



VisionPass SP

Installation guide



Warning

All Information and Intellectual property rights reserved at ©IDEMIA 2023.

Reproduction in whole or in part in any form or medium without the express written permission of IDEMIA is prohibited. The trademarks identified herein are the trademarks of registered trademarks of IDEMIA, or other third party.

This legend is applicable to all pages of this document.

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

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

Revision history

Version	Date	Reference	Description
01	January 2024	2023_2000073596	Document creation
02	April 2024		Update for UL294 certification
03	October 2024		Add Canada (IC) regulatory notices

Table of content

1 / Introduction	7
1.1 > VisionPass SP terminal	7
1.2 > Scope of the document	7
1.3 > Safety Instructions	8
1.3.1 > DC supply	8
1.3.2 > Power Over Ethernet Plus (POE+)	8
1.3.3 > Photobiological safety	8
1.4 > Wiring Recommendations	9
1.5 > Regulatory, safety and Environmental notices	10
1.5.1 > European Union (CE) regulatory notices	10
1.5.2 > USA (FCC) regulatory notices	11
1.5.3 > Canada (IC) regulatory notices	12
1.5.4 > Brazil (Anatel) regulatory notices	13
1.6 > Others recommendations	13
1.7 > Recommendations for terminal implementation	14

2 / General description	17
2.1 > Components of the initial package	17
2.2 > Terminal's front view description	18
2.3 > Terminal's rear view description	19
2.4 > VisionPass SP Technical Characteristics	20

3 / Installation procedure	23
3.1 > Before proceeding to the installation	23
3.2 > Installation	24
3.3 > Step by step procedure	25
3.3.1 > Drill the mounting holes	26
3.3.2 > Make the connections	28
3.3.3 > Attach the wall plate on the wall	29
3.3.4 > Connect the cables to the terminal	30
3.3.5 > Fix the cover plate	30
3.3.6 > Add silicon around cable and cover plate (optional)	31
3.3.7 > Fix the terminal to the wall plate	32

4 / Electrical interface	35
4.1 > Wiring overview	35
4.2 > Power Supply	36
4.3 > Output Relay	38
4.4 > Tamper Switch	39
4.5 > Wiegand wiring	40
4.6 > Wiegand output	41
4.7 > Serial port wiring	43
4.8 > GPIO wiring	45
4.9 > Ethernet connection	46
4.10 > Internal USB connection	48
4.11 > Secure communication	49

5 / User interface	50
5.1 > Modes for controlling access rights	50
5.1.1 > Introduction	50
5.1.2 > Identification mode	50
5.1.3 > Authentication (verification) mode	50
5.1.4 > Multi-factor mode	51
5.1.5 > Proxy mode	51
5.1.6 > External database mode (also called polling mode)	51
5.1.7 > Anti-tamper / anti-pulling switches	52

6 / Accessories and PC applications	53
6.1 > Compatible Accessories	53
6.1.1 > Low mounting bracket	53
6.1.2 > Spacer	54
6.1.3 > Visor	54
6.1.4 > Metal Mount	55
6.2 > Compatible PC applications	55

7 / Recommendations	56
----------------------------	-----------

8 / Annex 1: placement recommendations	59
8.1 > Main principles	59
8.2 > Positioning Guidelines	60
8.2.1 > Overview	60
8.2.2 > Specific guidelines for gates or turnstiles	61
8.2.3 > Lower positioning: 1105 mm	64

9 / Annex 2: Bibliography	65
9.1 > How to get the latest versions of documents	65
9.2 > Documents about the VisionPass SP terminal	65

10 / Annex 3: Support	67
10.1 > Troubleshooting	67
10.2 > Technical Support and Hotline	67

1 / Introduction

1.1 > VisionPass SP terminal

Congratulations for choosing VisionPass SP face recognition terminal.

To ensure the most effective use of your VisionPass SP terminal, we recommend that you read this Installation Guide completely.

1.2 > Scope of the document

This guide deals with the installation of VisionPass SP, which is made up of the following list of products:

VisionPass SP Commercial Name	Biometrics	Contactless smartcard reader		Regulatory Model Number (*)
		iCLASS® SEOS®	MIFARE® DESFire®	
VisionPass SP MD	✓		✓	MPH-AC008A
VisionPass SP MDI	✓	✓	✓	MPH-AC008A

(*) The Regulatory Model Number is the main product identifier in the regulatory documentation and test reports associated to the product.

1.3 > Safety Instructions

1.3.1 > DC supply

— — — means Direct Current (DC)

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 24V (-15% / +10%) 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 60950-1 or 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.

This product has been evaluated by UL in accordance to UL 294, Standard for Access Control System Units, Seventh Edition.

UL 294 performance levels:

Model Number	Access Control Line Security	Destructive Attack Level	Endurance	Stand-by Power	Conditions
MPH-AC008A	Level 1	Level 1	Level 4	Level 1	NA

For UL 294 compliance the product is to be powered via a UL 294 power supply or access control panel with a 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.

1.3.2 > Power Over Ethernet Plus (POE+)

The terminal is a Class 4 (25.5 W) PD (Powered Device) and required Power Over Ethernet Plus (POE+): 42,5-57V 25,5W.

Power can be provided through RJ-45 connector using a PSE (Power Sourcing Equipement) IEEE802.3at type 2 compliant.

For UL compliance, the units shall be powered via a UL 294B PSE power supply.

Note: UL compliance was verified with Phihong model POE36U-1AT-R Primary rated 100-240VAC 1Amp 50-60Hz; 56VDC, 0.6A Pin 3,6 Return = Pin 1,2

1.3.3 > Photobiological safety

This product has been tested according to IEC 62471:2006 "Photobiological safety of lamps and lamps systems") and is classified as exempt risk.

1.4 > Wiring Recommendations

IDEMIA recommends using an AWG16 gauge and 24V power supply when PoE+ supply is not used.

The voltage specified is the one measured on the product block connector: 12V-24V (-15% / +10%).

The voltage drop due to the cable shall be taken into account. The following table shows the maximum distance between power supply and one (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

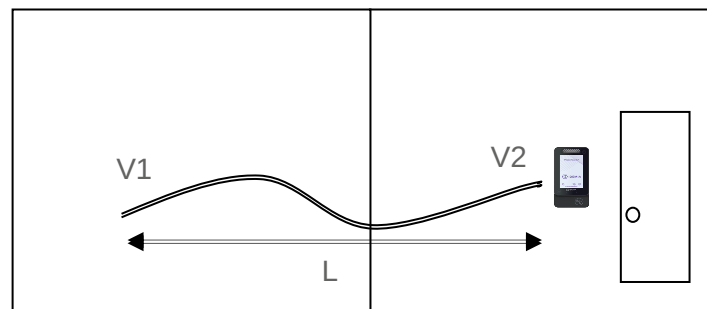


Figure 1: Power supply voltage dropout considerations

Drop voltage = loss of power due to wire resistance and its length: $V_2 = V_1 - \text{Drop voltage}$

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

1.5 > Regulatory, safety and Environmental notices

1.5.1 > European Union (CE) regulatory notices

Declaration of Conformity



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

Ecodesign Directive 2009/125/EC

RoHS Directive 2011/65/EU and 2011/65/UE

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

VisionPass SP terminals are intended to be used for professional application only (buildings, airport...).

The full Declaration of Conformity is available on demand to your reseller. Please, provide him the product model name or its Regulatory Model Number (Model on the label).

Products with wireless features (EMF)

This product meets the provisions of the EU's Council recommendation 1999/519/EC on the limitation of the exposure of the general public to electromagnetic fields (0 Hz to 300 GHz).

The device must be installed to provide a separation distance of at least 20cm from all persons.



1.5.2 > USA (FCC) regulatory notices

User Information according to FCC 15.21:

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

User Information according to Part 15 Statement acc. to FCC 15.19:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) this device may not cause interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

This device complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This device must be fixed installed.

Responsible Party:

IDEMIA Identity & Security, N.A

14 Crosby Drive, 2nd Floor

Bedford MA, 01730

USA

NOTA : *This equipment has been tested and found to comply with the limits for a Class B digital device, 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.

The product FCC ID is: ZBW-MPHAC008A.



1.5.3 > Canada (IC) regulatory notices

WARNING TO USERS IN THE CANADA

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

- (1) This device may not cause interference
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

This device complies with Industry Canada's defined levels of RF exposure requirements, limits set forth for an uncontrolled environment.
This device must be fixed installed.

Responsible Party:

IDEMIA Identity & Security Canada Inc.
Company Number: 907531-3
Address: 2872 Bristol Circle
Suite 100
Oakville, Ontario L6H 6G4
Canada

The product IC ID is: 11472A-MPHAC008A.

ATTENTION POUR LES UTILISATEURS AU CANADA

Cet appareil contient des émetteurs / récepteurs exemptés de licence conformes aux RSS (RSS) d'Innovation, Sciences et Développement économique Canada. Le fonctionnement est soumis aux deux conditions suivantes :

- (1) cet appareil ne doit pas provoquer d'interférences, et
- (2) cet appareil doit accepter toutes les interférences, y compris celles susceptibles de provoquer un fonctionnement indésirable de l'appareil.

Cet appareil est conforme aux niveaux définis par Industrie Canada en matière d'exposition aux radiofréquences, limites établies pour un environnement non contrôlé.

Cet appareil doit être installé de manière fixe.

Partie responsable :

IDEMIA Identity & Security Canada Inc.
Company Number: 907531-3
Adresse : 2872 Bristol Circle
Suite 100
Oakville, Ontario L6H 6G4
Canada

L' IC ID du produit est: 11472A-MPHAC008A.

1.5.4 > Brazil (Anatel) regulatory notices

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.

Para maiores informações, consulte o site da ANATEL : www.anatel.gov.br

1.6 > Others recommendations

Potential safety conditions notice

If you notice any of the following conditions (or if you have other safety concerns), do not use the product: crackling, hissing, or popping sound, or a strong odor or smoke coming from the product. It is normal for these conditions to appear when an internal electronic component fails in a safe and controlled manner. However, these conditions may also indicate a potential safety issue. Do not assume it is a safe failure. Turn off the product, disconnect it from its power source, and contact technical support for assistance.

Disposal of waste equipment by users



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.

1.7 > Recommendations for terminal implementation

Every installation is unique. Sometimes the issues are well defined and can be handled in a standard fashion; sometimes the issues are very specific and may not be immediately recognizable.

IDEMIA recommends following these steps for a successful installation:

Plan the installation - Choose the type of hardware required, decide if a network is required, and decide on the location and number of required terminals.

Unpack all items - Unpack all items and check against the packing list.

Install network hardware components - Install the cabling and components needed to run the system.

Install software - Install the software needed to set up the terminals.

Pre-configure device - Connect the terminals to the Ethernet, supply power to the terminals, and pre-configure the terminals.

Mount devices - Mount the terminals in their final locations

Power distribution and device hook up - Connect the terminals wiring via the back panel.

Power-up procedure - Check the power connections, and then start the system safely. First Boot Assistant screen is displayed, where you can perform **fundamental** configuration.

To secure properly an access, IDEMIA recommends installing the VisionPass SP terminal as a part of the typical Access Control environment described in the figure below.

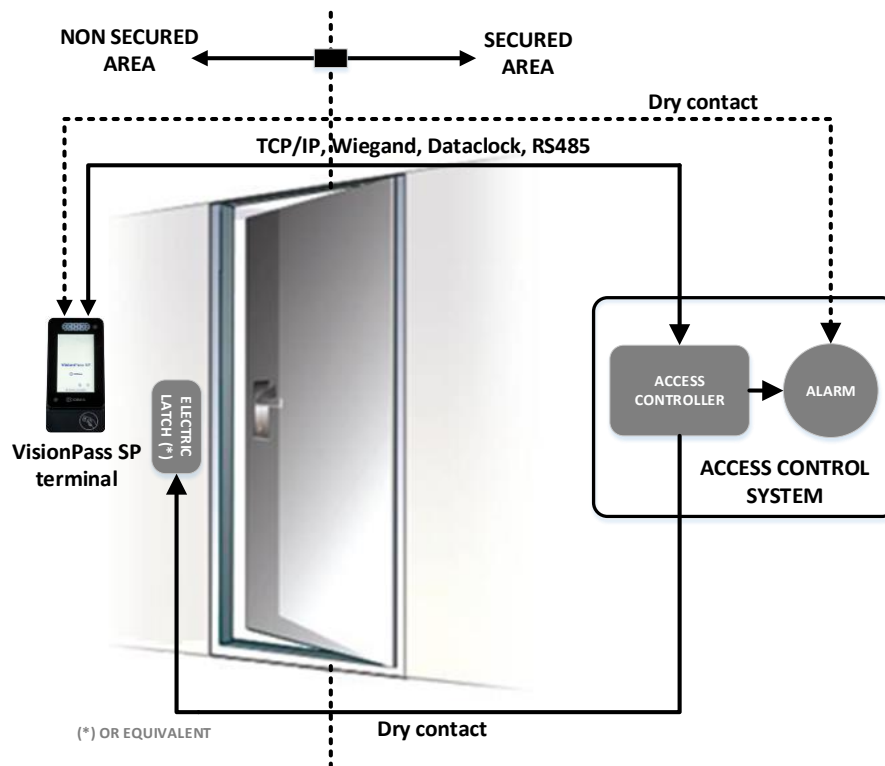


Figure 2: Implementation recommendations

This environment comprises:

The VisionPass SP terminal itself

Its role is to perform one-to-many biometric identification or one-to-one biometric verification, i.e. to identify the individual who is presenting his face by comparing his biometric data with the references previously stored in the terminal database (in the form of biometric templates) or to verify his identity using the reference stored in a contactless card presented to the terminal.

An Access Controller (3rd party product)

The Controller is the element which controls the access rights of the individuals to the secured area. For that reason, it must be located in the secured area.

