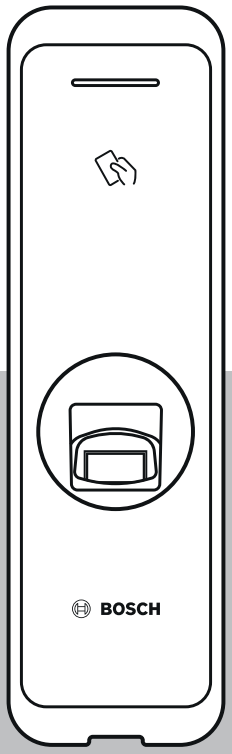
ARD-FPBEW2-H3 Fingerprint Reader, Multiclass

ARD-FPBEW2-H3



en Installation manual

Table of contents

1	**Safety and handling**	**4**
2	**Introduction**	**6**
2.1	Components	**6**
2.2	Names and function of parts	**7**
2.3	Cables and connectors	**8**
2.4	How to enroll a fingerprint	**10**
3	**Installation**	**12**
3.1	Fixing the bracket and the product	**12**
3.2	Power supply connection	**14**
3.3	Network connection - TCP/IP	**15**
3.4	Wiegand connection	**16**
3.5	RS485 connection	**17**
3.6	Resetting network settings	**17**
3.7	Restoring the factory defaults	**17**
4	**Technical data**	**18**
4.1	Product specifications	**18**
4.2	Dimensions	**20**
5	**UL**	**21**
5.1	UL 294 requirements	**21**
6	**FCC**	**22**
6.1	Compliance information	**22**

1 Safety and handling

Failure to follow these safety instructions could result in fire, electric shock, injury, or damage to the product or other property. Read all the safety information before installing or using the product.

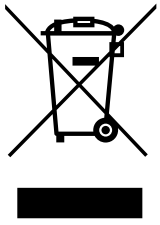
Download, read and follow the respective technical documentation at boschsecurity.com (where available) or read the documentation provided in the packaging. Retain documentation for future reference.

Installation

- Do not install the product in a place with direct sunlight, moisture, dust, or soot.
- Do not install the product in a place with heat from an electric heater.
- Do not install the power supply cable in a passage area.
- Do not install the product near highly magnetic objects.
- Do not install the product in a place with electromagnetic interference.
- Install the product in a dry place.
- When installing more than one device, allow space between the devices.

Notice!
In case of malfunction, contact Bosch After-Sales Service.
Do not attempt to repair the product yourself or free after-sales service will not be provided.

Old electrical and electronic equipment



This product and/or battery must be disposed of separately from household waste. Dispose such equipment according to local laws and regulations, to allow their reuse and/or recycling. This will help in conserving resources, and in protecting human health and the environment.

Handling the product

- Do not drop the product.
- Do not apply any impact to the product.
- Do not contaminate or damage the fingerprint contact unit with foreign substances.
- Do not spill any liquids on the product.
- Only operate the product from the type of power source indicated on the label. If unsure of the type of power supply to use, contact your dealer.

Cleaning the product

- Wipe the product with a soft and dry cloth.
- Do not apply water, benzene or alcohol.

Notice!
For more information about this product, read the documentation provided in the packaging, or visit us at http://www.boschsecurity.com.

Notice!

Use of the Wiegand interface

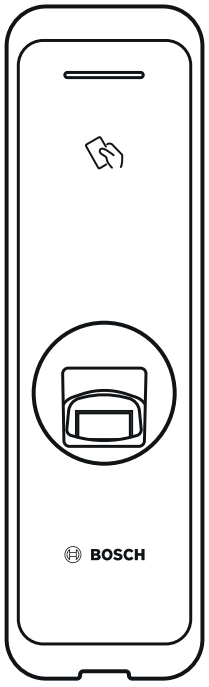
For data security reasons, the use of the Wiegand interface is not recommended. A secure encrypted data connection is only obtained with the use of the OSDP v2 protocol. The OSDP protocol is used via the RS485 connection.

Notice!

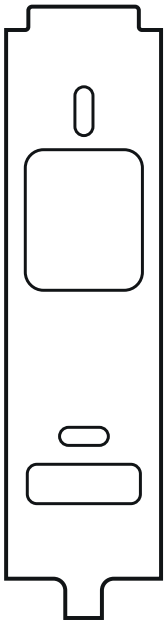
To ensure high security of data exchange between credentials and readers, only encoded cards such as MIFARE DESFire or iCLASS SE should be used in the access system.

