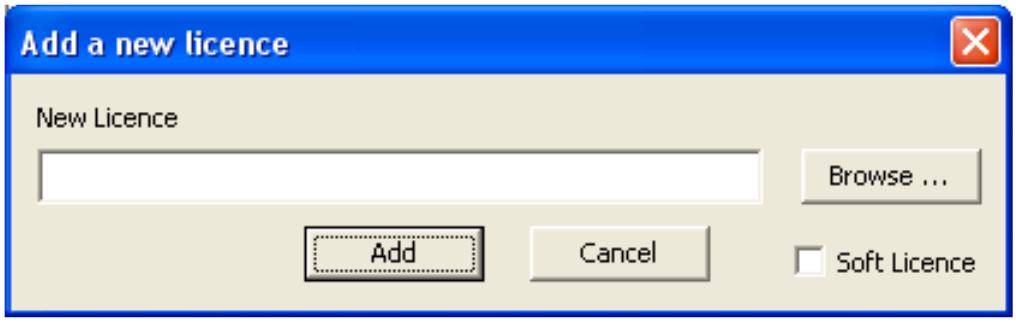


Figure 9: Adding a license in a Access and Time Biometric Terminals

For further information on how to use the license management tool (License Manager PC tool), the administrator needs to refer **SIGMA, SIGMA Extreme and SIGMA Lite Series License Management** document.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Terminal Firmware Upgrade

How to get latest version of firmware

The administrator can download the latest version of the Access and Time Biometric Terminal firmware from the IDEMIA web portal: https://biometricdevices.idemia.com/s/

How to Open/Close the Retrofit port

For SIGMA Range Series, MorphoWave® Compact and VisionPass, retrofit port or Firmware upgrade port can be set to open or close through a configuration key "comm_channels_state.upgrade_firmware".

How to upgrade the firmware

The administrator can upgrade the Access and Time Biometric Terminal firmware. This can be done from PC through an IP link, i.e., Ethernet or Wi-Fi™.

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

Note: The administrator must not switch the terminal off during a firmware upgrade. The administrator also needs to ensure that the power supply of the terminal is stable before starting a firmware upgrade. Otherwise instability can occurs.

Also ensure that the retrofit port is open before starting the firmware upgrade. To check if the retrofit is open or not, check the value of configuration key "*comm_channels_state.upgrade_firmware*" which should be set to 1. If the value is set to 0 then the retrofit port is closed and the firmware upgrade process could not be started.

Firmware upgrade using a USB Mass Storage Key

The administrator can update the firmware using a USB mass storage key.

This operation is possible by using USB Scripts created from **MorphoBioToolBox** software application.

Firmware upgrade tool for expert users

Upgrade Tool

For SIGMA Range Series, MorphoWave® Compact and VisionPass, a software application called MA_Sigma_Upgrade_Tool is available for expert users. This tool allows the

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

administrators to upgrade the firmware of a specified Access and Time Biometric Terminal, directly. This tool has no graphic interface. The firmware can be upgraded via the 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 the help menu.
-v	Verbose mode. This is optional.
-f path	Path to the binary file used for upgrade. This is mandatory.
-e IP_address	IP address of the terminal to upgrade. This is mandatory.
-t timeout	Timeout of the connection (in ms). This parameter is optional. Its default and minimal value is 10s.
-p port_number	TCP port number to be used to connect the terminal. This is an optional parameter. Its default value is 11010.

Samples

The following command upgrades firmware of terminal at IP address 192.168.1.2 using file new_firmware.bin

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

Upgrades firmware of terminal at IP 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 IP 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 relaunch RetrofitTool with the same command line. The

firmware upgrade is restarted from beginning and executes all commands including proper restarting of the terminal.

Terminal upgrade using Thrift commands

Upgrade firmware of Morpho*Wave*® SP, Morpho*Wave*® XP2 and VisionPass SP, could be manage using dedicated Thrift commands, allowing its integration in third party application.

The Thrift command to use is file_load with the File_type “firmware_upgrade”.

Please refer to “Access and Time Biometric Terminals Distant Commands Guide” for their implementation.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 4 : Terminal First Boot Assistant

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Assistant Initialization

First Boot Assistant (FBA) is launched as soon as the Access and Time Biometric Terminal is started for the first time. All the basic configurations can be done by following the simple and easy to follow menu on the FBA screen. FBA can also set to launch on terminal reboot.

The administrator needs to follow the access path mentioned below in order to access First Boot Assistant from the Management menu.

Access Path

Terminal Menu : First Boot Assistant

NOTE: In Enforced Security configuration, access to First Boot Assistant menu requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Screens & Steps

Figure 10: First Boot Assistant Screen displayed on Installation

1. By default, the First Boot Assistant screen will open when the terminal is powered up for the first time. The administrator can also access FBA settings by following the access path mentioned above.
2. The administrator can configure the basic parameters via the First Boot Assistant Screen. For more details, please refer to the sections below:

Date & Time Configuration

The administrator must configure the current date, time and time zone in the terminal, on the first boot or a reboot of the terminal.

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

Access Path

Terminal Menu :

First Boot Assistant

or

Administration Menu > System Menu > Terminal Settings > Date/Time Settings > Clock Parameters

Screens & Steps

1. Select **Date Settings**

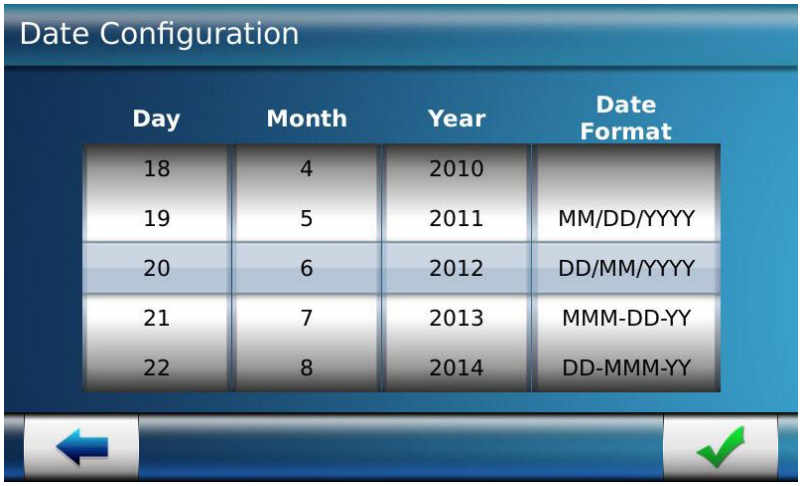


Figure 11: Configuring Current Date

2. Scroll up or down to select current **Day**, **Month**, and **Year**
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

4. Click on the Check button “” to save the setting
5. Select **Time Settings**

Figure 12: Configuring Current Time

6. Scroll up or down to select current **Hour**, **Minute**, and **Second**
7. Set **Hour Format** as analogue i.e. ‘12 Hour’ or digital i.e. ‘24 hour’
8. Set **Time Format** in the selection area which is used to select display format. The available formats are
   a. HH:MM:SS
   b. HH:MM.SS
9. Use Check button “” to save the setting

10. Select **Time Zone**

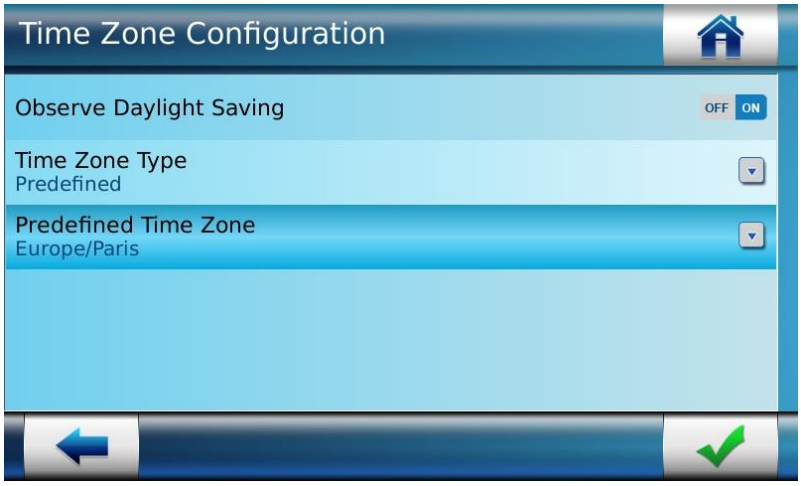


Figure 13: Configuring Time Zone

11. Select **Observe Daylight Saving** as 'On', in case the administrator needs to auto-schedule the time during the daylight saving months. By doing this, the terminal's time is automatically set to an hour later than the actual time while in the daylight saving time frame. For example, if the current time is 10 am then in the day light saving period, the time is automatically set to 11 am.
12. Select **Time Zone Type** as 'Predefined' or 'Custom'. If the administrator selects Predefined, the list of Predefined time zones of the entire world will be displayed to choose from. The administrator must specify a customized time zone when 'Custom' has been selected.
13. Use Check button " " to save the setting
14. Based on the **Time Zone Type**, Time Zone selection parameters are displayed next

Figure 14: List of Predefined Time Zones of World

15. The list of Predefined Time Zones of the entire world is displayed
16. Scroll up or down to select required **Time Zone** from the list
17. Click on the Check button "✓" to save the setting

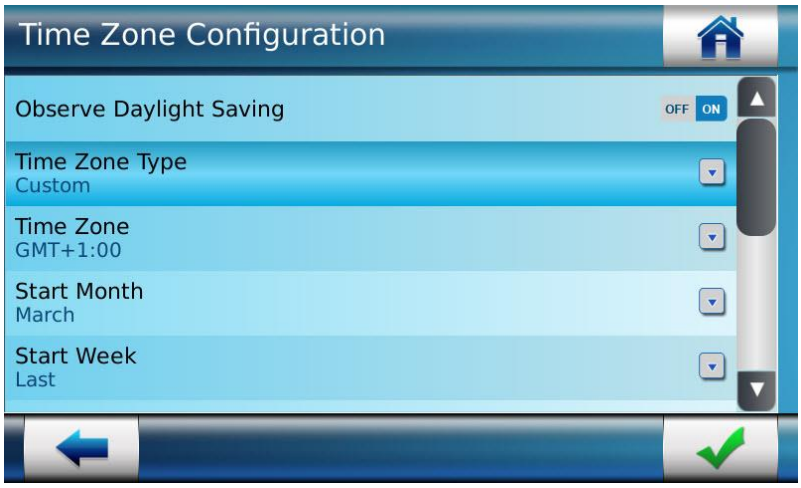


Figure 15: Custom Time Zone Setting

18. If the administrator selects the **Time Zone Type** as 'Custom', then an administrator need to define the below mentioned time zone parameters:
19. Select **Time Zone**

    NOTE: While setting a customized time zone, the administrator needs to ensure that the GMT offset that is set is the 'Standard GMT Offset' of the region.

20. **Start Month**, **Start Week**, **Start Day**, **Start Hour of Day**, **End Month**, **End Week**, **End Day** and **End Hour of the Day**
21. Click on the Check button "✓" to save the setting

Trigger Event

Access and Time Biometric Terminal will begin checking for access rights upon the occurrence of a specific event on the terminal. By setting these configurations the administrator can define as to when the terminal would commence performing access checks. The administrator can chose from the following events.

- **Biometric**, a finger, hand swipe or face 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 the 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.
- **QR code,** a QR code is detected and the authentication process starts with the User ID parsed from the QR code.

Access Path

Terminal Menu :

First Boot Assistant Assistant > Trigger Event

or

Administration Menu > Security Menu > User Control Settings > Trigger Event

Screens & Steps

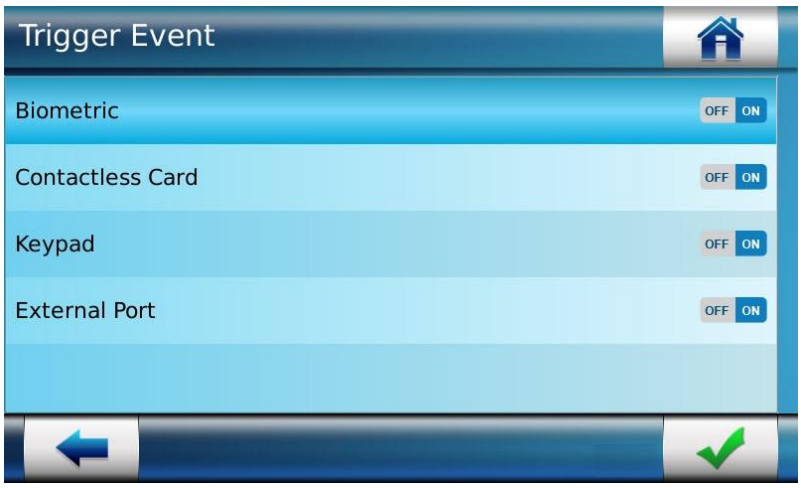


Figure 16: Selecting the event(s) that starts access control rights check process

1. The administrator can select from the above stated events. The event can be selected to be ON or OFF.
2. Click on the Check button “ ” to save settings

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Language Configuration

The administrator can select the language of the terminal's display by using this functionality. Multiple language options are available: English, French, Spanish and Arabic. 'English' is the default language selected.

Access Path

Terminal Menu :

First Boot Assistant > Language Settings

or

Home Screen > Language icon

Screens & Steps

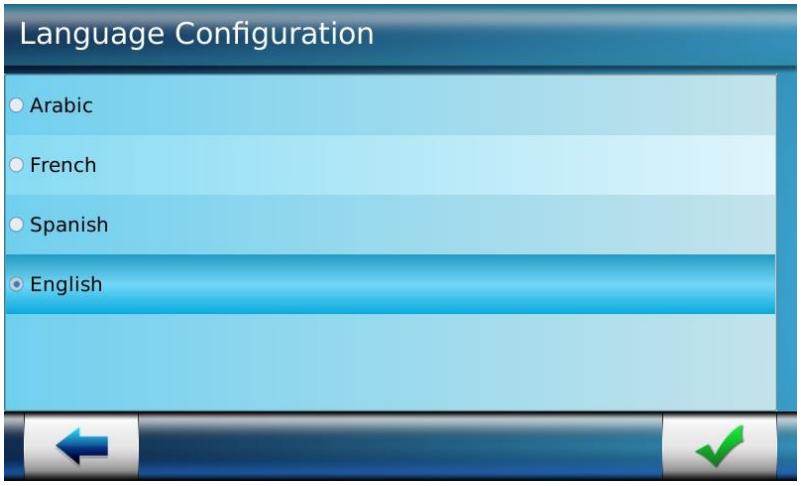


Figure 17: Configure Language

1. On the FBA screen, the administrator needs to select **Language Settings**
2. On the Home screen, the administrator needs to select the **Language icon** (refer to Figures 18 & 19)
3. Select a language
4. Click on the Check button " " to save the setting

Figure 18: Language selection on Home screen (Sigma)

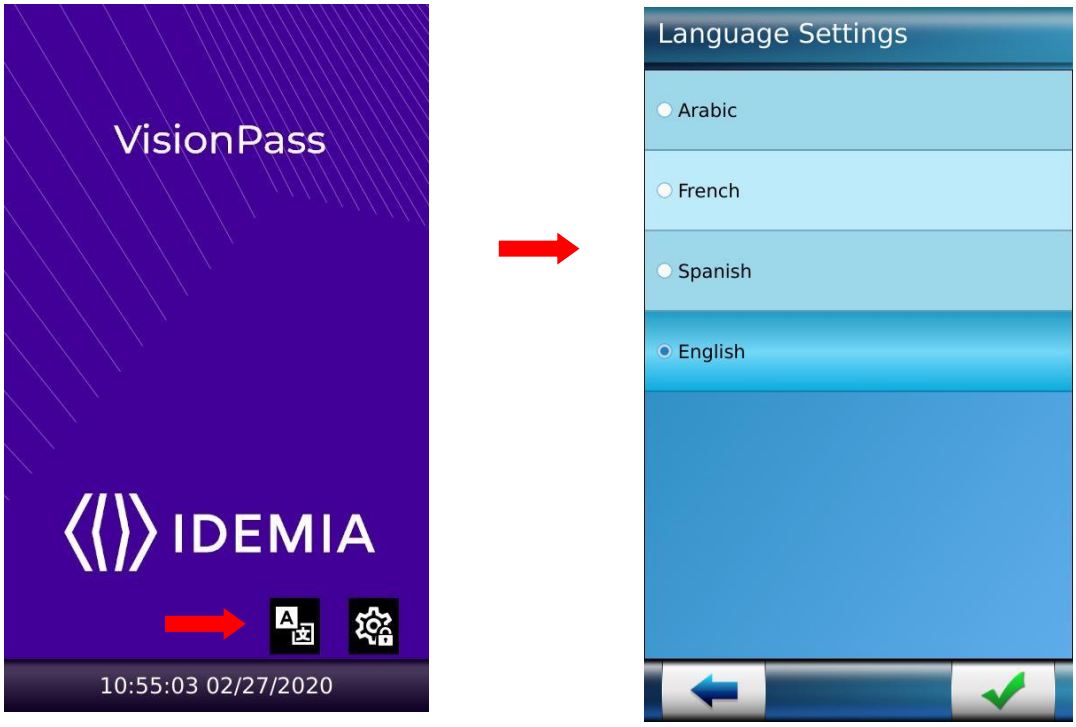


Figure 19: Language selection on Home screen (VisionPass)

Results

The preferred language is saved. The text display on the screen will be in the language selected by the administrator.

Note: The administrator must ensure that the audio messages played on the terminal must be in the same language as the one chosen. Administrator needs to upload the audio files from "Audio Settings" under Multimedia menu.

Show/Hide Language Icon

The administrator can chose whether to display the language icon on the home screen or not. This can be done via the Web Server application. The value of this parameter (misc.language_config_display) can be 0 or 1. The language icon will not be displayed on the home screen if the administrator sets misc.language_config_display to 0. The default value of this parameter is '1'.

Access Path

Terminal Menu :

Web Server > Complete Configuration > misc.language_config_display

Figure 20: Hide Language Icon (Sigma)

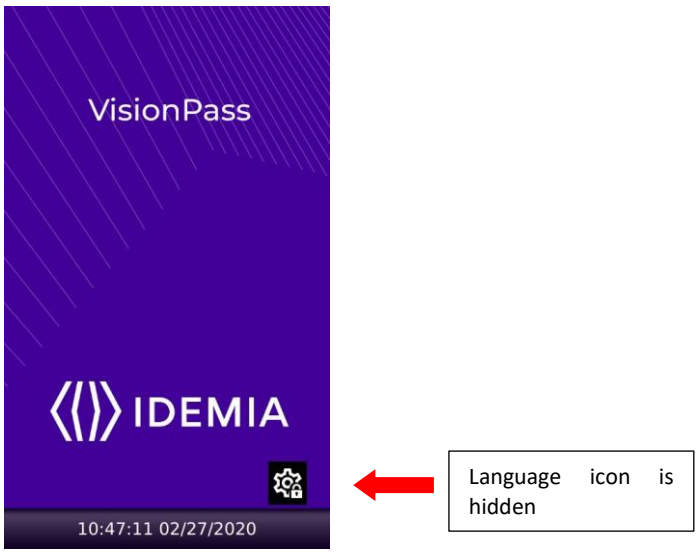


Figure 21: Hide Language Icon (VisionPass)

Ethernet Interface Settings

The administrator can connect the Access and Time Biometric Terminal to other servers and door panels via **Ethernet channel.** Using Ethernet connection, the terminal can make access request to the access controller and receive result messages.

The administrator can configure the terminal to communicate through Ethernet channel by means of the FBA screen or the Network Configuration screen. An administrator can set the IP attribution protocol as DHCP or Static.

- **'Static' mode**: The IP address shall be manually entered by the administrator.
- **'DHCP' mode**: The IP address is assigned automatically.

IP Mode is selected to be 'Static', by default.

Access Path

Terminal Menu :

First Boot Assistant > Network Settings

or

Administration Menu > Communication Menu > Network Interface

NOTE:

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

Terminal can support connection through Ethernet and 3G/GPRS/GSM (if supported) network simultaneously.

NOTE: In Enforced Security configuration, access to First Boot Assistant menu requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

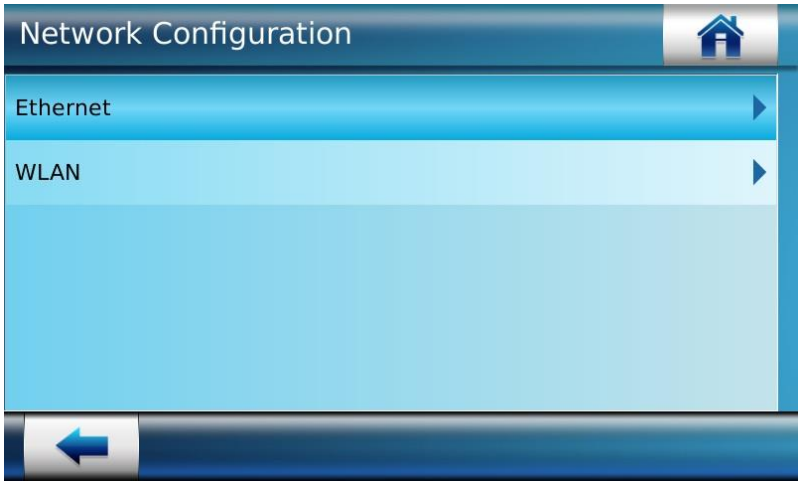


Figure 22: Selecting Ethernet-Network Configuration

1. Select **Ethernet**
2. Select **IP Settings**

Figure 23: Ethernet Configuration

3. select **IPV4** or **IPV6**

Figure 24: IP Mode Selection

4. Select **Static** or **DHCP** for network configuration update
5. For **Static Mode**, The administrator configures manually ‘IP Address’ of the terminal, ‘Subnet Mask’, 'Network Mask', 'Gateway Address' and 'DNS Servers

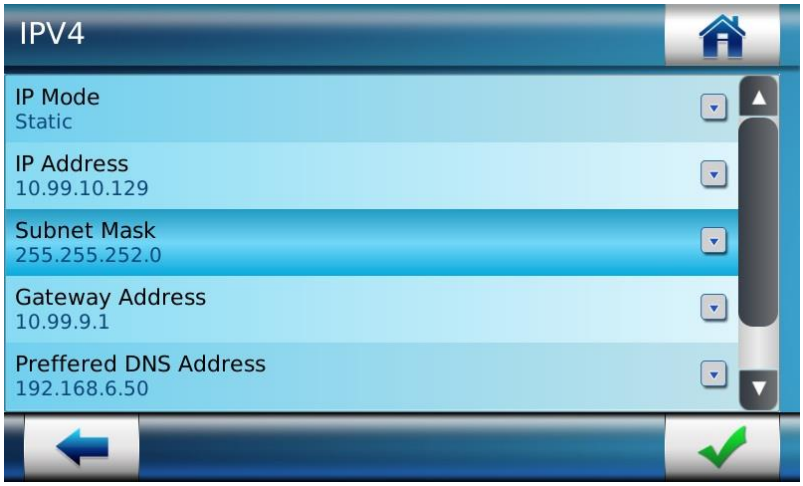


Figure 25: Configuring IP Address under Static IP Mode

For **DHCP Mode**, the‘IP Address’, ‘Subnet Mask’, 'Network Mask', 'Gateway Address' and 'DNS Servers’ of the terminal are automatically assigned.

6. Use Check button “ ” to save the setting

Results

Once the Ethernet Configuration is done, the terminal can be connected to a distant server. An administrator can also configure parameters to prevent unauthorized access to the terminal. These settings can be done from Security menu, refer "*Network & Communication Security Settings*".

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Password Configuration

The administrator can use this function to reset the default login password of the terminal. The administrator can use this password to access the administration menu and perform required configurations. It is highly recommended to change the default login password in order to avoid any unauthorized access to the administration menu of the terminal.

The administrator must change the login password periodically to ensure better security. The administrator can change password anytime from "*Change the LCD* Login Password" under Security Menu.

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

Access Path

Terminal Menu :

First Boot Assistant> Password Settings

or

Administration Menu > Security Menu > Change the LCD login Password

NOTE: In Enforced Security configuration, access to First Boot Assistant and Security Menu menu requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Webserver (not available In Enforced Security configuration, and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Welcome Admin > Change password

Screens & Steps

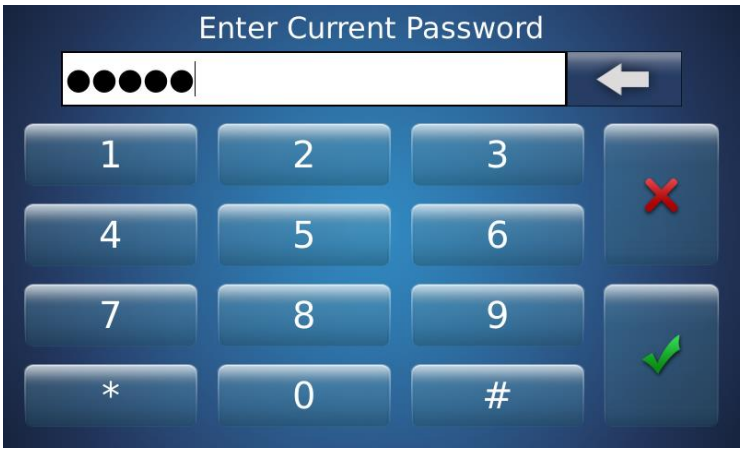


Figure 26: Resetting Device Password

1. Enter the **Current Password** and use “ ” button to move on next screen.

   By default, the login password of the terminal is set as “12345”

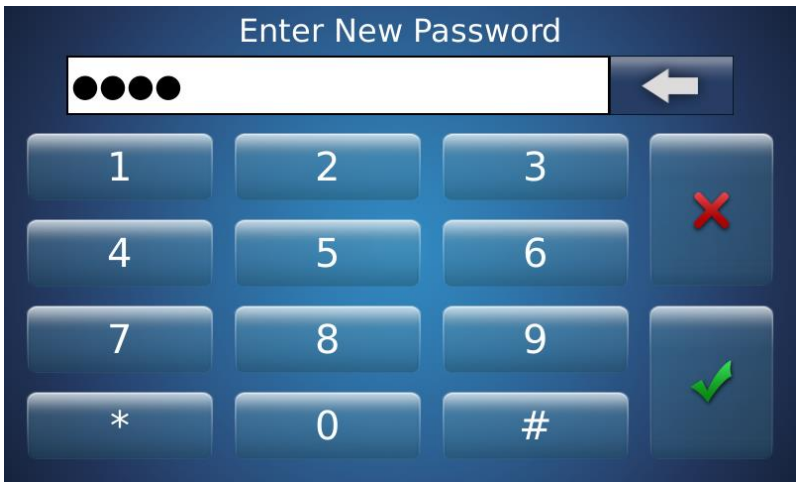


Figure 27: Entering New Password

2. Enter a **New Password** of your choice.
3. Use “ ” button to move on next screen

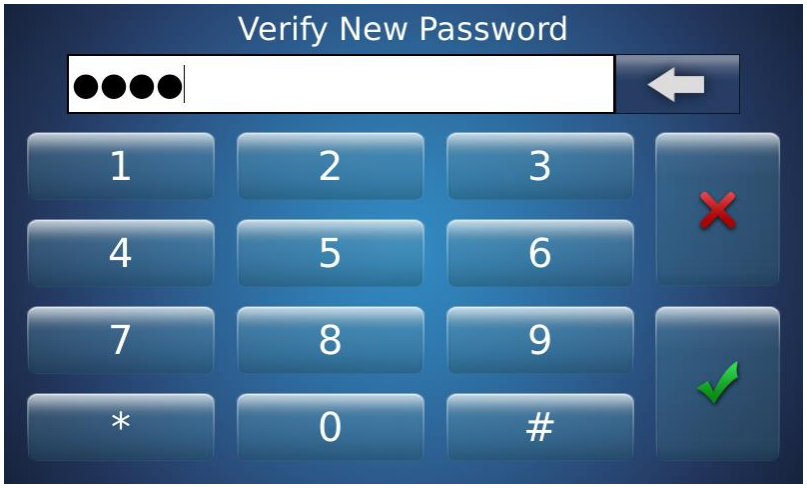


Figure 28: Verifying New Password

4. Re-enter the **New Password** for verification
5. Use “ ” button to **Save**

Results

The administration menu of the terminal can be accessed now by entering the new password.

First Boot Assistance At Next Boot Configuration

The configuration defined with the First Boot Assistant, can be either permanent or temporary. This is specified by the "First Boot Configuration Storage Type" parameter as described below:

- **ON**: At the next startup of the terminal, the First Boot Assistant (FBA) screen will be displayed with the configurations stored. The administrator can change the required parameters.
- **OFF**: At the next startup of the terminal, the First Boot Assistant (FBA) screen will not be displayed and the configurations stored previously will continue to apply.

Access Path

Terminal Menu :

First Boot Assistant> Boot Assistant At next Boot

or

Administration Menu > System Menu > First Boot Assistant> Boot Assistant At next Boot

NOTE: In Enforced Security configuration, access to First Boot Assistant and System menu requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Webserver (not available In Enforced Security configuration, and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

System Menu > First Boot Assistant > First Boot Assistance At Next Boot

Screens & Steps

Figure 29: First Boot Assistance At Next Boot

1. Select ON or OFF

2. Use Check button “ ” to save the setting

Results

The preferred value of “First Boot Assistant At Next Boot” is saved. The terminal will display FBA menu, based on the value this parameter.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Recover Corrupted Components

There is a mechanism in the terminal to recover corrupted data such as Smartcard Keys, Terminal Password, SSL Certificate, User Database, Transaction logs Database. This could have been corrupted in the event of a power failure or interrupt in ongoing operation. When booting up the terminal device, if corruption is detected in any of these data security components, the following message will be displayed on the screen.

Figure 30: Protected Data Corrupted Error

The administrator can view the list of corrupted components by clicking on “ ”. This has been illustrated in the snapshot below

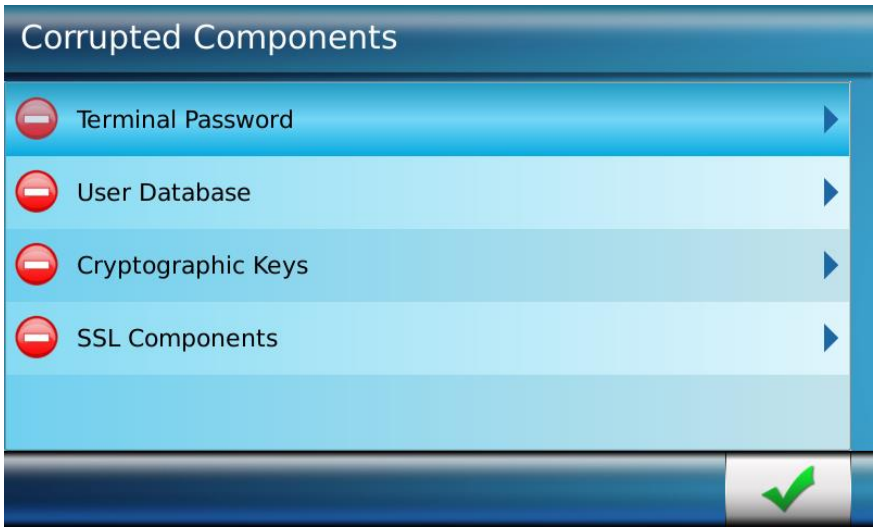


Figure 31: Corrupted Components

The corrupted components will restore to default values when select “ ”.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

NOTE: For VisionPass Range terminals, the configuration database will be automatically recovered if this database is considered as corrupted at the terminal boot. All configuration keys will be reset to the default value and no event will be reported to the administrator.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access to Administration Menu

The administration menu allows user to perform various actions and configurations on the terminal, through the categories of menu listed below. This section is about configurations that can be done via the terminal menu for almost Access and Time Biometric Terminals with LCD.

- **User Menu**: For enrolling and managing users
- **Multimedia Menu**: For uploading and managing Audio, Video and Images in the terminal
- **System Menu:** Allows configuration of the Terminal, Transaction Log and perform miscellaneous configurations.
- **Communication Menu**: For setting network interface and serial parameters.
- **Security Menu**: Allows the administrator to configure Biometric, Communication, Multi-user verification, LCD password change and additional user control
- **Reboot Menu:** allows the administrator to reboot the terminal.
- **USB Menu**: Allows to initialize USB Key, to format USB key, to import DATA into Terminal to USB key and to export DATA in USB key.
- **Information Menu:** Used for viewing information about terminal.

NOTE: In Enforced Security configuration, full access to Administration menu requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Access Path

Terminal Menu :

Home Screen

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

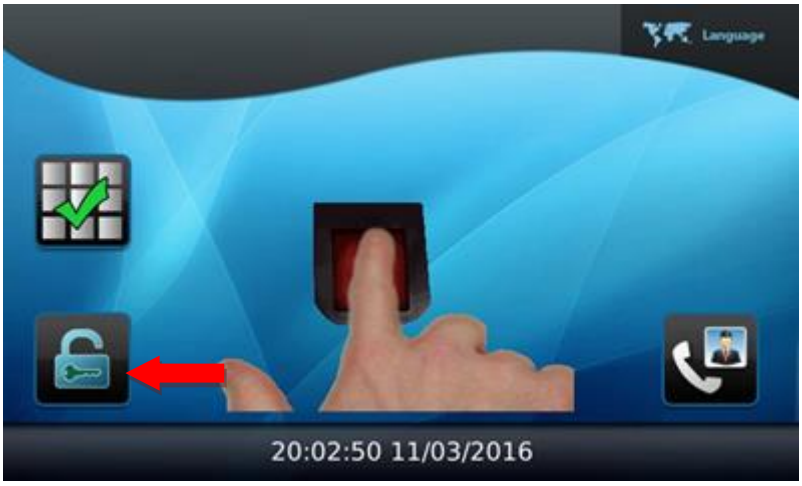


Figure 32: Logging in Device (Sigma)

Figure 33: Logging in Device (VisionPass)

1. Press on **key lock** icon

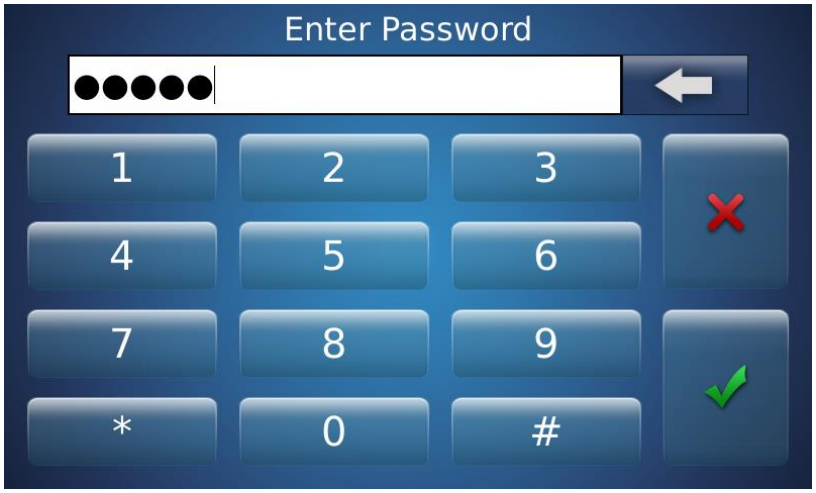


Figure 34: Entering Password

2. Enter **Password** and Press on validation button

NB Identification policy depends of misc.LCD_login_optionvalue :

0 - Password only *(**0** - Default)*
1 - ID + Password
2 - ID + BIO + Password
3 - ID + BIO

Figure 35: Administrator Menu

3. On successful login, The administration menu is displayed along with the various sub menus

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

User Menu

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

The administrator can only access this menu if enrolled with either Full Administrator Rights or Database Administrator Rights or Limited Database Administrator Rights and a biometric control is requested (the configuration key misc.LCD_login_option must be set to the values 2 or 3).

Figure 36: User Management Menu

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

User Enrollment in Database

By using this feature of Access and Time Biometric Terminal, the administrator can enroll new users in the terminal. The user information such as name, biometric data, User ID and PIN, access rights, etc. can be entered and stored in the terminal database.

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

Access Path

Terminal Menu :

User Menu > Add/Enroll User > DB Only

WebServer (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

User Management > User Enrollment > Enrollment mode > DB Only

Pre-requisites

Only an Administrator with 'Full Admin Rights' or 'Database Admin Rights' or 'Limited Database Admin Rights' can enroll new users

Screens & Steps

Figure 37: Entering User Identifier

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

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

- 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**.**

2. Press on “ ” button to save

Figure 38: Adding user information

3. Under **Enrolment Information** screen, an administrator needs to enter several parameters:

Figure 39: Enter First Name of User

4. First Name of user and Press on “ ” button to move to the next screen.

5. Similarly, on next screen, Enter **Last Name** of user and Press on “ ” button to move to the next screen.

6. When using MASigma or Fingerscan, press on **Capture Fingers** to enroll fingerprints of the user

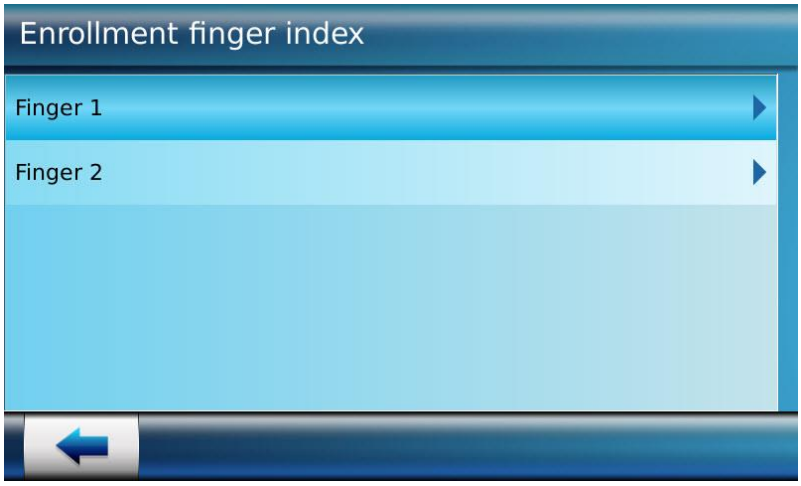


Figure 40: Enrolling Finger Index

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

Figure 41: Select first finger to capture

b. Select finger for biometric data capture

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

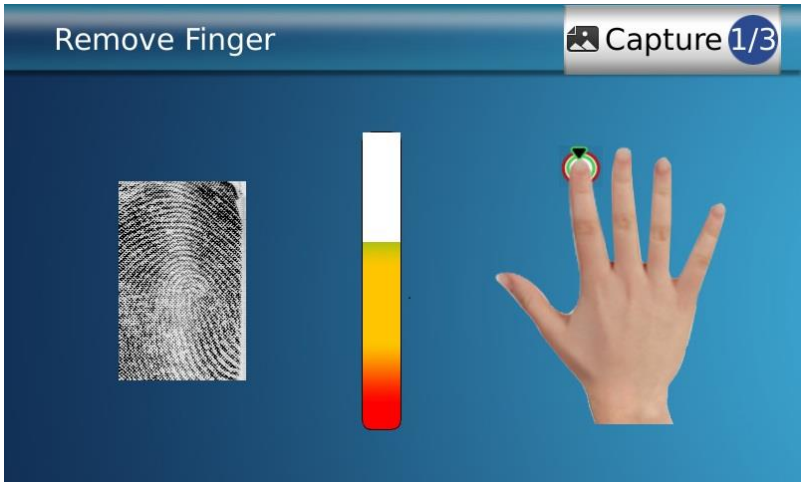


Figure 42: Biometric data capture

c. Place user's finger on **biometric Sensor**. If finger is not placed properly or within the time limit, an error message is displayed. Refer to "*SIGMA Range Series* Finger Placement Recommendation" section to know the correct position of finger.

d. Fingerprint is captured three times and the best quality image is auto-selected by the terminal

e. Once the fingerprint is stored, the administrator will be redirected to enrolment finger index screen, wherein the second finger should be selected for capture, The administrator needs to repeat steps 8 to 10 for enrolling finger 2

Figure 43: Set Duress Finger as ON

7. When using Morpho*Wave* Compact or Morpho*Wave* XP2, press on **Capture Hands** to enroll fingerprints of the user

Figure 44: Right Hand Enrolment

a. Select missing or bandaged fingers and validate

Figure 45: Wave hand

b. User swipes his hand. If it is not done properly or within the time limit, an error message is displayed.

c. Fingerprints are captured three times and the best quality image is auto-selected by the terminal

d. Once fingerprints are stored, left hand capture screen will be automatically displayed

8. When using VisionPass Range terminals, press on **Capture Face** to enroll face of the user

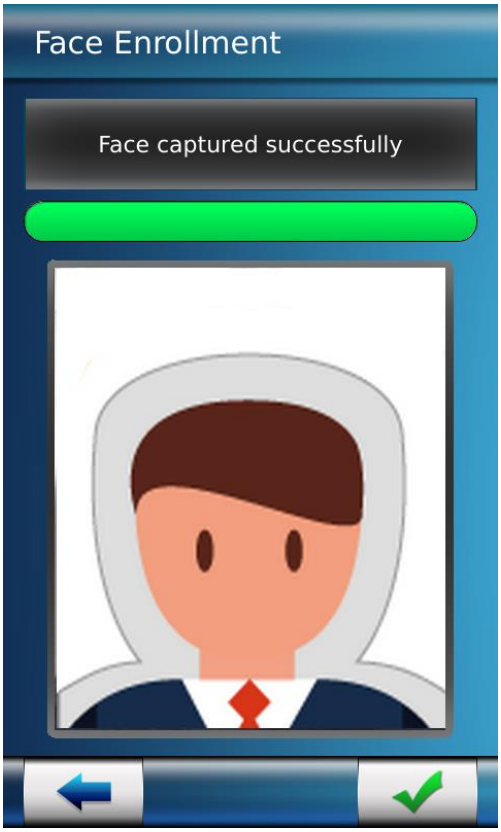


Figure 46: Face Enrollment

Before the start of the biometric acquisition, the user shall be correctly positioned in front of the terminal. Some position messages are displayed on the top of the screen to help the user to have the correct position.

As soon as his position is correct, the following message : “Don’t move” is displayed on the screen, the biometric acquisition is started and the bargraph is updated (it increases). During the acquisition, the user should not move.

The live feedback is displayed on the screen during the enrolment and it is replaced with the RGB user picture when the enrolment is finished.

9. Once the administrator completes capturing standard biometric data, an option for capturing **Duress Finger** is enabled, when using MASigma.

10. The administrator needs to select **ON** if it is required to capture duress finger. Follow steps 8 to 10, for enrolling duress finger

Figure 47: Assigning Access Rights

11. **Admin Rights** enables the administrator to select the 'rights' that can be given to the user.
    a. **No Administrator Rights:** The user is a regular user who has no right to access administration menu or modify the terminal configuration.Regular users can only use the terminal for requests of Access and/or Time & Attendance.
    b. **Database Admin:** The user is an administrator with database administration rights.He or She is capable of accessing User menu and performing all available actions in the User menu, except for **Update Admin Rights** operation.
    c. **Full Admin:** The user is an administrator with full Admin Rights. He or she can access all the menus in the administration menu and perform operations. An administrator with full Admin Rights can enroll regular users, as well as administrators.
    d. **Limited Database Admin:** The user is an administrator with limited database administration rights. He or she is capable of accessing User menu and performing all available actions in the User menu, except for **Edit User**, **Delete User or Update Admin Rights** operation.

The following tables sum up available features according to the administrator profile :

- User related features

Profile	User Menu					
	Add	Edit	Delete	Authenticate	Card manager	Update admin rights
No Admin right	✗	✗	✗	✗	✗	✗
Limited Database Admin	✓	✗	✗	✓	✓	✗
Database Admin	✓	✓	✓	✓	✓	✗
Full Admin	✓	✓	✓	✓	✓	✓

- USB related features

Profile	USB Menu								
	Initialize	Format	Import			Export			
			User Database	Contactless Key	Language	Transaction Log	Error log	User Database	Contactless key
No Admin right	✗	✗	✗	✗	✗	✗	✗	✗	✗
Limited Database Admin	✗	✗	✗	✗	✗	✗	✗	✗	✗
Database Admin	✗	✗	✗	✗	✗	✗	✗	✗	✗
Full Admin	✓	✓	✓	✓	✓	✓	✓	✓	✓

- Others features

Profile	Multimedia Menu	System Menu	Communication Menu	Security Menu	Reboot	Information Menu
No Admin right	✗	✗	✗	✗	✗	✓
Limited Database Admin	✗	✗	✗	✗	✗	✓
Database Admin	✗	✗	✗	✗	✗	✓
Full Admin	✓	✓	✓	✓	✓	✓

12. **Press** on “ ” to save setting

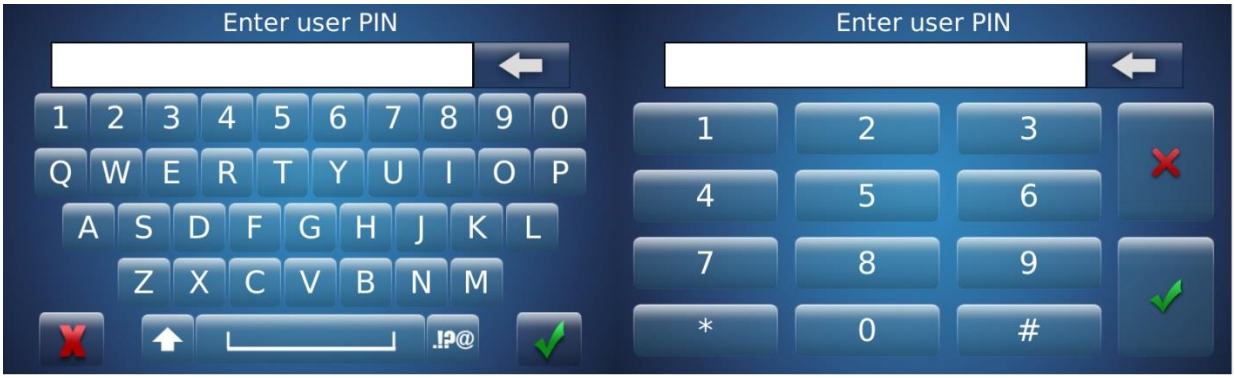


Figure 48: Enter User PIN – Alphanumeric/Numeric

13. The administrator has to enter **User PIN** which can be either numeric or alphanumeric based the *LCD_configuration.PIN_keypad_type*. Default value of this parameter is 1 which enables Numeric keypad for User PIN. On setting value to 0, terminal will enable Alphanumeric Keypad. The value will be of up to 15 digits alphanumeric/numeric. This PIN can be used by user, when PIN based authentication mode is enabled. The user will be required to enter PIN along with biometric check, for authentication.
14. Press on " " to save setting

Figure 49: Setting Job Code

15. The administrator can set a Job Code in a user profile. On access request, user has to enter job code along with biometric check and PIN. Only on successful authentication of the user, the access is granted. Press on **Job Code**

NOTE:

1. The administrator can enable the Job Code as a parameter for authentication. This can be done from the Biometric Security tab.
2. When the Time and Attendance mode is enabled, entering job code during authentication is optional despite the Job Code Check being enabled. It is based on the value of parameter *time_and_attendance.jobcode_by_key* and selected time and attendance key during authentication.

Figure 50: Setting Job Code in user profile

16. The list of Job Codes configured in terminal is displayed. An administrator can select a job code to associate with the profile.

NOTE: The Job Codes are configured in terminal using **MorphoBioToolbox**, Webserver or distant command.

17. Press on “ ” to save setting

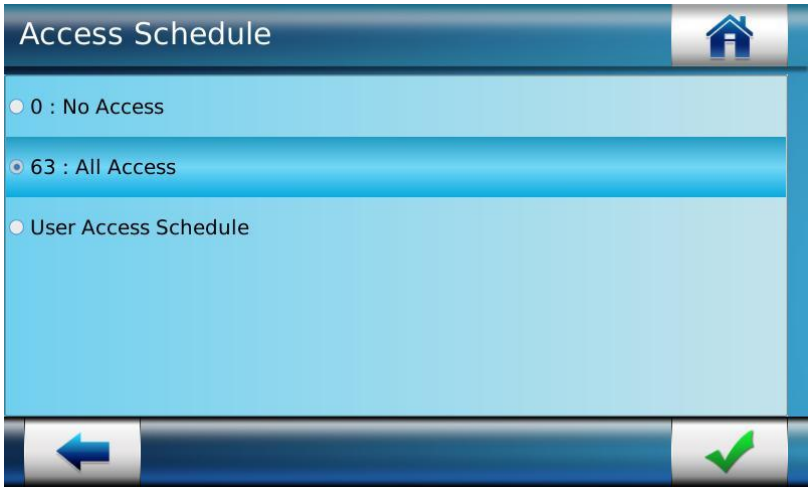


Figure 51: Assigning Access Schedule

18. The administrator can select an **Access Schedule**, if the access is to be allowed within a particular time period of the day. By default, the access schedule is selected as Schedule 63 which means access is allowed at any time of the day.

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

19. Press on "" to save

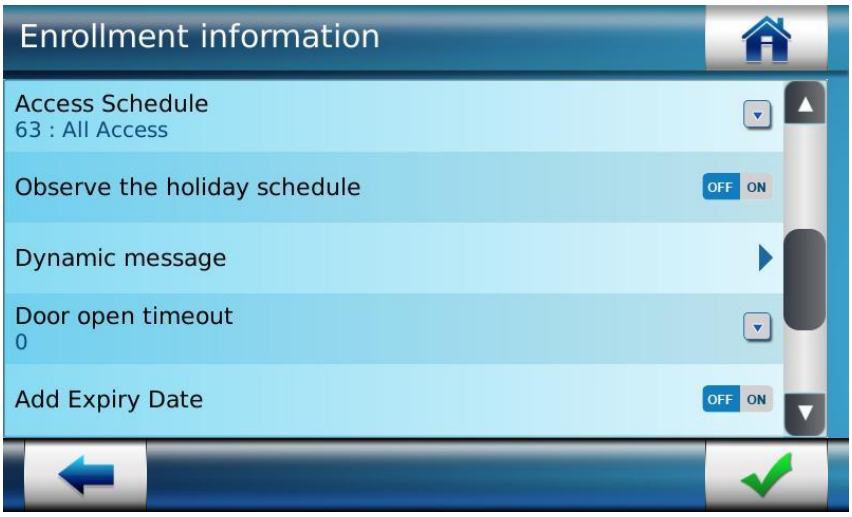


Figure 52: Enrolment Information Screen – Configuring parameters

20. The administrator can configure the **Observe Holiday Schedule** as ON or OFF. If this parameter is set as ON, then access on a holiday will be provided as per the defined holiday schedule. If this parameter is set as OFF, 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.

21. The administrator can select **Dynamic Message** as OFF or ON. Dynamic Message can include images or plain text. This message can be different for each user. This dynamic message will be displayed on the LCD screen on the occurrence of one or more user control events defined by "**dynamic_message.mode**" parameter. Please refer to **Parameters Guide** document for more details about this parameter. This dynamic mode configuration can also be done through Webserver (refer section **Erreur ! Source du renvoi introuvable.**).

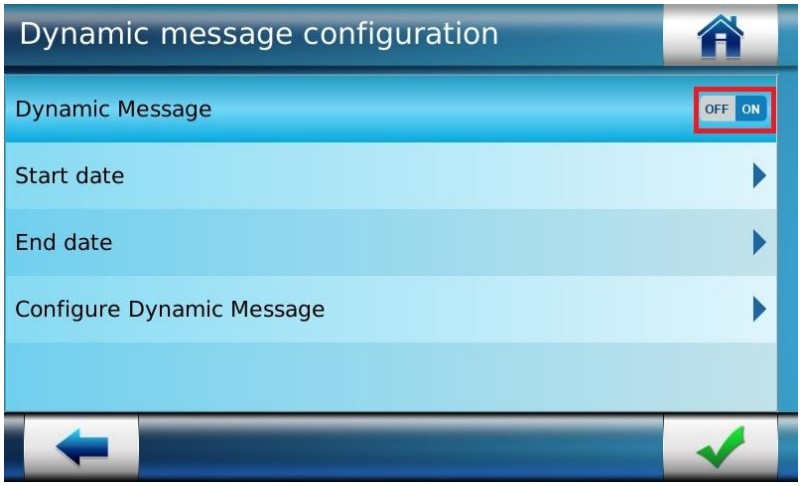


Figure 53: Configuring Dynamic Message for User

22. Set **Dynamic Message** as On

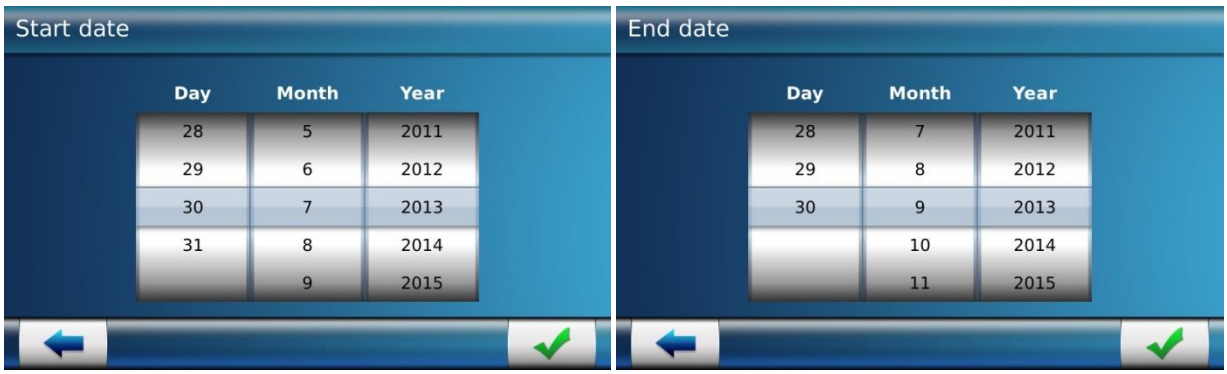


Figure 54: Setting duration for dynamic message

23. Select the duration for which the Dynamic Message is to be displayed on LCD screen by selecting the **Start Date and End Date**
24. Press on "✓" to save

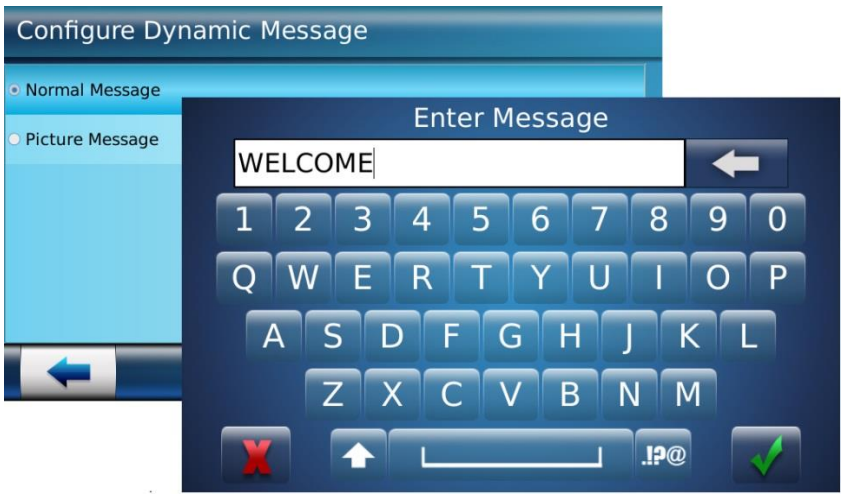


Figure 55: Configuring Dynamic Message for User

25. The administrator can select the type of dynamic message as "**Normal**" or a "**Picture Message**"
    a. If Normal Message is selected, then on the next screen the message to be displayed, needs to be entered by the administrator. Press on " " icon to save message
    b. If Picture Message is selected, then the image uploaded in Multimedia Menu > Images will be displayed on terminal LCD screen every time when access is granted to the user.

NOTE: Refer to "*Images Settings*" section in this document to know how the dynamic message can be uploaded.

26. Press on " " to save

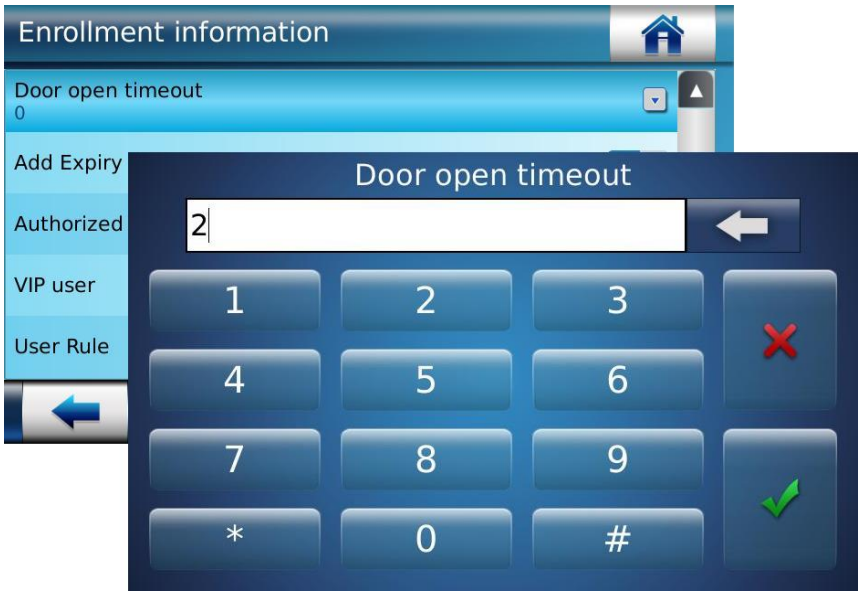


Figure 56: Configuring Door Open Time Out

27. The administrator can configure **Door Open Time Out** in seconds. The door stays open for the time duration defined here.

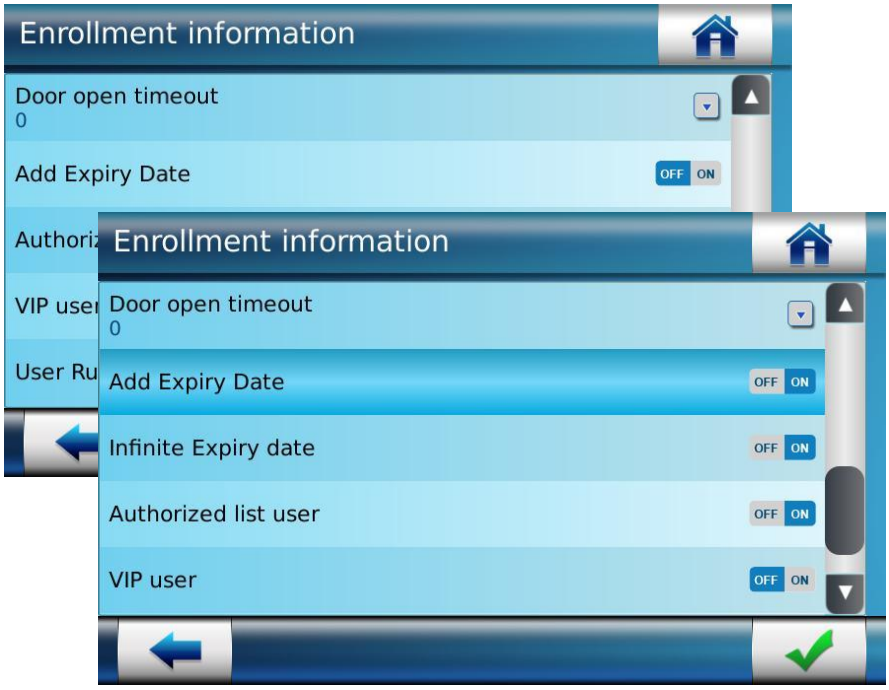


Figure 57: Enrolment Information Screen

28. The administrator can configure **Add Expiry Date** as ON or OFF. If **Add Expiry Date** is ON, then administrator can configure the user account expiry date parameter. This parameter indicates whether user account is active for specific duration or will remain active forever.
    a. To apply Infinite Expiry Date, select **Infinite Expiry Date** as ON.
    b. To apply specific Expiry Date, select **Infinite Expiry Date** as OFF and select **Expiry Date**
29. The administrator can configure **Authorized List User** as ON or OFF. Only if the user is in the Authorized list, access will be granted. This parameter is set as ON, by default.

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

30. The administrator can configure **VIP User** as ON or OFF. If the user is enrolled as a VIP user, then at the time of authentication, the terminal will not ask for biometric or PIN or BIOPIN (BIOPIN is not supported by VisionPass Range terminals).

31. The administrator can configure **User Rule**. This configuration panel allows the administrator to modify the general authentication rules that are applied to all users, into user specific settings.

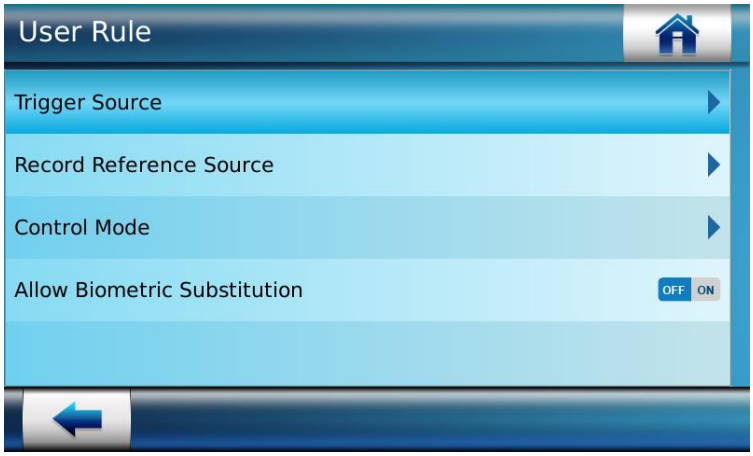


Figure 58: Defining User Rule

32. The User Rule settings includes below parameters:

Figure 59: Defining User Rule – Trigger Source

33. **Trigger Source**: The administrator can configure which of the following triggers the terminal for the access.
    a. Set **Biometric** as ON, if the administrator wants to allow user to access by biometric identification. If trigger event through biometric is OFF, then user cannot initiate the access rights check using biometry. And Biometric Check will be bypass for the particular user.
    b. Set **Contactless Card** as ON, if the administrator wants to allow the user to request access by presenting card authentication

c. Set **Keypad** as ON, if the administrator wants to allow the user to request access by entering User ID and PIN using keypad. The authentication is done by matching provided PIN with the stored data of the same user.

d. Set **External Port** as ON, if the administrator wants to allow the user to request access by providing his User ID through External port

e. Set **QR Code** as ON, if the administrator wants to allow the user to request access by providing a QR Code instead of the hand.

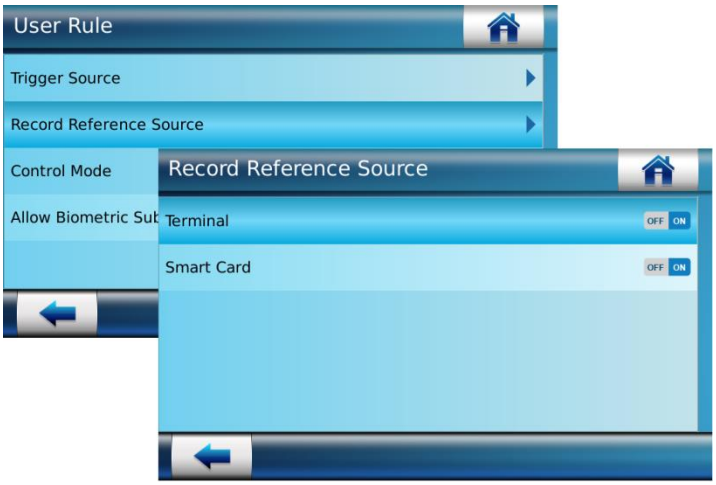


Figure 60: Defining User Rule – Record Reference Source

34. The administrator can configure whether user's information should be looked up in the Terminal database and/or on the Smartcard using **Record Reference Source**

    a. Select **Terminal** as ON, if it is required for the terminal to look up the user's profile in database

    b. Select **Smartcard** as ON, if it is required for the terminal to look up the user's profile in smartcard

Figure 61: Defining User Rule – Control Mode

35. The administrator can set the following parameters under Control Mode
    a. **PIN** mode as ON, if PIN based authentication is required
    b. **Biometric** as ON, if Biometric authentication is required
    c. **Time and Attendance** as ON, if T&A based authentication is required
    d. **Job Code** as ON, if job code based authentication is required

Figure 62: Defining Control Mode - Face Detection Mode

e. **Face Detection Mode:** (SIGMA Ranges only) The administrator can configure face authentication check rule as depicted in the snapshot above. Please refer to "*Additional User Control Settings"* to understand Face Detection workflow.

36. The administrator can set **Allow Bio Substitution** parameter as ON. It indicates that instead of Biometric, the user can be authenticated through a substitute such as BIO-PIN

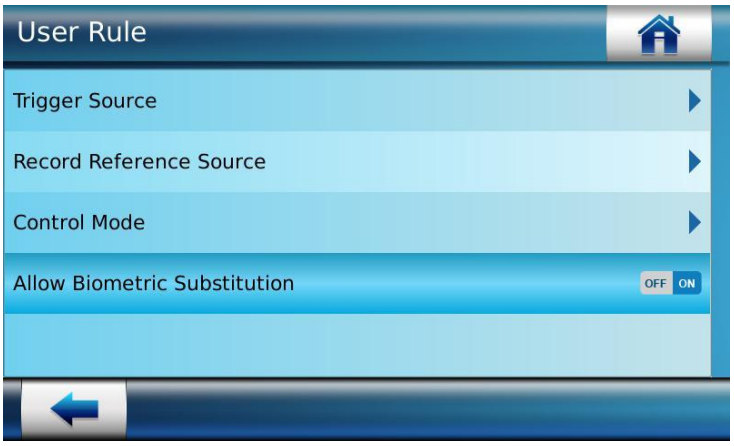


Figure 63: Defining User Rule – Biometric Substitution

37. Press on " " to **Save** user information

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 biometry, terminal will match the biometric capture with the records stored in the database and allow access on successful identification.

Recommendation: In case of authentication failure due to bad biometrics, the administrator can re-enroll the user.

User Enrolment in Card

The administrator can encode a contactless smartcard for a user, using this functionality. 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 user card.

Access Path

Terminal Menu :

User Menu > Add/Enroll User > Card Only

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

User Management > User Enrollment > Enrollment Mode > Card Only

Note: The face capture is not available in Webserver page for VisionPass Range terminals

Pre-requisites

Only an Administrator with 'Full Admin Rights' or 'Database Admin Rights' or 'Limited Database Admin Rights' can enroll new users

User name and first name stored in cards are limited to 20 characters. By consequence even if user name and first name until 40 characters are authorized for local enrolment, encoding card will be not possible if they are longer than 20 characters.

Screens & Steps

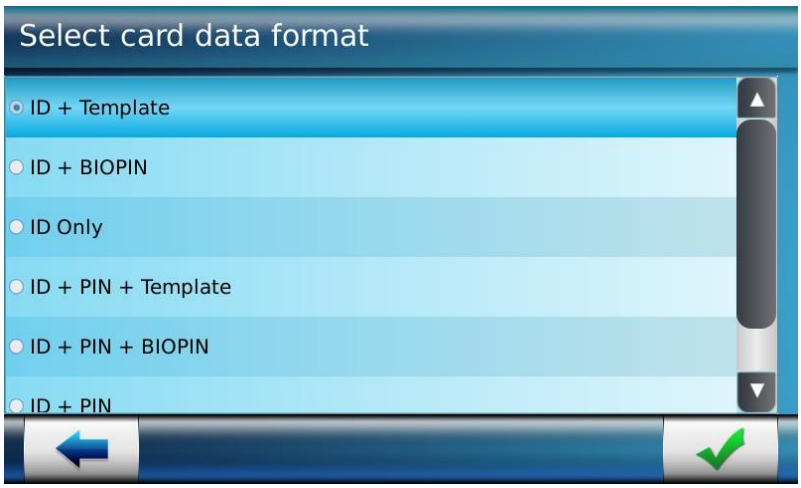


Figure 64: Select Card Data Format

1. The administrator can use the Card Data Format to select the data that will be used for user authentication. Following are the options available:
   a. **ID + Template:** When the administrator selects this format, it implies that the user authentication is done by verifying the User ID and biometric template.

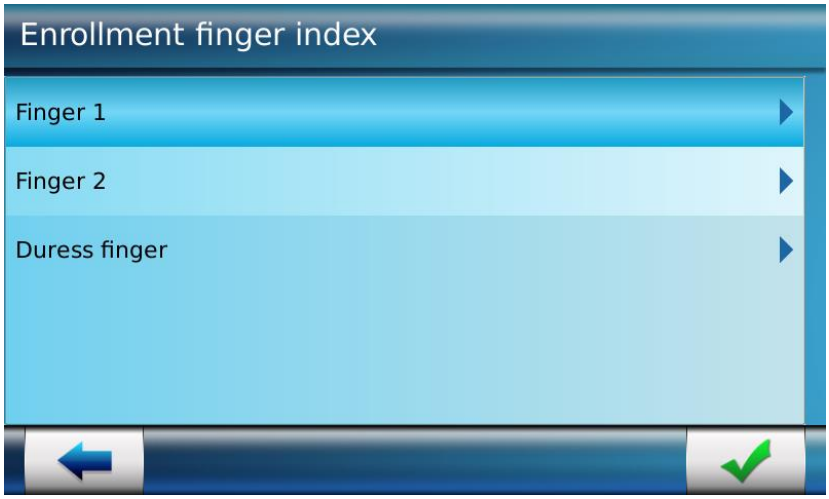


Figure 65: Enrollment Finger Index in Card

   b. **ID + BIOPIN:** When the administrator selects this format, it implies that the user authentication is done by verifying the User ID and BIOPIN (i.e. PIN that is used in place of biometric data)

      Note: this Card Data Format is not supported by VisionPass Range terminals

   c. **ID Only:** When the administrator selects this format, it implies that the user authentication is done by verifying the User ID
   d. **ID + PIN + Template:** When the administrator selects this format, it implies that the user authentication is done by verifying the User ID, PIN, and Biometric Template
   e. **ID + PIN + BIOPIN:** When the administrator selects this format, it implies that the user authentication is done by verifying the User ID, PIN, and BIOPIN
2. **Note:** this Card Data Format is not supported by VisionPass Range terminals
   a. **ID + PIN:** When the administrator selects this format, it implies 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 screens are for ID + Template format
3. Please refer steps 1 to 11 of section "*User Enrolment in Database*"
4. A message to place card at terminal is displayed.

5. **Place Smartcard** 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 for Access and Time Biometric terminals
- biometric/pin for VisionPass Range terminals

Note: The user’s data stored on card are not editable or viewable.

