

MorphoAccess[®] SIGMA Series



Administration Guide

COPYRIGHT© 2016 Morpho

Osny, France

WARNING

COPYRIGHT© 2016 All rights reserved.

Information in this document is subject to change without notice and do not represent a commitment on the part of MorphoAccess® SIGMA Series. 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 MorphoAccess® SIGMA Series.

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.

Revision History

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

| Version | Date | Description |
|-----------|---------------|---|
| 01 | November 2013 | First version |
| 02 | May 2014 | Updated - Terminal Rear View Diagram - USB port with a Wi-Fi™ adapter - Default Communication Parameter - Recommendations / SD card |
| 03 | June 2015 | Page #111, 112, 112, 164, 165, 165, 295, 306 are updated. |
| 04 | June 2015 | Updated - Web Server - Smart Card Enrollment - Photo Taking - LCD Configurations |
| 05 | August 2015 | Updated - Configure ELITE Mode - User Enrollment in Database for User PIN |
| 06 | December 2015 | Updated - First Boot Assistance At Next Boot Configuration - Note added for Job Code - Sensor Log Configuration - MiFare Plus Parameter Added |
| 07 | April 2016 | Updated for Learning Phase. Multiple JIRA tickets are corrected. |
| 08 | April 2016 | Add list of supported templates and Contactless cards (Page 32 & 371). |
| 09 | May 2016 | Spelling correction. |

Table of Contents

| | |
|--|-----------|
| WARNING | 2 |
| REVISION HISTORY | 3 |
| SECTION 1 : INTRODUCTION | 23 |
| MorphoAccess® SIGMA Series Terminal | 24 |
| Scope of the document | 25 |
| Safety Instructions | 27 |
| Wiring Recommendations | 27 |
| Europe information | 28 |
| USA information | 28 |
| About Biometrics | 29 |
| About fingerprint biometrics | 29 |
| Acquisition principles | 30 |
| Areas of interest | 30 |
| Ergonomics | 30 |
| Recommended fingers..... | 31 |
| Enrolment process | 31 |
| Template supported | 32 |
| SECTION 2 : DESCRIPTION OF TERMINAL | 33 |
| Interfaces Description | 34 |
| Introduction | 34 |
| Power Supply Interface..... | 37 |
| Administration Interface | 37 |
| Access Control System Synoptic | 39 |
| USB port usage | 40 |
| Plugging a USB Mass storage key | 40 |
| Plugging a USB Wi-Fi™ or 3G adapter..... | 41 |
| Connecting a Computer through USB..... | 42 |
| SECTION 3 : CONNECTING THE TERMINAL TO A PC | 43 |
| General | 44 |
| Why would one connect the terminal to a PC? | 44 |
| Connection methods..... | 44 |
| Network parameter initialization | 45 |
| Point to Point Ethernet Connection | 46 |

- Connection through only one Ethernet switch47**
- Connection through a LAN48**
 - Description..... 48
 - LAN with DNS Server..... 48
 - LAN without DNS Server 49
 - Static IP address (DHCP disabled)..... 49
 - Dynamic IP address (DHCP enabled) 49
- Wi-Fi™ Network configuration50**
 - Requirements..... 50
 - Configuration..... 50
 - Troubleshooting..... 50
- SECTION 4 : TERMINAL CONFIGURATION AND ADMINISTRATION51**
- Understanding MorphoAccess® Configuration.....52**
 - Presentation 52
 - Modifying the value of a parameter 52
 - Notation..... 53
- Configuring a Networked MorphoAccess®54**
 - Introduction 54
 - Network factory settings 55
 - Date/Time settings 55
 - SSL Securing 55
 - Network Wi-Fi™ configuration 56
- MorphoAccess® Terminal Database Management57**
 - General 57
 - Adding a user to the database 57
 - Removing a user from the database 57
 - Database Size 57
- MorphoAccess® Terminal License Management59**
 - User licenses 59
 - Logs licenses 60
 - Communication licenses 61
 - Access Control license..... 61
 - Time and Attendance (T&A) license 62
 - Getting a license for a MorphoAccess® SIGMA Series terminal 63
 - Checking licenses installed in the terminal with license manager application 63
 - Installing a new license..... 66

- Terminal Firmware Upgrade 67**
 - How to get last version of firmware 67
 - How to upgrade the firmware 67
 - Firmware upgrade using a USB Mass Storage Key 67
 - Firmware upgrade tool for expert users 67
- MorphoAccess® SIGMA Series Modes 69**
 - MorphoAccess® 500 or J Series legacy mode 69
 - L-1 Bioscrypt 4G Series legacy mode 69
 - MorphoAccess® SIGMA Series native mode 70
- SECTION 5 : FIRST BOOT ASSISTANT 71**
 - Assistant Initialization 72**
 - Date & Time Configuration 73**
 - Trigger Event 77**
 - Language Configuration 78**
 - Show/Hide Language Icon 80**
 - Ethernet Interface Settings 81**
 - Wi-Fi™ Configuration 83**
 - Protocol Configuration 89**
 - Password Configuration 91**
 - First Boot Assistance At Next Boot Configuration 93**
 - Recover Corrupted Components 94**
- SECTION 6 : ADMINISTRATION MENU 95**
 - Access to Administration Menu 96**
 - User Menu 98**
 - User Enrollment in Database 99
 - User Enrolment in Card 114
 - User Enrolment in Card & Database 116
 - Update User Information 118
 - Authenticate User 121
 - Delete User 123
 - Card Manager 126
 - Multimedia menu 157**
 - Audio Settings 158
 - Video Settings 161
 - Images Settings 164
 - System Menu 167**
 - Terminal Configurations 168

| | |
|---|------------|
| Transaction Log | 189 |
| Miscellaneous Settings | 194 |
| Web Server | 197 |
| Error Log Configuration | 197 |
| Sensor Log Configuration | 200 |
| Communication menu..... | 202 |
| Security recommendation | 203 |
| Ethernet Network Configuration | 203 |
| Wi-Fi™ Network Configuration..... | 206 |
| Configure Hostname..... | 212 |
| Serial Parameters | 213 |
| Security Menu | 216 |
| Biometric Security Settings..... | 217 |
| Anti-Tamper Switch For Terminal Security..... | 231 |
| Network & Communication Security Settings | 235 |
| Additional User Verification Settings..... | 249 |
| Change LCD Password | 252 |
| Additional User Control Settings | 254 |
| USB Menu..... | 260 |
| Format USB Mass Storage device..... | 261 |
| Initialize USB Mass Storage device..... | 263 |
| Import Data into Terminal..... | 265 |
| Export Data in USB Mass Storage Device..... | 271 |
| Information Menu | 280 |
| View Device Details | 281 |
| View Firmware Information | 283 |
| View Sensor Revision Information | 284 |
| View Communication Parameters..... | 285 |
| View Memory Status | 289 |
| View User Status..... | 290 |
| View Transaction Log Status | 291 |
| Reboot Terminal Menu | 292 |
| SECTION 7 : VIDEOPHONE FACILITY | 294 |
| Introduction to Videophone | 295 |
| Configure Video Phone Server..... | 296 |
| Viewing Video Phone Server Details..... | 299 |

| | |
|---|------------|
| Delete Video Phone Server | 300 |
| How User can make Video Call..... | 302 |
| SECTION 8 : TERMINAL CONFIGURATION THROUGH WEBSERVER | 304 |
| Introduction to Webserver | 305 |
| Security recommendation | 306 |
| Tamper Setting for Terminal Security..... | 307 |
| General Purpose Input Output Configuration | 309 |
| Single Door Access Control Settings | 310 |
| Time and Attendance Mode Configuration | 312 |
| Transaction Log Settings | 317 |
| Biometric Security Settings..... | 319 |
| Communication Settings..... | 320 |
| Controller Feedback..... | 325 |
| Date and Time Settings | 328 |
| Wiegand Parameters Settings..... | 330 |
| User Control Configurations | 333 |
| Threat Level Configuration | 337 |
| Event Configurations | 339 |
| Define Access Schedule..... | 340 |
| Define Holiday Schedule | 347 |
| Door Open Schedule Configuration | 351 |
| Complete Configuration (Advanced users only) | 352 |
| Reset Factory Settings | 353 |
| SECTION 9 : ACCESS CONTROL | 355 |
| Access control presentation | 356 |
| Typical architecture of an access control system | 356 |
| Typical access control process..... | 357 |
| Preliminary: adding a biometric template in local database | 358 |
| MorphoAccess® terminal operating modes | 359 |
| Standalone mode or Slave mode..... | 359 |
| Standalone mode: Identification and/or Authentication | 359 |
| Access Control Process in Identification Mode..... | 360 |
| Access Control Process in Authentication Mode | 361 |
| Access Control Process for VIP Users..... | 362 |
| Access Control Result | 363 |
| Information for the User..... | 363 |

| | |
|--|------------|
| <i>Information for the Administrator</i> | 363 |
| <i>Integration in an Access Control System</i> | 363 |
| <i>Access Granted</i> | 364 |
| <i>Access Denied</i> | 364 |
| SECTION 10 : ACCESS CONTROL BY IDENTIFICATION | 365 |
| <i>Identification Mode Description</i> | 366 |
| <i>Identification Process</i> | 366 |
| <i>Access Control by Identification</i> | 366 |
| <i>Result of the access control request</i> | 366 |
| <i>User's Data required in the terminal</i> | 366 |
| <i>Identification Modes (database extension licenses)</i> | 367 |
| <i>Compatibility with Access Control Systems</i> | 367 |
| <i>User Interface</i> | 368 |
| SECTION 11 : ACCESS CONTROL BY AUTHENTICATION | 369 |
| <i>Authentication Process</i> | 370 |
| <i>Introduction</i> | 370 |
| <i>Authentication process</i> | 370 |
| <i>Access control by authentication</i> | 370 |
| <i>Contactless Smart Card</i> | 371 |
| <i>List of contactless cards validated</i> | 371 |
| <i>Authentication Process Options</i> | 373 |
| <i>Manual bypass of biometric control</i> | 373 |
| <i>Automatic bypass of biometric control</i> | 375 |
| <i>Result of access control check</i> | 375 |
| <i>Compatibility with Access Control Systems</i> | 375 |
| <i>Selection of user's contactless card type (MIFARE® and/or DESFire®)</i> | 376 |
| <i>Biometric check, biometric data on user's card</i> | 378 |
| <i>Description</i> | 378 |
| <i>User's data required in the terminal</i> | 378 |
| <i>User's data required on the user's card</i> | 378 |
| <i>Activation key</i> | 378 |
| <i>User Interface</i> | 379 |
| <i>PIN verification - PIN stored on card</i> | 380 |
| <i>Description</i> | 380 |
| <i>User's data required in the terminal</i> | 380 |
| <i>User's data required on the user's card</i> | 380 |

| | |
|---|------------|
| Activation key | 380 |
| User Interface | 381 |
| BIOPIN verification - BIOPIN stored on card..... | 382 |
| Description..... | 382 |
| User's data required in the terminal | 382 |
| User's data required on the user's card | 382 |
| Activation key | 382 |
| User Interface | 383 |
| Biometric check and biometric data in local database | 384 |
| Description..... | 384 |
| User's data required in the terminal | 384 |
| User's data required on the user's card | 384 |
| Activation key | 385 |
| User interface | 385 |
| Authentication with local database: User ID entered from keyboard | 386 |
| Description..... | 386 |
| Activation key | 386 |
| Authentication with local database: ID input from Wiegand or Clock & Data..... | 387 |
| Description..... | 387 |
| Activation key | 387 |
| Wiegand Frame Configuration | 389 |
| Wiegand frame example (26 bits)..... | 390 |
| No biometric check, no User ID check | 391 |
| Description..... | 391 |
| User's data required in the terminal | 391 |
| User's data required on the user's card | 391 |
| Activation key | 392 |
| User Interface | 392 |
| No biometric check, User Identifier in the database..... | 393 |
| Description..... | 393 |
| User's data required in the terminal | 393 |
| User's data required on the user's card | 393 |
| Activation key | 394 |
| User Interface | 395 |
| Authentication process specified by User's card..... | 396 |
| Description..... | 396 |

| | |
|---|------------|
| <i>User's data required in the terminal</i> | 396 |
| <i>User's data required on the user's card</i> | 396 |
| <i>Activation key</i> | 397 |
| <i>User Interface</i> | 397 |
| Allowed format for User's identifier | 399 |
| <i>TLV structured data</i> | 399 |
| <i>Binary Data</i> | 401 |
| SECTION 12 : MULTIFACTOR ACCESS CONTROL MODE | 404 |
| Multi-factor Mode | 405 |
| <i>Description</i> | 405 |
| <i>User Interface</i> | 405 |
| <i>User's data required in the terminal</i> | 405 |
| <i>User's data required on the user's card</i> | 405 |
| <i>Activation keys</i> | 406 |
| SECTION 13 : TIME AND ATTENDANCE MODE | 407 |
| Time and Attendance Synoptic | 408 |
| <i>Normal Mode</i> | 408 |
| <i>Extended Mode</i> | 410 |
| <i>T&A Mode Mandatory or Optional Scenarios</i> | 412 |
| <i>T&A - Mandatory Mode Work Flow Diagram</i> | 413 |
| <i>T&A - Non Mandatory Mode Work Flow Diagram</i> | 414 |
| <i>Note on Terminal Clock Deviation</i> | 415 |
| SECTION 14 : PROXY MODE | 416 |
| Presentation of Proxy (or slave) mode | 417 |
| <i>Process</i> | 417 |
| <i>Local signals</i> | 418 |
| <i>Proxy mode use sample</i> | 419 |
| <i>Proxy mode activation</i> | 419 |
| SECTION 15 : POLLING MODE | 420 |
| Presentation of Polling mode | 421 |
| <i>Process</i> | 421 |
| <i>Polling mode activation</i> | 422 |
| SECTION 16 : MESSAGES SENDING | 423 |
| Principle | 424 |
| Events | 425 |
| Sending Interfaces | 426 |

| | |
|---|------------|
| SECTION 17 : COMPATIBILITY WITH AN ACCESS CONTROL SYSTEM | 427 |
| <i>Internal Relay activation on Access Granted result</i> | 428 |
| Description..... | 428 |
| Activation key | 429 |
| Configuration key | 429 |
| <i>External activation of the internal relay</i> | 430 |
| Description..... | 430 |
| Activation key | 431 |
| Configuration key | 431 |
| <i>Access Request Result Log File</i> | 432 |
| Description..... | 432 |
| Log File management | 432 |
| Log File size..... | 432 |
| Activation key | 433 |
| <i>Sending an Access Control Result Message.....</i> | 434 |
| Presentation | 434 |
| Ports and protocols..... | 434 |
| Serial Port (Output only)..... | 435 |
| Ethernet port | 437 |
| Wi-Fi™ Channel..... | 437 |
| Note about Terminal Clock Deviation..... | 438 |
| SECTION 18 : TERMINAL USER INTERFACE..... | 439 |
| <i>Audio Man Machine Interface.....</i> | 440 |
| Audible signal | 440 |
| Terminal States..... | 441 |
| Access Request Result..... | 446 |
| Enrolment | 447 |
| SECTION 19 : COMPATIBILITY ACCESSORIES, SOFTWARE LICENSES AND SOFTWARE APPLICATIONS..... | 450 |
| <i>Compatible Accessories & Software Licenses</i> | 451 |
| <i>Compatible software applications.....</i> | 452 |
| SECTION 20 : RECOMMENDATIONS | 453 |
| <i>Warning</i> | 454 |
| General precautions | 454 |
| Areas containing combustibles..... | 454 |
| Specific precautions for terminals fitted with a contactless smartcard reader | 454 |

| | |
|--|------------|
| <i>SD card</i> | 455 |
| <i>Ethernet connection</i> | 455 |
| <i>Date / Time synchronization</i> | 455 |
| <i>Cleaning precautions</i> | 455 |
| <i>Recommended Conditions for Face Detection</i> | 456 |
| ANNEX 1 : FINGER PLACEMENT RECOMMENDATION | 457 |
| ANNEX 2 : COMPARISON OF AUTHENTICATION MODE WITH CONTACTLESS CARD | 464 |
| ANNEX 3 : BIBLIOGRAPHY | 467 |
| ANNEX 4 : GLOSSARY, ACRONYMS AND ABBREVIATION | 472 |
| ANNEX 5 : SUPPORT | 476 |

Table of Figures

| | | |
|------------|---|----|
| Figure 1: | Minutiae are classified in two categories i.e. ridge ending and bifurcation..... | 29 |
| Figure 2: | Most Relevant Biometric Data in a Fingerprint..... | 30 |
| Figure 3: | Recommended Fingers for Capture | 31 |
| Figure 4: | MorphoAccess® SIGMA Series Terminal Front View | 35 |
| Figure 5: | MorphoAccess® SIGMA Series Terminal Rear View Diagram | 38 |
| Figure 6: | MorphoAccess® SIGMA Series terminal external USB port | 40 |
| Figure 7: | MorphoAccess® SIGMA Series terminal USB port with a Wi-Fi™ adapter..... | 41 |
| Figure 8: | MorphoAccess® SIGMA Series terminal USB port | 42 |
| Figure 9: | Direct Point to Point Ethernet Connection | 46 |
| Figure 10: | Connection through an Ethernet switch..... | 47 |
| Figure 11: | Connection through LAN..... | 48 |
| Figure 12: | Configuration of a MorphoAccess® SIGMA Series terminal by a Host System . | 54 |
| Figure 13: | Date and Time setting of Terminal from Webserver | 55 |
| Figure 14: | License Manager, adding a MorphoAccess® SIGMA Series terminal | 64 |
| Figure 15: | License Manager, entering an IP address for a MorphoAccess® SIGMA Series terminal | 64 |
| Figure 16: | Licenses installed in a MorphoAccess® SIGMA Series terminal | 65 |
| Figure 17: | Adding a license in a MorphoAccess® SIGMA Series terminal | 66 |
| Figure 18: | First Boot Assistant Screen displayed on Installation | 72 |
| Figure 19: | Configuring Current Date | 73 |
| Figure 20: | Configuring Current Time..... | 74 |
| Figure 21: | Configuring Time Zone | 74 |
| Figure 22: | List of Predefined Time Zones of World | 75 |
| Figure 23: | Custom Time Zone Setting | 75 |
| Figure 24: | Selecting the event(s) that starts access control rights check process | 77 |
| Figure 25: | Configure Language | 78 |
| Figure 26: | Language selection on main screen | 79 |
| Figure 27: | Hide Language Icon | 80 |
| Figure 28: | Ethernet Configuration | 81 |
| Figure 29: | IP Mode Selection | 82 |
| Figure 30: | Selecting available Wi-Fi™ network | 83 |
| Figure 31: | Enter Encryption Key..... | 84 |
| Figure 32: | Success message is displayed showing Wi-Fi™ network is configured | 84 |
| Figure 33: | Connected to Wi-Fi™ network | 84 |
| Figure 34: | Selecting Other Network to set up Wi-Fi™ network manually..... | 85 |
| Figure 35: | WLAN Parameter Configuration | 85 |
| Figure 36: | Setting SSID | 86 |
| Figure 37: | Selecting Encryption Mode | 86 |

| | | |
|------------|---|-----|
| Figure 38: | Define Encryption Key | 87 |
| Figure 39: | Entering in WLAN – IP Configuration | 87 |
| Figure 40: | WLAN – IP Configuration | 88 |
| Figure 41: | Success message is displayed showing Wi-Fi™ network is configured | 88 |
| Figure 42: | Protocol Configuration | 89 |
| Figure 43: | Resetting Device Password | 91 |
| Figure 44: | Entering New Password | 92 |
| Figure 45: | Verifying New Password | 92 |
| Figure 46: | First Boot Configuration Storage Type | 93 |
| Figure 47: | Protected Data Corrupted Error | 94 |
| Figure 48: | Corrupted Components | 94 |
| Figure 49: | Logging in Device | 96 |
| Figure 50: | Entering Password | 97 |
| Figure 51: | Administrator Menu | 97 |
| Figure 52: | User Management Menu | 98 |
| Figure 53: | Entering User Identifier | 99 |
| Figure 54: | Adding user information | 100 |
| Figure 55: | Enter First Name of User | 100 |
| Figure 56: | Enrolling Finger Index | 101 |
| Figure 57: | Select first finger to capture | 101 |
| Figure 58: | Biometric data capture | 102 |
| Figure 59: | Set Duress Finger as ON | 102 |
| Figure 60: | Assigning Access Rights | 103 |
| Figure 61: | Enter User PIN | 104 |
| Figure 62: | Setting Job Code | 104 |
| Figure 63: | Setting Job Code in user profile | 105 |
| Figure 64: | Assigning Access Schedule | 105 |
| Figure 65: | Enrolment Information Screen – Configuring parameters | 107 |
| Figure 66: | Configuring Dynamic Message for User | 108 |
| Figure 67: | Setting duration for dynamic message | 108 |
| Figure 68: | Configuring Dynamic Message for User | 108 |
| Figure 69: | Configuring Door Open Time Out | 109 |
| Figure 70: | Enrolment Information Screen | 109 |
| Figure 71: | Defining User Rule | 110 |
| Figure 72: | Defining User Rule – Trigger Source | 110 |
| Figure 73: | Defining User Rule – Record Reference Source | 111 |
| Figure 74: | Defining User Rule – Control Mode | 112 |
| Figure 75: | Defining User Rule | 112 |
| Figure 76: | Select Card Data Format | 114 |
| Figure 77: | Enrollment Finger Index in Card | 115 |
| Figure 78: | Select Card Data Format | 116 |
| Figure 79: | Selecting Search Criteria | 118 |

| | | |
|-------------|--|-----|
| Figure 80: | Entering first digits of the searched User ID | 118 |
| Figure 81: | Selecting User ID | 119 |
| Figure 82: | Enrolment Information screen is displayed for editing | 119 |
| Figure 83: | Authenticate User | 121 |
| Figure 84: | Entering User ID for authentication..... | 121 |
| Figure 85: | Deleting User..... | 123 |
| Figure 86: | Searching User ID | 123 |
| Figure 87: | Deleting User ID | 124 |
| Figure 88: | A confirmation message pop up for delete | 124 |
| Figure 89: | Select Delete action | 125 |
| Figure 90: | Confirm All User Deletion | 125 |
| Figure 91: | Accessing Card Manager | 126 |
| Figure 92: | Renewal of User Card..... | 127 |
| Figure 93: | Select Card Data Format | 128 |
| Figure 94: | Select search criteria..... | 128 |
| Figure 95: | Entering User ID to be searched | 129 |
| Figure 96: | Selecting User ID | 129 |
| Figure 97: | A success message is displayed showing user is stored in card | 130 |
| Figure 98: | Encoding Administrator card | 131 |
| Figure 99: | Select Card Type to be encoded | 132 |
| Figure 100: | Administrator card is encoded..... | 132 |
| Figure 101: | Encoding Visitor Card | 133 |
| Figure 102: | User ID for Visitor Card | 134 |
| Figure 103: | Smartcard Read Profile | 135 |
| Figure 104: | Smartcard Read Profile_Multi..... | 135 |
| Figure 105: | Smartcard Read Profile_iClass | 136 |
| Figure 106: | Smartcard Encode Profile | 137 |
| Figure 107: | Smartcard Encode Profile | 137 |
| Figure 108: | Selecting Card Type..... | 139 |
| Figure 109: | Generating Site Key..... | 140 |
| Figure 110: | Success message is displayed showing site key is generated in the terminal . | 140 |
| Figure 111: | Resetting keys in selected cards | 141 |
| Figure 112: | Setting No. of Start Block | 144 |
| Figure 113: | Keyset configuration | 145 |
| Figure 114: | Confirming reset key action | 146 |
| Figure 115: | Site Key is reset successfully | 146 |
| Figure 116: | Selecting Enroll User ID Format | 147 |
| Figure 117: | Selecting Enroll User ID Format | 147 |
| Figure 118: | Configuring Application ID and File ID | 150 |
| Figure 119: | Set Key Offset for iCLASS® cards | 151 |
| Figure 120: | Set Key Offset..... | 152 |
| Figure 121: | Configure Active Pages for iCLASS® cards..... | 153 |

| | | |
|-------------|---|-----|
| Figure 122: | Enter Active Pages..... | 154 |
| Figure 123: | Reset card..... | 155 |
| Figure 124: | Success message is displayed showing card is reset successfully | 156 |
| Figure 125: | Multimedia Menu | 157 |
| Figure 126: | Uploading Audio File in device..... | 159 |
| Figure 127: | Confirmation Pop-up..... | 159 |
| Figure 128: | Success message is displayed | 160 |
| Figure 129: | Uploading Video File in device | 161 |
| Figure 130: | Confirmation Pop-up..... | 162 |
| Figure 131: | Success message is displayed | 162 |
| Figure 132: | Uploading Image File in device | 165 |
| Figure 133: | Confirmation Pop-up..... | 165 |
| Figure 134: | Success message is displayed | 166 |
| Figure 135: | Image uploaded is displayed as wallpaper | 166 |
| Figure 136: | System Menu | 167 |
| Figure 137: | Reset Factory Default Settings..... | 168 |
| Figure 138: | Select Items to reset | 168 |
| Figure 139: | Confirmation message displayed..... | 169 |
| Figure 140: | Configuring Time Zone | 170 |
| Figure 141: | SDC Parameters configuration..... | 174 |
| Figure 142: | Selecting GPIO State | 174 |
| Figure 143: | Configuring Parameters in “SDC Mode” | 175 |
| Figure 144: | Selecting TOM State as On..... | 176 |
| Figure 145: | Setting TOM Duration | 177 |
| Figure 146: | Enabling Tamper | 178 |
| Figure 147: | Tamper Parameters Configuration | 179 |
| Figure 148: | LCD Brightness adjustment..... | 180 |
| Figure 149: | LCD Brightness adjustment..... | 181 |
| Figure 150: | Disable Sensor in Idle Mode | 182 |
| Figure 151: | Configuring Idle Screen Status | 183 |
| Figure 152: | Video Play Brightness Control..... | 184 |
| Figure 153: | Configuring Idle Screen Timeout..... | 185 |
| Figure 154: | Infinite Video Play on idle screen..... | 186 |
| Figure 155: | Setting Video Play Duration | 187 |
| Figure 156: | Selecting Transaction Logging Mode | 190 |
| Figure 157: | Setting Delete Log Status | 191 |
| Figure 158: | Defining number of logs to be deleted | 192 |
| Figure 159: | Deleting Transaction logs..... | 193 |
| Figure 160: | Terminal Global Volume | 194 |
| Figure 161: | Set Global Device Volume | 194 |
| Figure 162: | Enable AZERTY Keyboard | 196 |
| Figure 163: | AZERTY keypad..... | 196 |

| | | |
|-------------|---|-----|
| Figure 164: | Web Server..... | 197 |
| Figure 165: | Select Error Log Configuration | 198 |
| Figure 166: | Enable Error Logging | 199 |
| Figure 167: | Setting Error Log Debug Level | 199 |
| Figure 168: | Communication Menu | 202 |
| Figure 169: | Selecting Ethernet-Network Configuration | 203 |
| Figure 170: | Ethernet Configuration | 204 |
| Figure 171: | IP Mode Selection | 204 |
| Figure 172: | Configuring IP Address under Static IP Mode | 205 |
| Figure 173: | Selecting available Wi-Fi™ network..... | 206 |
| Figure 174: | Enter Encryption Key..... | 207 |
| Figure 175: | Success message is displayed showing Wi-Fi™ network is configured | 207 |
| Figure 176: | Connected to Wi-Fi™ network | 207 |
| Figure 177: | Selecting Other Network to set up Wi-Fi™ network manually..... | 208 |
| Figure 178: | WLAN Parameter Configuration | 208 |
| Figure 179: | Setting SSID | 209 |
| Figure 180: | Selecting Encryption Mode | 209 |
| Figure 181: | Define Encryption Key..... | 210 |
| Figure 182: | Entering in WLAN – IP Configuration | 210 |
| Figure 183: | WLAN – IP Configuration | 211 |
| Figure 184: | Success message is displayed showing Wi-Fi™ network is configured | 211 |
| Figure 185: | Configuring Hostname | 212 |
| Figure 186: | Defining Baud Rate..... | 213 |
| Figure 187: | Select Baud Rate | 214 |
| Figure 188: | Selecting Communication Type | 214 |
| Figure 189: | Enter Net ID..... | 215 |
| Figure 190: | Security Menu | 216 |
| Figure 191: | Configuring the events on which authentication/identification is triggered .. | 217 |
| Figure 192: | Set Duress Mode | 219 |
| Figure 193: | Setting Biometric Check Mode | 220 |
| Figure 194: | Selecting Biometric Matching Strategy..... | 222 |
| Figure 195: | Biometric Time Out..... | 224 |
| Figure 196: | Setting PIN Check Mode..... | 225 |
| Figure 197: | Setting number of PIN Check Attempts..... | 226 |
| Figure 198: | Setting PIN Check Timeout..... | 227 |
| Figure 199: | Setting Security Threshold | 230 |
| Figure 200: | Authorized IP addresses Configuration | 235 |
| Figure 201: | Authorized IP addresses Mode selection..... | 236 |
| Figure 202: | Adding IP for authorization | 236 |
| Figure 203: | Add IP address..... | 237 |
| Figure 204: | A success message is displayed showing IP Address is added successfully..... | 237 |
| Figure 205: | Entering IP Range for authorizing | 238 |

| | | |
|-------------|---|------------------------------------|
| Figure 206: | Viewing authorized IP Addresses..... | 239 |
| Figure 207: | Viewing IP Address Range..... | 239 |
| Figure 208: | Deleting an IP Address..... | 240 |
| Figure 209: | Delete an IP Address Ranges..... | 241 |
| Figure 210: | SSL Configuration..... | 244 |
| Figure 211: | Configuring SSL Mode and parameters..... | 245 |
| Figure 212: | Entering Secure Communication Port..... | 245 |
| Figure 213: | Selecting Communication Port..... | 246 |
| Figure 214: | Entering Communication Port..... | 246 |
| Figure 215: | Configuring TCP Channels..... | 247 |
| Figure 216: | Enabling/Disabling RS422/RS485 Serial Chanel..... | 248 |
| Figure 217: | Addition User Verification..... | 249 |
| Figure 218: | Additional User Verification Timeout..... | 250 |
| Figure 219: | Additional User Verification Timeout..... | 251 |
| Figure 220: | Resetting Device Password..... | 252 |
| Figure 221: | Entering New Password..... | 253 |
| Figure 222: | Verifying New Password..... | 253 |
| Figure 223: | Additional User Control..... | 254 |
| Figure 224: | Enable or Disable Face detection mode..... | 255 |
| Figure 225: | User Rule Check..... | 259 |
| Figure 226: | USB Menu in MorphoAccess® SIGMA Series Terminal..... | 260 |
| Figure 227: | Formatting USB Mass Storage device..... | 261 |
| Figure 228: | Confirmation message pop-up..... | 261 |
| Figure 229: | Success Message of USB Mass Storage device Formatted..... | 262 |
| Figure 230: | Initialize USB Mass Storage device..... | 263 |
| Figure 231: | A confirmation message is displayed..... | 264 |
| Figure 232: | Importing User Database..... | 266 |
| Figure 233: | Selecting file to be imported in the terminal..... | 266 |
| Figure 234: | Confirmation message to import User Database..... | 267 |
| Figure 235: | Enter password..... | 267 |
| Figure 236: | Success message of user data imported is displayed..... | 268 |
| Figure 237: | Importing Language file..... | 269 |
| Figure 238: | Selecting Language file to import..... | 269 |
| Figure 239: | Confirm import action..... | 270 |
| Figure 240: | A success message is displayed showing language file is imported..... | 270 |
| Figure 241: | Exporting transaction logs into USB Mass Storage Device..... | 272 |
| Figure 242: | Selecting a file format for exporting transaction logs..... | 272 |
| Figure 243: | A confirmation message pop-up..... | 273 |
| Figure 244: | A success message is displayed showing transaction log is exported..... | 273 |
| Figure 245: | Transaction Log in .CSV Format Sample..... | 274 |
| Figure 246: | Web Server..... | Erreur ! Signet non défini. |
| Figure 247: | Exporting data into USB Mass Storage Device..... | 276 |

| | | |
|-------------|---|-----|
| Figure 248: | A confirmation message pop-up..... | 276 |
| Figure 249: | A success message is displayed showing error log is exported | 277 |
| Figure 250: | Exporting data into USB Mass Storage Device..... | 278 |
| Figure 251: | A confirmation message pop-up..... | 278 |
| Figure 252: | Enter Passphrase..... | 279 |
| Figure 253: | A success message is displayed showing error log is exported | 279 |
| Figure 254: | Information Menu..... | 280 |
| Figure 255: | View Device Information..... | 281 |
| Figure 256: | View Device Regulatory Information | 281 |
| Figure 257: | MorphoAccess® SIGMA Series Terminal Firmware Version information..... | 283 |
| Figure 258: | Biometric Sensor data | 284 |
| Figure 259: | Selecting communication network | 285 |
| Figure 260: | Viewing information of Ethernet network..... | 286 |
| Figure 261: | Viewing information of GPRS/GSM network..... | 286 |
| Figure 262: | Viewing Serial Protocol Configuration | 287 |
| Figure 263: | View Hostname of the terminal..... | 288 |
| Figure 264: | Memory Status of the device is displayed | 289 |
| Figure 265: | View User Status | 290 |
| Figure 266: | Transaction Log Status is displayed | 291 |
| Figure 267: | Reboot Device | 292 |
| Figure 268: | Confirmation Message To Return to Home Screen | 293 |
| Figure 269: | Video Phone Call Flow Diagram sample | 295 |
| Figure 270: | Adding a Server for Video Phone | 296 |
| Figure 271: | Enter Server Name | 297 |
| Figure 272: | Enter Server IP..... | 297 |
| Figure 273: | Entering Server Port..... | 298 |
| Figure 274: | Videophone Server is added successfully | 298 |
| Figure 275: | Viewing Video Phone Server Parameters | 299 |
| Figure 276: | Deleting Video Phone Server | 300 |
| Figure 277: | Video Server Deleted Success Message..... | 300 |
| Figure 278: | Home Screen when NO VOIP profile is configured..... | 301 |
| Figure 279: | Making Video Call | 302 |
| Figure 280: | Select Server to make Video Call | 303 |
| Figure 281: | Making Video Call | 303 |
| Figure 282: | Homepage of Web Server | 305 |
| Figure 283: | Tamper Settings through Webserver..... | 307 |
| Figure 284: | GPIO Settings through Webserver | 309 |
| Figure 285: | SDAC Settings on Webserver | 310 |
| Figure 286: | Normal Time and Attendance mode | 313 |
| Figure 287: | Extended Time and Attendance mode | 314 |
| Figure 288: | User Interface on Terminal | 315 |
| Figure 289: | Time and Attendance UI in Normal mode | 315 |

| | | |
|-------------|---|-----|
| Figure 290: | Time and Attendance UI in Normal mode with Icons..... | 315 |
| Figure 291: | Time and Attendance UI in Extended mode | 316 |
| Figure 292: | Settings for Transaction Log..... | 317 |
| Figure 293: | Biometric Security Setting through Webserver | 319 |
| Figure 294: | Network parameters settings through Webserver..... | 321 |
| Figure 295: | Configuring Wi-Fi™ Network..... | 323 |
| Figure 296: | Configuring Wi-Fi™ Network manually | 323 |
| Figure 297: | Controller Feedback Settings | 325 |
| Figure 298: | Configuring Date and Time of Terminal from Webserver | 328 |
| Figure 299: | Setting Custom Time Zone from Webserver | 329 |
| Figure 300: | Wiegand Settings through Webserver..... | 331 |
| Figure 301: | User Control Configurations from Webserver | 333 |
| Figure 302: | Configuring TTL Based Threat Level, using Webserver interface | 337 |
| Figure 303: | Configuring Command Based Threat Level, using Webserver interface | 338 |
| Figure 304: | Events Monitoring Configuration..... | 339 |
| Figure 305: | Adding Access Schedule | 341 |
| Figure 306: | Adding Access Schedule | 342 |
| Figure 307: | Editing Access Schedule | 344 |
| Figure 308: | Editing Access Schedule | 345 |
| Figure 309: | Deleting an Access Schedule..... | 346 |
| Figure 310: | Deleting an Access Schedule..... | 346 |
| Figure 311: | Creating a Holiday Schedule | 347 |
| Figure 312: | Creating a Holiday Schedule | 348 |
| Figure 313: | Editing Holiday Schedule..... | 349 |
| Figure 314: | Editing Holiday Schedule..... | 349 |
| Figure 315: | Deleting a Holiday Schedule | 350 |
| Figure 316: | Deleting a Holiday Schedule | 350 |
| Figure 317: | Door Open Schedule Configuration | 351 |
| Figure 318: | Parameter Configuration Screen on Webserver..... | 352 |
| Figure 319: | Reset Factory Settings Screen on Webserver | 353 |
| Figure 320: | Typical access control system architecture | 356 |
| Figure 321: | Access Control Flow Diagram when Terminal is in Identification Mode | 360 |
| Figure 322: | Access Control Flow Diagram in Authentication Mode | 361 |
| Figure 323: | Access Granted Diagram | 364 |
| Figure 324: | Access Denied diagram | 364 |
| Figure 325: | Identification Mode | 368 |
| Figure 326: | Users trigger the authentication process by showing their card | 370 |
| Figure 327: | Authentication with user's fingerprints on contactless card..... | 379 |
| Figure 328: | Authentication with user's PIN Code and fingerprints on contactless card | 381 |
| Figure 329: | Authentication with user's BIOPIN on contactless card | 383 |
| Figure 330: | Authentication with biometric check, reference in database | 385 |
| Figure 331: | Authentication with User ID entered from Keyboard and biometric check.... | 386 |

| | | |
|-------------|--|-----|
| Figure 332: | Authentication without biometric check and with User ID check in card..... | 392 |
| Figure 333: | Authentication without biometric control, and with the user login | 395 |
| Figure 334: | Authentication process specified by user's card | 397 |
| Figure 335: | Using a Wiegand frame as User ID..... | 403 |
| Figure 336: | Multi-factor mode (identification or authentication)..... | 405 |
| Figure 337: | Time and Attendance Screen in Normal Mode | 408 |
| Figure 338: | Time and Attendance Screen in Extended Mode 1x16 | 410 |
| Figure 339: | Time and Attendance Screen in Extended Mode 2x8..... | 410 |
| Figure 340: | Time and Attendance in Mandatory Mode Workflow Diagram | 413 |
| Figure 341: | Time and Attendance in Non-Mandatory Mode Workflow Diagram..... | 414 |
| Figure 342: | PROXY sample with a remote Identification process | 419 |
| Figure 343: | Using the internal relay on the MorphoAccess® SIGMA Series terminal | 428 |
| Figure 344: | Internal relay activated by LED 1 signal | 430 |
| Figure 345: | Sending access control result message to a distant system | 434 |
| Figure 346: | Most Relevant Biometric Data in a Fingerprint | 458 |
| Figure 347: | Finger Height..... | 459 |
| Figure 348: | Finger Angle | 460 |
| Figure 349: | Finger Inclination | 461 |
| Figure 350: | Finger Rotation..... | 462 |

Section 1 : Introduction

MorphoAccess® SIGMA Series Terminal

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

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

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

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

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

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

Scope of the document

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

| Terminal Series | Terminal Name | Biometrics | Contactless smartcard reader | | | Outdoor |
|-------------------------------|--------------------------------------|------------|------------------------------|-----------------------------|-----------|---------|
| | | | iCLASS® iCLASS® SE | MIFARE® DESFire® NFC® | Prox ® | |
| MorphoAccess® SIGMA Series | MorphoAccess® SIGMA | ✓ | | | | |
| | MorphoAccess® SIGMA WR | ✓ | | | | ✓ |
| | MorphoAccess® SIGMA iCLASS® | ✓ | ✓ | | | |
| | MorphoAccess® SIGMA iCLASS® WR | ✓ | ✓ | | | ✓ |
| | MorphoAccess® SIGMA Multi | ✓ | | ✓ | | |
| | MorphoAccess® SIGMA Multi WR | ✓ | | ✓ | | ✓ |
| | MorphoAccess® SIGMA Prox | ✓ | | | ✓ | |
| | MorphoAccess® SIGMA Prox WR | ✓ | | | ✓ | ✓ |

NOTE: Here, WR indicates terminal is Weather Resistant.

The document discusses about the MorphoAccess® SIGMA Series terminal capabilities, and all the configurations done in the terminal.

An administrator can learn about Access Control Processes, Compatibility with access control systems, Time & Attendance mode and how terminal is configurable from Webserver, refer *“Terminal Configuration through Webserver”*.

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

Safety Instructions

The installation of this product should be made by a qualified service Person and should comply with all local regulations.

It is strongly recommended to use a class II power supply at 12V [9V-16V] and 1. min in conformity with Safety Electrical Low Voltage (SELV). The 12V power supply cable length should not exceed 10 meters.

This product is intended to be installed with a power supply complying with EN60950, in accordance with the NEC Class 2 requirements; or supplied by a listed EN60950 external Power Unit marked Class 2, Limited Power source, or LPS and rated 12VDC, 1A minimum.

In case of building-to-building connection it is recommended to connect 0V to ground. Ground cable must be connected with the terminal block 0V GND.

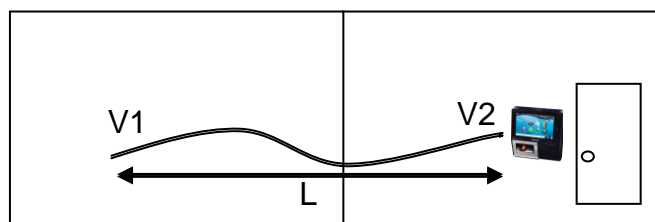
NOTE that all connections of the MorphoAccess® SIGMA Series terminal described hereafter are of SELV (Safety Electrical Low Voltage) type.

Wiring Recommendations

Morpho recommends using a gauge AWG20 for 12V power supply when POE supply is not used.

For information, this table shows the maximum weakening voltage observed on the terminal MorphoAccess® SIGMA Series:

| Gauge AWG | Diameter (mm) | Maximum weakening @ 1m (V) | Maximum weakening @ 5m (V) | Maximum weakening @ 10m (V) |
|-----------|---------------|----------------------------|----------------------------|-----------------------------|
| 20 | 0.812 | 0.0333 | 0.1665 | 0.333 |
| 22 | 0.644 | 0.05295 | 0.26475 | 0.5295 |
| 24 | 0.511 | 0.0842 | 0.421 | 0.842 |
| 26 | 0.405 | 0.134 | 0.67 | 1.34 |



Weakening = loss of power due to wire resistance and its length

$$V2 = V1 - \text{Weakening}$$

Europe information

Morpho hereby declares that the MorphoAccess® SIGMA Series terminal has been tested and found compliant with following listed standards: EN302 291-2 V.1.1.1 (2005-07) + recommendation 1999/519/CE with standard EN 50364; EN 301 489-3 V.1.4.1 (02), and low voltage Directive 2006/95/CE: CEI60950-1:2005 2nd edition.

USA information



This terminal complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this terminal may not cause harmful interference, and (2) this terminal must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Responsible Party:

SAFRAN Morpho,
11, boulevard Gallieni
92130 Issy-les-Moulineaux – France

NOTE: *This equipment has been tested and found to comply with the limits for a Class B digital terminal, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:*

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

Shielded cables must be used with this unit to ensure compliance with category B FCC restrictions.

About Biometrics

About fingerprint biometrics

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

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

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

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

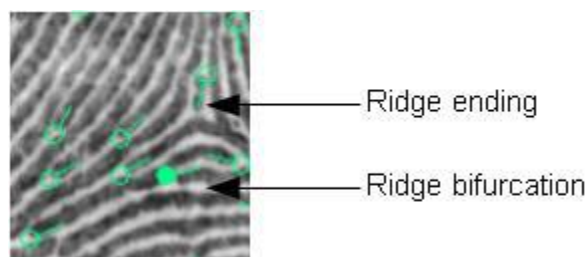


Figure 1: Minutiae are classified in two categories i.e. ridge ending and bifurcation

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

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

Acquisition principles

Areas of interest

The terminal is designed to capture the area containing the most useful biometric data. In fingerprints, this is usually at the centre of the first phalanx.

This is illustrated in the figure below:

Area containing
the maximum
information



Figure 2: Most Relevant Biometric Data in a Fingerprint

Ergonomics

Image acquisition is performed with CMOS camera. The optical imaging method depends on the kind of biometric data to be acquired. The fingerprint imaging process requires finger's first phalanx (fingerprint area, see Figure 2) to be in contact with the corresponding sensing area (square portion of the transparent surface). A finger tip guide has been designed to help user to place the first phalanx of the chosen finger in the centre of the fingerprint imaging area.

Recommended fingers

Our terminals have been designed for the use of index (fore), middle and ring fingers. Among these, we advise people to use preferably the middle finger, which is usually the most suitable, or the fore finger as a second option. The ring finger indeed is not recommended for those who have short fingers (see Figure 3).



Figure 3: Recommended Fingers for Capture

Enrolment process

The level of care taken during enrolment phase will impact all the next steps of the biometric recognition chain.

So it is absolutely necessary to teach individuals during the enrolment phase how to use properly the terminal according to the rules stated below, in order to acquire the best image quality. This will result at the end in the best quality of service.

It should be noted that the enrolment of a second finger gives a good alternative when the user is unable to show the first finger (holding an object, injured or dirty finger, gloved, etc.).

It is recommended to enroll as 1st finger, the one that the user will present most spontaneously.

The finger placement rules are detailed in "[Finger Placement Recommendation](#)".

Template supported

Morpho terminals are able to manage external templates. Find below the list of supported template formats

Morpho private fingerprint template formats

PK_COMPV2, fingerprint template format (minutiae).

PK_MAT, little endian fingerprint template format (minutiae).

PK_LITE, fingerprint template format (minutiae).

Morpho private multimodal template formats

PK_FVP multimodal template format.

L-1 Bioscrypt private fingerprint template formats

TEM from 4G, fingerprint template format (pattern) (only used for 1/1 matching)

VUR from 4G, fingerprint template format (pattern) (only used for 1/1 matching)

BUR from 4G, fingerprint template format (pattern and minutiae) (used for 1/1 and 1/N matching)

Public fingerprint template formats

ANSI INCITS 378-2004, fingerprint template format

ISO/IEC 19794-2 2004, Finger Minutiae Record

ISO/IEC 19794-2 2004, Finger Minutiae Card Record:

- Normal Size
- Compact Size
- Compact Size, minutiae ordered by Ascending Angle

MINEX_A, fingerprint template format

DIN V66400, Compact Size fingerprint template format (minutiae)

DIN V66400, Compact Size fingerprint template format (minutiae ordered by Ascending Angle)

Section 2 : Description of Terminal

Interfaces Description

Introduction

The MorphoAccess® SIGMA Series Installation Guide describes precisely each interface and connection procedure.

All connections of the MorphoAccess® SIGMA Series terminal described hereafter are of SELV (Safety Electrical Low Voltage) type.

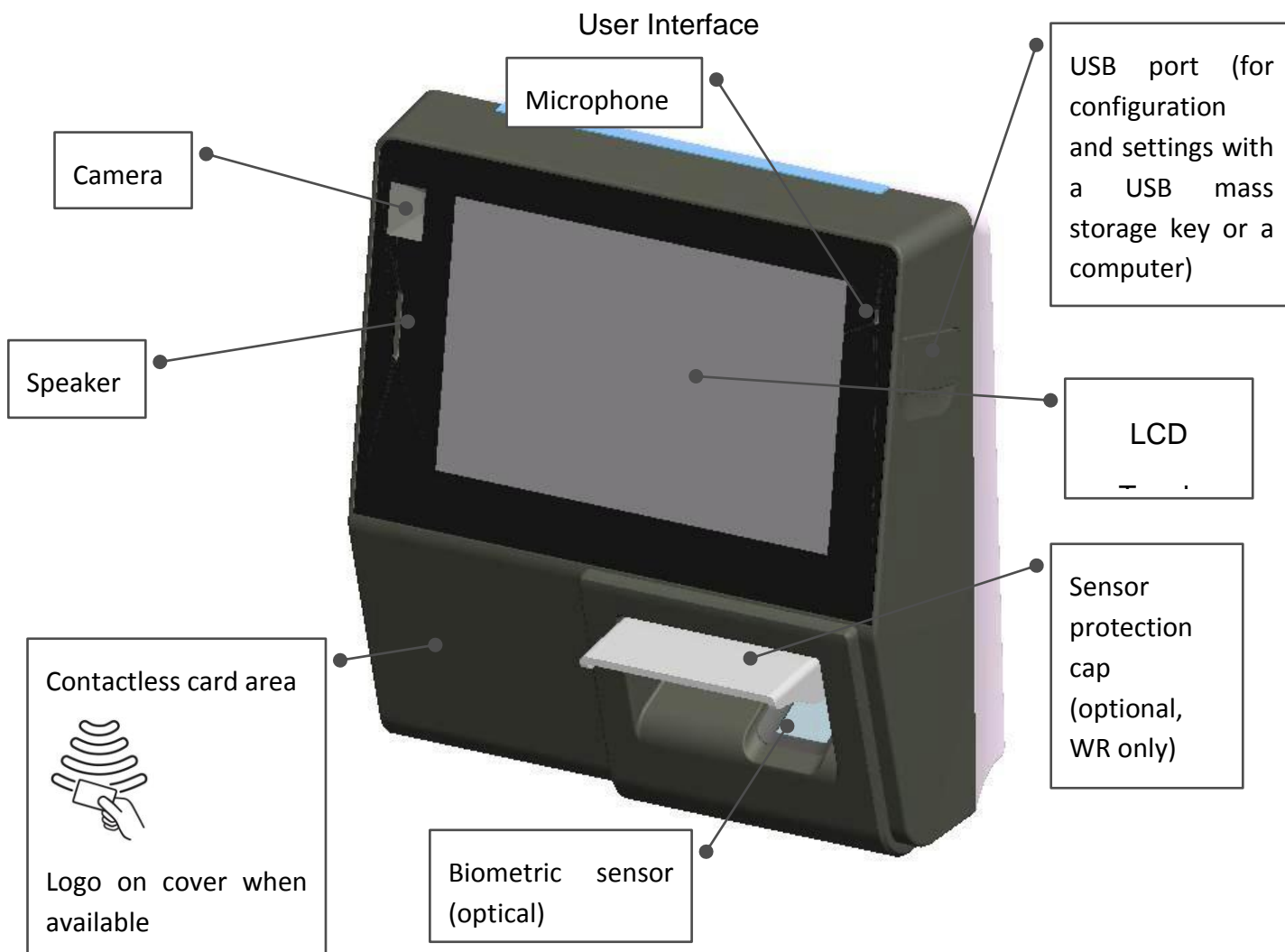


Figure 4: MorphoAccess® SIGMA Series Terminal Front View

The MorphoAccess® SIGMA Series terminals offer a simple and ergonomic man-machine interface designed for access control based on Fingerprint/Face recognition technology. A terminal consists (refer above figure):

1. Contactless card reader (MIFARE® and DESFire®)
2. A high quality optical scanner to capture finger biometric data
3. USB port (for configuration and settings with a USB mass storage key or a computer)
4. Sensor protection cap (optional, WR (Weather Resistant) terminals only)
5. Microphone
6. Speaker
7. Front camera
8. LCD / Touch panel

Power Supply Interface

POE and external power supply are not used at the same time: if both power supplies are used, priority is given to external power supply. If external power supply is shut down, switch to POE without reboot is not guaranteed.

External power supply

- Must comply with CEE/EEC EN60950 standard
- It is strongly recommended to use a class II power supply at 12V-24V and 1A min (at 12V)
- Could be provided by a 12 Volts Wiegand power supply, which complies with the Security Industry Association's Wiegand standard March 1995

Power over Ethernet

MorphoAccess® SIGMA Series terminal's power supply can also be provided by the Ethernet using RJ45 connection (Power Over Ethernet mode).

When the terminal is connected to the network by the RJ45 connector (ref RJ45/POE on MorphoAccess® SIGMA Series Terminal Rear View Diagram), it allows either the power supply over the Data pins or over the spare pins,

But when the terminal is connected to the network by the Ethernet connector block (Figure 5), only power supply over the data pins is possible.

Please contact an administrator network administrator to know which POE mode is provided by the network.

Hardware reset button

A hardware reset button (ref Figure 5) executes, when pressed, a power down/power up sequence and can therefore be used to force a full terminal restart (hardware and software).

Administration Interface

The terminal provides several ports for its management (Refer Figure 5):

- a RJ45 Ethernet connector (LAN 10/100 Mbps, using TCP or SSL protocol),
- a 5 wires Ethernet connector block (LAN 10/100 Mbps, using TCP or SSL protocol),
- a USB host port, to be used to plug a Wi-Fi™ USB adapter, or a 3G USB adapter
- Or a USB mass storage key, to execute punctual and limited modifications.

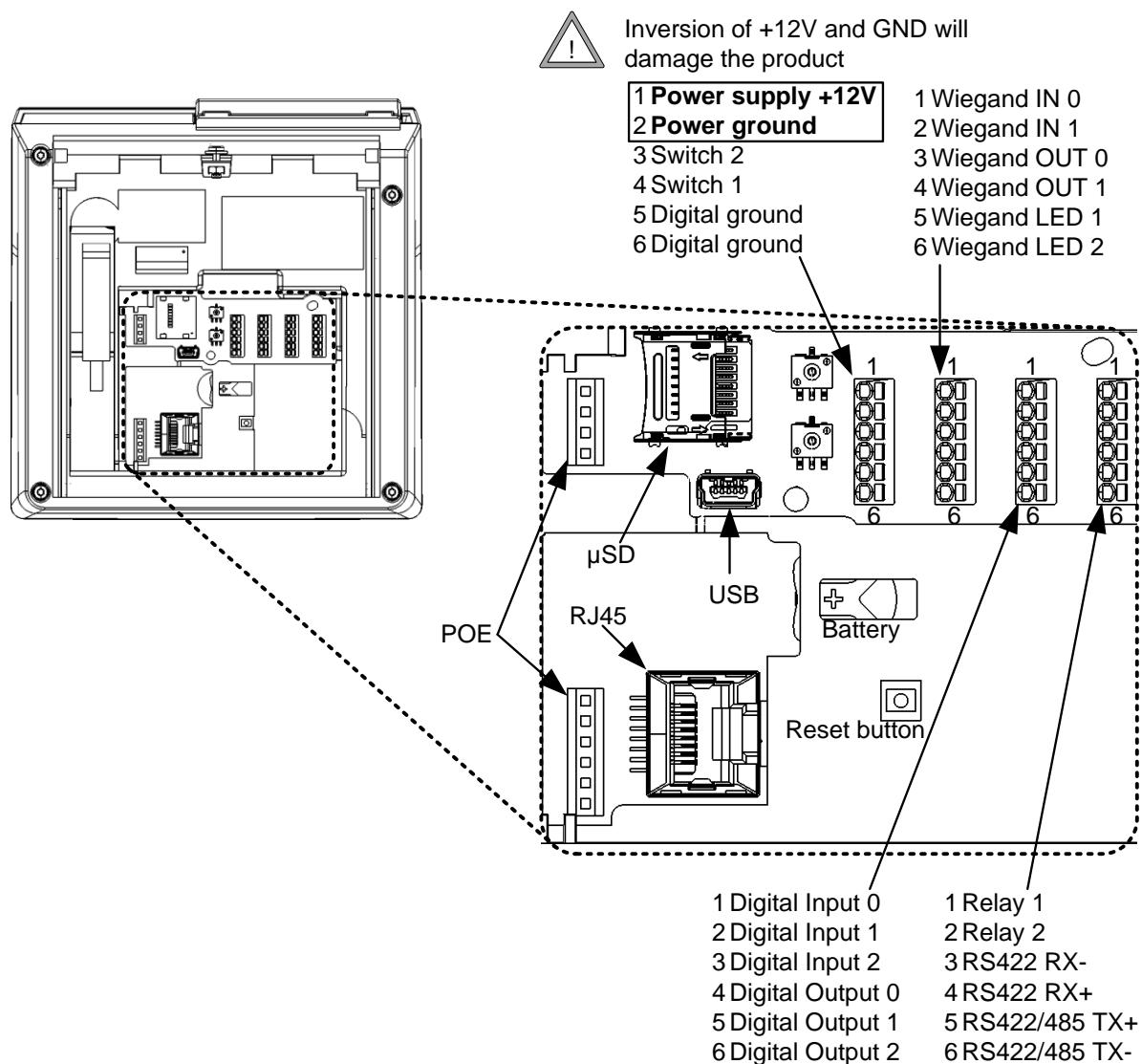


Figure 5: MorphoAccess® SIGMA Series Terminal Rear View Diagram

Access Control System Synoptic

The terminal provides several interfaces for an easy integration into a global access control system.

Sending of a message at the end of local access control

The terminal is able to send a message to a distant system when local checks are completed. This message can be used, by the distant system, for a simple storage of all access requests, or to start more sophisticated processes such as additional access rights checks.

This feature is described into “Sending an Access Control Result Message” a distant system section.

For this feature the terminal can use:

- an **Ethernet link**: through the RJ45 connector (ref RJ45/POE on Figure 5) or the connector block (ref B on Figure 5) using UDP or TCP or SSL protocol,
- a **Wi-Fi™ link**: by connecting a USB Wi-Fi™ adapter in the USB rear port (ref B on Figure 5), using the UDP or TCP or SSL protocol,
- A **Serial Port** (ref B on Figure 5), using the Wiegand or Clock & Data or RS422/RS485 protocol.

It is not allowed to use simultaneously the Ethernet link and the Wi-Fi™ link. But, it is allowed to use the serial port and either the Ethernet or the Wi-Fi™ link.

This feature is compatible with an administration through the Ethernet or Wi-Fi™ link.

Input signals and relay contacts

The MorphoAccess® SIGMA Series terminal offers several interfaces, listed below:

- A relay contact (RL1-RL2), to directly command a physical terminal such as a door lock. This feature is described in “Internal Relay activation on Access Granted result” section,
- A relay contact (SW1-SW2) which provides the status of the anti-tamper switch. This feature is described in “Anti-Tamper Switch For Terminal Security” section.

USB port usage

Plugging a USB Mass storage key

The external micro USB port of the MorphoAccess® SIGMA Series terminal is dedicated to the temporary connection of a USB Mass Storage key. This is used to:

- configure the terminal with command scripts,
- or to upgrade the firmware of the terminal (Morpho legacy mode only),
- or to load data in the terminal,
- or to export data from the terminal.

The port cover must be removed to allow the access to the USB port.

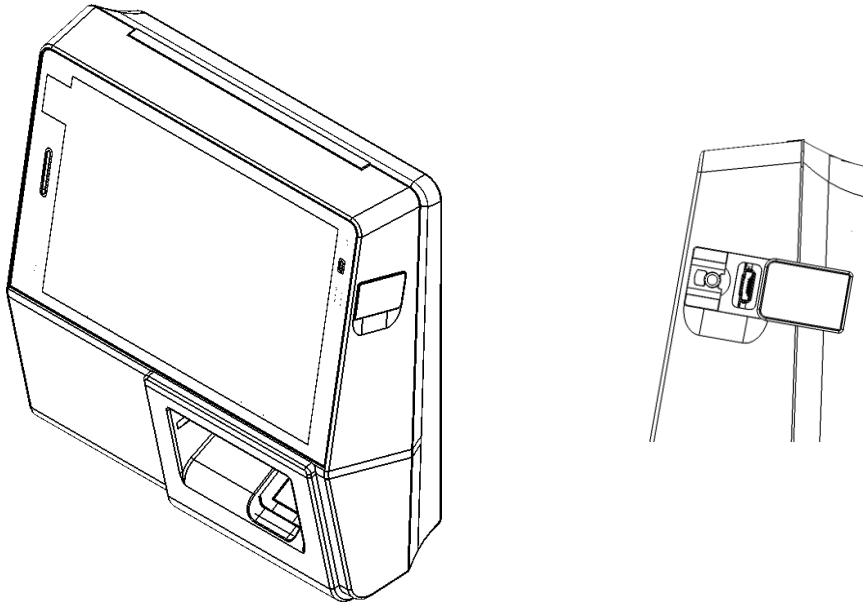


Figure 6: MorphoAccess® SIGMA Series terminal external USB port

Plugging a USB Wi-Fi™ or 3G adapter

The rear USB port of the MorphoAccess® SIGMA Series terminal is dedicated to the connection of a Wi-Fi™ or 3G USB adapter.

This micro USB port is located at the back panel of the terminal.

The Wi-Fi™ adapter accessory can be ordered under reference number "MA WI-FI™ PACK" at the same time as the license that unlocks the Wi-Fi™ feature on the terminal.

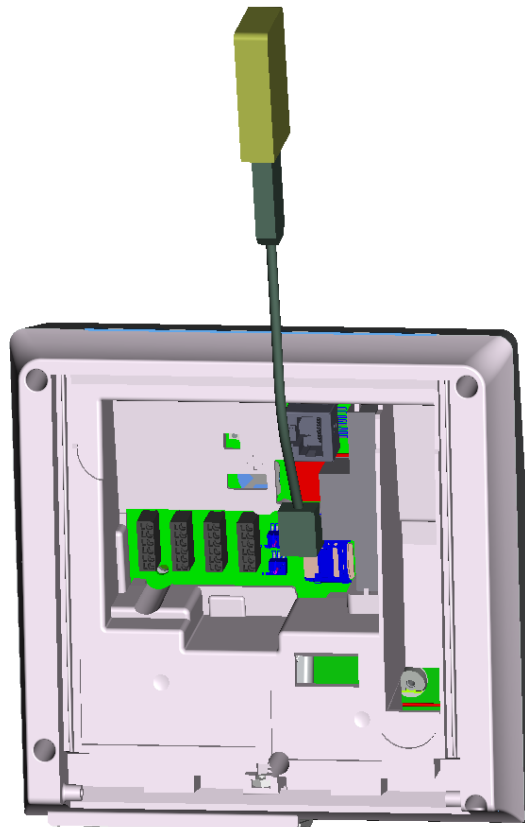


Figure 7: MorphoAccess® SIGMA Series terminal USB port with a Wi-Fi™ adapter

Connecting a Computer through USB

The external USB port of the MorphoAccess® SIGMA Series terminal is dedicated to the connection of a computer through a USB Cable. This is used to for firmware upgrade in the terminal using an application on a computer/server. Refer to “[Terminal Firmware](#)” for more information.

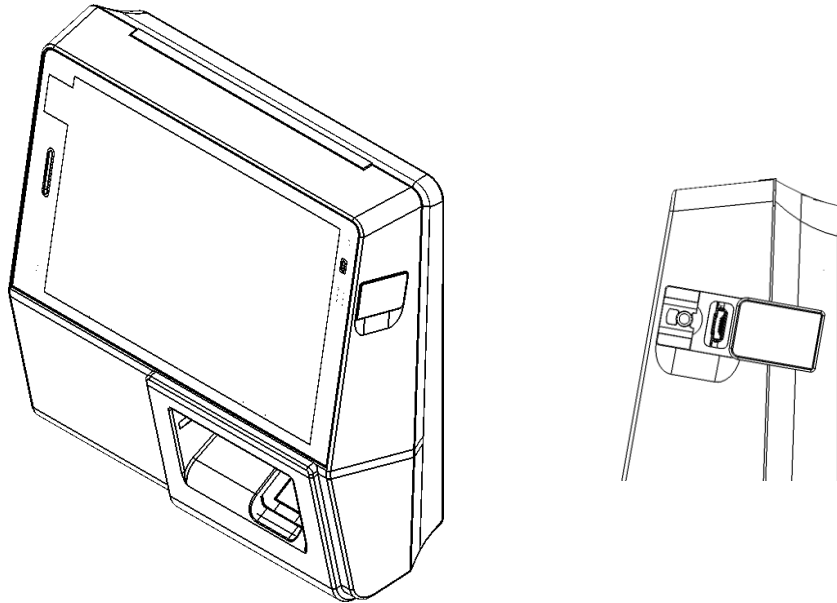


Figure 8: MorphoAccess® SIGMA Series terminal USB port

Section 3 : Connecting the Terminal to a PC

General

Why would one connect the terminal to a PC?

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

- terminal configuration,
- terminal maintenance: firmware upgrade, add a license (to unlock an optional feature),
- database management: add, modify or remove a user,
- log file management: get or delete log file,
- Wi-Fi™ connection configuration before use.

Connection methods

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

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

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

Network parameter initialization

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

| IP address Mode | Parameter | Factory value |
|--------------------------|---------------------|---------------|
| Dynamic (DHCP - Default) | Terminal IP address | 0.0.0.0 |
| | Gateway IP address | 0.0.0.0 |
| | Sub network mask | 0.0.0.0 |
| | Host name | MASigma |

If the terminal's default network parameter values cannot be used, the Communication menu provides the quickest method to change these values.

Point to Point Ethernet Connection

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

But there are some limits described in the next paragraphs.

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

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



Figure 9: Direct Point to Point Ethernet Connection

Connection through only one Ethernet switch

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

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

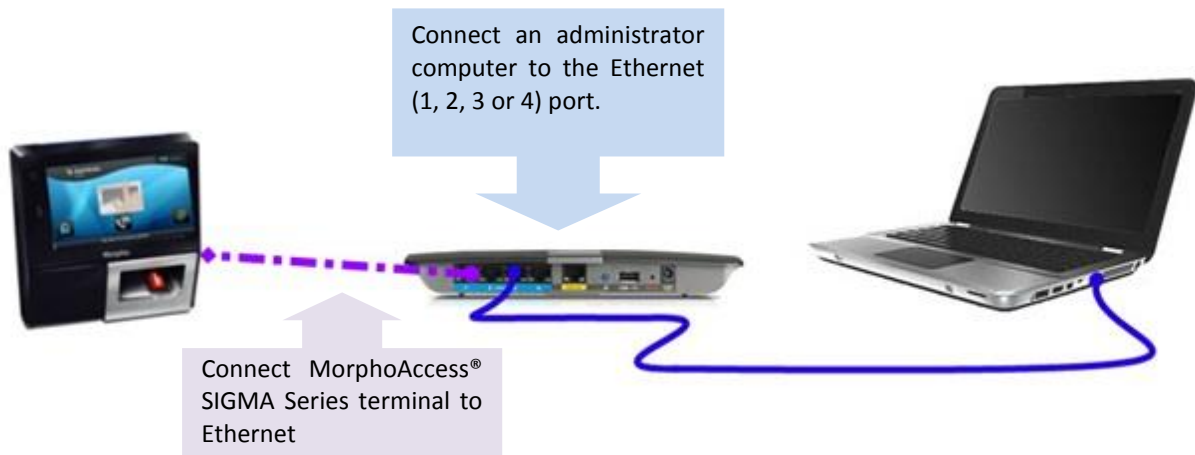


Figure 10: Connection through an Ethernet switch

Connection through a LAN

Description

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

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

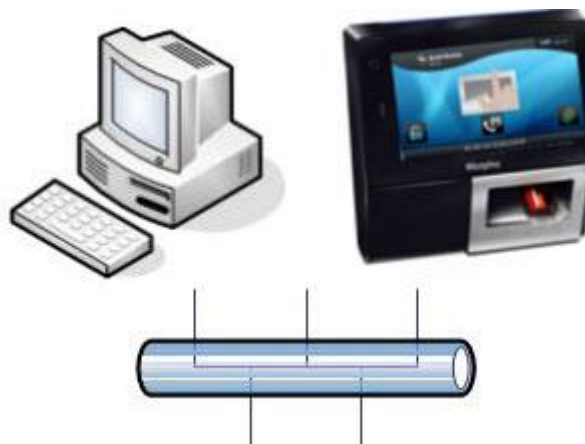


Figure 11: Connection through LAN

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

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

LAN with DNS Server

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

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

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

LAN without DNS Server

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

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

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

Static IP address (DHCP disabled)

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

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

- The MorphoAccess® SIGMA Series terminal IP address,
- Gateway IP address,
- Local subnet masks value.

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

Dynamic IP address (DHCP enabled)

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

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

Wi-Fi™ Network configuration

Requirements

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

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

After Wi-Fi™ license downloading and Wi-Fi™ USB adapter installation, make sure to reboot the terminal by pressing the reset button ([MorphoAccess® SIGMA Series Terminal Rear View Diagram](#)).

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

Configuration

The Wi-Fi™ network configuration is described in subsequent section [“Wi-Fi™ Network Configuration”](#)

Troubleshooting

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

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

To restart the terminal use the reset button located back of the terminal (ref [MorphoAccess® SIGMA Series Terminal Rear View Diagram](#)).

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

Section 4 : Terminal Configuration and Administration

Understanding MorphoAccess® Configuration

Presentation

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

- **Terminal Administration Menu:** An administrator can login to terminal and access several functionalities under administration menu. It allows administrator to perform configuration, add users, upload multimedia, download logs, etc. Entire Menus are covered in the subsequent sections of this document;
- **Webserver Application:** Webserver can be called a remote configuration panel of MorphoAccess® SIGMA Series terminal. It enables an administrator to configure any parameter of terminal connected remotely. Webserver is connected to terminal through Ethernet or Wi-Fi™ network. Only an administrator with full administrative rights can login to Webserver. Refer "[Introduction to Webserver](#)" in this document.
- Webserver application also has a module called "Complete Configuration" which is used for setting parameter keys of MorphoAccess® SIGMA Series terminal. For detailed description of all the parameters, please refer to MorphoAccess® SIGMA Series Parameters User Guide.

Modifying the value of a parameter

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

- Remotely through Ethernet or Wi-Fi™, with a client application/interface running on the Host System (such as Morpho Bio Toolbox or a web browser connected to the embedded Webserver),
- With a USB mass storage key, which contains a script prepared on a PC (for more information see document **MorphoAccess® terminals USB Key encoder User Guide**).

Notation

In this manual a parameter is presented using this format:

| Parameter name | Value | Description |
|----------------|-------|-------------|
| _ | _ | _ |

For example to allow additional attempt for biometric authentication:

| Parameter name | Value | Description |
|---|-----------|---|
| auth_param.additional_bio_heck_nb_attempt | 1, 2 or 3 | <p>A value of “2” means that after a first incorrect identification or authentication a second chance is given to place finger on the biometric sensor.</p> <p>Set this parameter to “1” to offer only one attempt to place finger.</p> <p>Set this parameter to “3” to offer 3 attempts.</p> |

Configuring a Networked MorphoAccess®

Introduction

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

The remote operations available are mainly:

- Time and Attendance configuration,
- read the value of parameters,
- modify the value of parameters,
- create access schedules,
- network configuration,
- Tamper settings, etc.

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

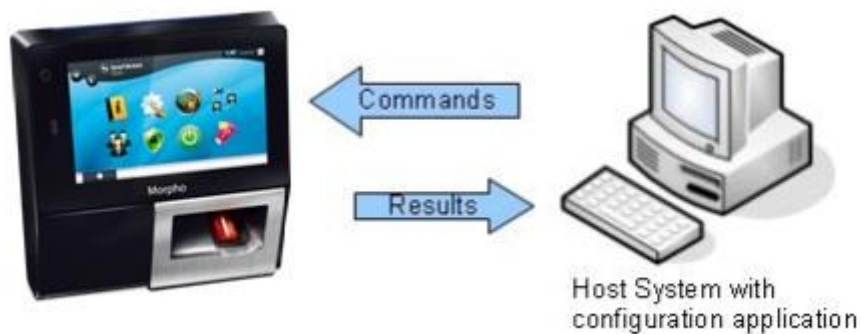


Figure 12: Configuration of a MorphoAccess® SIGMA Series terminal by a Host System

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

Refer to “Terminal Configuration through Webserver” section in this document, for details on actions that can be performed from Web Server.

Network factory settings

By default the terminal IP address is 134.1.32.214. This address can be changed by a distant system connected though an IP link or with a USB flash drive (USB Network Tool).

The default server port is 11010.

Date/Time settings

The date/time of the terminal can be initialized by a distant system or by local Administrator Menu.

