VisionPass SP

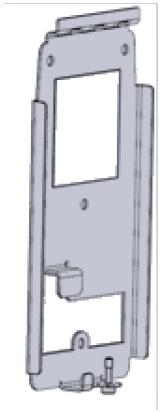
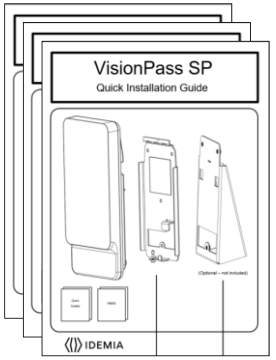
Quick User Guide

IDEMIA

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

VisionPass SP box content

Product packaging checklist:

Terminal	Wall mount	Cable kit	Cover Plate	Documentation package
				

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 2.5A 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, 2.5A minimum or 24VDC, 1.25 A minimum.

For UL 294 compliance the unit shall be powered via a UL 294 power supply with class 2 power limited output.

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 SP 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.

Table of Contents

Color	Step	Content
	One	Overview
	Two	Wiring
	Three	Communications
	Four	SDAC (Single Door Access Control)
	Five	Software
	Six	Administration
	Seven	Enrollment
	Eight	Optional features

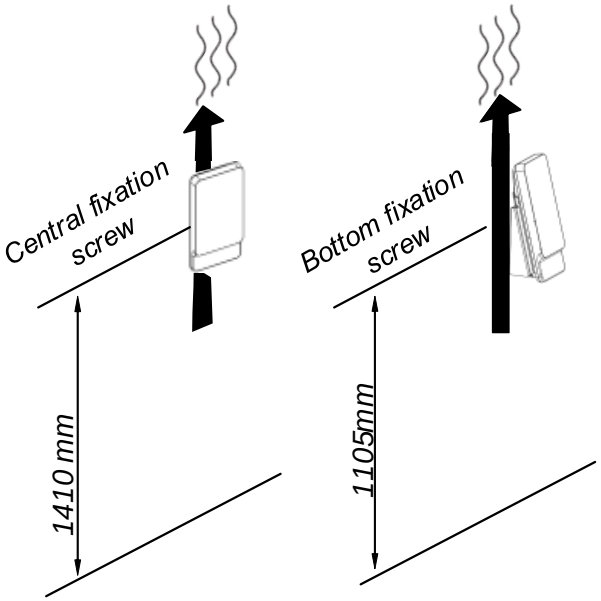
Product Overview

VisionPass SP 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, SmartMX, HID® iCLASS®*, HID® SEOS®*)
- Universal connectivity (Ethernet, RS485, Wiegand, Dataclock)
- Anti-tamper sensor

* Depending on product version

Installation recommendations / environment



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

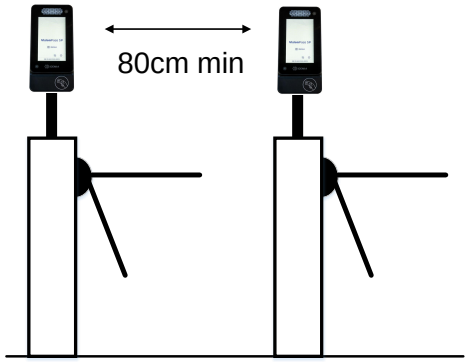
VisionPass SP is designed to operate indoor. To optimize VisionPass SP performance, it is better to follow the rules below:

- VisionPass SP processes biometric data faster when users walk towards the device. Lateral approach is not recommended, meaning that users shall not come by the side.
- 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 moving object in the field of view such as glass door
- Avoid any bright spot light very close to the device (closer than 1 meter)

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.



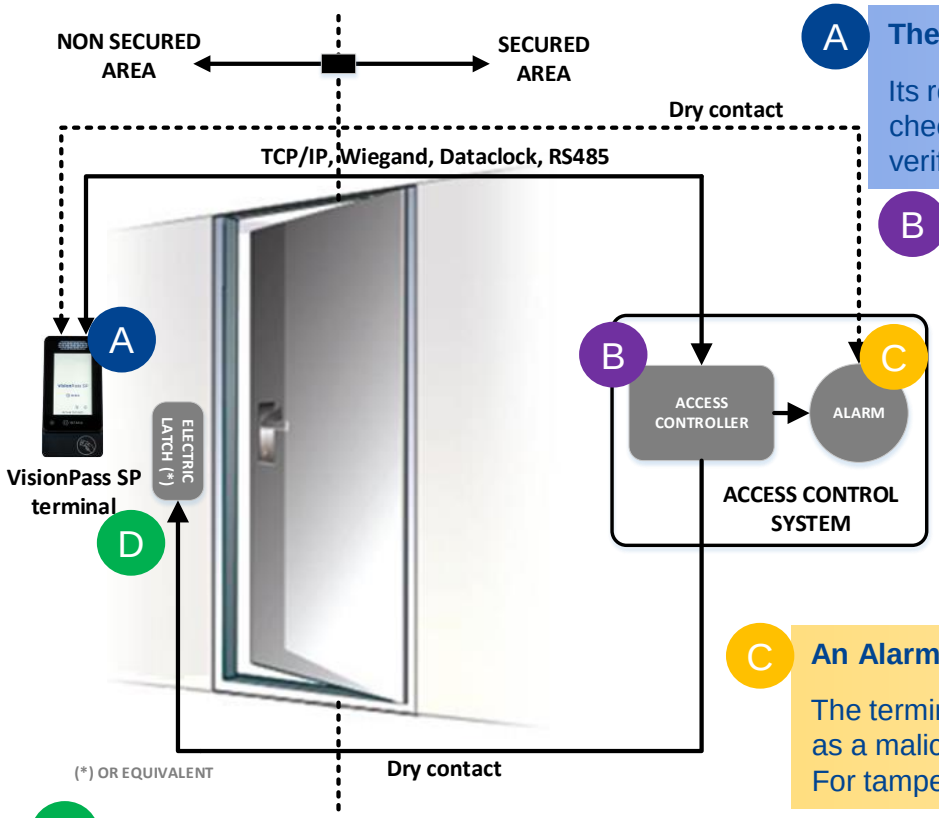
Keep those areas clear and clean : no sticker, no raindrops, no dust etc.

