dormakaba
access manager 92 30

MATRIX – TP4 client

Technical Manual

04048135 - 2020/10

9230-K7, TP4-Client

EN

dormakaba

dormakaba EAD GmbH
Albertistraße 3
78056 Villingen-Schwenningen
Germany
T: +49 7720 603-0
www.dormakaba.com
Company headquarters: Villingen-Schwenningen

Copyright © dormakaba 2020
All rights reserved.

No part of this document may be reproduced or used in any form or by any means without prior written permission of dormakaba Schweiz AG.

All names and logos of third-party products and services are the property of their respective owners.

Subject to technical changes.

04048135 - 2020/10

9230-K7, TP4-Client

Table of content

1 About this document 5
1.1 Validity 5
1.2 Target group 5
1.3 Contents and purpose 5
1.4 Additional documentation 6
1.5 Availability of additional documentation 7
1.6 Orientation in the document 7
1.7 Instructions 7
1.8 Abbreviations/term definitions 8
1.9 Warnings 9
1.9.1 Hazard categories 9
1.9.2 Symbols 9
1.10 Notes 9

2 Basic safety instructions 10
2.1 Assembly and installation 10
2.2 Service and maintenance 10
2.3 Accessories and spare parts 10
2.4 ESD prevention measures 11
2.5 Environmental protection 11
2.6 Data protection and IT security 12

3 Product description 13
3.1 Overview 13
3.2 Device versions 13
3.3 Specification 14
3.4 Technical data 16
3.4.1 Power supply 16
3.4.2 Data retention in case of power failure 16
3.4.3 Output voltages 16
3.4.4 Frequency bands and transmission power 17
3.4.5 Interfaces 17
3.4.6 Terminals 17
3.4.7 Inputs 17
3.4.8 Outputs 18
3.4.9 Ambient conditions 18
3.4.10 Dimensions/Weight 18
3.5 Conformity 19
3.6 Open source information 20
3.7 Identification 21
3.8 Included in supplied package 21
3.9 Accessories 22
3.9.1 Detection units 22

4 Construction and function 23
4.1 Light emitting diodes 23
4.1.1 Device status 23
4.2 Opening the housing 24
4.3 Tamper switch 25
4.4 Reading behaviour 26
4.4.1 Behaviour with two registration units 26
4.4.2 Behaviour of readers installed next to each other 26
4.4.3 Behaviour when several media are present in the field (anti-collision) 26
4.5 Access control with MATRIX 27

4.5.1 MRD principle 27
4.5.2 Wiegand principle 28
4.5.3 Mobile Access system overview 29
4.5.4 System requirements 30

5 Installation 31
5.1 Installation requirements 31
5.1.1 General 31
5.1.2 Installation site 31
5.1.3 Connections 31
5.1.4 Cable entry 32
5.2 Installation lines 33
5.2.1 General requirements 33
5.2.2 Ethernet 33
5.2.3 Lines to RS-485 devices 33
5.2.4 Line to the door opener, the door opener key, and the door contacts 34
5.2.5 Coaxial cables to registration units 34
5.2.6 Line to the Wiegand reader 34
5.3 Wall mounting 35
5.4 Routing of lines 36
5.5 Connections 36
5.5.1 Ethernet 36
5.5.2 Overview of connection terminals 37
5.5.3 Connecting registration units 38
5.5.4 Connection to RS-485 devices 39
5.5.5 Connecting the Wiegand reader 41
5.5.6 Inputs 42
5.5.7 Outputs 43
5.6 Fastening the cover 44

6 Commissioning 45
6.1 Network parameters 45
6.1.1 MAC address of the device 46
6.1.2 Change network parameters with 'MATRIX Device Scanner' 47
6.2 Configuration 49
6.3 Initialise the device for Mobile Access 50
6.4 Additional steps for Legic media technology 52
6.4.1 Grant read/write authorisation 52
6.4.2 Withdrawing read/write authorisation 53

7 Maintenance 54
7.1 Restart reader 54
7.2 Reset the device to factory settings 55

8 Decommissioning 56
8.1 Disassembly 56

9 Packaging/return 57
9.1 Complete devices 57
9.2 Electronic component assemblies 57
9.3 Labelling 58

10 Disposal 59

Index 60

1 About this document

1.1 Validity

This document describes the product:

Product designation:	dormakaba access manager 92 30
Product code:	9230-K7
Article number:	04079231
Firmware:	TP4 ≥ V4.03

This document describes all product variants and all optional accessories and functions. Options are subject to a charge and are thus only available if they have been purchased. Additional accessories and functions may not be available on the date of publishing and may only be available for purchase at a later point in time.

1.2 Target group

This manual is intended for skilled persons only.

The descriptions are intended for skilled persons trained by the manufacturer. This manual is not a replacement for product training.

For reasons of equipment safety, the installation, maintenance and service measures described in this documentation should only be carried out by skilled persons in accordance with EN 62368-1 (Audio/Video, Information and Communication Technology Equipment – Part 1: Safety Requirements).

Skilled person is the designation for people who have the appropriate technical training and experience in setting up the equipment. Skilled persons are expected to use their training and experience to identify any risks to themselves and others that may arise while carrying out these activities, and to minimise these risks as far as possible. It is the skilled person's responsibility to ensure that the conditions stated by the manufacturer and the applicable regulations and standards are complied with when carrying out these actions.

This documentation is also used to provide information for persons with the following tasks:

- Project planning and project implementation
- Commissioning the product within the network
- Connecting the product to user software by programming customer applications
- Customer-specific adjustments with product parameterisation

1.3 Contents and purpose

Contents are limited to the assembly, installation, commissioning and basic operation of the product.

1.4 Additional documentation

MATRIX system environment

Planning	Planning guideline • Mobile Access • Wireless
System software	User manual/online help • MATRIX Professional • MATRIX One
Access manager Function type: MATRIX – TP4 client	Technical manual • Access manager 92 00 [9200-K5] • Access manager 92 00 [9200-K7] • Access manager 92 30 [9230-K5] • Access manager 92 30 [9230-K7] • Access manager 92 90 Rack [9290-K5] • Access manager 92 90 Rack [9290-K7] • Access manager 92 90 Wall [9290-K5] • Access manager 92 90 Wall [9290-K7]
Compact reader Function type: Access manager	Technical manual, MATRIX – TP4-Client • Compact reader 91 04 • Compact reader 91 10 • Compact reader 91 12
Remote reader Function type: Access manager	Technical manual, MATRIX – TP4-Client • Remote reader 91 15 • Remote reader 91 25
S6-R reader	Technical manual
Interface 90 10 Function type: Access manager	Technical manual • Interface 90 10
Reader Interface	Technical manual
Programmer 1460	Technical manual
Wireless Gateway 90 40	Technical manual
Terminals	Technical manual • 96 00 • 97 00
Electronic fittings	Technical manual • c-lever (compact/pro/air) • XS-Fitting Pro
Electronic cylinders	Technical manual • Digital cylinder • XS-Cylinder Pro

[XXXX-K#] = Product code
There are several generations of the devices under the same product name.

1.5 Availability of additional documentation

Additional documentation is available on the dormakaba extranet.

You will need a user account to access the extranet. A user account can be created directly. Detailed information about this is available on the homepage.

dormakaba extranet
http://www.dormakaba.com/extranet-emea-en

1.6 Orientation in the document

This document contains the following features to help find specific topics:

- The table of contents at the beginning of the document offers an overview of all topics.
- The header contains the associated main section.
- Cross references indicate the number of the section containing additional information. Example [▸ 5.7].
- An index in alphabetical order is given at the end of the document.

1.7 Instructions

Structure and symbols of the instructions are illustrated in the following example:

✓ Prerequisite

1. Step 1

   ⇨ Interim result

2. Step 2

⇨ Result

1.8 Abbreviations/term definitions

Abbreviation	document	Explanation
AoC	Access on Card	With Access on Card, the authorisations are saved to RFID media.
APIPA	automatic private IP addressing	Devices/computers automatically get an IP address if there is no DHCP server present.
-	Bluetooth®	An international transmission standard based on radio technology for contactless exchange of data.
DoC	Data on Card	With Data on Card, the data is written from devices to RFID media. Example: Capacity of batteries
DP1	Device Protocol 1	Protocol for data transfer via RS-485 bus.
KCP	Kaba Communication Protocol	Protocol for data transfer via RS-485 bus.
NFC	Near Field Communication	An international transmission standard based on RFID technology for contactless exchange of data.
RFID	Radio-Frequency Identification	Technology for transmitter-receiver systems for the automatic and contactless identification of objects with radio waves.
TP4	Terminal Protocol 4	Protocol for data transfer via RS-485 bus or Ethernet.
VCP	Versatile Configuration Package	Configuration package for Mobile Access

1.9 Warnings

Warnings containing information/instructions and prohibitions designed to prevent personal injury or damage are specially marked.

Please pay attention to warnings! They are intended to help avoid accidents and prevent injury and damage.

1.9.1 Hazard categories

Warnings are divided into the following categories:

⚠ CAUTION

Low risk

Indicates a possibly dangerous situation which may lead to minor physical injury.

NOTICE

Important information on the correct use of the product.

Failure to comply with these instructions could lead to malfunctions. It is possible to damage the product.

1.9.2 Symbols

Symbols with the following meaning are used for warnings, depending on the source of danger.

General hazard

Danger of damage to electronic components from electrostatic discharge

1.10 Notes

Notes are indicated by an info symbol.

Tips and useful information.
These help you make the best use of the product and its functions.

2 Basic safety instructions

This product has been built to state-of-the-art standards and in line with established safety regulations. However, hazards for persons and property may arise when handling the product.

Read and observe the following safety instructions before using the product.

2.1 Assembly and installation

Check the device for visible damage caused by transport or incorrect storage. Do not start up any damaged device!

Assembly and installation of the product may only be done by skilled personnel (see chapter 1 Target group).

Mains voltage installations may only be carried out by a certified specialised company or authorised electricians.

When installing/inserting the product in end-use equipment all requirements of the mentioned test standards must be fulfilled.

The product should only be installed in locations which fulfil the environmental and technical conditions specified by the manufacturer.

The manufacturer is not liable for damage arising due to improper handling or incorrect installation.

2.2 Service and maintenance

Conversions and modifications to the product may only be done skilled personnel (see chapter 1 Target group). Any conversions and modifications performed by other persons will exempt us from any liability.

The elimination of faults and maintenance work may only be performed by skilled personnel (see chapter 1 Target group).

2.3 Accessories and spare parts

Accessories and spare parts must meet the manufacturer's technical requirements. This is guaranteed if original dormakaba accessories and spare parts are used.

2.4 ESD prevention measures

NOTICE

Risk for electronic components due to electrostatic discharge.

Incorrect handling of electronic PCBs or components can result in damage which will cause a complete breakdown or sporadic errors.

- General ESD prevention measures must be observed when installing or repairing the product.
- Wear an anti-static wrist strap when handling electronic components. Connect the end of the strap to a discharge box or a non-painted, earthed metal component. This way, static discharges are channelled away from your body safely and effectively.
- Handle a PCB along its edges only. Do not touch the PCB or connectors.
- Place dismantled components on an anti-static surface or in an anti-static shielded container.
- Avoid contact between PCBs and clothing. The wrist strap protects PCBs against an electrostatic discharge voltage from the body only. However, damage can also be caused by an electrostatic discharge voltage from clothing.
- Transport and ship dismantled modules in conductive anti-static bags only.

2.5 Environmental protection

It is prohibited to dispose of the device in your domestic waste.

Used devices contain valuable materials that should be recycled. Properly dispose of used devices.

Dispose of consumed batteries in accordance with state and local regulations.

Carefully store the batteries to be disposed of to avoid short circuits, crushing or destruction of the battery casing.

2.6 Data protection and IT security

The system software and the device must be configured for safe operation.

Unauthorised access to the device and the system is possible without further security settings.