Access Path

Terminal Settings > Date Time

Screens & Steps

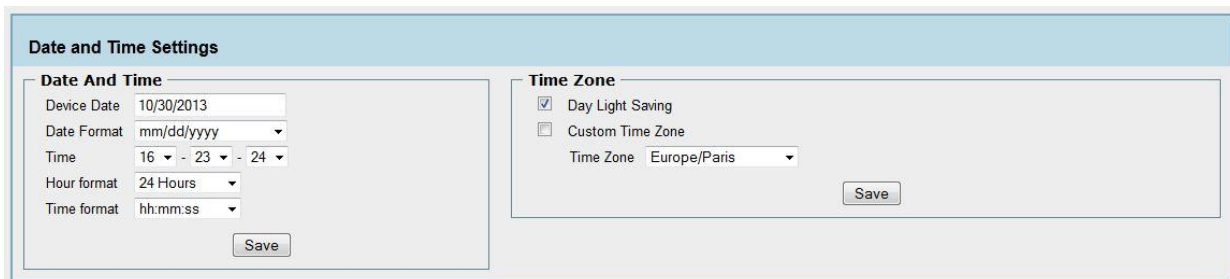


Figure 13: Date and Time setting of Terminal from Webserver

SSL Securing

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

These protocols are used to protect the communication between the MorphoAccess® SIGMA Series terminal 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
- See SSL Solution for MorphoAccess® documentation for details on SSL securing

Network Wi-Fi™ configuration

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

- A Morpho WI-FI™ USB adapter, ref. 189930722, must be plugged in the rear USB port of the terminal. Installation procedure is described in the MorphoAccess® SIGMA Series Installation Guide,
- A MorphoAccess® WI-FI™ License is loaded in the terminal (cf. NOTE 2 “Downloading a licensee”),
- The terminal must not be connected to a network with an Ethernet cable: WI-FI™ connection and Ethernet cable connection are mutually exclusive.

NOTE 1: A DHCP server and a DNS server are mandatory when the Wi-Fi™ interface is configured in DHCP mode.

- The DHCP server automatically attributes an IP address to the MorphoAccess® SIGMA Series terminal
- The DNS server links the terminal hostname to its real IP address
- It is also important that the DNS server is updated each time the DHCP server attributes another IP address to a terminal.

NOTE 2: A MorphoAccess® WI-FI™ License is mandatory.

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

See WI-FI™ parameters description in paragraph “Communication Settings” using Webserver.

MorphoAccess® Terminal Database Management

General

The management of the MorphoAccess® SIGMA Series terminal can be done by administration menu of the terminal or through Webserver application connected to terminal.

Adding a user to the database

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

- **Normal Users** are the ones to whom access is granted or rejected based on access rights check
- **Authorized Users List** are the ones, that the centralize access controller checks before granting access
- **VIP listed Users** are allowed access without performing biometric/PIN check by the terminal. Read more about VIP users under [“Access Control Process for VIP Users”](#)
- **Administrators** are stored also in the user database. Administrators can access to management menu of the terminal and perform configurations.

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

Removing a user from the database

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

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

Database Size

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

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

- Maximum Authorized User List Capacity, indicates the maximum number of users can be added to authorized user list, which is 250,000 users by default
- Maximum VIP user capacity, indicates the maximum capacity of the users can be enrolled as VIP users, that is 100 users by default
- By default, terminal can store up to 100,000 transaction

The database size can be increased by installing licenses. E.g. the user record storage size can be increased up to 100,000 user records with a MA_100K_USERS license. For each user, the terminal stores the biometric data of two fingers. For “MorphoAccess® Terminal License Management”, refer subsequent section for more details.

MorphoAccess® Terminal License Management

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

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

- MA_10K_USERS
- MA_50K_USERS
- MA_100K_USERS (extend database maximum size)
- MA_250K_LOGS
- MA_500K_LOGS
- MA_1M_LOGS (extend database maximum size)
- MA_PAC
- MA_TA
- MA_WI-FI™ (allows Wi-Fi™ connection)
- MA_3G

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

User licenses

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

- The **MA_10K_USERS** license extends the maximum size of the database to 10,000 user records (With two fingers per user record. In case, duress finger is enabled, it can have three fingers per user record).
- The **MA_50K_USERS** license extends the maximum size of the database to 50,000 user records (With two fingers per user record. In case, duress finger is enabled, it can have three fingers per user record).
- The **MA_100K_USERS** license extends the maximum size of the database to 100,000 user records (With two fingers per user record. In case, duress finger is enabled, it can have three fingers per user record).

WARNING: It is a pre-requisite that terminal should have SD card plugged in it on upgrading user's license. Otherwise the terminal will not boot up unless SD card is plugged.

Logs licenses

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

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

WARNING: It is a pre-requisite that terminal should have SD card plugged in it on upgrading logs license. Otherwise the terminal will not boot up unless SD card is plugged.

Communication licenses

MorphoAccess® SIGMA Series terminal supports 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. To enable this networks communication, it is required to install licenses.

Following types of communication licenses are available:

- MA_WI-FI

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

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

- MA_3G

The MA_3G license enables the 3G network (GPRS/GSM/3G) which replaces the standard Ethernet connection. The terminal can communicate with distant systems through 3G/ GPRS/GSM network.

Access Control license

- MA_PAC

The MA_PAC license enables following functionalities of the MorphoAccess® SIGMA Series terminal:

- Single Door Access Control (SDAC)
- Wiegand output
- Clock & data output
- IP output
- Serial output

Time and Attendance (T&A) license

- MA_TA

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

Getting a license for a MorphoAccess® SIGMA Series terminal

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

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

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

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

hotline.biometrics@morpho.com

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

Checking licenses installed in the terminal with license manager application

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

Screens & Steps

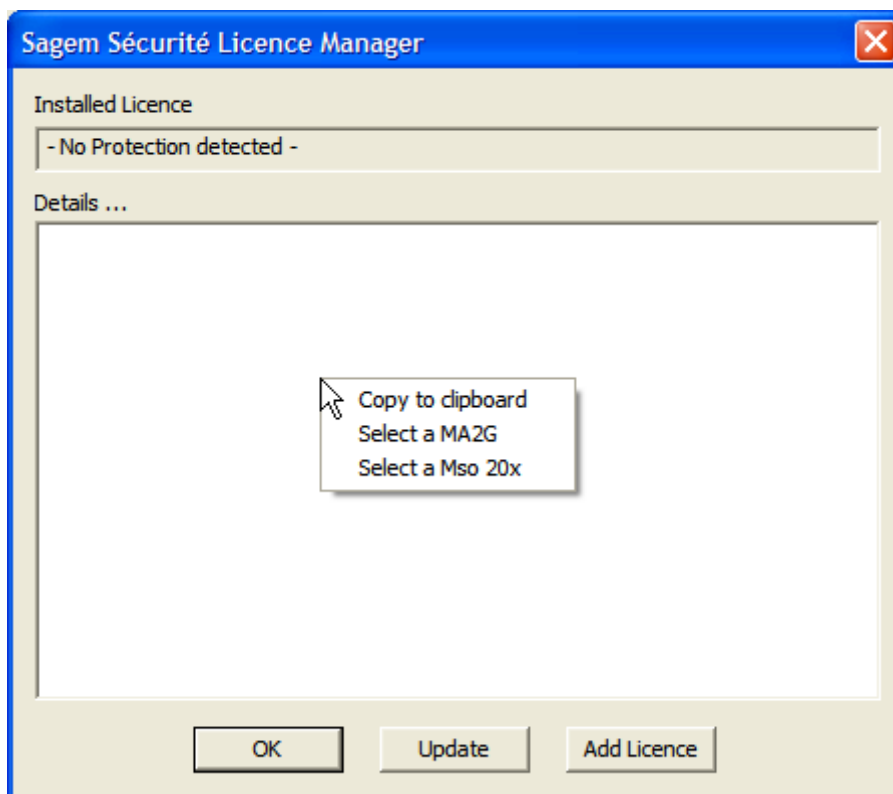


Figure 14: License Manager, adding a MorphoAccess® SIGMA Series terminal

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

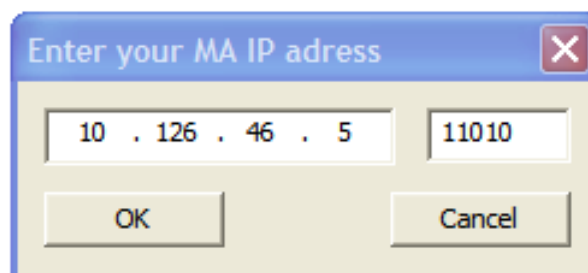


Figure 15: License Manager, entering an IP address for a MorphoAccess® SIGMA Series terminal

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

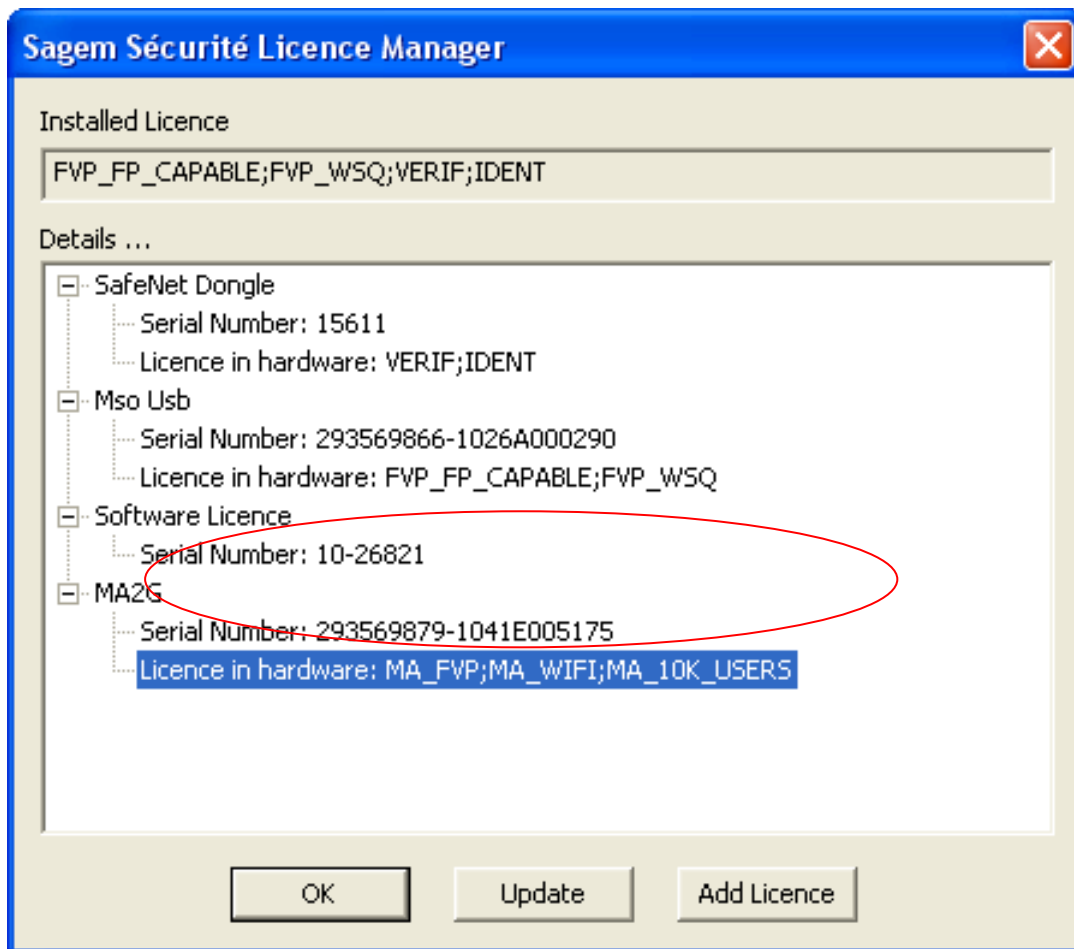


Figure 16: Licenses installed in a MorphoAccess® SIGMA Series terminal

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

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

Installing a new license

Proceed as follows to install a new license:

- Copy the received license file (.lic extension) on the PC
- launch the "License Manager" application then add the MorphoAccess® SIGMA Series terminal IP address as specified in the previous section,
- click "Add license", then "Browse..." to select the license file (.LIC),
- a specific window will open to indicate whether or not the license has been loaded successfully,
- The main window will then indicate the presence of the new license.

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

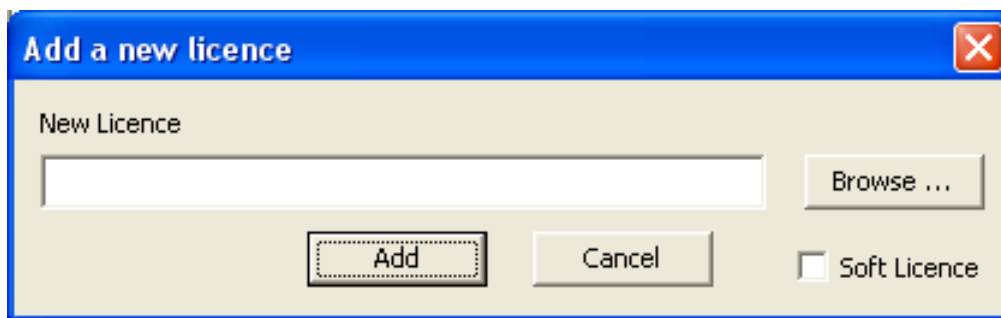


Figure 17: Adding a license in a MorphoAccess® SIGMA Series terminal

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

Terminal Firmware Upgrade

How to get last version of firmware

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

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

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

hotline.biometrics@morpho.com

How to upgrade the firmware

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

The easiest way to update the firmware is to use MorphoAccess® Administration software application (also named M2A), or MorphoBio ToolBox software application.

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

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

Firmware upgrade using a USB Mass Storage Key

It is possible to update the firmware, using a USB mass storage key, but only in Morpho Legacy mode. This feature is not available in native mode (MA5G mode).

Firmware upgrade tool for expert users

MorphoAccess® SIGMA Upgrade Tool

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

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

Syntax of the command-line

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

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

Samples:

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

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

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

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

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

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

Note: If the Ethernet connection is broken during the firmware upgrade process, user can re-plug the Ethernet cable and relaunch RetrofitTool with the same command line. The firmware upgrade is restarted from beginning and is entirely executed, with proper restarting of the terminal

MorphoAccess® SIGMA Series Modes

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

When MorphoAccess® SIGMA Series is set in any of the legacy modes; it supports the database structures and configurations of the selected legacy terminal. When the terminal is booted for the first time, user can select any of the legacy mode described in the next sections.

MorphoAccess® 500 or J Series legacy mode

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

Access Path

First Boot Assistant > Protocol Configuration > Legacy Morpho

L-1 Bioscrypt 4G Series legacy mode

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

In case, users are enrolled in MA5G mode, the user data cannot be exported when terminal is in L1 mode. There are certain other limitations, when MorphoAccess® SIGMA Series terminal is run in L1 Legacy mode. For details about these limitations, refer to MorphoAccess® SIGMA Series L-1 Bioscrypt Limitations document.

Access Path

First Boot Assistant > Protocol Configuration > Legacy L1

MorphoAccess® SIGMA Series native mode

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

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

Access Path

First Boot Assistant > Protocol Configuration > MA5G

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

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

Section 5 : First Boot Assistant

Assistant Initialization

First Boot Assistant (FBA) is launched as soon as the MorphoAccess® SIGMA Series terminal is started for the first time. All the fundamental settings can be done from an FBA screen itself. FBA can also set to launch on terminal reboot.

An administrator can access First Boot Assistant from Management menu, as give in access path.

Access Path

System Menu > First Boot Assistant

Pre-requisites

- Verify that the battery is plugged in the terminal beforehand. Battery backup is necessary for preventing data loss on power cut/power loss instance
- If terminal is unpowered for a too long time, it will be necessary to change the battery

Screens & Steps

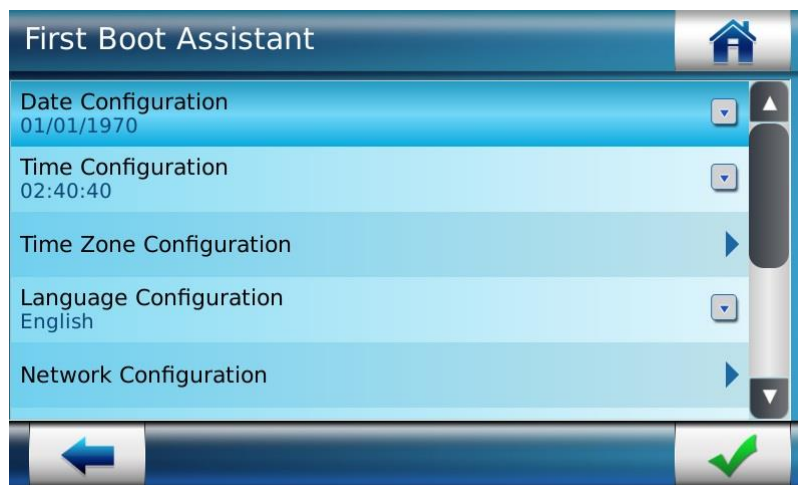


Figure 18: First Boot Assistant Screen displayed on Installation

1. On first time installation, by default First Boot Assistant will open. An administrator can also access FBA settings from Access path mentioned above.
2. In First Boot Assistant Screen, an administrator can configure basic parameters as mentioned in below:

Date & Time Configuration

On first boot or reboot of the terminal it is mandatory to set the current date, time and time zone in the terminal.

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

Access Path

System Menu > First Boot Assistant

Screens & Steps

1. Select **Date Configuration**

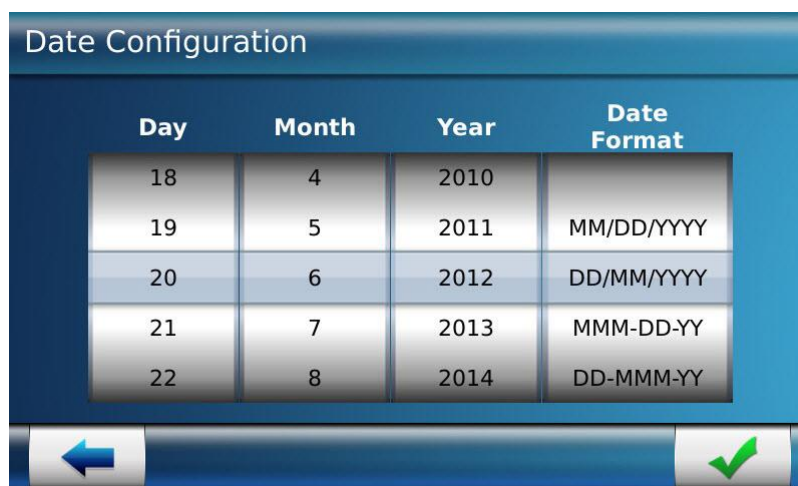



Figure 19: Configuring Current Date

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 (this format is not available, if terminal is set in L1 mode)
4. Use Check button “” to save the setting

5. Select **Time Configuration**

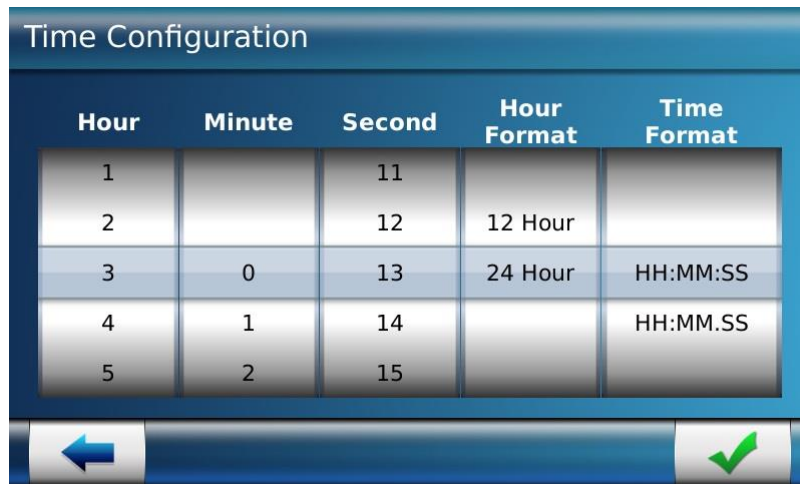



Figure 20: Configuring Current Time

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. The available formats are
 - a. HH:MM:SS
 - b. HH:MM.SS
9. Use Check button " " to save the setting
10. Select **Time Zone Configuration**

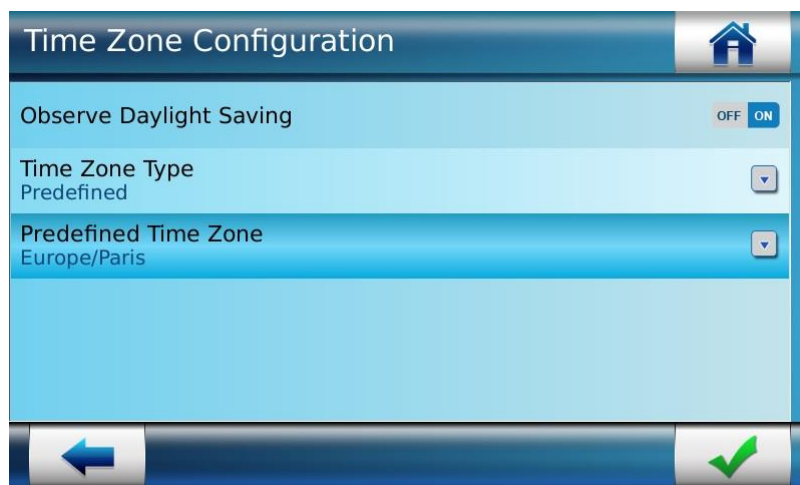


Figure 21: Configuring Time Zone

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



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



Figure 22: List of Predefined Time Zones of World

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

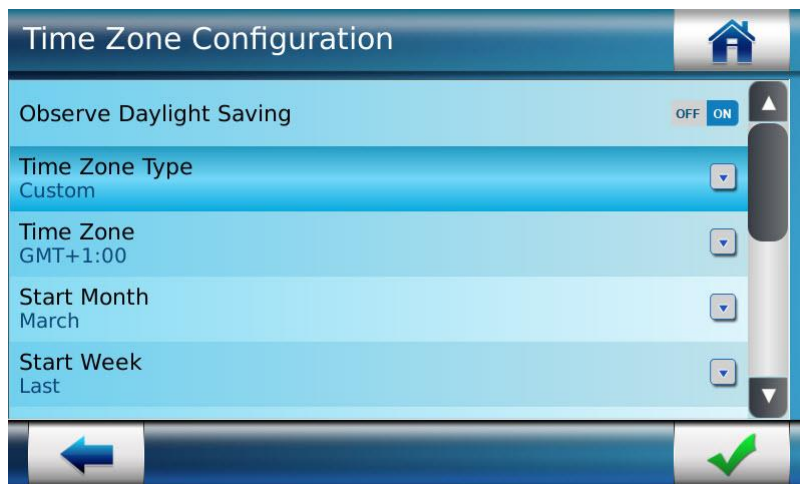


Figure 23: Custom Time Zone Setting

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

19. Select **Time Zone**

NOTE: While setting custom time zone, make sure the GMT offset to be 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. Use Check button “” to save the setting

Trigger Event

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

- **Biometric**, a finger is detected on the biometric sensor (which starts biometric identification process)
- **Contactless card**, a contactless card is detected, which starts authentication process using user's data found on user's card
- **Keypad**, a User ID is entered with the keypad
- **External Port**, a User ID is received on Wiegand or Clock and Data input port

Access Path

System Menu > First Boot Assistant > Trigger Event

Or

Security Menu > Biometric Settings > Trigger Event

Screens & Steps

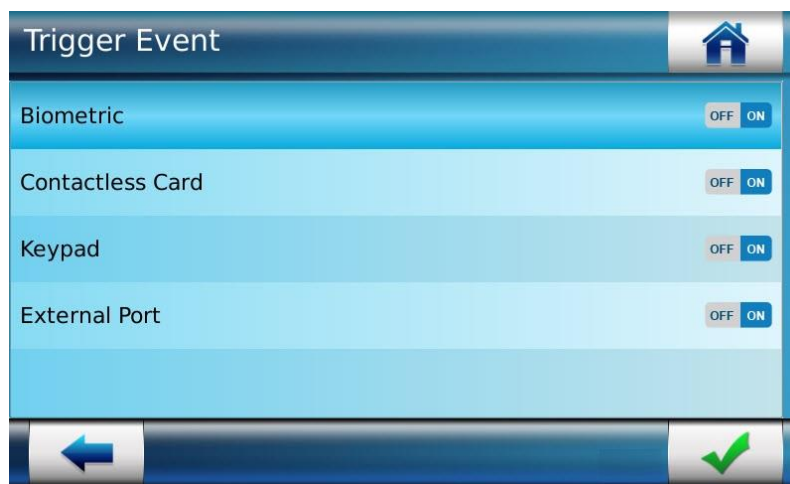



Figure 24: Selecting the event(s) that starts access control rights check process

1. Select the above stated events as ON or OFF
2. Use Check button “” to save settings

Language Configuration

Using this functionality an administrator can set the language in which terminal content is displayed. Multiple language options are available to select from, viz. English, French, Spanish or Arabic.

Access Path

System Menu > First Boot Assistant > Language Configuration

Screens & Steps

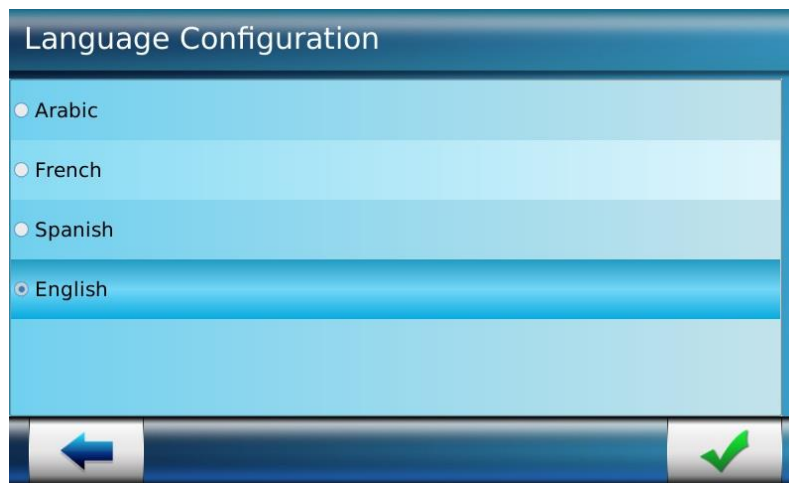


Figure 25: Configure Language


1. On FBA screen, select **Language Configuration**
2. By default, 'English' Language selected
3. An administrator can select from languages options Arabic, French, Spanish or English
4. Press Check button "" to save the setting



Figure 26: Language selection on main screen

Results

A user can select preferred language from the terminal main screen, as displayed in above figure.

Note: The Audio messages played on terminal must be same as the selected language of terminal. You can upload audio files from “Audio Settings” under Multimedia menu.

Show/Hide Language Icon

Using this functionality an administrator can opt whether to display the language icon on the terminal home screen or not, through the Web Server. The values of this parameter are 0, 1. If misc.language_config_display parameter value is set to '0' then the language icon from the terminal home screen is not displayed. The default value of misc.language_config_display is '1'.

Access Path

Web Server > Complete Configuration > misc.language_config_display



Figure 27: Hide Language Icon

Ethernet Interface Settings

MorphoAccess® SIGMA Series terminal can be connected 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 message.

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

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

Access Path

System Menu > First Boot Assistant > Network Configuration > Ethernet

Screens & Steps

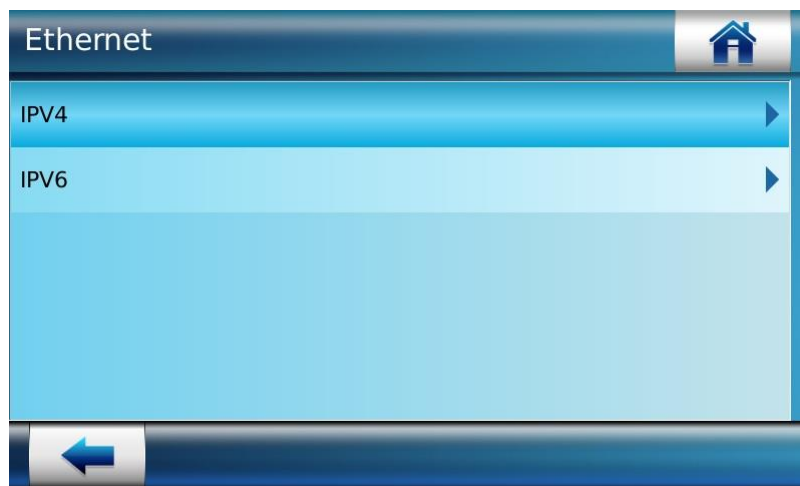


Figure 28: Ethernet Configuration

1. Under Ethernet, an administrator can select **IPV4** or **IPV6**
2. On next screen, default IP Mode is selected as DHCP. Press on **IP Mode**

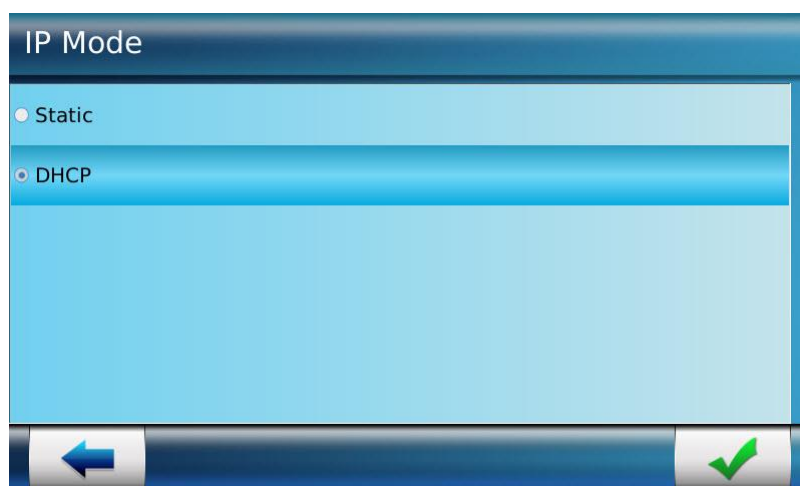



Figure 29: IP Mode Selection

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

Wi-Fi™ Configuration

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

At First Boot Assistant, an administrator can configure the terminal to communicate through WLAN. There are two ways to configure WLAN:

- **Automatic:** The available networks are listed automatically. An administrator can select the network and connect by entering encryption key
- **Manual:** The manual configuration is useful to connect with a hidden Wi-Fi™ network. An administrator can manually configure the WLAN, by entering SSID, Encryption Mode and Encryption Key.

Access Path

System Menu > First Boot Assistant > Network Configuration > WLAN

Pre-requisites

- Wi-Fi™ USB dongle should be plugged
- MA_WI-FI™ license should be installed on terminal

Screens & Steps

Automatic Configuration

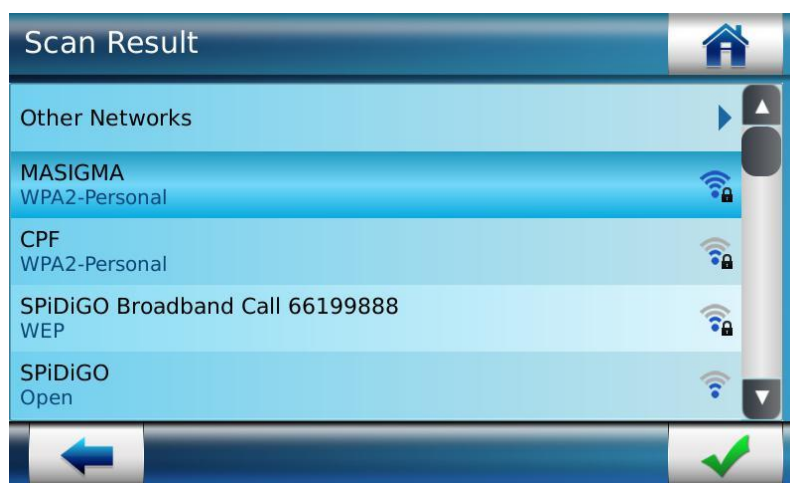


Figure 30: Selecting available Wi-Fi™ network

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



Figure 31: Enter Encryption Key

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



Figure 32: Success message is displayed showing Wi-Fi™ network is configured



Figure 33: Connected to Wi-Fi™ network

Manual Configuration

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



Figure 34: Selecting Other Network to set up Wi-Fi™ network manually

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

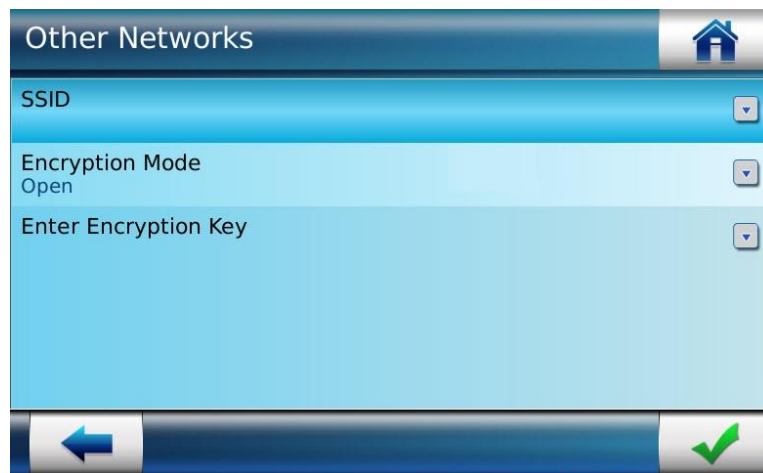


Figure 35: WLAN Parameter Configuration

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



Figure 36: Setting SSID



4. Enter **SSID** and click on “

Figure 37: Selecting Encryption Mode

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



Figure 38: Define Encryption Key

6. Enter Encryption Key to connect to Wi-Fi™. Only by entering Encryption Key, the Wi-Fi™ network can be accessed
7. Use Check button “” to save the setting

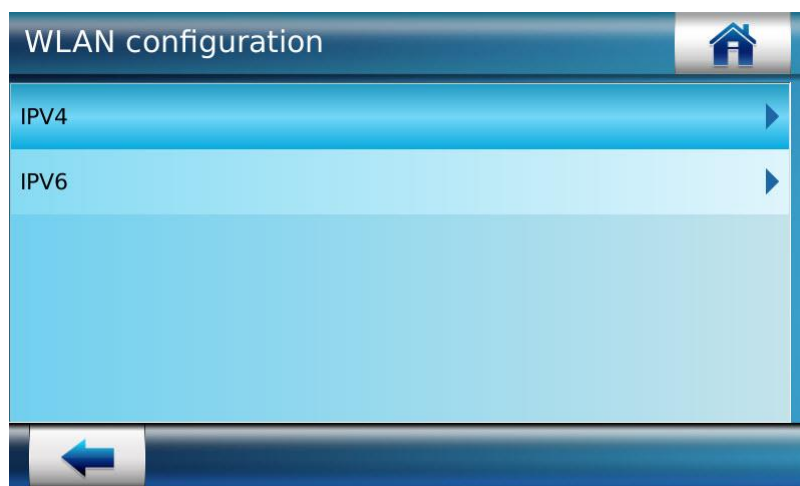


Figure 39: Entering in WLAN – IP Configuration

8. On WLAN screen select “IP Configuration” to set up the server IP which is required to be connected through WLAN
9. Select **IPV 4** or **IPV 6**

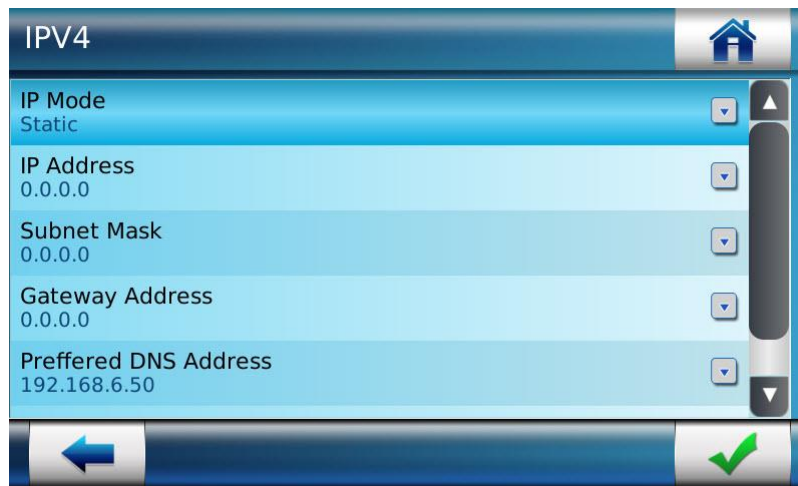


Figure 40: WLAN – IP Configuration


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



Figure 41: Success message is displayed showing Wi-Fi™ network is configured

Protocol Configuration

Using Protocol Configuration an administrator can set terminal mode as

- **Legacy L1** i.e. Bioscrypt 4G Series Legacy Mode terminals
- **Legacy Morpho** i.e. MorphoAccess® 500 or J Series legacy mode
- **MA5G** i.e. MorphoAccess® SIGMA Series native mode

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

Refer to "[MorphoAccess® SIGMA Series Modes](#)" section for detailed explanation on supported modes.

Access Path

System Menu > First Boot Assistant > Protocol Configuration

Pre-requisites

- If no SD card found on terminal while changing the protocol from e.g. MA5G to Legacy L1, then terminal database capacity to store users and transaction logs will be reduced to 3000 users and 100,000 logs, respectively.
- In absence of SD card, the dynamic message feature will not be available.

Screens & Steps

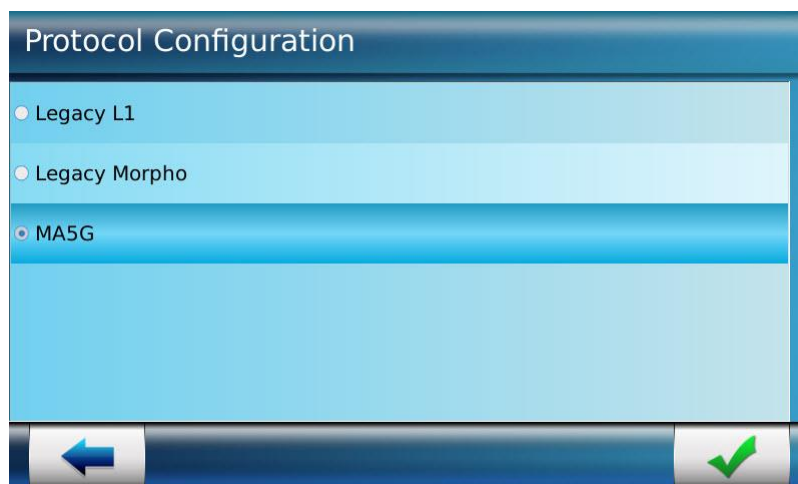



Figure 42: Protocol Configuration

1. Select Protocol from the list of modes
2. Use Check button " " to save the setting

Results

The protocol selected is saved. The terminal will be required to reboot, in order to use the terminal in any of the legacy modes. When one protocol is switched to another, MorphoAccess® SIGMA Series terminal will erase entire configuration and user database; except communication links and language settings.

Password Configuration

This function is used to reset terminal default login password. An administrator can use the password to access administration menu and perform required operations. In order to prevent any unauthorized access to the terminal administration menu, it is recommended to change the default login password on FBA (First Boot Assistant) screen itself.

The login password should be changed periodically to ensure better security. The administrator can change password anytime from “Change LCD Password” under Security Menu.

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

Access Path

System Menu > First Boot Assistant> Password Configuration

Screens & Steps

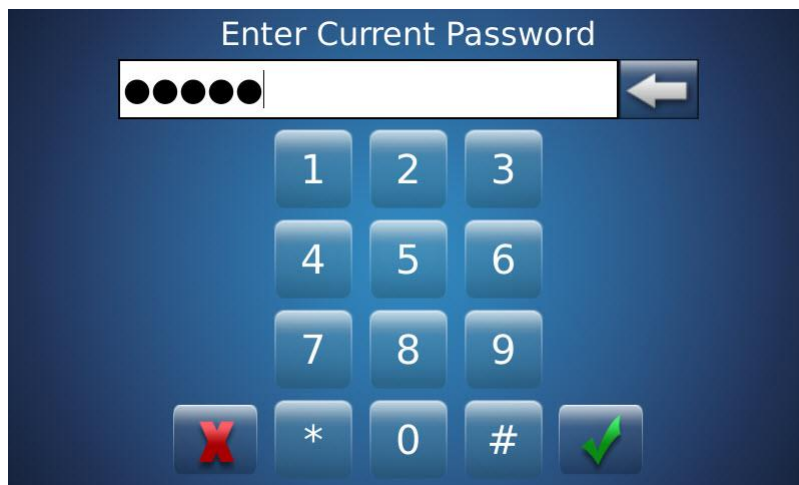


Figure 43: Resetting Device Password



1. Enter **Current Password** and use “” button to move on next screen. By default, the login password of the terminal is set as “12345”



Figure 44: Entering New Password

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

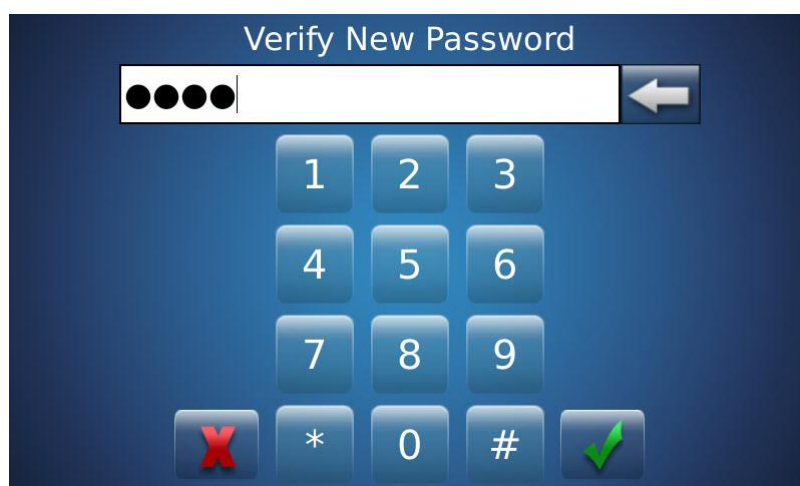



Figure 45: Verifying New Password

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

Results

The terminal administration menu is accessible only using a valid 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:** This value indicates that at next startup of the terminal, the First Boot Assistant (FBA) screen will be displayed with the configurations stored. User can change the required parameters.
- **OFF:** This value indicates that at next startup of the terminal, the First Boot Assistant (FBA) screen will not be displayed and the configurations stored will continue to apply.

Access Path

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

Screens & Steps

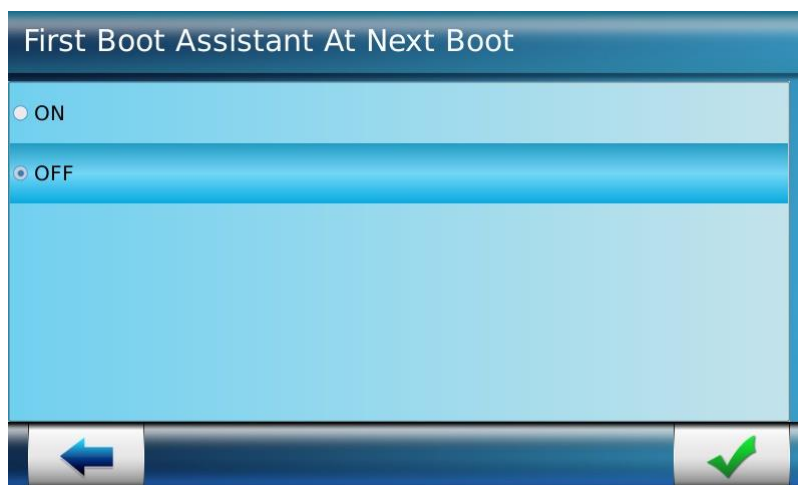


Figure 46: First Boot Assistance At Next Boot

1. Select ON or OFFPermanent
2. Use Check button “” to save the setting

Results


The validity of the configuration defined with FBA is specified, and the terminal is ready to use.

Recover Corrupted Components

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



Figure 47: Protected Data Corrupted Error

And on clicking on “” terminal lists all corrupted component as below.

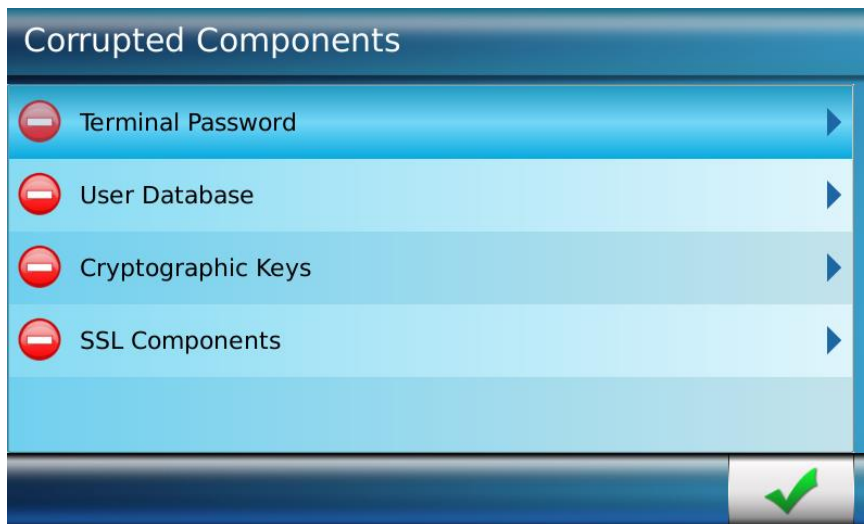



Figure 48: Corrupted Components

Once user select “”, corrupted component recovers to default state.

Section 6 : Administration Menu

Access to Administration Menu

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

- **User Menu:** For enrolling and managing users
- **Multimedia Menu:** For uploading and managing Audio, Video and Images in terminal
- **System Menu:** Allow configuration of Terminal, Transaction Log and Miscellaneous
- **Communication Menu:** For setting network interface and serial parameters
- **Security Menu:** Allows to configure Biometric, Communication, Multi-user verification, LCD password change and additional user control
- **USB Menu:** Allows initialize USB, Import and export data using USB
- **Information Menu:** Used for viewing information of terminal
- **Reboot Product:** Allows an administrator to reboot terminal

Access Path

Homepage

Screens & Steps



Figure 49: Logging in Device

1. Press on **key lock** icon



Figure 50: Entering Password

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



Figure 51: Administrator Menu

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

User Menu

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

An administrator enrolled with Full Administrator Rights or Database Administrator Rights can access this menu.



Figure 52: User Management Menu

User Enrollment in Database

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

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

Access Path

User Menu > Add/Enroll User > Only DB

Pre-requisites

- Only an Administrator with 'Full Admin Rights' or 'Database Admin Rights' can enroll new users
- If terminal is in Legacy L1 mode, then enrolment of users can be done only if Secure Admin station is equipped with a MorphoSmart™ MSO biometric sensor
- The data of the users enrolled in MA5G mode cannot be exported in L1 systems

Screens & Steps



Figure 53: 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.

NOTE: There is a configuration key, `misc.user_id_edit`, to make user ID field read only. With this parameter, the user id can be extracted from the Smartcard and

restrict user to edit this field. **misc.user_id_edit** is accessible from PC application or Web Server.

2. Press on “” button to save





Figure 54: Adding user information

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



Figure 55: Enter First Name of User

4. **First Name** of user and Press on “” button to move next
5. Similarly, on next screen, Enter **Last Name** of user and Press on “” button to move next
6. Press on **Capture Fingers** to enroll fingerprints of the user

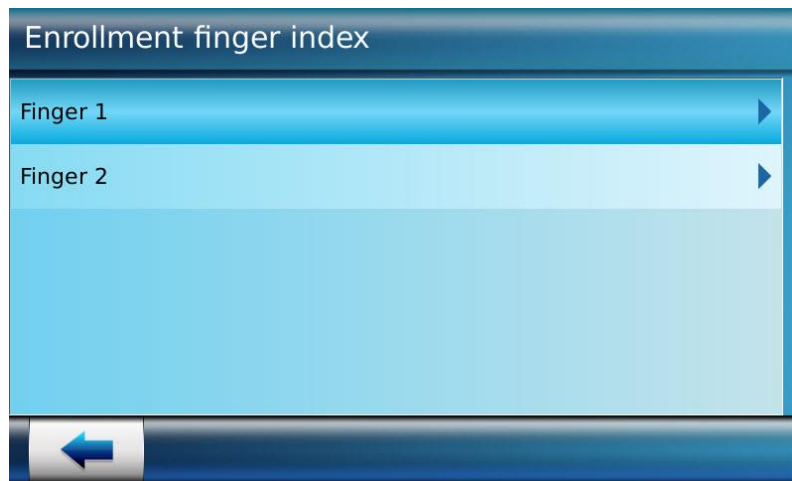


Figure 56: Enrolling Finger Index

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

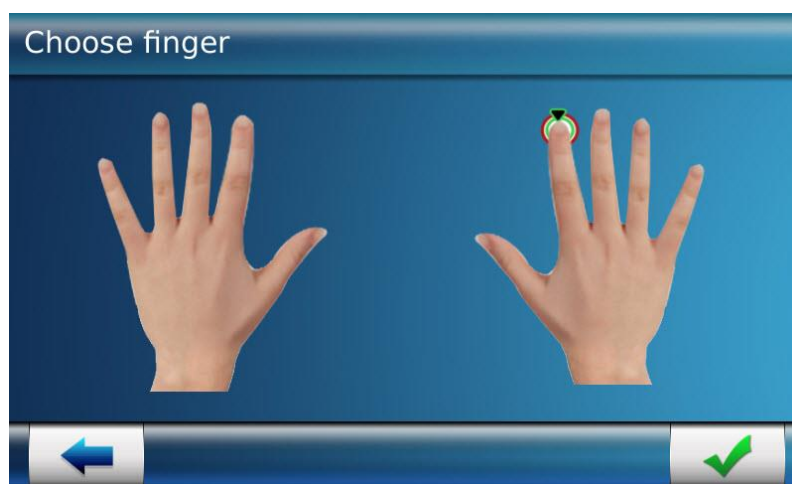


Figure 57: Select first finger to capture

8. Select first finger for biometric data capture

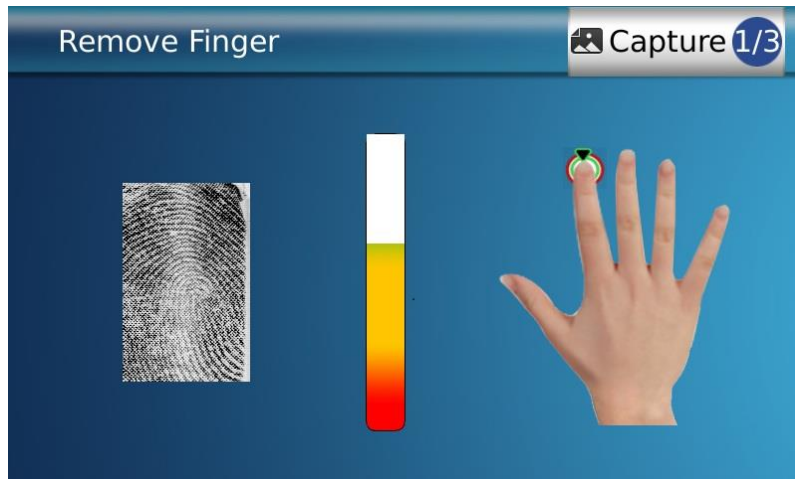


Figure 58: Biometric data capture

9. Place an administrator finger on **biometric Sensor**. If an administrator finger is not placed properly or within the time limit, an error message is displayed. Refer to *“Finger Placement Recommendation”* section to know the correct position of finger.
10. Fingerprint is captured three times and the best quality image is auto-selected by the terminal
11. Once fingerprint is stored, an administrator will be redirected to enrolment finger index screen, where an administrator needs to select the second finger to capture. Repeat steps 8 to 10 for enrolling finger 2



Figure 59: Set Duress Finger as ON

12. Once an administrator capture fingerprints, an option for capturing **Duress Finger** is enabled.
13. Select **ON** if an administrator requires capturing duress finger. Follow steps 8 to 10, for enrolling duress finger



Figure 60: Assigning Access Rights

14. **Admin Rights**, an administrator can select as below:

- a. **No Administrator Rights:** This indicates that a normal user who has no rights to access administration menu and perform any configuration. Normal users can only use the terminal for access request and/or Time & Attendance.
- b. **Database Admin:** An administrator with database administration rights will be able to access User menu and perform actions under user menu for normal user as well as administrators.
- c. **Full Admin:** An administrator with full Admin Rights can access to all the menus in administration menu and perform operations. An administrator with full Admin Rights can enroll normal users, as well as administrators.

15. Press on “” to save setting



Figure 61: Enter User PIN – Alphanumeric/Numeric

16. Enter **User PIN** which configurable based on *LCD_configuration.PIN_keypad_type*. Default value of this parameter is 1 which enable 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 fingerprints, for authentication.

17. Press on “” to save setting

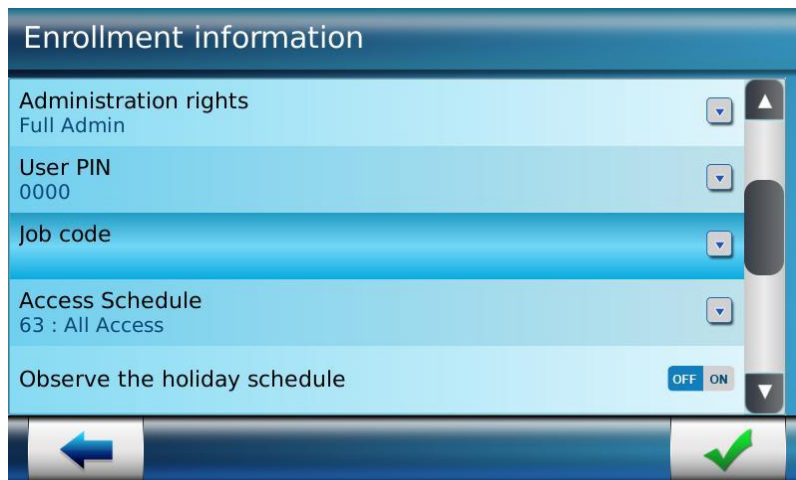


Figure 62: Setting Job Code

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

NOTE:

1. The Job Code Authentication must be enabled. From Biometric Security, Job Code can be activated.

- When Time and Attendance mode is enable, enter job code during authentication is optional even though Job Code Check is enable. It is based on the value of parameter *time_and_attendance.jobcode_by_key* and selected time and attendance key during authentication.

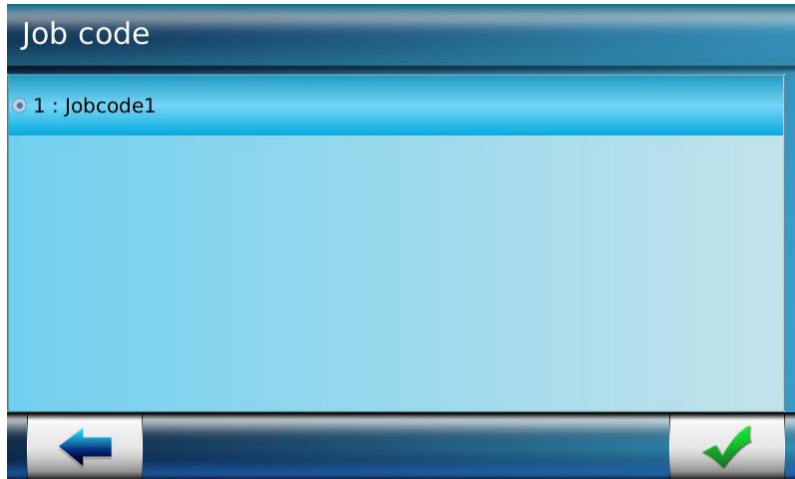


Figure 63: Setting Job Code in user profile

- 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 a distant command.

- Press on “” to save setting



Figure 64: Assigning Access Schedule

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

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

22. Press on “” to save

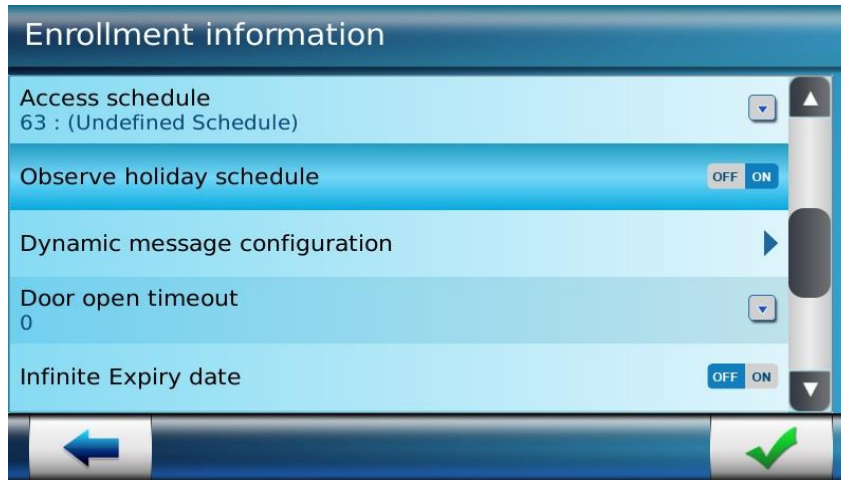


Figure 65: Enrolment Information Screen – Configuring parameters

23. Configure **Observe Holiday Schedule** as ON or OFF. If this parameter is set as ON, then access on holiday will be provided as per 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.

24. Select **Dynamic Message Configuration** as OFF or ON. Dynamic Message can include images or plain text. This message can be different for each user. When User access is granted, dynamic message is played on LCD screen.

NOTE: It is a pre-requisite to attach an SD card to the terminal, in order to configure and use Dynamic Message functionality.

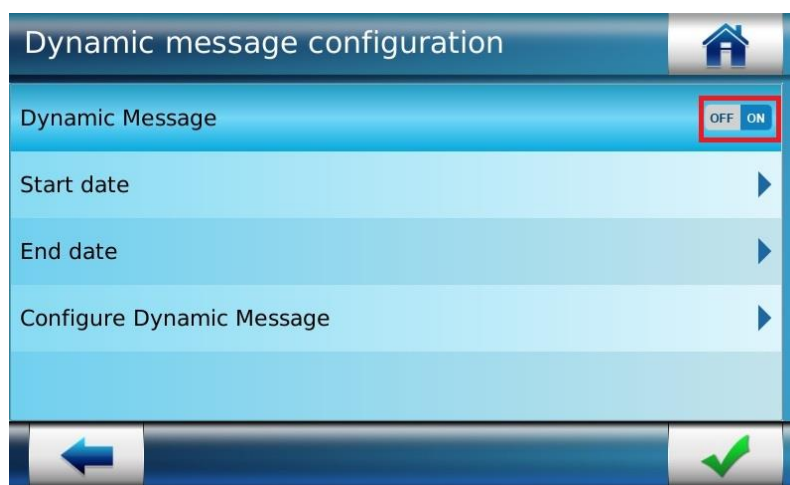


Figure 66: Configuring Dynamic Message for User

25. Set **Dynamic Message** as On

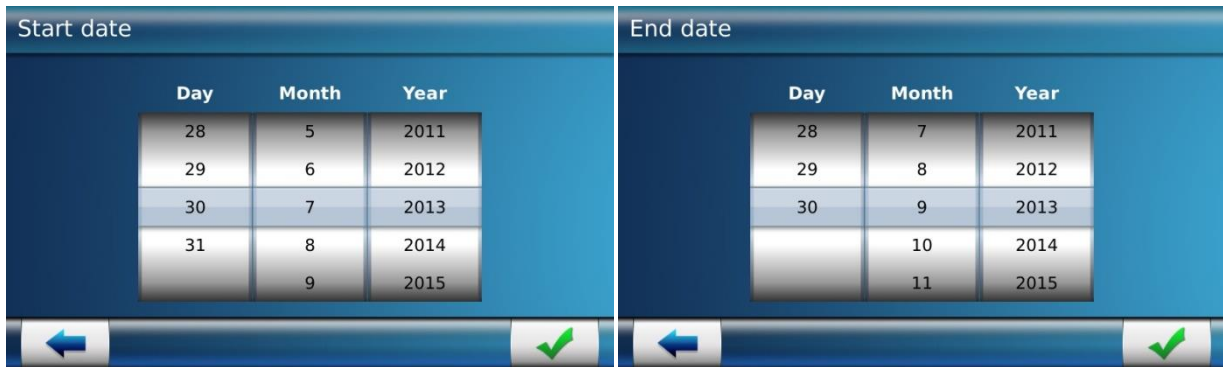



Figure 67: Setting duration for dynamic message

26. Define the duration of Dynamic Message to be displayed on LCD screen by selecting **Start Date and End Date**

27. Press on “” to save

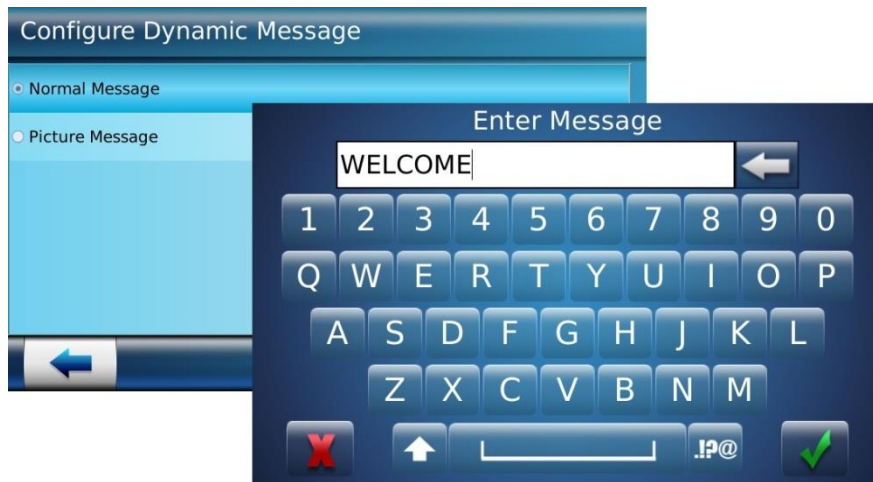




Figure 68: Configuring Dynamic Message for User

28. Select the type of dynamic message as “**Normal**” or “**Picture Message**”

- a. If an administrator selects Normal Message, then on next screen enter the message that an administrator need to display. Press on “” icon to save message
- b. If an administrator set it as Picture Message, then dynamic message 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 dynamic message can be uploaded.

29. Press on “” to save

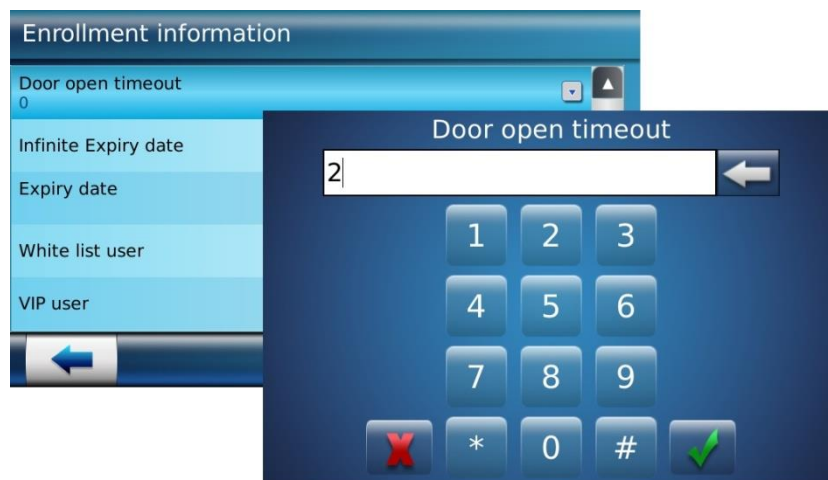


Figure 69: Configuring Door Open Time Out

30. Configure **Door Open Time Out** in seconds. The door stays open for the time duration defined here.

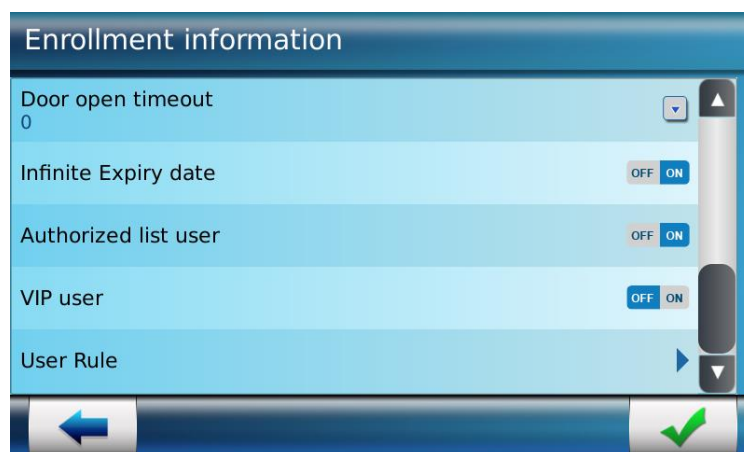


Figure 70: Enrolment Information Screen

31. Configure **Infinite Expiry Date** as OFF or ON. This parameter indicates whether user account is active for specific duration or will be active forever

a. If Infinite Expiry Date parameter is OFF, then select **Expiry Date**

32. Configure **Authorized List User** as ON or OFF. Only if the user is in Authorized list, access will be granted. By default, this parameter is set as ON.

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

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

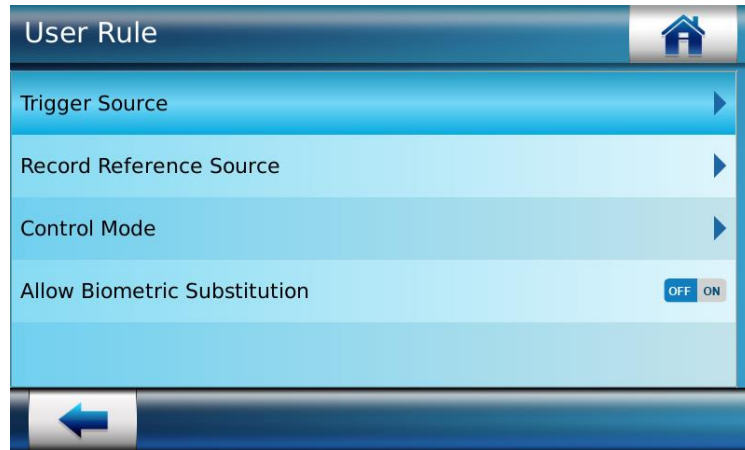


Figure 71: Defining User Rule

- 35. The User Rule settings includes below parameters:

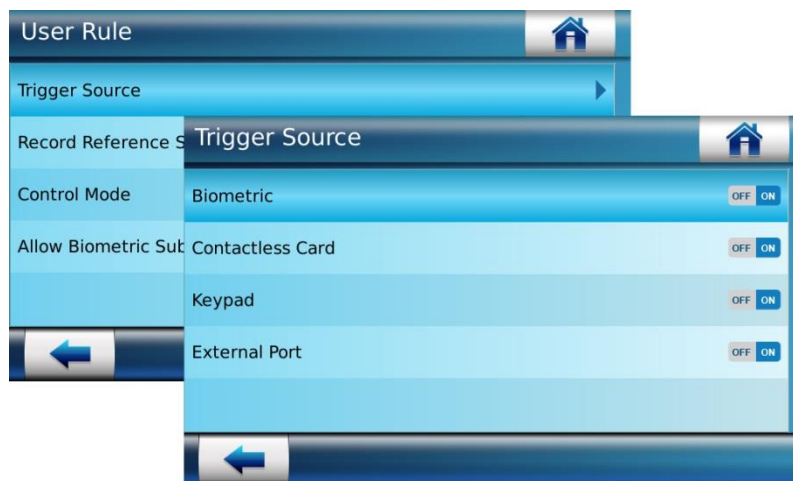


Figure 72: Defining User Rule – Trigger Source

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

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

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

- b. Set **Contactless Card** as ON, if an administrator want 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 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 an administrator allow a user to request access by providing his User ID through External port

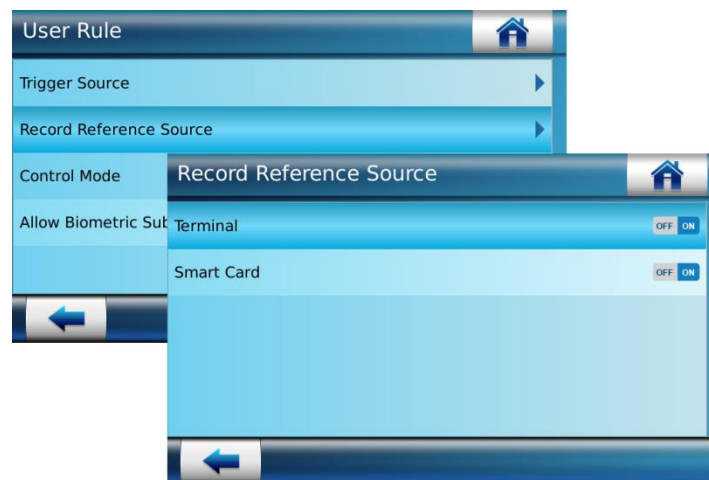


Figure 73: Defining User Rule – Record Reference Source

37. Under **Record Reference Source**, an administrator can configure whether user's information should be referred in Terminal database or/and Smart Card
 - a. Press on **Terminal** as ON, if terminal should refer to user's profile in database
 - b. Press on **Smart Card** as ON, if terminal should refer to user's profile in smart card

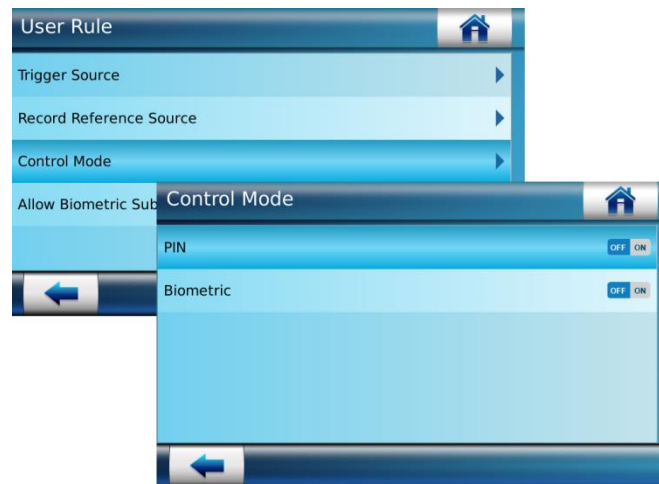


Figure 74: Defining User Rule – Control Mode

38. Under Control Mode, an administrator can set:
- PIN** mode as ON, if PIN based authentication is required
 - Biometric** as ON, if Biometric authentication is required

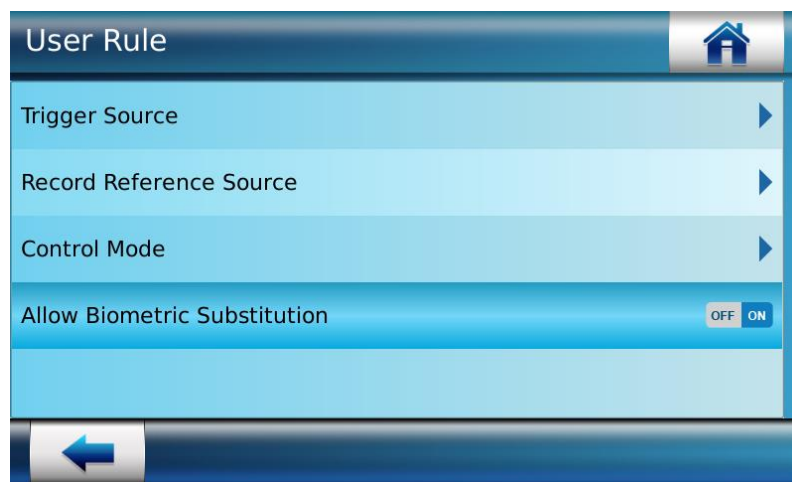



Figure 75: Defining User Rule

39. **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
40. 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 fingerprint, terminal will match the fingerprint with the records stored in the database and allow access on successful identification.