2 Introduction

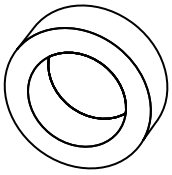
2.1 Components



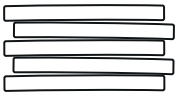
ARD-FPBEW2



Bracket



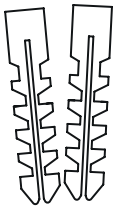
Ferrite Core
(1 EA)



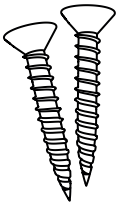
Heat shrink



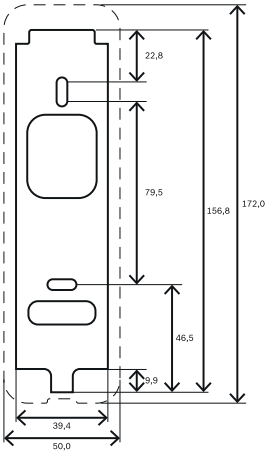
Bracket Fixing Screw
(Star Shaped)



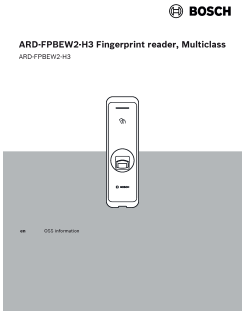
PVC anchor
(2 EA)



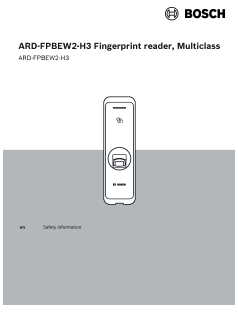
Fixing screw
(2 EA)