Please refer to the **Installation Guide** for full recommendations

Step one : overview

Terminal Implementation

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



A The VisionPass SP 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 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.
For tamper, another solution is to connect the alarm through the dry contact (SW1/SW2)

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..

*Note: UL only verified Wiegand

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 an "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.

Step one : overview

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 SP 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

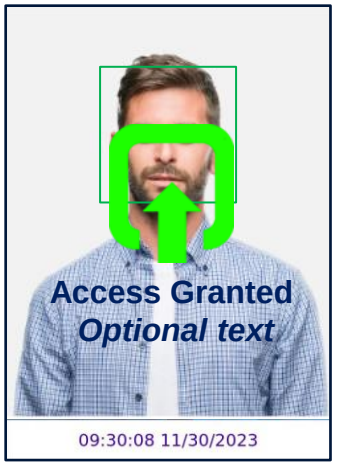
User Journey

Intention area

Live feedback on screen

Orange > User is outside the intention area and shall move forward

Green > User is inside the intention area and shall wait for identification



Access Granted > User must move to the access control point

Access Denied > User must exit from intention area to allow a next user identification

The screen automatically lights up in case someone is entering into the vicinity of the VisionPass SP.

The facial access control is only initiated when a user is entering the intention area. The user shall walk to the VisionPass SP, looking at the device screen until a green square is displayed on his face. The white LED may light up automatically during the approach in case of low light conditions.

The user shall eventually pause to be identified and wait for the access control user-right feedback. The user may leave on hat, glasses, mask, or any face covering to speed-up identification. Once the access granted message is displayed, the user shall move forward to the access control point.

If the user is not identified before the time-out (5 seconds), the access is denied. The user must clear the intention area for a next user.

After any granted or denied access, user must leave the intention area to allow a new user identification.
A user already identified (granted or denied) must leave the intention area for >2 seconds to trigger a new access.

Recommendations

User journey is optimized by configuring

- time-out for identification (from 2 to 10 s)
- size of the intention area (short, medium or long)

User Guidance

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

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.

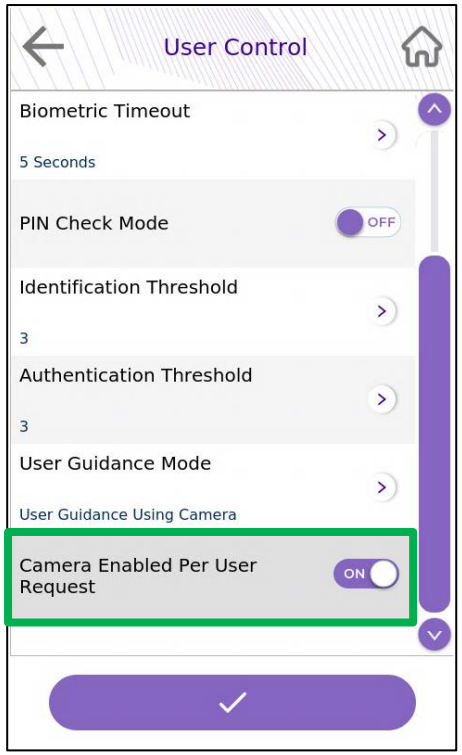
User Guidance Using Camera : terminal will display a live feedback of the camera

Deliberate trigger

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

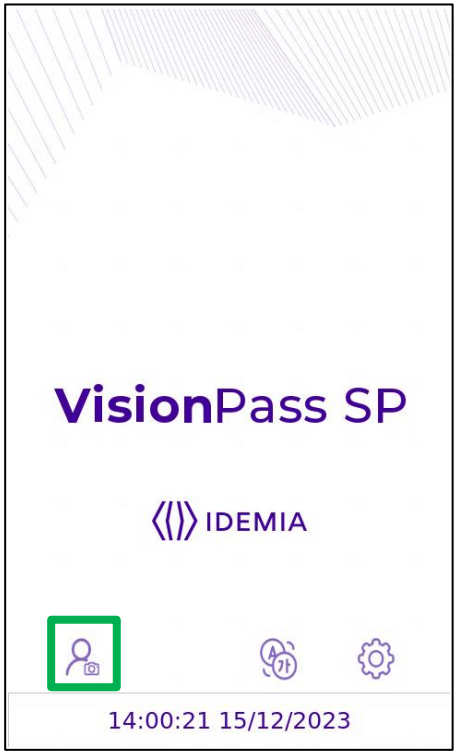
Even if the video stream is not recorded by the terminal, it can be requested to disable the cameras when they are not necessary, for privacy concerns.
VisionPass SP can be configured to enable the cameras on user request only :