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

User Enrolment in Card

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

Access Path

User Menu > Add/Enroll User > Card Only

Pre-requisites

- Only an Administrator with 'Full Admin Rights' or 'Database Admin Rights' can enroll new users
- If terminal is in Legacy L1 mode, then enrolment of users can be done only if the biometric sensor is a MorphoSmart™ MSO terminal
- The data of the users enrolled in MA5G mode cannot be exported in L1 systems

Screens & Steps

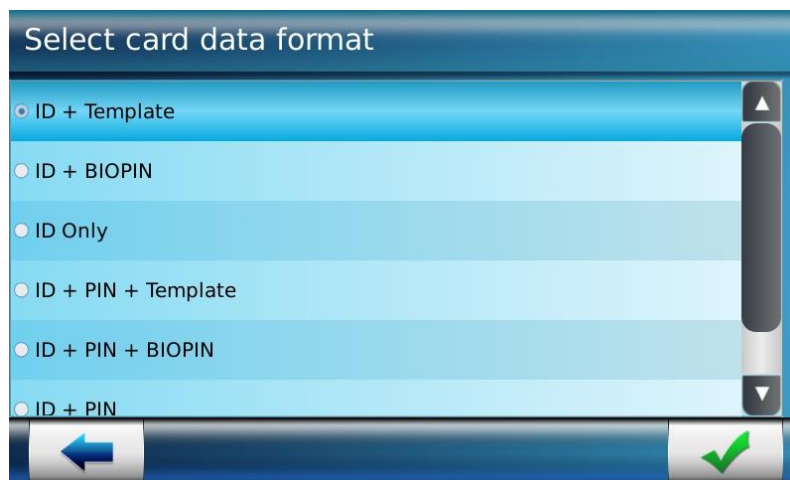


Figure 76: Select Card Data Format

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

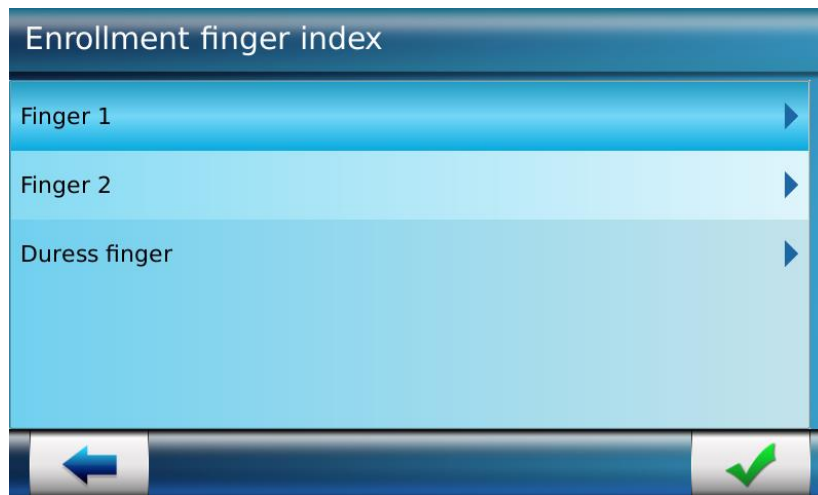


Figure 77: Enrollment Finger Index in Card

- b. **ID + BIOPIN:** This format indicates that the user authentication is done by verifying the User ID and BIOPIN (i.e. PIN that is used in place of biometric data)
 - c. **ID Only:** This format indicates that the user authentication is done by verifying the User ID
 - d. **ID + PIN + Template:** This format indicates that the user authentication is done by verifying the User ID, PIN, and Biometric Template
 - e. **ID + PIN + BIOPIN:** This format indicates that the user authentication is done by verifying the User ID, PIN, and BIOPIN
 - f. **ID + PIN:** This format indicates that the user authentication is done by verifying the User ID, and PIN
2. According to the selected Card Data Format, next user's data will be captured and stored in the card. The below screens are for ID + Template format
 3. Now refer steps 1 to 11 of section [User Enrolment in Database](#)
 4. A message to place card at terminal is displayed.
 5. **Place Smart Card** on the card reader. You may have to place card for 1 to 10 seconds, till the success message is displayed showing the user's data is stored in the card

Results

The user is enrolled successfully and user's data are 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 not editable or viewable.

User Enrolment in Card & Database

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

Access Path

User Menu > Add/Enroll User > Card + DB

Pre-requisites

- Only an Administrator with 'Full Admin Rights' or 'Database Admin Rights' can enroll new users
- If terminal is in Legacy L1 mode, then enrolment of users can be done only if Secure Admin station is equipped with a MorphoSmart™ MSO biometric sensor
- The data of the users enrolled in MA5G mode cannot be exported in L1 systems

Screens & Steps

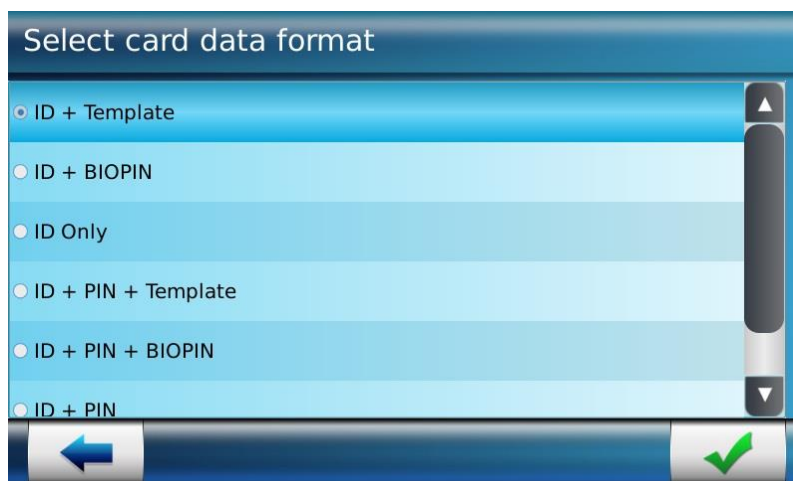


Figure 78: Select Card Data Format

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 40

3. A message to place card at terminal is displayed. **Place Smart Card** 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 and smartcard. The user can initiate access request by placing a card at terminal. The terminal will read User ID and ask user to enter required data, i.e. biometric/pin/biopin. The authentication of user's details is done based on **Record Reference Source** selected in User Rule.

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

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

Update User Information

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

Access Path

User Menu > Edit User

Screens & Steps

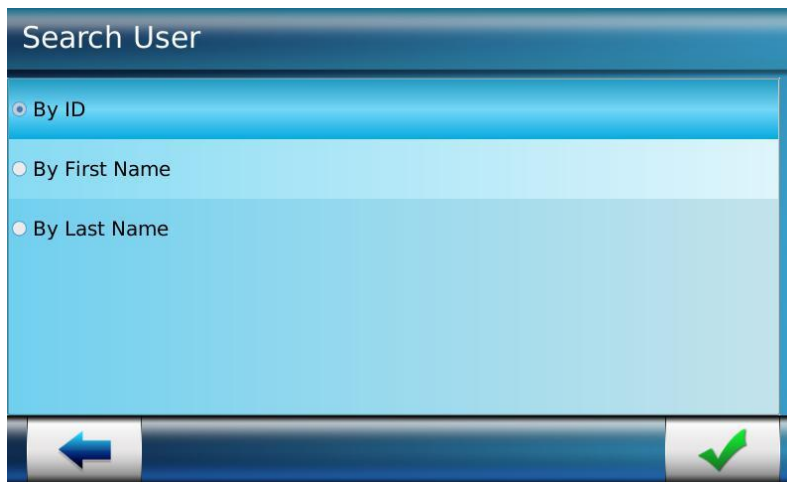


Figure 79: Selecting Search Criteria



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



Figure 80: 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

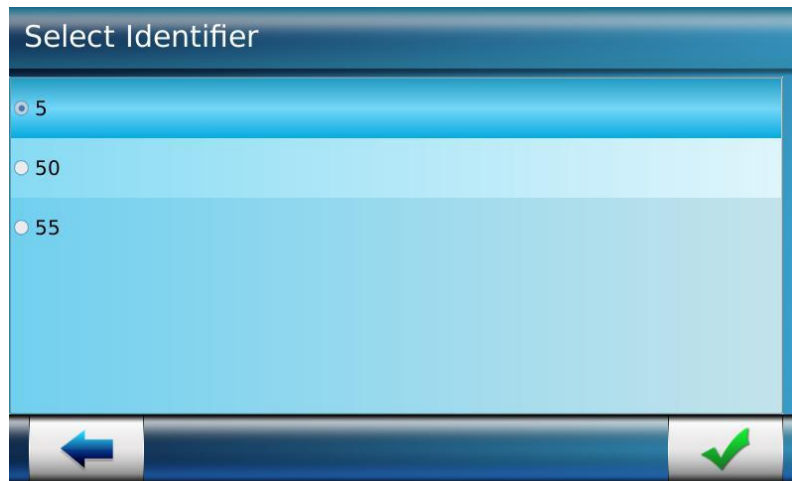



Figure 81: Selecting User ID

5. The list of User IDs matching enter id will be displayed. **Select User ID** from the list and Press on Save button



Figure 82: Enrolment Information screen is displayed for editing

6. Enrolment Information screen is displayed. An administrator can update below information:
 - a. First Name and Last Name of the user
 - b. Capture Fingerprints
 - c. Update Admin Rights

- d. Update User Pin
 - e. Assign Job Code
 - f. Configure Access Schedule
 - g. Set Observe Holiday Schedule
 - h. Set Door Open Timeout
 - i. Set Infinite Expiry Date
 - j. Configure Authorized list
 - k. Configure VIP User
 - l. Configure User Rules
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

Using this functionality, an administrator can authenticate user. This feature can be used by administrator to test whether the enrolled user is allowed access or not.

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

Access Path

User Menu > Authenticate User

Screens & Steps

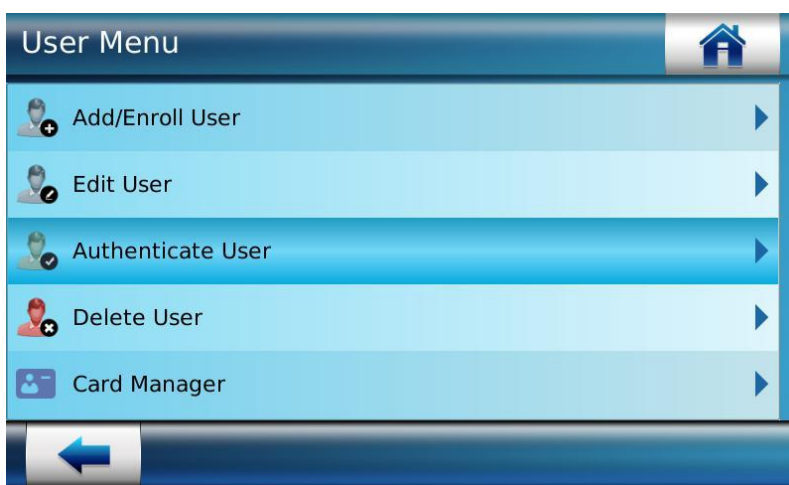


Figure 83: Authenticate User

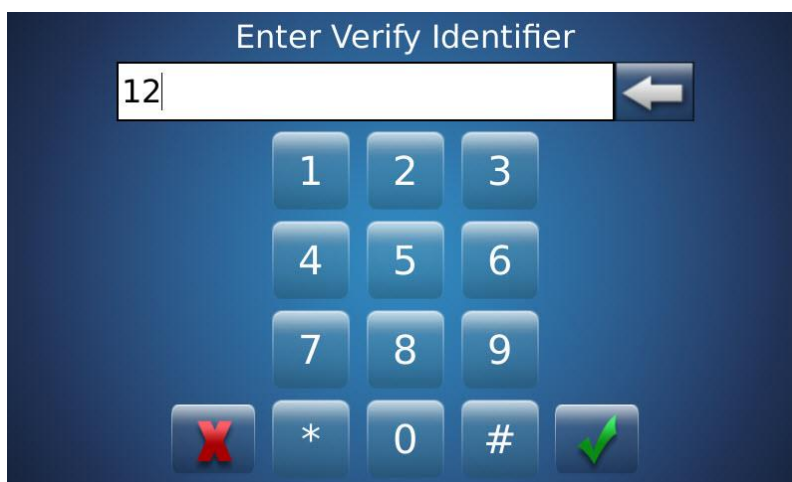



Figure 84: Entering User ID for authentication

1. Enter the **User ID** that is required to be authenticated and Press on 
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

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

User Menu > Delete User > Delete User

Screens & Steps

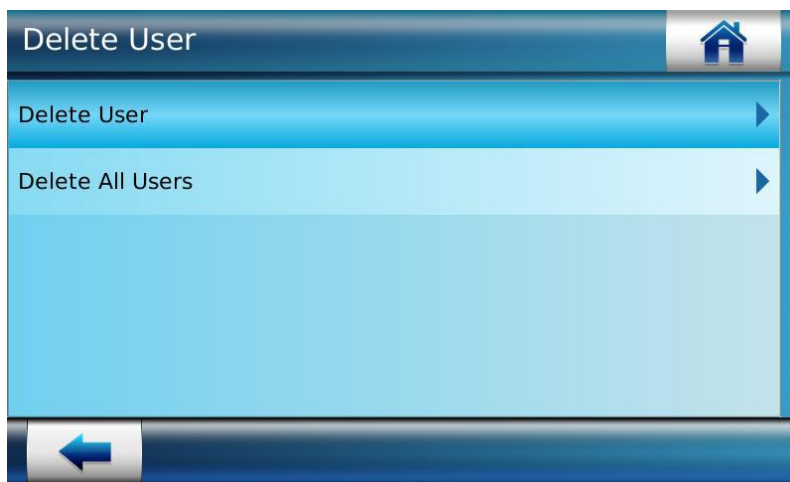


Figure 85: Deleting User

1. Select **Delete User**, if an administrator require to delete a single user



Figure 86: Searching User ID

2. Enter the **User ID** that an administrator need to delete

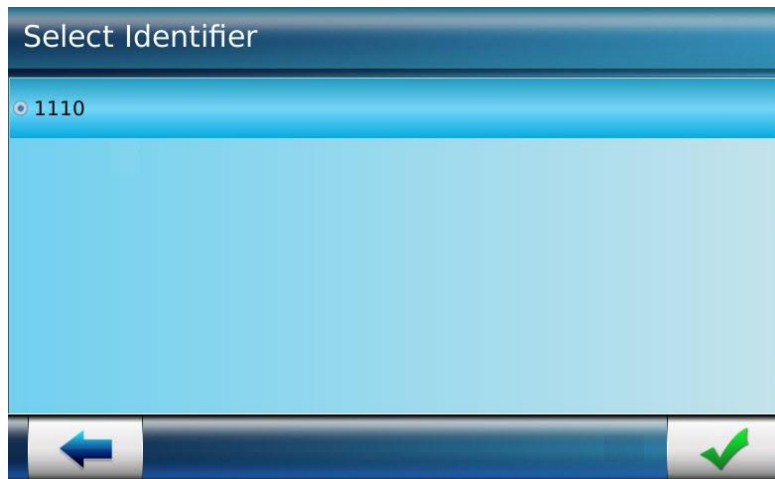



Figure 87: Deleting User ID

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

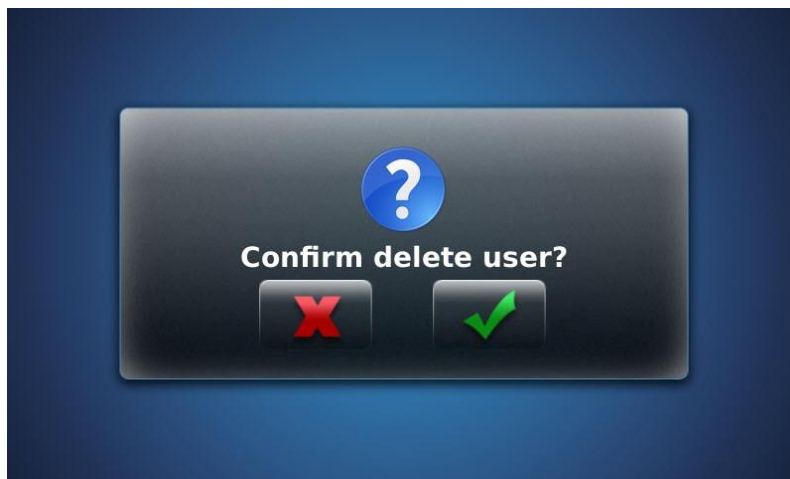



Figure 88: A confirmation message pop up for delete

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

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

Access Path

User Menu > Delete User > Delete All User

Screens & Steps

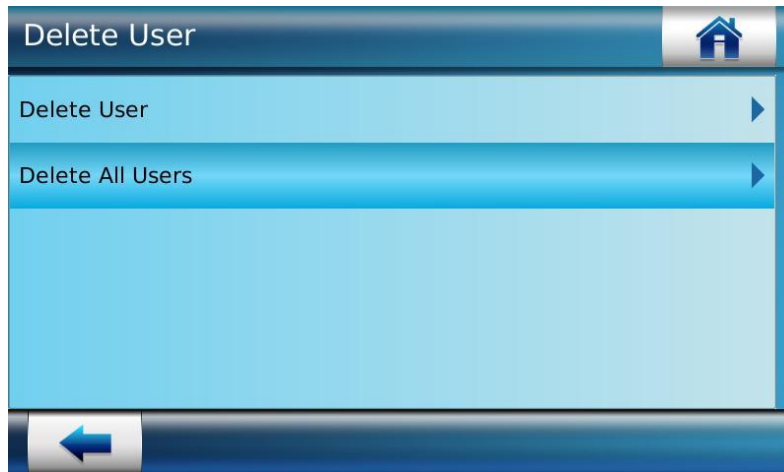


Figure 89: Select Delete action

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

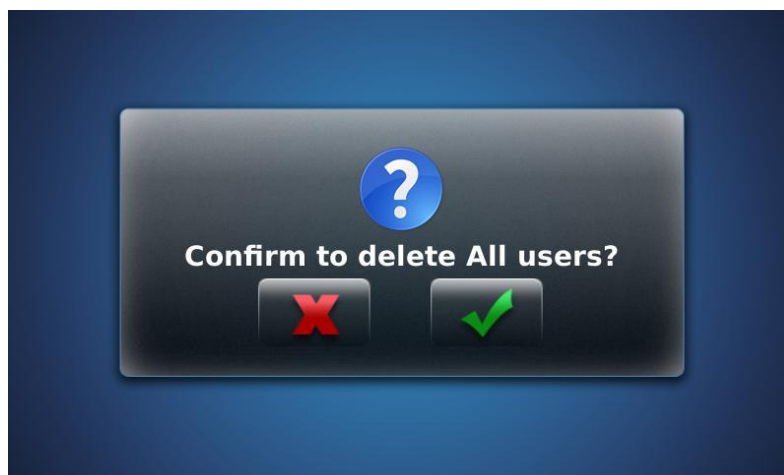



Figure 90: Confirm All User Deletion

2. A confirmation message is displayed, asking 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

Card Manager

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

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

Access Path

User Menu > Card Manager

Screens & Steps

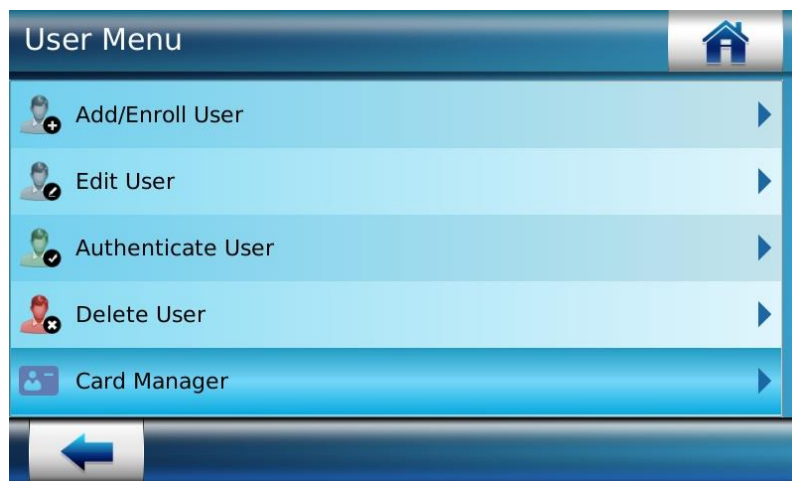


Figure 91: Accessing Card Manager

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

Renewal of User Card

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

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

Access Path

User Menu > Card Manager > Renewal User Card

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

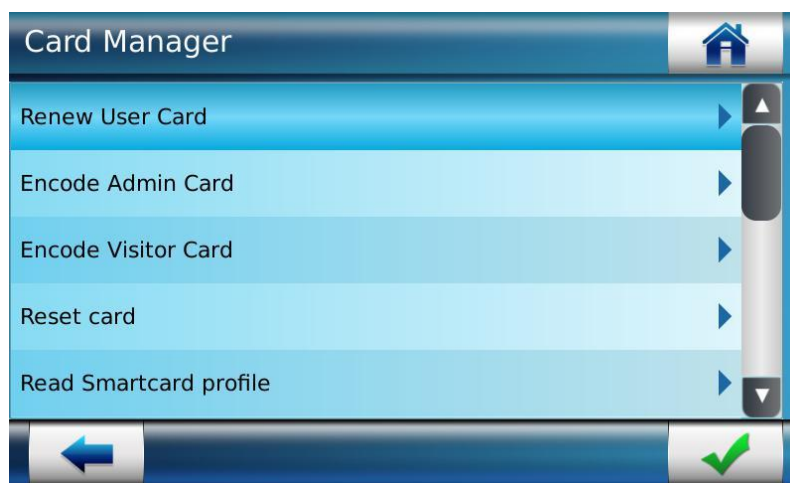


Figure 92: Renewal of User Card

1. Select **Renew User Card**

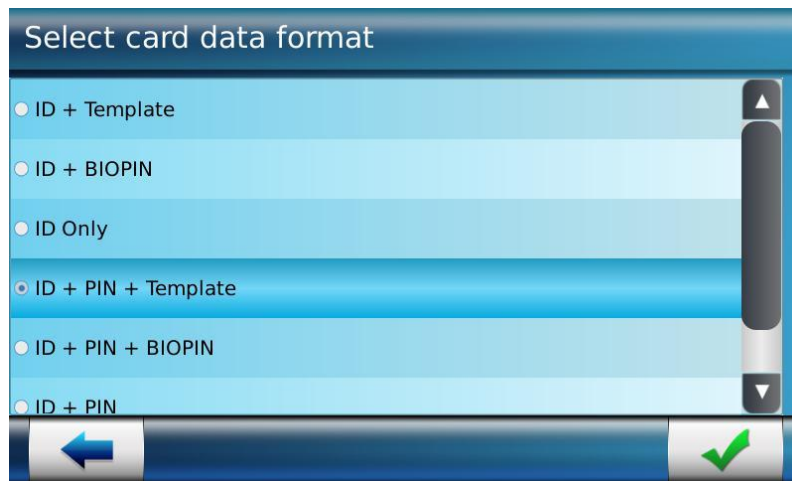


Figure 93: Select Card Data Format

2. Select the card data format from available options as below:
 - a. ID + Template (fingerprint)
 - b. ID + BIOPIN
 - c. ID Only
 - d. ID + PIN + Template
 - e. ID + PIN + BIOPIN
 - f. ID + PIN
3. Press on check box to move next

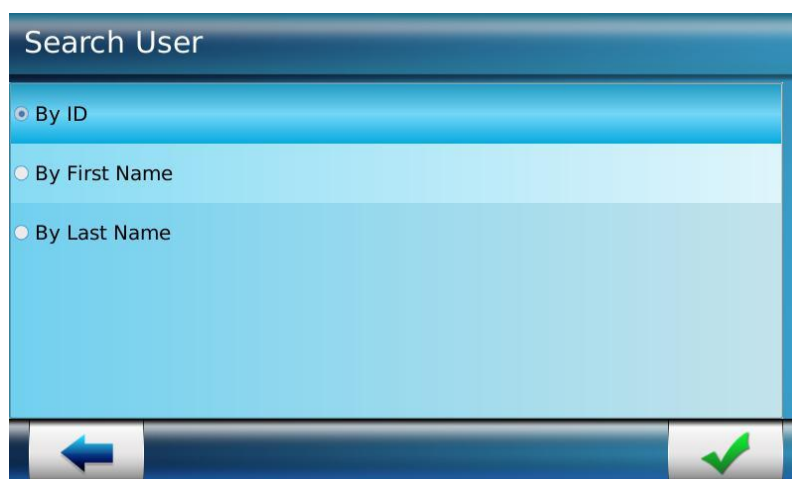


Figure 94: Select search criteria

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



Figure 95: Entering User ID to be searched

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

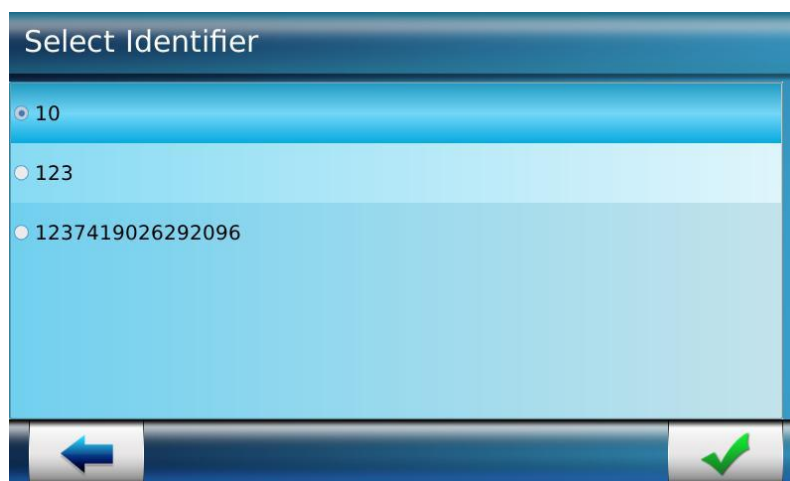


Figure 96: Selecting User ID

7. The list of User IDs matching the first characters entered in search criteria is displayed. Select a **User ID**, that an administrator need to write on card
8. Press on check box to move ahead
9. Terminal will ask for placing the card on card reader. **Place card**

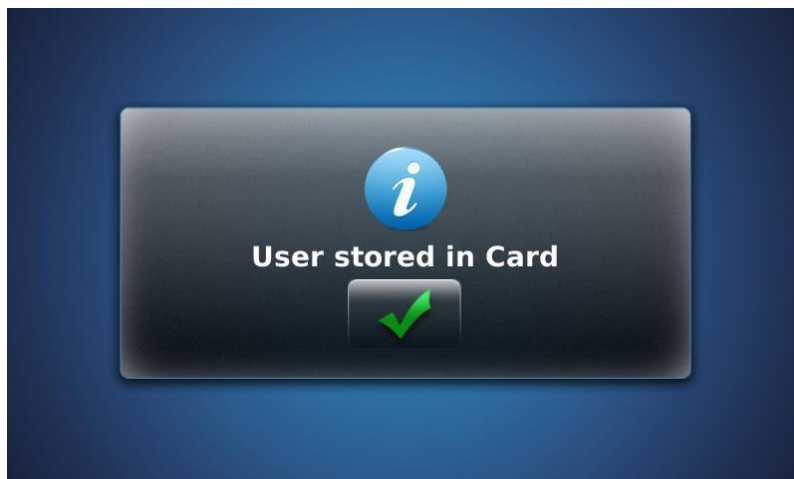


Figure 97: A success message is displayed showing user is stored in card

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 premise. In such scenario, an Administrator card can be used to change the site key in other terminals.

Encode Administrator card feature allows an administrator to store contactless site key in the card. The same site key can be copied to other terminals, using Administrator card.

NOTE: On changing site key using Administrator card, the terminal should support the same card type. For example, using MIFARE® Administrator card an administrator can change site key of the terminal that supports MIFARE® card. But an administrator cannot change site key of MorphoAccess® SIGMA Series iCLASS® terminal that supports only iCLASS® cards.

Access Path

User Menu > Card Manager > Encode Administrator 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

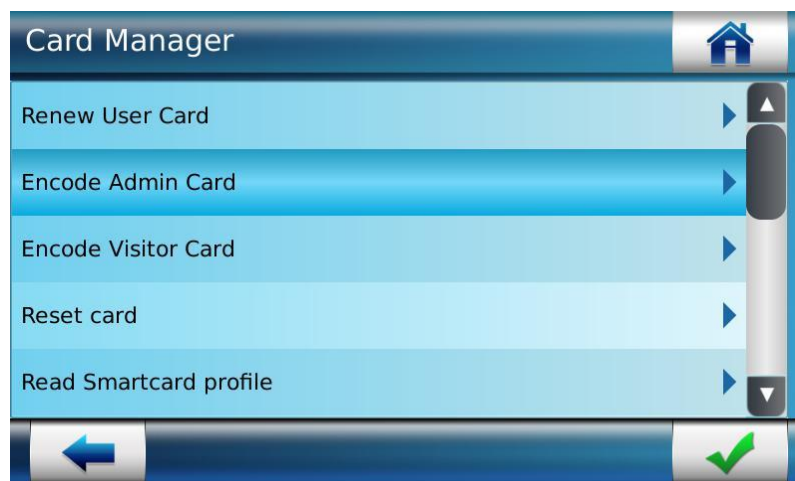


Figure 98: Encoding Administrator card


1. Select **Encode Administrator card**



Figure 99: 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: On encoding MIFARE® 1K and MIFARE® Plus 2K Cards, if no. of start block is set as 20 or more, then an error 'Error in Encoding Administrator card' is displayed. Refer to "*No. of Start Block for MIFARE® Cards*", to know how to configure no. of start block.

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

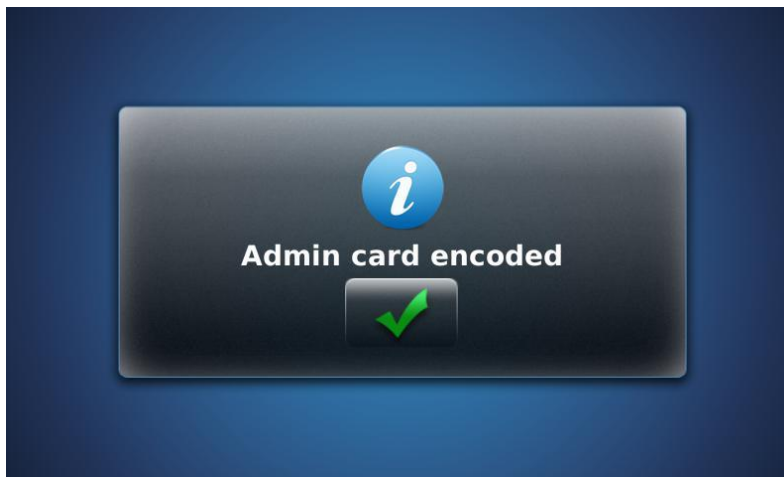


Figure 100: Administrator card is encoded

Results

A success message is displayed showing card is encoded. The site key in the terminal is copied in the administrator card. Using same administrator card, the site key of other terminals can be changed.

Encode Visitor Card

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

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

Access Path

User Menu > Card Manager > Encode Visitor Card

Pre-requisites

- Card Format for Visitor Card is forced to ID only

Screens & Steps

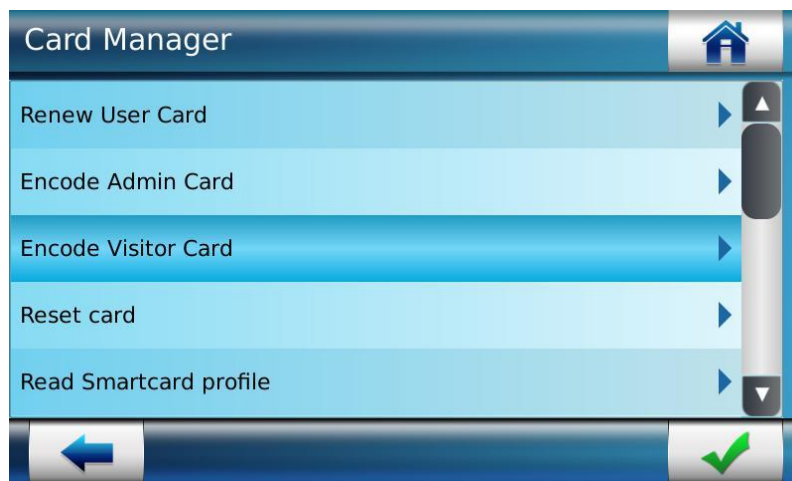


Figure 101: Encoding Visitor Card

1. Select **Encode Visitor Card**



Figure 102: User ID for Visitor Card

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

NOTE: Contactless card CSN can also be used as User ID, it can be set using parameter. Refer to “Smart Card” section in **MorphoAccess® SIGMA Series Parameters Guide**.

3. Press on check button
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

Smart Card Read Profile

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

Access Path

User Menu > Card Manager > Smart Card Read Profile

Screens & Steps

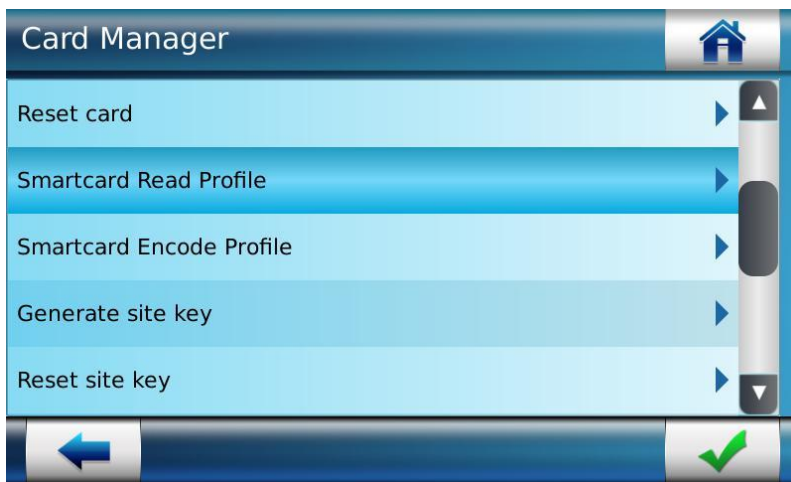


Figure 103: Smartcard Read Profile

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



Figure 104: Smartcard Read Profile_Multi

b. In case of iClass product.

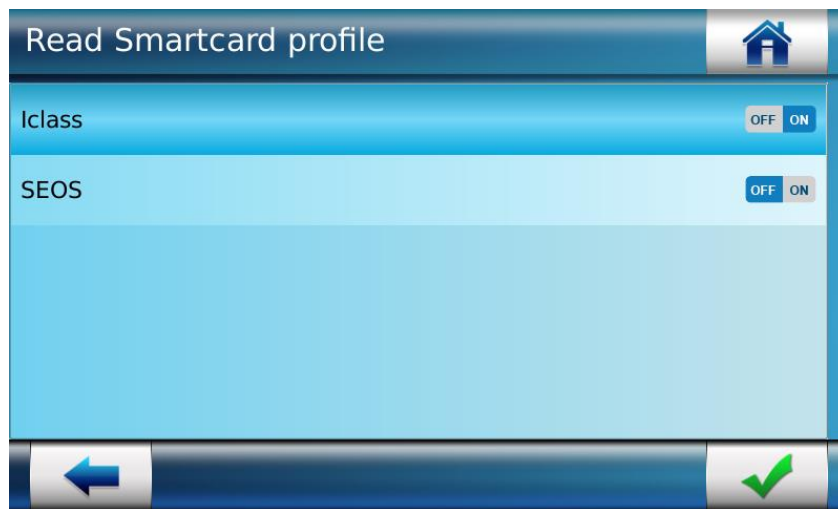


Figure 105: Smartcard Read Profile_iClass

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

→ In case of Multi Product

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

→ In case of iClass Product

- a. IClass®
- b. IClass®SE

3. Press on check button to save configuration

Smart Card Encode Profile

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

Access Path

User Menu > Card Manager > Smart Card Encode Profile

Screens & Steps



Figure 106: Smartcard Encode Profile

1. Select Smart card encode profile

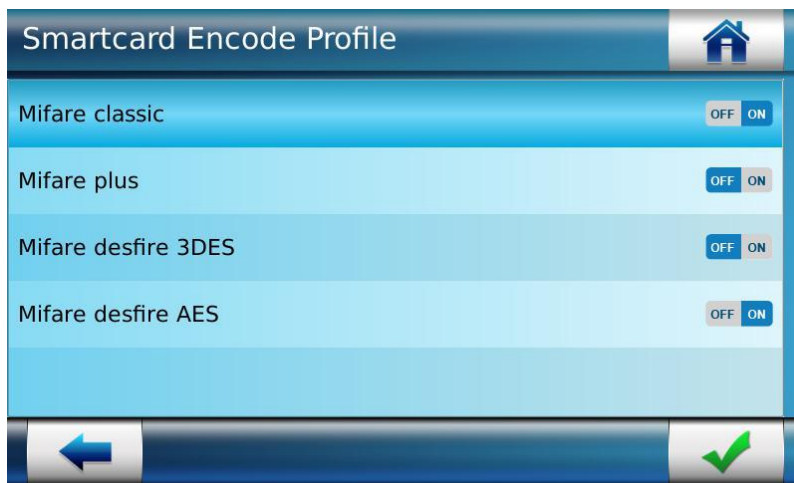


Figure 107: Smartcard Encode Profile

2. Set the following smartcards encode profile as ON, if an administrator require terminal to encode them:
 - a. MIFARE® Classic
 - b. MIFARE® Plus
 - c. MIFARE® DESFire® 3DES
 - d. MIFARE® DESFire® AES

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

3. Press on check button to save configuration

Generate Site Key

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

Access Path

User Menu > Card Manager > Generate Site Key

Screens & Steps

1. Select **Generate Site Key**



Figure 108: Selecting Card Type


2. Select the **Card Type**, for which site key is to be generated. Options are MIFARE® Classic, MIFARE® Plus, DESFire® 3DES, and DESFire® AES
3. Press on “” button to save and next



Figure 109: Generating Site Key

4. Enter the **Passphrase**, using keyboard
5. Use check button to save

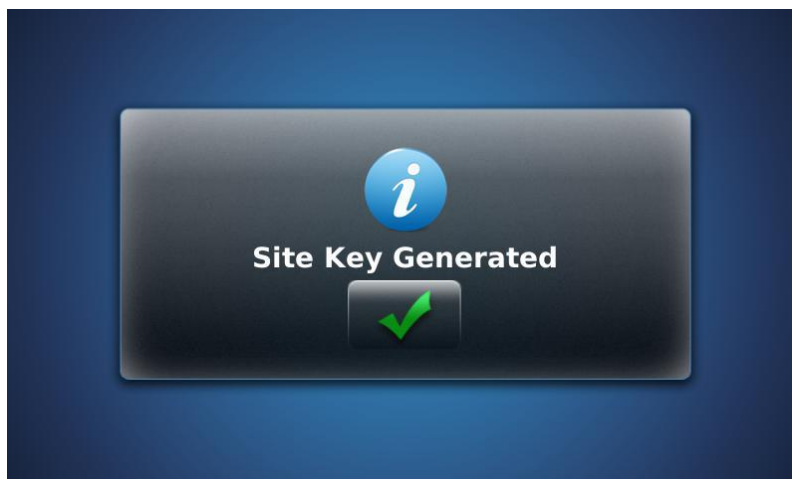


Figure 110: Success message is displayed showing site key is generated in the terminal

Reset Site Key

Using this functionality, an administrator can reset security keys stored in terminal to factory default settings. An administrator can select the card type from the available card types.

Access Path

User Menu > Card Manager > Reset Site Key

Screens & Steps

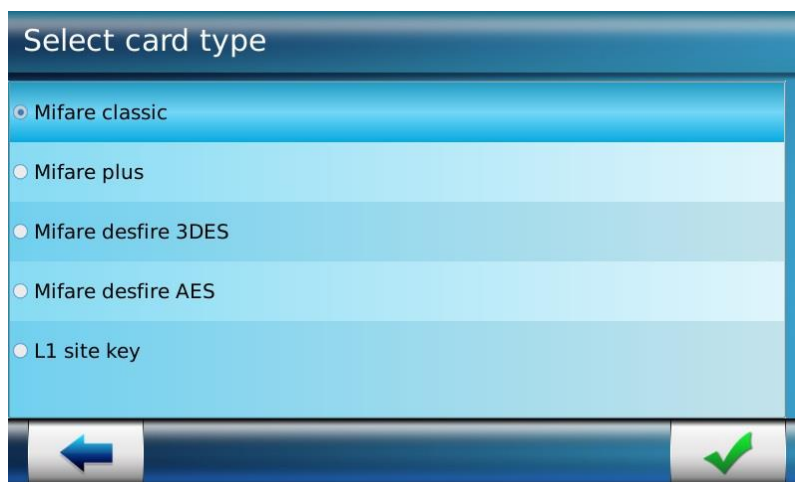



Figure 111: Resetting keys in selected cards

1. Select card type to be reset
 - a. MIFARE® Classic
 - b. MIFARE® Plus
 - c. MIFARE® DESFire® 3DES
 - d. MIFARE® DESFire® AES
 - e. L1 Site Key (not applicable in Legacy Morpho 'MA500' mode)
2. Use “” to save settings

Configure ELITE Mode

Using this functionality, an administrator can configure the iClass terminal in ELITE mode. An administrator can select the options to enable and/or disable ELITE mode. On enable terminal start accepting specific iCLASS card, ELITE card and start rejecting regular cards. There are two steps and two configuration card, to enable/disable this functionality as Key Roller Card & Configuration Card. This is applicable to only iClass terminal.

Access Path


User Menu > Card Manager > Present Key Roller Card

User Menu > Card Manager > Present Configuration Card

Screens & Steps to Enable ELITE Mode




Figure 112: 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. Check that terminal display Hold Card and than Remove Card
2. Select Present Configuration Card
 - a. Terminal will ask to Place Card.
 - b. Present the "Configuration card STD->Elite" Card
 - c. Check that terminal display Hold Card and than Remove Card
3. Use "" to save settings
4. Now terminal will accept iCLASS Card encoded with ELITE Key reject iCLASS – Standard Cards.

Screens & Steps to Disable ELITE Mode



Figure 113: Disable ELITE Mode

1. Select Present Key Roller Card
 - a. Terminal will ask to Place Card.
 - b. Present the “Key roller card Elite->STD” Card
 - c. Check that terminal display Hold Card and than Remove Card
2. Select Present Configuration Card
 - a. Terminal will ask to Place Card.
 - b. Present the “Configuration card Elite->STD” Card
 - c. Check that terminal display Hold Card and than Remove Card
3. Use “” to save settings
4. Now terminal will accept iCLASS – Standard Cards and reject iCLASS Card encoded with ELITE Key.

No. of 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 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, then insure that administrator data is stored from the same block number as user data on user cards.

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

User Menu > Card Manager > No. Of Start Block

Screens & Steps

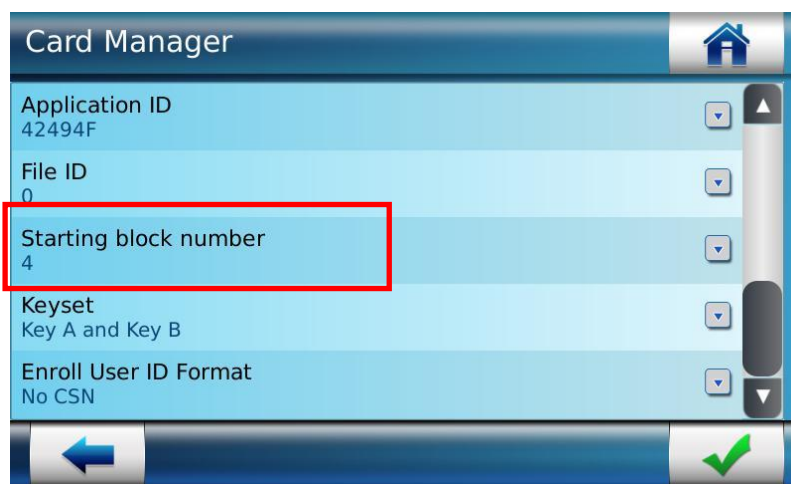


Figure 114: Setting No. of Start Block

1. Select **No. Of Start Block**
2. On next screen an administrator can enter the start block number using keypad
3. Tap check button to save changes

Select Keypset for Reading MIFARE® Cards

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

- Keys A only,
- Keys B only,
- Keys A then Keys B if failed

Access Path

User Menu > Card Manager > Key set

Screens & Steps

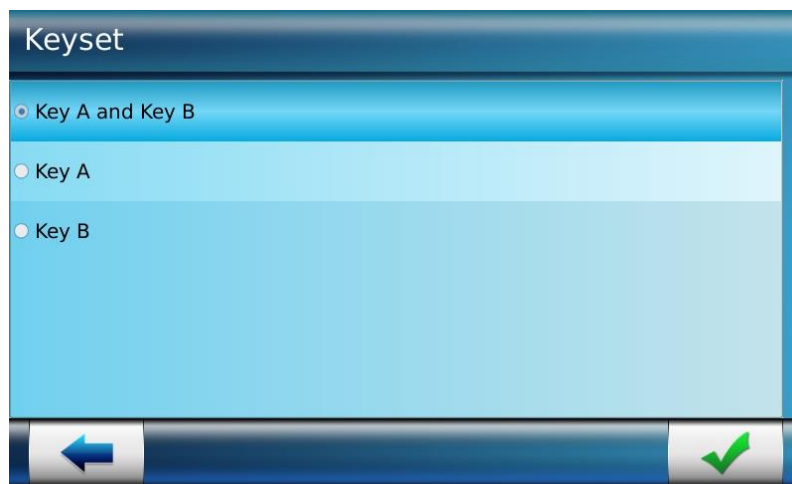


Figure 115: Keypset configuration

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

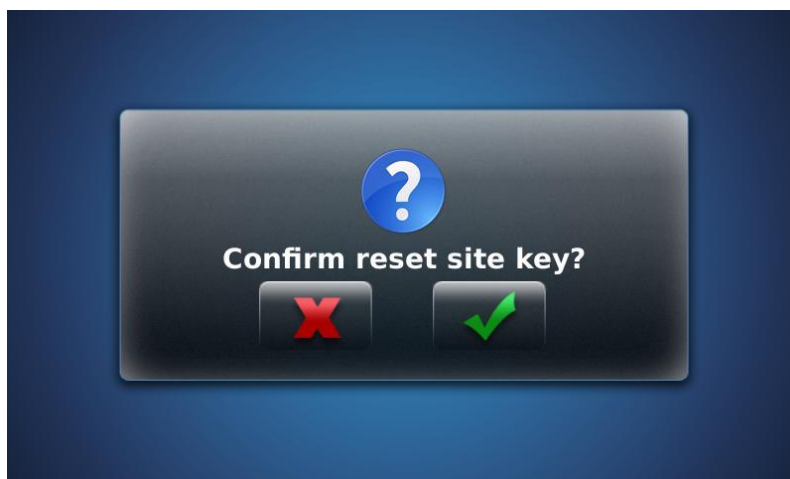


Figure 116: Confirming reset key action

3. Confirm reset site key action

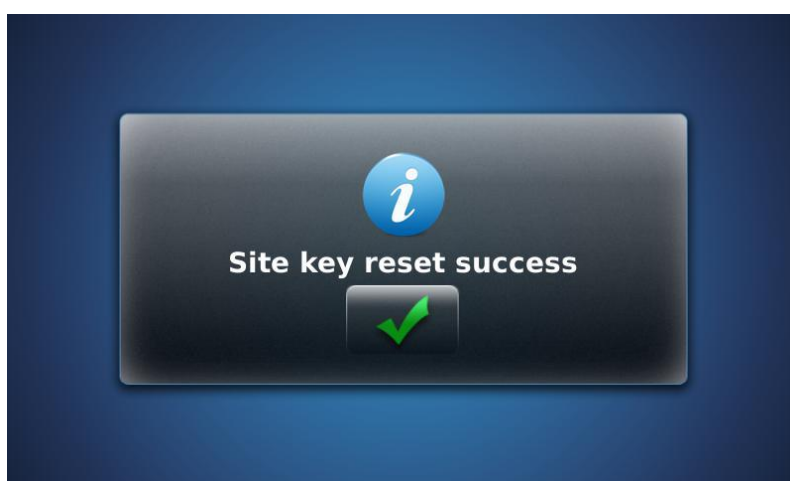


Figure 117: Site Key is reset successfully

Select Enroll ID Format

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

Access Path

User Menu > Card Manager > Enroll User ID Format

Screens & Steps



Figure 118: Selecting Enroll User ID Format

4. Select Enroll User ID Format

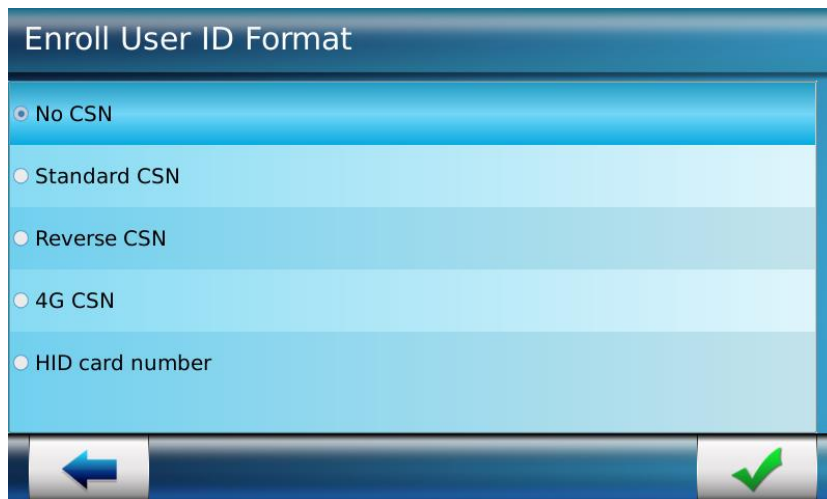


Figure 119: Selecting Enroll User ID Format

5. 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 CSN:** If this option is selected, the read contactless card serial number is manipulated as per 4G terminal. Manipulation is as per given below.

e.g.

Step 1 : CSN read from the card.

```
if (ICLASS)
{
    //Reverse all the bytes in case iclass card
}
else
{
    //Do not reverse
}
```

Step 2:

```
if(MIFARE) // 4 Byte CSN card
{
    //generate decimal from 4 Byte CSN.
}
else if(DESFire) // OR any 7 BYTE CSN card
{
    //Add 0 in beginning of CSN
    //reverse the first 4-bytes and reverse the next 4-bytes.
    //reverse the whole 8-byte after above manipulation
    //generate decimal from the manipulated HEX
}
else //ICLASS CARD
{
    //reverse the first 4-bytes and reverse the next 4-bytes.
    //reverse the whole 8-byte after above manipulation
    //generate decimal from the manipulated HEX
}
```

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

NOTE: This option only available in iClass product.

- f. **Reverse HID card number:** if this option is selected, terminal reverses the HID card number read from the iClass card.

NOTE: This option only available in iClass product and can only 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 :

111000000001001011111111111101100000001001011011000100111111111

Truncated value, using interface we propose, with programmed start bit to 11 and length to 53

CSN Binary value : 1001011111111111101100000001001011011000100111111111

ID Decimal value: 5348003102427647

- These keys are only accessible from PC Application or Web Server.

Defining Application ID and File ID for DESFIRE® Cards

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

Access Path

User Menu > Card Manager > Application ID

And

User Menu > Card Manager > File ID

Screens & Steps

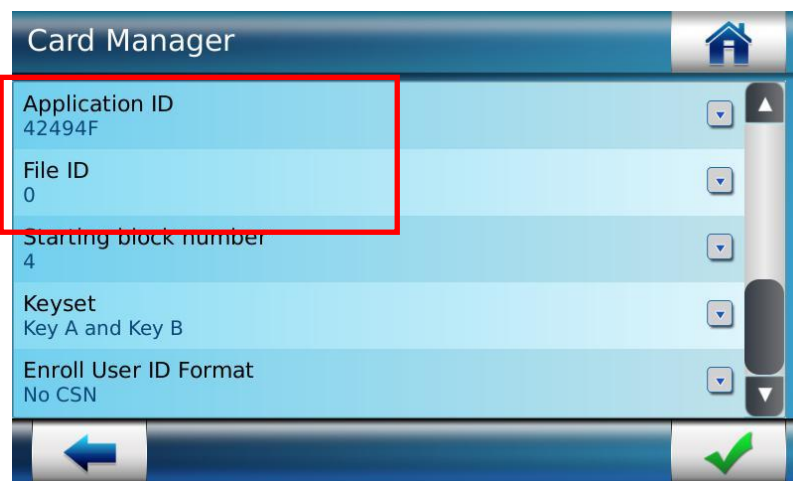


Figure 120: Configuring Application ID and File ID

1. Select **Application ID**
2. Enter Application ID from range of 0x000001-0xFFFFFFFF. 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

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

Access Path

User Menu > Card Manager > Offset

Pre-requisites

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

Screens & Steps

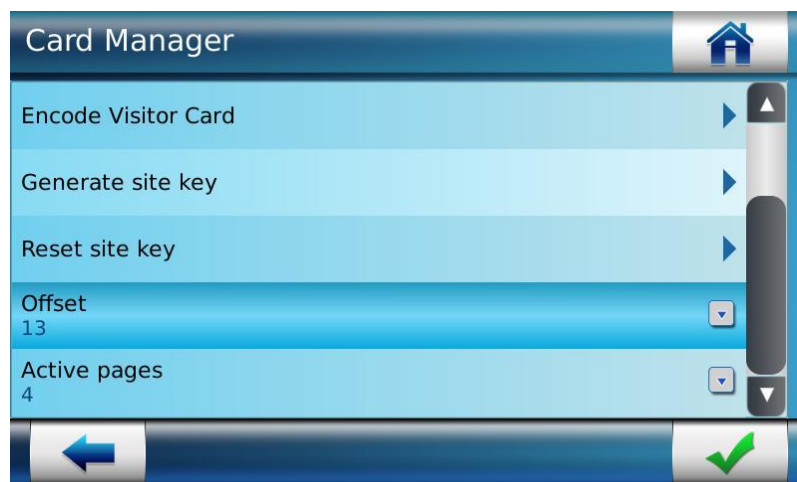


Figure 121: Set Key Offset for iCLASS® cards

1. Press on **Offset**



Figure 122: Set Key Offset

2. Enter **Offset value**. An administrator can configure offset from 0x13 to 0x9F (hex values)
3. Use check button to save the Offset value

Defining Active Pages for Reading iCLASS® Cards

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

Access Path

User Menu > Card Manager > Active Page

Pre-requisites

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

Screens & Steps

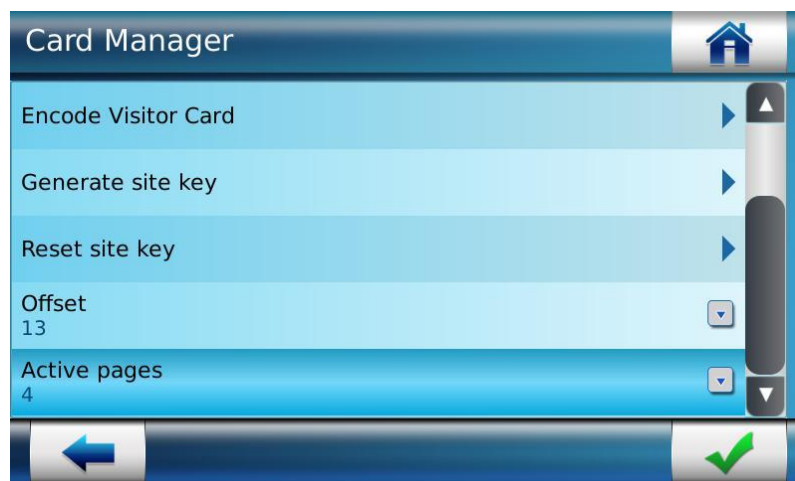


Figure 123: Configure Active Pages for iCLASS® cards

1. Select **Active Pages**



Figure 124: Enter Active Pages

2. Enter number of **Active Pages**
3. Select check button to save

Reset Card

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

Access Path

User Menu > Card Manager > Reset Card

Pre-requisites

- A smart card has a 2 templates with Id and biometric data
- Card is secured with the same key as on terminal

Screens & Steps

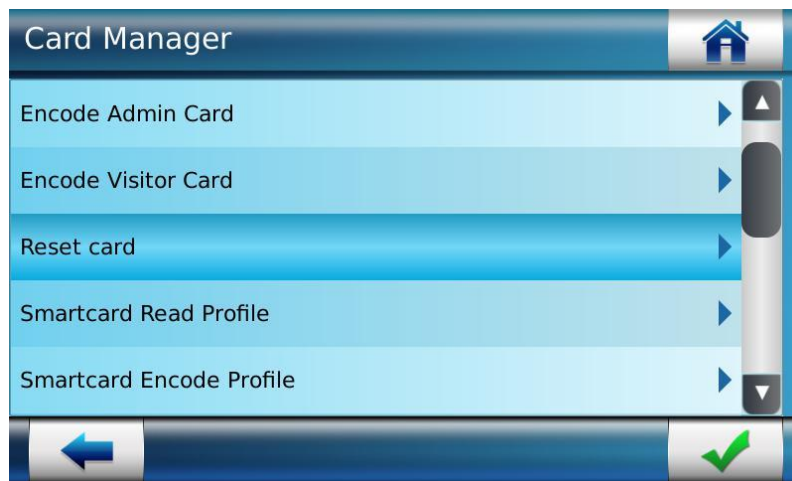


Figure 125: Reset card

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

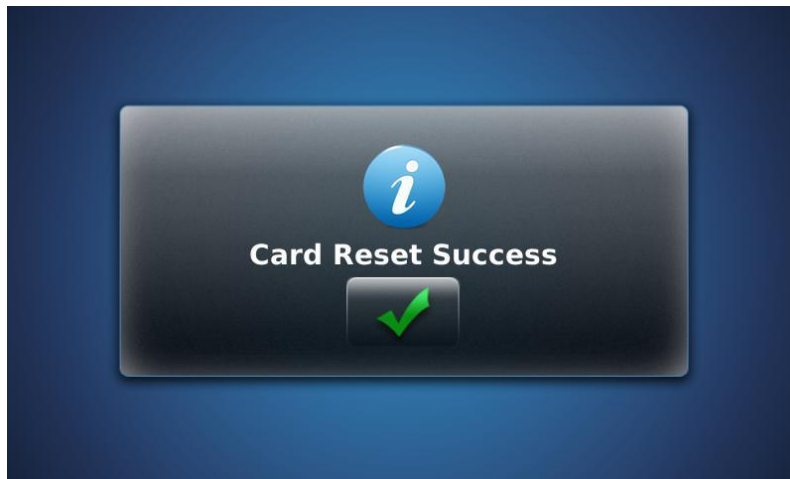


Figure 126: Success message is displayed showing card is reset successfully

Results

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

Multimedia menu

Using multimedia menu, an administrator can upload and manage audio, video and images on MorphoAccess® SIGMA Series terminal. These multimedia contents are used at various actions. For example Audio is used to be played as alarm on occasions like Tamper.

In below sections an administrator will learn how an administrator can upload the multimedia content in the terminal and the supported formats. Terminal can play multimedia files contained in **MKV** (video), **WEBM** (video), **OGG** (audio), and **WAV** (audio) container.



Figure 127: Multimedia Menu

Audio Settings

MorphoAccess® SIGMA Series Terminal is able to play sound on following actions:

- **Access Denied:** Audio is played when user verification is 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:

- Upload Audio files using USB mass storage device to the folder of the above listed actions
- Set the volume at which the sound should be played
- Remove an audio file from the folders of the above listed actions. This will lead to no sound play on action performed

Access Path

Multimedia Menu > Audio

Pre-requisites

- USB mass storage device must be properly initiated. It means USB mass storage device must have same folder structure as displayed in terminal. E.g. Audio to be played on tamper detection, should be stored in 'Tamper' folder. Refer "*Initialize USB Mass Storage device*" section to view 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 audio messages must be in the same language, as configured in terminal

Screens & Steps

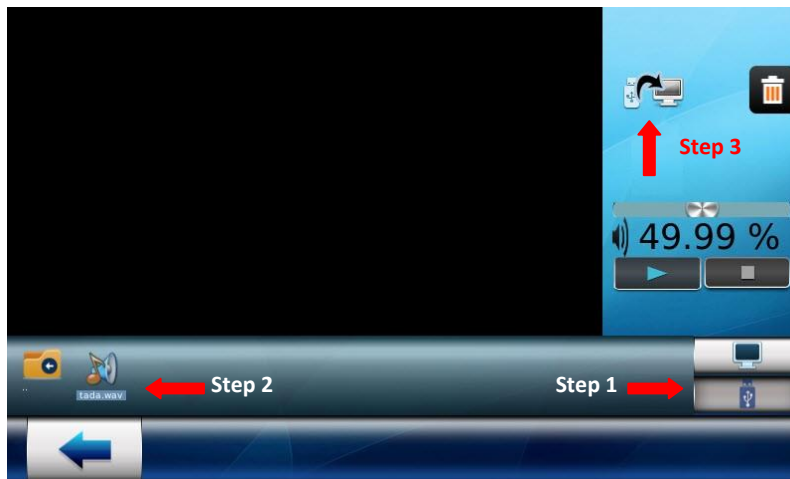



Figure 128: Uploading Audio File in device

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



Figure 129: Confirmation Pop-up

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

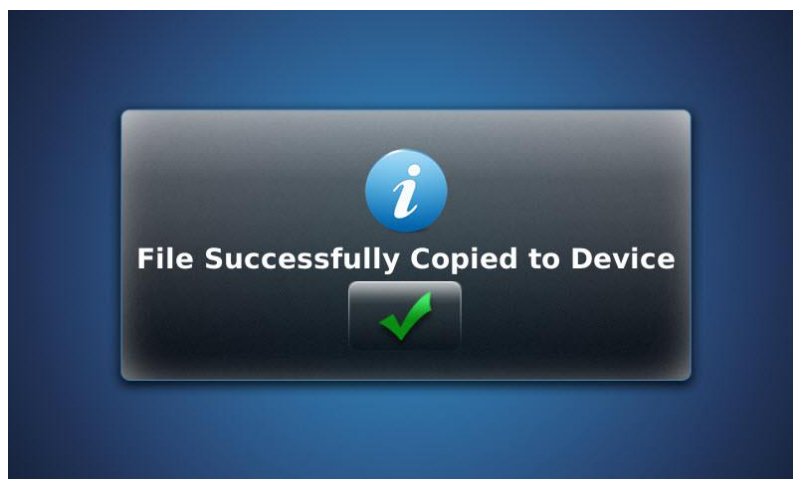


Figure 130: Success message is displayed

Results

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

Using “” button an administrator can **Delete** an audio file.

Video Settings

MorphoAccess® SIGMA Series terminal is capable of playing video when screen is idle. Using Video settings an administrator can configure below:

- Upload Video files using USB mass storage device
- Set the volume at which the sound should be played
- Remove video file. This will lead to no video play on screen idle

Access Path

Multimedia Menu > Video

Pre-requisites

- USB mass storage device must be properly prepared. It means USB mass storage device must have same folder structure as displayed in terminal. E.g. Video to be played on idle screen time out should be placed under 'Idle Screen' named folder. Refer "[Initialize USB Mass Storage device](#)" section to view how to initialize a USB mass storage device.
- The maximum supported Video file size is up to 10MB
- Supported Video files formats are MPEG-4 and VP8

Screens & Steps

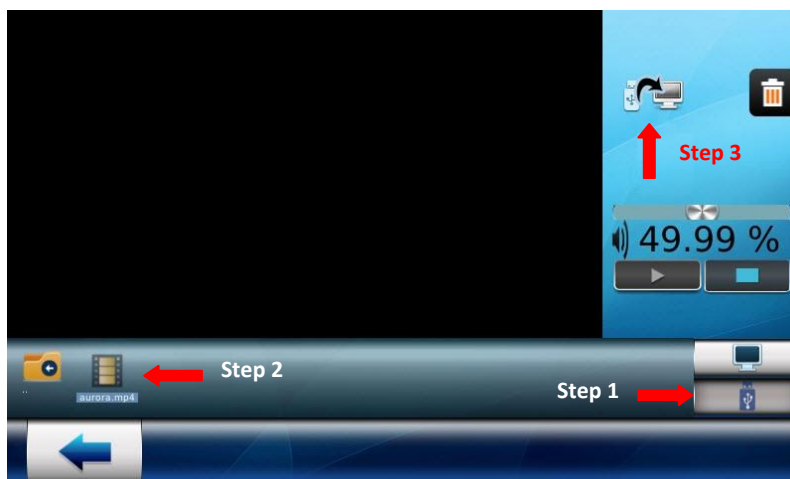



Figure 131: Uploading Video File in device

1. Select **USB Mode**
2. The folders present in USB mass storage device will be displayed
3. Select a **Video File** that is required to be uploaded on terminal

4. An 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 132: Confirmation Pop-up

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

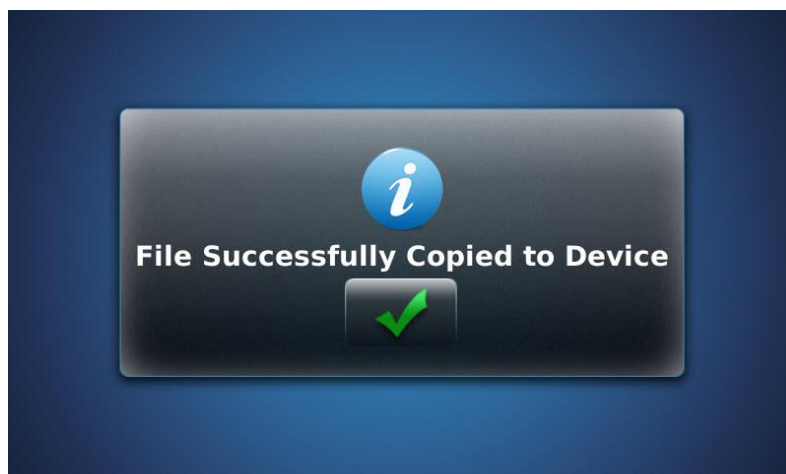


Figure 133: Success message is displayed

Results

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

Using “” button an administrator can **Delete** a video file.

References

- Refer to “Set Idle Screen Time Out” parameter under LCD Configuration
- To set duration of playing video, refer parameter “Set Infinite Video Play” under LCD Configuration.

Images Settings

MorphoAccess® SIGMA Series terminal is capable of displaying images on the LCD screen. The images can be used for purposes listed below:

- **Dynamic Message:** The dynamic message image is shown when a specific user access is granted. It is displayed only if parameter “Dynamic Message Configuration” is set as ON at the time of user enrolment. It is a pre-requisite to have SD card attached to the terminal, for activating dynamic message feature.
- **Wallpaper:** To set wallpaper to be displayed on home page.

Using Image Settings, an administrator can perform below actions:

- Upload image files using USB mass storage device
- Remove image file. This will lead to no image display

Access Path

Multimedia Menu > Image

Pre-requisites

- USB mass storage device must be properly initiated. It means USB mass storage device must have same folder structure as displayed in terminal. E.g. image to be played on wallpaper should be placed under wallpaper named folder. Refer “[Initialize USB Mass Storage device](#)” section to view how to initialize a USB mass storage device.
- Terminal can support Image file formats such as JPEG, GIF, PNG, and BMP

Screens & Steps

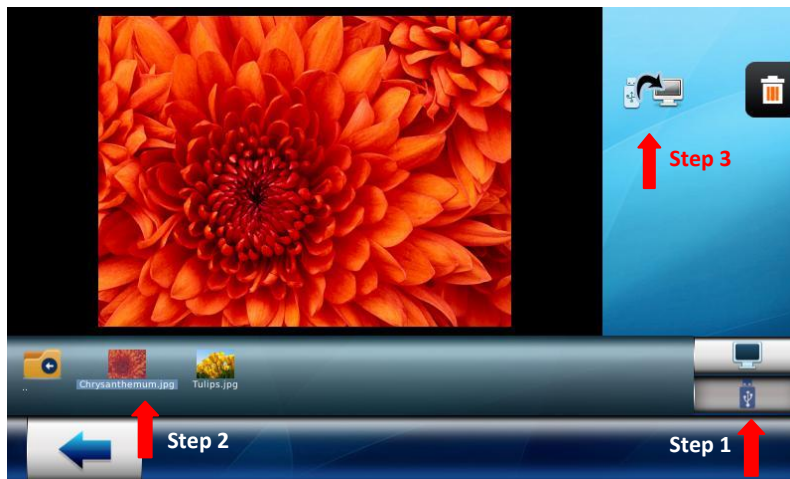



Figure 134: Uploading Image File in device

1. Select **USB mode**
2. The folders present in USB mass storage device will be displayed
3. Select an image file that is required to be uploaded on terminal
4. Press on **Copy** button (Step 3 in above figure) to copy file from USB mass storage device to Terminal



Figure 135: Confirmation Pop-up

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

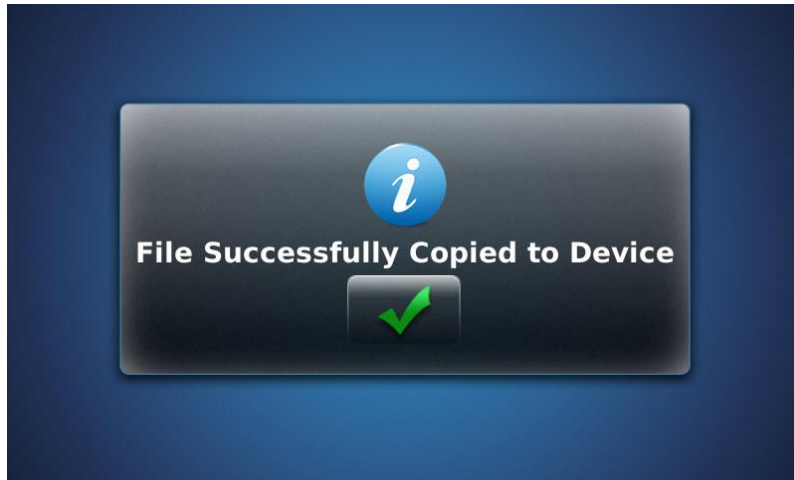



Figure 136: Success message is displayed



Figure 137: 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.

Using “” button an administrator can select and **Delete** images.

System Menu

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

Only an administrator with full administrative rights can access this menu.



Figure 138: System Menu

Terminal Configurations

Set Factory Default

This functionality is used for resetting all the parameters of MorphoAccess® SIGMA Series terminal to their default value. An administrator can also select particular parameters manually, for which values are needed to be reset as factory default value.