Security risks

- Data protection violation through unauthorised access to person-related data
- Unauthorised access
- Tampering/system failure

Recommended measures

- Device:
  - Keep the firmware current.
  - Before decommissioning: Reset the device to factory settings.
- System software:
  - Activate encrypted communication.
  - Switch off network ports that are not required.
  - Follow the dormakaba MATRIX security hardening guide.
  - Copy the latest patches.

The recommended actions refer only to the linking of the dormakaba access managers to the MATRIX system software without making any claims as to completeness and currency.

The facility operator of the system must ensure the protection of person-related data and IT security in their entire organisation by taking suitable measures.

3 Product description

3.1 Overview

The device is used as an access control terminal in an access control system.

The access control system is managed with the system software. In the system software, the access permissions are assigned and the connected devices are configured. The access permissions are saved in the device.

More devices are connected to the device. The connected registration units/readers read the data from media. The device checks the permission of the media.
The device supports Mobile Access. With Mobile Access, smartphones with the dormakaba mobile access app become media.

If a medium is authorised, the device releases the access.

The doors status is identified and evaluated via the digital inputs of the device.

3.2 Device versions

The variants have a different assembly of the connection terminals.

MRD

- 1 RS-485 interface
- 2 coaxial interfaces
- 1 RS-232 interface
- 4 inputs
- 3 outputs

Wiegand

- 2 Wiegand interfaces
- 1 RS-232 interface
- 4 inputs
- 3 outputs

3.3 Specification

System environment

- System software: MATRIX Professional/MATRIX ONE
- Access manager: TP4 client

Memory capacity

- Standard: max. 50,000 employee records

Installation

The device is fixed to the wall.

Special feature

- The power supply to the device is provided via PoE/PoE+.
- The device provides output voltages for power supply to other devices.
  - Reader: 5/12 V DC
  - Output 1: 12/24 V DC

Connections for readers/devices

Depending on the variant, the following readers/devices can be connected.	
MRD variant	**Wiegand** variant
• 1 RS-485 interface The protocol is determined in the system software. Depending on the protocol, the following devices can be connected. – KCP: up to 2 readers Compact reader 91 xx Only readers with functional type 'Access Manager' are supported. – DP1: up to 2 readers and 2 additional devices S6-R reader, door module, additional – phgCrypt: up to 2 readers from third-party manufacturers or • 2x registration units 90 xx via the coaxial interfaces	• 2 Wiegand interfaces
• 1 RS-232 interface – Reader with ASCII character transfer (9600 Baud, 8N1) e.g. barcode scanner	• 1 RS-232 interface – Reader with ASCII character transfer (9600 Baud, 8N1) e.g. barcode scanner

Inputs/outputs

- 4 digital inputs
  - For connecting insulated switches
  - Power supply integrated
- 3 outputs
  - Potential free switching contact
  - Output 1: Power supply 12/24 V DC possible with cable link

Security against attacks

- The communication with the system software can be encrypted.
- The device has two tamper switches.

Use

- Door management of 1 door
- Personal interlocks
- Arming intruder detection systems

3.4 Technical data

3.4.1 Power supply

The power supply is provided via Power over Ethernet (PoE).

- **PoE**, as per IEEE 802.3af
- **PoE+**, as per IEEE 802.3at
  - The availability is signalled via LED.

3.4.2 Data retention in case of power failure

The time, data and the configuration are retained without a power supply.

- Battery-backed real-time clock
  Battery type: CR2032

3.4.3 Output voltages

<table>
<tr><th colspan="2">Available output

The available output depends on the supply voltage.</th><th rowspan="2">Output voltages/power</th></tr>
<tr><td>PoE
max.
5 W
(7 W)*
↓</td><td>PoE+
max.
15 W
(17 W)*
↓</td></tr>
<tr><td colspan="2" rowspan="4">The available power is allocated to the output voltages.

The total of the connected power must not exceed the available power.

Note: The power reduces to max. 10 W as the device starts. If capacitive appliances are connected, the power must be reduced further.

→

* Applies only to the output voltage 12 V at OUT1 if no further output voltage is loaded.</td><td>• Output OUT1
– 12 V DC
→ max. 17 W
– 24 V DC
→ max. 12 W</td></tr>
<tr><td>• RS-232 interface
– 5 V DC
→ max. 2.5 W</td></tr>
<tr><td>MRD variant:
• RS-485 interface
– 12 V DC
→ max. 6 W</td></tr>
<tr><td>Wiegand variant:
• Available at Wiegand interfaces
– 12 V DC
→ WIEG A: max. 3.5 W
→ WIEG B: max. 3.5 W
– 5 V DC
→ WIEG A: max. 2.5 W
→ WIEG B: max. 2.5 W</td></tr>
</table>

3.4.4 Frequency bands and transmission power

- **RFID/NFC**: 13,56 MHz, 4,88 dBµA/m at 10 m distance

3.4.5 Interfaces

- **Ethernet**
  - 10/100 Mbit/s

    IEE802.3 compatible, auto-sensing, auto MDI-X
  - Signalling the status via LEDs
- **RS-232**
  - Transfer parameters (default): 9600 baud, 8 data bits, even parity, 1 stop bit

---

MRD variant:

- **RS-485**
  - KCP protocol

    Transmission parameters: 19200 baud, 8 data bits, even parity, 1 stop bit
  - DP1 protocol

    Transmission parameters: 2,400/4,800/9,600/19,200/38,400 baud, 8 data bits, even parity, 1 stop bit
  - phgCrypt protocol

    Transmission parameters: 9,600/19,200 baud, 8 data bits, no parity, 1 stop bit
- **ANT A/ANT B**
  - For connecting registration units
  - Impedance of the coaxial cable: 50 Ω

Wiegand variant:

- **2 Wiegand interfaces**

3.4.6 Terminals

- Conductor type: single-wire/multi-wire
- Conductor cross-section: 0.14–1.5 mm^2, AWG 28–16
- Insulation stripping length: 7 mm

3.4.7 Inputs

IN 1–IN 4

- For connecting insulated switches
- Integrated power supply: 5 V DC
- Signalling the status via LEDs

Tamper switch

- 2 tamper switches

3.4.8 Outputs

Out 1 - Out 3

- 3 relays
- Maximum load current: 30 V AC/DC; max. 2 A

  Power supply units must meet the following requirements.
  LPS and SELV as per IEC/EN/UL/CSA 60950-1 or ES1 and PS2 as per IEC/EN/UL/CSA 62368-1.
- Signalling the status via LEDs

Out 1:

- Contacts with output voltages
  - 12 V DC
  - 24 V DC
  - GND

3.4.9 Ambient conditions

- Ingress protection according to IEC 60529: IP40
- Relative humidity: 5% to 85%, non-condensing
- Ambient temperature:
  - 0 °C – +50 °C (operation)
  - -20 °C – +65 °C (storage)

3.4.10 Dimensions/Weight

- Length: 208 mm
- Width: 208 mm
- Depth: 48 mm
- Weight: approx. 0.6 kg

3.5 Conformity

You can download the original declaration of conformity in PDF format at www.dormakaba.com/conformity.

MRD variant

This product meets the provisions of the EU directives

- **2014/53/EU – Radio Equipment Directive (RED)**
- **2011/65/EU – Restriction of Hazardous Substances (RoHS)**

UL/CSA

This product complies with the following standards.

- **UL62368-1:2014-12**
- **CAN/CSA-22.2 No. 62368-1:2014-12**

FCC

FCC Code of Federal Regulations, CFR 47, Part 15, Sections 15.205, 15.207, 15.215 and 15.225

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

FCC § 15.21 (Warning Statement)

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

FCC § 15.105

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

IC

Industry Canada Radio Standards Specifications RSS-GEN Issue 5 and RSS-210 Issue 10

ICES-003

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Canada RSS-GEN 8.4

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:
(1) This device may not cause interference; and
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
1) l'appareil ne doit pas produire de brouillage;
2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Wiegand variant

This product meets the provisions of the EU directives

- **2014/35/EU – Low Voltage Directive (LVD)**

- **2011/65/EU – Restriction of Hazardous Substances (RoHS)**

UL/CSA This product complies with the following standards.

- **UL62368-1:2014-12**
- **CAN/CSA-22.2 No. 62368-1:2014-12**

3.6 Open source information

The firmware contains packages that are subject to open source licenses.

dormakaba provides the following legal information for each firmware version.

- List of open source packages
  - Name and version of the packages
  - Name and version of the licenses
- Detailed information on the individual packages
  - Detailed license texts
  - Information on copyright

The legal information can be accessed via the following.

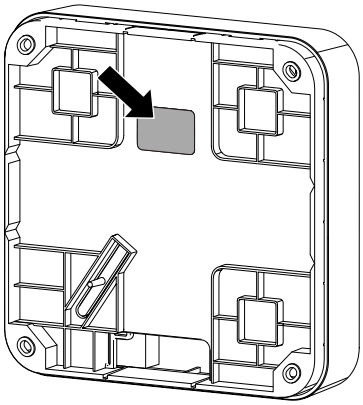
- dormakaba extranet

  The firmware and the legal information are packed in a ZIP file.
- Accessing the device via browser/console program

Disclaimer
In accordance with the conditions of the open source licenses, dormakaba points out that the developers of packages have excluded any liability and warranty for the packages and their properties. The details are available in the respective license conditions.

By pointing out this exclusion of liability, dormakaba exclusively fulfils the license conditions of the packages. Legal and contractual claims against dormakaba are not affected by this exclusion of liability.

3.7 Identification



Identification label

The following can be found on the identification label:

- Manufacturer's address
- Product code, function type
- Connection data of power supply
- Article number
- Hardware version
- Production date
- Protection type
- CE marking, optional additional conformity marks
- Note: Disposal as household waste is prohibited

3.8 Included in supplied package

- Access manager 92 30
- Quick guide
- For mounting to the wall:
  - 4.5 x 35 screw (4 pieces)
  - Washer (4 pieces)
  - Dowel (4 pieces)
- Cable tie (2 pieces) for internal cable routing
- Cable link for power supply to OUT1
- PT countersunk screw 3 x 8 (2 pieces) for fastening the housing cover
- Suppressor set for connecting up to 2 inductive appliances (electric strike, ...)

3.9 Accessories

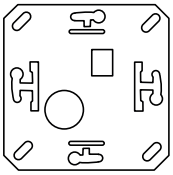
3.9.1 Detection units

Registration unit 90 00

Class of protection: -

Installation: On-site switch or socket ranges

For order code, see catalogue



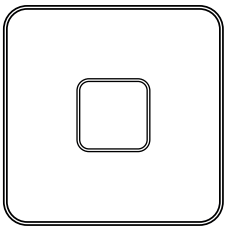
Registration unit 90 01

Colour: black or white

Class of protection: IP40 or IP54

Cable feed: Surface-mounted or flush-mounted

For order code, see catalogue



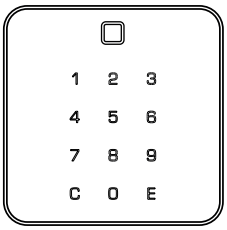
Registration unit 90 02

Colour: black or white

Class of protection: IP40 or IP54

Cable feed: Surface-mounted or flush-mounted

For order code, see catalogue



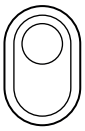
Registration unit 90 03

Colour: Black

Class of protection: IP55

Cable feed: Flush-mounted

For order code, see catalogue



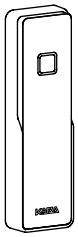
Registration unit 90 04

Colour: black or white

Class of protection: IP66

Cables: Length 8 m or 30 m

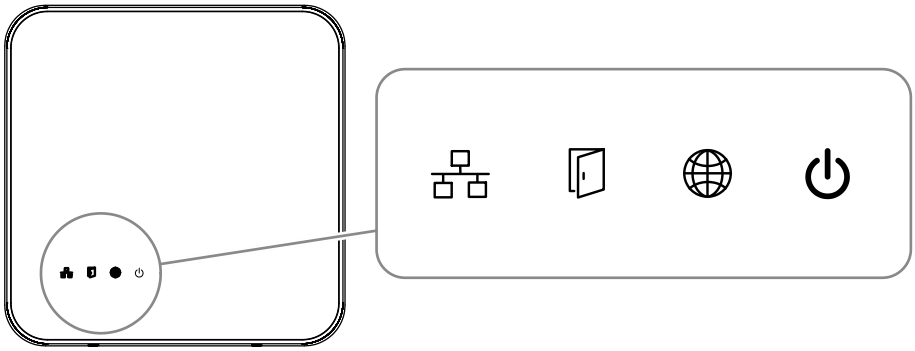
For order code, see catalogue



4 Construction and function

4.1 Light emitting diodes

The front housing contains 4 light emitting diodes for status display.