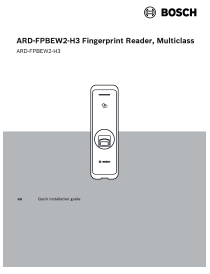
Drilling template



OSS Manual

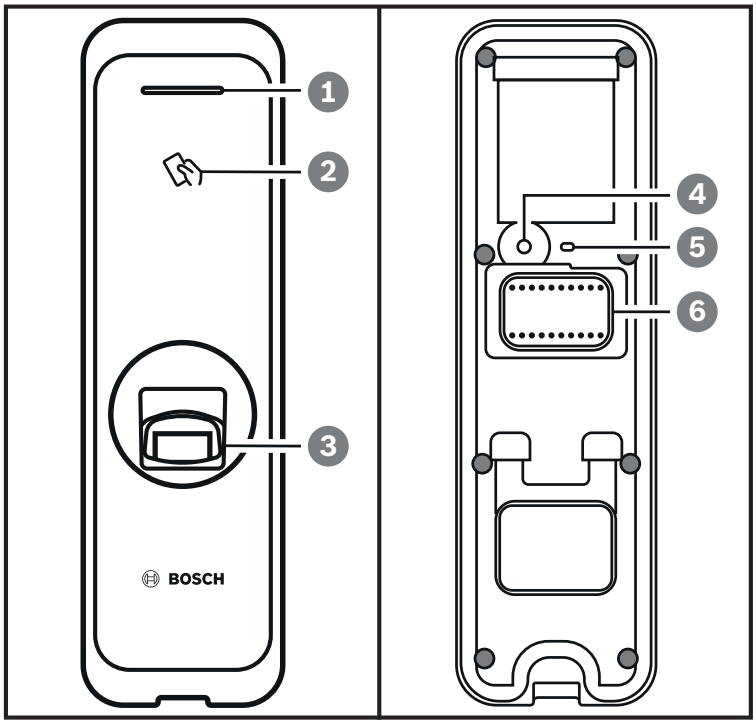


Safety
Instructions



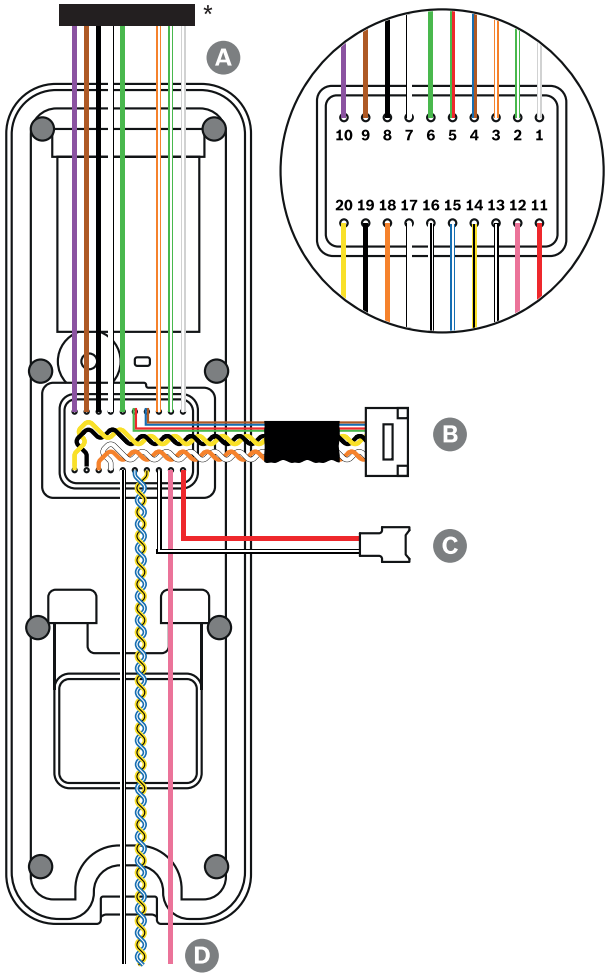
Quick
Installation
Guide

2.2 Names and function of parts



Item	Feature
1	LED lamp Indicates the operational status of the product with the color of the LED lamp.
2	RF card authentication unit Reads RF cards for entering and exiting.
3	Fingerprint authentication unit Reads fingerprints placed on it for entering and exiting.
4	Reset button For details, see chapters 3.6 and 3.7
5	LED lamp for Network Shows the status of the network connection.
6	Cable – Wiegand cable – Power cable – RS485 cable – Ethernet connector

2.3 Cables and connectors



* Cut the required wires off the connector plug.

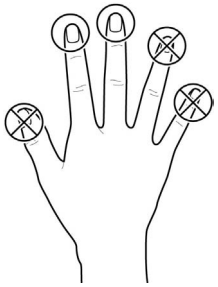
Cable	Cable name
A	Wiegand cable
B	Ethernet cable
C	Power cable
D	RS485 cable

Cable	Cable name	Color
1	WG Tamper NO	Gray (White stripe)
2	WG Tamper COM	Green (White stripe)
3	WG Tamper NC	Orange (White stripe)
4	Not used	Blue
		Brown
5	Not used	Red
		Green
6	WG D0	Green
7	WG D1	White
8	WG GND	Black
9	WG LED red	Brown
10	WG LED green	Purple
11	PWR +VDC	Red
12	Not used	Pink
13	PWR GND	Black (White stripe)
14	485 TRXN (RxTx-)	Yellow (Black stripe)
15	485 TRXP (RxTx+)	Blue (White stripe)
16	485 PAG	White (Black stripe)
17	ENET TXP	White
18	ENET TXN	Orange
19	ENET RXP	Black
20	ENET RXN	Yellow

2.4 How to enroll a fingerprint

In order to improve the fingerprint authentication rate, register the fingerprint correctly. The reader can recognize a fingerprint even if the angle and position of a user's fingerprint input change. If you register the fingerprint with attention to the following instructions, the authentication rate can be improved.

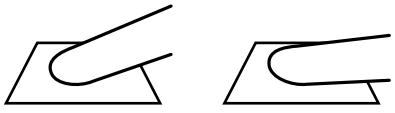
Selecting a finger for fingerprint input



- In preparation for the case that the fingerprint of a specific finger cannot be used, for example if the user is lifting a load with one hand or a finger gets hurt, up to 10 fingerprints for each user can be registered.
- In the case of a user whose fingerprint cannot be recognized well, the authentication rate can be improved by enrolling the same finger twice repeatedly.
- If a finger has a cut or the fingerprint is blurry, select another finger for the fingerprint.
- It is recommended to use the index finger or the middle finger when scanning the fingerprint. The authentication rate can be reduced if it is difficult to place another finger at the center of fingerprint sensor accurately.

Fingerprint enrollment method

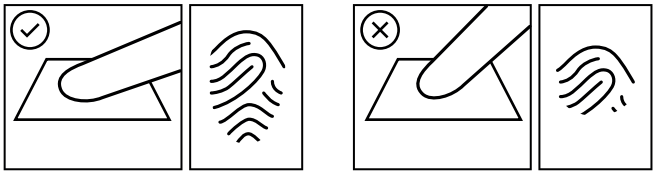
1. Place the finger with the fingerprint to be registered on the fingerprint authentication unit and press the finger gently for better authentication.
2. Wait for the instructions of the management system to place the finger a second time on the sensor. Scan the fingerprint of the registered finger again.