Access Path

System Menu > Terminal Settings > Set Factory Default

Screens & Steps

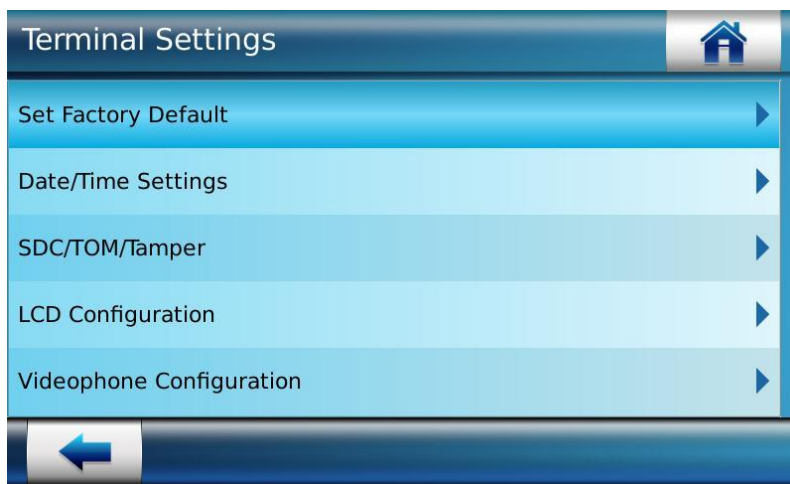


Figure 139: Reset Factory Default Settings

1. Select **Set Factory Default**

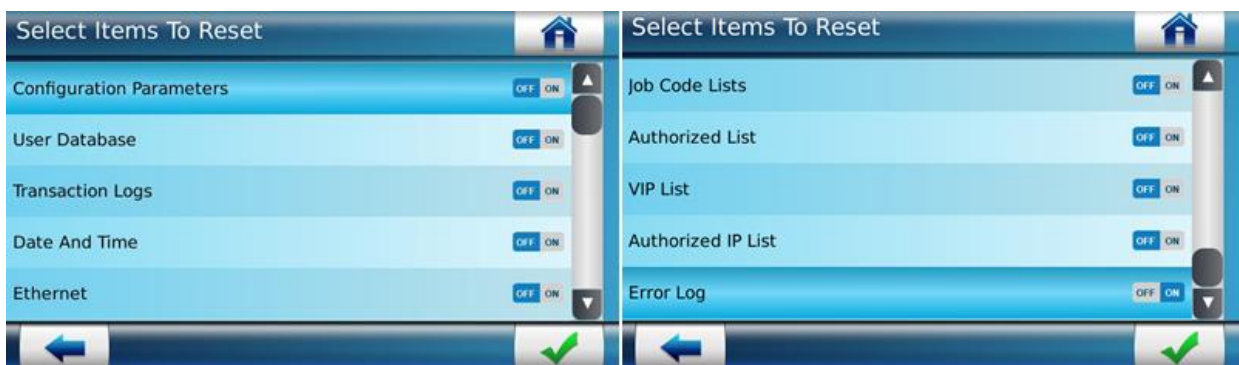


Figure 140: Select Items to reset

2. An administrator can select parameters from the list and set as ON. The parameters ON, will be reset.

3. Press on check button to move next

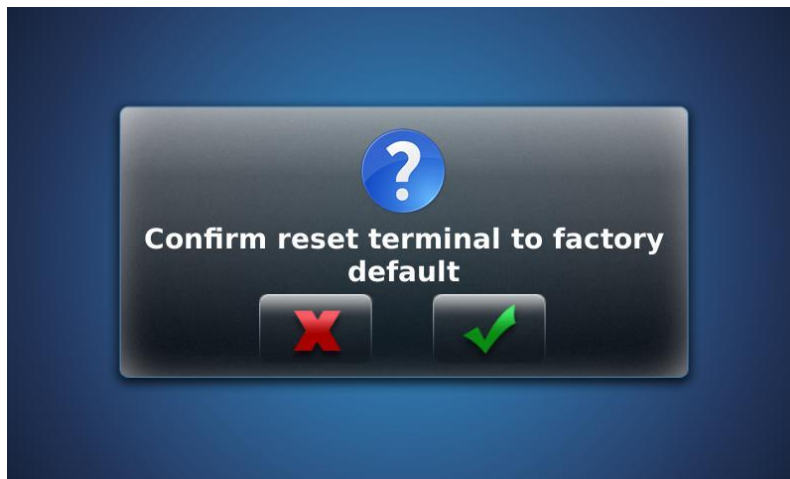


Figure 141: Confirmation message displayed

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 as their default values.

Date and Time Configuration

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

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

Set Time Zone

Access Path

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

Screens & Steps

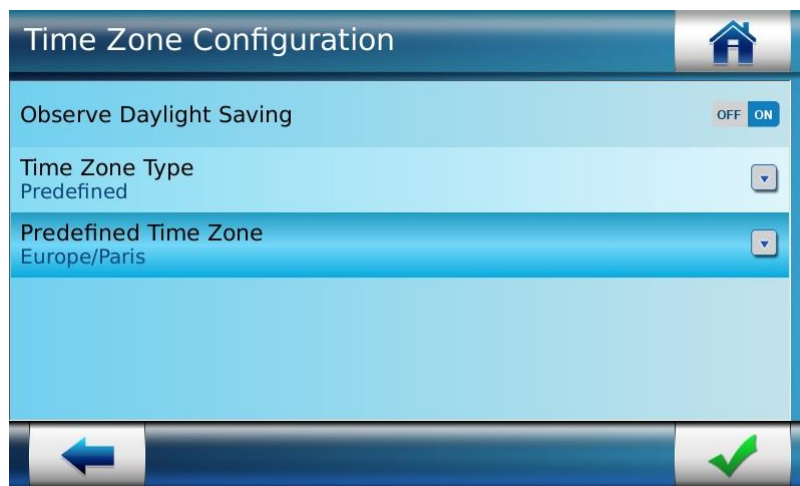


Figure 142: **Configuring Time Zone**

1. Please refer [Date and Time Configuration](#) section step #11 to 21 for more detail.

Results

Time Zone is saved in the terminal. Based on the configuration, the time and date will be calculated. During Daylight Saving, the time will be auto-adjusted.

Set Date

Using this functionality, an administrator can configure the current date in the terminal. An administrator can also select the preferred format of date to be displayed.

Access Path

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

Screens & Steps

2. Please refer "[Date and Time Configuration](#)" section step #1 to 4 for more detail.

Set Time

Access Path

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

Screens & Steps

1. Please refer "[Date and Time Configuration](#)" section step #4 to 9 for more detail.

Results

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

Single Door Controller (SDC) Configuration

Single Door Controller (SDC) is used to control the access through a door when specific actions are triggered on MorphoAccess® SIGMA Series terminal. For example, on successful identification of a user, door must open automatically to allow user access into 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 door panel through input-output lines on action triggered on terminal. By default, GPIO Mode is enabled.

- **GPI:** General Purpose Input (GPI) has three TTL line available, i.e. Line 0, 1 and 2. The GPI line can be configured **to trigger an action on the terminal from distant system**, when set as active (low and/or high).
- An administrator can active 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.
- **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
- **Finger not Detected:** When finger is not detected as per requirement
- **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 section “General Purpose Input Output Configuration” in this document.

SDC Mode:

Single Door Controller (SDC) mode is used 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 for controlling access at a particular door. When SDC mode is enabled, GPIO mode is disabled.

Access Path

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

Screens & Steps

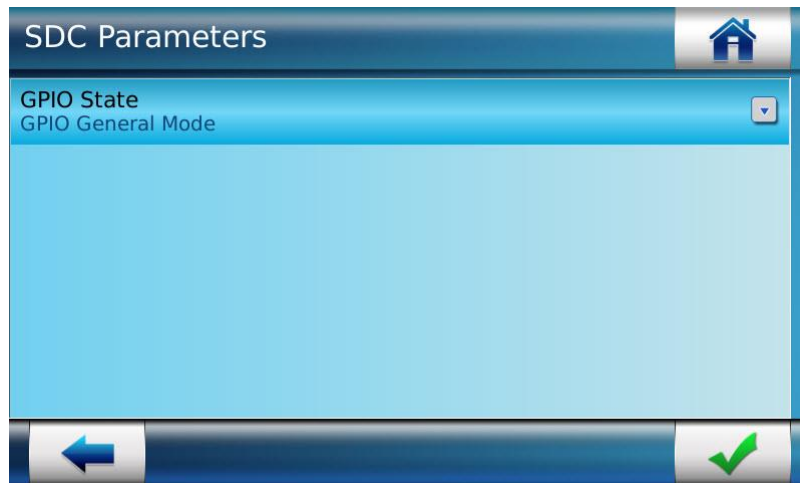


Figure 143: SDC Parameters configuration

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

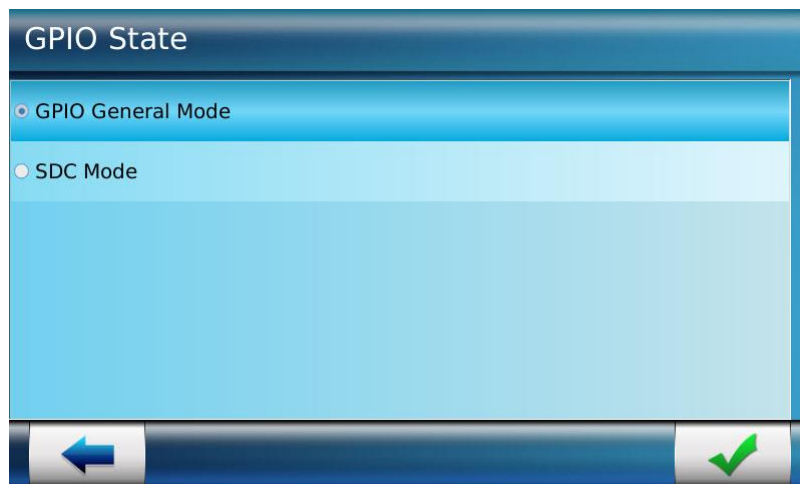


Figure 144: Selecting GPIO State


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 145: Configuring Parameters in “SDC Mode”

Once an administrator select **SDC Mode**, an administrator need to configure below parameters:

4. Press on **Door Unlock Time** field to set duration (in Seconds only) for which the door should be unlocked after access is granted. E.g. if 25 seconds is the Door Unlock Time, then the door will be unlocked for 25 seconds and after that the door will be locked automatically
5. Press on **Door Held Open Duration**, to set the duration (in Seconds only) within which door must be closed. Once Door Unlock Time is exceeded and door is not closed; the terminal will start counting Door Held Open Duration. If user is not closing the door within this duration, an auto-alert “Door Held Open Too Long” will be generated on terminal
6. Select **Exit Mode** as ‘None’, ‘Push button – Manual’, ‘Push button – Electric’
7. When Exit Mode is in ‘Push Button-Manual’, then an administrator needs to set **Egress Time Out**. Within the Egress Time, the door will remain open and on timeout it will lock automatically. An Egress Time should be configured between the range of 1 to 300 seconds
8. Select **Default Relay State** as ‘On’ or ‘Off’. An administrator can set a default state of the internal relay, which are 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

Time Override Mode (TOM) allows an administrator to temporarily suspend the need for verification of user for a specific time period on a terminal. Whenever TOM is triggered on terminal then door gets unlock and user can open Door without any authentication till TOM remains continue.

Access Path

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

Pre-requisites

- Single Door Access Controller (SDAC) must be enabled

Screens & Steps

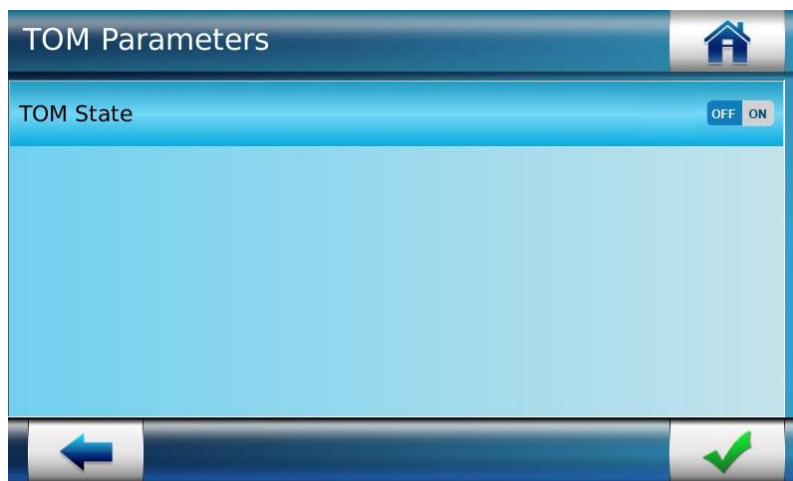


Figure 146: Selecting TOM State as On

1. Select **TOM State** as ON

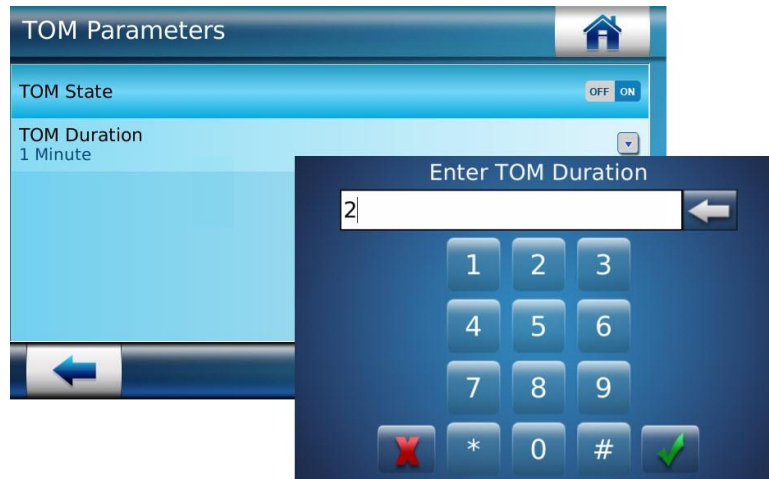




Figure 147: Setting TOM Duration

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

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

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

NOTE: Tamper switch triggers the alarm message. Please refer to **MorphoAccess® SIGMA Series Installation Guide** to identify tamper switch on the terminal.

Access Path

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

Pre-requisite

- Audio File for Tamper Alarm should be uploaded in Multimedia settings. Only then, an administrator can activate Play MMI for playing sound alarm

Screens & Steps

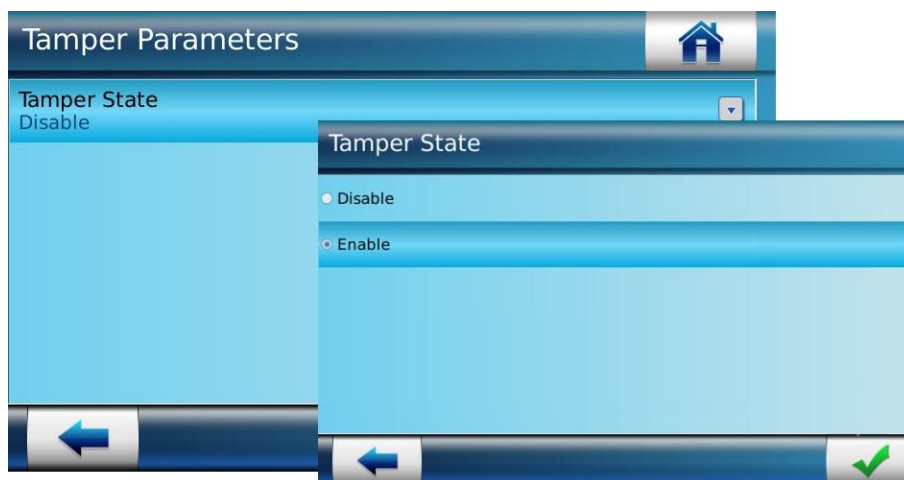



Figure 148: Enabling Tamper

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

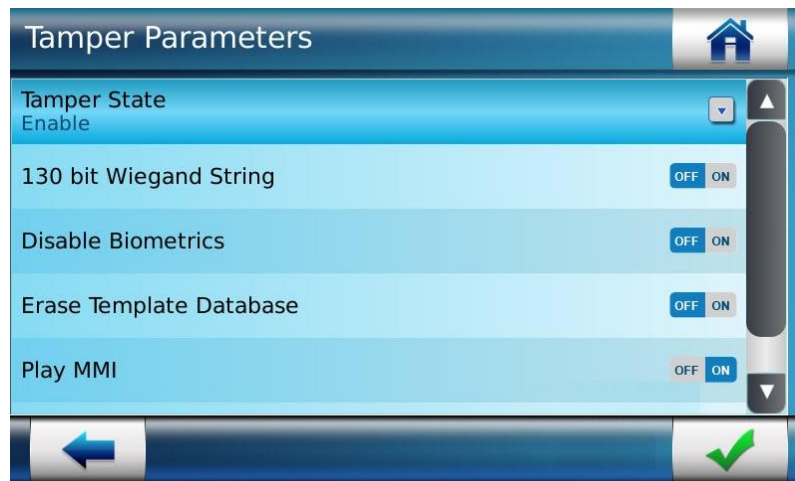



Figure 149: Tamper Parameters Configuration

Once an administrator enables Tamper State, an administrator requires configuring below parameters:

4. **130 bit Wiegand String** can be set as ON or OFF. When this parameter is set as ON, then on tamper detection, 130 bit Wiegand string is generated for tamper alarm through a Wiegand output line
5. **Disable Biometric** can be set as ON or OFF. This parameter if set as ON, then under Tamper state user will not be able to do biometric verification on terminal
6. **Erase Template Database** can be set as ON or OFF. This parameter if set as ON, then on Tamper detection, all the templates enrolled and save in the MorphoAccess® SIGMA Series terminal will be deleted
7. **Play MMI** can be set as ON if an administrator require to play a sound alarm on terminal on tamper detection. The audio file uploaded in the system will be played
8. **Erase Security Data** can be set 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 default key.
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, and required actions as configured above, are executed. 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.

LCD Configuration

LCD Configuration allows an administrator to control the look and feel of the content/multimedia displayed on the LCD touch screen of MorphoAccess® SIGMA Series terminal.

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

System Menu > Terminal Settings > LCD Configuration

Pre-requisites

- Video file must be uploaded for Idle Screen in Multimedia settings. Only then an administrator can configure Video Play Brightness and duration.

Screens & Steps

Screen Brightness Control

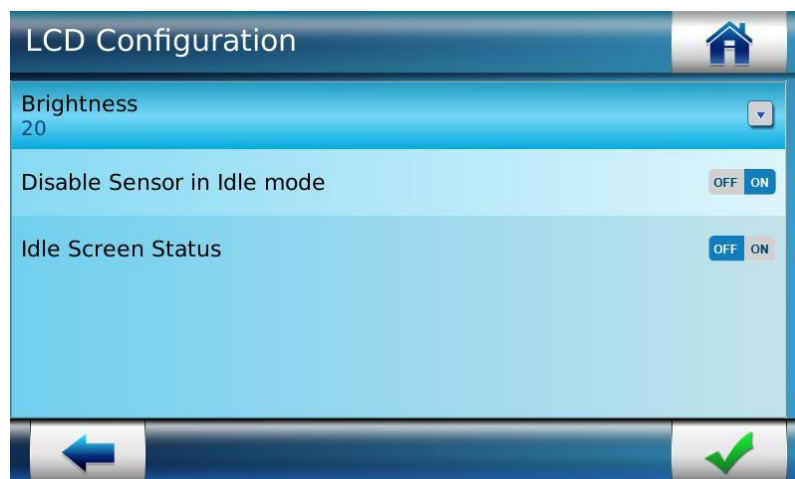


Figure 150: LCD Brightness adjustment

1. Press on **Brightness**

2. On next screen an administrator can adjust the brightness of LCD back light by scrolling the cursor left or right

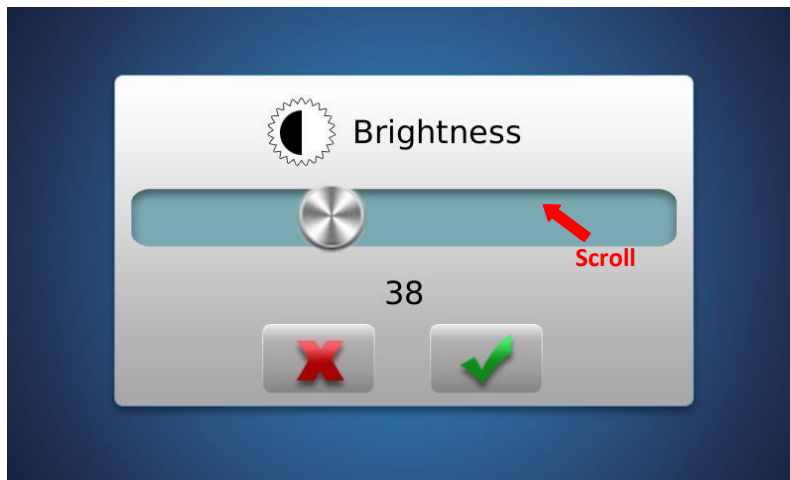



Figure 151: LCD Brightness adjustment

3. Move cursor left to reduce brightness and right to increase brightness of the LCD
4. Use “” icon to **Save** setting

Disable Sensor in Idle Mode

This parameter allows an administrator to disable the biometric sensor backlight when terminal is in idle mode. When terminal is in idle mode, the biometric sensor will automatically power off. It is also recommended for power saving. As soon as terminal is in use, the biometric sensor is powered on.

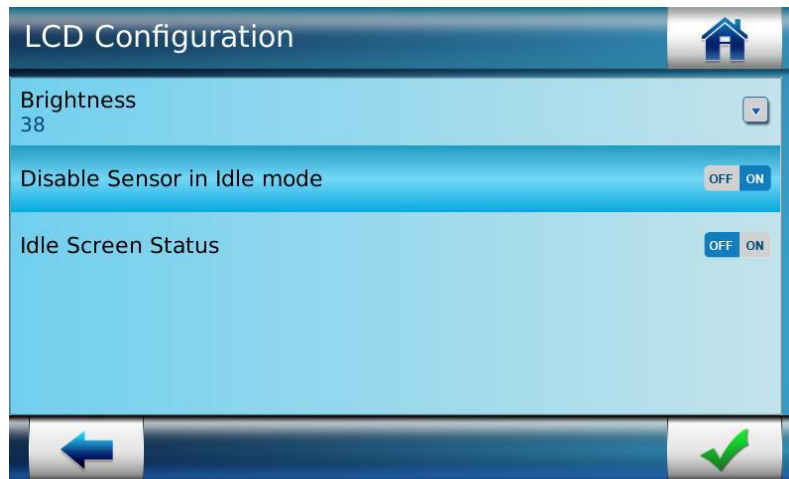



Figure 152: Disable Sensor in Idle Mode

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

Set Idle Screen Status

This parameter indicates that if no actions are triggered on terminal, then terminal should be auto locked and a video is played. The video to be played can be uploaded in the Idle Screen Video folder, using “Video Settings” functionality under Multimedia menu.

When terminal is in idle mode, the biometric sensor is powered off (if “Disable Sensor in Idle mode” parameter is configured). The Idle mode can be exit by touching the text zone on the LCD touch screen.



Figure 153: Configuring Idle Screen Status

1. An administrator can set **Idle Screen Status** as ON or OFF.
2. Select status as ON if an administrator requires 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

NOTE: If the video fails to be played in Idle Mode, then no error message is displayed and terminal reboots automatically.

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

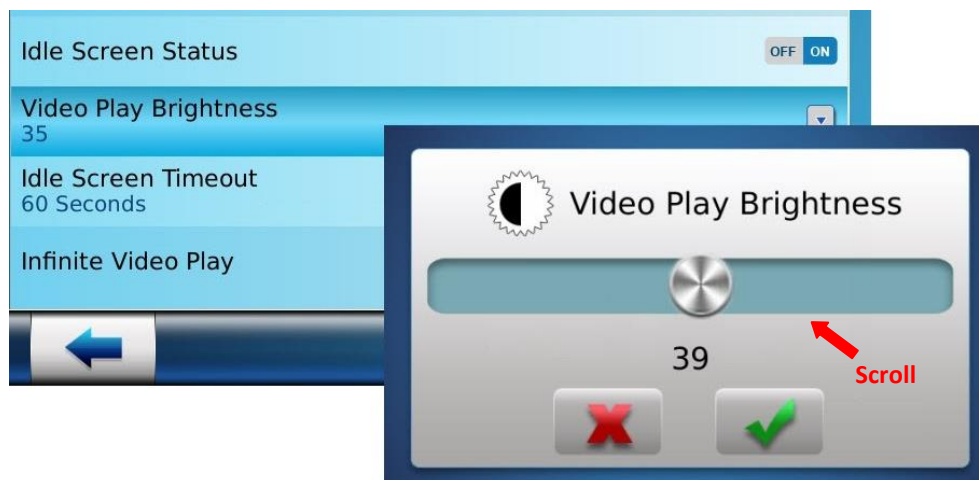



Figure 154: Video Play Brightness Control

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

Set Idle Screen Time Out

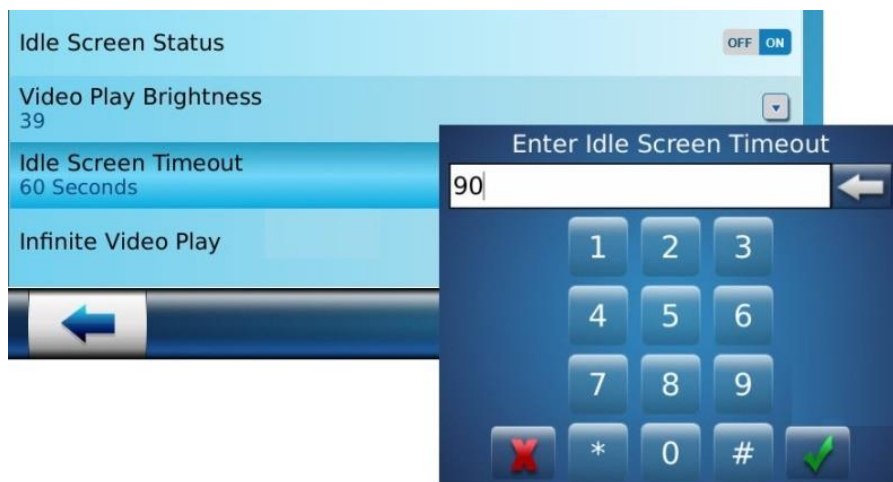



Figure 155: Configuring Idle Screen Timeout

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

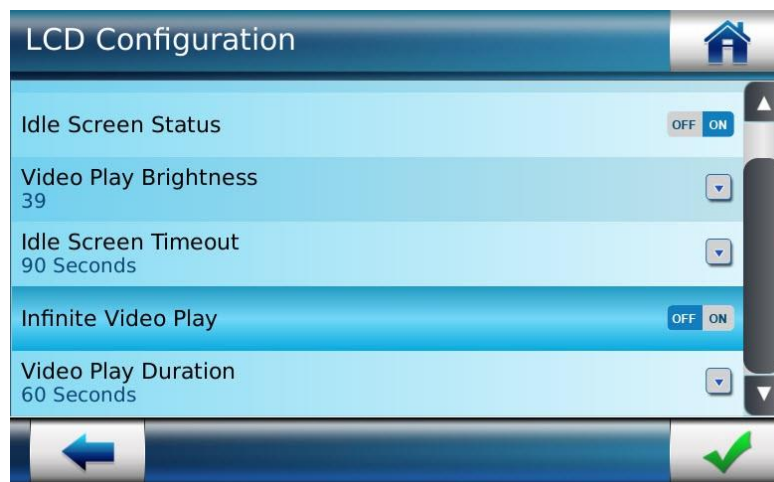


Figure 156: Infinite Video Play on idle screen

1. This parameter indicates whether the video to played on idle screen for infinite duration or not.
2. Select **OFF** or **ON**
3. If an administrator select Infinite video play OFF, then an administrator need to define duration for which video is to be played

Video Play Duration

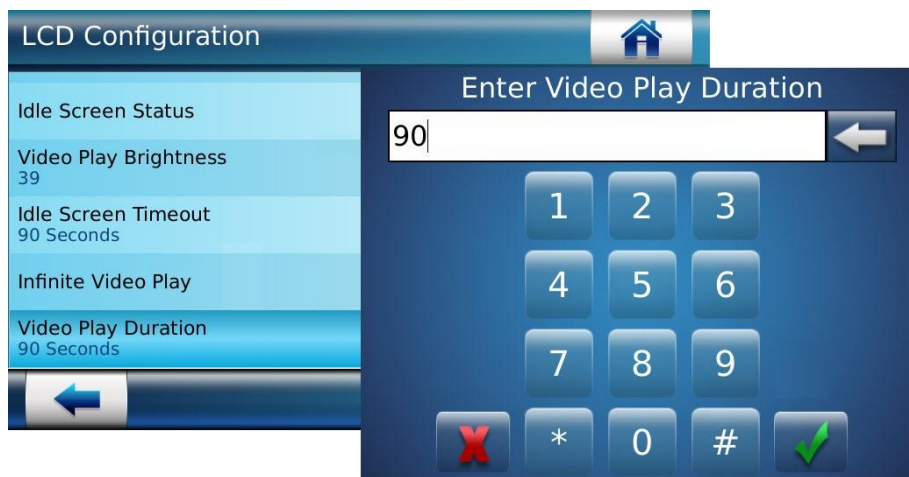




Figure 157: Setting Video Play Duration

1. Press on **Video Play Duration** and enter the number of seconds an administrator require 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 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. Terminal will then show LED MMI, for activities on 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 "*Videophone Facility*" section of this document for more information on Video Phone feature.

Transaction Log

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

- Access granted to the user
- Access denied to the user
- Time and Attendance actions
- Error occurred
- Face detection captured and picture stored
- Etc...

NOTE: The events that user has cancelled are not logged

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

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

In order to view transaction logs, an administrator require exporting logs using a USB mass storage device. Refer to "Export Data in USB Mass Storage Device" under USB Menu Section.

In subsequent sections of Transaction Log, the parameters that can be configured by Administrator who has full Admin Rights to access terminal.

Transaction Log parameters can also be configured through Web server interface, detailed under "Transaction Log Settings" of Webserver section in this document.

Configure Transaction Logging Mode

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

- **No Log:** An administrator can set Transaction Logging to 'No Log' mode. This indicates that no actions will be recorded and stored on terminal
- **Access Control Log:** This mode indicates that only user access request 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

System Menu > Transaction log > Transaction Logging

Screens & Steps

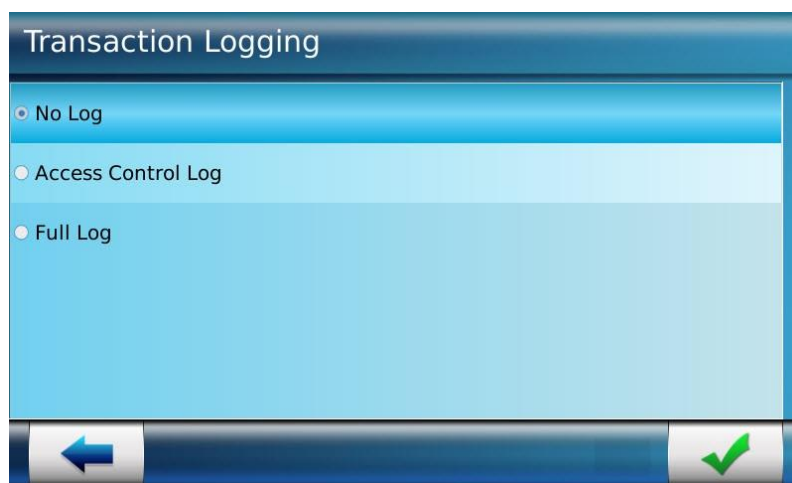



Figure 158: Selecting Transaction Logging Mode

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

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

- Delete Partial Logs
- Delete Full Logs

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

Access Path

System Menu > Transaction log > Actions on Log Full Event

Screens & Steps

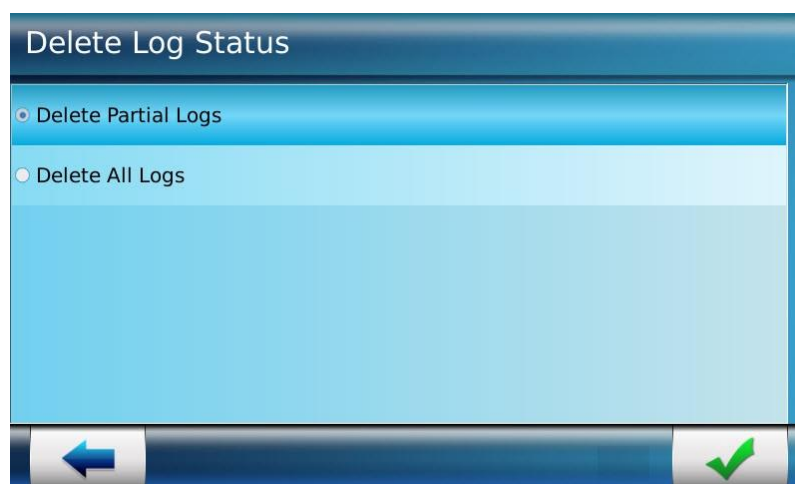



Figure 159: Setting Delete Log Status

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

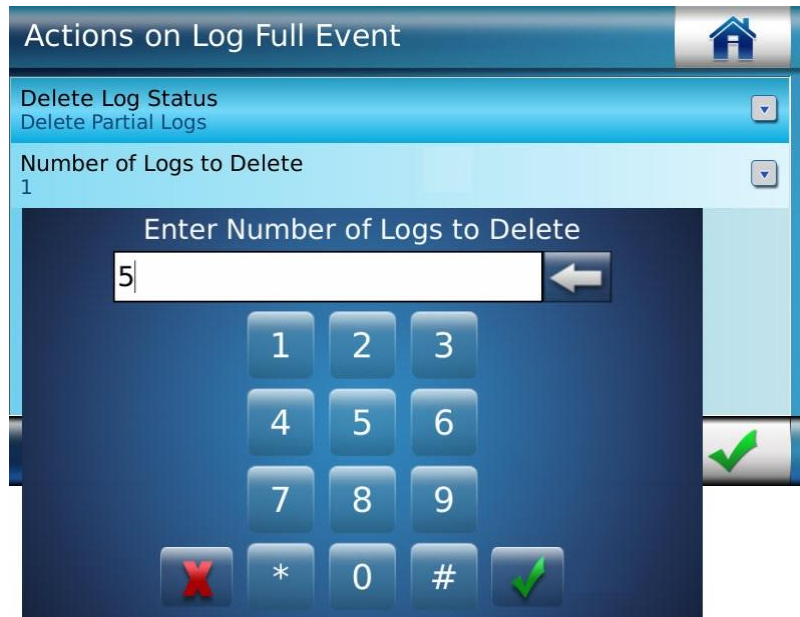



Figure 160: Defining number of logs to be deleted

3. If an administrator have selected Delete Partial Logs as delete log status, then an administrator need to define **Number of Logs to be Deleted** when delete action is triggered.
4. Press on “” button to save settings

Delete Transaction Logs

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

Access Path

System Menu > Transaction log > Delete All Logs

Screens & Steps

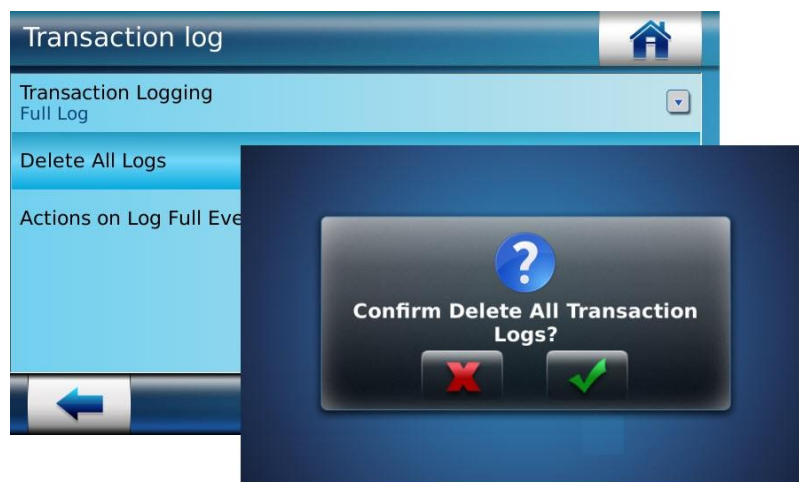




Figure 161: Deleting Transaction logs

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. An 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

MorphoAccess® SIGMA Series terminal is able to play sound when specific event occurs. Using Global Terminal Volume, an administrator can set volume of all the audio/video files that are uploaded in the terminal.

Access Path

System Menu > Miscellaneous Settings

Screens & Steps

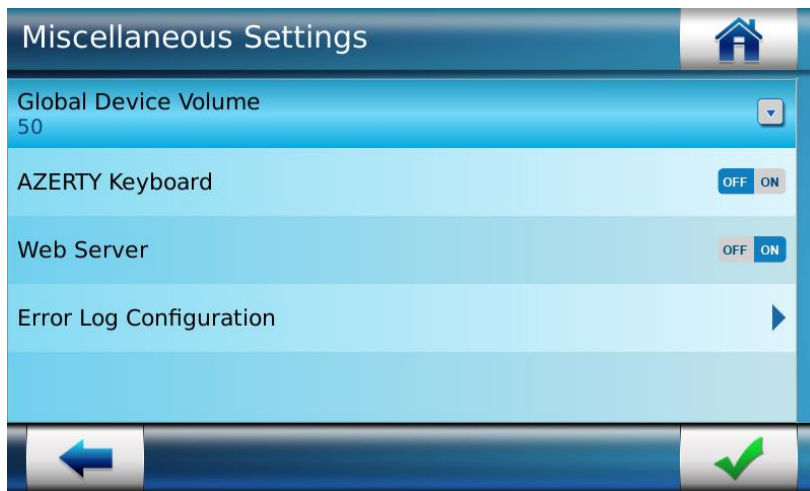


Figure 162: Terminal Global Volume

1. Select **Global Terminal Volume**

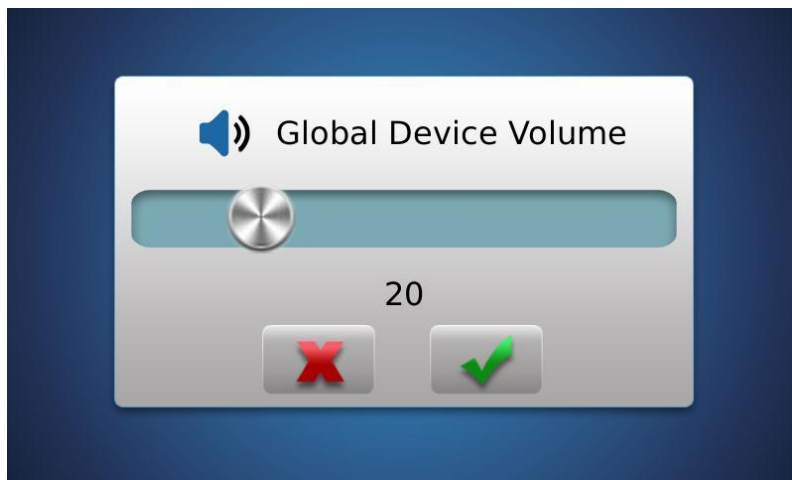


Figure 163: Set Global Device Volume

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

Results

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

References

- Refer to "[Multimedia menu](#)" to know how to upload audio/video files to terminal

Enable AZERTY Keyboard

By default, the keyboard displayed in MorphoAccess® SIGMA Series terminal is QWERTY (English standard keyboard). Using this functionality, an administrator can enable AZERTY (French standard) keyboard type.

Access Path

System Menu > Miscellaneous Settings

Screens & Steps

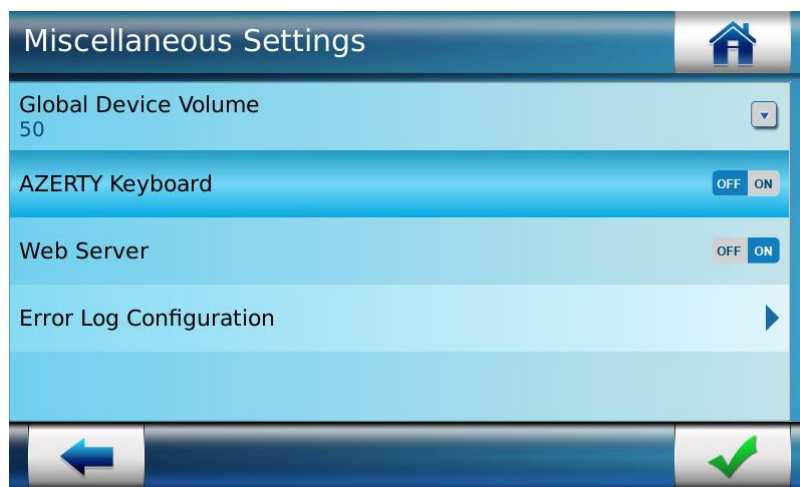


Figure 164: Enable AZERTY Keyboard

1. Select **AZERTY keyboard** as ON or OFF. If an administrator select ON, then keyboard will appear in AZERTY format, as shown in below image:

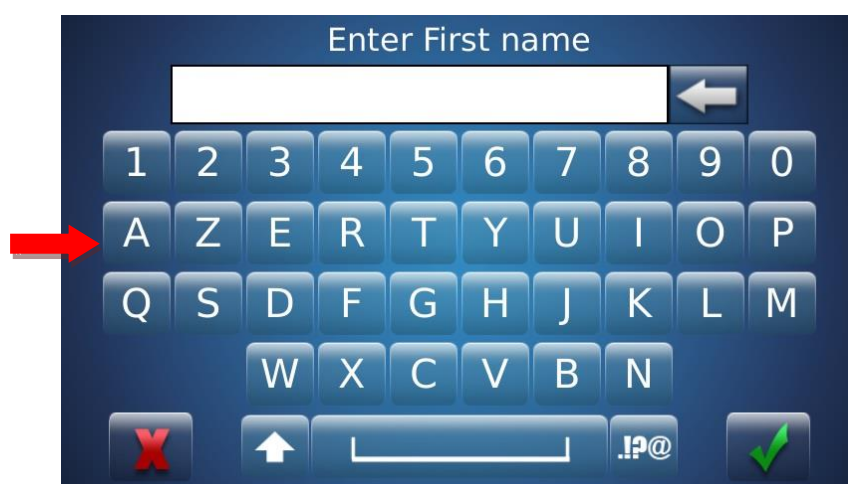


Figure 165: AZERTY keypad

Web Server

The MorphoAccess® SIGMA Series terminal allows an administrator to enable the access to the Web Server. It allows an administrator to configure any parameter of terminal by connecting remotely. Refer “Introduction to Webserver” in this document.

By default the access to Web Server is disabled in a MorphoAccess® SIGMA Series terminal.

Access Path

System Menu > Miscellaneous Settings > Web Server

Screens & Steps

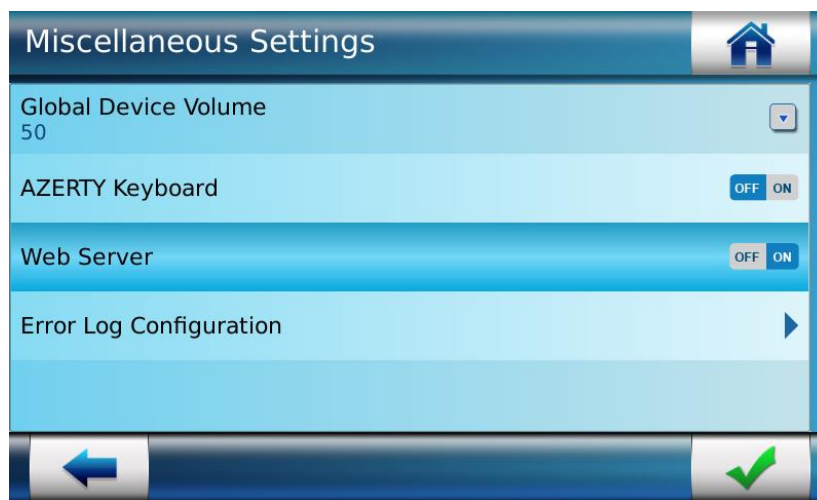


Figure 166: Web Server

1. Select **Web Server** as ON or OFF. If an administrator selects ON, then the administrator will be able to access the Web Server remotely.

Error Log Configuration

MorphoAccess® SIGMA Series terminal is capable of capturing logs of the events when access is denied or any error has occurred during operations.

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

Access Path

System Menu > Miscellaneous Settings > Error Log Configuration

Screens & Steps

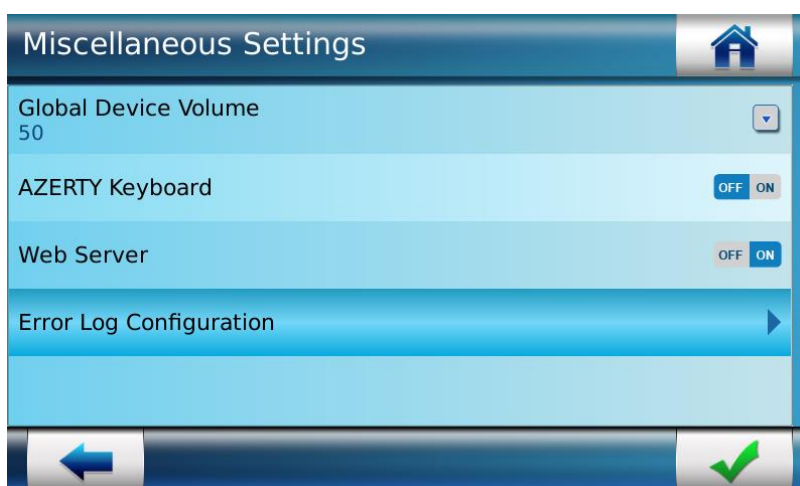


Figure 167: Select Error Log Configuration

1. Select **Error Log Configuration**

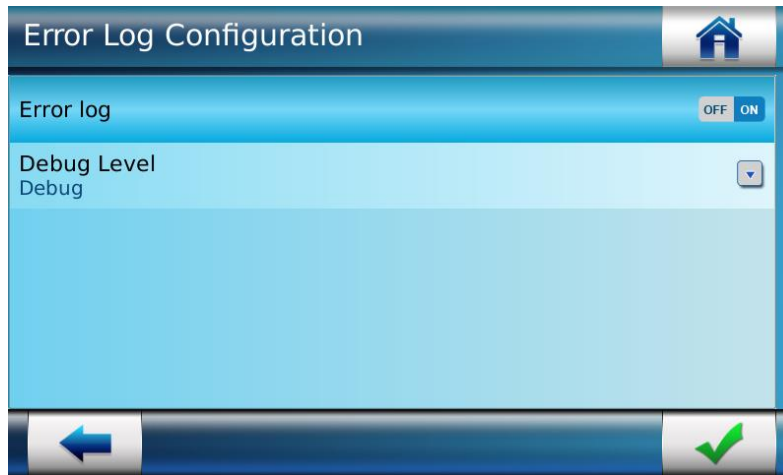


Figure 168: Enable Error Logging

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

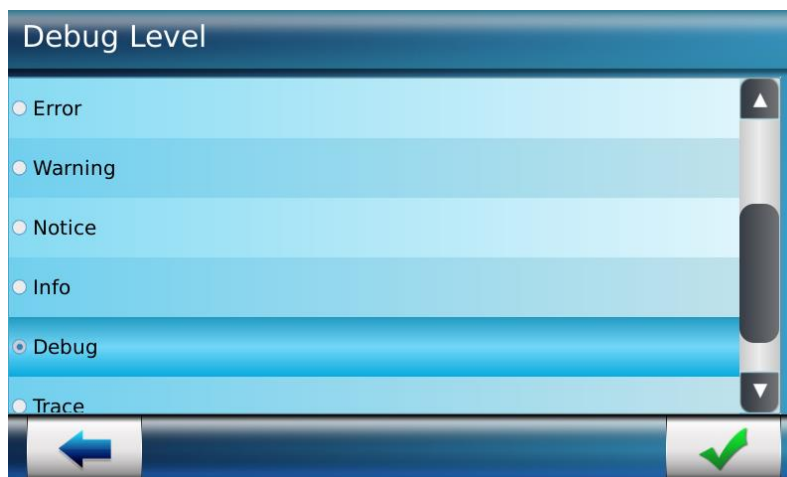


Figure 169: Setting Error Log Debug Level

3. Select **Debug Level** from the available list
 - a. Fatal
 - b. Alert
 - c. Critical
 - d. Error
 - e. WARNING
 - f. Notice
 - g. Info
 - h. Debug
 - i. Trace

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

- 4. Press on check button to save settings

Results

Error logs are captured and stored in terminal. Using Export functionality under USB menu, logs can be exported. Refer to “Export Data in USB Mass Storage Device”.

Sensor Log Configuration

MorphoAccess® SIGMA Series terminal is capable of capturing logs of the CBI sensor when any operation performed on CBI sensor

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

Access Path

System Menu > Miscellaneous Settings > Error Log Configuration

Screens & Steps

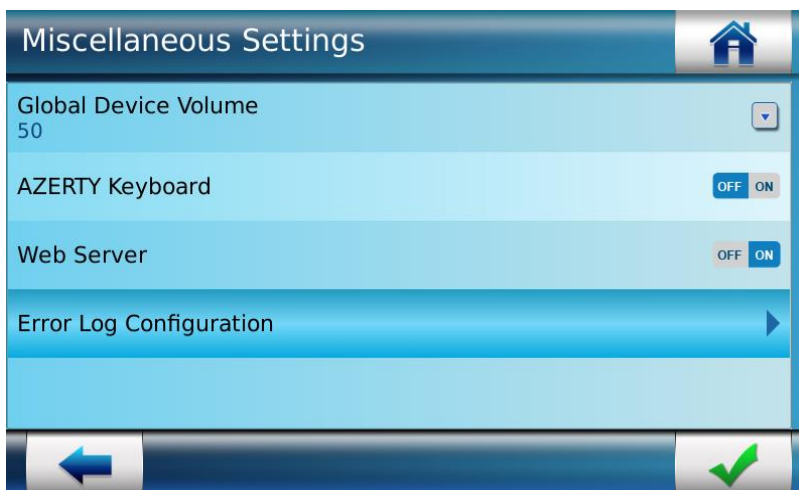


Figure 170: Select Error Log Configuraton

- 1. Select **Error Log Configuration**

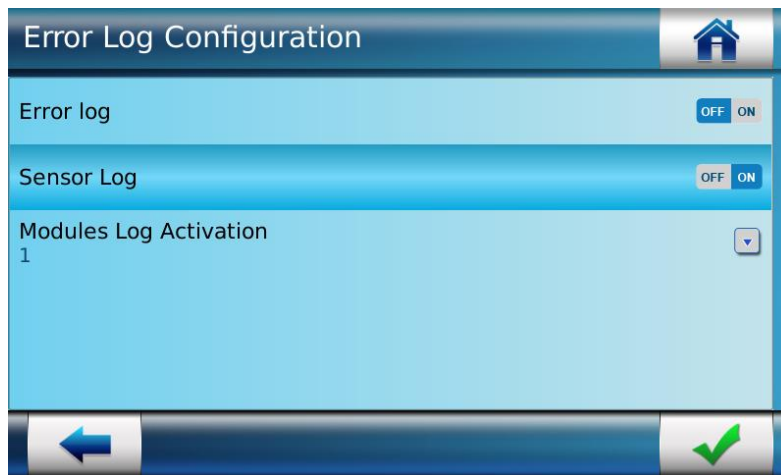


Figure 171: Enable Error Logging

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

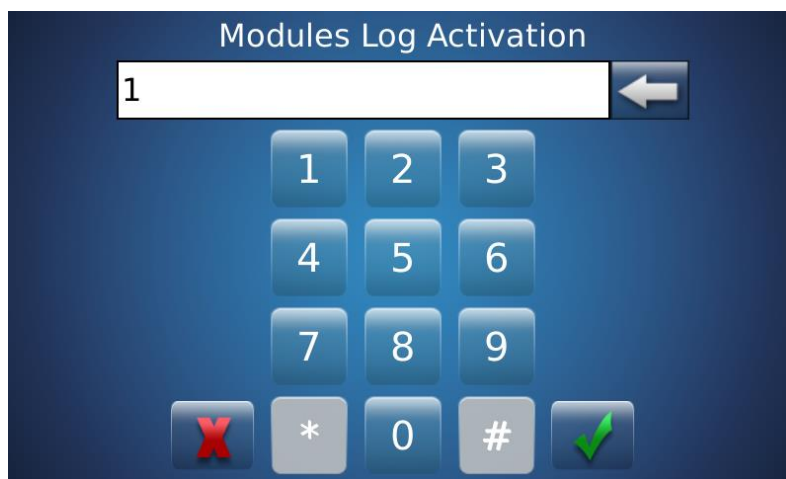


Figure 172: Sensor Modules Log Activation

3. Set **Module Log Activation** value inbetween 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 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.

4. Press on check button to save settings

Communication menu

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

- Require the conclusion of access rights check to a Central Access Controller, to grant or deny access to user
- terminal configuration
- terminal maintenance: firmware upgrade, add a license (to unlock an optional feature)
- database management: add, modify or remove a user
- log file management: get or delete log file
- Wi-Fi™ connection configuration

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

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



Figure 173: Communication Menu

Security recommendation

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

Ethernet Network Configuration

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

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

NOTE:

- Terminal can support connection through Ethernet and Wi-Fi™ both simultaneously.
- Terminal can support connection through Ethernet and 3G/GPRS/GSM network simultaneously.

Access Path

Communication Menu > Network Interface > Ethernet

Screens & Steps

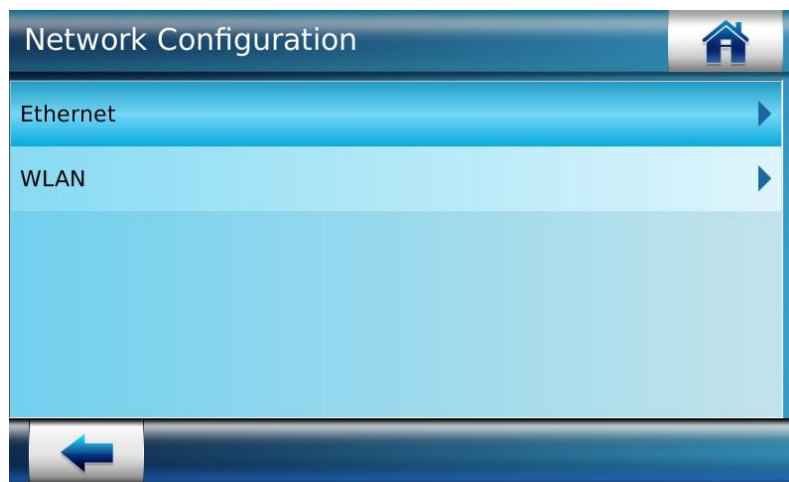


Figure 174: Selecting Ethernet-Network Configuration

1. Select **Ethernet**
2. Select **IP Configuration**



Figure 175: Ethernet Configuration

3. Under Ethernet, an administrator can select **IPV4** or **IPV6**
4. On next screen, default IP Mode is selected as DHCP. Press on **IP Mode** for update

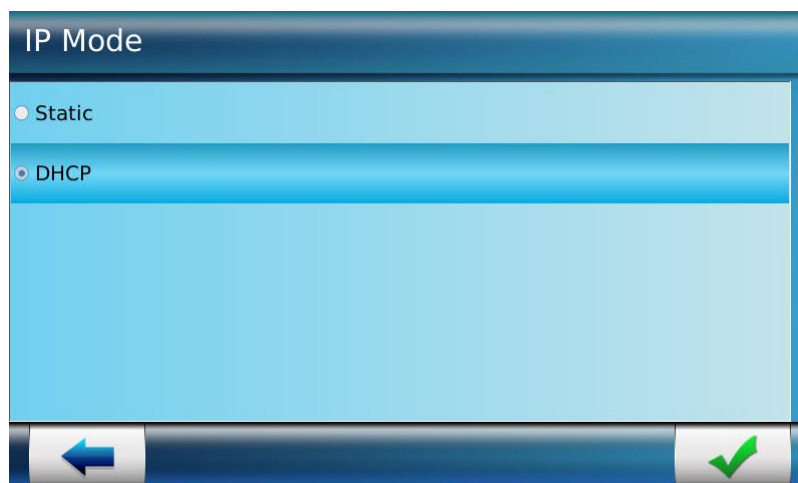



Figure 176: IP Mode Selection

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

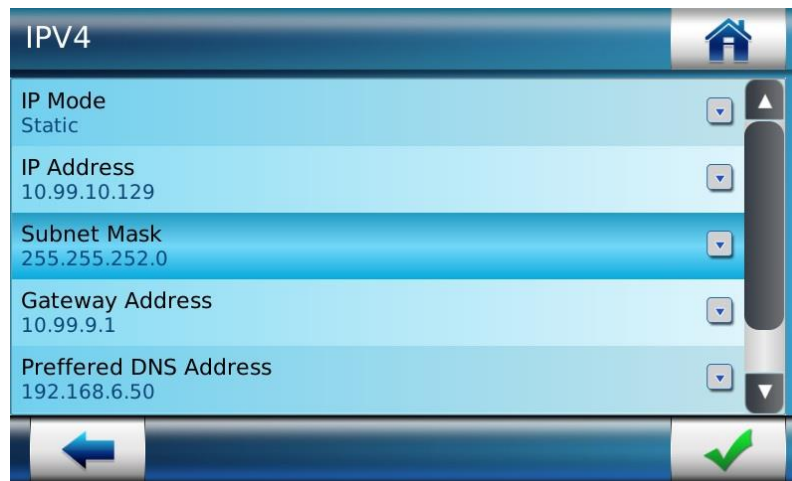


Figure 177: Configuring IP Address under Static IP Mode

7. Under Static IP Mode, an administrator can manually configure 'IP Address' of the terminal, 'Subnet Mask', 'Network Mask', 'Gateway Address' and 'DNS Servers

Results

Once the Ethernet Configuration is done, the terminal is connected to a distant server. An administrator can also set the IP restriction for preventing terminal from unauthorized access. These settings can be done from Security menu, refer "[Network & Communication Security Settings](#)".

Wi-Fi™ Network Configuration

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

At First Boot Assistant, an administrator can configure the terminal to communicate through WLAN. There are two ways to configure WLAN:

- **Automatic:** The available networks are listed automatically. An administrator can select the network and connect by entering Wi-Fi™ encryption key
- **Manual:** The manual configuration is useful to connect with a hidden Wi-Fi™ network. An administrator can manually configure the WLAN, by entering SSID, Encryption Mode and Encryption Key.

Access Path

System Menu > First Boot Assistant > Network Configuration > WLAN

Pre-requisites

- Wi-Fi™ USB dongle should be plugged into the terminal
- MA_WI-FI™ license should be installed on terminal

Screens & Steps

Automatic Configuration

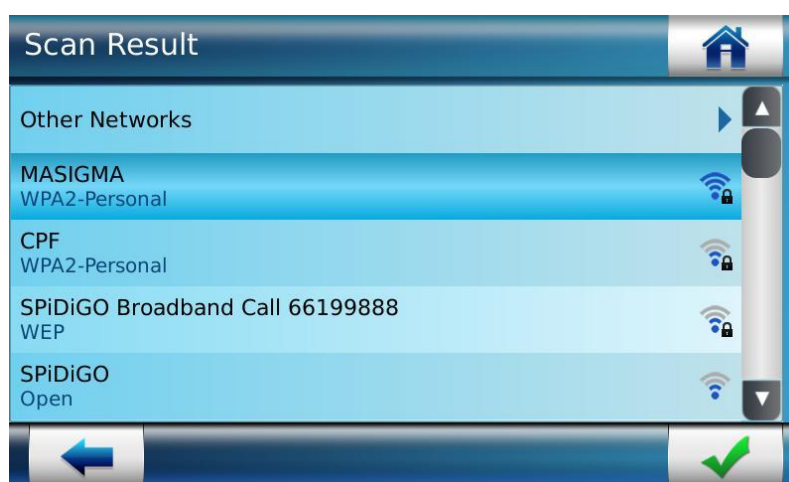


Figure 178: Selecting available Wi-Fi™ network

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



Figure 179: Enter Encryption Key

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



Figure 180: Success message is displayed showing Wi-Fi™ network is configured



Figure 181: Connected to Wi-Fi™ network

Manual Configuration

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



Figure 182: Selecting Other Network to set up Wi-Fi™ network manually

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

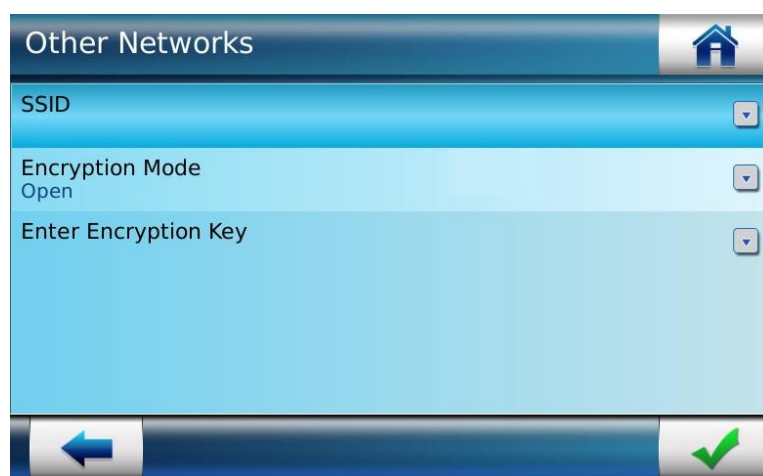




Figure 183: WLAN Parameter Configuration

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



Figure 184: Setting SSID

4. Enter **SSID** and click on “” button to save. To cancel the operation, use “” button

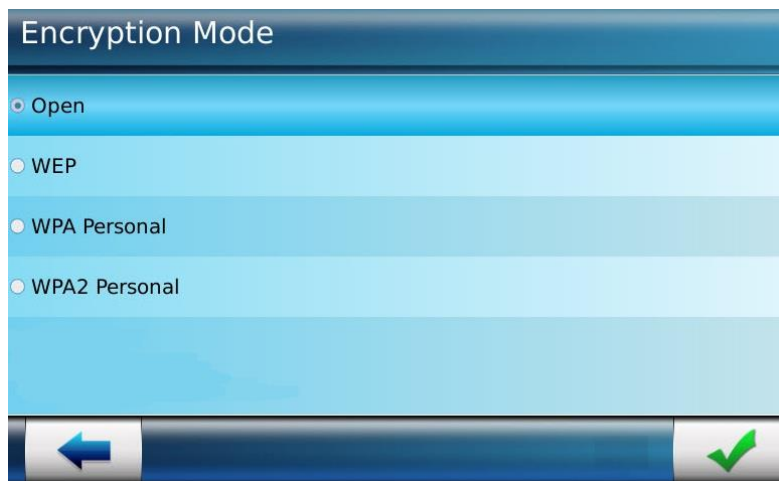



Figure 185: Selecting Encryption Mode

5. Select the **Encryption Mode**, as provided by the Wi-Fi™ network administrator. Encryption mode is selected for Wi-Fi™ security, to prevent from unauthorized access. The available Encryption modes are:
 - a. **Open** (none)
 - b. **WEP**
 - c. **WPA Personal**
 - d. **WPA2 Personal**



Figure 186: Define Encryption Key

6. Enter **Encryption Key** to connect to Wi-Fi™. Only by entering Encryption Key, the Wi-Fi™ network can be accessed
7. Use Check button “” to save the setting

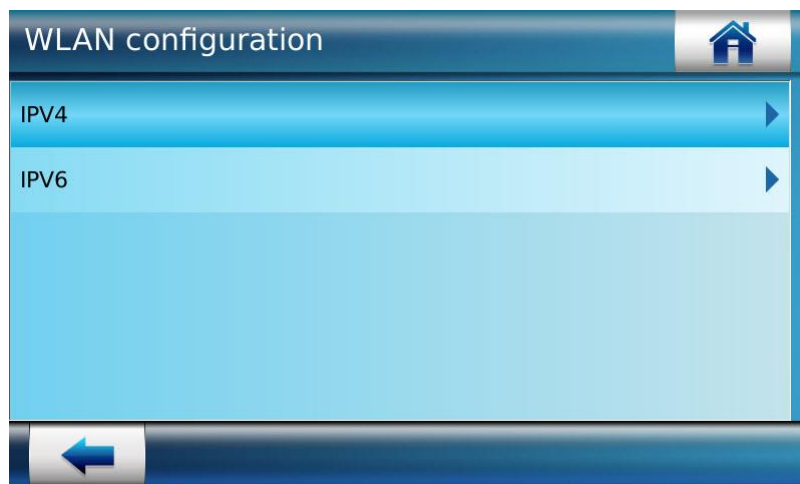


Figure 187: Entering in WLAN – IP Configuration

8. On WLAN screen select “IP Configuration” to set up the server IP which is required to be connected through WLAN
9. Select **IPV 4** or **IPV 6**

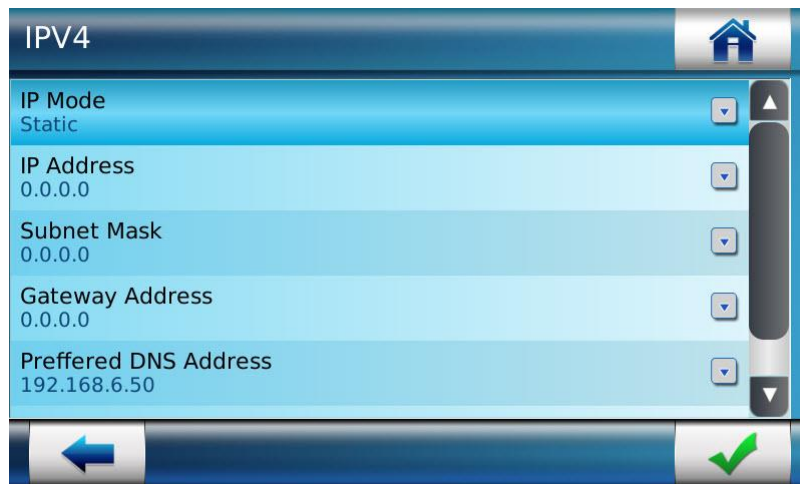


Figure 188: WLAN – IP Configuration


10. An administrator can select **IP Mode** as 'Static' or 'DHCP'
 - a. If IP Mode is 'Static', then enter parameters such as IP Address, Subnet Mask, Gateway Address, Preferred DNS Address and Alternate DNS Address must be entered manually
 - b. If IP Mode is 'DHCP', then IP address, and other network parameters, are allocated automatically to the terminal
11. Use Check button “” to save the setting



Figure 189: Success message is displayed showing Wi-Fi™ network is configured

Configure Hostname

When IP Mode is select as DHCP, the Hostname parameter can be configured. By Default, the hostname of a MorphoAccess® SIGMA Series terminal is MA<Serial Number>.

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


Access Path

Communication Menu > Network Interface > Hostname

Screens & Steps



Figure 190: Configuring Hostname

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

Serial Parameters

MorphoAccess® SIGMA Series 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. An administrator can configure parameters of serial channel from terminal or with Webserver interface.

NOTE: Serial channel cannot be used for terminal configuration using Webserver.

Access Path

Communication Menu > Serial Parameters

Screens & Steps

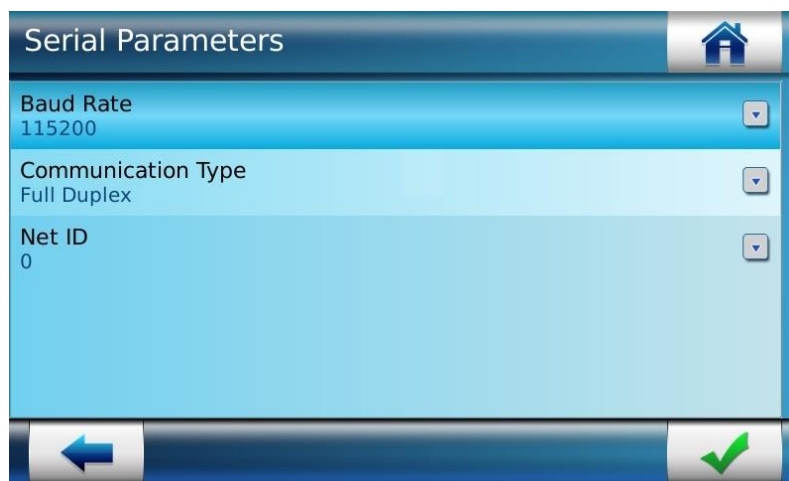


Figure 191: Defining Baud Rate

1. Select **Baud Rate**. Baud rate is the rate of message transmission from MorphoAccess® SIGMA Series terminal to distant system using serial channel

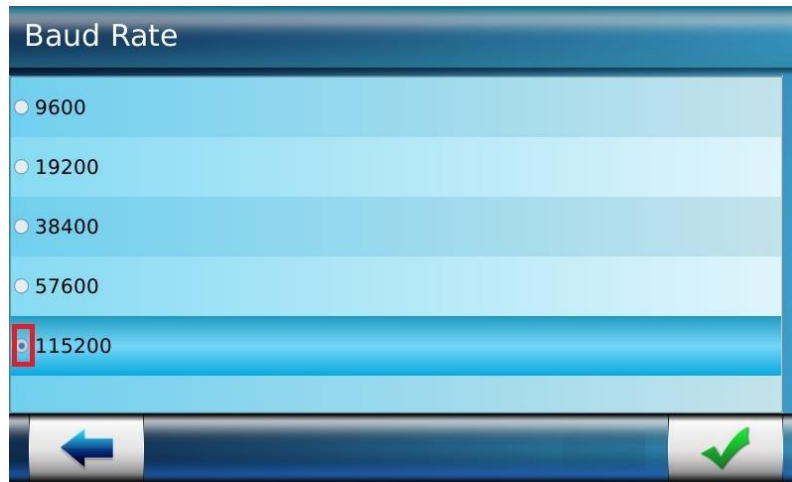



Figure 192: Select Baud Rate

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

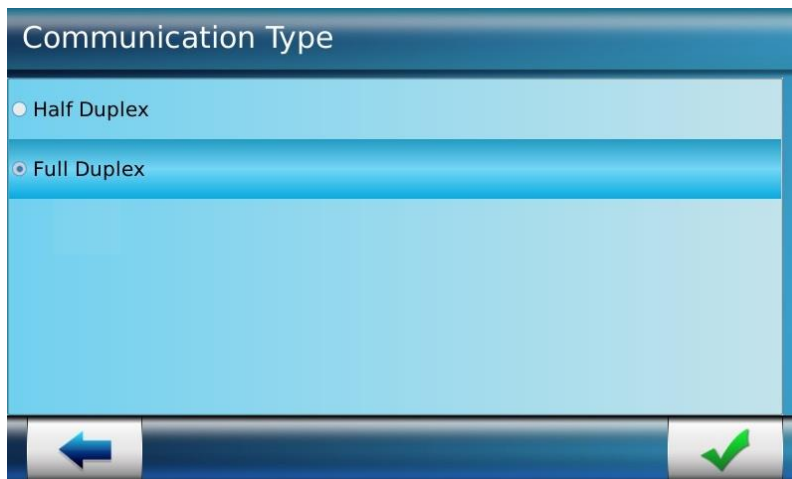


Figure 193: Selecting Communication Type




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



Figure 194: 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.

NOTE: The Serial configuration done will be lost in case the terminal mode is changed to MA5G, Legacy L1 or Legacy Morpho.

Security Menu

Security Menu allows to configure the parameters related to the level of security required on MorphoAccess® SIGMA Series terminal. Security menu deals with Biometric control, Network security, multi-user verification, LCD Login Password and User Control.



Figure 195: Security Menu

Biometric Security Settings

Configure Trigger Events

MorphoAccess® SIGMA Series terminal is able to perform identification and authentication operations when certain events occurs on terminal. Using this configuration an administrator can set on which events the terminal should perform operations. Below is the list of events available:

- **Biometric**, a finger is detected on the biometric sensor (which starts biometric identification process)
- **Contactless card**, detection of a contactless card (which starts authentication process with user's data read on user's card)
- **Keypad**, detection of a user id entered with touch screen keyboard (which starts authentication of the user with at least User ID)
- **External Port**, reception of a User ID from Wiegand / Clock and Data port (which starts authentication process with at least user id)

Access Path

Security Menu > Biometric Settings > Trigger Event

Pre-requisites

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

Screens & Steps

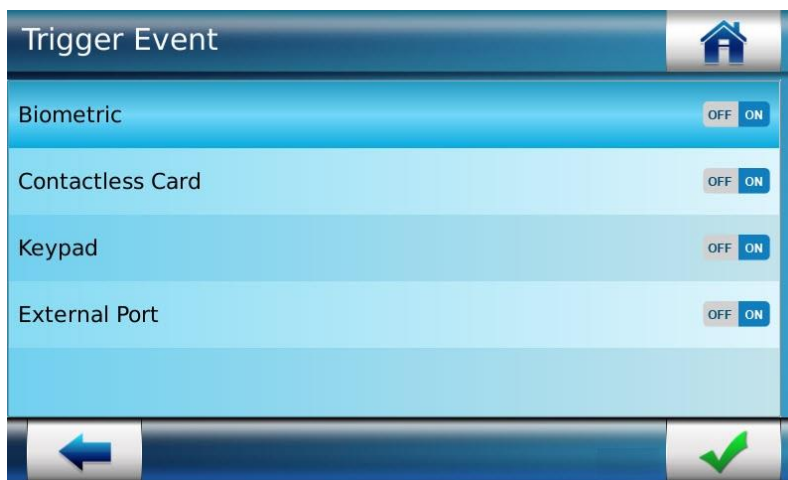



Figure 196: Configuring the events on which authentication/identification is triggered

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

Using this parameter, an administrator can enable Duress Mode in MorphoAccess® SIGMA Series terminal. Duress Mode will allow an administrator to capture duress finger of a user, in addition to two normal fingers.

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

MMI is played on successful authentication of user’s duress finger. 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

Security Menu > Biometric Settings > Set Duress Mode

Screens & Steps



Figure 197: 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

The access rights check process of the MorphoAccess® SIGMA Series terminal proceeds by comparison of the biometric data of a finger placed on the biometric sensor, with the biometric data of fingers stored in the database (identification) or stored in user's card (authentication).