Activate Camera Enabled Per User Request in the Security settings :



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

5 wires

2 wires

7 wires

8 wires

5 wires

Relay and Switch		
6	SW-P2	Pink
5	SW-P1	Light Blue
3	RLY-NC	Orange / White
2	RLY-NO	Yellow / White
1	RLY-COM	Grey / White

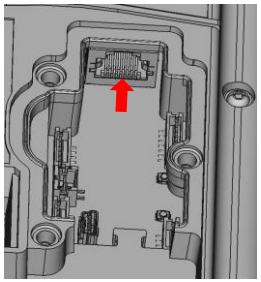
Power supply		
2	PWR+	Red
1	GND	Black

Wiegand IN and OUT		
1	IN0	Green / Red
2	IN1	White / Red
3	LED1	Blue
4	LED2	Blue / Red
5	OUT0	Green
6	OUT1	White
7	GND	Black

RS485		
1	RX-A	Blue / Black
2	RX-B	Blue / White
3	TX-Y	Green / Black
4	TX-Z	Green / White
5	GND	Black

GPIO		
8	GPO2	Yellow / Black
7	GPO1	Yellow / Red
6	GPO0	Yellow
5	GND	Black
4	GND	Black
3	GPI2	Orange / Black
2	GPI1	Orange / Red
1	GPI0	Orange

RJ-45 : Ethernet & PoE		
1	ETH TX+	Orange / White
2	ETH TX-	Orange
3	ETH RX+	Green / White
4	ETH VPORT+	Blue
5	ETH VPORT+	Blue / White
6	ETH RX-	Green
7	ETH VPORT-	Brown / White
8	ETH VPORT-	Brown
Shell	ETH GND	Drain wire (no color)



RJ45

Pin numbers shown in this document correspond to the internal connector pinout in the product.

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

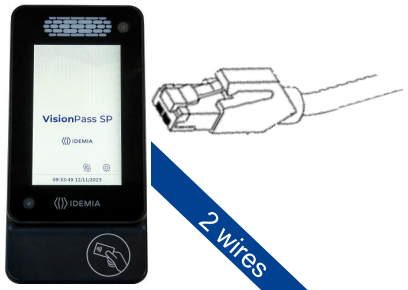
Power supply from electrical source shall be switched off before starting the installation.

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 2 hours (at 25°C) without external power supply.

Step two : wiring

Power supply



Power supply		
2	PWR+	Red
1	GND	Black

Power Over Ethernet (POE+): power can be provided through RJ-45 connector using a PSE (Power Sourcing Equipment) **IEEE802.3at type 2** compliant.

The terminal is a Class 4 (25.5 W) PD (Powered Device).
Note: UL compliance was verified with Phihong model POE36U-1AT-R Primary rated 100-240VAC 1Amp 50-60Hz; 56VDC, 0.6A

External Power Supply: 12-24V (regulated and filtered) 2.5A min @12V, IEC60950-1 or IEC 62368-1 standard compliant. If sharing power between devices, each unit must receive 2.5A at 12V (e.g. two units would require a 12 VDC, 5A supply).

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

IDEMIA recommends using a 24V 1.25A 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%).

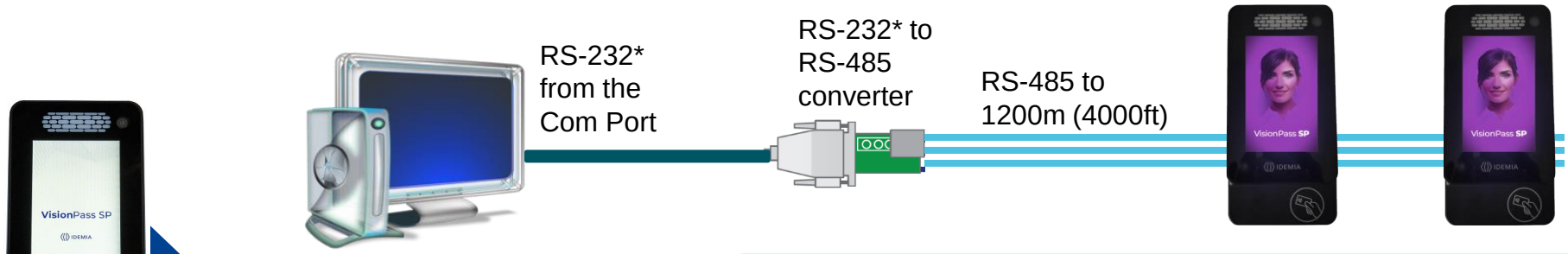
The product requires ~25W at all voltage conditions.

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%	12 V +/- 5%	24 V +/- 10%
16	1.31	15 m	30 m	250 m
18	0.82	10 m	20 m	180 m
20	0.52	8 m	15 m	120 m
22	0.32	4 m	7 m	60 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



RS485		
3	TX-Y (TX+)	Green / Black
4	TX-Z (TX-)	Green / White
5	GND	Black

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 TX-Y (TX+, Green / Black wire #3) and TX-Z (TX-, Green / White wire #4). Another conductor should be used for Signal Ground (Black wire #5).

