VisionPass

Quick User Guide

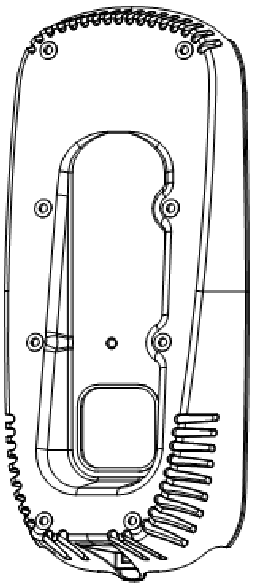
IDEMIA

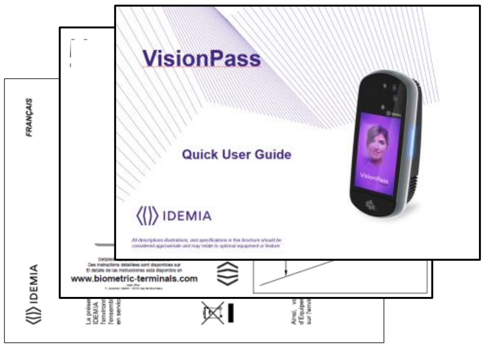
All descriptions illustrations, and specifications in this brochure should be considered approximate and may relate to optional equipment or feature

VisionPass box content

Product packaging checklist:

QTY	ITEM
1	VisionPass terminal
1	Wall Mounting Plate
1	Documentation package





VisionPass

Quick User Guide

IDEMIA

FRANÇAIS

www.biometric-terminals.com

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

Regulatory, safety and environmental notices

Products bearing the CE marking comply with one or more of the following EU Directives as may be applicable:

- Radio Equipment Directive (RED) 2014/53/UE
- RoHS Directive 2011/65/EU.

Compliance with these directives is assessed using applicable European Harmonised Standards.

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-24V and 3 A min (at 12V) in conformity with Safety Electrical Low Voltage (SELV). The AC power supply cable length should not exceed 10 meters.

This system must be installed in accordance with the National Electrical Code (NFPA 70), and the local authority having jurisdiction.

This product is intended to be installed with a power supply complying with IEC 60950-1 or IEC 62368-1 , in accordance with the NEC Class 2 requirements; or supplied by a listed IEC 60950-1or IEC 62368-1 external Power Unit marked Class 2, Limited Power source, or LPS and rated 12VDC, 3 A minimum or 24VDC, 1.5 A 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 Power Ground.

Note that all connections of the VisionPass terminal described hereafter are of SELV (Safety Electrical Low Voltage) type.

This symbol means do not dispose of your product with your other household waste. Instead, you should protect human health and the environment by handing over your waste equipment to a designated collection point for the recycling of waste electrical and electronic equipment.

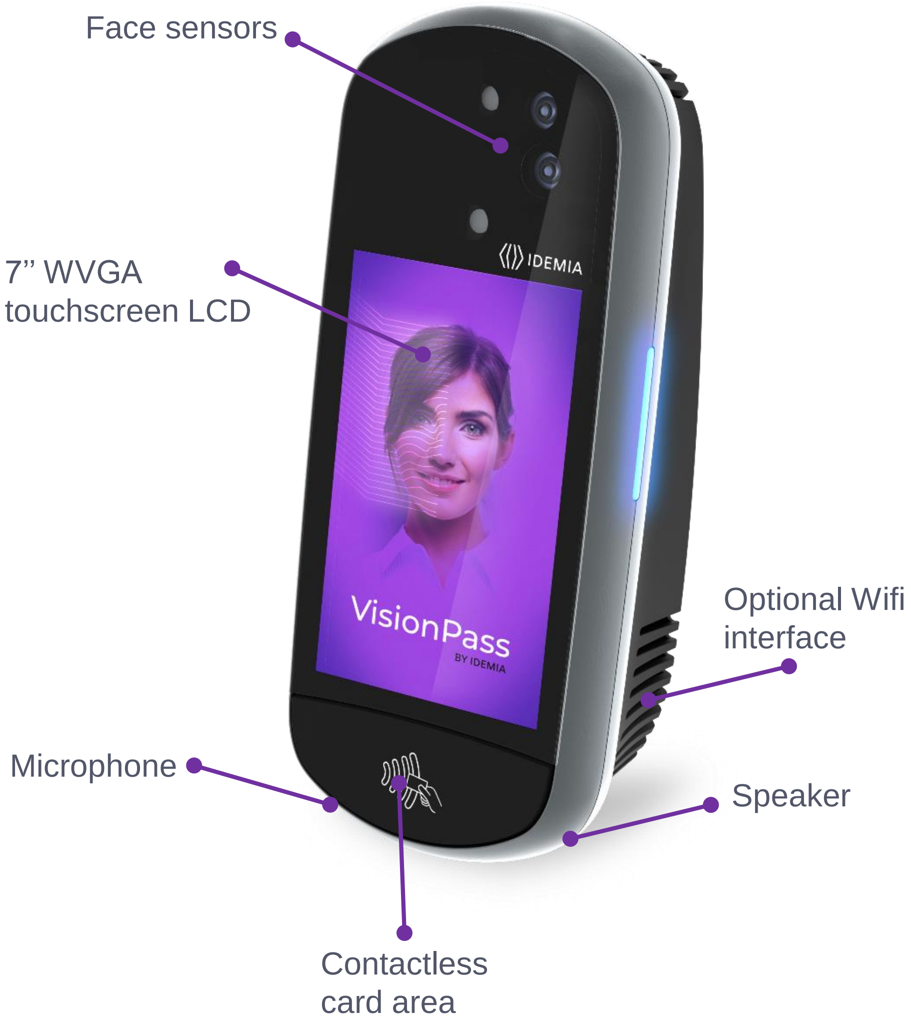
This product is classified as Class 1 Laser Product according to IEC 60825-1 : 2014

Table of Contents

Product Overview

VisionPass provides an innovative and effective solution for access control applications using very fast acquisitions of the face.

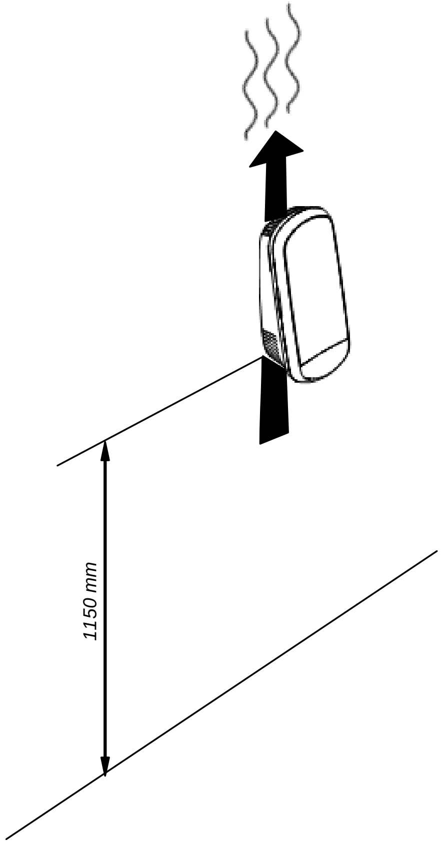
- ◆Access control and Time & Attendance
- ◆Biometric authentication by face acquisition
- ◆Simple and ergonomic man-machine interface
- ◆Contactless card reader (MIFARE Classic, MIFARE Plus, DESFire, HID® Iclass*, HID® PROX*)
- ◆Universal connectivity (Gigabit Ethernet, Wi-Fi™, RS485/422, Wiegand, Dataclock)
- ◆Anti-tamper sensor



* Depending on product version

Step one : overview

Installation recommendations / environment

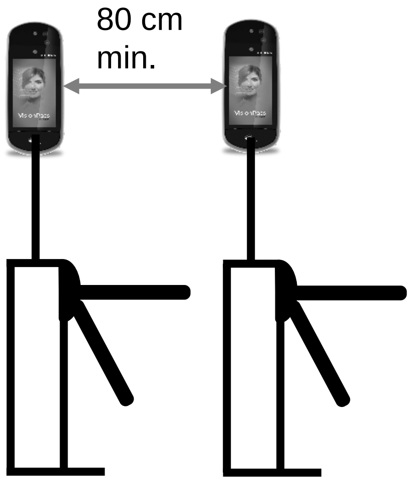


Please install Visionpass terminal vertically at the recommended height, and keep the openings clear to allow air flow.