An administrator can set **Biometric Check Mode** as on or OFF. If the biometric check mode is ON, then it is a pre-requisite to have user's biometric data in the terminal database or in user's card.

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

Security Menu > Biometric Settings > Identification

Screens & Steps



Figure 198: 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

In order to reduce the False Rejection Rate (FRR), MorphoAccess® SIGMA Series terminal allows an administrator to set Biometric Matching Strategy, in which multiple biometric check attempts are allowed to user. For instance, a user is allowed to place again his finger on the biometric sensor for a 2nd try, when the initial biometric check fails.

The 2nd try allows the user to upgrade the finger placement, or to place another finger. In addition, and also to reduce the FRR, during this 2nd try, the terminal executes a more powerful biometric check (which is also a little bit slower).

Biometric Check Attempts allows an administrator to set:

- **Standard Matching Strategy (1 Attempts):** User is allowed to place finger for only once. If biometric data does not match with the fingerprints enrolled in database then access is rejected.
- **Advance Matching Strategy (2 Attempts):** User is allowed to attempt two times. If biometric check fails on first try, terminal will ask user to place again his finger on the biometric sensor, and perform biometric check again.
- **Advanced Matching Strategy with MFU (2 Attempts):** User is allowed to attempt two times, if the access is rejected on first try. Under this strategy, on first attempt terminal will go to search for the user in the Most Frequent users list. If not identified, then user is given second try to place finger. On second try the terminal will search biometric in entire database. This option applies only to biometric identification process only. This option is useless with biometric authentication process.

Parameter Configuration

By default, the two attempts mode is activated, but can be disabled.

| Parameter name | Value | Description |
|---|-----------|---|
| auth_param.additional_bio_heck_nb_attempt | 1, 2 or 3 | <p>A value of “2” means that after a first incorrect identification or authentication a second chance is given to place finger on the biometric sensor.</p> <p>Set this parameter to “1” to offer only one attempt to place finger.</p> <p>Set this parameter to “3” to offer 3 attempts.</p> |

Access Path

Security Menu > Biometric Settings > Biometric Matching Strategy

Pre-requisites

- Biometric Check Mode should be set as ON

Screens & Steps

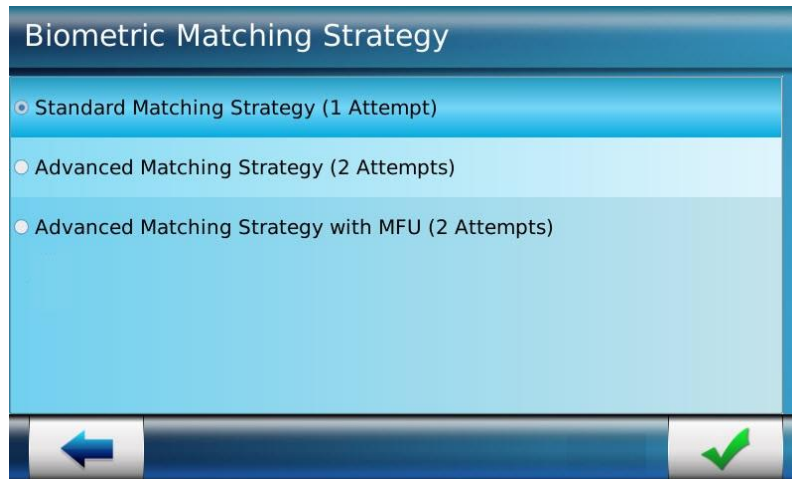



Figure 199: Selecting Biometric Matching Strategy

1. Select **Biometric Matching Strategy** as Standard, Advance or Advanced with MFU
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 user have to place finger on the biometric sensor of terminal. If user fails the place finger within time out, the access is rejected.

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.

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 process 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 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

Security Menu > Biometric Settings > Biometric Timeout

Pre-requisites

- Biometric Check Mode should be set as ON

Screens & Steps

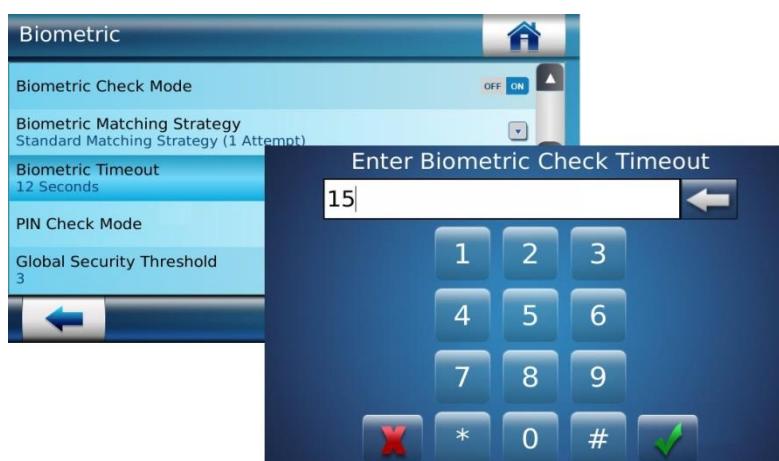



Figure 200: Biometric Time Out

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

PIN Check Mode

At the time of enrolment, a User ID and a PIN code are entered along with registering the biometric data of the user. An administrator can enable **PIN Check Mode** if an administrator require terminal to authenticate users based on the entered PIN.

In **Identification Mode**, if a match is found in database, for the biometric data provided by the user, then the terminal request the user to enter his PIN code. Access is granted, only if PIN entered matches with the PIN value stored in user’s record in database. In case biometric mode is disabled, User identification is done based on the PIN entered. Note that trigger event through biometric must be enabled for performing identification.

In **Authentication Mode**, user will require to enter User ID, and then Fingerprint. If fingerprint is matched, then terminal will ask user to enter PIN. Only on successful PIN verification, user access is granted. In case biometric check mode is disabled, 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

Security Menu > Biometric Settings > PIN Check Mode

Screens & Steps



Figure 201: Setting PIN Check Mode

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

PIN Check Attempts

This parameter indicates the number of attempts a user can enter PIN, if the PIN is rejected on first attempt. This feature is helpful in reducing False Rejection Rate, by allowing users to enter PIN accurately on 2nd try.

Access Path

Security Menu > Biometric Settings > PIN Check Attempts

Pre-requisites

- PIN Check Mode should be set as ON

Screens & Steps

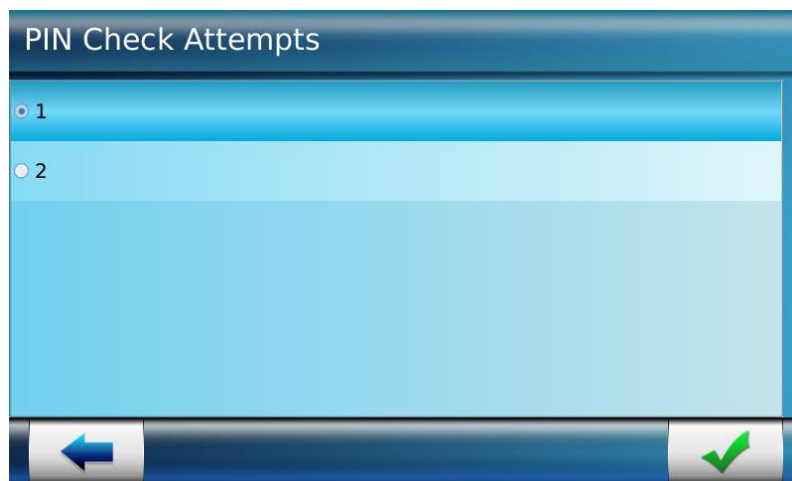



Figure 202: Setting number of PIN Check Attempts

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

PIN Check Time Out

PIN Check Time Out is the duration within which user is required to enter PIN. By default, the PIN Check Time Out is set as 5 seconds, which is configurable. 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, fingerprint and PIN for authentication.

Access Path

Security Menu > Biometric Settings > PIN Check Time Out

Pre-requisites

- PIN Check Mode should be set as ON

Screens & Steps

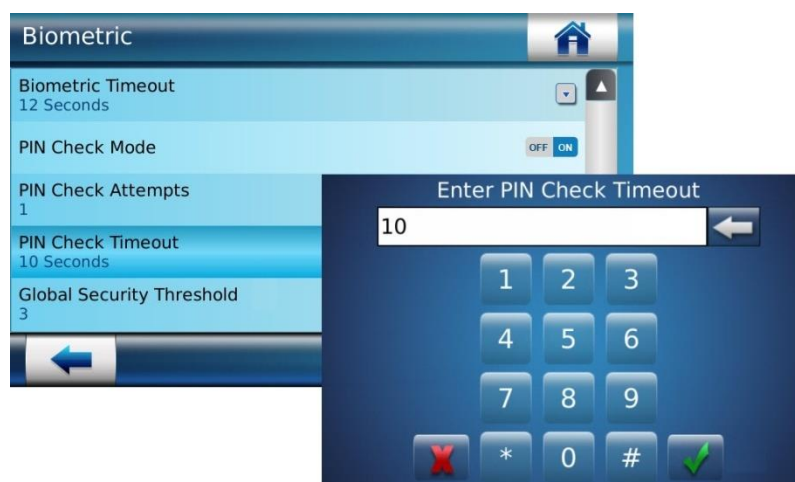



Figure 203: Setting PIN Check Timeout

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

Setting-up Matching Security Threshold

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

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

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

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

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

Parameter Configuration

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

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

Matching threshold values are detailed in the table below:

| Value | Description |
|-------|---|
| 0 | <p>Lowest threshold value: the number of false rejects is very low, but the number of false acceptances is too high for a secure usage.</p> <p>It is strongly advised not to use this value, because the terminal becomes too tolerant.</p> |
| 1 | FAR < 1 % |
| 2 | FAR < 0.5 % |
| 3 | <p>FAR < 0.1% (Default value)</p> <p>Recommended value for physical access control applications using identification.</p> |
| 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 | <p>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.</p> <p>It is strongly advised not to use this value, because the terminal becomes too restrictive.</p> |

Access Path

Security Menu > Biometric Settings > Global Security Threshold

Screens & Steps



Figure 204: Setting Security Threshold

1. Select **Global Security Threshold** from values 0 to 10
2. Press on “” button to **Save** settings

Results

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

Anti-Tamper Switch For Terminal Security

Description

The MorphoAccess® SIGMA Series terminal is able to detect the opening of the box. This detection is controlled by anti-tamper switch attached in the terminal. The opening of the external USB port cover is not detected, but the USB port is disabled by default.

When one of those events is detected, the terminal acts as required by the related parameter values:

- 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 **MorphoAccess® terminals Remote Messages Specification** document.

References

- Refer to section [“Tamper Configuration for Terminal Security”](#) to configure tamper parameters from terminal administration menu.
- An administrator can also configure Tamper parameters using Webserver interface. Refer [“Tamper Setting for Terminal Security”](#) under Webserver section to know more.
- Please refer to the **MorphoAccess® Sigma Series Installation Guide** for more information about the anti-tamper switch located on the terminal.

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 | Using this parameter, tamper detection can be enabled or disabled. Set parameter value as “0” for disabling the tamper detection, or set parameter value as “1” for enabling the tamper detection. |
| Tamper.action_auth_iden | 0 or 1 | Parameter value “0” indicates that authentication is not disabled on tamper detection. Parameter value “1” indicates that authentication is disabled on tamper detection. |
| tamper.action_erase_biometrics | 0 or 1 | Parameter value “0” indicates biometric database is not erased on tamper detection. Parameter value “1” indicates biometric database is erased on tamper detection. |
| tamper.action_erase_security_data | 0 or 1 | Parameter value “0” indicates security data is not erased on tamper detection. Parameter value “1” indicates security data is erased on tamper detection. |
| tamper.action_play_mmi | 0 or 1 | Using this parameter, an administrator can set terminal to play MMI (Audio), if tamper event is detected. Parameter value “0” indicates MMI is not played on tamper detection. Parameter value “1” indicates MMI is not played on tamper detection. |
| tamper.alarm_interval | 1500 milliseconds (default) | Using this parameter, an administrator can set tamper remote message alarm interval. As per the defined duration of interval, the tamper alarm is sent to distant systems after interval. |

Since the anti-tamper alarm message is sent by the same port/protocol as the access control result messages, this function must be enabled, otherwise the alarm message will not be sent (see section [Sending an Access Control Result Message](#))

Alarm Message Sent through Wiegand or Clock & Data

In addition, if the alarm message is to be sent 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 Configurations*” under Webserver section.
- For output to be sent in Clock and Data format, **External port output type** should be selected as Clock and Data. See “*Wiegand Parameters Settings*” under Webserver section

Tamper Alarm message using UDP

In case of tamper event, the terminal should send an alarm message to a distant system, through Ethernet (or Wi-Fi™), using UDP protocol.

An administrator need to configure parameter “**remote_msg_ip_conf.host_1_protocol**”, as value 1, 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 |

Network & Communication Security Settings

Authorized IP Configuration

This feature allows specifying the IP address of the computers allowed to communicate with the terminal. Connection to the terminal will be rejected for computers with an IP address not present in the list, even with a compatible configuration application.

This is a security feature that prevents, for example, unauthorized terminal configuration modifications.

Access Path

Security Menu > Communication > Authorized IP Configuration

Screens & Steps

Set Authorized IP Mode



Figure 205: Authorized IP addresses Configuration

1. Select **Authorized IP address Configuration**

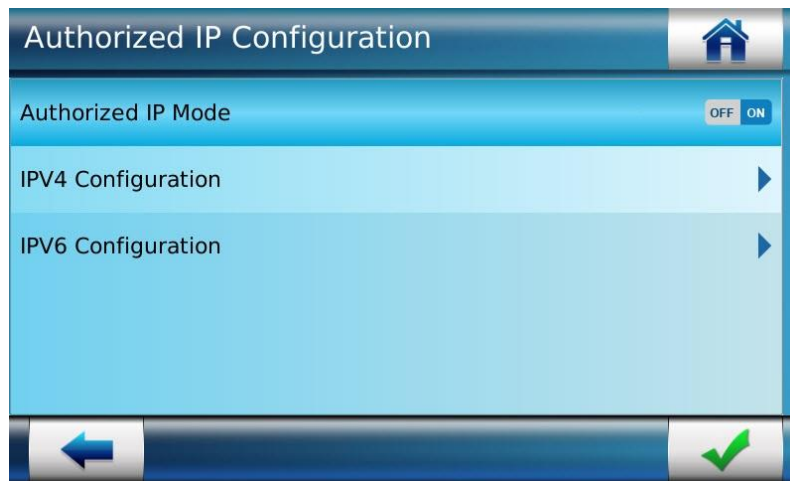


Figure 206: Authorized IP addresses Mode selection

2. Set **Authorized IP Mode** as ON or OFF. If an administrator select OFF, then any IP address is allowed to connect and communicate with terminal. If an administrator set it as ON, then an administrator require adding IP address, that are authorized to communicate with terminal.

Add Authorized IP Address

Using this function, an administrator can add several IP Addresses which are authorized to communicate with the terminal.

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



Figure 207: Adding IP for authorization

2. Select **Add IP Address**



Figure 208: Add IP address


3. **Add IP Address** that an administrator require to authorize, as shown in above screen
4. Press on “” icon to save




Figure 209: A success message is displayed showing IP Address is added successfully

Configure IP Addresses Range

Similar as IP Address, An administrator can add an IP Address Range, to authorize specific computers with IP addresses range to communicate with Morpho Access® terminal. Apart from the defined range of IP addresses, no other computer can communicate with the terminal.



Figure 210: Entering IP Range for authorizing

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

View IP Address

This functionality allows an administrator to view the IP Addresses that are added and authorized to communicate with terminal.

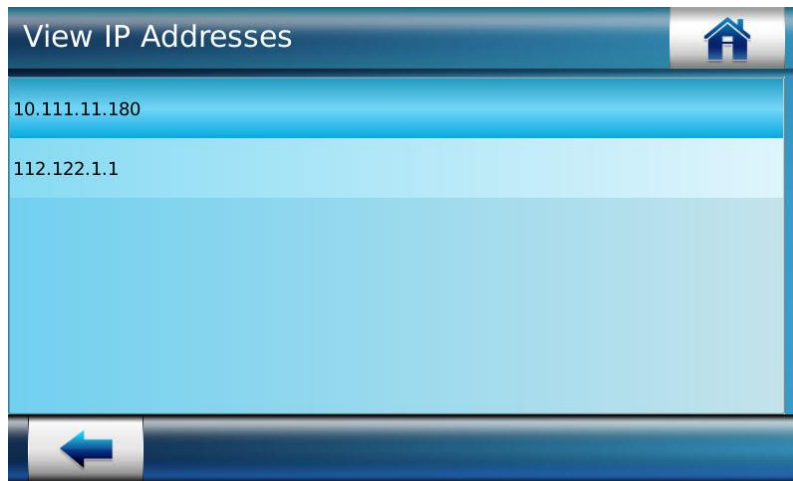


Figure 211: Viewing authorized IP Addresses

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

View IP Range

This functionality allows an administrator to view the Range of IP Addresses that are added and authorized to communicate with terminal.

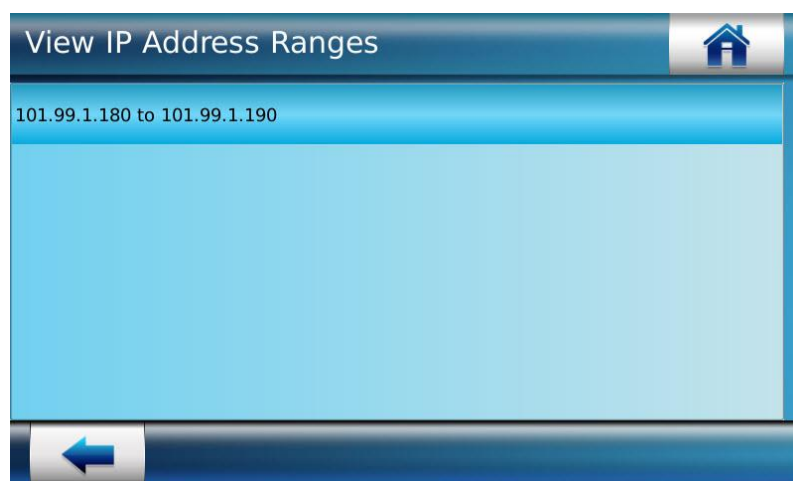


Figure 212: Viewing IP Address Range

1. Press on **View IP Address Range**. List of IP Addresses authorized is displayed

Delete IP Address

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

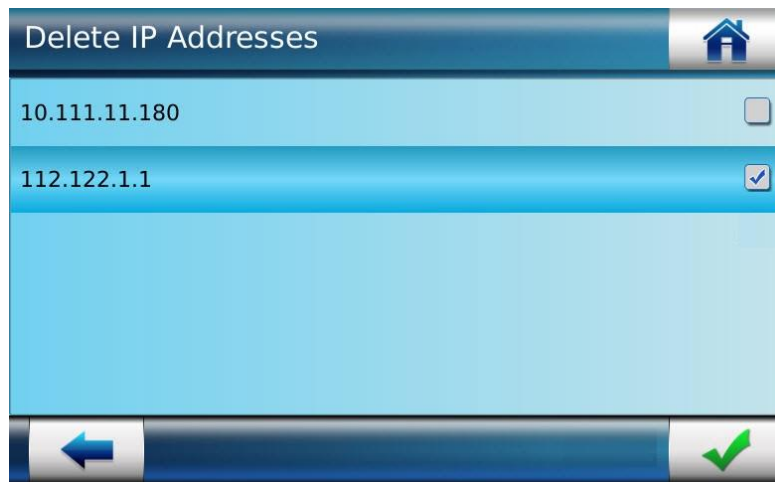


Figure 213: Deleting an IP Address

1. Select an **IP Address**, that an administrator require to delete (which will remove connection authorization)
2. Press on check box to delete an IP address
3. A confirmation message is displayed showing IP address is deleted

Delete IP Address Range

Using this functionality an administrator can delete an IP Address Range. It allows an administrator to select several IP addresses range and delete them. Once deleted, that computer with an IP address within the deleted range cannot communicate with terminal.

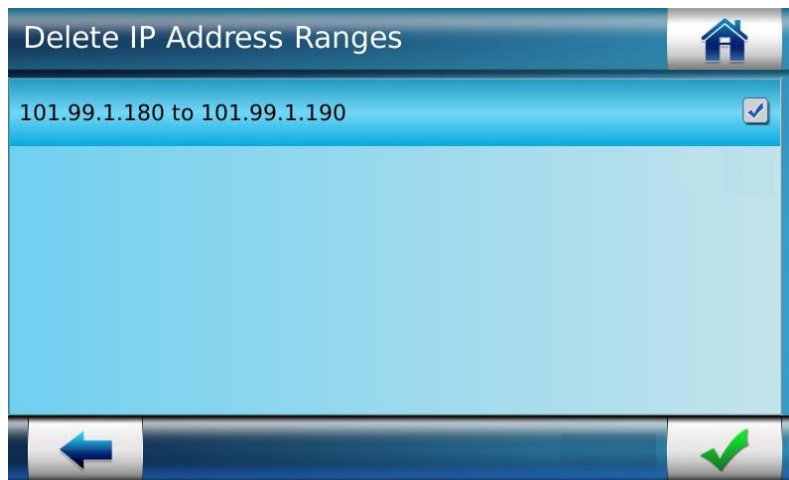



Figure 214: Delete an IP Address Ranges

1. Select an **IP Address Range**, that an administrator require to delete (which will remove connection authorization)
2. Use “” to delete
3. A confirmation message is displayed showing an IP Address Range is deleted

SSL Configuration

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 MorphoAccess® SIGMA Series terminal and a distant system, such as a central access controller or a terminal configuration station.

The cryptographic protocols supported by the terminal are listed below:

- SSLv3
- SSLv23
- TLS 1.0
- TLS 1.1
- TLS 1.2

The terminal supports the algorithms listed below for communication security:

- AES128-SHA OpenSSL cipher suite
- AES256-SHA OpenSSL cipher suite
- AES128-SHA256 OpenSSL cipher suite
- AES256-SHA256 OpenSSL cipher suite
- AES128-GCM-SHA256 OpenSSL cipher suite
- ECDHE-ECDSA-AES256-SHA OpenSSL cipher suite
- ECDHE-ECDSA-AES128-GCM-SHA256 OpenSSL cipher suite
- ECDHE-ECDSA-AES128-SHA256 OpenSSL cipher suite
- ECDHE-ECDSA-AES128-SHA OpenSSL cipher suite

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

Warning : As the Webserver uses http protocol (and not https protocol), it must be deactivated when TLS/SSL protocol is enabled, in order to avoid a security break.

Compatibility of cipher algorithms with SSL protocol versions

| Cipher Algorithm List | Protocol Version | | | | |
|--|------------------|-------|-------|---------|---------|
| | sslv23 | sslv3 | tlsv1 | tlsv1.1 | tlsv1.2 |
| AES128-SHA | Y | Y | Y | Y | Y |
| AES256-SHA | Y | Y | Y | Y | Y |
| AES128-SHA256 | N | N | N | N | Y |
| AES256-SHA256 | N | N | N | N | Y |
| AES128-GCM-SHA256 | N | N | N | N | Y |
| ECDHE-ECDSA-AES256-SHA:ECDH-ECDSA-AES256-SHA | Y | Y | Y | Y | Y |
| ECDHE-ECDSA-AES128-GCM-SHA256:ECDH-ECDSA-AES128-GCM-SHA256 | N | N | N | N | Y |
| ECDHE-ECDSA-AES128-SHA256:ECDH-ECDSA-AES128-SHA256 | N | N | N | N | Y |
| ECDHE-ECDSA-AES128-SHA:ECDH-ECDSA-AES128-SHA | Y | Y | Y | Y | Y |

NOTE: Cipher algorithm that ends with 'SHA256' supports only SSL protocol version tls1.2.

SSL Protocol Versions support for communication

| | | Client side (from PC application) | | | | |
|-------------|---------|-----------------------------------|--------|-------|--------|--------|
| | | sslsv23 | sslsv3 | tlsv1 | tlsv11 | tlsv12 |
| On Terminal | sslsv23 | Y | Y | Y | Y | Y |
| | sslsv3 | 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 client side application, when communication is started by terminal using specific protocol. E.g. If terminal starts communication using sslsv23 protocol, then client side application will be able to communicate using all the protocol versions. While if communication is initiated using sslsv3 protocol, then client application will only support sslsv23 and sslsv3 protocol versions for communication.

Refer to **SSL Solution for MorphoAccess® documentation** for details on SSL securing.

Access Path

Security Menu > Communication > SSL Configuration > Input Channel

Screens & Steps



Figure 215: SSL Configuration

1. Select SSL Configuration
2. On next screen select **Input Channel**

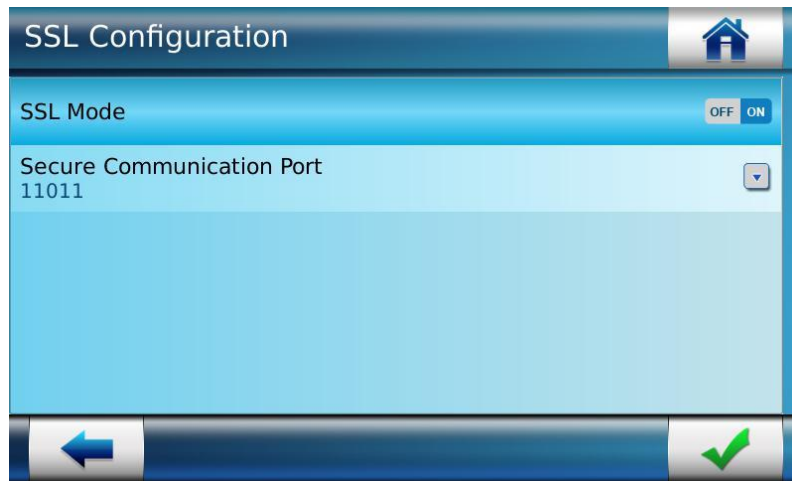



Figure 216: Configuring SSL Mode and parameters

3. Select **SSL Mode** as ON or OFF. Only if the SSL Mode is ON, the SSL protocol is used



Figure 217: Entering Secure Communication Port

4. Enter **Secure Communication Port**: port that will be used for TLS or SSL protocol
5. Use “” button to save

Default Communication Port

Using this functionality, you can define a default communication port that will be used for Ethernet connection.

Access Path

Security Menu > Communication > TCP Channel

Screens & Steps




Figure 218: Selecting Communication Port

1. Select **Communication Port** option



Figure 219: 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 MorphoAccess® SIGMA Series terminal and distant systems, such as external controllers or Webserver application, connected through Ethernet/Wi-Fi™.

By default, TCP Channel is enabled. If this parameter is disabled, the terminal will not be able to communicate (i.e. input or output of messages) with distant systems using Ethernet/Wi-Fi™.


Access Path

Security Menu > Communication > TCP Channel

Screens & Steps



Figure 220: Configuring TCP Channels

1. Select the **TCP Channel** as ON if an administrator require to use TCP protocol for communication
2. Use “” to Save

Enabling Serial Channel

Serial Channel is used for transmission of the input/output messages between the MorphoAccess® SIGMA Series terminal and distant systems, such as external controllers, connected through RS422 and RS485.

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

NOTE: Serial channel cannot be used for configuration of the terminal with the Webserver.


Access Path

Security Menu > Communication > Serial Channel

Screens & Steps



Figure 221: Enabling/Disabling RS422/RS485 Serial Chanel

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

Additional User Verification Settings

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 the fingerprint of two different users to grant the access.

Set Additional Users

Access Path

Security Menu > Communication > Additional User Verification > Additional Users

Screens & Steps

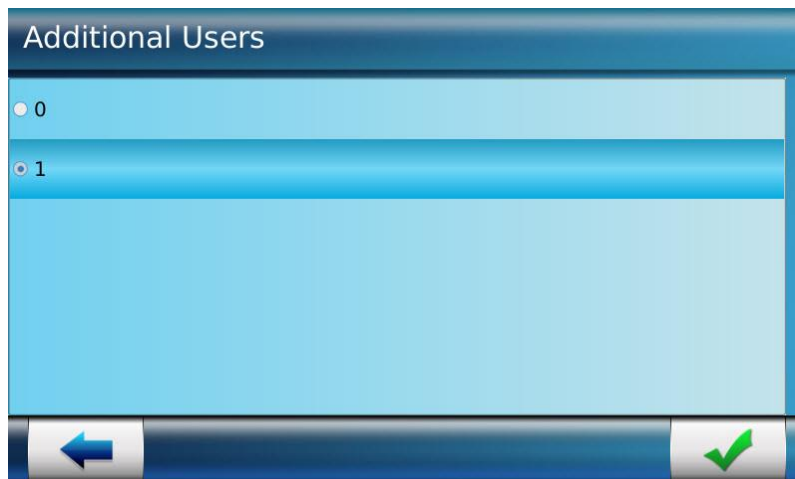



Figure 222: Addition User Verification

1. Select '0' (no additional user) to disable multiple users mode (default): access rights check requires the data of only one user
2. Select '1' (one additional user) to enable multiple users mode with 2 users : access rights check requires the data of two users
3. Use “” to **Save**

Set Additional Users Verification Timeout

This parameter indicates the duration within which the additional user has to place finger on biometric sensor. If finger is not presented with the time limit, then terminal will deny access.

Access Path

Security Menu > Communication > Additional User Verification > Additional Users Verification Timeout

Pre-requisites

- Multiple users feature must be activated: Additional Users should be selected as '1'

Screens & Steps

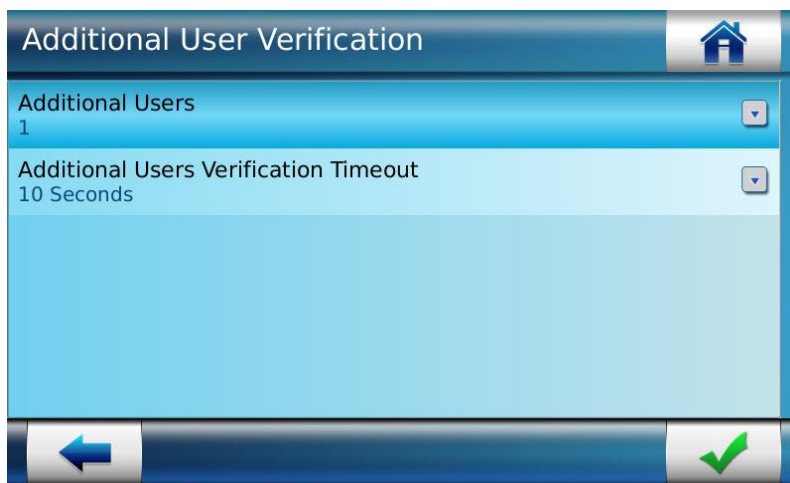



Figure 223: Additional User Verification Timeout

1. Press on **Additional Users Verification Timeout**



Figure 224: Additional User Verification Timeout

2. Enter the **Time limit**
3. Use “” button to save
4. Use “” to Save

Change LCD Password

An administrator can login to terminal using an LCD Password. In order to prevent from password theft or malpractice, it is recommended to change the password periodically. Change password functionality helps an administrator to secure terminal and prevent from any unwanted access and data loss.

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

Access Path

Security Menu > Communication > Change LCD Password

Pre-requisites

- Only an Administrator can change LCD Password

Screens & Steps

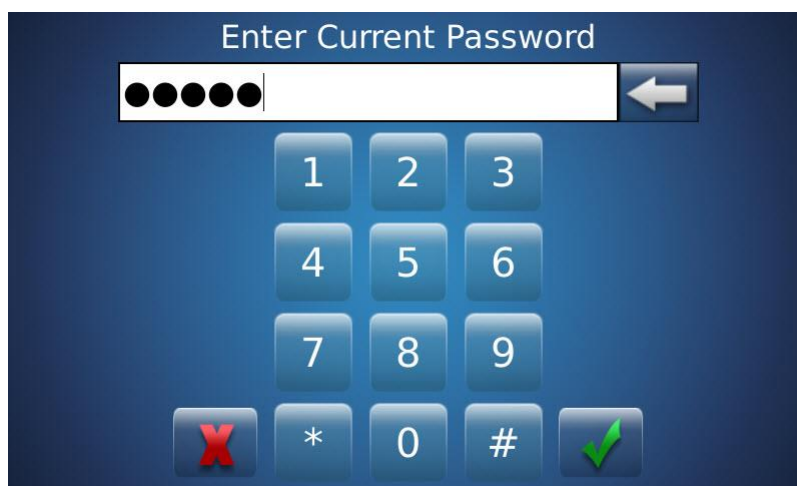



Figure 225: Resetting Device Password

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



Figure 226: Entering New Password

2. Enter the **New Password** of an administrator choice
3. Use “” button to move on next screen

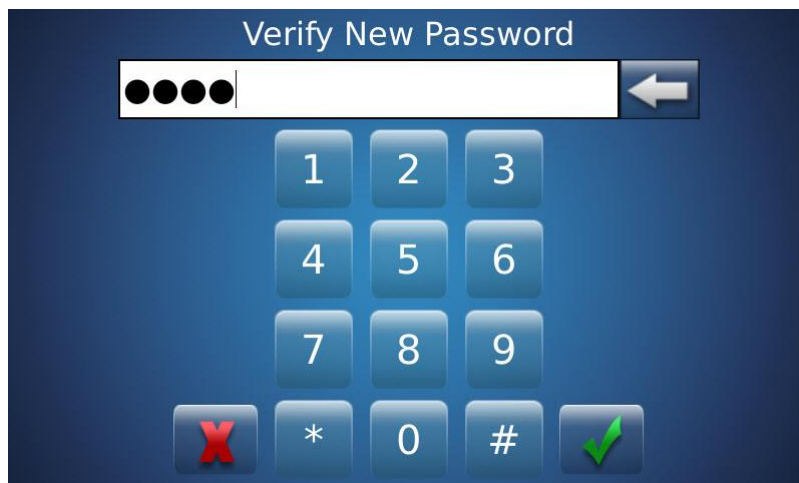



Figure 227: Verifying New Password

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

Using this configuration, an administrator can set which access control parameters are applicable to allow access to the additional users.

Access Path

Security Menu > Communication > Additional User Control

Pre-requisites

- Multiple Users feature must be enabled: Additional User Verification should be set to 1

Screens & Steps

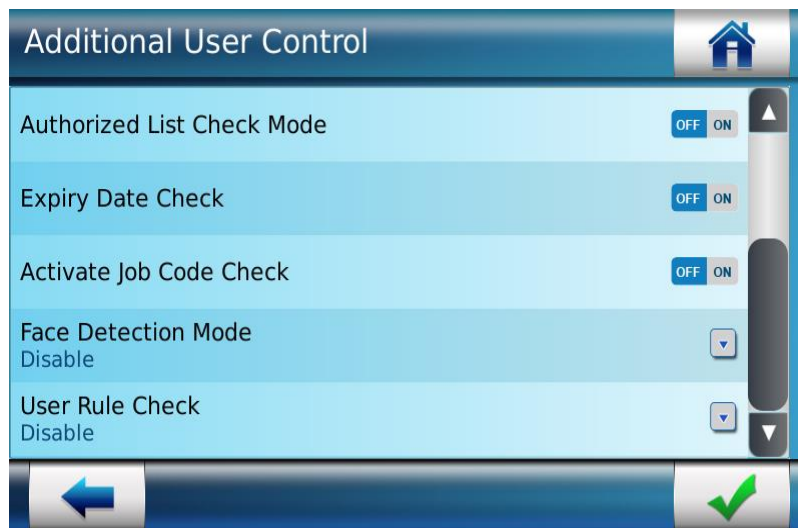


Figure 228: Additional User Control

Set below parameters for Additional User access control:

1. **Access Schedule:** This parameter indicates, whether terminal should check the access schedule of the enrolled user
2. **Holiday Schedule:** This parameter indicates, whether 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 an administrator can set whether the user is an authorized listed user or not. Authorized listed 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:** if this parameter is enabled, then at the time of user enrolment, an administrator can associate a Job Code. Every time when user tries to access, user have to place finger as well provide Job Code for verification

Note : When Time and Attendance mode is enable, enter job code during authentication is optional even though Job Code Check is enable. It is based on the value of 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 biometric check. If user fails to enter job code within this duration, the terminal will deny access (timeout occurs)
- 8. **Face Detection Mode:** This parameter defines face authentication check workflow rule. Possible values are “Disabled”, “Photo taking”, “Face detection (optional)” and “Face detection (mandatory)”.

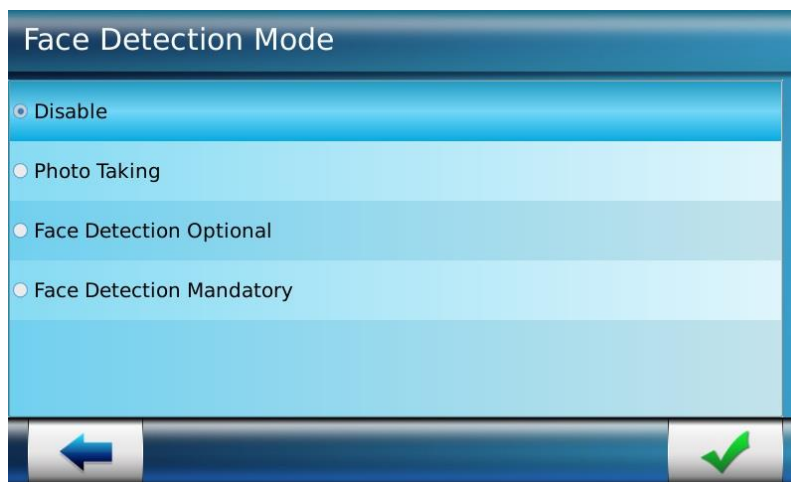


Figure 229: Enable or Disable Face detection mode

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 value is set as 1, then the user images for only successful user control will be saved. If the value is set to 2, then the user images for only failed user control will be saved. If the value is set to 3, then the user images for both successful and failed user control will be saved.

Refer below table for face authentication 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 |
| 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 |

| User Rule_Face Detection | Terminal_Face Detection | ucc.users_ photo_policy | Successful Identification | Failed Identification | Failed Authentication |
|--------------------------|--------------------------|-------------------------|---------------------------|-----------------------|-----------------------|
| | Mandatory | | | | |
| 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 |
| 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 |

| User Rule_Face Detection | Terminal_Face Detection | ucc.users_photo_policy | Successful Identification | Failed Identification | Failed Authentication |
|--------------------------|--------------------------|------------------------|---------------------------|-----------------------|-----------------------|
| 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 | As per 'disabled' |
| Photo Taking | Take one picture and save it according to logging policies | 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. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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 for face detection.

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".

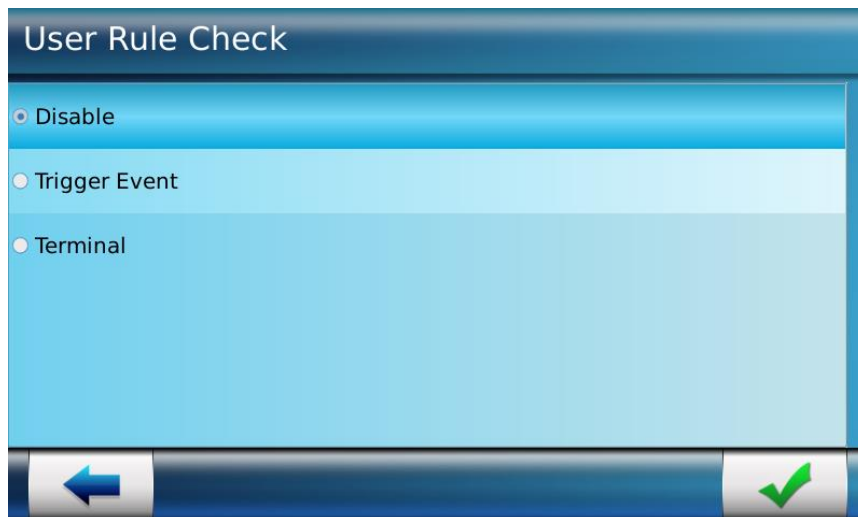


Figure 230: User Rule Check

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 (ref 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 “Disabled”

USB Menu

MorphoAccess® SIGMA Series terminal is equipped with a USB Port that is dedicated to a temporary connection of a USB Mass Storage.

Following are the uses of USB connection:

- Upgrade firmware
- Import data into the terminal, such as User Database, Audio files, Video files, and Images that can be used in Multimedia Configuration
- Export data from terminal to terminal. An administrator can export Transaction logs, Error Logs and User records



Figure 231: USB Menu in MorphoAccess® SIGMA Series Terminal

Format USB Mass Storage device

Format USB Mass Storage device functionality is used to delete entire data stored in an 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

USB Menu > Format USB

Screens & Steps

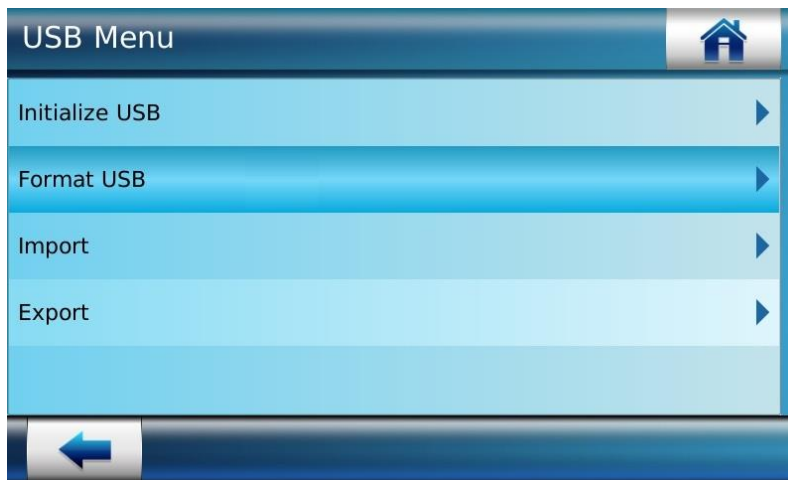


Figure 232: Formatting USB Mass Storage device

1. Connect USB Mass Storage device to terminal
2. Select **Format USB** option



Figure 233: 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 234: Success Message of USB Mass Storage device Formatted

Results

A success message is displayed showing USB Mass Storage device is formatted. Now the USB Mass Storage device can be initialized and used for data exchange.

Initialize USB Mass Storage device

It is a foremost requirement to have all the folders in the USB Mass Storage device, should be arranged similar to the folder structure save in database in the Terminal. Using **Initialize USB Mass Storage device** functionality, terminal will copy the same folder structure in the device.

Access Path

USB Menu > Initialize USB

Pre-requisite

- USB Mass Storage device must be empty.
- If any data is stored on USB Mass Storage device, then it is mandatory the device before initializing
- Connect the USB Mass Storage device for initialization, only once MorphoAccess® SIGMA Series terminal is up and running (even when terminal is rebooted, it must be up and running)

Screens & Steps

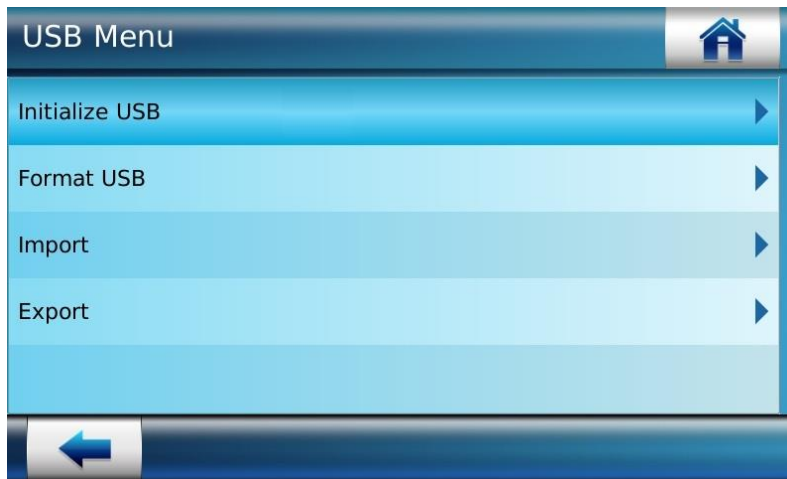


Figure 235: Initialize USB Mass Storage device

1. Connect USB Mass Storage device to terminal
2. Press on **Initialize USB**



Figure 236: 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, an administrator can use USB Mass Storage device for data exchange with terminal, like import data, upload multimedia, or export data.

Import Data into Terminal

MorphoAccess® SIGMA Series terminal is capable of importing several files in its local database. Using Import Data functionality, an administrator can import:

- **User Database:** It is a general practice to maintain a backup of the user database, to prevent from situations when terminal local database is lost. Using Import data functionality, the backup file of user database can be imported in the terminal, which allows terminal to perform access right check functions
- **Language File:** Terminal can support multiple languages. Using Import Language file, an administrator can customize and upload the language file in the terminal. The uploaded languages will be displayed to the user to select from. See "[Language Configuration](#)" for more information.
- **Multimedia Files:** An administrator can import multimedia content such as Audio, Video and Images that are played on terminal on several events. Refer "[Multimedia menu](#)" to view how to import multimedia content.

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 it is recommended to perform import data operation when terminal is in idle state.

Importing User Database

Access Path

USB Menu > Import

Pre-requisite

- USB Mass Storage device should be initialized and must have the user database file in the respective folder
- USB Mass Storage device should be plugged into the terminal

Screens & Steps

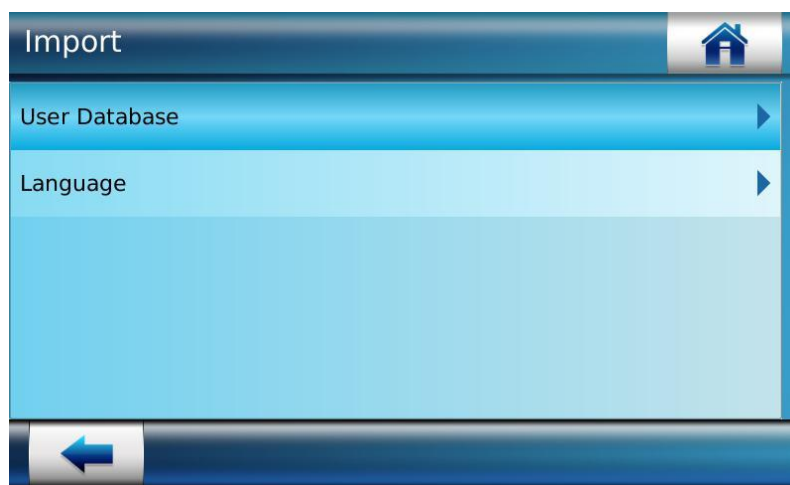


Figure 237: Importing User Database

1. Select **User Database**

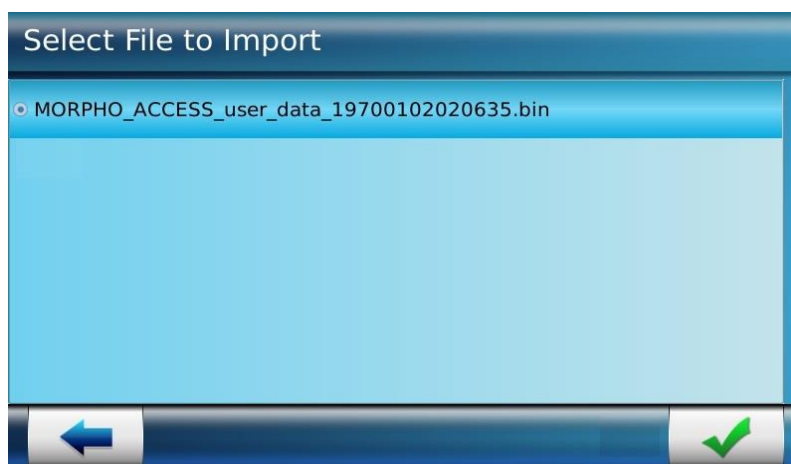


Figure 238: Selecting file to be imported in the terminal

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

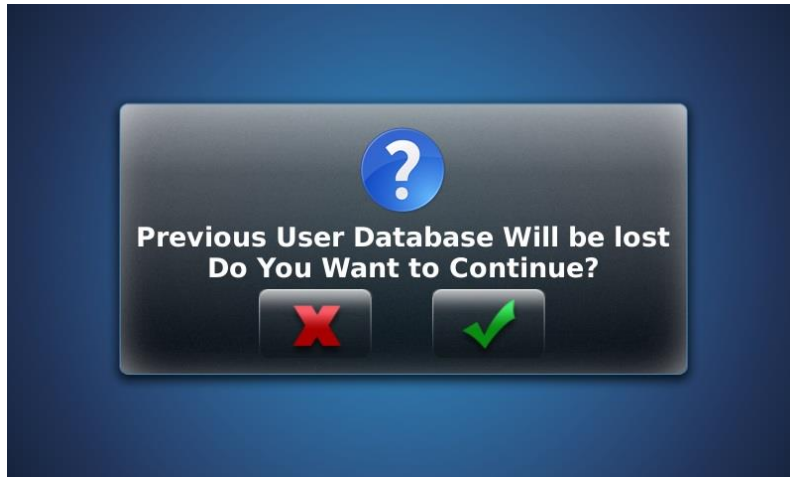


Figure 239: Confirmation message to import User Database



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 240: 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

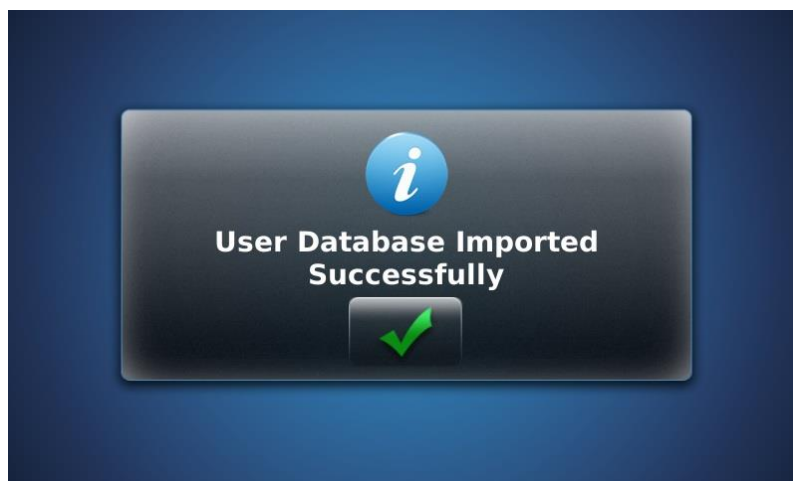


Figure 241: Success message of user data imported is displayed

Results

Once the user's database is imported, the user information can be edited and identification of users can be performed in terminal.

Importing Language File

Access Path

USB Menu > Import

Pre-requisite

- USB Mass Storage device should be initialized and must have the language file in the respective folder
- USB Mass Storage device should be plugged into the terminal

Screens & Steps

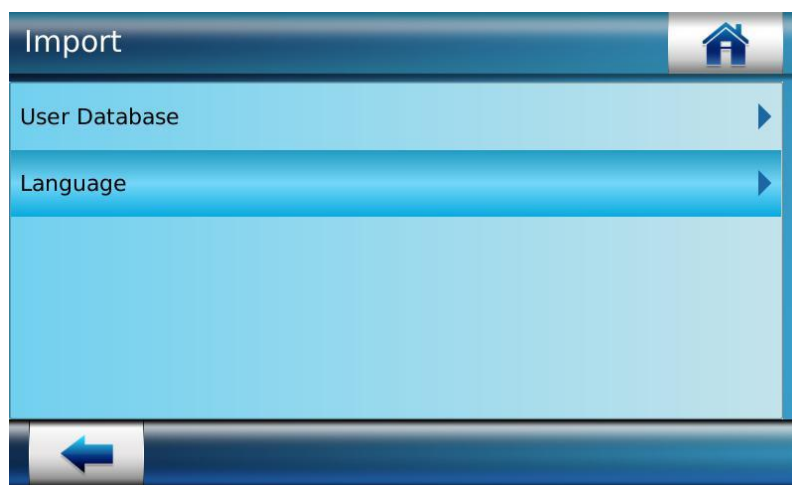


Figure 242: Importing Language file

1. Select **Language** to be imported

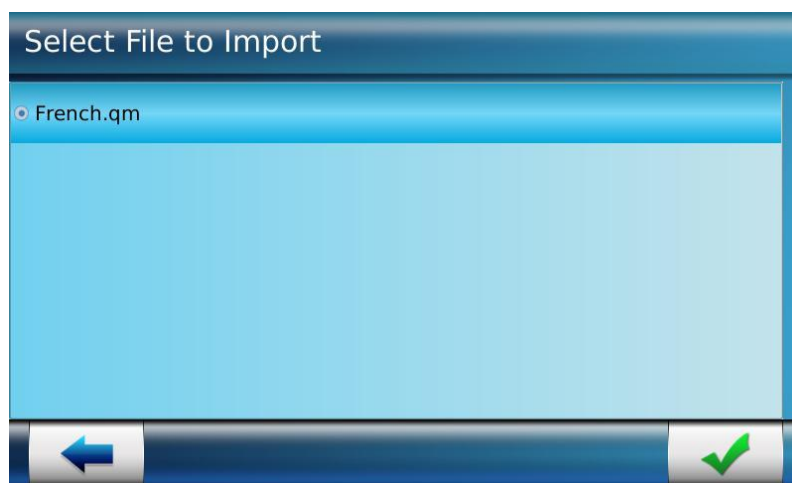


Figure 243: Selecting Language file to import

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

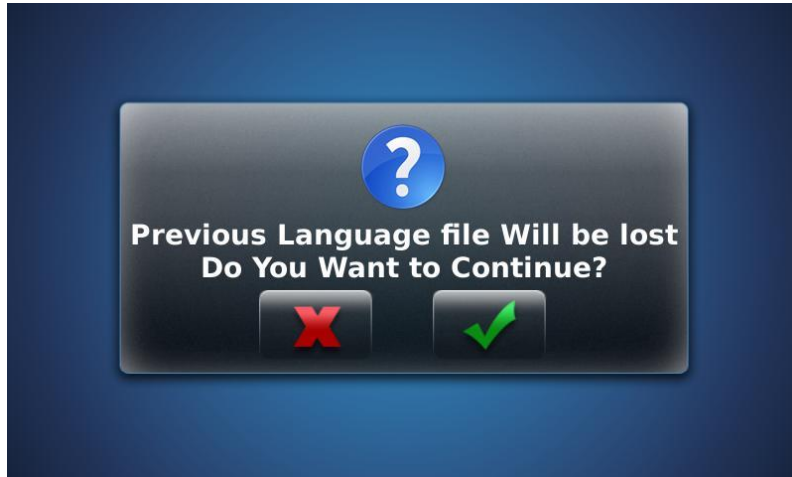


Figure 244: Confirm import action

5. A confirmation message is pop-up, select the check box to confirm import of language file. This action will remove previous language file with the new file



Figure 245: A success message is displayed showing language file is imported

Export Data in USB Mass Storage Device

Using this functionality, an administrator can export the information from terminal database into the USB Mass Storage Device. The terminal allows the exportation of the data listed below:

- **Transaction Logs:** there can be two modes of transaction logging,
- Access Control Logs, in which In-time and Out-time of the user is recorded
- Full Logs are the records of each and every activity performed in terminal, including configurations by administrator
- **Error Logs:** the record of events when access is denied or error occurred
- **User Database:** the record of entire user database

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 into the terminal may take longer duration depending on the data size. This consequently affects the terminal response time and other operations. Hence it is recommended to perform export data operation when terminal is in idle state.

How to Export & View Transaction Logs

Access Path

USB Menu > Export

Pre-requisites

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

Screens & Steps

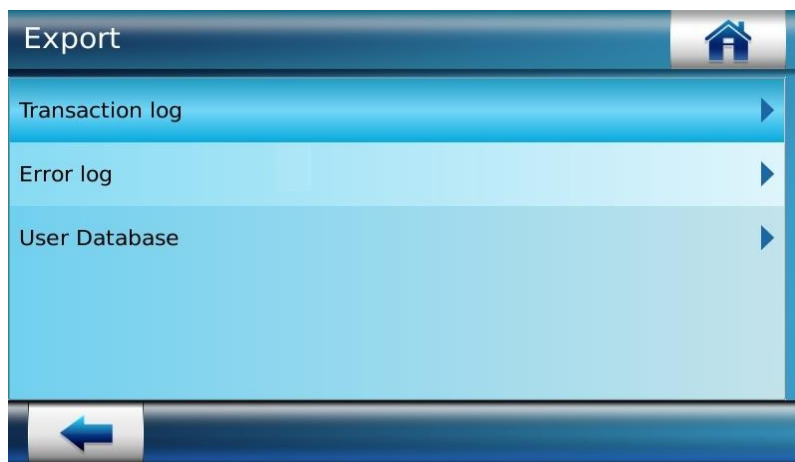


Figure 246: Exporting transaction logs into USB Mass Storage Device

1. Select a record type that an administrator requires to export into the USB Mass Storage Device. Press on **Transaction log**

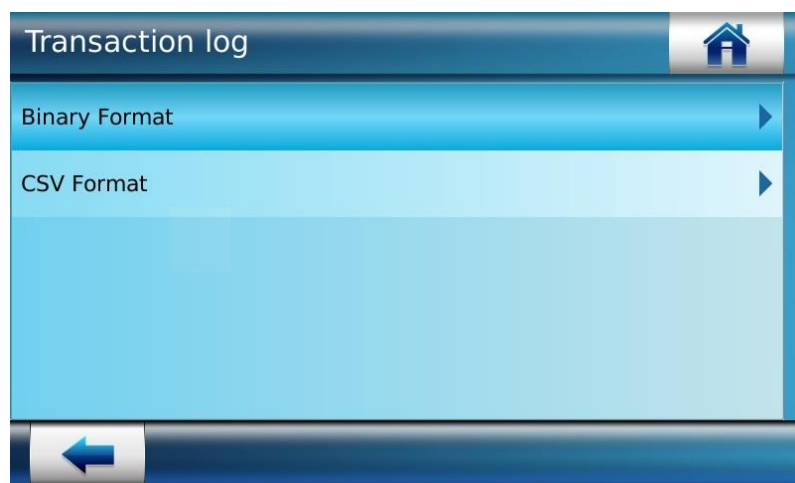



Figure 247: Selecting a file format for exporting transaction logs

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 248: A confirmation message pop-up

3. A confirmation message pop-up is displayed
4. Confirm an action to export log by using “” button

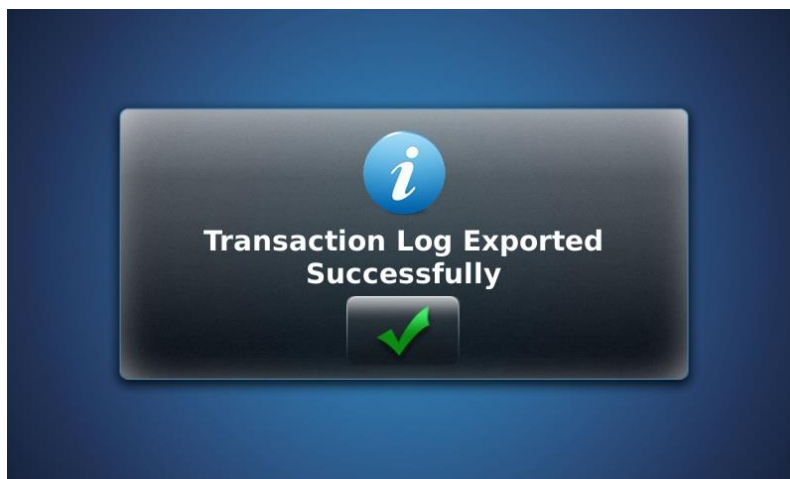


Figure 249: A success message is displayed showing transaction log is exported

| 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/C | Duration | Matched f | Matching | TNA Key | Usr Ctrl | Re Usr | Ctrl Cf | Usr Ctrl | Ch Error | Co |
| 2 | ##### | Pass | Terminal l | 0 | 0 | 0 | 0 | 0 | 0 | IO channe | No administr | ation rights | | | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 3 | ##### | Pass | Terminal l | 0 | 0 | 0 | 0 | 0 | 0 | IO channe | No administr | ation rights | | | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 4 | ##### | Pass | Settings cl | 1 | 0 | 0 | 0 | 0 | 0 | IO channe | No admin first_boot.storage_type | | | | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 5 | ##### | Pass | Settings cl | 1 | 0 | 0 | 0 | 0 | 0 | IO channe | No admin date_time_settings.24_hour_fr | | | | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 6 | ##### | Pass | Settings cl | 0 | 0 | 0 | 0 | 0 | 0 | IO channe | No admin date_time_settings.date_form | | | | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 7 | ##### | Pass | Settings cl | 0 | 0 | 0 | 0 | 0 | 0 | IO channe | No admin date_time_settings.time_form | | | | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 8 | ##### | Pass | Managem | 0 | 0 | 0 | 0 | 0 | 0 | LCD | No administr | ation rights | | | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 9 | ##### | Pass | Managem | 0 | 0 | 0 | 0 | 0 | 0 | LCD | No administr | ation rights | | | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |
| 10 | ##### | Pass | Managem | 0 | 0 | 0 | 0 | 0 | 0 | LCD | No administr | ation rights | | | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 |

Figure 250: 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 & View Error Logs

Access Path

USB Menu > Export

Pre-requisites

- Error Logging must be enabled. Refer to “[Web Server](#)”
- The MorphoAccess® SIGMA Series terminal allows an administrator to enable the access to the Web Server. It allows an administrator to configure any parameter of terminal by connecting remotely. Refer “Introduction to Webserver” in this document.
- By default the access to Web Server is disabled in a MorphoAccess® SIGMA Series terminal.
-

Access Path

System Menu > Miscellaneous Settings > Web Server

Screens & Steps

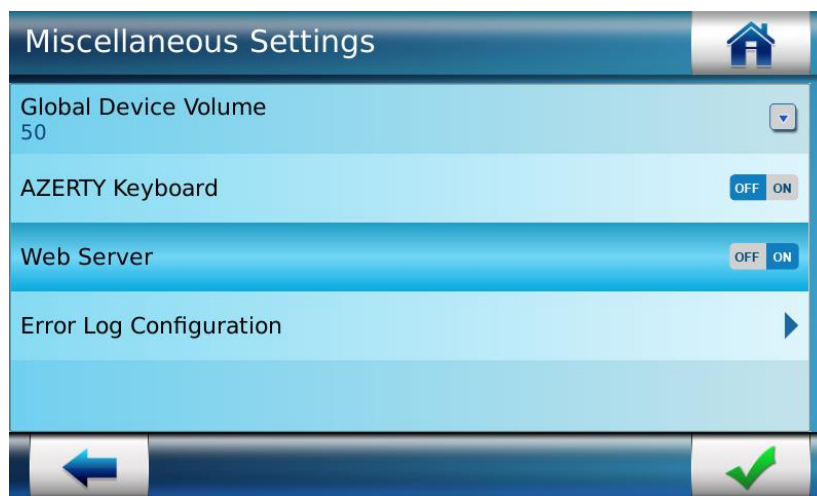


Figure 251: Web Server

5. Select **Web Server** as ON or OFF. If an administrator selects ON, then the administrator will be able to access the Web Server remotely.
- 6.
- 7.
8. Error Log Configuration” for more information about error log configuration

Screens & Steps

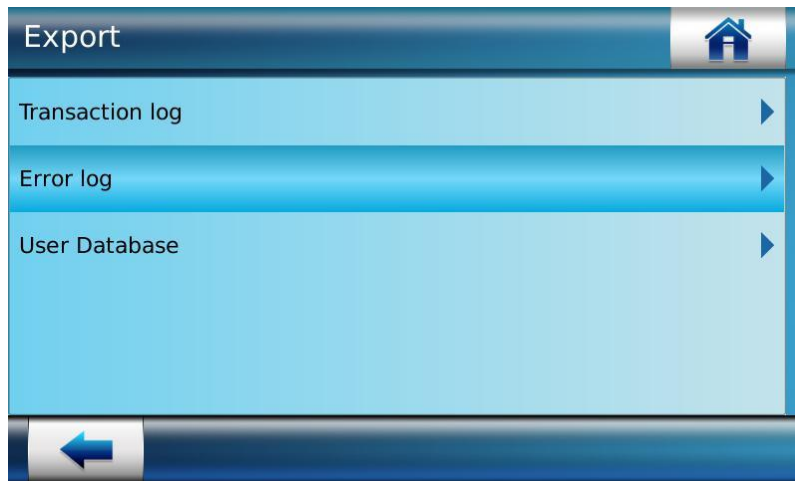


Figure 252: Exporting data into USB Mass Storage Device

1. Select a record type that an administrator requires to export into the USB Mass Storage Device. Press on **Error log**

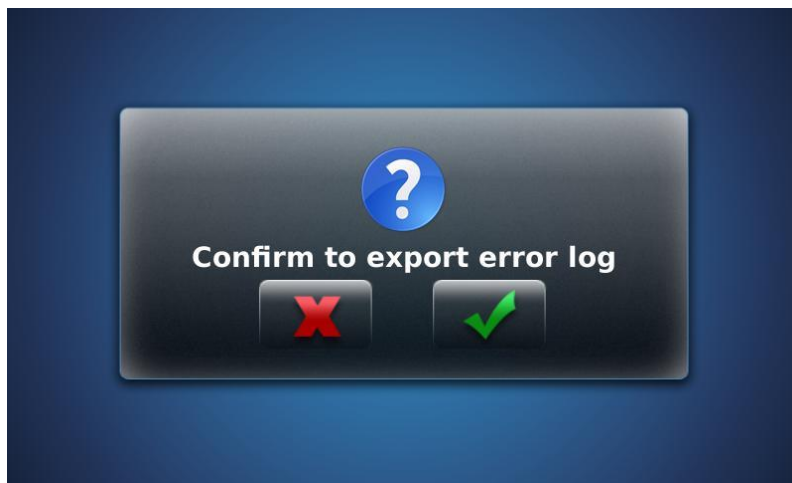


Figure 253: A confirmation message pop-up


2. A confirmation message pop-up is displayed
3. Confirm an action to export log by using “” button



Figure 254: 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 & View User Database

Access Path

USB Menu > Export

Screens & Steps

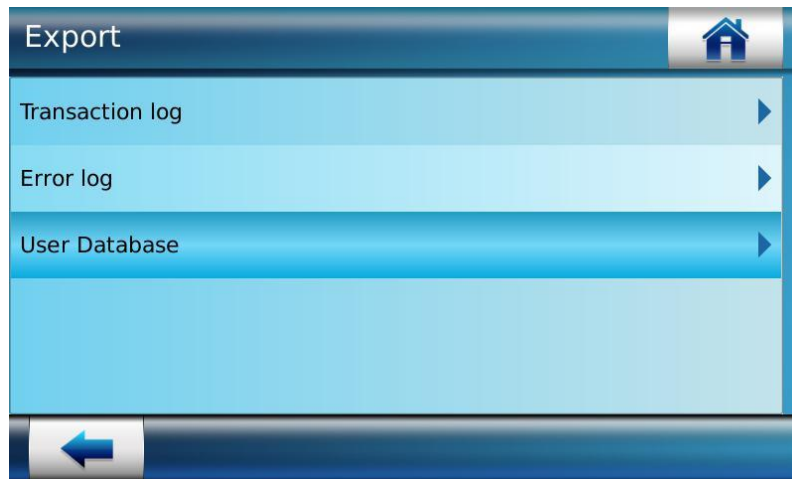


Figure 255: Exporting data into USB Mass Storage Device

1. Select a record type that an administrator requires to export into the USB Mass Storage Device. Press on **User Database**



Figure 256: A confirmation message pop-up


2. A confirmation message pop-up is displayed
3. Confirm an action to export database by pressing “” button



Figure 257: Enter Passphrase


4. Enter **Passphrase**. The same passphrase will be required on importing the user database in terminal
5. Press on “” button



Figure 258: 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.