IMPORTANT:

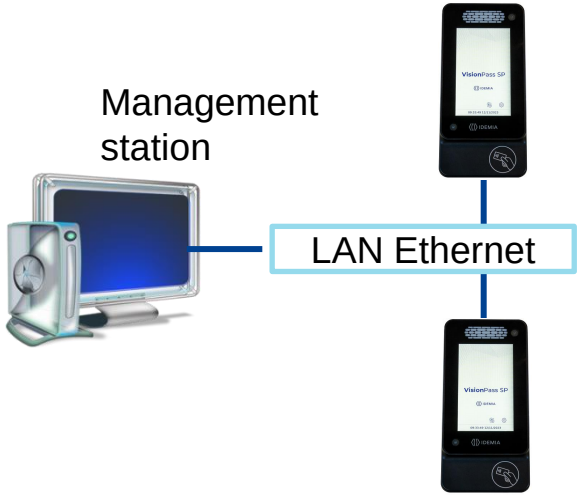
- A maximum of 31 devices may be installed on the same line.
- The maximum total cable length is 1200m (4000 ft.)
- The cable must be dedicated to this installation and not used for any other purpose

*Note: the RS-232 has not been UL evaluated.

Step three : communications

Ethernet and Wireless LAN

RJ-45 : Ethernet & PoE		
1	ETH TX+	Orange / White
2	ETH TX-	Orange
3	ETH RX+	Green / White
4	ETH VPORT+	Blue
5	ETH VPORT+	Blue / White
6	ETH RX-	Green
7	ETH VPORT-	Brown / White
8	ETH VPORT-	Brown
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 SP 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).

*Note: Not evaluated by UL

Step three : communications

Wiegand Communication

GPIO*		
6	GPO0	Yellow

Wiegand IN and OUT		
1	IN0	Green / Red
2	IN1	White / Red
3	LED1	Blue
4	LED2	Blue / Red
5	OUT0	Green
6	OUT1	White
7	GND	Black

LED In

Wiegand In

LED Out

Wiegand Out

Wiegand In/Out

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 **OUT0** (Green wire – Pin #5) to ACP Data 0,
- Connect **OUT1** (White wire – Pin #6) to ACP Data 1,
- Connect **GND** (Black wire – Pin #7) 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 outputs shall be open drain or 5 V +/- 5%

*Note: GPO0 has not been UL evaluated.

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.

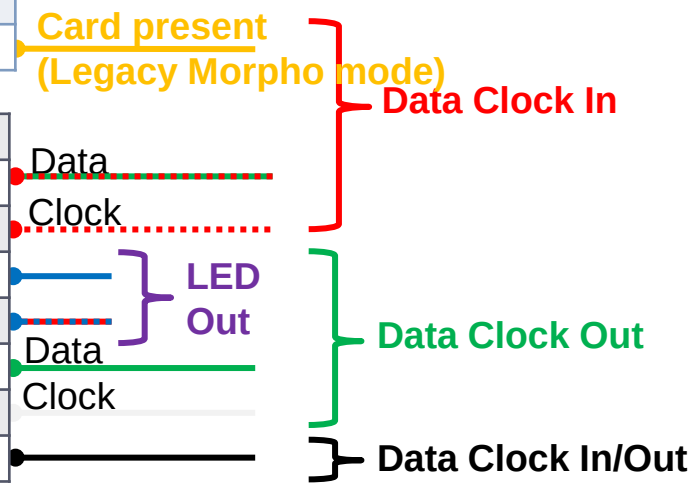
Format Example

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

GPIO		
6	GPO0	Yellow

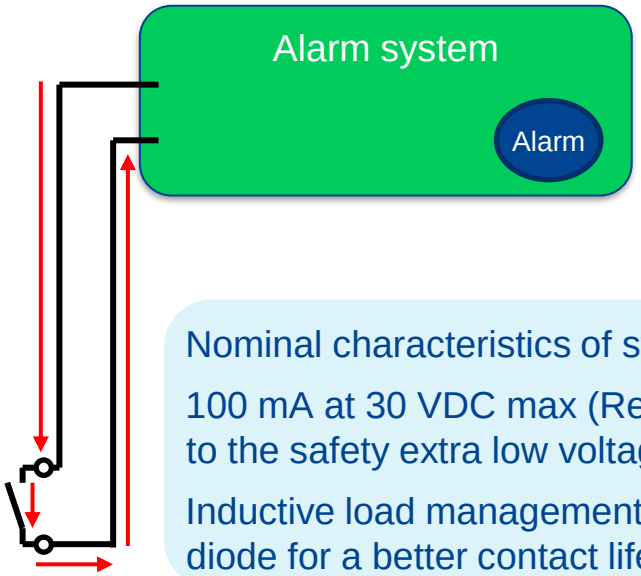
Wiegand IN and OUT		
1	IN0	Green / Red
2	IN1	White / Red
3	LED1	Blue
4	LED2	Blue / Red
5	OUT0	Green
6	OUT1	White
7	GND	Black



Step three : communications

Tamper switch - Alarm (with dry contact)

Tamper switch		
6	SW-PIN2	Pink
5	SW-PIN1	Light Blue



Nominal characteristics of switch block:

100 mA at 30 VDC max (Resistive load) according to the safety extra low voltage standard.

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

Operating principle for the switch:

- Product installed on the wall plate: switch enabled (contact closed).
- Product unmounted of the wall plate (rear connectors accessible): switch disabled (contact open).