Cautions for enrolling a fingerprint

When a fingerprint is recognized, it is compared with the initially registered fingerprint, so the initial fingerprint enroll is the most important. Pay attention to the following matters when enrolling the fingerprint:

1. Place the finger deep enough to contact with the sensor completely.
2. Place the center of the fingerprint in the center of the sensor.
3. If a finger has a cut or the fingerprint is blurry, select another finger for the fingerprint.
4. Scan the fingerprint correctly without moving according to the instruction on the screen.
5. If you make the finger upright so that the contact area with the sensor has decreased or the angle of finger has warped, fingerprint authentication may not be performed.



Failure during fingerprint recognition

The reader can recognize a fingerprint regardless of a change of season or finger condition. However, the authentication rate may vary according to the external environment or fingerprint input method.

If the fingerprint authentication cannot be done smoothly, it is recommended to take the following measures:

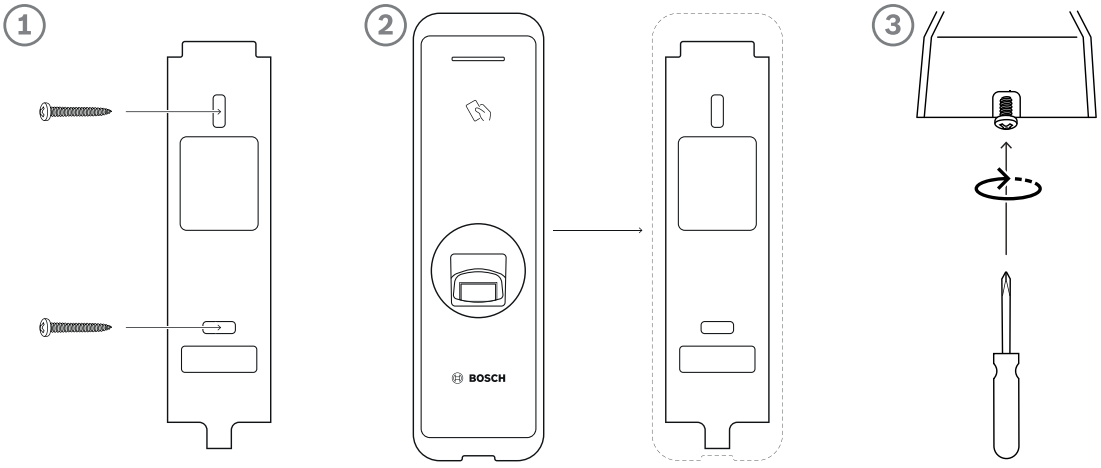
1. If the finger is smeared with water or sweat, dry off the finger and then scan the finger.
2. If the finger is too dry, blow your breath on the fingertips and then scan the finger.
3. If the finger has a cut, register the fingerprint of another finger.
4. The initially registered fingerprint often may have not been scanned correctly, so register the fingerprint again according to ‘Cautions for enrolling a fingerprint’.

3 Installation

3.1 Fixing the bracket and the product

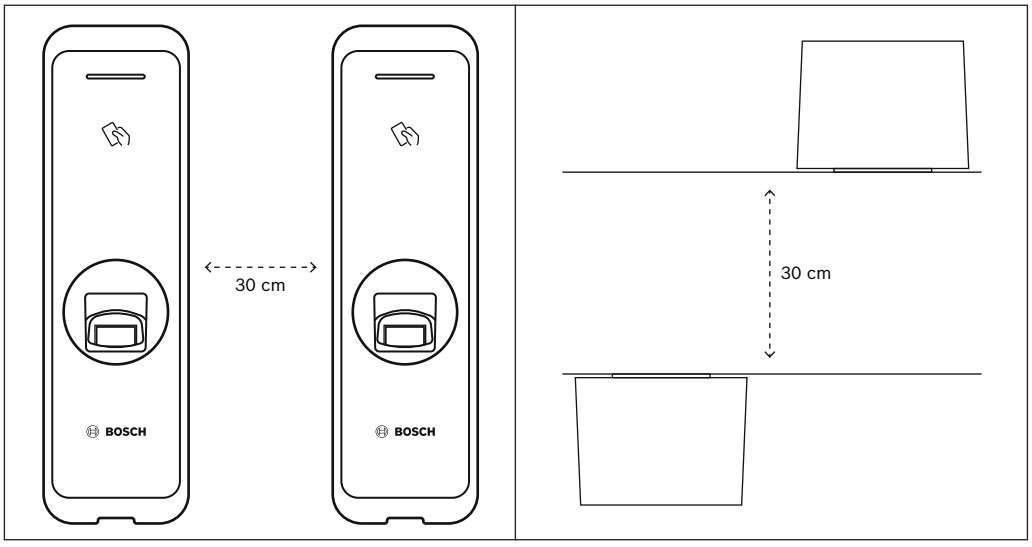
1. Determine the correct position to install the bracket using the provided drilling template.
2. Fix the bracket firmly using fixing screws through the bracket to the position where the device will be installed.
3. Install the device onto the fixed bracket.
4. Assemble the device to the bracket by rotating the star-shaped fixing screw.