Icon	Designation	Signal	Meaning
	Ethernet	yellow	Data transfer is active
		off	No data transfer
	Device status	See chapter Device status	
	no function	-	-
	Power	green	The power supply is stable.
		red	Overload at the output voltages. The output voltages at OUT1 are switched off.
		off	no power supply

4.1.1 Device status

The status LED indicates the device's status.

State-LED	Meaning
off	No power supply
Flashing green light	The device is ready for operation. The flashing frequency indicates the load of the CPU of the device. The slower the LED flashes, the more the CPU is loaded.
Solid green light	The device is ready for operation. The device's CPU is fully loaded.
Flashing red light	The device cannot access the DHCP server and has assigned itself an IP from the 169.254.x.x range via auto IP (RFC 3927). If the DHCP server is accessible again, the device detects the DHCP server only after a few seconds.
Solid red light	The device is not ready for operation.

4.2 Opening the housing

NOTICE

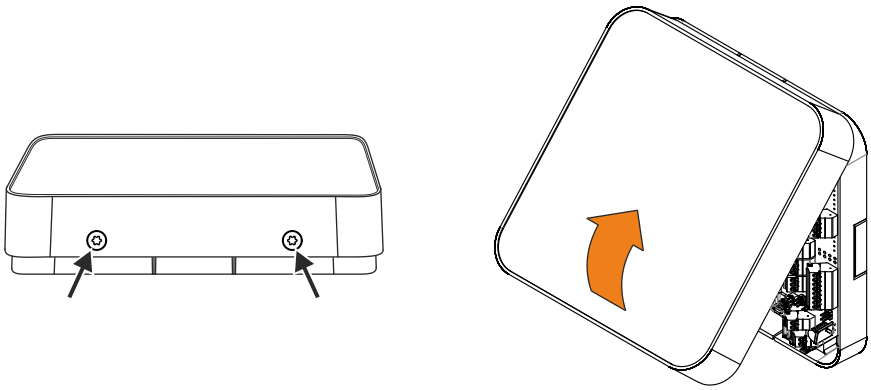
Danger for electronic components due to electrostatic discharge.

Improper handling can damage or destroy electrostatically sensitive components on printed circuit boards (PCB).

- General ESD protective measures must be observed and applied.

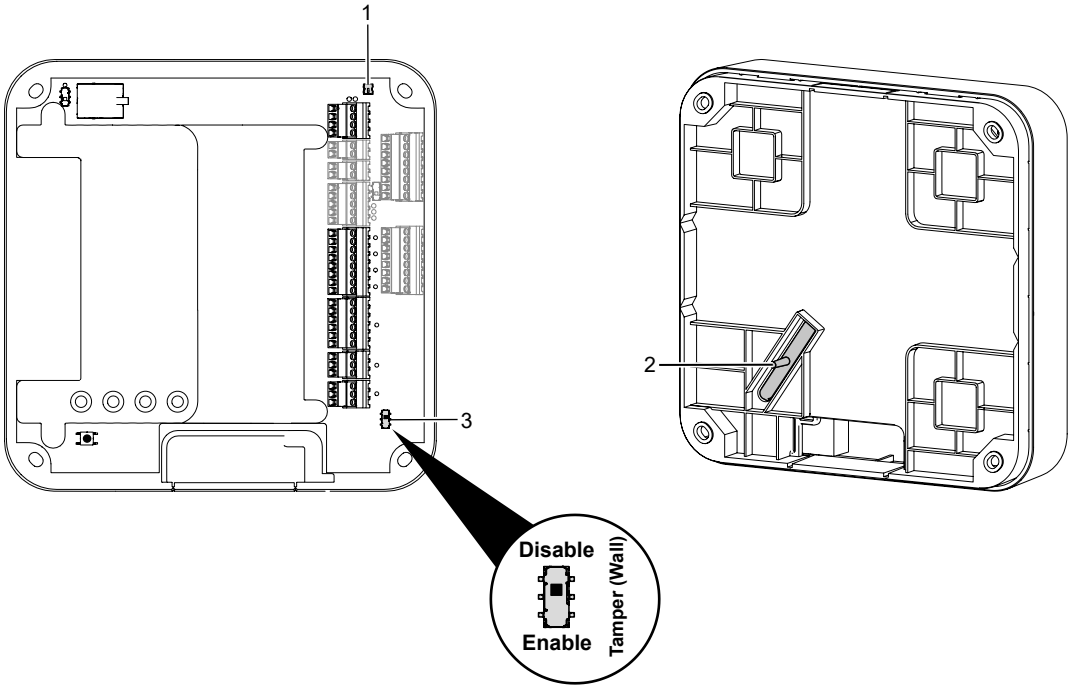
Remove the housing cover as follows:

1. Remove two PT countersunk screws 3 x 8 (TORX 8) from the underside of the device.
2. Pivot the cover and disconnect it at the top.



4.3 Tamper switch

The device has two tamper switches.



1 **Tamper switch Housing**

If the cover is removed, a tampering notification is triggered.

2 **Wall tamper switch**

If the device is removed from the wall, a tampering notification is triggered.

To avoid error messages in case of uneven walls, set the switch [3] to **Disable**.

3 Switch for wall tamper switch

- Disable: No tampering monitoring
- Enable: Tampering monitoring enabled

The function depends on the settings in the system software.

4.4 Reading behaviour

4.4.1 Behaviour with two registration units

The access manager communicates alternately via the connections “Ant. A” and “Ant. B” (toggle) with the registration units connected to it. Hence, the access manager cannot communicate with both registration units at the same time. This results in the following behaviour:

- During a longer read process, the respective other registration unit is blocked.
- The fields of the two connected registration units do not influence each other. Therefore, the two registration units can be installed close to each other.
- In case of such registration units installed close to each other, it may happen that the medium is read by both registration units in succession.

4.4.2 Behaviour of readers installed next to each other

Readers which are installed next to each other do not influence each other during the read process.
Minimum distance between two readers: approx. 30 cm

4.4.3 Behaviour when several media are present in the field (anti-collision)

Several RFID user media (prime, ISO14443A and ISO15693) can be detected in the field simultaneously. Only the first user medium that corresponds to the search criteria defined in the system is considered.

4.5 Access control with MATRIX

The device is used as an access control terminal in an access control system.

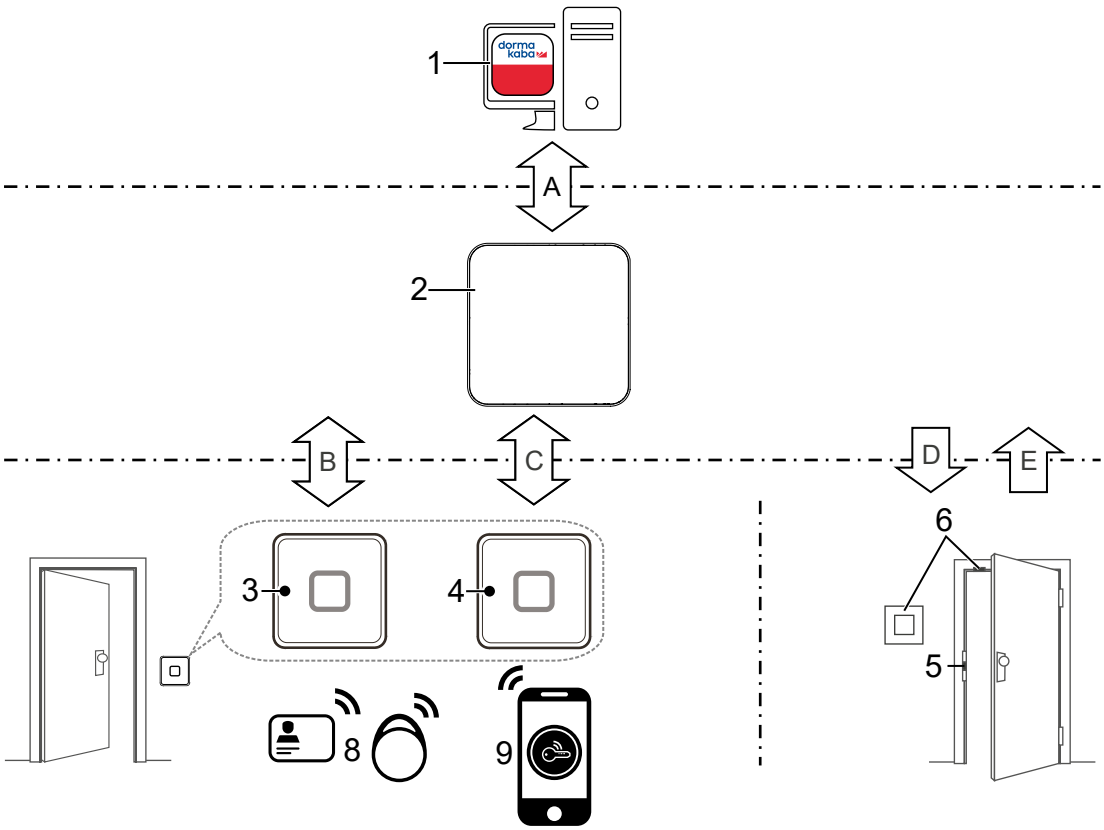
The access control system is managed with the system software. In the system software, the access permissions are assigned and the connected devices are configured. The access permissions are saved in the device.

More devices are connected to the device. The connected registration units/readers read the data from media. The device checks the permission of the media.
The device supports Mobile Access. With Mobile Access, smartphones with the dormakaba mobile access app become media.

If a medium is authorised, the device releases the access.

The doors status is identified and evaluated via the digital inputs of the device.