Information Menu

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

- Information related to Terminal commercial name and license
- Sensor Information
- Firmware version
- Network settings done in terminal, includes Ethernet, Wi-Fi™, Serial Channel, 3G, GSM, and GPRS connections
- Memory Status of the terminal
- User Status, showing count of enrolled, authorized listed and VIP users. Also shows maximum capacity of users supported in terminal
- Transaction Log Status shows count of current logs and maximum supports logs records in terminal



Figure 259: Information Menu

View Device Details

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

Access Path

Information Menu > Terminal

Screens & Steps

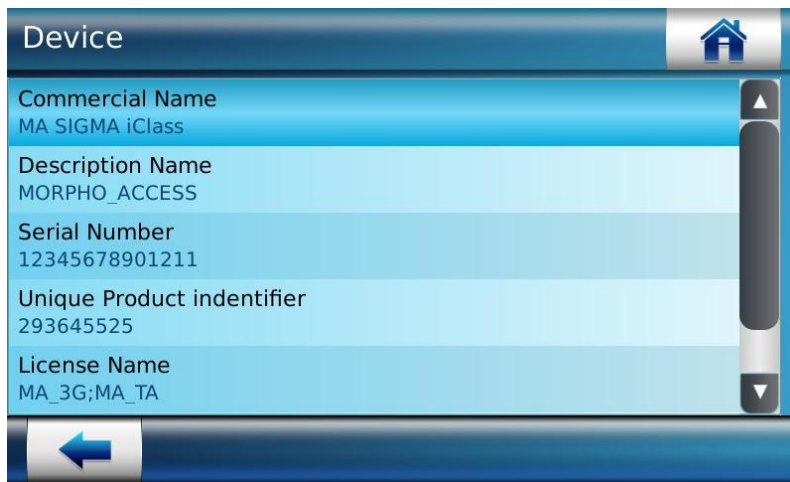


Figure 260: View Device Information

| | | |
|---|---|--|
| | | |
| | MorphoAccess® SIGMA iClass WR FCC ID : ZBW-MASIGMA13M MorphoAccess® SIGMA Multi WR FCC ID : ZBW-MASIGMA13M MorphoAccess® SIGMA Prox WR FCC ID : ZBW-MASIGMA125K MorphoAccess® SIGMA iClass FCC ID : ZBW-MASIGMA13M MorphoAccess® SIGMA Multi FCC ID : ZBW-MASIGMA13M MorphoAccess® SIGMA Prox FCC ID : ZBW-MASIGMA125K | MorphoAccess® SIGMA iClass WR MorphoAccess® SIGMA Multi WR MorphoAccess® SIGMA iClass MorphoAccess® SIGMA Multi |
| MorphoAccess® SIGMA iClass WR IC ID : 11472A-MASIGMA13M MorphoAccess® SIGMA Multi WR IC ID : 11472A-MASIGMA13M MorphoAccess® SIGMA Prox WR IC ID : 11472A-MASIGMA125K MorphoAccess® SIGMA iClass IC ID : 11472A-MASIGMA13M MorphoAccess® SIGMA Multi IC ID : 11472A-MASIGMA13M MorphoAccess® SIGMA Prox IC ID : 11472A-MASIGMA125K | MorphoAccess® SIGMA Prox WR MorphoAccess® SIGMA Prox | |

Figure 261: View Device Regulatory Information

1. Following information of terminal is displayed:
 - a. **Device Commercial Name**
 - b. **Device Description Name**
 - c. **Device Serial Number**
 - d. **Device Unique Product identifier**

- e. **License Name**
- f. **License Identifier**
- g. **Regulatory Information**

View Firmware Information

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

Access Path

Information Menu > Firmware

Screens & Steps

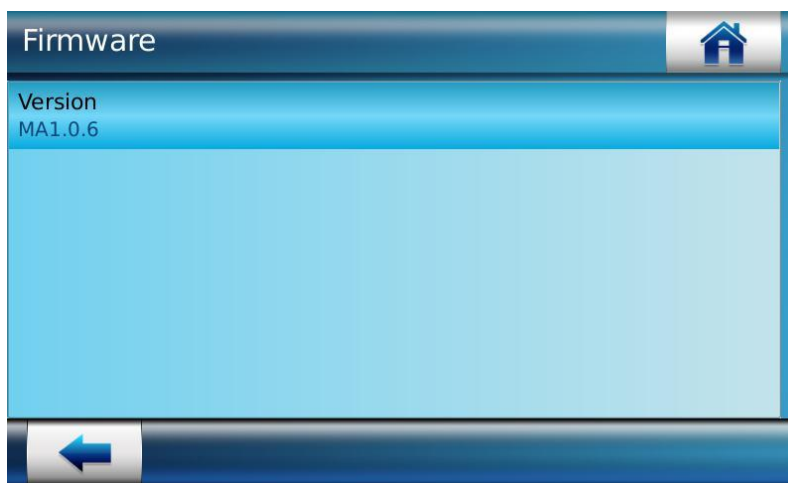


Figure 262: MorphoAccess® SIGMA Series Terminal Firmware Version information

1. The current terminal firmware version information is displayed

View Sensor Revision Information

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

Access Path

Information Menu > Sensor Revision

Screens & Steps

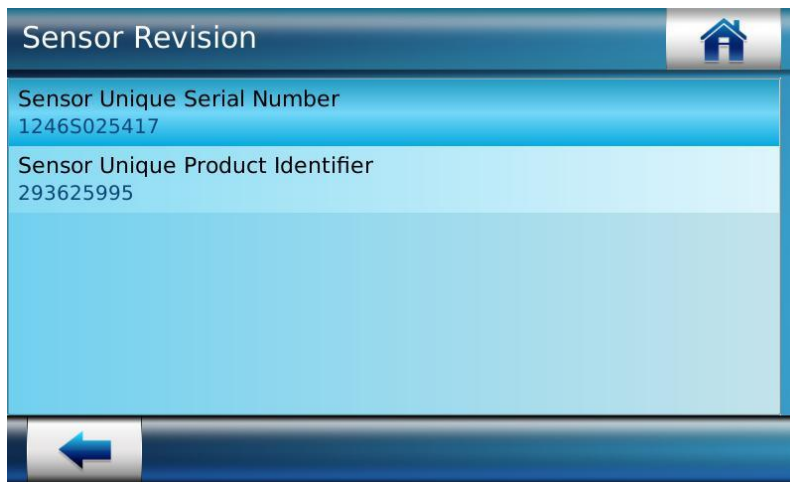


Figure 263: Biometric Sensor data

1. **Sensor Unique Serial Number**
2. **Sensor Unique Product Identifier** is displayed

View Communication Parameters

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

Access Path

Information Menu > Communication

Screens & Steps

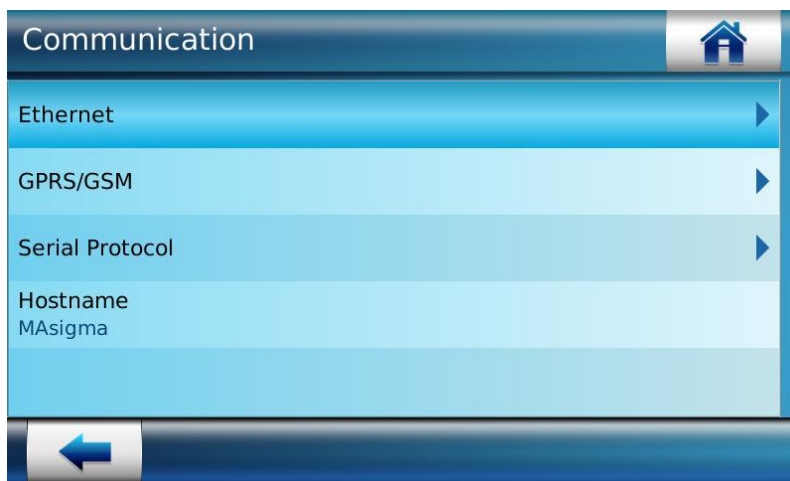


Figure 264: Selecting communication network

1. Select the type of communication network from following options :
 - a. Ethernet
 - b. GPRS/GSM
 - c. Serial Protocol
 - d. Hostname

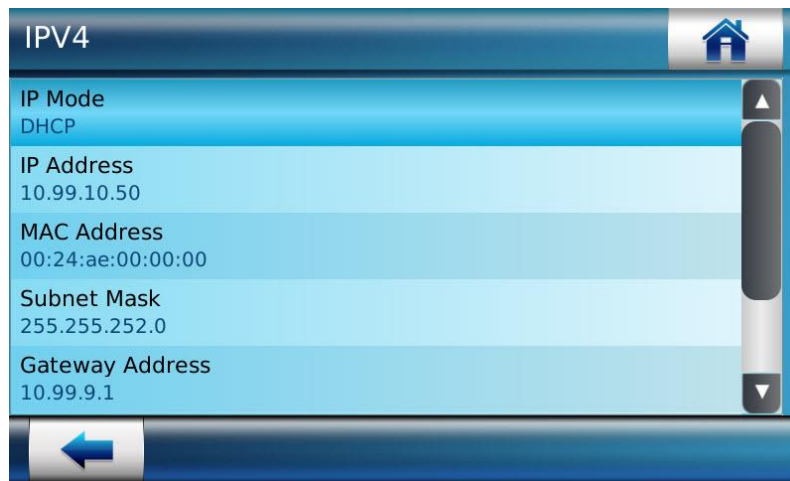


Figure 265: Viewing information of Ethernet network

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**

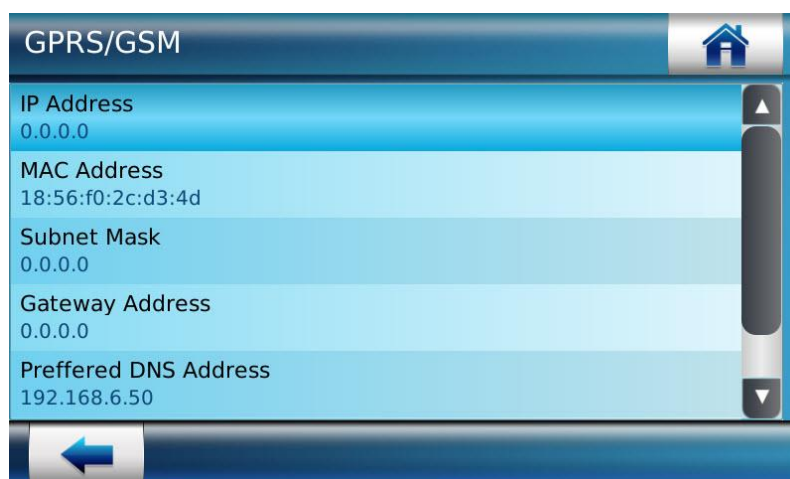


Figure 266: Viewing information of GPRS/GSM network

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**

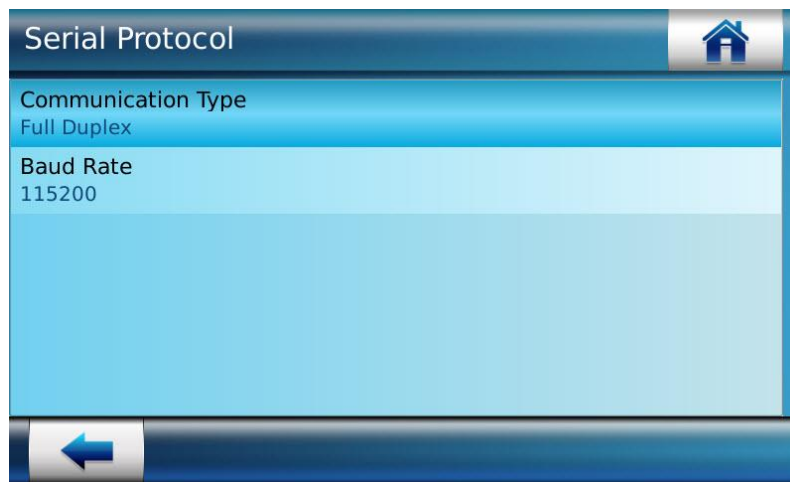


Figure 267: Viewing Serial Protocol Configuration

- 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

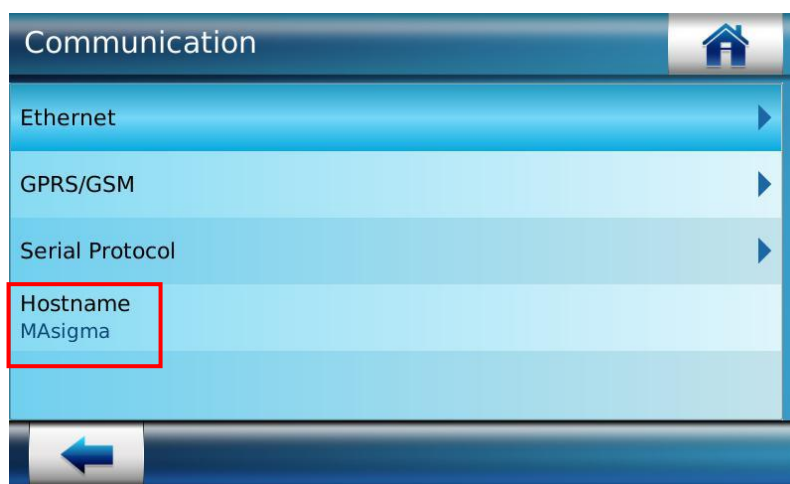


Figure 268: View Hostname of the terminal

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

View Memory Status

Using this functionality, an administrator can view the remaining Memory of the terminal.

Access Path

Information Menu > Memory Status

Pre-requisites

- SD card must be plugged in terminal

Screens & Steps

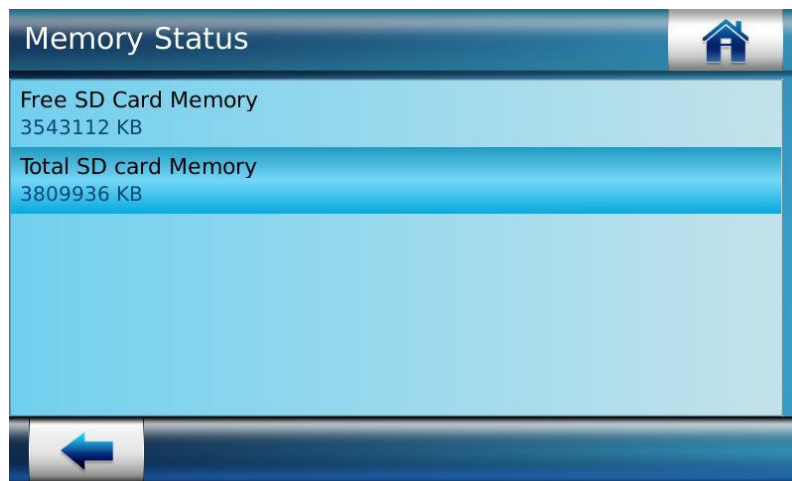


Figure 269: Memory Status of the device is displayed

1. Following information is displayed under Memory State:
 - a. Free SD card Memory
 - b. Total SD card Memory

View User Status

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

Access Path

Information Menu > View User Status

Screens & Steps

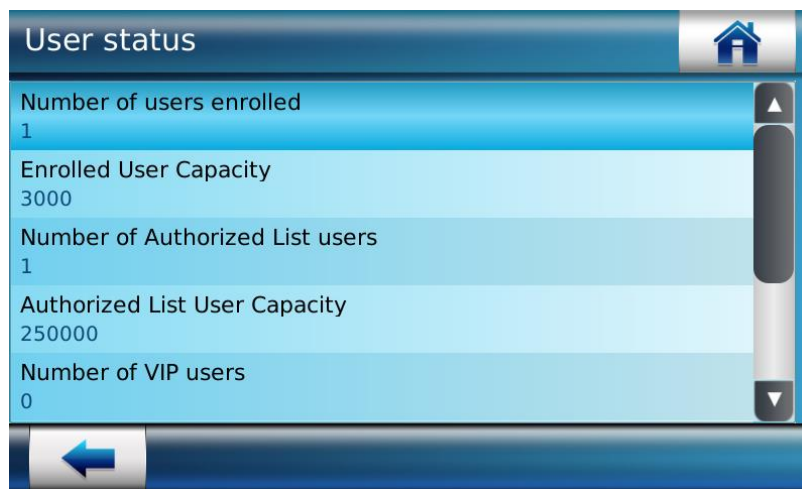


Figure 270: View User Status

Under User Status information section, following information is displayed:

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

View Transaction Log Status

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

Access Path

Information Menu > Transaction Log Status

Screens & Steps

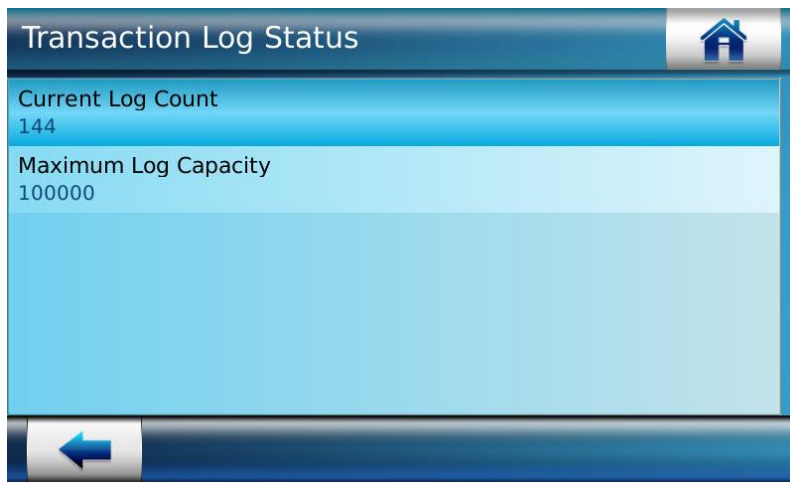


Figure 271: Transaction Log Status is displayed

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

Reboot Terminal Menu

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

- On firmware upgrade
- Installation of Wi-Fi™ USB Adapter
- When terminal legacy mode is changed to 'Legacy L1' or 'Legacy Morpho' or 'MA5G'
- After installation of a new license which upgrade terminal features



Figure 272: Reboot Device

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

The basic parameters of the terminal can be set on "First Boot Assistant" screen that is launched as soon as terminal is reset.

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.

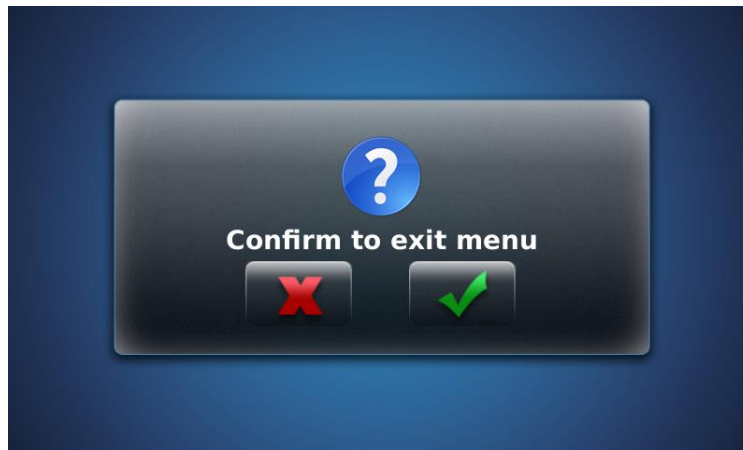


Figure 273: Confirmation Message To Return to Home Screen

Section 7 : Videophone Facility

Introduction to Videophone

MorphoAccess® Sigma 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 touch screen.

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 check by video.

The diagram below show a typical use of this feature:

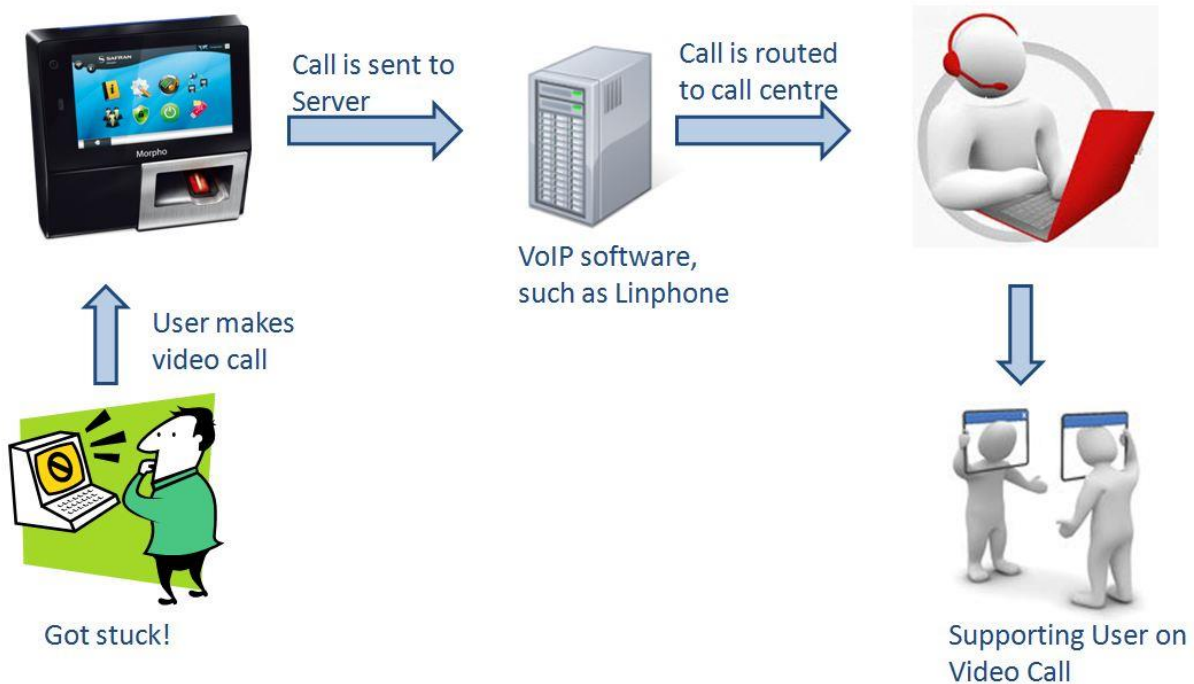


Figure 274: Video Phone Call Flow Diagram sample

For more information about Linphone, please visit Linphone web site at <http://www.linphone.org/>.

Configure Video Phone Server

In order to make a video 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 centre. Thus, an administrator need 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

System Menu > Terminal Settings > Video Phone Configuration

Pre-requisites

- Terminal can be connected with video phone servers only through Ethernet or Wi-Fi™ network

Screens & Steps

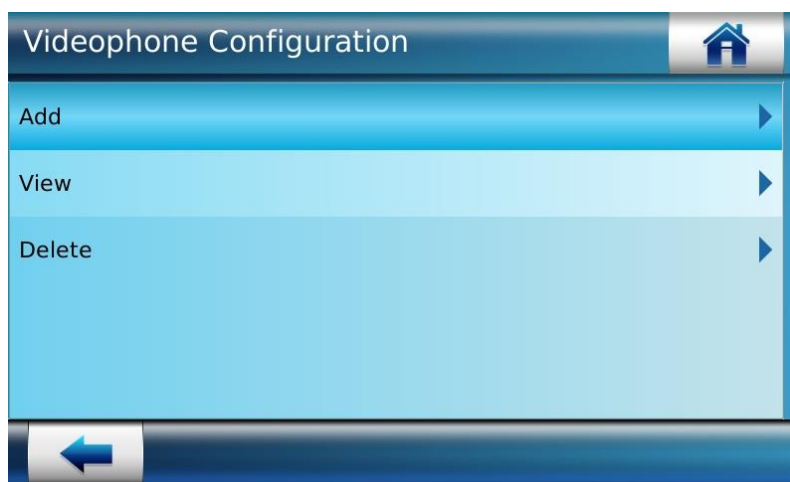


Figure 275: Adding a Server for Video Phone

1. Press on **Add** option for adding server with which video phone will be connected



Figure 276: Enter Server Name


2. Enter **Server Name**
3. Use “” button to move to next screen



Figure 277: Enter Server IP



4. Enter **Server IP Address**
5. Use “” button to move to next screen



Figure 278: Entering Server Port

6. Enter Server Port
7. Use “” button to save

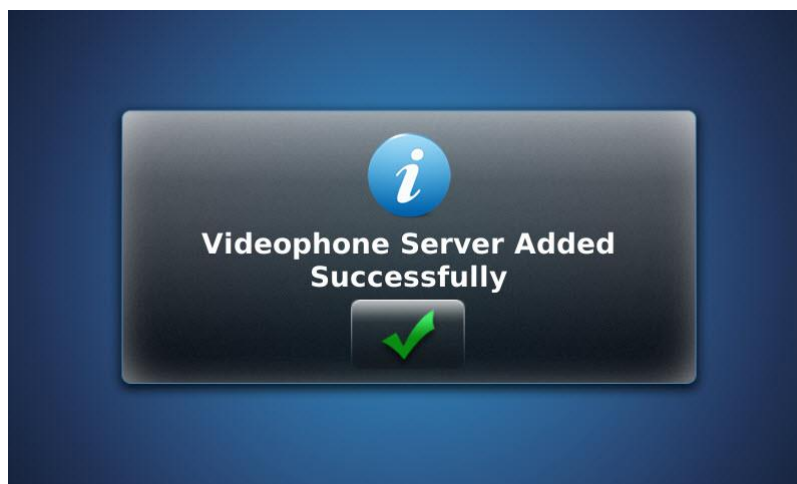


Figure 279: Videophone Server is added successfully

Results

A success message is displayed showing video phone server is added successfully. Video call can be connected once server is configured.

Viewing Video Phone Server Details

Using this feature an administrator can view parameters of video phone server configured on MorphoAccess® SIGMA Series terminal.

Access Path

System Menu > Terminal Settings > Video Phone Configuration

Screens & Steps

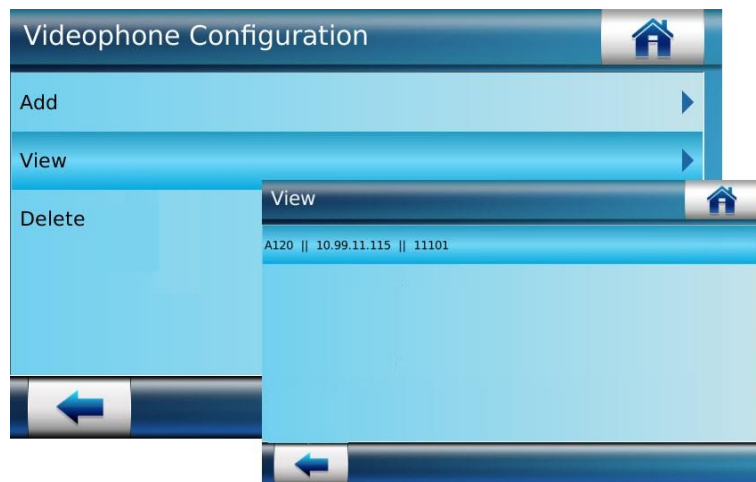



Figure 280: Viewing Video Phone Server Parameters

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 Phone Server

Using this functionality, an administrator can delete a registered videophone from the terminal.

Access Path

System Menu > Terminal Settings > Video Phone Configuration

Screens & Steps

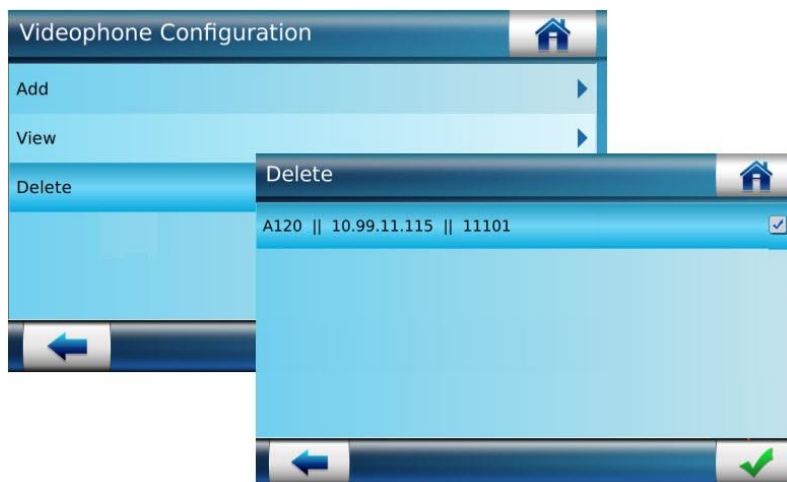



Figure 281: Deleting Video Phone Server

1. Press on **Delete**
2. On delete screen, select the server that is to be deleted
3. Press on “” button to delete server

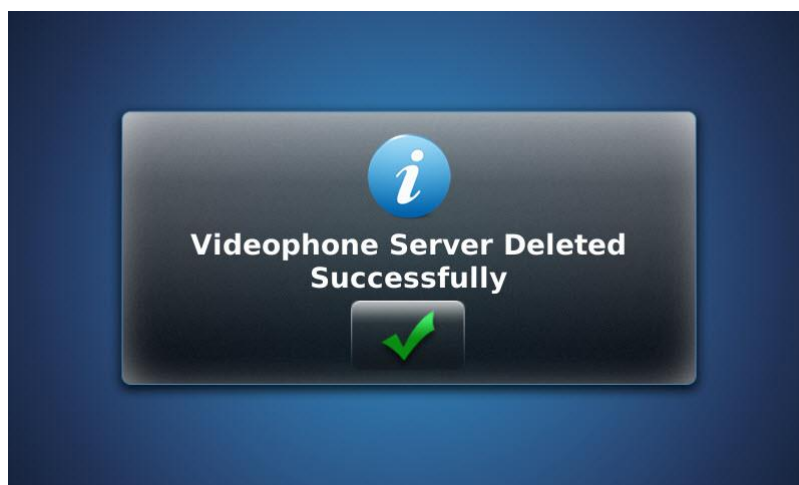


Figure 282: Video Server Deleted Success Message

Results

A success message is displayed on the screen showing video server is deleted. The record of the server is no longer available on 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



Figure 283: Home Screen when NO VOIP profile is configured

How User can make Video Call

Videophone feature of MorphoAccess® SIGMA Series terminal enables end users to make a video call to a customer care centre. The executive at customer care centre can view the user and solve all functional queries on call.

NOTE: During video phone call, terminal does not allow access control operations.

Access Path

Home Screen

Pre-requisites

- Video Phone Server must be pre-configured. Refer to "[Configure Video Phone Server](#)"

Screens & Steps



Figure 284: Making Video Call

1. On Home Screen of terminal, Press on **Call** icon, as shown in above screen

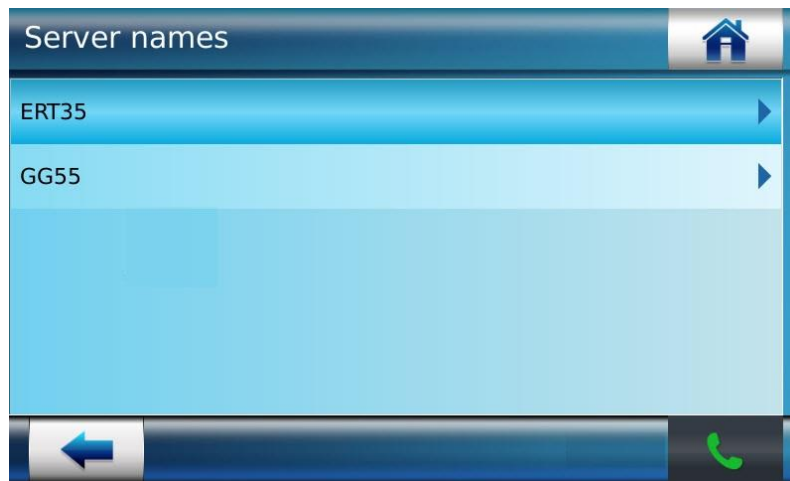


Figure 285: Select Server to make Video Call

2. The list of servers is displayed. Video call is connected to customer care centre through these servers.
3. Select a **Server Name**
4. Press on **Dial** icon

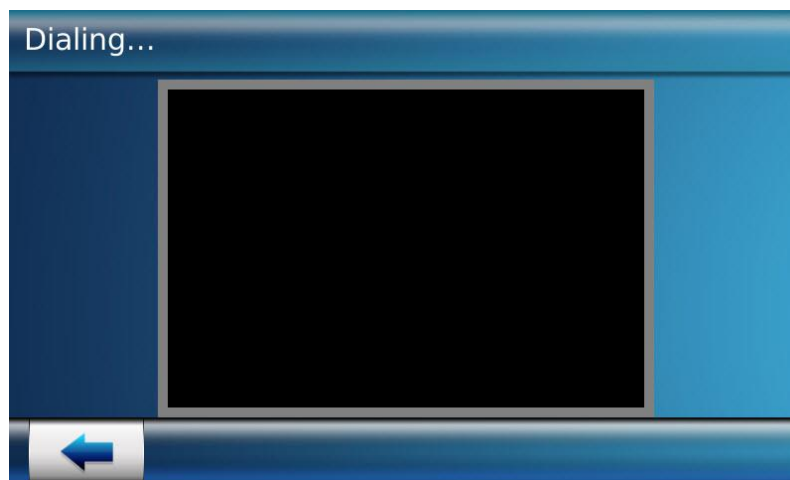


Figure 286: Making Video Call

Results

A Video Phone Call is established with customer care centre. Video of end user is displayed on terminal and transmitted from terminal to the PC of customer centre 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.

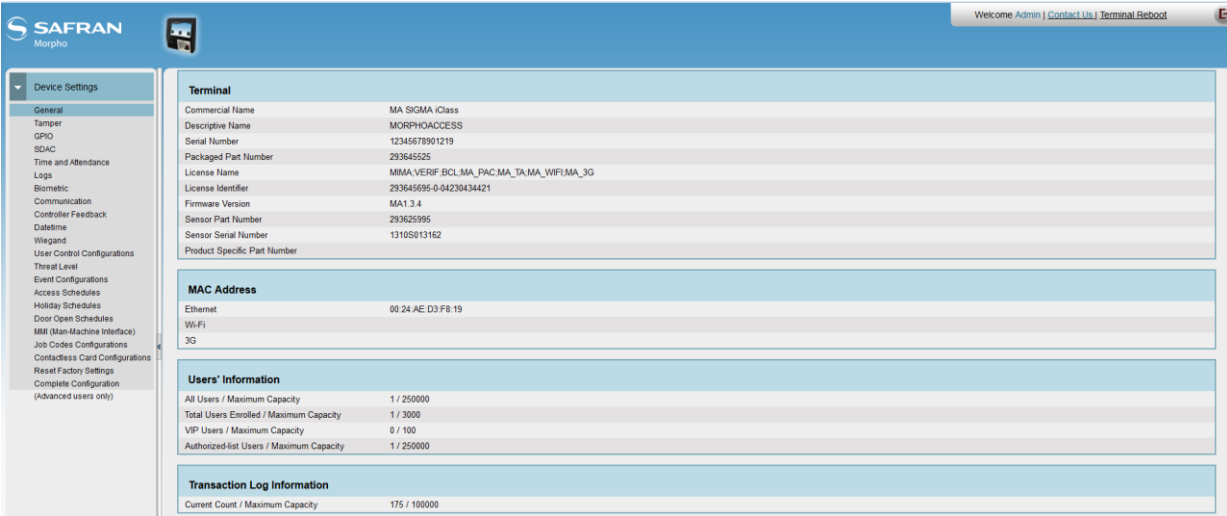
Section 8 : Terminal Configuration through Webserver

Introduction to Webserver

Webserver is a web-based application embedded in the MorphoAccess® SIGMA Series Terminal. Webserver enables the management of the settings of the terminal from any computer (desktop, laptop, tablet ...) equipped with a compatible Internet browser and connected to the same network as the terminal.

Webserver can be connected through MorphoAccess® SIGMA Series terminal through Ethernet or Wi-Fi™ network.

Using terminal login password and IP Address, an administrator can login to the Webserver.



The screenshot displays the MorphoAccess Web Server homepage. The interface includes a top navigation bar with the SAFRAN Morpho logo and a user welcome message. A left sidebar lists various configuration categories under 'Device Settings'. The main content area is divided into several sections:

- Terminal:** A table listing terminal details such as Commercial Name (MA SIGMA iClass), Descriptive Name (MORPHOACCESS), Serial Number (12345678901219), Packaged Part Number (293645525), License Name (MMA-VERIF-BCL-MA-PAC-MA_TA-MA_WIFI-MA_3G), License Identifier (293645695-0-04230434421), Firmware Version (MA1.3.4), Sensor Part Number (293625995), Sensor Serial Number (13105013162), and Product Specific Part Number.
- MAC Address:** A table showing Ethernet (00:24:AE:D3:F8:19), Wi-Fi, and 3G.
- Users' Information:** A table showing user capacity statistics: All Users / Maximum Capacity (1 / 250000), Total Users Enrolled / Maximum Capacity (1 / 3000), VIP Users / Maximum Capacity (0 / 100), and Authorized-list Users / Maximum Capacity (1 / 250000).
- Transaction Log Information:** A table showing Current Count / Maximum Capacity (175 / 100000).

Figure 287: Homepage of Web Server

Once an administrator is logged in, an administrator can view the terminal information on the homepage, which includes:

- Commercial Name of the Terminal
- Description Name
- Serial Number
- Package Part Number
- License Name, displaying compatible licenses
- License Identifier
- Current Firmware Version
- Sensor Part Number and Serial Number
- Product Specific Part Number

- The MAC Address of the terminal fetched from Ethernet and Wi-Fi™ is displayed
- All Users count is displayed along with maximum user storage capacity
- User Enrolled count is displayed along with maximum user stored capacity
- VIP listed users count is displayed along with maximum VIP listed user stored capacity
- Authorized listed users count is displayed along with maximum Authorized listed user stored capacity

All items of configuration menu are available on left side panel of the screen.

Security recommendation

The Webserver use http protocol, then it must be deactivated when TLS/SSL is enabled, to avoid a security break.

Tamper Setting for Terminal Security

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

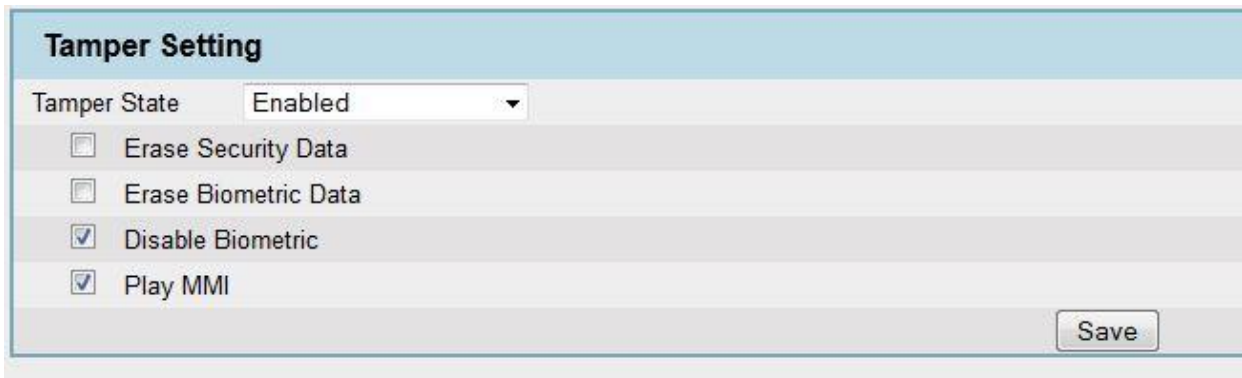
- Someone tries to steal the complete terminal,
- Someone tries to open the terminal

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

Access Path

Tamper

Screens & Steps



| Tamper Setting | |
|-------------------------------------|----------------------|
| Tamper State | Enabled |
| <input type="checkbox"/> | Erase Security Data |
| <input type="checkbox"/> | Erase Biometric Data |
| <input checked="" type="checkbox"/> | Disable Biometric |
| <input checked="" type="checkbox"/> | Play MMI |
| <input type="button" value="Save"/> | |

Figure 288: Tamper Settings through Webserver

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

- c. **Disable Biometric:** If this parameter is enabled, then under Tamper state user will not be able to do successful biometric check on the terminal (access will be denied)
 - d. **Play MMI** can be enabled if an administrator requires playing a sound alarm on terminal on tamper detection. The audio file uploaded in the terminal will be played
7. Click on **Save**

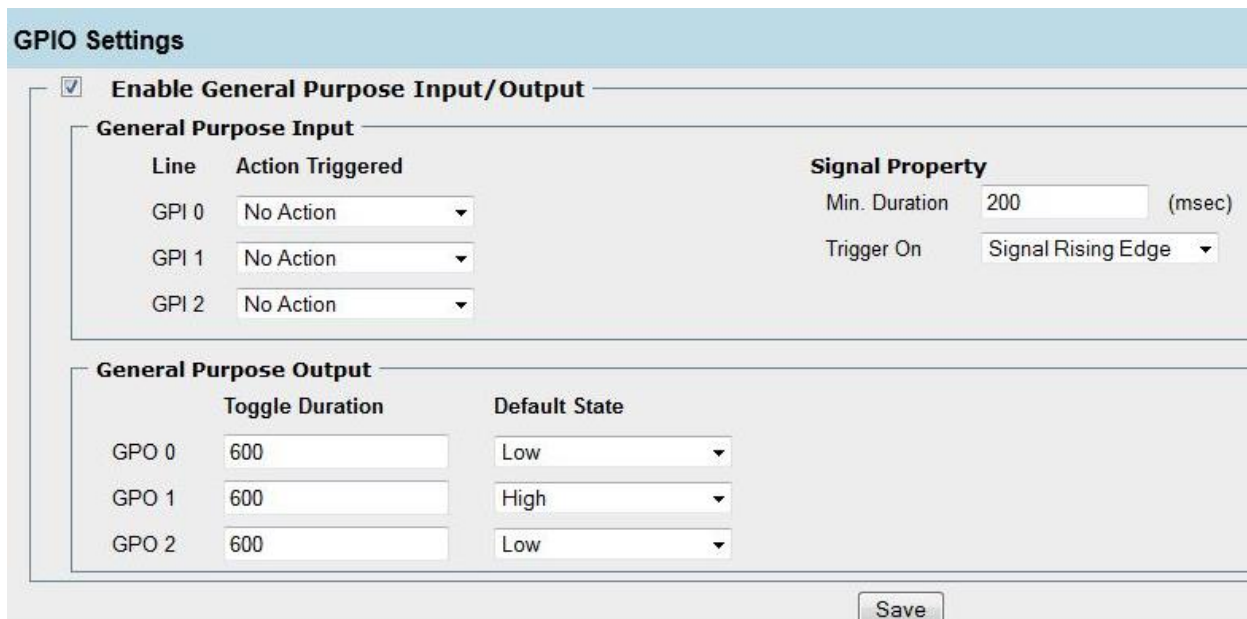
General Purpose Input Output Configuration

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

Access Path

GPIO

Screens & Steps



| General Purpose Input | | Signal Property | |
|-----------------------|------------------|-----------------|--------------------|
| Line | Action Triggered | Min. Duration | 200 (msec) |
| GPI 0 | No Action | Trigger On | Signal Rising Edge |
| GPI 1 | No Action | | |
| GPI 2 | No Action | | |

| General Purpose Output | | |
|------------------------|-----------------|---------------|
| | Toggle Duration | Default State |
| GPO 0 | 600 | Low |
| GPO 1 | 600 | High |
| GPO 2 | 600 | Low |

Figure 289: GPIO Settings through Webserver

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

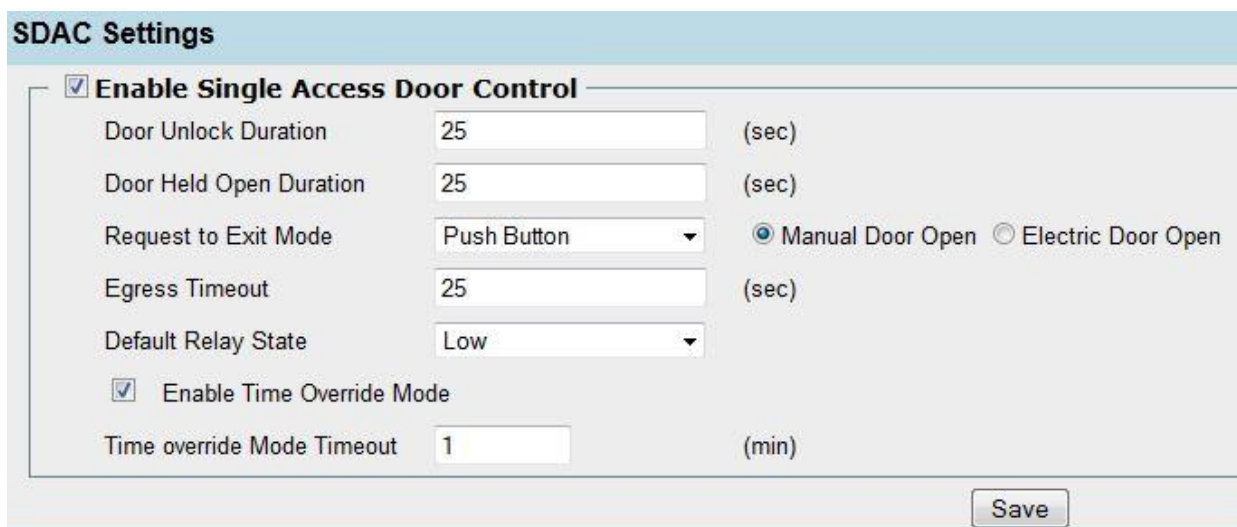
Single Door Access Control Settings

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

Access Path

SDAC

Screens & Steps



| SDAC Settings | | |
|--|--|--|
| <input checked="" type="checkbox"/> Enable Single Access Door Control | | |
| Door Unlock Duration | <input type="text" value="25"/> | (sec) |
| Door Held Open Duration | <input type="text" value="25"/> | (sec) |
| Request to Exit Mode | <input type="text" value="Push Button"/> | <input checked="" type="radio"/> Manual Door Open <input type="radio"/> Electric Door Open |
| Egress Timeout | <input type="text" value="25"/> | (sec) |
| Default Relay State | <input type="text" value="Low"/> | |
| <input checked="" type="checkbox"/> Enable Time Override Mode | | |
| Time override Mode Timeout | <input type="text" value="1"/> | (min) |
| <input type="button" value="Save"/> | | |

Figure 290: SDAC Settings on Webserver

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

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

- i. If an administrator selects Push Button as exit mode, then an administrator can select **Manual Door Open** or **Electric Door Open** actions
 - b. When Exit Mode is in 'Push Button-Manual Door Open', then an administrator needs to set **Egress Time Out**. Within the Egress Time, the door will remain open and on timeout it will lock automatically
4. Select **Default Relay** state as High or Low. Here an administrator can set a default state of the internal relay, which is powered or unpowered.
 - a. Select "0" for Low. It indicates that by default the internal relay will be unpowered and on access granted the internal relay state will change to high (it will be powered).
 - b. Select "1" for High. It indicates that by default the internal relay will be powered and on access granted the internal relay state will change to low (it will be powered off).
5. Enable **Time Override Mode (TOM)**, it allows an administrator to temporarily suspend the need for verification of users for a specific time period on a terminal. Whenever TOM is triggered on terminal then door gets unlock and user can open Door without any authentication till TOM remains continue.
 - a. **For example**, during lunch hours most of the employees head towards cafeteria. Suppose an administrator set TOM for 90 minutes, then during this period the door will be opened and employees will not require verifying for opening door.
6. Enter the number of minutes TOM will be active into the **Time Override More Timeout** field
7. Click on **Save**

Time and Attendance Mode Configuration

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

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

Function key # 1 (F1)

Function key # 2 (F2)

A user has to press respective F key, for an action. If user is entering in office, then user is required to first press F1 on the touch screen and then place finger for biometric authentication.

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

Refer to "[Time and Attendance Mode](#)" section for detailed description.

Using Webserver interface an administrator can configure the Time and Attendance parameters of the terminal. An administrator can configure two modes of Time and Attendance:

- **Normal/Simple:** This mode supports 4 keys, which can be configured and displayed to the user at the time of access request
- **Extended:** This mode supports 16 keys, which can be configured and displayed to the user at the time of access request

Below screens and steps shows an administrator how an administrator can configure T&A parameters.

Access Path

Time and Attendance

Screens & Steps

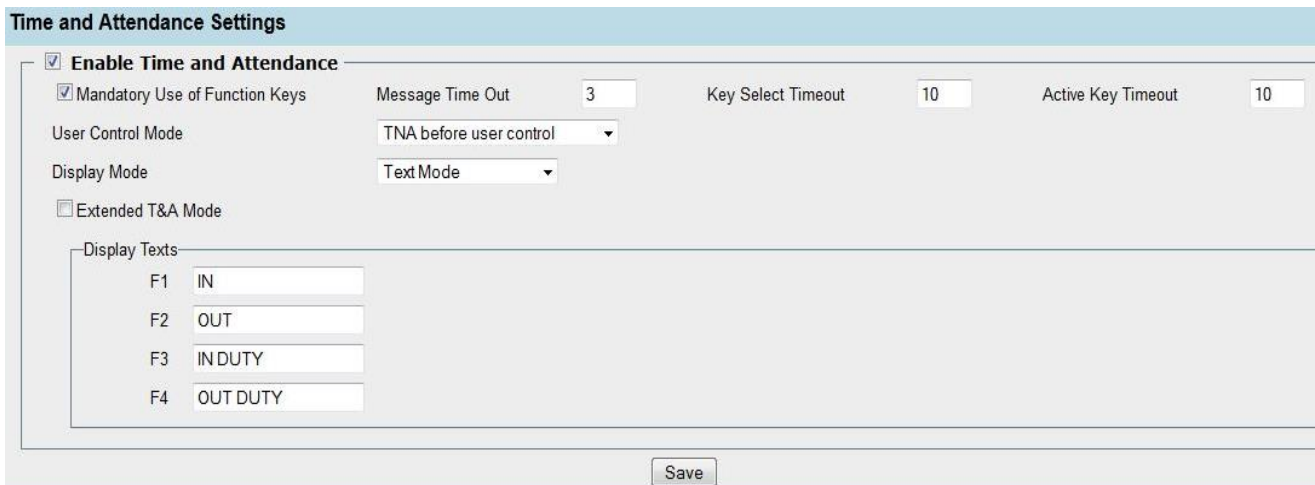


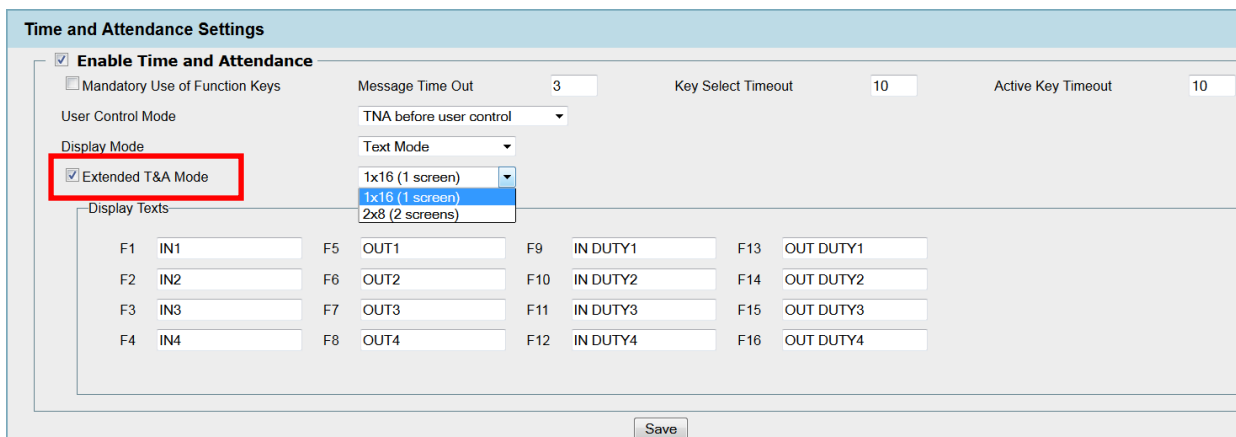
Figure 291: Normal Time and Attendance mode

1. Click on **Enable Time and Attendance**, for enabling this mode
2. Click on **Mandatory Use of Function Keys**. On enabling this, terminal will pop up T&A screen every time after user presents fingerprint. If mandatory is not selected, then user can select T& A option before
3. **Message Timeout:** an administrator can define the duration for which access result is displayed on the LCD screen of the terminal
4. **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.
5. **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.
6. 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).
7. 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.

8. If an administrator requires T&A in Normal mode, then do not select Extended T&A mode check box. In normal mode, only 4 functional keys are required to be configured

9. 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:
 - a. F1 = IN
 - b. F2 = OUT
 - c. F3 = IN DUTY
 - d. F4 = OUT DUTY



Time and Attendance Settings

Enable Time and Attendance

Mandatory Use of Function Keys Message Time Out: 3 Key Select Timeout: 10 Active Key Timeout: 10

User Control Mode: TNA before user control

Display Mode: Text Mode

Extended T&A Mode

Display Texts:

| | | | | | | | |
|----|-----|----|------|-----|----------|-----|-----------|
| F1 | IN1 | F5 | OUT1 | F9 | IN DUTY1 | F13 | OUT DUTY1 |
| F2 | IN2 | F6 | OUT2 | F10 | IN DUTY2 | F14 | OUT DUTY2 |
| F3 | IN3 | F7 | OUT3 | F11 | IN DUTY3 | F15 | OUT DUTY3 |
| F4 | IN4 | F8 | OUT4 | F12 | IN DUTY4 | F16 | OUT DUTY4 |

Save

Figure 292: Extended Time and Attendance mode

10. Click on **Extended T&A Mode** checkbox. Under extended mode 16 functional keys can be configured
11. 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.
12. Click on **Save** once required configurations done

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



Figure 293: User Interface on Terminal



Figure 294: Time and Attendance UI in Normal mode



Figure 295: Time and Attendance UI in Normal mode with Icons



Figure 296: Time and Attendance UI in Extended mode



Figure 297: Time and Attendance UI in Extended mode (2x8 - 2 screens)

Results

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

Transaction Log Settings

The MorphoAccess® SIGMA Series terminal logs various information related to each action performed by the terminal. Terminal can store User identified or not identified, it stores the result of each transaction, the date and time, the execution time, and the ID of the user.

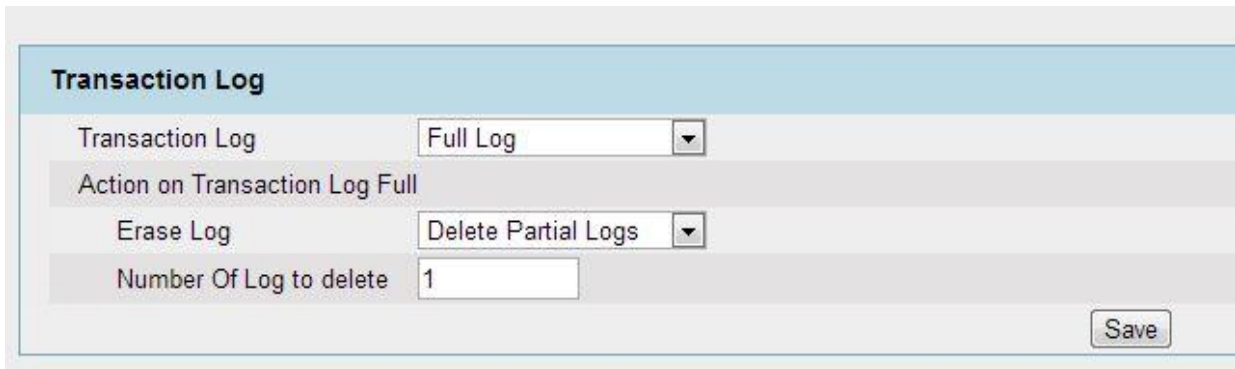
By default, 100,000 transaction logs can be stored in the terminal. An administrator can see more information about Logs storage capacity under “Database Size” section.

All events are recorded in a local file of the terminal. An administrator can export the transactions logs on a USB Mass Storage device connected to the terminal. Refer to “How to Export & View Transaction Logs” under USB Menu Section for more information on how to export transaction logs.

Access Path

Transaction Log

Screens & Steps



| Transaction Log | |
|-------------------------------------|---------------------|
| Transaction Log | Full Log |
| Action on Transaction Log Full | |
| Erase Log | Delete Partial Logs |
| Number Of Log to delete | 1 |
| <input type="button" value="Save"/> | |

Figure 298: Settings for Transaction Log

Using this functionality an administrator can select one of the modes listed below:

1. **No Log:** An administrator can set Transaction Logging to ‘No Log’ mode. This indicates that no actions will be recorded and stored on terminal.
2. **Access Control Log:** This mode indicates that only user access request whatever is the result (pass and fail) should be recorded and stored.
3. **Full Log:** This mode indicates all the action performed by the terminal including configurations done, login and logout attempts, user verification, etc. Entire Log is captured and stored in terminal.
4. An administrator can set Delete Log actions, under **Action on Transaction Log Full**. Whenever the delete action is taken, below settings are applied
5. Select **Erase Log Status** as:

- a. **Delete Partial Logs**, if specific number of logs to be deleted on delete log action triggered. If delete partial logs selected, then enter Number of Log to Delete
 - b. **Delete All Logs**, if all logs stored in database should be deleted on delete log action triggered
6. Click on **Save**

Results

Based on the configuration, terminal will capture transaction logs. When transaction logs storage in terminal database is full, the delete action is performed automatically by terminal based on the Erase Log status.

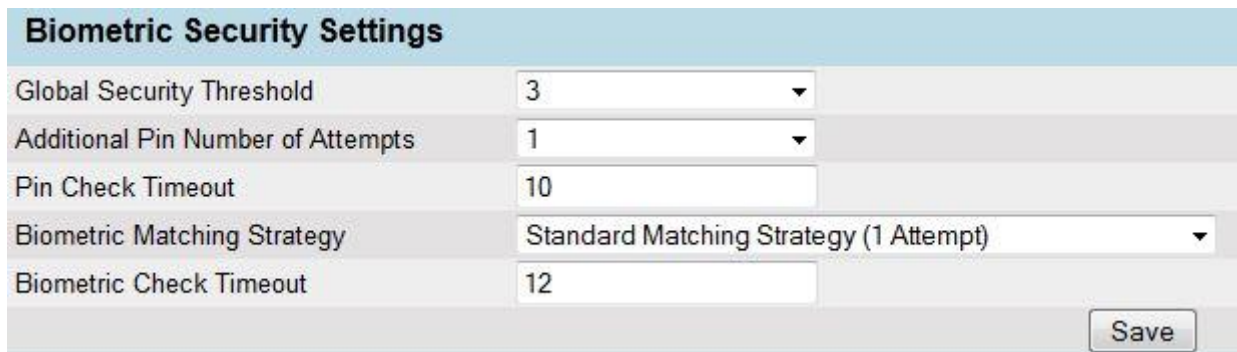
Biometric Security Settings

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

Access Path

Biometric

Screens & Steps



| Biometric Security Settings | |
|-----------------------------------|--|
| Global Security Threshold | 3 |
| Additional Pin Number of Attempts | 1 |
| Pin Check Timeout | 10 |
| Biometric Matching Strategy | Standard Matching Strategy (1 Attempt) |
| Biometric Check Timeout | 12 |

Save

Figure 299: Biometric Security Setting through Webserver

1. Select the **Global Security Threshold Level** for matching biometric data. This parameter allows controlling the false rejection rate and false acceptance rates. An administrator can set threshold level between level 0 to level 10. Refer to "[Setting-up Matching Security Threshold](#)" for False Acceptance Ratio at each level.
2. Select **Addition Pin Number of Attempt**. This allows user to again enter the PIN, if not authenticated at first attempt
3. Enter **PIN check Timeout**, the duration within which user have to re-enter the PIN code
4. **Biometric Matching Strategy** can be selected with multiple options. Please refer [Number of Biometric Check Attempt](#) section for more details
5. Enter **Biometric check Timeout**, the duration within which user have to again place finger on biometric sensor
6. Click on **Save** to save settings

Communication Settings

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

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

Access Path

Communication

Pre-requisites

- For Wi-Fi™ Network connection:
- Wi-Fi™ USB dongle should be plugged
- MA_WI-FI license should be installed on terminal

Screens & Steps

Communication Settings

Serial Configuration

| | | | | | |
|----------------------|-------------|-------------|---|---------------------|--------|
| Communication System | Full Duplex | Net ID | 0 | Baud Rate | 115200 |
| Parity | None | Stop Bit(s) | 1 | Character/Data Size | 8 |

IPv4 Network

| | |
|--|--|
| <p>Ethernet</p> <p><input checked="" type="checkbox"/> DHCP</p> <p>IP Address: 10.99.10.157</p> <p>Subnet Mask: 255.255.252.0</p> <p>Gateway: 10.99.9.1</p> | <p>WLAN</p> <p><input checked="" type="checkbox"/> DHCP</p> <p>IP Address: 10.99.11.121</p> <p>Subnet Mask: 255.255.252.0</p> <p>Gateway: 0.0.0.0</p> |
|--|--|

IPv6 Network

| | |
|---|---|
| <p>Ethernet</p> <p><input type="checkbox"/> DHCP</p> <p>IP Address: fe80::894c:bd17:c081:125</p> <p>Prefix Length: 64</p> <p>Gateway: fe80::d267:e5ff:fe25:300</p> | <p>WLAN</p> <p><input type="checkbox"/> DHCP</p> <p>IP Address: fe80::894c:bd17:c081:432</p> <p>Prefix Length: 12</p> <p>Gateway: fe80::d267:e5ff:fe25:300</p> |
|---|---|

Ethernet Security

IPv4 Authorization

| | |
|---|--|
| <p>Authorized IP List</p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>IP Address: <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Remove"/></p> | <p>Authorized IP Range List</p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>Start IP Address: <input type="text"/> - End IP Address: <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Remove"/></p> |
|---|--|

IPv6 Authorization

| | |
|---|--|
| <p>Authorized IP List</p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>IP Address: <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Remove"/></p> | <p>Authorized IP Range List</p> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <p>Start IP Address: <input type="text"/> - End IP Address: <input type="text"/> <input type="button" value="Add"/> <input type="button" value="Remove"/></p> |
|---|--|

Wi-Fi networks

| | |
|--|--|
| <p>Available Wi-Fi networks</p> <p><input type="button" value="Scan"/> <input type="button" value="Connect"/></p> | <p>Current Wi-Fi network connection (if any)</p> <p>SSID: MASIGMA</p> <p>BSSID: 00:18:f8:f8:f5:2b</p> <p>Network Type: Managed</p> <p>Encryption Type: WPA</p> <hr/> <p>Connect to a specific Wi-Fi network</p> <p>SSID: <input type="text"/></p> <p>Network Type: Managed</p> <p>Encryption Type: <input type="text" value="None"/></p> <p><input type="button" value="Connect"/></p> |
|--|--|

Figure 300: Network parameters settings through Webserver

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

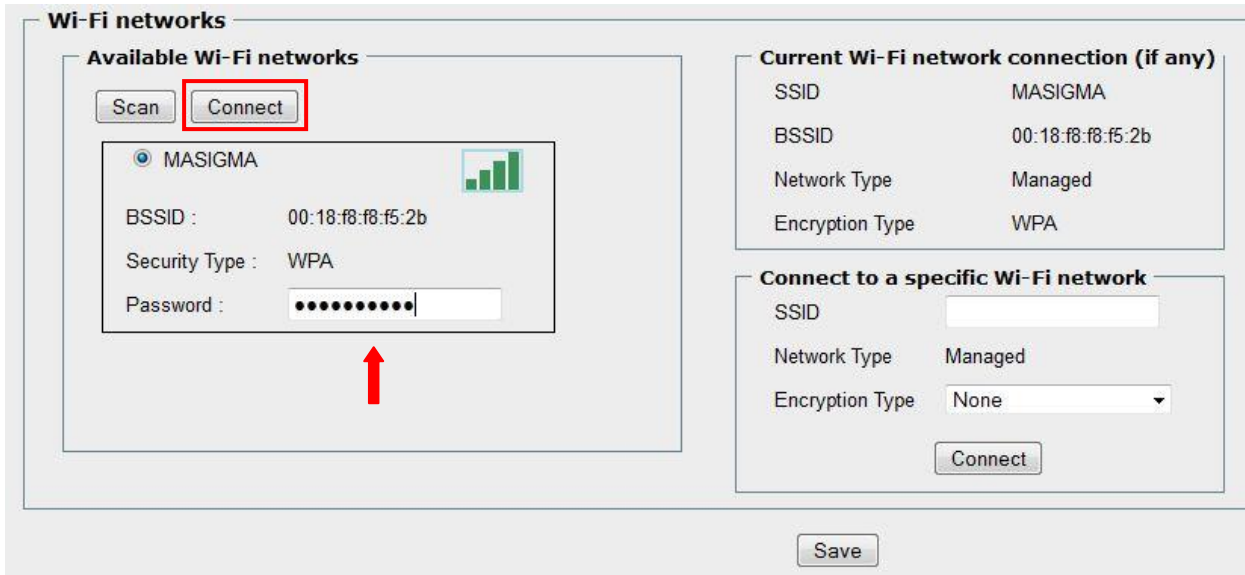


Figure 301: Configuring Wi-Fi™ Network

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

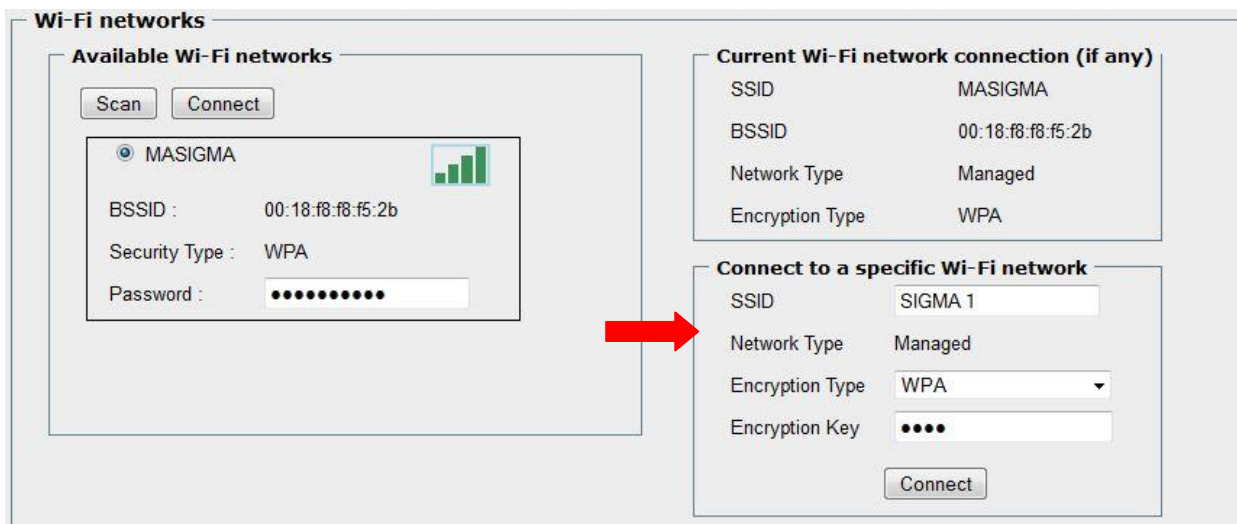


Figure 302: Configuring Wi-Fi™ Network manually

6. Use **Connect to a specific Wi-Fi™ Network** to manually set up a hidden Wi-Fi™ network
 - a. Enter **SSID**
 - b. **Network Type** is displayed as Managed or Ad hoc,

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

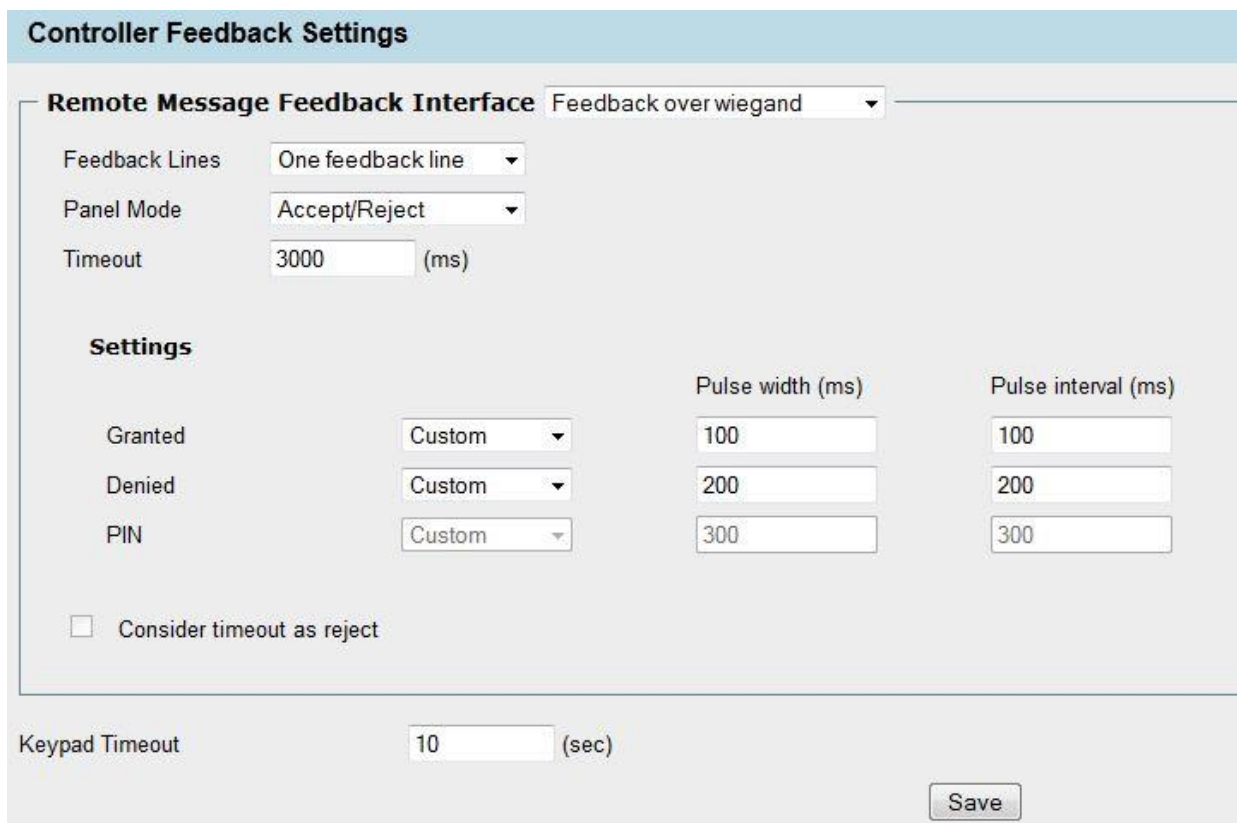
Controller Feedback

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

Access Path

Controller Feedback

Screens & Steps



Controller Feedback Settings

Remote Message Feedback Interface Feedback over wiegand

Feedback Lines: One feedback line

Panel Mode: Accept/Reject

Timeout: 3000 (ms)

Settings

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

Consider timeout as reject

Keypad Timeout: 10 (sec)

Save

Figure 303: Controller Feedback Settings

1. Select Remote Message Feedback Interface as:
 - a. **Disable:** If an administrator do not require to expect Controller Feedback, then an administrator can set interface as Disabled
 - b. **Feedback over IP:** Select Feedback over IP, if controller feedback is to be received on IP channel
 - c. **Feedback over Serial:** Select Feedback over Serial, if controller feedback is to be received on Serial channel
 - d. **Feedback over Wiegand:** Select Feedback over Wiegand, if controller feedback is to be received on Wiegand String. Only if Wiegand channel is used, you need to configure below parameters:

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 consist Accepted (Access Granted), Rejected (Access Denied) and PIN (Asks user to enter PIN). This mode is not applicable if Two Feedback Line is selected in previous step
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** – 100 pulse width and interval
 - ii. For **Access Denied** – 200 pulse width and interval
 - iii. For **PIN** – 300 pulse width and interval
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**

Date and Time Settings

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

Access Path

Date and Time

Screens & Steps

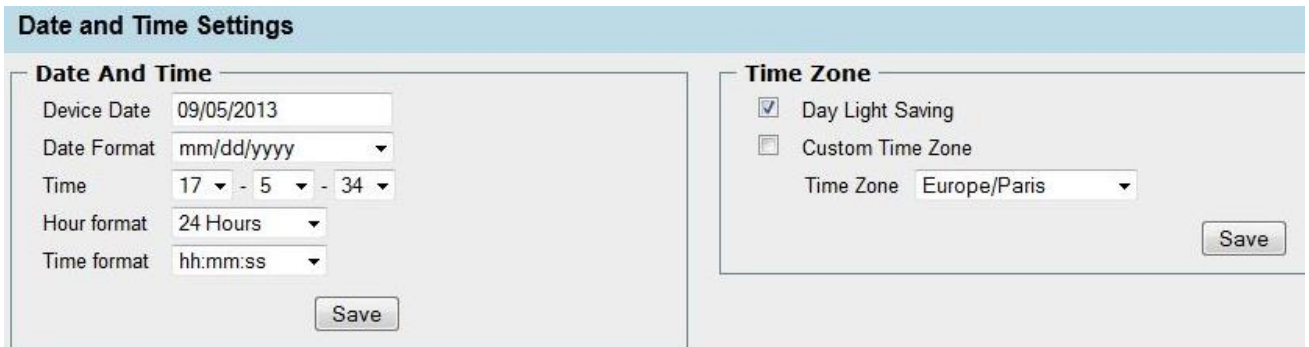
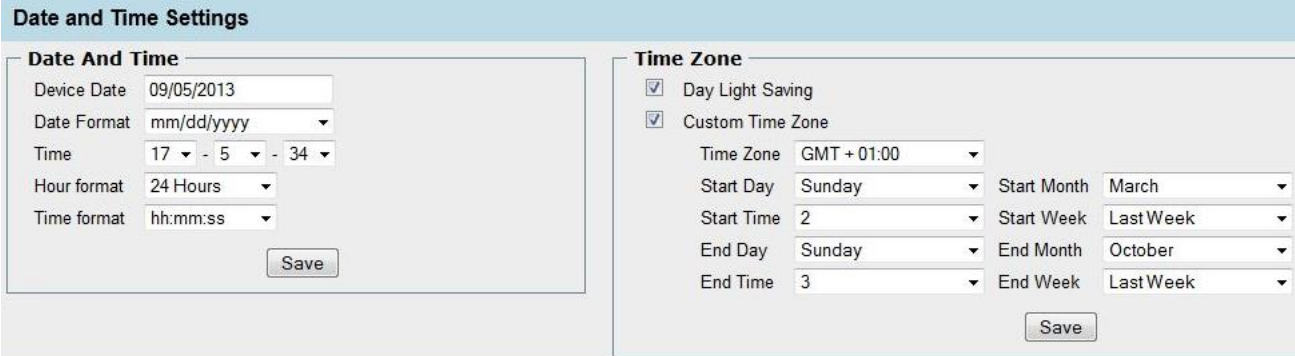


Figure 304: Configuring Date and Time of Terminal from Webserver

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



Date and Time Settings

Date And Time

Device Date: 09/05/2013
Date Format: mm/dd/yyyy
Time: 17 - 5 - 34
Hour format: 24 Hours
Time format: hh:mm:ss
Save

Time Zone

Day Light Saving
 Custom Time Zone
Time Zone: GMT + 01:00
Start Day: Sunday
Start Month: March
Start Time: 2
Start Week: Last Week
End Day: Sunday
End Month: October
End Time: 3
End Week: Last Week
Save

Figure 305: Setting Custom Time Zone from Webserver

a. Select **Time Zone**

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

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

- i. Select Start Day, Start Month, Start Week and Start Time
- ii. Select End Day, End Month, End Week and End Time

9. Click on **Save**

Results

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

Wiegand Parameters Settings

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

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

| Format | Type | Alt Site Code and Fail 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 | Standard | 0 - 4095 | 1 - 1048575 | N/A |
| HID 37-bit | Standard | 0 - 2047 | 1 - 16777215 | N/A |

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/Clock & Data.