User Enrolment in Card & Database

An administrator can use this functionality to enroll a new user and store the user data in a contactless smartcard as well as in the database of the terminal. As some information cannot be stored on card (ex :holiday schedule), this enrollment type allows first the checking of the user data available on the card and then complementary checking of user data available on the terminal. In addition, the administrator can configure whether user's information should be looked up in the Terminal database and/or on the Smartcard using User Rules setting

Access Path

Terminal Menu :

User Menu > Add/Enroll User > Card + DB

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

User Management > User Enrollment > Enrollment Mode > Db+Card

NOTE: The face capture is not available in Webserver page for VisionPass Range terminals

Pre-requisites

Only an Administrator with 'Full Admin Rights' or 'Database Admin Rights' or 'Limited Database Admin Rights' can enroll new users

Screens & Steps

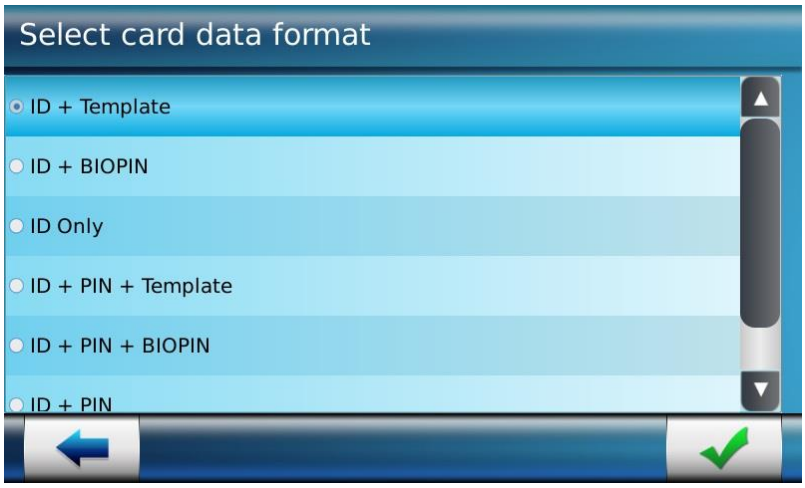


Figure 66: Select Card Data Format

1. The administrator can select the user data that is required for access rights check, by means of Card Data Format. The administrator must select the appropriate user data type and then encode the user's card accordingly.

2. Please refer to "*User Enrolment in Database*" section step # 1 to 40
3. Wait for the message to place card at terminal, to get displayed. **Place Smartcard now**
4. On placing card, the user's data is stored in the card

Results

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

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

Recommendation: If the user authentication has failed due to bad biometric data, the administrator can re-enroll the user.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Update User Information

The administrator can edit user information stored in database, by using this functionality. The administrator cannot update the user information if the user has been enrolled only in the card. However, it is possible to erase and rewrite the user's card with new data.

Access Path

Terminal Menu :

User Menu > Edit User

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

User Management > Users

Screens & Steps

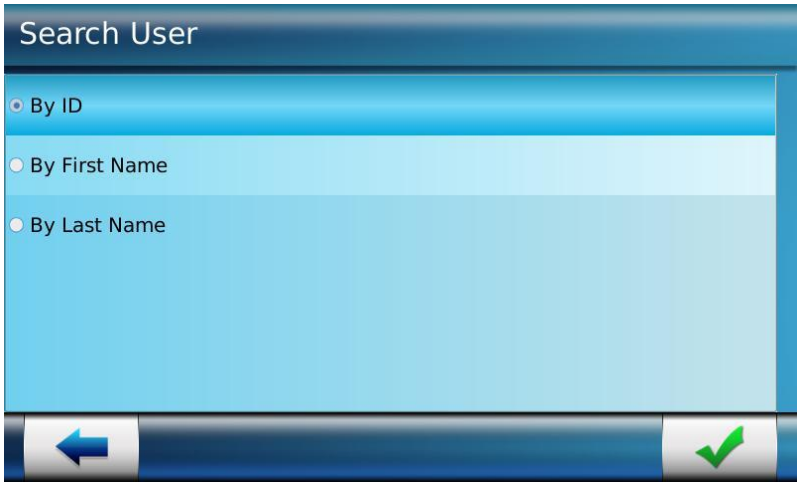


Figure 67: Selecting Search Criteria

1. Select Search User by **ID**, **First Name** or **Last Name**
2. Press on " " button to move on next screen

Figure 68: Entering first digits of the searched User ID

3. Enter the **User ID** of the user account which is required to be edited
4. Press on " " button to move to next screen

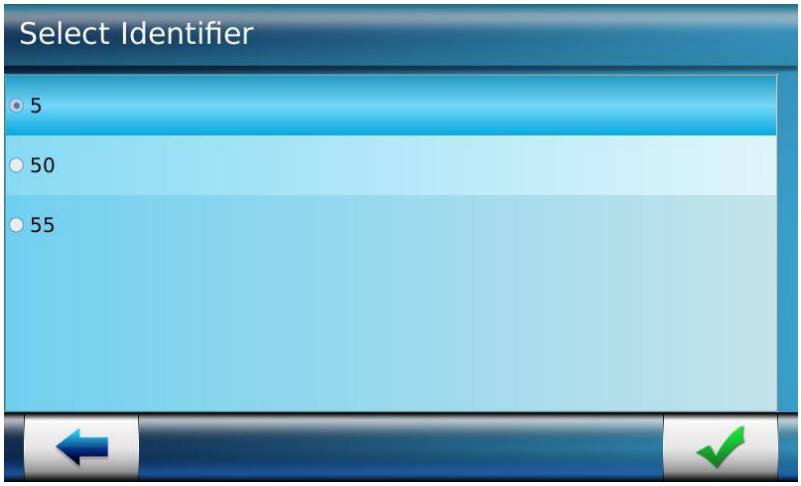


Figure 69: Selecting User ID

5. The list of User IDs matching with the entered id will be displayed. **Select User ID** from the list and Press on " " to proceed.

Figure 70: Enrolment Information screen is displayed for editing

6. Only an Administrator with 'Full Admin Rights' or 'Database Admin Rights' can update the following user details, by means of the Enrolment Information screen as depicted in the above snapshot.
    a. First Name and Last Name of the user
    b. Capture biometry
    c. Update Admin Rights (Only Administrator with 'Full Admin Rights' can update)
    d. Update User Pin
    e. Assign Job Code
    f. Configure Access Schedule
    g. Set Observe Holiday Schedule
    h. Set Dynamic Message
    i. Set Door Open Timeout
    j. Add Expiry Date
    k. Configure Authorized list
    l. Configure VIP User
    m. Configure User Rule
7. Press on " " 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.

Authenticate User (SIGMA Ranges only)

Only an Administrator with 'Full Admin Rights' or 'Database Admin Rights' can authenticate user by using this functionality. This feature can be used by the administrator to test whether the enrolled user is allowed access or not.

However the user can authenticate from the home screen, by entering in User ID and then placing finger when asked.

Access Path

Terminal Menu :

User Menu > Authenticate User

Screens & Steps

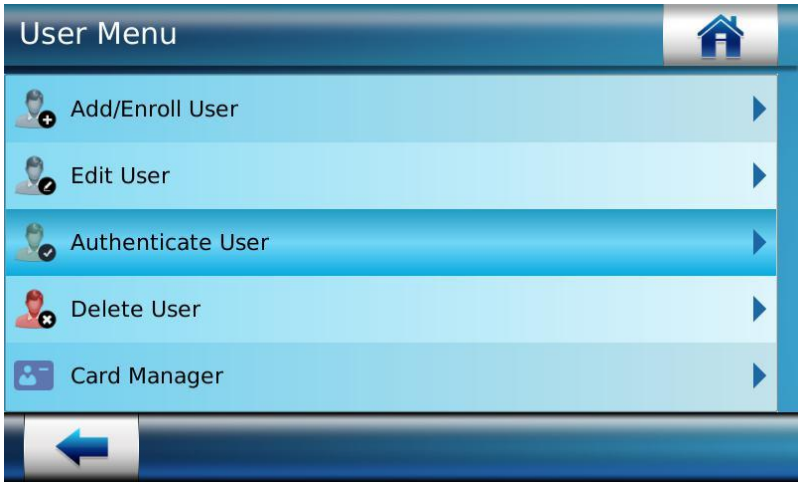


Figure 71: Authenticate User

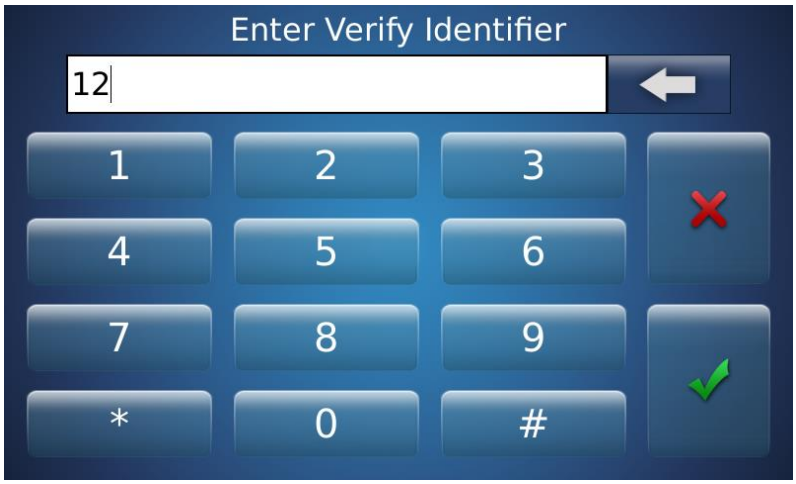


Figure 72: Entering User ID for authentication

1. Enter the **User ID** that is required to be authenticated and Press on “ ” button
2. Terminal will ask user to place finger on biometric sensor

Results

A success message is displayed and user will be granted access on successful authentication. In case authentication is not successful access is denied.

Delete User

Only an Administrator with ‘Full Admin Rights’ or ‘Database Admin Rights’ can delete user information by using this functionality. There are several options for deleting users:

Delete a User

Delete All Users

Delete a User

Access Path

Terminal Menu :

User Menu > Delete User > Delete User

Webserver (not available In Enforced Security configuration and in all configurations for “MorphoWave® SP”, “MorphoWave® XP2” and “VisionPass SP”):

User Management > Users

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

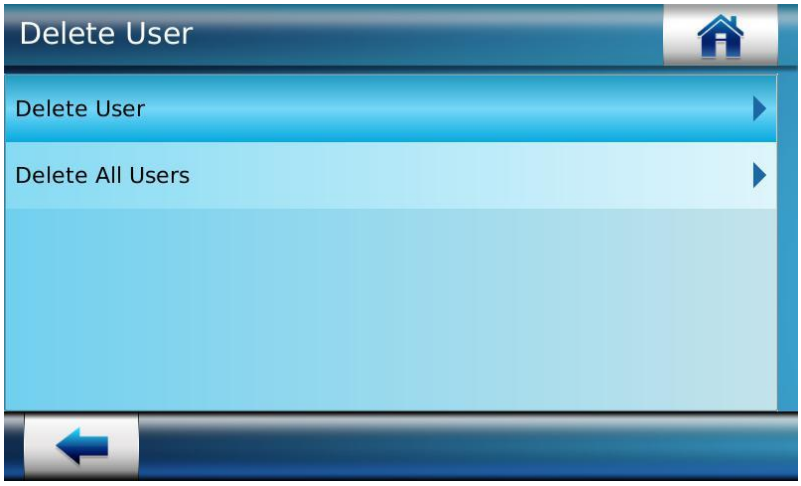


Figure 73: Deleting User

1. If the administrator needs to delete a single user, Select **Delete User**.

Figure 74: Searching User ID

2. The administrator needs to enter the **User ID** that needs to be deleted.

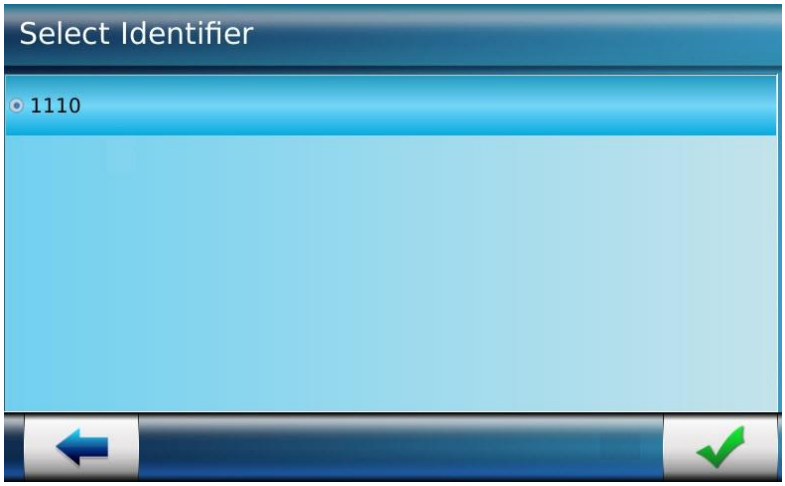


Figure 75: Deleting User ID

3. The list of User IDs matching entered User ID is displayed. Select a User ID
4. Press on “ ” button to move to next screen

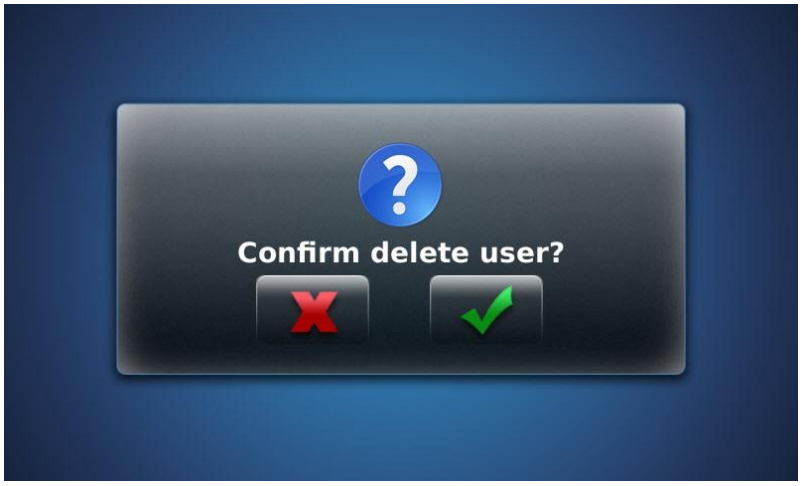


Figure 76: A confirmation message pop up for delete

5. A confirmation message is displayed, asking to confirm the action
6. Press on check “ ” to confirm delete action

Results

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

Delete All User ID

The administrator can use this functionality to delete all the users stored in terminal database.

Access Path

Terminal Menu :

User Menu > Delete User > Delete All Users

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

User Management > Users

Screens & Steps

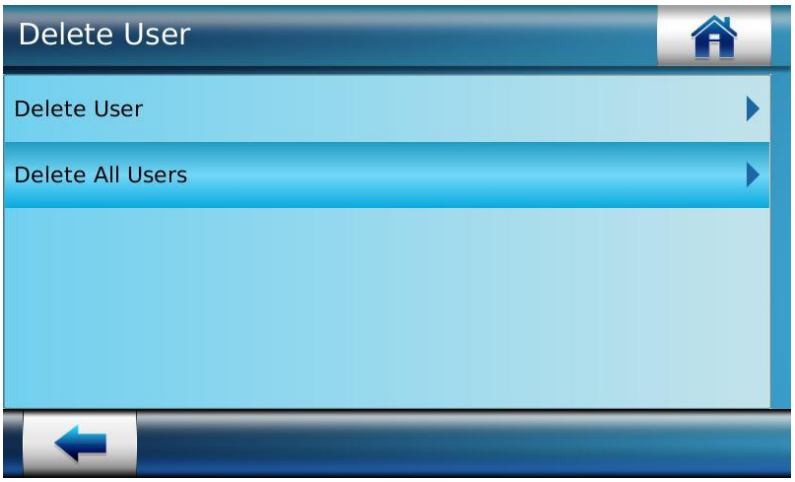


Figure 77: Select Delete action

1. The administrator needs to Select **Delete All Users** to delete all the users in the database

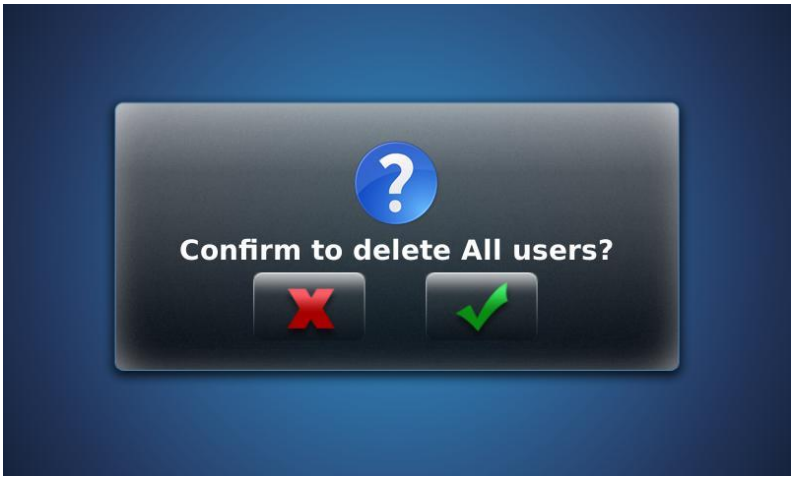


Figure 78: Confirm All User Deletion

2. A confirmation message is displayed, asking the administrator to confirm the action
3. Press on check “ ” to confirm delete all users action
4. A success message is displayed showing all users are deleted

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Card Manager

Access and Time Biometric terminals allow user enrolment and authentication using contactless smartcards. When the administrator enrolls a user on a smartcard, the User Identifier, Biometric Template and PIN/BIOPIN are stored in the card. The terminal will now refer to the information on the card for user authentication if configured to do so.

The administrator can configure the contactless smartcard parameters that are supported by Access and Time Biometric Terminals, by means of the Card Manager Menu.

Access Path

Terminal Menu :

User Menu > Card Manager

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > Contactless Card

The subsequent sections are pertaining to Access and Time Biometric Terminals.

Screens & Steps

Figure 79: Accessing Card Manager

For correct operation, the administrator needs to configure some parameters in the Card Manager tab. These parameters are explained in the subsequent section.

Renew User Card

A smartcard may have an expiry date. Once the smartcard has expired it is not useful for verification. The administrator can renew a contactless card that has expired with the same user data such as User ID, Biometric Template, PIN and BIOPIN that is saved in it. This can be done using the Renewal of User Card functionality. 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 loses 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

Terminal Menu :

User Menu > Card Manager > Renew User Card

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

User Management > Users

Pre-requisites

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

Card is secured with the same key as on terminal

To store fingerprint, user data should contain at least two finger templates, not only one

Screens & Steps

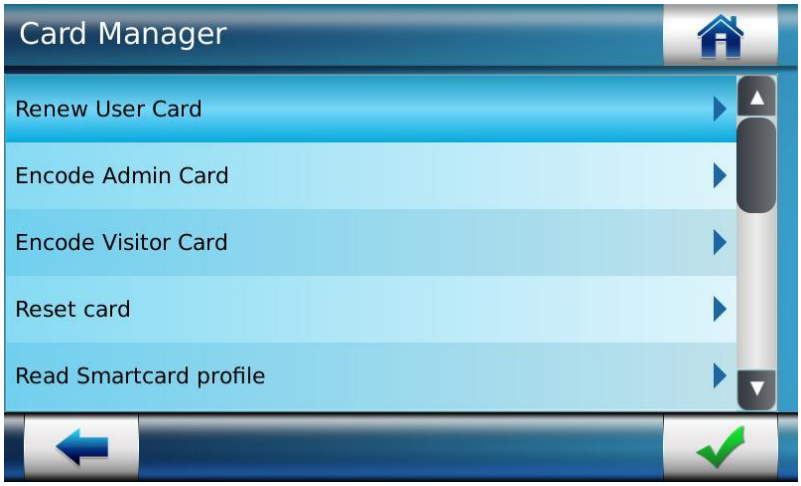


Figure 80: Renewal of User Card

5. Select **Renew User Card**

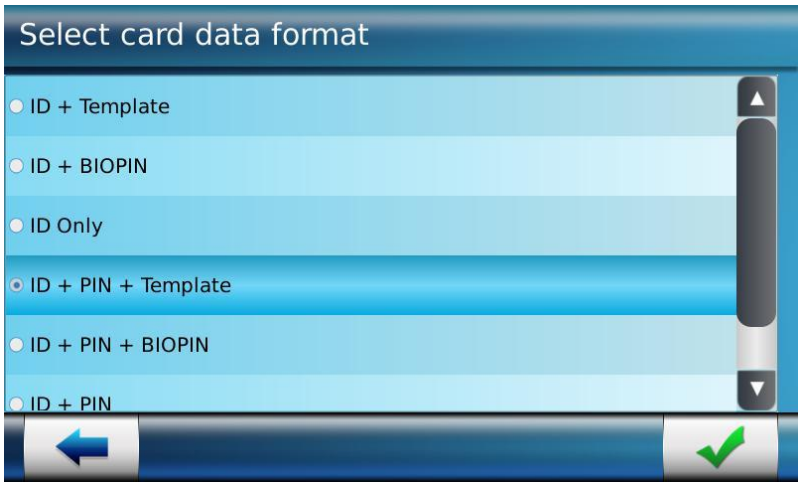


Figure 81: Select Card Data Format

6. Select the card data format from available options as below:
   a. ID + Template
   b. ID + BIOPIN

      NOTE: not supported for VisionPass Range terminals
   c. ID Only
   d. ID + PIN + Template
   e. ID + PIN + BIOPIN

   NOTE: not supported for VisionPass Range terminals
   f. ID + PIN
7. Press on check box to move next

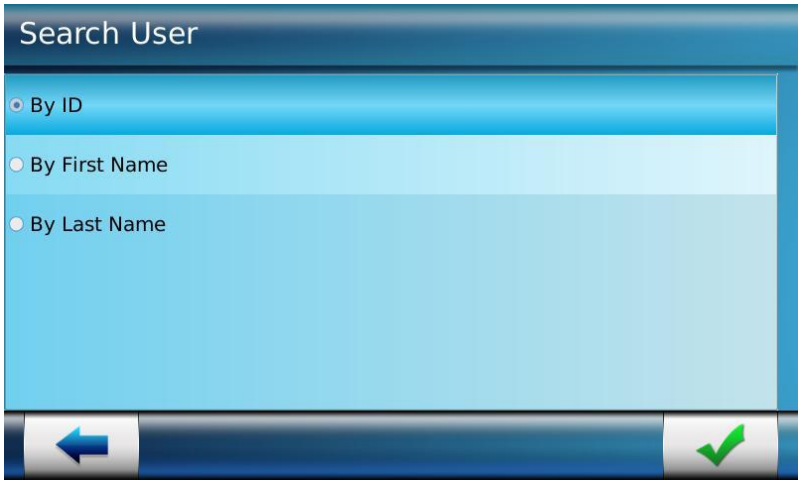


Figure 82: Select search criteria

8. Select criteria to search user by ID, First Name or Last Name
9. Press on check button to move next

Figure 83: Entering User ID to be searched

10. Enter the first characters of the selected search criteria. E.g. if search by User ID is selected, then enter User ID Prefix

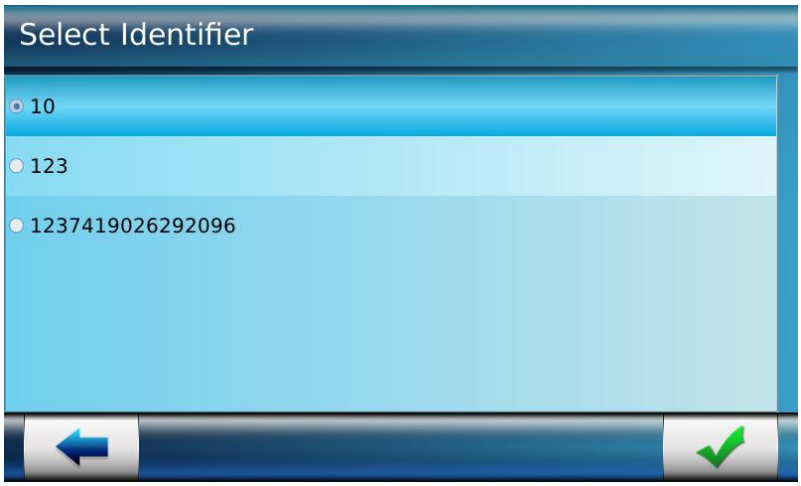


Figure 84: Selecting User ID

11. The list of User IDs matching the first characters entered in search criteria are displayed. The administrator will now have to select a **User ID** that needs to be written to the card.
12. Press on " " to move ahead
13. Terminal will ask for placing the card on card reader. **Place card**

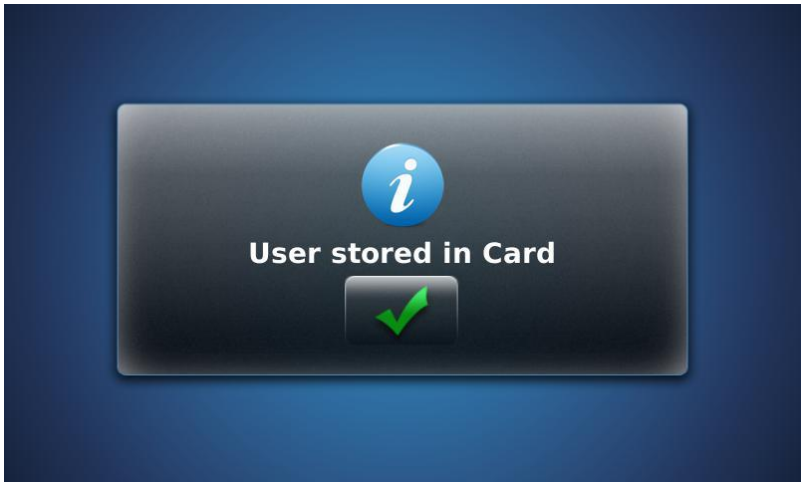


Figure 85: A success message is displayed showing user is stored in card

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.

Encode Administrator Card

When site key in a terminal is changed, it is required to load the same site key in all the terminals in a premises. In such scenario, an Administrator card can be used to change the site key in other terminals.

The administrator can use the Encode Administrator card feature to store contactless site key in the card. This can be copied to other terminals by using the administrator card.

NOTE:

- The administrator can change site key using Administrator card provided the terminal supports the same card type. For example, using MIFARE® Administrator card an administrator can change site key of the terminal that supports MIFARE® card.
- If you are using administration DESFire card to change site key (with begin/start validity date equal to day you used the administration card on the terminal), you could not change them again using distant command.

Access Path

Terminal Menu :

User Menu > Card Manager > Encode Admin Card

Pre-requisites

Card is encoded with terminal's key only, no user data is stored on administrator card

Default start block number is used for reading Administrator card

Screens & Steps

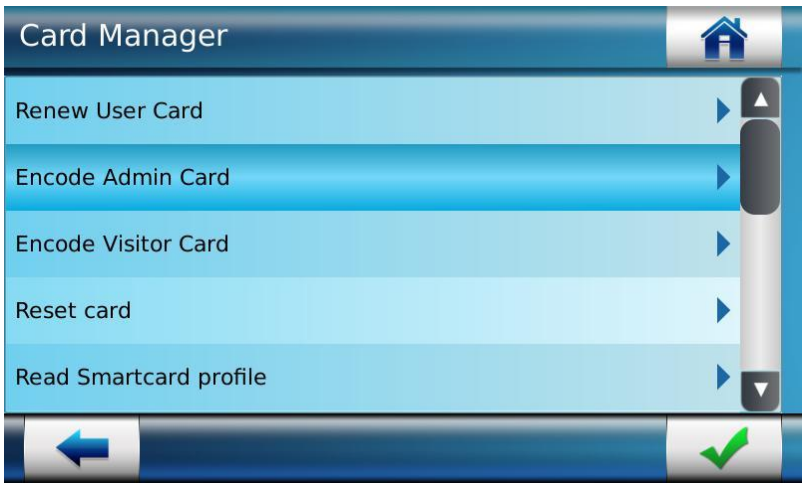


Figure 86: Encoding Administrator card

1. Select **Encode Admin Card**

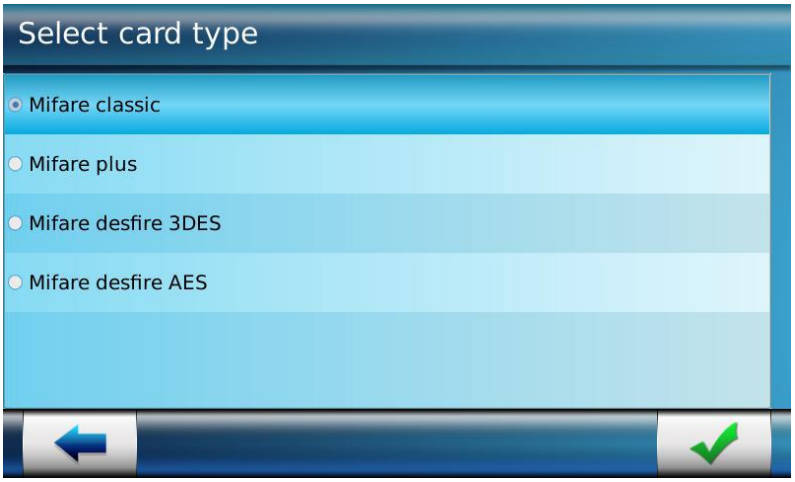


Figure 87: Select Card Type to be encoded

2. Select the **Card Type**, for which site key is to be generated. Options are MIFARE® Classic, MIFARE® Plus, DESFire® 3DES, and DESFire® AES

NOTE:

- The administrator must be careful while encoding MIFARE® 1K Cards. If the number of start block is set as 20 or more, then an error message, i.e., 'Error in Encoding Administrator card' is displayed. Refer to “No. of Start Block for MIFARE® Cards”, to know how to configure the number of start block.

3. Press on “ ” button to save and next
4. The Terminal will ask user to **Place Card** on card reader. Present the selected card type on card reader

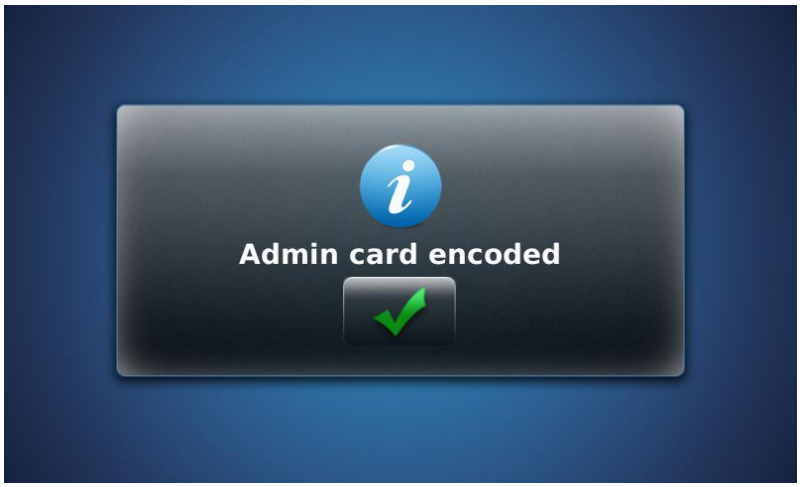


Figure 88: Administrator card is encoded

Results

A success message is displayed showing that the administrator card is encoded. The site key in the terminal is copied in the administrator card. The administrator can change the site key of other terminals using same administrator card.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Encode Visitor Card

Encoding means writing user data, which includes Name, Biometric data, PIN or BIOPIN; on contactless smartcards. Cards for normal users as well as visitors can be encoded.

The administrator can encode a contactless card for a visitor by means of this functionality. Basically, such a card is for a guest user who needs to enter the premises temporarily. For a visitor card, the Terminal does not require information such as Name, Biometric data, PIN or BIOPIN. On presenting visitor card, terminal will authenticate the visitor card, read User ID and allow access.

Access Path

Terminal Menu :

User Menu > Card Manager > Encode Visitor Card

Pre-requisites

Card data Format for Visitor Card is set to ID only

Screens & Steps

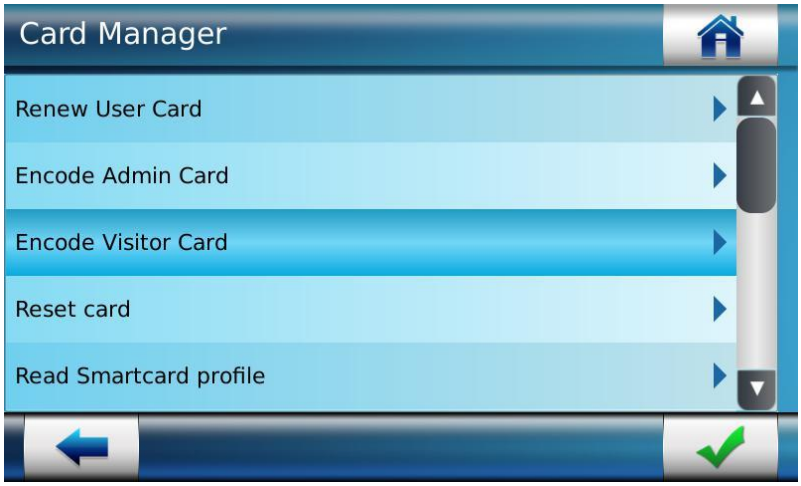


Figure 89: Encoding Visitor Card

1. Select **Encode Visitor Card**

Figure 90: User ID for Visitor Card

2. Terminal will prompt to enter **User ID**.

   NOTE: Contactless card CSN can also be used as User ID by configuring a specific parameter. For more details, please refer to “Smartcard” section in **Parameters Guide**.

3. Press on “ ” button to save and next
4. Terminal will ask user to present card on card reader. **Present Card** on card reader
5. A success message is displayed showing visitor card is encoded successfully

Read Smartcard Profile

The administrator can set the type of card that Access and Time Biometric Terminal will be able to read, by means of this functionality. This implies that these cards can be used for authentication purpose only. The data on the card cannot be changed.

Access Path

Terminal Menu :

User Menu > Card Manager > Read Smartcard profile

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > Contactless Card > General Parameters > Read Profile

Screens & Steps

Figure 91: Smartcard Read Profile

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

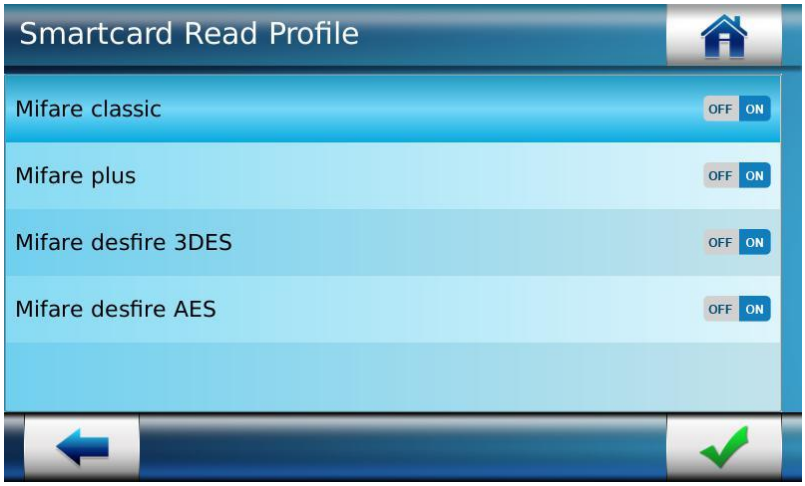


Figure 92: Smartcard Read Profile_Multi

b. In case of iClass product

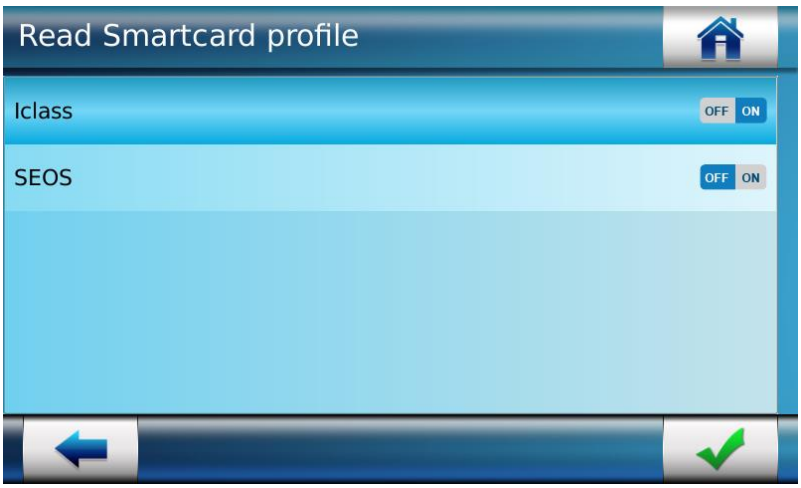


Figure 93: Smartcard Read Profile_iClass

2. The administrator must set the following card read profile as ON, if it is required to be readable by the terminal.

➔ <u>In case of MD Product</u>

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

➔ <u>In case of iClass Product</u>

a. IClass®
b. SEOS®

➔ In case of MD Product

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

➔ In case of MDPI Product

e. HID Prox
f. HID Prox + Mifare Plus
g. IClass®
h. SEOS®
i. MIFARE® Classic
j. MIFARE® DESFire® 3DES
k. MIFARE® DESFire® AES
l. MIFARE® Classic + MIFARE® DESFire® 3DES + MIFARE® DESFire® AES
m. MIFARE® plus
n. MIFARE® Plus + MIFARE® Classic
o. MIFARE® Plus + MIFARE® DESFire® 3DES
p. MIFARE® Plus + MIFARE® DESFire® AES
q. MIFARE® Plus + MIFARE® DESFire® 3DES + MIFARE® DESFire® AES
r. MIFARE® Plus + MIFARE® Classic + Mifare DESFire® 3DES
s. MIFARE® Plus + MIFARE® Classic + MIFARE® DESFire® AES
t. MIFARE® Plus + MIFARE® Classic + MIFARE® DESFire® 3DES + MIFARE® DESFire® AES
u. HID Prox + IClass®
v. HID Prox + SEOS
w. HID Prox + MIFARE® DESFire® 3DES
x. HID Prox + MIFARE® DESFire® AES
y. HID Prox + MIFARE® DESFire® 3DES + MIFARE® DESFire® AES
z. HID Prox + MIFARE® Classic
aa. IClass® + SEOS®

3. Press on “ ” button to save configuration

Encode Smartcard Profile

The administrator can set the type of card that Access and Time Biometric Terminal will be able to encode, by using this functionality. These cards can be used to store user's profile and for user authentication. The administrator can update or reset the data on the card.

Access Path

Terminal Menu :

User Menu > Card Manager > Encode Smartcard profile

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > Contactless Card > General Parameters > Encode Profile

Screens & Steps

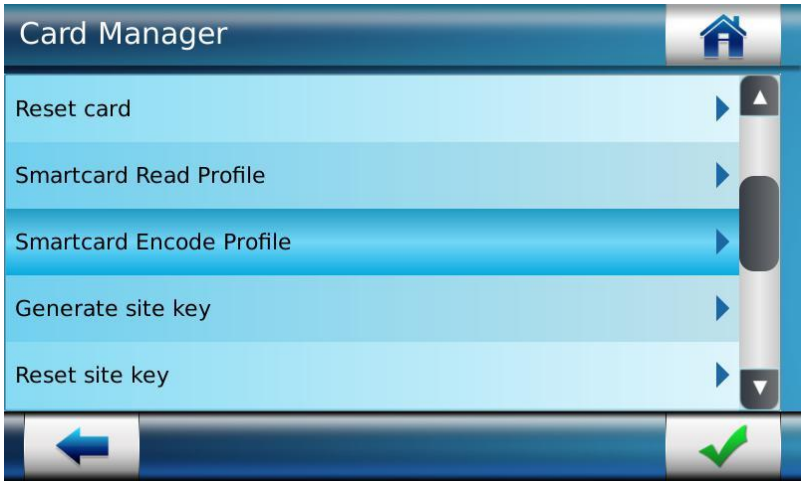


Figure 94: Smartcard Encode Profile

1. Select Encode Smartcard profile

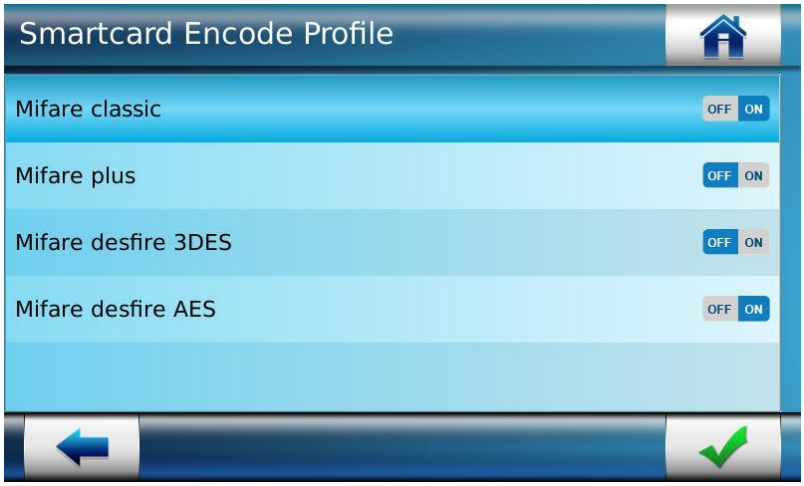


Figure 95: Smartcard Encode Profile

2. The administrator needs to set the smartcards encode profile as ON, if they are to be encoded by the terminal

   NOTE: It is not possible to encode several types of MIFARE (Classic) or DESFire (3DES and AES) cards at the same time.

3. Press on “ ” button to save configuration

On MDPI product, the encode profile list is the following :

bb. iClass®
cc. MIFARE® Classic
dd. MIFARE® DESFire® 3DES
ee. MIFARE® DESFire® AES
ff. MIFARE® Classic + MIFARE® DESFire® 3DES
gg. MIFARE® Classic + MIFARE® DESFire® AES
hh. MIFARE® plus
ii. MIFARE® Plus + MIFARE® DESFire® 3DES
jj. MIFARE® Plus + MIFARE® DESFire® AES

Generate Contactless Key

Securing card includes protecting the card by primary/secondary keys to prevent unauthorized use. At the time of authentication using a smartcard, the site key stored in card and the one in the terminal must match. There is a default site key which is present in the terminal as well as on the smartcard. The administrator can generate a new site key in the terminal for all card types and upload the same key in the card by using Generate Site Key functionality.

Access Path

Terminal Menu :

User Menu > Card Manager > Generate Contactless key

Screens & Steps

1. Select **Generate Contactless key**

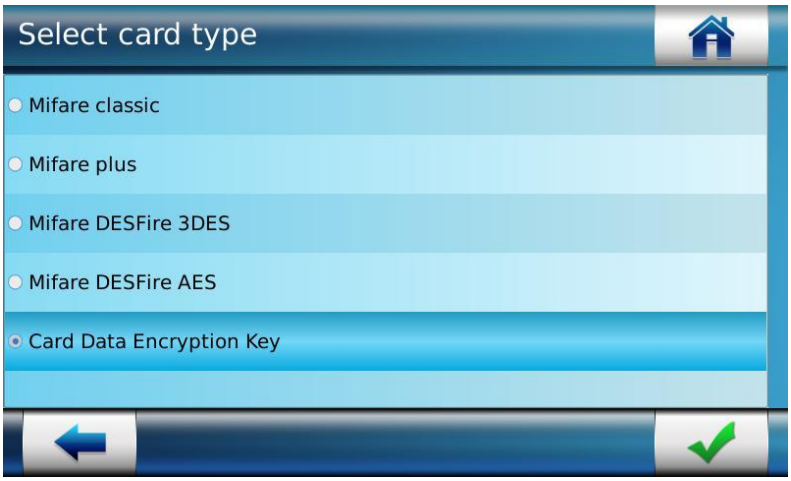


Figure 96: Selecting Key Type

2. Select the Key Type, for which site key is to be generated.
3. Press on “ ” button to save. Move to the next screen.

Figure 97: Generating Site Key

4. Enter the Passphrase to generate Site key using keyboard.
5. Use check button to save

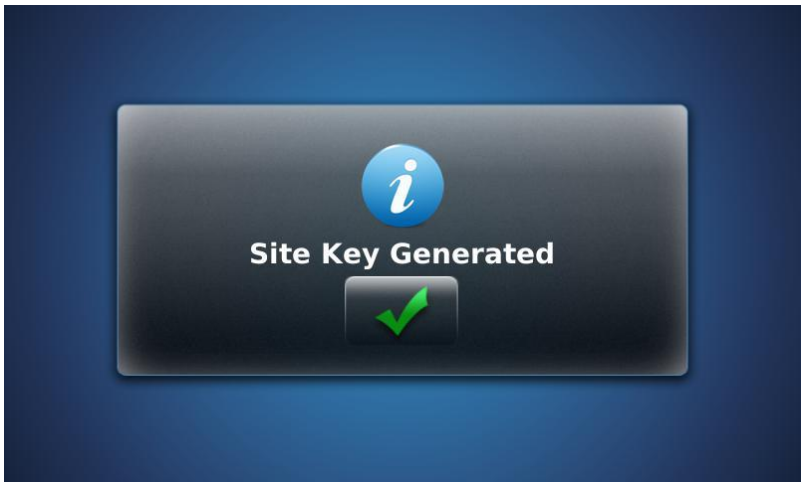


Figure 98: Success message is displayed showing site key is generated in the terminal

Reset Contactless Key

The administrator can reset security keys stored in terminal to factory default settings by using this functionality. The administrator can select the card type from the available card types.

Access Path

Access Path

Terminal Menu :

User Menu > Card Manager > Reset contactless key

Screens & Steps

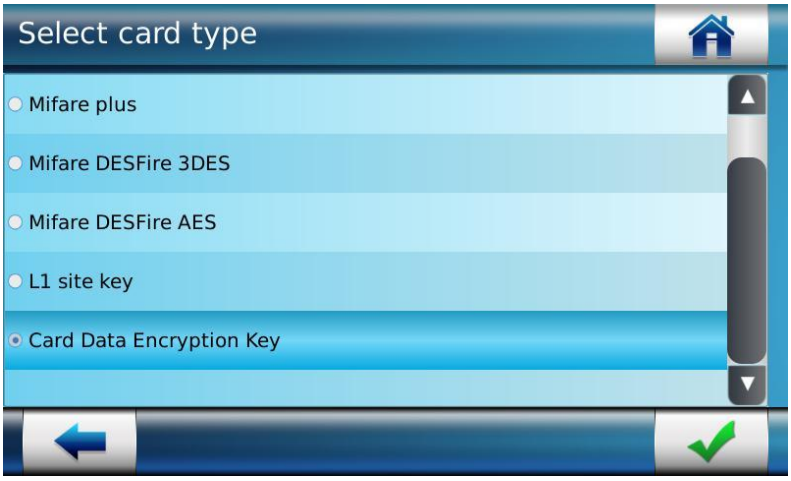


Figure 99: Resetting keys

1. Select contactless type to be reset
2. Use “ ” to save settings

NOTE: For VisionPass MD and VisionPass SP MD, card types are Mifare classic, Mifare Plus, DESFire 3DES and DESFire AES

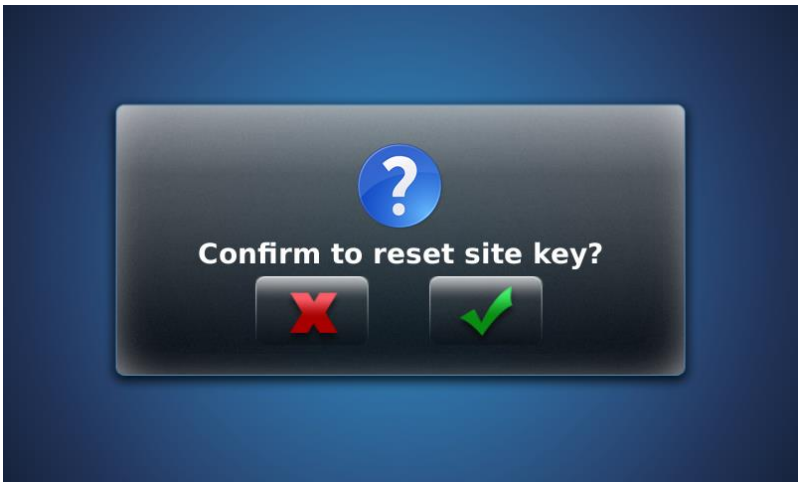


Figure 100: Confirming reset key action

3. Confirm reset contactless key by click on “ ”

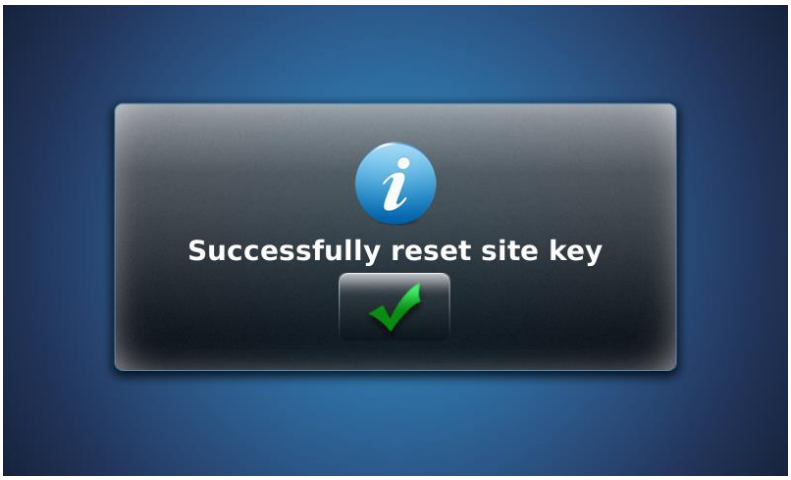


Figure 101: Contactless Key is reset successfully

Activate Card Data Encryption

The administrator can enable Card Data Encryption. This configuration encrypts the smartcard data during the encoding operation and decrypts these encrypted data during the reading operation. The card data encryption depends on an encryption key generated by the administrator.

By default, Card Data Encryption is disabled.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access Path

Terminal Menu :

User Menu > Card Manager > Activate Card data Encryption

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > Contactless Card > General Parameters > Activate Card data Encryption

Screens & Steps

Figure 102: Activate Card Data Encryption

1. Enable the Activate Card Data Encryption Parameter
2. Use " " to save settings

<u>Note :</u>

The Card Data Encryption Key will be generated and stored in KMS as soon as "Activate Card Data Encryption" is ON and the administrator selects "Generate contactless key".

The Card Data Encryption Key will be reset to an hardcoded value and stored in KMS as soon as "Activate Card Data Encryption" is ON and the administrator selects "Reset contactless key".

Configure ELITE key

The administrator can load in the iClass or MDPI terminal, HID ELITE key by using this functionality. When ELITE keys are loaded, the terminal will start accepting specific iCLASS or

Seos card, ELITE cards, and starts rejecting the regular cards. There are two steps and two configuration card, to load these keys, Key Roller Card & Configuration Card. This is applicable to only iClass and MDPI terminals.

Access Path

Terminal Menu :

User Menu > Card Manager

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

User Menu > Card Manager

Screens & Steps to load ELITE keys

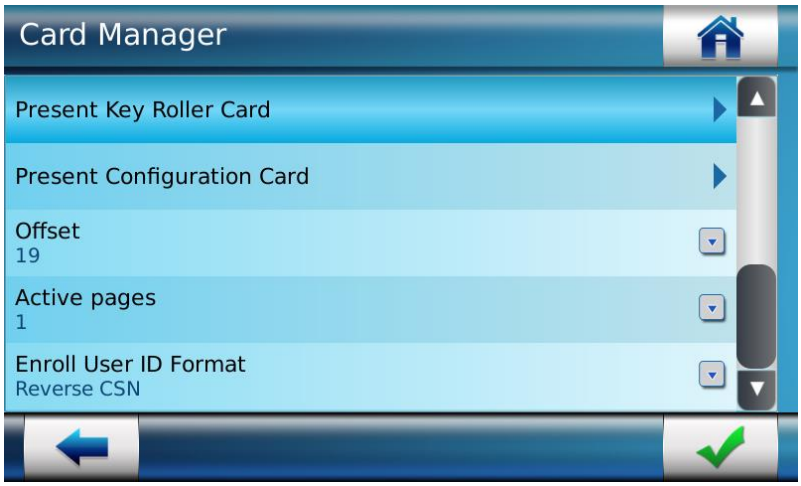


Figure 103: Enable ELITE Mode

1. Select Present Key Roller Card
   a. Terminal will ask to Place Card.
   b. Present the "Key roller card STD->Elite" Card
   c. Wait until the "Hold Card" message disappears before to remove Card
2. Select Present Configuration Card
   a. Terminal will ask to Place Card.
   b. Present the "Configuration card STD->Elite" Card
   c. Wait until the "Hold Card" message disappears before to remove Card
3. Use "✓" to save settings
4. Now terminal will accept iCLASS Card encoded with ELITE Key and reject iCLASS – Standard Cards.

Load Seos or HID Mobile Credential keys

The administrator can load Seos keys in the iClass or MDPI terminal and load HID Mobile Credential key in the MDPI-M terminal, by using this functionality. There is only one step and one configuration card, to load these keys. This is applicable to only iClass and MDPI terminals.

NOTE 1:

OSDP communication has to be disable during this procedure.

Access Path

Terminal Menu :

User Menu > Card Manager > Present Configuration Card

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

User Menu > Card Manager > Present Configuration Card

Screens & Steps to Enable ELITE Mode

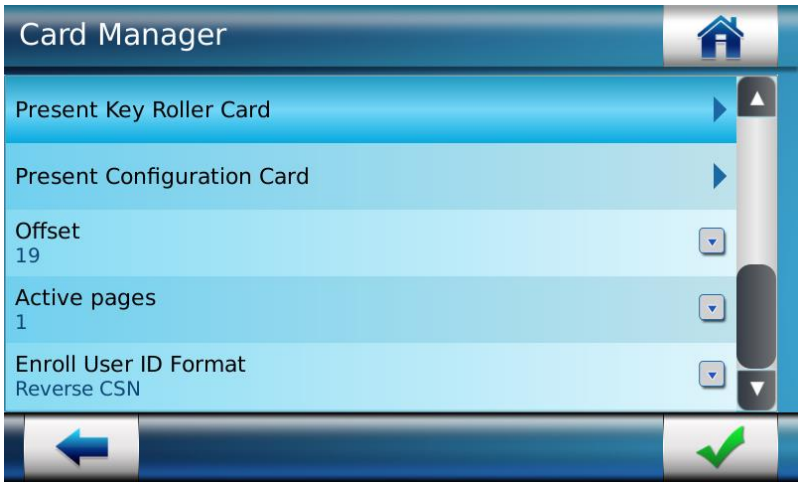


Figure 104: Load Seos or HID Mobile Credential keys

5. Select Present Configuration Card
   a. Terminal will ask to Place Card.
   b. Present the "Configuration card" (Seos or HID Mobile Credential)
   c. Wait until the "Hold Card" message disappears before to remove Card
6. Use " " to save settings

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

7. Now terminal will accept Seos Card or HID Mobile Credential protected by these keys.

NOTE 1:

Default Seos keys are preloaded in iClass Sigma Range terminals. There are not in MDPI terminals: the previous procedure should be applied.

NOTE 2:

This step could require a long time. The configuration card should not remove before end the process.

No. of Start Block for MIFARE® Cards

The administrator can specify the location of the access control data on the contactless card, by configuring the number of the first block to read on the card. By default, the 1st block to read is block # 4.

NOTE 1:

The value specified for the start block applies also to the administrator cards, Hence the administrator needs to ensure that the administrator data is also stored from the same block number as user data on user cards.

NOTE 2:

In case of 1 K MIFARE®, the administrator can set start block no. 4 to block 48.

In case of 4 K MIFARE®, the administrator can set start block no. 4 to block 216.

Access Path

Terminal Menu :

User Menu > Card Manager > Starting block number

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

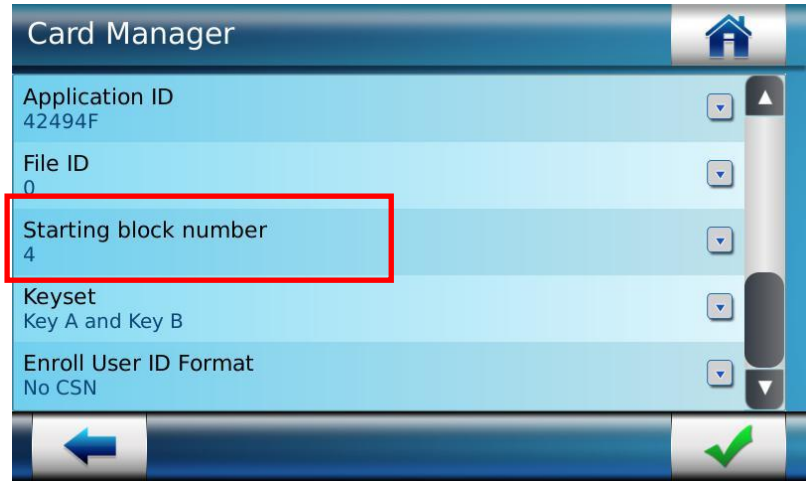


Figure 105: Setting No. of Start Block

1. Select **Starting block number**
2. On next screen the administrator can enter the start block number using keypad
3. Use “ ” to save settings

Select Keyset for Reading MIFARE® Cards

The administrator can select a key set that is used by terminal for authentication and reading MIFARE® cards, by means of this functionality. Following are the key set values that can be configured:

Keys A only,

Keys B only,

Keys A then Keys B if failed

Access Path

Terminal Menu :

User Menu > Card Manager > Keyset

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

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

Screens & Steps

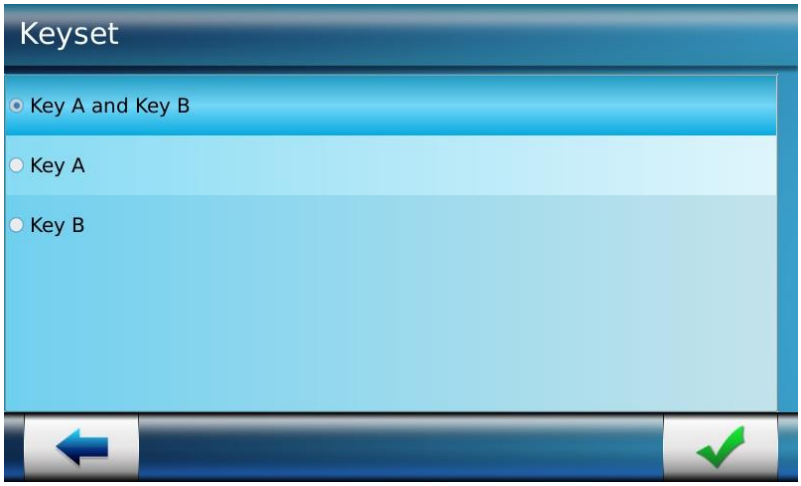


Figure 106: Keyset configuration

1. Select a **keyset**
2. Press on check "✓" button to save changes

Select Enroll User ID Format

The administrator can set the User ID format to be encoded on card, by using this functionality.

Access Path

Terminal Menu :

User Menu > Card Manager > Enroll User ID Format

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > Contactless Card > General Parameters > Enroll User ID

Screens & Steps

Figure 107: Selecting Enroll User ID Format

1. Select **Enroll User ID Format**

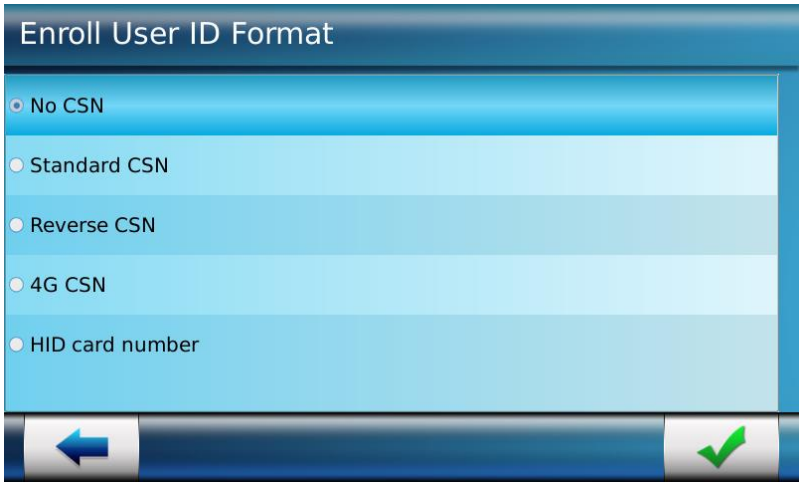


Figure 108: Selecting Enroll User ID Format

2. Select one of the following User ID formats:
   a. **No CSN**: this value indicates that the serial number on the contactless card will not be used as User ID.
   b. **Standard CSN:** This indicates that the serial number on the contactless card is considered as User ID at the time of enrolment and authentication.
   c. **Reverse CSN:** This indicates that the serial number on the contactless card in reverse byte order is considered as User ID at the time of enrolment and authentication.
   d. **4G CSN:** This indicates that the contactless card serial number read, is manipulated as per 4G terminal. Manipulation is as follows.

