Handbuch
Datafox EVO 2.8 Pure

Flexible data collection with method

datafox devices

© 2024 Datafox GmbH

This document has been created by Datafox GmbH and is copyrighted against third parties. Datafox GmbH considers all contained information, knowledge and depictions as its sole property. All rights, including also translation, reprint or copy of the whole document or parts of it, require written consent of Datafox GmbH.
The assertion of all rights in this respect is reserved to Datafox GmbH, especially in case of the grant of a patent. The handover of this documentation does not establish a claim to the license or the use of the soft- and hardware. Copies of the floppy disks and CDs may only be made for the purpose of data backup. Every unauthorized copy of this documentation or the Datafox software will be prosecuted.

Alternations

Alternation in this Dokument

Date	Chapter	Discription
06.08.2017	all	Revision the manual to new version 04.03.10.xx
05.07.2017	all	Revision the manual to new version 04.03.11.xx
15.06.2021	all	Revision the manual to new version 04.03.17.xx
16.04.2024	All	Revision the manual to new version 04.03.21.xx

Alternations of the version

With the device generation IV a new versioning scheme has been introduced. According to this scheme the file name of the device firmware and the setup program (DatafoxStudioIV) is composed as follows:

Product name	XX. Device generation	YY. Compatibility (which versions can be used together)	ZZ. Version number (functional extension)	Build Troubleshooting (with a new version the Build number is reset)
z. B. AE-MasterIV	04.	03.	9.	04

The use of the manual depends on the version of the firmware and the DatafoxStudioIV or the DFComDLL. Gather from the following table which manual matches which version. For different combinations no support can be offered.

Firmware StudioIV and DLL validity

Firmware: 4.03.21.xx.

Studio: 4.03.21.xx

Dll: 4.03.21.xx

The DatafoxStudioIV is backward compatible. This means that you can configure a device with a newer DatafoxStudioIV also older firmware, the device only supports the natural functions that are implemented in the older firmware version. Ie, relevant to the functions that are possible, is always the manual state that the firmware associated with the Setup equivalent. It is not possible to provide a centering firmware configured with a stand of DatafoxStudioIV to who is older than the firmware.

recommendation:

If possible, use always the current version of DatafoxStudioIV.

What features are supported in which software versions, is from the file:

Datafox MasterIV, SW version xxx.pdf list as shown.

The file is located on the Datafox DVD and for download on the homepage. Please also note the instructions in each chapter in the manual. The updates are available on our website under www.datafox.de download.

Inhalt

1.   For your Safety
Safety Information for Datafox Products

The EVO 2.8 Pure must only be operated according to the instructions given in the manual. Do no insert any foreign objects into the openings and ports. The device must not be opened. All maintenance work must only be performed by authorized specialists.

Some devices contain a lithium ion battery or a lithium battery.
Do not throw into fire!

Attention!

Supply voltage: 12 Volt DC
See respective type label / technical data.
The device must only be operated with a power-limited power supply according to EN 60950-1. If you do not observe these instructions, the device may be damaged.
The following temperature ranges must be observed
Working area / storage temperature: -20° C bis +70° C
Mobile communications module: -20° C bis +55° C

In areas with cellphone ban, GPRS, WLAN and other cellular modems must be turned off.
Persons with heart pacemakers:
When using the device, maintain a distance of at least 20 cm between the heart pacemaker and the device in order to avoid possible interferences. Turn the device off immediately if interferences are assumed.

Protection class: Observe the technical data of the respective device. In case of laser devices of class 2, the eye is protected by the blink reflex and/or turning reactions if you briefly and accidentally look into the laser beam. The devices may be used without further protective measures. Nevertheless, avoid looking directly into the laser beam of the laser scanner

Observe the additional notes in the chapter,
"Proper use and environmental protection"

We declare under our sole responsibility that the product described fullfills the protection requirements of European Directive 89/336 / EEC as amended by 91/236 / EEC, 92/31 / EEC, 93/97 / EEC and 93/68 /. See the manual of the devices for the standards. Evidence is provided by compliance with the following standards:EN 55022 : 2010
-    EN 55024 : 2010 + A1 : 2015
-    EN 61000 – 6 – 2: 2005
-    IEC 61000-3-2 : 2014
-    IEC 61000-3-3 : 2013
-    IEC EN 60950-1 : 2006 + A11 : 2009 + A1 : 2010

2. Introduction

Datafox data terminals have been developed to fulfill the requirements of modern personnel time recording where users have high demands concerning flexible and elegant design. Furthermore, the Datafox Embedded-Concept also covers access control. All relevant data can be recorded with modern technology and be transferred to the analysis software immediately. Billings, calculations or other analyses can be performed in a timely manner; processes can be monitored and controlled actively. This saves time and ensures the data quality and immediacy required.
Datafox data terminals are based on the Datafox Embedded-System which is equipped with modern technology for data collection and of course also data transfer. You make your entries comfortably via keyboard, touch display, RFID or barcode. The device is available with fingerprint, GPS, GSM, GPRS, USB etc. It fulfills all conditions for a flexible usage not only for personnel or order time recording but also for further scopes. This constitutes a real added value. The powerful tools Datafox-StudioIV and DLL facilitate quick and easy integration in any IT solutions. Due to scalability, numerous options are available. You can select according to your company's requirements and only pay what you really need.

2.1. Structure of the Documentation

The manual contains a change history as well as a general part with safety information, the introduction and information concerning system requirements and system structure.
The general part is followed by the main part of the manual. It contains the chapter Product Description Device. In this chapter, device-specific components are described as well as the device's functions.
The final part of the manual provides technical data about the device and a glossary whose purpose it is to ensure a consistent understanding between user and manufacturer.

2.2. Guarantee Restriction

All installers are responsible for the use of the device and its accessories in accordance with its intended purpose and in compliance with the applicable laws, standards and directives.
All data in this manual has been checked carefully. Nevertheless, errors cannot be excluded. Therefore, we offer no guarantee nor accept any liability for consequences that derive from errors of this manual. Of course we are grateful if you point out errors to us. We reserve the right to make modifications in respect of technical progress. Our general terms and conditions of business apply.

> **Note:**
> Due to DatafoxStudioIV, Datafox devices offer many functions and combinations of functions not all of which can be tested in the case of updates. This applies especially to setups defined by you as customer. Before updating your device, please ensure by tests that your individual setup works without any errors. If you encounter a problem, please inform us immediately. We will take care of the clarification of the problem on short notice.

2.3. Typography of the Documentation

FW .... Abbreviation for firmware (software in the device)
SW .... Abbreviation for software
HW .... Abbreviation for hardware
GV .... Abbreviation for global variable
<Name;Software Version.pdf> .... File names

> ☞ **Note:**
> Useful information which helps you avoiding possible mistakes during the installation, configuration and commissioning is given here.

> **! !** **Caution:**
> Here, notes are provided which must be strictly observed. Otherwise, malfunctio
> the system will occur.

2.4. Important General Notes

> **!** **Caution:**
> Use the devices only according to regulations and follow the installation, commissioning and operating instructions. Installation and commissioning may only be performed by authorized specialists.

Subject to technical alterations.

> **!** **Caution:**
> Due to technical development, illustrations, function steps, procedures and technical data may vary slightly.

The Datafox device has been developed for the purpose of creating a flexible and easily integrated terminal for data recording serving for a great variety of applications. The device is robust and easy to use. Due to the PC setup program, the device is quickly and easily configured for its application field so that you save time.

Numerous optional features, such as bar code reader, transponder reader, digital inputs etc., enable you to use the device for:

PZE - Personnel time recording
AZE - Order time recording
BDE - Operating data recording (I/O-processing)
ZK - Access control
FZDE - Vehicle data recording / telematics

This manual describes the creation of setups with the setup program DatafoxStudioIV without covering specific applications. Potential problems and difficulties are pointed out.
This manual describes the functionality of the EVO 2.8 Pure and explains its characteristic features. For example, installation, operation and equipment of the device are described.

In order to define the behavior of the device, a setup must be created. For this purpose, the DatafoxStudioIV has been developed.

With some practice it will be possible to create a complete compilation for the EVO 2.8 Pure within half an hour. If you need functions that are not available, please contact us.

> **Note:**
> If you need support for the compilation of setups, we offer you our services. Due to our extensive experience with the setup, we work very quickly and can make your setup even more efficient through useful advices, so that the input at the device can be performed quickly and securely.

> **Note:**
> Due to DatafoxStudioIV, Datafox devices offer many functions and combinations of functions not all of which can be tested in the case of updates. This applies especially to setups defined by you as customer. Before updating your device, please ensure by tests that your individual setup works without any errors. If you still encounter problems after thoroughly testing your setup, please inform us immediately. We will fix the error on short notice.

3. Intended Use and Environmental Protection

3.1. Regulations and Notices

According to the current state of the art, measures were taken to ensure that the device meets the technical and legal regulations as well as safety standards. Nevertheless, malfunctions due to interferences through other devices can still occur.
Please observe local regulations when using the device.

3.2. Power supply

Only operate the device externally with a limited power source in accordance with EN 60950-1.

Connection voltage of the MasterIV devices: 12 to 24 volts DC

If the devices run with rechargeable batteries, note the instructions in chapter "Rechargeable Battery".

> **!** **Caution:**
> In the event of non-compliance with these instructions, the device or the battery (if any) can be damaged or destroyed!

In order to ensure maximum battery life, it is recommended to recharge the battery only after complete discharge.

See respective type label of the device EVO 2.8 Pure.

3.3. Environmental Influences

Extreme environmental influences may damage or destroy the device and should be avoided. This includes fire, extreme sunlight, water, extreme cold and extreme heat.
See respective type label of the device.

3.4. Mounting outdoors

3.4.1. Degree of protection

The terminal device has IP54 on the front side.

The connection area is set up to the top of the apparatus,
so that no water coming from above (e.g., rain) could
penetrate. Only jet water from below would be a problem.
Should additional conditions beyond the normal weather
cause the water to come from below, the terminals can
be sealed to the wall when mounting.
For the EVO terminals it is advisable to mount the units
on the heel of the front shell.
This would sink the entire back of the device with the
connections and in the inaccessible area.
In order to allow such mounting, a mounting surface must
be provided by the customer. For example, In boxes with
front panel.
In the case of bell systems / mailboxes / barriers, mount-
ing plates are usually already available which can be
used for this purpose.
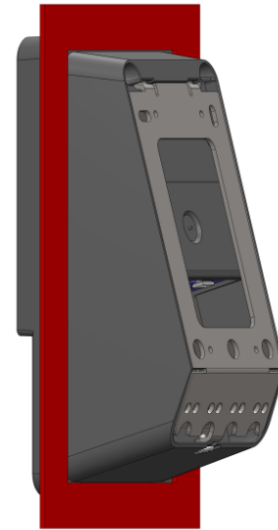
View recessed
Installation in
A front plate /
Mounting plate .

3.5. Temperature

The device has an approved temperature range of - 20 ° C to + 60 ° C.
A heater is not necessary for outdoor use.
Due to the inherent heat of the electronics and power supply, the temperatures in the unit are higher even at ambient temperatures below -20 ° C.
Condensation water only occurs when a cold object comes into the heat and would therefore only be an issue for mobile devices.
We recommend, if you use the devices outside, then let it running permanently. Both in terms of temperature as well as condensation, it is recommended to not switch off devices which are used outdoors.

3.6. Repair

Except for the battery replacement in mobile devices, Datafox devices are maintenance-free and must only be opened by authorized professionals. In case of defects, please contact your dealer or the Datafox service hotline.
If a definite defect is present, you can also send the device directly to Datafox.

https://www.datafox.de/reparaturen.de.html?file=files/Datafox_Devices/PDF/Support/Data-fox%20Reparaturbegleitformular%20V3%2C%20D-GB_2020.09.25.pdf

3.7. Cleaning

Never use scouring milk or caustic cleaning agents to remove dirt. Especially the displays as well as the keyboard and fingerprint modules must be cleaned carefully.
Wet wipes are permitted with:
- Water
- Soapsuds
- Glass cleaner
- Sagrotan
- antifect® N liquid (disinfectant for devices in medical field).

CAUTION
Risk of explosion if batteries are replaced improperly.
Dispose used batteries according to the instructions.

3.8. Further Notices

Do not expose the device to strong magnetic fields, especially during operation.
Operate the slots and connections of the device only with the appropriate intended equipment.
Ensure that the device is secured during transport. For reasons of safety, do not use the device while driving a vehicle. Also ensure that technical equipment of your vehicle is not compromised by the device.
In order to prevent SIM card misuse, have your SIM card blocked immediately in cases of loss or theft of the device.

3.9. Disposal

Observe local regulations concerning the disposal of packaging material, used batteries and scrapped electrical equipment.

This product complies with the EU Directive No. 2002/95/EC, its appendices and the Council Decision laying down the restrictions of the use of hazardous substances in electrical and electronic equipment.

The device is covered by the European Directive on Waste Electrical and Electronic Equipment which came into force on February 13, 2003 and was translated into the legislation of the Federal Republic of Germany on August 18, 2005.
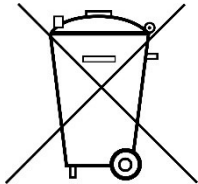
 Do not dispose the device in domestic waste!

As the user, it lies within your responsibility to dispose electrical and electronic equipment via the designated collection facilities. The correct disposal of electrical and electronic equipment protects human life and the environment.

For more information regarding the disposal of electrical and electronic equipment, please contact your local authorities or waste disposal companies.

4. System Requirements / Hardware

4.1. System Structure

The system consists of the Datafox device, the DatafoxStudioIV, the communication DLL and a software for processing the generated data.

Create setup   **Save setup**   **Transfer setup to device**

Software for processing the generated data
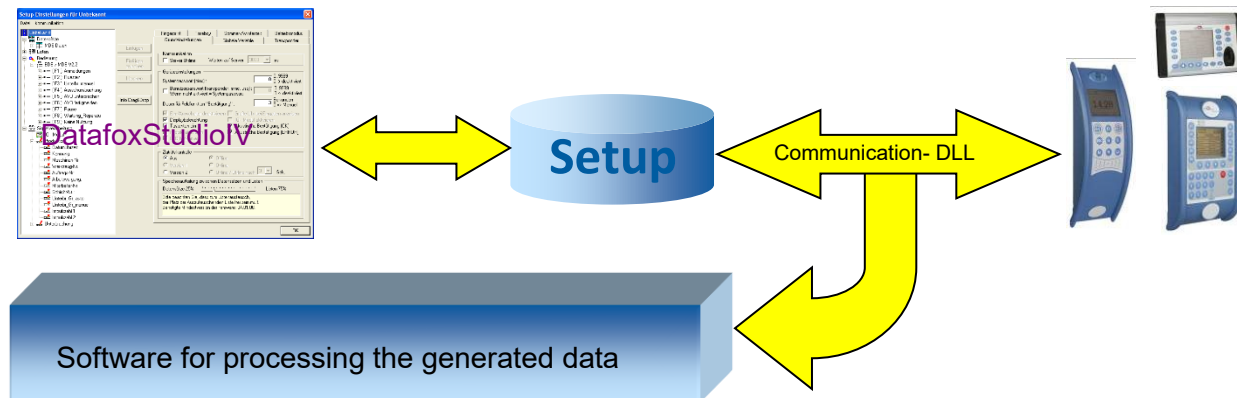
4.2. Installation requirements for Operating Datafox Devices

In order to operate the Datafox device, you need a 230 V power connection for the Datafox power supply. Depending on the main communication set, you need a corresponding transfer medium or connection cable.
Main communication:

- USB → one standard USB-A to USB-micro Cable (see the chapter connection USB).
- RS485 → a transmission path in accordance with the EIA-485 standard (see Connection RS485).
- 2G; 4G→ a distortion-free mobile connection
- WLAN WiFi→ a distortion-free channel to an access point (802.11 b/g/n) within reach (see Connection WLAN).
- at least one standard Ethernet cable, no „cross over" (see Connection TCP)
- HTTP (internet) via LAN → TCP/IP connection with free internet access. The data are sent to a server.