4.5.1 MRD principle



1	System software		6	Repeater (Contacts, buttons, switches)
2	Access manager 92 30			
3	Reader		Media	
4	Registration unit		8	ID card/key fob
5	Locking device		9	Smartphone

A Access rights, bookings, notifications, configuration

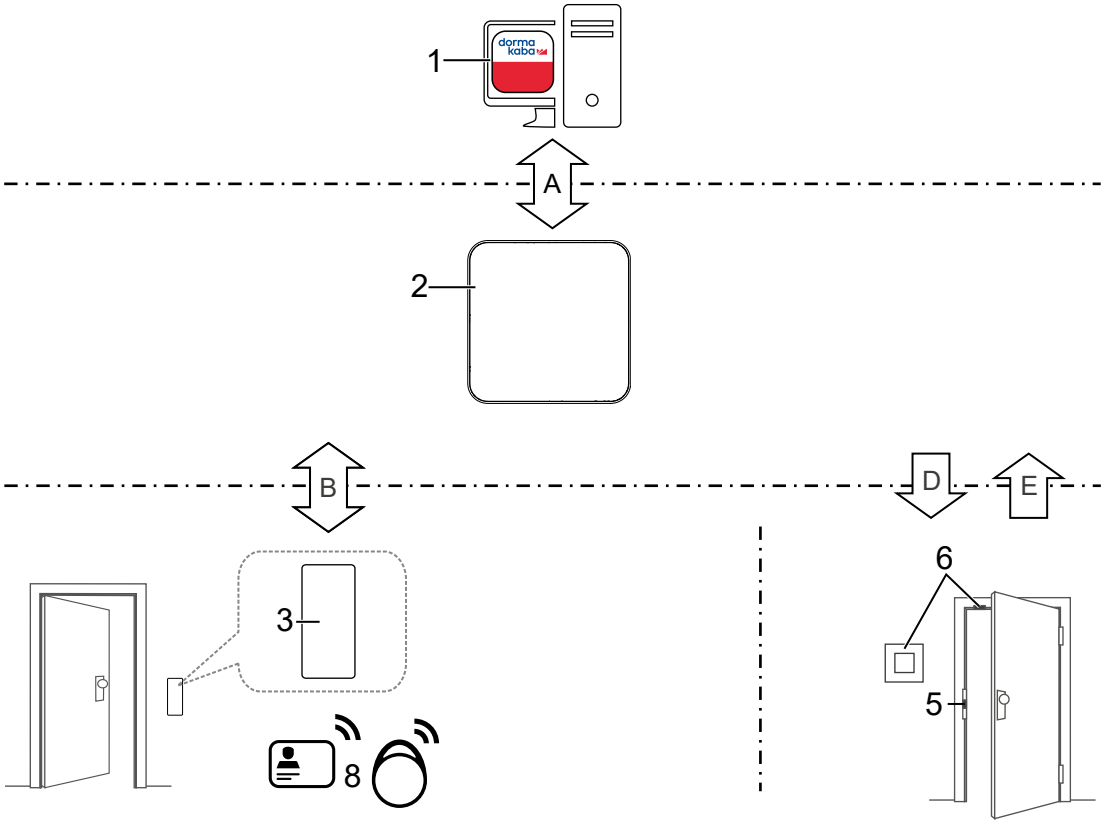
B Data from media, signalling, configuration

C Data from media, signalling

D Activating the locking device/signal transmitter

E Repeater status

4.5.2 Wiegand principle



1	System software		6	Repeater (Contacts, buttons, switches)
2	Access manager 92 30			
3	Reader		Media	
5	Locking device		8	ID card/key fob

A Access rights, bookings, notifications, configuration

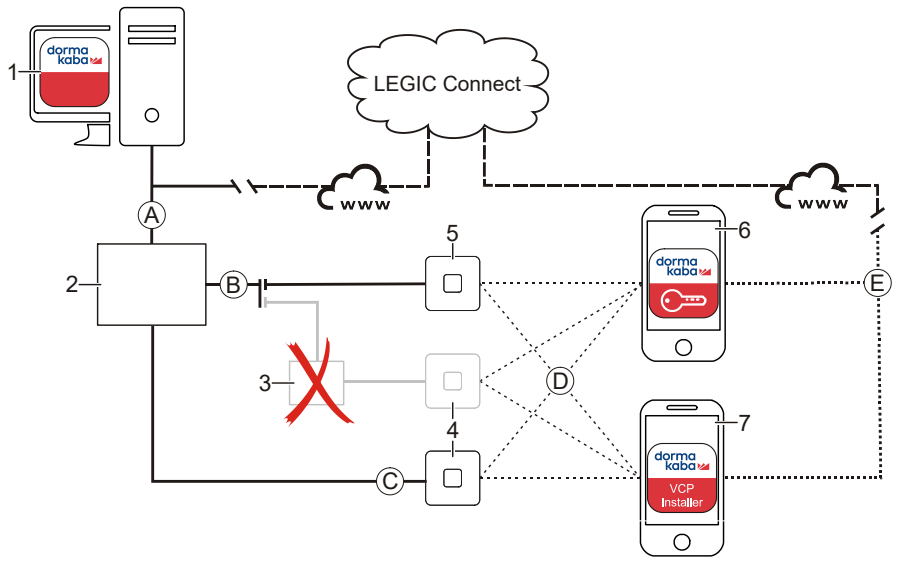
B Data from media, signalling

D Activating the locking device/signal transmitter

E Repeater status

4.5.3 Mobile Access system overview

The system software distributes the access permissions via **LEGIC Connect** to the smartphones.



A	Ethernet		D	NFC or Bluetooth
B	RS-485		E	WLAN/mobile data
C	Coaxial cable/HF RFID			

1	System software	
2	Access manager	

		NFC	Bluetooth
3	The remote readers are not supported on this device.		
4	**Registration unit**		
	90 00 -K5	●	–
	90 01 -K5	●	–
	90 01 -K6	●	●
	90 02 -K5	●	–
	90 03 -K5	●	–
	90 04 -K5	●	–

		NFC	Bluetooth
5	**Compact reader**		
	91 04 -K5	●	–
	91 04 -K6	●	●
	91 10 -K5	●	–
	91 12 -K6	●	●

		Operating system	NFC	Bluetooth
6	Smartphone with **dormakaba mobile access** app The Mobile Access bookings are carried out with it.	**Android**	●	●
		iOS	–	●
7	Smartphone with **VCP Installer** app The VCP Installer initialises the Mobile Access function.	**Android**	●	●
		iOS	–	–

● yes – no

4.5.4 System requirements

Function	Access manager firmware	System software
	• TP4 client	• MATRIX Professional • MATRIX ONE
General	≥ Version 4.03	≥ Version 3.2.x
Mobile Access	≥ Version 4.0#	≥ Version 3.2.x • MATRIX Professional – with option Mobile Access

4.5.4.1 Mobile Access system requirement

General
- The access control system is set up by dormakaba for Legic Connect

System software
- See the chapter System requirements
- A connection has been set up to Legic connect

Reader
- The reader supports Mobile Access.
- The reader is configured in the system software for Mobile Access.
- The configuration is transferred.
- The reader is installed and ready for operation.

Also see
- Mobile Access System Overview chapter
- Planning guideline, Mobile Access

5 Installation

5.1 Installation requirements

5.1.1 General

An accurate installation of all components is a basic requirement for a properly functioning device. The following installation instructions must be adhered to.

5.1.2 Installation site

- The device is designed for a fixed installation in buildings. Installing it in vehicles is not permitted.
- Install the device only in rooms that meet its ambient conditions.
- Install the device within the secured range.
- The device must not be installed in an area exposed to strong electromagnetic fields produced by elements such as switching power supply units, electric power lines and phase control modulators!
- The device is designed for wall assembly.

5.1.3 Connections

The following connectors must have been prepared at the installation site of the access manager:

- Ethernet cable with RJ45 connector

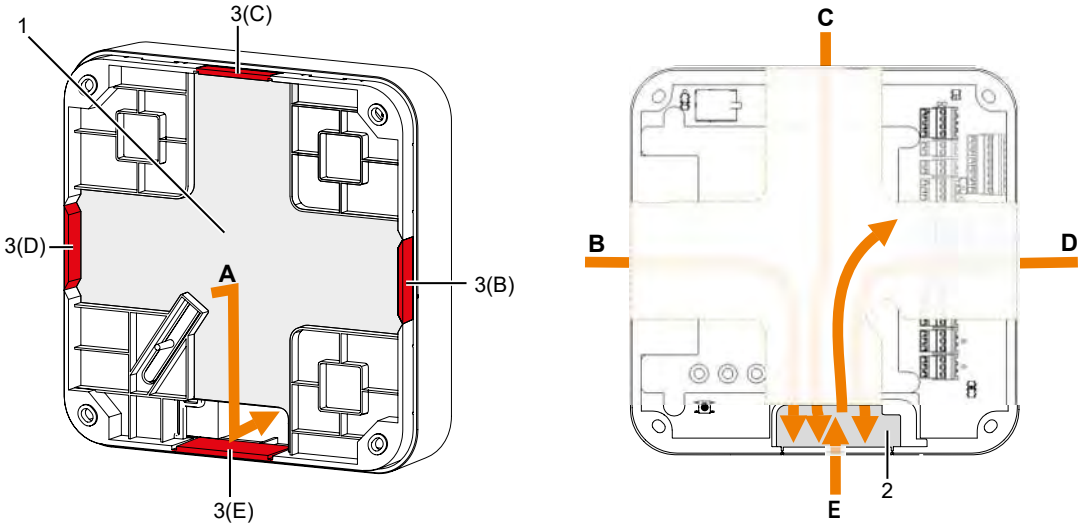
  For the power supply a PSE (Power Sourcing Equipment) must be provided.

  Possible methods for feeding the power supply via the PSE:

  – End span (direct supply, e.g. via PoE switch)

  – Midspan (supply via intermediate sources, e.g. PoE injector)
- Signal lines to door openers and contacts
- Coaxial lines to the registration units and/or data lines to the readers.

5.1.4 Cable entry



The lines are routed from behind [A] or to the side [B–E].

- Route the lines at the rear in a stream [1], through the opening [2] to the connections at the front.
- For cable routing on the side, remove the prepared breakouts [3].

5.2 Installation lines

5.2.1 General requirements

The installation of the cables must conform to the current national and local regulations. In general, the following requirements apply.

- Protection against manipulation
  - Install the cables inside the security areas.
  - Install the cables so that they are hidden or difficult to access.
- Avoiding malfunctions
  - Keep the cable routes short.
  - Lay low-voltage and data lines away from sources of interference.

5.2.2 Ethernet

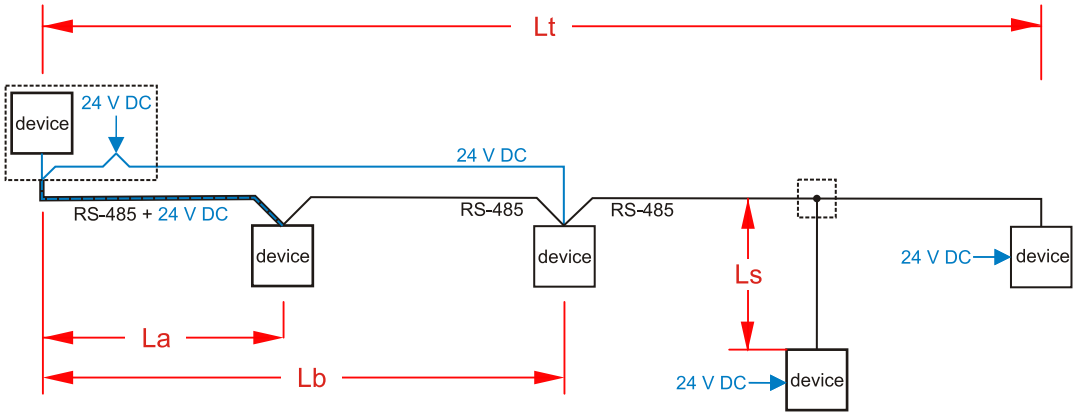
Network cable with RJ45 plug, line requirement: CAT.5 S-UTP 4 x 2 AWG 24 oder AWG 22 (according to EIA/TIA568) or higher quality.

5.2.3 Lines to RS-485 devices

The RS-485 devices are connected via a bus in 2-wire technology.

Wiring requirements

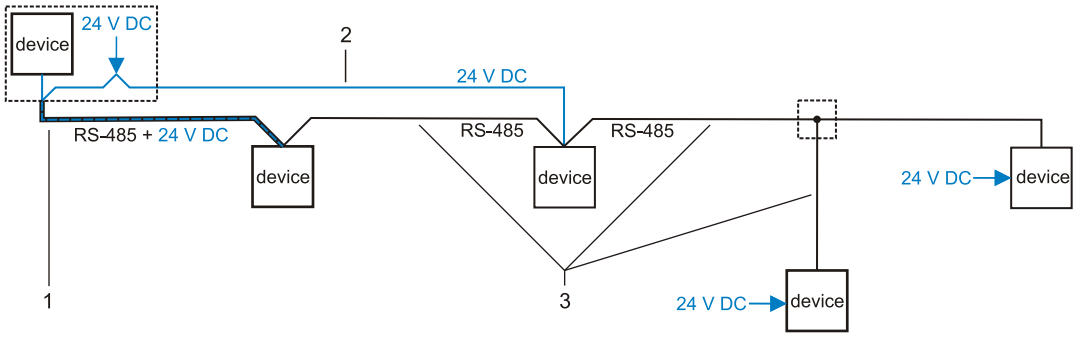
- Shielded line with twisted wire pairs.
- No other signals may be carried in the wire, except for the low voltage for the power supply to the RS-485 devices.
- Cable lengths:



Lt	The total permissible length (master and branch lines) is max. 1200 m.
La	If the RS-485 bus and the extra-low voltage is led through one cable, the max. permissible length is 20 m. • If the distance is long, lay a separate line for the low voltage.
Lb	Low voltage in a separate cable • The length depends on the voltage drop of the cable. The voltage must conform to the requirement of the RS-485 device. • For longer distances, use a local power supply.
Ls	The permissible length per branch line is max. 100 m. • Not recommended, since branch lines can cause malfunctions.