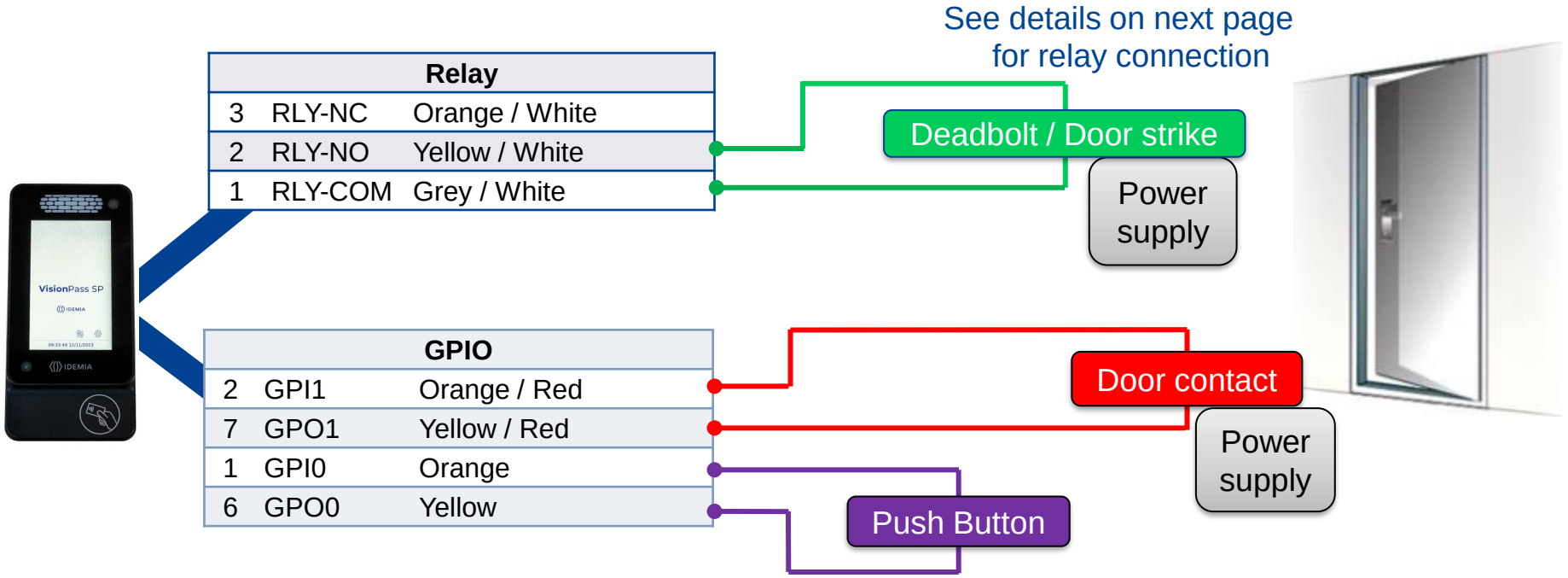
Warning

➢ **This VisionPass SP terminal is part of security system; it is customer's responsibility to connect the tamper switch (contact) to physical access controller, in order to prevent the access to the connector blocks. UL has verified this product for access control functions only.**

Step three : communications

Single Door Access Control (SDAC)

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



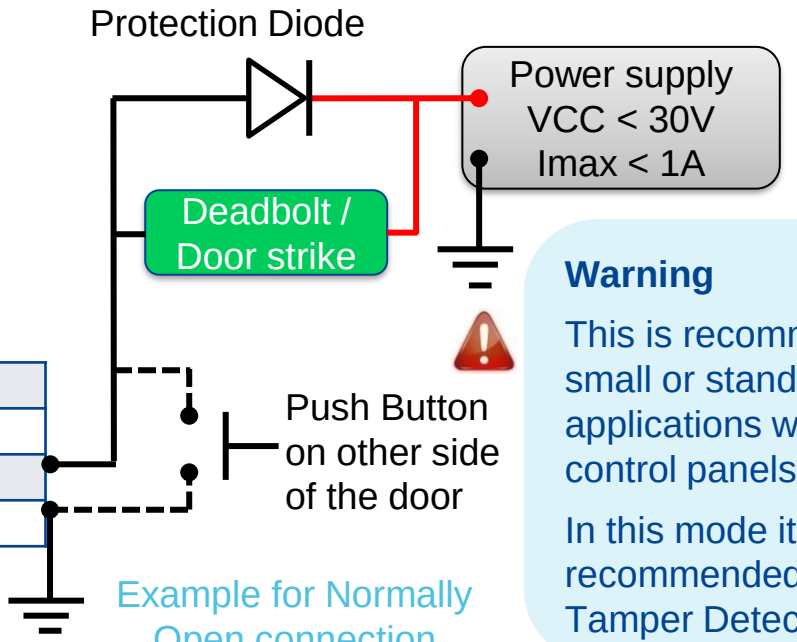
If door contact is not used, GPI1 (#2) and GPO1 (#7) shall be connected together

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

Step four: SDAC

Internal Relay Wiring

	Relay	
3	RLY-NC	Orange / White
2	RLY-NO	Yellow / White
1	RLY-COM	Grey / White



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 DC. 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

Software for Remote Administration and Enrollment

MorphoManager

VisionPass SP Terminals are compatible with MorphoManager application (version 16.3 or higher)