      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
}
```

NOTE: This option is not available in VisionPass Range products.

e. **HID card number:** This indicates that the HID number read by the terminal from the iClass card serves as the User ID.

NOTE: This option is only available in iClass product.

f. **Reverse HID card number:** This indicates that the HID number read by the terminal from the iClass card is reversed to serve as the User ID.

NOTE: This option is available only in iClass product and can be set via PC application or Webserver.

Partial CSN

- Configuration keys are available to use partial CSN in enroll and verify modes.
- For each of mode there are start bit key and a length key (in bits) as below.
  For Enrollment, sc.enroll_csn_start and sc.enroll_csn_length
  For Verification, sc.verify_csn_start and sc.verify_csn_length
  start bit key: range 0 to 79, default value 0
  length key: range 0 to 80, default value 0. Value 0 will be associated to the use of the full card CSN, whatever the start bit value.
- These keys are only used when the keys “Enroll” or “Verify” are set to “ReverseCSN” or “StandardCSN”.
- To use these keys, user should know length of CSN of the cards he is using. If the start bit is too high, compare to the length of the card CSN, the partial length will be equal to 0.
  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
- These keys are only accessible from PC Application or Web Server.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Defining Application ID and File ID for DESFIRE® Cards

The administrator can specify the value of the Application ID and File ID for reading DESFire® cards, by means of this functionality. 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

Terminal Menu :

User Menu > Card Manager > Application ID

User Menu > Card Manager > File ID

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

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

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

Screens & Steps

Figure 109: Configuring Application ID and File ID

1. Select **Application ID**
2. Enter Application ID from range of 0x000001-0xFFFFFF. By default, application ID 0xEEE600
3. Now select File ID
4. Enter File ID using keypad, from range of 0 – 15. By default, File ID is set as 0
5. Press on check " " button to save changes

Defining Offset for Reading iCLASS® Cards

The administrator can configure the offset to read the data from 2APP iCLASS® cards, by using this functionality. 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

Terminal Menu :

User Menu > Card Manager > Offset

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

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

Pre-requisites

Access and Time Biometric iCLASS® terminal required to configure Offset for reading iCLASS® card

Screens & Steps

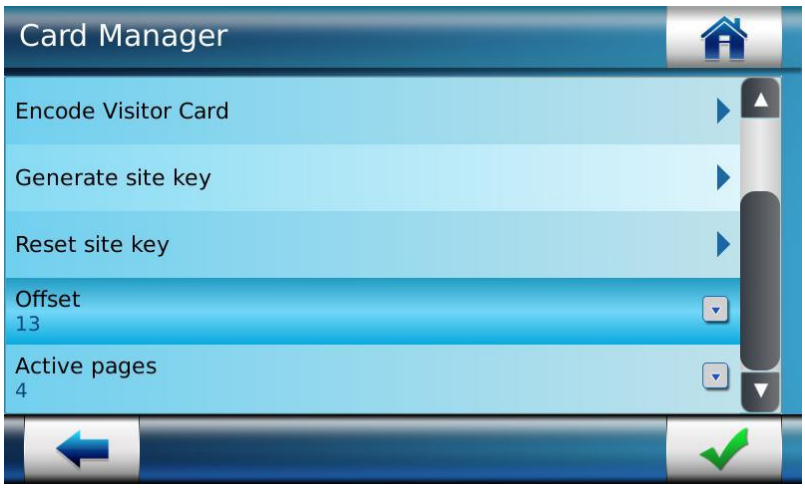


Figure 110: Set Key Offset for iCLASS® cards

1. Press on **Offset**

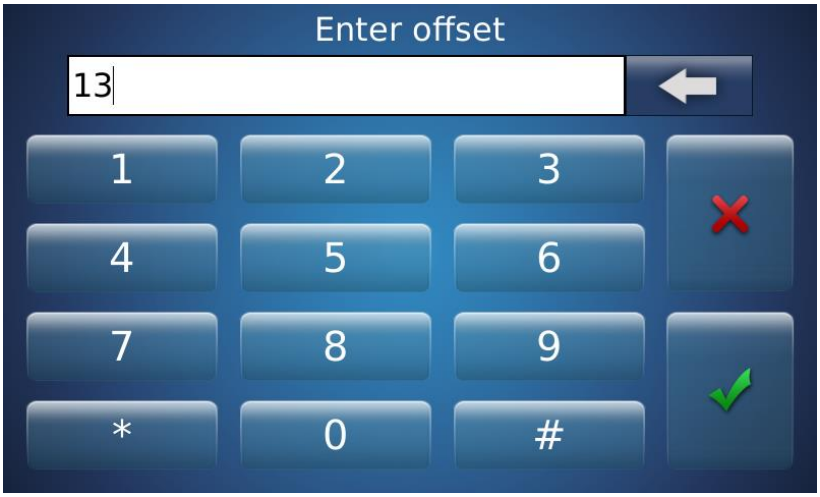


Figure 111: Set Key Offset

2. Enter **Offset value**. An administrator can configure offset from 0x13 to 0x9F (hex values)

3. Press on check “ ” button to save the Offset value

Defining Active Pages for Reading iCLASS® Cards

The administrator can configure the active page for reading data from 16APP iCLASS® cards, by using this functionality. 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

Terminal Menu :

User Menu > Card Manager > Active Page

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

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

Pre-requisites

The administrator needs to ensure that the Access and Time Biometric iCLASS® terminal is configured Active pages for reading iCLASS® card

Screens & Steps

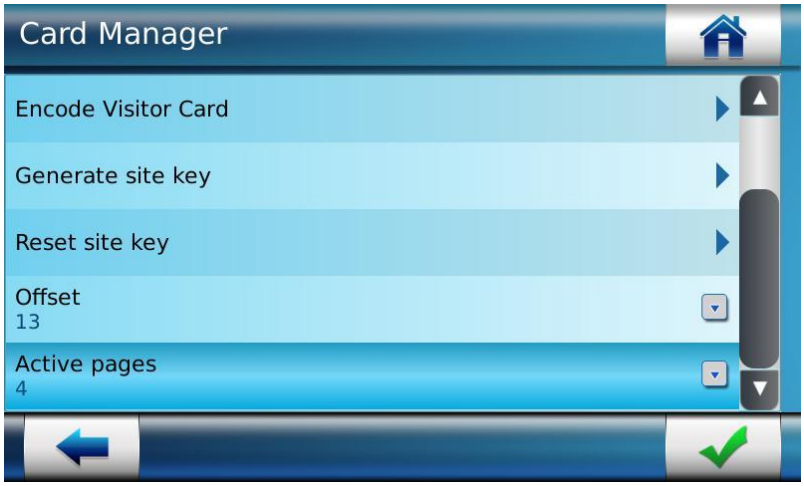


Figure 112: Configure Active Pages for iCLASS® cards

1. Select **Active Pages**

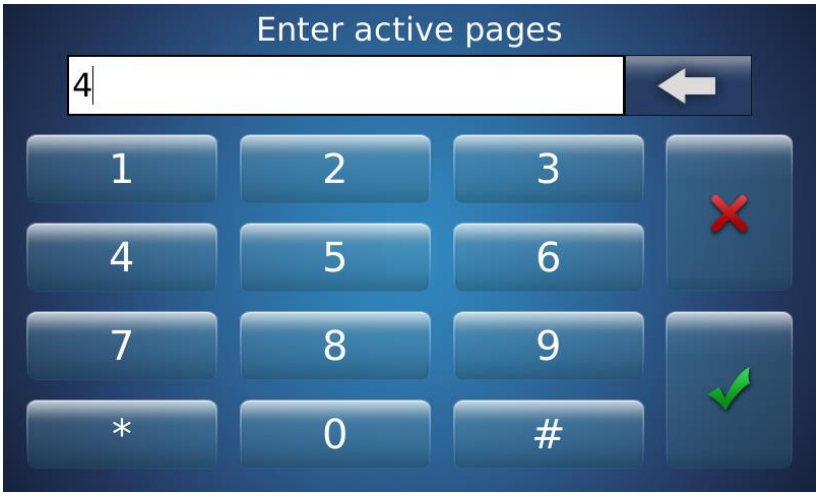


Figure 113: Enter Active Pages

2. Enter number of **Active Pages**
3. Press on check “ ” button to save

Defining ADF OID & DO TAG for HID iCLASS® SEOS® Cards

The administrator can specify the value of ADF OID and DO TAG in the **Erreur ! Il n'y a pas de texte répondant à ce style dans ce document.**terminal for reading HID iCLASS® SEOS® cards by means of this functionality. Encoding from terminal is not supported.

Access Path

Terminal Menu :

User Menu > Card Manager > ADF OID

User Menu > Card Manager > DO TAG

Pre-requisites

The administrator needs to make sure that the bit 7 of parameter “sc.read_profile” is set to 1, in order to activate reading of HID iCLASS® SEOS® cards. Please refer to **Parameters Guide** document for more details.

Screens & Steps

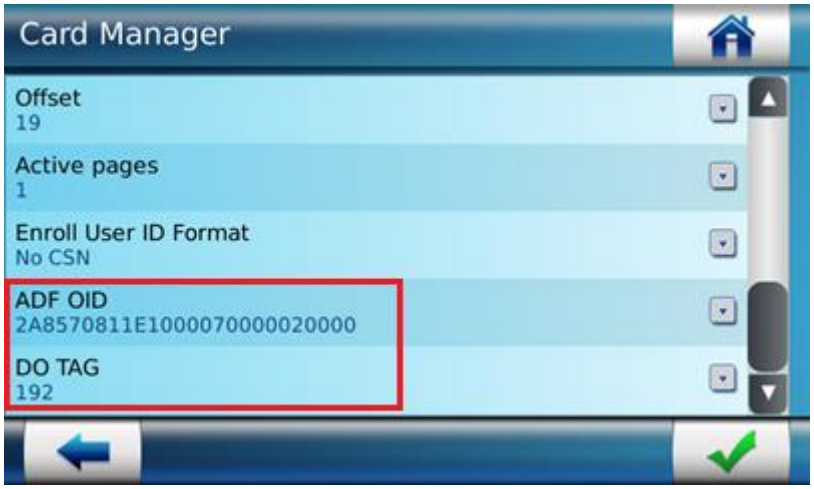


Figure 114: Configure ADF OID & DO TAG for HID iCLASS® SEOS® cards

1. Select **ADF OID**

Figure 115: Enter ADF OID

2. Enter ADF OID number
3. Press on check “ ” button to save
4. Select DO TAG

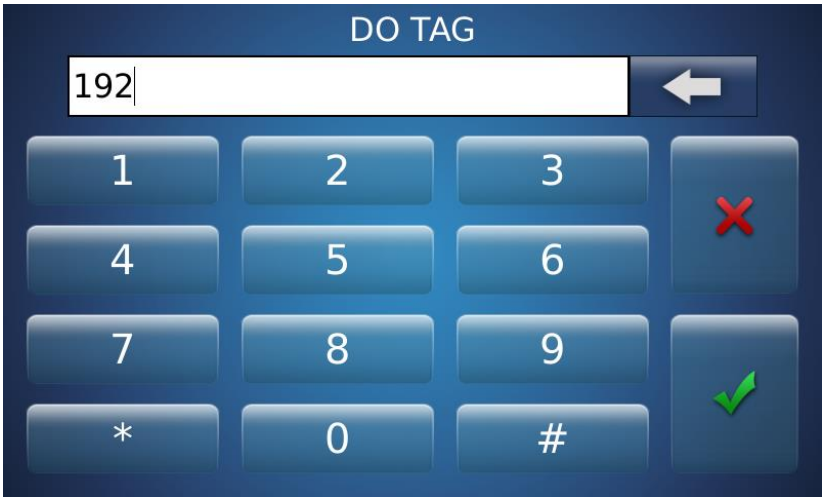


Figure 116: Enter ADF OID

5. Enter DO TAG number
6. Press on check “ ” button to save

Reset Card

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

Access Path

Terminal Menu :

User Menu > Card Manager > Erase Card

Webserver (not available In Enforced Security configuration and in all configurations for “MorphoWave® SP”, “MorphoWave® XP2” and “VisionPass SP”):

User Management > User Enrollment > Erase Card

Pre-requisites

A smartcard has user details stored.

Card is secured with the same key as on terminal.

Screens & Steps

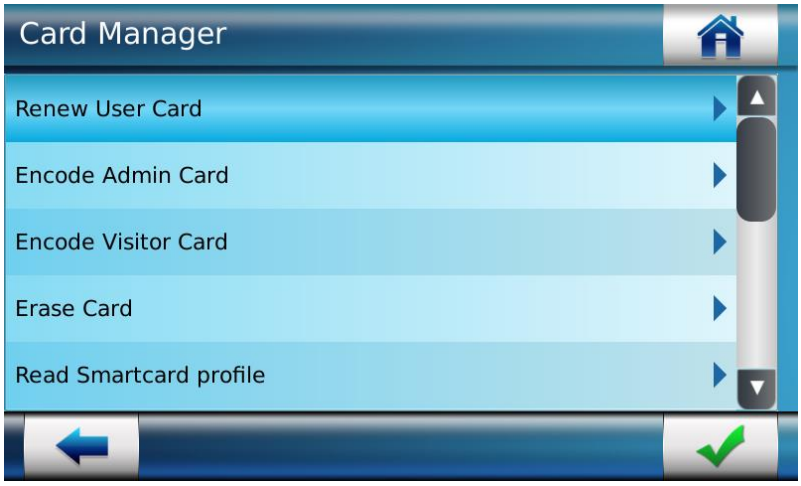


Figure 117: Reset card

4. Select **Reset Card**
5. Terminal will ask to **Place Card** at card reader.
6. Once the administrator places the card, terminal will read and reset the card by erasing the stored data. This will also reset the card key to default value.

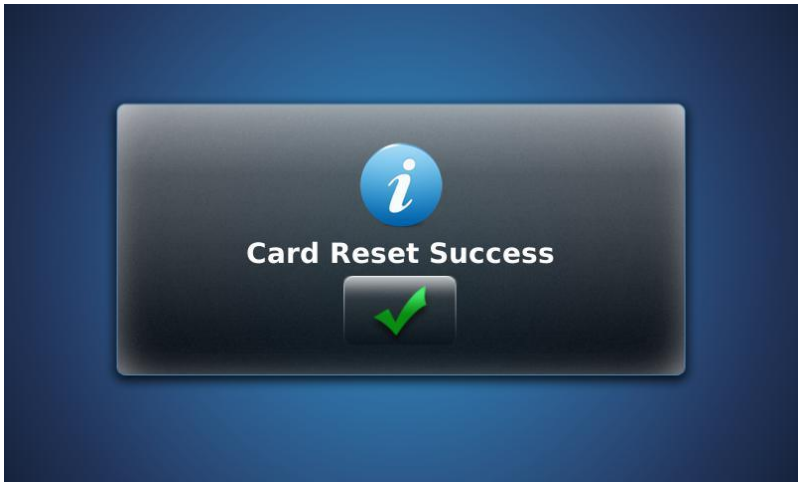


Figure 118: Success message is displayed showing card is reset successfully

Results

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

Multimedia menu

The administrator can upload and manage audio, video and images on Access and Time Biometric Terminal, by using the multimedia menu. These multimedia contents are used to perform various tasks such as to play an alarm when the terminal is tampered.

The administrator needs to refer to the following sections in order to understand as to how one can upload the multimedia contents in the terminal and the supported formats. Terminal can play multimedia files contained in **MKV** (video), **WEBM** (video), **OGG** (audio), and **WAV** (audio) container.

NOTE: In Enforced Security configuration, access to Multimedia menu requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Figure 119: Multimedia Menu

Audio Settings

The administrator can configure the Access and Time Biometric Terminal to play a notification sound on the following events:

Access Denied: Audio is played when user verification has failed and access is denied

Access Granted: Audio is played when user verification is successful and access is granted

Message Attention: Audio is played on instances such as door is left opened

Tamper Detection: Audio alarm is played when tamper is detected

Using Audio settings an administrator can perform the action listed below:

The administrator can upload Audio files using USB mass storage device to specific folders that can be found in the Multimedia Menu > Audio path. Please note that each folder will be having a unique name that corresponds to the action or event which leads to a notification sound. For e.g., the administrator must ensure that the audio that is to be played on event of a tamper need to be uploaded in the Multimedia Menu > Audio > Tamper folder.

Set the volume at which the sound should be played

The administrator can delete the audio file corresponding to a given event, in case it is not required to notify that event with a sound.

Access Path

Terminal Menu :

Multimedia Menu > Audio

Pre-requisites

The administrator must make sure that the USB mass storage device has been properly initialized. This implies that the USB mass storage device must have exactly the same folder structure as displayed on the terminal. For example, the Audio to be played on tamper detection should be stored in the 'Tamper' folder. Refer to "*Initialize USB Mass Storage device*" section to understand as to how to initialize a USB mass storage device.

The maximum supported Audio file size is up to 500KB

Supported audio file formats are FLAC, PCM, and VORBIS

The administrator must ensure that the audio messages must be in the same language, as configured in the terminal

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

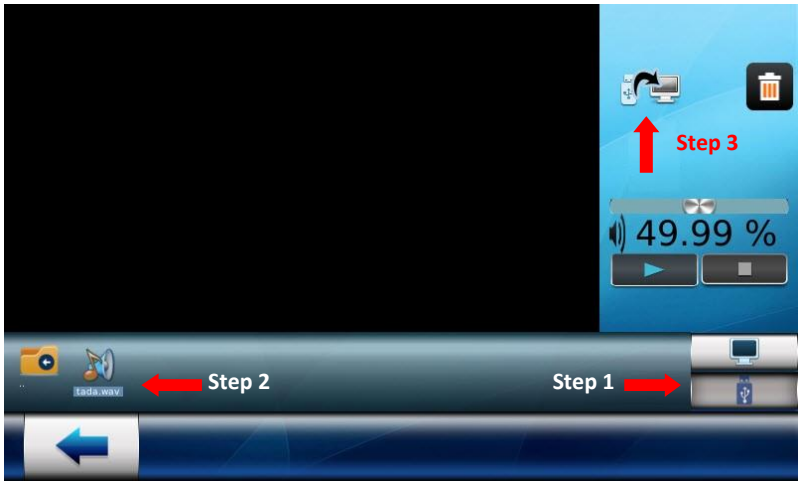


Figure 120: Uploading Audio File in device

1. Select **USB mode**
2. The administrator can view the folders present in USB mass storage device.
3. Select an Audio file that is required to be uploaded on terminal
4. The administrator can play the audio file and also adjust its volume
5. Press on **Copy** button to copy file from USB mass storage device to Terminal

Figure 121: Confirmation Pop-up

6. A confirmation pop-up will appear. Press on “ ” icon to copy file from USB mass storage device to terminal

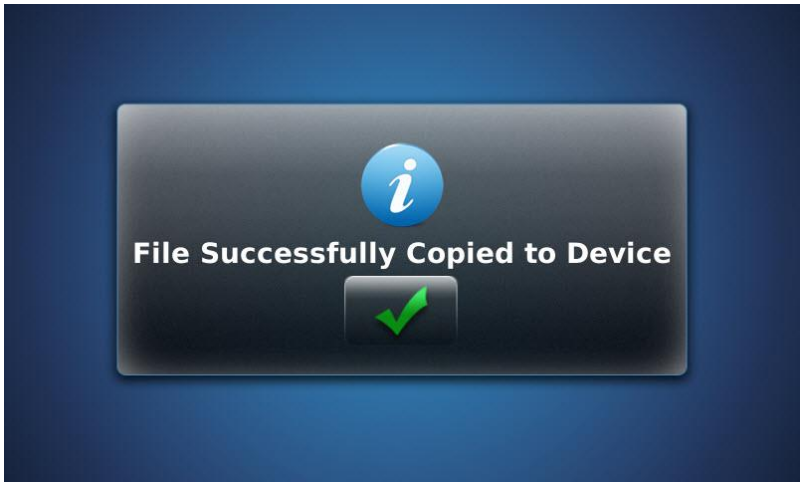


Figure 122: Success message is displayed

Results

Success message is displayed showing Audio file is copied to terminal. Audio is played on respective action on terminal.

The administrator can use the“ ” button to **Delete** an audio file.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Video Settings

SIGMA Wide, SIGMA Extreme, Morpho*Wave*® Compact and VisionPass terminals are capable of playing video when screen is idle, except VisionPass SP. The administrator can configure the following, by using Video settings:

- Upload Video files using USB mass storage device
- Set the volume at which the sound should be played
- Remove video file. In this case, No video will be played when the screen is idle.

NOTE: Remove video file means that no video will be played in background on Home screen on the VisionPass terminal (if video in background feature is activated)

Access Path

Terminal Menu :

Multimedia Menu > Video

Pre-requisites

The administrator must ensure that the USB mass storage device must be properly initialized. This implies that the USB mass storage device must have the same folder structure as displayed on the terminal. For example the administrator must place the video to be played on idle screen time under the folder named 'Idle Screen'. The administrator can refer to "*Initialize USB Mass Storage device*" section in order to understand the process of initializing a USB mass storage device.

The maximum supported Video file size on SIGMA Wide series terminal is up to 10MB

The maximum supported Video file size on SIGMA Extreme series, Morpho*Wave*® Compact and VisionPass terminals is up to 50MB

Supported Video files formats are MPEG-4 and VP8

Note : Morpho*Wave*® Compact and VisionPass terminals are not able to play custom video files with resolution 1280x720

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

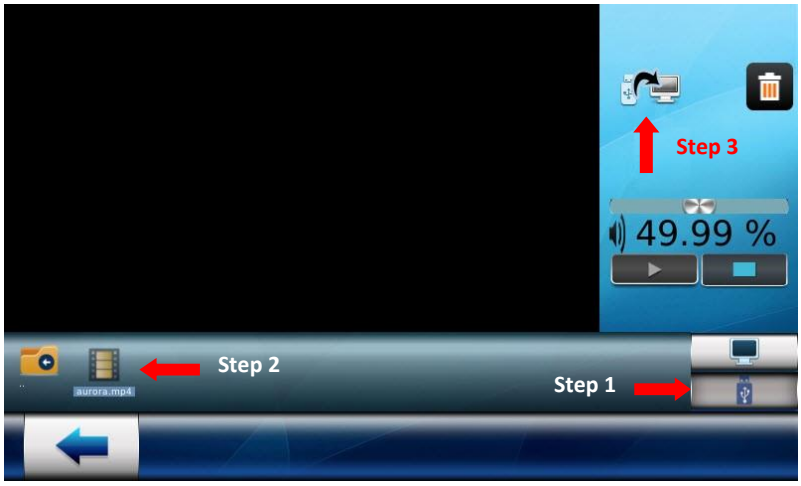


Figure 123: Uploading Video File in device

1. Select **USB Mode**
2. The administrator can view the folders present in USB mass storage device.
3. Select a **Video File** that is required to be uploaded on terminal
4. The administrator can play video file and also adjust its volume
5. Press on Copy button to copy file from USB mass storage device to Terminal

Figure 124: Confirmation Pop-up

A confirmation pop-up will appear. Press on “ ” icon to copy file from USB mass storage device to terminal

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

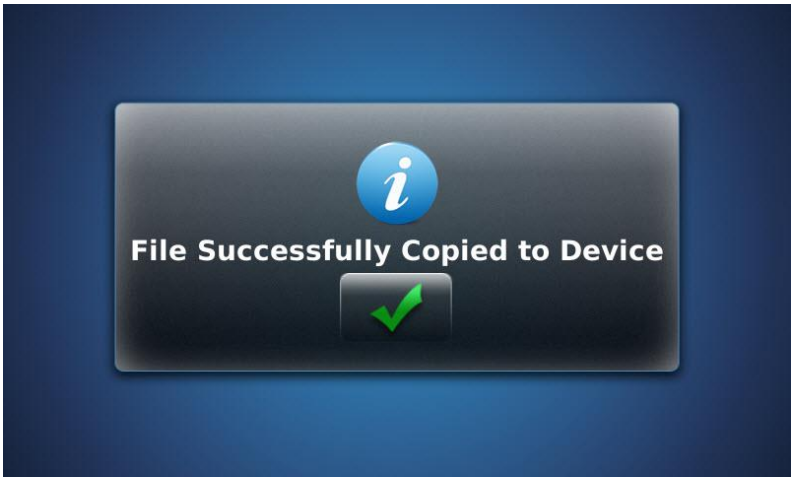


Figure 125: Success message is displayed

Results

Success message is displayed showing Video file is copied to terminal. The uploaded video is played on idle screen time out.

The administrator can click on the “ ” button to **Delete** a video file.

References

Refer to “Idle Screen Time Out” parameter under LCD Configuration

The administrator needs to refer to the parameter “Set Infinite Video Play” under LCD Configuration, in order to set the time duration for which the video is played.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Images Settings

Access and Time Biometric Terminal is capable of displaying images on the LCD screen. The images can be used for purposes listed below:

Dynamic Message: The administrator must set the “Dynamic Message Configuration” as ON at the time of user enrolment if it is required to display an image when the user is granted access.

Wallpaper: This is to set wallpaper to be displayed on the home page.

AccessGrantedLogo: This is to set customize logo to be displayed on terminal LCD for access granted event. When the user is granted access, this customized logo will display rather than default green color logo. The administrator can set to be displayed only logo without “Access Granted” string by uploading user defined LCD language file with empty translation of “Access Granted” string.

AccessDeniedLogo: This is to set customize logo to be displayed on terminal LCD for access denied event. When the user is denied access, this customized logo will display rather than default red color logo. The administrator can set to be displayed only logo without “Access Denied” string by uploading user defined LCD language file with empty translation of “Access Denied” string.

The maximum supported picture file size on SIGMA Range is up to 5MB and on Morpho*Wave*® Compact and VisionPass Range terminals is up to 1MB.

Supported picture files formats are PNG and JPG.

Access and Time Biometric Terminal is capable of displaying animation on the LCD screen. The animation can be used for purposes listed below:

CardAnimation: This is to set customize animation to be played on LCD when terminal is idle and trigger event is set to card only.

BiometricAnimation: This is to set customize animation to be played on LCD when terminal screen is idle and trigger event is set to biometric only.

QRAnimation: This is to set customize animation to be played on LCD when terminal screen is idle and trigger event is set to QR Code only.

CardBioAnimation: This is to set customize animation to be played on LCD when terminal screen is idle and trigger event is set to card + biometric only.

QRFingerAnimation: This is to set customize animation to be played on LCD when terminal screen is idle and trigger event is set to QR code + biometric only.

CardQRCodeAnimation: This is to set customize animation to be played on LCD when terminal screen is idle and trigger event is set to QR code + Card only.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

CardQRBioAnimation: This is to set customize animation to be played on LCD when terminal screen is idle and trigger event is set to Card + QR code + biometric only.

The maximum supported picture file size on SIGMA Range is up to 5MB and on Morpho*Wave*® Compact and VisionPass Range terminals is up to 1MB. Supported picture files format is GIF.

The table below provides the resolution of original pictures.

	Sigma	Lite+	Extrem	MW XP	ViP	ViP SP
Wallpaper & video	800*480	240*320	480*800	480*800	480*800	480*800
Animation	621*316	NA	480*350	350*350	NA	NA
Access granted and denied	621*316	99*110	266*296	266*296	193*217	193*217

The administrator can perform the following actions, using Image Settings:

Upload image files using USB mass storage device

Remove image file: no image will be displayed in this case.

Access Path

Terminal Menu :

Multimedia Menu > Image

Pre-requisites

The administrator must correctly initialize the USB mass storage device, please refer to "*Initialize USB Mass Storage device*" section to understand as to how to initialize a USB mass storage device.

Terminal can support Image file formats such as JPEG, GIF, PNG, and BMP.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

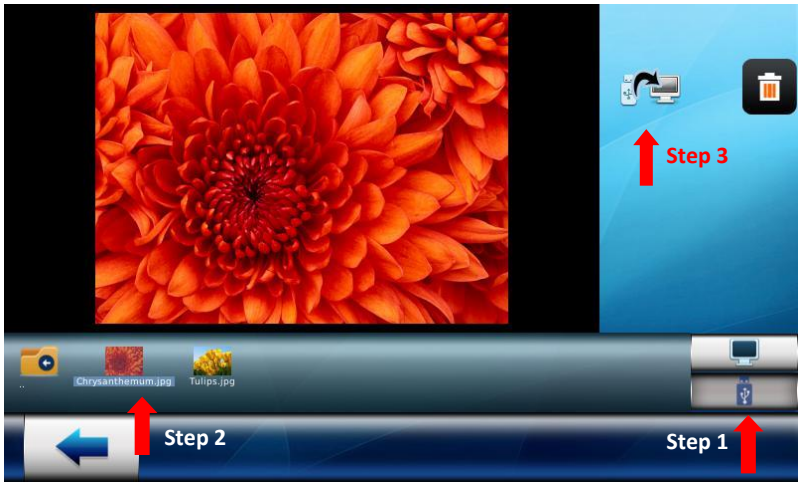


Figure 126: Uploading Image File in device

1. Select **USB mode**
2. The administrator can view the folders present in USB mass storage device
3. Press on **Copy** button (Step 3 in above figure) to copy file from USB mass storage device to Terminal

Figure 127: Confirmation Pop-up

4. A confirmation pop-up will appear. Press on “ ” icon to copy file from USB mass storage device to terminal

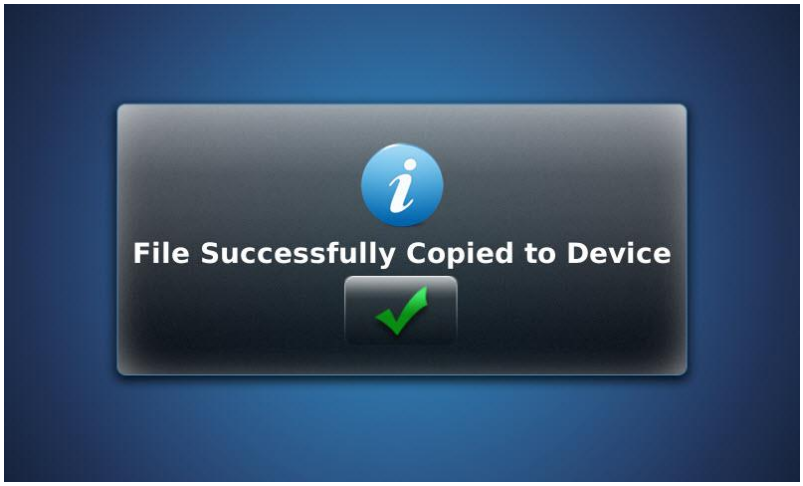


Figure 128: Success message is displayed

Figure 129: Image uploaded is displayed as wallpaper

Results

Success message is displayed showing image file is copied to terminal. The uploaded image is displayed as wallpaper or dynamic message.

The administrator can select and **Delete** images using “ ” button.

NOTE: CardAnimation, BiometricAnimation,… all folders with “animation” name are not managed on VisionPass Range terminals because no animation is present on the Home screen.

System Menu

The administrator can configure fundamental parameters of Terminal such as LCD screen parameters and transaction log settings, using the System menu. System menu also allows an administrator to launch the First Boot Assistant that has all basic parameters in one screen.

NOTE: Only an administrator with full administrative rights can access this menu. In Enforced Security configuration, it requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Figure 130: System Menu

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Terminal Settings

Set Factory Default

Access and Time Biometric Terminals have factory default settings or reset values for all the supported functionalities. The administrator can configure the terminal depending on the desired level of security using these methods:

- Terminal Administration Menu (except for SIGMA Lite and MorphoWave® SP Series)
- Webserver Application (except for MorphoWave® SP, MorphoWave® XP2, VisionPass SP Series)
- Distant system Application
- USB Scripts
- MorphoBioToolBox

Through GUI/Webserver

While resetting the terminal through software, an administrator can select particular parameters manually, for which values are needed to be reset as factory default value.

Access Path

Terminal Menu :

System Menu > Terminal Settings > Set Factory Default

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Webserver > Reset Default

Screens & Steps

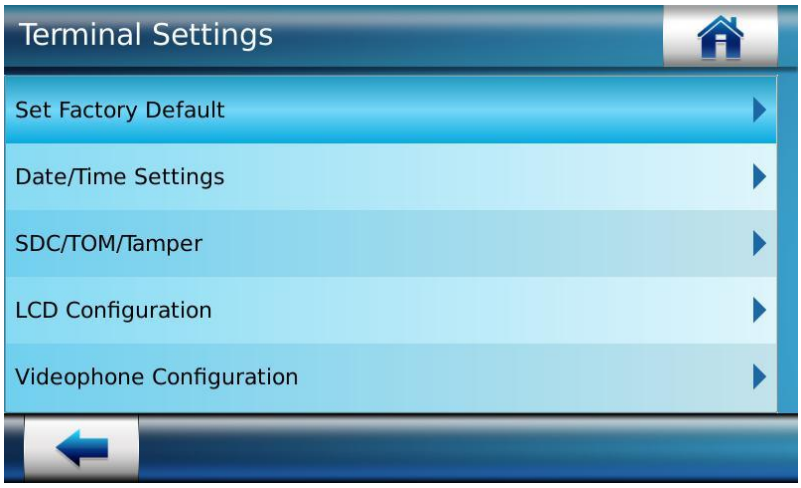


Figure 131: Reset Factory Default Settings

1. Select **Set Factory Default**

Figure 132: Select Items to reset

2. The administrator can select parameters from the list and set as ON. The parameters that are marked ON, will be reset.
3. Press on check button to move next

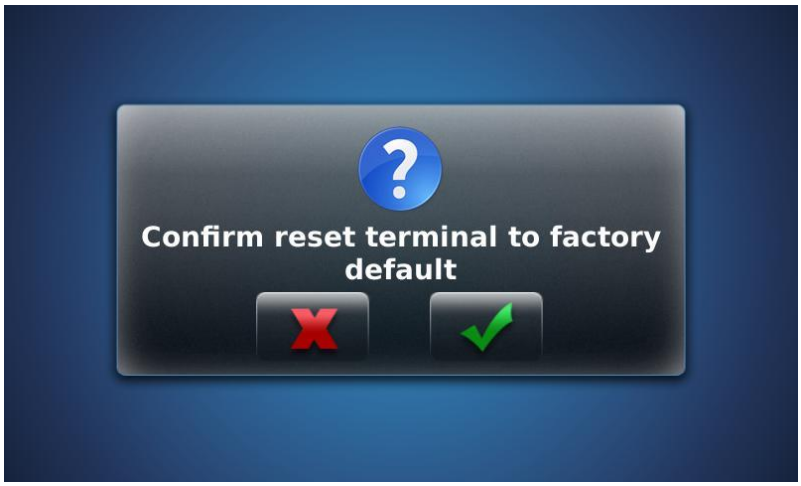


Figure 133: Confirmation message displayed

4. Select check button to confirm resetting of selected parameters of the terminal to factory default settings

Results

The values of selected parameters will be reset at their default values.

Through Hardware Settings

This feature allows the administrator to reset the terminal to factory default settings through hardware settings i.e. by connecting a combination of GPIO and Wiegand external pins as described below:

Steps to perform Factory Reset through Hardware settings

Step 1 : Power off the terminal

Step 2 : The terminal is detached from the wall

Step 3 : Access the external pins of the terminal and connects the following pins:

- GPO_0 to the WIEGAND_IN0
- GPI_1 to the WIEGAND_OUT1

Step 4 : Power-on the terminal

Step 5 : After the terminal power on, the terminal is reset to the factory settings

List of setting to be reset

1. Clear all databases
2. Remove all custom files
3. Clear KMS
4. Set all the configuration parameters to default value

NOTE:

The reset will occur only when the hardware pins are connected and the tamper is triggered for the terminal (i.e. terminal is detached from the wall).

This reset will put back the secure mode if it was previously unlocked.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Date and Time Settings

The administrator can set the time zone, current date and time in the Access and Time Biometric Terminal, by means of this functionality. Besides this, there are options to set the format of date and time. The administrator needs to configure these basic parameters on the first boot of the terminal.

NOTE: For MorphoWave® Compact and VisionPass, the time stored in the product is lost if power supply is removed for up to 48 hours. The date and time will be reinitialized to the firmware generation date.

For SIGMA Range Series, MorphoWave® SP, MorphoWave® XP2 and VisionPass SP, the time stored in the product is lost if power supply is removed for up to few hours. The date and time will be reinitialized to the last value received from the command Terminal_set_configuration or firmware generation date if this command was never applied.

Set Time Zone

Access Path

Terminal Menu :

System Menu > Terminal Settings > Date and Time Settings > Time Zone

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Date Time

Screens & Steps

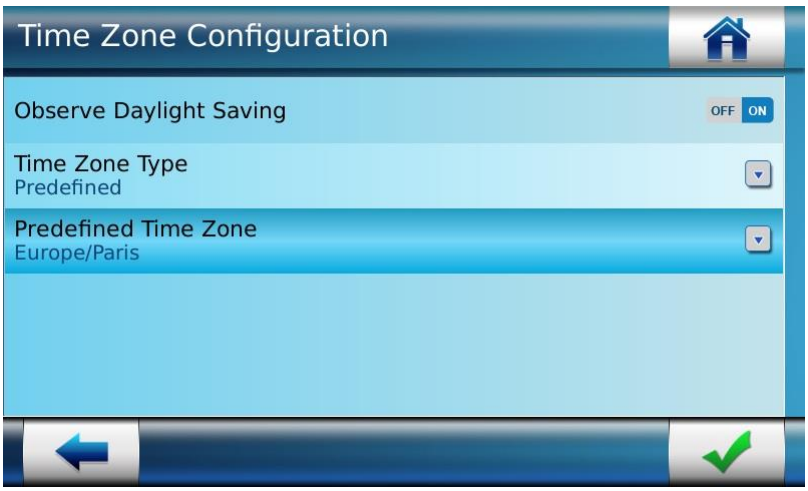


Figure 134: Configuring Time Zone

1. Please refer to the "*Date and Time Configuration"* section step #11 to 21 for more details.

Results

Based on the selected time zone, the time and date will be calculated and set in the terminal. During Daylight Saving, the time will be auto-adjusted.

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. This can be done from the Webserver using the same path as mentioned above.

Set Date

The administrator can configure the current date and the format in which it is to be displayed on the terminal, by using this functionality.

Access Path

Terminal Menu :

System Menu > Terminal Settings > Date and Time Settings > Clock Parameters > Date Configuration

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Date Time

Screens & Steps

Please refer to "*Date and Time Configuration*" section step #1 to 4 for more detail.

Set Time

Access Path

Terminal Menu :

System Menu > Terminal Settings > Date and Time Settings > Clock Parameters > Time Configuration

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Date Time

Screens & Steps

Please refer to "*Date and Time Configuration*" section step #4 to 9 for more detail.

Results

The administrator can view the configured date and time at the bottom of the home screen on the terminal.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Single Door Controller (SDC) Configuration

The administrator can configure the Single Door Controller (SDC) parameters in order to control the access through a door when specific actions are triggered on Access and Time Biometric Terminal. For example, on successful identification of a user, door must open automatically to allow the user into the premises.

SDC Configuration allows an administrator to set either of the two states as below:

GPIO General Mode:

General Purpose Input Output (GPIO) mode is used for passing multiple signals to the door panel when an action is triggered on the terminal. By default, GPIO Mode is enabled.

GPI: General Purpose Input (GPI) has three TTL lines available, i.e., Line 0, 1 and 2. The administrator can configure a GPI line **to trigger an action on the terminal from a distant system**, when set as active (low and/or high). The administrator can activate multiple lines for same action or multiple actions. The signal is sent when following actions are triggered on terminal:

Delete Templates: On selection of this action, terminal will erase all the biometric templates of specified template ID i.e. if more than one template are available with different index then all those templates will be removed. The signal is sent when following actions are triggered on terminal.

Reboot Terminal: This action will reboot terminal

Alarm: Terminal will buzzer the alarm for 5 seconds. This alarm can be stop from Tamper screen with Reset, even though it is not really a Tamper Alarm.

GPO: General Purpose Output has three TTL line available, i.e. Line 0, 1 and 2. **Terminal can send Signals** simultaneously through multiple configured GPO lines to the door panel. The signal is sent when following actions are triggered on terminal:

Verify/Identify Passed: After a successful verification

Verify/Identify Failed: After verification failed

Full Administrator User: When administrator with full administrative rights tries to login, an action is triggered on GPO line

Biometric Administrator User: When administrator with database (biometric) administrative rights tries to login, an action is triggered on GPO line

Device Boot up: When a terminal is booted up, either from a power cycle or from a soft reboot.

Tamper Occurred: When Tamper Mode is enabled and if tamper gets triggered i.e. Physical movement of the terminal housing triggers a reed switch which in turn activates user specified Tamper options on the terminal.

Duress Finger Detected: When Duress Mode is enabled at Wiegand line and duress finger is detected.

Banned Listed Card: When the card detected is in Banned List, and user tries to access, an action is triggered through GPO line to the door panel for denying access

User not in Authorized List: When user is not in Authorized listed, action is triggered on GPO line

Pin Mismatch: When PIN entered by user is not matched, an action is triggered through GPO line to the door panel

Time and Attendance Action: If parameters are configured in time and attendance configuration, then on every T&A action, an action is triggered GPO line to door panel/distant systems

NOTE: The settings of GPIO can be done from Web Server. Please refer to the section "*General Purpose Input Output Configuration*" in this document.

SDC Mode:

The administrator can configure Single Door Controller (SDC) mode for controlling access of a single door. Various parameters such as door unlock duration, alarm when door held open, and time over mode can be configured to control access at a particular door. When SDC mode is enabled, GPIO mode is disabled.

Access Path

Terminal Menu :

System Menu > Terminal Settings > SDC/TOM/Tamper > SDC Parameters

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > SDAC

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

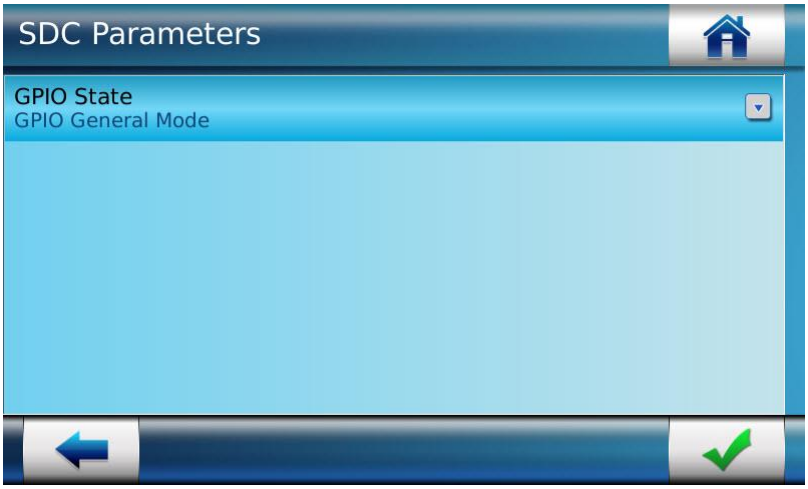


Figure 135: SDC Parameters configuration

1. Press on **GPIO State** to select modes

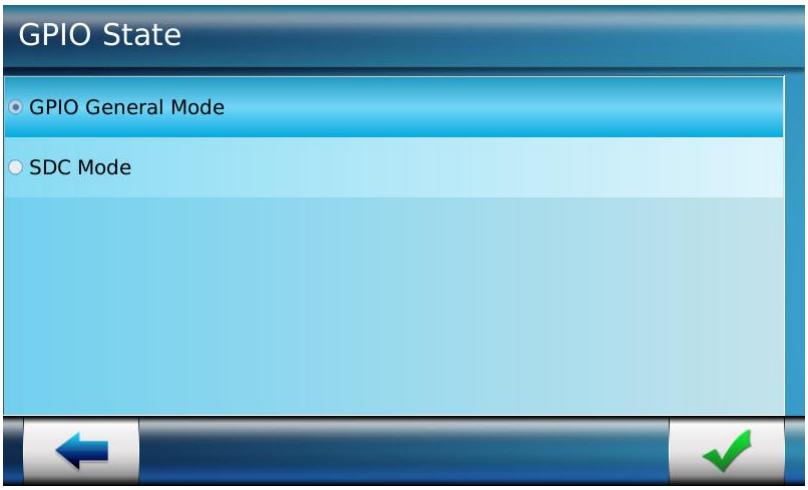


Figure 136: Selecting GPIO State

2. By default, "**GPIO General Mode**" is selected. In order to configure SDC on a terminal, select **SDC Mode**
3. Use Check Button " " to save settings

Figure 137: Configuring Parameters in "SDC Mode"

The administrator can select the following parameters when the **SDC Mode** is enabled.

4. Press on **Door Unlock Time** field to set the 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
5. Press on **Door Held Open Duration**, to set the duration (in Seconds only) within which the door must be closed. Once Door Unlock Time has elapsed and the door has not been closed; the terminal will start counting the Door Held Open Duration. If user has not closed the door within this duration, an auto-alert "Door Held Open Too Long" will be generated on terminal
6. Select the **Exit Mode** as 'None', 'Push button – Manual' or 'Push button – Electric'
7. The administrator needs to set the **Egress Time Out** when Exit Mode is in 'Push Button-Manual' mode. Within the **Egress Time Out** period, the door will remain open and on timeout it will lock automatically. An **Egress Time Out** should be configured between the range of 1 to 300 seconds
8. The administrator can Select **Default Relay State** as 'On' or 'Off' which translates to 'powered' or 'unpowered'.
    a. "OFF" 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. "ON" 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).

Time Override Mode (TOM) Configuration

The administrator can temporarily suspend the need for verification of a user for a specific time period, by using the Time Override Mode (TOM). Whenever TOM is triggered on terminal then door gets unlocked and user can open Door without any authentication till TOM remains active.

Access Path

Terminal Menu :

System Menu > Terminal Settings > SDC/TOM/Tamper > TOM Parameters

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > SDAC > Enable Time Override Mode and Time override Mode Timeout

Pre-requisites

Single Door Access Controller (SDAC) must be enabled

Screens & Steps

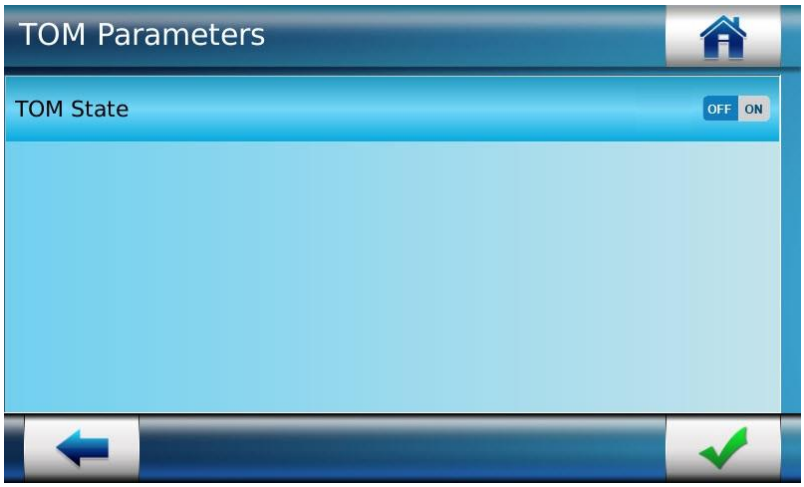


Figure 138: Selecting TOM State as On

1. Select **TOM State** as ON

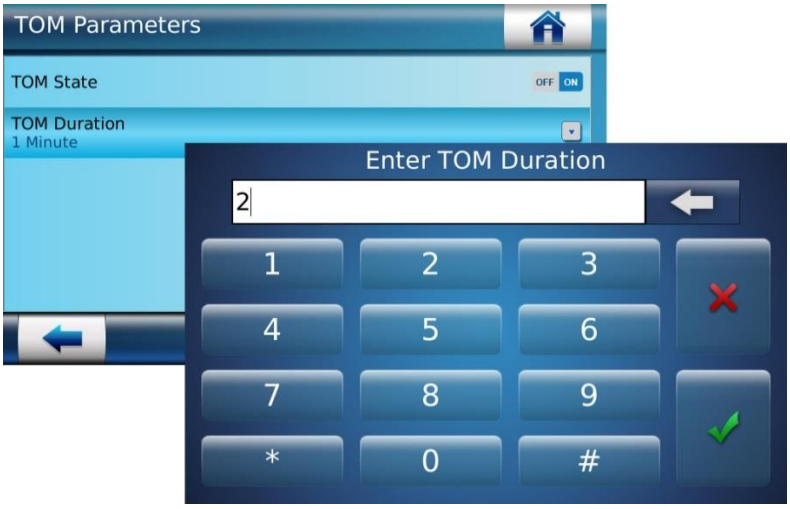


Figure 139: Setting TOM Duration

2. Press on **TOM Duration** to set the duration for which door should be under TOM
3. Enter the number of minutes TOM will be active into the Time Override Duration field and use “ ” button to save
4. Use Check button “ ” to activate TOM on the terminal.

Results

The TOM is set successfully. Thirty seconds before TOM is set to expire, the terminal beeps. After TOM expires, the terminal returns to using the existing SDC settings.

Tamper Configuration for Terminal Security

The Access and Time Biometric Terminal can detect two types of intrusion attempts:

- Someone tries to steal the complete terminal
- Someone tries to open the terminal

The administrator can configure the Tamper parameters in order to take necessary actions on tampering of the terminal. In the event of an intrusion (tamper), Tamper switch is triggered on terminal and Tamper alarm is played on the 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).

NOTE: Tamper switch triggers the alarm message. Please refer to the **Installation Guide** corresponding to your product to identify tamper switch on the terminal.

Access Path

Terminal Menu :

System Menu > Terminal Settings > SDC/TOM/Tamper > Tamper Parameters

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Tamper

Pre-requisite

The administrator must upload the Audio File for Tamper Alarm in the Multimedia settings. Only then the administrator can activate Play MMI for playing sound alarm

Screens & Steps

Figure 140: Enabling Tamper

1. Press on **Tamper State**
2. In next screen, an administrator can set **Tamper State** as Disable or Enable
3. Select **Enable** and use "✓" button to Save

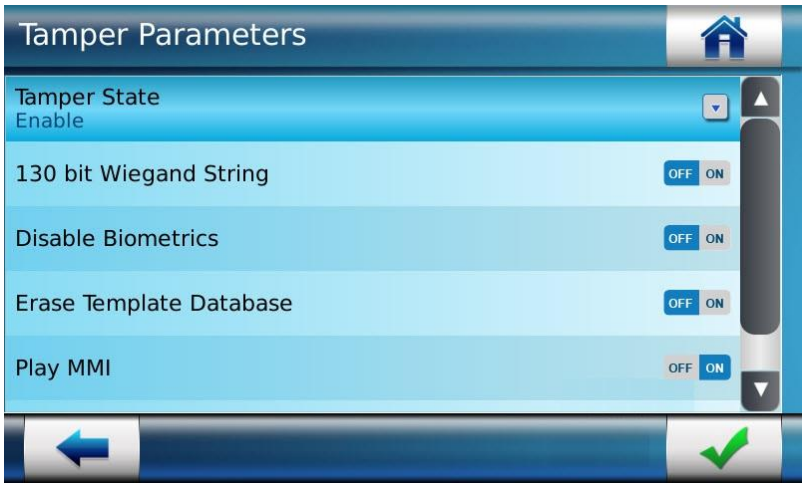


Figure 141: Tamper Parameters Configuration

The administrator needs to configure the following parameters, once the Tamper State is enabled:

4. **130 bits Wiegand String** can be set as ON or OFF. When this parameter is set as ON, then on tamper detection, 130 bits Wiegand string is generated for tamper alarm through a Wiegand output line.
5. **Disable Biometric** The administrator can set this as ON if biometric verification needs to be disabled in the event of a tamper.
6. **Erase Template Database** The administrator turns this as ON/OFF. When ON, all the templates enrolled and saved in the Access and Time Biometric Terminal will be deleted on Tamper detection.
7. **Play MMI** The administrator can set this as ON if it is required to play a sound alarm on tamper detection. The audio file uploaded by the administrator in the system will be played.
8. **Erase Security Data** The administrator can set this as ON or OFF. When this parameter is set as ON, then on tamper detection, the custom site keys stored for all contactless cards will be deleted and reset to the default value.
9. Use "✓" button to **Save.**

Results

Once the Tamper Parameters are configured, possible intrusions can be detected and personal data theft can be prevented. When tamper is triggered, sound alarm is played. Additionally, all of the above mentioned actions if configured as ON, shall be carried out. Once the anti-tamper switches are closed, it is required to set the tamper state as "**Cleared and Re-enabled**". Only then, the tamper alarm will be stopped and terminal will be accessible.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

LCD Settings

The administrator can control the look and feel of the content/multimedia displayed on the LCD touch screen of Access and Time Biometric Terminal's LCD, by using this functionality.

Several Parameters that an administrator can configure are:

- Brightness of the touch screen LCD
- Disable Biometric Sensor when terminal is idle
- Enable or Disable Idle Mode. Basically, an idle mode is when there is no action triggered on LCD. If enabled a video is played when terminal is in Idle Mode
- Set brightness of the video to be played
- Set duration of the video to be played

Access Path

Terminal Menu :

System Menu > Terminal Settings > LCD Settings

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Webserver > MMI (Man-Machine Interface)

Pre-requisites

The administrator must upload the video that is to be played while the screen is idle, using Multimedia settings. Only then the administrator is allowed to configure the video brightness, volume and other parameters.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

Screen Brightness Control

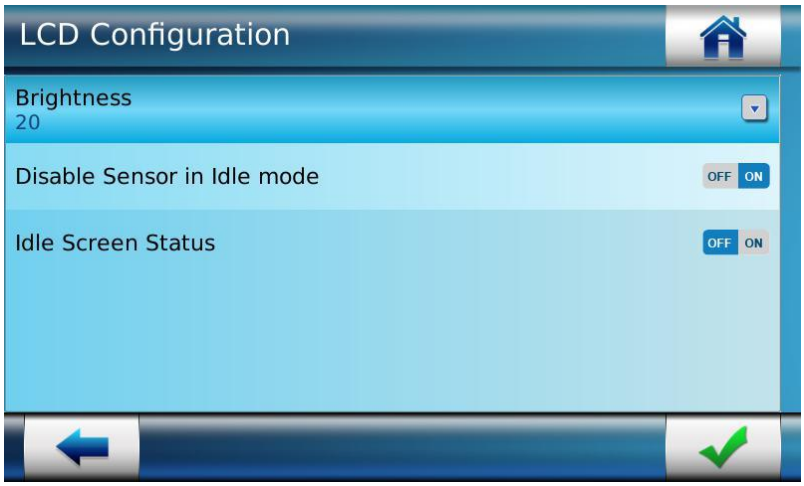


Figure 142: LCD Brightness adjustment

1. Press on **LCD Brightness**
2. On next screen an administrator can adjust the brightness of LCD back light by scrolling the curser left or right

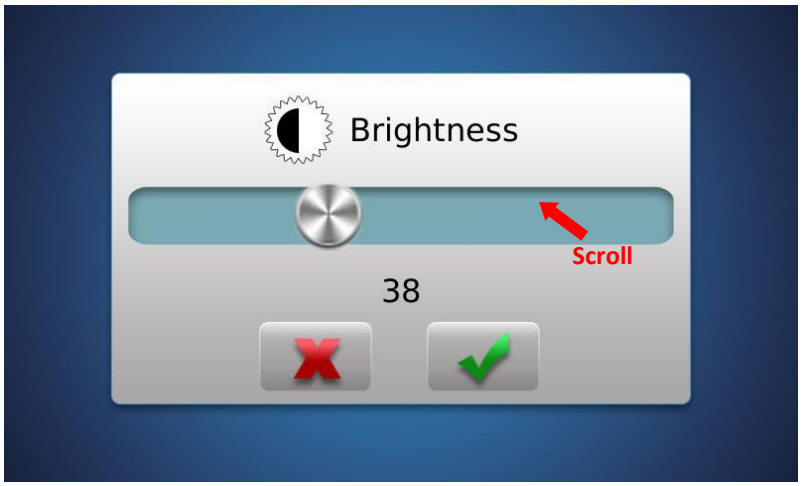


Figure 143: LCD Brightness adjustment

3. Move curser left to reduce brightness and right to increase brightness of the LCD
4. Use " " icon to **Save** setting

Disable Sensor in Idle Mode

The administrator can disable the biometric sensor backlight when terminal is in idle mode, by configuring this parameter. When turned ON, the biometric sensor will automatically power off, if the terminal is in idle mode. This is recommended for power saving. As soon as terminal is in use, the biometric sensor is powered on.

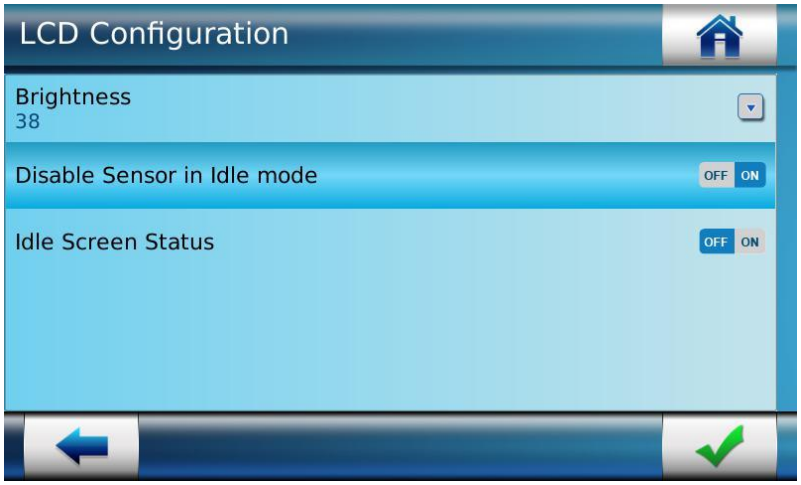


Figure 144: Disable Sensor in Idle Mode

1. Set **ON**, to disable the biometric sensor in idle mode or set it as **OFF** to keep sensor working even in idle mode
2. Use “ ” icon to **Save** setting

NOTE: This option is not available on VisionPass Range terminals.

Idle Screen Status

The administrator sets this to be ON when it is desired that the terminal must be auto locked and a video needs to be played, in case no activity is detected on the terminal. The video to be played can be uploaded in the Idle Screen Video folder, using "Video Settings" functionality under the Multimedia menu.

When the terminal is in idle mode, the biometric sensor is powered off (if the administrator has turned the "Disable Sensor in Idle mode" parameter ON). One can exit the idle mode by touching the text zone on the LCD touch screen.

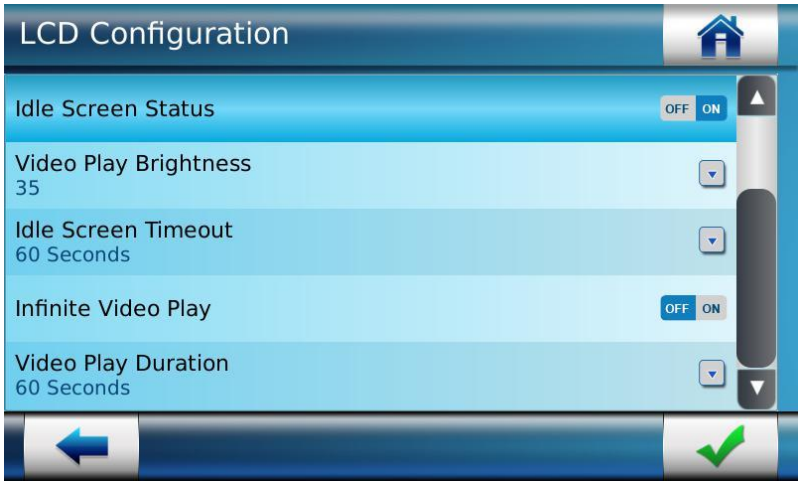


Figure 145: Configuring Idle Screen Status

1. The administrator can set **Idle Screen Status** as ON or OFF.
2. Select status as ON if it is required to auto-lock the terminal when idle.
3. If an administrator select status as OFF, then subsequent parameters to set Video will be disabled, as shown in above screen

Recommendation: If network intensive or database intensive operations are performed on terminal, it can affect the response time of the terminal until this background operation is completed. Hence it is advisable to do such network or database intensive operation when terminal is in idle state.

Video Play Brightness Control

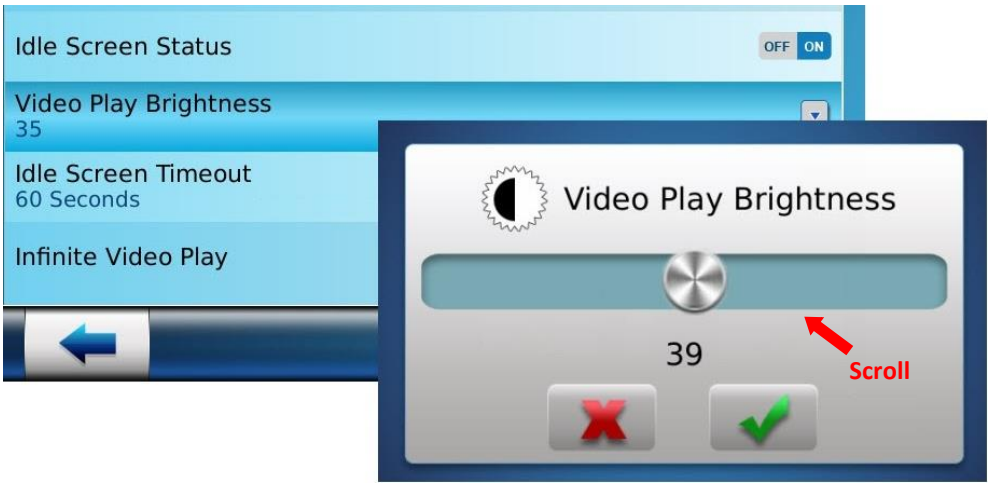


Figure 146: Video Play Brightness Control

1. Press on **Video Play Brightness**
2. In the next screen, the administrator can adjust the brightness of the video by scrolling the curser left or right
3. Move curser left to reduce brightness and right to increase brightness of the Video
4. Use “ ” icon to Save setting

NOTE: This option is not available on VisionPass Range terminals. The video is playing using the LCD Brightness.

Idle Screen Time Out

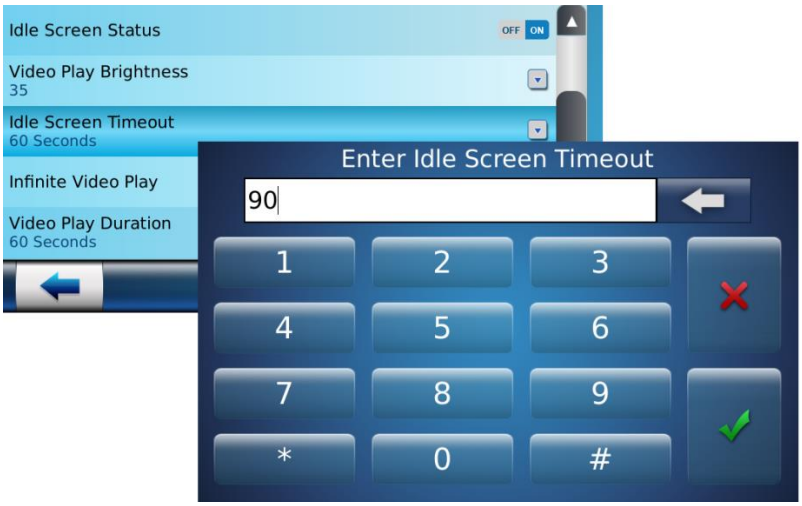


Figure 147: Configuring Idle Screen Timeout

1. Idle Screen Timeout parameter indicates that if there is no action taken on LCD for specified duration, then screen should be auto-locked and video play starts
2. Press on Idle Screen Timeout parameter.
3. On next screen enter duration (in seconds only).
4. Use " " icon to **Save** setting.

Set Infinite Video Play

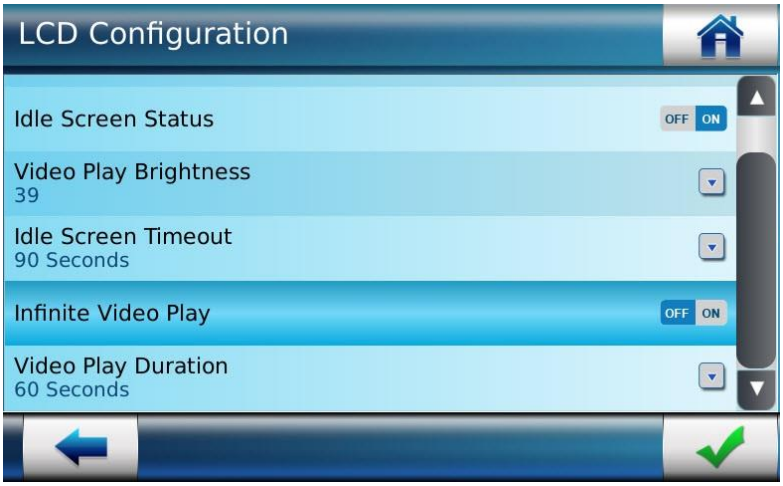


Figure 148: Infinite Video Play on idle screen

1. This parameter indicates whether the video needs to be played on idle screen for infinite duration or not.
2. Select **OFF** or **ON**
3. The administrator must define duration for which video is to be played, if the 'Infinite video play' is set to be OFF.

Video Play Duration

Figure 149: Setting Video Play Duration

1. Press on **Video Play Duration** and enter the number of seconds it is required for the video to be played when terminal is idle.
2. Use " " icon to **Save** setting.
3. Use " " icon on LCD Configuration screen to **Save** all parameters.

Results

Video will be played on the LCD screen as per the configuration done. Once the video play duration is completed, the video will be stopped, and terminal will go into Low Consumption Mode.

Video in Active Mode

1. Select **OFF** or **ON** to disable or enable the play of the video file in background of the Home Screen.

This feature allows to display the video multimedia in background and in loop even if an identification process is ongoing. The video is paused during the display of the user control result and is resumed as soon as the user control result is removed.

NOTE: This option is only available on VisionPass terminal.

Video Phone Configuration

This feature allows user to make a video call from terminal to the customer care center for resolving any queries.

Video phone feature requires server configuration. Refer to “Configure Video Phone / Audio Phone Server” section of this document for more information on Video Phone feature.

NOTE: This option is not available on VisionPass Range terminals.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Transaction Log

The Access and Time Biometric Terminal records each event taken place on a terminal. The events that can be logged are:

- Access granted to the user
- Access denied to the user
- Time and Attendance actions
- Configuration change
- Alarm
- Face detection captured and picture stored (SIGMA Range only)

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, Role of User; Time of trigger, Biometric Matching Score, etc.

The administrator has to export logs using MorphoBioToolBox, Webserver or a USB mass storage device In order to view transaction logs. Refer to "*Export Data in USB Mass Storage Device*" under USB Menu Section.

The administrator could chooses between 2 types of logs:

- Basic Mode : up to 1 000 000, no identifier
- Identified Mode: up to 100 000, each log has a unique identifier

Choose of type of logs is done by setting the configuration key transaction_log.format.

The administrator needs to refer to the subsequent sections in order to understand the parameters that can be configured in the 'Transaction Log'. The administrator who has full Admin Rights to access terminal can able to configure these parameters.

NOTE: We recommend to regularly retrieve and erase transaction logs. Keep too many logs inside the terminal could make it slow down.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Configure Transaction Logging Mode

The administrator can choose as to which event will 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 pass and fail 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

Terminal Menu :

System Menu > Transaction log > Transaction Logging

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Webserver > Logs

Screens & Steps

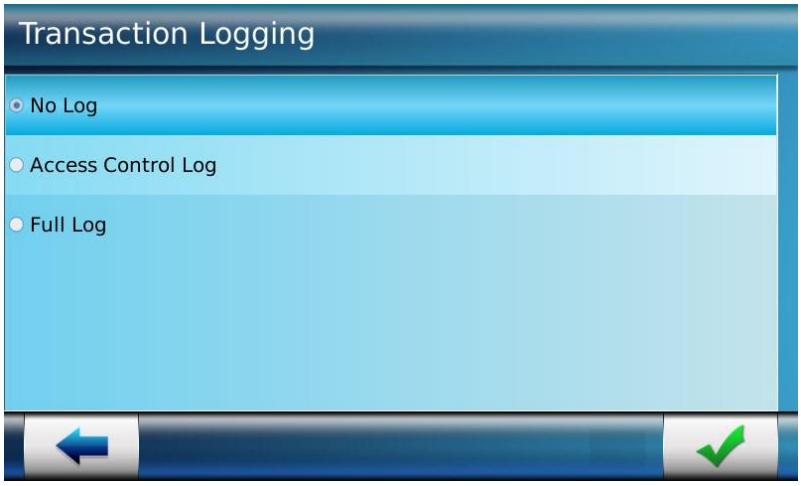


Figure 150: Selecting Transaction Logging Mode

1. Select **Transaction Logging Mode** as 'No Log', 'Access Control Log' or 'Full Log'
2. Press on "✓" 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.

Define Actions on Log Full Event

The administrator can select the action to perform when there is no room for a new log record, by using this functionality:

Delete Partial Logs

Delete Full Logs

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

Access Path

Terminal Menu :

System Menu > Transaction log > Actions on Log Full Event

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Logs > Action on Transaction Log Full

Screens & Steps

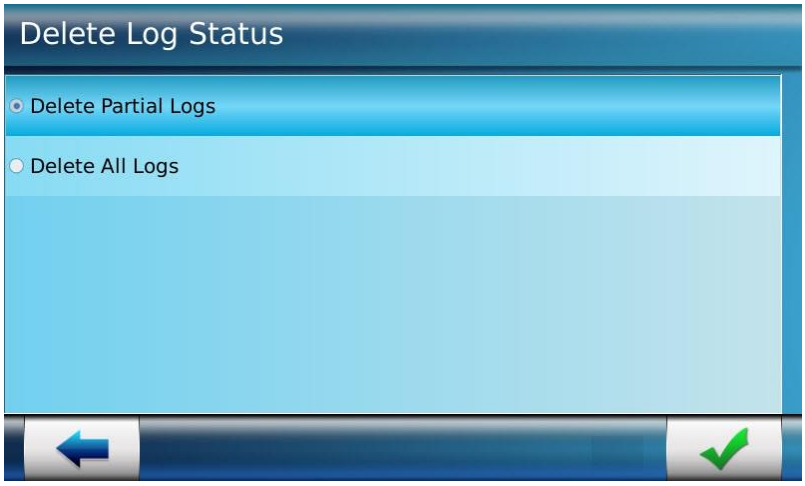


Figure 151: Setting Delete Log Status

1. Select **Delete Log Status** as:
    a. **Delete Partial Logs**, if specific number of logs to be deleted on delete log action triggered

b. **Delete All Logs**, if all logs stored in database should be deleted on delete log action triggered

2. Press on "✓" button to save settings

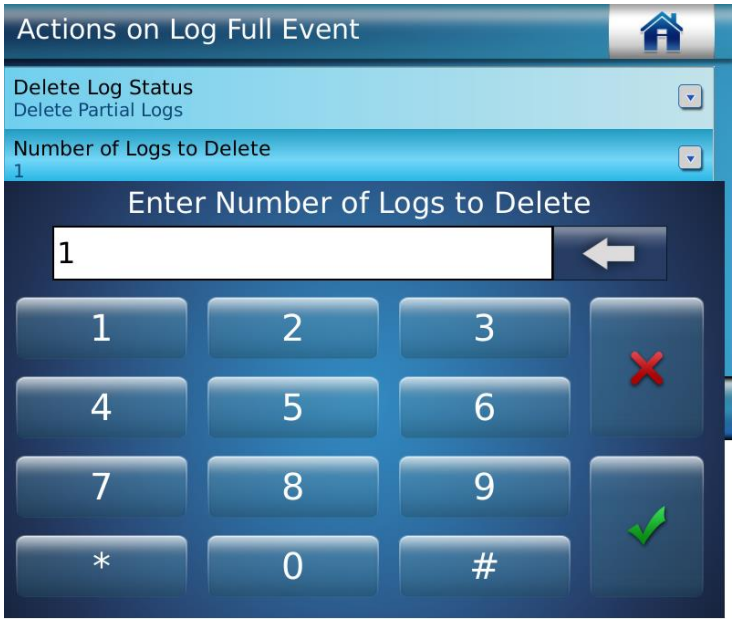


Figure 152: Defining number of logs to be deleted

3. The administrator needs to define **Number of Logs to be Deleted** when delete action is triggered and Delete Partial Logs is set to be ON.
4. Press on "✓" button to save settings

NOTE: We recommend to regularly retrieve and erase transaction logs. Keep too many logs inside the terminal could make it slow down.

Delete Transaction Logs

The administrator can delete all transaction logs recorded and stored in terminal database, by using this functionality.

Access Path

Terminal Menu :

System Menu >Transaction log > Delete All Logs

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Logs > Transaction Log > Delete All Transaction Logs

Screens & Steps

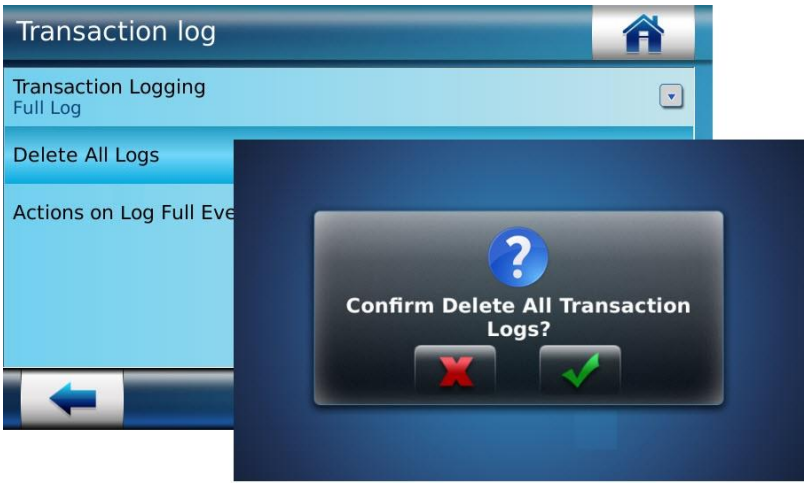


Figure 153: Deleting Transaction logs

1. Press on **Delete All Logs**
2. A confirmation message will pop-up to confirm an action to delete all transaction logs
3. Press on "✓" button to delete. If this is not intended the administrator can Press on "✗" button to cancel

Results

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

Miscellaneous Settings

Global Device Volume

The administrator can set volume of all the audio/video files that are uploaded in the terminal by using Global Terminal Volume.

Access Path

Terminal Menu :

System Menu > Miscellaneous

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

MMI > Audio Volume

Screens & Steps

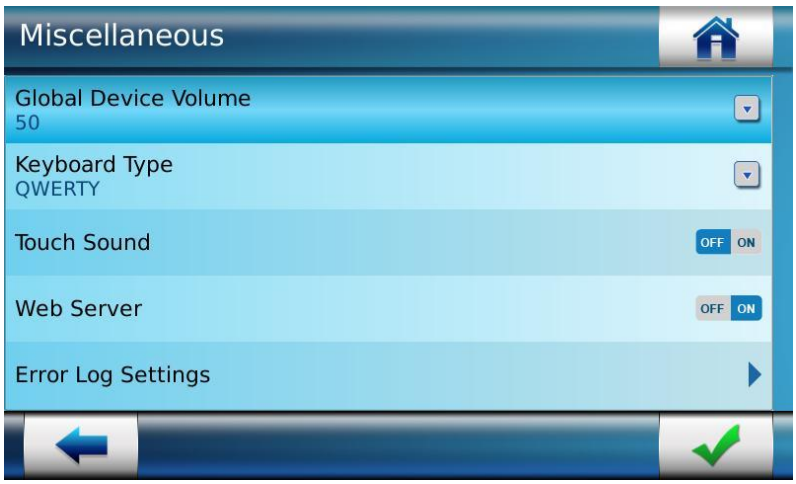


Figure 154: Terminal Global Volume

1. Select **Global Device Volume**

Figure 155: Set Global Device Volume

2. Scroll the radio button to right side for increasing the volume and scroll towards left to decrease the volume
3. Press on " " button to save settings

Results

Sound will be played as per the configured Global Terminal Volume.

References

Refer to "*Multimedia menu*" to know how to upload audio/video files to terminal

Select Keyboard Type

The administrator can select keyboard type, by using this functionality.

The default keyboard for MA SIGMA Range is QWERTY (English standard keyboard).

The default Keyboard for Morpho*Wave*® Compact, Morpho*Wave*® XP2 and VisionPass Range terminals is ALPHABETIC.

Access Path

Terminal Menu :

System Menu > Miscellaneous

Screens & Steps

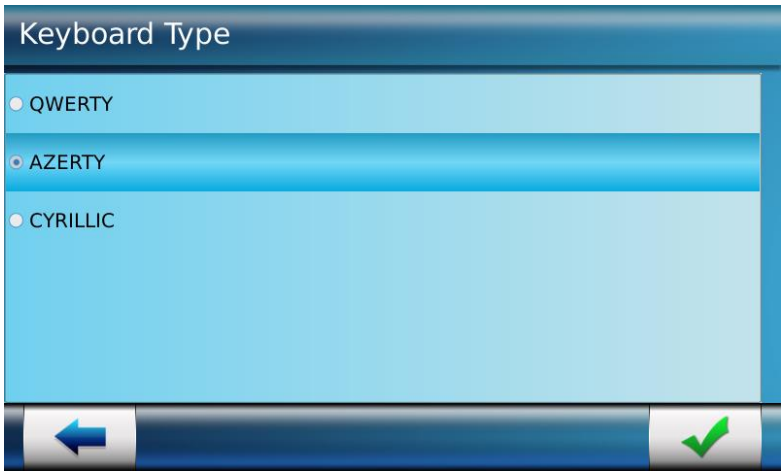


Figure 156: Selection of Keyboard Type

Figure 157: View of of AZERTY Keyboard selection

2. Select Keyboard type & select **AZERTY keyboard** from the drop-down list. Following snapshot depicts the **AZERTY keyboard**:

Figure 158: AZERTY keypad

3. The Cyrillic keyboard is available in following screens for entering First Name & Last Name.
   a. Menu -> User Menu -> Add/Enroll User -> DB Only
   b. Menu -> User Menu -> Edit User
   c. Menu -> User Menu -> Delete User -> Delete User
   d. Menu -> User Menu -> Card Manager -> Renew User Card

Figure 159: CYRILLIC keypad

NOTE: the VisionPass Range terminals supports only ALPHABETIC and CYRILLIC.

Touch Sound

The administrator can configure a Touch Sound. If enabled, a beep sound will be played on every keypress. By default the Touch Sound is disabled in a SIGMA Range Series terminals.

Access Path

Terminal Menu :

System Menu > Terminal Settings > LCD Settings

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Webserver > MMI

Screens & Steps

Figure 160: Touch Sound

NOTE: The Touch Sound feature is not available for VisionPass Range terminals.

Web Server

The administrator can access the Web Server on Access and Time Biometric Terminals, except “MorphoWave® SP”, “MorphoWave® XP2” and “VisionPass SP”. Web Server allows an administrator to configure any parameter of the terminal by connecting remotely. Please refer the “*Access to Administration Menu through Webserver*” in this document.

By default the access to Web Server is disabled in a SIGMA Wide, SIGMA Extreme Series, VisionPass and Morpho*Wave*® Compact terminals and enabled in SIGMA Lite Series and Morpho*Wave*® SP terminals.

Access Path

Terminal Menu :

System Menu > Miscellaneous > Web Server

Screens & Steps

Figure 161: Web Server

1. If the administrator selects **Web Server** as ON, then the terminal can be configured from a remote machine.

Error Log Settings

Access and Time Biometric terminals are capable of capturing logs of the events when access is denied or any error has occurred during operations.

The administrator can enable/disable error logging and configure related parameters, using 'Error log Settings' feature.

Access Path

Terminal Menu :

System Menu > Miscellaneous > Error Log Settings

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Logs > Error Log > Error Logging

Screens & Steps

Figure 162: Select Error Log Configuration

2. Select **Error Log Settings**

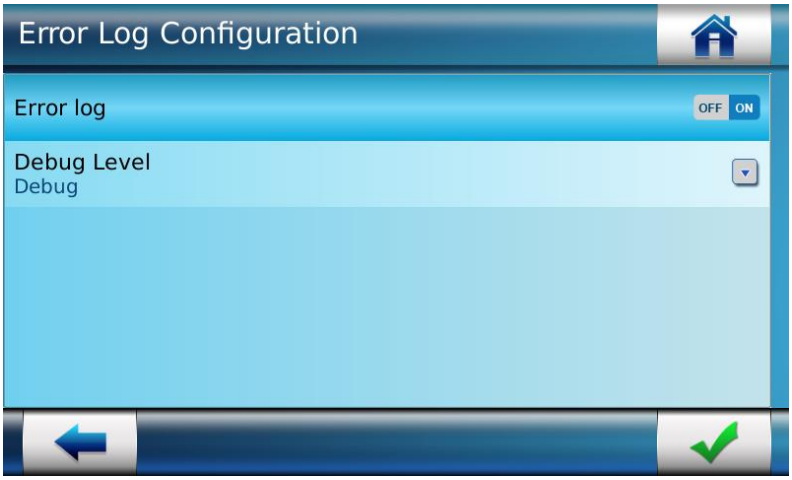


Figure 163: Enable Error Logging

3. Select **Error Log** as ON, to enable error logging

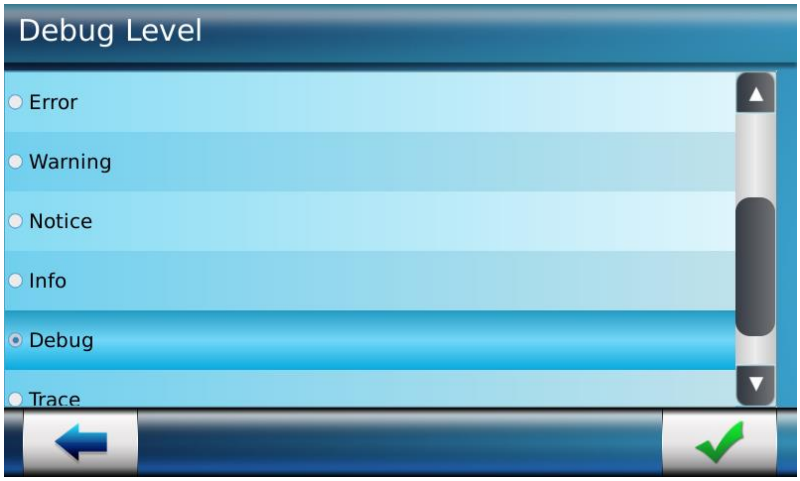


Figure 164: Setting Error Log Debug Level

4. 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: If the administrator selects **Debug Level** as WARNING, then all the messages of the Error, Fatal, Alert and Critical category, will be logged. Messages in the 'Notice', 'Info' , 'Debug' and 'Trace' category will not be displayed.

5. Press on "✔" button to save settings

Results

The Error logs are captured and stored on the terminal. The administrator can use the Export functionality under USB menu, to export the logs. Refer to "*Export Data in USB Mass Storage Device*".

Sensor Log Configuration

Access and Time Biometric terminals are capable of capturing logs of the CBI sensor when any operation is performed on CBI sensor.

The administrator can enable/disable sensor logging, and configure related parameters, by using Sensor log configuration feature.

Access Path

Terminal Menu:

System Menu > Miscellaneous > Error Log Settings

Screens & Steps

Figure 165: Select Error Log Configuration

1. Select **Error Log Settings**

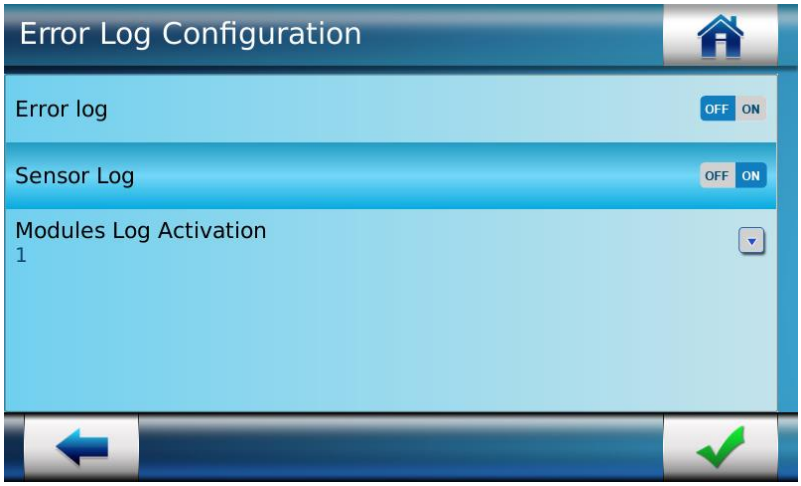


Figure 166: Enable Error Logging

2. Select **Sensor Log** as ON, to enable sensor logging.