The individuals who are authorized to access the secured area have their User ID listed in a so-called "Authorized User List" (in contrast with a banned card list).

The VisionPass SP terminal and the Controller are communicating according to one of the TCP/IP, Wiegand, Dataclock or RS485 protocols¹:

The VisionPass SP terminal sends User ID to the Controller

The Controller sends its decision to the VisionPass SP terminal (which displays access granted or access denied depending on the answer)

¹ Note: UL only verified Wiegand

The VisionPass SP terminal sends an alarm signal to the Controller as soon as a malicious operation is detected (terminal pulled out from the wall or opened for maintenance operations); refer the paragraph dealing with anti-pulling and anti-tamper switches for more explanations.

The Controller is part of the global Access Control System of the secured area, which can provide useful features such as manage:

- Authorized user lists (i.e. for VisionPass SP),

- Banned card lists (i.e. for lost user cards),

- An access request log (who and when, access granted or denied ...),

- An event log (i.e. tamper detection, access control for evacuation of the building ...).

The VisionPass SP terminal is able to work alone, without Controller, but the protection level of the secured area is lower.

An Alarm (3rd party product)

The VisionPass SP terminal sends the command to activate the Alarm as soon as a malicious operation (terminal pulled out from the wall or having its bottom cover opened out of maintenance operations) is detected; refer the paragraph dealing with anti-pulling and anti-tamper switches for more explanations.

This element can also be connected directly to the VisionPass SP terminal through a dry contact and shall be for access control applications use only.

Please note that alarm points are not used for UL burglary standard applications.

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

This element once activated opens the access. The Controller is the one which sends the command to activate the latch if access is granted (i.e. if the individual's User ID is listed in the Controller Authorized User List). Connection between these two elements is done through a dry contact.

Please note that if a door latch is used for UL compliance it shall be UL 294 Access Control Single point device or UL 1034 Burglary Resistant Electronic door strikes/latches compliant.

2 / General description

2.1 > Components of the initial package

1. One (1) Terminal
2. One (1) Wall plate
3. One (1) Cable kit
4. One (1) Cover plate
5. Documentation package

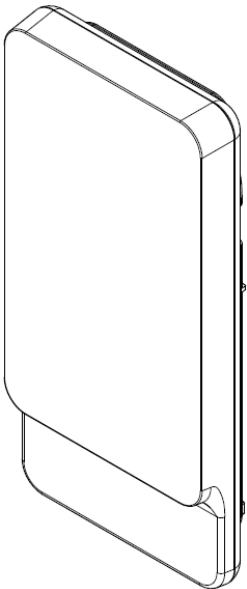
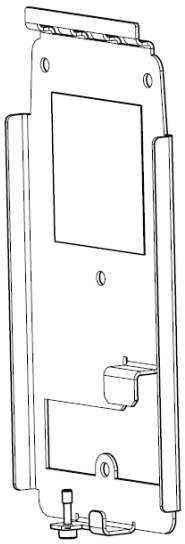
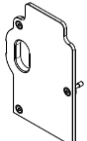
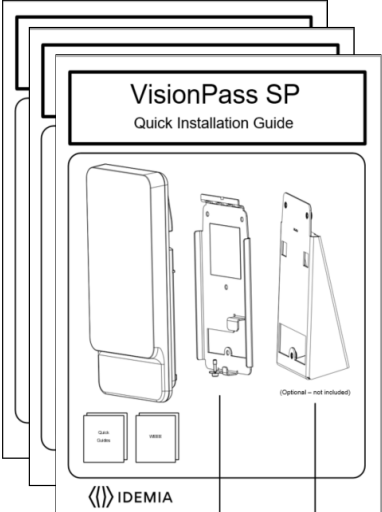
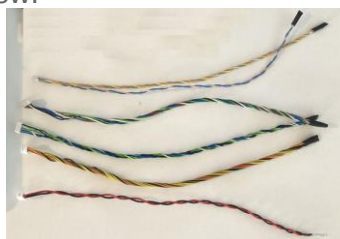
				
Terminal	Wall plate	Cable kit	Cover plate	Documentation package

Figure 3: Box content

The cable kit is composed of 5 cable nappes with connectors. Description of colors and functions are provided in 4.1 > Wiring overview.



2.2 > Terminal's front view description



Figure 4: VisionPass SP terminal front view

2.3 > Terminal's rear view description

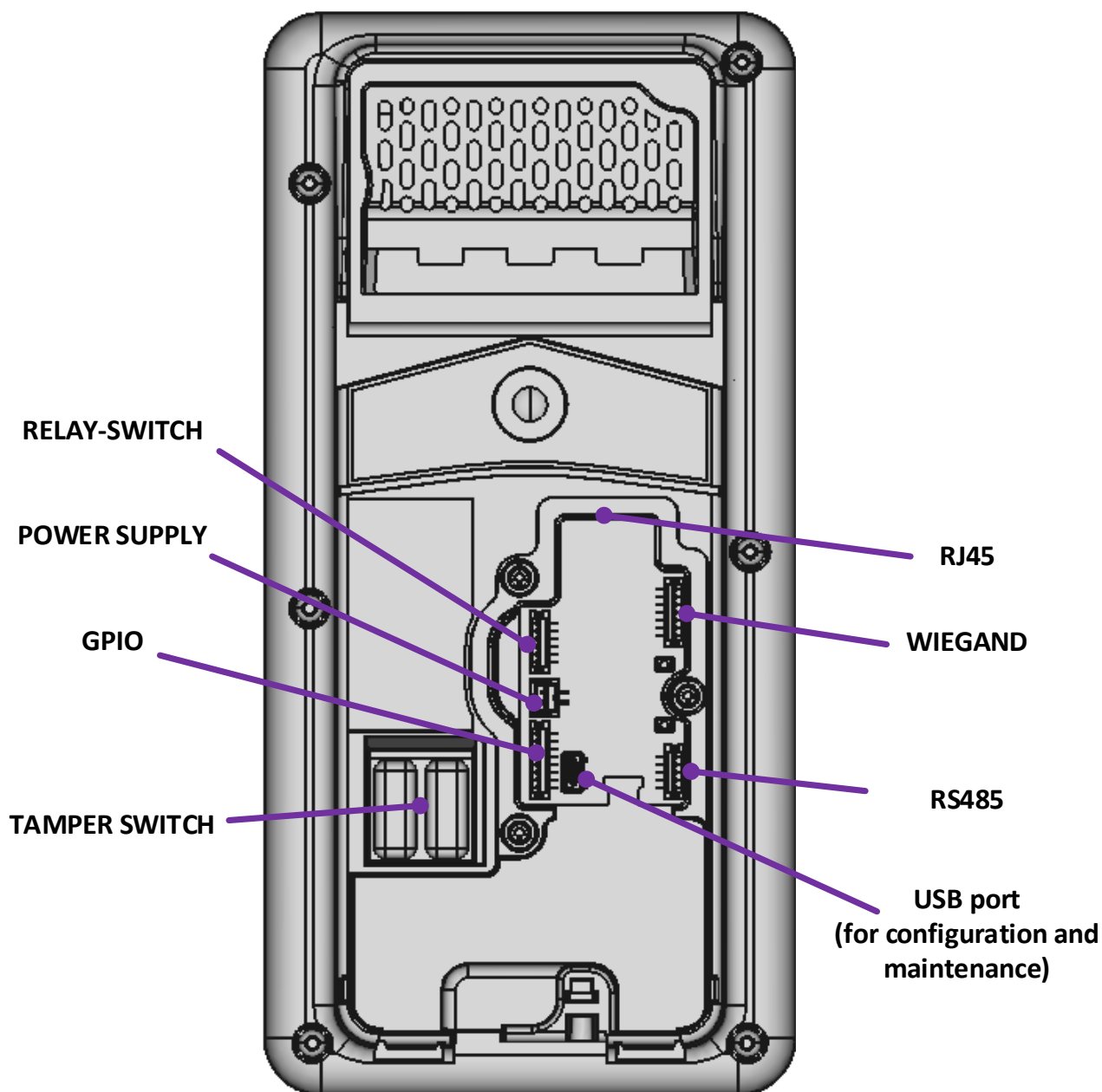


Figure 5: VisionPass SP terminal rear view

2.4 > VisionPass SP Technical Characteristics

Item	Description
Access control modes	Identification (search for faces in a local database)
	Authentication with contactless smartcard, with or without face check
	Multi-factor: identification or authentication
	Proxy: the access control check is fully driven by a remote system
Man Machine Interface	5" WVGA Touchscreen LCD
	Buzzer
Biometrics	Face acquisition: White leds and Infra-red leds
	False Acceptance Rate (FAR) adjustable from 1% to 10 ⁻⁷ % Note: self-declared and not evaluated by UL
	Database capacity: up to 50 000 users (depending of product configuration)
Log capacity	1 000 000
LAN/WLAN connection	For terminal configuration and data transfer: Ethernet 100 Base T Either TCP, SSL or TLS protocol Note: for UL compliance, the connection is for supplemental use only and is not evaluated by UL

RFID cards (depending on product version)	MIFARE® Classic 1KB & 4KB (4b and 7b UID) MIFARE® Plus cards ISO/IEC 14443 Type A, 13.56 MHz, Baud rate: 106kBits/s
	DESFire® EV0 (first generation of DESFire® cards, 3DES only) DESFire® EV1 (3DES and AES) DESFire® EV2 (3DES and AES) is supported in compatibility EV1 mode ISO/IEC 14443 Type A, 13.56 MHz, Baud rate: 106kBits/s
	SmartMX® (dual technology MIFARE® and DESFire®)
	HID® iCLASS cards: iCLASS® legacy, iCLASS® SR, iCLASS® SE ISO/IEC 15693, 13.56 MHz, Baud rate: 26.48kBits/s
	HID® SEOS® ISO/IEC 14443 Type A, 13.56 MHz, Baud rate: 106kBits/s
Radio frequency characteristics	Frequencies and magnetic fields or RF output power: RFID: 13.553 to 13.567 MHz: 10 dBμA/m max Radar sensor: 60 to 61.50 GHz: 10 dBm (Output power EIRP) - For local compliance, this radar sensor can be turn off with no radio frequency emission in 60 to 61.50 GHz. Please refer to the administration guide.
Serial port	The serial port supports WIEGAND, DATACLOCK (ISO2), RS485 protocols Note: only WIEGAND was evaluated by UL
GPIO	3 GPI, 3 GPO (not evaluated by UL)
Output relay switches	Access granted: 1 switch two outputs (normally “open” and normally “closed”) 30VDC – 1A max (Resistive loads, 100 000 cycles)

USB host port	Terminal configuration through a USB mass storage key Not evaluated by UL
Input signals	LED1/LED2 to activate the access granted relay Output type required: Open drain or 5V+/-5%
Power supply	12 to 24 VDC (-15% / +10%) power supply (2.5A min @12VDC, 1.25A min @24VDC) POE+ 42.5-57V 25.5W Note for UL 294 Compliance power supply shall be UL 294 with power limited output
Security of the terminal	Anti-tamper-pulling switches Tamper-pulling detection: one switch closed when product wall mounted, open when pulled out
Size and weight	H x W x D: 211 mm x 103 mm x 37 mm (8.31" x 4.1" x 1.46") Weight: 0.69kg (Device 0.53kg + wall mounting 0.12kg + cabling 0.04kg)
Environmental conditions	Operating temperature: -10 °C to +45 °C (14°F to 113°F)
	Operating humidity 10 % < RH < 80 % (non condensing)
	Storage temperature -25 °C to +70 °C (-13°F to 158°F)
	Storage humidity 5% < RH < 95 %
	For UL 294 compliance, the product is rated for indoor use
	The terminal should be installed in controlled lighting conditions Avoid direct exposure to sunlight or to UV lights

3 / Installation procedure

3.1 > Before proceeding to the installation

Make sure that you have all the components described in § “2.1 > Components of the initial package” section at your disposal.

Remove the wall plate from the terminal. Keep these elements at hand.

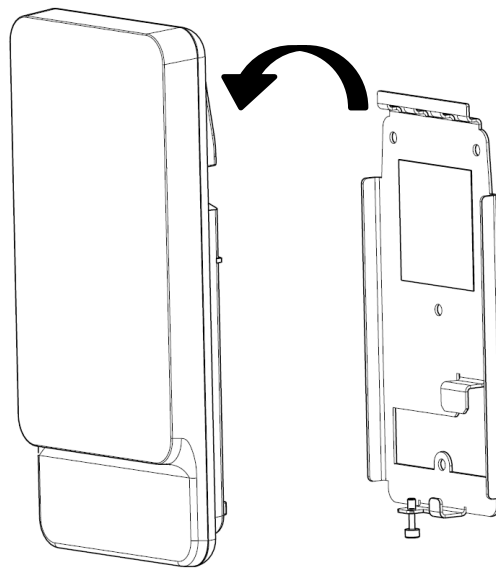


Figure 6: Removing wall frame



For an optimal use, the terminal must be installed in an area where the lighting conditions are controlled. Avoid direct exposure of the sensor to the sun light and ensure good ambient lighting for face detection if used.

⇒ **READ FIRST §8 / Annex 1: placement recommendations**

3.2 > Installation

Required tools (not supplied)

Three (3) raw plugs + three (3) screws ø4mm max and length adapted to the wall material.

One (1) screwdriver adapted to screws above.

One (1) Drill (with a drill bit diameter adapted to raw plugs above).

One (1) hole saw (depending on installation case).

A (1) H2 screwdriver

A (1) Torx T10 screwdriver

Deadbolt/door strike

Snubber diode required to protect regulated DC power supply from inductive kickback (1N4007 diode or equivalent recommended)

Separate power supply for the deadbolt/door strike based on supplier's recommendations.

External relay (if required)

Networking cable

For UL 294 compliance, an earthed screen in the wire or around all wires to/from product is only required when the wires share space/compartment/tube with high voltage cables.