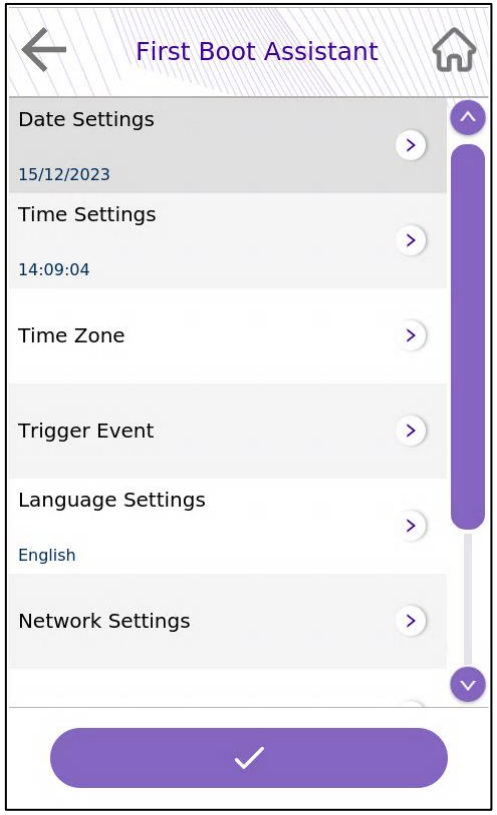
Step five: software

Local Administration - First Boot Assistant

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

It is automatically launched at first terminal startup.

It can also be launched on demand, through System Menu, if available (shall not be done in a secure system, as described below).



Main settings managed by FBA

Date & Time & Time Zone Settings

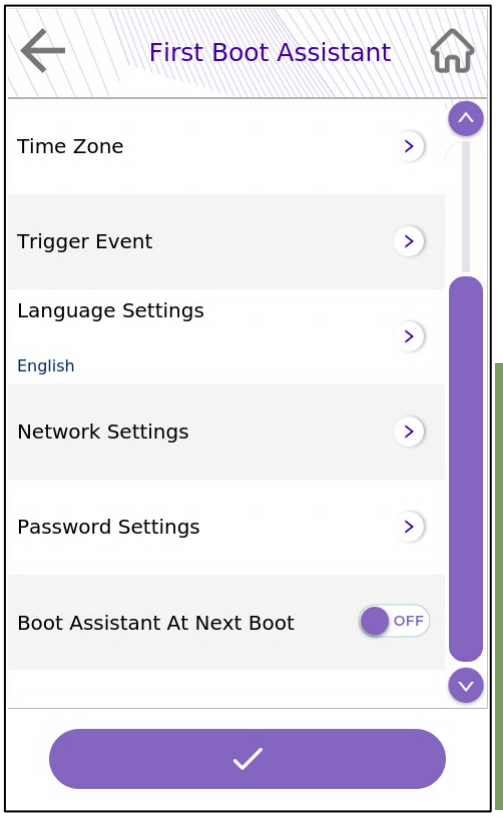
Trigger Event: select event(s) to be processed as an access request by a user

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 six: administration

Enforced security configuration

The VisionPass SP terminal has a default configuration enforcing security:

- Webserver disabled
- IP connection possible only in TLS 1.2 or higher
- Configuration from on-screen menu disabled, except for IP configuration
- Thrift commands from RS485 disabled
- Configuration with a script hosted on a USB dongle not possible

The default configuration is recommended by IDEMIA for operations. To use the features non available by default, the **On-demand security** state of VisionPass SP can be unlocked with MorphoBioToolBox.

This shall not be done unless the end customer is made aware and an assessment on the system security is done.