– When assembling the product with the bracket, use the included bracket fixing screw (star-shaped) instead of the product fixing screw for enhanced security.



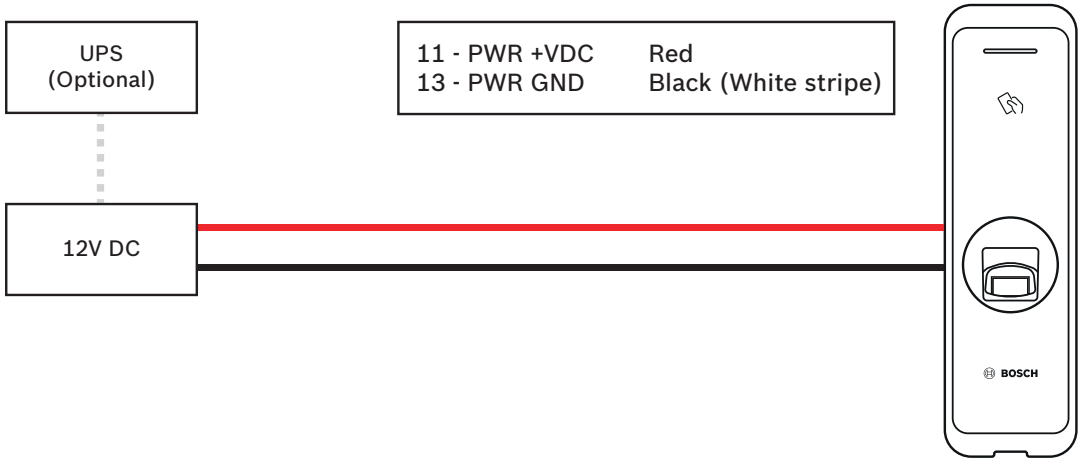
Installing the device on a concrete wall

1. Drill holes on the wall.
2. Insert the PVC anchors.
3. Fix the anchors with fixing screws.
4. Maintain a minimum separation distance to avoid RF interference (see table below).



Wall thickness	Distance
100 mm	270 mm
120 mm	250 mm
150 mm	170 mm

3.2 Power supply connection



Warning!
When connecting to an AMC2-4R4CF controller, note that the 12V power supply is used.

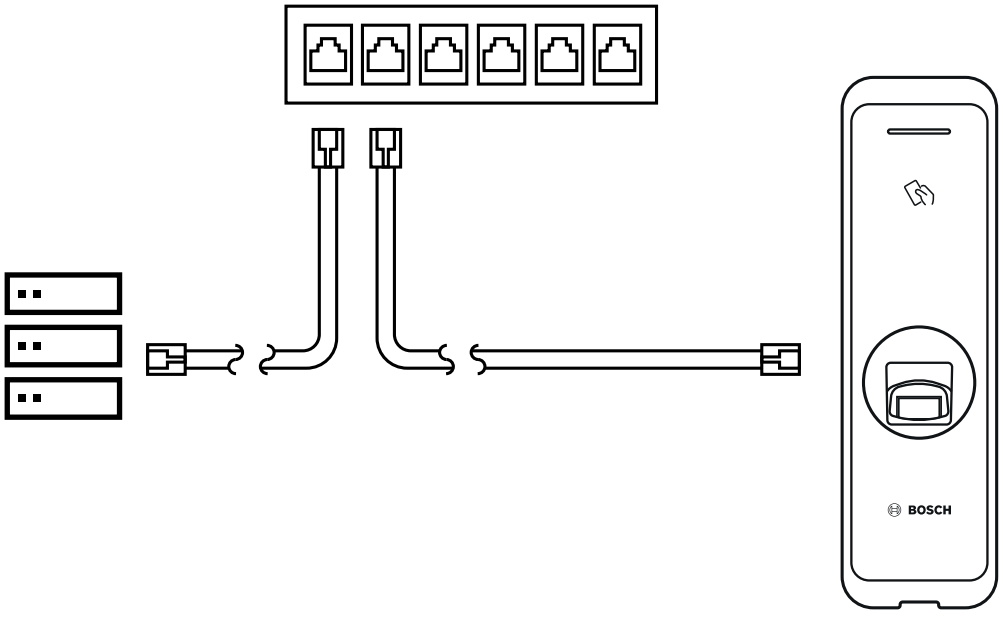
Warning!
Do not connect the device to the DC power supply(or adapter) and PoE power supply at the same time.