VisionPass is designed to operate in most environmental conditions. Anyway, to optimize VisionPass performance, it is better to follow the rules below :

- Avoid sunlight coming directly on the device (for instance, avoid installing the device facing a window).
- Avoid direct sunlight on the user's face.
- Avoid strong left/right or top/bottom contrast, and shadows on the user's face due to lighting configuration.
- Prefer a neutral color background in the field-of-view of the product
- Avoid any bright spot light very close to the device (closer than 1 meter)
- Protect the front glass from raindrops as it might affect the sensors

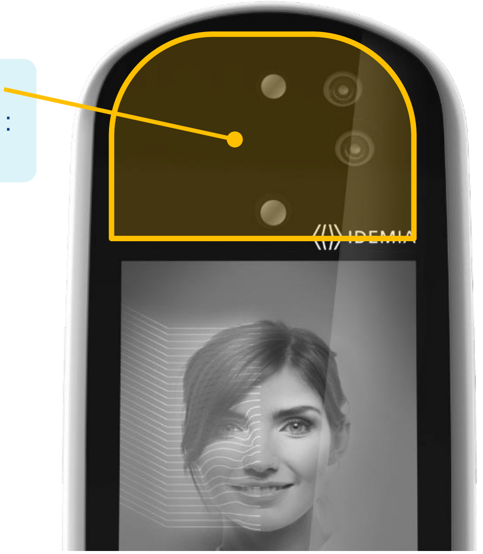
NB : Caution : when operating, the internal radiator may be hot.



If several devices are installed in parallel lanes (typically for gates or turnstiles), then a minimum distance of 80cm must be kept between the devices.

Alternately, devices can be tilted so that one device field of view does not interfere with the other one.

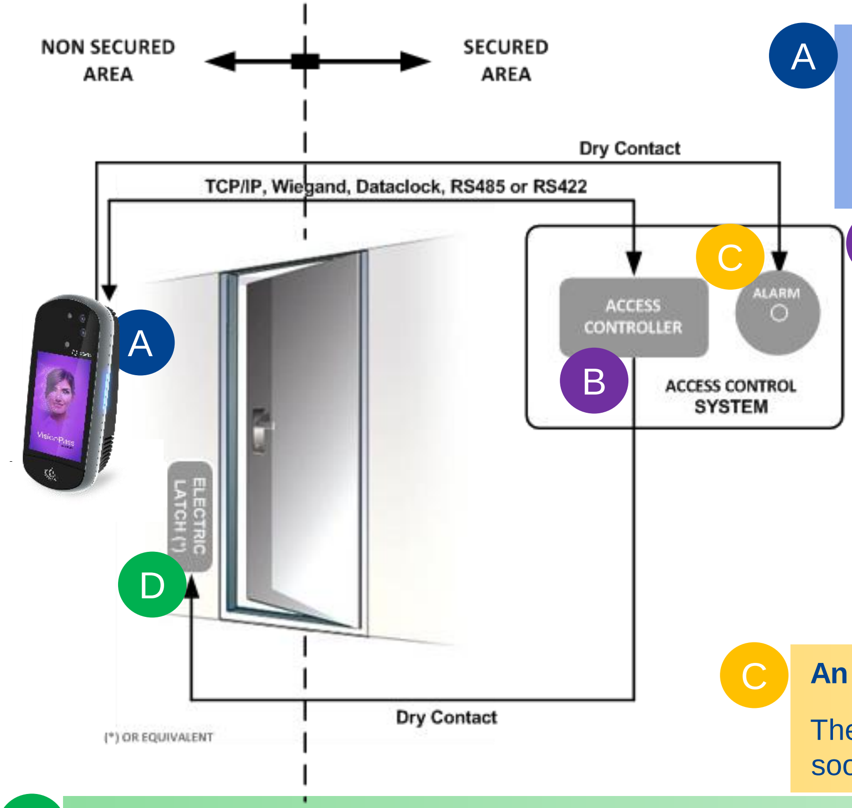
Keep this area clear and clean : no sticker etc.



Step one : overview

Terminal Implementation

To secure an access, IDEMIA recommends installing the VisionPass terminal as a part of a typical Access Control system, which consists of the components described below.



A **The VisionPass terminal**

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

B **An Access Controller (3rd party product)**

The terminal interfaces with an Access Controller (using TCP/IP, Wiegand, Data Clock, RS485 or RS422 protocol):

After access request, the terminal sends the result of user's access rights to the Access Controller (this message contains at least the User ID)

The Access Controller performs additional checks, and returns the final decision (access granted/denied) to the terminal (which displays the result to the user), and to the door controller which opens the door (if the access has been granted).

C **An Alarm (3rd party product)**

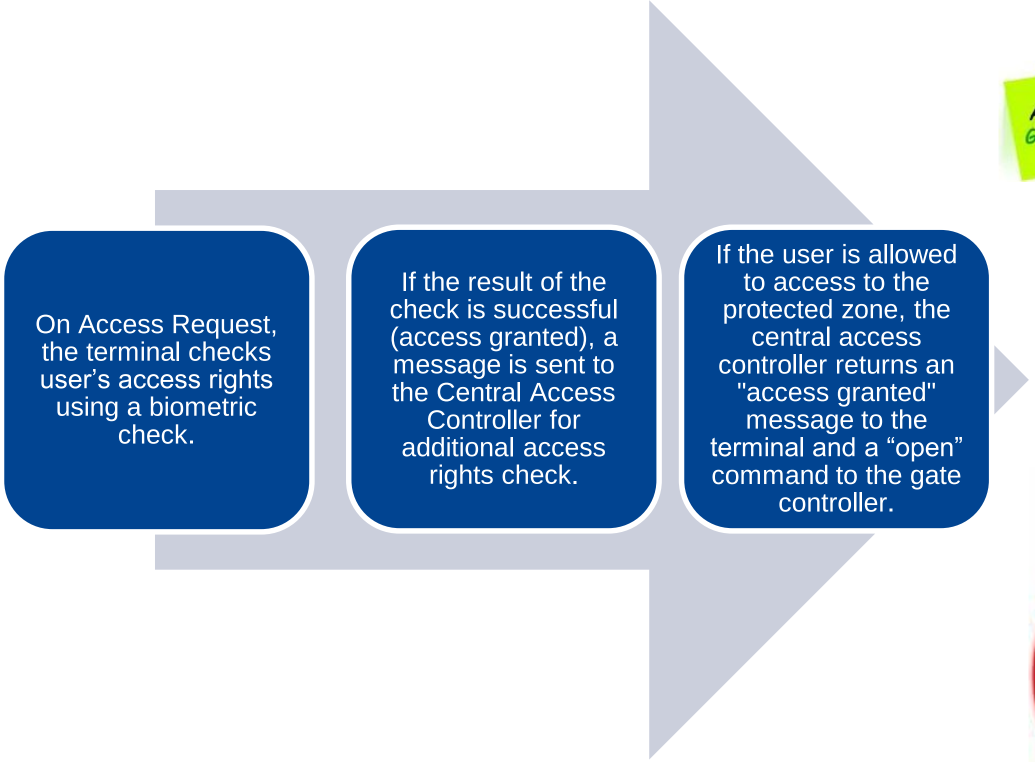
The terminal sends a message to the Access Controller, to activate the Alarm as soon as a malicious activity, such as tamper or pulling, is detected

D **A Door Electric Latch or equivalent (3rd party product)**

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

Step one : overview

Typical Access Control Process



On Access Request, the terminal checks user’s access rights using a biometric check.

If the result of the check is successful (access granted), a message is sent to the Central Access Controller for additional access rights check.

If the user is allowed to access to the protected zone, the central access controller returns an "access granted" message to the terminal and a “open” command to the gate controller.

Note: One user must be enrolled in the terminal database, in order to be able to perform biometric check.

Access Control Modes

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

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

(*) or the user enter their Identifier on the keypad, or a Wiegand frame is received from an external device

(**) stored on the contactless card or in the user record in the terminal's local database

Deployment Environment

Operating temperature	-10° to +45 °C (14°to 113°F)
Operating humidity	10 % < RH < 80 % (non condensing)
Storage temperature	-25°to + 70 °C (-13°to 158°F)
Storage humidity	5% < RH < 95 %

General precautions

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

Areas containing combustibles

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

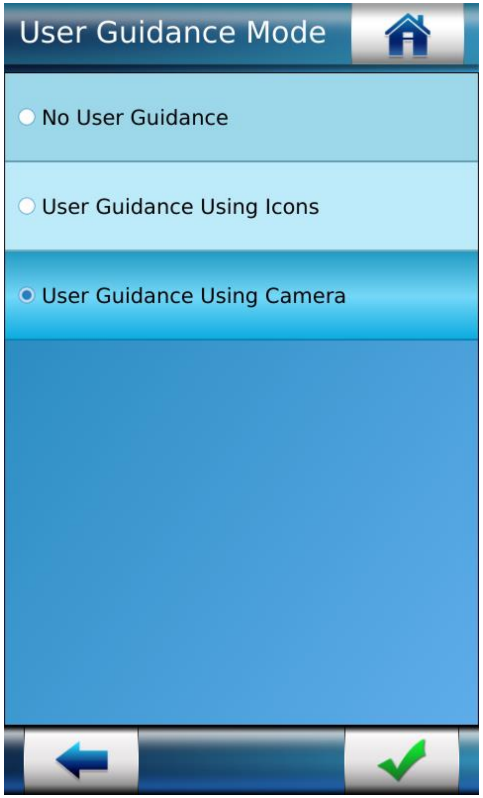
The terminal should be installed in controlled lighting conditions

- Avoid exposure of the biometric sensor to direct sunlight.