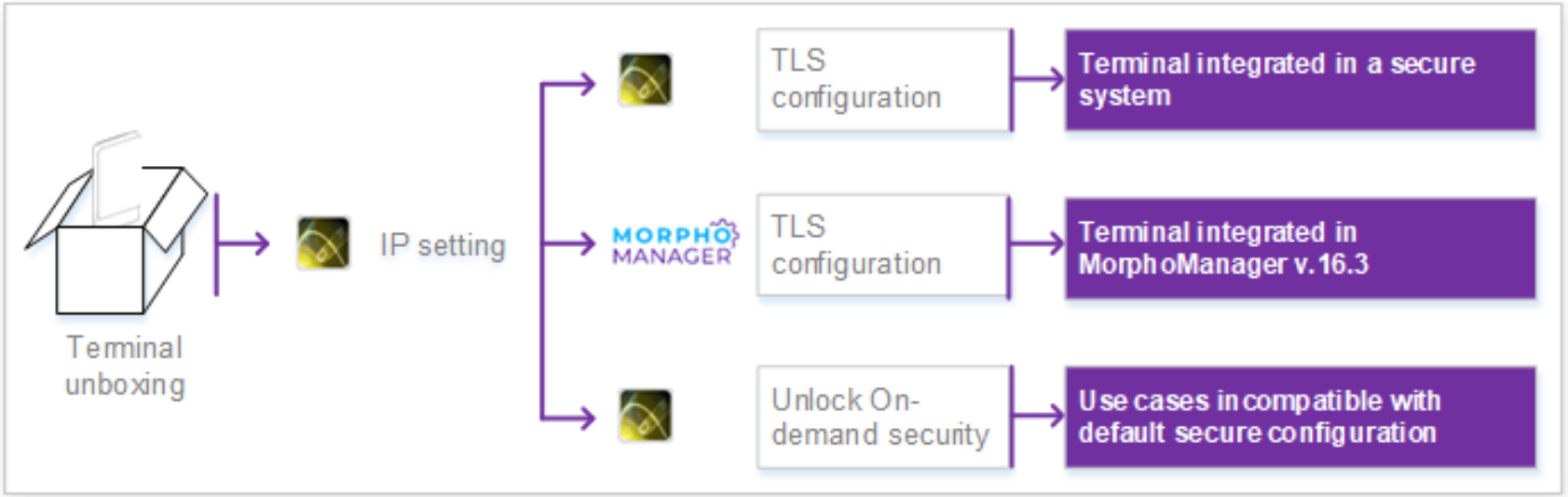
Step six: administration

Administration of secure communication

IP communication is by default mandatorily based on TLS for secure communication.

The communication configuration can be done **MorphoBioToolBox**
This Windows application can also be used for the full terminal configuration.

Starting from version 16.3, MorphoManager can also configure the TLS communication of a VisionPass SP terminal as soon as the latter has a valid IP address.



Step six: administration

Local Enrollment Process

A new user can easily be added by using the administration menu of the VisionPass SP terminal.

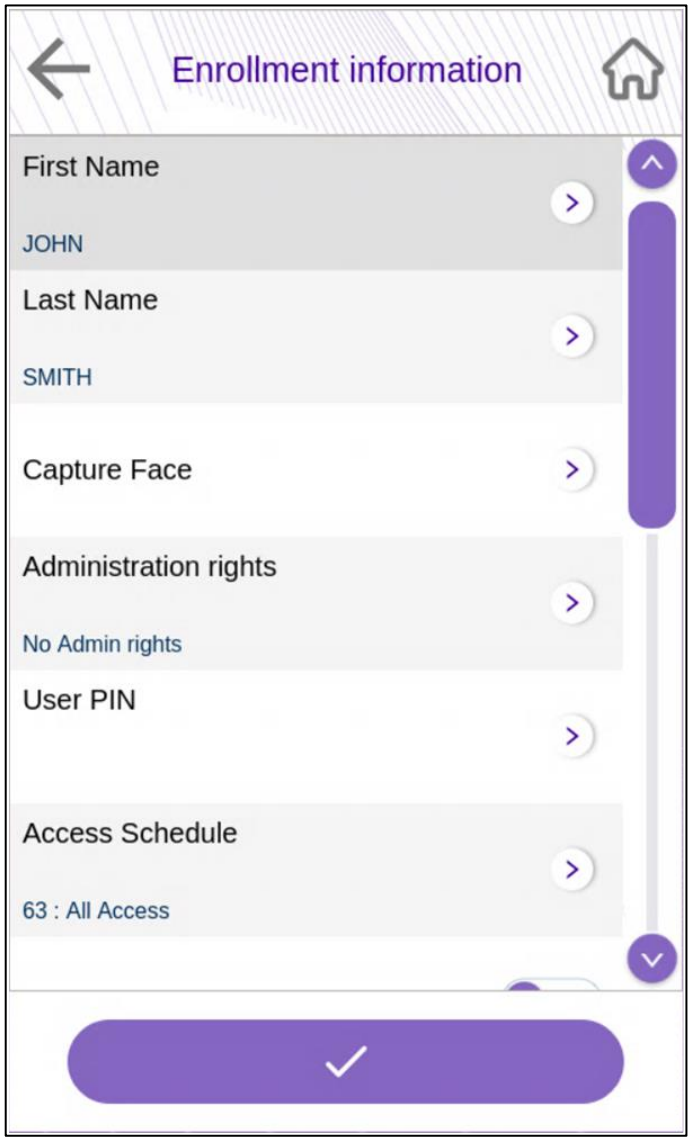
This menu allows a user's record to be added in the local database, with the following reference data:

- 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

Optionally, a contactless card can be created.

Please refer to the User enrollment section in VisionPass SP Administration Guide.

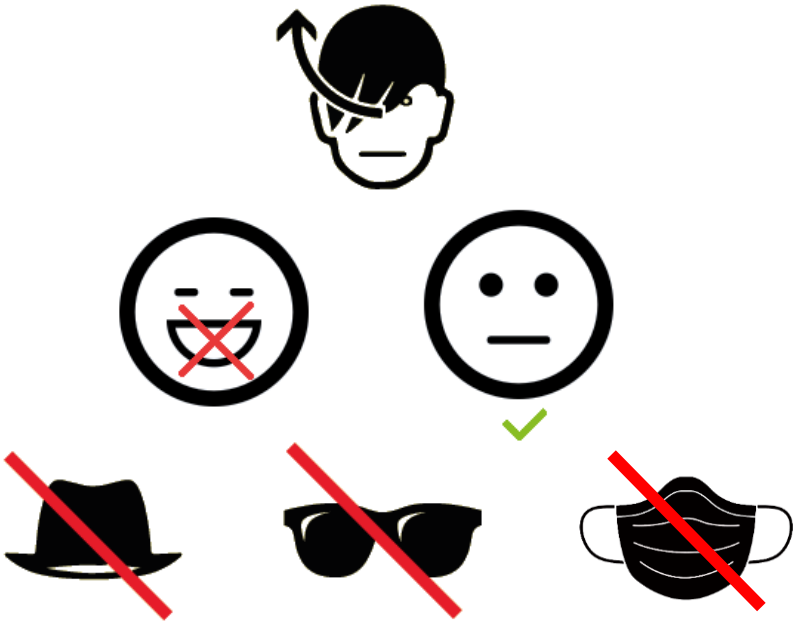
"Local enrollment" shall not be used in a secure system, where it should be performed on an enrolment station (a PC with a dedicated application such as MorphoManager).