Figure 167: Sensor Modules Log Activation

3. Set **Module Log Activation** value in-between 0 to 65535

NOTE: The sensor logs of modules WRAPPER, SDK, IHM, SCFG, LOG, SETTING_SENSOR, IMG_PROCESSING, FFD, DTPR, ACQ_MGR, LIBBIO, BIODB, SRV, PARAM, PAL Modules based on the value set in Module Log Activation will be included in the Error Log File. For example, if an administrator set the value 57343 in Module Log Activation, then the Error Log file will consist of the sensor logs of modules WRAPPER, IHM, SCFG, LOG, SETTING_SENSOR, IMG_PROCESSING, FFD, DTPR, ACQ_MGR, LIBBIO, BIODB, SRV, PARAM, PAL and will not consist log of SDK module.

NOTE: The sensor logs level for VisionPass is the **Debug** level

4. Press on check button to save settings

Communication menu

Access and Time Biometric terminals are standalone terminals, it means the configuration and operations are performed without any connection to a host application. However, Access and Time Biometric Terminals are 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 the following functions:

Connect to Central Access Controller in order to grant or deny the access to the user across multiple locations.

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

Configuring the Wi-Fi™ connection.

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 "*Connect the Terminal to a* PC" to understand in detail.

The administrator can configure network parameters to enable communication with distant systems, using Communication Menu.

NOTE: Only an administrator with full administrative rights can access this menu. In Enforced Security configuration, it requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Figure 168: Communication Menu

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Security recommendation

It is recommended to disable unused communication channels to avoid security issues, however ensure to let at least one way to configure the terminal.

Ethernet Network Configuration

The Access and Time Biometric Terminal can be connected to devices (such as central access controller, and door controller) via **Ethernet.** The administrator can configure an IP Mode, which can be static or DHCP (dynamic). This can be done via 'Ethernet' in the 'Network Configuration' depicted below. For more information on Ethernet Configuration, please refer to "*Ethernet Interface Settings*" under FBA.

Access Path

Terminal Menu :

Communication Menu > Network Interface > Ethernet

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Communication

Screens & Steps

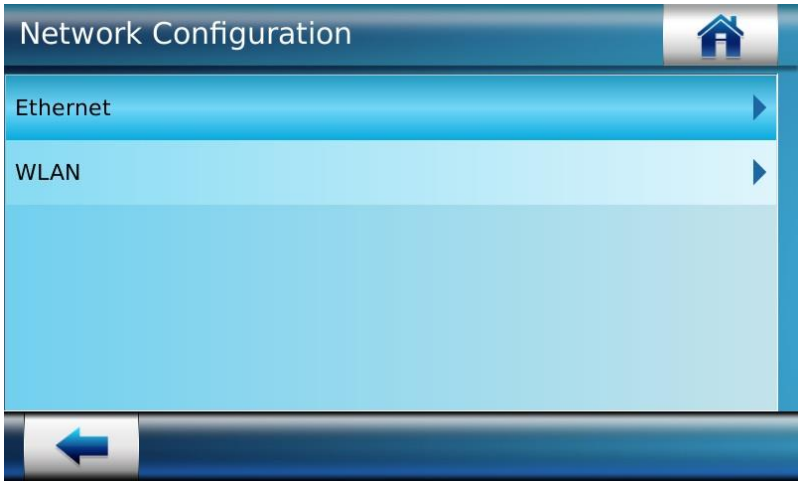


Figure 169: Selecting Ethernet-Network Configuration

6. Select **Ethernet**
7. Select **IP Settings**

Figure 170: Ethernet Configuration

8. Under Ethernet tab, the administrator can select **IPV4** or **IPV6**
9. On next screen, default IP Mode is selected as static. Press on **IP Mode** for update

Figure 171: IP Mode Selection

10. An administrator can select **IP Mode** as 'Static' or 'DHCP'
11. Use Check button " " to save the setting

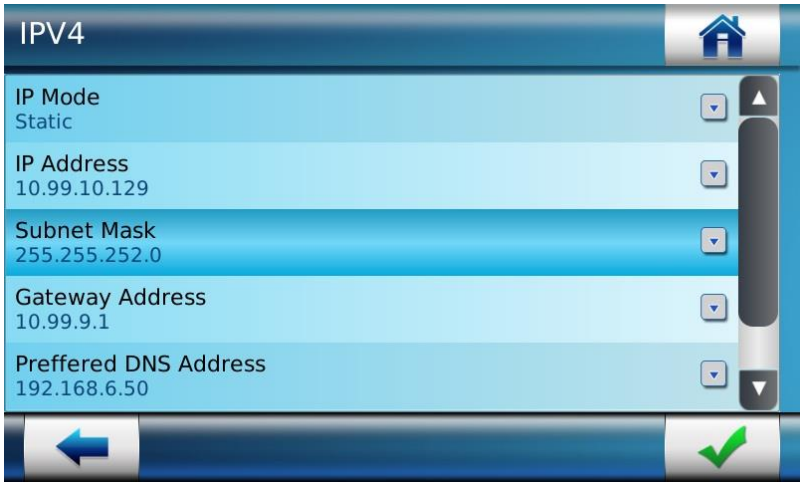


Figure 172: Configuring IP Address under Static IP Mode

12. The administrator can manually configure ‘IP Address’ of the terminal, ‘Subnet Mask’, 'Network Mask', 'Gateway Address' and 'DNS Servers under the Static IP Mode.

Results

Once the Ethernet Configuration is done, the terminal can be connected to a distant server. An administrator can also configure parameters to prevent unauthorized access to the terminal. These settings can be done from Security menu, refer “*Network & Communication Security Settings*”.

Wi-Fi™ Network Configuration

Access and Time Biometric Terminal can be connected to devices (such as central access controller and door controller) via **WLAN (Wi-Fi™ network).** The terminal needs the Wi-Fi™ connection to make operations such as requesting access to the access controller and receiving the result message.

At First Boot Assistant, an administrator can configure the terminal to communicate through WLAN. For detailed description, please refer to “*Wi-Fi Network Configuration*.

Mobile Network Configuration

SIGMA Range terminals can be connected to devices (such as central access controller and door controller) via **Mobile Network.** Using Mobile Network connection, the terminal can make access request to the access controller and receive result message.

The administrator can configure parameters to communicate through Mobile Network from terminal.

NOTE: The Administrator needs to contact mobile network provider for the settings for their network.

Access Path

Terminal Menu :

Communication Menu > Network Interface > Mobile Network

Pre-requisites

3G USB modem must be plugged into the terminal

MA_3G license must be installed on terminal

Screens & Steps

Figure 173: Enter APN

1. Enter APN Name. Press on “ ” button to set.

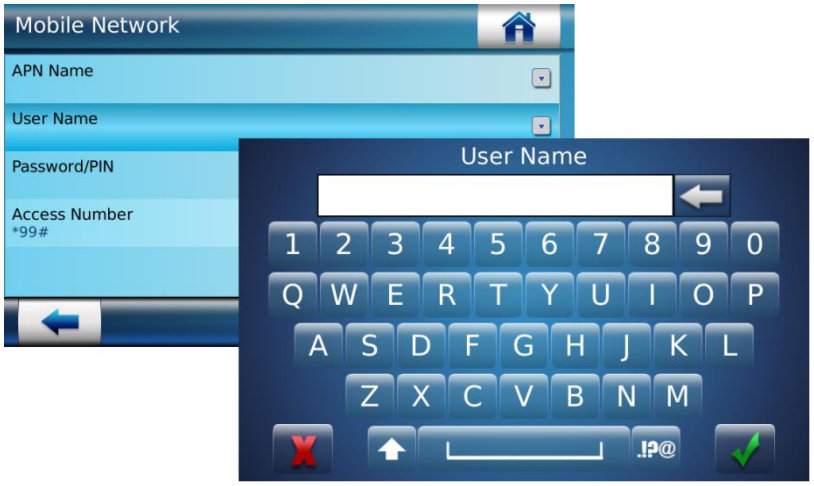


Figure 174: Enter User Name

2. Enter User Name. Press on " " button to set.

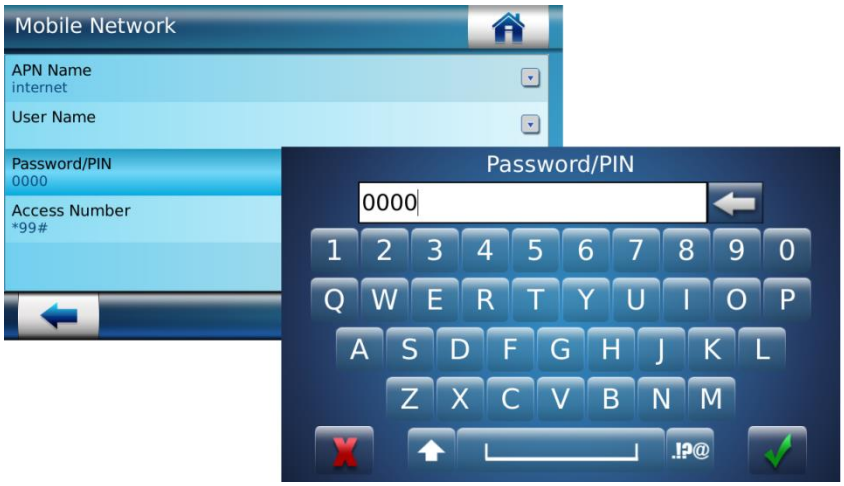


Figure 175: Enter Password / PIN

3. Enter Password / PIN. Press on " " button to set.

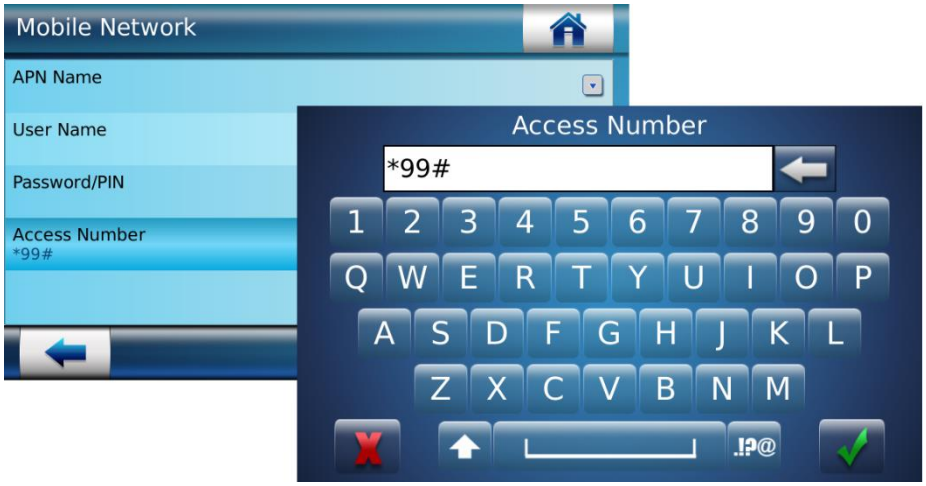


Figure 176: Enter Access Number

4. Enter Access Number. Press on " " button to set.
5. Press on " " button to save all setting on Mobile Network parameter menu.

Configure Hostname

The administrator can configure the Hostname when the IP Mode is selected as DHCP.

The host name is used instead of the IP address, when a DNS (Domain Name Server) exists in the network.

Access Path

Terminal Menu :

Communication Menu > Network Interface > Mobile Network

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Communication > IPv4 Network

Screens & Steps

Figure 177: Configuring Hostname

1. Enter the Hostname, by using the keyboard on terminal
2. Use Check button " " to save the setting

Serial Parameters

Access and Time Biometric Terminal is able to communicate with external controller using Serial Port, through RS422 or RS485 protocols. When terminal is communicating (i.e. receiving inputs and sending outputs) through RS422, it will not be able to communicate through RS485, and vice versa.

Serial channel is also used for sending distant commands to terminal. The administrator can configure parameters of the serial channel from terminal or via Webserver interface.

NOTE: Webserver application cannot use the Serial channel for configuring the terminal

Access Path

Terminal Menu :

Communication Menu > Serial Parameters

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Communication > Serial Configuration

Screens & Steps

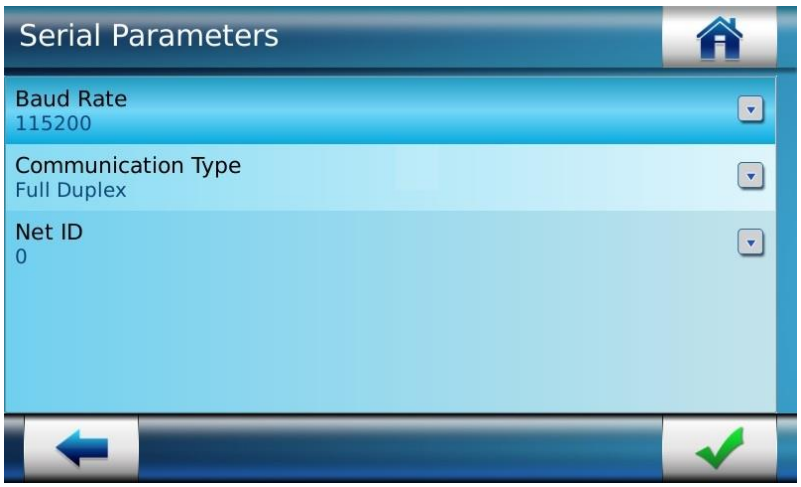


Figure 178: Defining Baud Rate

1. Select **Baud Rate**. Baud rate is the rate of message transmission from Access and Time Biometric Terminal to distant system using serial channel

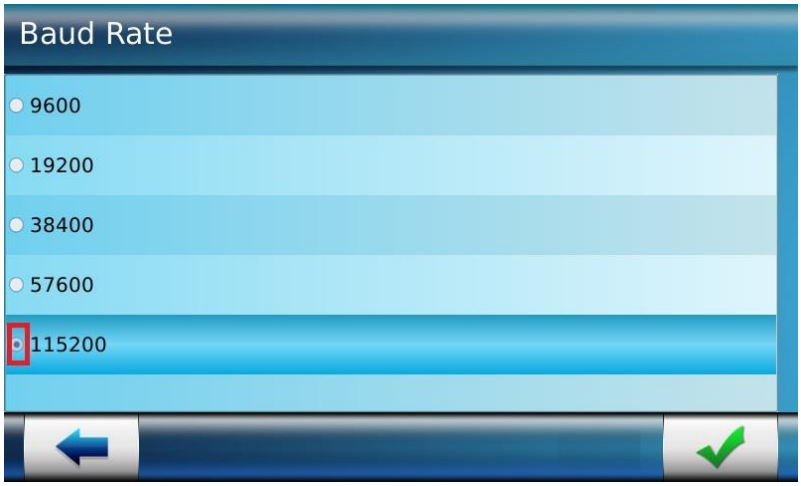


Figure 179: Select Baud Rate

2. The list of supported Baud Rates is displayed. Select the required **Baud Rate**
3. Use Check button “ ” to save

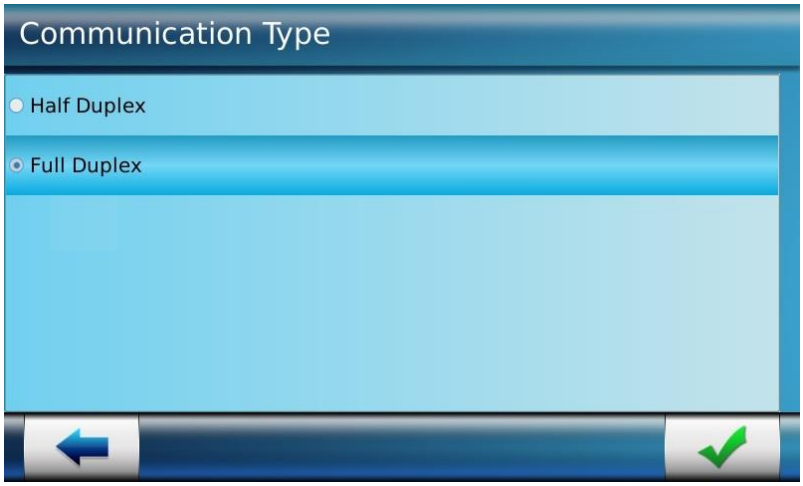


Figure 180: Selecting Communication Type

4. Select **Communication Type** as ‘Half Duplex’ or ‘Full Duplex’
5. Use Check button “ ” to save

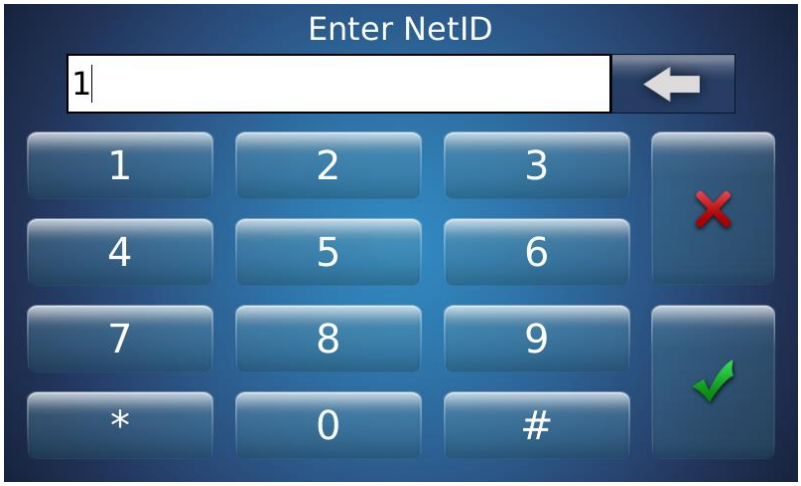


Figure 181: Enter Net ID

6. Enter a **Net ID** (will be used to identify the terminal in a RS485 network connection)
7. Press on " " button to save
8. Use Check button " " on Serial Parameters screen to save all settings

Results

The serial channel parameters are configured successfully. Terminal can communicate with distant systems using serial channel.

Security Menu

The administrator can configure security parameters to guard the Access and Time Biometric Terminal against unauthorized access, by means of the Security Menu. Security menu deals with Biometric control, Network security, multi-user verification, LCD Login Password and User Control.

NOTE: Only an administrator with full administrative rights can access this menu. In Enforced Security configuration, it requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Figure 182: Security Menu

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

User Control Settings

Configure Trigger Events

The administrator can configure as to which of the following events trigger the Access and Time Biometric Terminal. The terminal when triggered, begins the identification and authentication process.

Biometric: a finger, or face, is detected on the biometric sensor, this starts the biometric identification process.

Contactless card: detection of a contactless card, this starts the authentication process with user's data read on the contactless card.

Keypad: detection of a user id entered with touch screen keypad. The entered User ID serves as references for authentication.

External Port: reception of a User ID from Wiegand / Clock and Data port. The received User ID serves as references for authentication.

QR code: a QR code is detected and the authentication process starts with the User ID parsed from the QR code.

NOTE: Refer to the parameter guide for available triggers depending on the terminal

Terminal Menu :

Security Menu > User Control Settings > Trigger Event

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configurations > User Control

Pre-requisites

- Only an administrator with full administrative or database administrative rights, can configure Biometric Security Parameters

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

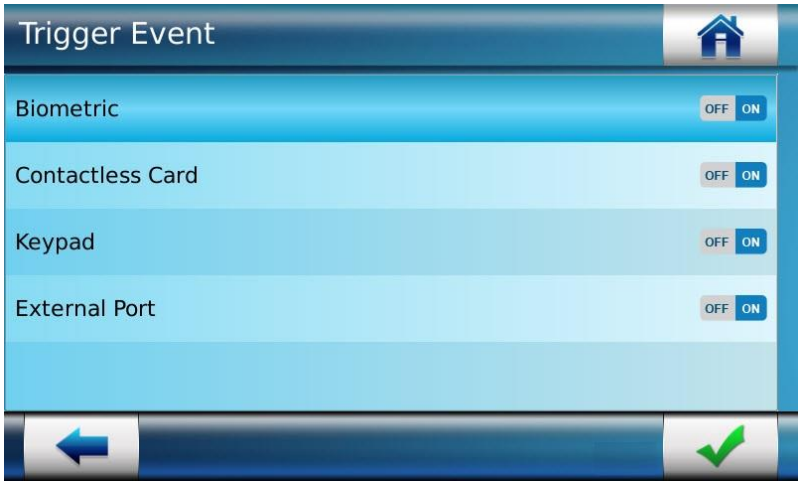


Figure 183: Configuring the events on which authentication/identification is triggered

1. Select the events listed in the trigger event screen (above) as **ON** or **OFF**
2. Use Check button " " to save settings

Set Duress Mode

The administrator can enable Duress Mode in SIGMA Range by using this parameter. The administrator can allow capturing of a user's duress finger in addition to two normal fingers, by setting the Duress Mode. Duress Mode is not available in Morpho*Wave®* and VisionPass terminal ranges.

On detection of a Duress finger, the terminal will send a "Duress Finger Event" to the controller using a communication channel such as IP channels, Wiegand, Clock and Data, RS485/RS422 or TTL outputs.

MMI is played when the Duress finger is successfully authenticated. An MMI for duress finger event is similar to normal finger event on access granted. Refer to "

Audio Settings" for more information about MMI configuration.

Duress Finger Event is logged in transaction logs with action 'Duress Finger detected' on successful identification and action 'VERIFY_DURESS_ID / VERIFY_DURESS_TEMPLATE' on successful authentication. Refer to "*How to Export & View Transaction Logs*" section for more information on exporting and viewing transaction log.

Access Path

Terminal Menu :

Security Menu > User Control Settings > Set Duress Mode

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configurations > User Control

Screens & Steps

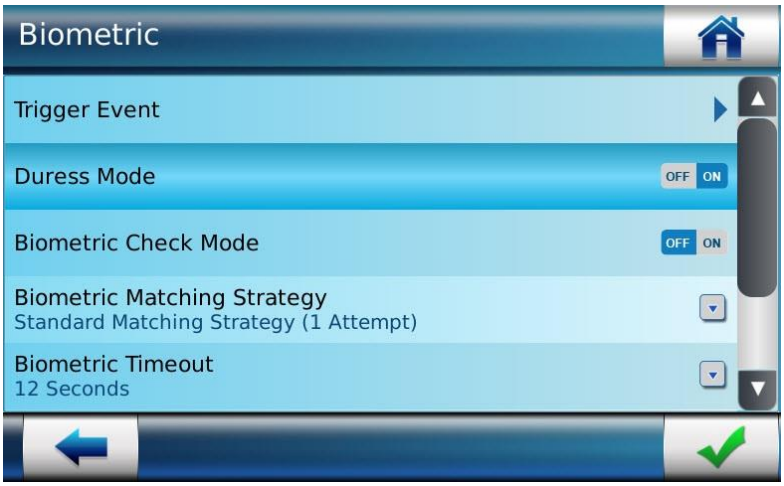


Figure 184: Set Duress Mode

1. An administrator can set **Duress Mode** as ON or OFF. Only if the Duress Mode is on, the terminal will ask for capturing duress finger at the time of enrolment.
2. Use Check button " " to save settings

Biometric Check Mode

If the administrator sets this mode as ON, the captured biometric data is compared with the corresponding one that is stored in the terminal database (identification) or in the card of the user (authentication).

The administrator can set **Biometric Check Mode** as ON or OFF. However it is a 'must' to have user's biometric data in the terminal database or in user's card, if this mode is ON.

If the biometric check mode is OFF, then terminal will not ask user to place finger on the biometric sensor. Instead user can be authenticated using Card and Keypad modes.

Access Path

Terminal Menu :

Security Menu > User Control Settings > Biometric Check mode

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > User Control > Finger Biometric authentication rule

Screens & Steps

Figure 185: Setting Biometric Check Mode

1. Set **Biometric Check Mode** as OFF or ON.
2. Use Check button "✓" to save settings

Number of Biometric Check Attempt

The administrator can configure the Biometric Matching Strategy by means of which multiple biometric check attempts are allowed to the user. This is to reduce the False Rejection Rate

(FRR). For instance, a user is allowed to place again his finger on the biometric sensor for a 2nd try, when the first one fails.

The 2nd try allows the user to upgrade the finger placement, or to place another finger, on fingerprint terminals. On VisionPass, it allows the user to remove hat or any accessory partially hiding his face.

Biometric Check Attempts allows an administrator to set:

Standard Matching Strategy (1 Attempt): If the administrator has configured this mode, the user is allowed to place finger or present face only one time. Access is rejected if the authentication fails in the first attempt.

Advance Matching Strategy (2 Attempts): If the administrator has configured this mode, the user is allowed to place finger up or present face to two times. This means that, if authentication fails on the first attempt, terminal will ask user to place again his finger on the biometric sensor, or present his face, and perform biometric check again.

This matching strategy is not available for VisionPass SP. Indeed, the VisionPass SP terminal is trying to recognize user until success result or timeout.

Parameter Configuration

By default, the **Advance Matching Strategy** mode is enabled. Except for VisionPass terminal, the **Standard Matching Strategy** mode is selected by default.

Please refer to the table below for further details.

Parameter name	Value	Description
auth_param.additional_bio_check_nb_attempt	1, 2 or 3	Set this parameter to '1' to offer only one attempt. If parameter is '2', terminal allow to perform biometric second time after a first incorrect identification/authentication attempt. Setting value to '3' results in workflow similar to two attempts and also enables MFU (Most Frequent User).

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access Path

Terminal Menu :

Security Menu > User Control Settings > Biometric Matching Strategy

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Biometric > Biometric Security Settings > Biometric Matching Strategy

Pre-requisites

The administrator needs to set the Biometric Check Mode as ON

Screens & Steps

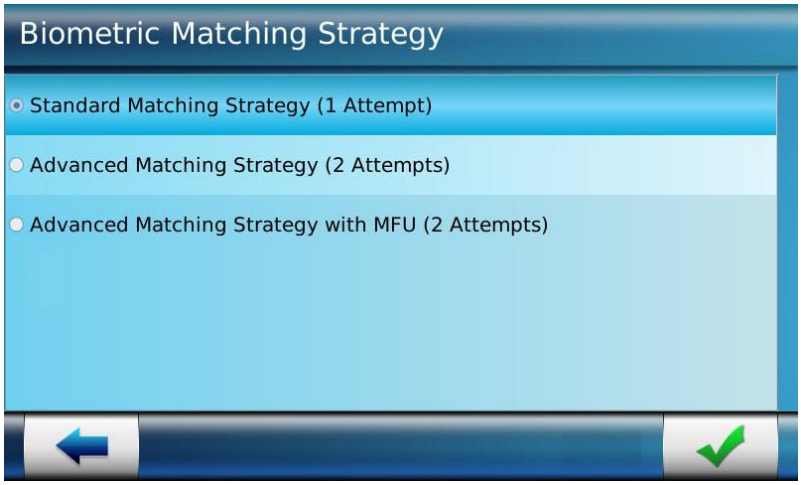


Figure 186: Selecting Biometric Matching Strategy

1. Select **Biometric Matching Strategy** as Standard, Advance or Advanced with MFU

Standard Matching Strategy

NOTE: The **MFU Advanced Matching Strategy Mode** is not available on VisionPass Range terminals.

2. Press on " " button to **Save** settings

Results

Terminal performs biometric check as per the configured strategy.

Biometric Timeout

This parameter defines the duration within which the user needs to place finger, or present his face, to the biometric sensor of the terminal. If user fails to place the finger, or present his face, within that period, the access is rejected.

Using fingerprint terminals, in case of biometric authentication process, after User ID acquisition, the terminal lights on the backlight of the biometric sensor to request the user to place his finger on the sensor. This parameter applies to the wait time for user's finger.

Using fingerprint terminals, in case of biometric identification process, if user's finger is not recognized, the user has 5 seconds to place again one of his fingers on the biometric sensor. If a finger is placed on the sensor after this delay, then the terminal processes it as a new access request.

The value of this delay is defined by a dedicated parameter:

Parameter name	Value	Description
auth_param.additional_bio_check_timeout	2 – 60	Time allowed to the user, to place again his finger, or present his face, after a first identification which fails. The time can be defined in terms of seconds.

An administrator can follow below screens and steps to configure timeout from terminal.

Access Path

Terminal Menu :

Security Menu > User Control Settings > Biometric Timeout

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Biometric > Biometric Security Settings > Biometric Timeout

Pre-requisites

Biometric Check Mode should be set as ON

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

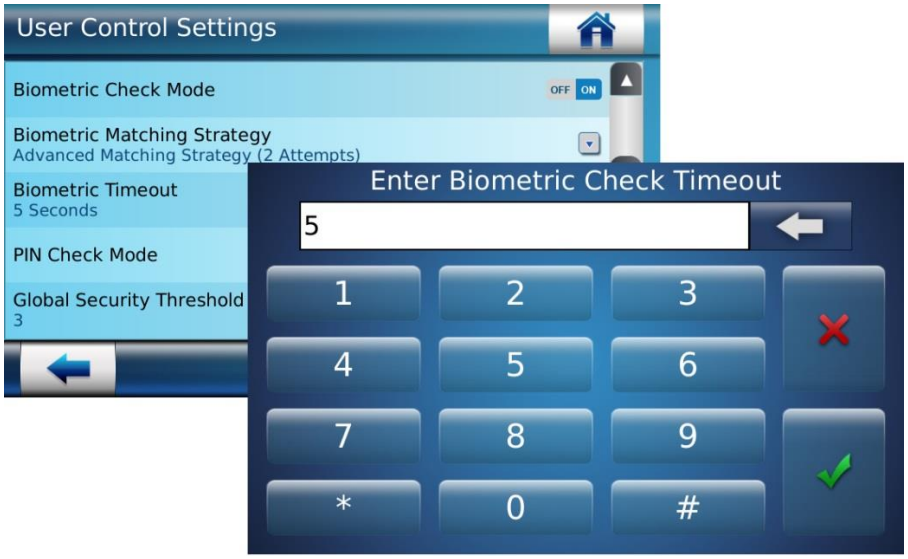


Figure 187: Biometric Time Out

1. Enter the duration for Biometric Check Timeout. The entered duration is in terms of seconds
2. Use “ ” to save settings

NOTE: Whatever the duration for Biometric Check Timeout, SIGMA Lite will blink yellow 5 seconds after first unsuccessful biometric attempt before to come back to blue default light. Second biometric attempt could be done during all Biometric Check Timeout duration, whatever the light, yellow blinking or blue fix.

PIN Check Mode

At the time of enrolment, administrator can provide the PIN code along with the biometric data of the user. The administrator can enable **PIN Check Mode** if it is required to authenticate users based on the entered PIN.

In **Identification Mode**, if match is found in database, for the biometric data provided by the user, then the terminal requests the user to enter his PIN code. Access is granted, only if the PIN entered matches with the PIN value stored in database for the user. If the administrator has disabled the biometric mode, the user identification is done based on the entered value of the PIN.

Note: The administrator must set the trigger event through biometric for performing identification.

In **Authentication Mode**, the user will have to enter User ID followed by Fingerprint or face recognition. If biometry of the user matches with the corresponding one in the database, then terminal will ask user to enter PIN. Only on successful PIN verification, user access is granted. In case the administrator has disabled the biometric check mode, user authentication is done based on the User ID and PIN.

PIN Check Mode if enabled with Biometric Check Mode, makes the authentication process strong and provides better security.

Access Path

Terminal Menu :

Security Menu > User Control Settings > PIN Check Mode

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > User Control > Pin authentication rule

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

Figure 188: Setting PIN Check Mode

1. Set **PIN Check Mode** as OFF or ON.

PIN Check Attempts

The administrator can set this parameter, it indicates the maximum number of attempts a user can get before entering the correct PIN. This feature is helpful in reducing False Rejection Rate, by allowing users to enter PIN accurately on 2nd try.

Access Path

Terminal Menu :

Security Menu > User Control Settings > PIN Check Attempts

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Biometric > Biometric Security Settings > Additional Pin Number of Attempts

Pre-requisites

PIN Check Mode should be set as ON

Screens & Steps

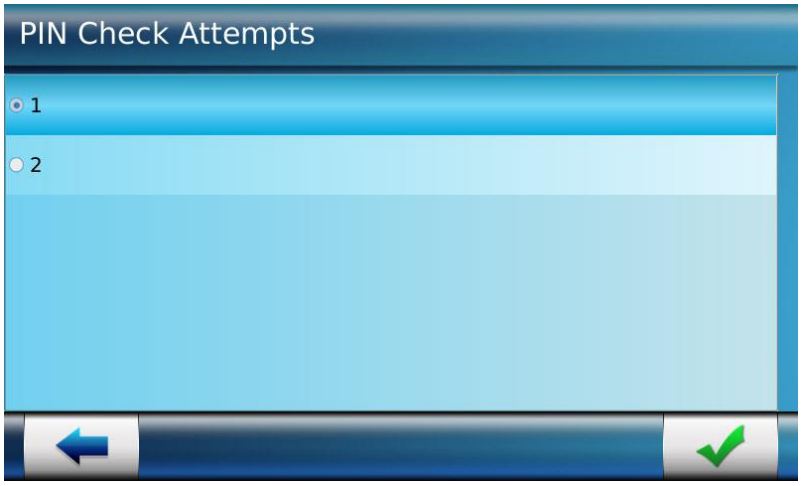


Figure 189: Setting number of PIN Check Attempts

1. Select number of PIN Check Attempts as 1 or 2
2. Press on “ ” button to **Save** settings

PIN Check Time Out

The administrator can configure the PIN Check Time Out. This stands for the duration within which user is required to enter PIN. By default, the PIN Check Time Out is set as 5 seconds, the terminal will deny access, if user fails to enter PIN within the time limit. On access denied, user is again required to enter User ID, biometry and PIN for authentication.

Access Path

Terminal Menu :

Security Menu > User Control Settings > PIN Check Time Out

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Biometric > Biometric Security Settings Additional Pin Number of Attempts > Pin Check Timeout (in seconds)

Pre-requisites

PIN Check Mode should be set as ON

Screens & Steps

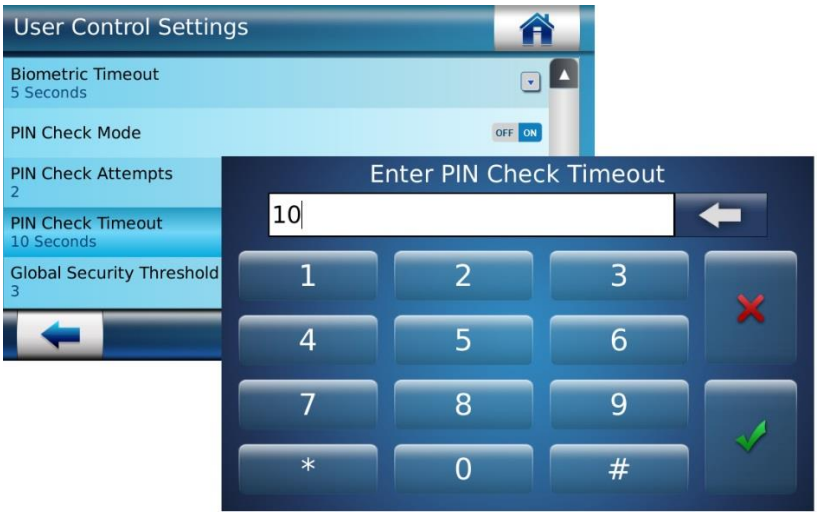


Figure 190: Setting PIN Check Timeout

1. Enter the duration for Pin Check Timeout. The entered duration is in terms of seconds
2. Use " " to save settings

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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.

The FAR value can be set according to the level of security decided by the administrator who typically is at the customer's end. 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 terminal depending on the security level targeted.

Parameter Configuration

The False Acceptance Rate is tuned by a parameter value, which means higher the parameter value lower is the FAR value.

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 corresponding one in the database.
bio_security_settings. authentication_matching_threshold	0 to 10	Using this parameter, an administrator can set the threshold for matching the biometric data provided by the user for authentication, with the corresponding one in the database

Matching threshold values are detailed in the table below:

Value	Description

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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.

NOTE: 2,4,10 Matching threshold values are not supported for VisionPass Range terminals.

Access Path

Terminal Menu :

Identification Threshold: Security Menu > User Control Settings > Identification Threshold

Authentication Threshold: Security Menu > User Control Settings > Authentication Threshold

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Biometric

Screens & Steps

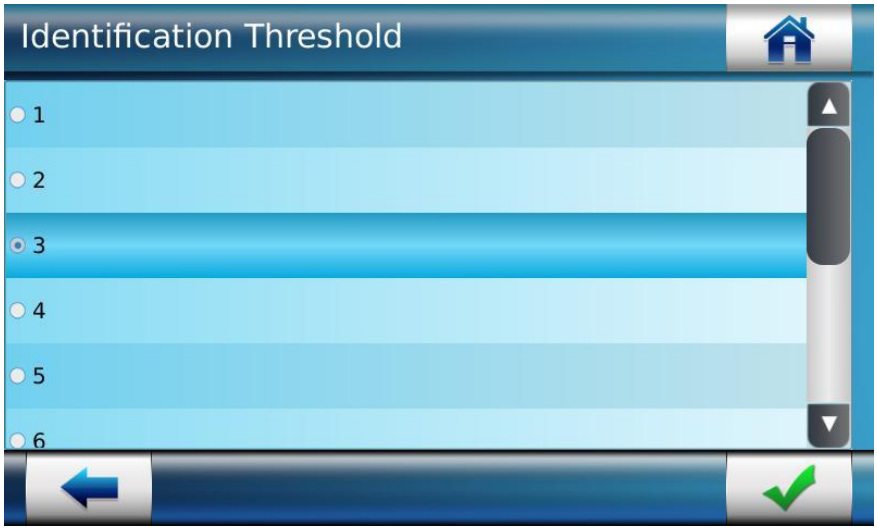


Figure 191: Identification Threshold

Figure 192: Authentication Threshold

1. Select **Identification/Authentication Threshold** from values 0 to 10

NOTE: 2,4,10 Matching threshold values are not supported for VisionPass Range terminals.

2. Press on “ ” button to **Save** settings

Results

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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Anti-Tamper Switch For Terminal Security

Description

The Access and Time Biometric Terminal is able to detect the opening of the box. This detection is controlled by the anti-tamper switch attached in the terminal. The opening of the external USB port cover is not detected.

The administrator can configure the response of the terminal, upon the occurrence of such an event.

Ignore the event (default setting): useful during normal maintenance operations.

- Send an alarm message to a distant system through the channel already used by the access control result messages (see *Sending an Access Control Result Message* section),
- Emits a local audible signal (see *Terminal States* section).
- Deletes biometric database
- Erase security data (such as contactless authentication keys)

The format of the alarm message is described in the **Host System and Remote Message Interfaces** document.

NOTE: if VisionPass SP terminal is power off with the anti-tamper switch open, it will immediately lost date and time.

References

Refer to section "*Tamper Configuration for Terminal Security*" to configure tamper parameters from the terminal administration menu.

- Please refer to the **Installation Guide** for more information about the location of the anti-tamper switch on the terminal.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Parameter Configuration

The action(s) to be performed by the terminal on tamper detection is defined by several dedicated parameters:

Parameter Name	Parameter Value	Description
tamper.state	0 or 1	Tamper detection can be enabled or disabled. “0” for disabling the tamper detection “1” for enabling the tamper detection.
tamper.action_auth_iden	0 or 1	“0” indicates that authentication is not disabled on tamper detection. “1” indicates that authentication is disabled on tamper detection.
tamper.action_erase_biometrics	0 or 1	“0” indicates biometric database is not erased on tamper detection. “1” indicates biometric database is erased on tamper detection.
tamper.action_erase_security_data	0 or 1	“0” indicates security data is not erased on tamper detection. “1” indicates security data is erased on tamper detection.
tamper.action_play_mmi	0 or 1	The administrator can configure this parameter to play MMI (Audio), if tamper event is detected. “0” indicates MMI is not played on tamper detection. “1” indicates MMI is played on tamper detection.
tamper.alarm_interval	1500 milliseconds (default)	The administrator can configure alarm interval to send tamper remote message, by using this parameter. As per the defined duration of interval, the tamper alarm is sent to distant systems.

Since the anti-tamper alarm message is sent via the same port/protocol as the access control result messages, the administrator must enable this function, otherwise the alarm message will not be sent (see section “*Sending an Access Control Result Message*”)

Alarm Message Sent through Wiegand or Clock & Data

If the administrator needs to send the alarm message through the serial port using Wiegand or Clock & Data protocol; it is mandatory to set below:

Enable **Tamper event**, to be triggered and send to controller on tamper detection.

Enable **Tamper Cleared** event, to be triggered and send to controller. Only when Tamper Clear button is pressed, the tamper alarm is stopped and tamper cleared event is sent to controller

Wiegand Output is activated and External Port Output type is selected as Wiegand

Configure Wiegand Parameter "**wiegand.event_tamper**". It allows setting a Wiegand Output Format which will be used to send the Device Serial Number as ID to alert the door controller about the tamper detection.

Below are the parameter values which can be set for defining Wiegand string format:

Parameter Values	Format Type	Description
0	tamper_wiegand_fmt_none	No Format
1	wiegand_fmt_130_bit_serial_number	Generate 130 bit Wiegand string containing 128 bit terminal serial number
10	wiegand_fmt_custom_slot0	Custom Wiegand format slot 0
11	wiegand_fmt_custom_slot1	Custom Wiegand format slot 1
12	wiegand_fmt_custom_slot2	Custom Wiegand format slot 2
13	wiegand_fmt_custom_slot3	Custom Wiegand format slot 3
14	wiegand_fmt_custom_slot4	Custom Wiegand format slot 4
15	wiegand_fmt_custom_slot5	Custom Wiegand format slot 5
16	wiegand_fmt_custom_slot6	Custom Wiegand format slot 6
17	wiegand_fmt_custom_slot7	Custom Wiegand format slot 7

Here, Custom Slot indicates the customer format defined for sending Wiegand String. Custom Format can only be set in parameter, if format is defined in corresponding slot.

Configure parameter "**remote_msg_conf.interface**" is set as value '3', which indicates communication is done using Wiegand channel

An administrator can also set Clock and Data Identifier for sending alarm message, 65535 (0 – 65535). See "*Event Configuration*".

For output to be sent in Clock and Data format, **External port output type** should be selected as Clock and Data. See "*Wiegand Parameter Settings*".

Tamper Alarm message using UDP

The administrator can configure the terminal to send an alarm message to a distant system, in case of a tamper event. This communication can happen through Ethernet (or Wi-Fi™), using UDP protocol.

The administrator needs to configure parameters such as "**remote_msg_ip_conf.host_1_protocol**" to 1. This is for enabling communication using UDP protocol

Parameter Name	Parameter Values	Format Type	Description
remote_msg_ip_conf.host_1_protocol	0	Host_TCP	uses TCP protocol for communication (Default)
	1	Host_UDP	uses UDP protocol for communication
	2	Host_SSL	uses SSL over TCP for communication

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Network & Communication Security Settings

Authorized IP Configuration

The administrator can use this feature to specify the IP address of the computers that are allowed to communicate with the terminal. Connection requests to the terminal will be rejected for the computers with an IP address not present in the list, despite having a compatible configuration application.

This is a security feature that prevents situations such as modification to the terminal configuration from an unauthorized source.

Access Path

Terminal Menu :

Security Menu > Communication > Authorized IP Configuration

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® Range Series" and "VisionPass SP"):

Terminal Settings > Communication > Ethernet Security

Screens & Steps

Set Authorized IP Mode

Figure 193: Authorized IP addresses Configuration

1. Select **Authorized IP address Configuration**

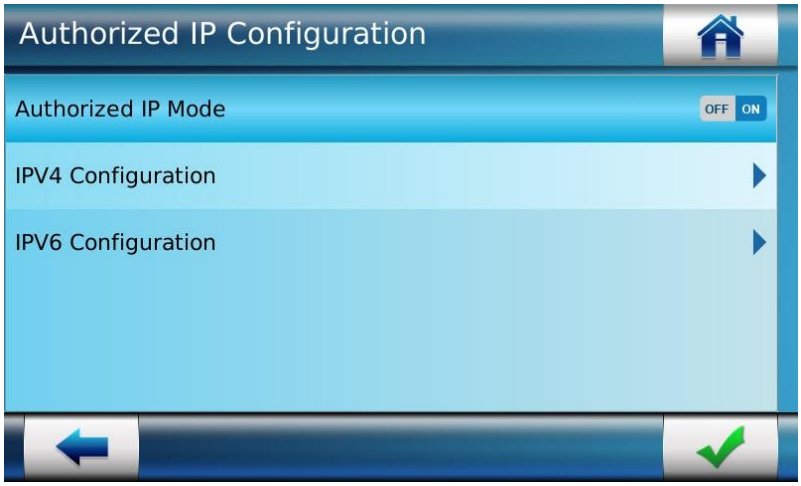


Figure 194: Authorized IP addresses Mode selection

2. The administrator can set the **Authorized IP Mode** as ON or OFF. If this is set as OFF, then any IP address is allowed to connect and communicate with the terminal. If this is set as ON, then the administrator requires adding IP addresses that are authorized to communicate with the terminal.

Add Authorized IP Address

The administrator can add several IP addresses which are authorized to communicate with the terminal, by using this function.

1. Enter IP Addresses by selecting required protocol, i.e. **IPV4** or **IPV6**

Figure 195: Adding IP for authorization

2. Select **Add IP Address**

Figure 196: Add IP address

3. The administrator can Add IP Address of the computer that can talk to the terminal.
4. Press on “ ” icon to save

Figure 197: A success message is displayed showing IP Address is added successfully

Configure IP Addresses Range

The administrator can add an IP Address Range, this is to authorize computers having IP addresses in the specified range to communicate with the terminal. None other than the specified range of computers can communicate with the terminal.

Figure 198: Entering IP Range for authorizing

1. Select **Add IP Range**. Enter **Start IP Address**
2. Enter End IP Address
3. Press on “ ” icon to save

View IP Address

The administrator can view the IP Addresses that are added and authorized to communicate with the terminal, by using this functionality.

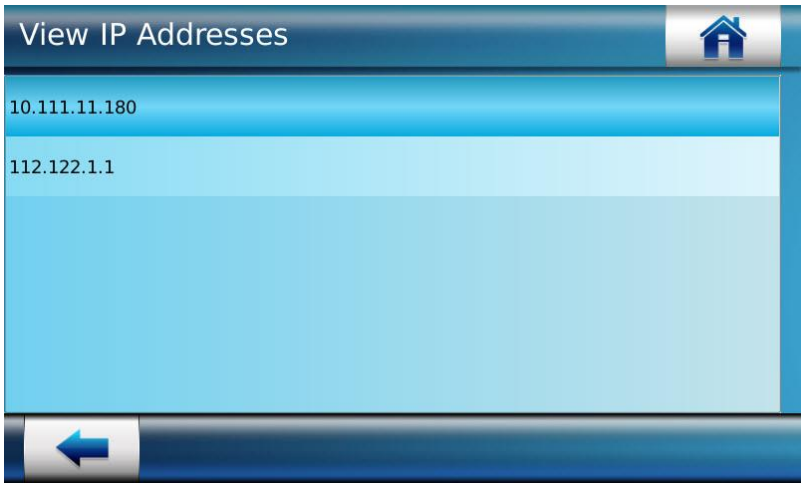


Figure 199: Viewing authorized IP Addresses

1. Press on **Authorized Addresses**. List of IP Addresses authorized is displayed

View IP Range

The administrator can view the Range of IP Addresses that are added and authorized to communicate with terminal, by using this functionality.

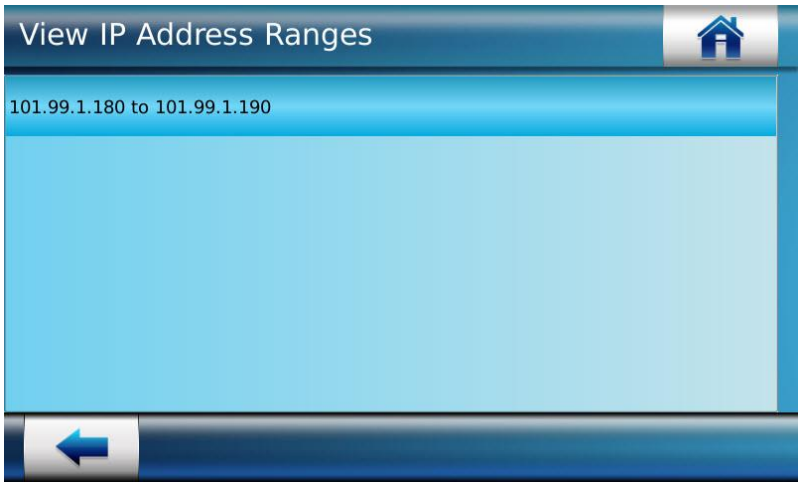


Figure 200: Viewing IP Address Range

1. Press on **Authorized Ranges**. List of IP Ranges authorized is displayed

Delete IP Address

The administrator can delete an IP Address, by using this functionality. It allows the administrator to select several IP addresses and delete them. Once deleted, that computer cannot communicate with the terminal.

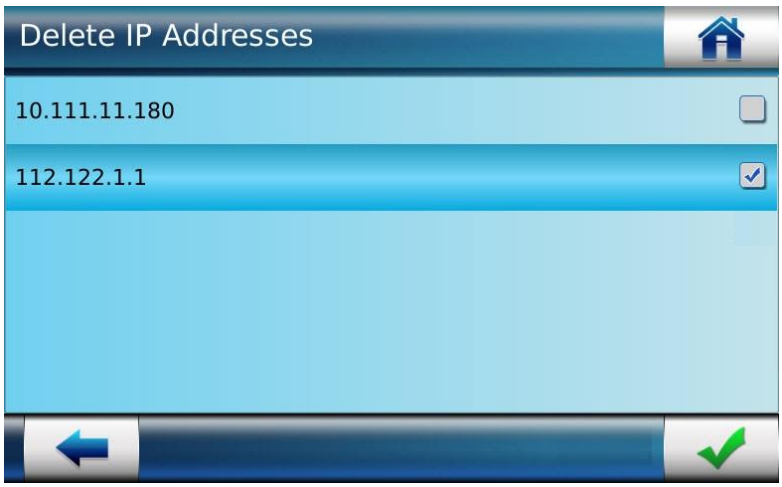


Figure 201: Deleting an IP Address

1. Select an **IP Address** that the administrator needs to delete.
2. Press on “ ” to delete an IP address.
3. A confirmation message is displayed showing IP address is deleted

Delete IP Address Range

The administrator can delete an IP Address Range, by using this functionality. It allows an administrator to select several IP addresses range and delete them. Once deleted, computers having IP addresses in that range are not allowed to communicate with terminal.

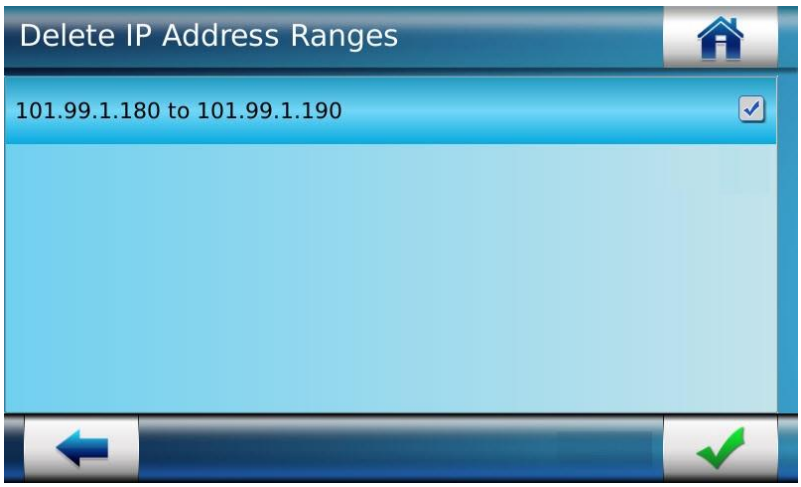


Figure 202: Delete an IP Address Ranges

1. Select an **IP Address Range** that the administrator needs to delete.
2. Use “ ” to delete
3. A confirmation message is displayed showing that the IP Address Range is deleted

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 Access and Time Biometric 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:

- From SSL v3 to TLS 1.2 for all terminals
- TLS 1.3 for “MorphoWave® SP”, “MorphoWave® XP2” and “VisionPass SP”

The terminal supports the algorithms listed below for communication security:

Compatibility of cipher algorithms with SSL protocol versions

In Enforced Security configuration:

	Protocol Version		
Cipher Algorithm List	sslv23 (TLS1.2, TLS1.3)	tlsv1.2	TLS1.3 (MWSP only)
ECDHE-ECDSA-AES128-GCM-SHA256 TLS_AES_128_GCM_SHA256	Y	Y	Y
ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_AES256_GCM_SHA384	Y	Y	Y
ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_AES_128_GCM_SHA256	Y	Y	Y
ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_AES256_GCM_SHA384	Y	Y	Y

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

In On-Demand security mode:

Cipher Algorithm List	Protocol Version					
	sslv23 (TLS1.2, TLS1.3)	sslv3	tlsv1	tlsv1.1	tlsv1.2	tls1.3 (MWSP only)
AES128-SHA	Y**	Y	Y	Y	Y	N
AES256-SHA	Y**	Y	Y	Y	Y	N
AES128-SHA256	Y**	N	N	N	Y	N
AES256-SHA256	Y**	N	N	N	Y	N
AES128-GCM-SHA256	Y**	N	N	N	Y	N
ECDHE-ECDSA-AES256-SHA:ECDH-ECDSA-AES256-SHA	Y**	Y	Y	Y	Y	N
ECDHE-ECDSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256: /TLS_AES_128_GCM_SHA256	Y** /Y*	N	N	N	Y	Y
ECDHE-ECDSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256	Y**	N	N	N	Y	N
ECDHE-ECDSA-AES128-SHA:ECDH-ECDSA-AES128-SHA	Y**	Y	Y	Y	Y	N
ECDHE_RSA_WITH_AES_128_GCM_SHA256:/ TLS_AES_128_GCM_SHA256	Y	N	N	N	Y	Y
ECDHE_RSA_WITH_AES_256_GCM_SHA384/ TLS_AES256_GCM_SHA384	Y	N	N	N	Y	Y
ECDHE_RSA_WITH_AES_256_CBC_SHA	Y**	Y	Y	Y	Y	N
ECDHE_RSA_WITH_AES_128_CBC_SHA	Y**	Y	Y	Y	Y	N
ECDHE_ECDSA_WITH_AES_256_GCM_SHA384/ TLS_AES_256_GCM_SHA384	Y*	N	N	N	Y	Y

NOTE:

* : This cipher is applicable with TLS1.3 with ephemeral key only.

** : Cipher suite only applicable with TLS1.2

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 highest security level that is common between the client and the server.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

SSL Protocol Versions support for communication

		Client side (from PC application)				
		sslv23	sslv3	tlsv1	tlsv11	tlsv12
On Terminal	sslv23	Y	Y	Y	Y	Y
	sslv3	Y	Y	N	N	N
	tlsv1	Y	N	Y	N	N
	tlsv11	Y	N	N	Y	N
	tlsv12	N	N	N	N	Y

The above table describes the protocol versions supported by the client side application, when communication is started by the terminal using a specific protocol. E.g. If the terminal starts communication using sslv23 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 sslv23 and sslv3 protocol versions for communication.

Access Path

Terminal Menu :

Security Menu > Communication > SSL/TLS Settings

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Communication > SSL Configuration

Screens & Steps

Figure 203: SSL Configuration

1. Select **SSL/TLS Mode** as ON or OFF. Only if the SSL/TLS Mode is ON, the SSL/TLS protocol is used

Figure 204: Entering Secure Communication Port

2. **Enter Secure Communication Port**: port that will be used for TLS or SSL protocol
3. **Use** “ ” button to save

Default Communication Port

The administrator can define a default communication port that will be used for Ethernet connection, by using this functionality.

Access Path

Terminal Menu :

Security Menu > Communication > TCP Channel

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Communication > Communication Channels Configuration

Screens & Steps

Figure 205: Selecting Communication Port

1. Select **Communication Port** option

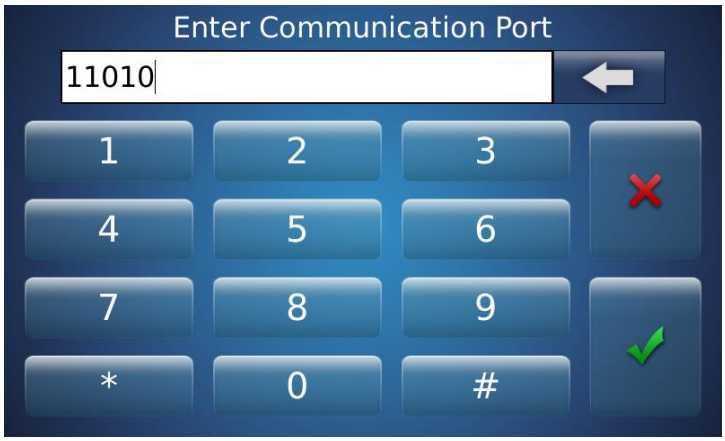


Figure 206: Entering Communication Port

2. Enter **Communication Port**: port that will be used for TCP (plain text)
3. Use “ ” button to save

Enabling TCP Channel

Transmission Control Protocol (TCP) is a protocol that is used for transmission of the input/output messages between the Access and Time Biometric Terminal and distant systems, such as external controllers or Webserver application, connected through Ethernet/Wi-Fi™.

By default, the TCP Channel is disable In Enforced Security configuration and enable in On-Demand security mode. In Enforced Security configuration it is not possible to enable it. If the administrator has disabled this parameter, the terminal will not be able to communicate (i.e. input or output of messages) with distant systems using Ethernet/Wi-Fi™.

Access Path

Terminal Menu :

Security Menu > Communication > TCP Channel

Webserver (not available In Enforced Security configuration and in all configurations for “MorphoWave® Range Series” and “VisionPass SP”):

Terminal Settings > Communication > Communication Channels Configuration

Screens & Steps

Figure 207: Configuring TCP Channels

1. The administrator needs to select the **TCP Channel** as ON if it is required to use TCP protocol for communication
2. Use “ ” to Save

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Enabling Serial Channel

Serial Channel is used for transmission of the input/output messages between the Access and Time Biometric Terminal and distant systems, such as external controllers, connected through RS422 and RS485.

By default, Serial Channel is disabled. If the administrator enables this parameter, the terminal will able to communicate (i.e. input/output messages) with distant systems using Serial channel.

NOTE: Serial channel cannot be used for configuration of the terminal with the Webserver.

Access Path

Terminal Menu :

Security Menu > Communication > Serial Channel

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Communication > Serial Configuration

Screens & Steps

Figure 208: Enabling/Disabling RS422/RS485 Serial Chanel

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

Multi User Settings

When the administrator enables this feature, the terminal evaluates the access rights with the data of two different users, instead one user. It implies that, when access rights are based on the biometric data check, the terminal requires the fingerprint of two different users, to grant the access.

NOTE: Multi User Verification feature is not available for VisionPass Range terminals.

Set Multi User

Access Path

Terminal Menu :

Security Menu > Multi User Settings > Multi User

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > User Control

Screens & Steps

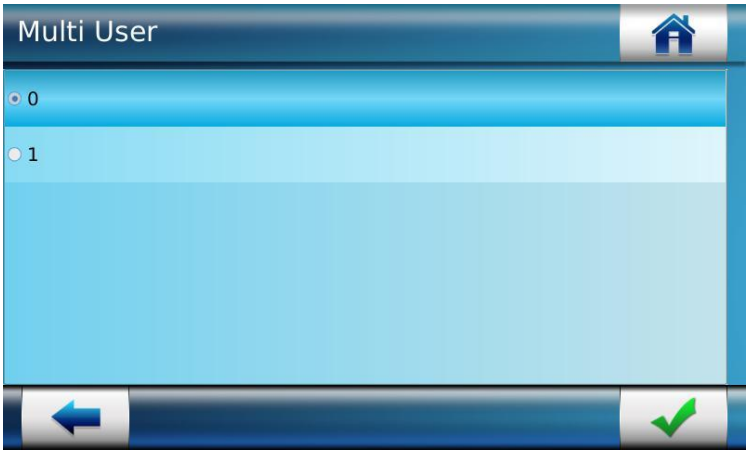


Figure 209: Addition User Verification

1. Select '0' to disable multi user mode (default): access rights check requires the data of only one user
2. Select '1' to enable multi user mode with 2 users: access rights check requires the data of two users
3. Use " " to **Save**

Set Next User Verification Timeout

The administrator can set this parameter to set the duration within which the additional user has to place finger on the biometric sensor. If the finger is not presented on the sensor within the time limit, access will be denied.

Access Path

Terminal Menu :

Security Menu > > Multi User Settings > Next User Verification Timeout

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > User Control Configurations > Multi-finger Timeout (sec)

Pre-requisites

- multi user feature must be activated: multi User should be selected as '1'

Screens & Steps

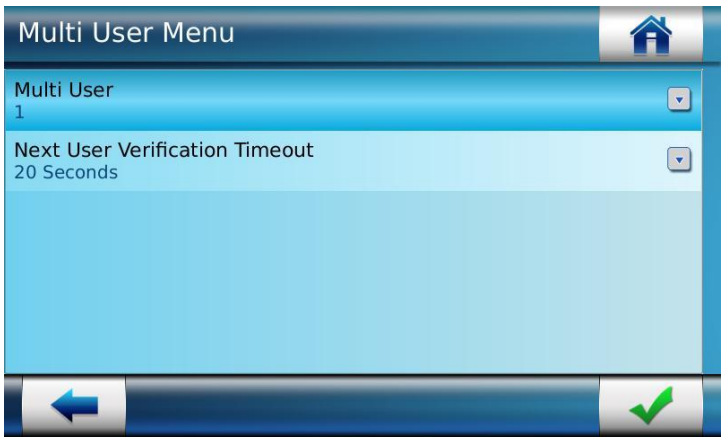


Figure 210: Next User Verification Timeout

1. Press on **Next User Verification Timeout**

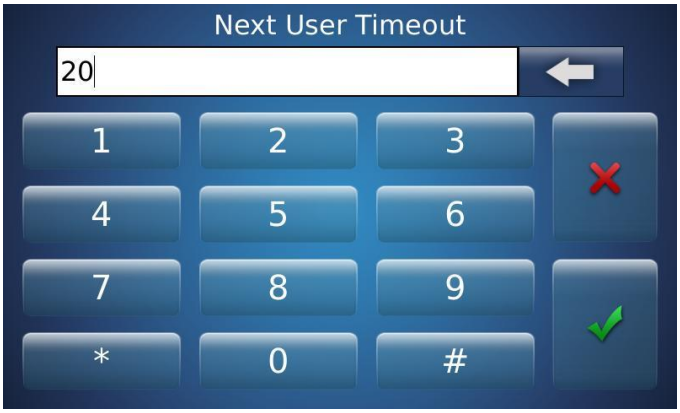


Figure 211: Next User Timeout

2. Enter the **Time limit**
3. Use “ ” button to save

Change the LCD Login Password

An administrator can login to the terminal using an LCD Password. In order to prevent any unauthorized access, it is recommended to change the password periodically. The administrator can change the LCD password, by using this functionality.

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

NOTE: In Enforced Security configuration, login to the terminal using an LCD Password only doesn't provide full access to Administration menu, only to information menu.

Access Path

Terminal Menu :

Security Menu > Change the LCD Login Password

Pre-requisites

Only an Administrator can change LCD Password

Screens & Steps

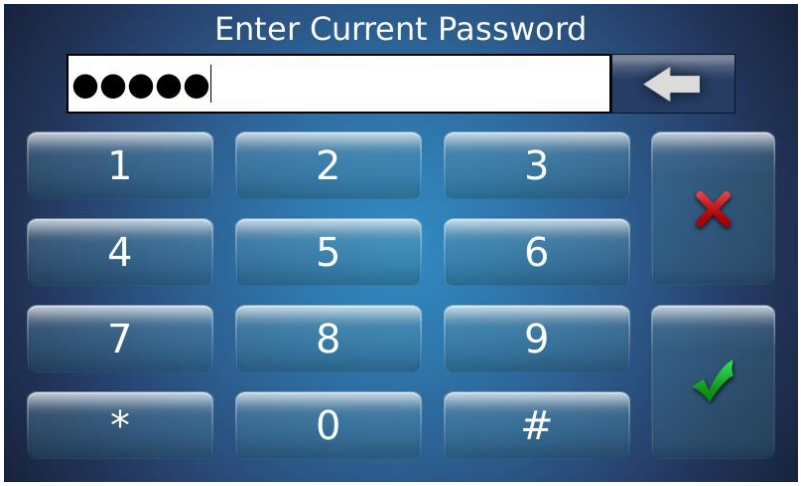


Figure 212: Resetting Device Password

1. Enter **Current Password** and use " " button to move on next screen

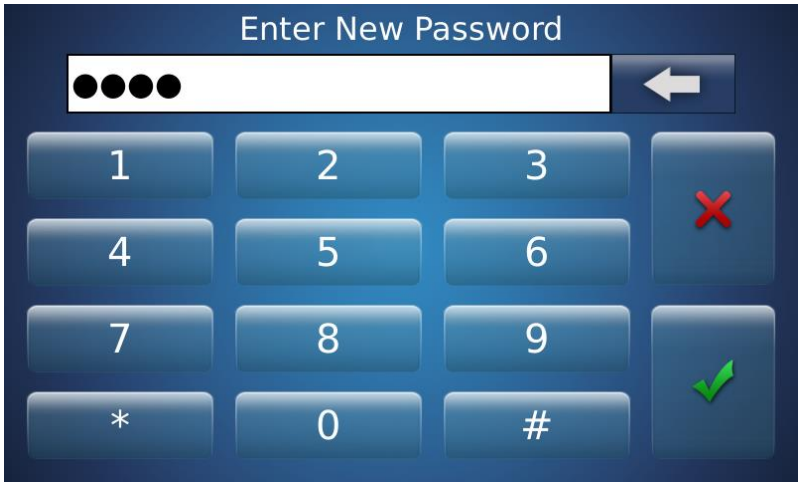


Figure 213: Entering New Password

2. Enter the **New Password** of choice
3. Use “ ” button to move on next screen

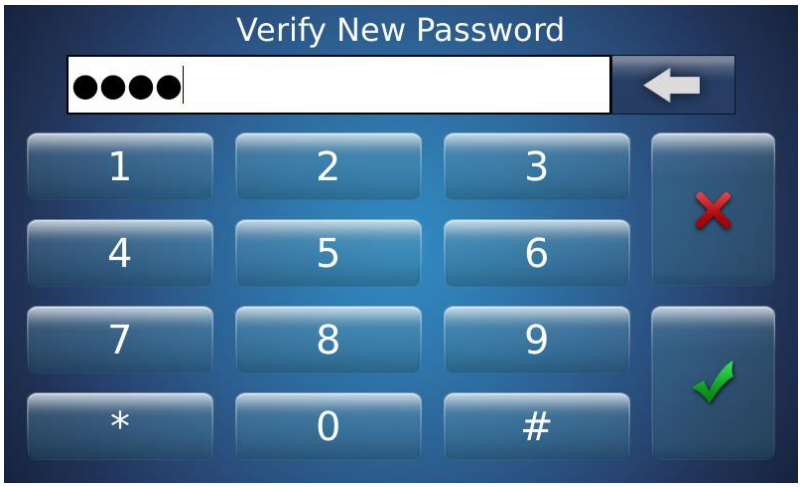


Figure 214: Verifying New Password

4. Re-enter the **New Password** for verification
5. Use “ ” button to **Save**

Results

Administrator can login to LCD using the new password.

Additional User Control Settings

The Access and Time Biometric Terminal administrator can set as to which access control parameters are applicable to allow access to the additional users, by using this functionality.

Access Path

Terminal Menu :

Security Menu > Additional User Control

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Control Configuration > User Control

Pre-requisites

Multiple Users feature must be enabled: Additional User Verification should be set to 1

Screens & Steps

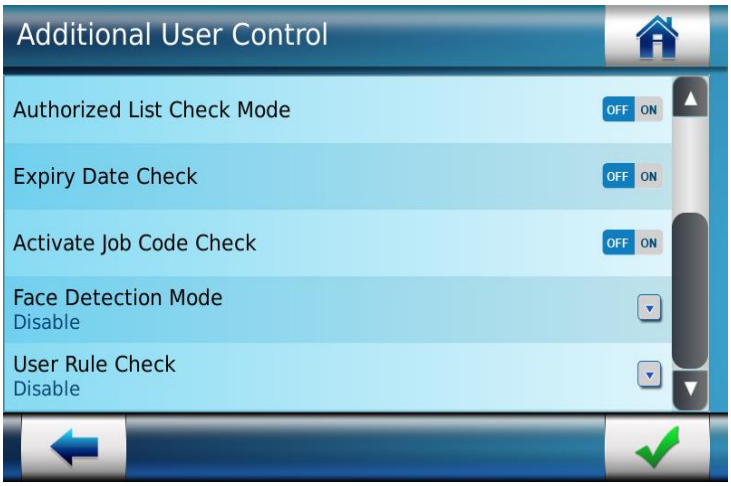


Figure 215: Additional User Control

The administrator can configure the parameters mentioned below for Additional User access control:

1. **Access Schedule:** This parameter indicates whether the terminal should check the access schedule of the enrolled user
2. **Holiday Schedule:** This parameter indicates whether the terminal should check the holiday schedule of the enrolled user
3. **Door Open Schedule:** This parameter indicates whether terminal should check the door open schedule of the enrolled user

4. **Authorized List Check Mode:** At the time of enrolment the administrator can set whether the user is an authorized user or not. Authorized user does not need to provide biometric verification
5. **Expiry Date Check:** this parameter indicates whether terminal should check the expiry date of the enrolled user
6. **Job Code Check Activation:** When the administrator enables this parameter, each time the user tries to access, user will have to place finger, or present face, as well provide Job Code for verification. The administrator can set a job code for a given user at the time of enrollment.

   Note: When the Time and Attendance mode is enabled, entering the job code during authentication is optional even though the Job Code Check is enabled. It is based on the value of the parameter *time_and_attendance.jobcode_by_key* and selected time and attendance key during authentication.
7. **Job Code Check Duration:** this parameter indicates the duration within which user will be required to enter the job code after a biometric check. If user fails to enter job code within this duration, the terminal will deny access.
8. **Face Detection Mode:** (SIGMA Range) The administrator can configure face authentication check rule as depicted in the snapshot below.

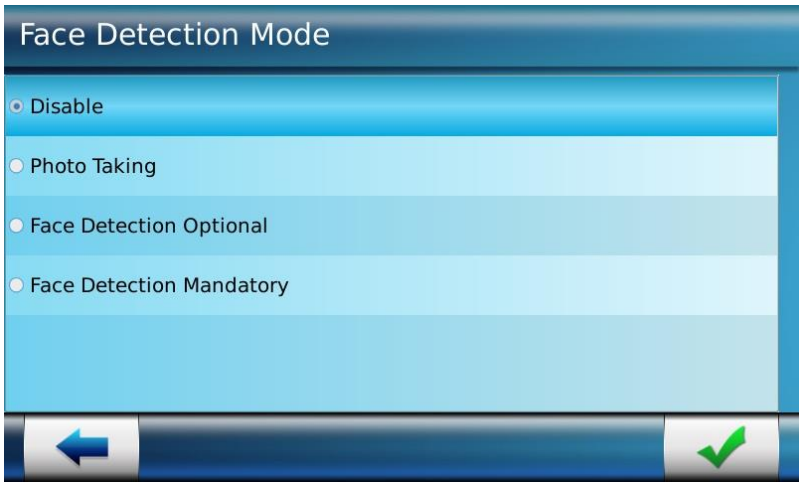


Figure 216: Enable or Disable Face detection mode

A parameter has been added in the “Complete Configuration” Screen of the Web Server named ucc.users_photo_policy, whose possible values can be 1, 2 or 3.

- If the administrator sets this as 1, the images for only those users who have been granted access, shall be saved.
- If the administrator sets the as 2, the images for only those users who have not been granted access, shall be saved.
- If the administrator sets the as 3, the images for users that are granted as well as not granted access, shall be saved.

Please refer to the table below in order to understand the face detection workflow:

User Rule_Face Detection	Terminal_Face Detection	ucc.users_ photo_policy	Successful Identification	Failed Identification	Failed Authentication
Disable	Disable	1	No	No	No
Disable	Disable	2	No	No	No
Disable	Disable	3	No	No	No
Disable	Photo Taking	1	Yes	No	No
Disable	Photo Taking	2	No	Yes	Yes
Disable	Photo Taking	3	Yes	Yes	Yes
Disable	Face Detection Optional	1	Yes	No	No
Disable	Face Detection Optional	2	No	Yes	Yes
Disable	Face Detection Optional	3	Yes	Yes	Yes
Disable	Face Detection Mandatory	1	Yes	No	No
Disable	Face Detection Mandatory	2	No	Yes	Yes
Disable	Face Detection Mandatory	3	Yes	Yes	Yes
Photo Taking	Disable	1	Yes	No	No
Photo Taking	Disable	2	No	No	Yes
Photo Taking	Disable	3	Yes	No	Yes
Photo Taking	Photo Taking	1	Yes	No	No
Photo Taking	Photo Taking	2	No	Yes	Yes
Photo Taking	Photo Taking	3	Yes	Yes	Yes
Photo Taking	Face Detection Optional	1	Yes	No	No
Photo Taking	Face Detection Optional	2	No	Yes	Yes
Photo Taking	Face Detection Optional	3	Yes	Yes	Yes

User Rule_Face Detection	Terminal_Face Detection	ucc.users_ photo_policy	Successful Identification	Failed Identification	Failed Authentication
Photo Taking	Face Detection Mandatory	1	Yes	No	No
Photo Taking	Face Detection Mandatory	2	No	Yes	Yes
Photo Taking	Face Detection Mandatory	3	Yes	Yes	Yes
Face Detection Optional	Disable	1	Yes	No	No
Face Detection Optional	Disable	2	No	No	Yes
Face Detection Optional	Disable	3	Yes	No	Yes
Face Detection Optional	Photo Taking	1	Yes	No	No
Face Detection Optional	Photo Taking	2	No	Yes	Yes
Face Detection Optional	Photo Taking	3	Yes	Yes	Yes
Face Detection Optional	Face Detection Optional	1	Yes	No	No
Face Detection Optional	Face Detection Optional	2	No	Yes	Yes
Face Detection Optional	Face Detection Optional	3	Yes	Yes	Yes
Face Detection Optional	Face Detection Mandatory	1	Yes	No	No
Face Detection Optional	Face Detection Mandatory	2	No	Yes	Yes
Face Detection Optional	Face Detection Mandatory	3	Yes	Yes	Yes
Face Detection Mandatory	Disable	1	Yes	No	No
Face Detection Mandatory	Disable	2	No	No	Yes
Face Detection Mandatory	Disable	3	Yes	No	Yes
Face Detection Mandatory	Photo Taking	1	Yes	No	No
Face Detection Mandatory	Photo Taking	2	No	Yes	Yes
Face Detection Mandatory	Photo Taking	3	Yes	Yes	Yes

User Rule_Face Detection	Terminal_Face Detection	ucc.users_ photo_policy	Successful Identification	Failed Identification	Failed Authentication
Face Detection Mandatory	Face Detection Optional	1	Yes	No	No
Face Detection Mandatory	Face Detection Optional	2	No	Yes	Yes
Face Detection Mandatory	Face Detection Optional	3	Yes	Yes	Yes
Face Detection Mandatory	Face Detection Mandatory	1	Yes	No	No
Face Detection Mandatory	Face Detection Mandatory	2	No	Yes	Yes
Face Detection Mandatory	Face Detection Mandatory	3	Yes	Yes	Yes

Table 1 : Face Authentication Workflow

Refer below table for face authentication workflow for normal user and VIP user:

Face Detection Mode	Behavior	Behavior for VIP user
Disabled	Do not take pictures	Disabled
Photo Taking	Take one picture and save it according to logging policies(ucc.users_photo_policy)	As per 'Photo Taking'
Face Detection Optional	Take multiple pictures and perform face detection. If a face is detected in one or multiple photo, save the photo with the best face detection quality measure. • Face detection process ends when user control workflow gets completed • No use of face detection timeout	As per 'Face Detection Optional'
Face Detection Mandatory	Take multiple pictures and perform face detection. If no photo contains a face, the user is rejected. • Perform face detection till timeout if no face is detected (even if user control workflow gets completed)	As per 'Face Detection Optional'

Table 2 : Face Authentication Workflow for Normal and VIP User