The terminal should be installed in controlled area in order to avoid water on the sensor

User Guidance

VisionPass proposes 3 ways to guide the user to best position his / her face for identification.



User Guidance Mode

○ No User Guidance

○ User Guidance Using Icons

● User Guidance Using Camera

No User Guidance : terminal acquisition volume is large enough to allow the user to be recognized easily as soon as he / she looks at it. This way is adapted to daily users.

User Guidance Using Icons : intuitive icons indicate the user to move back or closer, or move left or right.

User Guidance Using Camera : terminal will display a live feedback of the camera

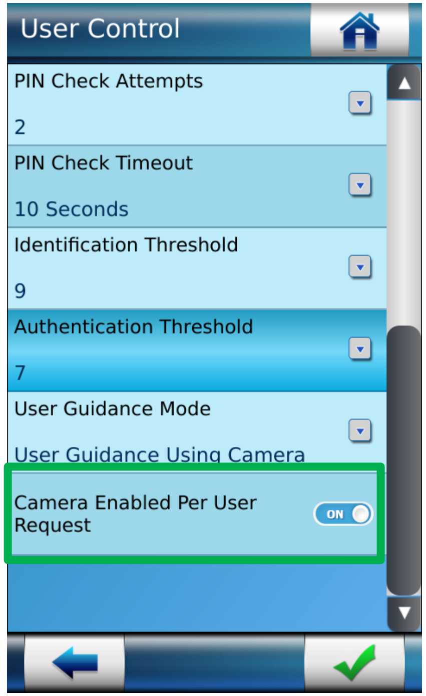
Step one : overview

Deliberate trigger

By default, VisionPass will react when a user enters in the intention area, and will start facial acquisition as soon as a user enters in the coding area and looks at the terminal. Note that the video stream is never recorded by VisionPass.

Even if the video stream is not recorded by the terminal, it can be requested to disable the cameras when they are not necessary, for privacy concerns.
VisionPass can be configured to enable the cameras on user request only :

Activate Camera Enabled Per User Request in the Security settings :



User Control

PIN Check Attempts
2

PIN Check Timeout
10 Seconds

Identification Threshold
9

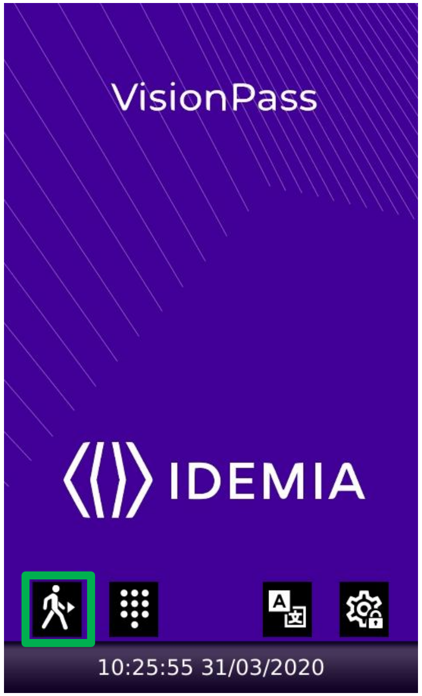
Authentication Threshold
7

User Guidance Mode
User Guidance Using Camera

Camera Enabled Per User Request ON

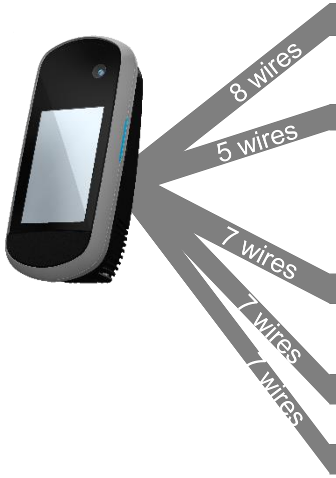
To use the terminal, user has to click on the icon 🚶

Note : cameras will be enabled also by entering ID on keypad or tap the smartcard if theses triggers are enabled



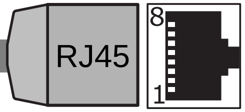
Step one : overview

Wiring Overview



RJ-45 : Ethernet

1	ETH TX+	Orange / White
2	ETH TX-	Orange
3	ETH RX+	Green / White
4		
5		
6	ETH RX-	Green
7		
8		
Shell	ETH GND	Drain wire (no color)



Pin numbers shown in this document correspond to the internal connector pinout in the product. The connector attached to the cable is for test only and should be removed for installation.

RS-422 and 485

7	RS485_RX_A	Blue / Black
8	RS485_TX_Z	Green / White
9	RS485_RX_B	Blue / White
10	RS485_TX_Y	Green / Black
11	RS485_GND	Black / Red

GPIO

19	GPI2	Orange / Black
20	GPO2	Yellow / Red
17	GPI1	Orange / Red
18	GPO1	Yellow / Red
15	GPI0	Orange
16	GPO0	Yellow
22	GPIO_GND	Black / Red

Power supply & Tamper switch

13	RLY_NC	Orange / White
14	RLY_NO	Yellow / White
12	RLY_COM	Grey / White
5	SWITCH_PIN1	Light Blue
6	SWITCH_PIN2	Pink
1,3	Power + 12V	Red
2,4	Power GND	Black

Wiegand IN & Wiegand OUT

25	WIEGAND_LEDOUT1	Blue
28	WIEGAND_LEDOUT2	Blue / Red
23	WIEGAND_IN1	White / Red
24	WIEGAND_OUT0	Green
26	WIEGAND_OUT1	White
21	WIEGAND_IN0	Green / Red
27	WIEGAND_GND	Black / Red

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

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

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

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

Step two : wiring

Power supply

1-3	Power + 12V	Red
2-4	Power GND	Black

External Power Supply: 12-24 V (regulated and filtered) 3A min @12V, IEC60950-1 or IEC 62368-1 standard compliant. If sharing power between devices, each unit must receive 3A (e.g. two units would require a 12 VDC, 6A supply).

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

IDEMIA recommends using a 24V 3A power supply and AWG16 gauge cable. The voltage measured on the product block connector of the terminal must be equal to 12V-24V (-15% / +10%).

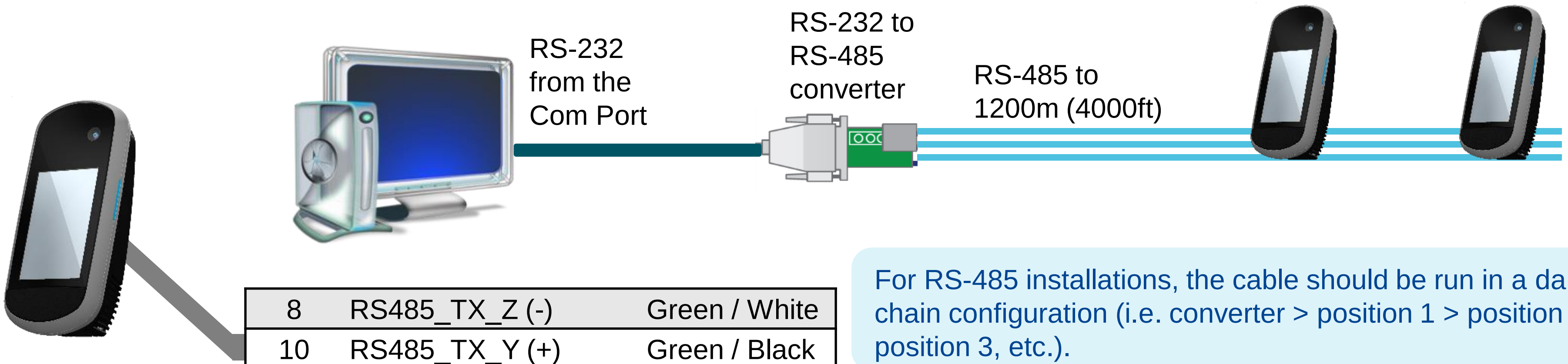
The product requires 36 W at all voltage conditions.

The voltage drop due to the cable shall be taken into account. The table at the right, shows the maximum distance between power supply and 1 unique device, depending on cable gauge and power supply rating.

Gauge AWG	Section (mm^2)	Maximum distance (meters) vs power source rating			
		12 V +/- 10% 3,6 A	12 V +/- 5% 3,5 A	24 V +/- 10% 2 A	24 V +/- 10% 3 A
16	1.31	6 m	12 m	68 m	121 m
18	0.82	4 m	8 m	43 m	76 m
20	0.52	2 m	5 m	27 m	48 m
22	0.32	1 m	3 m	16 m	30 m

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

RS-485 Communication



8	RS485_TX_Z (-)	Green / White
10	RS485_TX_Y (+)	Green / Black
11	RS485_GND	Black / Red

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

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

Use CAT-5 UTP (or better) cable (shielded recommended) with a characteristic impedance of 120 ohms.