Equipment from the initial package to use

One (1) Terminal

One (1) Wall plate

One (1) Cable kit

One (1) Cover plate

3.3 > Step by step procedure

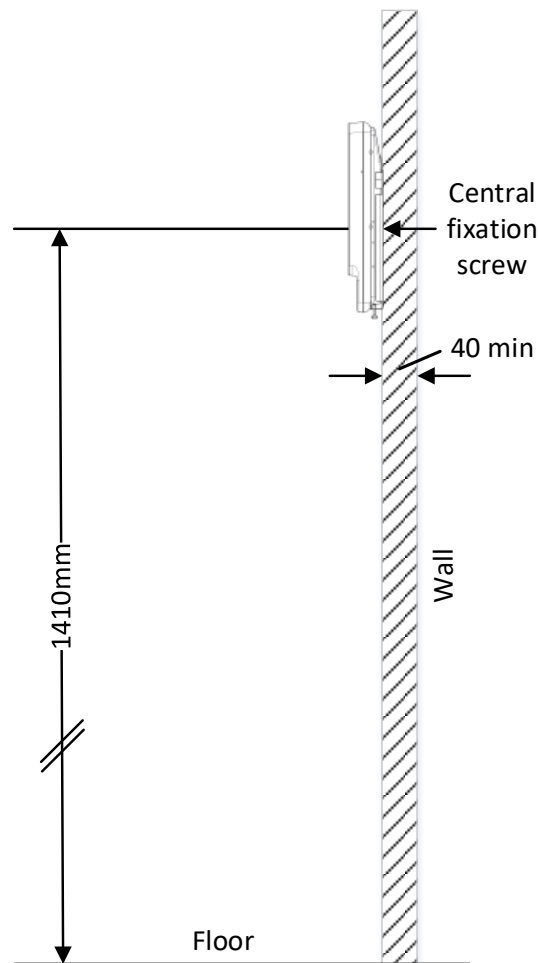


Figure 7: Face camera viewing angle

The recommended height for fixing of the terminal is 1.41 m (distance between the ground and the central fixation screw).



For an optimal use, the terminal must be installed in an area where the lighting conditions are controlled. Avoid direct exposure of the sensor to the sun light.



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



The strength of the attachment depends on the solidity of the wall on which the terminal is mounted.

3.3.1 > Drill the mounting holes



Be sure that the wall behind the wall plate has a good flatness.

This template can be found at the right scale in the “Quick Installation Guide”. The figure below is not at the right scale.

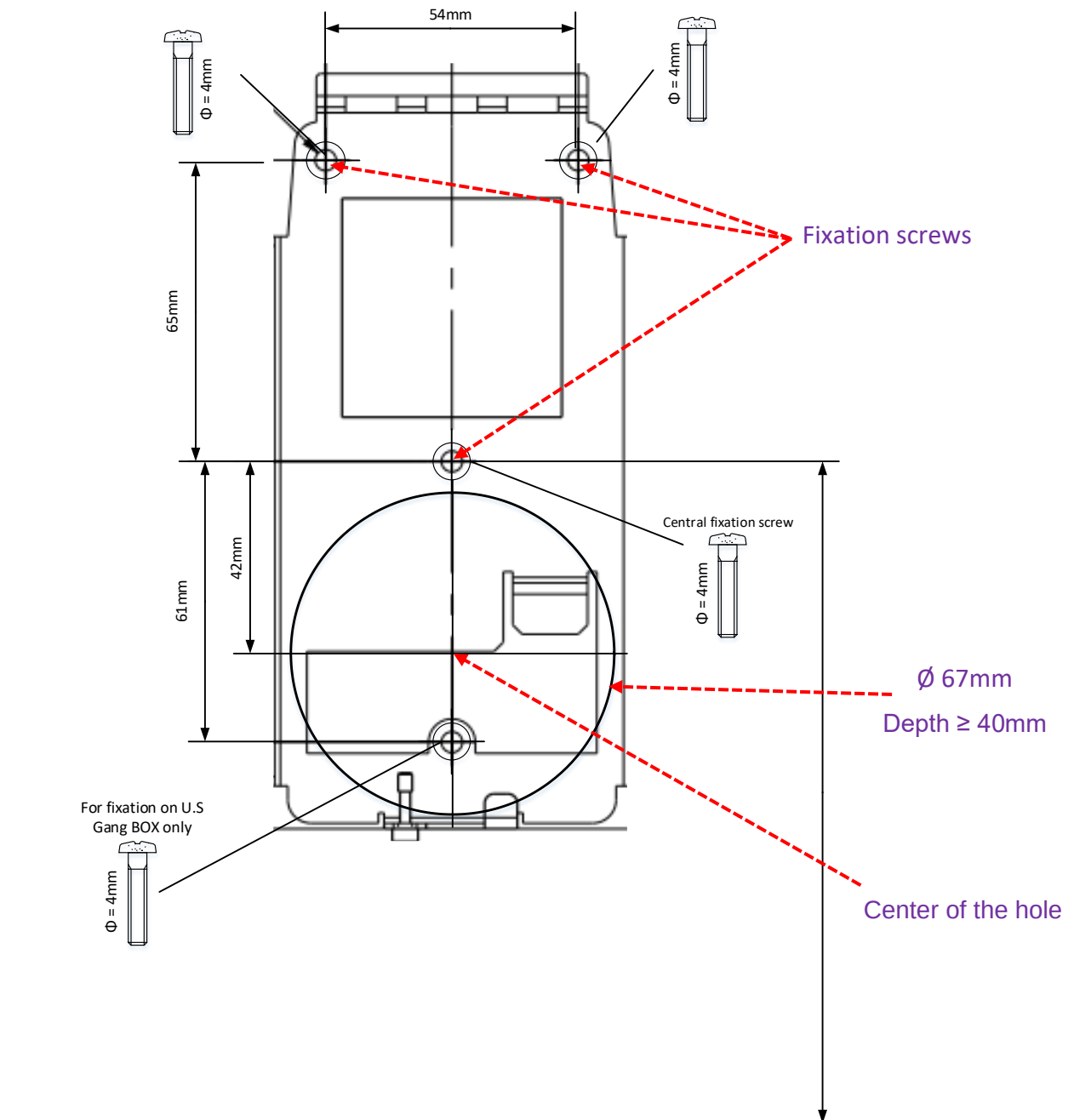


Figure 8: Drilling template

If not present, drill in the wall a hole with a diameter adapted to the width of the terminal and the cable to be hosted in (see Figure 8: Drilling template).

The 67 mm diameter hole (cf. drilling template) should be at least 40 mm deep in order to fit the connections and cables. A deeper hole as recommended is possible, to make the connection process easier.

Confirm the presence inside the hole of all the cables needed for the electrical installation.

Drill in the wall 3 holes with a diameter adapted to fixation screws and fit them with the raw plugs (see Figure 8: Drilling template).

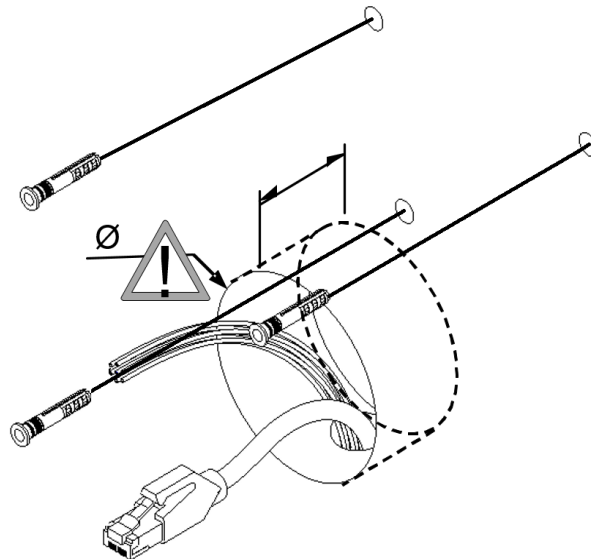


Figure 9: Fit the hole with the raw plugs



Be sure that a sufficient space is reserved in the wall for the passage of cables, in particular for Ethernet.

3.3.2 > Make the connections



Before any connection, switch off / unplug power supply.



Before making the connection between the installation cable and the ones provided in the cable kit, cut them in the middle of heat shrink tube (except for power supply cable).

Please refer to § “4 / Electrical interface” for explanations of how cables/wires should be connected, according to wire color code.

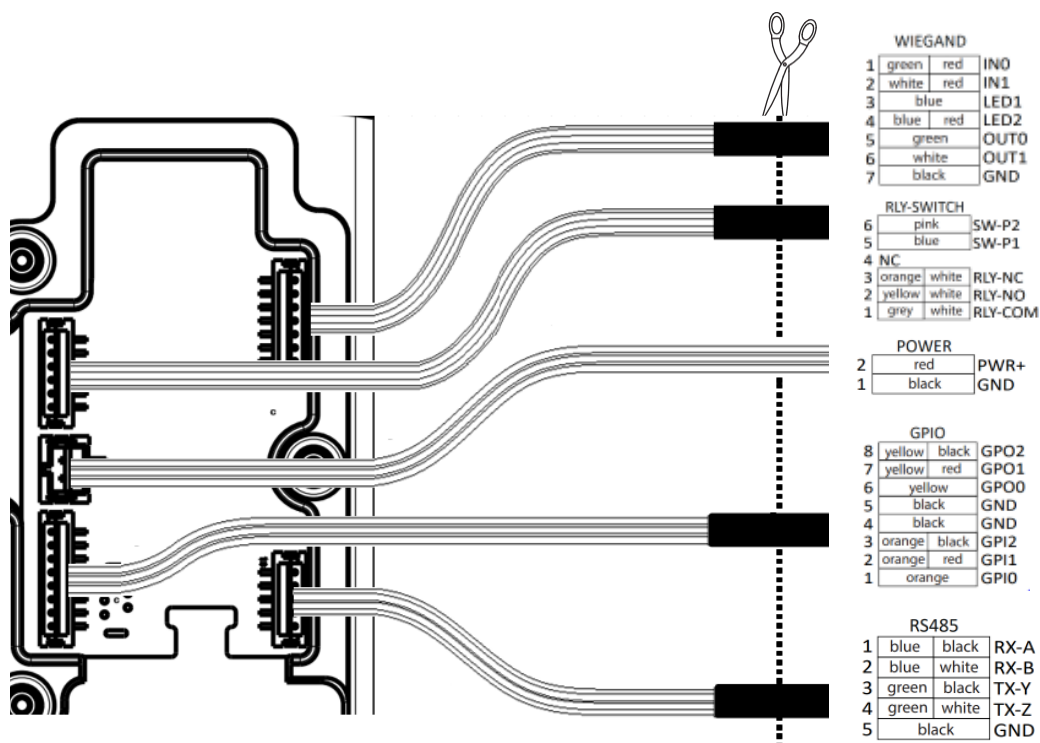
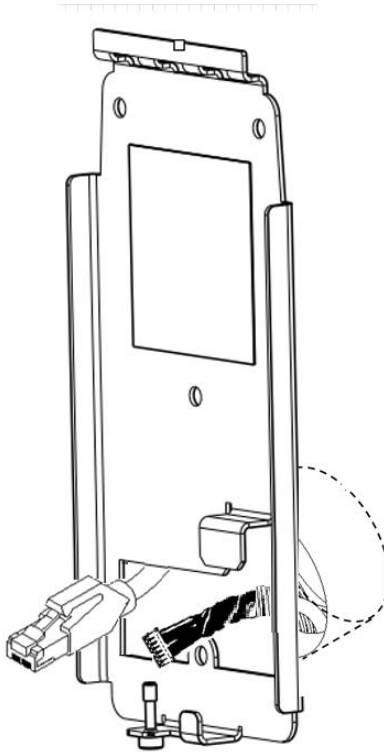


Figure 10: Cable preparation: cable position for water tightness

Installation cable for wiring shall be AWG 16 to 22, length shall be adapted to the size of the hole in the wall, to terminal connections, and to the distance between the electric source and the terminal itself.