References

Refer to "*Recommended Conditions for Face Detection*" for knowing the correct position of the user and required lighting conditions in order to achieve correct face detection.

VisionPass: On VisionPass Range terminals, the administrator can activate only photo taking. Face detection options are not available because it is always done. There is no user rule dedicated to photo taking on VisionPass Range terminals, only a global rule.

9. User Rule Check: This parameter defines the user rule check flow, whether to apply the user rules configured on terminal or on trigger event. The possible values are "Disabled", "Trigger Event" and "Terminal".

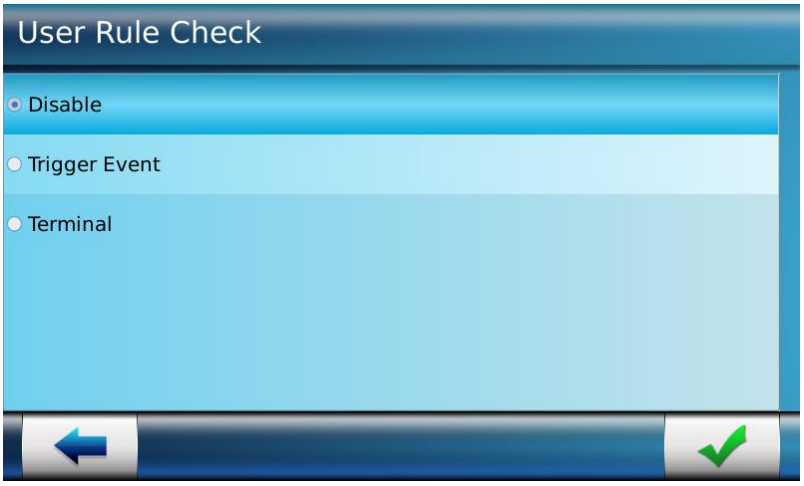


Figure 217: User Rule Check

If the per user rule (ucc.per_user_rule) is defined to Terminal then Terminal will verify user data (source of data defined from ucc.user_record_reference) based on User Rule configured in Terminal (reference: *User Enrollment in Database*). If User Rule is set to "Trigger Event", the configuration/details from which user control is initiated are applied. The default value of "User Rule Check" is "Disable".

USB Menu

Access and Time Biometric Terminal is equipped with a USB Port that is to connect a USB Mass Storage, temporarily.

Following are the uses of USB connection:

The administrator can upgrade firmware

The administrator can import data to the terminal such as the User Database. It is also used to import the Audio files, Video files, and Images that are used in Multimedia Configuration.

The administrator can export data from the terminal. Transaction logs, Error Logs and User records can be exported from the terminal.

NOTE: In Enforced Security configuration, it is not possible to enable the USB port by consequence functionalities from USB menu are not available

Figure 218: USB Menu in SIGMA Wide Series Terminal

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Enable or Disable USB port

Access and Time Biometric Terminal Administrator Menu can enable or disable USB port. All the USB functionalities (like USB script execution, USB Import/Export etc) are available for the user only if the USB port is enabled.

The administrator can also enable or diable USB port from **Webserver** or **MorphoBioToolBox** by using parameter “comm_channels_state.USB_script”.

Access Path

Terminal Menu :

USB Menu > USB port enable

MorphoBioToolBox :

MorphoBioToolBox > Manage Configuration Keys

Webserver (not available In Enforced Security configuration and in all configurations for “MorphoWave® SP”, “MorphoWave® XP2” and “VisionPass SP”):

Webserver > Complete Configuration

Screens & Steps

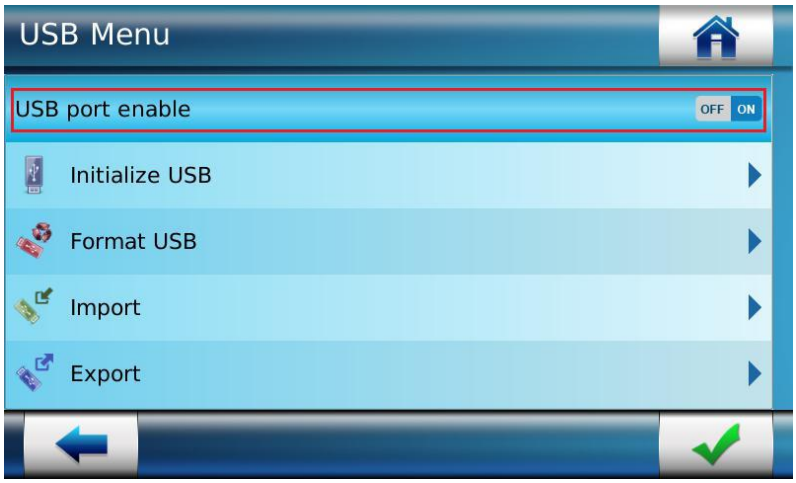


Figure 219: Enable/Disable USB port

1. Select ‘ON’ to enable USB port or ‘OFF’ to disable USB port
2. Use “ ” to **Save.**

Initialize USB Mass Storage device

The Access and Time Biometric Terminal administrator must ensure that all the folders in the USB Mass Storage device have the same structure as on the terminal. This can be done using the **Initialize USB Mass Storage device** functionality. By using this, the terminal will copy the same folder structure in the USB Mass Storage device.

Access Path

Terminal Menu :

USB Menu > Initialize USB

Pre-requisite

USB Mass Storage device must be empty.

Prior to store any data on USB Mass Storage device, it is mandatory that the device is initialized.

Connect the USB Mass Storage device for initialization, only once Access and Time Biometric Terminal is up and running (even when terminal is rebooted, it must be up and running)

Screens & Steps

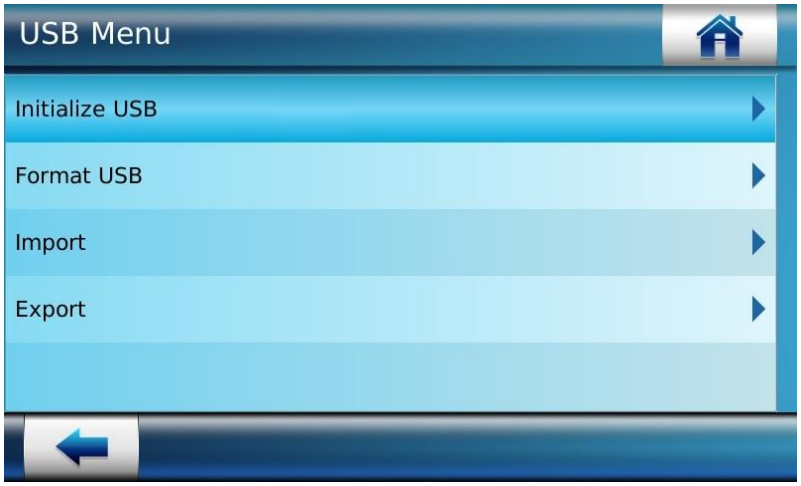


Figure 220: Initialize USB Mass Storage device

1. Connect USB Mass Storage device to terminal
2. Press on **Initialize USB**

Figure 221: A confirmation message is displayed

3. Confirm Initialize USB Mass Storage device by using “ ” button

Results

A success message is displayed showing USB Mass Storage device is initialized. Now the administrator can use the USB Mass Storage device to upload or download data to or from the terminal.

Format USB Mass Storage device

The administrator can use the Format USB Mass Storage device functionality to delete the entire data stored in a USB Mass Storage device. Once the device is formatted, it can be initialized to store the same folder structure as in the terminal.

Access Path

Terminal Menu :

USB Menu > Format USB

Screens & Steps

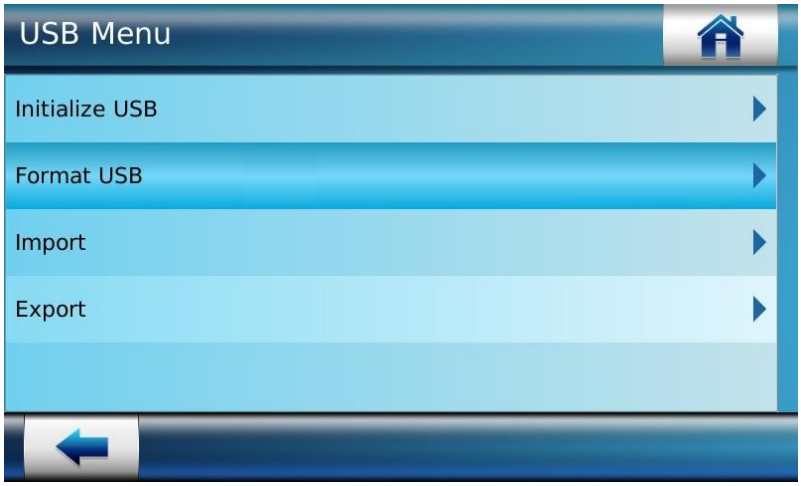


Figure 222: Formatting USB Mass Storage device

1. Connect USB Mass Storage device to terminal
2. Select **Format USB** option

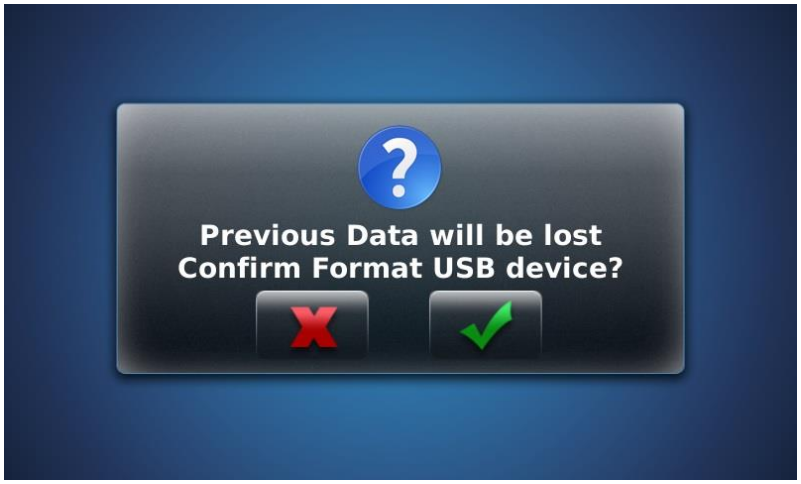


Figure 223: Confirmation message pop-up

3. A confirmation message pop-up is displayed, notifying that the previous data in the USB Mass Storage device will be lost.
4. Confirm action by using “ ” button

Figure 224: Success Message of USB Mass Storage device Formatted

Results

A success message is displayed showing that the USB Mass Storage device is formatted. Now the USB Mass Storage device can be initialized and used for data exchange.

Import Data into Terminal

Access and Time Biometric Terminal is capable of importing several files in its local database. The administrator can import the following files to the terminal by using Import Data functionality:

User Database: It is a general practice to maintain a backup of the user database, to prevent situations such as database loss. Using the Import data functionality, the backup file of the user database can be imported in the terminal.

Contactless key: The administrator can import the contactless key. The terminal used the key to identify the card. Terminal can perform the card operation which is not encoded it self by importing the security key of the card.

Language File: Terminal can support multiple languages. The administrator can customize and upload the language file in the terminal, by using Import Language file. The uploaded language will be displayed to the user to select from. See "*Language Configuration*" for more information.

NOTE: The administrator can upload new font style using file_load() distant command. User information message like Access granted/Denied/Dynamic messages will be displayed in new font style once font file is uploaded into the terminal.

Customized language will be displayed in the new font style, if new font is uploaded in to the terminal in addition to the customized language file.

Multimedia Files: The administrator can import multimedia content such as Audio, Video and Images that are played on terminal upon the occurrence of specific events. Please refer to the "*Multimedia menu*" to learn as to how to import multimedia content.

NOTE: Import user's biometric data in an empty terminal doesn't automatically turn on the biometric sensor. You have to reboot it.

Recommendation

Importing data into the terminal may take longer duration depending on the data size, which consequently affects the terminal response time and other operations. Hence the administrator is recommended to perform import data operation when the terminal is in idle state.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

How to Import User Database

Access Path

Terminal Menu :

USB Menu > Import

Pre-requisite

USB Mass Storage device should be initialized and must have the user database file in the correct folder

USB Mass Storage device should be plugged into the terminal

Screens & Steps

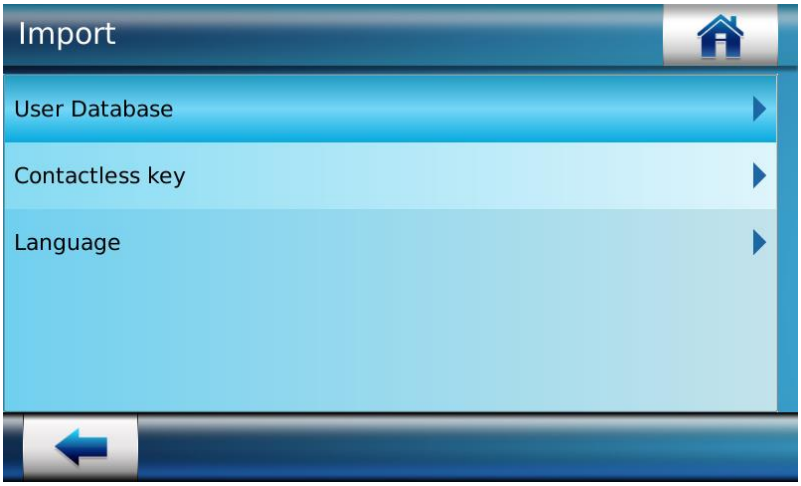


Figure 225: Importing User Database

1. Select **User Database**

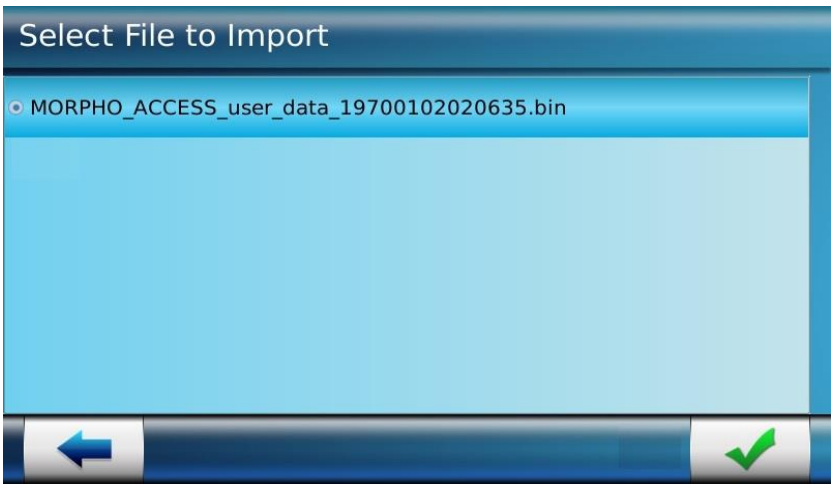


Figure 226: Selecting file to be imported in the terminal

2. The list of files present in the user database folder in USB Mass Storage device is displayed
3. Select a file to be imported

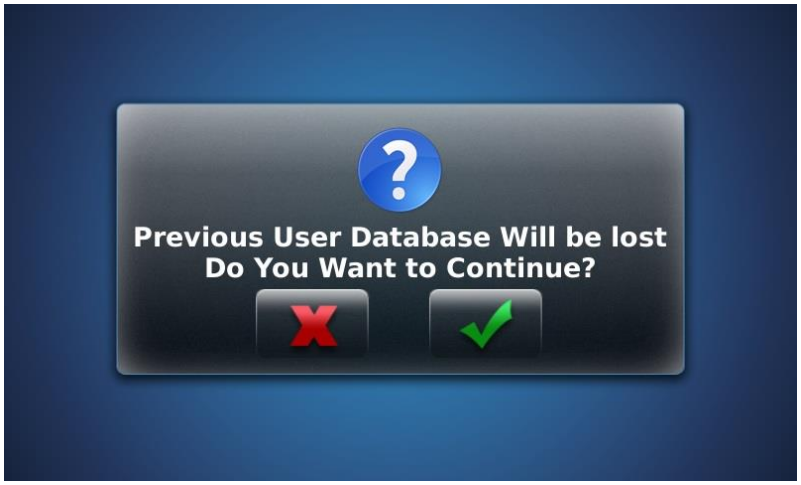


Figure 227: Confirmation message to import User Database

4. A confirmation message is displayed asking to confirm action. It also notifies that on importing file, the previous user database will be lost
5. Confirm by using “ ” button

Figure 228: Enter password

6. Enter a **Passphrase**. The passphrase set at the time of exporting user database is required to be entered for importing the same user database file in terminal.

7. Use “ ” button to complete an action

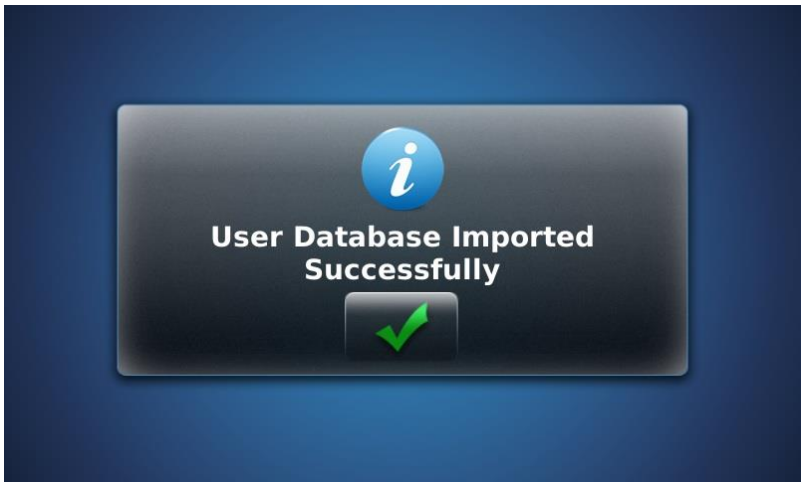


Figure 229: Success message of user data imported is displayed

Results

Once the user’s database is imported, the user information can be edited and identification of users can be performed on the terminal.

How to Import Contactless key

Access Path

Terminal Menu :

USB Menu > Import

Pre-requisite

USB Mass Storage device should be initialized and must have the contactless key file in the correct folder

USB Mass Storage device should be plugged into the terminal

Screens & Steps

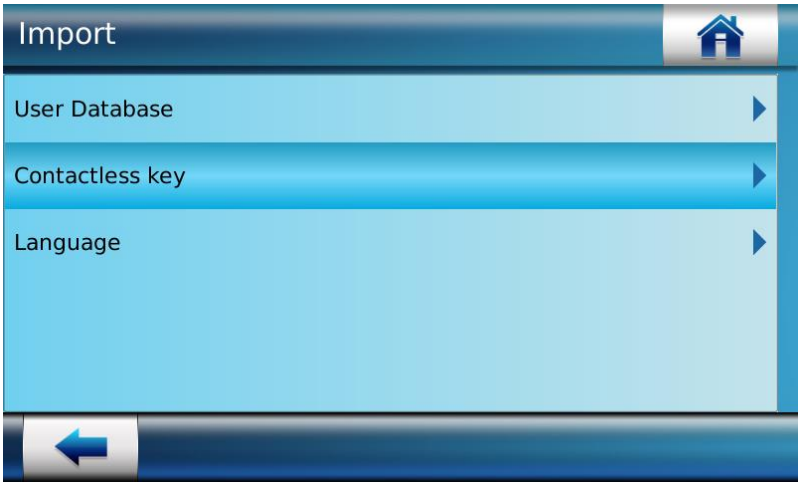


Figure 230: Importing contactless key

1. Select **Contactless key**

Figure 231: Selecting file to be imported in the terminal

2. The list of files present in the user database folder in USB Mass Storage device is displayed
3. Select a file to be imported

Figure 232: Enter password

4. Enter a **Passphrase**. The passphrase set at the time of exporting user database is required to be entered for importing the same user database file in terminal.
5. Use “ ” button to complete an action

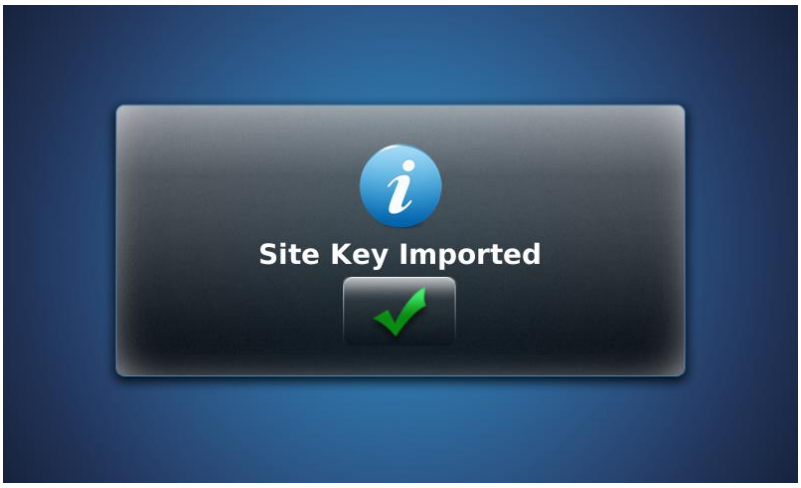


Figure 233: Success message of contactless key imported is displayed

Results

Once the user’s site key is imported, the card can be edit, erase and renew.

How to Import Language

Access Path

Terminal Menu :

USB Menu > Import

Pre-requisite

USB Mass Storage device should be initialized and must have the language file in the correct folder

USB Mass Storage device should be plugged into the terminal

Screens & Steps

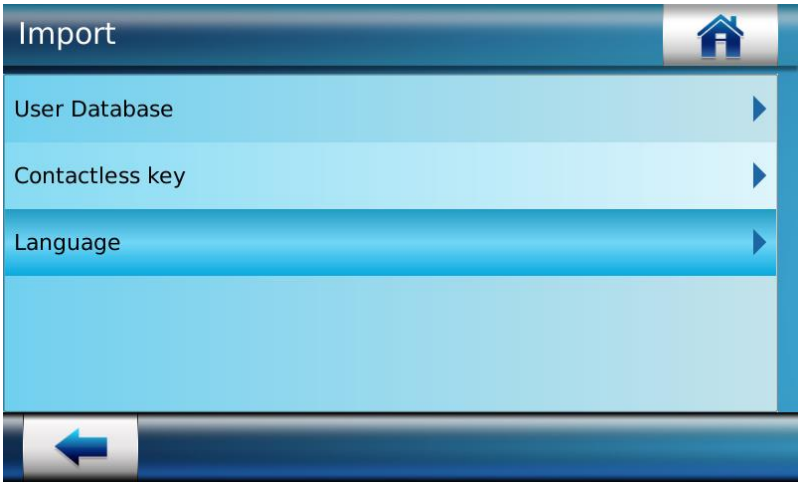


Figure 234: Importing Language file

1. Select **Language** to be imported

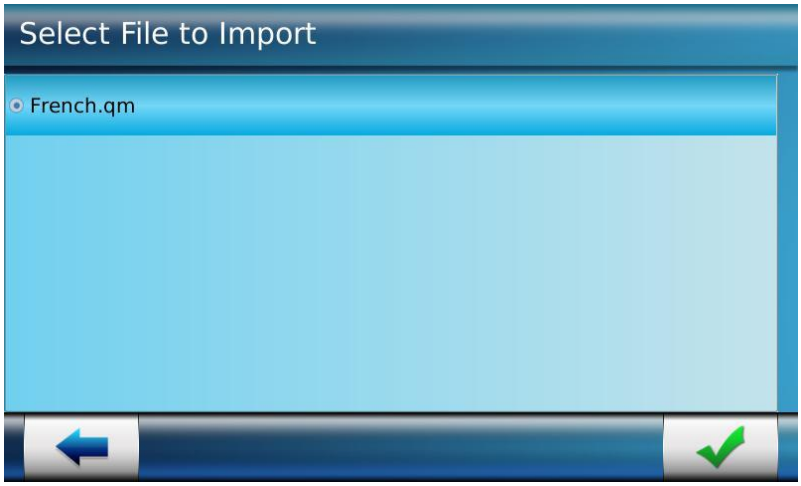


Figure 235: Selecting Language file to import

2. The language files present in USB Mass Storage device is displayed. The language file will be in '.qm' format
3. Select a language file that is required to be uploaded
4. Press on check box " ".

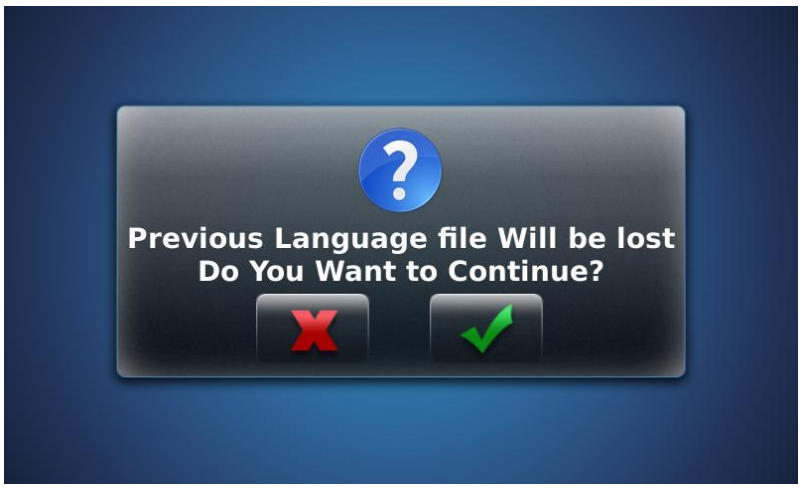


Figure 236: Confirm import action

5. A confirmation message is displayed as a pop-up, select the check box to confirm import of language file. This action will replace the previous language file with the new file

Figure 237: A success message is displayed showing language file is imported

Export Data in USB Mass Storage Device

The administrator can export the information from terminal database into the USB Mass Storage Device, by using this functionality. The terminal allows the export of the following categories of data.

Transaction Log: there can be two modes of transaction logging,

Error Log: Contains the record of failed attempts to access as well as other errors that have occurred

User Database: This contains user database.

Contactless key: This contains the contactless card security keys

The logs and user database can be exported in Binary (.bin) format, which is a non-readable file. Transaction log can also be exported in .CSV format.

The data exported in USB Mass Storage device can be used as a backup and imported in the terminal, on instances when terminal database is formatted.

Recommendation

Exporting data from the terminal may take longer duration depending on the data size. This consequently affects the terminal response time and other operations. Hence the administrator is recommended to perform export data operation when terminal is in idle state.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

How to Export & View Transaction Logs

Access Path

Terminal Menu :

USB Menu > Export > Transaction Log

Pre-requisites

The administrator must enable the Transaction Logging Mode for the transaction logs to be recorded in the terminal

Screens & Steps

Figure 238: Exporting transaction logs into USB Mass Storage Device

1. Select the **Transaction log** option.

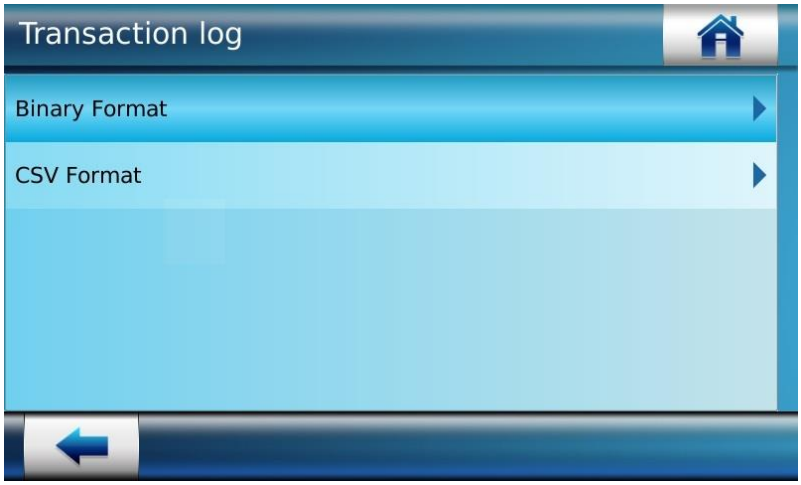


Figure 239: Selecting a file format for exporting transaction logs

2. Select the format in which data should be exported in, such as **Binary Format** or **CSV Format**

NOTE: Only Transaction Log has option to be exported in .bin or .csv format. Error logs and User database is exported in encrypted format by default.

Figure 240: A confirmation message pop-up

3. A confirmation message pop-up is displayed
4. Confirm an action to export log by using “ ” button

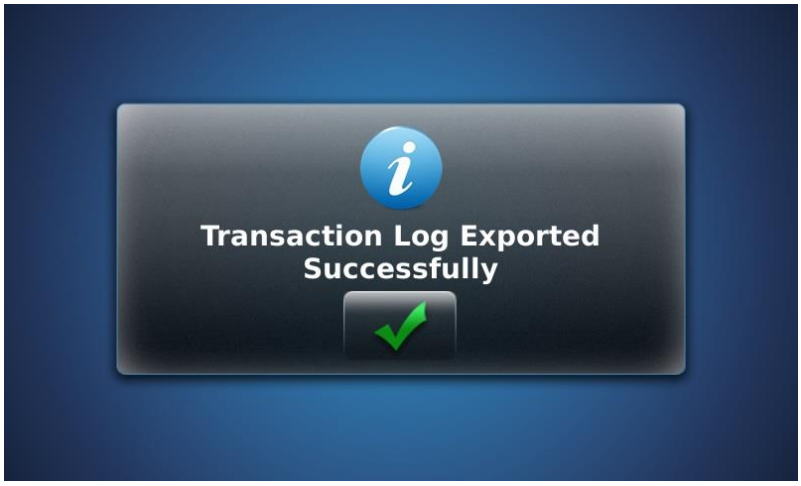


Figure 241: A success message is displayed showing transaction log is exported

A1 YYYY-MM-DD HH:MM:SS

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1	YYYY-MM-	Result	Action	Action Da	Action Da	Action Da	Action Da	Action Da	Channel	Administr	Name	First Nam	User ID/C	Jobcode/(	Duration	Matched F	Matching	TNA Key	Usr Ctrl Re	Usr Ctrl Ch	Usr Ctrl Ch	Error Co
2	########	Pass	Terminal	0	0	0	0	0	IO channe	No administration rights				0	0	0	0	0	3	0	0	
3	########	Pass	Terminal	0	0	0	0	0	IO channe	No administration rights				0	0	0	0	0	3	0	0	
4	########	Pass	Settings cl	1	0	0	0	0	IO channe	No admin	first_boot.storage_type			0	0	0	0	0	3	0	0	
5	########	Pass	Settings cl	1	0	0	0	0	IO channe	No admin	date_time_settings.24_hour_f			0	0	0	0	0	3	0	0	
6	########	Pass	Settings cl	0	0	0	0	0	IO channe	No admin	date_time_settings.date_form			0	0	0	0	0	3	0	0	
7	########	Pass	Settings cl	0	0	0	0	0	IO channe	No admin	date_time_settings.time_form			0	0	0	0	0	3	0	0	
8	########	Pass	Managem	0	0	0	0	0	LCD	No administration rights				0	0	0	0	0	3	0	0	
9	########	Pass	Managem	0	0	0	0	0	LCD	No administration rights				0	0	0	0	0	3	0	0	
10	########	Pass	Managem	0	0	0	0	0	LCD	No administration rights				0	0	0	0	0	3	0	0	

Figure 242: Transaction Log in .CSV Format Sample

Results

The file for the exported transaction logs is created and stored in the USB Mass Storage Device, in .csv format.

How to Export Error Log

Access Path

Terminal Menu :

USB Menu > Export > Error Log

Pre-requisites

The administrator must explicitly enable the Error Logging. Refer to "*Error Log Configuration*" for more information about error log configuration

Screens & Steps

Figure 243: Exporting data into USB Mass Storage Device

1. Select the **Error log** option.

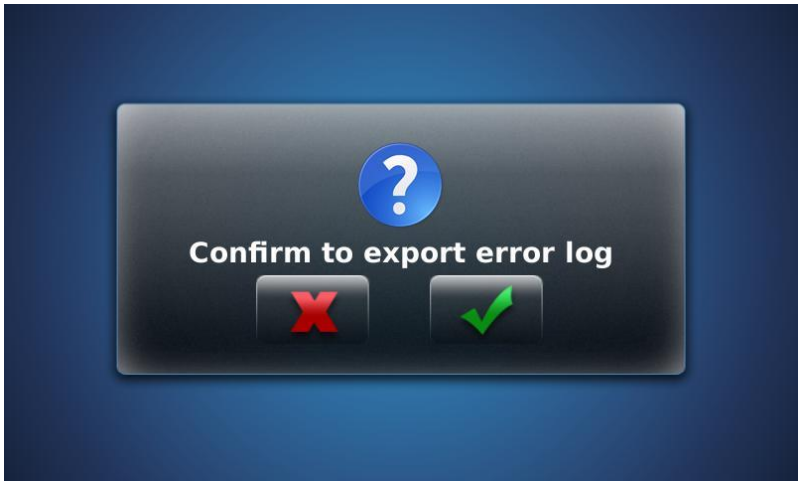


Figure 244: A confirmation message pop-up

2. A confirmation message pop-up is displayed
3. Confirm an action to export log by using “ ” button

Figure 245: A success message is displayed showing error log is exported

Results

The file for the exported error logs is created and stored in the USB Mass Storage Device, in .tar format. The file is encrypted and non-readable, for security purpose.

How to Export User Database

Access Path

Terminal Menu :

USB Menu > Export > User Database

Screens & Steps

Figure 246: Exporting data into USB Mass Storage Device

1. Select the **User Database** option.

Figure 247: A confirmation message pop-up

2. A confirmation message pop-up is displayed
3. Confirm an action to export database by pressing“ ” button

Figure 248: Enter Passphrase

4. Enter **Passphrase**. The same passphrase will be required on importing the user database in terminal
5. Press on “ ” button

Figure 249: A success message is displayed showing error log is exported

Results

The file for the user database is created in .BIN format and stored in the USB Mass Storage Device. The file is encrypted and non-readable, for security purpose.

How to Export Contactless key

Access Path

Terminal Menu :

USB Menu > Export > Contactless key

Screens & Steps

Figure 250: Exporting data into USB Mass Storage Device

1. Select the **Contactless key** option.
2. Select the key you want to export and press “ ” button.

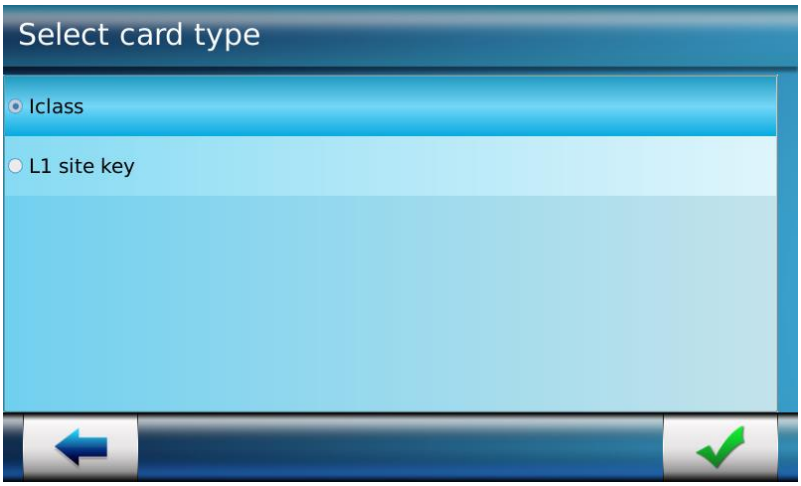


Figure 251: Enter Passphrase

3. Enter **Passphrase**. The same passphrase will be required on importing the user contactless key in terminal
4. Press on “ ” button

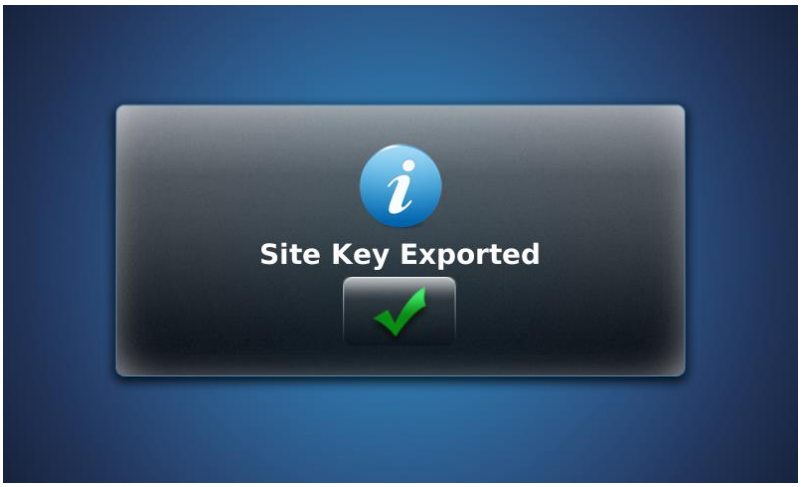


Figure 252: A success message is displayed showing error log is exported

Results

The file for the contactless key is created in .BIN format and stored in the USB Mass Storage Device. The file is encrypted and non-readable, for security purpose.

Information Menu

The administrator can view important data such as the ones listed below, from a single panel. This can be achieved by means of the Information Menu.

Information related to Terminal's commercial name and license

Sensor Information

Firmware version

Network settings done in terminal, that includes Ethernet, Wi-Fi™, Serial Channel, 3G, GSM, and GPRS connections

Memory Status of the terminal

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

Transaction Log Status shows count of current logs and maximum log records supported on the terminal

Figure 253: Information Menu

View Device Details

The administrator can view the information related to the Access and Time Biometric Terminal, by using this functionality.

Access Path

Terminal Menu :

Information Menu > Device

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Webserver > Terminal Info

Screens & Steps

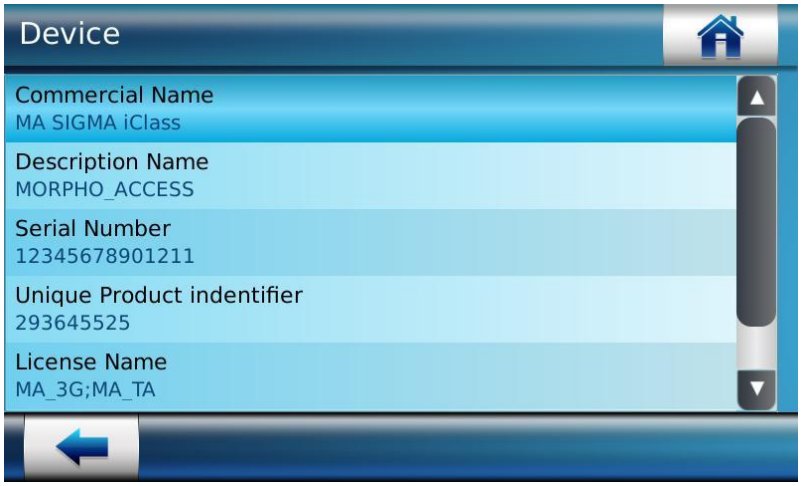


Figure 254: View Device Information

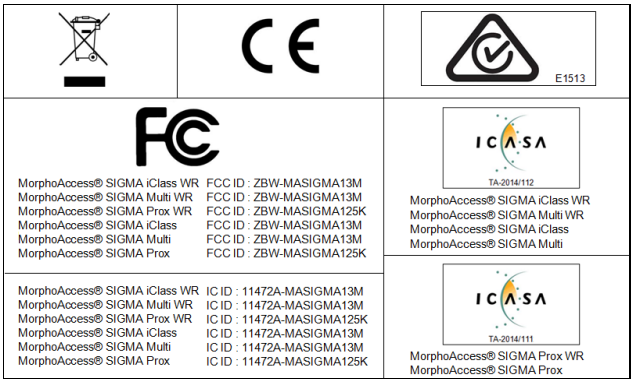


Figure 255: View Device Regulatory Information

1. Following information of the terminal are displayed:
    a. **Device Commercial Name**
    b. **Device Description Name**
    c. **Device Serial Number**
    d. **Device Unique Product identifier**
    e. **License Name**
    f. **License Identifier**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

View Firmware Information

The administrator can view information regarding the current version of the Terminal firmware by using this functionality. The firmware version is upgradeable.

Access Path

Terminal Menu :

Information Menu > Firmware Version

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Webserver > Terminal Info

Screens & Steps

Figure 256: SIGMA Range Version information

1. The current terminal firmware version information is displayed
2. The current terminal protocol information is displayed

Figure 257: Morpho*Wave*® Compact terminal Firmware Version information

1. The current terminal firmware version information is displayed

View Sensor Revision Information

The administrator can view the information related to the biometric sensor, by using this functionality.

NOTE: The Sensor Revision Information is not available on VisionPass Range terminals.

Access Path

Terminal Menu :

Information Menu > Sensor Revision

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Info > Terminal

Screens & Steps

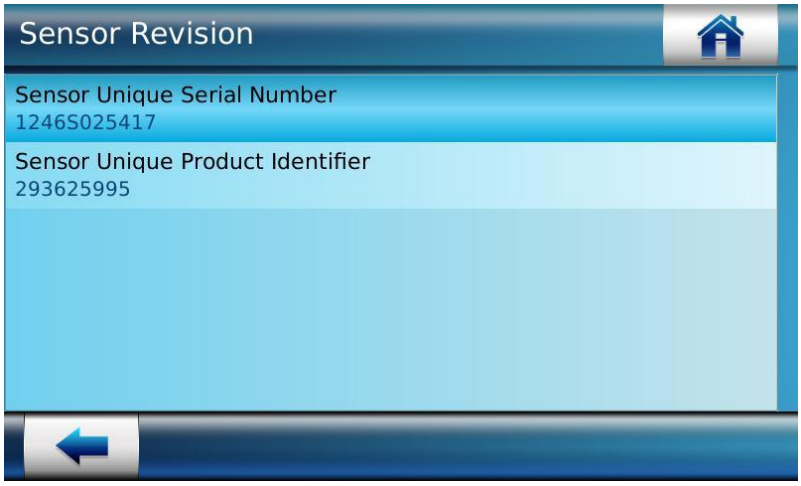


Figure 258: Biometric Sensor data

1. **Sensor Unique Serial Number**
2. **Sensor Unique Product Identifier** is displayed

View Communication Parameters

The administrator can view the information of various Networks interface through which the terminal is connected with distant systems, Under **Communication** tab.

Access Path

Terminal Menu :

Information Menu > Communication

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Settings > Communication > IPv4/IPv6 Network

Screens & Steps

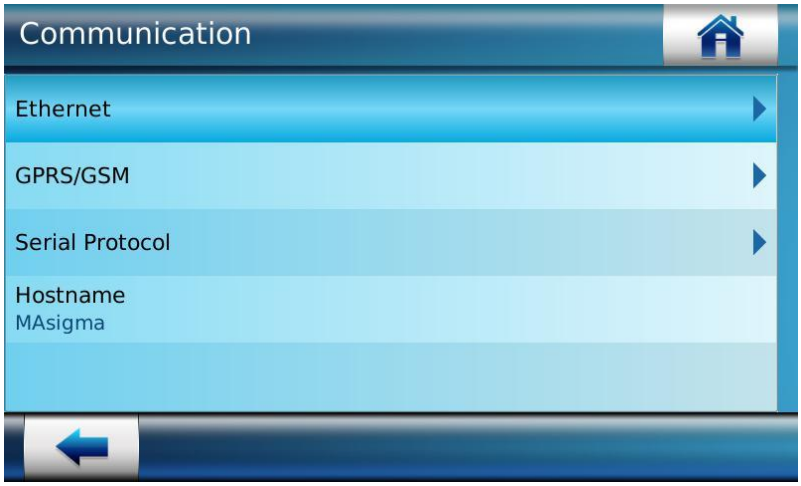


Figure 259: Selecting communication network

1. Select the type of communication network from the following options:
    a. Ethernet
    b. GPRS/GSM
    c. Serial Protocol
    d. Hostname

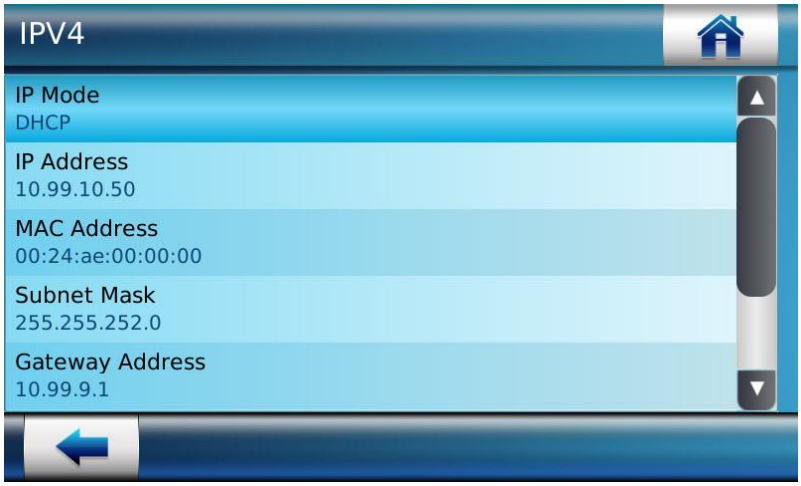


Figure 260: Viewing information of Ethernet network

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**

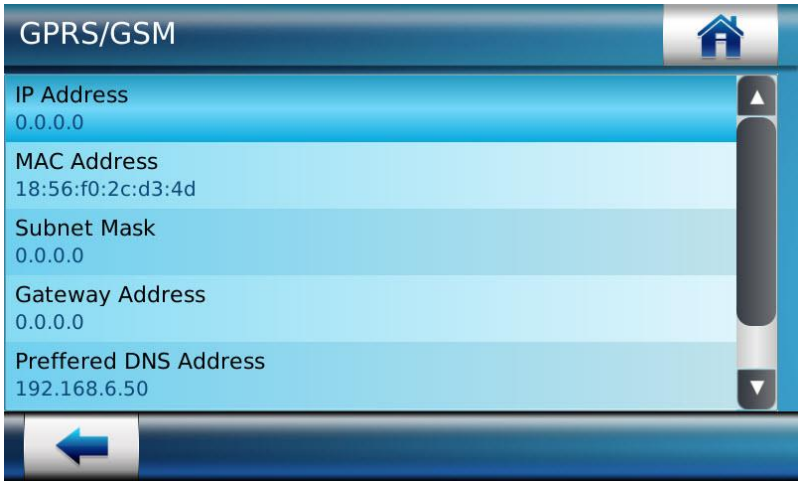


Figure 261: Viewing information of GPRS/GSM network

4. Following information of GPRS/GSM connection is displayed:

a. **IP Address** of the terminal

b. **MAC Address** of the terminal

c. **Subnet Mask**

d. **Gateway Address**

e. **Preferred DNS Address**

f. **Alternate DNS Address**

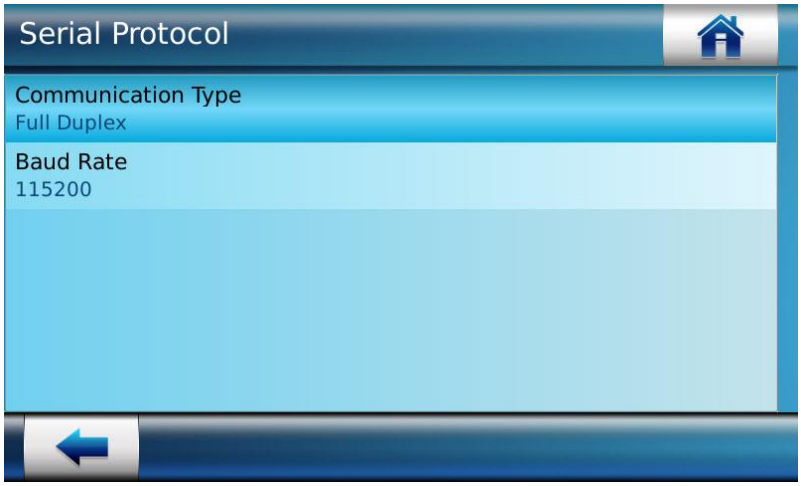


Figure 262: Viewing Serial Protocol Configuration

5. If terminal is communicating with distant server using serial port, then parameters listed below are displayed:

   a. **Communication Type** i.e. Half Duplex or Full Duplex

   b. **Baud Rate** i.e. data transmission rate through serial port

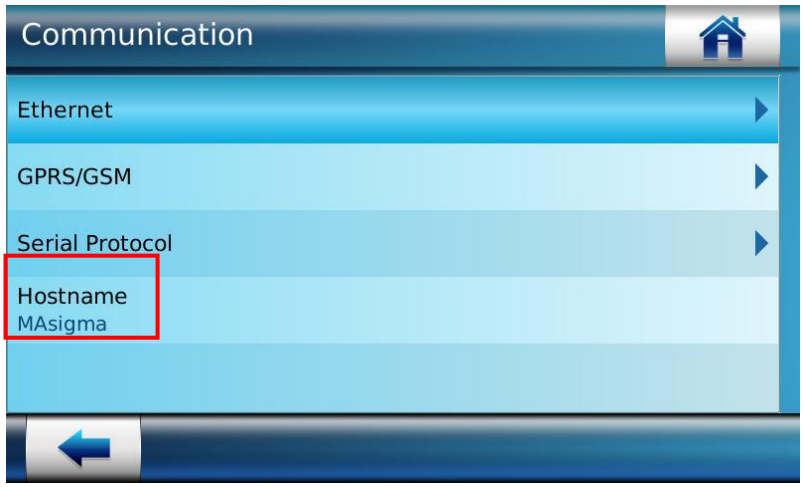


Figure 263: View Hostname of the terminal

6. Hostname of the terminal is displayed

View Memory Status

The administrator can view the remaining memory of the terminal, by using this functionality.

NOTE: The SD Card Status is not available on VisionPass and Morpho*Wave*® terminal ranges.

Access Path

Terminal Menu :

Information Menu > Memory Status

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Info > SD Card Information

Pre-requisites

The administrator must have the SD card plugged in the terminal

Screens & Steps

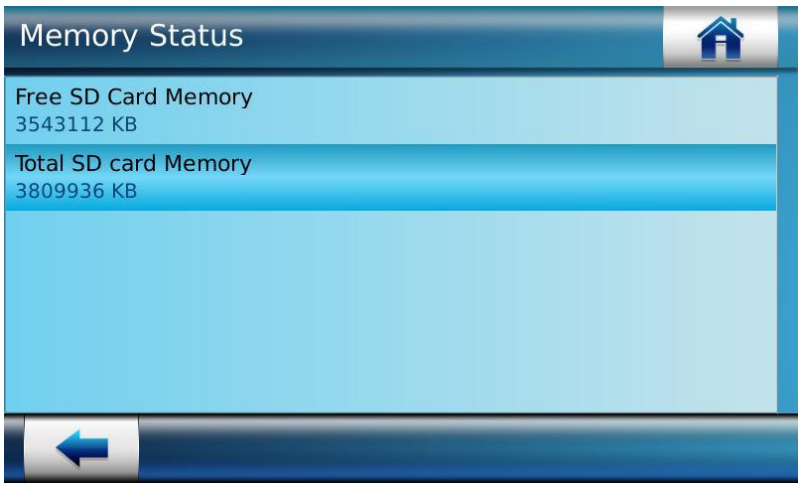


Figure 264: Memory Status of the device is displayed

1. Following information is displayed under Memory State:
   a. Free SD card Memory
   b. Total SD card Memory

View User Status

The administrator can view the summary of number of enrolled users, number of authorized listed users and number of VIP users by following the **View User Status** tab.

Access Path

Terminal Menu :

Information Menu > User status

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Info > User's Information

Screens & Steps

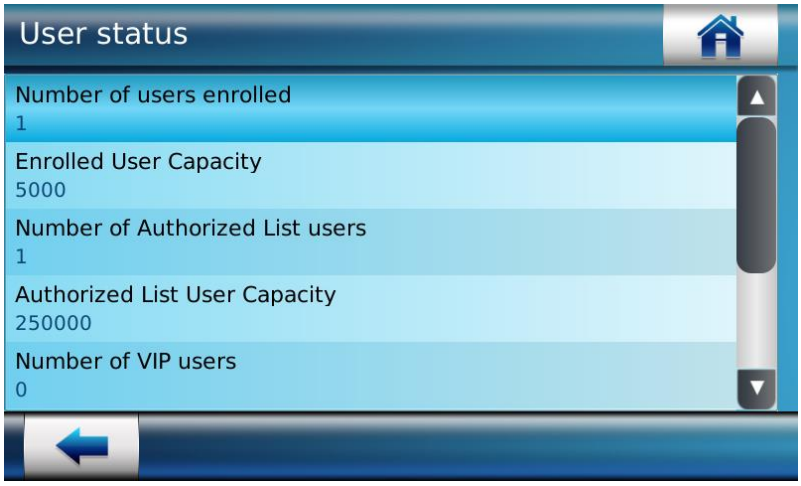


Figure 265: View User Status

Under User Status information section, following information is displayed:

1. **Number of Users Enrolled** in the terminal is displayed
2. **Enrolled user Capacity** indicates the maximum number of users that can be enrolled. Basic capacity of the terminal is to store 5,000 users' database. The administrator can step up this capacity to 100,000 user's records, by installing users' license. Refer to "Terminal License Management " for more information.
3. **Number of Authorized List Users,** the number of users enrolled as Authorized listed users
4. **Authorized List User Capacity** indicates the maximum number of users that can be added in the authorized list. This is 250,000 users by default.
5. **Number of VIP users**, the number of 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. By default the number of VIP users is 100.
7. **All Users** indicates the users number of all types in Database

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

View Transaction Log Status

The administrator can view the Transaction log status, by following the access path mentioned below. It displays the number of current logs recorded in the terminal database as well as the maximum capacity of logs that can be stored in the terminal.

Access Path

Terminal Menu :

Information Menu > Transaction Log Status

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Terminal Info > Transaction Log Information

Screens & Steps

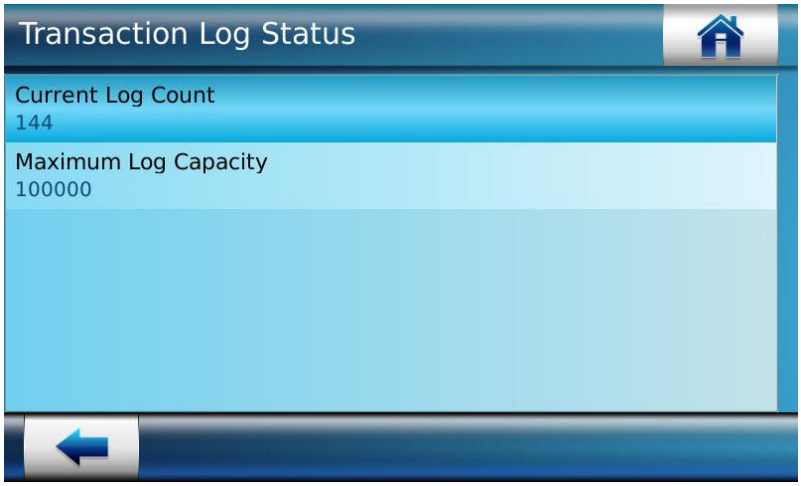


Figure 266: Transaction Log Status is displayed

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

Reboot Terminal

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

Change Smartcard Read Profile

Installation of Wi-Fi™ USB Adapter

Import of User database

Enable Support L1 Cards

Enable or disable the user binary ID

Modify level of diagnostic logs

Change the transaction log mode

After installation of a new license that upgrades the terminal features

Access Path

Terminal Menu :

Reboot

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Webserver Home Screen > Welcome Admin

Figure 267: Reboot Device

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

After reboot all the settings are unchanged. If the administrator needs to reset the terminal to default factory settings, please use the corresponding function “System Menu > Terminal Settings > Set Factory Default”.

NOTE: *By pressing on the home icon at the top right end of the terminal, user can return to the home screen from any of the management menu screens. When user presses the home icon, a warning message first appears seeking confirmation. The user can confirm to return to the home screen by pressing “ ” button. By pressing button” “, the user can stay in the current screen to validate changes.*

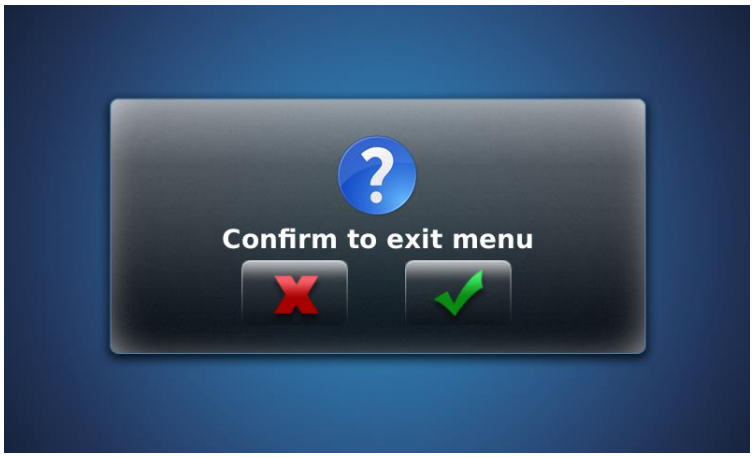


Figure 268: Confirmation Message To Return to Home Screen

Section 6 : **Terminal Videophone /Audiophone Facility**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Introduction to Videophone

SIGMA Wide and SIGMA Extreme Series terminal provides a Videophone feature which allows a user to initiate a video call by pressing an icon on the main screen of the terminal. Morpho*Wave®* Compact provides an audiophone feature without video.

“MorphoWave® SP”, “MorphoWave® XP2” and “VisionPass SP” don’t provide Videophone or audiophone features.

VisionPass Range terminals provide no Audio/Videophone feature.

This feature requires a Videophone server which is a PC with a VOIP client application using SIP protocol, such as Linphone.

This feature is useful for users to call access control administrator for help using the terminal, or to allow the administrator to check his face, a police badge, or any item which can be checked by video.

The diagram below show a typical use of this feature:

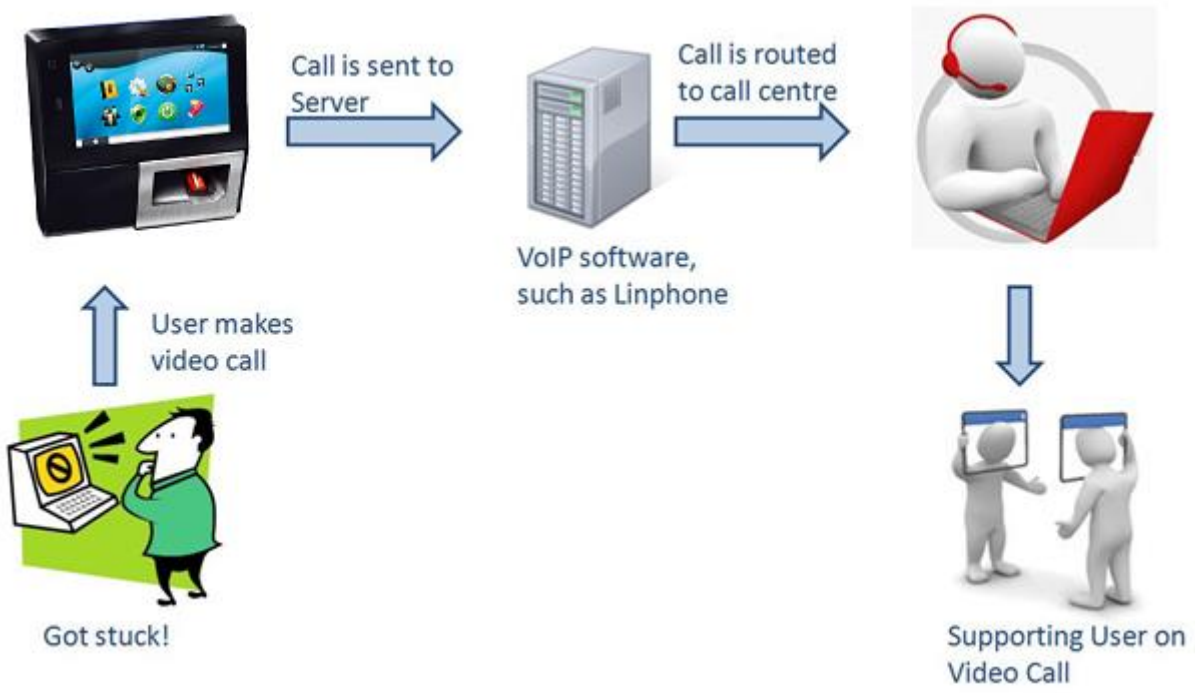


Figure 269: Video Phone Call Flow Diagram sample

For more information about Linphone, please visit Linphone web site at http://www.linphone.org/.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Configure Video Phone / Audio Phone Server

In order to make a video/audio phone call, it is a pre-requisite for the terminal to connect to computer based software, which can route the video call to the call center. Thus, the administrator needs to configure the server parameters, on which VoIP client application is installed. These servers are named as video phone servers.

An administrator can configure several video phone servers using **Add** functionality.

Access Path Access Path

Terminal Menu :

System Menu > Terminal Settings > Video Phone Configuration

NOTE: Only an administrator with full administrative rights can access this menu. In Enforced Security configuration, it requires a biometric control of the administrator. The configuration key misc.LCD_login_option must be set to the values 2 or 3.

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

MMI (Man-Machine Interface) > Video Phone Configuration

Pre-requisites

Terminal can be connected with video phone servers only through Ethernet or Wi-Fi™ network

Screens & Steps

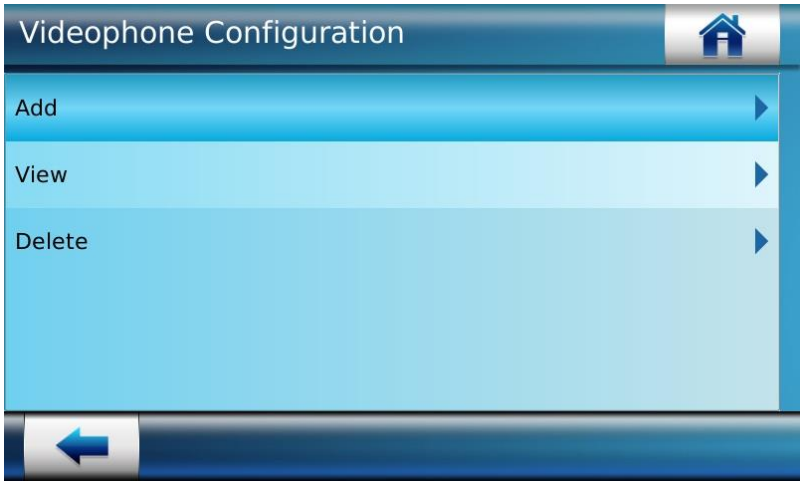


Figure 270: Adding a Server for Video Phone

1. Press on **Add** option for adding server with which video phone will be connected

Figure 271: Enter Server Name

2. Enter **Server Name**
3. Use "✓" button to move to next screen

Figure 272: Enter Server IP

4. Enter Server IP Address
5. Use "✓" button to move to next screen

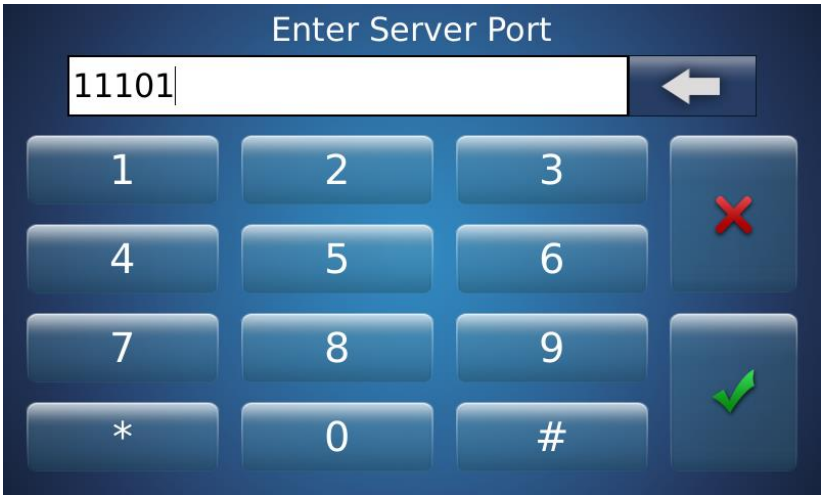


Figure 273: Entering Server Port

6. Enter Server Port
7. Use “ ” button to save

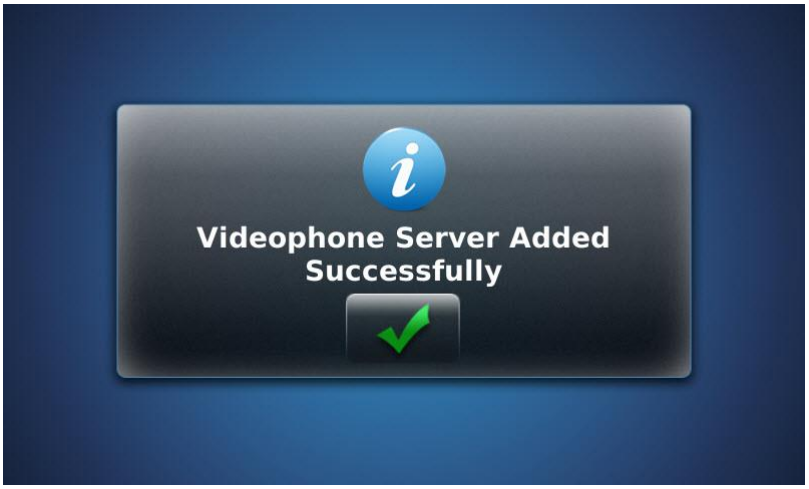


Figure 274: Videophone Server is added successfully

Results

A success message is displayed showing video phone server is added successfully. Video call can be connected once server is configured.

Viewing Video/Audio Phone Server Details

The administrator can view parameters of the video phone or audio phone server configured on Access and Time Biometric Terminal, by using this feature.

Access Path

Terminal Menu :

System Menu > Terminal Settings > Video /Audio Phone Configuration

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

MMI (Man-Machine Interface) > Video /Audio Phone Configuration

Screens & Steps

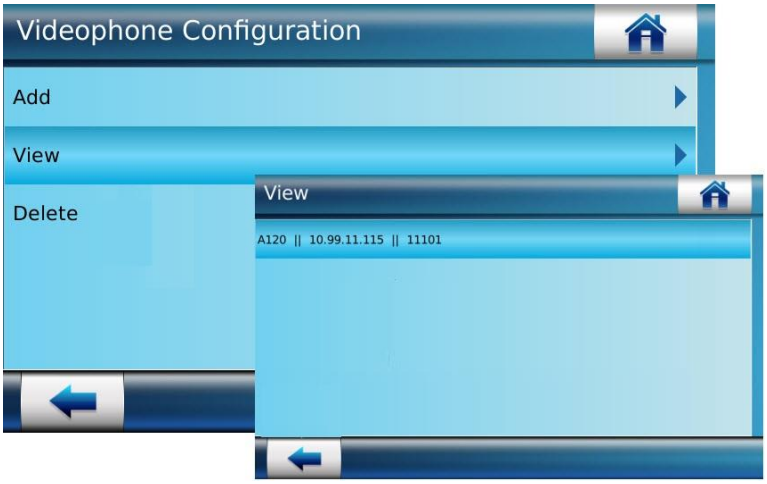


Figure 275: Viewing Video Phone Server Parameters

1. Press on **View** option
2. The configuration of server is displayed as below:
   a. **Server Name**
   b. **Server IP Address**
   c. **Server Port**
3. Use " " button to go back

Delete Video/Audio Phone Server

The administrator can delete registered videophone/audiophone from the terminal, by using this functionality.

Access Path

Terminal Menu :

System Menu > Terminal Settings > Video /Audio Phone Configuration

MMI (Man-Machine Interface) > Video /Audio Phone Configuration

Screens & Steps

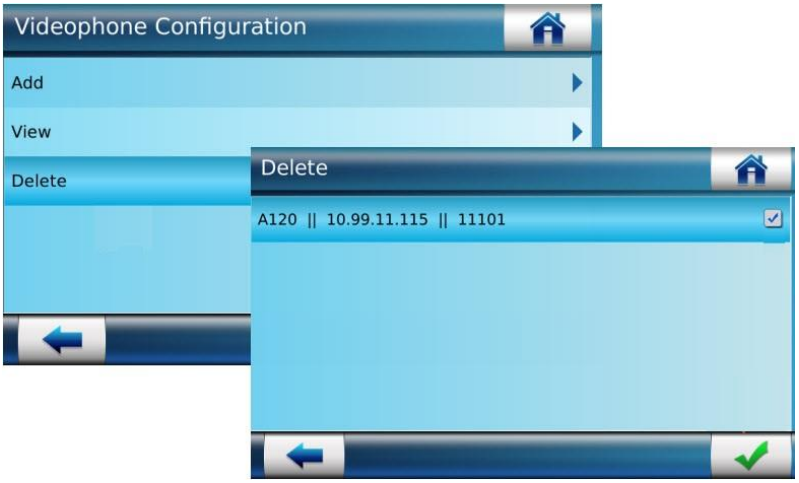


Figure 276: Deleting Video Phone Server

1. Press on **Delete**
2. On delete screen, select the server that is to be deleted
3. Press on "✔" button to delete server

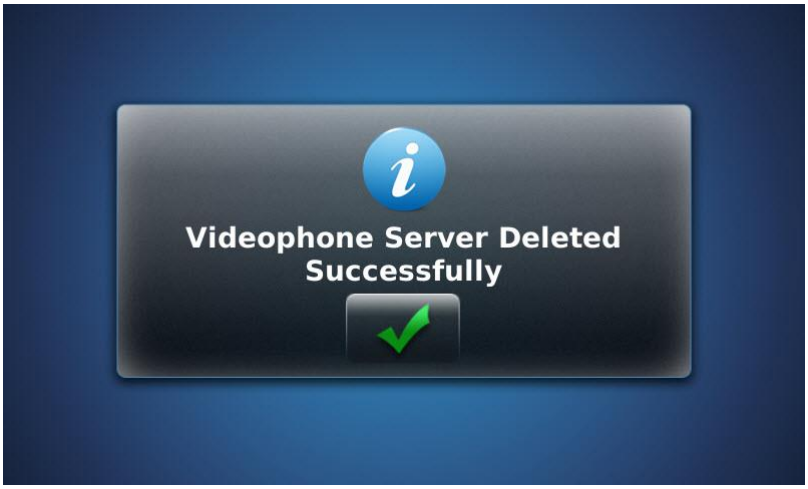


Figure 277: Video Server Deleted Success Message

Results

A success message is displayed on the screen showing video server is deleted. The record of the server is no longer available on the terminal

NOTE: The videophone icon on idle screen shall not be displayed if the videophone feature is not configured. The videophone icon is displayed on terminal only if at least a single VOIP profile is registered on the terminal

How User can make Video/Audio Call

Videophone feature of SIGMA Range or audiophone feature of Morpho*Wave®* Compact enable end users to make a video/audio call to a customer care center. The executive at customer care center can view the user and solve all functional queries on call.

NOTE: During the video phone call, the terminal does not allow any access control operations.

Pre-requisites

Video Phone Server must be pre-configured. Refer to "*Configure Video Phone /* Audio Phone Server"

Screens & Steps

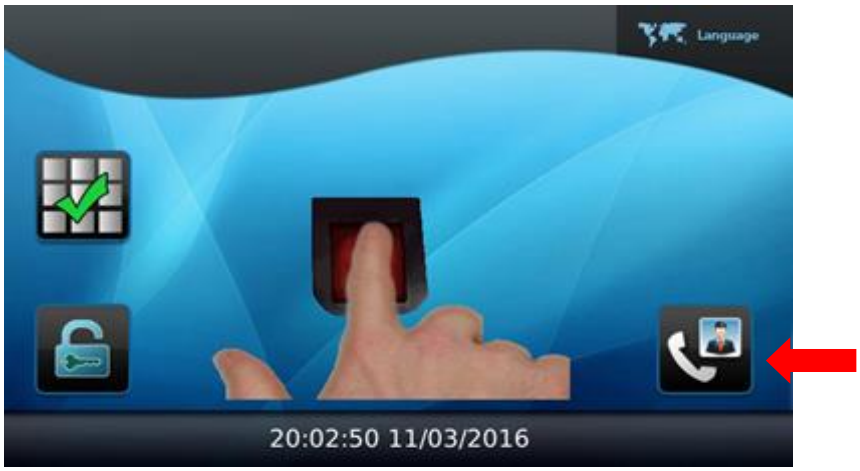


Figure 278: Making Video Call

1. On Home Screen of terminal, Press on **Call** icon, as shown in above screen

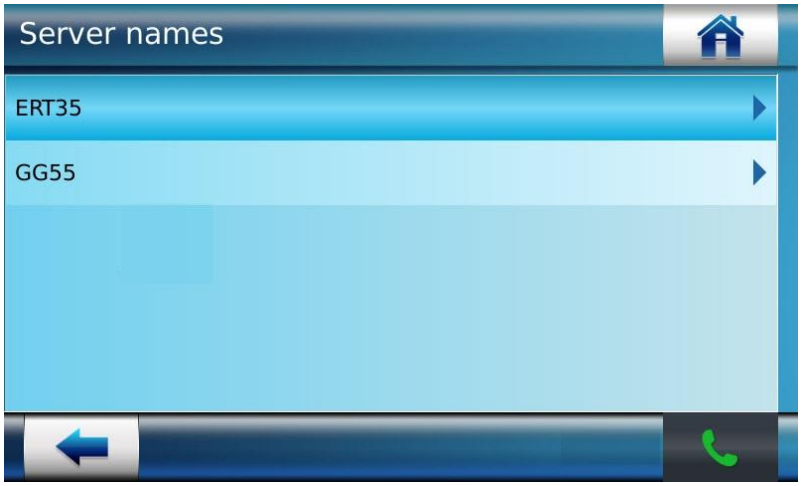


Figure 279: Select Server to make Video Call

2. The list of servers is displayed. Video call is connected to customer care center through these servers.
3. Select a **Server Name**
4. Press on **Dial** icon

Figure 280: Connecting to remote server

5. Press on **"Push to talk"** icon once video phone call is established with remote server

Figure 281: Push to talk

The user must press “ ” button and speak. The user must understand that this communication is one way in nature, hence when he speaks by enabling the microphone, he cannot hear the executive’s response.

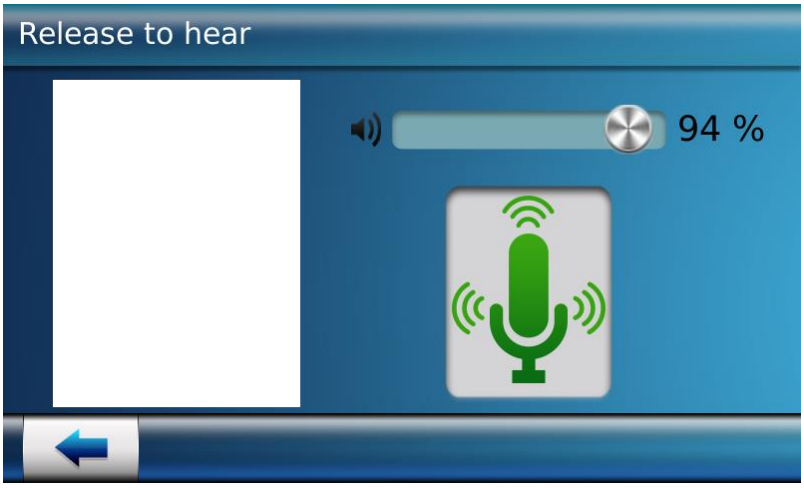


Figure 282: Release to hear

In order to enable hearing, the user must release the same button from the terminal end.

Results

A Video Phone Call is established with remote server. Video of end user is displayed on terminal and transmitted from terminal to the PC of customer center executive (CCE). It means only CCE can view the end user. While audio of both played at both end, means both end user and CCE can talk on a video call.

Section 7 : **Terminal Menu for SIGMA Lite+ Series**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

SIGMA Lite+ Series terminal Screens

This section is about the screens displayed on SIGMA Lite+ Series terminals.

Terminal Home Screen

During the power up, the IDEMIA Logo and boot up animation will be displayed.

Idle screen will display wallpaper, date and time with different icons.

There will be four icons on the SIGMA Lite+ Series home screen

- Information icon – To show 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 for IN and OUT are displayed.

Figure 283: Terminal Home Screen

The wallpaper can be set via external commands, please refer to "*Steps to Setup Wallpaper*" section.

Terminal Information Menu

When Information button " " is pressed, below Information Menu screen is displayed.

Figure 284: Information Menu

Terminal Details

The Terminal details will be displayed when “ ” icon is pressed.

Figure 285: Terminal Details

Communication Details

The communication parameters and their default settings will be displayed when “ ” icon is pressed.

Figure 286: Communication Details

Steps to Setup Wallpaper

On boot up, the SIGMA Lite+ Series home screen may either display the wallpaper (if set) or the default company logo. The wallpaper can be set by external commands. Following are the steps to set the wallpaper

- Login to MorphoBioToolBox
- Navigate to File Management >> Files Management
- Select an image to set as wallpaper, Select Picture as 'File Type' and Select Wallpaper as 'File Subtype' and Click on 'Set file'

Verify that the wallpaper on screen is the one set in the steps above.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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 issues such as power failure or interrupt in operation, corruption may occur. While booting up device if there is any corruption found in secure container component, terminal will display following screen in ® SIGMA Lite Series terminal.

Figure 287: Protected Data Corrupted Error

And on clicking on “ ” terminal lists all corrupted component as follows.

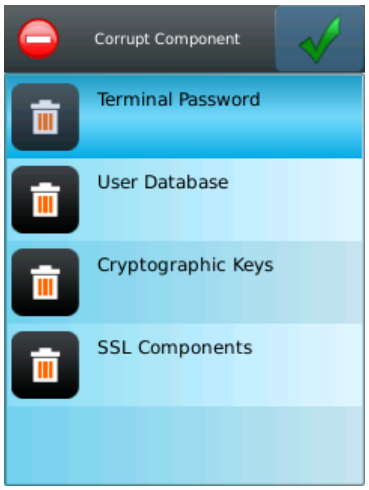
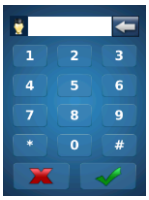
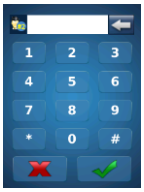
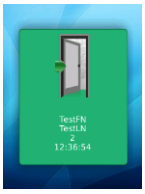
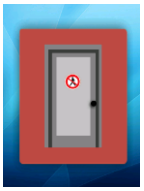
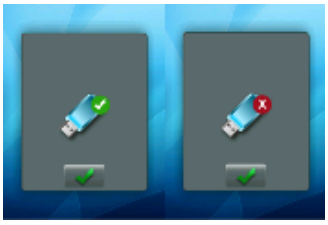
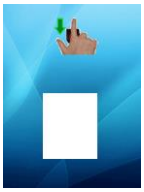
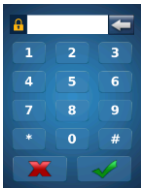


Figure 288: List Of Corrupted Components

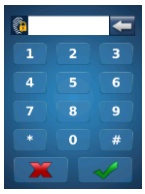
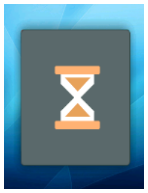
Once user selects “ ”, corrupted component recovers to default state after terminal Reboot.

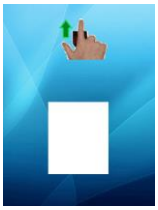
Display Screens and Actions

The following table, enlists the various actions and indications on the SIGMA Lite+ Series terminal and the corresponding screen appearance.

Display Screen	Action/Indication
	**Keypad Authentication**
	**Keypad Authentication for second user (In case of Multi User Mode)**
	**Access Granted**
	**Access Denied**
	**USB Information**
	**Live Finger Feedback with Animation**
	**Pin Entry Request**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Display Screen	Action/Indication
	**BIOPIN Entry Request**
	Bootup Animation Screen (default)
	**Please Wait…Action in Progress**
	Tamper Detected
	Distant Session Is Opened
	Controller Feedback
	Animation with Door Open
	Configuration Failed for Device

Display Screen	Action/Indication
	Configuration Failed for Communication
	Place Card
	Remove Card
	Prompt for second attempt
	Admin Card Detected
	Firmware Upgrade Started
	**Remove Finger**

Display Screen	Action/Indication
	Invalid Input
	Time Override Mode – Active
	Sensor DB Upgrade
	Terminal Blocked

Section 8 : **Terminal Configuration through Webserver**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access to Administration Menu through Webserver

NOTE: The Webserver is not available In Enforced Security configuration.

NOTE: The Webserver is no more available for “MorphoWave® SP”, “MorphoWave® XP2” and “VisionPass SP”.

The Webserver allows user to perform various actions and configurations on terminal, through below listed menus:

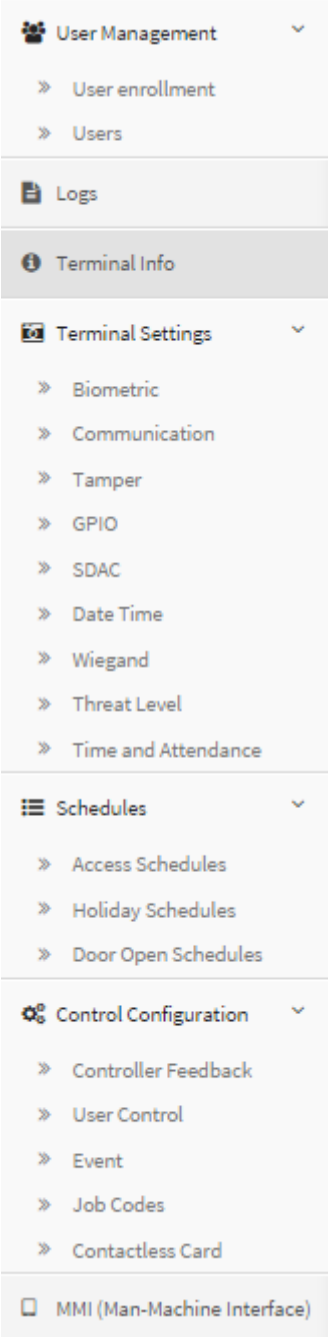


Figure 289: Webserver Administration Menu

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

MMI Menu : Used to configure LCD display parameters and modify graphical user interface.

Login to Webserver

An administrator can login to Access and Time Biometric Terminal through Webserver using password. An administrator can enroll new user in the system, edit user information, delete users from the terminal database, and reset user information from contactless smartcards.

Default password

For “MorphoWave® Compact Series” and “VisionPass Series”, default Webserver password value is “12345”.

Since the firmware 4.18.3, for “SIGMA Range Series”, there is no default password value anymore. Administrator has to set a password value first, using MorphoBioToolBox, before to connect to Webserver.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

Figure 290: Logging in Webserver

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

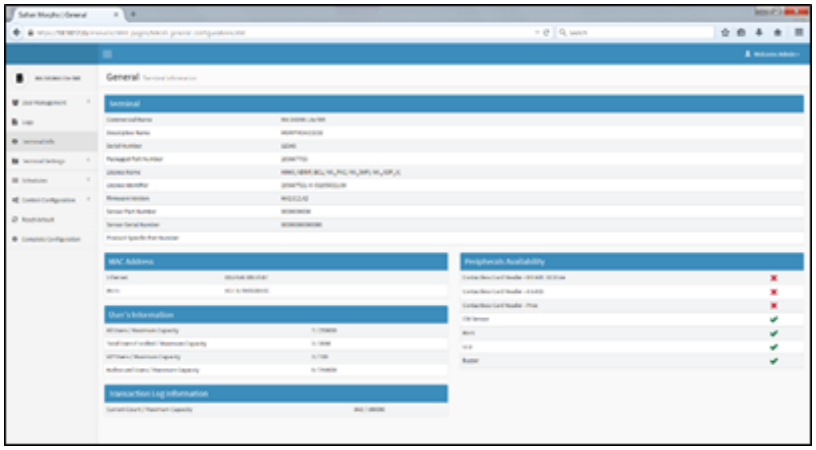


Figure 291: Administrator Menu

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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

User Enrollment in Database

This feature of Access and Time Biometric terminals allows an administrator to enroll new users in the terminal. The user information such as name, biometric data, 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.

Note: For VisionPass Range terminals, the biometric data acquisition is not available on Webserver tool.

Access Path

User Management > User Enrollment > Enrollment mode > DB Only

Screens & Steps

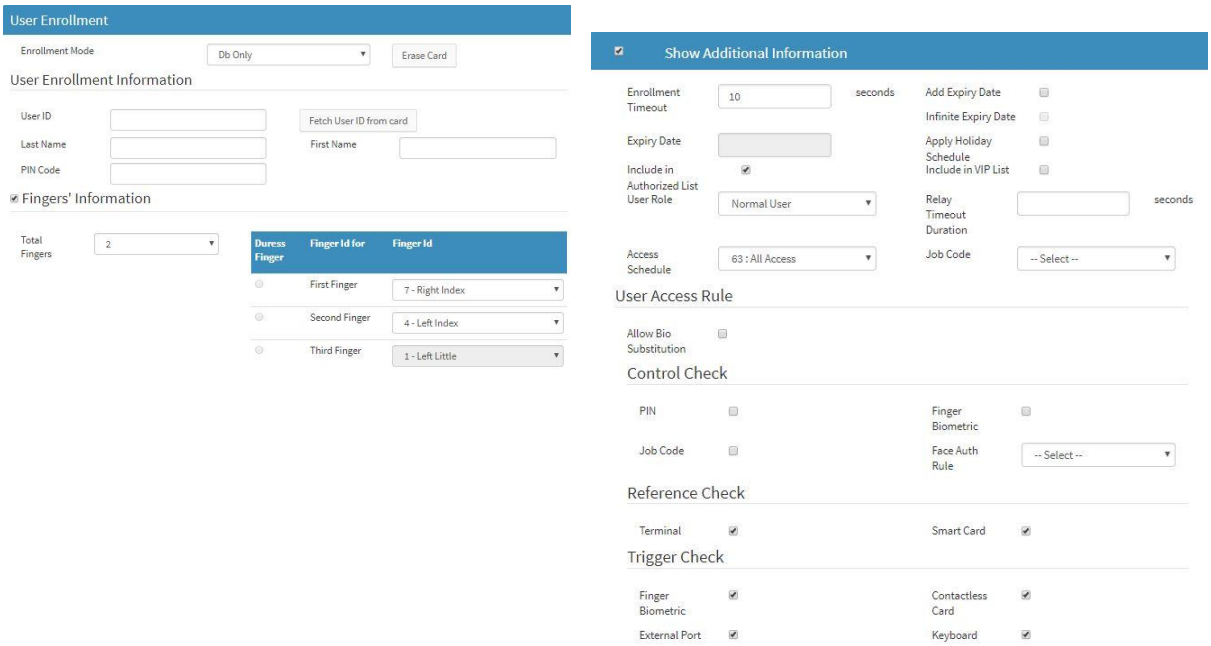


Figure 292: Adding user information

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.
- 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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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

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

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

   c. Select the Finger Id for First and Second Finger to enroll fingerprints of the user

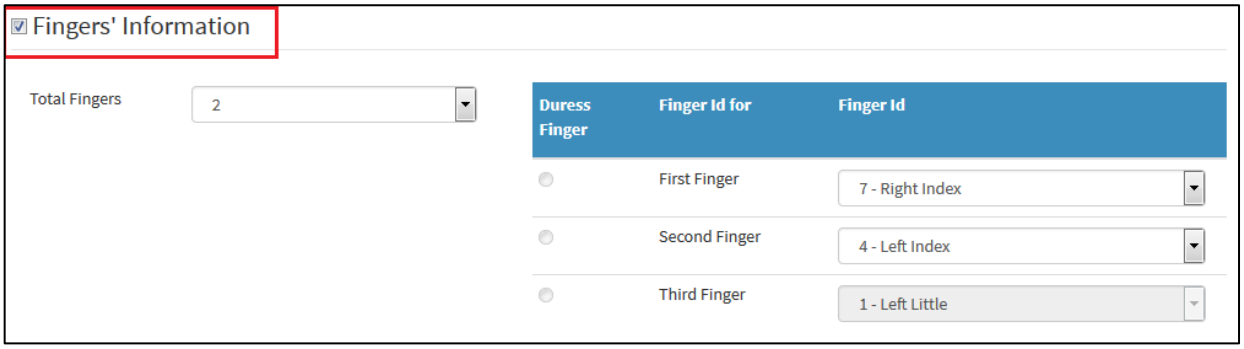


Figure 293: Enrolling Finger Index

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

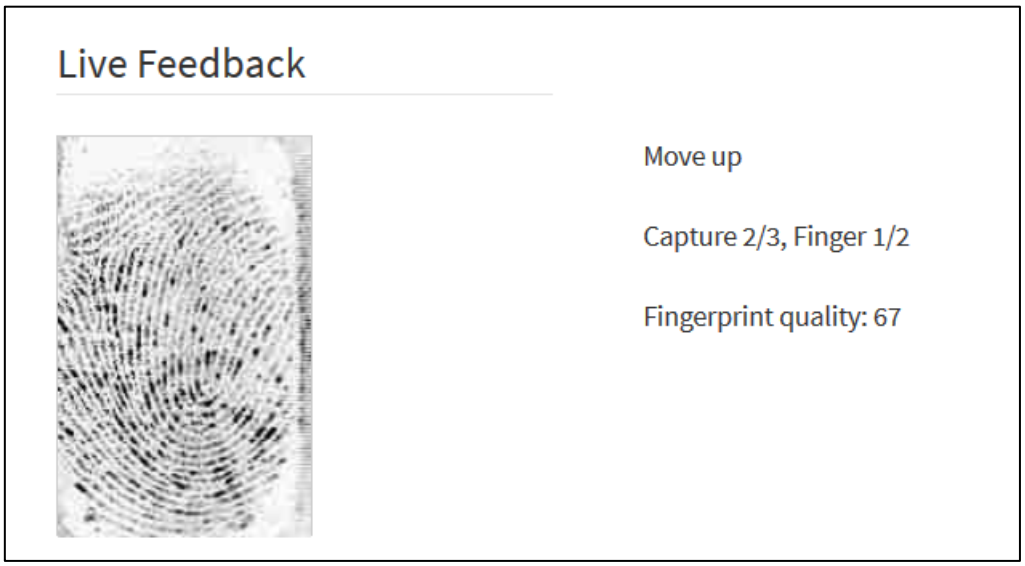


Figure 294: Biometric data capture

5. 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 "*SIGMA Range Series* Finger Placement Recommendation" section to know the correct position of finger.

6. Three Fingerprints are captured of the same user and the best quality image is auto-selected by the terminal
7. 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
8. If the administrator wants to capture Duress Finger, the Total Fingers to enroll should be set as '3'
9. Repeat steps 8 and 9 to enroll the duress finger.

Figure 295: Enter User PIN

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

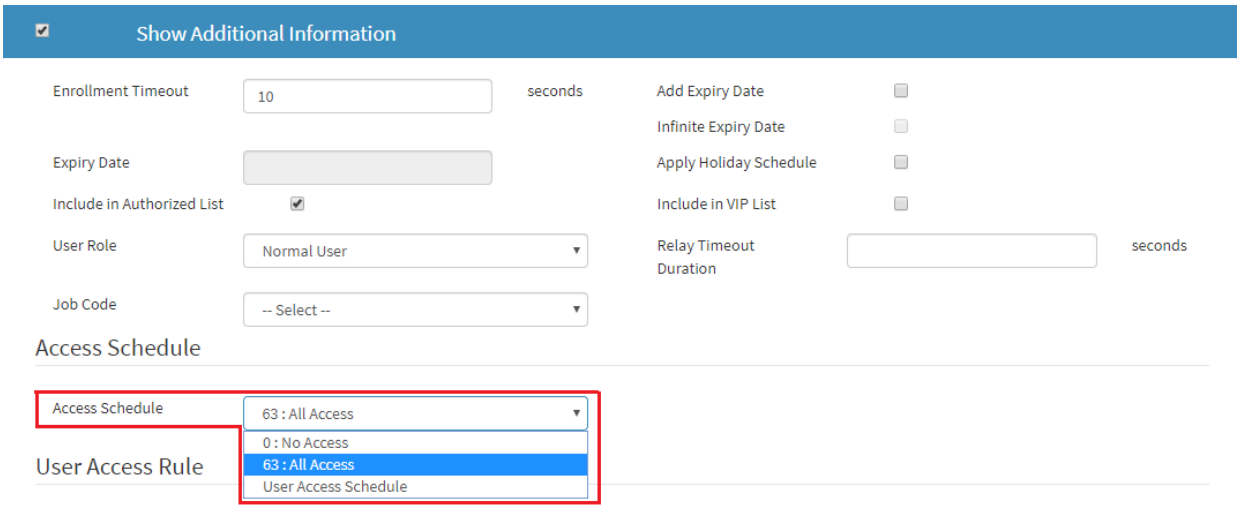


Figure 296: Assigning Access Schedule

11. 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" and "Define User Access Schedule"* under Configuration through Webserver section to know more about access schedule.

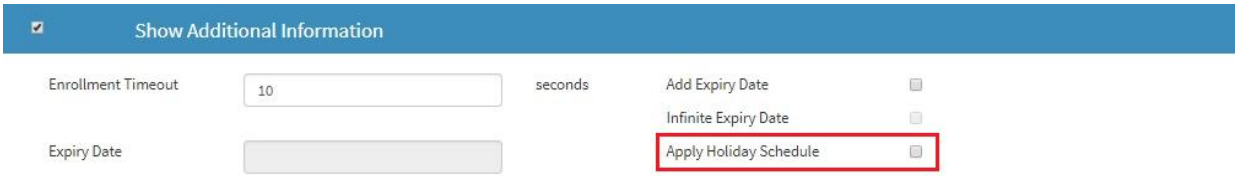


Figure 297: Enrolment Information Screen – Configuring parameters

12. 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 know more about access schedule.

13. Configure **Relay Timeout Duration** in seconds. The door stays open for the time duration defined here for the particular user.
14. Configure user **Expiry Date** in case user account requires to activate for specific duration or it can be activated forever
    a. If Infinite Expiry Date parameter is set to ON, 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.
15. 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 "Check User ID Authorized List" is ON, under Control Configuration > User Control.

16. 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.

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

Figure 298: Defining User Rule

18. The User Rule settings includes below parameters:
19. 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 biometric identification. If trigger event through biometric is OFF, then user cannot initiate the access rights check using biometric. And Biometric Check will be bypass for the particular user.
    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, 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
20. Under **Reference Check**, an administrator can configure whether user's information should be referred from Terminal database or/and Smartcard
    a. Set **Terminal** as ON, if terminal should refer to user's profile in database
    b. Set **Smartcard** as ON, if terminal should refer to user's profile in smartcard

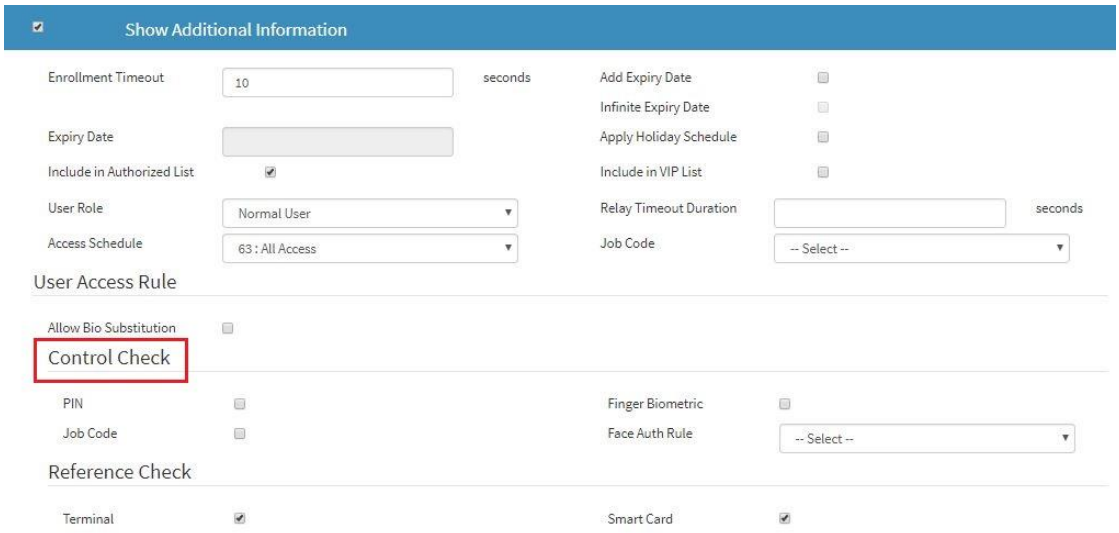


Figure 299: Defining User Rule – Control Check

21. Under Control Check, an administrator can set:
    a. **PIN** mode as ON, if PIN based authentication is required
    b. **Finger Biometric** as ON, if Biometric authentication is required
    c. **Job Code** as ON, if Job Code based authentication is required
    d. **Face Auth Rule,** this configuration defines face authentication check workflow rule. Possible values are “Disabled”, “Photo taking”, “Face detection (optional)” and “Face detection (mandatory)”. This is only available for SIGMA Wide and SIGMA Extreme Series terminals. Please refer to the section “*Additional User Controls*” for understanding the face detection workflow
22. **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
23. 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 biometric, terminal will match the biometric data captured 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.

User Enrolment in Card

The administrator can encode a contactless smartcard for a user, using this functionality. 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 user’s card.

Access Path

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

Screens & Steps

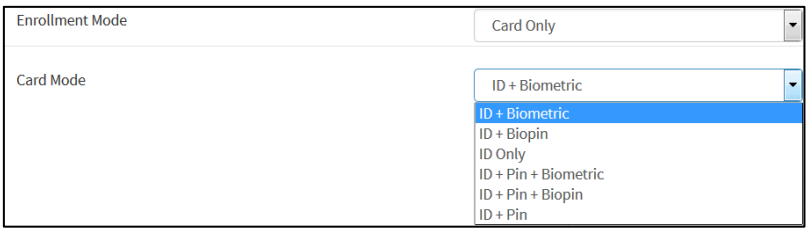


Figure 300: Select Card Data Format

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.
   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)

      Note: For VisionPass Range terminals, ID + BIOPIN option is not available
   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

      Note: For VisionPass Range terminals, ID + PIN **+ BIOPIN** option is not available
   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 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

The 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

Screens & Steps

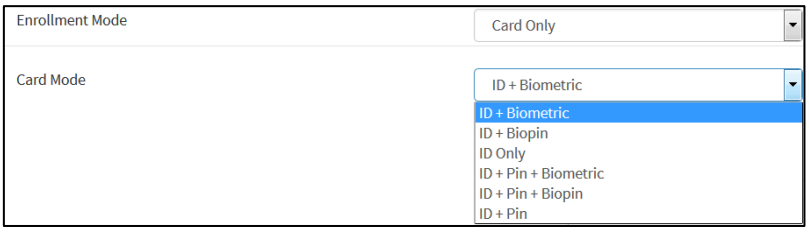


Figure 301: Select Card Data Format

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

Update User Information

The administrator can edit the user information stored in database, using this functionality. 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

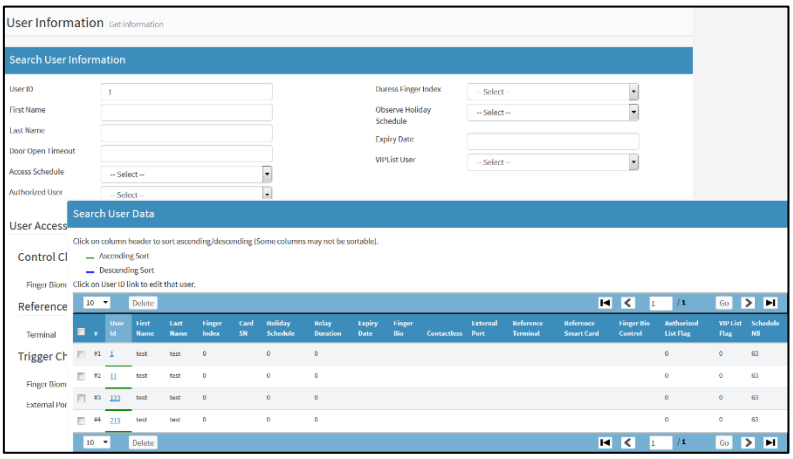


Figure 302: Selecting User ID

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

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.

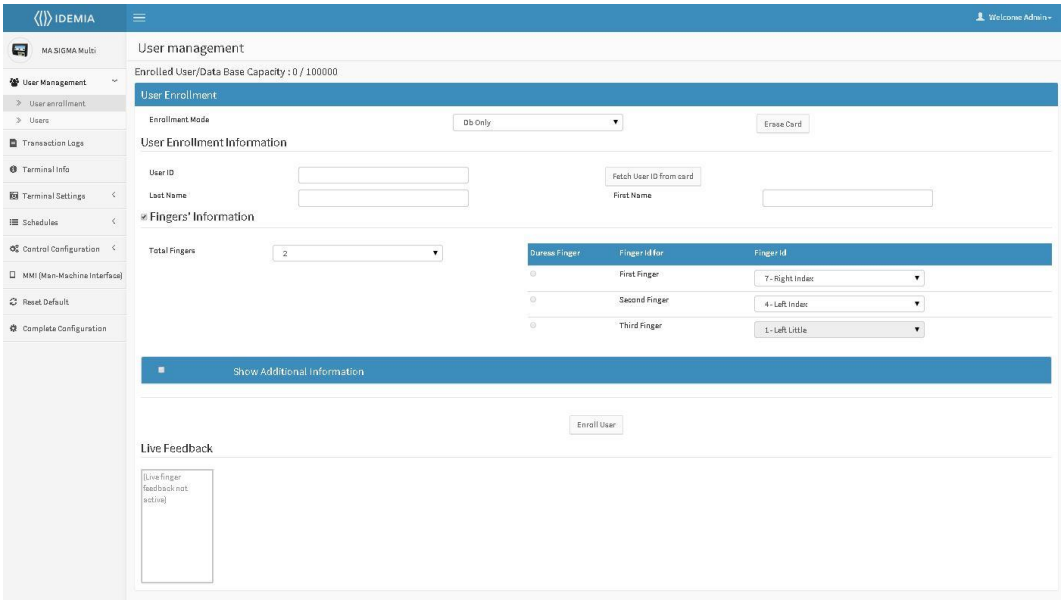


Figure 303: Enrolment Information screen is displayed for editing

1. Enrolment Information screen is displayed. An administrator can update below information:
   a. First Name and Last Name of the user
   b. Capture biometric data
   c. Update User Pin
   d. Configure Access Schedule
   e. Set Observe Holiday Schedule
   f. Set Door Open Timeout
   g. Add Expiry Date
   h. Configure Authorized list
   i. Configure VIP User
   j. Configure User Rules
2. To update a user field without capture biometric, uncheck the Fingers' Information box.
3. 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

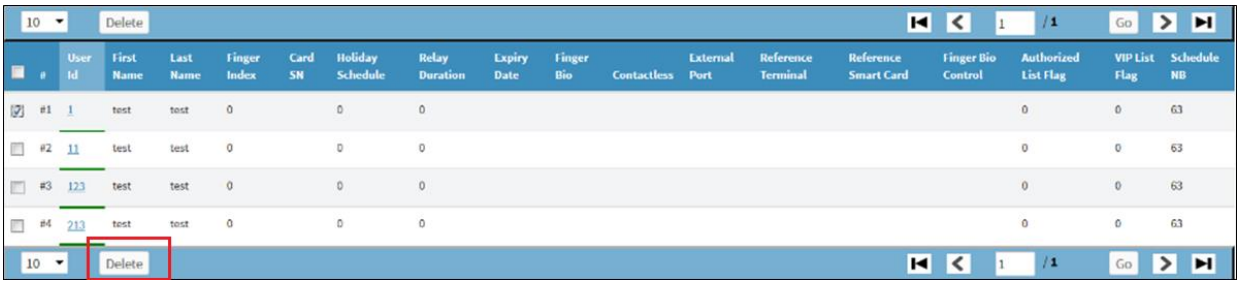


Figure 304: Deleting User

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

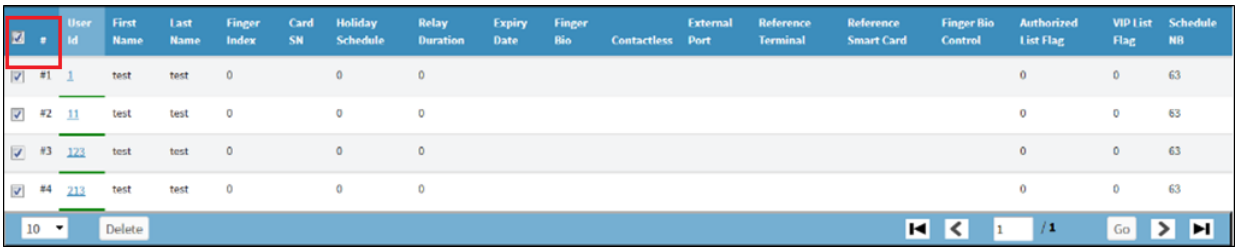


Figure 305: Select Delete All Users action

1. Select **Delete All Users** to delete all the user in the database
2. A confirmation message is displayed, asking to confirm the action
3. Press on **OK** to confirm delete all users action

Card Manager

Access and Time Biometric terminals allow user enrolment and authentication using contactless smartcards. When a user is enrolled on smartcard, the User Identifier, biometric Template and PIN/BIOPIN are stored in the card. Terminal can check this information on card for authenticating a user.

Note: For VisionPass Range terminals, BIOPIN is not stored in the card.

Using Card Manager Menu, an administrator can configure the contactless smartcard parameters, which are supported by Access and Time Biometric terminals.

Access Path

User Menu > Card Manager

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

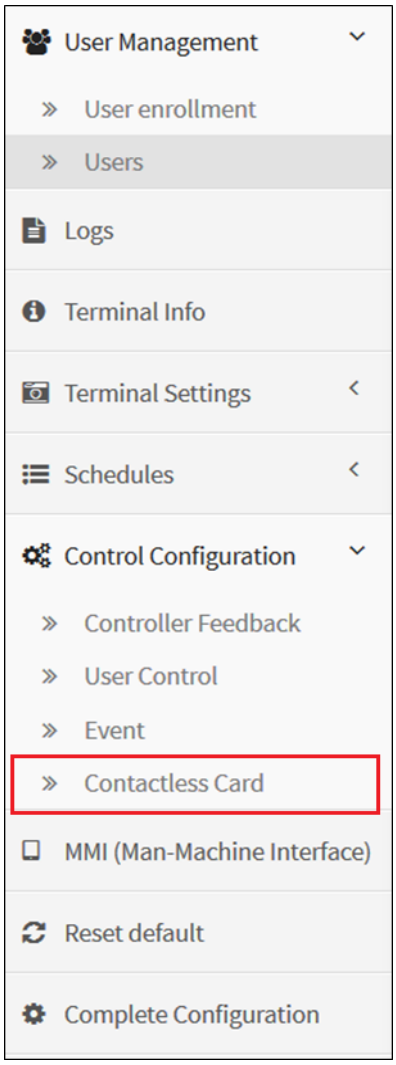


Figure 306: Contactless Card Configuration – Webserver

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 smartcard may have an expiry date. Once the smartcard 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, biometric template, 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 loses 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

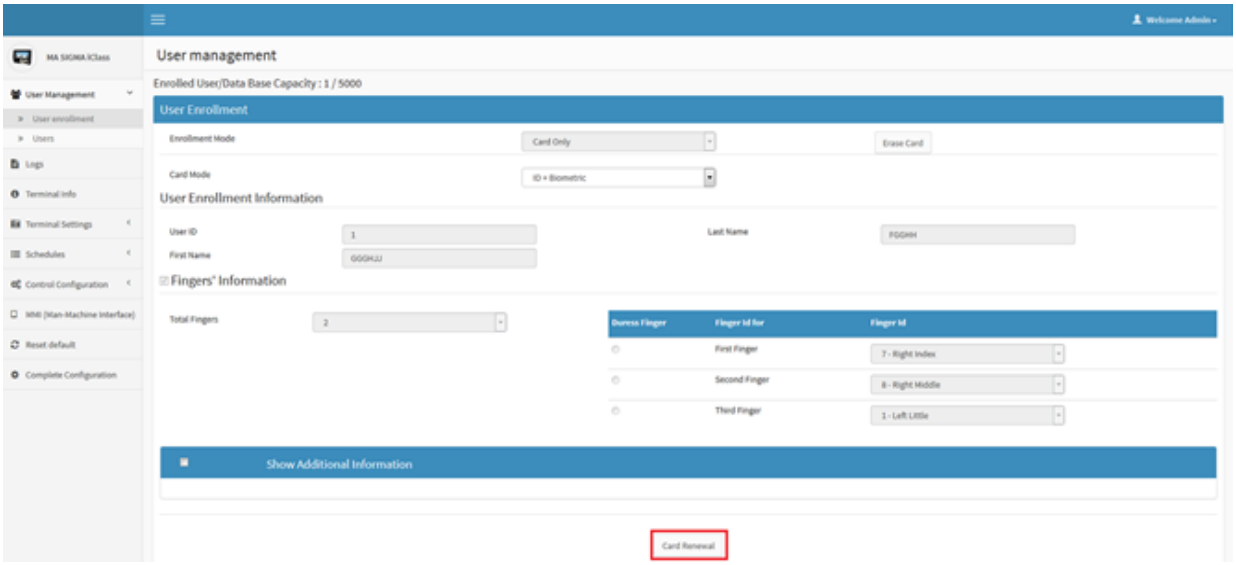


Figure 307: Renewal of User Card

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
    b. ID + BIOPIN

    Note: For VisionPass Range terminals, **ID+ BIOPIN** option is not available

    c. ID Only
    d. ID + PIN + Biometric
    e. ID + PIN + BIOPIN

    Note: For VisionPass Range terminals, **ID + PIN + BIOPIN** option is not available

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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 if it is configured. Now user can use this card for authentication.

Read Smartcard Profile

The administrator can set the type of card that Access and Time Biometric terminals will be able to read, using this functionality. 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 Parameters> Read Profile

Screens & Steps

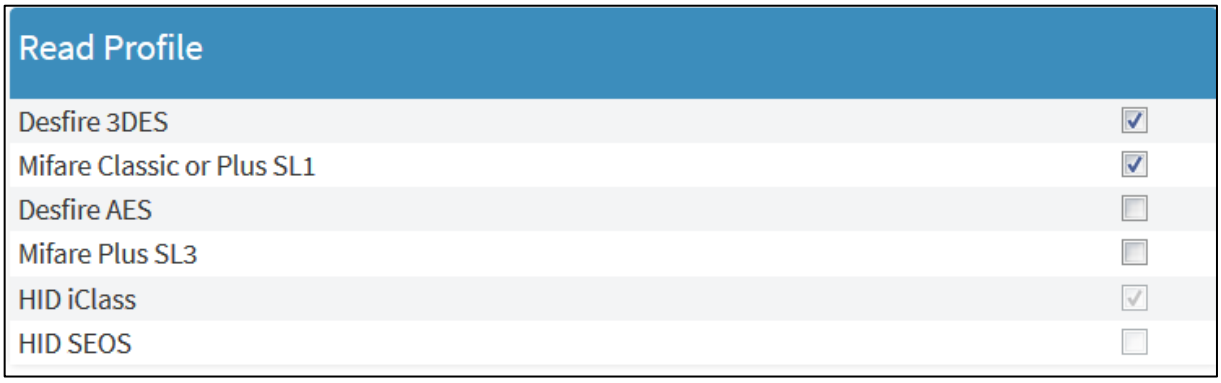


Figure 308: Smartcard Read Profile

Select **Read Smartcard Profile**

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

   ➔ <u>In case of MD Product</u>

   a. MIFARE® Classic

   b. MIFARE® Plus

c. MIFARE® DESFire® 3DES

d. MIFARE® DESFire® AES

➔ In case of iClass Product

a. HID IClass®

b. HID SEOS

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

Encode Smartcard Profile

The administrator can set the type of card that Access and Time Biometric terminals will be able to encode, using this functionality. 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 Parameters> Encode Profile

Screens & Steps

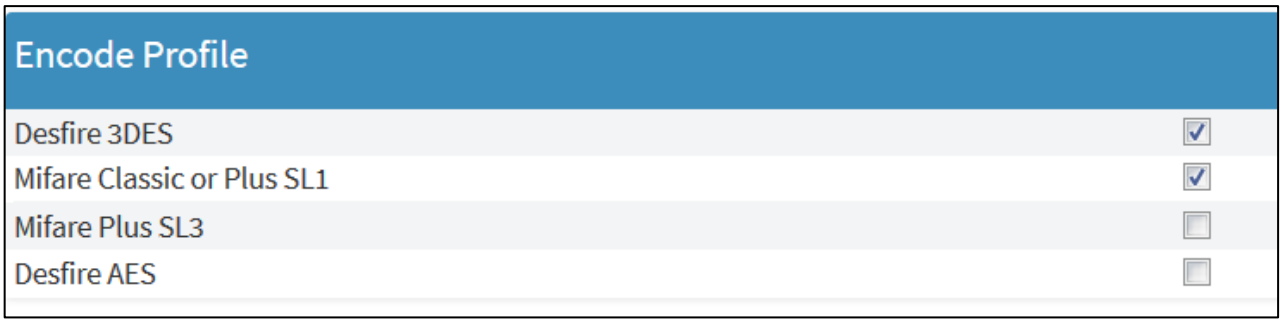


Figure 309: Smartcard Encode Profile

Select **Smartcard Encode Profile**

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

NOTE:

- It is not possible to encode several type of MIFARE (Classic or Plus) 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 encoding.

2. 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 configuration > MIFARE Start Block

Screens & Steps

Figure 310: Setting No. of Block & Start Block

Select **No. of Blocks** & **Start Block**

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

Select Keyset for Reading MIFARE® Cards

The administrator can select a key set that is used by terminal for authentication and reading MIFARE® cards, using this functionality. 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 configuration > MIFARE Key Policy

Screens & Steps

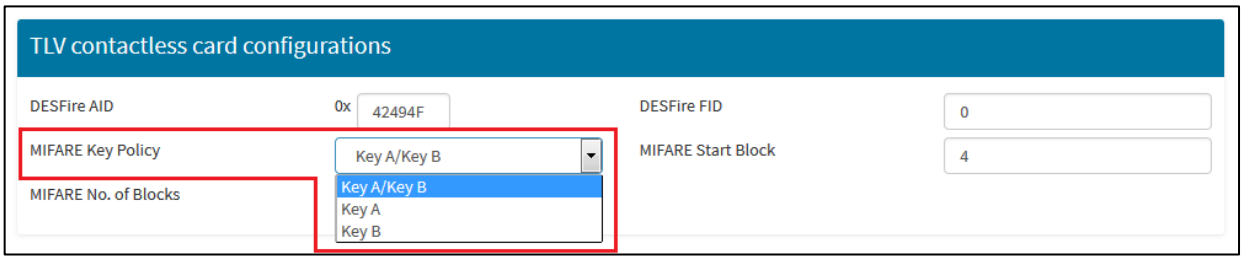


Figure 311: Key Policy configuration

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

Select Enroll ID Format

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

Access Path

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

Screens & Steps

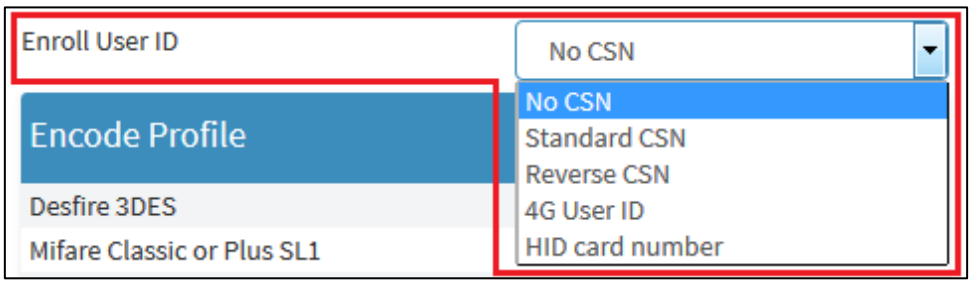


Figure 312: Selecting Enroll User ID Format

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
{
```


DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

```
                    //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
            }
```

Note: This option is not available in VisionPass Range terminals.

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

Note: This option is only available in iClass product.

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

Configure Partial CSN

The 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, using this functionality.

Access Path

Webserver > Control Configuration > Contactless Card > Partial CSN Configuration

Screens & Steps

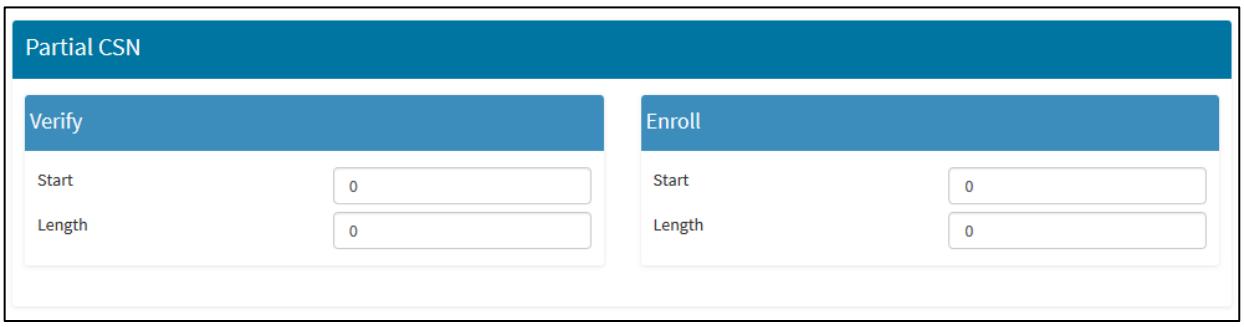


Figure 313: Configure Partial CSN for Enroll and Verify

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 “Reverse CSN” or “Standard CSN”.

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

The administrator can specify the value of Application ID and File ID for reading DESFire® cards, using this functionality. 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 configuration > DESFire AID

And Webserver > Control Configuration > Contactless Card > TLV contactless card configuration > DESFire FID

Screens & Steps

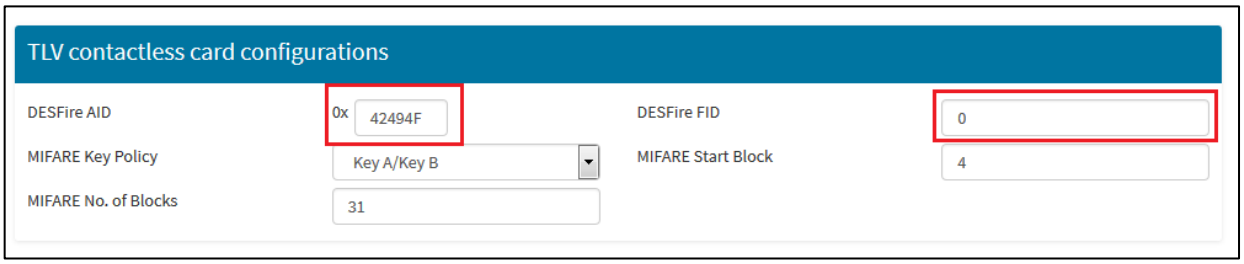


Figure 314: Configuring Application ID and File ID

1. Select Application ID
   a. Configure Application ID in range of 0x000001-0xFFFFFF.
   b. Default Application ID 0x42494F

   Note: Default Application ID is 0x464143 for VisionPass Range terminals.

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

The administrator can configure the offset to read the data from 2APP iCLASS® cards, using this functionality. 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 configuration > I-Class Page Offset

Pre-requisites

SIGMA Range Series iCLASS®, Morpho*Wave*® MDPI, Morpho*Wave*® XP2, VisionPass MDPI, VisionPass SP MDI required to configure Offset for reading iCLASS® card.

Screens & Steps

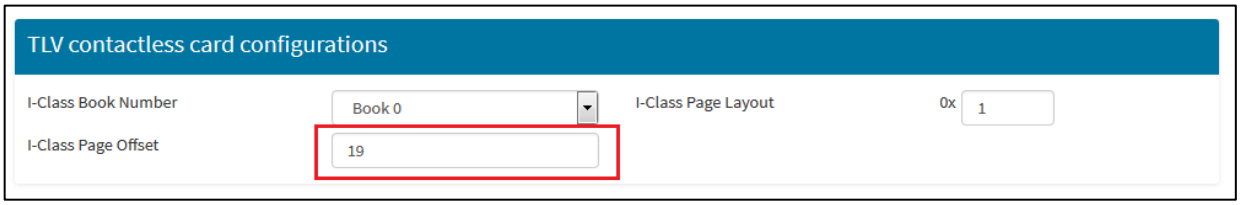


Figure 315: Set Key Offset for iCLASS® cards

1. Select **-Class Page Offset**

   a. Configure **Page Offset** in range of 0-255.

   b. Default **Page Offset** is 19

2. Press on **Save** button to save the Offset value

Defining Active Pages for Reading iCLASS® Cards

The administrator can configure the active page for reading data from 16APP iCLASS® cards, using this functionality. 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 configuration > I-Class Page Layout

Pre-requisites

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

Screens & Steps

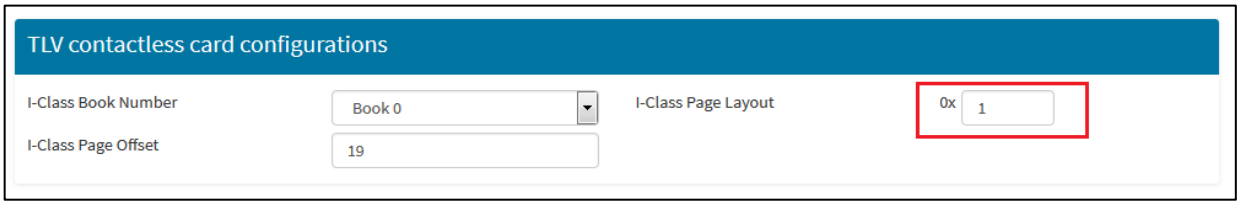


Figure 316: Configure Active Pages for iCLASS® cards

1. Select I-**Class Page Layout.**
    a. Configure **Page Layout** in range of 0-5.
    b. Default **Page Layout** is 1
2. Press on **Save** button to save

Reset Card

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

Access Path

Webserver > User Management > User Enrollment

Pre-requisites

A smartcard has user details stored

Card is secured with the same key as on terminal

Screens & Steps

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Figure 317: Reset card

Click on **Reset Card**

1. Terminal will ask to **Place Card** at card reader.
2. 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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 9 : **USB Scripts**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

USB Scripts

NOTE: USB scripts are not available In Enforced Security configuration.

Access and Time Biometric terminal can be configured using encrypted USB scripts. These scripts can be created from MorphoBioToolBox. When user connects the USB drive which contains the USB scripts to the terminal, the intended operations will be performed and corresponding results will be written into the USB drive. User can check the result of executing these scripts with the help of **MorphoBioToolBox** to “Read response” functionality. Using this feature, user can change the configuration of those terminals which are not connected to the network. Please refer to the **MorphoBioToolBox** User guide for more details.

Note: User can use the same USB Scripts to configure one or more terminals. In such cases user needs to ensure that the result of each USB Script execution will overwrite the previous result.

User can create the following scripts, using MorphoBioToolBox:

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

MorphoBioToolBox :

Login to MorphoBioToolBox > Device Settings > USB Scripts

Pre-requisites

USB Drive

NOTE: USB mass storage key should not be partitioned but should contain only one drive.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 10 : **Access Control**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access control presentation

Typical architecture of an access control system

Typical access control system architecture includes:

One Access and Time Biometric terminal per area for access control.

A user management or administration menu.

A Central Security Controller to take centralized decision, in order to provide physical access commands (open the door).

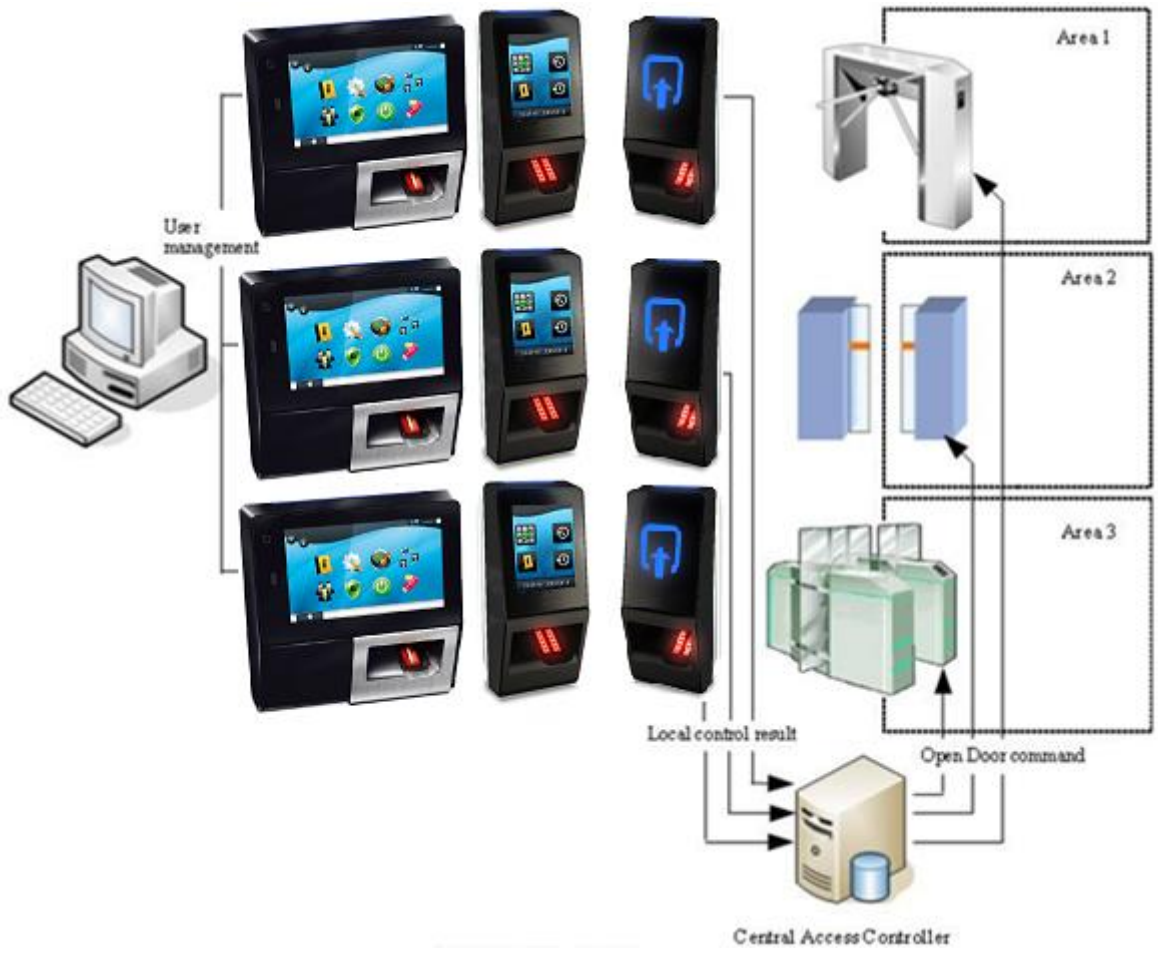


Figure 318: Typical access control system architecture for Access and Time Biometric Terminal

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Typical access control process

1. The administrator must enroll all the authorized users. This means that a record is created for each user, containing a unique identifier and biometric.
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 an "access granted" message to the terminal and an "open" command to the gate controller.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Preliminary: adding a biometric template in local database

Access Path

Terminal Menu :

Administration Menu > User Menu

Webserver (not available In Enforced Security configuration and in all configurations for "MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP"):

Webserver > User Management Menu

For SIGMA Wide, SIGMA Extreme, Morpho*Wave*® Compact, Morpho*Wave*® Compact XP2

The administrator can manage a biometric database in the Access and Time Biometric Terminals by following the steps enlisted on the User Menu or by means of the User Management Menu of the Webserver. This includes User enrolment and encoding Contactless cards containing user templates.

The local database can be exported ciphered to other Access and Time Biometric Terminals using a USB Mass Storage Device.

For SIGMA Lite Series and & Morpho*Wave*® SP Series

The management of internal biometric database can be done externally (through the Webserver) in SIGMA Lite Series terminals. This includes generating contactless cards containing user templates and User enrolment.

The local database cannot be exported to other terminals via USB Mass Storage Device for SIGMA Lite Series.

A message can be sent to a distant host from SIGMA Range Series, Morpho*Wave*® Range Series, to inform that changes were made on the internal biometric database of the terminal. These changes can be exported to the host centralized database.

For VisionPass Range terminals

The administrator can manage a biometric database in the Access and Time Biometric Terminals by following the steps enlisted on the User Menu.

The local database can be exported ciphered to other Access and Time Biometric Terminals using a USB Mass Storage Device.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access and Time Biometric Terminal operating modes

Standalone mode or Slave mode

The Access and Time Biometric terminals support two exclusive operating modes:

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

Standalone mode: Identification and/or Authentication

When in standalone mode, the Access and Time Biometric Terminal supports mainly two types of access control processes. These can be used separately or together:

- The 'identification' process, starts when the user places his finger on the biometric sensor.

  For VisionPass, we have 2 types of 'identification' process

  - With intentional biometric capture is enabled: in this case the facial biometric acquisition is started as soon as the user places his face in front of the terminal
  - With intentional mode disabled: in this case the facial biometric acquisition is started as soon as the user presses on specific icon and places his face in front of the terminal

  This option is available in **Security Menu > User Control Settings > Camera Enabled Per User Request**. The value is ON/OFF

  OFF (intentional biometric capture is enabled) means Camera is activated in continue.

  ON (intentional biometric capture is disabled) means Camera is activated on user's request.

  This process is described in the "*Access Control by Identification*" section. This section is still compliant, we have just added that the Facial Biometric is started as soon as a face is detected on the biometric area (if intentional biometric capture is enabled) or an identification request is launched by the user via the icon button (if intentional biometric capture is enabled)

- 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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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.

For VisionPass Range terminals, we have 2 types of 'authentication' process

- With intentional mode enabled: in this case the facial biometric acquisition is started as soon as the user places his face in front of the terminal and before the smartcard presentation, ID entering…
- With intentional mode disabled: in this case the facial biometric acquisition is started as soon as the user presents his smartcard to the card reader, entered an ID on keypad,… and places his face in front of the terminal

This option is available in **Security Menu > User Control Settings > Camera Enabled Per User Request**. The value is ON/OFF

- OFF (intentional biometric capture is enabled) means Camera is activated in continue.
- ON (intentional biometric capture is disabled) means Camera is activated on user's request.

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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access Control Process in Identification Mode

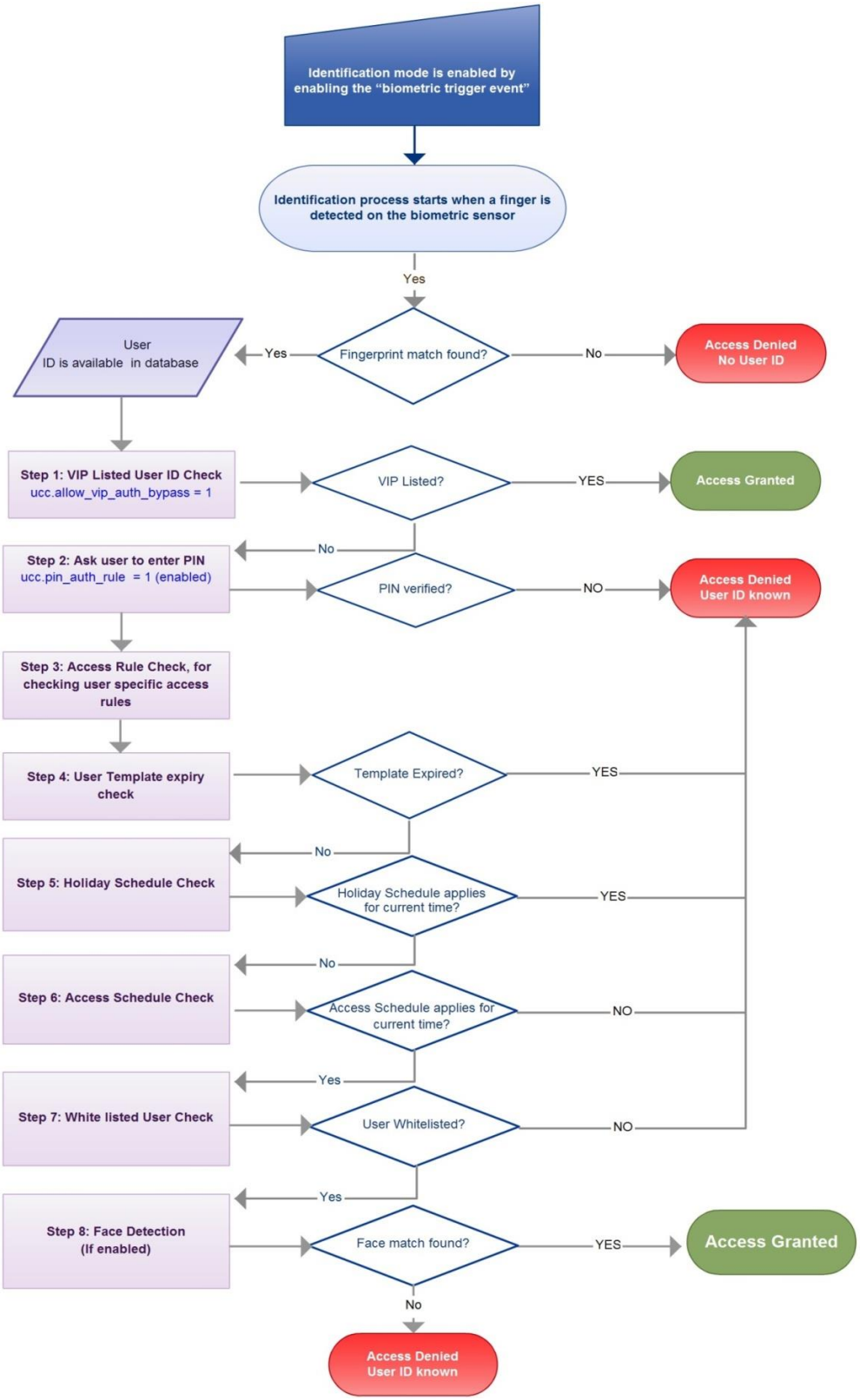


Figure 319: Access Control Flow Diagram when Terminal is in Identification Mode

Access Control Process in Authentication Mode

Figure 320: Access Control Flow Diagram in Authentication Mode

Note: Face detection applies only for SIGMA Wide and SIGMA Extreme Series terminal.

Access Control Process for VIP Users

If the administrator lists a user as VIP, the access control flow for that user will differ from the general access control flow. When a user is enrolled as VIP and the VIP bypass is enabled, then the VIP user is exempted from authentication using biometric data, PIN, BIOPIN or Face detection.

The Access Control Process for VIP users has following steps:

1. A user initiate access request
2. Once identified as a VIP user, terminal will not ask for any biometric data
3. Other checks such as (if configured), access schedule, holiday schedule, banned card, authorized list, expiry date, trigger event check, etc. are done as per the authentication process. Please refer to Step 5 in *Access Control Flow Diagram in Authentication Mode*
4. On successful authentication, access is granted to a VIP 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	The administrator can enable or disable VIP user authentication bypass for threat level 0 by using this parameter. If this parameter is set to “0”, VIP user authentication bypass is not allowed. If this parameter is set to “1”, VIP user authentication

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

		bypass is allowed. A VIP user is granted access without authentication checks.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access Control Result

Information for the User

The Access and Time Biometric Terminal communicates the result of the access right check by a local audible and visible signal. These signals are described in the "*Audio Man Machine Interface*" section.

For example:

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

when the access is denied, the terminal emits a low pitched note.

NOTE: The duration to display Access control result messages on terminal LCD, can be configured using the 'time_and_attendance.tna_message_timeout' parameter.

For more information about this parameter, please refer to **Parameters Guide.**

Information for the Administrator

The Access and Time Biometric 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 Access and Time Biometric 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 includes the user's identifier) that is sent to the distant system is described in the **Remote Message Specification** document.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access Granted

Figure 321: Access Granted Diagram for Access and Time Biometric Terminal

Access Denied

Figure 322: Access Denied diagram for Access and Time Biometric Terminal

Section 11 : **Access Control by Identification**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Identification Mode Description

Identification Process

The identification process consists in retrieving the identity of an unknown person, by comparing the data (presented by the unknown person) with a database that contains similar 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 on the Access and Time Biometric Terminal begins by comparison of the acquired biometric data by the sensor, with the biometric data 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 or face 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. These signals are described in the **"***LED Buzzer Sequence***"** section.

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 the user.

For more information on the management of the internal database, please refer to the "*Terminal Database Management*" section.