AWG 24 should be the minimum wire gauge used.

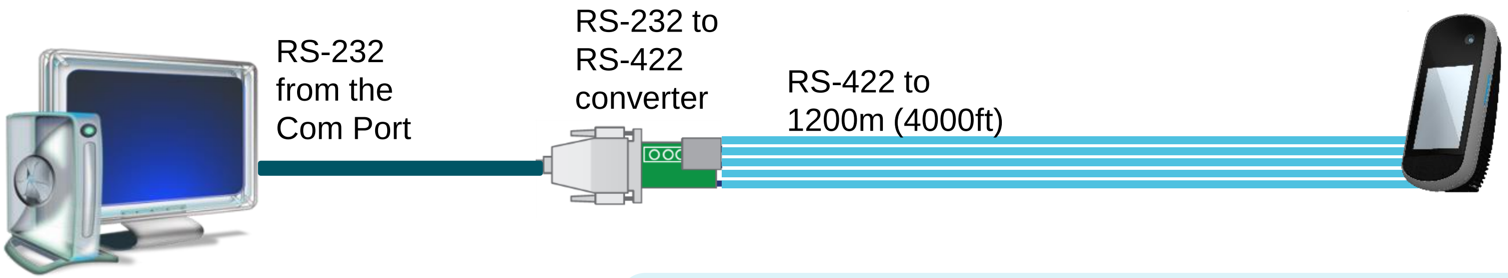
Choose one twisted pair of conductors to use for RS485_TX_Y (TX+, Green / Black wire - 10) and RS485_TX_Z (TX-, Green / White wire - 8). Another conductor should be used for Signal Ground (Black / Red wire - 11).

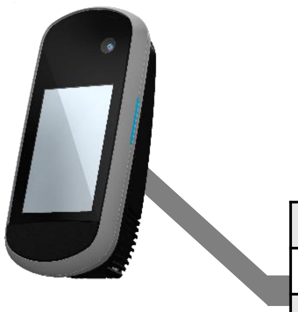
⚠

IMPORTANT:

- A maximum of 31 devices may be installed on the same line.
- The maximum total cable length is 1200m (4000 ft.)
- The cable must be dedicated to this installation and not used for any other purpose

RS-422 Communication





7	RS485_RX_A (RX+)	Blue / Black
8	RS485_TX_Z (TX-)	Green / White
9	RS485_RX_B (RX-)	Blue / White
10	RS485_TX_Y (TX+)	Green / Black
11	RS485_GND	Black / Red

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

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

Choose one twisted pair of conductors to use for RS485_TX_Y (TX+, Green / Black wire - 10) and RS485_TX_Z (TX-, Green / White wire - 8).

Choose one twisted pair of conductors to use for RS485_RX_A (RX+, Blue / Black wire - 7) and RS485_RX_B (RX-, Blue / White wire - 9).

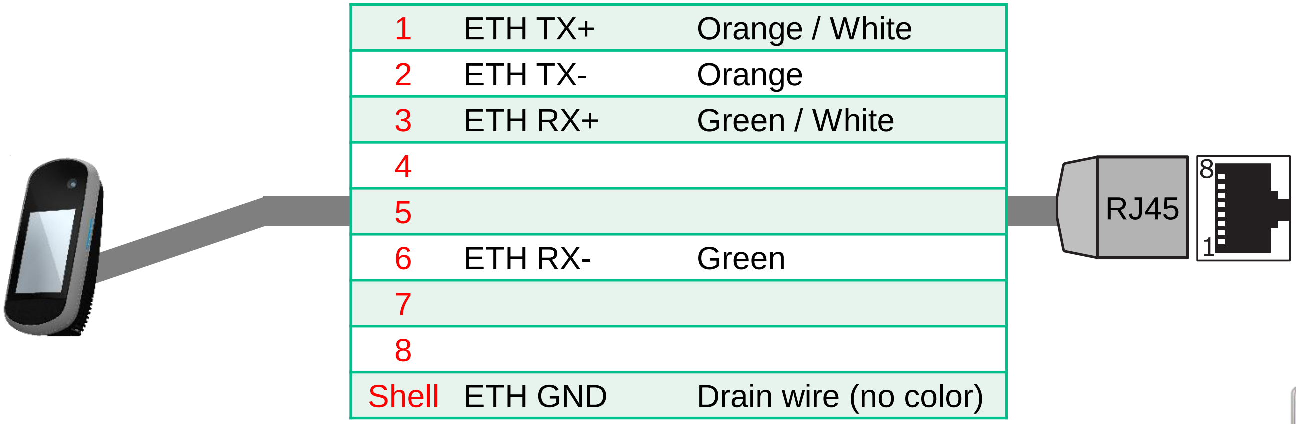
Another conductor should be used for Signal Ground (Black / Red wire - 11).

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

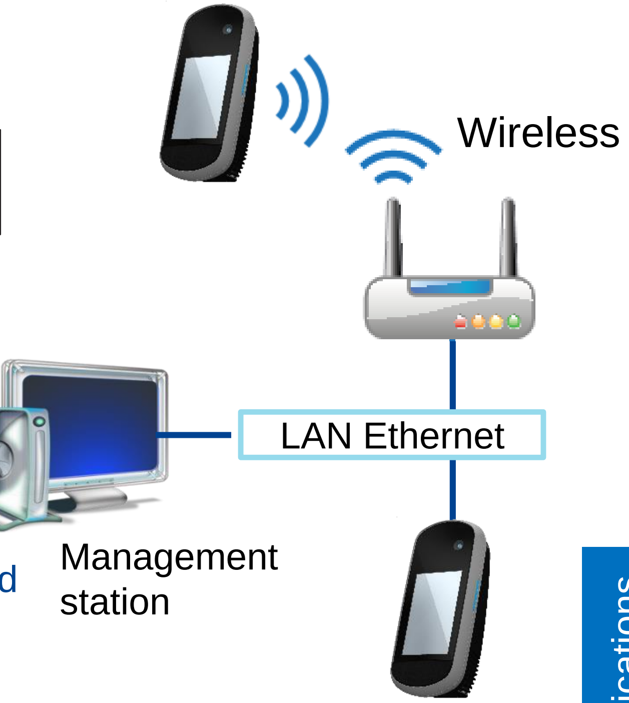
The cable must be dedicated to this installation and not used for any other purpose

Step three : communications

Ethernet and Wireless LAN



1	ETH TX+	Orange / White
2	ETH TX-	Orange
3	ETH RX+	Green / White
4		
5		
6	ETH RX-	Green
7		
8		
Shell	ETH GND	Drain wire (no color)



Use a category 6 shielding cable (120 Ohms) or better. It is strongly recommended to insert a repeater unit every 90 m.

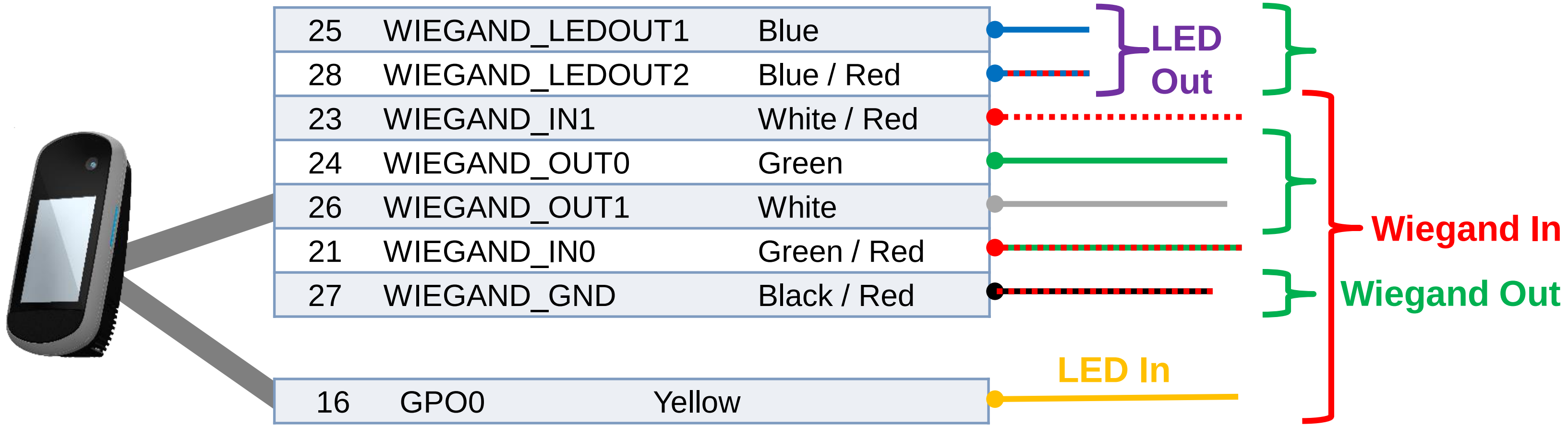
Static mode is enabled by default on VisionPass terminals (factory setting) : IP=192.168.1.10, Gateway=192.168.1.254, Mask= 255.255.254.0

Terminal Block Ethernet connection

- Extreme care must be taken while connecting Ethernet wire to the block board since low quality connection may strongly impact Ethernet signal sensibility.
- Connect Rx+ and Rx- with the same twisted-pair wire (and do the same with Tx+/Tx- and the other twisted-pair wire).