☞ **Note:**
With increasing demands on transfer rate and interference immunity, the demands on the transmission path increase as well with regard to quality (interference immunity).

Ideally, the cables should be provided in a flush-mounted box. Please note this
please provide the height information in the assembly instructions.
Assembly instructions on our homepage:

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/informationsmaterial-evo-serie/11500x_Datafox_EVO_4.3_4.6_7.0_Montage_und_Inbetriebnahme.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/evo-3-5-universal/122001_Datafox_EVO_3.5_Universal_Montage_und_Inbetriebnahme.pdf

https://www.datafox.de/d67/unternehmen/downloads/zubehoer-module/zutrittsleser/12300x_Datafox_EVO_Agera_Montage_und_Inbetriebnahme.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/evo-3-5-pure/1140x1_Datafox_EVO_2.8_3.5_5.0_Pure_Montage_und_Inbetriebnahme.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/kyo-cenloc/124401_Datafox_KYO_Cenloc_Rack_-_TKSS_Montageanleitung.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/kyo-cenloc/124011_Datafox_KYO_Cenloc_Wall_Bohrschablone.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/kyo-inloc/11x402_Datafox_KYO_Inloc_HS_flach_Montageanleitung.pdf

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/pze-master-iv/105406_Datafox_PZEMIV_Wandhalterung_Montageanleitung.pdf

4.3. General Hardware Information

4.3.1. Hardware equipment

The devices with hardware V4 are equipped with a flash memory. Depending on the device type or selected option with 4 or 16 MB.
For the data, the memory is used as a quasi-ring buffer. If the complete ring buffer is written to full without the data being retrieved, the terminal reports "Memory full", please notify the admin". No further data is stored during this time.
Data that has already been read is gradually transferred. The entire memory is always used to minimize the number of accesses per individual memory cell.

An ARM microcontroller with 32-bit technology is used.

Depending on the type of device, the device has a Goldcap capacitor for buffering the time.
This ensures that the watch continues to run correctly for up to one week if the power supply is interrupted.

In other devices, such as EVO 4.3 or PZE-Master V4, a buffer battery is installed in addition to the capacitor. With this, the watch retains its value for approx. 4 years.
The exact equipment can be found in the last chapter Technical Data.

4.3.2. Behavior in case of power failure

The device boots automatically when the power supply is switched on again.
All data that was not sent or retrieved by the application software before the power failure is stored on the device.
These are not lost. After booting, this data is available again.

4.3.3. UPS

A corresponding UPS for the V4 hardware is in preparation.
We currently recommend equipping the devices with a POE module if a "UPS" is to be used. Then connect the devices via a POE switch and supply the switch via a standard UPS.

4.4. Compatibility

The compatibility must be observed urgently between:
- Datafox devices and the device firmware
- Device firmware and device setup
- Device firmware and communication DLL
- Communication DLL and DatafoxStudioIV
- DatafoxStudioIV and device setup

4.4.1. Firmware File Archive (*.dfz)

Description

The Firmware archive combines device specific firmware files into an archive container. This archive uses the file extension DFZ (abbreviation for Datafox Zip). When uploading firmware to a device through DatafoxSudioIV of the DFCom library, simply use this archive.

> ☞ **Note:**
> The firmware archive does not only contain software for the current device generation (HardwareIV), it contains software for previous hardware versions as well You can update any Datafox device using this archive and upload the current version of the device firmware in this way..

Function of the Archive

The transfer routine of the device file selects the right file from the firmware file archive on the basis of the hardware options available in the device. Thus, it is guaranteed that all hardware components available in the device are supported by the corresponding firmware.

4.4.2. Datafox Devices and Device Firmware

Each Datafox device has an electronic flat module. The module has specific hardware equipment concerning the options (e.g. mobile radio, WLAN, fingerprint, ...). Due to technical conditions, different options are mutually exclusive. Currently there are conditions where not all hardware options can be supported in one firmware file due to limited program memory. This means that each device with specific hardware options needs a proper firmware to support the hardware options by the software.

> **!** **Caution:**
> In general, the newest version of DatafoxSudioIV should be used, since this version is capable to support the current device hardware version. Should you opt for using an older version of DatafoxStudioIV, please keep the following minimal version requirements in mind:
> - DatafoxStudioIV Version 04.03.00.x or newer is offering support for Hardware Generation IV and III
> - DatafoxStudioIV Version 04.02.00.x or newer is offering support for Hardware Generation III

4.4.3. Device Firmware and Device Setup

The firmware (operating system) of the device and the device setup (*.aes data file = application program) form a unit. By the device setup, the runtime behavior of the device (the firmware) is determined. This means the response of the device to input events by the user or the environment (e.g. digital inputs). In principle, only those functions of the device are executed that are supported by the firmware and defined via the setup. Prior to the productive commencement, you should therefore test each setup with the corresponding device or on a device with the same hardware options and firmware.

4.4.4. Device Firmware and Communication DLL

A firmware supports certain functions, dependent on the hardware options. The communication DLL is the interface between the firmware and the DatafoxStudioIV or your processing software. Therefore, the firmware must always have the same or a lower version number as the communication DLL.

> ☞ **Note:**
> If your application uses a newer version of the communication DLL than the firmware does, you can only use functions that are supported by the firmware.
> Otherwise, you will receive an error message (e.g. function not supported) which has to be analyzed.

4.4.5. Communications DLL and DatafoxStudioIV

> ☞ **Note:**
> The DatafoxStudioIV and the communication DLL are developed and released as a bundle. Therefore, they have to be used as a bundle.
> A newer version of DatafoxStudioIV does not work with an older DLL.

4.4.6. DatafoxStudioIV and Device Setup

With the DatafoxStudioIV, you create a device setup (application program) for the Datafox device. That means that in the setup only those functions were defined which were available in the DatafoxStudioIV version at the time of the setup creation. The DatafoxStudioIV you use for opening a device setup may thus only be newer but never older than the DatafoxStudioIV version you used to create the device setup.

> ☞ **Note:**
> The updates are always available for download on our homepage www.datafox.de.

> **!** **Caution:**
> When new devices are delivered, the latest firmware is loaded on the devices. If you wish to work with an older firmware version, please perform a downgrade. Please observe the compatibility notes in the release notes of the respective firmware version.

The data file <Device name>, Software version <version number>.pdf shows which functions are supported by which software release.
You will find the file on the product CD. Please also follow the instructions given in the chapters of the manual.

4.4.7. Update / Downgrade

A firmware update or downgrade is a very sensitive process. Possibly, a reset of the main communication to RS232 may occur. In any case, consider the information regarding the compatibility in the software version list.

Firmware Update

> **!** **Caution:**
> Before starting a firmware update, please check on the basis of the software version list whether there are any version dependencies that must be observed.

For example: when changing from Version 04.00.xx to version 04.01.xx, at least version 04.00.23.769 or higher must be present in order to run the update to version 04.01.xx successfully.

Firmware Downgrade

A firmware downgrade is not recommended.
We are constantly working towards improving the software/firmware; all functionalities are still included in new versions. New software always offers better functionalities and possible bugs are fixed.

> **!** **Caution:**
> When performing a firmware downgrade the firmware has to be transmitted to the device twice. This has technical reasons. Errors shown on the display of the device after the first transfer can be ignored.

5. Device

> **Note:**
> It is necessary to ensure suitable protection from direct sunlight as synthetic materials are not 100% UV resistant. Fading is simply an optical defect that does not compromise the functionality of the device.

> **!** **Caution:**
> Please keep in mind that MasterIV terminals use a flash memory. According to the manufacturer, each memory sector (512 byte) can be written to a maximum of 100,000 times. The firmware of the terminals distributes the access to the memory sectors, this technique is called wear levelling. Bad blocks in case of write or read failures are not used anymore. However, despite this technique, it is not advisable to write the memory too frequently. The application should initialize a new list transfer only after a change of the list data but not cyclically.
>
> Keep in mind the message - FlashService - in the display of the device. It means that the live time of the flash memory according to the manufacturer instruction will be reached soon. Then the device has to be sent to Datafox for service.

5.1. Commissioning

On delivery, the device is fully functional and configured with a demo setup so that you can test the input immediately. After establishing the power supply the device will switch on automatically. The EVO 2.8 Pure automatically starts booting, recognition of the hardware options and loading the setup. After having finished booting, the device switches to operation. Now itEVO 2.8 Pure is ready for use.

> **Note:**
> On delivery, the main communication is set to TCP/IP and on DHCP.
> If TCPI/IP not on bord, then is the main communication set to USB.

> **!** **Caution:**
> If external modules (e.g. access control, signal processing via the digital inputs) with an external power supply are used, ensure to comply with all limits (max. voltage and current) before commissioning the system.

5.2. Operation and display elements of the Evo 2.8

The terminal works with a resistive touch display.
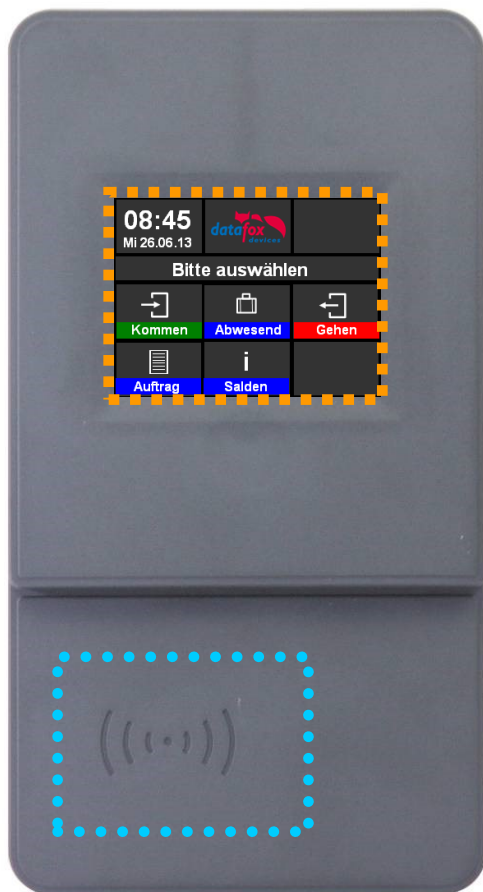
display and touch area

Reading range of the transponder

5.2.1. Display and Bios of the EVO-Line 2.8 Pure

5.2.1.1. Structure of normal display

The entire display area is equipped with a touch screen. Simply tap the tile you want with your finger to select.

Date Time tile	Tile for company logo and status indicator The logo can be load to the terminal via Datafox StudioIV under the Configuration → Display-Designer tab.

Tile for „ESC" if neccessary

Texts according to setup (header line 2)
Name of EK and Name des Eingabefeldes.

Function keys according to Setup
(up to 6 pcs.)
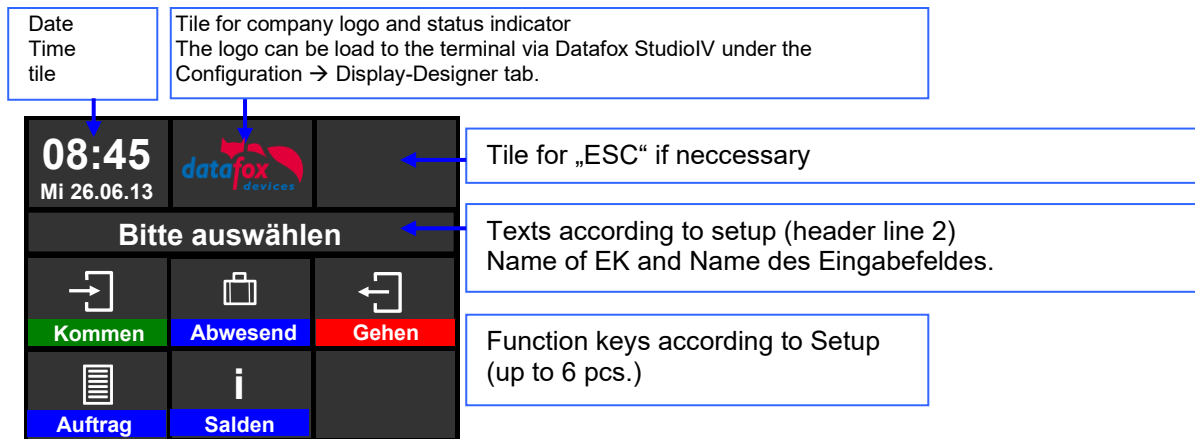
- **Date Time** corresponds to the system time of the device, which is also used for the data records.
- ▢ **Number of records** in memory (display up to 99, then 99+).
- **Communication** field with symbols for:
  - TCP IP TCP /IP When this communication is active, this symbol is displayed. TCP IP ⬇⬆.
  - Wlan communication
    - ⬝ WLAN as main communication
    - 📶 Wlan connected
    - 📶 ⬇⬆ Wlan Communication is currently active
    - ▾ ⬝⬝ 📶 📶 📶 signal strength wifi
  - ⬝ USB
  - ⬝ USB Host (Save the data to USB stick)
  - rs 485 RS 485
  - GPRS With status display e.g.[33] See "Status messages on the display".
    - ⬝ Mobile modem is off
    - ⬝ Mobile modem is switched on, but no connection to the provider.
    - ⬝ Mobile modem is switched on, connection to the provider exists.
  - Mobilfunk (BG-96 und EG-95), status display e.g.[33]] See "Status messages on the display".
    - OFF Mobile modem is off
    - X Mobile modem is on, but no connection to the provider.
    - E Mobile modem is on, edge connection to the provider.
    - 3G , H , H+ , Mobile modem is on, 3G connection to the provider..
    - LTE , MI , NBI , Mobile modem is on, LTE connection to the provider.

- **Display on the display**
  - The header lines 1 and 2 of the setup are displayed in the main menu.
  - The header lines 3 and 4 stored in the setup are displayed in menus and input chains.
  - During the transmission of a setup or firmware update, the device enters the system stop and displays this symbol „⚒ Systemstop" in this window.
  - Display in the left part of the window:
    - ⬝= Transponder input (Accept value of transponder)
    - ⬝= Check in (coming) - booking
    - ⬝= check out (going) - booking

5.2.1.2. Structure of display EVO 2.8 Pure in the Bios menu

The Bios menu can be accessed by pressing the tile for company logo/status for 2 seconds.
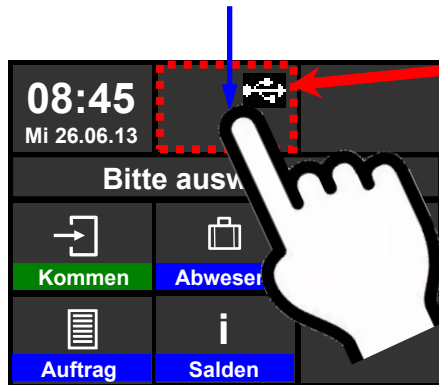
Display of status icons:

Briefly tap the logo to display the status incobs. You can also change the display of the icons in the user settings:
- Constantly instead oft he logo
- Constantly in the „ESC" tile
- For 60 seconds instead oft he logo
- off

Is there a BIOS-password, this can be typed here.
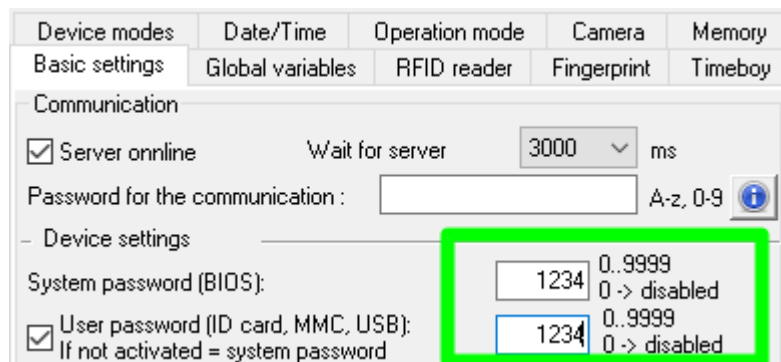
Display in BIOS menu:

To select the respective menus, simply tap on them with your finger.