Access Path

Wiegand

Pre-requisites

- MA_PAC license should be uploaded on terminal
- Terminal has factory default settings

Screens & Steps

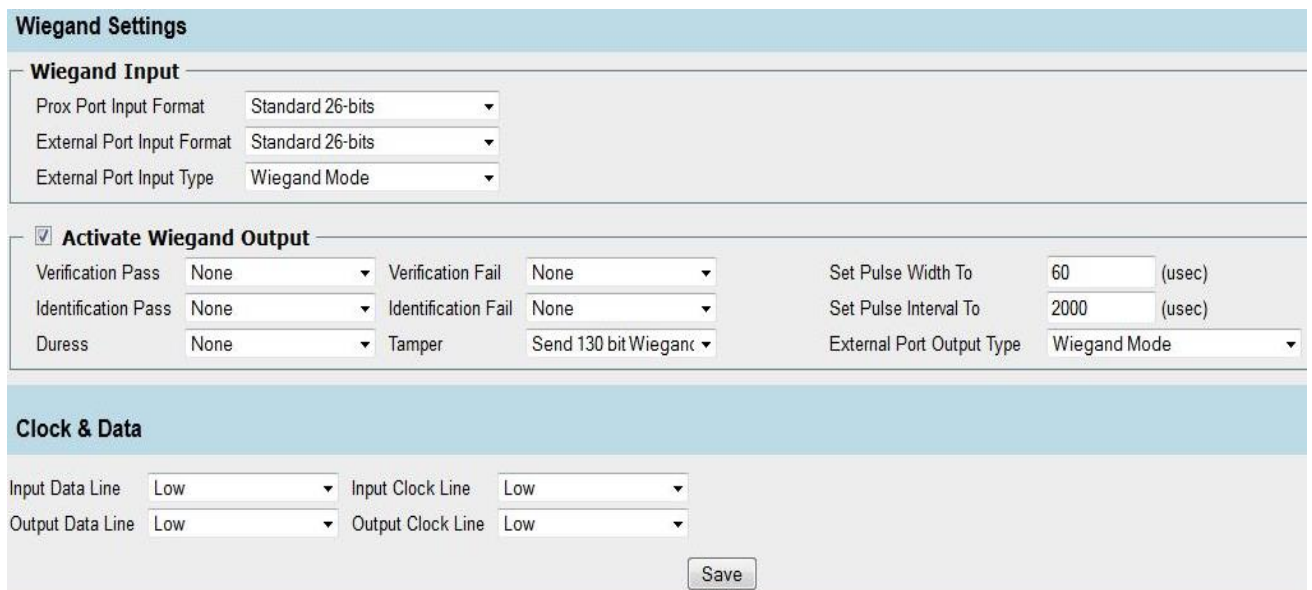


Figure 306: Wiegand Settings through Webserver

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

2. **Activate Wiegand Output:** This parameter is enabled to allow the Wiegand 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, playing alarm, alerting security personnel, etc.
 - f. Select **Tamper** detection format as 'None' or 'Send 130 bit Wiegand string with terminal serial number'. It is a pre-requisite to enable Tamper settings in the terminal. When tamper event is detected, terminal will send terminal serial number in a Wiegand string format to access controller, for alerting controller about the Tamper detection.
 - g. Select **External Port Output Type** as 'Wiegand Mode' or 'Clock & Data mode'. If you select Clock & Data mode, then respective format will be used for sending data over Wiegand port.
 - h. **Set Pulse Width To** in terms of microseconds
 - i. **Set Pulse Interval To** in terms of microseconds
3. If External Port Input Type and Output Type is selected as Clock & Data, then configure Clock & Data parameters:
 - a. Select **Input Data Line** as Low or High
 - b. Select **Output Data Line** as Low or High
 - c. Select **Input Clock Line** as Low or High
 - d. Select **Output Clock Line** as Low or High
4. Click on **Save**

User Control Configurations

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

Access Path

User Control Configurations

Screens & Steps

| Property | Threat Level 1 | Threat Level 2 | Threat Level 3 |
|--------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Finger biometric trigger | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Contactless card trigger | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Keyboard trigger | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| External port trigger | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| Allow record fallback | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Allow VIP authentication bypass | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Finger Biometric authentication rule | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Pin authentication rule | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Check User ID whitelist | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Enable external database | <input type="checkbox"/> | | |
| Check access schedule | <input type="checkbox"/> | | |
| Check holiday schedule | <input type="checkbox"/> | | |
| Check stolen card list | <input type="checkbox"/> | | |
| Check expiry date | <input type="checkbox"/> | | |
| Check additional users | 0 | 0 | 0 |
| Allow duress finger | Disabled | Disabled | Disabled |
| User record reference | Trigger event | Trigger event | Trigger event |
| Per user rules | Disabled | Disabled | Disabled |
| Allow Bio-pin user rule | Disabled | Disabled | Disabled |
| Face authentication rule | Disabled | Disabled | Disabled |

Figure 307: User Control Configurations from Webserver

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

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

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

2. **Contactless Card Trigger:** If this parameter is enabled, terminal starts access rights check, using authentication process, when a user card is detected by embedded contactless card reader. This parameter can be enabled or disabled for terminals having internal Smartcard reader and internal Prox card reader.

3. **Keyboard Trigger:** This parameter can be enabled to start access rights check, using authentication process, when a data is entered with 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. **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, then if this parameter is enabled, terminal will use biometric data corresponding to the user stored in the terminal database to perform BIO check.
6. **Allow VIP Authentication Bypass:** If this parameter is enabled then users in the VIP list are exempted from authentication checks (finger bio, 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. 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"*

7. **Finger Biometric Authentication Rule:** This parameter indicates whether terminal should check biometric of the user as a part of user control workflow.
8. **Pin Authentication Rule:** This parameter indicates whether terminal should check PIN of the user as a part of user control workflow.
9. **Check User ID authorized list:** This parameter controls authorized list check during user control workflow. If enabled, the terminal will check whether user is authorized listed or not
10. **Enable external database:** if enabled, the terminal polling mode will be activated, and check the user's data with the data stored in external database. Refer "Polling Mode" for understanding polling mode.
11. **Check access schedule:** indicates whether terminal should check the access schedule before granting access to the user
12. **Check holiday schedule:** indicates whether terminal should check the holiday schedule before granting access to the user
13. **Check banned card list:** If this parameter is enabled, terminal searches for users card in banned card list before starting user's authentication. User's presented smartcard serial number is checked against the list of banned card stored on terminal.
14. **Check expiry date:** If this parameter is enabled terminal will check the expiry date of user account.

15. **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 (additional one more user required). If a single user is successfully identified multiple times, the duplicates are ignored and the terminal again prompts for the additional user, until the workflow times out. If one of the users fails the workflow is interrupted.
16. **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 alarm" event is raised before the eventual user acceptance or rejection.
17. **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.
18. **Per user rules:** Defines additional rules reference (i.e. rules to add to terminal defined rules). Possible values are “Disabled”, “Trigger Event” and “Terminal”.
 - a. If set to “Disabled”, then only terminal configuration defined controls are performed,
 - b. If set to “Trigger Event”, then user rules are retrieved based on user control trigger source i.e. user rule retrieved from smartcard for smartcard triggered user control operation and user rule retrieved from terminal database for other trigger source.
 - c. If set to “Terminal”, then user rule is retrieved from terminal database for all trigger source.

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

19. **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

20. Face authentication rule: This parameter defines face authentication check workflow rule. Possible values are “Disabled”, “Photo taking”, “Face detection (optional)” and “Face detection (mandatory)”. Refer below table for face authentication workflow for normal user and VIP user:

| face_auth_rule | Behavior | Behavior for VIP user |
|--------------------------|---|----------------------------------|
| Disabled | Do not take pictures | As per ‘disabled’ |
| photo_taking | Take one picture and save it according to logging policies | 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • Perform face detection till timeout if no face is detected (even if user control workflow gets completed) | As per ‘face_detection_optional’ |

21. 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.

Threat Level Configuration

This feature allows an administrator to set threat levels using the TTL input lines. When enabled, the TTL signals can define the level of security and also can be used to compel users to use a specific authentication method. The available choices are Card Only and Card + Biometrics. For example, if Threat level 1 is set to Card + Biometrics and the TTL input for GPI 0 is triggered, a successful verification requires presenting a smart card and a finger to the terminal.

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

Access Path

Threat Level

Screens & Steps

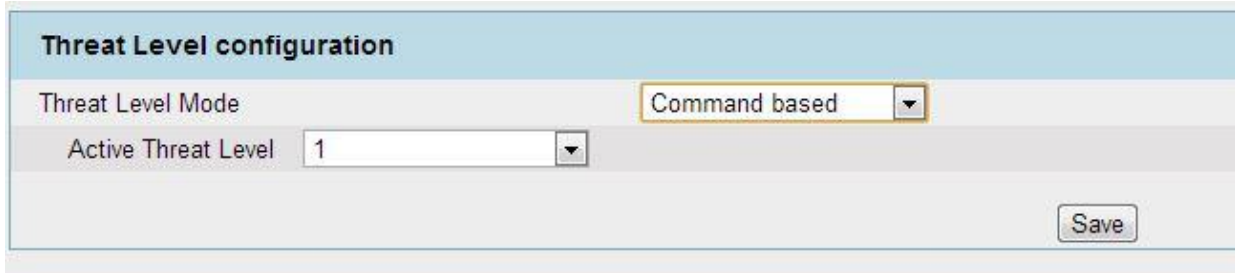


| Threat Level configuration | | | |
|-------------------------------------|-------|-----------|--------------|
| Threat Level Mode | | TTL based | |
| GPI to Threat level mapping | | | |
| Current State | GPI 1 | GPI 0 | Threat Level |
| | 0 | 0 | 0 |
| | 0 | 1 | 1 |
| | 1 | 0 | 2 |
| <input checked="" type="checkbox"/> | 1 | 1 | 3 |

Save

Figure 308: Configuring TTL Based Threat Level, using Webserver interface

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**



Threat Level configuration

Threat Level Mode

Active Threat Level

Figure 309: Configuring Command Based Threat Level, using Webserver interface

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

Event Configurations

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

Access Path

Events Configurations

Screens & Steps

| Event Settings | | | | | | |
|--------------------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------|
| Event Name | Enable | Send To Controller | GPO0 | GPO1 | GPO2 | DataClock ID |
| Duress Finger Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 65535 |
| Fake Finger Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 65535 |
| User Control Successful Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| Biometric Mismatch Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 65535 |
| Pin Mismatch Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 65535 |
| User ID Not In DB Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 65535 |
| Control Timeout Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 65535 |
| Rejected By schedule Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | 65535 |
| User Temporal Validity Expired Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | 65535 |
| User Not In Authorized List Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 65535 |
| Card In Banned List Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 65535 |
| Face not Detected Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | 65535 |
| Multi-User Intermediate ID Event | <input checked="" type="checkbox"/> | | | | | |
| Transaction Log File Full Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | |
| Controller Feedback Event | <input checked="" type="checkbox"/> | | | | | |
| Job Code Check Failure Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | 65535 |
| Door Opened For Too Long Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | |
| Forced Door Open Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | |
| Door closed After Alarm Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | |
| Door Unlocked Event | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | |

Figure 310: 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

Define Access Schedule

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

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

Maximum 64 access schedules can be created, where by

- By default, Schedule no. 0 is defined as access denied whatever the time of access request
- By default, Schedule no. 63 is defined as none access denied time slot. On user enrolment, Access Schedule 63 is assigned by default.
- Schedule no. 59 to Schedule no. 62 is reserved for internal use. Please don't assign one of these schedules to any user.

On user enrolment, administrator can select the required access schedule and associate with user account. E.g. Access Schedule create has access right in time slot from 10:00 am to 20:00 pm, with interval from 13:00 pm to 14:00 pm. User is granted access only between 10:00 to 13:00 and from 14:00 to 20:00.

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

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

Access Path

Access Schedule

Screens & Steps

Adding a New Access Schedule

Access Schedules

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

No Access

All Access

| Index | Name | | Time slots | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------|--|---|--|------------|-----|---|---|--|-----|---|---|------------|-----|---|---|--|-----|---|---|------------|-----|---|---|--|-----|---|---|------------|-----|---|---|--|-----|---|---|------------|-----|---|---|--|-----|---|---|------------|-----|---|---|--|-----|---|---|
| 0 | <input type="text" value="No Access"/> | | <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="text-align: center; vertical-align: middle;">Sun</td> <td># 1</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td></td> <td># 2</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">Mon</td> <td># 1</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td></td> <td># 2</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">Tue</td> <td># 1</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td></td> <td># 2</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">Wed</td> <td># 1</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td></td> <td># 2</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">Thu</td> <td># 1</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td></td> <td># 2</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td style="text-align: center; vertical-align: middle;">Fri</td> <td># 1</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> <tr> <td></td> <td># 2</td> <td>Start Time: <input type="text" value="N.A."/></td> <td>End Time: <input type="text" value="N.A."/></td> </tr> </table> | Sun | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | Mon | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | Tue | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | Wed | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | Thu | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | Fri | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> |
| Sun | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mon | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tue | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Wed | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Thu | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Fri | # 1 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | Start Time: <input type="text" value="N.A."/> | End Time: <input type="text" value="N.A."/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figure 311: Adding Access Schedule

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

| Access Schedules | | |
|------------------|--|--|
| Index | Name | Time slots |
| 1 | <input type="text" value="Schedule_1"/> | |
| | <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |
| | Sun | # 1 Start Time: <input type="text" value="N.A."/> End Time: <input type="text" value="N.A."/> # 2 Start Time: <input type="text" value="N.A."/> End Time: <input type="text" value="N.A."/> |
| | Mon | # 1 Start Time: <input type="text" value="08:00"/> End Time: <input type="text" value="14:00"/> # 2 Start Time: <input type="text" value="15:00"/> End Time: <input type="text" value="20:00"/> |
| | Tue | # 1 Start Time: <input type="text" value="08:00"/> End Time: <input type="text" value="14:00"/> # 2 Start Time: <input type="text" value="15:00"/> End Time: <input type="text" value="20:00"/> |
| | Wed | # 1 Start Time: <input type="text" value="08:00"/> End Time: <input type="text" value="14:00"/> # 2 Start Time: <input type="text" value="15:00"/> End Time: <input type="text" value="20:00"/> |
| | Thu | # 1 Start Time: <input type="text" value="08:00"/> End Time: <input type="text" value="14:00"/> # 2 Start Time: <input type="text" value="15:00"/> End Time: <input type="text" value="20:00"/> |
| | Fri | # 1 Start Time: <input type="text" value="08:00"/> End Time: <input type="text" value="14:00"/> # 2 Start Time: <input type="text" value="15:00"/> End Time: <input type="text" value="20:00"/> |
| | Sat | # 1 Start Time: <input type="text" value="N.A."/> End Time: <input type="text" value="N.A."/> # 2 Start Time: <input type="text" value="N.A."/> End Time: <input type="text" value="N.A."/> |

Figure 312: Adding Access Schedule

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

NOTE:

- *In MA5G mode, two time slots per day can be defined with one interval in between*
- *If terminal is in L1 Legacy mode, then Access Schedule can be configured from Secure Admin. Where an administrator can also define “Schedule Tolerance” duration that allows user access early/late than the scheduled access time.*
- *Moreover, in L1 Legacy mode, an administrator can set two intervals in a day.*
- *If terminal is in Legacy Morpho mode, then access schedule can be configured, using Time Mask feature in MorphoBioToolBox (MTTB) application.*

5. Click on **Apply**

Results

An Access Schedule is created and it is available for assignment to users at the time of user enrolment. User is allowed to access only during the access time scheduled. If user tries to access at another time, then MorphoAccess® SIGMA Series terminal will show message “User not scheduled” after authentication/identification.

Editing Access Schedule

Access Schedules

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

- No Access
- Schedule_1**
- All Access

| Index | Name | Time slots | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------|---|--|----------|------|------------|----------|-----|-----|------|------|-----|------|------|-----|-----|-------|-------|-----|-------|-------|-----|-----|-------|-------|-----|-------|-------|-----|-----|-------|-------|-----|-------|-------|-----|-----|-------|-------|-----|-------|-------|
| 1 | <input type="text" value="Schedule_1"/> | <table border="1"><thead><tr><th>Day</th><th>Slot</th><th>Start Time</th><th>End Time</th></tr></thead><tbody><tr><td rowspan="2">Sun</td><td># 1</td><td>N.A.</td><td>N.A.</td></tr><tr><td># 2</td><td>N.A.</td><td>N.A.</td></tr><tr><td rowspan="2">Mon</td><td># 1</td><td>08:00</td><td>14:00</td></tr><tr><td># 2</td><td>15:00</td><td>20:00</td></tr><tr><td rowspan="2">Tue</td><td># 1</td><td>08:00</td><td>14:00</td></tr><tr><td># 2</td><td>15:00</td><td>20:00</td></tr><tr><td rowspan="2">Wed</td><td># 1</td><td>08:00</td><td>14:00</td></tr><tr><td># 2</td><td>15:00</td><td>20:00</td></tr><tr><td rowspan="2">Thu</td><td># 1</td><td>08:00</td><td>14:00</td></tr><tr><td># 2</td><td>15:00</td><td>20:00</td></tr></tbody></table> | Day | Slot | Start Time | End Time | Sun | # 1 | N.A. | N.A. | # 2 | N.A. | N.A. | Mon | # 1 | 08:00 | 14:00 | # 2 | 15:00 | 20:00 | Tue | # 1 | 08:00 | 14:00 | # 2 | 15:00 | 20:00 | Wed | # 1 | 08:00 | 14:00 | # 2 | 15:00 | 20:00 | Thu | # 1 | 08:00 | 14:00 | # 2 | 15:00 | 20:00 |
| Day | Slot | Start Time | End Time | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Sun | # 1 | N.A. | N.A. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | N.A. | N.A. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Mon | # 1 | 08:00 | 14:00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | 15:00 | 20:00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Tue | # 1 | 08:00 | 14:00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | 15:00 | 20:00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Wed | # 1 | 08:00 | 14:00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | 15:00 | 20:00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Thu | # 1 | 08:00 | 14:00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | # 2 | 15:00 | 20:00 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figure 313: Editing Access Schedule

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

NOTE: The default access schedules cannot be modified.

| Index | Name | Time slots | |
|-------|--|---------------------------------------|---------------------------------------|
| 1 | Schedule_1 | | |
| | <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | |
| | Sun | # 1 Start Time: 00:00 End Time: 24:00 | # 2 Start Time: N.A. End Time: N.A. |
| | Mon | # 1 Start Time: 08:00 End Time: 14:00 | # 2 Start Time: 15:00 End Time: 20:00 |
| | Tue | # 1 Start Time: 08:00 End Time: 14:00 | # 2 Start Time: 15:00 End Time: 20:00 |
| | Wed | # 1 Start Time: 08:00 End Time: 14:00 | # 2 Start Time: 15:00 End Time: 20:00 |
| | Thu | # 1 Start Time: 08:00 End Time: 14:00 | # 2 Start Time: 15:00 End Time: 20:00 |
| | Fri | # 1 Start Time: 08:00 End Time: 14:00 | # 2 Start Time: 15:00 End Time: 20:00 |
| | Sat | # 1 Start Time: N.A. End Time: N.A. | # 2 Start Time: N.A. End Time: N.A. |

Figure 314: Editing Access Schedule

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

Delete Access Schedule

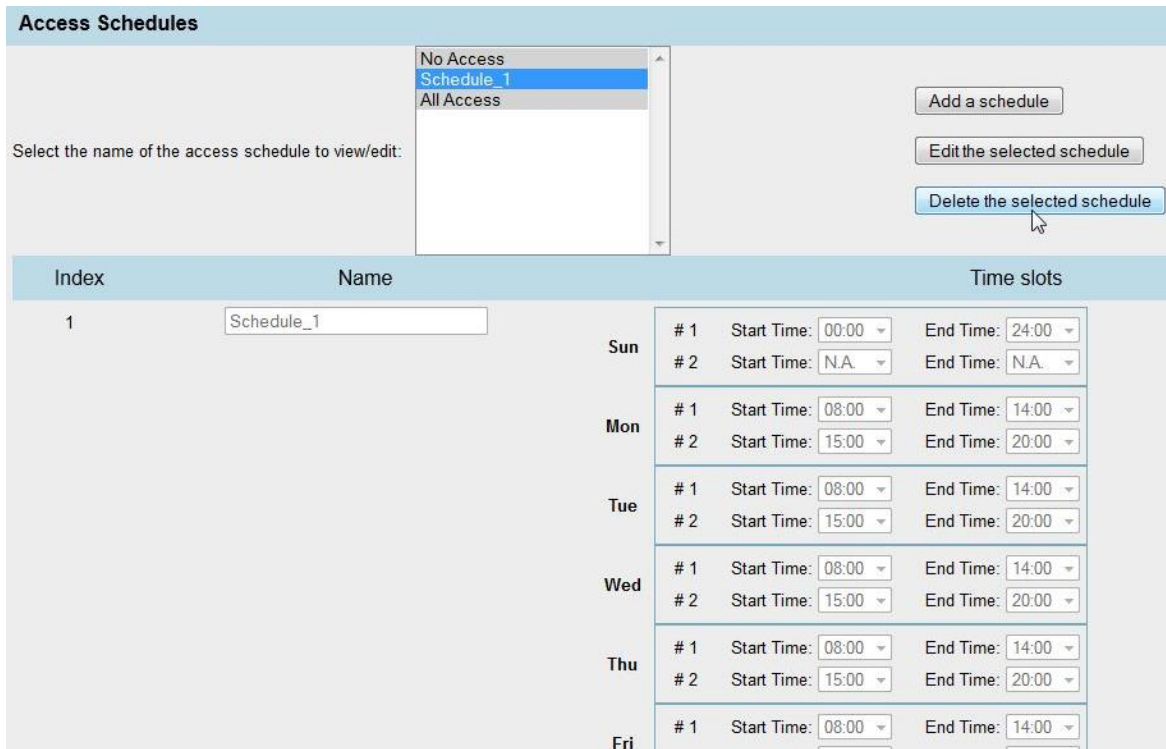


Figure 315: Deleting an Access Schedule

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

NOTE: The default access schedules cannot be deleted.

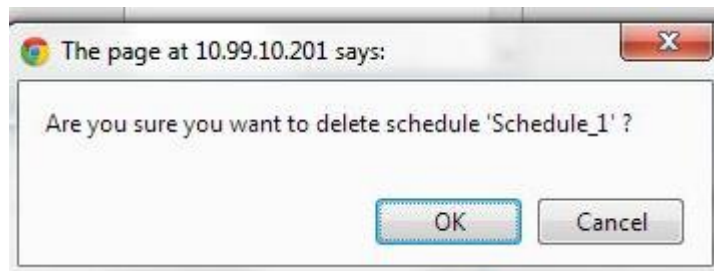


Figure 316: Deleting an Access Schedule

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

Results

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

Define Holiday Schedule

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

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

Access Path

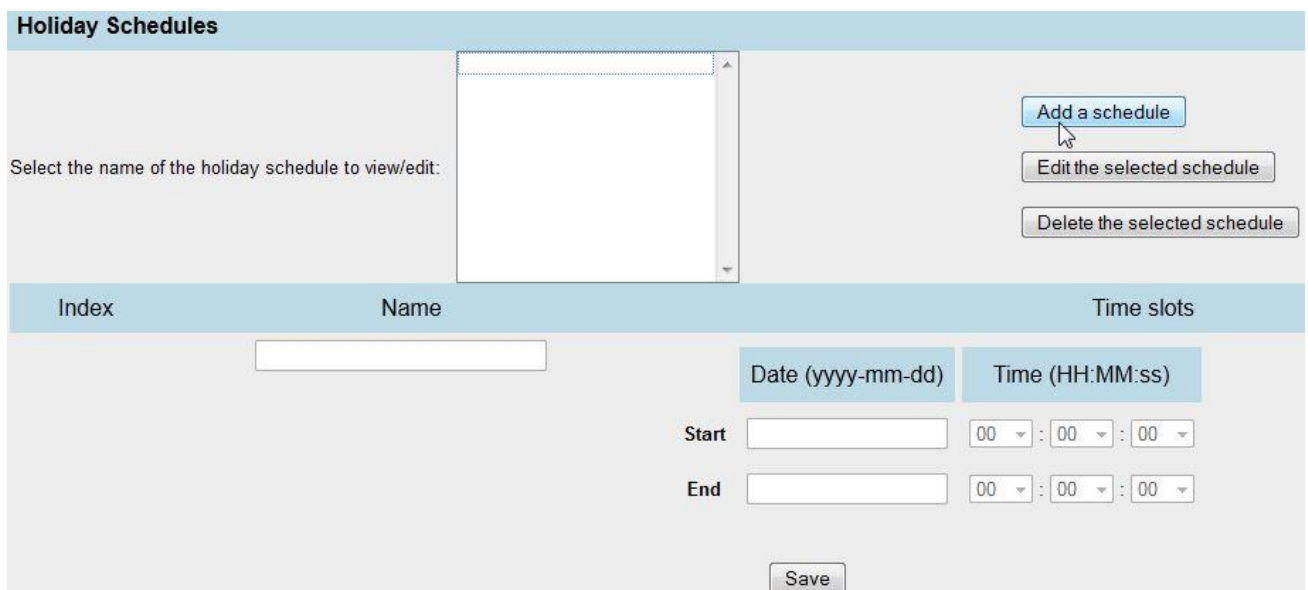
Holiday Schedule

Pre-requisites

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

Screens & Steps

Add a Holiday Schedule



| Index | Name | Time slots | | | | | | |
|----------------------------|----------------------|---|-------------------|-----------------|----------------------------|--------------|--------------------------|--------------|
| | <input type="text"/> | <table border="1"><thead><tr><th>Date (yyyy-mm-dd)</th><th>Time (HH:MM:ss)</th></tr></thead><tbody><tr><td>Start <input type="text"/></td><td>00 : 00 : 00</td></tr><tr><td>End <input type="text"/></td><td>00 : 00 : 00</td></tr></tbody></table> | Date (yyyy-mm-dd) | Time (HH:MM:ss) | Start <input type="text"/> | 00 : 00 : 00 | End <input type="text"/> | 00 : 00 : 00 |
| Date (yyyy-mm-dd) | Time (HH:MM:ss) | | | | | | | |
| Start <input type="text"/> | 00 : 00 : 00 | | | | | | | |
| End <input type="text"/> | 00 : 00 : 00 | | | | | | | |

Save

Figure 317: Creating a Holiday Schedule

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

| Holiday Schedules | | | |
|-------------------|--|---|---|
| Index | Name | Time slots | |
| 0 | <input type="text" value="Schedule_0"/> | Date (yyyy-mm-dd) | Time (HH:MM:ss) |
| | <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | Start <input type="text" value="2013-08-15"/> | <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/> |
| | | End <input type="text" value="2013-08-15"/> | <input type="text" value="23"/> : <input type="text" value="59"/> : <input type="text" value="59"/> |

Figure 318: Creating a Holiday Schedule

1. Enter **Schedule Name**, usually the name of the holiday (such as "independence day")
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.

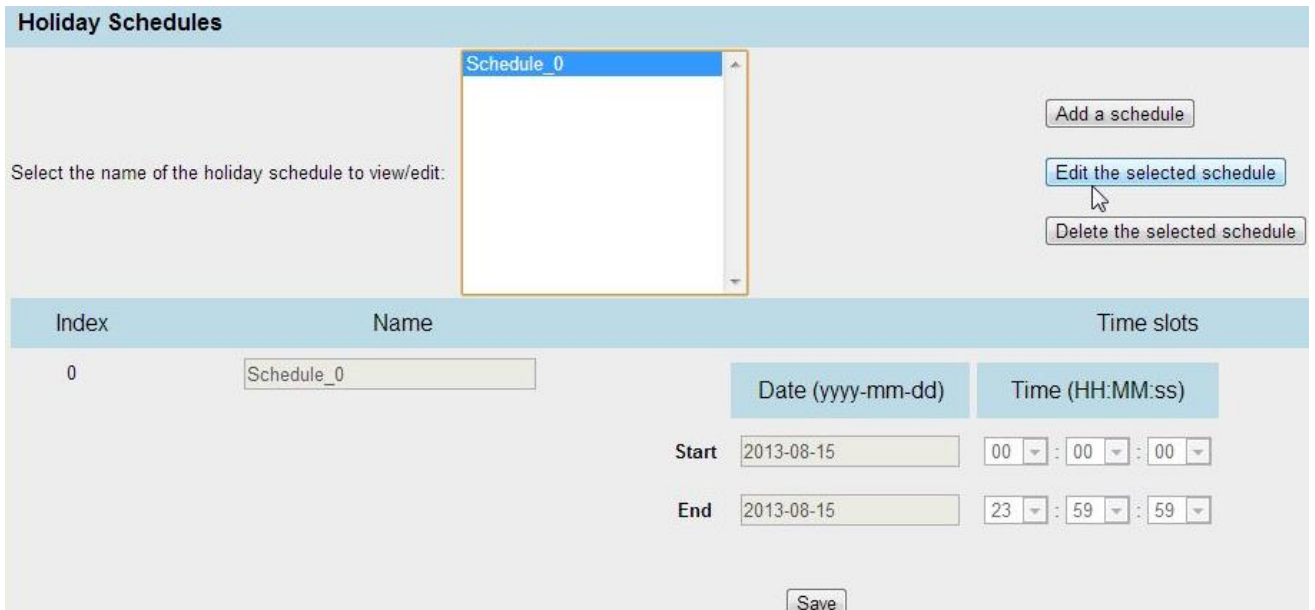
NOTE: If terminal is in L1 Legacy mode, then Holiday schedule is defined using Secure Admin. The Time slot with maximum interval can be set.

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 on defined holiday's user is not allowed to access. Terminal will show message "User not scheduled" after authentication/identification.

Edit Holiday Schedule



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

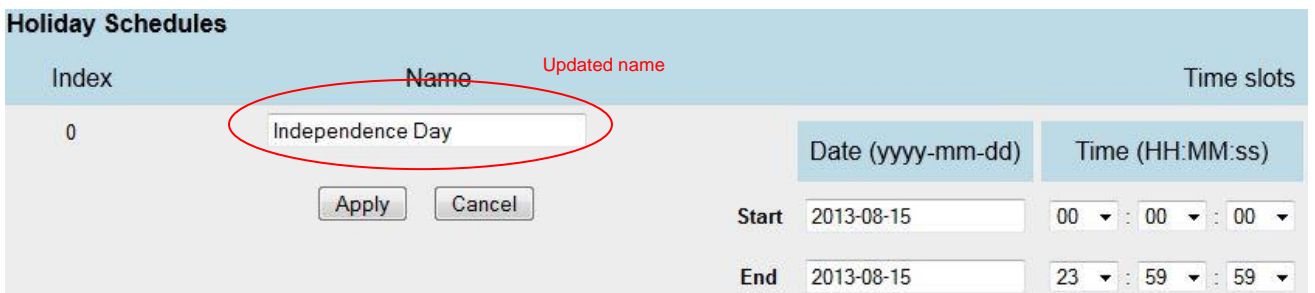
Buttons: Add a schedule, Edit the selected schedule, Delete the selected schedule

| Index | Name | Time slots | |
|-------|------------|-------------------|-------------------------|
| 0 | Schedule_0 | Date (yyyy-mm-dd) | Time (HH:MM:ss) |
| | | Start | 2013-08-15 00 : 00 : 00 |
| | | End | 2013-08-15 23 : 59 : 59 |

Buttons: Save

Figure 319: Editing Holiday Schedule

1. Select a Holiday Schedule that an administrator require to update
2. Click on **Edit the Selected Schedule**



Buttons: Apply, Cancel

| Index | Name | Time slots | |
|-------|------------------|-------------------|-------------------------|
| 0 | Independence Day | Date (yyyy-mm-dd) | Time (HH:MM:ss) |
| | | Start | 2013-08-15 00 : 00 : 00 |
| | | End | 2013-08-15 23 : 59 : 59 |

Figure 320: Editing Holiday Schedule

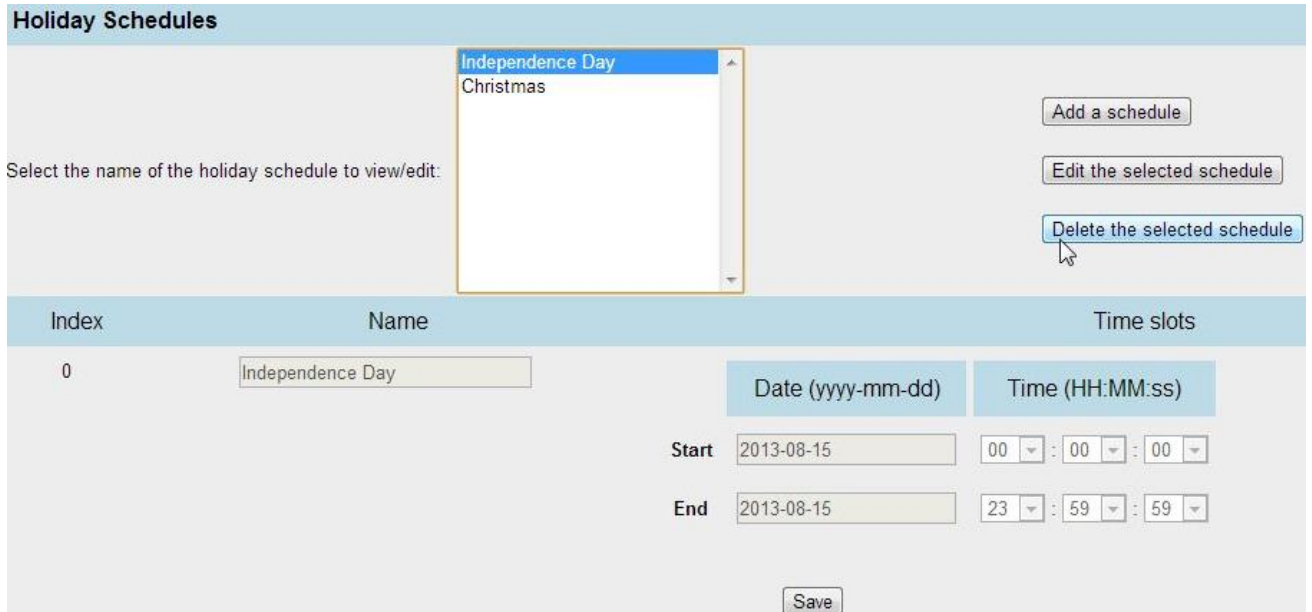
3. Update necessary information in Name of holiday schedule, Date and Time slots
4. Click on **Apply**

Results

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

Delete a Holiday Schedule

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



| Index | Name | Date (yyyymm-dd) | Time (HH:MM:ss) |
|-------|------------------|------------------|-----------------|
| 0 | Independence Day | 2013-08-15 | 00:00:00 |
| | | 2013-08-15 | 23:59:59 |

Figure 321: Deleting a Holiday Schedule

1. Select a name of the Holiday Schedule from the list
2. Click on **Delete the Selected Schedule**



Figure 322: Deleting a Holiday Schedule

3. A confirmation message pop-up, asks to confirm delete action. Click on Ok to delete Holiday Schedule

Results

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

Door Open Schedule Configuration

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

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

Access Path

Door Open Configuration

Pre-requisites

- SDAC must be activated

Screens & Steps

| Door Open Schedules | | | | | | | | | | | | | | | |
|---------------------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|------|
| | Sun | | Mon | | Tue | | Wed | | Thu | | Fri | | Sat | | |
| | S.T. | E.T. | S.T. | E.T. | S.T. | E.T. | S.T. | E.T. | S.T. | E.T. | S.T. | E.T. | S.T. | E.T. | |
| # 1 | 12:30 | 14:30 | 12:30 | 14:30 | 12:30 | 14:30 | 12:30 | 14:30 | 12:30 | 14:30 | 12:30 | 14:30 | 12:30 | 14:30 | # 1 |
| # 2 | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | # 2 |
| # 3 | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | # 3 |
| # 4 | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | # 4 |
| # 5 | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | # 5 |
| # 6 | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | # 6 |
| # 7 | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | # 7 |
| # 8 | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | # 8 |
| # 9 | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | # 9 |
| # 10 | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | N.A. | # 10 |

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

Figure 323: Door Open Schedule Configuration

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

Results

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

Complete Configuration (Advanced users only)

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

Access Path

Complete Configuration

Screens & Steps

| Parameter Key | | Parameter Value |
|--|--------------------------|-----------------|
| LCD_configuration.brightness | <input type="checkbox"/> | 70 |
| LCD_configuration.enable_azerty_kbd | <input type="checkbox"/> | 0 |
| LCD_configuration.idle_screen_status | <input type="checkbox"/> | 1 |
| LCD_configuration.idle_screen_timeout | <input type="checkbox"/> | 60 |
| LCD_configuration.idle_video_timeout | <input type="checkbox"/> | 60 |
| LCD_configuration.low_power_disable_sensor | <input type="checkbox"/> | 1 |
| LCD_configuration.video_play_brightness | <input type="checkbox"/> | 35 |
| NTP_server.primary_ip_address | <input type="checkbox"/> | 198.101.234.139 |
| NTP_server.secondary_ip_address | <input type="checkbox"/> | |
| SSL_profile_0.cipher_list | <input type="checkbox"/> | 511 |
| SSL_profile_0.name | <input type="checkbox"/> | Profile_0 |

Figure 324: Parameter Configuration Screen on Webserver

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

Reference

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

Reset Factory Settings

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

Access Path:

Reset Factory Settings

Screens & Steps

| Reset Factory Settings | |
|--------------------------|--------------------------|
| (Select All) | <input type="checkbox"/> |
| Configuration Parameters | <input type="checkbox"/> |
| Date-Time | <input type="checkbox"/> |
| Ethernet | <input type="checkbox"/> |
| Serial | <input type="checkbox"/> |
| Wi-Fi | <input type="checkbox"/> |
| Video Phone | <input type="checkbox"/> |
| Crypto Keys | <input type="checkbox"/> |
| Passwords | <input type="checkbox"/> |
| SSL Components | <input type="checkbox"/> |
| Banned Card List | <input type="checkbox"/> |
| Authorized List | <input type="checkbox"/> |
| VIP List | <input type="checkbox"/> |
| Job Code Lists | <input type="checkbox"/> |
| Access Schedules | <input type="checkbox"/> |
| Holiday Schedules | <input type="checkbox"/> |
| Door Schedules | <input type="checkbox"/> |
| Authorized IP List | <input type="checkbox"/> |
| Logs | <input type="checkbox"/> |
| Passphrases | <input type="checkbox"/> |
| Languages | <input type="checkbox"/> |
| Multimedia Files | <input type="checkbox"/> |
| User DB | <input type="checkbox"/> |
| Dynamic Message | <input type="checkbox"/> |
| Events | <input type="checkbox"/> |
| Error Log | <input type="checkbox"/> |

Figure 325: Reset Factory Settings Screen on Webserver

1. The list of all the parameters are displayed which can be reset to factory default values through Webserver.

2. To reset any parameter, select the checkbox next to the corresponding parameter name
3. Click on Reset
4. The corresponding parameter values are reset to the factory default settings.

Section 9 : Access Control

Access control presentation

Typical architecture of an access control system

Typical access control system architecture includes:

- One MorphoAccess® terminal per area to protect,
- A user management or administration menu
- A Central Security Controller: for area access final check and physical access command (open the door).

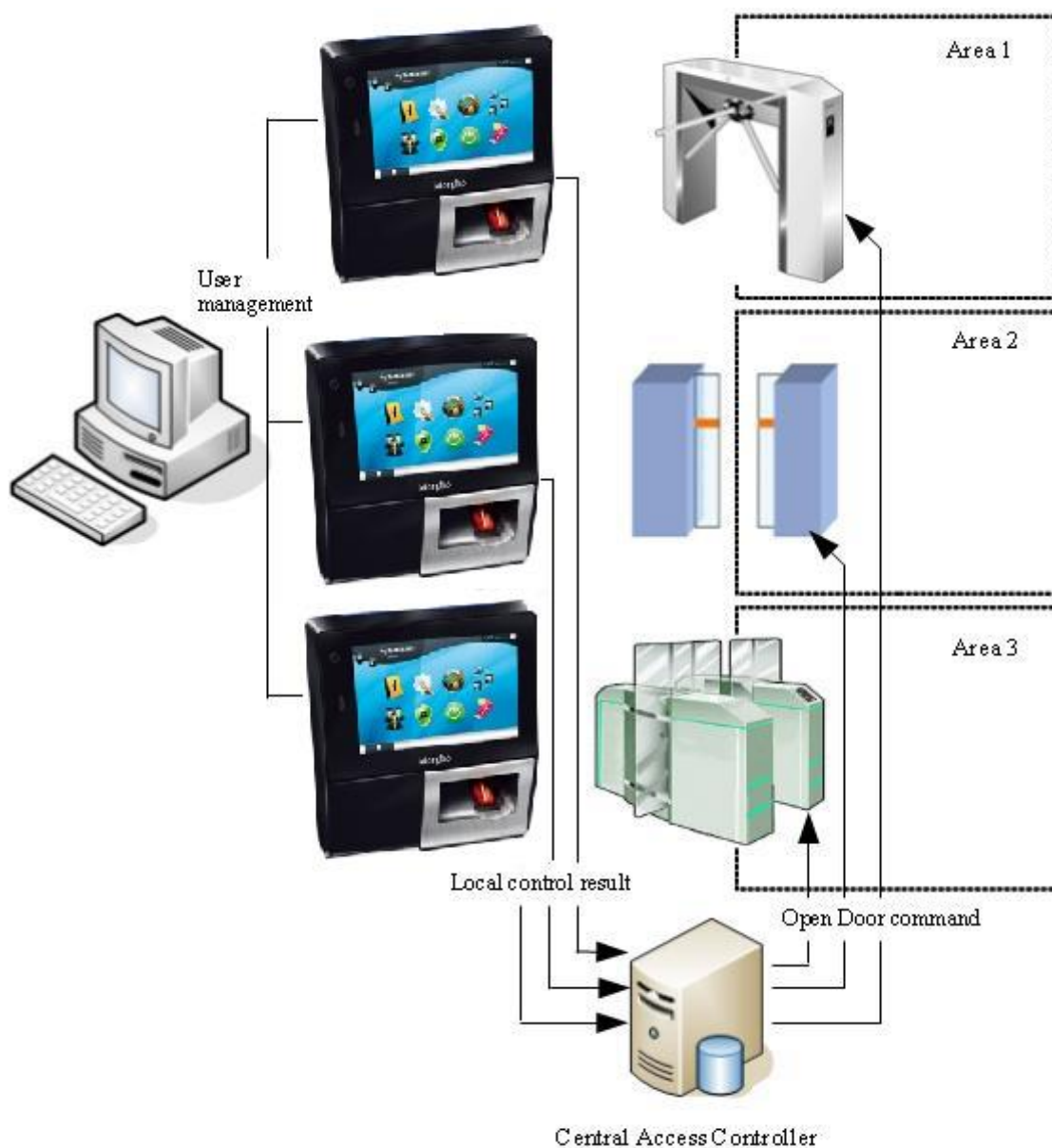


Figure 326: Typical access control system architecture

Typical access control process

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

Preliminary: adding a biometric template in local database

The management of internal biometric database can be done locally (through the User Menu) in MorphoAccess® SIGMA Series terminals.

User enrolment can be done by administrator from User Menu.

The local database can be exported ciphered to other MorphoAccess® SIGMA Series terminals using a USB Mass Storage Device.

Contactless cards containing user templates can be generated from User Menu.

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

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

MorphoAccess® terminal operating modes

Standalone mode or Slave mode

The terminal supports two exclusive operating modes:

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

Standalone mode: Identification and/or Authentication

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

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

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

Access Control Process in Identification Mode

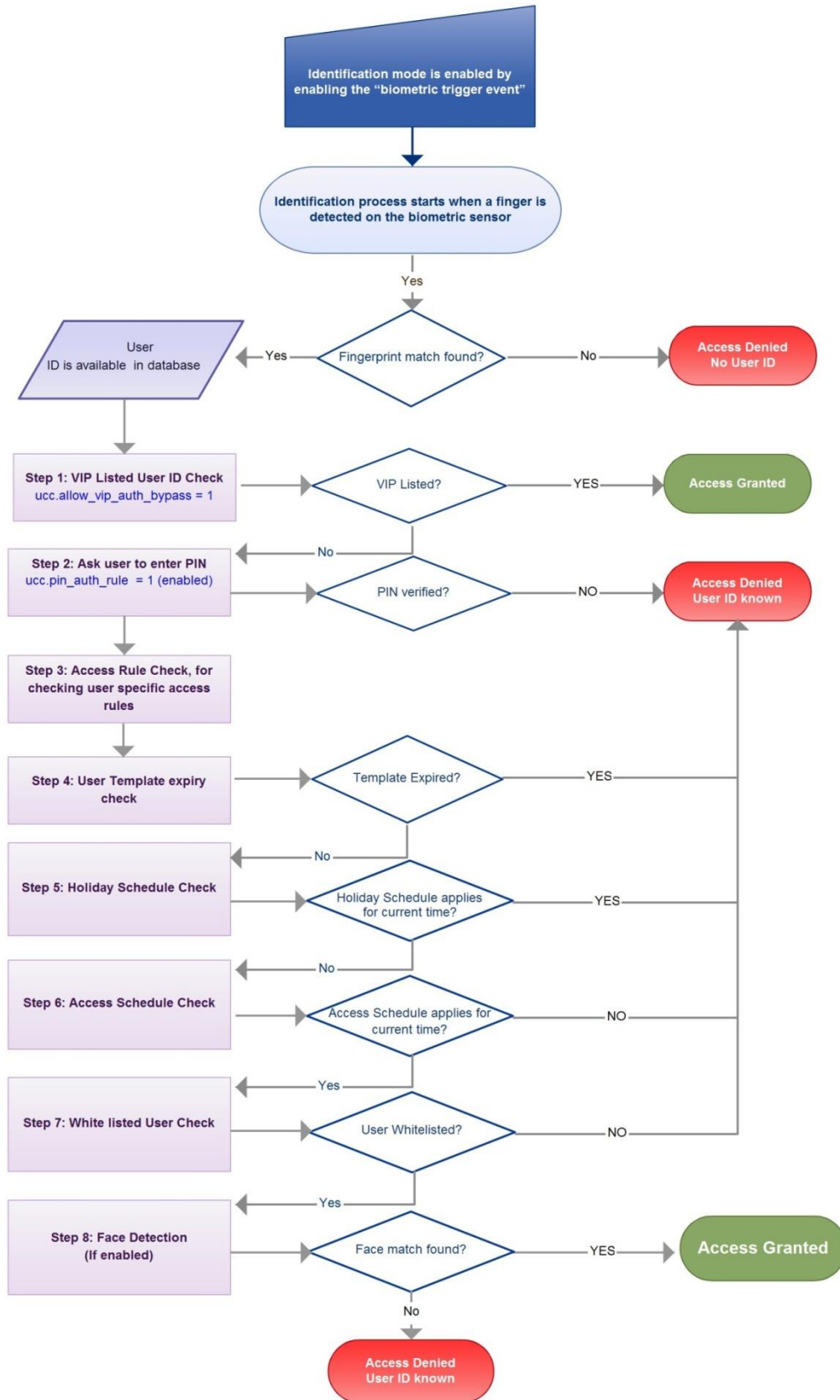


Figure 327: Access Control Flow Diagram when Terminal is in Identification Mode

Access Control Process in Authentication Mode

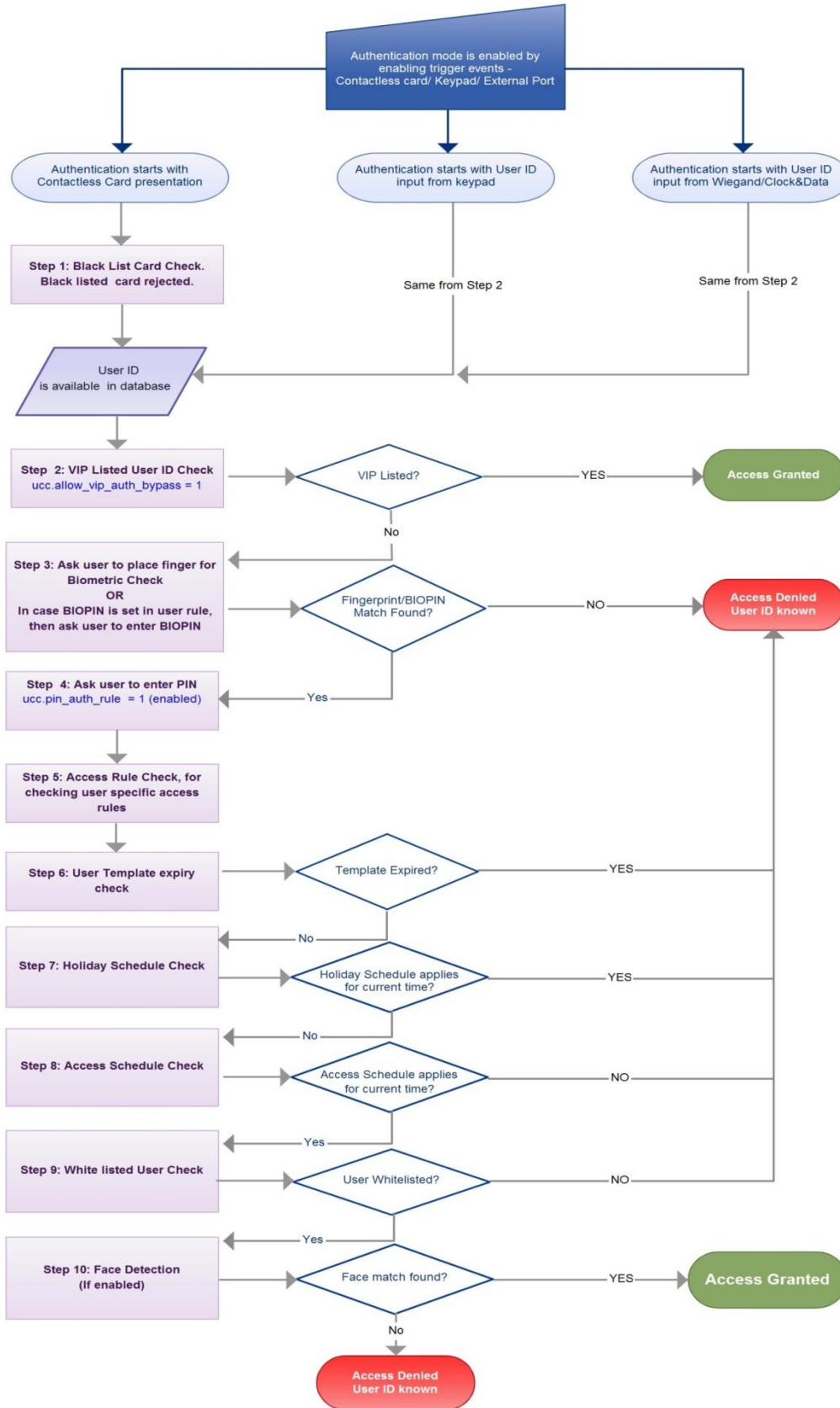


Figure 328: Access Control Flow Diagram in Authentication Mode

Access Control Process for VIP Users

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

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

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

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

Configuration Key

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

Access Control Result

Information for the User

The MorphoAccess® SIGMA Series 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.

Information for the Administrator

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

This feature is described in the “Access Request Result Log File” section.

Integration in an Access Control System

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

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

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

Access Granted



Figure 329: Access Granted Diagram

Access Denied



Figure 330: Access Denied diagram

Section 10 : Access Control by Identification

Identification Mode Description

Identification Process

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

Access Control by Identification

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

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

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

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

Result of the access control request

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

User's Data required in the terminal

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

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

Identification Modes (database extension licenses)

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

- MA_10K_USERS
- MA_50K_USERS
- MA_100K_USERS (extend database maximum size)

Refer to "[User licenses](#)" section for more details about licenses.

Compatibility with Access Control Systems

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

- internal relay activation when the access is granted, as described in "[Internal Relay activation on Access Granted result](#)" section,
- external activation of the internal relay, as described in "[External activation of the internal relay](#)" section,
- send access control result message to a remote system, as described in "[Sending an Access Control Result Message](#)" section

User Interface

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

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



Place finger on
biometric sensor

Figure 331: Identification Mode

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

- if a match is found, then the user is identified (the terminal has its identifier) and access is granted to the user,
- Otherwise, if no match found, the user remains unknown (the user’s identifier is unavailable), and the access is denied.

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

When the identification process is completed, whatever is the result (identified or not identified), the terminal automatically restarts to the initial state: wait for finger placement on the biometric sensor.

When there is no user stored in the database, the identification process is disabled. No user is able to grant the access. The terminal notifies this invalid state to the user as described in *“Terminal States”* section.

Section 11 : Access Control by Authentication

Authentication Process

Introduction

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

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

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

Authentication process

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

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

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

Access control by authentication

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



Figure 332: Users trigger the authentication process by showing their card

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

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

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

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

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

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

Contactless Smart Card

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

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

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

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

List of contactless cards validated

If you have a request outside this list, please contact your Morpho representative.

MASigma/Lite Prox

- HID ProxCard II

MASigma/Lite Multi

- MIFARE® Classic - 1K/4K for 7 Bytes and 4 Bytes CSN
- DESFire® EV1 with legacy 3DES and AES encryption
- DESFire® EV0 with 3DES

MASigma/Lite iClass
iCLASS SE® Card

| HID MODELS | | card description | Standard for contactless communications | Morpho readers |
|----------------|----------------------|---|---|---------------------------|
| PVC Technology | Composite Technology | | | MA SIGMA MA SIGMA Lite |
| 3000 | 3050 | 2k bit (256 Bytes) card | ISO 15693/14443B | Limited support * |
| 3001 | 3051 | 16k bit (2k Bytes) card with 2 application areas | ISO 15693/14443B | supported |
| 3002 | 3052 | 16k bit (2k Bytes) card with 16 application areas | ISO 15693/14443B | supported |
| 3003 | 3053 | 32k bit (4k Bytes) 16k/2+16k/1 | ISO 15693/14443B | supported |
| 3004 | 3054 | 32k bit (4k Bytes) 16k/16 + 16k/1 | ISO 15693/14443B | supported |

iCLASS® Card

| HID MODELS | | card description | Standard for contactless communications | Morpho readers |
|----------------|----------------------|---|---|---------------------------|
| PVC Technology | Composite Technology | | | MA SIGMA MA SIGMA Lite |
| 2000 | 2100 | 2k bit (256 Bytes) card | ISO 15693 | Not supported |
| 2001 | 2101 | 16k bit (2k Bytes) card with 2 application areas | ISO 15693/14443B | supported |
| 2002 | 2102 | 16k bit (2k Bytes) card with 16 application areas | ISO 15693/14443B | supported |
| 2003 | 2103 | 32k bit (4k Bytes) 16k/2+16k/1 | ISO 15693/14443B | supported |
| 2004 | 2104 | 32k bit (4k Bytes) 16k/16 + 16k/1 | ISO 15693/14443B | supported |

*: only HID CN (from PAC data) could be used. Encoding is not supported

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

Authentication Process Options

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

The user's reference biometric data can be located:

- either on his personal card, as described in "Biometric check, biometric data on user's card" section,
- or in a record of the internal database, as described in "Biometric check and biometric data in local database" section

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

Manual bypass of biometric control

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

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

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

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

For example,

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

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

For example,

- If User rule is "Keypad + BIO" and biometric check is disabled then also for that user BIO check is performed (Logical OR operation).

- If User rule is “Keypad only” and biometric check is enabled then also for that user BIO check is performed (Logical OR operation).

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

- Disabled terminal biometric check
- Enable BIO check in user rule for all the user
- Disable BIO check for user for whom BIO check needs to be bypassed

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

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

- The terminal doesn’t require the user to place a finger on the biometric sensor. The access is granted without biometric check.
- According to the authentication process selected, the terminal:
- doesn’t perform any check on the user’s identifier, as described in section “No biometric check, no User ID check”
- The terminal checks that the user’s identifier is in the terminal database, as specified in the section “Biometric check and biometric data in local database”

Automatic bypass of biometric control

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

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

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

Result of access control check

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

Compatibility with Access Control Systems

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

- internal relay activation when the access is granted, as described in "Internal Relay activation on Access Granted result" section,
- external activation of the internal relay, as described in "External activation of the internal relay" section,
- send access control result message to a remote system, as described in "Sending an Access Control Result Message" section

Selection of user’s contactless card type (MIFARE® and/or DESFire®)

Contactless Card type

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

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

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

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

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

Parameter Configuration

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

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

Compatibility with “Authentication” modes

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

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

Biometric check, biometric data on user's card

Description

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

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

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

User's data required in the terminal

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

User's data required on the user's card

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

- the user's identifier (User ID),
- The biometric data of two reference fingers of the user.

All other data are ignored.

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

Activation key

- Card Type selected at the time of User Enrolment should be at least User ID + Biometric
- Using Webserver, the User Record Reference parameter value must be set to Card for authentication using smart card. Refer to "User Control Configurations" under Webserver

User Interface

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



Figure 333: Authentication with user's fingerprints on contactless card

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

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

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

When the authentication process is completed, whatever is the result (identity confirmed or not), the terminal automatically restarts to the initial state: wait for another user's card presentation.

PIN verification - PIN stored on card

Description

In this mode, each user's card contains an identifier, PIN Code and the biometric data of two different fingers of the user. The terminal compares the entered PIN Code with the corresponding code in the user's card. If PIN verified successfully and biometric check is mandatory, then terminal will compare the biometric data of the finger placed on the biometric sensor, with the reference biometric data of the two user's fingers read on the card. If a match is found, the access is granted, otherwise the access is denied.

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

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

User's data required in the terminal

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

User's data required on the user's card

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

- the user's identifier (User ID),
- the PIN code of user
- the biometric data of two reference fingers of the user.

All other data are ignored.

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

Activation key

- Card Type selected at the time of User Enrolment should be at least "User ID + PIN" or "User ID + Biometric + PIN"
- Using Webserver, the User Record Reference parameter value must be set to Card for authentication using smart card. Refer to "User Control Configurations" under Webserver

User Interface

The authentication process starts when the user presents his contactless card in front of the terminal (where the antenna of the contactless card reader is located). If it is compatible (same authentication keys, and mandatory data present on card), the user is invited to enter its PIN Code, for PIN Verification.

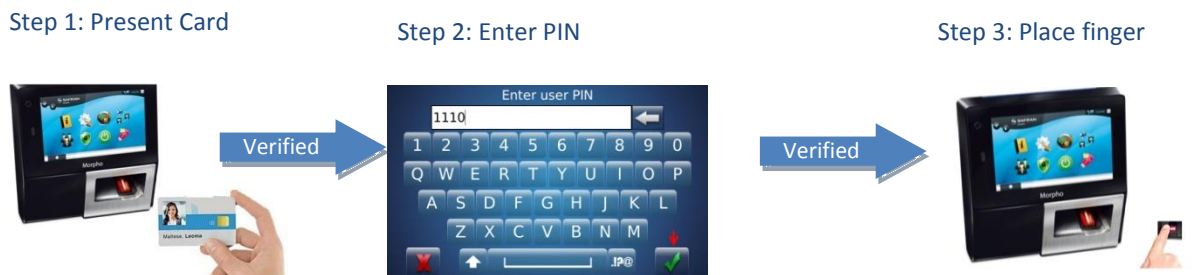


Figure 334: Authentication with user's PIN Code and fingerprints on contactless card

Once the PIN Code is verified, and biometric check is enabled, then the user is invited to place his finger on the biometric sensor, for biometric authentication. The terminal compares the biometric data of the finger placed on the sensor, with the reference biometric data of the two reference fingers read on user's card.

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

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

When the authentication process is completed, whatever is the result (identity confirmed or not), the terminal automatically restarts to the initial state: wait for another user's card presentation.

BIOPIN verification - BIOPIN stored on card

Description

In this mode the card should contain a Biometric PIN (BIOPIN). The goal of this code is to replace fingerprints authentication by BIOPIN code verification when the fingerprints of the user are not available during enrolment for any reason. Each user's card contains an identifier and BIOPIN. Authentication process starts when user presents card at terminal card reader and enters BIOPIN. Entered BIOPIN is matched with the BIOPIN stored in card, and then access is granted. This authentication mode doesn't use the database of the terminal.

This feature enables to support two kind of users in the same access control system: normal user with fingerprints (biometric check), and special user without fingerprints but with a BIOPIN code (BIOPIN check instead of biometric check).

User's data required in the terminal

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

User's data required on the user's card

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

- the user's identifier (User ID),
- the BIOPIN code of user

All other data are ignored.

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

Activation key

- Card Type selected at the time of User Enrolment should be at least User ID + BIOPIN
- Using Webserver, the User Record Reference parameter value must be set to Card for authentication using smart card. Refer to "*User Control Configurations*" under Webserver

- Following parameter is required to be configured:

| Parameter Name | Parameter Value | Description |
|----------------------------|-----------------|--|
| ucc.allow_biopin_user_rule | 0 or 1 | Set this parameter to “0”, to disable BIOPIN check Set this parameter to “1”, to enable BIOPIN check Set this parameter to “2”, to set PIN check |

User Interface

The authentication process starts when the user presents his contactless card in front, instead of requested to place his finger on the biometric sensor of the terminal (where the antenna of the contactless card reader is located). If it is compatible (same authentication keys, and mandatory data present on card), the user is asked to enter Biometric PIN (BIOPIN) using keypad, instead of requested to place his finger on the biometric sensor.

Step 1: Present Card



Step 2: Enter BIOPIN



Figure 335: Authentication with user's BIOPIN on contactless card

The terminal compares the BIOPIN entered, with the BIOPIN read from user's card.

The authentication process is successful (identity confirmed) if the entered BIOPIN is matched with the BIOPIN stored on user's card.

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

When the authentication process is completed, whatever is the result (identity confirmed or not), the terminal automatically restarts to the initial state: wait for another user's card presentation.

Biometric check and biometric data in local database

Description

In this mode, the identifier of the user is the only one data read on user's card. The biometric data of two different fingers of the user are stored in the internal database, with the same user's identifier as the one on the user's card.

The terminal compares the biometric data of the finger placed on the biometric sensor, with the user's biometric data found in the database (in user's record). If a match is found, the access is granted, otherwise (no match found) the access is denied.

User's data required in the terminal

This mode requires the use of the terminal's internal database and the presence of a record for each authorized user. Each record contains:

- the same user's identifier value as the one stored on user's card,
- the biometric data of two user's fingers.

If the user's identifier, read on the user's card, is not found in the database, then the access is denied.

The size and the management of the internal database are described in "*MorphoAccess® Terminal Database Management*" section.

User's data required on the user's card

The only data required on the user's card is the user's identifier. All other data is ignored.

The terminal is able to read the user's identifier either stored in a TLV structure or to be read directly at a given offset on the card (binary format) (MIFARE® card only).

The TLV format is described in the MorphoAccess® SIGMA Series terminals Contactless Card Specification document.

Activation key

- Card Type selected at the time of User Enrolment should be User ID
- Trigger event “Card” must be ON
- Using Webserver, the User Record Reference parameter value must be set to Card for authentication using terminal database. Refer to “User Control Configurations” under Webserver

User interface

The authentication process starts when the user presents his contactless card in front of the terminal (where the antenna of the contactless card reader is located). If the user’s identifier read on the card is found on the terminal’s internal database, then the user will be invited to place his finger on the biometric sensor, for biometric authentication.



Figure 336: Authentication with biometric check, reference in database

The terminal then compares the biometric data of the finger on the sensor with the reference biometric data found in the database record.

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

The result of the authentication process is notified to the user by an audio signal, as described in Terminal states section.

When the authentication process is completed (whatever is the result), the terminal automatically restarts to the initial state: wait for another user’s card presentation.

When there is no user stored in the database, this authentication process is disabled. No user is able to grant the access by this way. The terminal notifies this invalid state to the user, as described in “Terminal States” section.

Authentication with local database: User ID entered from keyboard

Description

In this mode, the User ID of the user is entered using the MorphoAccess® SIGMA Series terminal keyboard. If the User ID exists in the database, the terminal performs an authentication using the biometric templates associated to this User ID.



Figure 337: Authentication with User ID entered from Keyboard and biometric check

The authentication process starts when the user enters User ID, using keyboard on terminal. If the user's identifier is found on the terminal's internal database, then the user will be invited to place his finger on the biometric sensor, for biometric authentication.

The terminal then compares the biometric data of the finger on the sensor with the reference biometric data found in the database record. The authentication process is successful (identity confirmed) if the captured finger data matches with one of the two references finger data. Otherwise (no match found) the authentication process fails (identity not confirmed).

Activation key

- Trigger event "Keypad" must be ON
- Using Webserver, the User Record Reference parameter value must be set to Card for authentication using terminal database. Refer to "*User Control Configurations*" under Webserver

Authentication with local database: ID input from Wiegand or Clock & Data

Description

This mode requires an external card reader that will send the user’s ID to authenticate to the MorphoAccess® SIGMA Series terminal through Wiegand or Clock & Data input.

The default screen invites the user to pass his badge so the external reader sends the User ID to the terminal’s Wiegand or Clock & Data input. If the ID exists in the database, the terminal performs an authentication using the biometric templates associated to this ID.

If the authentication is successful, the terminal triggers the access or returns the User ID to the Central Access Controller.

Once the user authentication is done, terminal will automatically loops back and waits for a new input ID. If the identifier sent by the reader is not present in the local database, authentication is not launched.

Activation key

The activation of this mode is controlled by following parameter:

| Parameter name | Value | Description |
|-------------------------------------|-----------|---|
| ucc.trigger_event | 1 to 15 | Use this parameter to enable finger, contactless, keypad and external port trigger. Only when external port trigger is enabled, the terminal would receive trigger from Wiegand or Clock & Data. <ul style="list-style-type: none"> Set ‘0’ to enable External Port Note: Trigger Event through “ <i>Configure Trigger Events</i> ” through Terminal and “ <i>Event Configurations</i> ” through Webserver. |
| wiegand.external_port_input_type | 0 or 1 | Storing current external port input type as: <ul style="list-style-type: none"> Set ‘0’ for Wiegand format input (default) Set ‘1’ for Clock & Data format input |
| wiegand.external_port_output_status | 0, 1 or 2 | To enable/disable Wiegand output functionality. <ul style="list-style-type: none"> Set ‘0’ to never send data using Wiegand Port Set ‘1’ to always send data using Wiegand Port (default) |

| Parameter name | Value | Description |
|-----------------------------------|--------|--|
| | | <ul style="list-style-type: none">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: <ul style="list-style-type: none">Set '0' for Wiegand format outputSet '1' for Clock & Data format output |

References

- Wiegand Parameters are configurable from Webserver; refer to "[Wiegand Parameters Settings](#)" in this guide.
- You can also refer to **MorphoAccess® SIGMA Series Parameters Guide** for complete list of Wiegand parameters.
- If the MorphoAccess® SIGMA Series terminal is in L1 legacy mode, then Wiegand parameters can be configured from SecureAdmin application

Wiegand Frame Configuration

When set up to communicate with Wiegand protocol, the MorphoAccess® SIGMA Series terminal can handle several data formats for reading Wiegand string; refer to “Wiegand Format and Associated Values”.

The default format of Wiegand string is Standard 26 Bits. An authentication is initiated through User ID input from Wiegand string, which consists below information:

- **Total Bits:** The number of Wiegand bits in the Wiegand string (maximum 512 bits length)
- **ID Start Bit:** the start bit of the ID Field (where the first bit is Bit 0)
- **Total ID Bits:** the number of bits in the ID Field (must be contiguous bits).

Using these parameters, when a card is presented to the terminal, it attempts to decode the ID Field and uses that information as the User Identifier (User ID of a template). All Site codes, Parity, and any other data are ignored.

Using the decoded ID, the terminal will verify corresponding User IDs stored in the database.

If the ID is not found in the terminal database, the verification attempt fails and Wiegand output string is set to the Wiegand Port in the configured format. There is no communication with central access controller.

If the ID is valid and a successful verification is performed, the Wiegand Output String is sent to Wiegand port in the configured format.

Note: For sending Wiegand Output, it is required to enable ‘Activate Wiegand Output’ parameter from Webserver. If this parameter is disabled, then no Wiegand output is sent by terminal on verification fail or pass.

Wiegand frame example (26 bits)

For Standard 26 bit - [(26, 9, 16) (1, 8, 10) P1 = (0, Even, 1-12) P2 = (25, Odd, 13-24)],

Wiegand string sent from Terminal 1 to terminal2 will be as below:

| | | | | | | | | | | | | | |
|----------|--------|---|---|-----|---|---------|----|----|----|-----|----|----|----------|
| 0 | 1 | 2 | 3 | ... | 8 | 9 | 10 | 11 | 12 | ... | 23 | 24 | 25 |
| Parity 1 | SITE | | | | | ID | | | | | | | Parity 2 |
| 0 | 8 bits | | | | | 16 bits | | | | | | | 1 |

Here,

- **(26,9,16)**: consists ID total length, ID start bit, ID length
- **(1,8,10)**: consists Site code start bit, length, value
- **Parity1 (P1)**: Even parity calculated on 0 bit from 1 to 12 bit. Parity Bit is a check whether the data sent from one device to other is same.
- **Parity2 (P2)**: Odd parity calculated on 25 bit from 13 to 24 bit

No biometric check, no User ID check

Description

This authentication mode is the version of the “Biometric check, biometric data on user's card” authentication mode with biometric check disabled.

The terminal searched only for the user's identifier on the user's card. No other check is performed: the user's identifier is not searched in the local database, and there is no biometric check.

A user's card which disables the biometric control is useful when the biometric data capture is not required (for example, for a short period visitor), or impossible (physically or legally). This kind of cards can be realized without user's presence and the same card used for different visitors.

The internal database of the terminal is not used. The MorphoAccess® SIGMA Series terminal acts as a simple contactless card reader.

The access is granted only if the user's card is encrypted with the authentication keys stored in the terminal, and if the terminal is able to read a user's identifier. Otherwise, the card is ignored and the access denied.

User's data required in the terminal

In this authentication mode, the terminal's internal database is not used. No user data is required.

User's data required on the user's card

To be compatible with this authentication mode, the user's card must contain a User Identifier (User ID). It can be in a TLV structured data, or a Binary data to be read on the card (MIFARE® card only).

- All other data is ignored.

The TLV format is described in the **MorphoAccess® terminals Contactless Card Specification** document.

The MorphoAccess® SIGMA Series terminal doesn't perform any check on the value of the user's identifier.

Activation key

- Card Type selected at the time of User Enrolment should be User ID only
- Using Webserver an administrator can set **User Record Reference** parameter as Card for authentication using smart card, refer “User Control Configurations”
- If no PIN code check and no biometric check are required for the user, then the best is to provide him a Visitor card. Refer “Encode Visitor Card”

User Interface

The authentication process starts when the user presents his contactless card to terminal. As shown below:



Figure 338: Authentication without biometric check and with User ID check in card

The authentication process succeeds if the user's identifier is found. Otherwise, the authentication process fails.

The result of the authentication process is notified to the user by an audio signal, as described in Terminal states section.

When the authentication process is completed (whatever is the result), the terminal automatically restarts to the initial state: wait for another user's card presentation.

No biometric check, User Identifier in the database

Description

This authentication mode is the version of the *“Biometric check and biometric data in local database”* authentication mode, when biometric check is disabled.

The user’s identifier is the only data read on user’s card. The terminal checks if the user’s identifier exists in the database, but doesn’t perform any biometric check.

The access is granted if the user’s identifier read on the user’s card is found in the internal database. Otherwise (user’s identifier not found in the database), the access is denied.

User’s data required in the terminal

This mode requires a local database, and a record must be created for each allowed user. Each record contains:

- the same identifier as the one on the user’s card,
- the reference biometric data of two fingers of the user (not used, but required)

If the terminal doesn’t find a record with the user’s identifier read on the card, the access is denied.

The size and the management of the internal database are described in **MorphoAccess® Terminal Database management** section.

User’s data required on the user’s card

In order to be compatible with this authentication mode, the user’s card must contain a User ID. It can be in a TLV structured data, or a Binary data to be read on the card (MIFARE® card only).

- All other data are ignored.

The TLV format is described in the **MorphoAccess® terminals Contactless Card Specification** document.

Activation key

- Card Type selected at the time of User Enrolment should be User ID only
- Using Webserver an administrator can set **User Record Reference** parameter as Terminal for authentication using terminal database, refer "[User Control Configurations](#)"
- Following parameter is required to be configured:

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

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 339: Authentication without biometric control, and with the user login

The user's identifier is read on the user's card and searched in the local database.

The authentication process succeeds if the user's identifier is found in the local database. Otherwise, the authentication process fails.

The result of the authentication process is notified to the user by an audio signal as described in Terminal states section. Once the authentication process is completed (regardless of the result), the terminal automatically loops back and waits for another user's card presentation.

Authentication process specified by User's card

Description

When this mode is enabled, the access rights check to perform is specified by a dedicated data on user's card. It means that the same terminal can execute a different process according to a data found on the user's card:

- the biometric check is performed with the reference biometric data found on user's card,
- the PIN check is performed with the reference PIN data found on user's card,
- the PIN + biometric check is performed with the reference PIN + biometric data found on user's card,
- The biometric check is disabled, and only the presence of the user's identifier on the user's card is checked.