WLAN option
IDEMIA wireless enabled devices support 802.11b and 802.11g standards. WEP Open, WPA and WPA2 are supported.

Wiegand Communication



25	WIEGAND_LEDOUT1	Blue
28	WIEGAND_LEDOUT2	Blue / Red
23	WIEGAND_IN1	White / Red
24	WIEGAND_OUT0	Green
26	WIEGAND_OUT1	White
21	WIEGAND_IN0	Green / Red
27	WIEGAND_GND	Black / Red
16	GPO0	Yellow

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

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

- Connect **WIEGAND_OUT0** (Green wire – Pin 24) to ACP Data 0,
- Connect **WIEGAND_OUT1** (White wire – Pin 26) to ACP Data 1,
- Connect **WIEGAND_GND** (Black / Red wire – Pin 27) to ACP reader common (0vDC).

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

All controller output shall be open drain or 5 V +/- 5%

Step three : communications

Wiegand Communication (continued)

Important

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

Note

On installation, the system administrator will be prompted to select either a pre-existing Wiegand frame format or create a custom format, and upload it to the unit before the first use.

Data Clock

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

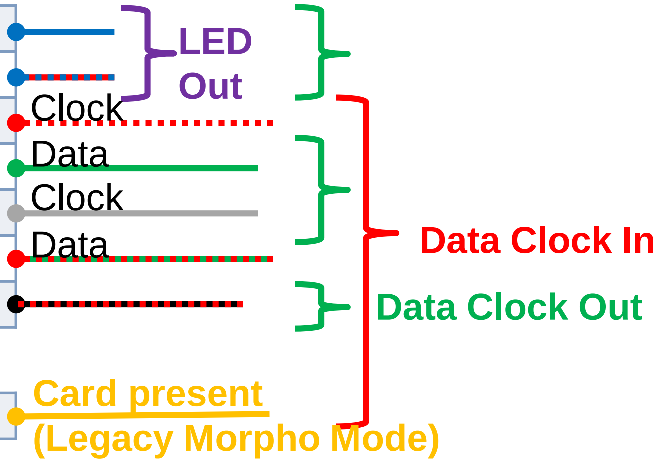
Example Format Information

Type: **Standard 26-bit**

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

25	WIEGAND_LEDOUT1	Blue
28	WIEGAND_LEDOUT2	Blue / Red
23	WIEGAND_IN1	White / Red
24	WIEGAND_OUT0	Green
26	WIEGAND_OUT1	White
21	WIEGAND_IN0	Green / Red
27	WIEGAND_GND	Black / Red

16	GPO0	Yellow



LED Out

Clock

Data

Clock

Data

Data Clock In

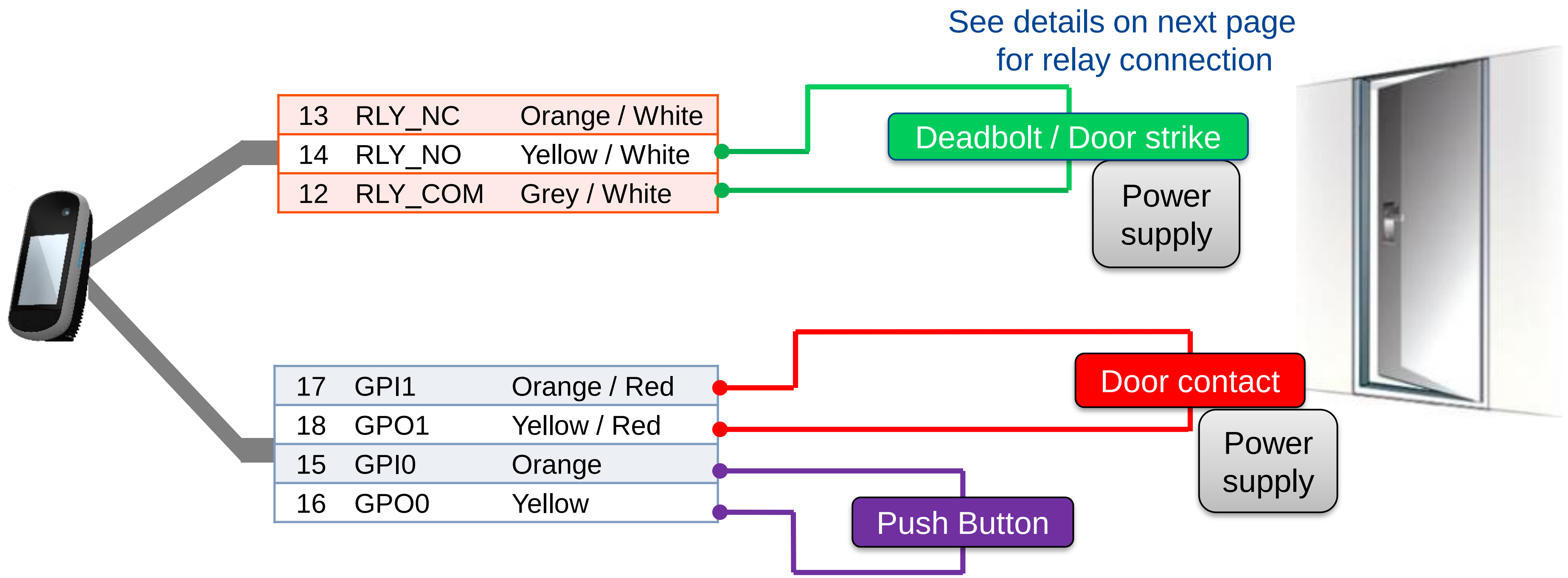
Data Clock Out

Card present

(Legacy Morpho Mode)

Single Door Access Control (SDAC)

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



See details on next page
for relay connection

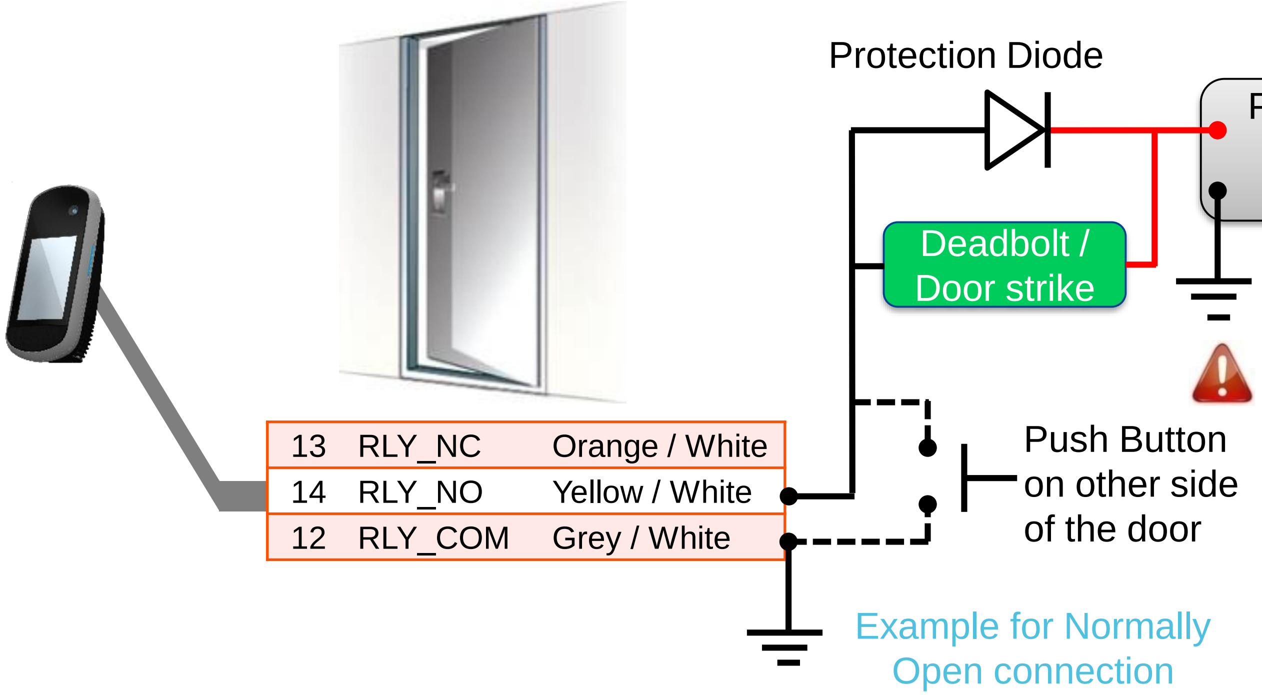
13	RLY_NC	Orange / White
14	RLY_NO	Yellow / White
12	RLY_COM	Grey / White