3.3.3 > Attach the wall plate on the wall

Fit the cables through the wall plate:



Fix the wall plate to the wall with the 3 screws:

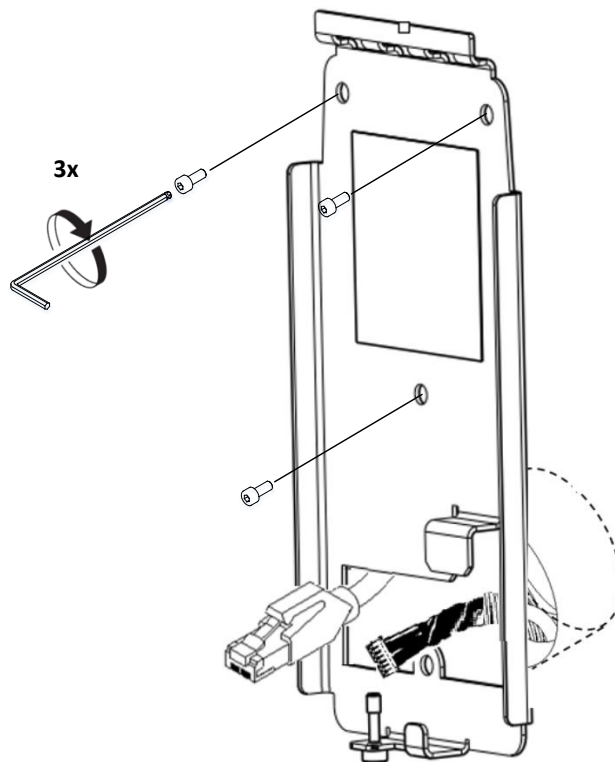


Figure 11: Wall plate fixation on the wall

3.3.4 > Connect the cables to the terminal

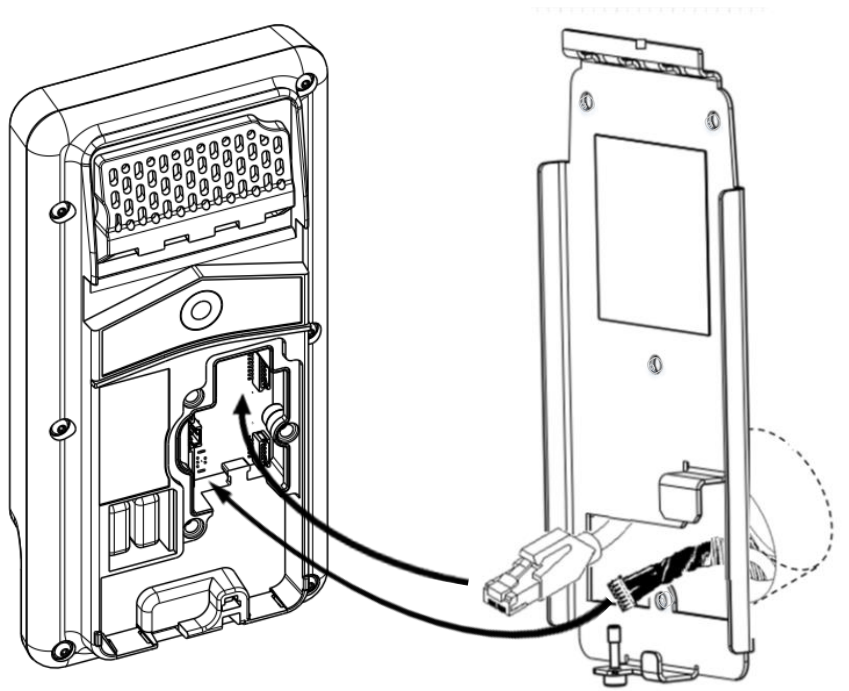


Figure 12: Cable connection to the terminal

3.3.5 > Fix the cover plate

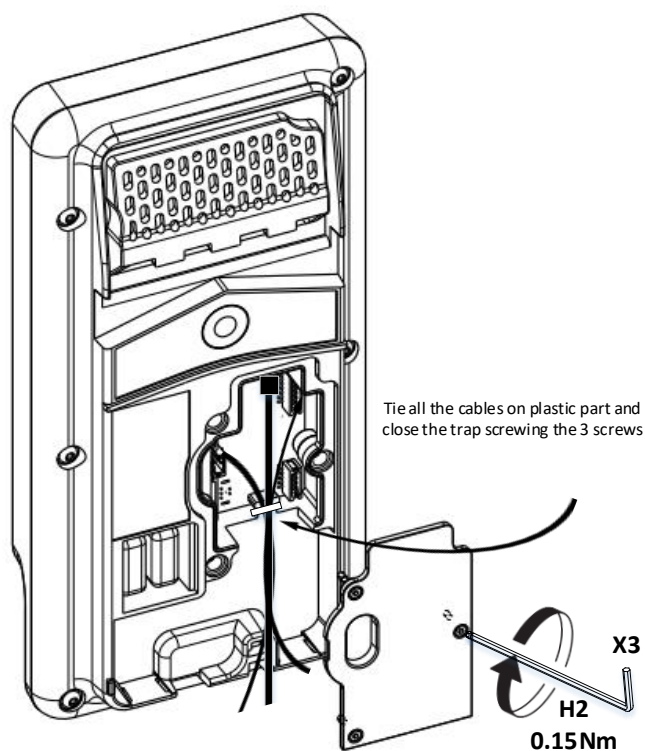


Figure 13: Fix the cover plate

3.3.6 > Add silicon around cable and cover plate (optional)

Add silicon for dust/particles => required for IP6X sealing only

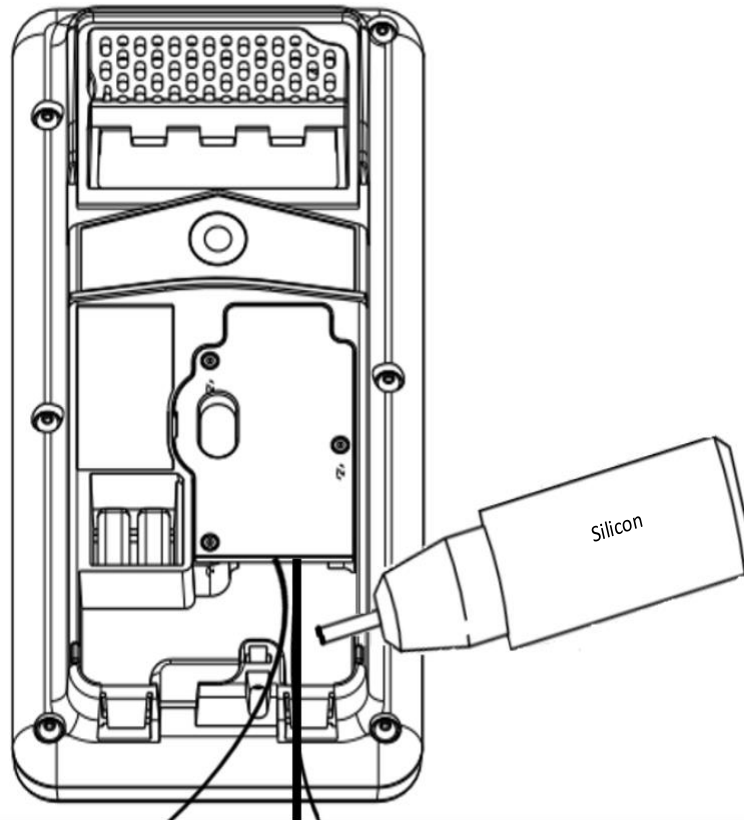
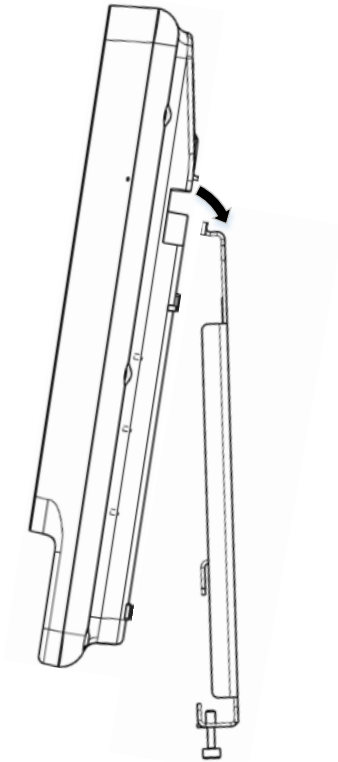


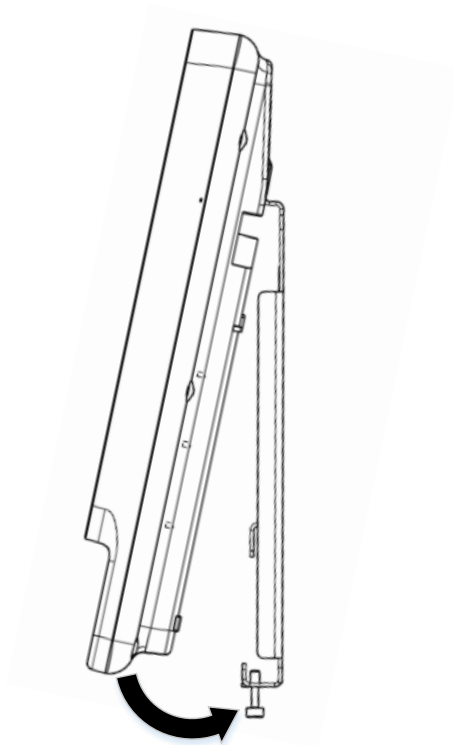
Figure 14: Add silicone (optional)

3.3.7 > Fix the terminal to the wall plate

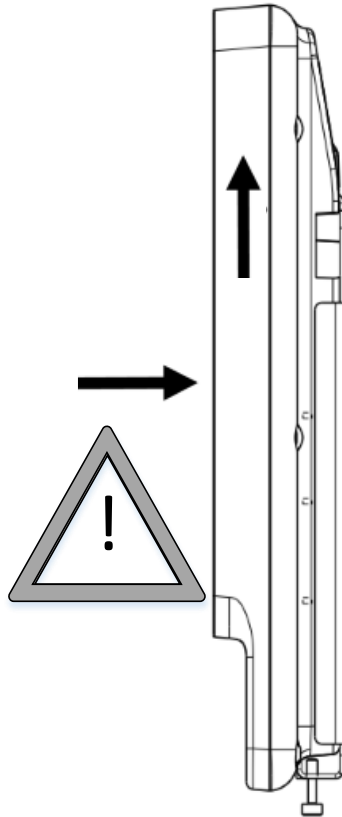
A - Place the device on the wall plate:



B - Turn the device:



C - Translate the device upwards and push:



D - Keep pushing and translate the device down:

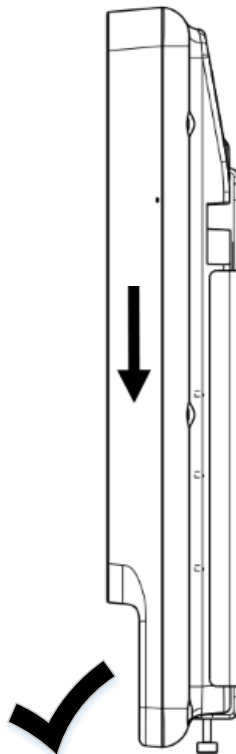


Figure 15: Product fixation on wall frame

Then to secure the device on the plate, attach the last screw on the bottom of the device:

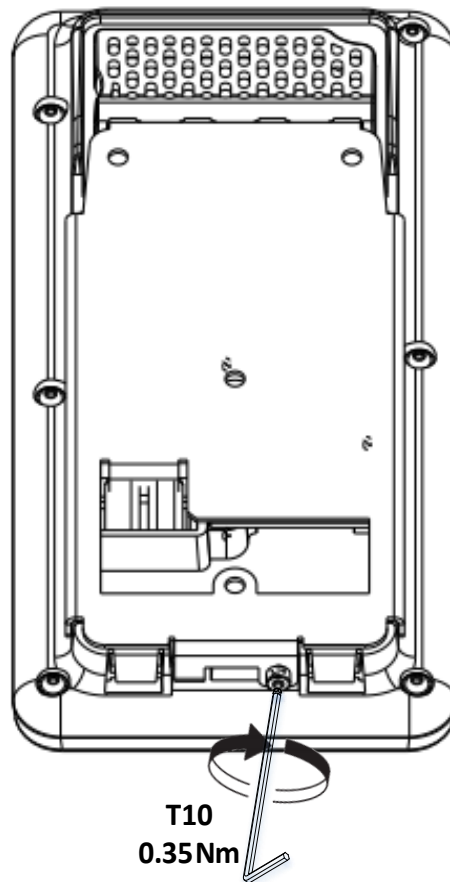


Figure 16: Locking the product

The hardware installation of the product on the wall is complete!

Power can be switched ON just after closing it.



Depending on storage conditions during transportation, condensation may appear in front of cameras after the first power on and disappear in 2 hours.



If the product has to be stored for a long time (more than 2 hours), do not forget to restore its configuration before use.

4 / Electrical interface

4.1 > Wiring overview



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).



Power supply ground shall not be used for peripheral ground. All other grounds can be used indifferently.

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

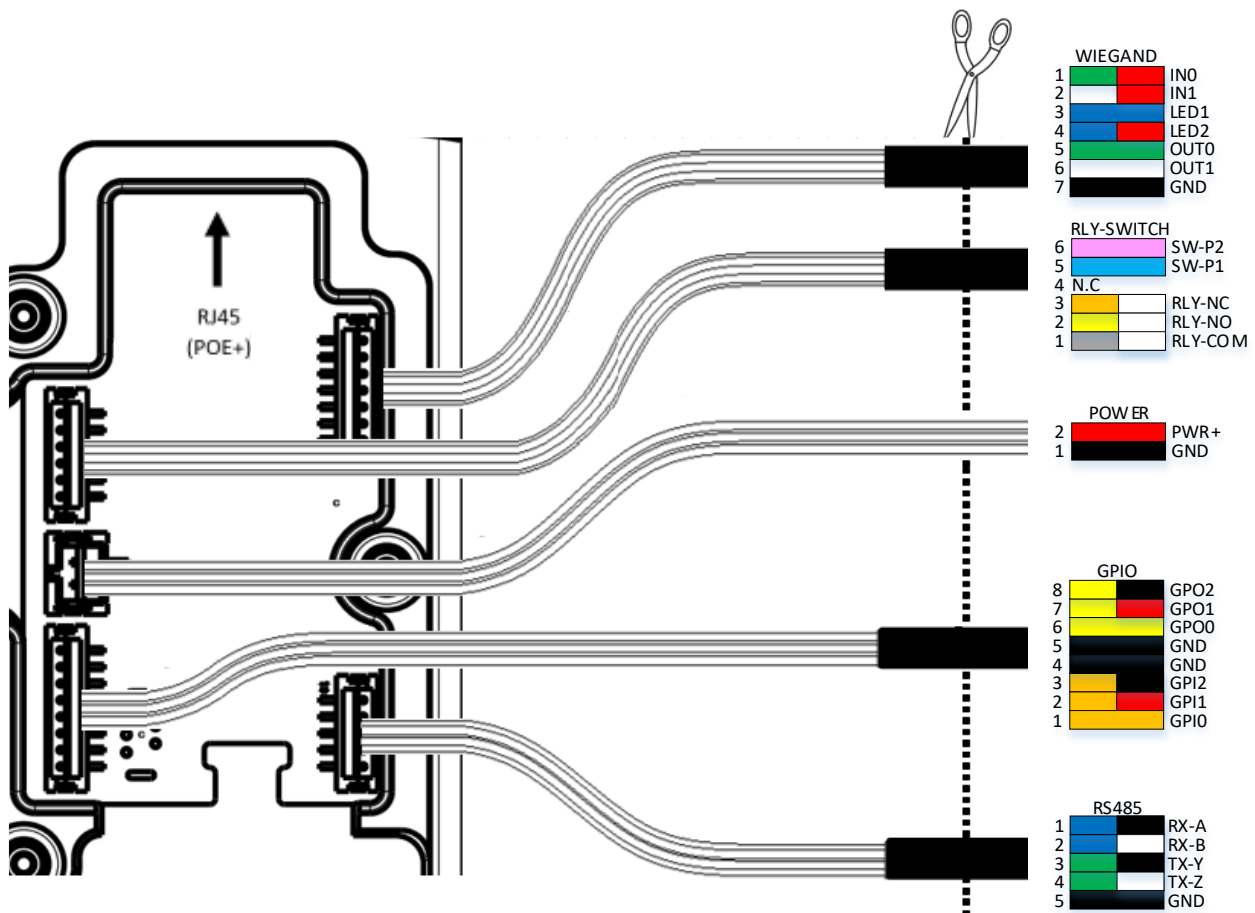
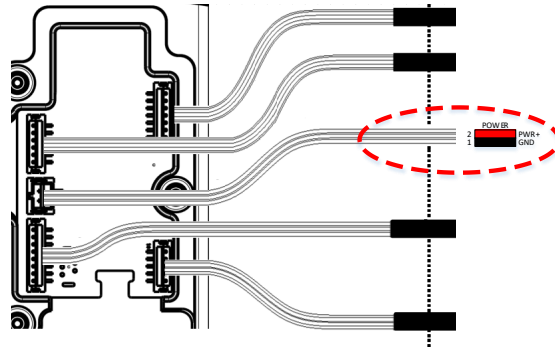