General information:

- Firmware Info
- Last message / No message available
- Transponder test
- Memory usage
- signal strength
- Provider
- Data memory   3068kB
- List memory   1028kB

The respective submenus should be self-explanatory. The respective display depends on the hardware configuration.

System menu BIOS:

08:45		ESC
▶ Systemmenü Bios		
Firmwareinfo	∧	
Systeminfo		
Kommunikation	∨	
Anzeige/Signallautstärke		

The respective submenus should be self-explanatory. The respective display depends on the hardware configuration.

Set communication:

08:45		ESC
▶ Kommunikation		
Interface LAN	∧	
active-mode nein		
http-mode nein	∨	
lanparameters		

Select the interface for the communication.

Parameter for active connection   (Standard = no)

Parameter for http   (Standard = no)

Settings for TCP/IP Parameter (IP-adress)

TCP / IP / DHCP **- settings:**

08:45		ESC
▶ lan parameters		
MAC E4:F7:A1:00:01:0C	∧	
DHCP no		
IP 192.123.123.155	∨	
Netmask 255.255.255.000		

If the device is set to DHCP (yes), you can no longer change the IP address manually. However, the IP assigned by the server is displayed.

TCP / IP – settings:

08:45		
▶ lan parameters		
Gateway 192.123.123.1	∧	
Port 8000		
	∨	

Set IP:

IP			ESC
192.123.123.155			
1	2	3	0
4	5	6	←
7	8	9	↵

Transponder menu

The settings existing in the transponder menu can also be set to Setup.

name	meaning
Type	Type of the transponder reader
Version	Version oft he transponder reader
Write ID card	Beginn with Writing
Inkrement	Autoinkrement
Segment4 => 1001	Beginn in segment 4 with the set value.

Some settings for writing the ID cards have to be customized in the setup.

Name	Meaning
Transponder type	The correct type of transponder must be specified here.
Segment No.	In which segment the write/read is to be done
Start value	Defines the start value of the number to be programmed.
Autoinkrement	If activated, the programming value always increments the corresponding number.
Password	The password to read/write the badges.

☞ **Hint:**
If badges are to be written with a password, the password must first be programmed to this password.

❗ **Attention:**
A programmable transponder type and a programmable segment must be set in the setup. E.g:
- Hitag 2   -> from Segment 4
- Mifare Classic -> from Sector 0 block 1

Otherwise, only the type and version of the transponder reader is shown.

Buzzer volume:

08:45 07.03.14		↵
Piezo-Hupe		
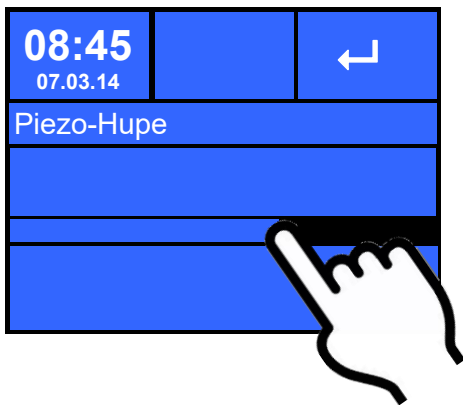
You will find this menu under
"User Preferences" -> "Display/Signal Volume".
Piezo horn" -> "Piezo horn".
Simply tap on the bar in the middle to change the volume.

Touch kalibration:

08:45		
▶ Touchkalibrierung		
Kalibrieren		
Test		

You will find this menu under
„User Preferences" -> „Display/Signal Volume".

+		+
▶ Touchkalibrierung		
+		+
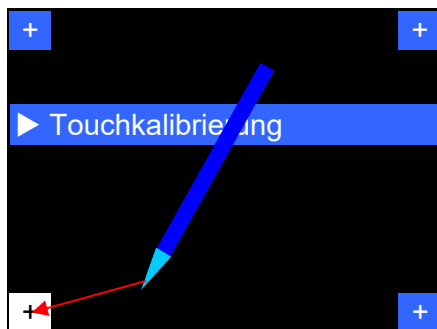
1.) Tap on the touch surface with a stylus
The corresponding cross switches the color.

2.) Now move the stylus as close as possible to the cross.

3.) The respective corner is only calibrated when you release it.
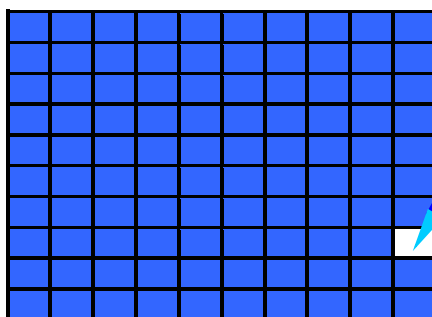
To test the touch, simply move the stylus over the display. The respective tile must then change colour to white.

If no operation is performed for 7 seconds, the calibration test is automatically terminated.

5.2.1.3. Bios Menu Setting WLAN

As of firmware 04.03.11, you have the option of changing the settings for the WLAN connection not only with the DatafoxStudioIV, but also directly at the device.

You may edit the individual configurations in the bios menu "WLAN parameters".
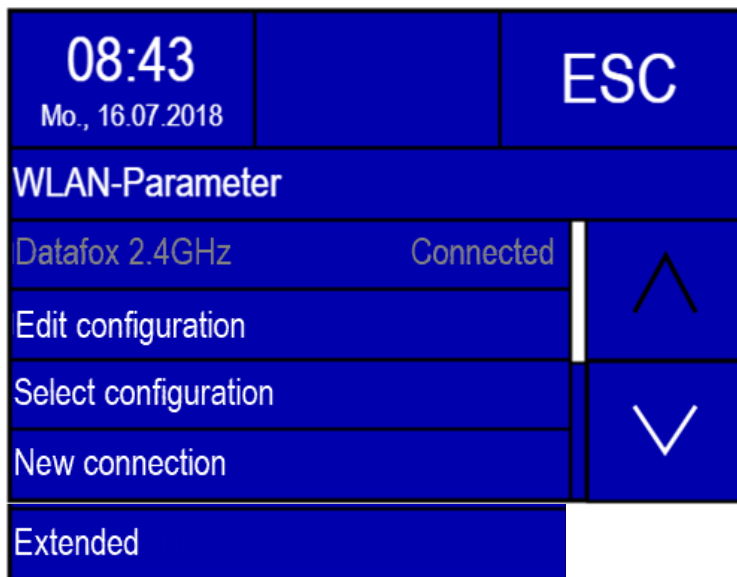
Here you can see which configuration the device is currently using to connect.
Here in the example:
„Datafox 2.4GHz"

Edit Config:
Next, you can edit the currently loaded configuration in the menu item "Config. Edit" The options that can be set correspond to the network configuration section in the Studio. It is possible to switch between DHCP and static IP address and to adjust the port. In addition, there is the option to define a configuration as the default. This is selected if the automatic selection of the configuration is switched off.

> **!** **Attention:**
> This function is only supported on EVO 2.8 Pure, 3.5 Pure, 3.5 Universal and 4.3.

If changes have been made, you will be asked whether they should be saved when you exit the menu. Yes → saves the changes and exits the menu. No → exits the menu without saving the changes. By pressing ESC, you will find yourself back in the change menu and can view the changes you have made again.

Change Config.

In the menu item "Config. Switch" you can switch between configurations. Furthermore, the automatic selection of the configuration can be set here. If a network is selected here that can also establish a connection to an access point, it is not guaranteed that this network will be selected again when leaving the BIOS menu. If automatic selection of the configuration is activated, the network with the best reception quality is selected. However, if you want to connect to a specific network, this must be set as the default and the automatic configuration selection needs to be switched off.

08:43 Mo., 16.07.2018	ESC
WLAN-Parameter	
Datafox 2.4 GHz connected	∧
Edit configuration	
Select configuration	∨
New Connection	

08:43 Mo., 16.07.2018	ESC
Select configuration	
Auto config selection no	∧
*Datafox 2.4GHz -27dbm	
WIFI sales -57dbm	∨
WIFI development -61dbm	

08:43 Mo., 16.07.2018	ESC
Select configuration	
AndriodAP -66dbm	∧
WIFI manufacturing -90dbm	
	∨

New Connection

When this menu item is selected, a network scan is carried out. Afterwards, one of the networks can be selected from the list. A key is then entered (Figure 4). An attempt is then made to establish a connection with the network. The result of the connection is displayed on the screen (figure 5). If a connection could be established, a storage location is selected in the next dialogue. The configuration is then saved. If desired, the new configuration can be used directly as the standard (figure 6). In addition, it is possible to enter the SSID manually. In this way, networks that are not within range or do not transmit the SSID can be added.

!	**Attention:** Currently, however, only the connection to WPA2 networks is supported when entering with SSID.

08:43 Mo., 16.07.2018	ESC
WLAN-Parameter	
Datafox 2.4GHz Connected	∧
Edit configuration	
Select configuration	∨
New connection	

08:43 Mo., 16.07.2018	ESC
New connection	
Please Wait ... **Searching WIFI Networks**	

08:43 Mo., 16.07.2018	ESC
New connection	
Datafox 2.4GHz -25dbm	∧
?WIFI sales -60dbm	
?WIFI development -72dbm	∨
Add network	

Enter SSID			
shift	abc	def	ESC
ghi	jkl	mno	←
pqrs	tuv	wxyz	
123	⎵	äöüß	↵
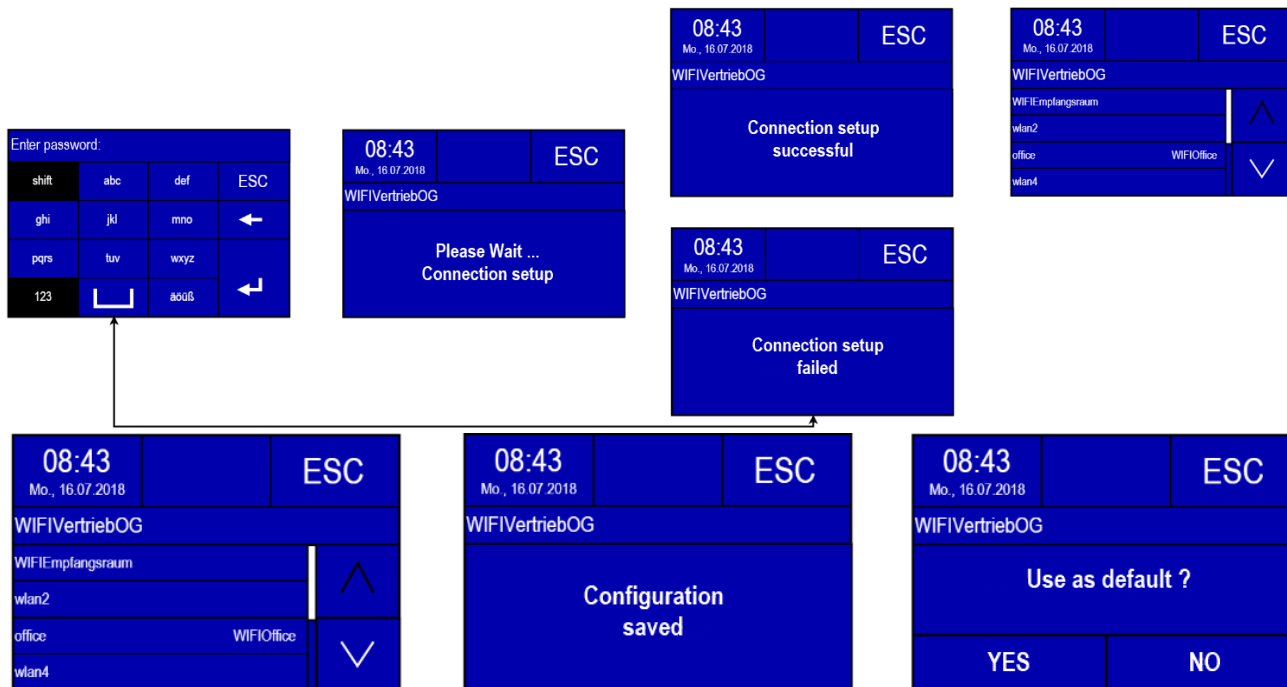
System Info/Advanced

In the menu item System Info/Advanced, information about the WLAN hardware can be requested. This includes the current IP address, the MAC address of the WLAN chip and the firmware of the WLAN module. The number of configurations currently in use is indicated in Saved networks. By selecting the item Reset configurations, all configurations can be deleted. The configurations then correspond to a new, still unfilled LAN and WLAN configuration. More information on the current communication parameters can be found in the user settings.
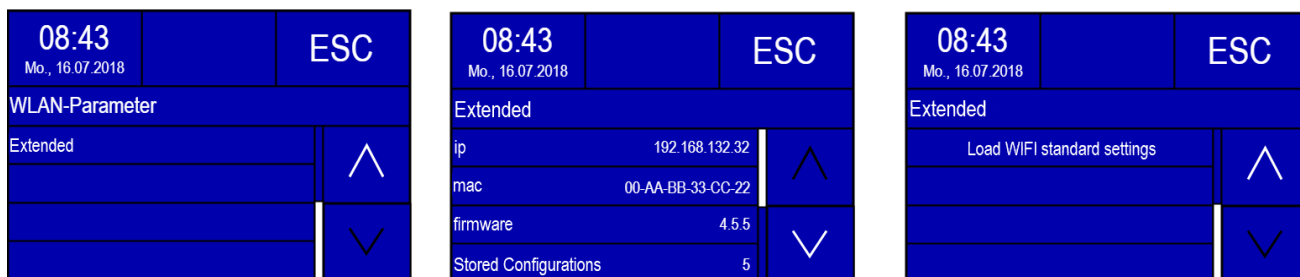
Keyboard Entry

👉 **Note:**
The input of the SSID and the key are limited to 32 characters. Values of the "Latin1" character set are permitted as input, with the exception of the control characters.

5.2.1.4.   Setting of the Proximity- & ambient Light-Sensor

The following parameters of the proximity and ambient light sensor can be controlled:
- "Proximity sensor" on / off switches;
- "Sensitivity" of the proximity sensor from 0% (~ 0.5Meter) to 100% (~ 1.2Meter);
- "display off after" the last detection of the proximity sensor (from 10 to 65534 sec.);
- "ambient light sensor" on / off.