17	GPI1	Orange / Red
18	GPO1	Yellow / Red
15	GPI0	Orange
16	GPO0	Yellow

⚠ **If door contact is not used, GPI1 (17) and GPO1 (18) shall be connected together**

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

Internal Relay Wiring



13	RLY_NC	Orange / White
14	RLY_NO	Yellow / White
12	RLY_COM	Grey / White

Example for Normally Open connection

Warning

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

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

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

Warning

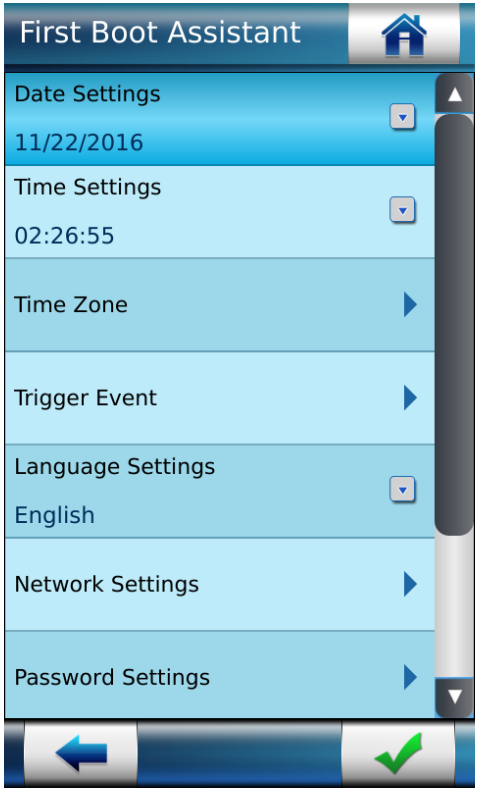
- ➢ **The internal relay is limited to a maximum current of 1A @ 30V. If the deadbolt / door strike draws more than 1A, damage to the device may occur. If the deadbolt / door strike load exceeds 1A, an external relay must be used.**
- ➢ **The internal relay is designed for 100.000 cycles. If more cycles are needed, an external relay driven by GPO must be used.**

Step four: SDAC

Local Administration - First Boot Assistant

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

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



First Boot Assistant

Date Settings
11/22/2016

Time Settings
02:26:55

Time Zone

Trigger Event

Language Settings
English

Network Settings

Password Settings

Main settings managed by FBA

Date & Time & Time Zone Settings

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

Language Settings: user interface language selection,

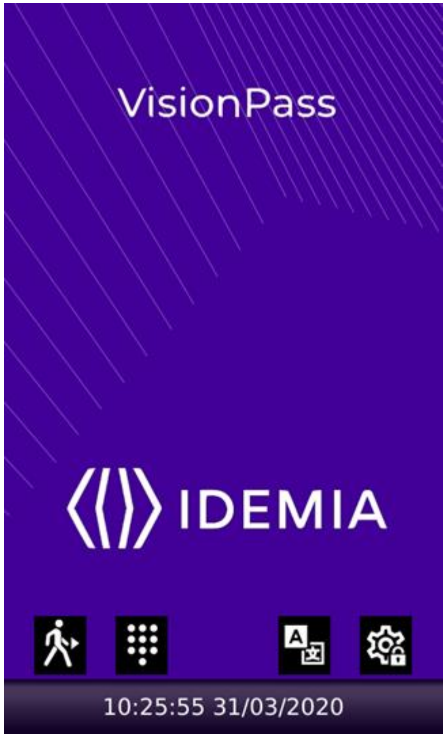
Network Settings: LAN or WLAN parameters

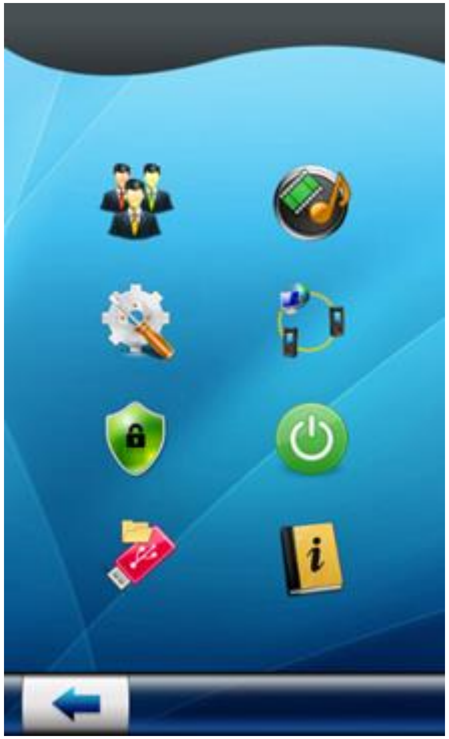
Password Settings: terminal administration password modification

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

Step five: Administration

Local Administration – Using Touch Screen Menu





Press on ⚙ icon to access to administrator menu (default security code is 12345).

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

Frequently used icons

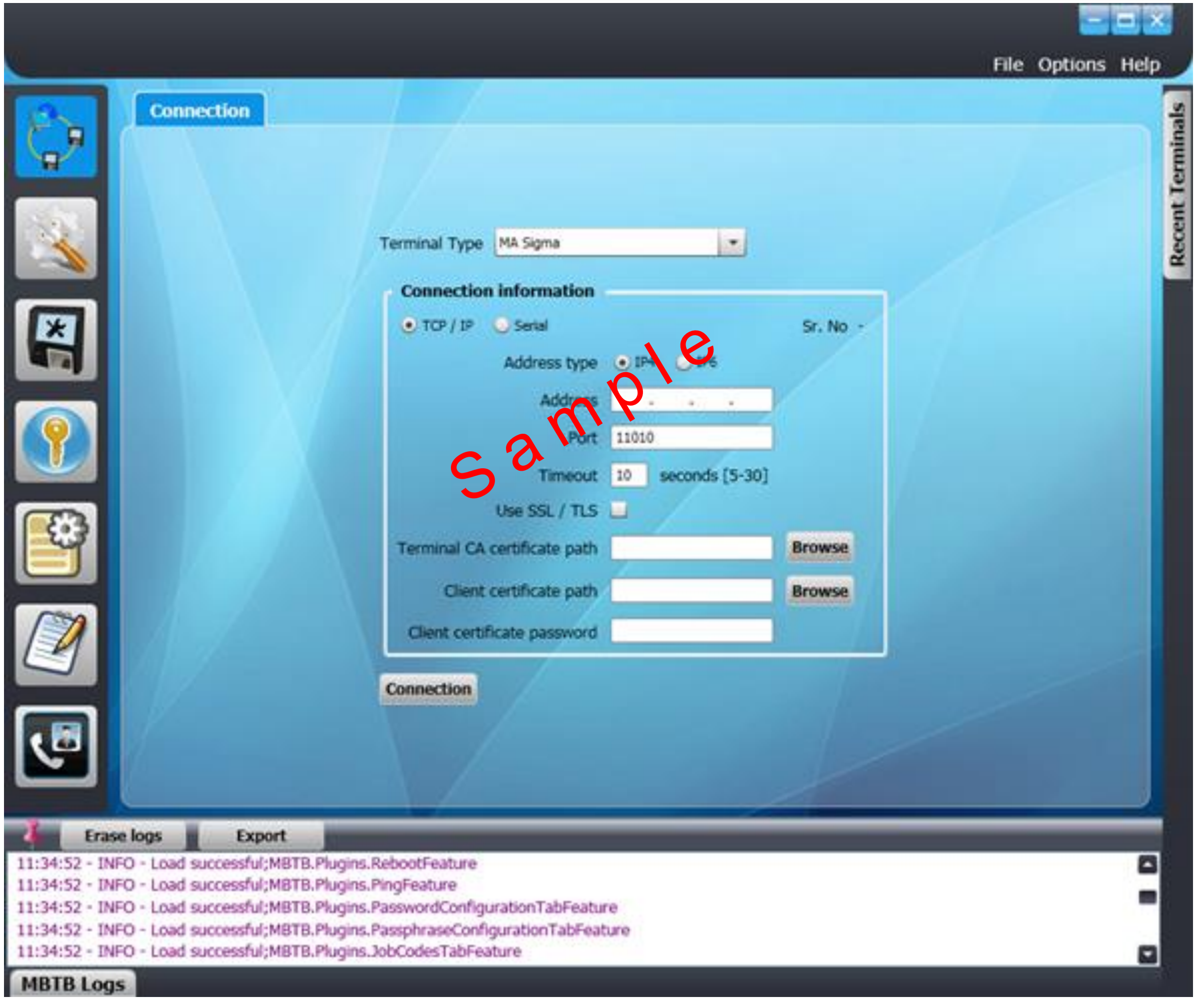
← Back (and Cancel)	⌂ Exit or Go Home
✗ Cancel or refuse	✓ Validation or confirmation

Step five: Administration

Administration with MorphoBioToolBox application

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

Terminal administration with MorphoBioToolBox (MBTB) application



Terminal Type: MA Sigma

Connection information

● TCP / IP ○ Serial Sr. No -

Address type: ● IPv4 ○ IPv6

Address: . . .