Figure 17: Cabling layout

4.2 > Power Supply

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

External Power supply



POWER				
2	Red	PWR+	In	Positive 12-24 Volts, power supply
1	Black	GND	In	Ground power supply

Figure 18: Power supply wiring

The External power supply

Must comply with IEC 60950-1 or IEC 62368-1 standard marked Class 2, Limited Power source (LPS) 12V to 24V DC (-15% / +10%, regulated and filtered) 2.5A min at 12V.

If sharing power between devices, each unit must receive 2.5A at 12V (e.g. two units would require a 12VDC, 5A supply).

IDEMIA recommends using a 24V 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 voltage drop due to the cable shall be taken into account. The table below shows as an example the maximum distance between power supply and one (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



If several terminals are powered by the same cable, make sure to select a wire gauge that complies with maximum voltage drop, cable length, and power source minimum voltage rating.

PoE+ (Power over Ethernet Plus)

VisionPass SP terminal's power supply can also be provided by the Ethernet using RJ45 connection (Power over Ethernet Plus mode - IEEE802.3at type 2 compliant).

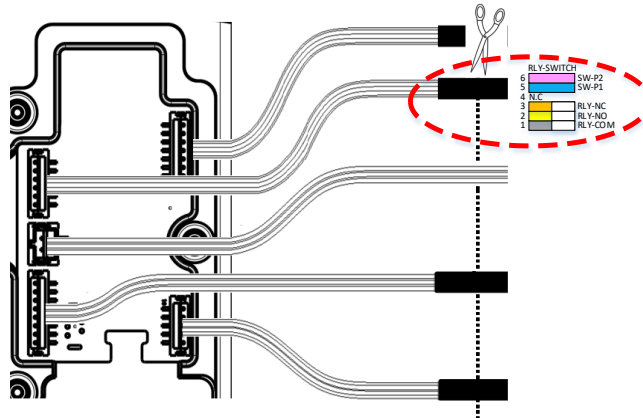
The terminal may be powered via a UL 294B PSE PoE+ Limited power source (IEEE802.3at type 2 compliant).



If several terminals are powered through the same PoE+ switch, make sure the switch is capable of providing enough power to each device (25.5W).

Please refer to “Using PoE+” recommendations section 7 / for more details about the best practices for powering the VisionPass SP terminals with PoE+.

4.3 > Output Relay



RELAY				
3	Orange / White	RLY_NC		Contact relay (normally closed)
1	Grey / White	RLY_COM		Contact relay common
2	Yellow / White	RLY_NO		Contact relay (normally open)

Figure 19: Output relay wiring

Nominal characteristics of relay

Load characteristics:

1 A max @ 30 VDC (according to the safety extra low voltage requirements independently of the power supply),

Resistive load or inductive load; see warning information hereafter for inductive load,

The internal relay is designed for at least 100 000 cycles (resistive load).



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

Example of connection for electrical door locks

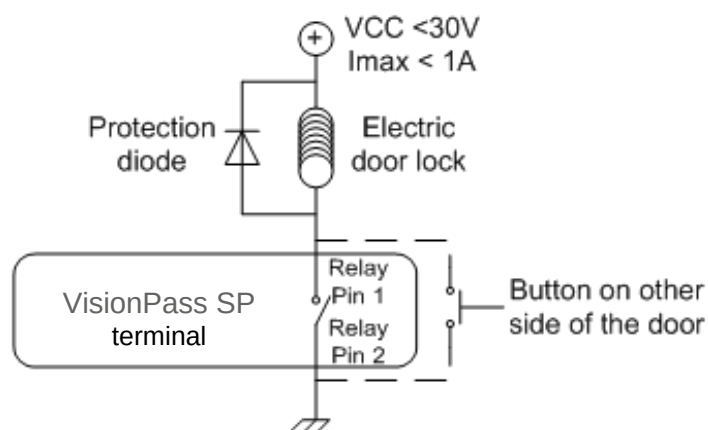
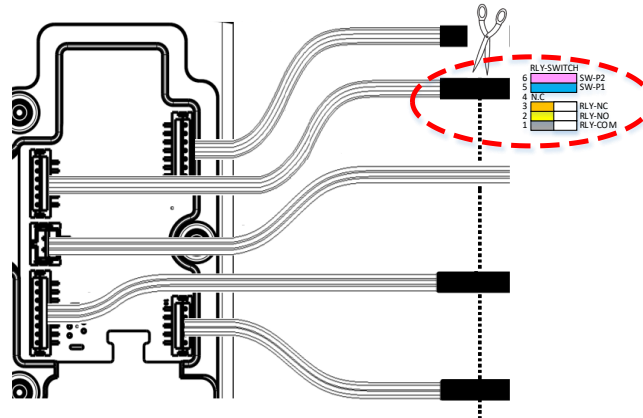


Figure 20: Example of electric latch connection

4.4 > Tamper Switch



SWITCH				
6	Pink	SW-PIN2		Strip on tamper switch
5	Light Blue	SW-PIN1		Tamper switch contact

Figure 21: Tamper switch wiring

Operating principle for the switch

Product installed on the wall plate: switch enabled (contact closed).

Product opened (rear connectors accessible): switch disabled (contact open).

Nominal characteristics of switch block

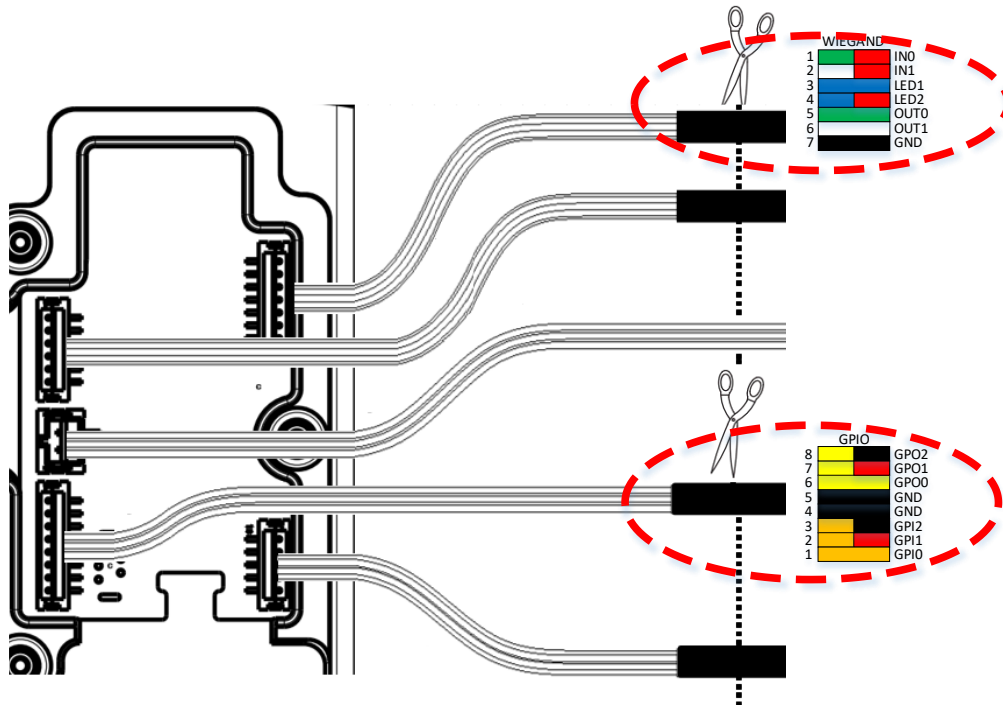
100 mA at 30 VDC max (Resistive load) according to the safety extra low voltage standard.



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.

4.5 > Wiegand wiring

Wiegand input



WIEGAND				
1	Green / Red	IN0	In	Wiegand IN D0 (Output type required: Open drain or 5V+/-5%)
2	White / Red	IN1	In	Wiegand IN D1 (Output type required: Open drain or 5V+/-5%)
7	Black	GND		Ground for Wiegand
GPIO				
6	Yellow	GPO0	Out	Wiegand LEDIN (typical = 5VDC) (option)

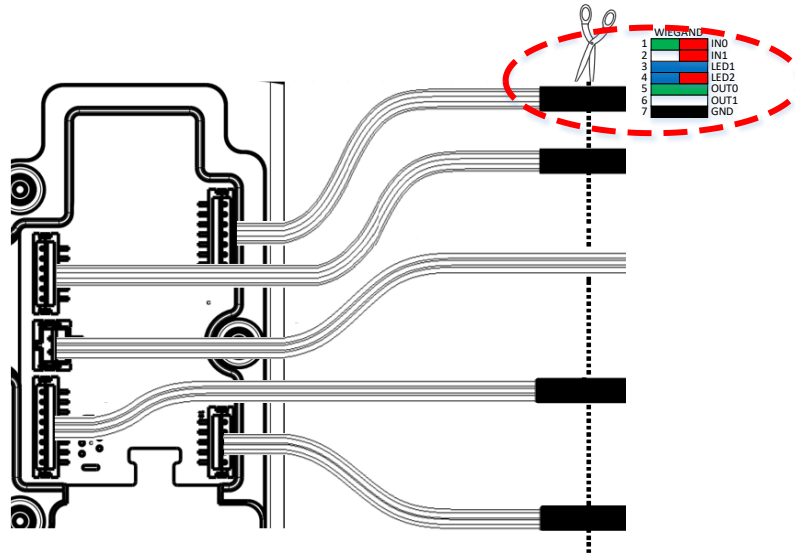
Figure 22: Wiegand input wiring



If pull-up's to 12V have been added on Wiegand IN D0 and Wiegand IN D1 inputs on a previous installation with a MorphoAccess® 500 Series terminal, these resistors must be removed to avoid any damage to the VisionPass SP terminal.

4.6 > Wiegand output

The following figure shows how to cable the wires of the serial port of the terminal for the Wiegand protocol



WIEGAND				
3	Blue	LED1	In	Wiegand LED IN 1 (option): panel feedback (Output type required: Open drain or 5V+/-5%)
4	Blue / Red	LED2	In	Wiegand LED IN 2 (option): panel feedback (Output type required: Open drain or 5V+/-5%)
5	Green	OUT0	Out	Wiegand OUT D0 (5V TTL)
6	White	OUT1	Out	Wiegand OUT D1 (5V TTL)
7	Black	GND		Ground for Wiegand

Figure 23: Wiegand output wiring

The use of LED1 and LED2 wires is described in the paragraphs below.

The controller supports neither LED1 nor LED2 signals

When the access controller has no relay contact to provide an answer to the VisionPass SP terminal, then the decision to emit either the “Access granted” signal or the “Access denied” signal is taken by another way. It is either the VisionPass SP terminal itself that decide, or it waits for the access controller answer through the local area network (TCP), or on the serial port in (RS485).

It is strongly recommended to disable the LED IN feature, to avoid any interference on VisionPass SP terminal behavior.

The controller supports only LED1 signal

When the access controller has only one relay contact which is dedicated to the “access granted” answer, this one must be connected between the LED1 and GND wires. The LED1 wire is set to the low level by closing the contact between the LED1 and the GND wires, and it means “access granted”.

The VisionPass SP terminal uses the timeout of the wait for a low level on the on LED1 wire or LED2 wire as “access denied” answer.

To minimize at most the waiting time of the user, the VisionPass SP terminal timeout value, must be adjusted to a value a little bit higher than the maximal value of the controller response time.

Warning: if the LED2 wire is connected, it must be constantly maintained in the high state.

The controller supports LED1 and LED2 signals

When the controller supports one relay contact for each of the possible answers then:

The « access granted » contact must be connected between the LED1 and the GND wires of the terminal

The « access denied » contact must be connected between the LED2 and the GND wires of the terminal.