Bios menu:
The menu for the Proximity sensor you find here:
-Bios menu -> usersetting-> display /signals-> Proximity- & ambient Light-Sensor
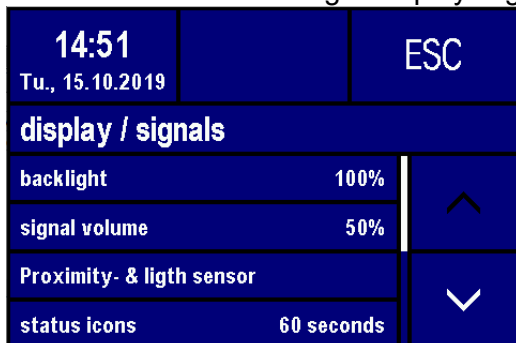
Is the Sensor activated, have you this display:

no motion detected!

motion detected!
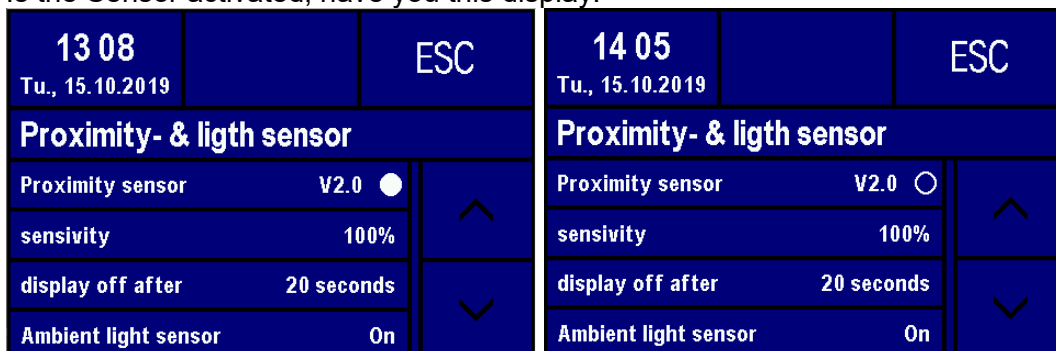
Sensor is deactivated:
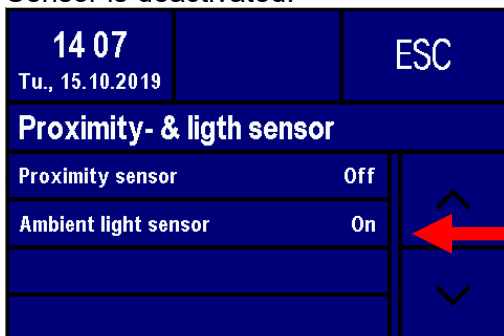
The ambient light sensor set automatically the brightness of the display.

Information's: Proximity- & ambient Light -Sensor

When a Datafox terminal is not in use, it should be in a low power mode. Display and backlights should be off or only slightly active. This is to save energy, in addition, the life of LED or display back lights is also significantly extended.

The Proximity Sensor is a sensor capable of detecting nearby objects without physical contact. A proximity sensor emits an infra-red beam and receives the reflected beam. The reception area looks something like this:
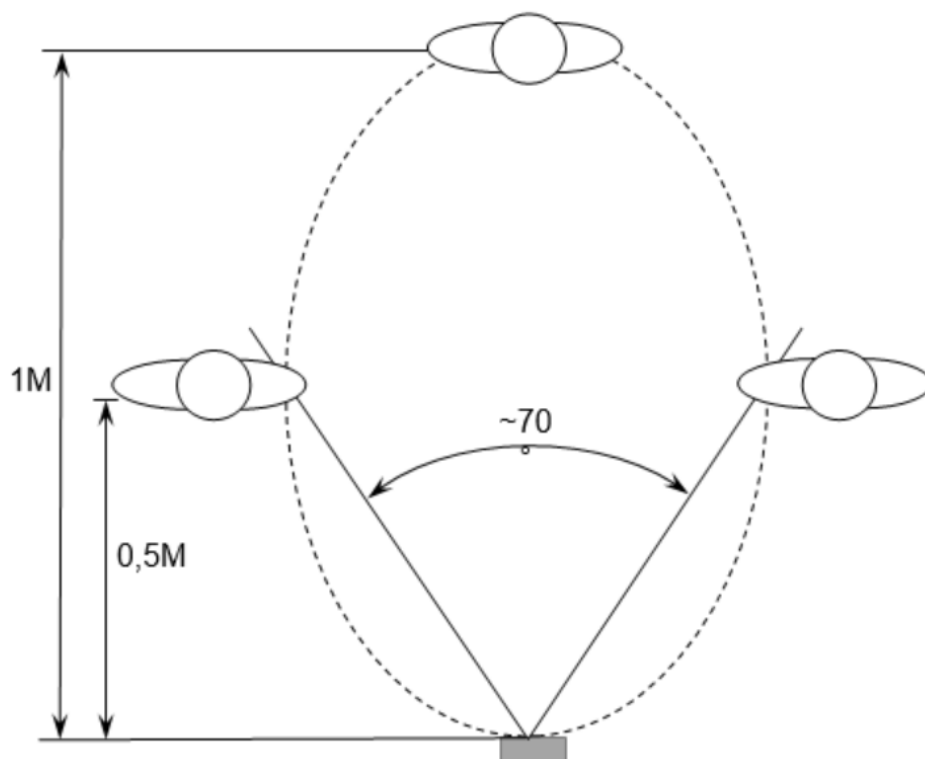
The detection distance (sensitivity) is quite dependent on the area and the re-inflecting properties of the object. That is, the larger the reflective surface, the greater the detection distance. White Fabrice reflect better than dark Fabrice.

Due to the automatic sensitivity settings, the objects in the vicinity of the device, as well as solar radiation and strong electromagnetic interference can reduce the sensitivity.
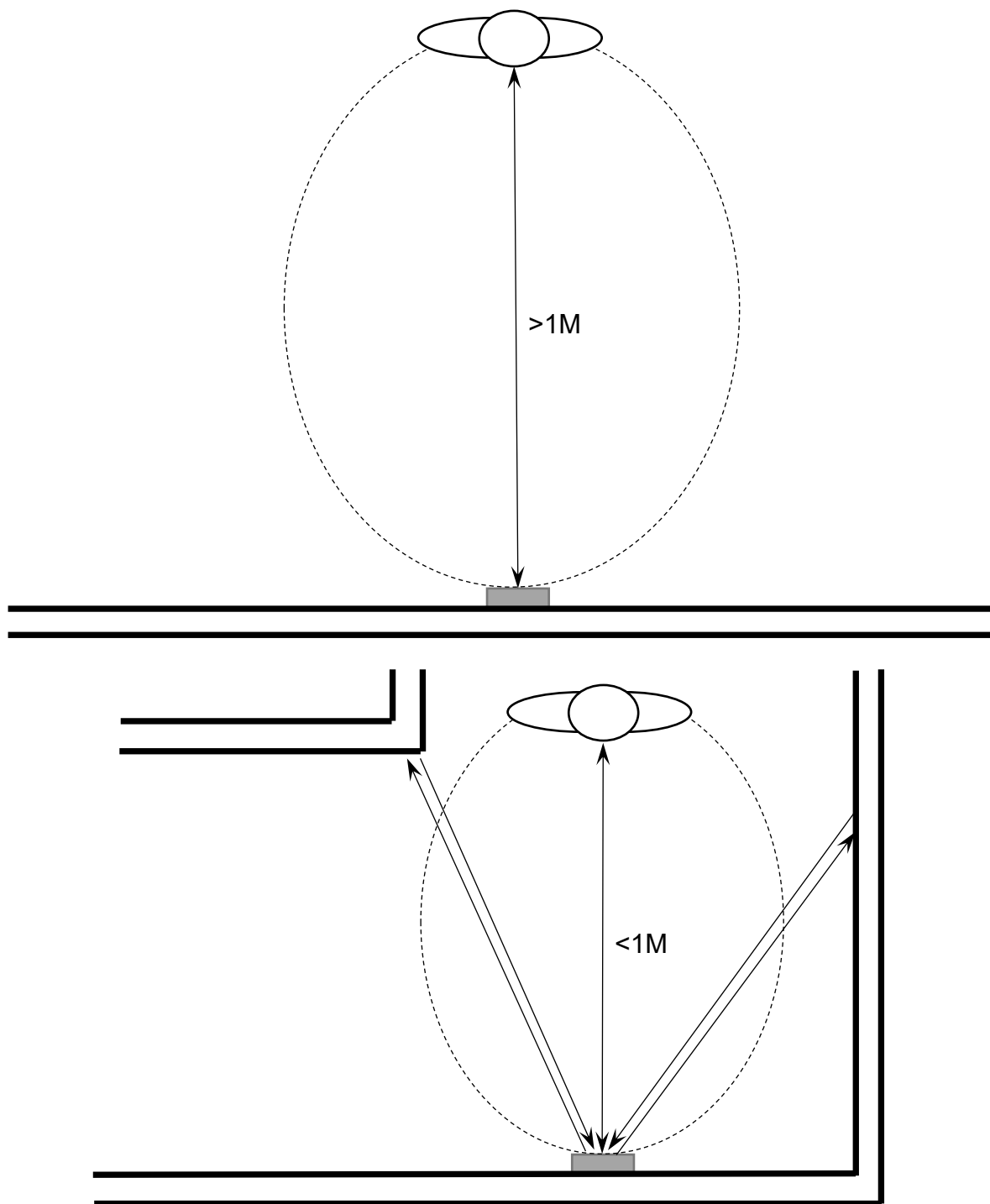
The ambient light sensor controls the brightness of the display independently of the proximity sensor. In bright ambient light, the backlight is operated at the set brightness. In darker surroundings, the value is automatically reduced to 10%.

5.2.2. Displaydesigner

scope of application:

			4.3/4.6	2.8/3.5	5.0	Uni-versal	Agera ZK	Inloc	Mobil Box	IO-Box	Oneloc			EVO-PC
☒	☒	☒	☒	☒	☒	☒	☒							

For the devices AE-MasterIV V4, PZE-MasterIV V4 and PZE-MasterIV Basic V4 is the Designer only usable for color display.

With the Display-Designer, Datafox offers the possibility for partners and users to customize the display according to your requirements. But due to the necessary operating sequences, this cannot be a completely free design, but things like headlines, menu structures and footers have to be guaranteed. The aim of the display designer is to enable the feasible settings with minimal effort.

Create an individual Display-Design for your Company:

Example picture for EVO 4.3 and 4.6 FlexKey
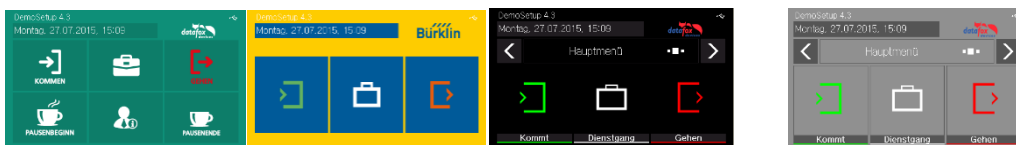
Example picture for EVO 2.8 / 3.5

Example picture for PZE-/ AE- Master V4 with color display

To create an individual ad for your device, you need at least that DatafoxStudioIV 04.03.09.05.

The display designer can be open via the Configuration menu or directly from the setup edit mask.
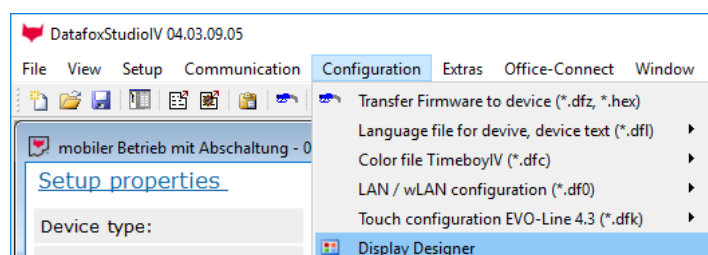
5.2.2.1. Color Setting for the Display
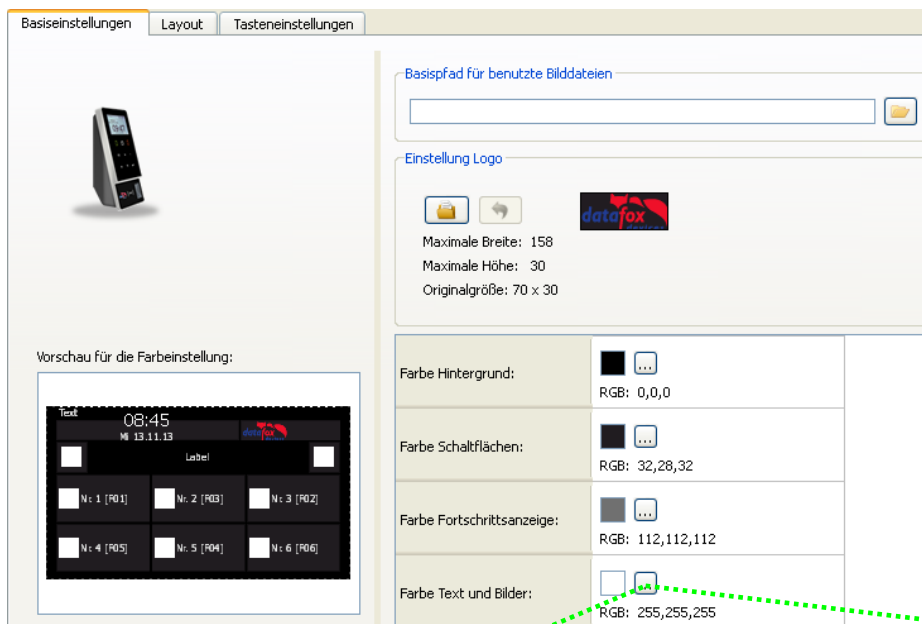
Example Picture:
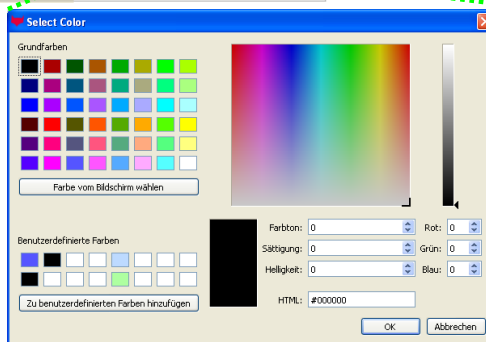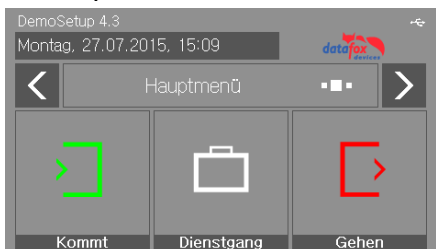
5.2.2.2. Default Setting

The device is delivery in the default „PZE"-design.

This design is also set as default when you first create a new theme in Display Designer.