Port: 11010

Timeout: 10 seconds [5-30]

Use SSL / TLS: □

Terminal CA certificate path:

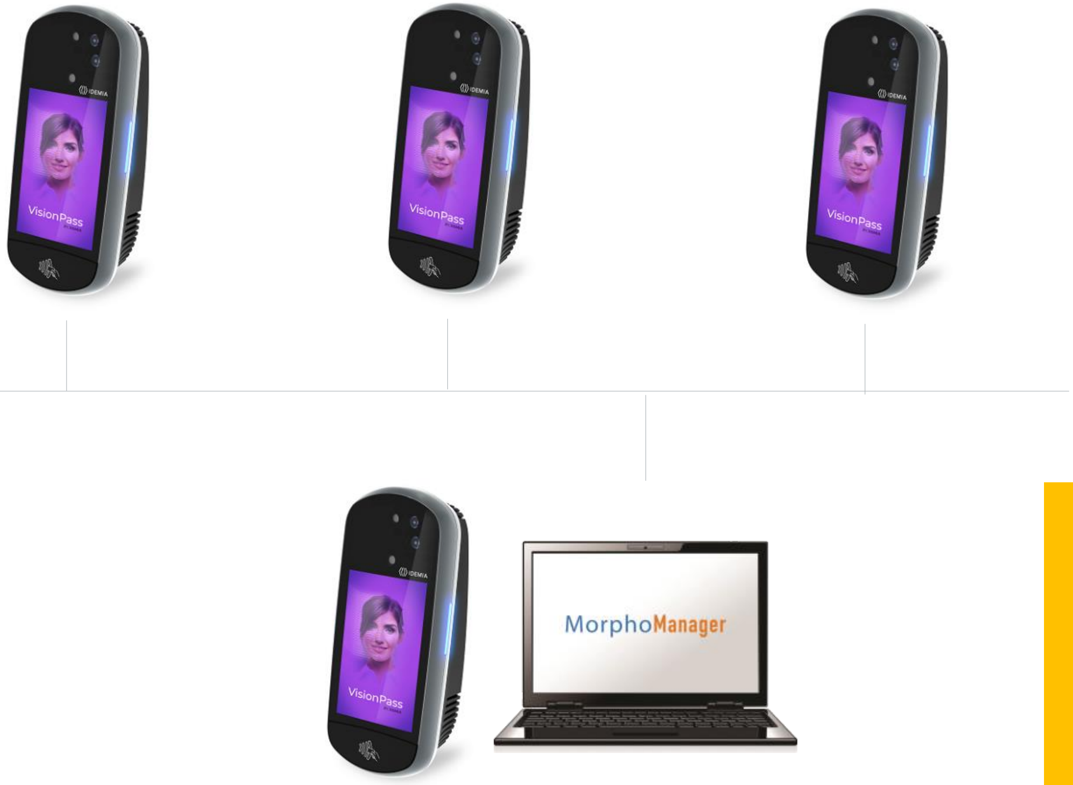
Client certificate path:

Client certificate password:

```
11:34:52 - INFO - Load successful;MBTB.Plugins.RebootFeature
11:34:52 - INFO - Load successful;MBTB.Plugins.PingFeature
11:34:52 - INFO - Load successful;MBTB.Plugins.PasswordConfigurationTabFeature
11:34:52 - INFO - Load successful;MBTB.Plugins.PassphraseConfigurationTabFeature
11:34:52 - INFO - Load successful;MBTB.Plugins.JobCodesTabFeature
```

Software for Terminal Remote Administration and Enrollment

VisionPass Terminals are compatible with MorphoManager application (version 14.3 or higher)



MorphoManager

Local Enrollment Process

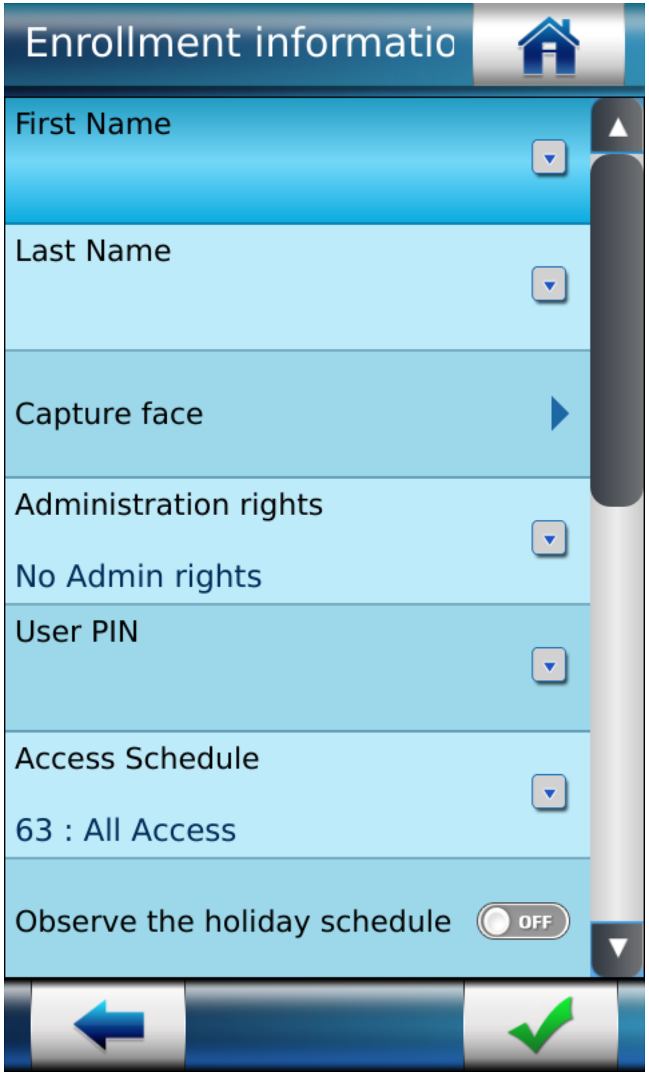
A new user can easily be added by using the administration menu of the VisionPass terminal.
This “local enrolment” is recommended only for small or stand alone installations or testing purposes. For professional systems enrolment should be performed remotely with an enrolment station, which is a PC with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

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

Enrolment gathering user’s data listed :

- User’s first name and last name
- User’s face (for biometric check)
- User’s administration rights (none, database, full, limited database)
- User’s PIN (for PIN check)
- User’s access schedule and holiday schedule
- User’s dynamic message setting
- Door open timeout
- User’s record expiry date
- User to include in authorized list or in VIP list
- User specific access rules definition

Note: Refer to User enrollment section in VisionPass Administration Guide.