Step seven: enrollment

Enrollment Process Recommendations

Instruction for User for enrollment



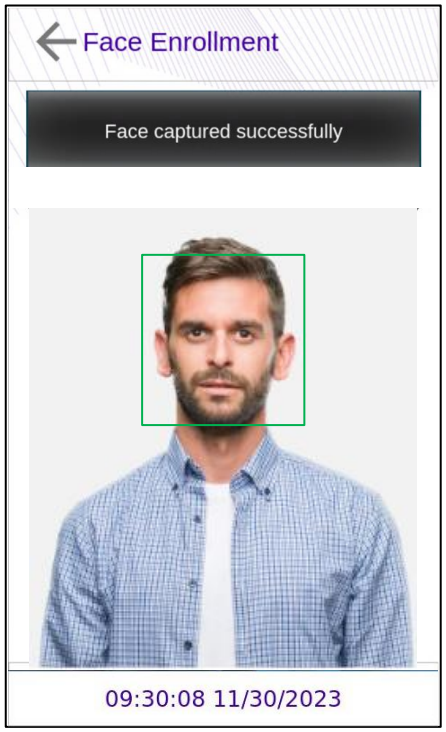
Please stand in front of the device without moving

Please look at the screen with a neutral expression (no smile)

The face shall be clearly visible

- Remove hair covering face and eye(s)
- Remove all « non-always on » accessories
- Remove your glasses
- Remove face masks.

Display during enrollment



Recommendations for operator
Floor marking is recommended at 60 cm from the device to invite the user to stand at the right place, before launching the enrollment process.

Step seven: enrollment

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.

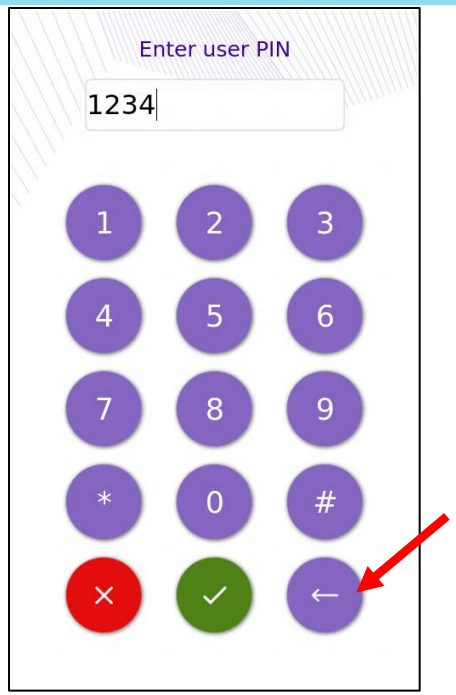
Place user's RF card in front of embedded contactless card reader which is located behind the contactless logo.

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 data from the card would be more or less long depending on the quantities of data to extract and type of card.

Input PIN



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 and validate by clicking on: ←

Step seven: enrollment

Time and Attendance feature

VisionPass SP 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 (IN)
- Exit (OUT)
- Beginning of a task (IN DUTY)
- Ending of a task (OUT DUTY)

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 SP 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 an external support such a mass storage key

Date / Time synchronization

- The VisionPass SP terminal clock has a +/- 20 ppm typical time deviation at +25°C (roughly +/- 2sec 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.

Precautions for screen life duration:

- To ensure the proper operation of the product and prevent image retention on LCD screen, it is highly recommended not to display a static image on the screen for extended periods of time and to configure the device to repeatedly refresh the image displayed on the screen.
- Please note that image retention on LCD screen is considered improper use of the product and is not covered by the product warranty.

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)

Overvoltage

- IDEMIA recommends the Biometric devices to be protected with an external accessory in order to avoid overvoltage on input wires or connectors of the device. Typically, risks of overvoltage have been identified on external power management wire, POE connector and wiegand input wire.

Documentation

Documents about installing the terminal

Quick Installation Guide
This document describes the main step for wall mounting.

General Security Notice
This document provides an introduction to the security configuration and provides cybersecurity guidelines for all stakeholders.

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

Enforced security, new default configuration
This document provides user guides for TLS secure communication.

Documents about administrating / using the terminal

Quick User Guide
This document gives a quick overview of the product and the basics of configuration and use.

Administration Guide
This document describes the different functions available on the terminal and the procedures for configuring the terminal.

Parameters Guide
This document contains the full description of all the terminal configuration parameters.

Documents for the developer

Host System and Remote Message Interfaces
This document describes the commands supported by the terminal and 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

USA & Canada
Mail: support.bioterminals.us@idemia.com
Tel: +1 888 940 7477

LATAM (Latin America)
Mail: support.bioterminals.us@idemia.com
Tel: +1 714 575 2973

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

APAC (Asia & Pacific)
Mail: support.bioterminals.in@idemia.com
Tel: +91 8929 159 665

India
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
https://biometricdevices.idemia.com
To get your login and password please contact your sales representative.