Function Key's are not displayed in the default setting.
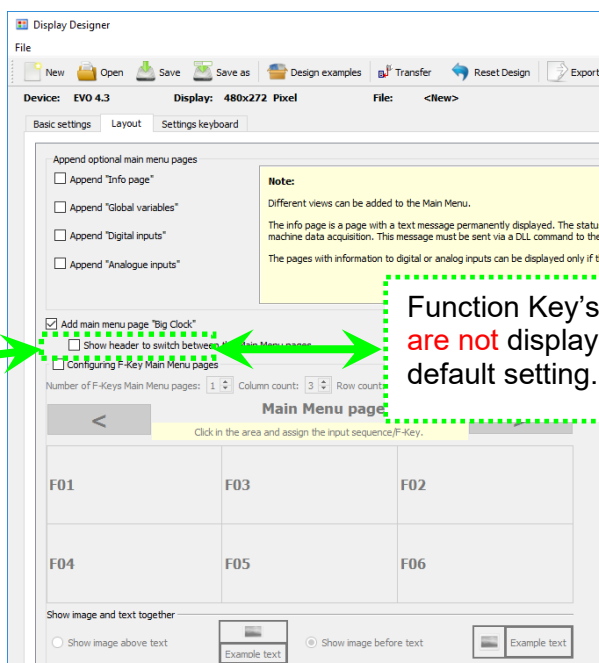
5.2.2.3. Display function buttons on the EVO 4.3 / 4.6 / 2.8 / 3.5 /5.0 display

By showing the function buttons from the setup, the number of buttons displayed in the display can be adjusted.
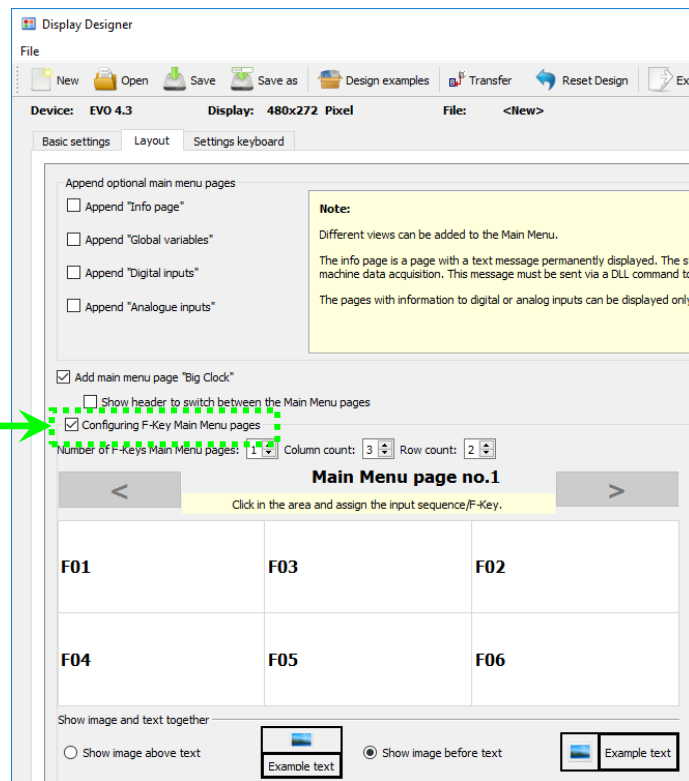
Example:
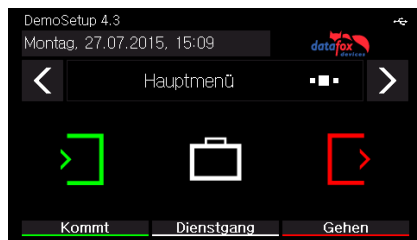
5.2.2.4. Upload images for function buttons of EVO 4.3 / 4.6 / 2.8 / 3.5 /5.0

Under this menu item "Key settings" you can import the image file for each function key.

Sample picture for the key figures:
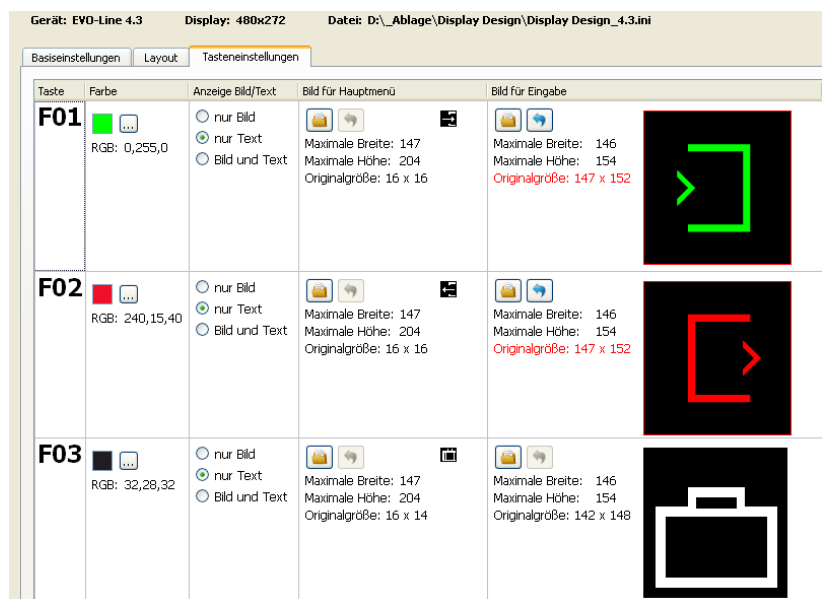
5.2.2.5. Transfer additional images

Additional images can also be stored on the terminal. These can either be displayed during data storage, in input fields, as a keyboard layout or in the fingerprint menu. In this way, your terminal can be adapted and individualized even better to your requirements and areas of application.

5.2.2.6. Picture for the Fingerprint Menu

Terminals with a fingerprint area sensor have a separate menu for teaching, training and deleting the fingerprint templates. In the menu item "Check" you can put your finger on the sensor and a picture of the fingerprint will be displayed. This allows you to check the position of the finger on the sensor and the contact pressure.

In order to clarify the correct position and the correct pressure again, a picture can be displayed for comparison. This can be selected here if it deviates from the standard.
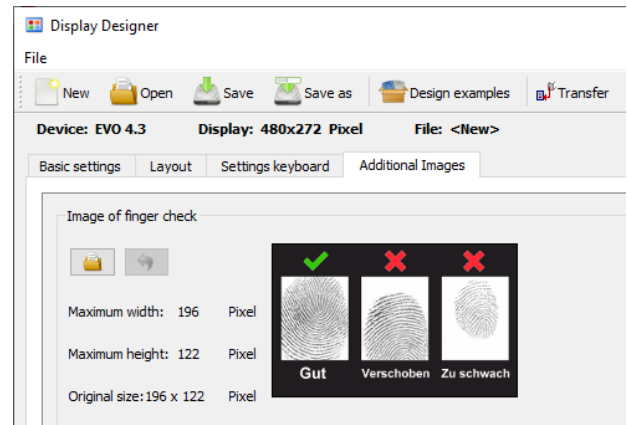
5.2.2.7. Picture for save record message

The three confirmation messages after completion and storage of a Record can Now be shown with a Graphic.

The graphics to be seen are standard and are instead of the messages shown on the display of the terminal.

If you want to set your own pictures for these messages, they have to be set and transmitted once.

The file names must follow name restrictions as followed:
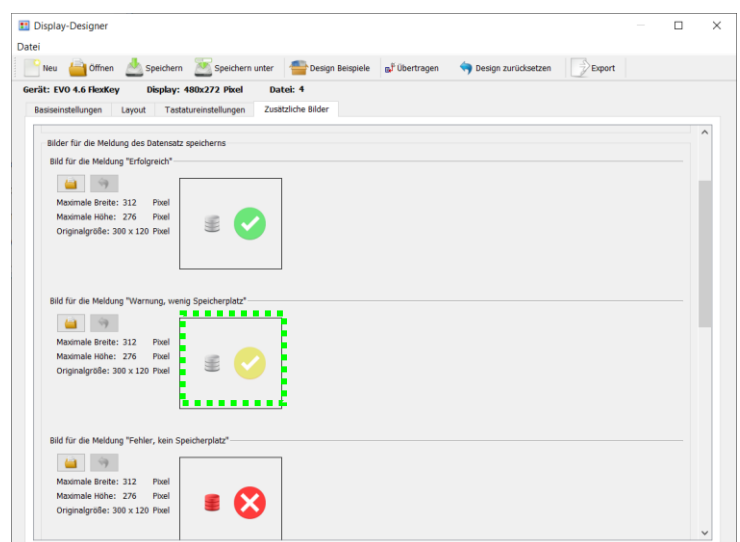
filename - Data storage successful:	*save_ok.bmp*
filename - Data storage almost full:	*save_warning.bmp*
filename - Data store full! Notify admin:	*save_error.bmp*
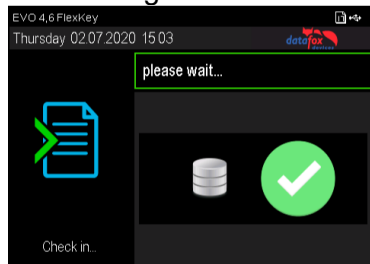
Data storage successful !   Data storage almost full
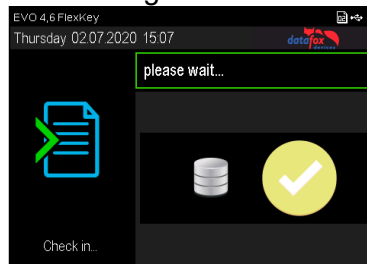
Data store full!
Notify admin !
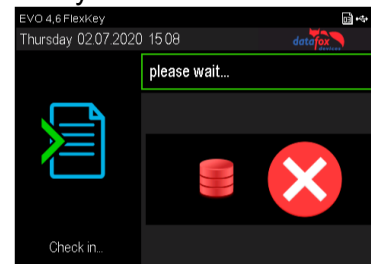
Note:

The graphics do not have to be activated separately, i.e. it is sufficient to transfer them to the device. As soon as one of the graphics is available, it is always displayed instead of the text.

This option is available for all terminals with colour display:

			4.3/4.6	2.8/3.5	5.0	Uni-versal	Agera ZK	Inloc	Mobil Box	IO-Box	Oneloc			EVO-PC
☒	☒	☒	☒	☒	☒	☒	☒							

5.2.2.8. Image display in the main menu

In the main menu of the terminal, you can now choose a graphic instead of the "big clock", global variables, etc.
This can include information such as the appointment for the next company party or the current canteen meal plan.

File name: *main.bmp*
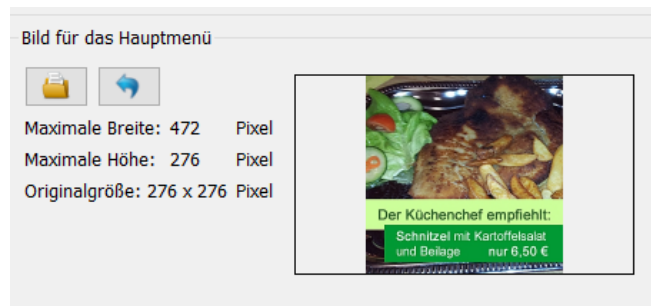
Note:

To activate the graphic, it is sufficient to transfer it to the device. I.e. as soon as it is available in the device, it is displayed preferentially when changing to the main menu. The other main menu pages activated in the display designer can still be reached by swiping.

5.2.2.9.   Keyboard graphics a. touch config. for the EVO 4.6 FlexKey and 5.0 Pure

The representation of the touch buttons
(Keyboard area) of the EVO 4.6
unlike the EVO 4.3,
not by a printed layout of
the glass front, but as a graphic file,
which is shown on the display.
This is individually changeable and
customizable as needed.
This keyboard graphic and the
associated touch configuration
can be edited in the menu
"Image for the key area" on the
EVO 4.6.
The following apply to the graphic
restrictions:
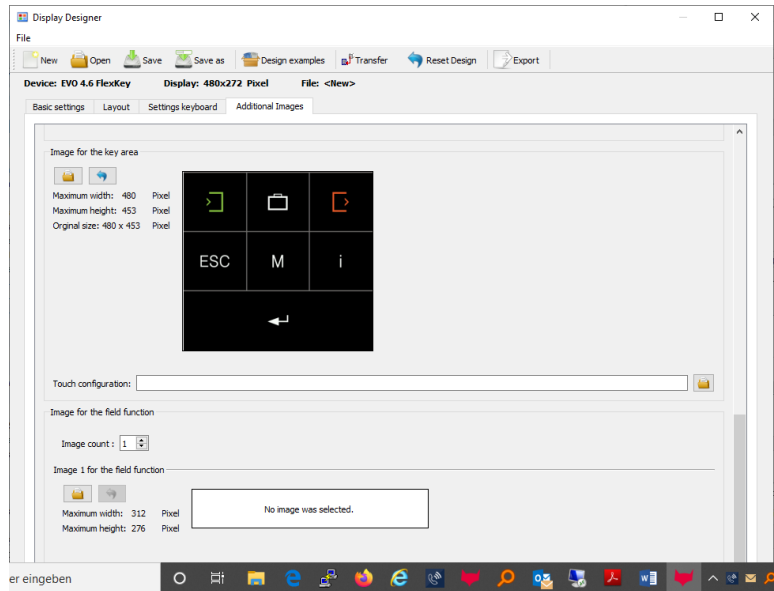
width: up to 480 pixels
height: up to 453 pixels
filename: *touch_buttons.bmp*

☞ **Note:**
After the graphic has been transferred to the device, it is displayed immediately.
This also applies when replacing an existing keyboard graphic.

The associated touch file can be created as usual in the DatafoxStudioIV for the respective key-board layout. See chapter "Configuration of touch data".
This can be selected directly for the corresponding keyboard image and transferred together with the display design.

Example picture for the touch:
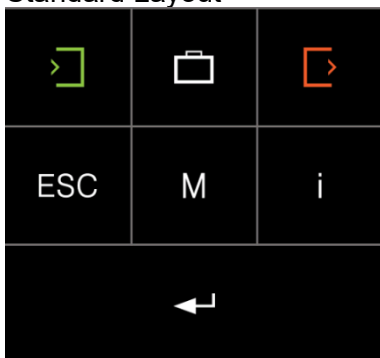
Standard Layout   Layout with fox-design white   Layout with fox-design black
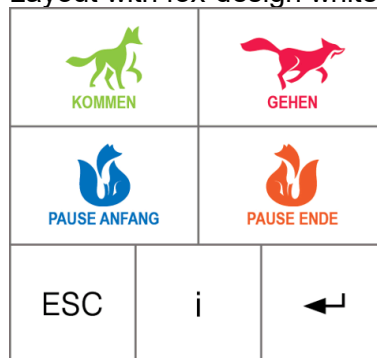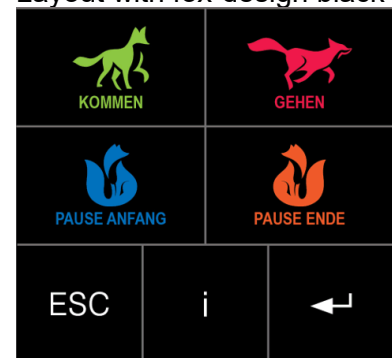
You fount the Immage for the touch in the installation of the DatafoStudioIV:
Here the standard installation path:
C:\Program Files (x86)\Datafox\data\touch\EVO_5_0
C:\Program Files (x86)\Datafox\data\touch\EVO_4_6
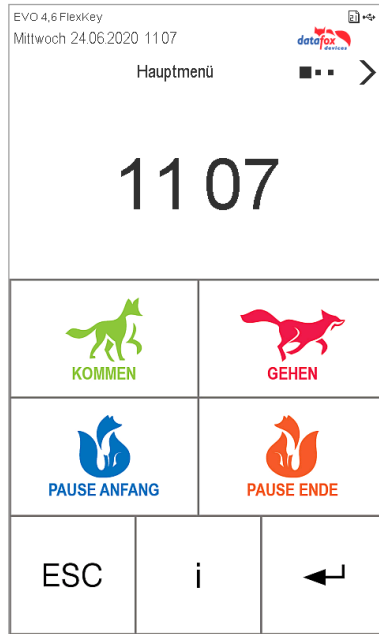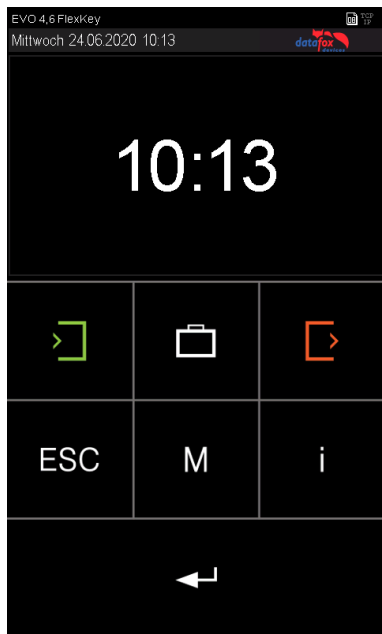
5.2.2.10. Show images during inputs

In the input fields "Normal", "Fingerprint", "Confirmation" and "Display or wait message" it is possible to display an image instead of text or the large clock.
The name of the input field defines which stored image is displayed. The image name must be entered in the following form in the name of the field query. *:img: images.bmp*

Here you must replace images.*bmp* with the name of the images. Ex. „*rfid.bmp*".

!	**Caution:** Since a maximum of 16 characters can be entered for the name of the field query and the label for an image must begin with ": img:", the actual image name may consist of a maximum of eleven characters.