Enrollment informatio

First Name

Last Name

Capture face

Administration rights

No Admin rights

User PIN

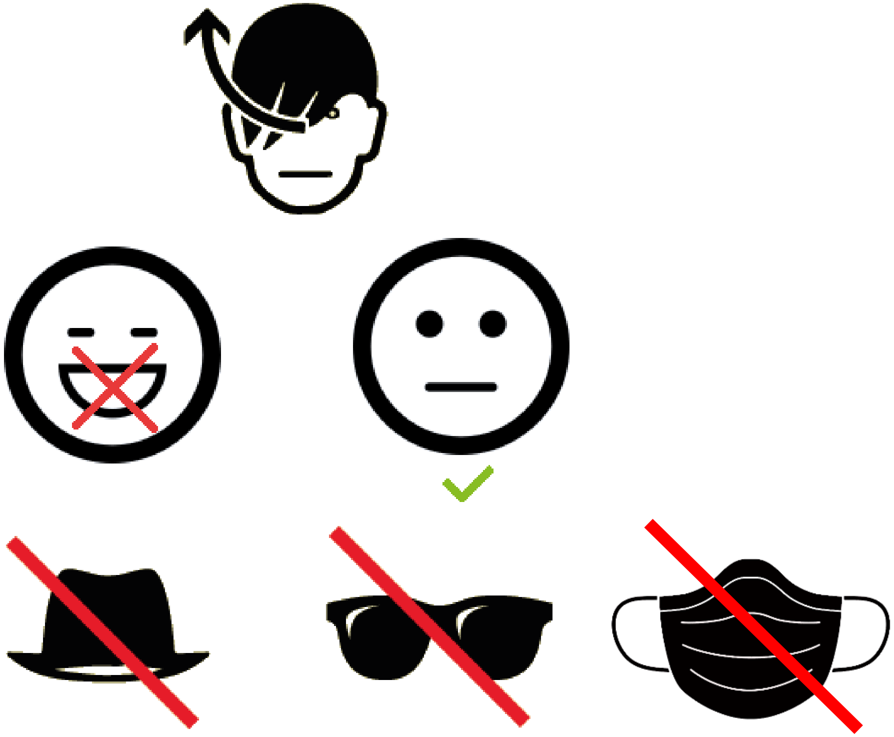
Access Schedule

63 : All Access

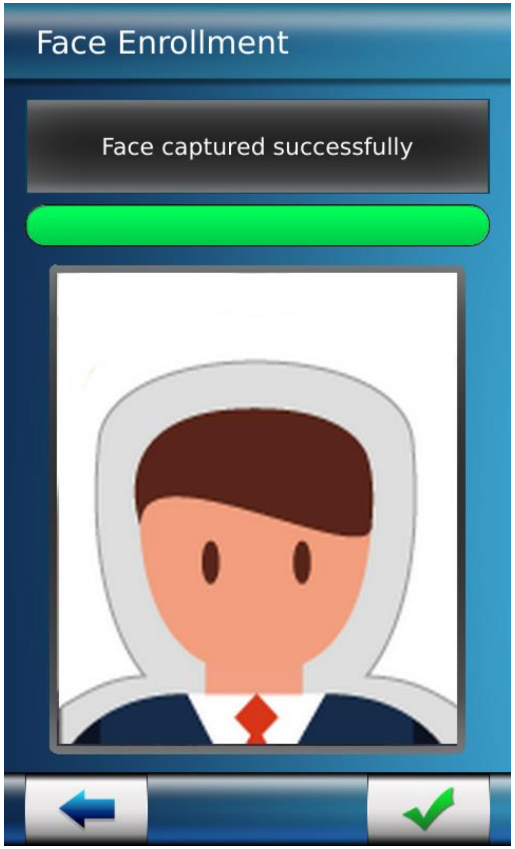
Observe the holiday schedule OFF

Step seven: capture basics

Enrollment Process Recommendations



Please stand still in front of the product with your face clearly visible
Remove all « non-always on » accessories. Remove your glasses.
Remove face masks.



Face Enrollment

Face captured successfully

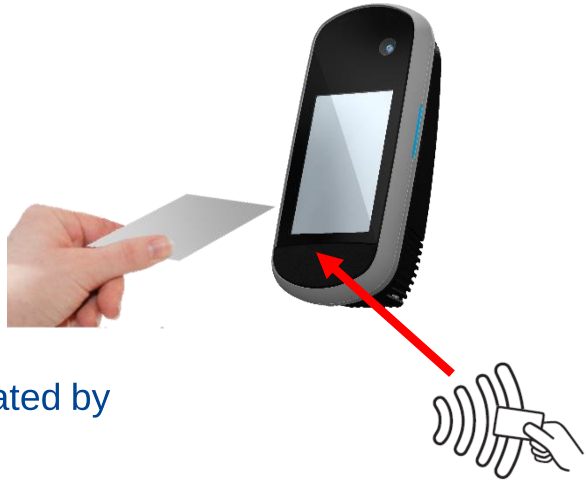
Step seven: capture basics

Contactless Card Position – PIN input

Contactless Card Position

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

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

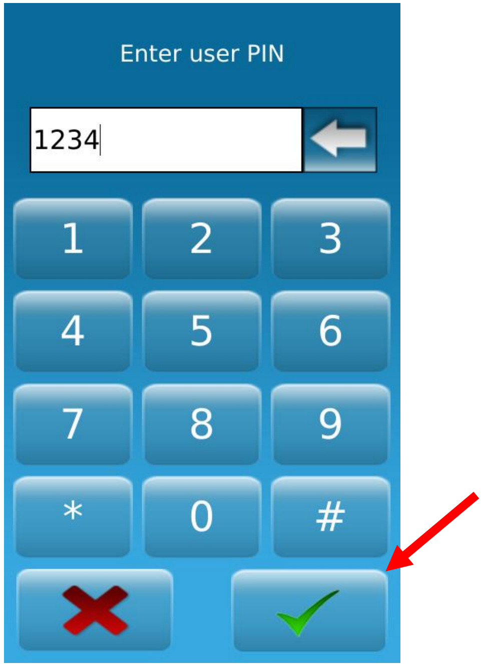


The authentication process is initiated by the detection of a user card by the contactless card reader.

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

NB : Time to read all datas from the card would be more or less long depending on the quantities of datas to extract and type of card.

Input PIN



Enter user PIN

1234

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

The PIN code is entered using a numeric keypad displayed on the LCD touch screen.

Step seven: capture basics

Time and Attendance feature

VisionPass terminals support an optional Time and Attendance (T&A) feature.

For this, the terminal adds a specific T&A information to each identification or authentication record stored in the embedded event log database.

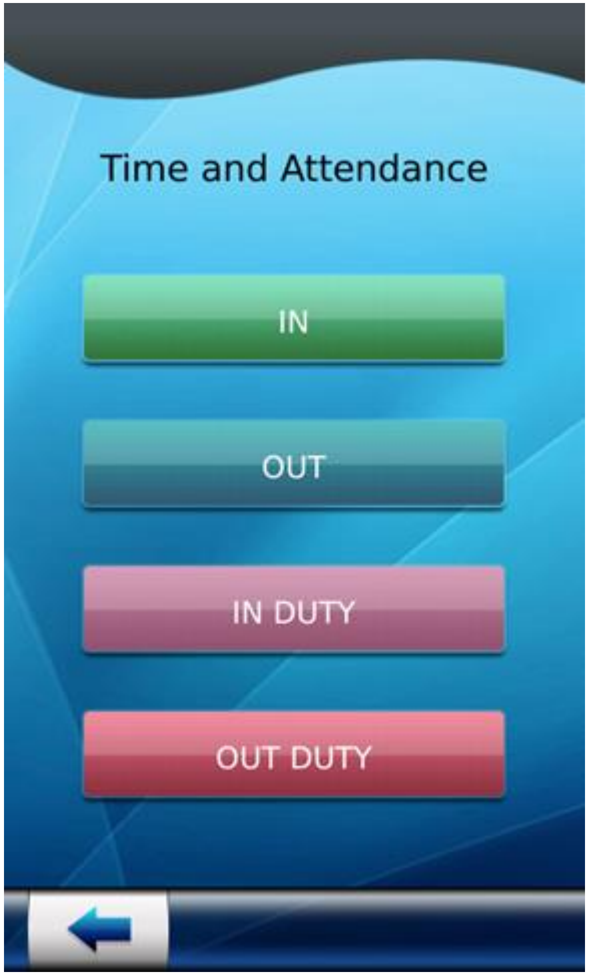
This information is provided by the user through a specific screen displayed during identification or authentication process.

The new screen contains 4 dedicated function keys :

- Entry
- Exit
- Beginning of a task
- Ending of a task

The user is expected to press one of the keys to provide the specific Time & Attendance information to the terminal.

This screen is displayed after the biometric check of the user or the contactless card reading in front of the reader.
An extended mode is also available with 16 function keys.



Step eight: optional features

Recommendations

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

Repair and Accessories

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

Standalone terminals (not connected to a network)

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

Date / Time synchronization

- The VisionPass terminal clock has a +/- 10 ppm typical time deviation at +25°C (roughly +/- 1sec per day). At lower and higher temperature, deviation may be greater (maximum : 8 seconds per 48 hours).
- When the terminal is used for applications requiring high time precision, it is strongly recommended to synchronize the terminal with an external clock.

Cleaning precautions

- A dry cloth should be used to clean the terminal, especially the glass in front of biometric sensor.
- The use of acid liquids, alcohol or abrasive materials is prohibited.
- Use dry air spray to remove the dust out of the sensor glass

Firmware release

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

Documentation

Documents about installing the terminal

VisionPass Installation Guide, Ref. 2019_2000045728
This document describes the terminals physical mounting procedure, electrical interfaces and connection procedures.

Documents about administrating / using the terminal

VisionPass Quick User Guide, Ref. 2019_2000045730 (this document)
This document gives a quick overview of the product and the basics of configuration and use.

Biometric terminals Administration Guide, Ref. 2018_2000036794
This document describes the different functions available on the terminal and the procedures for configuring the terminal. It also contains the full description of all the configuration parameters for the terminal.

MWC - VisionPass Parameters Guide, Ref. 2018_2000035285
This document contains the full description of all the terminal configuration parameters.

Documents for the developer

MorphoAccess 5G Series Host System Interface Specification, Ref. 2016_2000022602
This document describes the commands supported by the MorphoAccess® terminal.

MorphoAccess 5G Series Remote Message Specification, Ref. 2016_2000022373
This document describes the format of messages sent by the terminal to a distant system.

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…

Contacts

Technical Support and Hotline

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

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

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

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

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

293750462-C