Notice!
Make sure to isolate the power connector cables if PoE is used for power supply.

3.3 Network connection - TCP/IP

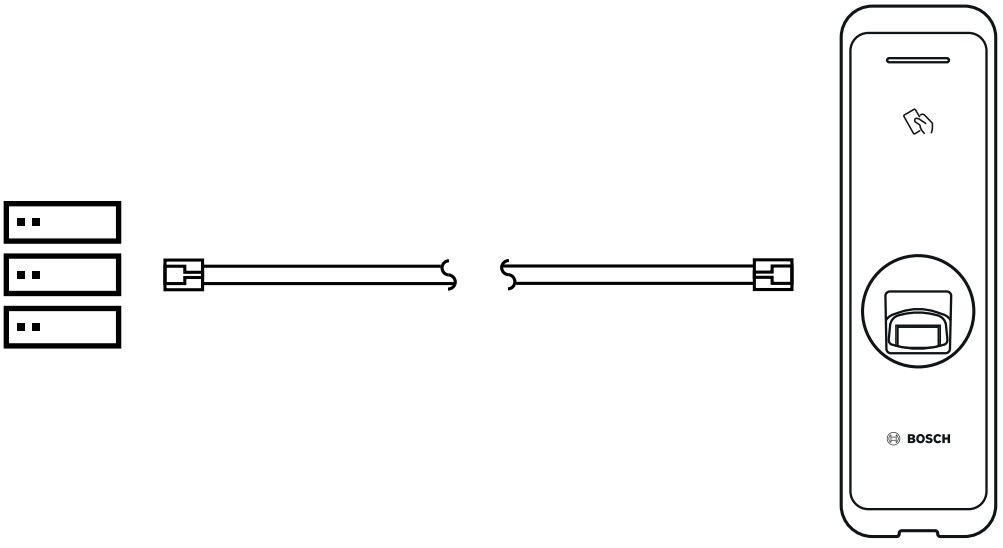
LAN connection (connecting to a hub)

You can connect the product to a hub using a general type CAT-5 cable (or higher).