Recommended cabling

For the RS-485 bus, use only cables of the same type.



1	CAT.5 S/UTP 4x2 AWG 22 or J-Y(ST)Y 2x2x0.6
2	J-Y(ST)Y 2x1x0.8
3	CAT.5 S/UTP 4x2 AWG 24 or J-Y(ST)Y 2x1x0.6

5.2.4 Line to the door opener, the door opener key, and the door contacts

Line requirements: Cable diameters from 0.5 mm to 0.8 mm.

Recommended cable: CAT.5 S-UTP 4 x 2 AWG 24 or AWG 22 (according to EIA/TIA568) or higher.

5.2.5 Coaxial cables to registration units

Registration units are connected to the access manager via coaxial cables The coaxial cable transfers the HF signals from the RFID antenna, keyboard data and trigger data for the optical and acoustic signal generators.

Line requirements: Coaxial cable 50 ohms, type RG174/U.

Maximum cable length: 30 m

Recommended cable length: < 10 m

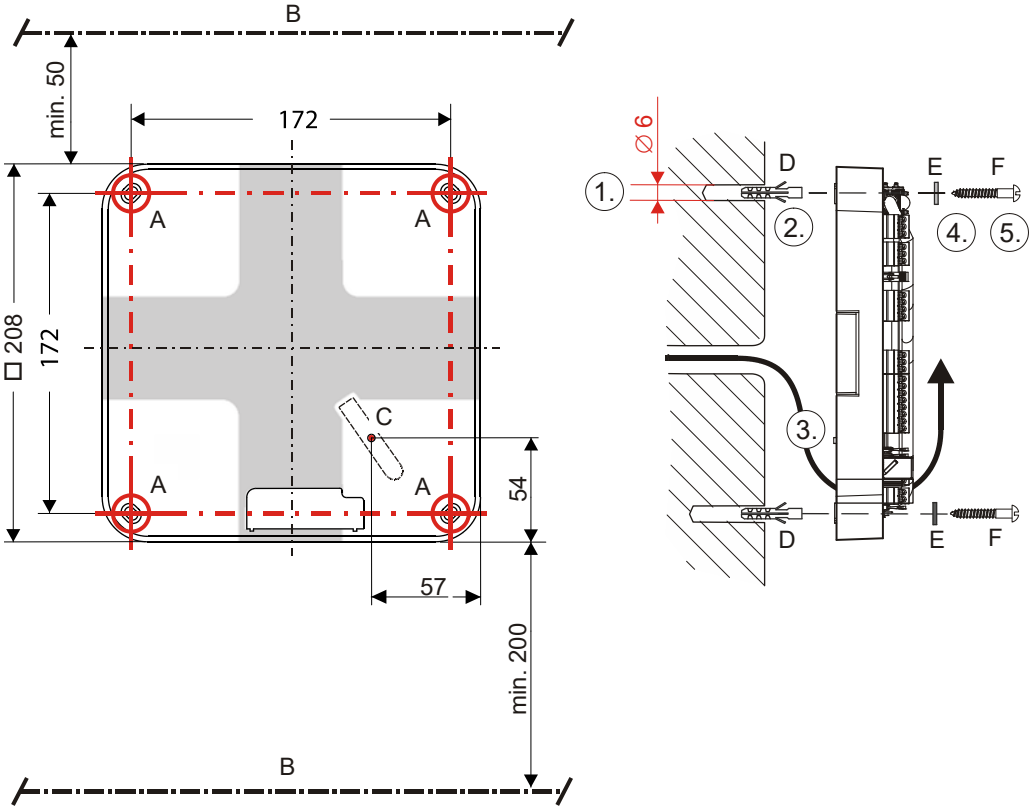
5.2.6 Line to the Wiegand reader

Line requirements: Shielded line 6 x 0.6 mm (0.34 mm^2) or 6 x 22 AWG

Maximum line length: 10 m

Length and technical design of the line must comply with the requirements specified by the reader manufacturer.

5.3 Wall mounting



All dimensions in mm

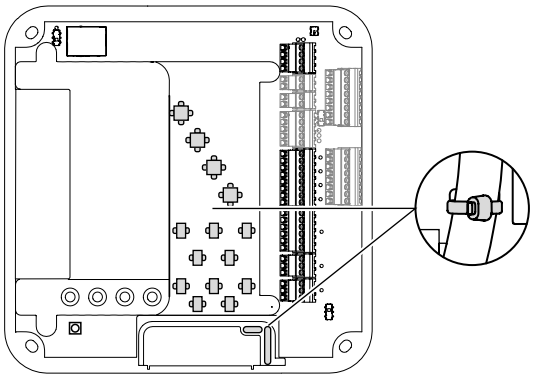
A	Mounting points	D	4x dowel
B	Required space	E	4x washer
C	Wall tamper switch	F	4x screw

✓ For side cable feed only: Breakouts have been removed.

1. **NOTICE! Make sure not to damage any in-wall lines!**
   Drill 4x holes
2. Insert dowels (D)
3. **NOTICE! Route cable in rear duct. Do not crush the cable.**
   Position the device on the wall
4. Push the washers (E) onto the screws (F)
5. Screw the device in place

On uneven walls the function of the tamper switch (C) is not assured.
The tamper switch can be deactivated to prevent false alarms.
See Vandal contact

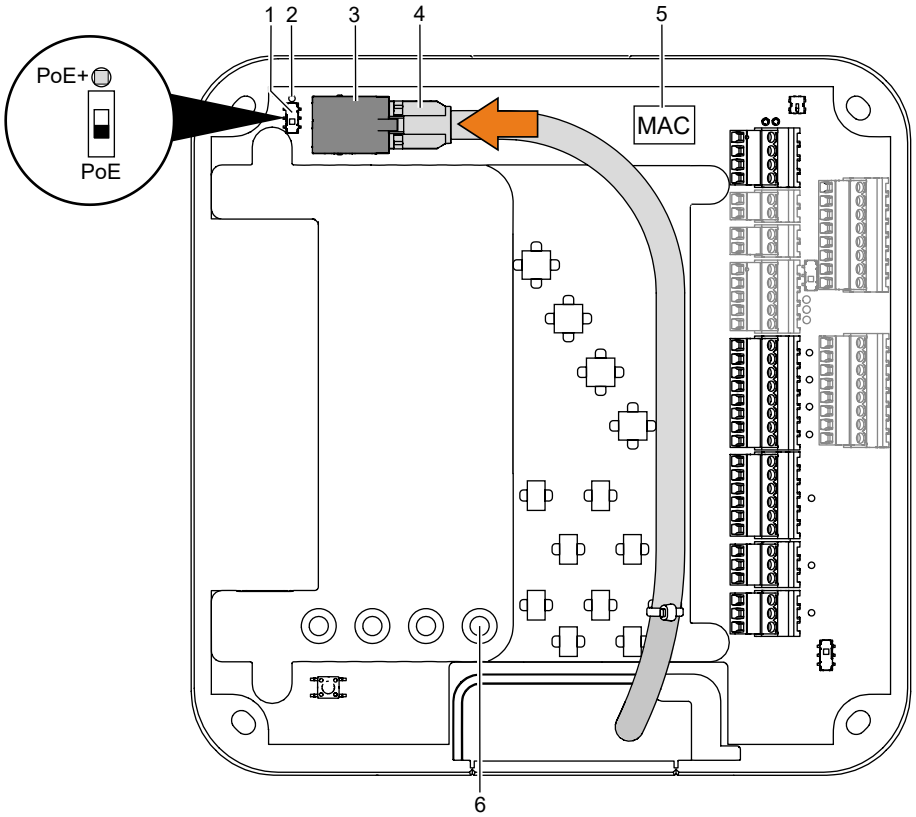
5.4 Routing of lines



The lines are routed using cable ties. Lugs are available to fasten the cable ties.

5.5 Connections

5.5.1 Ethernet



✓ The power supply through a PSE (Power Sourcing Equipment) is ensured.

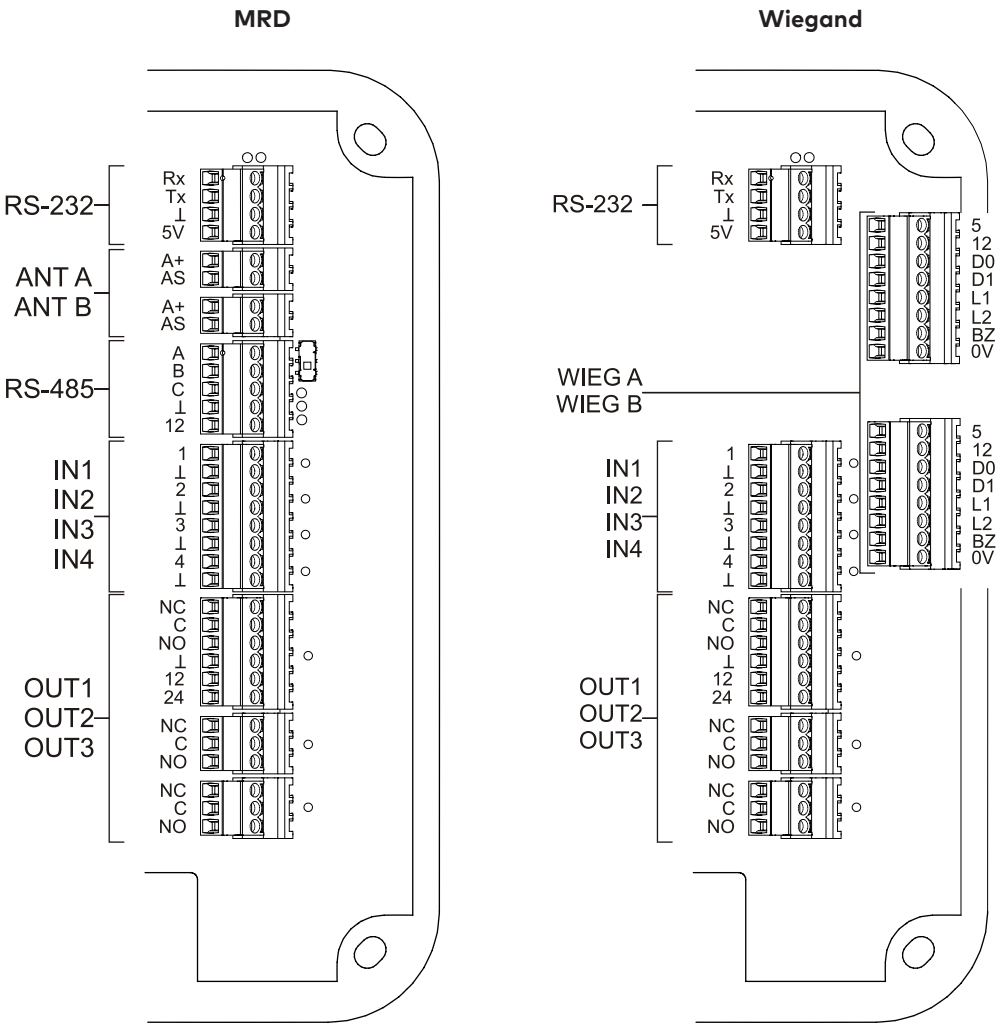
1. Set the power supply **PoE** or **PoE+** using the switch [1].
2. Plug in the network cable [4] in the ethernet socket [3].