!	**Caution:** With the PZE and AE MasterIV devices, this function is only available in conjunction with a color display. This feature is not possible for EVO 2.8 Pure, EVO 3.5 Pure and EVO 3.5 Universal, otherwise the F-keys for operation could no longer be displayed.

Example: Field function „Normal" & „Show message":
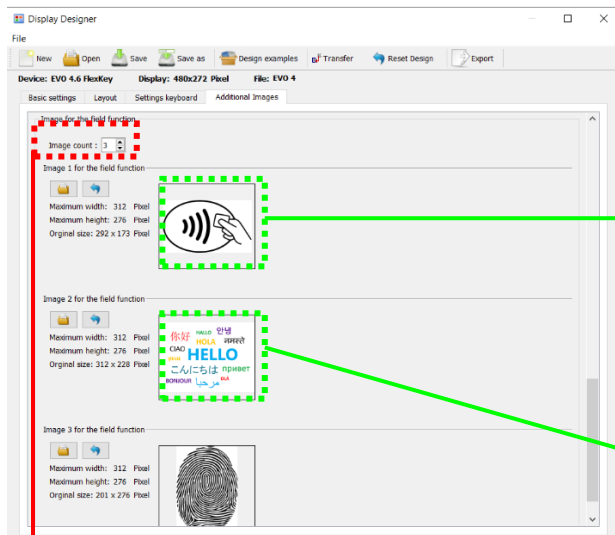
The number of images to be loaded can be individually
set. All the pictures linked here
are also transferred to the terminal.
If these are not referenced in an input field,
the images are not displayed either.
In this case, note that the available
storage space in the terminal is thereby reduced.

5.2.2.11. Design examples in the designer

With the installation of the DatafoxStudioIV you get several design examples for the devices.
Click on the "Design Examples" button to open them.

Datafox gradually extends the examples.
If you have any suggestions or wishes, please let us know.

5.3. Installation of the EVO 2.8 / 3.5 /5.0 Pure Terminal

The wall mounting takes place by means of a wall bracket. This is attached to the wall via 4 attachment points.

The terminal is mounted at the top

On the down site can you fixed the terminal with a screw.

Fixing holes

Fixed screw

*Flat-head screw torx **T10***

Attachment for cable ties for strain relief.
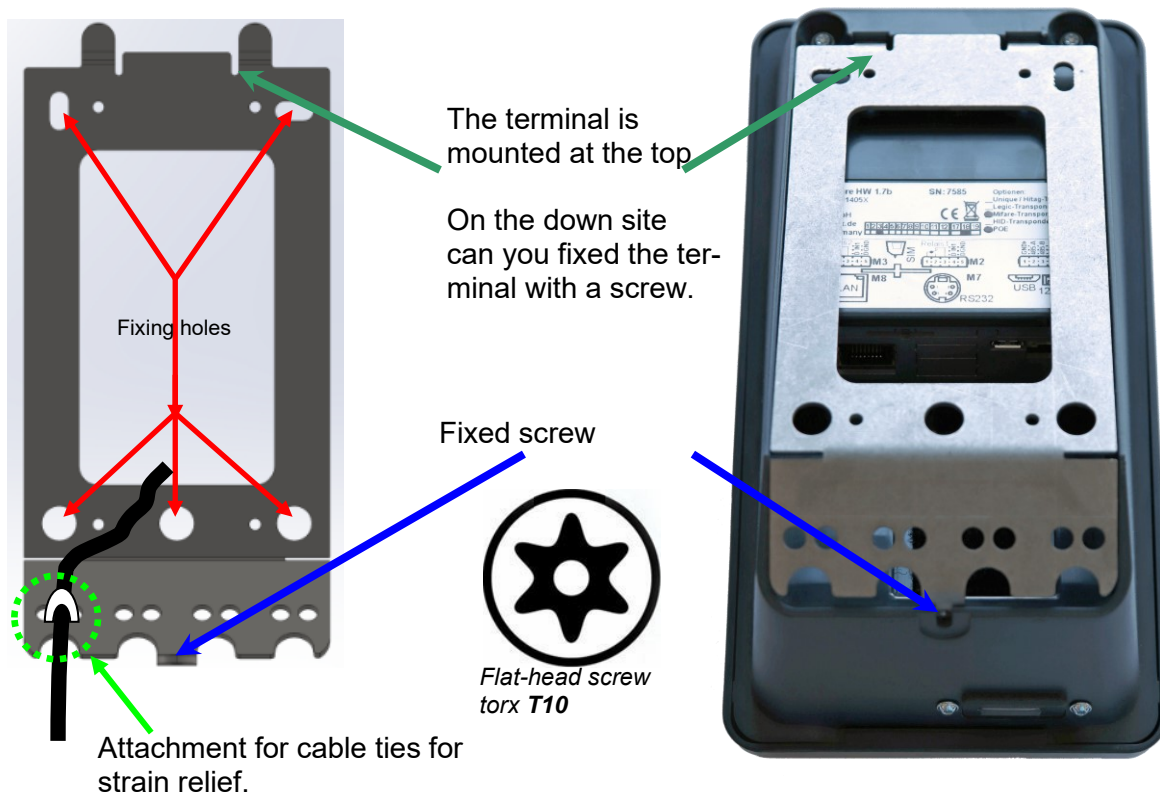
5.3.1. Mounting height of the EVO 2.8/3.5/5.0

Depending on the size of the person a Installation height from 1.20 to 1.40 m recommended.

If the device is equipped with a finger scanner, you Depending on the size of the person a Installation height from 1.20 to 1.40 m recommended.
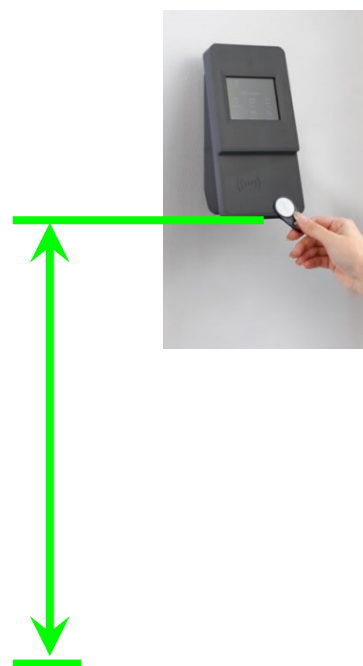
5.3.2. All dimensions for the EVO terminal

ANSICHT 2-2

Boden / floor

DETAIL 1
Massstab
Scale 1 : 3

DETAIL 3
Massstab
Scale 1 : 3
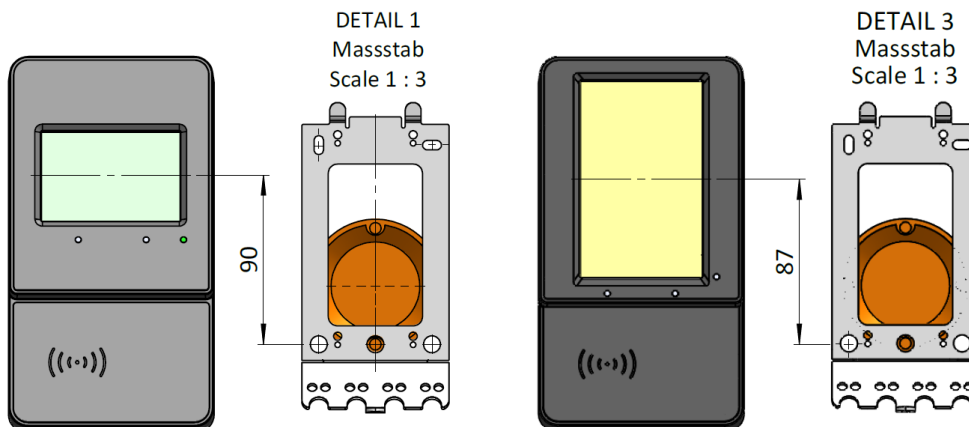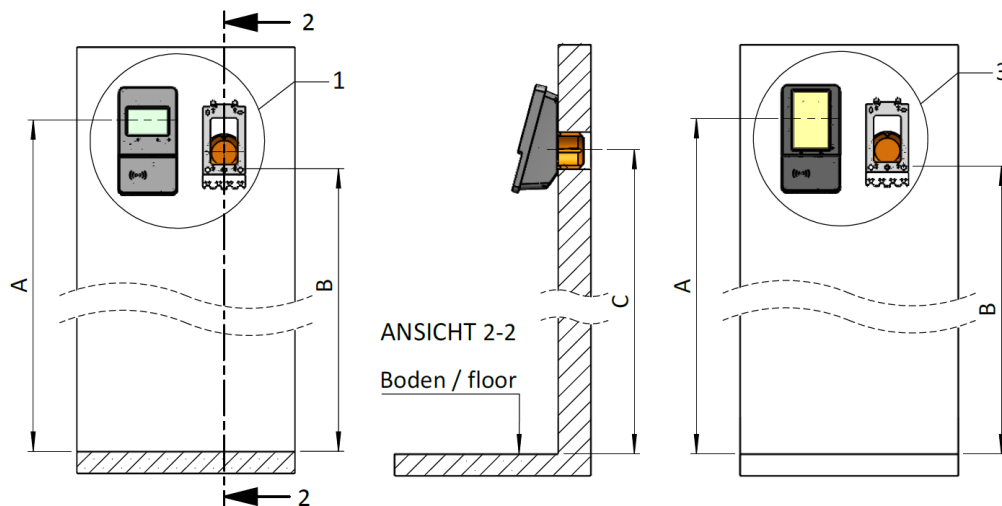
		EVO 3.5 / 5.0 Pure ohne / without FP	EVO 3.5 / 5.0 Pure mit / with FP
A	empfohlene Einbauhöhe *recommended installation height*	1350mm	1250mm
B	Höhe Montagebohrung Wandhalterung *Height of mounting hole Wall bracket*	1230mm	1130mm
C	empfohlene Höhe Kabelausgang / UP-Dose *recommended height cable outlet / flush-mounted box*	1260mm	1160mm

Here the complete assembly and setup instructions:

https://www.datafox.de/d67/unternehmen/downloads/informationsmaterial/evo-3-5-pure/1140x1_Datafox_EVO_2.8_3.5_5.0_Pure_Montage_und_Inbetriebnahme.pdf

5.4. Connecting of EVO 2.8 /3.5 /5.0 Pure Terminals

5.4.1. Connecting plugs

The EVO 2.8 Pure has 5 integrated module places. On this places you can order different modules. You can choose the modules on the pricelist.
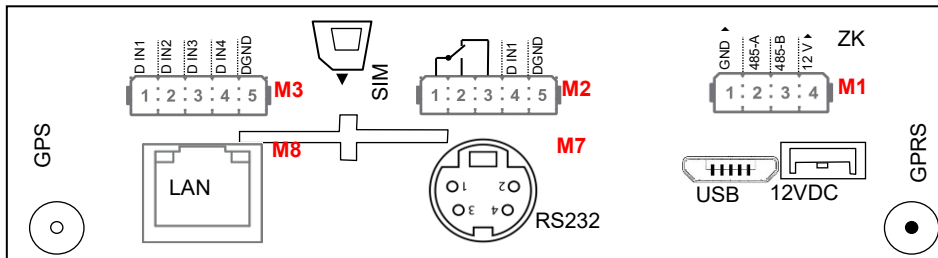
Connector strip of the EVO 2.8 Pure V4

Bezeichnung	Modul	PIN	Beschreibung
Module Slot 1	1	1	ground
		2	A RS 485 for accesscontrol
		3	B RS 485 for accesscontrol
		4	12 V
Module Slot 2	2	4-5 1-3	Standard: 1 digital input 1 digital output with nc and no contact
Module Slot 3	3	1	1 digital input
		2	2 digital input
		3	3 digital input
		4	4 digital input
		5	ground
Module Slot 7 RS 232 Mini-DIN M004	7	1	TXD
		2	RXD
		3	+ 5 V
		4	Ground / GND
Module Slot 8	8		TCP/IP - LAN RJ 45

5.4.2. Powersupply of the EVO 2.8 / 3.5 / 5.0 Pure

The delivery power supply has 12V DC / 18 W.
The terminal itself can be supplied with a supply voltage of 24 V DC.

The power supply:

Reverse polarity protected connector
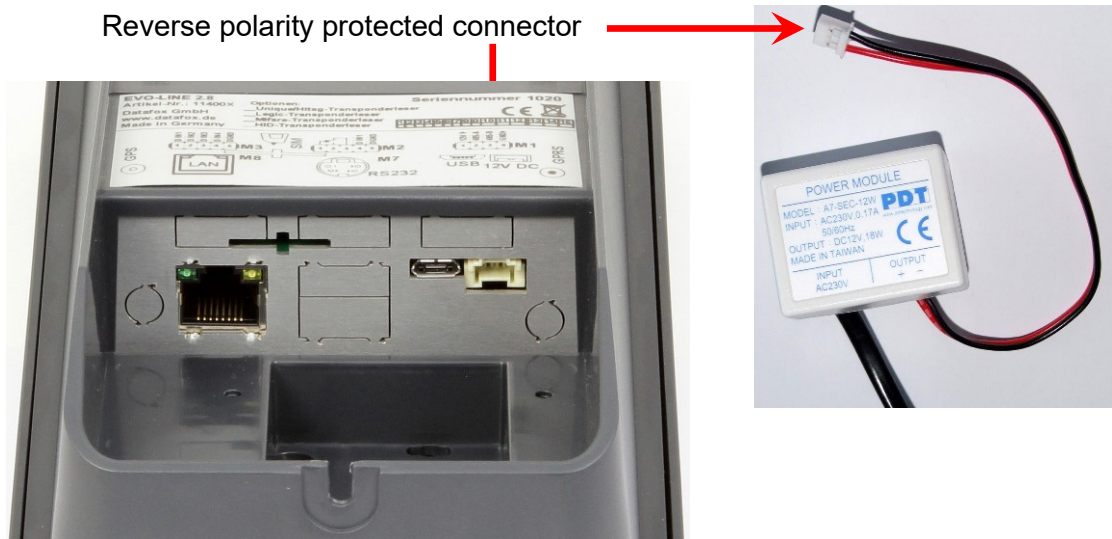
5.5. Power via POE for 2.8/ 3.5 /5.0

An option for the power is a POE-module (Art. Nr: 115117).
This POE-module supports 2 standards.

PoE-Standard		power	useable power
PoE	IEEE 802.3af	15,4 Watt	12,95 Watt
PoE+	IEEE 802.3at	25,4 Watt	21,90 Watt

If power is supplied via POE, an external access-reader can also be supplied via the access control plug.

5.5.1. Modules for devices of hardware V4

5.5.1.1. Description of the various extension modules

The Datafox devices of the generation V4 are particularly distinguished by the variable configuration of individual modules.
Depending on the device, a certain number of module locations are available.
These can be individually equipped with the individual available modules.
Depending on the size of the module, the individual modules occupy one or two module locations.
Thus, e.g. the GPRS module (mobile radio) requires 2 module slots and one relay module only needs one module slot.