A user's card which disables the biometric control is useful when the biometric data capture is not required (for example, for a short period visitor), or impossible (physically or legally). This kind of cards can be realized without user's presence and the same card used for different visitors. The internal database of the terminal is not used in such case.

User's data required in the terminal

This authentication mode doesn't use the internal database of the MorphoAccess® SIGMA Series terminal. There is no personal data stored in the terminal.

User's data required on the user's card

- To be compatible with this authentication mode, the user's card must contain at least the user's identifier and the process selector data.
- If the biometric check is requested, the biometric data of two fingers of the user must be present on the user's card.
- If PIN code check is required, the user's PIN code must be on user's card.
- All other data is ignored.
- The required data must be stored according to TLV format. The user's card format (and the TLV format) is described in the **MorphoAccess® terminals Contactless Card Specification** document.

Activation key

- Card Type selected at the time of User Enrolment should be “User ID only”, “User ID + PIN”, “User ID or Template” or “User ID + PIN + Template” as required
- Using Webserver an administrator can set **User Record Reference** parameter as Card for authentication using Card data, refer “[User Control Configurations](#)”
- If no PIN code check and no biometric check are required for the user, then the best is to provide him a Visitor card. Refer “[Encode Visitor Card](#)”

User Interface

Start

The authentication process starts when the user presents his contactless card at card reader of terminal.

The terminal searches on the user’s card, for the data that indicates which kind of check is mandatory or disabled. If this data is found, the terminal executes the required process (with or without PIN code check, and with/without biometric data check).

Step 1: Present Card



Step 2: Place finger



Step 3: Enter PIN



Figure 340: Authentication process specified by user's card

The result of the authentication process is notified to the user by an audio signal as described in Terminal states section.

Once the authentication process is completed (regardless of the result), the terminal automatically loops back and waits for another user’s card presentation.

PIN check disabled, Biometric check mandatory

The terminal requires the user to place a finger on the biometric sensor. Then it executes a comparison of the biometric data of the finger placed on the sensor and the reference biometric data read on user's card.

The process is identical to the one described in "*Biometric check, biometric data on user's card*" section.

PIN check disabled, Biometric check disabled

The result of the authentication process is positive (identity confirmed), if the user's identifier is found on the user's card.

The terminal doesn't require the user to place a finger on the biometric sensor, and doesn't perform any biometric check.

The process executed is identical to the one described in "*No biometric check, no User ID check*".

PIN check mandatory, Biometric check mandatory

On User ID verification, the terminal requires user to enter a PIN code. The PIN entered by user is matched with the PIN stored on Card.

On successful verification of PIN, the user is asked to place a finger on the biometric sensor. Then it executes a comparison of the biometric data of the finger placed on the sensor and the reference biometric data read on user's card.

The process is identical to the one described in "*PIN verification - PIN stored on card*" section.

PIN check mandatory, Biometric check disabled

On User ID verification, the terminal requires user to enter a PIN code. The PIN entered by user is matched with the PIN stored on Card.

The process is identical to the one described in "*PIN verification - PIN stored on card*" section.

Allowed format for User's identifier

TLV structured data

The user's identifier is stored in ASCII characters within a TLV structure.

This is the default configuration of the MorphoAccess® SIGMA Series terminal: the related parameters are listed in the table below for each type of card:

| Parameter Name | Parameter Value | Description |
|---------------------------|---|--|
| sc_tlv_desfire.aid | 0 to 16777215 (0x000000 to 0xFFFFFFFF) (0x42494F - Default) | 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 - 1 (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 - 177 (19 - Default) | Sets iCLASS® card Page offset for 2APP for TLV card. |
| sc_tlv_mifare.key_policy | 1, 2 or 3 | Sets key policy to read MIFARE® card for TLV mode. Set "1" - Try to read card first with Key A then Key B (Default) Set "2" - Try to read card with Key A Set "3" - Try to read card with Key B |
| sc_tlv_mifare.num_block | 4 - 215 (31 - Default) | Sets number of blocks to read MIFARE® card for TLV mode. |

| Parameter Name | Parameter Value | Description |
|------------------------------------|---------------------------|---|
| sc_tlv_mifare_plus. key_policy | 1, 2 or 3 | Sets key policy to read MIFARE® Plus card for TLV mode. Set “1” - Try to read card first with Key A then Key B (Default) Set “2” - Try to read card with Key A Set “3” - Try to read card with Key B |
| sc_tlv_mifare_plus. start_block | 0 - 215 (4 - Default) | Sets start block number to read MIFARE® plus card for TLV mode. |
| sc_tlv_mifare.start _block | 4 - 215 (4 - Default) | Sets start block number to read MIFARE® card for TLV mode. |
| sc_tlv_mifare_plus. num_block | 0 - 216 (31 - Default) | Sets number of blocks to read from MIFARE® plus card for TLV mode. |
| sc_tlv_iclass.num_ block | 0 to 255 (128 – Default) | Sets number of blocks to read from iCLASS® card for TLV mode. |

The contactless smartcard logical structure is described in a dedicated document:
MorphoAccess® terminals Contactless Card Specification.

Binary Data

Description

The MorphoAccess® SIGMA Series terminal is able to use a binary value to read on specific location on user's card, as user's identifier. The terminal in legacy modes can also write smart card in binary data format.

As a sample of binary value, the serial number of the card can be used, as explained in the "Example: MIFARE® card Serial Number" in this section subsequently.

The MorphoAccess® SIGMA Series terminal is able to read a binary value which is not aligned on complete bytes. This ability is useful to extract the user's identifier from a Wiegand frame written on the user's card. A sample is described in "Example: 32 bits user's identifier within a 37-bits Wiegand frame" section.

No TLV structure is required on user's card: the MorphoAccess® SIGMA Series terminal is able to proceed with user's cards written by other systems.

Card type compatibility

This feature can only be used when the "MIFARE® card only" mode is set (User ID in binary or TLV format). Then the related configuration key must be set to zero.

| Type of contactless smartcard enabled | |
|---------------------------------------|---|
| sc.encode_profile = 2 | MIFARE® card only (identifier of the user is a binary value). |

Configuration keys

The binary data to be read is defined by:

- the first block containing the data,
- the offset of the first byte and first bit of the data, inside the sector. This value must not exceed 15 bytes. The terminal can read data that doesn't start on a full byte,
- the length in bytes and additional data bits; this must not exceed 8 bytes. The terminal can read data where the length is not a multiple of 8 bits,
- the read direction: MSB or LSB.

| User Identifier to be read in binary format | |
|---|--|
| sc_binary_read.data_format = 1 | Binary format |
| sc_tlv_MIFARE®.start_block | [1-215] 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. 8.0). |
| 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. 15.0) |
| sc_binary_read.data_type_direction | Byte read acquisition method: 0.1 (binary data, MSB first) 0.0 (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 |

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.

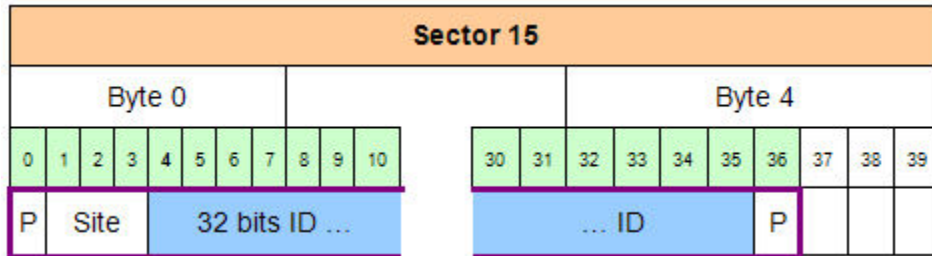


Figure 341: Using a Wiegand frame as User ID

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 = 0.1 | Binary identifier, MSB format |
| sc_binary_read.data_length_num_bytes = 4.0 | Size = 4 bytes |
| sc_binary_read.data_offset_num_bytes = 0.4 | User’s identifier begins at bit 4 of the first byte of the block specified below |
| sc_tlv_MIFARE®.start_block = 46 | Read from first block of sector 15 (i.e. block 46) |

When the user’s identifier must be sent to a distant system using Wiegand protocol, it is possible to configure the terminal to add automatically the start and stop bits to the Wiegand output frame.

Section 12 : Multifactor Access Control Mode

Multi-factor Mode

Description

The MorphoAccess® SIGMA Series terminal authorizes simultaneous activation of the access control mode by identification and one of the access control modes by authentication.

This is the first user action which automatically selects the access right control process to be executed.

User Interface

In this mode the terminal is waiting for the placement of a finger on the biometric sensor, or for the presentation of a user's card. It will run:

- the identification process if the user places his finger on the biometric sensor first,
- Or the authentication process if the user shows his card first.



Figure 342: Multi-factor mode (identification or authentication)

When there is no database, the identification mode (with finger) is automatically disabled, but the authentication mode is still available (by showing the card).

User's data required in the terminal

These are the same data as those required by the "Identification Mode Description".

These are also the same data as those required by the "Authentication Process". Please see corresponding section.

User's data required on the user's card

The items required on the user's card depend on the activated authentication mode(s). Please refer to the appropriate section for further details.

Activation keys

- Trigger event through Biometric, Contactless Card, Keypad and External Database should be enabled

Section 13 : Time and Attendance Mode

Time and Attendance Synoptic

MorphoAccess® SIGMA Series terminals can be configured to work in Time and Attendance (T&A) mode. When T&A mode is enabled, each terminal event logged would have some attendance information (such as entry time, exit time, etc.).

When the time and attendance feature is activated, the home screen of the terminal displays certain function keys or a bitmap file. For example, LCD Displays below keys as T& A action:

F1 = IN

F2 = OUT

F3 = Lunch IN

F4 = Lunch OUT

Instead of texts, icons can be selected to be displayed to the user. Along with biometric presentation, use is also required to select applicable function key (F Key). Suppose, user is entering office in the morning, than F key displaying 'IN' must be pressed. Similarly on every exit and entry the appropriate option must be selected.

T&A action inputs are logged by the terminal. This information is used to track the attendance of an employee, analyze employee productivity and overall organization productivity. Thus Time and Attendance mode becomes a crucial feature for human resource management.

Time and Attendance can be configured in one of the modes listed below:

Normal Mode

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 343: 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.

An administrator can configure the Time & Attendance mode by configuring relevant parameters using Web server interface.

Parameter Configuration

| Time and Attendance Mode Activation | |
|--|--|
| <i>time_and_attendance.tna_mode</i> | <p>If an administrator selects parameter value as 0, the T&A mode is disabled.</p> <p>If an administrator selects parameter value as 1, the T&A mode is enabled. When T&A is enabled, it is by default in normal mode, showing 4 F keys.</p> |

Extended Mode

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:

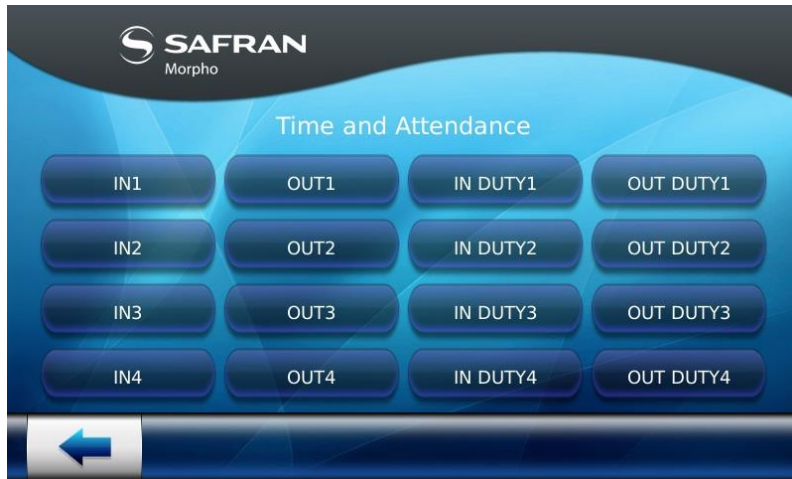



Figure 344: Time and Attendance Screen in Extended Mode 1x16



Figure 345: 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  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 MorphoAccess® SIGMA Series 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 finger 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 detected on 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 | |
|--|--|
| <i>time_and_attendance.tna_extended_mode</i> | <p>When Time & Attendance extended mode is enabled, there are 16 function keys that are configurable and displayed to user to select from.</p> <p>If an administrator selects parameter value as 0, the extended mode is disabled. If disabled, then T&A will be by default on normal mode where only 4 F keys are displayed.</p> <p>If an administrator selects parameter value as 1, the extended mode is enabled.</p> |

T&A Mode Mandatory or Optional Scenarios

- **Mandatory:** An administrator can set T&A Mode as Mandatory. It means it is mandatory for the user to input T&A action by selecting function key, in order to get access. There are three scenarios when T&A is normal mandatory mode and user initiates access request,
- **T&A before User Control with F Key:** It means user first selects a T&A action, then terminal will ask user to place his finger on the sensor or present his card. Then, after user's data acquisition, the terminal checks access rights and display the result for the user.
- **T&A before User Control without F Key:** In this scenario, user will place his finger on the sensor or present his card. Instead of access rights check, terminal will first prompt user to enter a T&A action. Once function key is selected, user access rights check will begin and terminal will display access result
- **T&A after User Control without F Key:** In this scenario, user will place his finger on the sensor or present his card. Terminal will first authenticate the user. On access granted result, terminal will prompt user to enter a T&A action. Once function key selected, terminal will allow access
- **Optional:** If T&A Mode is not mandatory, then user has a choice to whether input the function key or not. The terminal will initiate access rights check without T&A input. However, the transaction logs generated has the records, provided user has input the F key.

Parameter Configuration

| Time and Attendance Mandatory/Normal Mode Selection | |
|---|---|
| <code>time_and_attendance.tna_mandatory_mode</code> | If an administrator selects parameter value as 0, the mandatory mode is disabled. If an administrator selects parameter value as 1, the mandatory mode is enabled. |

Refer to "[Time and Attendance Mode Configuration](#)" to know more on how to configure T&A parameters using Webserver interface.

T&A - Mandatory Mode Work Flow Diagram

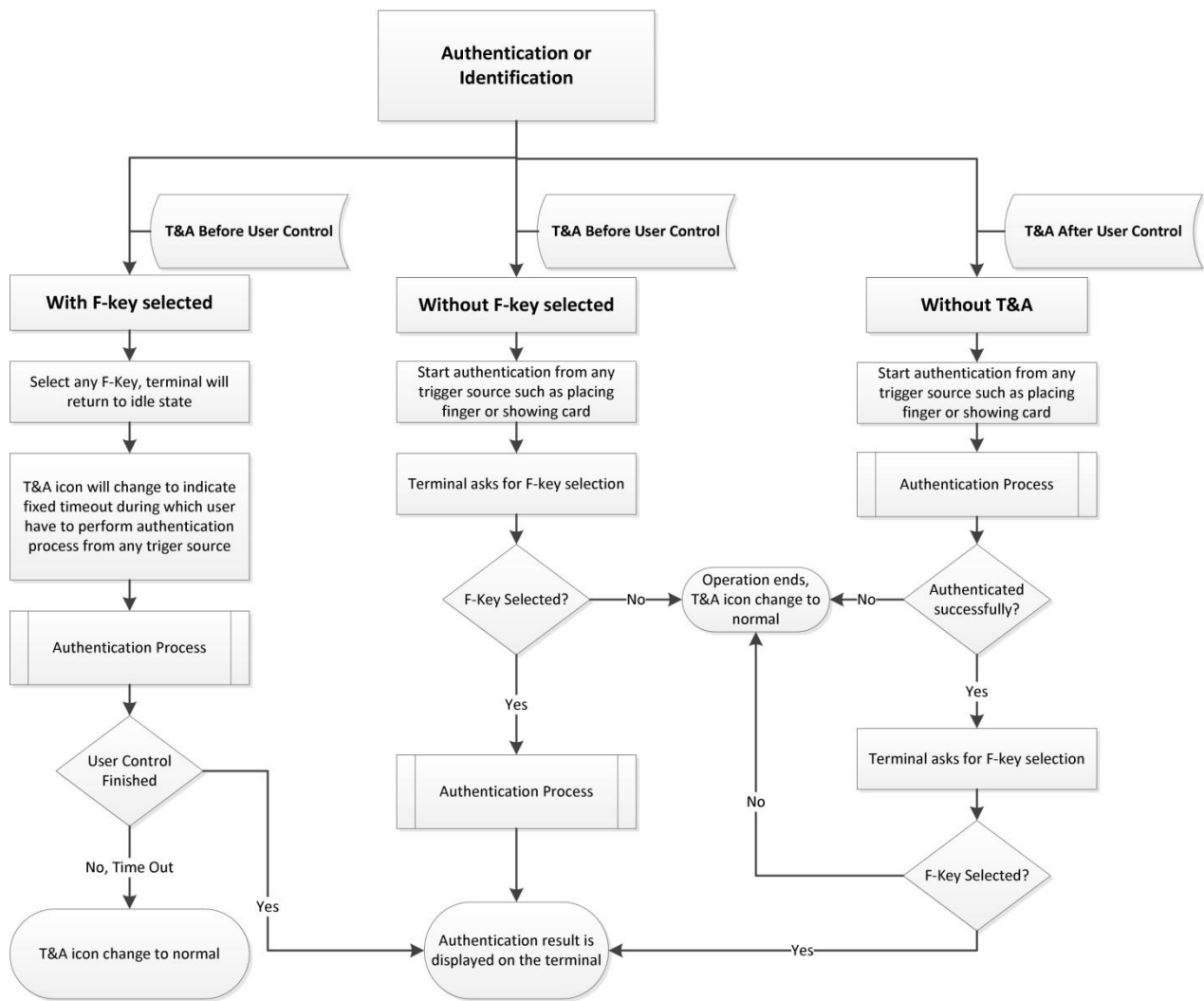


Figure 346: Time and Attendance in Mandatory Mode Workflow Diagram

T&A - Non Mandatory Mode Work Flow Diagram

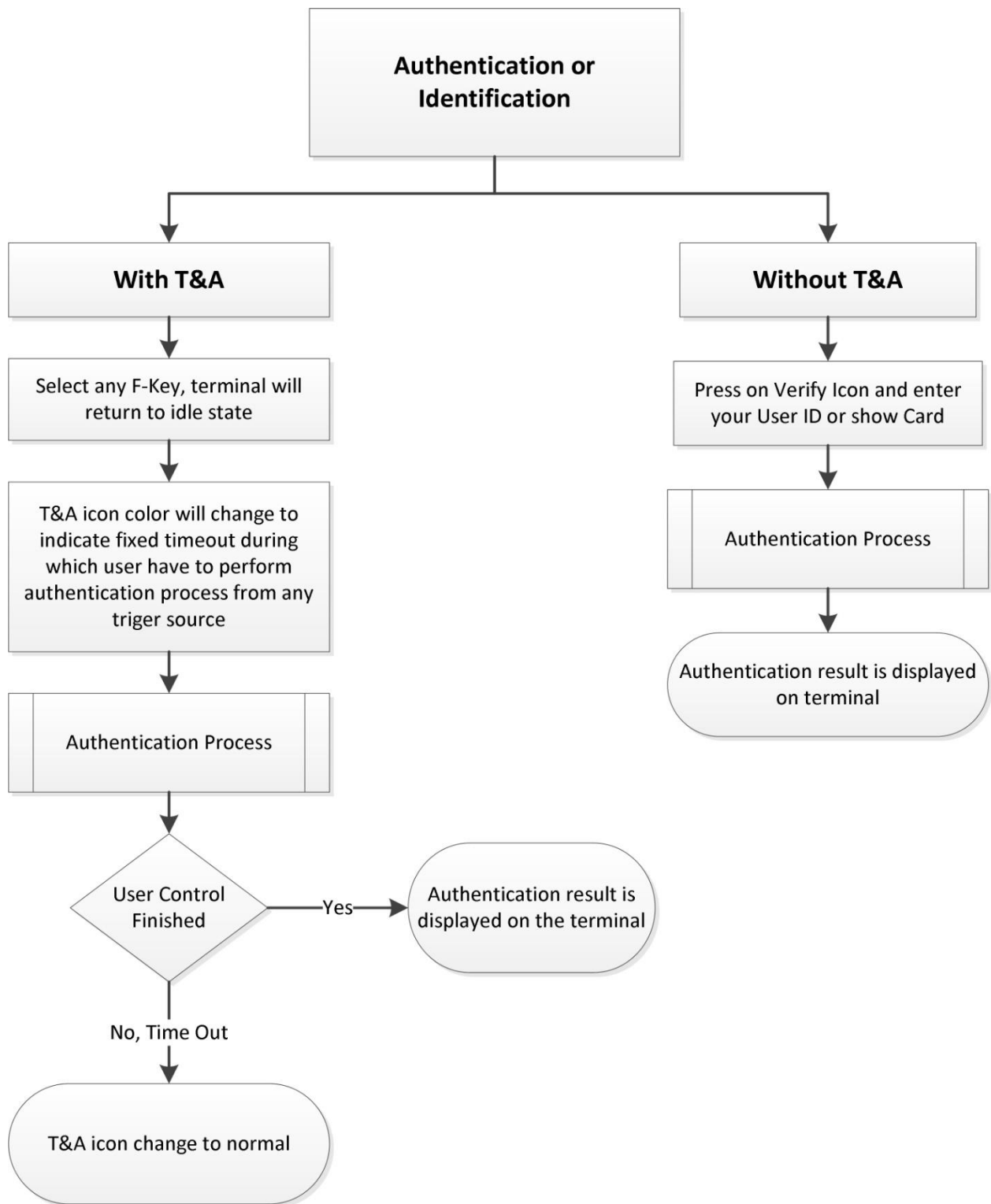


Figure 347: Time and Attendance in Non-Mandatory Mode Workflow Diagram

Note on Terminal Clock Deviation

The terminal clock has a +/- 4 sec per day typical time deviation at +25°C. At 50°C, the time deviation may be up to -8 sec per day.

For application requiring time precision (such as SSL, DESFire®), MorphoAccess® SIGMA Series terminal clock must be synchronized regularly with an external reliable clock.

Section 14 : Proxy Mode

Presentation of Proxy (or slave) mode

Process

This operating mode allows to control the MorphoAccess® SIGMA Series terminal remotely (the link is IP or RS422) using a set of biometric and databases management commands.

In Proxy mode the access control is performed remotely by the Host System: the MorphoAccess® SIGMA Series terminal works as a slave waiting for external commands such as:

- user identification,
- user verification,
- relay activation,
- read data on a contactless smart card,
- Biometric database management,
- terminal configuration changes,
- read an entry from the keyboard,
- display a message,
- read a contactless smart card.

The MorphoAccess® SIGMA Series terminal is driven through an Ethernet (or Wi-Fi™) link using TCP or SSL protocol.

The terminal acts as a server: it is either waiting for a command or executing a command.

Please refer to **MorphoAccess® Host System Interface Specification**: this document explains how to remotely manage a terminal.

For further details about SSL on the MorphoAccess® SIGMA Series terminal, please refer to the **SSL Solution for MorphoAccess® documentation**.

Local signals

When the terminal is waiting for a command from the distant system, there is no local signal (biometric sensor backlight off, status light off).

But when a command is in progress the terminal emits the signals related to the function.

It means, for example, that:

- when the Identify command is in progress, the terminal displays the same signals as the standalone Identification mode,
- when the terminal receives the “access granted” command from the distant system, it emits the “access granted” signal as described in the “Access Request Result”
- The local signals are described in the “Terminal User Interface” section.

Proxy mode use sample

When terminal is in proxy mode, then using distant commands an administrator can control several functions of the terminal. For example, realize the backup of terminal database, an administrator can activate proxy mode of the terminal, do a backup of database in the remote server, and deactivate the proxy mode.

Within proxy mode, none of the actions can be performed using terminal LCD touch screen.

The sample below describes a typical exchange between the terminal and the distant system for a basic access control by identification driven by the distant system.

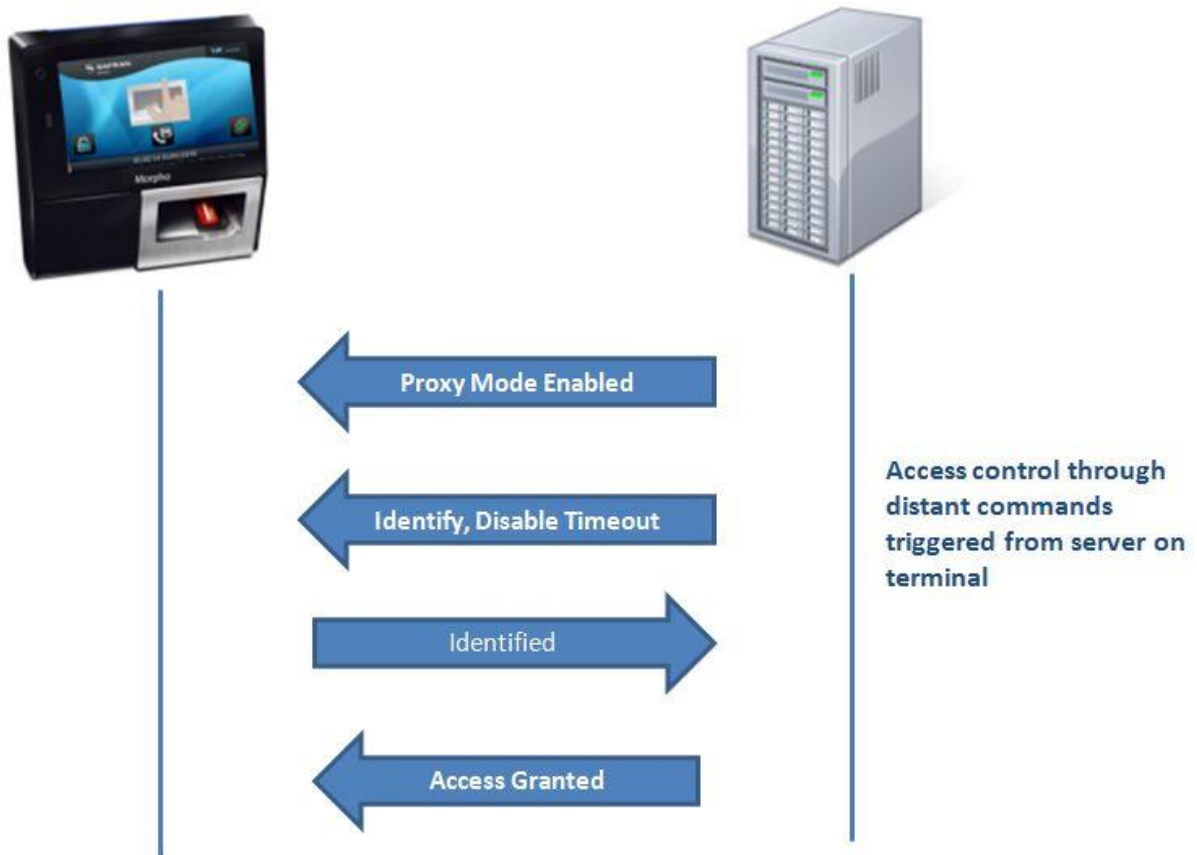


Figure 348: PROXY sample with a remote Identification process

Proxy mode activation

Proxy mode can be enabled using distant command through a server connected to terminal using serial channel.

Please refer to **MorphoAccess® Host System Interface Specification**: this document explains how to remotely manage a terminal using distant commands.

Section 15 : Polling Mode

Presentation of Polling mode

When polling mode is activated, the MorphoAccess® SIGMA Series terminal does not verify user template in its local database. This mode is useful when the user templates are stored in external database.

When authentication is initiated on the terminal, the terminal will expose the User ID to external controller via polling buffer; the terminal accepts distant commands that provide a reference, overriding the reference specified in parameter `ucc.user_record_reference`, the `ucc.allow_fallback_rule` and the user `ref_check` rule.

- If `ucc.per_user_rules` = 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` = Terminal then user rule provided by distant command will be used.
- If `ucc.per_user_rules` = Disabled then user rule check is disabled.

Process

Polling using buffer:

- The user's input ID will be queued in the terminal's queue, which is polled by external application.
- External application waits for the User ID by polling the buffer. After getting an ID, it will search the template in database and send template to terminal for further authentication.
- The user is authenticated by the external terminal and granted access accordingly.

MorphoAccess® SIGMA Series terminal also has distant commands to retrieve polling buffer status and polling buffer data. Refer to **MorphoAccess® SIGMA Series Host System Interface Specification** guide.

Polling mode activation

Polling mode can be activated through Webserver > Complete Configuration, by setting “**ucc.enable_external_database**” parameter value as ‘1’. Only an administrator can activate polling mode. An administrator can refer to **MorphoAccess Sigma Series_Parameters User Guide** to know how to set this parameter.

NOTE: When terminal is in L1 legacy mode, then polling mode can be configured using Secure Admin application.

Section 16 : Messages Sending

Principle

When specific events occurred during the MorphoAccess® SIGMA Series terminal access control application's working, some messages can be generated and sent to another physical entity.

The events that produce messages sending are:

- Result of access rights check (after access request by a user)
- Internal log file full
- Tamper detected
- Time and Attendance actions
- Duress Finger detected

Please refer to **MorphoAccess® SIGMA Series Remote Messages Specification** for details about the messages content.

Events

MorphoAccess® SIGMA Series terminal allows an administrator to select several events on which messages can be sent to external controller. An administrator can enable or disable events using Webserver or distant command.

Refer to “[Event Configurations](#)” under Webserver section in this document, to learn more on various events that can be selected.

Sending Interfaces

The terminal allows choosing the number of interfaces that will be available for the messages sending process.

By default, no interface is available. Set below parameter for activating remote message sending:

| Number of available interfaces | |
|--|--|
| <i>Remote_msg_conf.send_ethernet_state</i> | <ul style="list-style-type: none"> This parameter can be set as “1” to enable message sending over Ethernet |
| <i>Remote_msg_conf.send_serial_state</i> | <ul style="list-style-type: none"> This parameter can be set as “1” to enable message sending over Serial |

For each interface available, the following parameters are customizable:

- Communication layer
- Protocol used
- Parameters depending on the layer and the protocol used.

There is TCP protocol on the IP layer that is available. In that case, the parameters available are for host 1 are as below:

| TCP parameters | |
|---|--|
| <i>remote_msg_ip_conf.host_1_ip</i> | The distant IP address to contact |
| <i>remote_msg_ip_conf.host_1_port</i> | The distant port to connect to |
| <i>remote_msg_ip_conf.host_1_protocol</i> | Protocol Type used for communication through TCP channel |
| <i>remote_msg_ip_conf.host_1_timeout</i> | Timeframe within which terminal is required to connect with host 1 remote controller and read/write the commands |

The same parameter is configurable for host 2, in case terminal is not able to connect to host 1 server, and then it will attempt to send message on host 2. Please refer to **MorphoAccess® SIGMA Series Parameters Guide** for further details about the interfaces configuration.

Section 17 : Compatibility with an Access Control System

Internal Relay activation on Access Granted result

Description

If the result of the access rights check is successful, the internal relay may be optionally activated, for example, to directly trigger a door switch.

The duration of the activation of the internal relay can be modified by a specific configuration key.

Access control installation using internal relay offers a lower security level, than an installation with a central access controller which is the only one allowed opening the door.

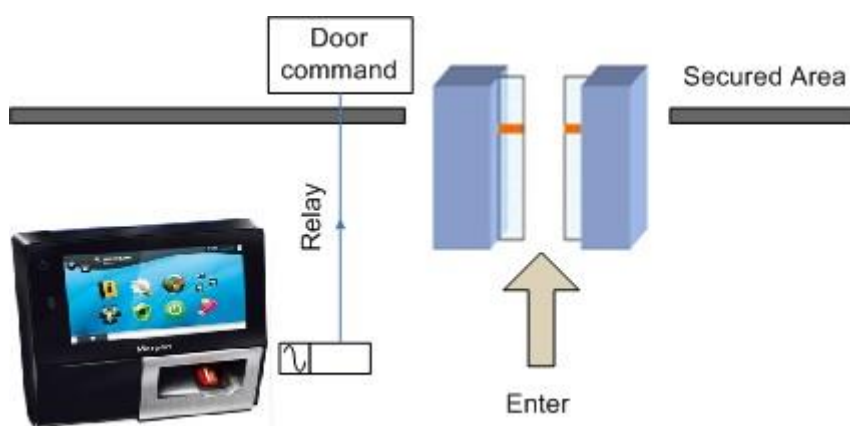


Figure 349: Using the internal relay on the MorphoAccess® SIGMA Series terminal

Activation key

Configuration key enables internal relay activation on access granted is:

| Parameter name | Value | Description |
|-------------------------------|--------|---|
| gpio.sdac_relay_default_state | 0 or 1 | <p>Using this parameter, an administrator can set a default state of the internal relay, which is powered or unpowered.</p> <p>Select “0” for Low. It indicates that by default the internal relay will be unpowered and on access granted the internal relay state will change to high (it will be powered).</p> <p>Select “1” for High. It indicates that by default the internal relay will be powered and on access granted the internal relay state will change to low (it will be powered off).</p> |

Configuration key

| Parameter name | Value | Description |
|---------------------------|-----------------------------|--|
| gpio.sdac_door_unlock_dur | 2 - 60 sec. (25-Default) | <p>Configuration for duration for which SDAC door should be opened after access is granted. This parameter can be set only when gpio.func_mode is set as “2” (SDAC).</p> |

External activation of the internal relay

Description

This function allows the activation of the terminal internal relay via a push button connected between the LED1 and the GND wires. Then the internal relay is activated in two cases: when the terminal authorizes the access after access rights check, and when a contact is closed between the LED1 and GND terminals.

A typical application of this feature is to open the door from inside an area protected by a MorphoAccess® SIGMA Series terminal (as described in figure below):

- to enter in the protected area the user must be successfully recognized by the MorphoAccess® SIGMA Series terminal,
- to exit from the protected area, the user presses a simple push-button connected between the LED1 and GND wires of the MorphoAccess® SIGMA Series terminal.

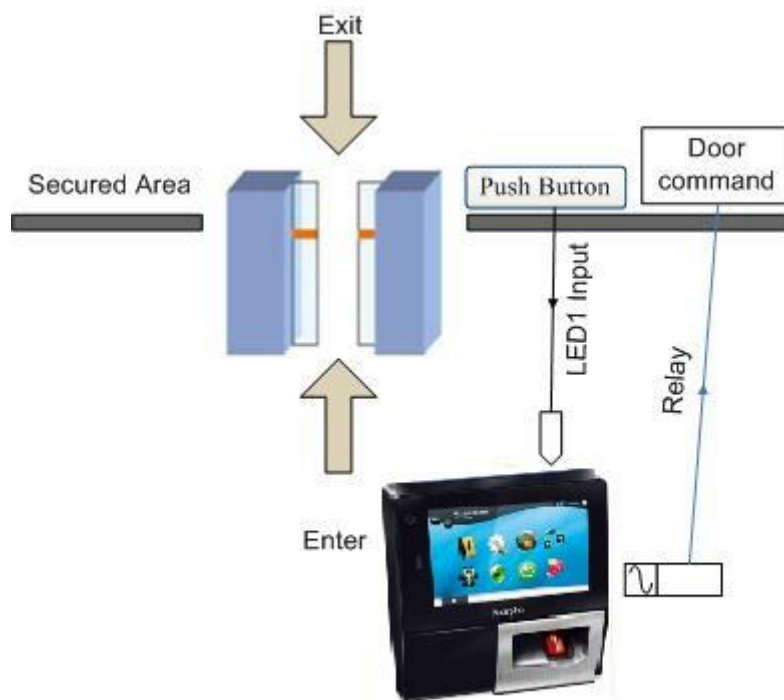


Figure 350: Internal relay activated by LED 1 signal

Activation key

A specific configuration key enables this feature.

| Parameter name | Value | Description |
|--------------------|-----------|---|
| gpio.sdac_rte_mode | 0, 1 or 2 | Using this parameter, an administrator can set an exit mode in SDAC. Following parameter values can be configured: <ul style="list-style-type: none">• Parameter value “0” means None• Parameter value “1” means Push Button. Push button exit mode is selected when a push button is located at exit gate and users are allowed push the exit button to open the exit door. |

Configuration key

| Parameter name | Value | Description |
|------------------------------|---------------------|---|
| gpio.sdac_rte_egress_timeout | 1 to 300 Seconds | Using this parameter, an administrator can define an egress time, the duration for which door will be opened on exit and on timeout door is closed automatically. |

Access Request Result Log File

Description

When enabled, the terminal creates a record for each access request in a local log file. Each record includes:

- the date and the time of record creation (when access control result is known),
- the user's identifier (if available),
- the access control process executed (Identification, Authentication with biometric check, etc.),
- the result of the access control: granted or denied, and if denied for which reason, (user not recognized, outside authorized time slot, etc.),
- and other data used for statistical reasons.

The format of a log record is described in the **MorphoAccess® SIGMA Series Host System Interface Specification** document.

Log File management

Three commands are available for log file management:

- a command which returns the current status of the log feature (enabled/disabled, number of records),
- a command which returns the content of the log file,
- a command that deletes the log file.

For more information about these commands, refer to the **MorphoAccess® SIGMA Series Host System Interface Specification** document.

Log File size

The capacity of the internal log file is customizable up to 1,000,000 records by installing “Logs licenses” (default value is 100,000).

When the file is full, the log will stop automatically and, depending on the terminal settings, a WARNING message may be sent to a remote system.

The format of the “Log File Full Warning” message is described in the **MorphoAccess® terminals Remote Messages Specification** document.

Activation key

The creation of a record for each access request is enabled (and disabled), by only one configuration key.

| Parameter name | Value | Description |
|-------------------------|-----------|---|
| transaction_log.logging | 0, 1 or 2 | <p>This parameter allows an administrator to set transaction log logging status, as below:</p> <ul style="list-style-type: none">• Set parameter value “0”, to disable transaction logging• Set parameter value “1”, to enable access control logging. It means only user access accepted and rejected, along with timings and profile details are logged.• Set parameter value “2”, to enable full logging. Full logs include record of each action performed on terminal. |

Sending an Access Control Result Message

Presentation

After access control rights check, the MorphoAccess® SIGMA Series terminal can send a message which contains the result of the control, to a distant terminal. The MorphoAccess® SIGMA Series terminal is able to use different channels and different protocols, to send this message.

This message can be used for different actions, depending on the role of the receiver in the access control system: simple logging of access requests (no response expected), or performing additional checks on access rights (expected response: access authorized or denied).

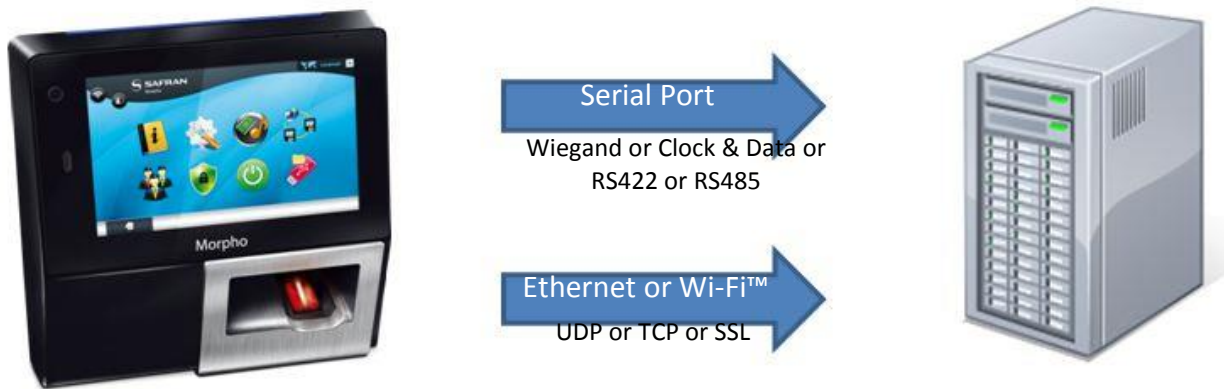


Figure 351: Sending access control result message to a distant system

Ports and protocols

The MorphoAccess® SIGMA Series terminal is able to send the access control result messages to a distant system, using the following ports and protocols:

- Serial Port : Wiegand or Clock & Data or RS485 or RS422,
- Ethernet or Wi-Fi™ link: UDP or TCP or SSL.

This is detailed in the next sections.

Please refer to **MorphoAccess® terminals Remote Messages Specification** for more information about the format and the protocol of the access control result messages.

Serial Port (Output only)

Protocol selection

MorphoAccess® SIGMA Series terminal has two serial ports:

- One for Wiegand or Clock & Data protocols
- One port for RS485 or RS422 protocols

Wiegand protocol

The Wiegand frame includes only the User Identifier (which must be a numeric value).

By default, the message is sent only when the local access control result is positive (access authorized). But this message can also be sent when the result is negative (access denied). In this case, the User Identifier is replaced by an error code indicating the reason for access denial.

The activation and format of the outgoing Wiegand frame can be configured by the user through Webserver. Refer to "[Wiegand Parameters Settings](#)" under Webserver.

An administrator can also configure using below parameter:

| Parameter name | Value | Description |
|-----------------------------------|--------|--|
| wiegand.external_port_output_type | 0 or 1 | This parameter allows an administrator to set an external port output type. Below are parameter values that can be selected: If an administrator set "0", it indicates external port type is Wiegand. |

Clock & Data protocol

The description provided for Wiegand protocol (see previous section) applies also to Clock & Data protocol.

The sending of the message is conditioned to only one configuration key.

| Parameter name | Value | Description |
|-----------------------------------|--------|---|
| wiegand.external_port_output_type | 0 or 1 | This parameter allows an administrator to set an external port output type. Below are parameter values that can be selected: If an administrator set “1”, it indicates external port type is clock & data. |

RS422/RS485 protocol

The message is sent whatever the control result is, and it contains more information than the Wiegand and the Clock & Data frames:

- date and time
- User Identifier (if available),
- result from the local access right (authorized, denied, reason for deny).

The sending of the message is conditioned to the following configuration keys:

| Parameter name | Value | Description |
|-----------------------------------|--------|--|
| remote_msg_conf.send_serial_state | 0 or 1 | Using this parameter, an administrator can select remote message sending state over Serial channel. Select parameter value as “0”, to disable message sending on serial port. Select parameter value as “1”, to enable message sending on serial port. |

Ethernet port

Protocol selection

The protocol used to send the message through the Ethernet link, must be only one of these protocols: UDP or TCP or TLS/SSL.

MorphoAccess® SIGMA Series terminal is able to send message to two different distant system: one preferred (host # 1) and one alternate (host #2).

| Parameter name | Value | Description |
|--|-----------|--|
| remote_msg_ip_conf.host_1_protocol or remote_msg_ip_conf.host_2_protocol | 0, 1 or 2 | Using this parameter, an administrator can set a protocol type that will be used for communicating with remote controller host 1. Below are the values: Set “0”, for using TCP protocol for communication Set “1”, for using UDP protocol for communication Set “2”, for using TLS/SSL over TCP for communication |

For details on more parameters for sending remote message to access controller, refer to MorphoAccess® SIGMA Series Parameters Guide.

For details about SSL protocol, please refer to **SSL Solution for MorphoAccess®** document.

Wi-Fi™ Channel

Instead of Ethernet connection, the terminal can be connected using a wireless Wi-Fi™ b/g connection. Please refer to “Wi-Fi™ Network Configuration” section for more information.

The message format and the protocols supported are the same as the Ethernet channel: UDP, or TCP or SSL.

WARNING: it is not possible for a terminal to be connected through Ethernet and through Wi-Fi™ at the same time.

Note about Terminal Clock Deviation

The message sent through IP and RS422 or RS485 protocols includes the date/time of access control result.

The terminal clock has a +/- 4 sec per day typical time deviation at +25°C.

At 50°C, the time deviation may be up to -8 sec per day.

For features requiring time precision (such as SSL protocol or DESFire® contactless card), the internal clock/calendar of the MorphoAccess® SIGMA Series terminal must be synchronized regularly with an external terminal (using the appropriated ILV command or the MorphoAccess® SIGMA Series terminal administration interface).

Section 18 : Terminal User Interface

Audio Man Machine Interface

Audible signal


The volume of the audible signal can be tuned by a specific configuration key.

| Parameter name | Value | Description |
|----------------|----------|---|
| audio.volume | 0 to 100 | Using this parameter, an administrator can set global audio volume that will be played on specific events. (default value is 50) |

Terminal States


Identification, Authentication or Multi-factor mode: waiting for a finger or a card

- In identification mode, the terminal is waiting for a finger to be placed on the biometric sensor.
- In Authentication mode, the terminal is waiting for a user’s card close to the embedded contactless smartcard reader.
- In multi-factor mode, the identification mode and one of the authentication modes are activated simultaneously. Then the terminal is expecting a finger on the biometric sensor or a card close to the smartcard reader.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | OFF |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


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.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Fixed Red |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


Identification: Finger detected, Acquisition of biometric data of the finger is in process

After detection of a finger on the biometric sensor, the terminal emits this signal during the whole biometric data acquisition (of the finger on the sensor) process. Do not remove the finger while this signal is emitted.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Fixed Red |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


Identification or Authentication: database blank or absent

This signal is emitted when the activated mode requires a database (identification mode, or authentication mode with biometric data in the database) and it isn't created or is empty.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


Proxy mode - waiting for distant system command

When the proxy mode is enabled and when the terminal is expecting for a command from the distant system, there is no local signal.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


Incorrect finger position

The terminal emits this signal when the position of the finger on the biometric sensor is not good enough. Remove the finger from the biometric sensor and follow the recommendations detailed in “Finger Placement Recommendation” section.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |

Biometric Sensor start up error


The terminal fails to start the biometric sensor. If the trouble persists after several terminal start-ups, please contact our customer service.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |

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.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


Terminal in Low Consumption Mode

When terminal is in idle mode, a video is played till configured video play duration. Once Video play duration is reached, terminal stops playing video and shifts to Low Consumption Mode indicated by LED blinking.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | Slow Blue Blinking  |
| Buzzer | None |


Maintenance: Biometric Sensor firmware update

This signal is emitted when the biometric Sensor firmware update is in progress. This update occurs only at first startup of the terminal after terminal firmware update.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


Maintenance: USB mass storage key can be removed

This signal is emitted when the USB Mass Storage key, used to configure the terminal, can be removed from the USB port. The USB Mass Storage key must be removed to complete the maintenance process.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | two medium pitched |

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.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | Low pitched notes |

Access Request Result


Identification or Authentication - Access granted

The user is recognized and the access is allowed.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Not Significant |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | 1 second high pitched Notes |


Identification or Authentication - Access denied

The user is not recognized, or the access is not allowed to this user (by Time Mask feature or by the Central Access Controller).

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Not Significant |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | 1 second low pitched Notes |


Authentication - Timeout while waiting for finger on the sensor

Authentication mode only: time-out occurs during the wait for a finger on the sensor

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Not Significant |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | 1 second low pitched Notes |

Finger removed too early


The terminal emits this signal when the finger is removed before the end of biometric data acquisition (while the finger biometric data acquisition is still in progress).

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Off |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |

Enrolment


Waiting for a finger

The enrolment sequence is launched and the terminal is waiting for a user to place a finger on the biometric sensor.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Fixed Red |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


Acquisition in process

The user has placed a finger on the biometric sensor and is awaiting completion of the acquisition process (notified by the Acquisition complete event).

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Fixed Red |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


Current positioning - Acquisition complete (but not enrolment sequence)

The current acquisition is complete and the user may remove their finger from the terminal.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Fixed Red |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | High 0.5 Sec Beep |


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.

| | |
|-------------------------------------|---|
| Biometric Sensor backlight | Fixed Red |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


Current finger – Acquisition complete (but not enrolment sequence)

The current finger acquisition has completed with success and the user has just removed their finger from the terminal. If acquisition of another finger is required, the terminal will emit the Waiting for finger signal.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Fixed Red |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |


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.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Fixed Red |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |

Enrolment complete – Registration of biometric data in process

The enrolment sequence is complete and registration of biometric data is in process.

| | |
|-------------------------------------|--|
| Biometric Sensor backlight | Fixed Red |
| Status LED (On top of the terminal) | On, Permanent Blue  |
| Buzzer | None |

Section 19 : Compatibility Accessories, Software Licenses and Software Applications

Compatible Accessories & Software Licenses

The following items can be ordered directly to Morpho or to an official distributor, so as to enjoy all the features of an administrator MorphoAccess® SIGMA Series terminal:

- Power supply units,
- Power Over Ethernet module: enabling POE capabilities on the terminal,
- Contactless smartcards: MIFARE® 4K; DESFire® 2K, 4K or 8K, HID iCLASS®, Prox®
- MA WI-FI™ PACK: containing a Wi-Fi™ USB dongle and a Wi-Fi™ license to activate Wi-Fi™ capability on an administrator terminal,
- MA 3G PACK: containing a 3G USB dongle and a 3G license to activate 3G network communication on an administrator terminal,
- User database size licenses (MA_10K_USERS, MA_50K_USERS, and MA_100K_USERS): enabling database size upgrade from 3,000 to 10,000, 50,000 or 100,000 users' capacity (*2 fingers per record) at creation of the database. Requires µSD card in the terminal.
- Log size licenses (MA_250K_LOGS, MA_500K_LOGS, MA_1M_LOGS): enabling logs size upgrade from 100,000 to 250,000, 500,000 or 1,000,000. Requires µSD card in the terminal.
- MA_PAC license: enabling physical access control mode.
- MA_TA license: enabling time and attendance mode.

Compatible software applications

MorphoAccess® SIGMA Series terminals are fully compatible with:

- the low level protocol using thrift commands, for more information refer to “Host System Interface Guide”
- Morpho Integrator’s Kit (MIK) software development kit (version 6 or later).
- M2A management application

Using Legacy Morpho mode, MorphoAccess® SIGMA Series is also compatible with:

- MEMS,
- MIK 5 or later,

With the following limitations:

- Refer to MorphoAccess® SIGMA Series - Legacy Morpho limitations document

Using Legacy L1 mode, MorphoAccess® SIGMA Series is also compatible with:

- SecureAdmin(version v4.1.19.0.0.a10.0 or later),

With the following limitations:

- Refer to MorphoAccess® SIGMA Series - L1 – Bioscrypt Legacy limitations document

Section 20 : Recommendations

Warning

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

General precautions

- Do not attempt to repair the MorphoAccess® SIGMA Series terminal as yourself. The manufacturer cannot be held responsible for any damage/accident that may result from attempts to repair components. Any work carried out by non-authorized personnel will void an administrator warranty.
- Do not expose the terminal to extreme temperature
- Only use the terminal with its original accessories. Attempts to use unapproved accessories with an administrator terminal will void an administrator warranty.
- Due to electrostatic discharge, and depending on the environment, synthetic carpeting should be avoided in areas where the MorphoAccess® SIGMA Series terminal has been installed.

Areas containing combustibles

It is strongly recommended that you do not install your MorphoAccess® SIGMA Series 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 MorphoAccess® SIGMA Series terminals equipped with a contactless smartcard reader at a certain distance (> 30cm) from metallic elements such as iron fixations or lift gates. Performances in terms of contactless badge reading distance will decrease when metallic elements are closer.

SD card

- Even if the SD card is provided with the terminal, we advise an administrator to use Brand name card such as Verbatim.
- Use the class card type 10 for better performances.
- Do not switch SD card from one terminal to another.

Ethernet connection

It is recommended to use a category 5 shielding cable (120 Ohms). It is also strongly recommended to insert a repeater unit every 90m.

Extreme care must be taken while connecting Ethernet wire to the MorphoAccess® SIGMA Series terminal block board since low quality connection may strongly impact Ethernet signal sensibility.

It is recommended to connect Rx+ and Rx- with the same twisted-pair wire (and to do the same with Tx+/Tx- and the other twisted-pair wire).

Date / Time synchronization

If you want to use the MorphoAccess® SIGMA Series terminal for application requiring high time precision, we recommend synchronizing regularly your MorphoAccess® SIGMA Series terminal time with an external clock.

The MorphoAccess® SIGMA Series terminal clock has a +/-10 ppm typical time deviation at +25°C (roughly less than +/- 1 sec per day).

Cleaning precautions

A dry cloth should be used to clean the terminal, especially the biometric sensor.

The use of acid liquids, alcohol or abrasive materials is prohibited.

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)
- The user should not wear glasses. Glasses must be taken off before the identification procedure

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 face)

Annex 1 : Finger Placement Recommendation

Most Useful Areas for Biometric Data

The terminal is designed to capture the area containing the most useful biometric data. In fingerprints, this is usually at the center of the first phalanx.

This is illustrated in the figure below:

Area containing
the maximum
information



Figure 352: Most Relevant Biometric Data in a Fingerprint

The sensor is designed so that when the fingertip is in contact with the rounded hollow guide, the central zone of the first phalanx is aligned with that of the section dedicated to fingerprint capture.

Position of Finger

Finger Height

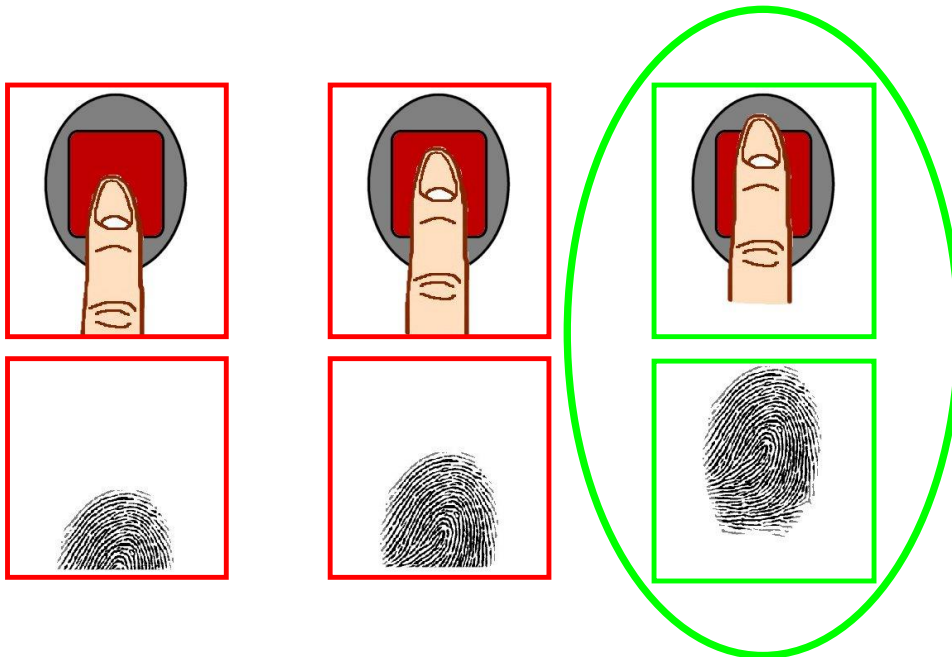


Figure 353: Finger Height

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

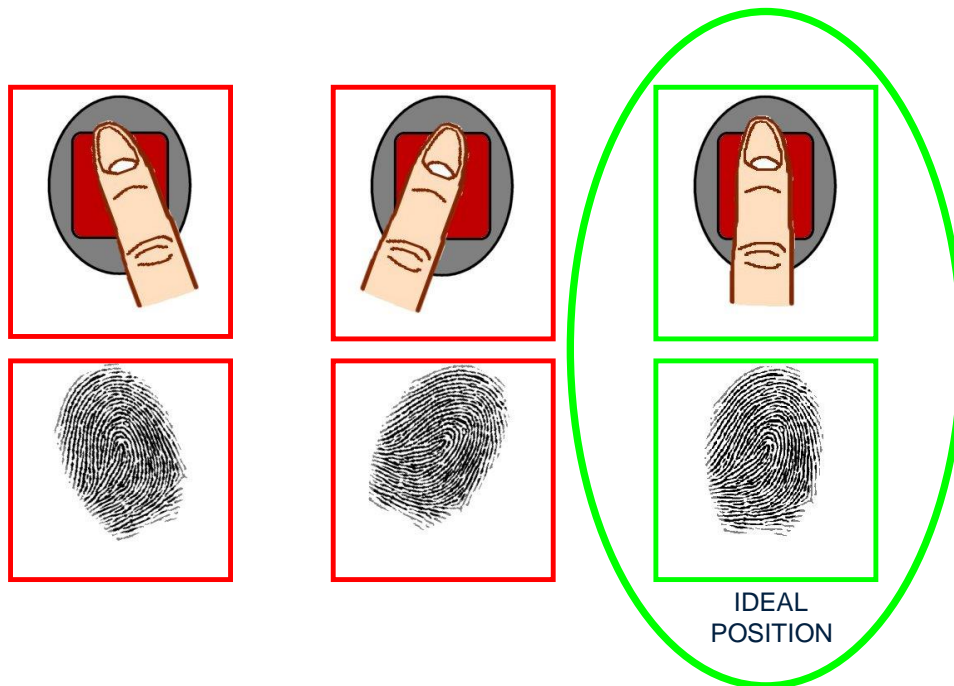


Figure 354: Finger Angle

Incorrect Position:

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

Correct Position:

- The finger must be parallel to sensor sides

Finger Inclination

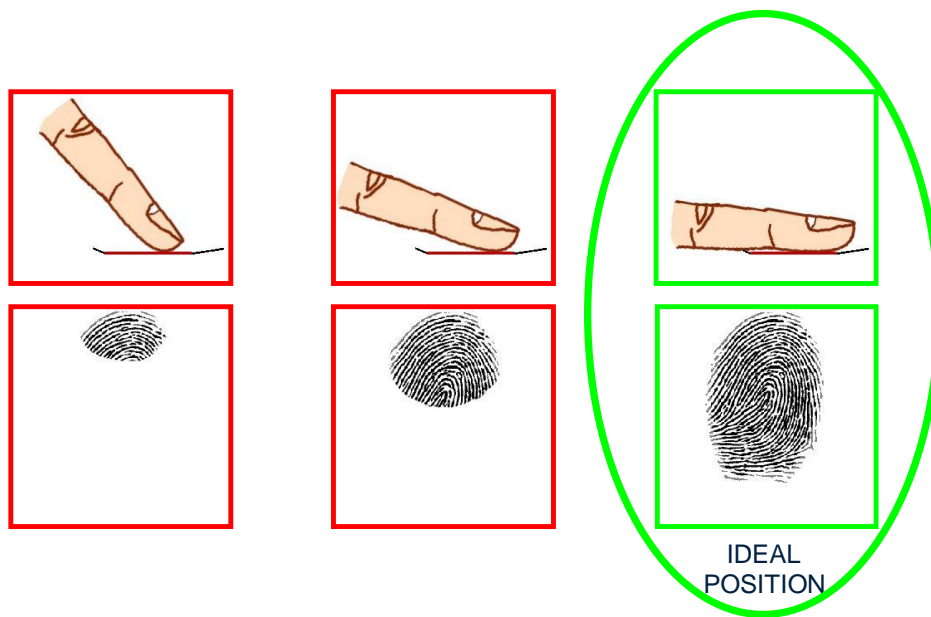


Figure 355: Finger Inclination

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

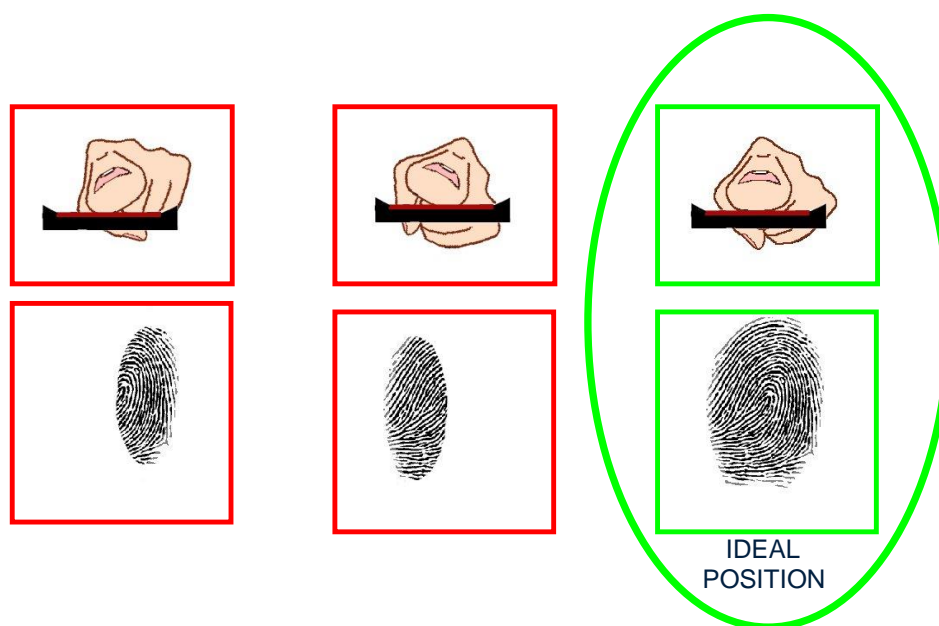


Figure 356: Finger Rotation

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

Annex 2 : Comparison of Authentication mode with Contactless Card

Contactless Modes Table

| Operation | Actions Performed by Terminal |
|---|---|
| Authentication with biometric templates in database | <ul style="list-style-type: none"> • Read ID on contactless card. • Retrieve corresponding templates in database. • Biometric authentication using these templates. • Send ID if authentication is successful. |
| Authentication with biometric templates on card | <ul style="list-style-type: none"> • Read ID and templates on contactless card. • Biometric authentication using these templates. • Send ID if authentication is successful. |
| Card mode authentication | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • Read ID on contactless card. • Send ID. |
| Card mode authentication – biometric control disabled | <ul style="list-style-type: none"> • Read card mode, ID, templates (if required by card mode) on contactless card. • Whatever card mode, send ID. |

Required Tags on Contactless Card

| Operation | ID | CARD MODE | Template 1 | Template 2 | PIN | BIOPIN |
|--|-----|-----------|------------|------------|-----|--------|
| Authentication with templates in database | Yes | No | No | No | No | No |
| Authentication with templates on card | Yes | No | Yes | Yes | No | No |
| Card mode authentication (ID_ONLY) | Yes | Yes | No | No | No | No |
| Card mode authentication (PKS) | Yes | Yes | Yes | Yes | No | No |
| Authentication with templates in database – biometric control disabled | Yes | No | No | No | No | No |
| Authentication with templates on card – biometric control disabled | Yes | No | No | No | No | No |
| Card mode authentication (ID_ONLY) – no PIN code check, no biometric check | Yes | Yes | No | No | No | No |
| Card mode authentication (PKS) – no PIN code check, with biometric check | Yes | Yes | Yes | Yes | No | No |
| Authentication by BIOPIN code check only | Yes | No | No | No | No | Yes |
| Authentication by PIN code check only | Yes | No | No | No | Yes | No |

With :

- ID_ONLY : no PIN code check, no biometric check
- PKS : no PIN code check, with biometric check

Annex 3 : Bibliography

How to get latest version of the documents

The last version of the documents is available on a CD-ROM package from our factory, or can be downloaded from our web site at the address below:

www.biometric-terminals.com

(Login and password required).

To request a login, please send us an email to the address below:

hotline.biometrics@morpho.com

Documents concerning the MorphoAccess® terminal

Document about installing the terminal

MorphoAccess® SIGMA Series Installation Guide,

ref. SSE-00000xxxxx

This document describes terminal physical mounting procedure, electrical interfaces and connection procedures. This document is in English.

Documents about administrating/using the terminal

MorphoAccess® SIGMA Series Administration Guide,

ref. SSE-0000100663-01

This document describes the different functions available on the terminal and procedures for configuring the terminal. This document is in English.

MorphoAccess® SIGMA Series – Morpho Legacy Mode Limitations,

ref. SSE-0000100831-01

This document describes the limitations of MorphoAccess® SIGMA Series terminal operating in Legacy Morpho mode. This document is in English.

MorphoAccess® SIGMA Series – Morpho L-1 Bioscrypt Legacy Mode Limitations,

ref. SSE-0000100872-01

This document describes the limitations of MorphoAccess® SIGMA Series terminal operating in L-1 Bioscrypt Legacy mode. This document is in English.

MorphoAccess® SIGMA Series Quick Start Guide,

ref. SSE-00000xxxxx

This document is a short summarized guide that is used for learning the basic steps for initializing the terminal operations. This document is in English.

Documents for Developer

MorphoAccess® SIGMA Series Parameters Guide,

ref. SSE-00000xxxxx

This document contains the full description of all the configuration parameters for the terminal. This document is in English.

MorphoAccess® SIGMA Series Host System Interface Specifications,

ref. SSE-00000xxxxx

This document describes all the commands supported by a MorphoAccess® SIGMA Series terminal.

MA5G_distant_commands,

ref. SSE-00000xxxxx

This document describes thrift commands supported by a MorphoAccess® SIGMA Series terminal

MorphoAccess® terminal Serial Command Manual

ref. SSE-00000xxxxx

This document details all the distant commands supported by MorphoAccess® 4G terminals and MorphoAccess® SIGMA Series terminals in L1 legacy mode.

MorphoAccess® terminal Command Support Matrix

ref. SSE-00000xxxxx

This document has command support matrix for all MorphoAccess® 4G terminals and MorphoAccess® SIGMA Series terminals in L1 legacy mode.

SSL Solution for MorphoAccess® terminals,

ref. SSE-00000xxxxx

This document describes the activation of the SSL protocol on MorphoAccess® SIGMA Series terminals.

MorphoAccess® SIGMA Series Contactless Card Specifications,

ref. SSE-00000xxxxx

This document describes the contactless cards supported by a MorphoAccess® SIGMA Series terminal. It also describes the format of the data on the contactless card.

MorphoAccess® SIGMA Series Remote Messages Specification,

ref. SSE-00000xxxxx

This document describes the protocols, and the format of the data, supported by a MorphoAccess® SIGMA Series terminal.

Configurations tools user's guide

MorphoAccess® SIGMA Series USB Network Tool User Guide,

ref. SSE-0000043164

This document explains how to use the application that enables to configure the network parameters of a MorphoAccess® SIGMA Series terminal with a USB mass storage key.

MorphoAccess® SIGMA Series USB encoder User Guide,

ref. SSE-0000050386

This document explains how to use the application that enables to configure the MorphoAccess® SIGMA Series terminal with a USB mass storage key.

MorphoAccess® SIGMA Series Terminal License Management,

ref. SSE-0000066855

This document explains how to use the License manager application. This tool enables to read and to load software licenses in a MorphoAccess® SIGMA Series terminal.

Release Note

For each firmware version, a release NOTE is published describing the new features, the supported products, the potential known issues, the upgrade / downgrade limitations, the recommendations, the potential restrictions, etc.

Annex 4 : Glossary, Acronyms and Abbreviation

GLOSSARY

- **Access Controller/Controller:** This term is used for centralized access controller. Terminal communicates with controller for granting or denying access to the user.
- **Terminal:** This term is used for MorphoAccess® SIGMA Series terminal
- **Device:** This term is used for an external device attached to MorphoAccess® SIGMA Series terminal, such as USB Mass Storage device.
- **Admin/Administrator:** A user who is authorized to manage the settings and user information of a fingerprint reader. Administrators can enroll or delete users and change terminal settings.
- **Capacitive Sensor:** A device that detects the voltage differences between the sensing surface and individual fingerprint ridges. MorphoAccess® SIGMA Series terminal supports only Optical Sensor for better biometric performance.
- **Core:** A term used to describe an area of the finger-scan characterized by ridgelines with the tightest curvature and most unique content. Although the entire finger-scan has significant data, the "core" is the most data-intensive area and thus is extremely important to the algorithm. Normally, the core is located in the middle of the fingerprint.
- **Duress Mode:** A mode that offers users a way of indicating a duress situation (such as being forced to open a door). The user verifies with a specially designated finger resulting in an inverted Wiegand output that is detectable on certain Access Control Panels.
- **Finger Print Capture:** The process of extracting features of a fingerprint image obtained from a fingerprint sensor, and saving them into the internal memory of a device. The fingerprint data is called a fingerprint template.
- **User Enrolment:** creation of a record in a database with personal data of a unique user, or creation of a card with personal data of a user
- **Firmware:** The set of programs contained permanently in a hardware device (as read-only memory) that controls the unit.
- **Host Mode:** The normal mode of operation when the device is waiting for a card to be presented to the terminal.
- **Optical Sensor:** A device that detects that detects the intensity or brightness of light. Morpho biometric sensors are used to create graphical representations of fingerprints.
- **Single Door Access Control (SDAC):** The capability of controlling/monitoring all functions related to a single entry/exit point.
- **Software** The set of programs associated with a computer system.

- **Template:** A term used to describe the data that is stored during the enrolment process. The data is a mathematical representation of the ridge pattern of the enrolled finger scan.
- **Primary Template:** This is the template that resides in the first template slot on the smart card. When verification is initiated, this primary template is the first template that is used in that verification process.
- **Secondary Template:** This is an optional second template stored on the smart card that is also used in the verification process if the primary template verification fails.
- **Users:** The individuals that use a hardware system.
- **User Groups:** The sets of users grouped together in a system (usually by the similarity of the functions they perform).
- **1:1 Mode:** In 1:1 mode, a user enters his or her User ID first. Then the user is requested to provide a personal data such as place a finger on a sensor or enter a PIN. Then the acquired data is matched against the reference data linked to user ID (example: fingerprint found on users' card which provides the User ID at beginning of the process).
- **1: N Mode:** In 1: N mode, a user places his or her finger on the device without entering an ID. The terminal compares the user's scanned finger with the many enrolled fingers in its internal database.
- **Identification (Searching or 1:N):** The operation of Identifying a user by comparing a live finger scan against all stored finger-scan records in a database to determine a match. Identification uses the finger scan only - no cards or PINs. Identification is only available on devices that are in 1:N mode.
- **Authentication (1:1):** The operation of confirming a user is who he claims to be by comparing a live finger scan image against a stored fingerprint template. The result (pass or fail) that is returned is based on whether the score is above a pre-defined threshold value. Some type of credential (PIN, Prox card, smart card, etc.) is necessary to initiate the biometric verification.
- **Webserver:** Webserver is a web-based application embedded in the MorphoAccess® SIGMA Series terminal. Webserver enables the management of the settings of the terminal from any computer (desktop, laptop, tablet ...) equipped with a compatible Internet browser and connected to the same network as the terminal.
- **SecureAdmin:** Client software for managing terminal configuration for MorphoAccess® SIGMA Series terminal running in L-1 Bioscrypt Legacy mode

Acronyms and Abbreviations

- **AUX:** Auxiliary
- **LCD:** Liquid Crystal Display
- **LED:** Light Emitting Diode
- **MAC (address):** Media Access Control, a unique identifier assigned to network interfaces for communications on the physical network segment
- **IPv4:** Internet Protocol version 4
- **IPv6:** Internet Protocol version 6 - IPv6 is intended to replace IPv4, which still carries the large majority of Internet traffic (2013).
- **DNS:** Domain Name Server. It provides naming for all systems, computers, terminals in a network
- **DHCP:** Dynamic Host Configuration Protocol
- **TCP:** Transmission Control Protocol
- **UDP:** User Datagram Protocol
- **SSL:** Secure Sockets Layer
- **VIP:** Very Important Person. The users in the system can be enrolled under VIP list.
- **PIN:** Personal Identification Number
- **BIOPIN:** Biometric Personal Identification Number. The BIOPIN is used for authentication when biometric authentication is not required
- **F Key:** Function Key
- **MA:** MorphoAccess®, a generic name of the physical access control terminals by Morpho.
- **T&A:** Time and Attendance Mode
- **MMI:** Man Machine Interface
- **SDAC:** Single Door Access Control
- **GPIO:** General Purpose Input Output

Annex 5 : Support

Troubleshooting

Customer service

Morpho

SAV Terminaux Biométriques

Boulevard Lénine - BP428

76805 Saint Etienne du Rouvray

FRANCE

Phone: +33 2 35 64 53 52

Hotline

Morpho

Support Terminaux Biométriques

18, Chaussée Jules César

95520 Osny

FRANCE

hotline.biometrics@morpho.com

Phone: + 33 1 58 11 39 19

(9H00am to 6H00pm French Time, Monday to Friday)

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

A login and password are required to access the full site content. If an administrator doesn't have one, please send us an email to the address above to request one.

Contact by email is preferred.

May 2016



Registered Office:

Morpho

11, boulevard Gallieni

92130 Issy-les-Moulineaux – France

www.morpho.com