⇨ When power is supplied to the device, the power LED [6] glows.

⇨ If PoE+ is supplied by PSE, the **PoE+** LED [2] glows.

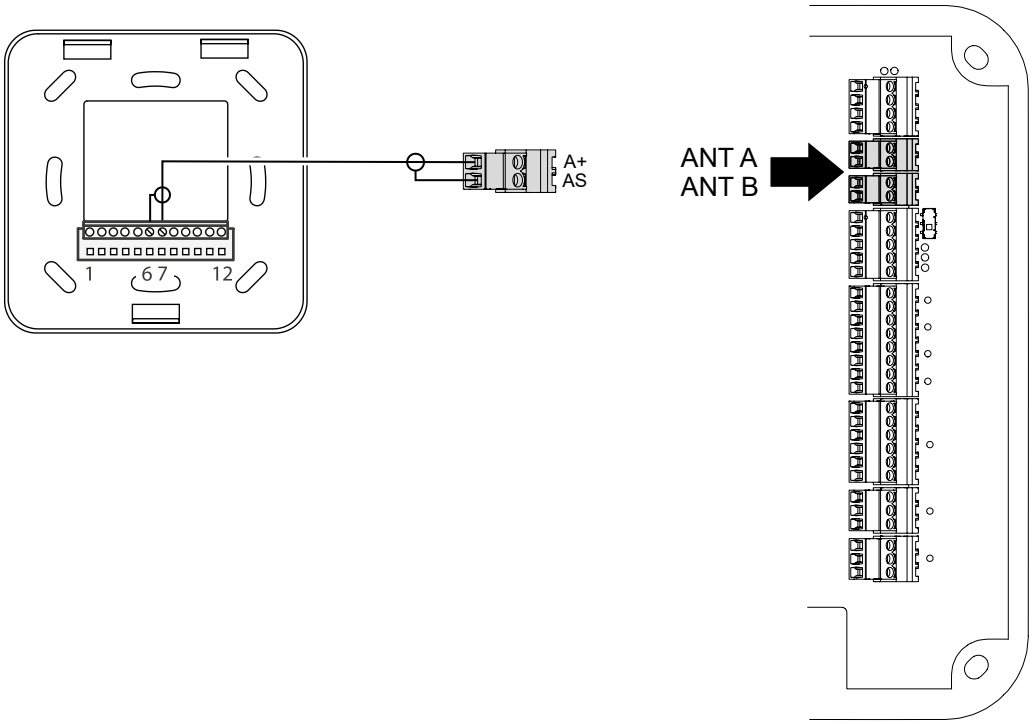
The MAC address of the device can be found on a label [5].

5.5.2 Overview of connection terminals



Connection	Connection for
RS-232	Barcode scanner/reader
ANT A/ANT B	Registration units
RS-485	Readers and other RS-485 devices
WIEG A/WIEG B	Wiegand reader
IN1–IN4 (Inputs)	Repeater Example: Electric strike button, door handle, door frame, deadbolt, passage contact, other...
OUT1–OUT3 (Outputs)	Locking device/signal transmitter Example: Electric strike, motor lock, turnstile drive, other...

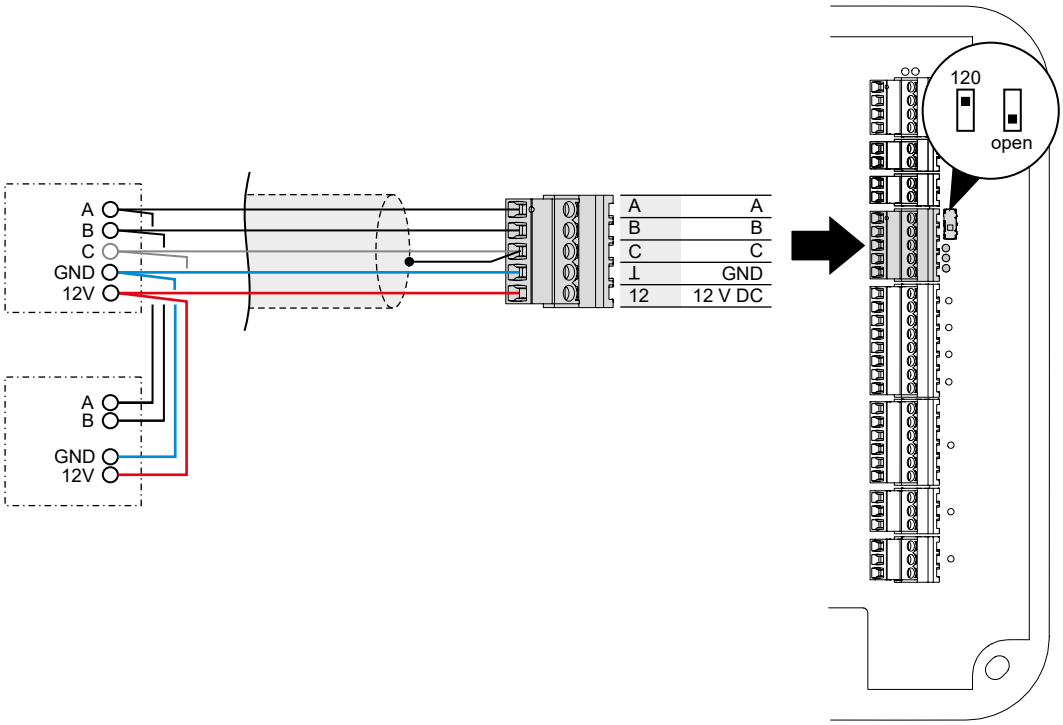
5.5.3 Connecting registration units



Example: Registration unit connection 90 01/90 02.

Connection identification	Assignment
A+	Coaxial cable neutral conductor
AS	Coaxial cable shield

5.5.4 Connection to RS-485 devices



Connection diagram

- A ↔ A; B ↔ B
- optional C ↔ C
- Connect the cable shield on one side of the terminal C of the access manager.

An output voltage of 12 V DC is available for power supply to the RS-485 devices.

Observe the dependencies of output voltages.
See Output voltages [▸ 3.4.3]

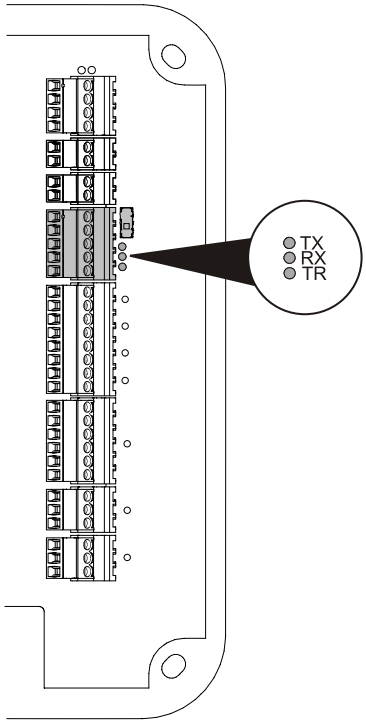
Terminal resistance

Set the terminating resistor with the switch.

Position of the switch	Usage
120	• **Bus wiring** The device is connected at the end of the bus. • **Star wiring**
open	• **Bus wiring** The device is connected within the bus.

5.5.4.1 Signaling

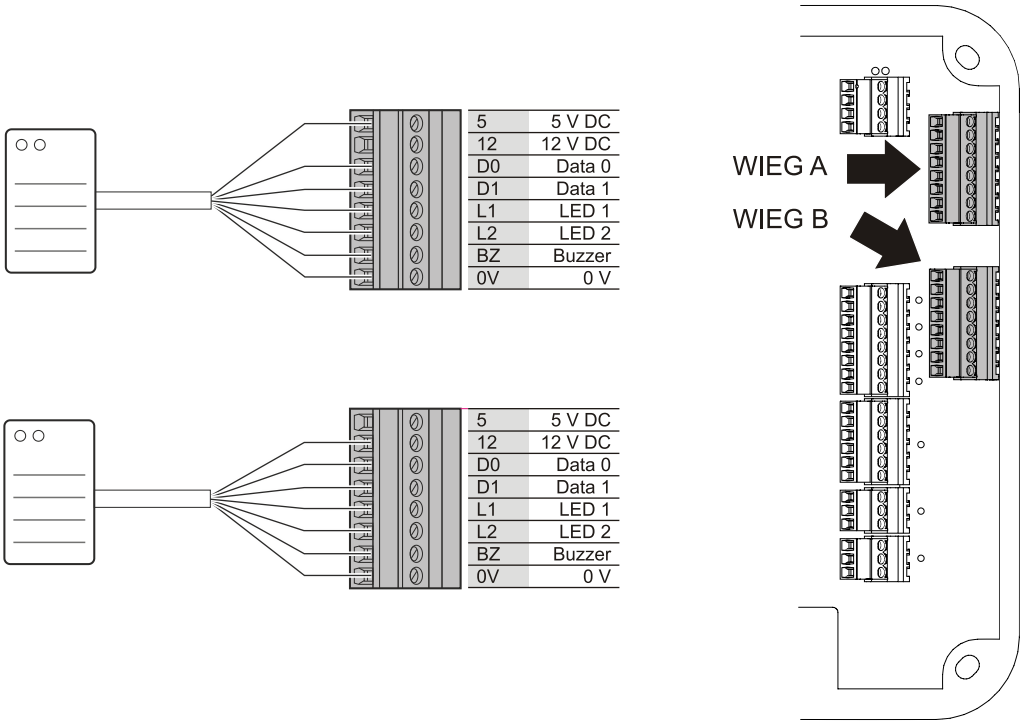
Three LEDs signal the statuses of the RS-485 interface.



The signals have the following meaning:

Designation	Signal	Meaning
TR	Off	Transmission direction, not ready to receive
	Shines	Ready to receive
TX	Off	No data
	Lights up/flashes	Data is being transmitted
RX	Off	No data
	Lights up/flashes	Data is being received

5.5.5 Connecting the Wiegand reader



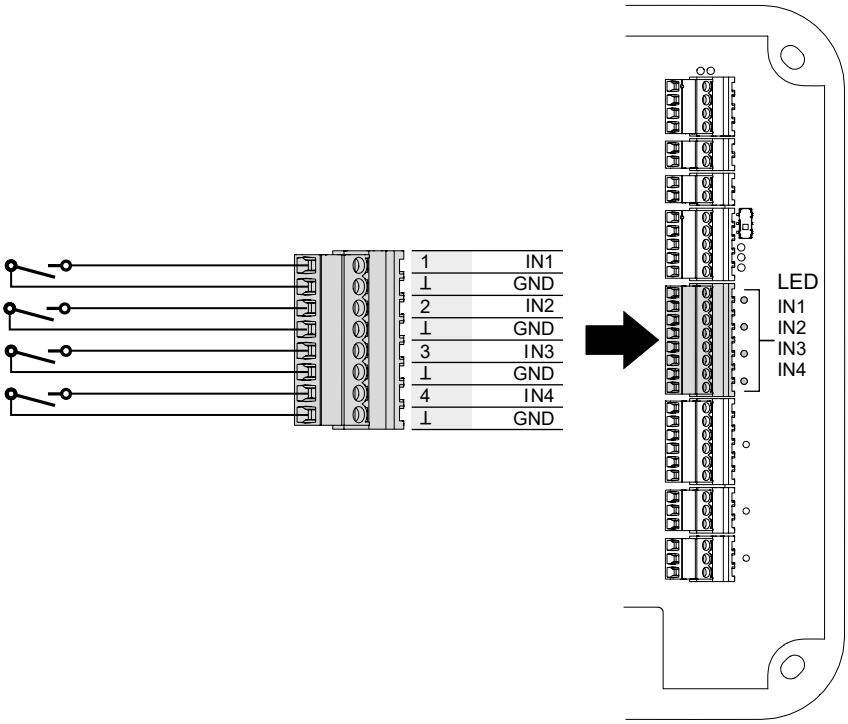
The connection takes place as specified by the manufacturer.