<u>**Overview of the different optional modules:**</u>

modul description	Required module slots	Description in the BIOS-Menu and Module mumber.:	Max. possible number of module	items No. for the plug	overprint & Colour
RS 232 - mini DIN Barcode	1	032 Serial port mini DIN	1		
RS 485 access control	1	014 RS485 + 12V Supply	4	A3100004-01	**485** ⊥ A B ±
RS 485 main communication	1	035 RS 485 Com Port	1	A3100004-01	**485** ⊥ A B ±
GPRS Mobile (Cell phone) network	2	Mobile MC 55i	1		
TCP/ IP	1	011 Ethernet Port	1		
WLAN (Wi-Fi)	1	001 WLAN	1		
4x digital Out	1	051 Digital out activ **ground**	1	A3100005-08	**Dig-out-4-GND**
4x digital Out	1	051 Digital out activ posi-tiv (Plus)	1	A3100005-05	**Dig-out-4-Plus** +12V
2x digital Out	1	005 Relais Output	8	A3100005-01	**Relay-2**
1x digital In + 1x digital Out	1	012 Digital In-/Output	8		**ZK-Opt** 1 ⊥
4x digital In	1	006 Digital Input	8	A3100005-02	**Dig-in-4** 1 2 3 4 ⊥
4x anlog In	1	008 Analog Input	8	A3100005-03	**Ana-in-4** 1 2 3 4 ⊥

How many module places are usable you can see in the device manual in the chapter "Connection of device".

5.6.   Read the optional placement of the device
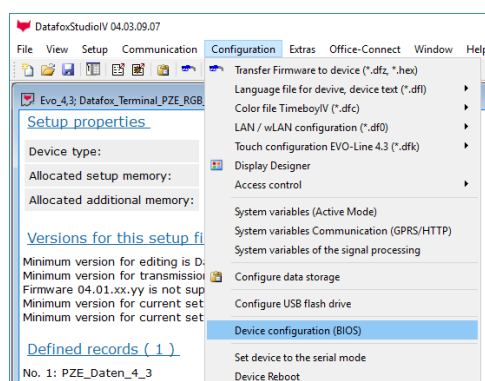
Click on:
„Configuration → Device configuration (Bios)"
Then click on „Read".

Display in the Bios-Menu:

Here you can see all modules that are fitted in the device:
You see which module is on which place. You get extended information like MAC address, the number and order of the inputs and outputs.

Example 1:
- Module place = M1
- Digital Input 1 to 4
- Module Number: = 006 digital input

Example 2:
- Module slot = M4
- Analog Input 5 to 8
- Module Number: = 008 analog Input

E.g. Type label of an IO-Box V4:
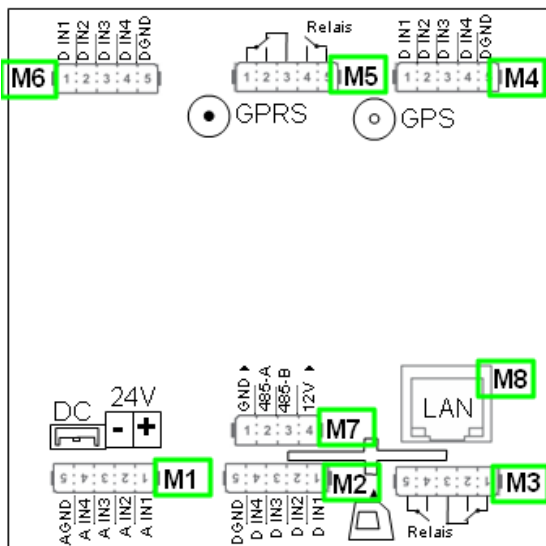
You can see here, in the IO-Box

8 module places are usable. This can be individually fitted.
Exceptions:
- Module place 8, only here TCP is possible.
- RS 485 for access control - maximum 4 Modules can be fitted.

5.6.1.1.   Read out important module information from the device
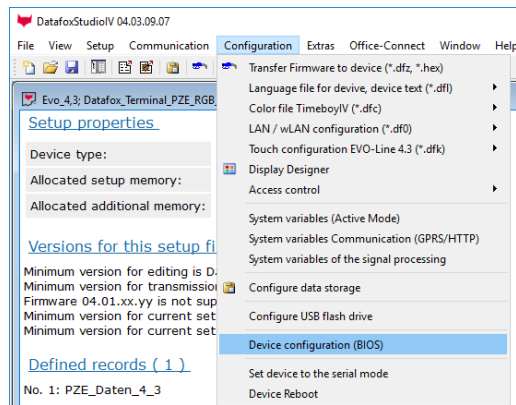
Click on:
"Configuration → Device Configuration BIOS"
Then click on "Status" thereafter
Click "Read".

Here you will find a whole series of important information about the terminal.
Here are some explanations of the individual lines:

1) Name of the setup, this is also available when reading out.
2) The date when the setup was loaded into the device.
3) State of the digital inputs. All inputs which are physically present and defined in the setup are displayed here with their status.
   a.   00000000 = Digital inputs defined in the setup
   b.   0 = Input on LOW   (logical 0)
   c.   1 = Input on HIGH   (logical 1)

4) If digital inputs are defined in the setup as counter, the current count value is displayed here.
5) Status of the digital outputs: Output 1 is continuous here from left to right.
6) Analog inputs from left to right with respective currently applied voltage.
7) Different timers, which are set in the setup, are shown. The figure in brackets is the actual time to the next trigger.
8) Number of stored records in the device and memory used.

5.6.1.2. Connection of the individual modules

The connector / socket for the module always has the following assignment:

Socket on the device:
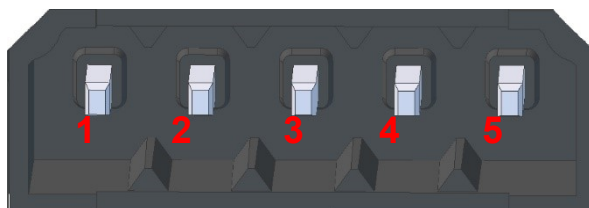
The plug can be inserted only in one direction and is therefore protected against reverse polarity.
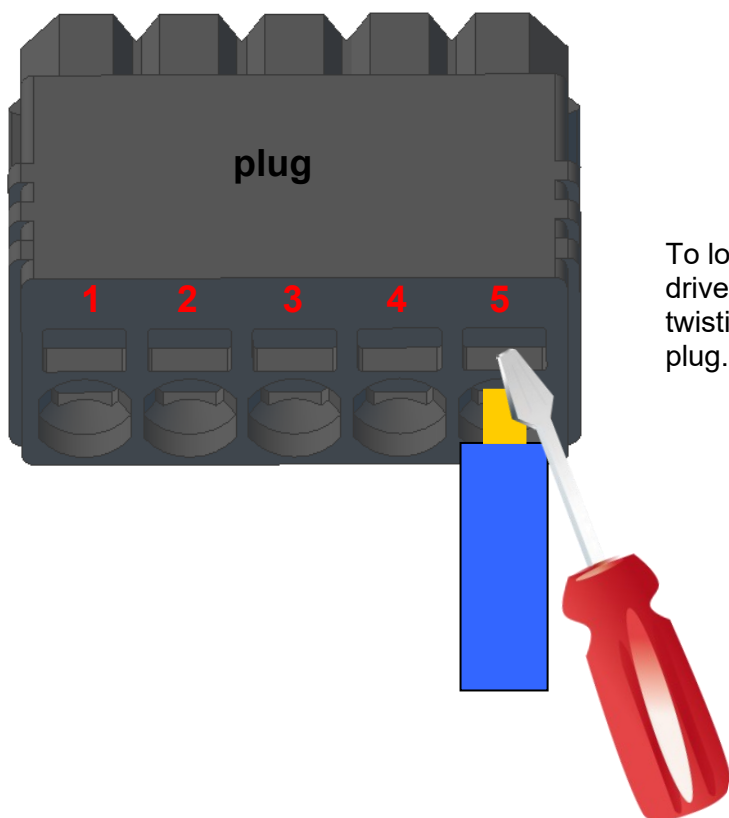
plug

To loosen the cable, use a small screwdriver. Solid wires can be loosened by twisting back and forth on the wire and plug.

5.6.1.3. Analog inputs, 4 x analog IN

common ground;
GND / Ground

+ 0-10 V signal 4

+ 0-10 V signal 3

+ 0-10 V signal 2

+ 0-10 V signal 1
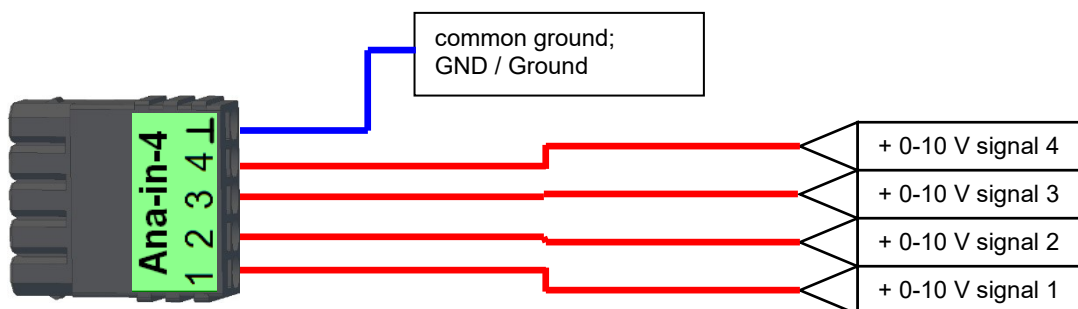
5.6.1.4. 2 x digital out

Connection example:
(Connection of a signal light and a signal horn via a potential-free contact):

max. 30V AC/DC / 2A / 60W
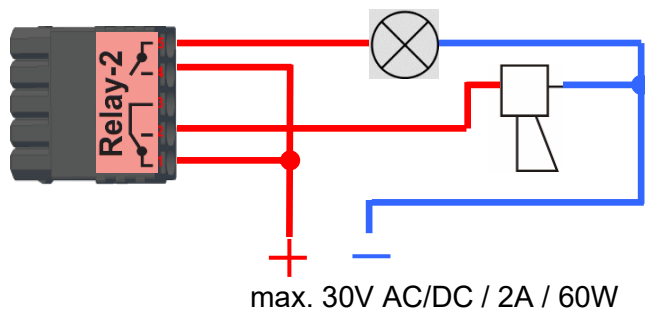
5.6.1.5. 1 x digital Out 1x digital IN

Connection example (Connection of a signal light and a door contact):

max. 30V
0 - 1,5 V   Input logical 0
3,5 V - 30 V   Input logical 1
- Galvanically isolated
- up to 250Hz

e.g .: Door contact

max. 30V AC /DC
2A / 60W
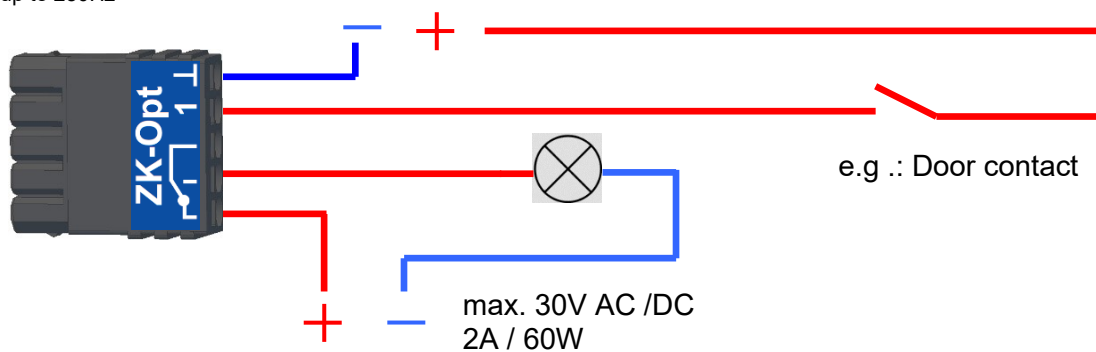
5.6.1.6. 4 x digital IN

Connectiom example (Connection of 4 contacts):

e.g.: 4x digital in

max. 30V
0 - 1,5 V   Input logical 0
3,5 V - 30 V   Input logical 1
- Galvanically isolated
- up to 250Hz
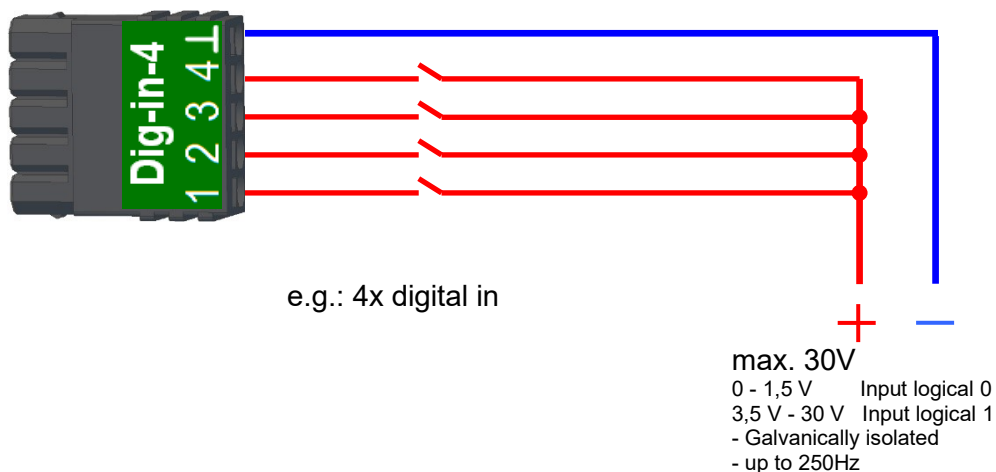
5.6.1.7. 4 x digital OUT activ-Low (ground switched)

The digital output modules provide 4 switching outputs on a single module. The module 51 (Art.-Nr. xxx 172) can 12 V DC output, the module 105 (Art.-Nr. xxx 173) switch on ground. (Open Drain).
By switching to ground, the module 105 can switch quite large currents, e.g. for lockers or electric door openers.
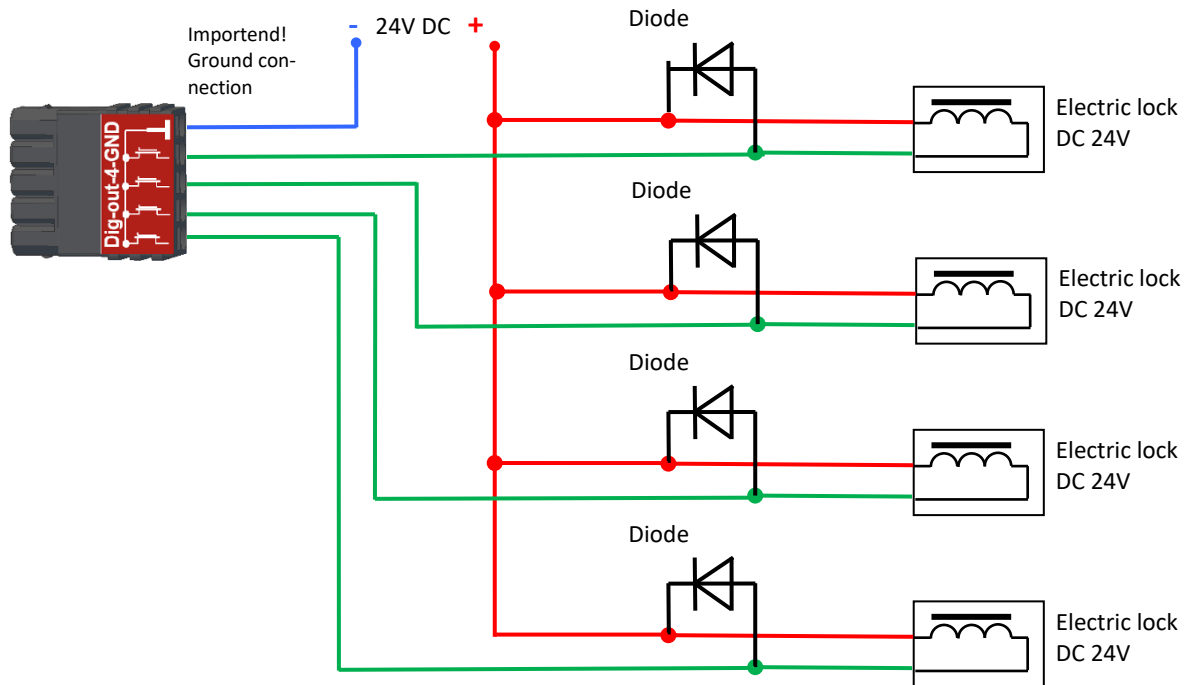
5.6.1.8. 4 x digital OUT aktive-Hi (plus switched)

Example connection for indicator lamp, module 51
In this way, the malfunction indicator lamp can be connected with just a single plug.
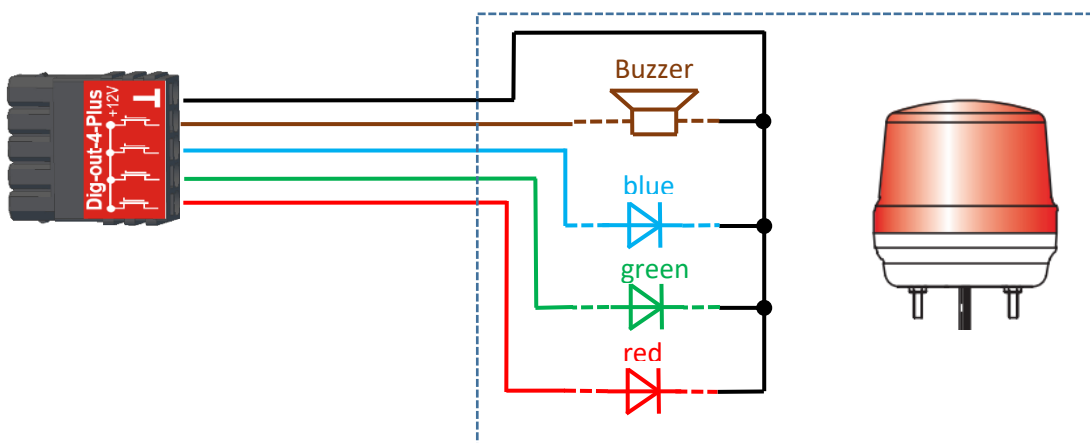
5.6.1.9. RS-485 bus for access control

The access control option provides the connection for external readers on the device.
The pin assignment looks as follows:

12V +

GND -

The power supply is sufficient for max. 1 external reader.