Identification Modes (database extension licences)

Identification process relies on the database. User data is stored at the time of enrolment and this serves as a reference for the identification process. For more details on database of Access and Time Biometric Terminals, please refer to "*database size*" section. By default, the biometric data of two fingers per user record is stored in SIGMA Wide and SIGMA Extreme

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Series terminals, eight fingers in Morpho*Wave®* Series terminals, a face template based on 3 images (RGB, NIR, 3D) in VisionPass terminals, a face template based on 1 image (RGB) in VisionPass SP terminals. The maximum database capacity can be extended by installing specific licenses. For more details on supported licenses, please refer to "*Terminal License Management*" section.

Compatibility with Access Control Systems

When the identification mode is activated, the Access and Time Biometric 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 distant system, as described in "*Sending an Access Control Result Message*" section

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

User Interface

In this mode, the Access and Time Biometric Terminal waits for the placement of a finger, or the swipe of an hand, or detection of face on the biometric sensor. This state is displayed to the user by a specific signal, as described in "*Terminal States*" section.

The identification process begins when the user's finger or face is detected on the biometric sensor/area.

Place finger on biometric sensor

Figure 323: Identification Mode

The biometric data are captured, and then compared to the biometric database on 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.

When the identification process is completed, whatever is the result (identified or not identified), the terminal automatically goes back to its initial state: This implies that it will wait for finger to be placed on the biometric sensor or new user's face to be detected.

If a user, already identified, arrives less than 3 seconds after passing in front of the VisionPass SP, it will display the message "already matched" or "already denied".

When the administrator has not enrolled any users into the terminal database, the identification process is disabled. None of the users are granted access. The terminal notifies this invalid state to the user as described in "*Terminal States*" section.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 12 : **Access Control by Authentication**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Authentication Process

Introduction

The Access and Time Biometric Terminal offers an authentication mode designed to work with contactless smartcards. These contactless smartcards are 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' refers to 'contactless smartcard'.

Authentication process

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

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 instead compares the data provided by the user with the reference data provided by the same user during the enrolment phase.

Access control by authentication

To provide his identity, the user presents his personal identity card that contains the User ID. This action starts the authentication process.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Figure 324: 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 the 'biometric check' is required, the captured biometric data is compared with the reference biometric data of the user, acquired during enrolment process.

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

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

The Access and Time Biometric Terminal allows the 'identification' and 'authentication' modes to begin concurrently, as specified in "*Multifactor Access Control Mode*" section.

Contactless Smartcard

The terminal ignores contactless cards encrypted with unknown 'Card-terminal' authentication keys. The terminal shall not allow access if the user authentication key on the 'card' does not match with the corresponding key stored in the terminal database.

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

All authentication modes begin with a valid User ID. The other data that is required to complete authentication depends on the authentication mode that is selected.

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

List of contactless cards validated

Please refer to the **Contactless Card Specification** document.

Authentication Process Options

The Access and Time Biometric Terminal offers several authentication methods depending on the reference biometric data location of a user and the level of security 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.

Additionally the administrator can disable the biometric check as specified in the sections "*Manual bypass of biometric control*" and "*Automatic bypass of biometric control*".

Manual bypass of biometric control

The administrator can disable the 'Biometric control', which is enabled by default. The administrator can also define a user rule for a particular user. In this rule, the trigger event through biometric can be disabled while the trigger event through 'Card' can be enabled.

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

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

The terminal doesn't require the user to present a finger or face to the biometric sensor. The access is granted without a 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 Access and Time Biometric Terminal offers an authentication mode which depends on the content of the user's 'card'.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

The terminal searches the user card for data to ascertain if biometric control is mandatory or not.

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 notified to the user by audible and visible signals, as described in the "*Terminal User Interface*".

Compatibility with Access Control Systems

When the identification mode is activated, the Access and Time Biometric 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 distant system, as described in "*Sending an Access Control Result Message*" section

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Biometric check, biometric data on user's card

Description

In this mode, each user's card contains an identifier and the biometric data of the user. The terminal compares the biometric data captured by the sensor, with the reference biometric data 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 as a reference.

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

Since the data on the 'card' is used as a reference source, the internal database of the Access and Time Biometric Terminal is not used. This implies that the administrator needs not encode any of the user information into the terminal database at the time of enrolment.

User's data required on the user's card

The administrator must encode at least the following information into the user's card.

the user's identifier (User ID),

The biometric data of user.

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

Activation key

The administrator needs to ensure that the 'card' Type selected at the time of User Enrolment must be able to accommodate at least the User ID + Biometric.

Using Terminal Menu or Webserver, the administrator can configure the User Record Reference parameter appropriately. This is to enable the usage of 'card' for authentication. Please refer to "*User Enrolment in Database*" *(Step: 37)*.

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 present his finger to the biometric sensor, for biometric authentication.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

NOTE: the face biometric acquisition is done in background for VisionPass Range terminals (no invitation).

Figure 325: Authentication with user's fingerprints on contactless card

The terminal compares the captured biometric data, with the reference biometric data on user's card.

The authentication process is successful (identity confirmed) if the captured biometric data matches with one of the reference biometric data. The authentication process fails (identity not confirmed) if the captured biometric data does not match.

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

On completion of the authentication process, irrespective of the outcome, the terminal will automatically go to its initial state. This implies that it will wait for another user's card to be detected.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

PIN verification - PIN stored on card

Description

In this mode, each user's card contains a User ID, unique PIN Code and the biometric of the user. The terminal detects the user by means of the User ID on his 'card'. For authentication, it compares the entered PIN Code with the corresponding PIN on the user's card. The terminal will now expect the user to present his finger or face to the biometric sensor, provided biometric checks are enabled and the PIN has matched. The captured biometric data is then compared with the reference biometric data on the card. If a match is found, the access is granted, otherwise the access is denied. The administrator needs to carefully encode the User ID, PIN Code and biometric data at the enrolment time.

This authentication mode doesn't use the internal database of the terminal as a source of reference.

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

NOTE: This section is not applicable for SIGMA Lite and Morpho*Wave*® SP Series.

User's data required in the terminal

This authentication mode doesn't use the internal database of the Access and Time Biometric Terminal as a source of reference. Hence the administrator needs not encode the user information into the terminal database.

User's data required on the user's card

For this mode of authentication to work correctly, the administrator must correctly encode the following information into the user's card. This must be carefully done at enrolment time.

User ID (Identifier)

User PIN

The biometric data of user.

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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Activation key

The administrator must select a ‘card’ type that can accommodate at least “User ID + PIN” or “User ID + Biometric + PIN”. This needs to be done at user enrolment time.

The administrator needs to configure the User Record Reference parameter appropriately such that it indicates using a ‘contactless smartcard’ for authentication. This can be done via Terminal Menu or Webserver. Please refer to “*User Enrolment in Database*” *(Step: 37)*

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 the PIN, for PIN Verification.

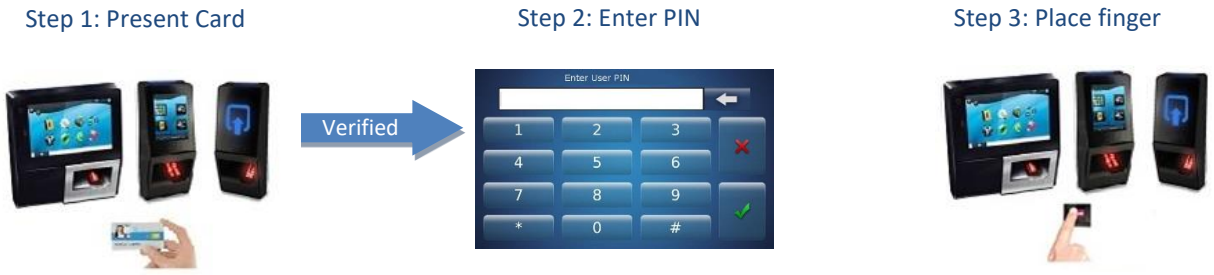


Figure 326: Authentication with user's PIN Code and fingerprints on contactless card

The user is expected to put his finger on the biometric sensor or swipe his hand, or present his face for (biometric) authentication, provided PIN Code is verified, and biometric check is enabled. The terminal compares the biometric data captured by sensor, with the reference biometric data on the user's card.

The authentication process is successful (identity confirmed) if the PIN is verified and the captured biometric data matches with one of the reference biometric data. The authentication process fails (identity not confirmed), if the pin and/or biometric data does not match.

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

The terminal reverts to its initial state, when the authentication process is completed, irrespective of its outcome. This implies that the terminal will now look for another card detection.

BIOPIN verification - BIOPIN stored on card

Description

In this mode the card should contain a Biometric PIN (BIOPIN). The goal of this mode is to substitute fingerprint based authentication by BIOPIN based authentication. This is useful when the fingerprints of the user are not available during enrolment for some reason. The administrator must enroll the user with a User ID and BIOPIN. Authentication process begins when the user presents card at the card reader on the terminal followed by entering BIOPIN. If the entered BIOPIN matches with the BIOPIN stored in the card, access is granted. This authentication mode does not use the database of the terminal.

The administrator can enable this feature in order to support two kind of users in the same access control system, i.e., normal user with fingerprints (biometric check), and special user without fingerprints but with a BIOPIN (BIOPIN checking instead of fingerprint matching).
NOTE: This section is not applicable for SIGMA Lite Series and VisionPass Range terminals.

User's data required in the terminal

The administrator need not encode user information on the terminal database in this mode. Since this mode does not use the internal database of the Access and Time Biometric Terminal, as a reference source.

User's data required on the user's card

The administrator must encode the following on the user's card for this mode to work successfully.

User's identifier (User ID),

User BIOPIN

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

Activation key

The administrator must select a Card Type that can accommodate at least User ID + BIOPIN, at the time of enrolment.

The administrator needs to correctly configure the User Record Reference parameter value to enable authentication using smartcard, from the Terminal Menu or Webserver application. Please refer to "*User Enrolment in Database*" *(Step: 37).*

Following parameter is required to be configured:

Parameter Name	Parameter Value	Description
ucc.allow_biopin_user_rule	0, 1, 2	“0”, to disable BIOPIN check “1”, to enable BIOPIN check “2”, to set PIN check

User Interface

The authentication process starts when the user presents his contactless card instead of placing his fingers on the biometric sensor of the terminal. The card is placed near the antenna of the contactless card reader. 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 requesting the user to place his finger on the biometric sensor.

Figure 327: 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 matches 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.

The terminal reverts to its initial state, when the authentication process is completed, irrespective of its outcome. This implies that the terminal will now look for a card detection.

Biometric check and biometric data in local database

Description

In this mode, only the User ID is read from the card. The biometric data of the user are stored in the internal database, with the same User ID as the one on the user's card.

The terminal compares the biometric data captured by the 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

Since this mode uses the terminal's internal database for reference, the administrator must encode the following user information at the time of enrolment.

Same User ID on the terminal as on the card.

The biometric data of the 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 "*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 ID (user's identifier). All other data is ignored.

The TLV format is described in the Access and Time Biometric Terminals Contactless Card Specification document.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Activation key

The administrator must select a Card Type that can accommodate User ID.

The Trigger event corresponding to 'Card' must be set to ON

The administrator needs to configure the User Record Reference parameter value to Card for authentication using terminal database, by using Terminal Menu or Webserver. Please refer to "*User Enrolment in Database*" *(Step: 37)*.

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 asked to present his finger or face or swipe his hand, for biometric authentication.

Figure 328: Authentication with biometric check, reference in database

The terminal then compares the captured biometric data with the reference biometric data found in the terminal database.

The authentication process is successful (identity confirmed), if the captured biometric data matches with one of the reference data. Authentication fails, if the captured biometric data does not match the corresponding one in the terminal database.

The result of the authentication process is notified to the user by an audio signal, as described in "*Terminal States*" section.

The terminal reverts to its initial state, when the authentication process is completed, irrespective of its outcome. This implies that the terminal will now look for a card detection.

When no users have been enrolled in the database, the authentication process is disabled. Users are not allowed access in this mode. The terminal notifies this invalid state to the user, as described in "*Terminal States*" section.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Authentication with local database: User ID entered from keyboard

Description

In this mode, the User ID is entered using the Access and Time Biometric 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 329: 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 requested to place his finger or present his face or swipe his hand on the biometric sensor, for biometric authentication.

The terminal then compares the captured biometric data with the reference biometric data found in the terminal database. The authentication process is successful (identity confirmed) if the captured biometric data matches with one of the references data. If no match is found, the authentication process fails (identity not confirmed).

NOTE: This section is not applicable for SIGMA Lite and Morpho*Wave*® SP Series.

Activation key

The administrator needs to enable 'Keypad' as the Trigger event.

The administrator needs to configure the User Record Reference parameter to 'Card for authentication using terminal database', by using Terminal Menu or Webserver. Please refer to "*User Enrolment in Database*" *(Step: 37)*.

Authentication with local database: ID input from Wiegand or Clock & Data

Description

This mode requires an external card reader that will send the User ID to authenticate to the Access and Time Biometric 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 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 31	Use this parameter to enable biometric, contactless, keypad, external port trigger and QR code 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:** Set Trigger Event through "*Configure Trigger Events*" through Terminal. QR code feature is not supported for SIGMA Range terminals and the key value can be 1 to 15.
wiegand.external_port_input_type	0 or 1	Storing current external port input type as: • Set '0' for Wiegand format input (default)

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Parameter name	Value	Description
		• Set '1' for Clock & Data format input
wiegand.external_port_output_status	0, 1 or 2	To enable/disable Wiegand output functionality. • Set '0' to never send data using Wiegand Port • Set '1' to always send data using Wiegand Port (default) • Set '2' 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 Parameter Settings*" in this guide.
- You can also refer **Parameters Guide** for complete list of Wiegand parameters.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Wiegand Frame Configuration

When set up to communicate with Wiegand protocol, the Access and Time Biometric 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 in the event of a verification fail or pass.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Site-code Propagation

Site code propagation allows the usage of site code received from Wiegand input frame and apply the same to the output Wiegand frame. Configuration key "wiegand.site_code_propagation" is used to enable site code propagation

0 - Disable site code propagation (Default)

1 - Enable site code propagation

Site code is stored each time, authentication happens. It is extracted from a Wiegand input frame, or Prox card or a HID Card number contained in an HID contactless card or an HID Mobile Credential. This site code will be used as output site code in the Wiegand frame corresponding to the **"wiegand.event_verify_fail"** and **"wiegand.event_verify_pass"** formats. For more details, please refer to Site-code Propagation section on **MA SIGMA - Application note - Wiegand formats**.

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 calculated on 25 bit from 13 to 24 bit

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

No biometric check, no User ID check

Description

This authentication mode is a version of the "*Biometric check, biometric data on user's card*" authentication mode, such that the biometric check is disabled.

When the administrator enables this mode, the terminal searches only for the User ID on the user's card. No other check is performed, i.e., the user's identifier is not searched in the terminal database and no biometric checks are performed.

This mode of authentication comes handy when there is no need (for a short term visitor) or it is impossible (physically or legally) to perform biometric authentication. These kind of cards can be encoded (with a unique User ID) without user's presence and the same card can be used for different visitors.

The internal database of the terminal is not used. The Access and Time Biometric Terminal acts as a simple contactless card reader that only looks for the User ID.

The access is granted provided the user's card is encrypted with the authentication keys stored in the terminal and the terminal is able to read the User ID. Otherwise, the card is ignored and the access is denied.

User's data required in the terminal

The administrator need not encode any data in the terminal, while in this authentication mode. This is because the terminal's database is not used as a reference for user authentication.

User's data required on the user's card

In order to be compatible with this mode of authentication, the administrator must correctly encode the User ID into the user's card. 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 **Contactless Card Specification** document.

The Access and Time Biometric Terminal doesn't perform any check on the value of the user's identifier.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Activation key

The administrator needs to select the Card Type, such that it can accommodate User ID. This must be ensured at the time of user enrolment.

The administrator needs to correctly configure the **User Record Reference** parameter by using Terminal Menu or Webserver. The value should be such that authentication mode is chosen via 'card'. Please refer to "*User Enrolment in Database*" *(Step: 37)*.

If no PIN check and no biometric check are required for a given user, it is best to provide him with a Visitor card. For more details, please refer to "*Encode Visitor Card*"

User Interface

The authentication process starts when the user presents his contactless card to terminal. As shown below:

To provide his identity, the user presents his personal identity card that contains the User ID. This action starts the authentication process.

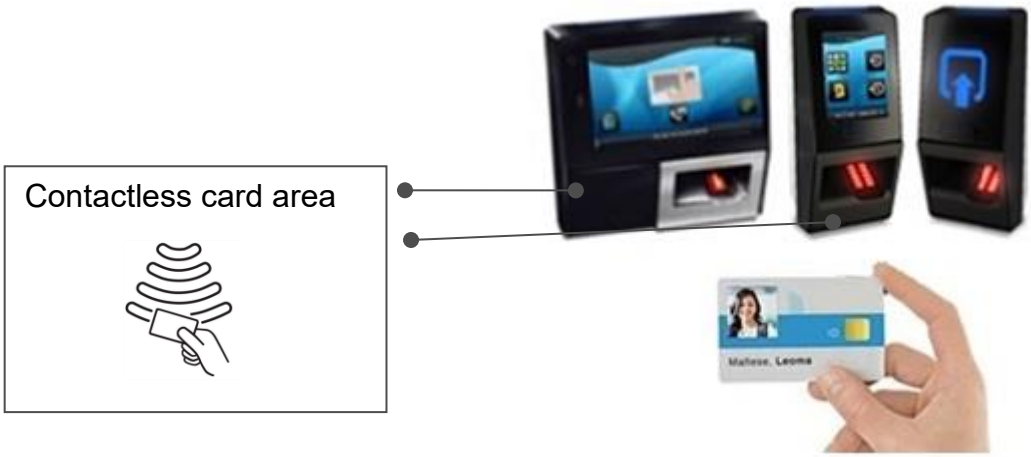


Figure 330: Authentication without biometric check and with User ID check in card

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.

Upon completion of the authentication process (irrespective of the outcome), the terminal automatically reverts to the initial state, wherein it waits for a card detection.

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. Only if the User ID read from the card exists in the terminal database, user is allowed access.

User's data required in the terminal

The administrator must ensure that the following user data is loaded into the terminal database, at the time of user enrolment.

the same identifier as the one on the user's card.

If there is no record in the terminal database that corresponds to the User ID, access will be denied to the user in question.

Activation key

- The administrator needs to select Card Type at the time of User Enrolment, such that it can accommodate User ID.

The administrator needs to correctly configure the **User Record Reference** parameter by using Terminal Menu or Webserver. The value should be such that authentication mode is chosen via 'terminal database'.

- Following parameter is required to be configured:

Parameter Name	Parameter Value	Description
ucc.user_record _reference	0 or 1	If "0", then reference source is based on trigger event *(Default)* If "1", reference is terminal for all trigger sources.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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 331: Authentication without biometric control, and with the user login

The User ID is read on the user's card and searched in the local database.

The authentication process succeeds if the User ID 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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Authentication process specified by User's card

Description

When the administrator enables this mode, the conditions for allowing access are specified by a dedicated data on the user's card. This implies that different authentication checks can be performed on the same terminal for different users, based on a 'specific' data present on the user's card. Following are the possible authentication checks

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 ID 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 in case of a short term visitor, or impossible from physical or legal aspects. Such cards can be encoded without user's presence and the same card can be used for different visitors. The internal database of the terminal is not utilized in such case.

NOTE: PIN check is not applicable to SIGMA Lite and Morpho*Wave*® SP Series.

User's data required in the terminal

Since this authentication mode does not use the internal database of the Access and Time Biometric Terminal, the administrator need not save any user specific data to the terminal database.

User's data required on the user's card

The administrator needs to choose a Card Type that can accommodate at least the User ID (user's identifier) as well as the data that determines the 'type' of authentication method to be used. For example, if the administrator sets the PIN + biometric check as ON, the User biometric data as well PIN must be encoded onto the user's card.

If the administrator selects the biometric check as ON, it must be ensured that the biometric data of the user, must be encoded onto the user's card.

If PIN check is required, the user's PIN must be on user's card.

All other data is ignored.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

The required data must be stored according to TLV format. The user's card format (and the TLV format) is described in the **Contactless Card Specification** document.

Activation key

The administrator can select the Card Type to be 'User ID only' or 'User ID + PIN' or 'User ID or Template' or 'User ID + PIN + Template', based on the requirements. This is decided prior to user enrolment.

The administrator can set **User Record Reference** parameter as trigger event by using Terminal Menu or Webserver. Please refer to "*User Enrolment in Database*" *(Step: 37)*.

If PIN code check and biometric check are not required for the user, then providing a Visitor Card, is the best option. For more details, please refer to "*Encode Visitor Card*"

User Interface

Start

The authentication process starts when the user presents his contactless card at card reader of the terminal.

The terminal looks for the data that describes as to which check is mandatory or disabled, by scanning the user's card. If this data is found, the terminal executes the required process corresponding to the authentication method indicated by this data, which could be with/ without PIN code check, and with/without biometric data check

Figure 332: 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, the terminal automatically loops back and waits for another user's card presentation, irrespective of the outcome of the authentication process (pass/fail).

PIN check disabled, Biometric check mandatory

When the administrator enables this mode, the terminal requires the user to present finger or face to the biometric sensor. It executes a comparison of the biometric data captured by 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

If the administrator enables this mode, 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 present finger or face to 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

If the administrator enables this mode, 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 asked to present finger or face to the biometric sensor. Then the biometric data captured by the sensor and the reference biometric data read on user's card are compared to see if a match exists or not.

The process is identical to the one described in "*PIN verification - PIN stored on card*" section.

PIN check mandatory, Biometric check disabled

If the administrator enables this mode, then on successful 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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Allowed format for User's identifier

TLV structured data

The User ID (user's identifier) is stored in ASCII characters within a TLV structure.

This is the default configuration of the Access and Time Biometric 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 for SIGMA Range) (0x774176 – Default for Morpho*Wave*® Compact, Morpho*Wave*® XP2 and Morpho*Wave*® SP) (0x464143 – Default for VisionPass Range terminals)	Sets DESFire® application ID to read data on TLV card.
sc_tlv_desfire.fid	0 to 31 (0x00 to 0x1F) (0x00 - Default)	Sets DESFire® file ID to read data on TLV card.
sc_tlv_iclass.book_number	0 - 16777215 (0 - Default)	Sets iCLASS® card book number for 16APP 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	19 - 255 (19 - Default)	Sets iCLASS® card Page offset for 2APP for TLV card.
sc_tlv_mifare.key_policy	1, 2 or 3 (1 - Default)	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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Parameter Name	Parameter Value	Description
		Set “3” - Try to read card with Key B
sc_tlv_mifare.num_block	0 - 216 (31 – Default for except VisionPass Range terminals) (84 – Default for VisionPass Range terminals)	Sets number of blocks to read MIFARE® 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 administrator can refer to the document: **Contactless Card Specification.** This is a dedicated document that describes the logical structure of the contactless smartcard.

Binary Data

Description

The Access and Time Biometric Terminal is able to use a binary value to read on specific location on user's card, as user's identifier.

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 Access and Time Biometric 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 Access and Time Biometric Terminal is able to proceed with user's cards written by other systems.

Card type compatibility

This feature can only be used with MIFARE® contactless card.

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_binary_read.data_type_format = 1	Binary format
sc_tlv_mifare.start_block	[4 - 215] First block to read on card
sc_binary_read.data_length_num_bytes	User ID length in bytes and additional bits limited to 8 bytes (i.e. 8).
sc_binary_read.data_offset_num_bytes	Offset (from the start of the block) of 1st byte and 1st bit of data: 15 bytes maximum (i.e. 15)
sc_binary_read.data_type_direction	Byte read acquisition method:

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

	1 (binary data, MSB first) (default value) 0 (binary data, LSB first)

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_format = 1	Binary format
sc_binary_read.data_type_direction = 0.1	Binary MSB format
sc_binary_read.data_length_num_bytes = 4~~.0~~	Size = 4 bytes, no additional bit
sc_binary_read.data_offset_num_bytes = 0~~.0~~	First byte of the block
sc_tlv_mifare.start_block = 1	First block of the card

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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.

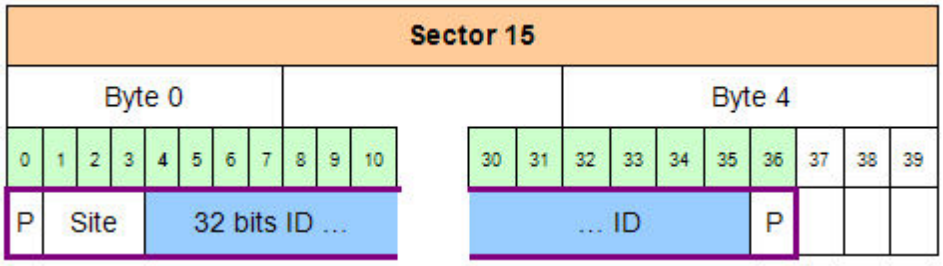


Figure 333: Using a Wiegand frame as User ID

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_format = 1	Binary format
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 automatically add the start and stop bits to the Wiegand output frame.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 13 : **Fingerscan accessory**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Functionality

VisionPass SP can be fitted with Fingerscan accessory. It allows user identification or authentication by fingerprint. The Fingerscan is integrating a CBM-E4 Idemia sensor. The connection between the Fingerscan and the VisionPass SP is secured.

When Fingerscan is present the VisionPass SP user data base is extended to store fingerprint templates too. By consequence it is possible for each user to store facial and/or fingerprint biometric template.

Identification

The fingerprint acquisition function is available when VisionPass SP biometric trigger is activated. The Fingerscan is turned on, ready to finger acquisition when the VisionPass SP is wake up. The Fingerscan turns off when the VisionPass SP switches in standby mode.

When biometric trigger is activated, if the face of user, front of the terminal, is not recognized, the VisionPass SP waits a configurable timeout before to display the access denied result, providing to user the possibility to present his finger. It is not possible to activate only one biometric identification.

The intentional mode doesn't affect the Fingerscan, user doesn't need to press the button before to put his finger.

Authentication

When biometric control is mandatory in the user authentication workflow, if only fingerprint template is available, it will replace the facial recognition. If both biometric templates are available, a facial recognition will be executed.

Dual biometric control

It is possible to require a dual biometric check, fingerprint and face. It can be activated for all users, please refer to the Access and Time Biometric Terminals Parameters Guide, or for specific users, with user rules from card code or terminal database.

When dual biometric control is executed in an identification workflow, the biometric not already verified will be requested after identification: if user presents his face first, the fingerprint sensor will turn on to request a fingerprint acquisition, if user presents his finger first the facial MMI acquisition will be played.

When dual biometric control is executed in an authentication workflow, facial recognition will be first requested and fingerprint secondly.

When dual biometric check is requested, the access control will be denied if any of both biometric is failed, due to matching failure or missing data.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Fingerscan parameters

The Fingerscan matching threshold is managed separately from the face one. Please refer to the Access and Time Biometric Terminals Parameters Guide.

The Fingerscan fake finger detection level is managed separately from the fake face detection level. Please refer to the Access and Time Biometric Terminals Parameters Guide.

It is possible to configure a retry in case of fingerprint matching failure. Please refer to the Access and Time Biometric Terminals Parameters Guide.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 14 : **Multifactor Access Control Mode**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Multi-factor Mode

Description

The Access and Time Biometric 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 detection of finger or face, or for the presentation of a user's card. It will execute the following:

the identification process if the user present his finger or face to the biometric sensor first,

Or the authentication process if the user shows his card first.

Figure 334: Multi-factor mode (identification or authentication)

In case the User database is empty, the identification mode is automatically disabled, but the authentication mode is still available (by showing the card).

User's data required in the terminal

The same data as that is required by the "*Identification Mode Description*" and "*Authentication Process*", needs to be configured in the terminal database. Please refer to the corresponding sections.

User's data required on the user's card

The items required on the user's card depend on the activated authentication mode(s). For example, the User's Card needs to have the User ID + User Pin, when PIN verification is mandatory. Please refer to "*Authentication Process*" section for more details.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Activation keys

The administrator needs to enable the Trigger event through Biometric, Contactless Card, Keypad and External Database.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 15 : **Security Administration**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Tamper Setting

The Access and Time Biometric Terminal can detect two intrusion attempt types:

Someone tries to steal the complete terminal,

Someone tries to open the terminal
Besides Webserver, these configurations are possible via **MorphoBioToolBox** and distant commands also. For more information please refer to "*Anti-Tamper Switch for Terminal Security*" section.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Biometric technology Settings

The Access and Time Biometric Terminal provides two parameters that can be configured separately to balance security with user experience and select the most appropriate configuration for the targeted use case:

- Biometric threshold, to set the False Acceptance Rate

Parameter 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.

- Anti-spoofing feature with four configuration levels: disabled, low, medium, high. Depending on the model, the Fake Biometric Detection feature is based on different techniques. Increasing the level of fake detection results in both: more intrusion attempts are detected; and more legitimate access attempts may be rejected as erroneously considered suspicious.

  Note: IDEMIA recommends integrators to leverage fake warnings in the solution to implement appropriate countermeasures after a fake biometric sample is detected, for instance:

  - blacklist the end-user
  - take a picture of the user
  - send a silent alarm message to security team

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Recommendations for a Secure Installation

For full details about security, please refer to the IDEMIA dedicated document.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 16 : **Wiegand Configurations**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Wiegand Parameters Settings

Access and Time Biometric 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 Access and Time Biometric Terminals and are designated as a Standard type in the table below. They contain an ID of 32 bits or less. All Access and Time Biometric 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. Besides Webserver, these configurations are possible via distant commands also.

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
Auto Detect	Custom	As per the user field (site-code length) defined in the custom slot.	As per the Id length defined in the custom slot.	Configurable (if parameter ‘sc.support_l1_cards’ is configured to value ‘2’)

Table 3 : 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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Wiegand Parameters Configuration through Webserver

Access Path

Webserver > Terminal Settings > Wiegand

Screens & Steps

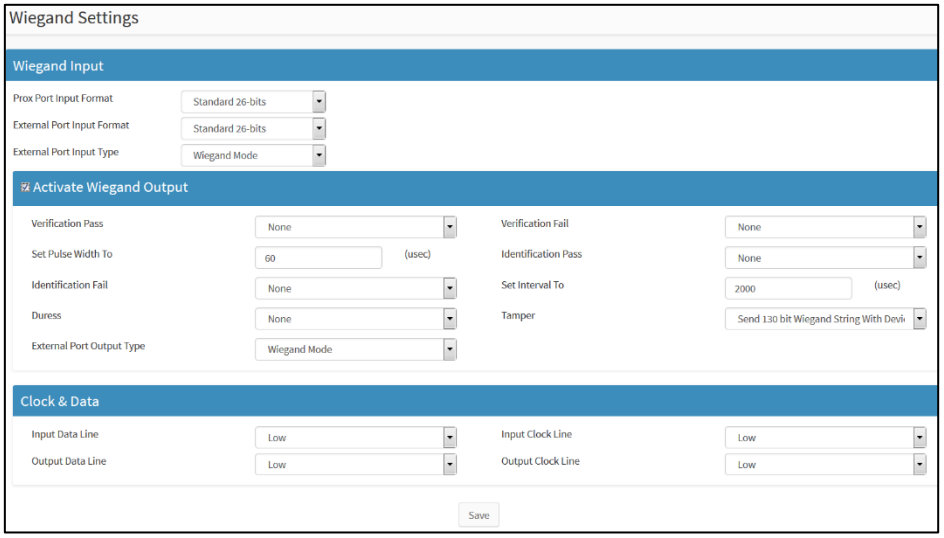


Figure 335: Wiegand Settings through Webserver

1. Configure below Wiegand Input parameters, for action triggered through Wiegand to terminal:
    a. Select **Prox Port Input Format** from available format list, as mentioned under "*Wiegand Format and Associated Values*"
    b. Select **External Port Input 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.

Auto-Detect can be configured for **Prox Port input format/HID Card Number Format** and **External Port Input Format**. Please refer to **MA SIGMA - Application note - Wiegand formats** for more information. Kindly follow the notes for Auto-Detect.

1. It is mandatory to configure at least one Wiegand custom slot.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

2. If there are multiple formats defined in the custom slots having same length, then first matching slot will be considered.

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 bits Wiegand String with Device 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

Wiegand Propagation

The last received input Wiegand frame format can be applied on the output Wiegand format, as defined in "*Complete control configuration*". This can be activated by applying the value, "**Wiegand Last Format Input**" to "**Wiegand event Verification fail**" or "**Wiegand event Verification pass**" configuration. Please refer to Wiegand

Propagation section in **MA SIGMA - Application note - Wiegand formats,** for more information. Kindly follow the notes mentioned below :

1. It is mandatory to define custom format slot 0 to enable "***Wiegand Last Format Input***".
2. If trigger source for authentication is keyboard or distant command, the Wiegand last format output will considered as per custom slot_0.

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**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 17 : **Threat Level Configurations**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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.

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

Besides Webserver, these configurations are possible via **MorphoBioToolBox** and distant commands also.

Threat Level Configuration through Webserver

Access Path

Webserver > Terminal Settings > Threat Level

Screens & Steps

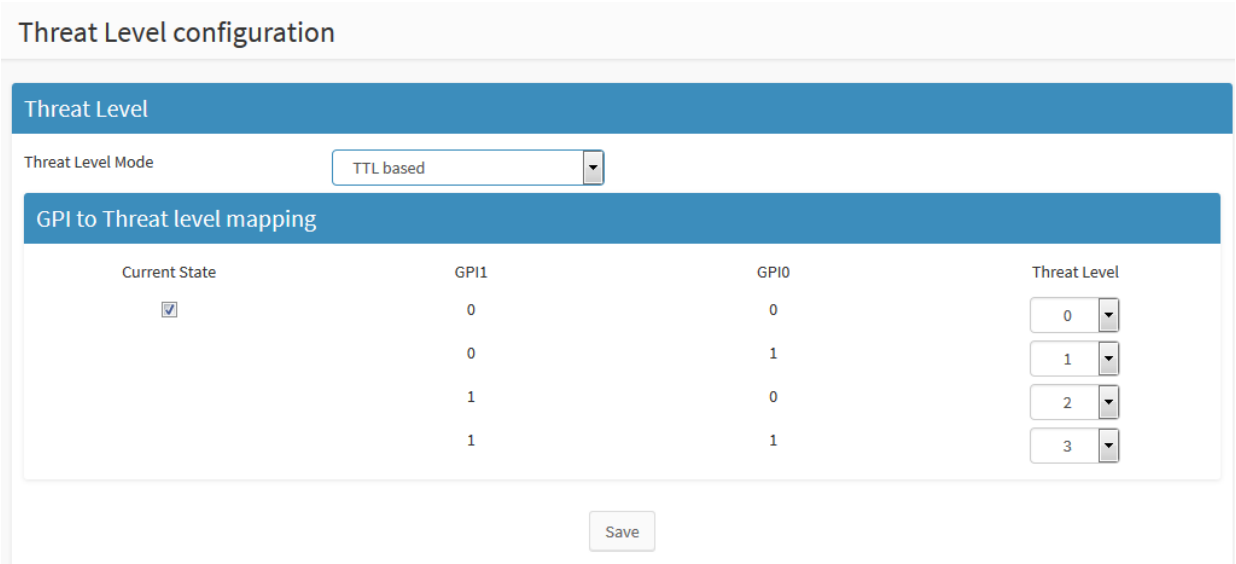


Figure 336: Configuring TTL Based Threat Level

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.
2. 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
3. Click on **Save**

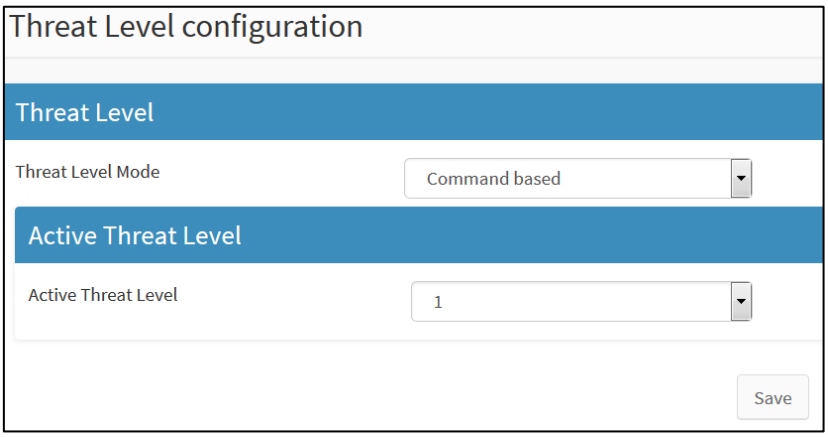


Figure 337: Configuring Command Based Threat Level

4. 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.
5. Command based threat level can also be modified using threat level parameters under Webserver > Complete Configuration and also distant commands.
6. Select **Active Threat Level** from dropdown menu
7. Click on Save

Section 18 : **Time and Attendance Configurations**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

T&A Synoptic

Access and Time Biometric 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.

Along with biometric presentation, user is also required to select applicable function key (F Key). Suppose user is entering office in the morning, then 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. This Time and Attendance mode becomes a crucial feature for human resource management.

T&A Modes and Function Keys	SIGMA and SIGMA Extreme Series, MorphoWave ® Compact, MorphoWave ® XP2	SIGMA Lite Series, MorphoWave ® SP	SIGMA Lite+ Series	VisionPass Series
Two Function Key Mode	✗	✗	✓	✗
Normal Mode (4 Function Keys: IN, OUT, IN DUTY(LUNCH IN), OUT DUTY(LUNCH OUT)	✓	✗	✗	✓
Extended Mode (16 Function keys)	✓	✗	✗	✓
T&A Mandatory Mode Selection	✓	✗	✓	✗
T&A per User	✗	✗	✗	✓

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Parameter Configuration

Time and Attendance Mode Activation	
time_and_attendance.tna_mode	0, the T&A mode is disabled. 1, the T&A mode is enabled. When T&A mode is enabled, 2 F-keys for SIGMA Lite+ Series and 4/16 F-keys for all Access and Time Biometric Terminals are displayed. The F-keys number depends on T&A Extended mode.

Time and Attendance Mandatory/Normal Mode Selection	
time_and_attendance.tna_mandatory_mode	0, the mandatory mode is disabled. 1, the mandatory mode is enabled.

Besides Webserver, these configurations are possible via **MorphoBioToolBox** and distant commands also.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

T&A Mode in SIGMA Lite+ Series

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 338: Two Function Key Mode for SIGMA Lite

In the above sample screen, the IN function is associated to" " key, OUT function is associated to " " key. A user can select any of the Function Keys to input required T&A action

T&A Normal Mode for all other Access and Time Biometric Terminals

In normal mode, there are 4 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 339: Time and Attendance Screen in Normal Mode

In the above sample screen, the IN function is associated to F1 key, OUT function is associated to F2 key, IN Duty is to F3 and OUT Duty is to F4. A user can select any of the Function Key to input required T&A action. Instead of texts, icons can be selected to be displayed to the user.

Parameter Configuration

Time and Attendance Text/Icon Mode Selection	
time_and_attendance.message_text_mode	Parameter to choose whether 4 actions mode uses texts or icons. In text mode, text displayed on LCD can be customized. In icon mode, the pre-set icons/images are displayed for function keys 0 - 4 actions in texts (0 - Default) 1 - 4 actions in icons

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

T&A Extended Mode for all other Access and Time biometric Terminals

In extended mode, there are 16 function keys that can be configured and displayed to the user. When T&A data is required from the user, the terminal displays the Time and Attendance screen below:

Figure 340: Time and Attendance Screen in Extended Mode 1x16

Figure 341: Time and Attendance Screen in Extended Mode 2x8

In the above sample screen,

- IN1 function is associated to F1 key,
- OUT1 function is associated to F2 key,
- IN Duty1 is to associated to F3,
- OUT Duty1 is to associated to F4,
- In case of 2x8, click on “ ” key to go to the second screen.
- ... Up to 16 function keys.

A user can select any of the Function Key to input required T&A action.

The selected function is written in the access request record, stored in the log file, and included in the "User Identifier" message sent to a distant system.

After selection, the Access and Time Biometric Terminal switches in biometric mode (identification or authentication).

The selected function is written in the log file and sent to the host. For extended time attendance, the code of the pressed key is logged (i.e. 0x31 for key 1, 0x32 for key 2 …).

If the user has selected the wrong operation (IN/OUT...), back button “ ” can be used at any moment during wait for a biometric capture or a card, to abort the verification. In this case, nothing is logged or sent to the controller.

After 20 seconds of inactivity on identification mode (no finger or face detected by the sensor), the terminal switches back to the selection screen. In this case the operation result is logged and/or sent to the controller (result = timeout).

Parameter Configuration

Time and Attendance Extended Mode Selection	
time_and_attendance.tna_extended_mode	0, the extended mode is disabled. Only 4 F-keys are displayed. 1, the extended mode is enabled. 1 screen (1x16 F-keys) or 2 screens (2x8 F-keys) are displayed

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 possible scenarios when T&A is in mandatory mode and user initiates an access request.

- **T&A before User Control by selecting F Key:** 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 selecting F Key:** 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 selecting F Key:** In this scenario, user will place his finger on the sensor or present his card. Terminal will first authenticate the user.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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 which states that user has input the F key.

Results

Once T&A parameters are configured, T&A icon is displayed on the home screen of the Access and Time Biometric 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.

NOTE: The optional scenario is not available for VisionPass Range terminals. The VisionPass Range terminals requests a T&A action systematically after the biometric user control (never before). The T&A action is requested if T&A mode is enabled or user's T&A mode is enabled.

T&A request on VisionPass Range terminals

This session resumes the T&A request on VisionPass Range terminals according to T&A configuration.

	VisionPass					
	time_and_attendance.tna_mode = 0		time_and_attendance.tna_mode = 1			
	time_and_attendance.mandatory_mode = 1		time_and_attendance.mandatory_mode = 0		time_and_attendance.mandatory_mode = 1	
	ucc.per_user_rules = 0	ucc.per_user_rules = 1	ucc.per_user_rules = 0	ucc.per_user_rules = 1	ucc.per_user_rules = 0	ucc.per_user_rules = 1
user T&A control (tna_control) = 0 or smartcard rules	No T&A request	No T&A request	NA	NA	T&A request	T&A request
user T&A control (tna_control) = 1	No T&A request	T&A request	NA	NA	T&A request	T&A request

	Imposed by terminal configuration
	Imposed by user rule

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

T&A configuration through Webserver

Access Path

Webserver > Terminal Settings > Time and Attendance

Screens & Steps

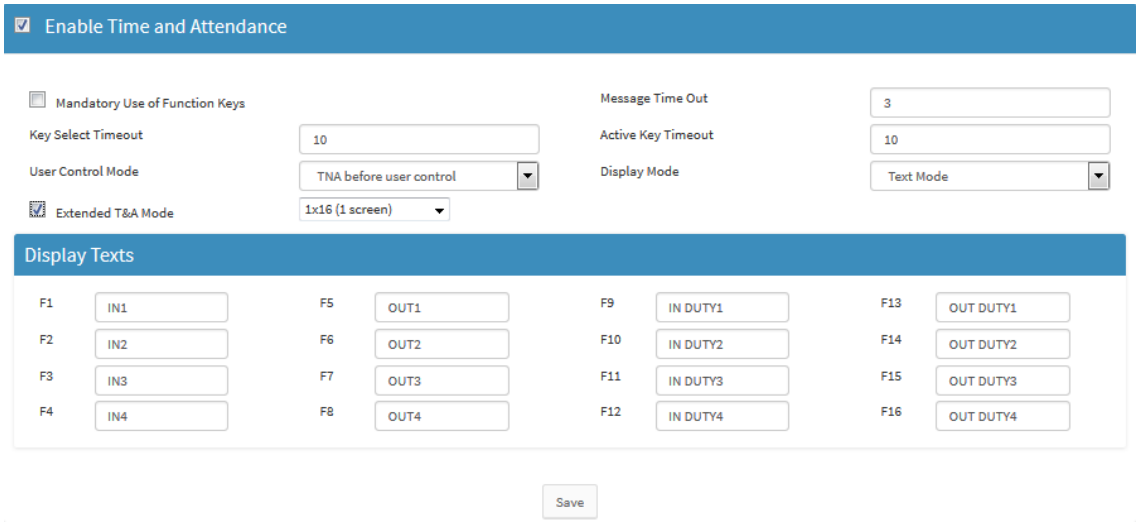


Figure 342: Normal Time and Attendance mode

1. Click on **Enable Time and Attendance**, for enabling this mode

Click on **Mandatory Use of Function Keys**. On enabling this, terminal will pop up T&A screen every time after user is identified or authentified. If mandatory is not selected, then user can select T&A option before

Message Timeout: an administrator can define the duration for which access result is displayed on the LCD screen of the terminal

Key Select Timeout: an administrator can define a 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 1 to 60 seconds.

Active Key Timeout: within this duration the key should be pressed, if operation failed first time. Valid range of timeout is 1 to 60 seconds.

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).

Select **Displayed Mode** as “Text mode” or “Icon Mode”. By default text is selected. If an administrator select “Icon mode”, than instead of F key with text, icons are displayed, refer “*Time and Attendance UI in Normal mode with Icon*”.

NOTE: Icon mode display is not applicable for T&A extended mode. Text mode is not available for SIGMA Lite+ Series.

If an administrator requires T&A in Normal mode, then do not select Extended T&A mode check box. In normal mode, only 2/4 functional keys are required to be configured

Enter **Display Text**. In this section an administrator can customize the text associated with the Functional Keys. The text length should be 1 to 20 characters only. By default below text is displayed, which is editable (applicable to SIGMA Wide and SIGMA Extreme Series):

a. F1 = IN
b. F2 = OUT
c. F3 = IN DUTY
d. F4 = OUT DUTY

Click on **Extended T&A Mode** checkbox. Under extended mode 16 functional keys can be configured

Enter **Display Text**. In this section an administrator can customize the text associated with the Functional Keys. The text length should be 1 to 20 characters only.

Click on **Save** once required configurations done.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

T&A - Mandatory Mode Work Flow Diagram

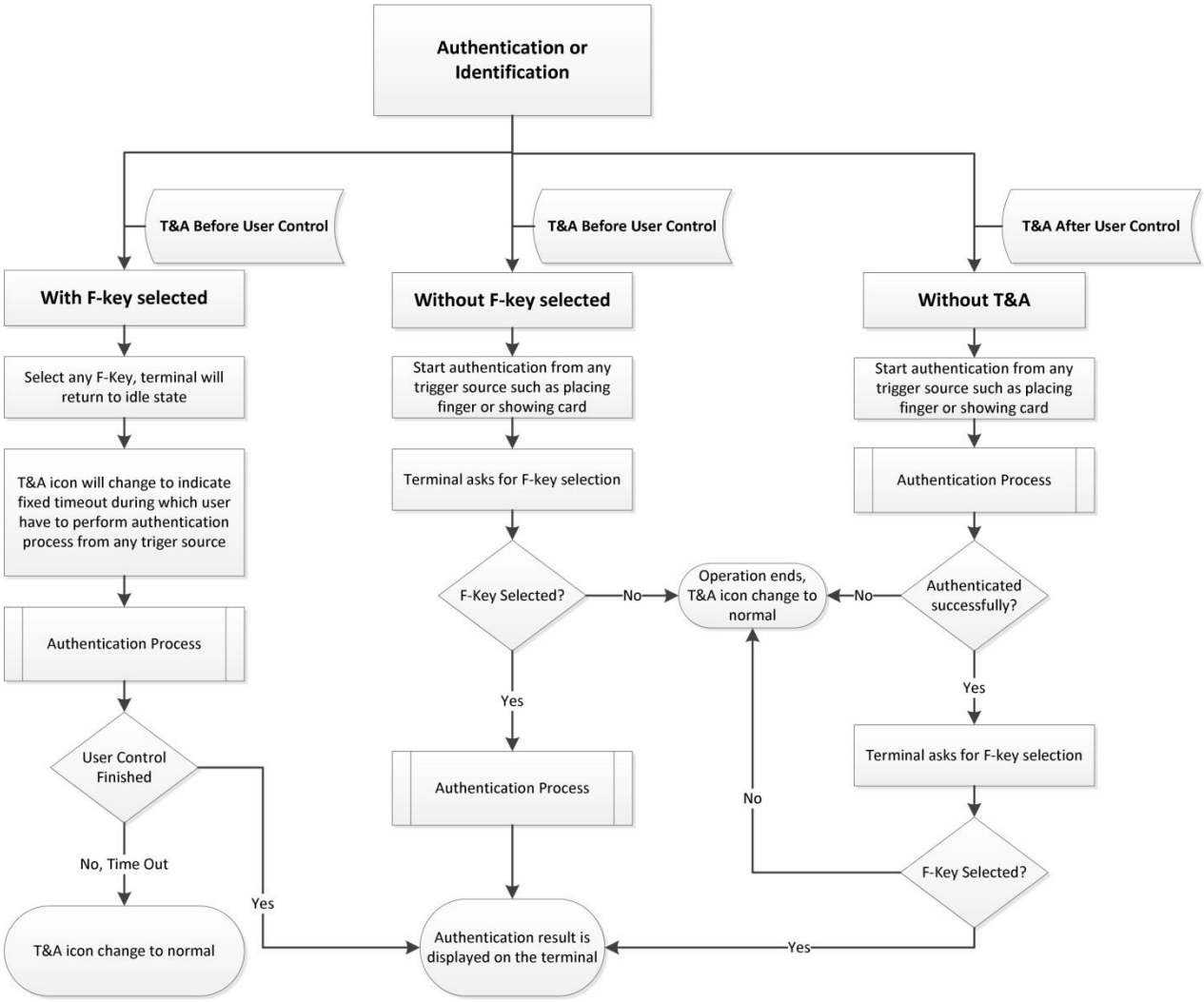


Figure 343: Time and Attendance in Mandatory Mode Workflow Diagram

T&A - Non Mandatory Mode Work Flow Diagram

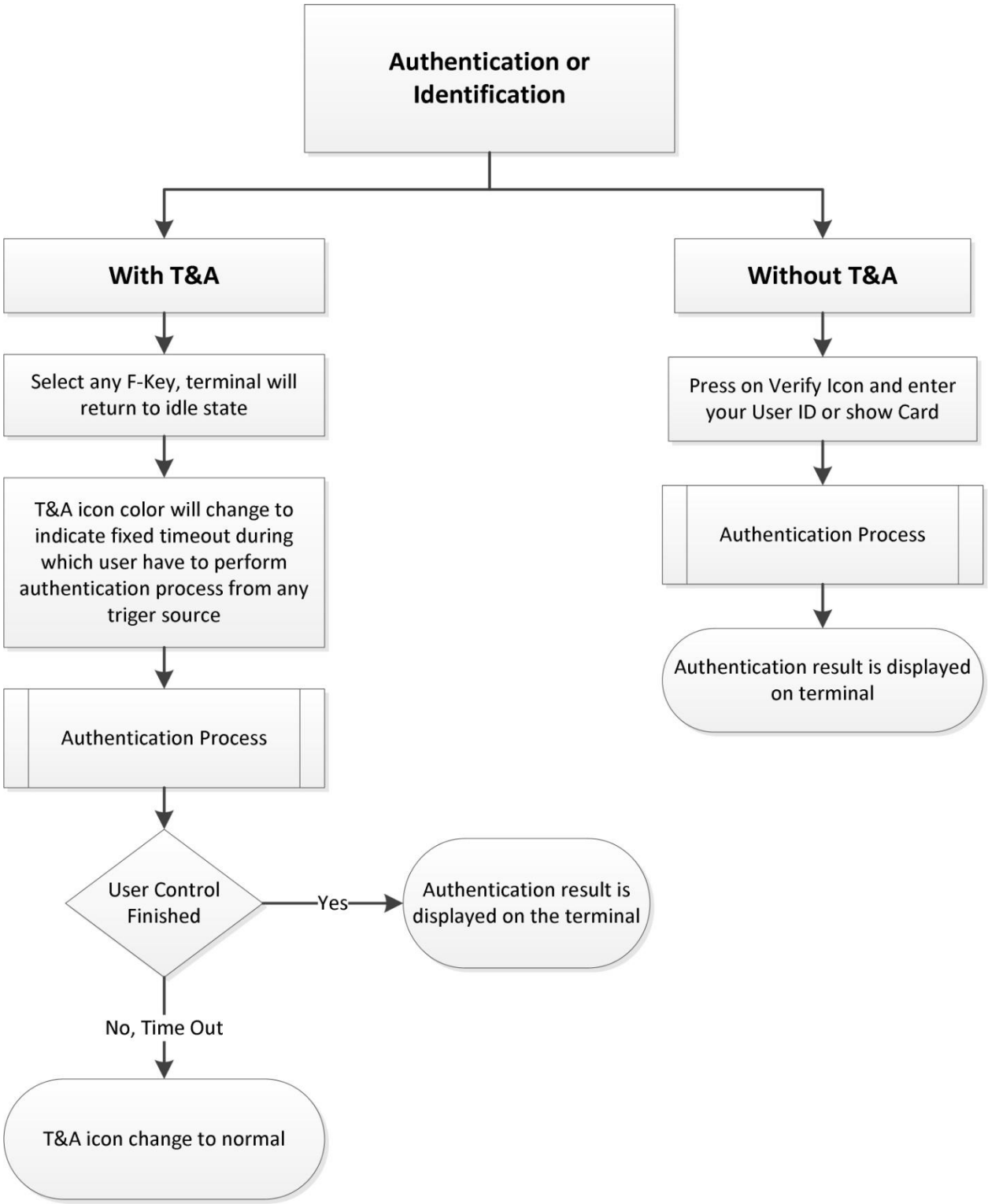


Figure 344: Time and Attendance in Non-Mandatory Mode Workflow Diagram

Section 19 : **Schedules configuration**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Schedules Configuration

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 the authentication is successfully.

Access schedule enables to define time slots for entire week. A time slot is defined by selecting one or several successive quarter hours (For 1 day, the maximal number of quarter-hour is 96. It means a full day).

64 access schedules are manage by terminal

- 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. 62 is defined as “User Access Schedule”, if this schedule number is selected for a user then user specific schedule is refered.
- Schedule no. 59 to Schedule no. 62 are reserved for internal use and cannot be assigned to any user.
- Schedule no. 1 to no. 58 are configurable

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 8:00 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 8:00 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 SIGMA Range terminals. Besides Webserver, these configurations are possible via distant commands also.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Add/Edit/Delete an Access Schedule through Webserver

Access Path

Webserver > Schedules > Access Schedules

Screens & Steps

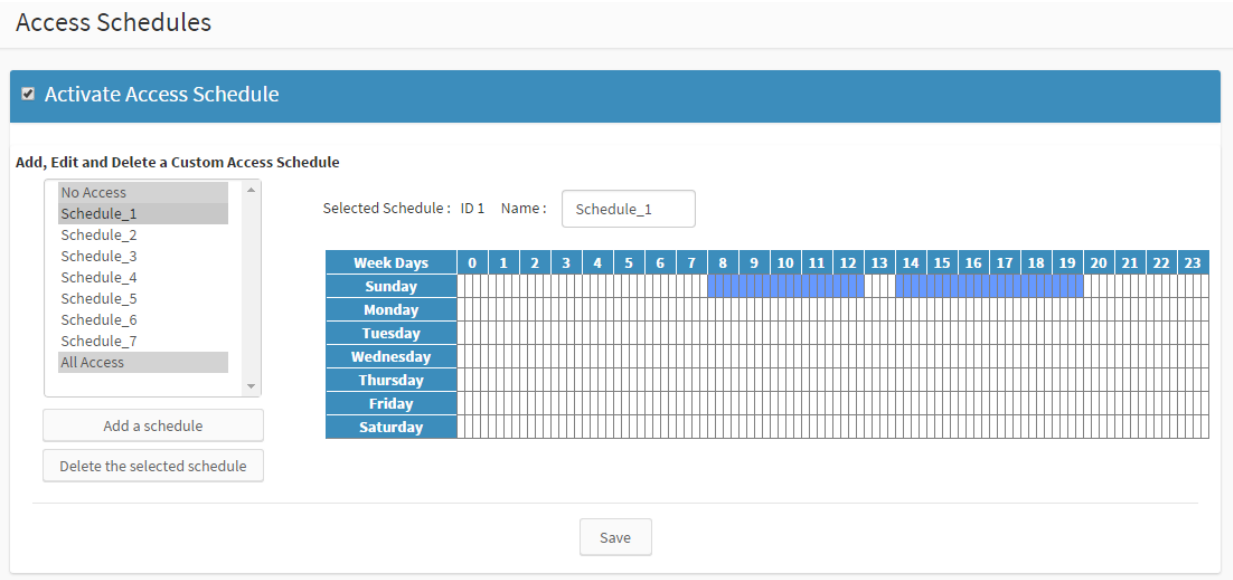


Figure 345: Adding Access Schedule

1. The list of default access schedules is displayed as “No Access” and “All Access”. Default access schedules are available by default 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. Select the appropriate block according to start & stop time for each day, by single click on individual block or by selecting multiple blocks inside the table area. The selected area will be seen in different color and it will define the time slot during which the access will be granted to user.
5. Repeat above step 2, step 3 and step 4 to add more schedules.
6. Click on **Save** to save all previously defined access schedules in the terminal.
7. An administrator can edit Access Schedule Name and Time Slots. To edit the access schedule, select an access schedule from the list and follow the above steps 3 to 6.
8. The Administrator can delete one or several access schedules.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

9. To delete an access schedule, select an access schedule from the list and click on the **Delete** the Selected Schedule. Repeat these operations for each access schedule to delete. Finally click on Save to save all deleted access schedules in the terminal.

NOTE: The default access schedules cannot be modified.

Add/Edit/Delete an Access Schedule through distant commands

Refer to Distant Commands Guide document

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 scheduled access time. If user tries to access at another time, then Access and Time Biometric Terminal will deny access to the user.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Define User Access Schedule

User Access Schedule is similar to Access Schedule but these are defined on user level and are stored in the user records. Terminal refer to user access schedule when the schedule number is set to 62. If the user access schedule is not defined in user database, by default “All Access” is given to user.

User Access schedule defined as time slots for entire week. A time slot is defined by selecting one or several successive quarter hours (For 1 day, the maximal number of quarter-hour is 96. It means a full day).

User access schedule can be created while user enrollment via. Webserver or distant command. If user access schedule is selected while user enrollment via. GUI then by default “All Access” is set as user access schedule for that user.

Add a User Access Schedule through Webserver while user enrollment

Screens & Steps

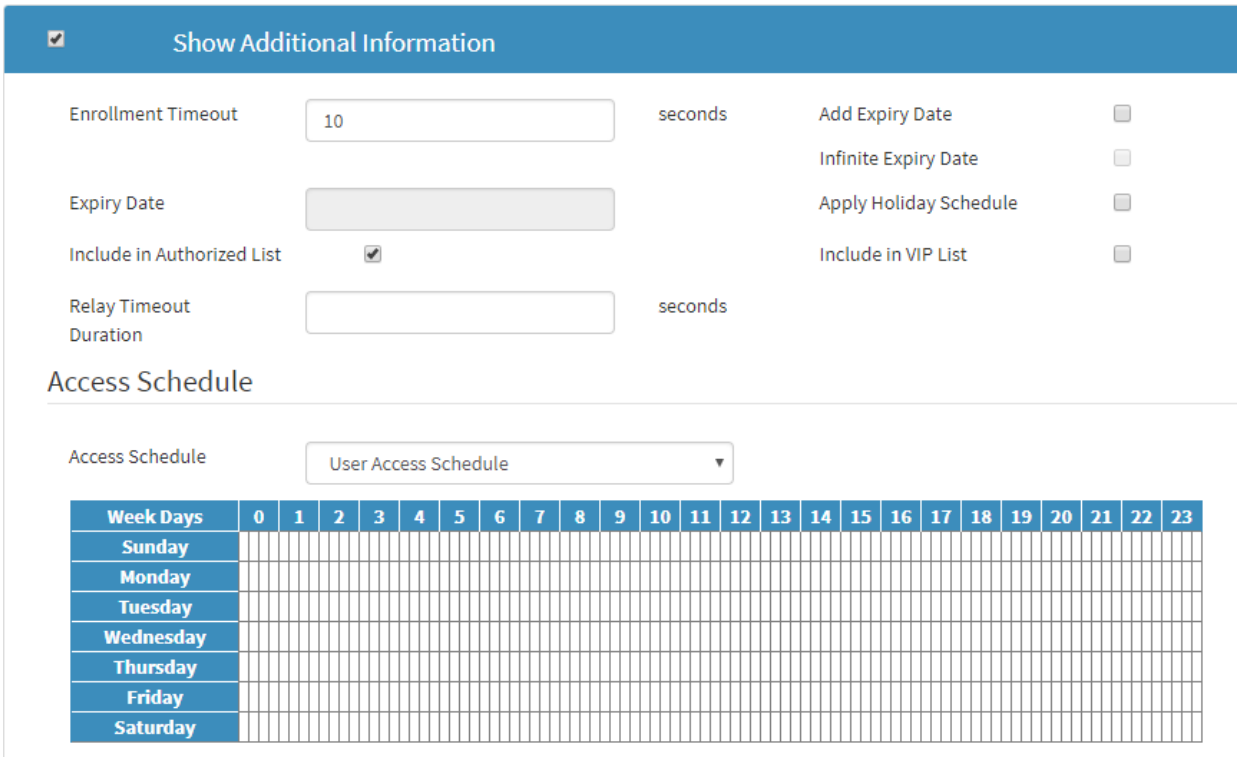


Figure 346: User Access Schedule through Web Server

1. Enroll a new user through Web Server and while enrollment select “Show Additional Information”.
2. Under Access Schedule section select “User Access Schedule” from the drop-down menu.

3. Define Time Slots. Select the appropriate block according to start & stop time for each day, by single click on individual block or by selecting multiple blocks inside the table area. The selected area will be seen in different color and it will define the time slot during which the access will be granted to user.
4. Click on “Enroll User” button to enroll the user.

Add a User Access Schedule through GUI while user enrollment

Screens & Steps

Figure 347: User Access Schedule through GUI

1. Enroll a new user through terminal GUI and select Access Schedule from the menu.
2. Select “User Access Schedule” as access schedule for the user and click on OK button to enroll the user.
3. The user is enrolled with user access schedule and user access schedule set as “All Access”(default value).

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.

Besides Webserver, these configurations are possible via **MorphoBioToolBox** and distant commands also.

Access and Time Biometric Terminal can support up to 46 holiday schedules.

Add a Holiday Schedule through Webserver

Access Path

Webserver > Schedules > Holiday Schedules

Pre-requisites

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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

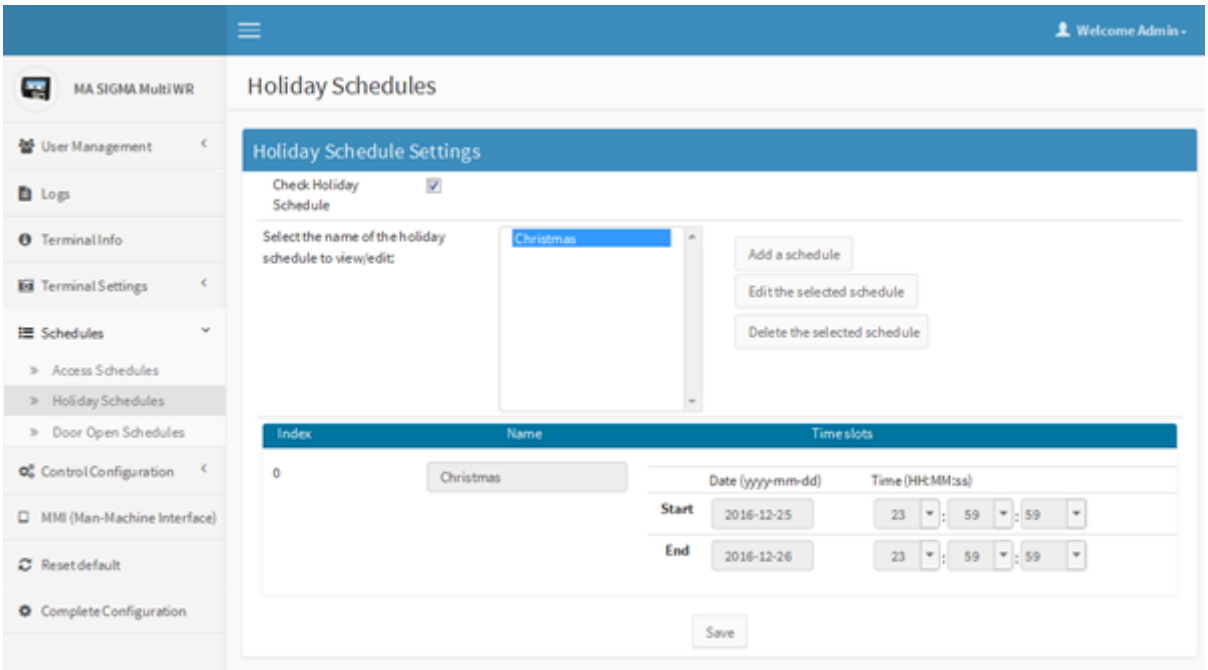


Figure 348: Creating a Holiday Schedule

1. Enter **Schedule Name**, usually the name of the holiday (such as "Christmas")
2. 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
3. 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.
4. 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.

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 any 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.

Besides Webserver, these configurations are possible via **MorphoBioToolBox** and distant commands also.

Door Open Schedule Configuration through Webserver

Access Path

Webserver > Schedules > Door Open Schedules

Pre-requisites

SDAC must be activated

Screens & Steps

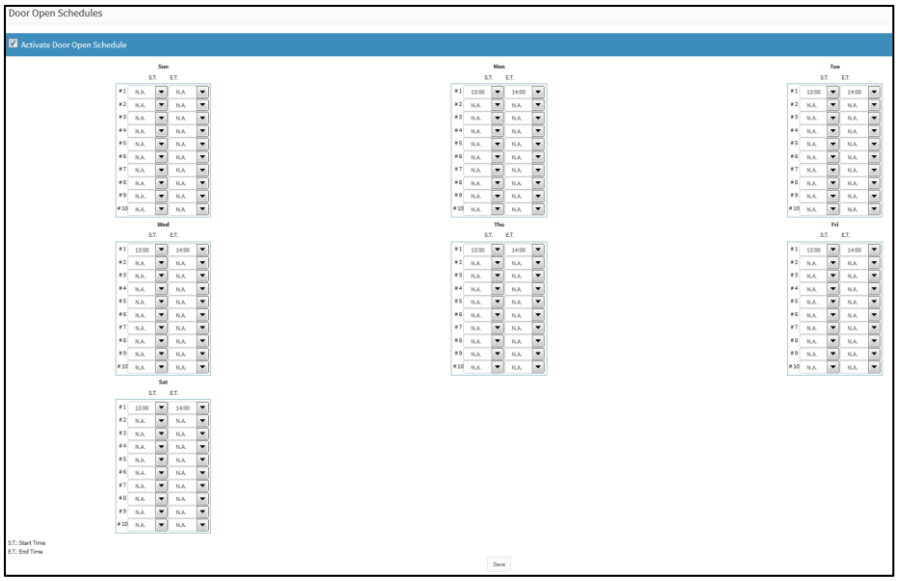


Figure 349: Door Open Schedule Configuration

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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 20 : **Controller Feedback**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Controller Feedback

The administrator can configure parameters that enable the Access Controller to send feedback messages on every event reported by the terminal. Besides Webserver, these configurations are possible via distant commands also.

Access Path

Webserver > Control Configuration > Controller Feedback

Screens & Steps

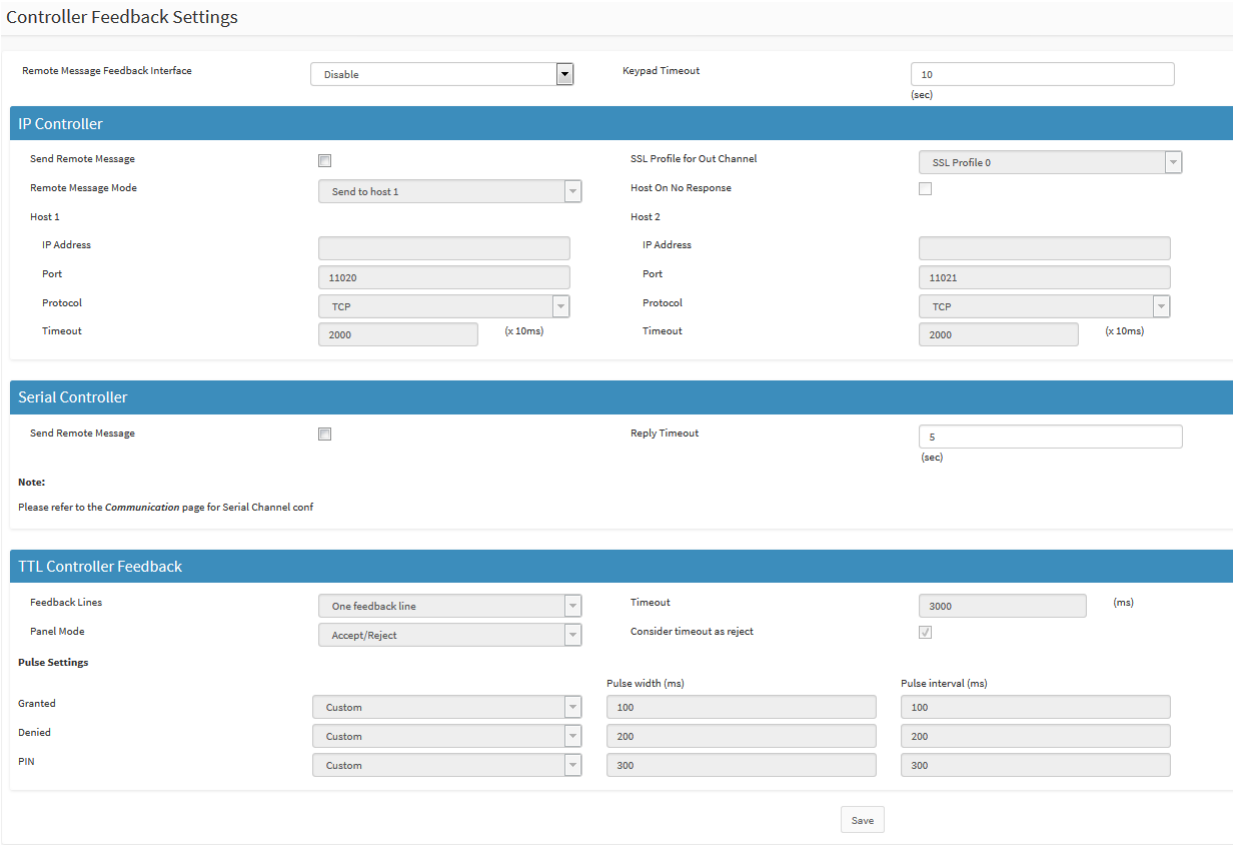


Figure 350: Controller Feedback Settings from Webserver

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 Serial:** Select Feedback over Serial, if controller feedback is to be received on Serial channel (Applicable only to SIGMA Wide and SIGMA Extreme Series terminals)

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

d. **Feedback over TTL:** Select Feedback over TTL, if controller feedback is to be received on Wiegand String. The following parameters need to be configured, only if Wiegand channel is used.