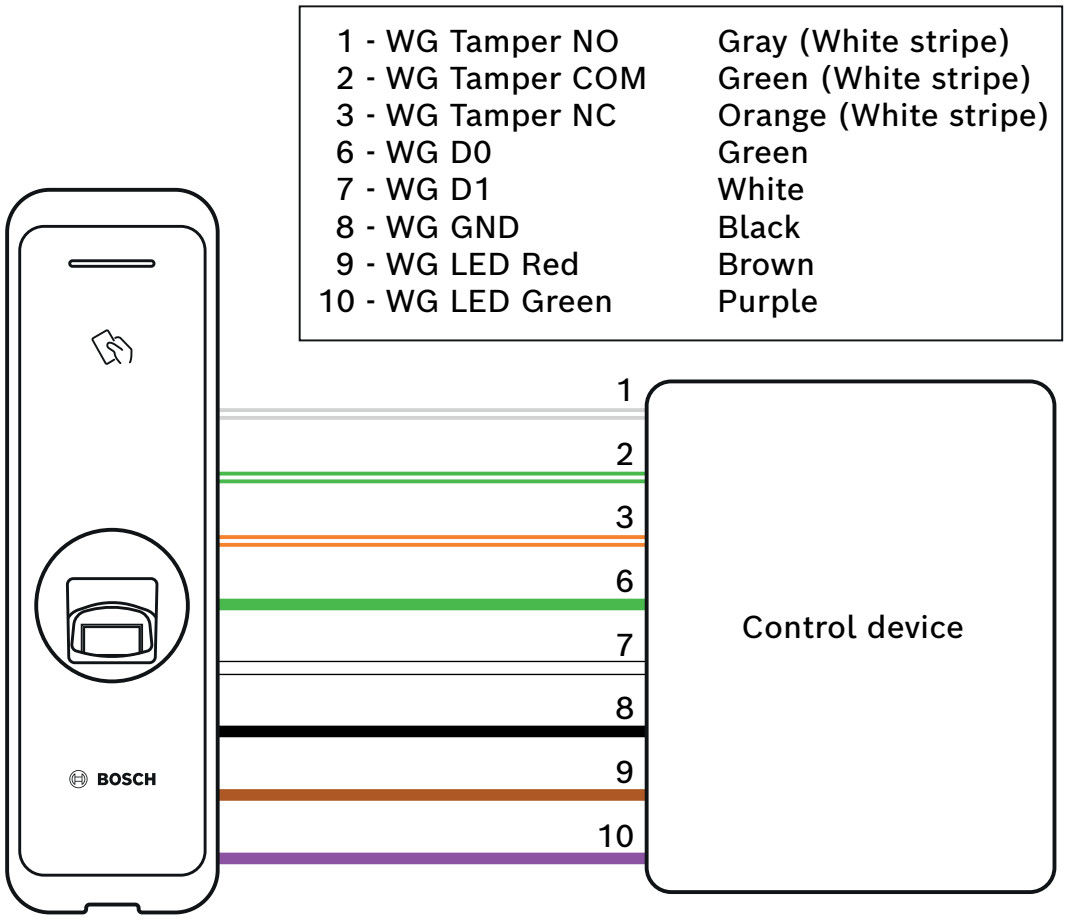


LAN connection (connecting to a PC directly)

The ARD-FPBEW2 has an automatic MDI/MDIX function so that it can be connected to a PC directly using a normal straight type CAT-5 cable (or higher), not a cross cable.

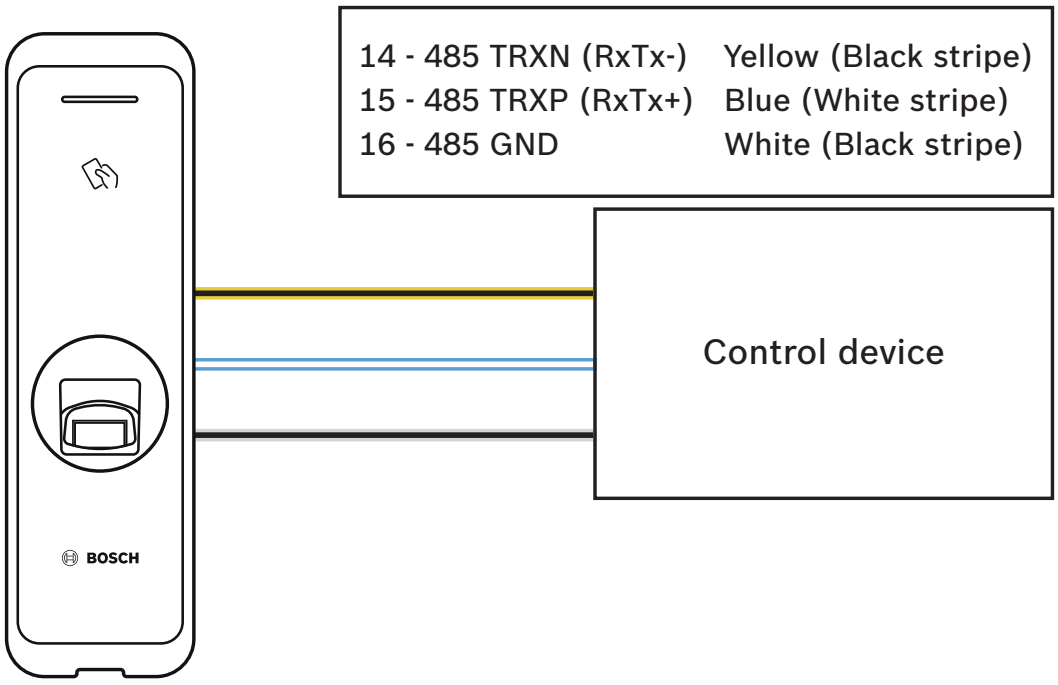


3.4 Wiegand connection



Notice!
When using the Wiegand interface, there is only an optical (LED) and no acoustic feedback (buzzer) from the reader.

3.5 RS485 connection



3.6 Resetting network settings

1. Turn the power on.
2. Press the network reset button on the rear of device until the device restart automatically.
3. Connect the device with default values.

– TCP/IP address: DHCP address assignment (If DHCP address assignment is fails, 169.254.x.x will be set.)
– Server mode: Disabled
– RS-485: PC connection, 115200 bps

4. Change the TCP/IP address or RS-485 information.
5. Turn the power off later on and then check the network setting is properly.