The VisionPass SP terminal considers that:

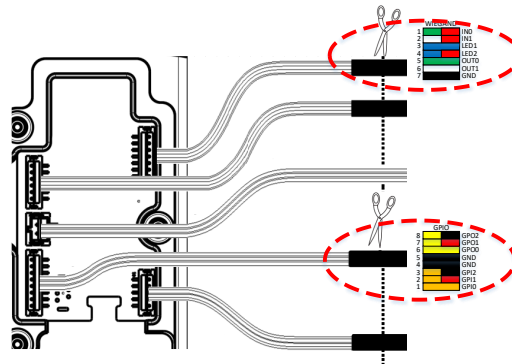
The answer of the controller is "access granted", when the controller puts the LED1 wire to the low state (by closing a contact between the LED1 and the GND wires), **and leaves the LED2 wire to the high state.**

The answer of the controller is "access denied", when the controller puts the LED2 wire to the low state (by closing a contact between the LED2 and the GND wires), **whatever is the state of the LED1 wire.**

The VisionPass SP terminal also considers that the answer of the controller is "access denied" in case of time-out while expecting for a closure between LED1 and GND wires, or between LED2 and GND wires.

4.7 > Serial port wiring

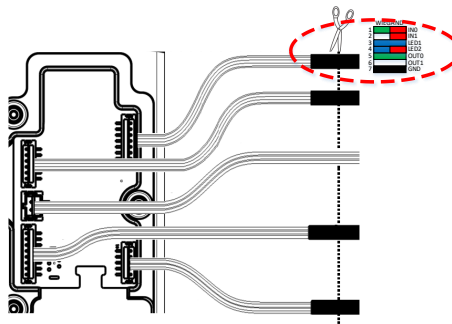
DataClock Input



WIEGAND				
1	Green / Red	IN0	In	Data (Output type required: Open drain only)
2	White / Red	IN1	In	Clock (Output type required: Open drain only)
7	Black	GND		Ground for Wiegand
GPIO				
6	Yellow	GPO0	Out	Card present signal (if configured, only one selectable for IDEMIA Legacy)

Figure 24: Serial port wiring – DataClock Input

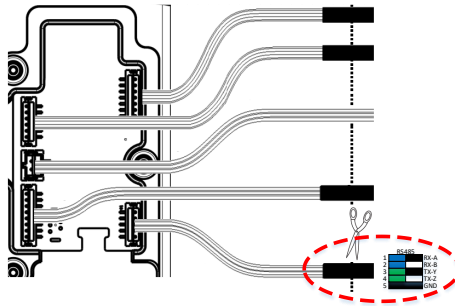
DataClock Output



WIEGAND				
3	Blue	LED1	In	LED IN 1 (option): panel feedback (Output type required: Open drain or 5V+/-5%)
4	Blue / Red	LED2	In	LED IN 2 (option): panel feedback (Output type required: Open drain or 5V+/-5%)
5	Green	OUT0	Out	Data (5V TTL)
6	White	OUT1	Out	Clock (5V TTL)
7	Black	GND		Ground for Wiegand

Figure 25: Serial port wiring – DataClock Output

RS485



RS485				
3	Green / Black	TX-Y	In/Out	RS485 Rx/Tx non inverting signal (A)
4	Green / White	TX-Z	In/Out	RS485 Rx/Tx inverting signal (B)
5	Black	GND		Ground

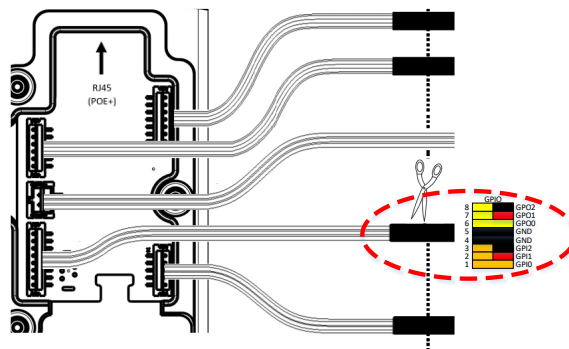
Figure 26: Serial port wiring – RS485

RS485 implementation is limited to half-duplex communication. So only Tx+, Tx- and ground reference signals are necessary.

Depending on the RS485 network, an impedance adaptation may be required.

For farthest terminal, a 120-Ohms resistor termination may be added outside the terminal between TX+ and TX-.

4.8 > GPIO wiring



GPIO				
8	Yellow / Black	GPO2	Out	Digital Output (5V – 5mA max)
7	Yellow / Red	GPO1	Out	Digital Output (5V – 5mA max)
6	Yellow	GPO0	Out	Digital Output (5V – 5mA max)
5	Black	GND		Ground
4	Black	GND		Ground
3	Orange / Black	GPI2	In	Digital Input (1,8V to 5V)
2	Orange / Red	GPI1	In	Digital Input (1,8V to 5V)
1	Orange	GPI0	In	Digital Input (1,8V to 5V)

Figure 27: GPIO wiring

Single Door Access Control (SDAC) implementation

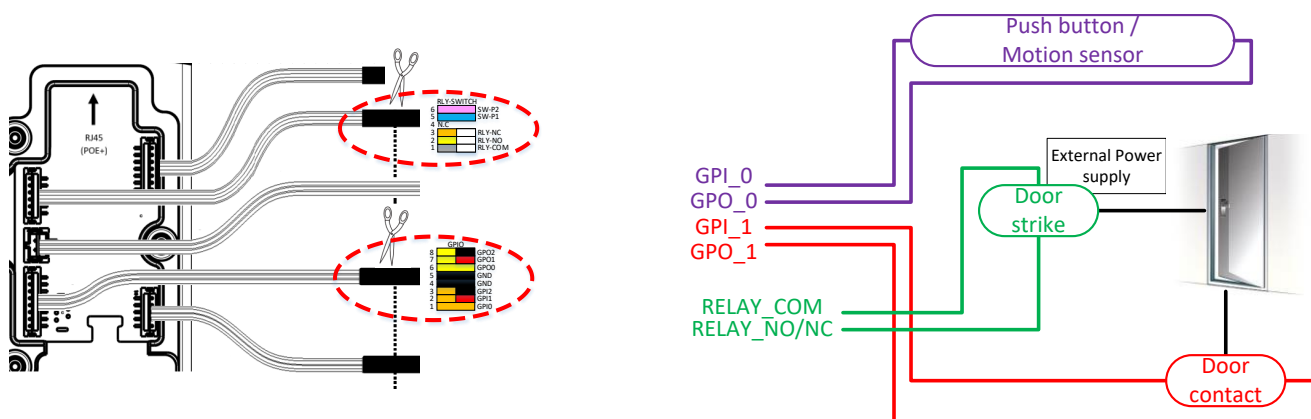


Figure 28: SDAC wiring



If door contact is not used, GPI1 and GPO1 shall be connected together

4.9 > Ethernet connection

Use a category 6² shielding cable (120 Ohms) or better. It is strongly recommended to insert a repeater unit every 90 m.

Recommendations for RJ45 wiring

Pin	1	2	3	4	5	6	7	8
Signals	Data pair 1	Data pair 1	Data pair 2	NC/POE pin dedicated (+) Data pair 3	NC/POE pin dedicated (+) Data pair 3	Data pair 2	Ground/ pin dedicated (-) Data pair 4	NC/POE pin dedicated (-) Data pair 4
EIA / TIA T568B Colors	White orange	Orange	White green	Blue	White blue	Green	White brown	Brown
EIA / TIA T568A Colors	White green	Green	White orange	Blue	White blue	Orange	White Brown	Brown
Corel L120 Colors	Grey	White	Pink	Orange	Yellow	Blue	Purple	Brown

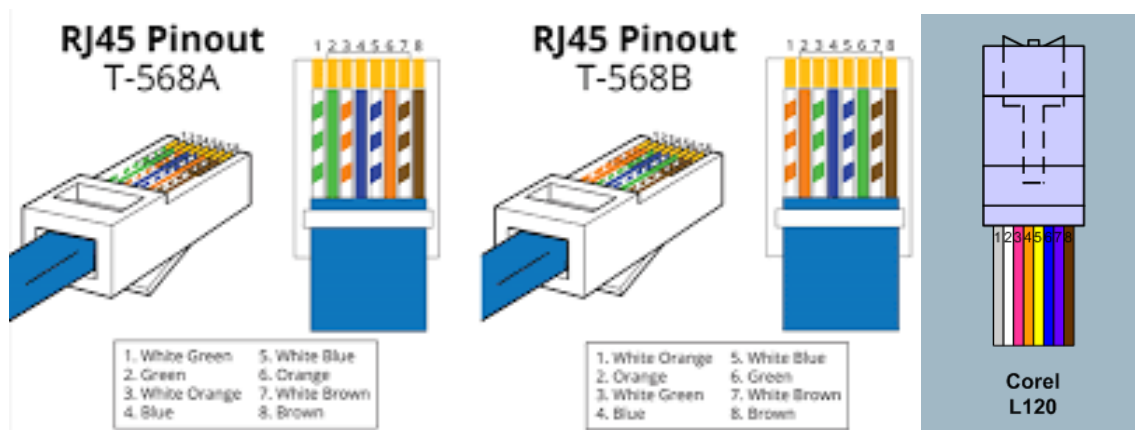


Figure 29: RJ45 wiring

RJ45 plug pinout is compliant with 100 Base T, IEEE802.3 Specification.



Ethernet cable shall be shielded

Default Ethernet configuration

By default, VisionPass SP terminal is configured in STATIC mode with the following configuration:

IP address: 192.168.1.10; Subnet Mask: 255.255.254.0

² Note: Not evaluated by UL

4.10 > Internal USB connection

Remove the cover plate by unscrewing the 3 screws of the cover plate, as shown on the following drawing.

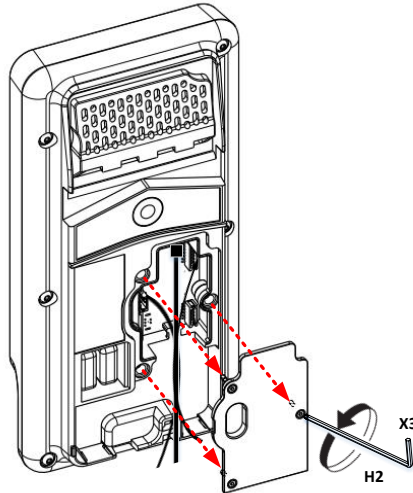


Figure 30: Cover plate removing

Then you can see a Mini USB plug.

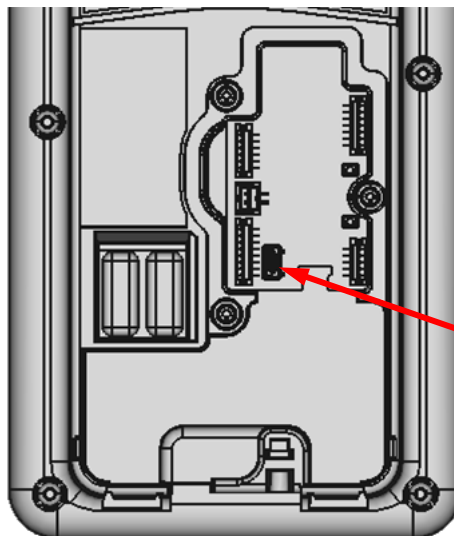


Figure 31: Internal USB connection

The internal Mini USB-type B can be used for administration only to connect a mass storage USB key (with a standard Mini USB-type B / USB-type A female OTG adapter).

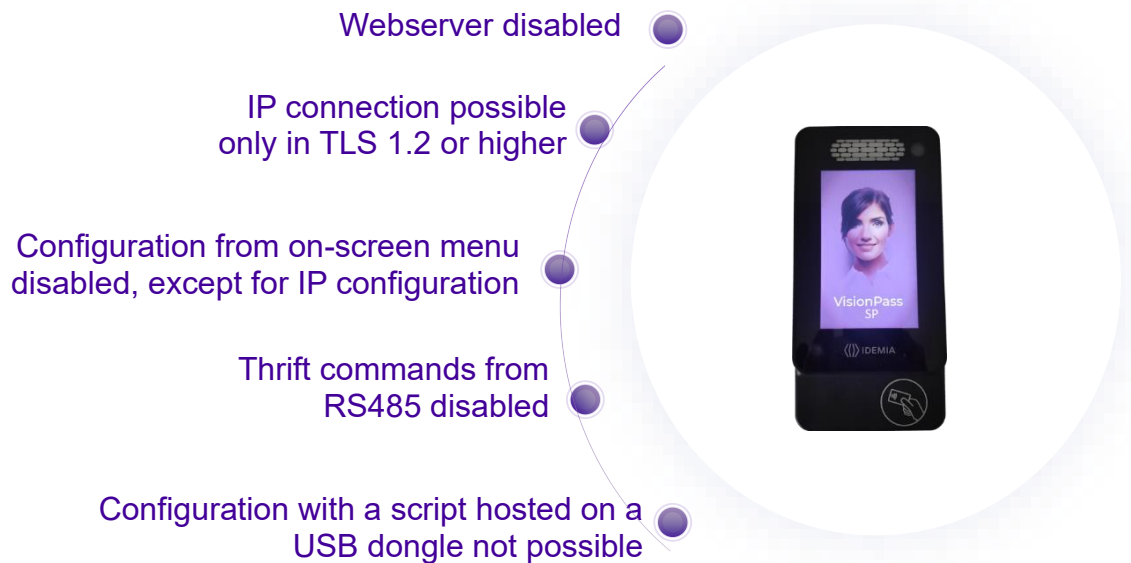
Please refer to VisionPass SP Administration Guide for more information.