The following voltages are available for power supply to Wiegand readers.

- 12 V DC
- 5 V DC

Observe the dependencies of output voltages.
See Output voltages [▸ 3.4.3]

5.5.6 Inputs



Each input has two contacts (IN, GND). One input is activated by closing the two contacts.

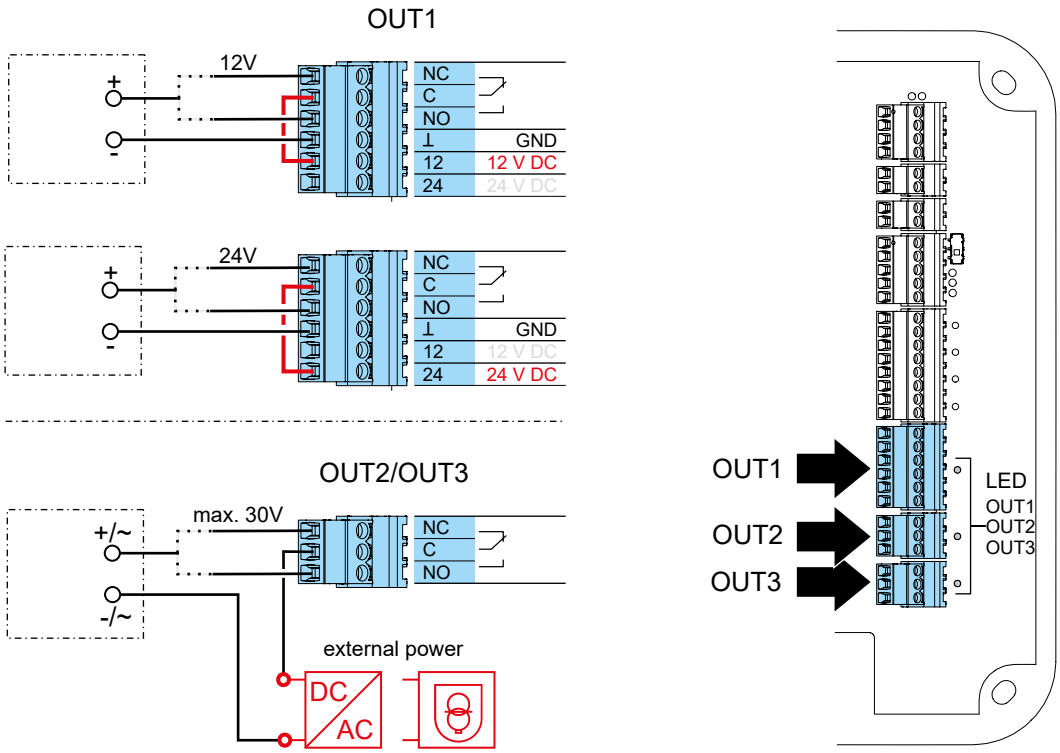
The function depends on the settings in the system software.

Signaling

The LEDs **IN1–IN4** signal the status of the inputs.

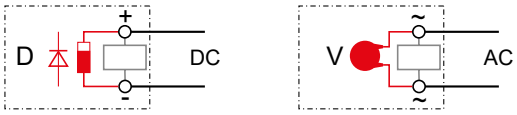
- **Off:** The input is not active. The contacts are open.
- **Solid green light:** The input is active. The contacts are closed.

5.5.7 Outputs



If an inductive appliance (relay, electric strike, ...) does not have separate interference suppression measure, the following interference suppression measure must be attached to the appliance:

- Direct current (DC): Connect a diode [D] parallel to blocking direction.
- Alternate current (AC): Connect a varistor [V] parallel.



The following voltages are available at **OUT1**.

- 12 V DC
- 24 V DC

Observe the dependencies of output voltages.
See Output voltages [▸ 3.4.3]

Route the required output voltage with the cable link (scope of delivery) to the contact.

The power supply at **OUT1** can alternatively be provided via an external power supply unit. External power supply units are required for the power supply at **OUT2** and **OUT3**.

- Maximum load current: 30 V AC/DC; max. 1 A

  Power supply units must meet the following requirements.
  LPS and SELV as per IEC/EN/UL/CSA 60950-1 or ES1 and PS2 as per IEC/EN/UL/CSA 62368-1.

Signaling

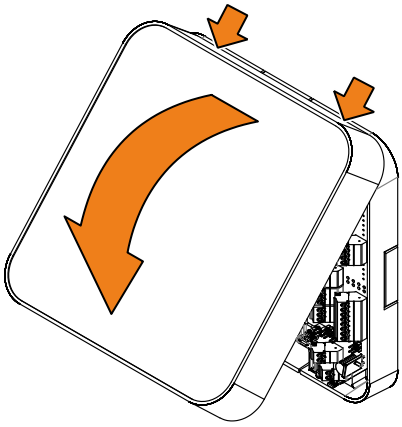
The LEDs **OUT1–OUT3** signal the status of the outputs.

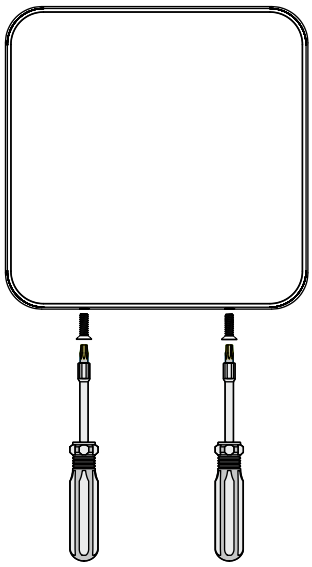
- **Off:** The relay is not triggered.
- **Solid green light:** The relay is triggered.

5.6 Fastening the cover

Fasten the housing cover as follows:

1. Connect the holding brackets for the top housing cover to the lower section of housing.
2. Pivot the housing cover down and close the housing.
3. Secure the housing cover to the lower section of housing with two PT countersunk screws 3 x 8 (TORX 8).





6 Commissioning

6.1 Network parameters

Agree on the network parameters of the network, the device and the system software, and set them.

Overview of the ports		Setting		
Designation	**Number**			
• **Server command** (TCP) for data transfer from the device to the system software	Standard: 3000 Range: 1–32,767	●	■	🔓
• **Terminal command** (TCP) for data transfer from the system software to the device	Standard: 3001 Range: 1000–32,765	●	■	🔓
• **ITM** (TCP) Inter-terminal communication	= *Terminal command* +1	○	■	🔓
• **Network monitoring** (TCP) Network monitoring of units among each other	= *Terminal command* +2	○	■	–
• **Telnet** (TCP) Access to service functions via Telnet.	Standard: 23 Range: 1–32,767	◐	■	🔓
• **mDNS** (UDP) Multicast DNS	5353 (fix)	◐	■	–
• **DNS** (TCP/UDP) Host name resolution by DNS server	53 (fixed)	○	–	–
• **HTTP/HTTPS** (TCP) You can use a browser to open a configurable transaction page via the web server	Standard: 80/443 Range: 1–32,767	○	–	🔓
• **SNMP** (UDP) To monitor the LAN interface with SNMP	Standard: 161 Range: 1–161	○	–	–

Setting

Network: Firewall

The required ports must be released and activated.

- ● required
- ◐ needed for MATRIX Device Scanner, otherwise optional
- ○ optional

Device: Supplied state

- ■ On
- – Off

The following ports can be activated/deactivated in the system software.

- Telnet

- HTTP/HTTPS
- SNMP

Other settings:

- Ports=Standard
- DHCP operation: on
- Host name = '<MAC-Adresse>.local'. The MAC address is input without the ':'.

System software

🔓 Optionally encrypted communication can be activated.

– Encryption not possible.

The IP address or the host name must be input in the system software.

6.1.1 MAC address of the device

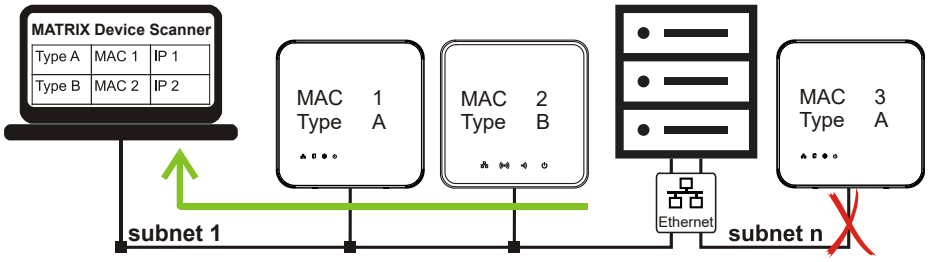
The MAC address of the device can be found on a label. (see chapter Ethernet [▶ 5.5.1])

The host name in the delivered state is = '<MAC-address>.local'. The MAC address is input without the ':'.

Recommended:
Note the device's MAC address. The device can be uniquely identified in the network based on the MAC address.

6.1.2 Change network parameters with 'MATRIX Device Scanner'

The program 'MATRIX Device Scanner' finds dormakaba devices with an Ethernet interface on a network.



Prerequisites

- The necessary ports are activated on the network.
- The devices are installed and available.
- The devices can be found in the same subnet.
- Microsoft Windows compatible laptop
  - LAN interface
  - Network setting:
    - Automatically get IP address (DHCP on)
    - Automatic private IP address (APIPA)
    With this setting, devices are found on networks without a DHCP server.

Functions The program offers the following functions.

- The network parameters of the devices can be set for the initial setup.
  - Use DHCP
  - Assign static IP (IP address, network mask, gateway IP)
- The IP addresses of the devices are discoverable.

Installation The program must be installed on a laptop. The installer can be found on the MATRIX DVD in the folder 'MATRIX Device Scanner'.

Illustration After program start-up, dormakaba devices are searched for on the network. The devices found are listed.

Columns				
Type	MAC address	IP address	Action	Comment

Column	Explanation
Type	The type of the devices
MAC address	The MAC address of the devices **Note:** The MAC address can be found on a label on the devices.
IP address	The current IP address of the devices
Action	• **Empty field** The network parameters are set. • **Change network setting...** The network parameters must be set.
Comment	• **Empty field** The network parameters must be set.

	• **Device is already in use (...)** The network parameters are set. – (Device number ##) MATRIX device number – (Telnet not available) – (Password changed) only wireless gateway

Operation **Change the network parameters of the device**

✓ The device cannot be configured by MATRIX.
Alternatively: Reset the device to factory settings.

✓ The MAC address is known.

1. Search for the device on the list. (MAC address, type)
2. Click the 'Change network settings...' button.
   ⇨ A new window opens.
3. Set the network parameters
4. Click the 'Change settings' button.
   ⇨ This window closes.

⇨ The network parameters of the device have been changed.

6.2 Configuration

The configuration of the device is done in the system software.

Requirements

- The necessary ports are activated on the network.
- The system software is installed and ready for operation.
- The device is installed and ready for operation.
- The network parameters of the device are set for the existing network.
- The IP address or the host name of the device is known.

In the system software, carry out the following steps. A login as user with administrator rights is necessary.

1. Create and configure the device
2. Transfer the configuration data
3. Define access permissions for the doors
4. Define access permissions for persons

In existing systems, all the steps do not have to be carried out.

6.3 Initialise the device for Mobile Access

See also:
- Mobile Access system overview
- Planning guideline, Mobile Access

Initialisation depends on the readers used.

Reader	Initialisation
Registration unit	The access manager is initialised via a registration unit.
Compact reader	Every compact reader must be initialised.

Prerequisites

General
- The access control system is set up by dormakaba for Legic Connect

System software
- See the chapter System requirements
- A connection has been set up to Legic connect

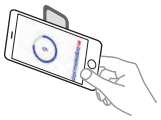
Reader
- The reader supports Mobile Access.
- The reader is configured in the system software for Mobile Access.
- The configuration is transferred.
- The reader is installed and ready for operation.