3.7 Restoring the factory defaults

This will delete all data and root certificate on the device and reset the settings.

1. Turn the power on.
2. Press the reset button three times quickly.
3. When the yellow LED is blinking, press the reset button again.

NOTE

– If there is no root certificate on the device, you cannot restore the factory defaults.

4 Technical data

4.1 Product specifications

Audio

Audio output	Multi-tone buzzer (only OSDP)

Capacity

Number of users	– 400,000 (1:1 matching) – 100,000 (1:N matching)
Templates in DB	4,000,000 (10 templates per person; 1:1 matching)

Connectivity

Reader interfaces	Wiegand; RS485
Host interface	Ethernet

Electrical

Operating voltage (VDC)	12 VDC
Current consumption (mA)	600 mA

Environmental

IP rating	IP67
Impact protection (EN 50102)	IK09
Operating temperature (°C)	-20 °C – 50 °C
Operating temperature (°F)	-4 °F – 122 °F
Operating relative humidity, non-condensing (%)	0% – 80%
Storage relative humidity (%)	0% – 90%
Storage temperature (°C)	-40 °C – 70 °C
Storage temperature (°F)	-40 °F – 158 °F

Mechanical

Material	Polycarbonate
Dimension (H x W x D) (mm)	50 mm x 172 mm x 38.2 mm (top) 50 mm x 172 mm x 43.5 mm (bottom)
Weight (g)	251 g

Operation

Credential type	Biometric data
Color	Black/Silver
LED indication	Multi-color

Reading format	MIFARE classic (Bosch data record); MIFARE DESFire EV1 (Bosch data record); iCLASS; iCLASS SE; EM 4102; HID Prox; Seos; HID Corporate-1000; MIFARE DESFire EV2
Protection	Tamper (micro switch)

Storage

Storage templates	– Template on device* – Template in secure database of AMS or BIS/ACE

System requirements

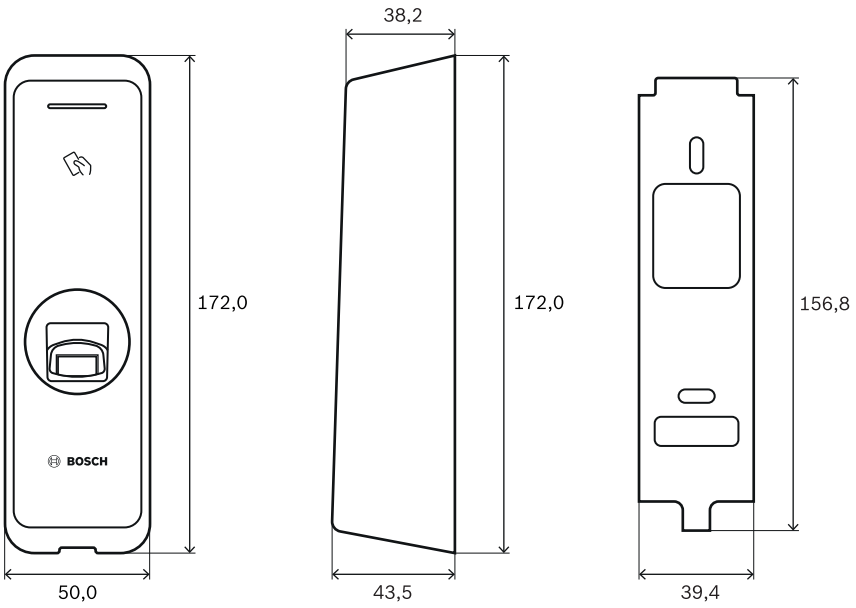
Memory (RAM) (MB)	256 MB
Processor type	1.2 GHz Quad Core

* For more information on templates, refer to BIS/ACE and AMS installation manuals.



Notice!
Data stored in the reader can be deleted by the Operator through the host system, if requested.

4.2 Dimensions



5 UL

5.1 UL 294 requirements

The following UL 294 levels apply:
- Destructive attack - level 2
- Line security - level 2
- Endurance - level 1
- Standby power- level 1

If the unit is powered by an external power supply, you can use:
- UL Listed Class 2 power supply with 12VDC
- UL 294B Listed PoE power source

6 FCC

6.1 Compliance information

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: 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 or more 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.

This appliance and its antenna must not be co-located or operation in conjunction with any other antenna or transmitter.
A minimum separation distance of 20 cm must be maintained between the antenna and the person for this appliance to satisfy the RF exposure requirements.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2022

Building solutions for a better life.

202206301752