USB connection is limited to USB key connection (power consumption shall not exceed 200mA)

4.11 > Secure communication

The VisionPass SP terminal has a default configuration enforcing security:



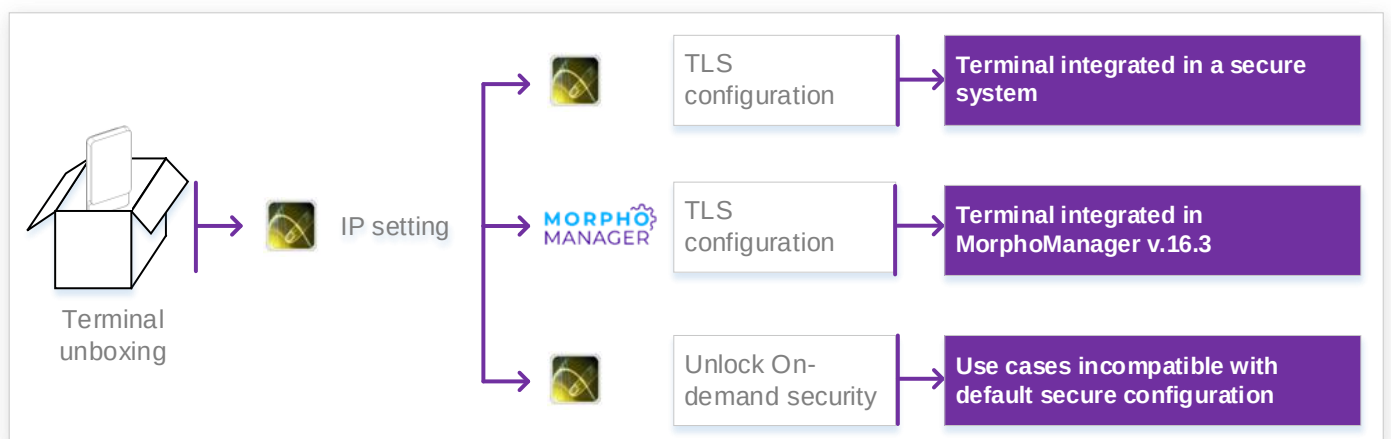
The default configuration is recommended by IDEMIA for operations. To use the features non available by default, the On-demand security state of VisionPass SP can be unlocked with MorphoBioToolBox.

	<i>This shall not be done unless the end customer is made aware and an assessment on the system security is done</i>
---	--

Administration of secure communication:

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

	The communication configuration can be done with 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



5 / User interface

5.1 > Modes for controlling access rights

5.1.1 > Introduction

The VisionPass SP terminal offers several methods for controlling access rights: it needs to be configured in one of the following four modes:

- Identification mode,
- Authentication mode,
- Multi-factor mode,
- Proxy mode

Refer to VisionPass SP Administration Guide for more information on Access Control.

5.1.2 > Identification mode

The Identification process of the VisionPass SP terminal proceeds by comparison of the biometric data of the face placed on the biometric sensor, with all the biometric data stored in the database.

It means that the biometric data of the allowed users must be stored in the internal database before they can request the access on the terminal. This biometric data is acquired either directly on the terminal (using the embedded firmware), or on an enrollment system using the same type of biometric sensor.

The access control by identification process is started when a face is detected in front of 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).

For further information, please see the "Identification mode" section in the VisionPass SP Administration Guide.

5.1.3 > Authentication (verification) mode

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 enrollment phase. The data can be on a card presented to the terminal or in a database and ID is provided by the user.

Access is authorized if the terminal finds a correspondence.

For further information, please see the "Authentication mode" section in the VisionPass SP Administration Guide.

5.1.4 > Multi-factor mode

In this mode, the "identification" and "authentication" modes are available simultaneously; the user decides which control method will be used:

- by presenting his face to the sensor, thereby triggering the identification process,

- by placing his contactless card on the reader, thereby triggering the authentication process,

This is the default mode for terminals fitted with a contactless smartcard reader.

For further information, please see the "Multi-factors method" section in the VisionPass SP Administration Guide.

5.1.5 > Proxy mode

The Proxy mode is an operating mode where the access control main application is located in a distant system. This is not a standalone mode like Identification and Authentication modes.

It means that the terminal becomes a slave of the host system application. The access control application is running on the host system and uses VisionPass SP terminal high level functions:

- Identification function

- Authentication function

- Read data on a contactless card

- Access control result signal command

The VisionPass SP terminal is driven through an Ethernet link using TCP, SSL or TLS protocol.

The VisionPass SP terminal acts as a server: it is either waiting for a command or executing a command.

The commands allowed by the VisionPass SP terminal are described in the VisionPass SP Host System Interface Specification document.

For further details about SSL or TLS on the VisionPass SP terminal, please refer to the VisionPass SP Administration Guide.

5.1.6 > External database mode (also called polling mode)

When external database mode is activated, the VisionPass SP 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 poll the user ID to external controller. On polling out the ID, the corresponding template (if exists) is fetched from the external database and is authenticated against user's biometric on the terminal. Once the template request is posted to the external database, the terminal shall wait for the face template from the external database to start authentication. Further process shall be same as authentication.

Polling Process 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 device and granted access accordingly.

VisionPass SP terminal also has distant commands to retrieve polling buffer status and polling buffer data. Refer to the VisionPass SP Host System Interface Specification document.

How to Activate?

External database mode can be activated by setting “ucc.enable_external_database” parameter to 1. Only an admin user can activate polling mode. You can refer to the VisionPass SP Host System Interface Specification document to know how to set this parameter.

5.1.7 > Anti-tamper / anti-pulling switches

Please refer also to “Tamper Switch” section.

These switches are activated as soon as there is enough pressure applied on the terminal against the wall. They are deactivated as soon as this pressure is not big enough, e.g. when the terminal is pulled out of the wall.

When the switches are deactivated, the VisionPass SP terminal acts as required by the related configuration key (see VisionPass SP Administration Guide for key configuration description):

- | Ignore the event (default): useful during normal maintenance operations.
- | Send an alarm message to the Central Access Controller, through the usual channel of the access control result messages (Wiegand, DataClock, RS485, Ethernet). An alarm switch (relay contact) is directly available on block terminal « tamper switch pins ». Please refer to “Wiring overview” and to “Tamper Switch” sections.
- | Generate an audible alarm signal with the buzzer and an alert message on the screen.

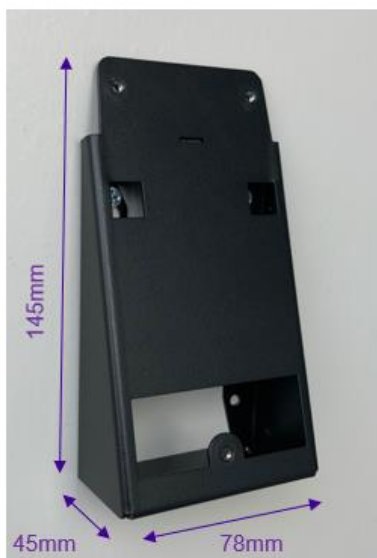
6 / Accessories and PC applications

6.1 > Compatible Accessories

The following items can be ordered directly to IDEMIA or to an official distributor, so as to enjoy all the features of your VisionPass SP terminal.

6.1.1 > Low mounting bracket

This mounting bracket with 15° angle allows to lower the installation height (see § 8.2.3 > Lower positioning: 1105 mm) to facilitate the usage from person in wheelchair or in case higher installation is not possible. The mounting keeps the vertical angle for VisionPass SP, to identify users between 120 to 200cm tall.



Dimensions of VisionPass SP lower mounting bracket



Mounting of the wall mount with 3 included screws



Dimensions with VisionPass SP

6.1.2 > Spacer

This spacer provides a 30mm thickness spacer.

Dimensions:

- ⇒ Height: 150mm
- ⇒ Width: 78mm
- ⇒ Thickness: 30mm



Mounting of the wall mount with 3 included screws

6.1.3 > Visor

The Visor provides an external protection to the VisionPass SP.



The wall mount is attached to the wall, and fixes the Visor in sandwich

6.1.4 > Metal Mount

Metal Mount provides a solution to install VisionPass SP on a speed gate. The Speedgate top shall be at 100cm height.



6.2 > Compatible PC applications

VisionPass SP terminals are fully compatible with:

- MorphoManager (version 16.3 or higher)
- MorphoBioToolBox (version 4.8 or higher)

7 / Recommendations

Global warning

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

For UL 294 compliance, in standalone mode, the unit shall be installed in protected area.

General precautions

Do not attempt to repair your 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 invalidate your warranty.

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.

Do not expose your terminal to extreme temperatures.

Use your terminal with original accessories. Attempts to integrate unapproved accessories to the terminal will void your warranty.

Due to electrostatic discharge, and depending on the environment, synthetic carpet should be avoided in areas where the terminal has been installed.

Do not tilt the product.

Do not use blunt force on the product.

Do not attach anything to the product.

Do not place anything on the product.

Switch off the device before unplugging it.

To ensure the proper operation of the product and prevent degradation due to overvoltage, it is highly recommended to protect the devices with external accessory. Typically, risks of overvoltage have been identified on external power management wire, POE connector and wiegand input wire.

Biometric performance

Do not scratch the product, particularly on the glass, because the performance of the product depends of the state of the glass surface and its anti-reflective face.

Clean the glass every day to optimize performance of the product.

Avoid direct sun light on the product.

Areas containing combustibles

It is strongly recommended that you do not install your 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 equipped with a contactless smartcard reader

It is recommended to install terminals equipped with a contactless smartcard reader at a certain distance (> 30cm) from metallic elements such as iron fixations or lift gates or radio product (such as contactless smartcard reader). Performances in terms of contactless badge reading distance will decrease when metallic elements are closer.

Ethernet connection

It is recommended to use a category 6³ 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 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).

Using PoE+

The VisionPass SP can consume more power than the 13 Watt allowed by the PoE standard and must be connected to a network switch supporting PoE+.

The VisionPass SP will need the maximum power during acquisition (user in front of the product) and when reading a contactless card.

The PoE+ standard can support devices consuming up to 25.5W of power. The network switch will detect automatically that the device is a PoE+ device (802.3at compliant) at power up and provide the required power so the device can start.

However, the standard also specifies a LLDP protocol that is used after the device is started. The LLDP protocol is bidirectional and is carried over Ethernet frames. It allows the network switch and the device to negotiate the amount of power needed by the terminal and the amount of power that the switch is allocating for the device.

It is important to configure the switch to allocate the proper amount of power for the VisionPass SP so it can work properly.

A typical sign of misconfiguration is that, during an identification or enrollment, the terminal will reboot because the switch will refuse to provide the required amount of power.

The VisionPass SP will send a LLDP request for 25.5W and a “Critical” level. The switch shall be configured to allow the terminal to consume up to 25.5W of power.

Managed vs non-managed PoE+ switches

Managed switches will tend to control the power distribution in a very precise way and need to be properly configured but will not overcommit their power supply.

Unmanaged PoE+ switches may be more tolerant about the power distribution and may only limit the total power distributed. In this case, it is important to evaluate the peak power supply necessary for all the connected terminals and insure that it does not exceed the power supply of the switch.

Example of PoE+ Switch configuration: HP ARUBA switches 2530-24-PoE+

For the ARUBA switches, two options are possible for the configuration setting:

- Fixed : Allocate 30W for each PoE+ port

This option will limit the number of VisionPass SP terminals connected to the switch because it will refuse to overcommit its power supply.

The commands to set this configuration are:

```
(config)# interface X poe-allocate-by value
```

```
(config)# interface X poe-value 30
```

³ Note : Not evaluated by UL

Where X is the port number.

- Usage : Allocate the power dynamically to the device as required

This second option will be more flexible because the devices are unlikely to be consuming the maximum amount of power at the same time.

The commands to set this configuration are:

```
(config)# interface X poe-allocate-by usage
```

```
(config)# interface X poe-lldp-detect enabled
```

Where X is the port number.

Date / Time synchronization

The terminal clock has a +/-20 ppm typical time deviation at +25°C (roughly around +/- 2 sec per day). At lower and higher temperature (but within normal operating temperatures), deviation may be more important (worst case: 8 seconds per 48 hours).

If the terminal is used in an application requiring high time precision, we recommend synchronizing regularly your terminal time with an external clock (using NTP). Every 24 hours is usually enough for most applications.

Please note that the date/time of the terminal is protected from power failure during at least 2 hours at 25°C. If the duration of the power failure or power down is longer, the date/time of the terminal will be lost.

Cleaning precautions

Use a dry cloth to clean the terminal, especially the front face. It is recommended that the product be cleaned daily to ensure the best performance level over its lifetime.

The use of acid liquids, alcohol or abrasive materials is prohibited.

Use dry air spray to remove the dust out of the sensor glass.

8 / Annex 1: placement recommendations

8.1 > Main principles

VisionPass SP is designed to operate indoor.

To optimize VisionPass SP performances, it is recommended to follow the rules below for the positioning.

For VisionPass SP used for enrollment, those rules must be followed.

User walking to the device

- VisionPass SP processes biometric data faster when users walk towards the device in the direction of the access point. Avoid position of the VisionPass SP where a user is approaching from the side.

Sun illumination

- 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.

Background (behind user face)

- 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 bright spot light appear in the background (halo may appear which can lead to over exposure of the face image). In any case, no bright spot light closer than 1 meter to the device

Cleanness

- Protect the front glass from raindrops as it might affect the sensors
- Clean the glass every day to optimize performance of the product.

Instruction for the presentation of the user in front of the VisionPass SP is described in the Quick User Guide

8.2 > Positioning Guidelines

VisionPass SP flexibility makes it perfectly fit many use cases. Depending on the configuration of the surrounding area, it may be located and orientated in various ways. Due to the infinite diversity of configurations, it is not possible to provide accurate recommendations for all of them. The following section provides guidelines to optimize both the user experience and the flow management.

8.2.1 > Overview

The field of view of the VisionPass SP camera, representing the geometrical volume in which a face can be identified, is a cone. Please refer to the Quick User Guide to run the device.

During installation, visualizing the camera field may help positioning the device in a way it will properly work. This is done enabling the User Guidance based on Camera.

The flow of users is optimized when people hardly have to stop in front of the biometric terminal before the physical barrier (door, turnstile, optical gate, etc.) opens. **VisionPass SP processes biometric data faster when users walk towards the device in the direction the physical barrier behind it.**

If several VisionPass SP terminals are installed in parallel, a minimum distance of 80 cm must be ensured between the devices. Otherwise, the optical system of one device interferes with the other, reducing the biometric performance.