Smartphone
- The VCP Installer is installed and registered with the telephone number with Legic Connect.
  The registration code received via SMS is entered.
- Access to the Internet is possible (WLAN or mobile data).
- The password for the VCP file is known.

Procedure

- On the smartphone:
  - Start the VCP Installer.
  - Ensure that the method of transmission of the smartphone and the device is identical
    Select the transmission type NFC or Bluetooth.
  - Select the VCP file.
    If the desired VCP file is not present, select 'Update'. Then, the smartphone downloads the VCP file.
  - Select 'Send'.
  - Input the password for the VCP file.
  - Transmission type:

NFC



Hold the smartphone in front of the reader.

Bluetooth

Keep the smartphone within Bluetooth range of the device.

If a device other than the one desired flashes: In the system software, match the 'RSSI filters' of the devices.

- Reader to which the smartphone is held:

  - After successful initialisation: Three signals are sounded.
  - After a **failed** initialisation: no signalling
  - Then, the device signals the base state defined in the parent system.
- Smartphone:
  - After successful initialisation: display of the serial number of the device.

6.4 Additional steps for Legic media technology

With Legic media technology, a write/read authorisation is required in the following cases:

- If it is necessary to write to a write-protected segment of a medium.

  Example: AoC
- If a read-protected segment of a medium is to be read.

6.4.1 Grant read/write authorisation

The authorisation is granted via a registration unit.

The term "Write authorisation" is used in this chapter for the terms "Write authorisation" and "Read authorisation".

A write authorisation with a LEGIC prime SAM 63 card is only valid for LEGIC prime.

A write authorisation with a LEGIC advant SAM 63 card is valid for LEGIC prime and LEGIC advant 15693 and 14443A.

In this chapter, the names "Security card C2" are used for the card names "SAM 63" and "Security card C2 (SC-C2)" .

Requirements

- A security card C2 with the corresponding segment zone is present.
- The ISO standard 14443A must have been activated with the security card C2.
- The ISO standard of the SAM 63 card must conform to the parameterised ISO standard.
- The device is in normal operation and waits for a RFID input.

Procedure

1. Hold the security card C2 in the RFID field until the signalling takes place

   ⇨ Signalling after successful write authorisation:
   3x beep
   glows red till the next booking takes place

   ⇨ Signalling after **unsuccessful** write authorisation:
   - "Access not authorised"

   Possible reasons
   - The security card C2 was removed too early from the RFID field.
   - If no reaction: ISO 14443A is not activated in the system
   - If using SAM+ media: there are no credits available

2. Remove the security card C2 from the RFID field.

6.4.2 Withdrawing read/write authorisation

Read/write authorisation must be withdrawn in the following cases:

- If no more data is to be written to write-protected segments of a medium.
- If reading from read-protected segments of a medium is no longer to be read.

In this chapter, the term 'write authorisation' shall be used to refer to both 'write authorisation' and 'read authorisation'.

6.4.2.1 Withdrawing all write access issued via a write authorisation

Reset the device to factory settings. (See chapter Maintenance)

6.4.2.2 Withdrawing individual write access issued via a write authorisation

The withdrawal is carried out via a regestration unit.

Requirements

- For cancelling the write authorisation, a SAM 64 card with the corresponding segment zone is required.
- The device and the registration unit are ready for operation.

Procedure

1. Present the master medium.
   ⇨ A brief signal sounds and glows green briefly.
2. Present the SAM 64 card uninterrupted to the compact reader (approx. 15 s).
   ⇨ The regestration unit glows green during the process.
   ⇨ 3x beeps: Write authorisation was cancelled

   If write authorisation has already been revoked before with the same SAM 64 card, this is signalled immediately with three beeps.

   ⇨ No signal: Write authorisation has **not** been revoked.

   Possible reasons
   - The SAM 64 card was removed from the RFID field too early
   - ISO 14443A is not activated in the system
   - If using SAM+ media: there are no credits available
3. Remove the SAM 64 card from the field.

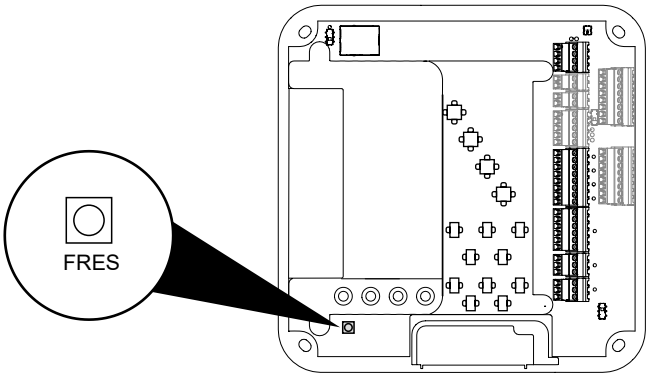
7 Maintenance

7.1 Restart reader

Usage
The device does not respond anymore.

Impact

- The operating system and the application are loaded again.
- The access points remain blocked during the restart.
- The data and the configuration are retained.



The Reset button carries the name 'FRES'.

Procedure	~ Time (s)	Status LED
-	-	Flashing green light
• Press the Reset button and hold it down.	1	Solid yellow light
	2	-
Signaling • Release the Reset button	3	**briefly glows red**
→ The device starts afresh.	-	-
→ The device is ready for operation.	-	Flashing green light

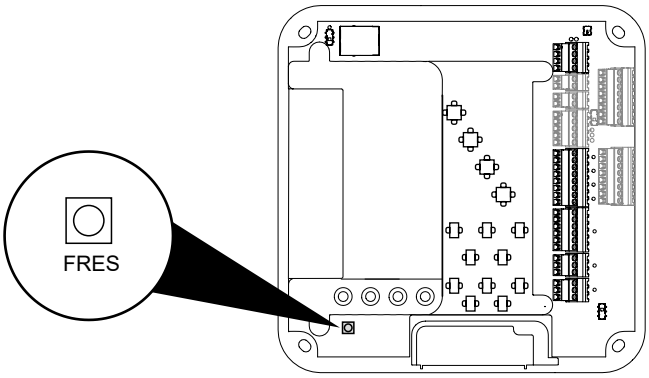
7.2 Reset the device to factory settings

Usage

- The device is decommissioned. (Data protection and IT security)
- Essential modification in the system.

Impact

- The database is deleted. (Access data, events, ...)
- The network settings are reset.
- The configuration is deleted.



The Reset button carries the name 'FRES'.

Procedure	~ Time (s)	Status LED
✓ The power supply is switched off. 1. Press the Reset button.	-	Off
• Keep the Reset button pressed and switch on the power supply.	1	Solid yellow light
	2	Solid red light
	3	Solid yellow light
	4	Solid red light
	5	Solid yellow light
	6	
	7	
	8	
	9	
! Signaling • Release the Reset button	10	**Flashing red**
→ The device is returned to its factory settings.	-	-

8 Decommissioning

Usage

- The device is replaced with another device.
- The device is installed at another location.
- The device is disposed of.

Procedure

- Delete the person-related data.
  - Reset the device to factory settings.
- In the parent system, set the device to inactive or delete.
- Maintain the changes in the system software.
- Switch off the power supply.

8.1 Disassembly

Removing data and extra-low-voltage cables

1. Remove the cable tie at the strain relief.
2. Disconnect the relay outputs from the device.
3. Disconnect the inputs from the device.
4. Disconnect the data lines from the device.
5. Pull the data lines and extra-low-voltage cables from the device.

Removing device from wall

1. Remove the four screws.
2. Remove the device from the wall.

9 Packaging/return

Improperly packed assembly groups and devices may produce extra costs due to damage during transport.

Please observe the following instructions when sending dormakaba products.

dormakaba are not liable for damage to products which are due to inadequate packaging.

9.1 Complete devices

The original packaging is specially made for the device. It provides optimum protection against transport damage.

Always use the original packaging to return the device!

If this is not possible, you must provide packaging which will prevent any damage to the device.

- Use a sturdy, thick-walled transport case or a box. The transport case should be large enough to allow 8–10 cm clearance between the unit and container wall.
- Wrap device in a suitable foil or place in a bag.
- Pad heavily around the device with foam padding or air bags, for example. The device must not be able to move around within the packaging.
- Use dust-free, environmentally friendly fill material.

9.2 Electronic component assemblies

ESD-sensitive electronic component assemblies such as PCBs and readers should be stored, transported and shipped in suitable anti-static packaging. Electronic component assemblies must be packed at ESD-protected workstations. This should be carried out by persons who are familiar with and comply with general ESD protection regulations.

Electronic component assemblies must be returned in packaging with sufficient ESD protection to

- make warranty claims in the event of malfunctions of any type.
- Delivery of replacements for electronic PCBs and components in replacement procedure.

Electronic components shipped in packaging without adequate ESD protection will not be analysed or repaired to maintain a high quality standard; they will be taken directly for disposal instead.

9.3 Labelling

Including all returns paperwork and labelling the package correctly enables us to process your case quickly. Please ensure that a delivery note is enclosed in each package. The delivery note should contain the following information:

- Number of devices or components in each package.
- Article numbers, serial numbers, designations, order number.
- Address of your company/contact person.
- Reason for return, e.g. repair exchange.
- Accurate description of fault.

Returns from countries outside the EU also require a customs invoice with an accurate customs value and customs tariff number.

10 Disposal

The device is indicated with the adjacent symbol which means prohibition of its disposal as household waste.

The device's integral components must be separated before they are taken for recycling or disposal. Old and used devices contain valuable recyclable materials which must be recycled. Toxic and hazardous components may cause long-term damage to the environment if you dispose of them incorrectly.

The facility operators are obliged to return electrical and electronic devices to their manufacturer, point of purchase or designated public collection points at the end of their service life.

Disposal in Germany:
dormakaba EAD GmbH will take responsibility for correct disposal of supplied goods once they are no longer in use as per statutory regulations (ElektroG in Germany). The owner of the used electrical appliance bears any costs incurred for transport to the manufacturer's plant.

Disposal in Switzerland:
The device is to be returned to an electrical appliance return point as per the Regulation on Returning, Taking Back and Disposing of Electrical and Electronic Equipment (VREG).

In the EU, electrical appliances should be taken for disposal in accordance with the country's respective disposal and environmental guidelines.

Deletion of personal data

The owner/operator is responsible for deleting their personal data.

Dispose of packaging in an environmentally responsible fashion.
The packaging materials are recyclable. Do not dispose of packaging in the household waste; take it to a recycling point instead.

Index

A

Access manager 29
Access on Card 8
Ambient conditions 18
Ambient temperature 18
AoC 8, 52
APIPA 8

B

Basic safety instructions 10
Bluetooth 8, 29

C

Cable link 43
Coaxial cable 34
Configuration 49

D

Data on Card 8
Data protection and IT security 15, 55, 56
Dimensions 18
Disposal 59
DoC 8
dormakaba mobile access App 29
DP1 8, 14

E

ESD prevention measures 11
Ethernet 36
Ethernet-LED 23

F

Fastening the cover 44
firmware 30
function type 21

I

Identification label 21
Inductive appliance 43
Ingress protection 18
Installation lines 33
Interference suppression measure 43
iOS 29

K

KCP 8, 14

L

Legic Connect 30, 50
LEGIC Connect 29
Light emitting diodes 23
Locking device 27, 28

M

MAC address 36, 46, 47
Manufacturer 21

N

Network cable 33
network parameters 45
NFC 8, 17, 29

O

Output voltage 23, 43

P

Packaging 57
phgCrypt 14
PoE 16, 36
PoE+ 16, 36
power supply 36
Power-LED 23, 36
Product code 21

R

Registration unit 14, 38
Relative humidity 18
Repeater 27, 28
Reset button 54, 55
Return 57
RFID 8, 17

S

Safety Instructions 10
Scope of delivery 43
Smartphone 29, 50
Status-LED 23

System software 14, 29, 30, 49, 50

T

Tamper switch 25
TP4 8

V

VCP 8
VCP file 50
VCP Installer 29
VCP Installer App 50

W

WEEE guideline 59
Weight 18