2. 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”
3. 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 consists of 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
4. Enter **Timeout** within which the feedback is sent by controller to the terminal
5. 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
      ii. The **Pulse Interval** can vary between 50 to 1000 milliseconds and value 0. (When the pulse interval is set to 0 the terminal expects to receive one pulse with the width specified by Pulse width setting)
   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 rejected message. You can configure whether to consider timeout as reject. Refer step 6.
   e. Default value for customer fields is as below:
      i. For **Access Granted** – Pulse width and interval is 100ms, by default
      ii. For **Access Denied** – Pulse width and interval is 200ms, by default
      iii. For **PIN** – Pulse width and interval is 300ms, by default

6. **Consider Timeout as Reject:** This function is valid for Access Denied feedback only. If it is enabled, then on timeout the LCD text specified for Access Rejected will be displayed on terminal LCD. If 'Consider timeout as Reject' is unchecked, "Timeout" message will be displayed on LCD.
7. Enter **Keypad Timeout**, for user to enter the PIN. This is used when Panel Mode selected as Accept/Reject/PIN and controller feedback contains PIN (asks user to enter PIN).
8. Click on Save

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 21 : **OSDP Protocol Support**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Description

Access and Time Biometric terminals is able to communicate with external Control Panel (CP) using OSDP (Open Supervised Device Protocol). OSDP is a communication protocol that allows Peripheral Devices (PD) such as Access and Time Biometric terminals to interface with Control Panels (CP) or other security management systems. Security Industry Association (SIA) has developed this protocol to foster interoperability among security devices.

The Peripheral Devices (PD) respond to the commands received from external Control Panel (CP). The protocol supports interfacing of one or more Peripheral Devices (PD) to a Control Panel (CP). The communication between CP and PD is in the form of 'interrogation/reply' mode. The communication is only initiated by CP through OSDP commands. CP can communicate to the PD's in unicast mode or in a broadcast mode, the CP needs to use the address 0x7F for broadcasting to all PD's. The PD responds to the OSDP commands via OSDP responses.

Idemia terminals are managing Open Supervised Device Protocol (OSDP) Version 2.2.2.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Terminal Configuration

The parameters of the OSDP feature are the following:

Parameter name	Value	Description
comm_channels_state.serial	0 - 1 (0 - Default)	start/stop communication over serial channel '0' - to disable '1' - to enable
OSDP.channel	0 - 1 (0 - Default)	Enable/disable the OSDP '0' - to disable '1' - to enable
OSDP.secure_connection	0 - 1 (0 - Default)	Enable/disable the OSDP secure connection '0' - to disable '1' - to enable
OSDP.device_serial_address	0 - 127 (127 - Default)	Contain the OSDP device identifier (Physical Device Address)

The terminal configuration to establish an OSDP connection over the RS485 serial link is the following:

- Connect RS-485 connecter cables to the RS_TX+ and RS_TX- i/o pin of terminal.
- enable the OSDP protocol (OSDP.channel = 1)
- enable the communication over serial channel (comm_channels_state.serial = 1)

The terminal configuration to establish a secure OSDP connection over the RS485 serial link is the following:

- Connect RS-485 connecter cables to the RS_TX+ and RS_TX- i/o pin of terminal.
- enable the OSDP protocol (OSDP.channel = 1)
- enable the OSDP secure channel (OSDP.secure_connection = 1)
- enable the communication over serial channel (comm_channels_state.serial = 1)

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

The other parameters associated to the following features: PIN, BIOMETRIC, SCHEDULE, INTRUSION DETECTION… should be disabled or enabled according to the terminal and control panel usages.

For example:

To manage intrusion, the tamper detection shall be enabled (tamper.state = 1).

OSDP connection icon:

For Idemia terminals with screen, an icon is providing the OSDP connection status.

When OSDP is activated, OSDP.channel set to 1, the icon status is red until the connection with the controller is established, then the icon status switch to green.

When OSDP secure connection is not activated, connection is established as soon a successful standard request and answer is exchange.

When OSDP secure connection is activated, connection is established as soon the mutual authentication is successfully executed.

When OSDP standard connection is lost or OSDP secure session is terminated, the icon status comes back to red.

Red status

Green status

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

OSDP Commands and Responses

The OSDP commands and responses supported terminals are the following :

Request/Command (CP -> PD)	Responses (PD -> CP)
CP commands and PD responses	
osdp_ID : ID Report Request	osdp_PDID : Device Identification Report
osdp_CAP : Peripheral Device Capabilities Request	osdp_PDCAP : Device Capabilities Report
osdp_LSTAT : Local Status Report Request	osdp_LSTATR : Local Status Report
osdp_RSTAT : Reader Status Report Request	osdp_ACK : General Acknowledge, Nothing to Report
osdp_COMSET : Communication Configuration Command	osdp_COM : Communication Configuration Report
osdp_LED : Reader LED Control Command Note: for SIGMA Lite and MorphoWave® SP Series amber color is replaced by yellow	2 possibilities - osdp_ACK : General Acknowledge, Nothing to Report - osdp_NAK : Negative Acknowledge – SIO Comm Handler Error Response
osdp_TEXT : Reader Text Output Command	
osdp_BUZ : Reader Buzzer Control Command	
osdp_POLL : Pool	3 possibilities - osdp_ACK : General Acknowledge, Nothing to Report - Report of an asynchronous command (osdp_BiomatchR) - Report of a terminal action (osdp_RAW, osdp_KEYPAD, osdp_LSTATR)
osdp_BIOMATCH : Scan and Match Biometric Template	First response : - osdp_ACK : General Acknowledge, Nothing to Report - osdp_NAK : Negative Acknowledge – SIO Comm Handler Error Response Asynchronous response if previous reply is osdp_ACK : - osdp_BIOMATCHR : Scan and Match Biometric Template
PD sends this following reply when it is already processing a command and a new command is submit by CP	
CP submits a command	osdp_BUSY : PD Busy Reply **NOTE**: if terminal receives MMI OSDP cmmands (osdp_LED, osdp_TEXT, osdp_BUZ) and it is already displaying specific screen, like user finger request, it will acknowledge the command, not answer busy.
PD sends these following replies via OSP_POLL	
Terminal's action/status change	osdp_RAW : Card Data Report, Raw Bit Array As soon as a smartcard is read by terminal, the terminal provides a GETID information to the Control Panel Note : The format code is the WIEGAND format.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

	The wiegand format will be the wiegand format set in wiegand.event_verify_pass/wiegand.event_identify_pass parameters.
	osdp_KEYPAD : Keypad Data Report As soon as a PIN or a user_ID is entered on terminal, the terminal provides the GETID information to the Control Panel
	osdp_LSTATR : Local Status Report As soon as an intrusion is detected by terminal, the terminal returns this information to the Control Panel via osdp_LSTATR osdp_LSTATR is send as answer to the first osdp_POLL request, following a reboot of the device, too.
Specific commands/replies to initialize an OSDP secure communication	
osdp_CHLNG : Challenge and Secure Session Initialization Request	2 possibilities - osdp_CCRYPT : Client's ID, Random Number, and Cryptogram - osdp_NAK : Negative Acknowledge – SIO Comm Handler Error Response
osdp_SCRYPT : Server Cryptogram	2 possibilities - osdp_RMAC_I : Initial R-MAC The secure session is established with the SCBK default key or with the SCBK custom key provided by osdp_KEYSET command - osdp_NAK : Negative Acknowledge – SIO Comm Handler Error Response
osdp_KEYSET : Encryption Key Set Command	2 possibilities - osdp_ACK : General Acknowledge, Nothing to Report The new SCBK custom key is set on terminal and osdp_CHLNG & osdp_SCRYPT should be sent again by control panel to establish a secure session with this new encryption key. - osdp_NAK : Negative Acknowledge – SIO Comm Handler Error Response

About the osdp_BIOMATCH command

The osdp_Biomatch command enables the SIGMA Series and Morpho*Wave*® Series terminal ranges only to perform biometric scan and match it against the template provided in the command. CP can configure BIO_FORMAT parameter of BIOMATCH command as mentioned below.

NOTE: The osdp_Biomatch command is not available for the VisionPass Range terminals.

Parameter name	Value
BIO_FORMAT	0x0 – Enables the SIGMA Series and Morpho*Wave*® ranges series terminal only to use the template format specified by the terminal configuration parameter 'auth_param.template_type'. Please refer to **Parameters Guide** document for the supported formats. 0x1 – Not supported. Terminal responds with osdp_NAK with error code 0x09 0x2 –ANSI 2004 FMR

When the terminal is waiting for finger during a osdp_BIOMATCH command, osd_LED, osd_TEXT and osd_BUZZER commands are acknowledge without playing because the terminal executes its own MMI.

osdp_BIOMATCH command with multiple fingerprint templates

Morpho*Wave*® Series ranges can manage multiple fingerprint templates in osdp_BIOMATCH command. To do this, administrator as to set the configuration parameter auth_param.template_type is set to -1.

Only TLV format is supported for multiple fingerprint templates. By consequence the BIO_FORMAT parameter of the osdp_BIOMATCH command should be equal to 0x00. Then TLV templates just must be write consecutively in the BIO_DATA parameter of the osdp_BIOMATCH command (TLV1 TLV2 TLV3).

TLV format is described in the document "*2016_0000022619 - MA5G - Contactless Cards Specification*".

About the osdp_POLL command

osdp_POLL command is used as general inquiry by the panel. The following are the possible responses for osdp_POLL command.

1. osdp_RAW: Terminal responds with this command when it completes the authentication process of smartcard/external port/Prox card or the biometric identification process.

   After authentication or the biometric identification process, the terminal puts the user's Id into the polling queue in the form of Wiegand format. The Wiegand format is defined by the terminal's Wiegand configuration for Identification Pass/Fail and Verification Pass/Fail parameters.

2. osdp_KEYPAD: Terminal responds with this command when it completes the authentication process by keypad.

3. osdp_LSTAT: Terminal responds with this command when it detects change of tamper status or recent power failure or to the first osdp_POLL command following a reboot.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

4. osdp_BIOMATCHR: Terminal responds with this command when the biometric match process is completed by BIOMATCH command.

All above responses are logged in internal buffer of the terminal and they are sent as response to the osdp_POLL command in FIFO manner. If there is no response logged in the internal buffer of the terminal, then osdp_ACK is sent as a response to osdp_POLL command.

About the osdp_COMSET command

The supported baudrate are: 9600, 19200, 38400, 57600, 115200 for osdp_COMSET.

About the osdp_CAP command

The Control Panel can obtain the capabilities of the terminals with the osdp_CAP command. The PD will execute OSDP commands according to the terminal's capability.

OSDP capability answer are:

Function 1: No contact status monitoring, because we don't manage OSDP commands for Single Door Access Control.

Function 2: No output control, because we don't manage OSDP commands for Single Door Access Control.

Function 3: Terminal sends card data to the controller as array of bits, not exceeding 1 024 bits.

Function 4:

- Terminal controls a LED. Because there is no OSDP value corresponding to multi-color LED, device answers bi-color LED.
- On Sigma Wide, Sigma Extreme, Sigma Lite+, Morpho*Wave* and VisionPass terminal ranges, when this command is received a "LED" icon of the corresponding color is displayed on every screen.
- On all terminals, amber color is replaced by yellow.

Function 5: All terminals have an audible output and support timed commands. On Sigma Wide, Sigma Extreme, Morpho*Wave* Compact and VisionPass, we have speaker and not buzzer, by consequence there could be delay to play sound.

Function 6: Sigma Wide, Sigma Extreme, Sigma Lite+, Morpho*Wave* Compact, Morpho*Wave* XP2 and VisionPass Range terminals, have a text output that supports 4 rows of 16 characters. Sigma Lite and Morpho*Wave* SP has no text output.

Function 8: All terminals are supporting CRC mode.

Function 9: If the configuration key OSDP.secure_connection is disable terminal is not supporting secure communication. If the configuration key OSDP.secure_connection is activate terminal is supporting secure communication.

Function 11: All terminals are supporting 1440 bytes as largest combined message size (max. of OSDP as of now).

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Function 12: terminals are supporting not OSDP commands to communicate directly with a smartcard.

Function 13: terminals have only one credential reader devices present.

Function 14: Sigma series and Morpho*Wave* series are biometric fingerprint devices. Because Face recognition is not included in OSDP specification, VisionPass Range terminals answer no biometric.

About OSDP secure channel

When a secure channel connection is established, the terminal remembers the key. To reset it, apply the reset contactless key command.

When secure OSDP is enable, terminal answers osdp_NAK to commands send in not secure protocol, except commands dedicated to initialize the secure communication and osdp_CAP, osdp_ID and osdp_COMSET, that are still supported.

Please refer to Open Supervised Device Protocol (OSDP) Version 2.2.2 on SIA Website https://www.securityindustry.org/Pages/Standards/OSDP.aspx for more details about te OSDP commands and replies.

Demonstration of osdp_LED and osdp_TEXT command for SIGMA terminal

OSDP exchanges between the CP and PD to update the Text and LED color on SIGMA terminal as depicted in the Figure 348.

Sequence	Tx/Rx	Command/Response Syntax with Example
1	CP -> PD (Start/Request of a command)	osdp_TEXT (0, 2, 0, 1, 6, 32, “HELLO WELCOME”) Syntax: osdp_TEXT (Reader Number, Text Command, Temp Text time, Row, Column, Text Length, String)
2	PD -> CP (Response to a command)	osdp_ACK in case of Success else osdp_NACK for failure
3	CP -> PD (Start/Request of a command)	osdp_LED (0, 0, 0, 0, 0, 0, 0, 0, 1, 10, 0, 2, 0) Syntax: osdp_LED (Reader number, LED Number, Temp Control Code, On time, Off time, On colour, Off colour, Timer LSB/Timer MSB, Perm Control code, On time, Off time, On colour, Off colour)
4	PD -> CP (Response to a command)	osdp_ACK in case of Success else osdp_NACK for failure

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Figure 351: OSDP LED and TEXT Screen on SIGMA Wide terminal

Terminals with LCD integrate the OSDP display in the home display.

Demonstration of osdp_LED and osdp_TEXT command for SIGMA Lite+ terminal

OSDP exchanges between the CP and PD to update the Text and LED color on SIGMA Lite+ terminal as shown in Figure 349.

Sequence	Tx/Rx	Command/Response Syntax with Example
1	CP -> PD (Start/Request of a command)	osdp_TEXT (0, 2, 0, 1, 6, 32, “HELLO WELCOME”) Syntax: osdp_TEXT (Reader Number, Text Command, Temp Text time, Row, Column, Text Length, String)
2	PD -> CP (Response to a command)	osdp_ACK in case of Success else osdp_NACK for failure
3	CP -> PD (Start/Request of a command)	osdp_LED (0, 0, 0, 0, 0, 0, 0, 0, 1, 10, 0, 2, 0) Syntax: osdp_LED (Reader number, LED Number, Temp Control Code, On time, Off time, On colour, Off colour, Timer LSB/Timer MSB, Perm Control code, On time, Off time, On colour, Off colour)
4	PD -> CP (Response to a command)	osdp_ACK in case of Success else osdp_NACK for failure

Figure 352: OSDP LED and TEXT Screen on SIGMA Lite+ terminal

The SIGMA Lite+ terminal has a dedicated full-screen display for OSDP.

The user can return to the home screen by clicking on the back button “ ” on the OSDP screen. The OSDP screen will display again after 3 seconds.

Demonstration of osdp_LED command for SIGMA Lite terminal

OSDP exchanges between the CP and PD to change the color of LED on SIGMA Lite.

Sequence	Tx/Rx	Command/Response Syntax with Example
1	CP -> PD (Start/Request of a command)	osdp_LED (0, 0, 0, 0, 0, 0, 0, 0, 1, 10, 0, 2, 0) Syntax: osdp_LED (Reader number, LED Number, Temp Control Code, On time, Off time, On colour, Off colour, Timer LSB/Timer MSB, Perm Control code, On time, Off time, On colour, Off colour)
2	PD -> CP (Response to a command)	osdp_ACK in case of Success else osdp_NACK for failure

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

How to ignore MMI OSDP commands and play Idemia MMI

OSDP is designed for the interaction of a panel (access controller) with a basic user-facing device: Man-to-Machine Interface (MMI) is either buzzer or LED or text.

IDEMIA Access and Time Biometric Terminals feature a large screen, enhancing the user experience while extending the possibilities. But due the above mentioned OSDP limitations, when the Terminal is connected to an OSDP controller, the screen capabilities cannot be leveraged.

In order to provide customers with a solution exceeding the standard, IDEMIA introduced the 'Ignore MMI' feature.

Basic principle is: the biometric terminal discards panel requests associated to MMI, and provides the usual ‘Access Granted’ or ‘Access Denied’ user experience.

Ignore MMI is a terminal parameter. When this mode is activated, device doesn’t execute any osdp_LED, osdp_BUZ, osdp_TEXT command but acknowledge them, for the Access Controller not to generate an alarm.

OSDP.ignore_MMI set to 1

“Access Granted” user experience is triggered by an OSDP_LED command with parameters LED temporary green

“Access Denied” user experience is triggered by an OSDP_LED command with parameters LED temporary red

OSDP.ignore_MMI set to 3

“Access Granted” user experience is triggered by a specific OSDP frame

“Access Denied” user experience is triggered by another specific OSDP frame

2 configuration keys specify the OSDP commands that will generate access granted and access denied: OSDP.access_granted and OSDP.access_denied

These keys contain beginning of OSDP command that should generate access granted and access denied. Keys values are hexadecimal and length will be variable from one byte to a maximum size of 128 bytes.

These key values should be equal to part of the OSDP command that device should detect, starting from command field and follow by beginning of data field.

When device receives OSDP commands starting with the key value contained in OSDP.access_granted or OSDP.access_denied, device is playing the dedicated Idemia MMI, access granted or access denied.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Configuration example for OSDP.ignore_MMI set to 3

Let's suppose the Access Controller is designed to:

Trigger an "access granted" message when receiving the OSDP_LED command 0x69000002050502xxxxxxxxxxxxxxxxxxxx (command OSDP LED, first Reader, first LED, temporary state, ON during 5 ms, OFF during 5 ms, ON color Green, other parameters not specified)

Trigger an "access denied" message when receiving the OSDP_LED command 0x69000002050501xxxxxxxxxxxxxxxxxxxx (command OSDP LED, first Reader, first LED, temporary state, ON during 5 ms, OFF during 5 ms, ON color Red, other parameters not specified)

The Biometric Terminal needs to be configured likewise:

OSDP.ignore_MMI set to 1

OSDP.access_granted = 0x69000002050502

OSDP.access_denied = 0x69000002050501

Behavior:

When receiving OSDP command 0x690000020505020A00000000000000000000 or any other OSDP command starting by 0x69000002050502, device will play access granted MMI.

When receiving OSDP command 0x690000020505010A00000000000000000000 or any other OSDP command starting by 0x69000002050501, device will play access denied MMI.

Because in this case, commands are OSDP_LED, there will be not executed, only acknowledged. **Terminal will play IDEMIA Access Granted or Denied MMI.**

About Idemia MMI customization

When OSDP.ignore_MMI set to 3, current language device configuration is applied, the access granted or denied icon customizations are applied, modification of the text "access granted" or "access denied", by language file, is applied.

Customization of the "access granted" content (choose of display: user ID, Name, timestamp) using the configuration key "success_message.display_information" is not applied because device doesn't know the user ID and name to display when receiving the OSDP command

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

PIN over OSDP

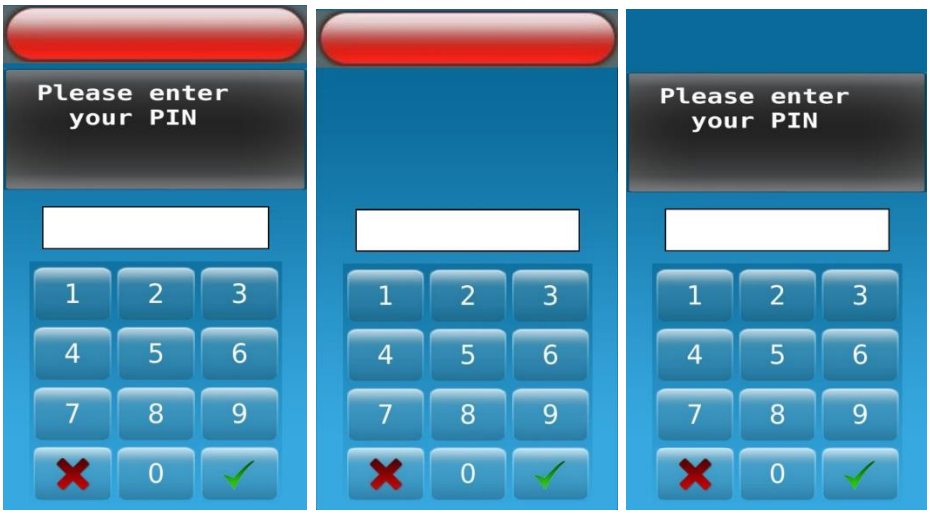
With a specific terminal configuration, it is possible to send user PIN to the OSDP controller, to allow its verification by this one.

This functionality is

PIN check has to be requested, using “per user rule” or “global PIN control”.

Additionally the send PIN to controller has to be activated by setting to 1 the configuration key OSDP.pin_over_osdp.

When user is authenticated or identified, if a PIN control is requested, a specific keyboard is displayed. The displayed screen will include LED and TEXT displayed if the associated OSDP commands are executed.



OSDP PIN keyboard with or without LED and/or Text displayed

When user press any key, an osdp_KEYPAD frame containing the key value is send. Additionally a “dot” is displayed on the dedicated screen case for each pressed key.

When red cross key is pressed, current PIN acquisition is aborted, workflow is reset and display comes back to idle screen.

When green check is pressed, a osdp_KEYPAD frame containing the associated value (0x0D) is send.

Code value associated to “*” is never send.

Report user rejection event with OSDP

IDEMIA Access and Time Biometric terminals can report user rejection event, using the OSDP command osdp_MFGREP, answering to OSDP_poll. These events are not automatically reported, because all OSDP controllers are not managing them. Administrator has to activate it by setting the key OSDP.event_report.

Every OSDP controllers are not managing MMI (LED, text and buzzer) in case of user rejection, by consequence there is a configuration key to enable or disable the terminal default access denied MMI display, named OSDP.Display_Access_denied. This key has an effect only if OSDP is activated.

Here the OSDP answer to OSDP_poll for user rejection event:

0	CMND/RPLY	0x90	osdp_MFGREP	Value
1	DATA	0x00	Vendor Code 1st	CEM IEEE Idemia : 0024AE
2		0x24	Vendor Code 2nd	
3		0xAE	Vendor Code 3rd	
4		0x01	Failed Trans ID	Failed transaction message indication
5		See next table	Transaction Code	A unique code for each required transaction type (See next table)
6		0x00	Reader Number	Number
7		0x00 = raw bit arr. 0x01 = Wiegand	Format Code	Format of included data
8		0x00-0xFF	Bit Count (LSB)	2-byte size (in bits) of the card data at the end of the record
		0x00-0xFF	Bit Count (MSB)	
9				
10-N		0x00-0xFF	Card Data	8 bits of card data per data byte MSB to LSB (left justified)

Here the value and data for each type of rejection event:

Code value	Transaction Code	Card Data
0x01	Duress finger	Wiegand frame defined by wiegand.event_duress_finger
0x02	Fake biometry	0 if identification (no user ID) Wiegand frame defined by wiegand.event_verify_fail if authentification
0x03	biometric mismatch	0 if identification (no user ID) Wiegand frame defined by wiegand.event_verify_fail if authentification

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

0x04	pin mismatch	Wiegand frame defined by wiegand.event_verify_fail
0x05	User ID not in DB	Wiegand frame defined by wiegand.event_verify_fail
0x06	control timed out	Wiegand frame defined by wiegand.event_verify_fail
0x07	rejected by schedule	Wiegand frame defined by wiegand.event_verify_fail
0x08	temp validity expired	Wiegand frame defined by wiegand.event_verify_fail
0x09	user not in authorized list	Wiegand frame defined by wiegand.event_verify_fail
0x0A	face not detected (Applicable to MASigma and Extreme only)	Wiegand frame defined by wiegand.event_verify_fail
0x0B	job code check failure	Wiegand frame defined by wiegand.event_verify_fail
0x0C	user rule check failure	Wiegand frame defined by wiegand.event_verify_fail
0x0D	user timed anti passback	Wiegand frame defined by wiegand.event_verify_fail
0x0F	Invalid QR code	Wiegand frame defined by wiegand.event_verify_fail
0x10	Invalid card	Wiegand frame defined by wiegand.event_verify_fail
0x11	Invalid user data	Wiegand frame defined by wiegand.event_verify_fail

Recommendation and limitation for OSDP integration

We recommend to not send OSDP commands with higher frequency that 100ms between each one. Else some commands can be acknowledged without being executed.

Terminal could not execute user enrolment during OSDP connection.

Terminal should not be connected with OSDP and Wiegand at the same time.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 22 : SSCP

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Description

MorphoWave® SP", "MorphoWave® XP2" and "VisionPass SP" terminals are able to communicate with external Control Panel (CP) using SSCP (Open Supervised Device Protocol). SSCP is a communication protocol that allows Peripheral Devices (PD) such as Access and Time Biometric terminals to interface with Control Panels (CP) or other security management systems.

The Peripheral Devices (PD) respond to the commands received from external Control Panel (CP). The protocol supports interfacing of one or more Peripheral Devices (PD) to a Control Panel (CP). The communication between CP and PD is in the form of 'interrogation/reply' mode. The communication is only initiated by CP through SSCP commands. CP can communicate to the PD's in unicast mode or in a broadcast mode, the CP needs to use the address 0x00 for broadcasting to all PD's. The PD responds to the SSCP commands via SSCP responses.

To enable the SSCP functionality, Access and Time Biometric terminals requires the BT_SSCP license.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Terminal Configuration

The parameters of the SSCP feature are the following:

Parameter name	Value	Description
comm_channels_state.serial	0 - 1 (0 - Default)	start/stop communication over serial channel '0' - to disable '1' - to enable
SSCP.channel	0 - 1 (0 - Default)	Enable/disable the SSCP '0' - to disable '1' - to enable
SSCP.device_serial_address	0 - 127 (127 - Default)	Contain the SSCP device identifier (Physical Device Address)
SSCP.intercharacter_timeout	0 - 20 *(**20** - Default)*	Timeout to receive two consecutive bytes.
SSCP.start_of_frame_timeout	0 - 8000 *(**8000** - Default)*	Timeout to wait new start of command.
tamper.action_reset_SSCP	0 - Disable *(**0** - Default)* 1 - Reset SSCP key	When tamper is triggered: action to reset SSCP Authentication key to default value.

The terminal configuration to establish an SSCP connection over the RS485 serial link is the following:

- Connect RS-485 connecter cables to the RS_TX+ and RS_TX- i/o pin of terminal.
- enable the SSCP protocol (SSCP.channel = 1)
- enable the communication over serial channel (comm_channels_state.serial = 1)

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

The other parameters associated to the following features: PIN, BIOMETRIC, SCHEDULE, INTRUSION DETECTION… should be disabled or enabled according to the terminal and control panel usages.

For example:

To manage intrusion, the tamper detection shall be enabled (tamper.state = 1).

Contactless card reading is done using the TransceiveAPDU SSCP command. By consequence the complete reading sequence has to be implemented in the CP.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

SSCP Commands and Responses

The SSCP commands and responses supported terminals are the following :

Request/Command (CP -> PD)	Responses (PD -> CP)
CP commands and PD responses	
Authenticate: the controller and the terminal establish a secure messaging channel.	ACK
Scan_A_RAW: this API detects smartcards that are compatible with ISO7816-3/4 type A.	No card detected: • NbCard=0 Card detected: • NbCard=1 • SAK, ATQA, UID • Option: ATS
TransceiveAPDU	DataOut = C-APDU = CLA + INS + P1 + P2 + Lout + DATAout : 255 byte max
SetBaudRate: Apply the baudrate passed in parameter on the next command in the current session.	ERR_CODE_READER_00_OK
Set485Address: • Apply the address of the terminal on the next command in the current session • Store the address in the config database in "SSCP.device_serial_address"	ERR_CODE_READER_00_OK
SetInterByteTimeout • Change the interByteTimeout of the serial communication for the next command in the current session. • Store the interByteTimeout in the config database in "SSCP.interchar_timeout" • The terminal must wait for a full new command;i.e. wait for SOF, if an interbyte-timeout is triggered.	ERR_CODE_READER_00_OK
GetInterByteTimout • Returns the "SSCP.interchar_timeout" from the config database.	ERR_CODE_READER_00_OK
Outputs • the color of the LEDs and LED ON duration (ms), • the buzzer ON duration (ms)	ERR_CODE_READER_00_OK
ChangeISKeys(ChangeReadKey) Store the key used for the authentication in the KMS/AES	ERR_CODE_READER_00_OK
Verify	Match: 1 success / 0 fail

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

• Matching of input template against the fingerprint on sensor. • The format of the template is defined by “auth_param.template_type” configuration key	
Identify • Return result of input biometric identification matching. • With VisionPass SP, randomly, execution of the command can exceed the timeout parameter value, until 10 seconds.	
OutputRGB • Play buzzer for a delay • Light on RGB LEDs for a delay • Activate/deactivate the alarm mode not implemented	ERR_CODE_READER_00_OK
SetTamperSwitchSettings • This command sets the anti-tamper configuration	ERR_CODE_READER_00_OK
GetTamperSwitchInfos • This command gets the anti-tamper configuration and the current status	ERR_CODE_READER_00_OK

About the Verify command

This command is supported by the following fingerprint terminals: MorphoWave® XP2, MorphoWave® SP.
This command is not supported by facial terminals, VisionPass SP.

About the OutputRGB command

MorphoWave® SP terminal doesn’t support the orange color.
The expert mode is not implemented.

Section 23 : User Control Configurations

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

User Control Configurations

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

Besides Webserver, these configurations are possible via **MorphoBioToolBox** and distant commands also.

User Control Configurations through Webserver

Access Path

Webserver > Control Configuration > User Control

Screens & Steps

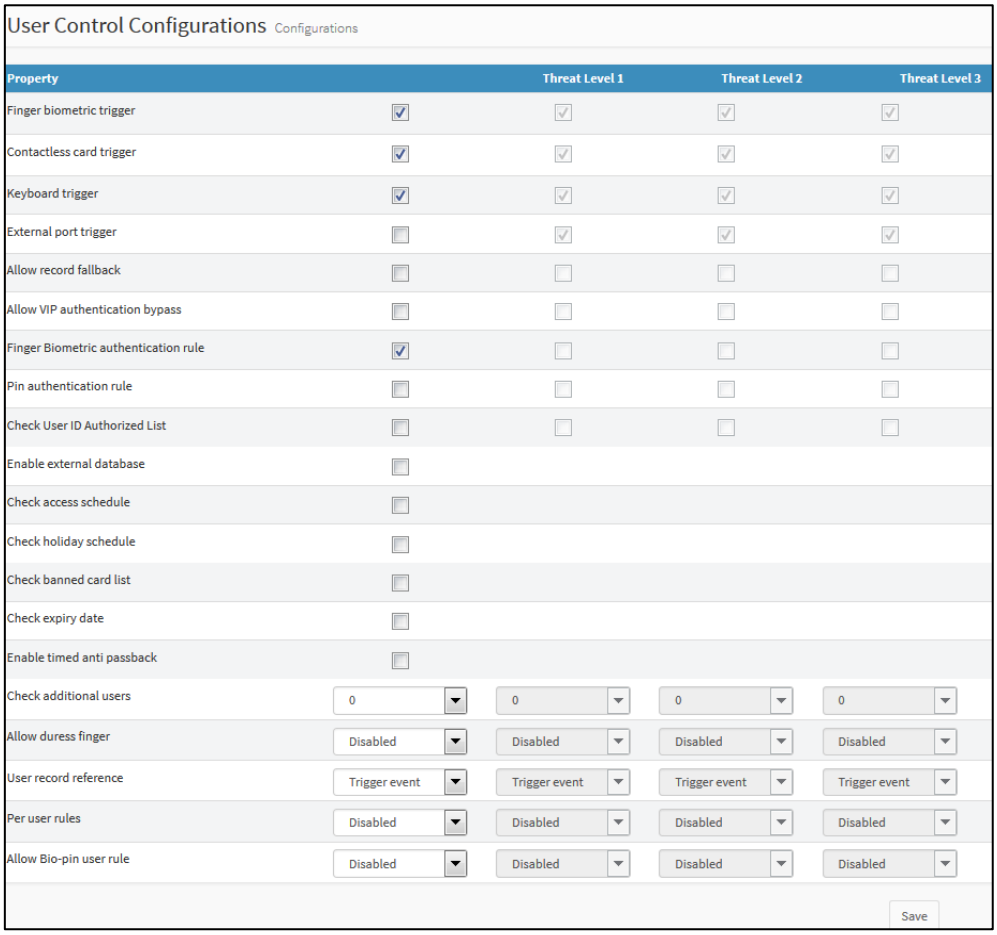


Figure 353: User Control Configurations from Webserver

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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

1. **Biometric Trigger:** A user control operation can be triggered by presenting finger or face to 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.
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. **QR Code Trigger:** This parameter can be enabled to start QR code control check, using authentication process, when a QR code is presented to the terminal.
6. **Allow Record Fallback:** To allow terminal to use references from database if references from smartcard are not present. E.g. for smartcard triggered 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.
7. **Allow VIP Authentication Bypass:** If this parameter is enabled then users in the VIP list are exempted from authentication checks (biometric, pin, face detection), 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.

Note: Face capture is still performed if configured for SIGMA Series terminal. Other checks such as access schedule, holiday schedule, banned card, authorized list, expiry date, trigger check, reference check, etc. are still performed normally. Refer to "Access Control Process for VIP Users"

8. **Biometric Authentication Rule:** This parameter indicates whether terminal should check biometric of the user as a part of user control workflow.
9. **Pin Authentication Rule:** This parameter indicates whether terminal should check PIN of the user as a part of user control workflow.

10. **Check User ID Authorized list:** This parameter controls authorized list check during user control workflow. If enabled, the terminal will check whether user is in authorized list or not.
11. **Enable external database:** If enabled, the polling mode of the terminal will be activated, in that case user's data will be checked with the data stored in external database. Refer "*Polling Mode*" for understanding polling mode.
12. **Check access schedule:** This indicates whether terminal should check the access schedule before granting access to the user
13. **Check holiday schedule:** This indicates whether terminal should check the holiday schedule before granting access to the user
14. **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.
15. **Check expiry date:** If this parameter is enabled terminal will check the expiry date of user account.
16. **Enable timed anti passback:** If this parameter is enabled then the repeated access control for a user till **Timed Anti Passback Timeout** is not allowed on the terminal.
17. **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). When this feature is activated, the terminal evaluates the access rights with the data of two different users, instead of the data of only one user. It means that, when access right is based on biometric data check, the terminal requires biometric data of two different users to grant the access.

    Transaction logs will contain one line for each of the 2 users control operation but only second one could be sent as event. 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.

    Note: Option is not available in VisionPass Range terminals
18. **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.

    Note: Option is not available in VisionPass Range terminals
19. **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.

20. **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, then the controls specified for all users in the terminal configuration will be applied.

21. ***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

    Note: BIOPIN option is not available in VisionPass Range terminals

22. ***Face* authentication rule:** This parameter defines face authentication check workflow rule. Possible values are "Disabled", "Photo taking", "Face detection (optional)" and "Face detection (mandatory)". This applies only to SIGMA Series terminal only. Please refer to the section "*Additional User Controls*" for understanding the face detection workflow

    Note: Option is not available in VisionPass Range terminals

23. Click on **Save**

References

Refer to "*Recommended Conditions for Face Detection*" for knowing the correct position of the user and required lighting conditions for face detection.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 24 : **Event Configurations**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Event Configurations

Events which can be monitored in Access and Time Biometric Terminal are listed in 'Event' 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 are to be sent to access controller, GPO TTL lines and its data clock id.

Besides Webserver, these configurations are possible via distant commands also.

Event Configurations through Webserver

Access Path

Webserver > Control Configuration > Event

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Screens & Steps

Event Settings

Event Name	Enable	Send To Controller	GPO0	GPO1	GPO2	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
Face not Detected Event	☑	☐				65535
Multi-User Intermediate ID Event	☑					
Transaction Log File Full Event	☑	☐				
Controller Feedback Event	☑					
Job Code Check Failure Event	☑	☐				65535
Door Opened For Too Long Event	☑	☐				
Forced Door Open Event	☑	☐				
Door closed After Alarm Event	☑	☐				
Door Unlocked Event	☑	☐				
Door Locked Back Event	☑	☐				
Management Menu Login Event	☑	☐	☐	☐	☐	
Management Menu Logout 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	☑					

Save

Figure 354: 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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Note: Duress Finger, **Face not Detected, Multi-User Intermediate ID** events are not available in VisionPass Range terminals

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 25 : MMI (Man-Machine Interface) Configurations

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

MMI (Man-Machine Interface) Menu

This section provides various configurations that an administrator can make to the terminal LCD.

MMI Features/Function name	SIGMA and SIGMA Extreme Series MorphoWave® Compact MorphoWave® XP2	SIGMA Lite+ Series MorphoWave® SP	VisionPass Series
Enable AZERTY Keyboard	✓	✗	✗
Administration If this parameter is enabled, the information menu on the terminal shall be displayed)	✓	✓	✓
Audio for successful Verification	✓	✗	✓
Audio for Message Attention	✓	✗	✓
Display Reason for Access Denied	✓	✗	✓
Display Name on Access Granted	✓	✓	✓
Brightness (Range of this parameter is 5-100)	✓	✓	✓
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)	✓	✓	✓
Idle Screen Video Brightness	✓	✗	✗
Face Detection Timeout	✓	✗	✗
Disable Sensor (In Low-Power Mode)	✓	✓	✗
Idle Screen Status	✓	✓	✓
Audio for Failed Verification	✓	✗	✓
Audio for Tamper	✓	✗	✓
Display User ID on Access Granted	✓	✓	✓

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Display Time Stamp on Access Granted	✓	✓	✓
Log-in Option	✓	✗	✓
Idle Video Timeout	✓	✗	✓
Audio Volume	✓	✗	✓
Terminal Language	✓	✗	✓
Video Phone	✓	✗	✗
Dynamic Message	✓	✗	✓
Video in background	✗	✗	✓
User Guidance MMI	✗	✗	✓

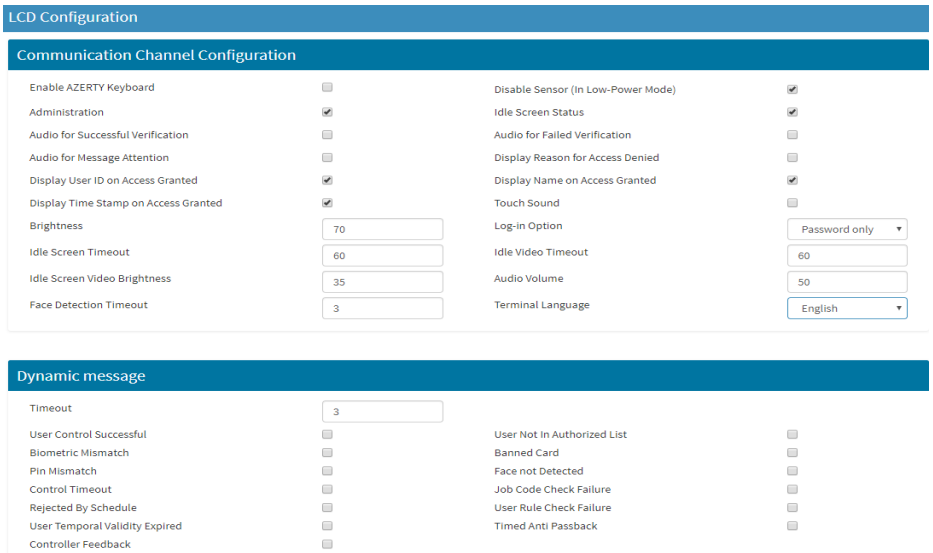
Besides Webserver, these configurations are possible via **MorphoBioToolbox** and distant commands also.

MMI Configurations through Webserver

Access Path

Webserver > MMI (Man-Machine Interface)

Screens



Section 26 : **Distant Commands Mode**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Presentation of Distant Commands mode

Process

The administrator can configure the Access and Time Biometric Terminal MDPI terminal in the Distant Commands mode. This operating mode allows controlling the Access and Time Biometric Terminal MDPI terminal remotely via IP link or RS422 (Applicable to SIGMA Wide, SIGMA Extreme, Morpho*Wave®* Compact and Morpho*Wave®* SP Series only). This is achieved by using a set of biometric and databases management commands.

In Distant Commands mode the Host System plays the master. It performs access control remotely, while the Access and Time Biometric Terminal works as a slave waiting for external commands.

Commands are described in the **Distant Commands Guide** document

The Access and Time Biometric Terminal MDPI 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 **Host System Interface Specifications**: this document explains how to remotely manage a terminal.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Distant Commands mode use sample

When terminal is use in Distant Commands mode, then the administrator can control several functions of the terminal. For example, if it is required to take the backup of terminal database, the administrator can take a backup.

The snapshot below describes a typical exchange between the terminal and the distant system for a basic access control by identification. One would see that the distant system is the master, while the terminal is the slave.

Figure 355: Distant commands sample with a remote Identification process

Section 27 : **Polling Mode**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Presentation of Polling mode

If the administrator enables the polling mode, the Access and Time Biometric 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** = If set to Auto 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** = If set to Terminal, then user rule provided by distant command will be used.

If **ucc.per_user_rules** = If set to Disabled, then user rule check is disabled.

Process

Polling using buffer:

The User ID will be queued in the terminal's queue. This, is polled by external application.

External application waits for the User ID by polling the buffer. After receiving the User ID, it will search the template in its database. Thereafter, it sends the template to terminal for further authentication.

The user is authenticated by the external terminal.

Access and Time Biometric Terminal also has distant commands to retrieve status and data of the polling buffer. Please refer to **Host System Interface Specifications** guide, for more details.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Polling mode activation

The administrator can activate the Polling mode through **Webserver > Complete Configuration**. This is done by setting the parameter "**ucc.enable_external_database**" to '1'. Please refer to **Parameters Guide** to know as to how to set this parameter.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 28 : **Messages Sending**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Principle

The administrator can configure the Access and Time Biometric Terminal, to generate and send messages to another physical entity, upon the occurrence of specific events during the access control process.

The events that lead to generation and sending of messages sending are, as follows.

Result of access rights check (after access request by a user)

Internal log file full

Tamper detected

Time and Attendance actions

Duress Finger detected (Not supported on VisionPass Range terminals)

Please refer to **Remote Message Specification** for details regarding the message content.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Events

The Access and Time Biometric Terminal allows the administrator to select one or more events on which messages can be sent to the external controller. An administrator can enable or disable events using Webserver or distant command.

Please refer to "*Event Configuration*" in this document, to learn more on various events that can be selected.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Sending Interfaces

The administrator can choose the interfaces that will be available for the messages sending process.

By default, no interface is available. The administrator needs to set the parameters mentioned below for activating remote sending message:

Number of available interfaces	
remote_msg_conf.send_ethernet_state	This parameter can be set as “1” to enable message sending over Ethernet
remote_msg_conf.send_serial_state	This parameter can be set as “1” to enable message sending over Serial Interface

For each interface available, the following parameters are customizable:

- Communication layer
- Protocol used
- Parameters depending on the layer and the protocol used.

TCP protocol is available on the IP layer. Following are the parameters that can be configured for host 1, in order to communicate via TCP protocol.

TCP parameters	
remote_msg_ip_conf.host_1_ip	• The IP address of the distant system.
remote_msg_ip_conf.host_1_port	• Port address 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 the remote controller on host 1 and perform read/write operations.

The same parameters are configurable for host 2, in case the terminal is unable to connect to host 1 server. Terminal will now attempt to send message on host 2. Please refer to **Parameters Guide** for further details on interface configuration.

Send messages format is defined in **Remote Message Specification.pdf** .

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 29 : **Compatibility with an Access Control System**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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. In case of a centralized access, the decision to open the door is taken by a central host, thus making the process more secure.

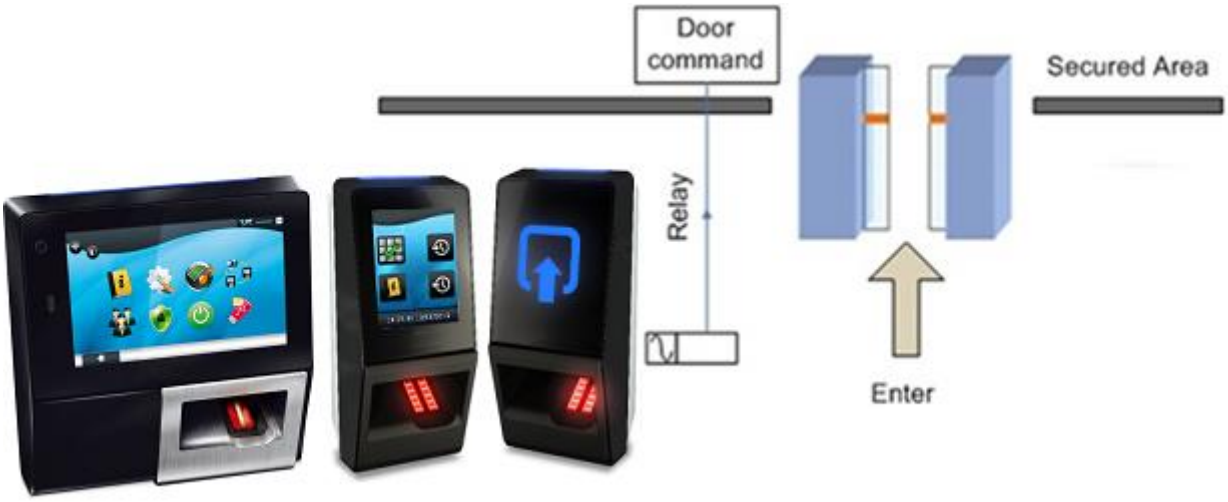


Figure 356: Using the internal relay on the Access and Time Biometric Terminal

Activation key

The administrator can configure the following parameters. These parameters are related to internal relay activation, in the event of an access being granted.

Parameters	SIGMA Series SIGMA Extreme Series Morpho*Wave*® Series VisionPass Series	SIGMA Lite Series
gpio.sdac_relay_default_state	✓	✗
gpio.func_mode	✓	✓
gpio.sdac_door_unlock_dur	✓	✓

Parameter name	Value	Description
gpio.sdac_relay_default_state	0 or 1	The administrator can set a default state of the internal relay, by using this parameter. The internal relay can be either, powered or unpowered. Select “0” for Low. This is the default value of this parameter and it indicates that by default the internal relay will be unpowered. On access being 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 being granted the internal relay state will change to low (it will be powered off).

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Parameter name	Value	Description
gpio.func_mode	0, 1 or 2	Configuration for GPIO functional mode Select “0” to enable GPIO general mode (default) Select “1” to enable Threat Level mode Select “2” to enable SDAC mode

Configuration key

Parameter name	Value	Description
gpio.sdac_door_unlock_dur	2 - 60 sec. (10-Default)	The administrator can configure this parameter to set the 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).

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

External activation of the internal relay

Description

The administrator can enable this function to allow the activation of the terminal internal relay via a push button connected between the LED1 and the GND wires. When this function has been enabled, 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 Access and Time Biometric Terminal (as depicted in the figure below):

To enter in the protected area the user must be successfully recognized by the Access and Time Biometric Terminal,

To exit from the protected area, the user presses a simple push-button connected between the LED1 and GND wires of the Access and Time Biometric Terminal.

Figure 357: 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	The administrator can set an exit mode in SDAC, by using this parameter. Following values can be configured: • "0" means None • "1" means Push Button. Push button exit mode is selected when a push button is located at exit gate and users are allowed to push the exit button to open the exit door.

Configuration key

Parameter name	Value	Description
gpio.sdac_rte_egress_timeout	1 to 300 Seconds (25– Default)	The administrator can define an egress timeout, by using this parameter. The 'egress timeout' is defined as the duration for which terminal will not generate an alarm, if door is opened by using a push button, manual or forced method of opening. No user control is performed within this duration. The door closes automatically, once the 'egress timeout' period elapses. For this to work gpio.sdac_rte_mode should be either set to 1 or 2 gpio.func_mode must be set to SDAC mode

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Access Request Result Log File

Description

The administrator can enable this functionality so that, 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 ID or in other words, user's identifier (if available),

the access control process executed (Identification, Authentication with biometric check, etc.),

the result of the access control, which can be granted or denied. If denied then the reason could be user not recognized or access requested outside the authorized time slot, for an instance).

and other data used for statistical reasons.

Log File format

The transaction log feature is available in two formats :

- "Basic Mode "
- "Identified Mode"

The Identified format has :

- a field to associate a unique_id at each log
- a reading status to tag the log as read or as not read

This information helps administrator to retrieve or erase records based on unique log ID.

By default the transaction log format is in 'Basic Mode'.

It can be changed to 'Identified Mode' by configuring following parameter :

Parameter name	Value	Description
transaction_log.format	0 or 1 (0 – Default)	Set "0" to configure transaction log in 'Basic Mode'. Set "1" to configure transaction log in 'Identified Mode'.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

For more information, refer to the **Host System Interface Specification** document.

NOTE: When 'transaction_log.format' parameter value is changed from current value, all previous transaction log entry will be erased on next reboot of terminal and new entry will be stored according to mode.

Maximum capacity to store logs will be restricted to 100 000 logs for 'Identified Mode' log format and to 1 000 000 logs for 'Basic Mode' log format

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 the **Host System Interface Specification** document.

Log File size

When the capacity off the internal log file is full, the logging process will stop automatically. Depending on the terminal settings, a WARNING message may be sent to a distant system.

The format of the "Log File Full Warning" message is described in the **Remote Message Specification** document.

Activation key

The administrator can enable or disable the creation of a record for each access request, by using only one configuration key.

Parameter name	Value	Description
transaction_log.logging	0, 1 or 2 (2 – Default)	• The administrator can configure this parameter to select the type of transaction logging that is carried by the terminal. Set "0", to disable transaction logging

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

		Set “1”, to enable access control logging. It means only user access requests (regardless of the outcome), along with access timings and corresponding user details are logged. Set “2”, to enable full logging. Full logs include record of each action performed on terminal.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Sending an Access Control Result Message

Presentation

The administrator can configure the Access and Time Biometric Terminal to send a message which contains the result of the access control, to a distant terminal. It can send the access control result using different channels and different protocols. The administrator can configure the protocol and channel of communicating the access control result.

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 358: Sending access control result message to a distant system

Ports and protocols

The Access and Time Biometric 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 sections that follow.

Please refer to **Remote Message Specification** for more information about the format and the protocol used for sending the access control result messages.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Serial Port (Output only)

Feature/Function name	SIGMA Series SIGMA Extreme Series MorphoWave® Series VisionPass Series	SIGMA Lite Series
Wiegand or Clock & Data protocols (For Serial Communication)	✓	✓
RS485 (Serial Protocol)	✓	✓
RS422 (Serial Protocol)	✓	✗

Protocol selection

Access and Time Biometric 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 administrator through Webserver. Please refer to "*Wiegand Parameter Settings*" under Webserver.

The administrator can activate the Wiegand output by configuring the following parameter:

Parameter name	Value	Description
wiegand.external_port_output_type	0 or 1	The administrator can set the external port output type, by configuring this parameter "0": it indicates external port type is Wiegand.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Clock & Data protocol

The description provided for Wiegand protocol (see previous section) applies to Clock & Data protocol as well.

The sending of the message is conditioned to only one configuration key.

Parameter name	Value	Description
wiegand.external_port_output_type	0 or 1	The administrator can set the external port output type, by configuring this parameter "1": it indicates external port type is clock & data.

RS422/RS485 protocol

The administrator can configure to send the access control result message via RS422/RS485 protocol for Access and Time Biometric Terminal. RS422 is not supported by SIGMA Lite Series terminals. The message is sent irrespective of the access control result. 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 administrator can configure the following parameters. For more details, please refer to the section below.

Parameter name	Value	Description
remote_msg_conf.send_serial_state	0 or 1	The administrator can select remote message sending state over Serial channel, by using this parameter. Select "0", to disable message sending on serial port. Select "1", to enable message sending on serial port.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Ethernet port

Protocol selection

The administrator can configure the terminal to send the access control result messages via an Ethernet link. The protocol could be one of UDP/TCP and TLS/SSL.

Access and Time Biometric Terminal is able to send message to two different distant system: one preferred host (host # 1) and one alternative host (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	The administrator can set a protocol type that will be used for communicating with remote controller host 1, by using this parameter. Set to “0”, for using TCP protocol for communication Set to “1”, for using UDP protocol for communication Set to “2”, for using TLS/SSL over TCP for communication

For details on configuration of other parameters that help in managing the process of sending remote message to access controller, please refer to **Parameters Guide.**

Wi-Fi™ Channel

The administrator can configure the terminal to send the access control result messages via a wireless Wi-Fi™ b/g connection, instead of Ethernet connection. Please refer to “*Wi-Fi™ Network Configuration* Wi-Fi™ Network Configuration” section for more information.

The message format and the protocols supported are the same as for the Ethernet channel: UDP, or TCP or SSL.

WARNING: The terminal cannot be connected through Ethernet and through Wi-Fi™, simultaneously.

Note about Terminal Clock Deviation

The message sent through IP and RS422 or RS485 protocols includes the date/time of access control result.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Please refer to "*Date / Time synchronization*" section for more details.

Section 30 : **Terminal User Interface**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Audio Man Machine Interface

Audible signal

The administrator can tune the volume of the audible signal by tweaking the following configuration key. The terminal can be configured to emit an audio signal, in the event of access being granted or denied or the terminal being tampered, for an instance.

Parameter name	Value	Description
audio.volume	0 to 100	The administrator can set global audio volume that will be played on specific events, by using this parameter (default value is 50).

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Terminal States

In this section, **signal** means popup display, led state change, buzzer change, animation display, guidance MMI…

Identification, Authentication or Multi-factor mode: waiting for biometric capture or a card

In identification mode, the terminal is waiting for presentation of finger or face to 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 simultaneously. Then the terminal is expecting presentation of finger or face to the biometric sensor or a card close to the smartcard reader.

NOTE:
The VisionPass Range terminals in disabled intentional mode never wait for a user's card before starting to capture Biometric data. The biometric data acquisition starts as soon as a user is detected in the biometric area.

The VisionPass Range terminals in active intentional mode enabled wait for a user's card before starting to capture Biometric data. The biometric data acquisition starts as soon a user requests a biometric acquisition (press on a specific button, presentation of a card, ID entering…).

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.

NOTE: VisionPass Range terminals emit no signal / no information while waiting for a face except if a the user guidance MMI via icon or live feedback is activated

Identification: Finger detected, Acquisition of biometric data of the finger is in process

After detection of a finger by the biometric sensor, the terminal emits this signal during the entire biometric data acquisition process. Do not remove the finger while this signal is emitted.

NOTE: VisionPass Range terminals emit no signal while waiting for a face except if a the user guidance MMI via icon or live feedback is activated.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Identification or Authentication: database blank or absent

This signal is emitted when, the activated mode requires a database but the database is either not created or is empty.

NOTE: VisionPass Range terminals emit no signal if no database

Incorrect finger position

The terminal emits this signal when the position of the finger on the biometric sensor is not good enough, for an image capture. Please remove the finger from the biometric sensor and follow the recommendations detailed in "*SIGMA Range Series* Finger Placement Recommendation" section.

NOTE: VisionPass Range terminals emit no signal / no information if face position is incorrect except if the user guidance MMI via icon or live feedback is activated.

Biometric Sensor start up error

The terminal fails to start the biometric sensor. Please reboot the terminal and if the trouble persists after restarting the terminal, 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.

Terminal in Low Consumption Mode

When terminal is in idle mode, a video is played till the configured video play duration. Once Video play duration has elapsed, terminal stops playing video and shifts to Low Consumption Mode indicated by LED blinking. This state is applicable for SIGMA Wide, SIGMA Lite+ and SIGMA Extreme Series and VisionPass terminals.

Maintenance: Biometric Sensor firmware update

This signal is emitted when the biometric Sensor firmware update is in progress. This update occurs at first startup of the terminal after terminal firmware update.

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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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.

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 safely removed from the USB port. The USB Mass Storage key must be removed to complete the maintenance process.

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 authenticated and the access is allowed.

Identification or Authentication - Access denied

The user is not authenticated, or the access is not allowed to the given user (by Time Mask feature or by the Central Access Controller).

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Authentication - Timeout while waiting for finger or face detection by the sensor

Authentication mode only: time-out occurs while waiting for finger or face detection by the sensor.

Finger removed too early

The terminal emits this signal when the finger is removed before the end of biometric data acquisition.

Enrolment

Waiting for biometric detection

The enrolment sequence is launched and the terminal is waiting for a user to place a finger or face.

Acquisition in process

The user has placed his finger or face 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 his finger or his hand or his face 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 finger from the terminal. If acquisition of another finger is required, the terminal will emit the Waiting for finger signal.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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 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.

NOTE: The enrolment on VisionPass Range terminals request only one capture. The enrolment is done in 3 steps: Waiting for biometric detection, acquisition in process and Enrollment completed.

LED – Buzzer Sequence

For MA SIGMA / SIGMA Extreme Series, MorphoWave® Compact, MorphoWave® XP2, VisionPass series

Terminal States	Biometric Sensor backlight	blue LED status	Buzzer
Identification, Authentication or Multi-factor mode: waiting for a finger or a card	OFF		
Authentication mode, after presentation of a card, waiting for a finger or biometric data acquisition of the finger is in progress	Fixed Red		
Identification: Finge detected, Acquisition of biometric data is in process	Fixed Red		
Identification or Authentication: database blank or absent	OFF		

Terminal States	Biometric Sensor backlight	blue LED status	Buzzer
Waiting for distant system command	OFF		
Incorrect finger position	OFF		
Biometric Sensor start up error	OFF		
Maintenance: terminal configuration in process	OFF		
Terminal in Low Consumption Mode	OFF		
Maintenance: Biometric Sensor firmware update	OFF		
Maintenance: USB mass storage key can be removed	OFF		2 medium pitched notes
Anti-tamper alarm	OFF		Low pitched notes
Identification or Authentication - Access granted	Insignificant		1 second high pitched notes
Identification or Authentication - Access denied	Insignificant		1 second low pitched notes
Timeout while waiting for finger or face	Insignificant		1 second low pitched notes
Finger removed too early	OFF		
Waiting for finger or face	Fixed Red		
Acquisition in process	Fixed Red		
Current positioning - Acquisition complete (but not enrolment sequence)	Fixed Red		High 0.5 Sec Beep
Current capture complete – Remove finger from terminal to proceed with next finger	Fixed Red		
Current finger – Acquisition complete (but not enrolment sequence)	Fixed Red		
Enrolment complete	Fixed Red		

NOTE: Only the column “Blue LED status” is applicable for VisionPass terminal.

NOTE: Only the column “Buzer” is applicable for VisionPass SP terminal.

For SIGMA Lite and MorphoWave® SP Series

Action	**LED**						**Buzzer**
	Red	Green	Blue	Yellow	Purple	Cyan	
Default MMI when Database is Empty and only Biometric Trigger is Enabled				√ (Blink)			
Default MMI when Database is Empty and Trigger is not Biometric only			√				
Default MMI when Database is not empty and only Biometric Trigger is Enabled							
Default MMI when Database is not empty and Trigger is not Biometric			√				
Distant Session is Open					√ (Blink)		
Distant Command Cancelled	√						
USB Key Detected							√
USB Script In Progress					√ (Blink)		
USB Script Successful		√					√
USB Script Error	√						√
First Boot up on SIGMA LITE Prox	√		√				
First Boot up on SIGMA LITE MD	√						
First Boot up on SIGMA LITE iClass	√						
Change Key OK		√					√
Change Key Not OK	√						√
Alarm (15 times)	√ (Blink)						√
Access Emergency	√						√
TOM		√					√
Access Granted		√					√
Access Denied	√						√
Access Timeout	√						√
Place Finger Wave your right/left hand				√ (Blink)			
Change Finger/hand		√					
End of Acquisition							√

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Action	**LED**						**Buzzer**
	Red	Green	Blue	Yellow	Purple	Cyan	
Enrolment Complete		√					√
Enrolment Failed	√						√
Missing Data from Card	√						√

Section 31 : **Compatibility Software Applications**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Compatible software applications

Access and Time Biometric Terminals are fully compatible with:

The low level protocol using thrift commands, for more information, please refer to "**Host System Interface Guide**"

Morpho Integrator's Kit (MIK) software development kit (version 6 or later).

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Section 32 : **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 Access and Time Biometric Terminal by 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 Access and Time Biometric Terminal has been installed.

Areas containing combustibles

It is strongly recommended that you do not install your Access and Time Biometric Terminal in the vicinity of gas stations, petroleum processing facilities or any other facility containing flammable or combustible gasses or materials.

Specific precautions for terminals fitted with a contactless smartcard reader

It is recommended to install Access and Time Biometric Terminals equipped with a contactless smartcard reader at a certain distance (> 30cm) from metallic elements such as iron fixations or elevator doors. Performances in terms of reading the contactless badge from a distance will decrease when metallic elements are closer.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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 Access and Time Biometric 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

The terminal clock typically has a +/- 4 sec time deviation, per day 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 Access and Time Biometric Terminal must be synchronized regularly with an external terminal (using the appropriated ILV command)

WARNING: Time deviation is a function of temperature and must be taken care of.

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.

Recommended Conditions for Face Detection

User Face Position

The user should face toward the terminal while identification/authentication.

The user should stand at the distance where terminal can recognize face (not too far or too close).

Lighting Condition

The user shall not be against the light.

The background of the user shall be as neutral as possible (avoid images which could be mixed up with the face)

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Annex 1 : SIGMA Range Series 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 359: 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.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Position of Finger

Finger Height

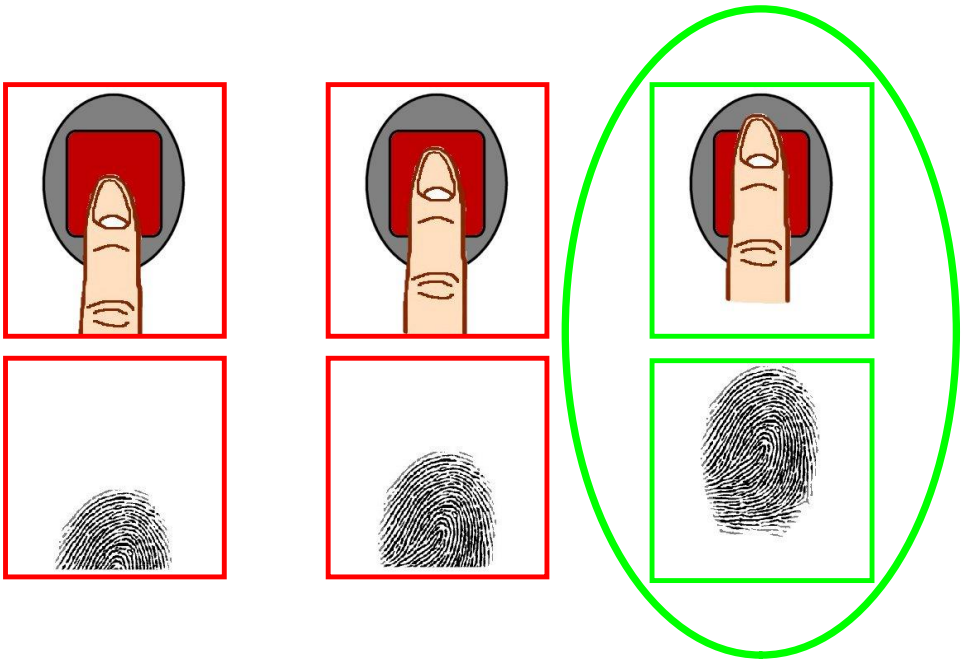


Figure 360: Finger Height

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

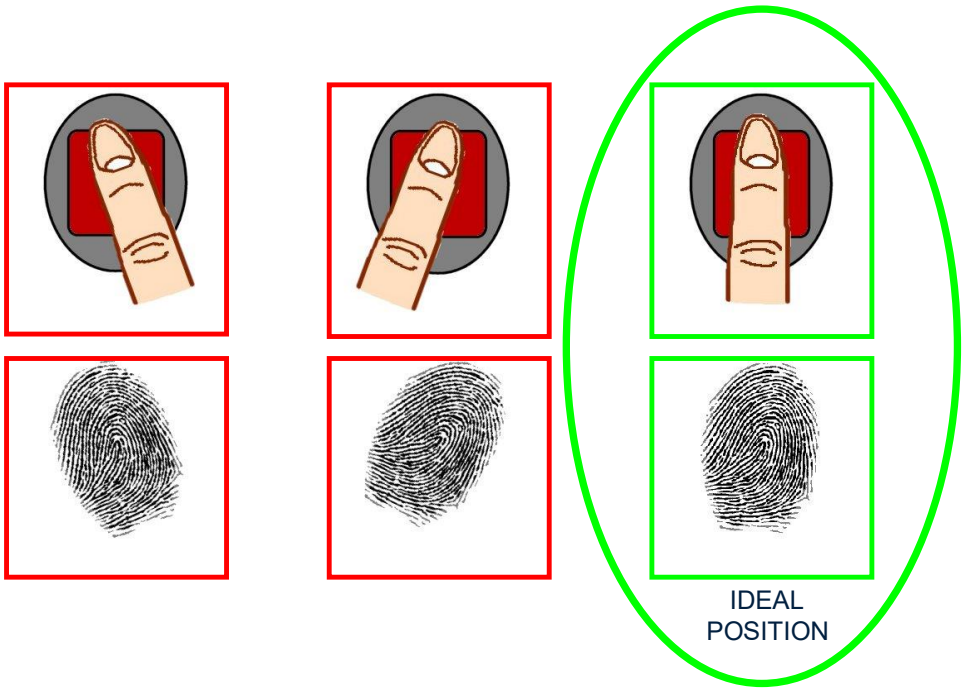


Figure 361: Finger Angle

Incorrect Position:

Do not tilt the finger on right or left side of the sensor

Correct Position:

The finger must be parallel to the sides of the sensor

Finger Inclination

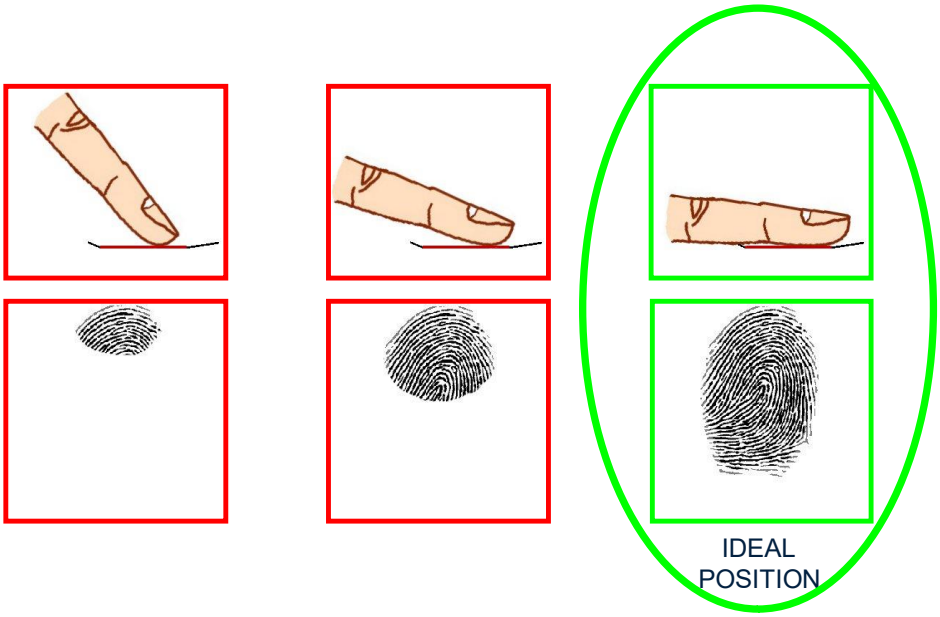


Figure 362: Finger Inclination

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

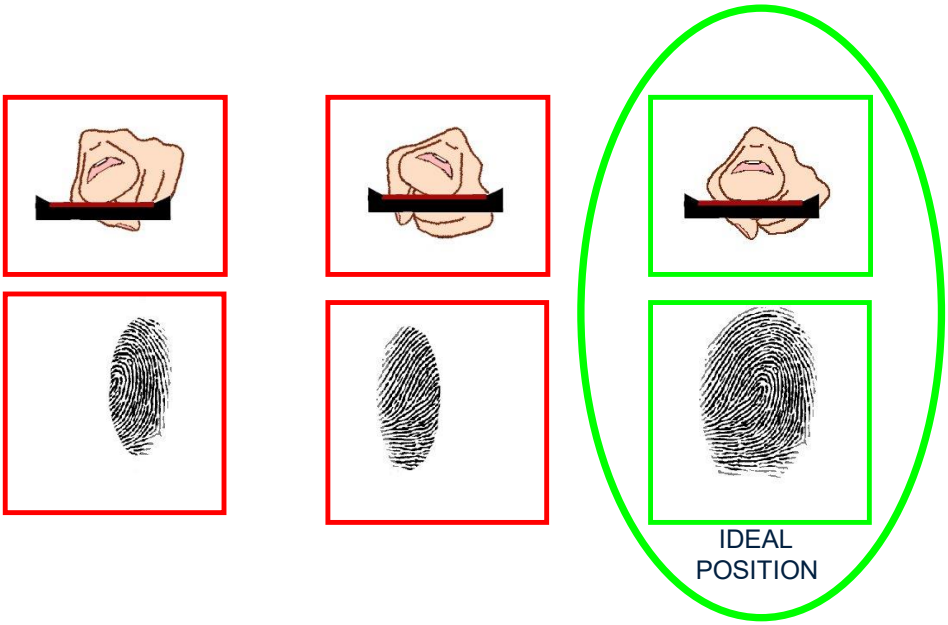


Figure 363: Finger Rotation

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, and from the 2nd phalanx of the finger

Do not press or tense finger to avoid blood vessels constriction

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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 from the 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. Irrespective of the card mode, send ID.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Annex 3 : **Bibliography**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

How to get latest version of the documents

The last version of the documents can be downloaded from our web site at the address below:

www.biometricdevices.idemia.com

(depending on the document, login and password may be required).

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Annex 4 : **Glossary, Acronyms and Abbreviation**

GLOSSARY

Access Controller/Controller: This term is used for centralized access controller. Terminal communicates with controller for decisions regarding access, to the user.

Terminal: This term is used for Access and Time Biometric Terminal, unless explicitly specified.

Device: This term is used for an external device attached to Access and Time Biometric Terminal, such as USB Mass Storage device.

Admin/Administrator: A user who is authorized to manage the settings and user information of a terminal. 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. Access and Time Biometric 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 the intensity or brightness of light. Idemia 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.

Primary Template: This is the template that resides in the first template slot on the smartcard. When verification is initiated, this primary template is the first template that is used in that verification process.

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Secondary Template: This is an optional second template stored on the smartcard 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, present his face 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 present his finger or face to 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 biometric data capture against a stored biometric 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, smartcard, etc.) is necessary to initiate the biometric verification.

Webserver: Webserver is a web-based application embedded in the Access and Time Biometric Terminal. Webserver enables the management of the settings of the terminal from any computer (desktop, laptop or a tablet) equipped with a compatible Internet browser and connected to the same network as the terminal.

SecureAdmin: Client software for managing terminal configuration for Access and Time Biometric Terminal running in L-1 Bioscrypt Legacy mode

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

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 IDEMIA.

T&A: Time and Attendance Mode

MMI: Man Machine Interface

SDAC: Single Door Access Control

GPIO: General Purpose Input Output

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Annex 5 : **Support**

DOCUMENT - REPRODUCTION AND DISCLOSURE PROHIBITED.

Technical Support and Hotline

https://biometricdevices.idemia.com/s/contactus

Web site

For the latest firmware, software, document releases, and news, please check our websites :

https://biometricdevices.idemia.com/s/

February 2026

Head office :

IDEMIA

2, place Samuel de Champlain

92400 Courbevoie France

www.idemia.com