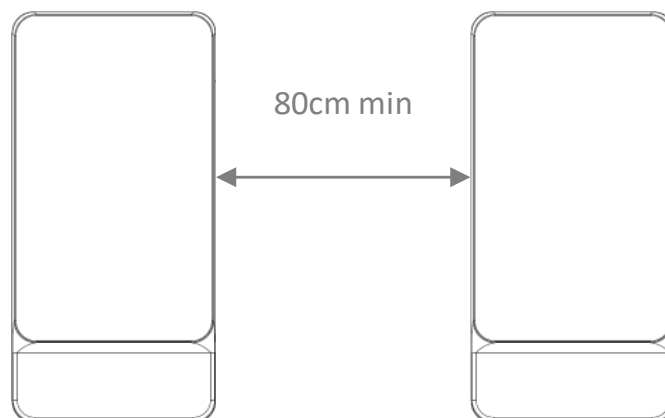


Figure 32: Minimum distance between devices (front view)

In case of two accesses to be secured with 2 VisionPass SP terminals, overlapping of scanning cones is best avoided positioning the VisionPass SP terminals on the opposite walls.

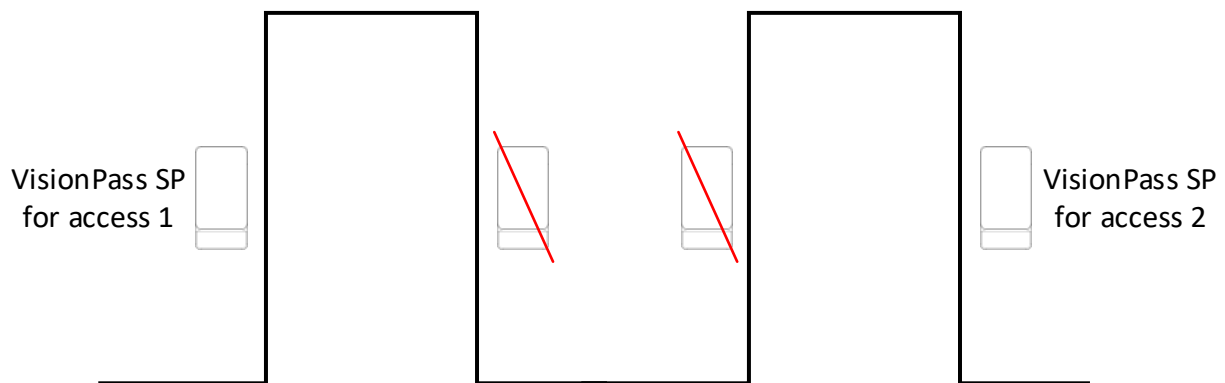


Figure 33: Avoid positioning 2 devices close to each other (front view)

8.2.2 > Specific guidelines for gates or turnstiles

The installation of VisionPass SP terminals on gates or turnstiles, for instance in an entrance lobby, has some specificities that require dedicated recommendations on top of the ones exposed above.

In case of multiple lanes, rotating the terminals compared to the direction of the user motion may have several benefits:

- It makes it clear for users which terminal allows access to which lane
- It enables users to go through the lane in its center, as opposed to the side nearing the VisionPass SP terminal

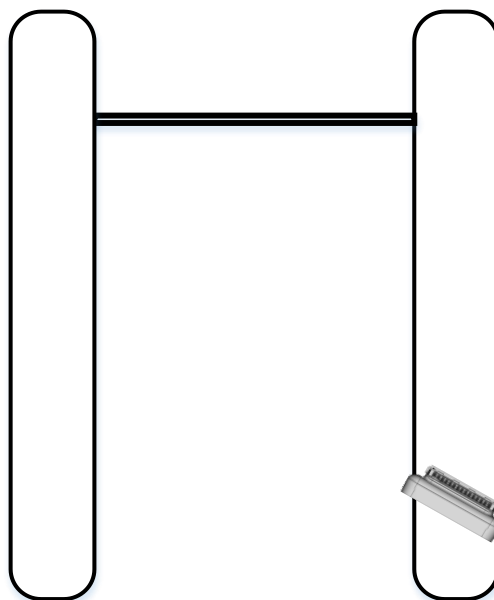


Figure 34: Principle of rotation (top view)

Rotating devices may also be beneficial in case the natural flow of users is not symmetric. For instance if users come from an un-centered lobby desk.

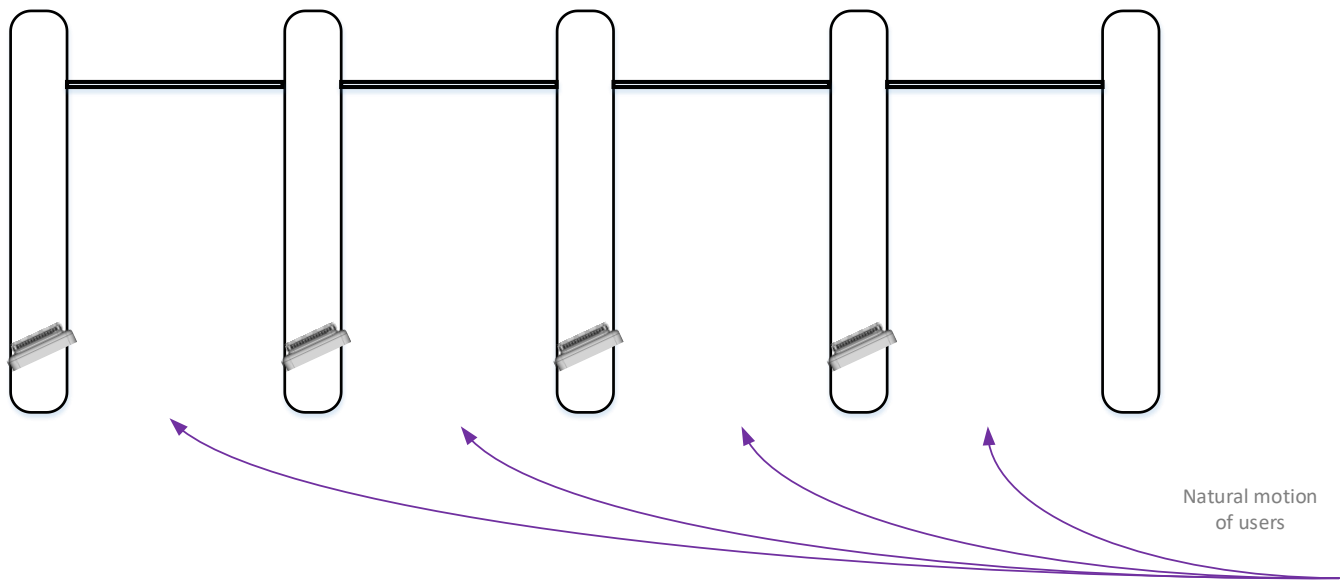


Figure 35: Rotation based on natural user flow (top view)

A rotation angle of 20° is recommended, and a value of 25° should not be exceeded.

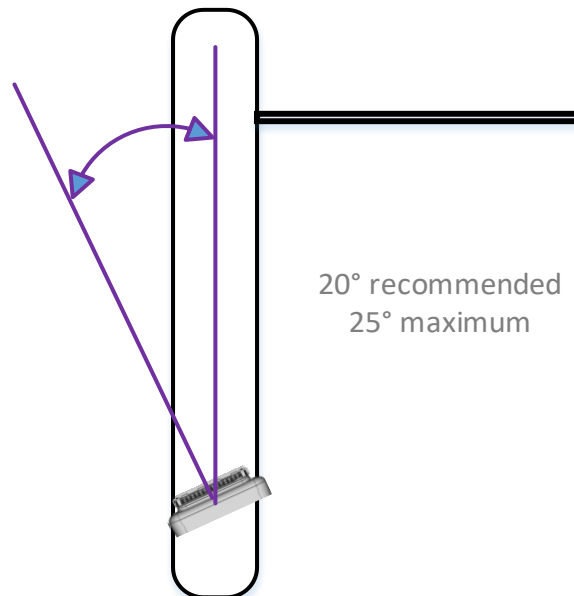


Figure 36: Rotation angle (top view)

For best user experience and biometric performance, VisionPass SP is to be positioned at 1460 mm from the ground. In case the terminal is installed on a lower stand, IDEMIA recommends compensating the height with a pole.

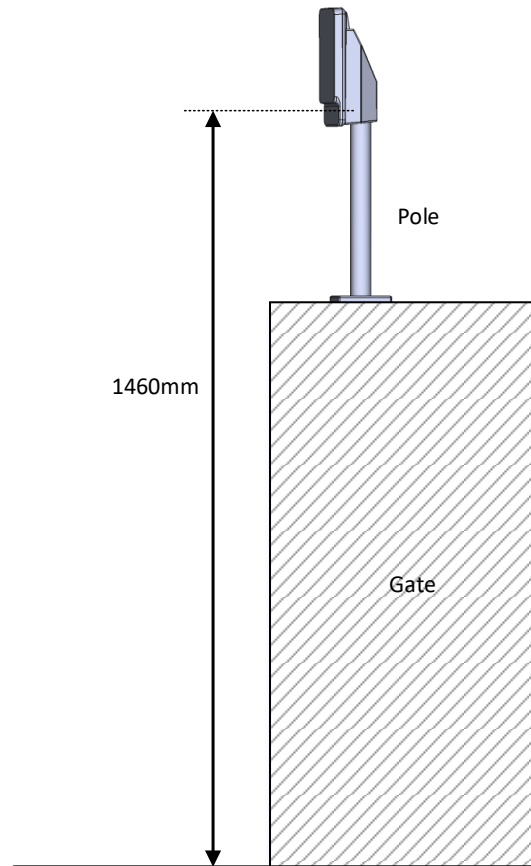


Figure 37: Recommended height installation (side view)

8.2.3 > Lower positioning: 1105 mm

In case VisionPass SP should be positioned lower than the recommended height, there is an accessory “Low level wall mount” that can be used (see “6 / Accessories and PC applications”). This accessory allows to position VisionPass SP at 1105mm (from bottom screw) which reduced the height of around 300mm.

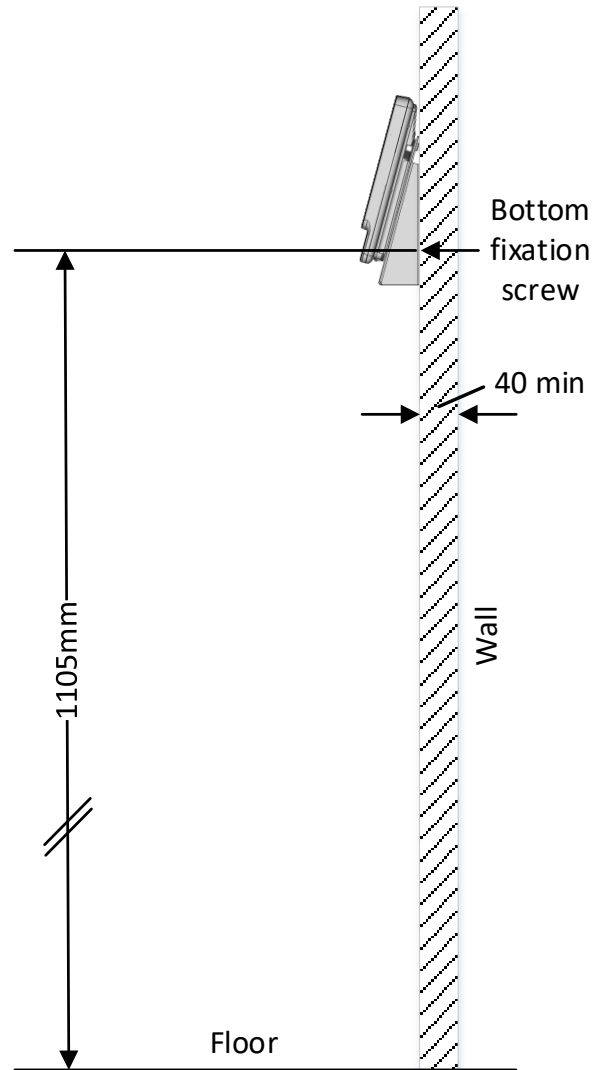


Figure 38: Lower installation positioning – 1105 mm (side view)

9 / Annex 2: Bibliography

9.1 > How to get the latest versions of documents

For the latest firmware, software, document releases, and news, please check our website:

biometricdevices.idemia.com

To get your login and password please contact your sales representative.

9.2 > Documents about the VisionPass SP terminal

Documents about installing the terminal

Quick Installation Guide,

This document describes the main steps for wall mounting.

Installation Guide,

This document describes terminal physical mounting procedure, electrical interfaces and connection procedures. This document is in English.

Documents about administrating / using the terminal

Quick User Guide,

This document gives a quick overview of the product and the basics of configuration and use. This document is in English.

Administrator Guide,

This document describes the different functions available on the terminal and procedures for configuring the terminal. This document is in English.

Parameters Guide,

This document contains the full description of all the terminal configuration parameters. This document is in English.

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. This document is in English.

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...

10 / Annex 3: Support

10.1 > Troubleshooting

The terminal IP address is unknown or it is not possible to connect to the terminal

Use terminal interface to configure a valid set of network parameters in your terminal.

The sensor is switched off

Check that the database contains at least one record.

Check that the identification mode is enabled.

The terminal returns erratic responses to Ping commands

Check the subnet mask.

Ask the network administrator for the correct value.

Check that each device connected to the network has a different IP address.

10.2 > 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

Website

For the latest firmware, software, document releases, and news, please check our website:

biometricdevices.idemia.com

To get your login and password please contact your sales representative

COPYRIGHT IDEMIA 2023



Head office:

IDEMIA
2, place Samuel de Champlain
92400 Courbevoie - France
www.idemia.com