This voltage must not be combined with other voltage sources.
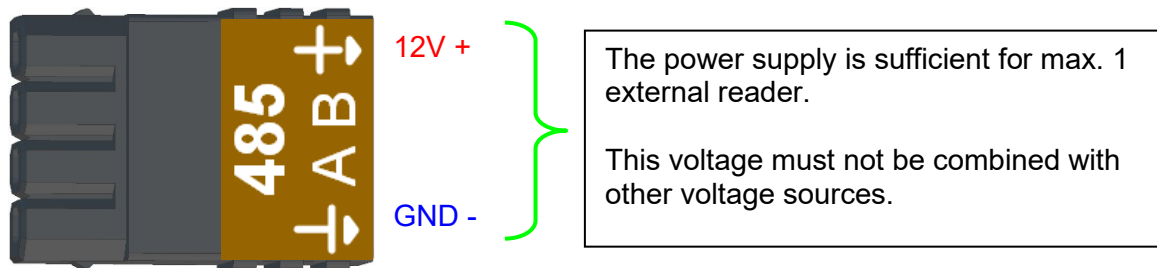
☞ Note:
The 12 V are only present when the access control on the device is activated and all access lists have been played on the device.

Furthermore, the connection for a digital input and output is available.
The pin assignment looks as follows:

How the individual access components are connected or wired, can be found in the chapter "Access control"

5.7. Communication of Hardware V4 Devices

> **Caution:**
> The type of communication depends on the device.
> All possible communications are listed in the device.

> **Note:**
> Datafox-devices are able to communicate encrypted.
> Read more in the manual for the „DatafoxStudioIV".

The switching of the communication can be done
via :
1. the system menu bios on the device
2. with firmware version 04.02.04 and up with the function „Switch communication".
3. from the Firmware version 04.02.04 upwards with the field function „switch communication".
   Read more in the manual for the „DatafoxStudioIV"

Possible communication types are:
1. USB   (on PC)
2. USB Host, Save data on a USB-stick
3. TCP/IP over LAN
4. TCP/IP over the internet (with HTTP)
5. TCP/IP over WLAN
6. GPRS connection with mobile cell network.

5.7.1. Communication via USB

Every EVO-Line Device is equipped with an USB interface.
The Micro-USB-B Port can be connected directly to a PC.
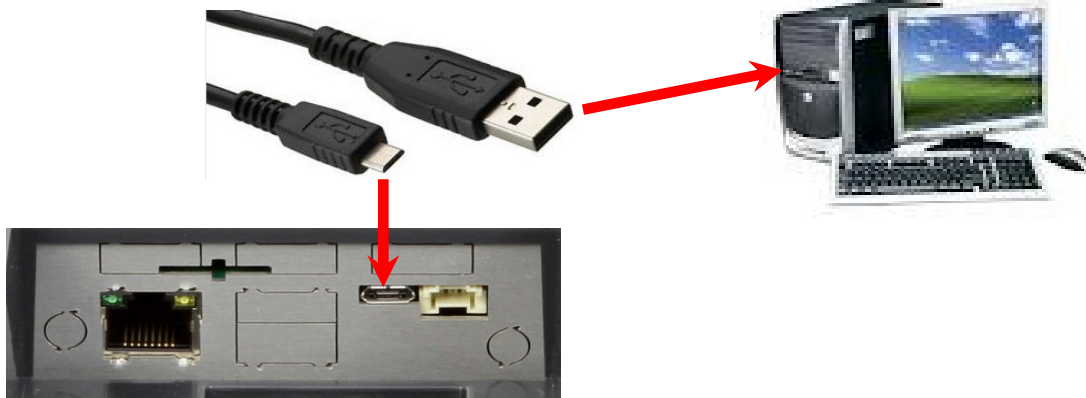
> **Caution:**
> The Terminal works with a USB-B Interface. This means that the device works in slave mode only. So it is not possible for the device to control any other devices via USB.

5.7.1.1. Automatic detected connected USB to PC

If the terminal is connected to a PC it will recognize the connection and will switch the communication to USB.

DatafoxStudioIV will recognize the device and a notification will pop up.
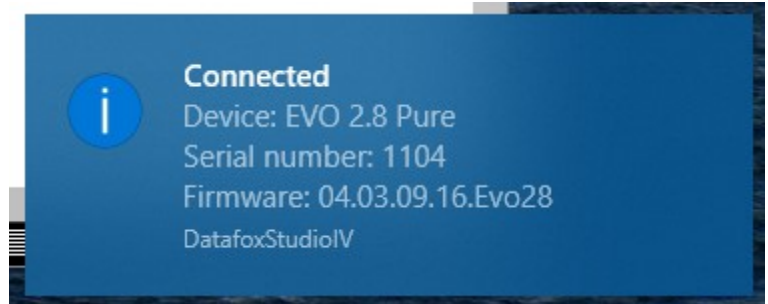
The studio will generate an entry for the device.
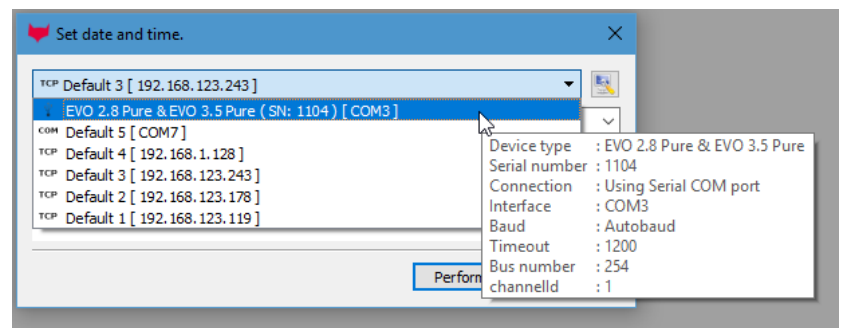
following icon is displayed:

It is not necessary to switch the main communication to USB manually.
It's especially useful for boxed devices.
This will save much time in the parameterizing process.

> **Note:**
> If the device is connected to a PC no other connections (for example Wi-Fi) will happen. If the USB-cable is disconnected, it will automatically switch to the configured main communication.

5.7.1.2. Installing USB driver for Hardware V4 Devices

Installation for Windows 10 and 11
The USB-Driver is a small installer which will do the necessary configuration.
Just launch the .exe file.
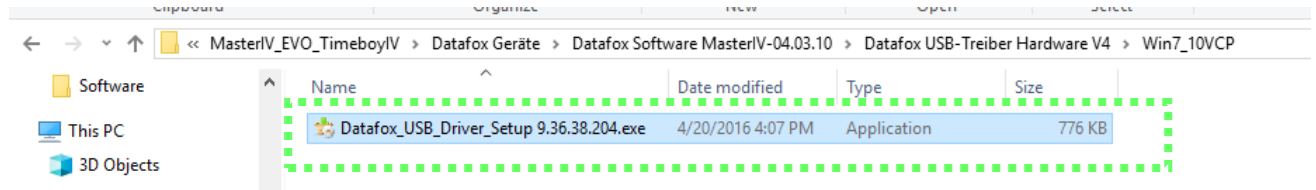
Follow the instructions on the screen:
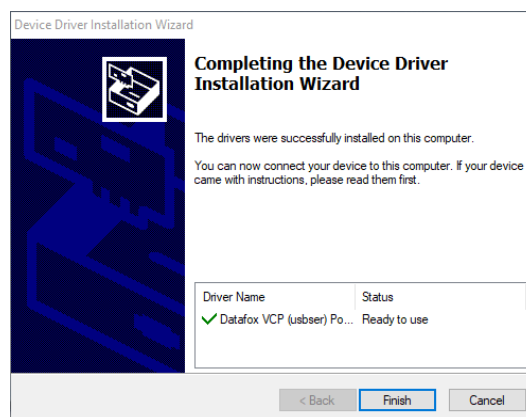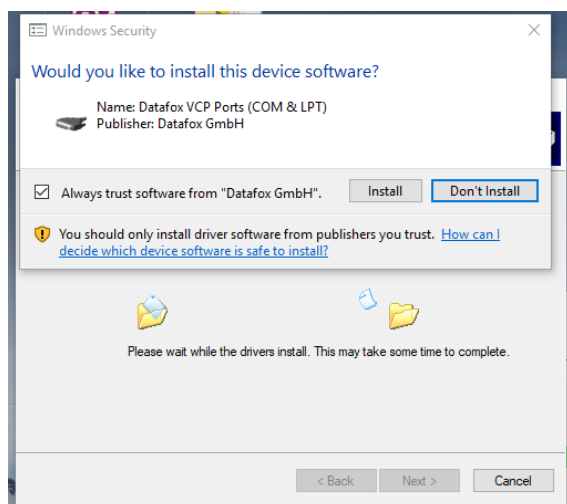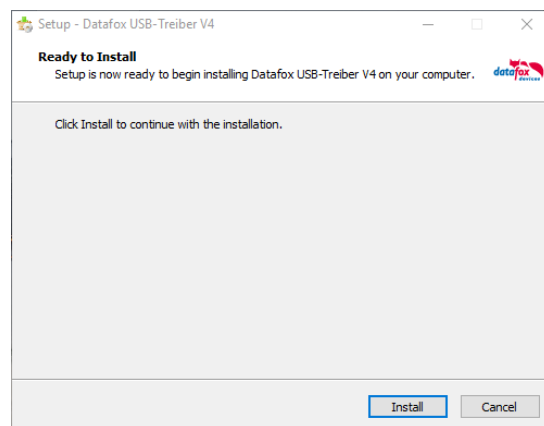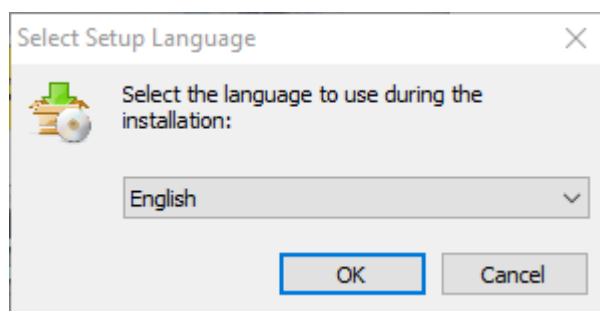
| ! | **Caution:**
Only use the driver which are delivered with the device! |

| ☞ | **Note:**
If you have DatafoxStudioIV installed, the USB-driver will already be installed on your PC. |

5.7.2. Communication / record transfer via USB-Stick (Host)

To be able to transfer data from the device to a
USB stick, the device must have the option
"USB host".
You can see this at the neckline.

The USB-Stick must be in **FAT(32).**

The device detected the stick automatically, when the stick is plugged in.
The main communication must be set on "USB-Host". You see the activated main communication
by this symbol (Icon) .
You can change the main communication in the bios-menu.

USB - Stick adjust:
The USB stick is configured with the help of DatafoxStudioIV.
You find the configuration menu under the point „Configuration"→ Configure USB flash drive.
More description you find in the manual "DatafoxStudioIV".

> ☞ **Note:**
> We recommend to use a password for the communication with the USB-stick.

> ❗ **Caution:**
> The USB cable to the PC must not be connected if you want to use the stick on the device.

> ❗ **Caution:**
> Lists of access control can be transferred individually, operation lists must always be transmitted in complete form. All lists defined in the setup must also exist on the stick in the "List" directory.

5.7.2.1. Error messages by using USB-Stick (Host)

Error code	Description
1	**Read Error**
2	**Write Error**
3	**Error during the communication with the USB host**
4	**Error during the changing the directory**
5	**Error by the check of the stick**
6	**Error by the list directory**
7	**Error to create a data directory**
8	**Error handle**
9	**Error to open a file**
10	**Error not find the path**
11	**Error, the file is already open**
12	**Error to open a file**
13	**Error by closing the file**
14	**Error by closing the file, false handle**
15	**Error by checking the handle**
16	**Error by checking the handle, the file is not open**
17	**Error write protect**
18	**Error by the record structure**
19	**Error during the firmware update**
20	**No USB stick**
21	**Incorrect password**
22	**No list**

5.7.3. Communication via TCP / IP

The setting of the LAN / WLAN parameters is done via DatafoxStudioIV under the menu item "Configuration" → "LAN / WLAN – Configuration (*.df0)".
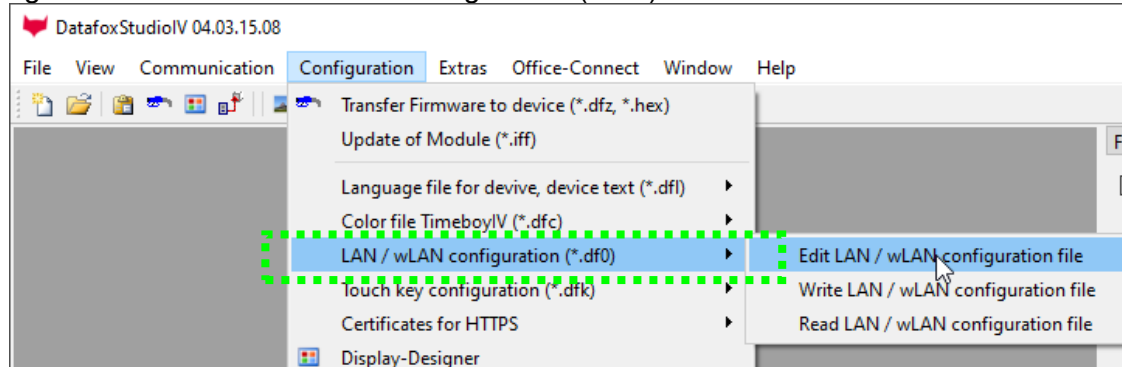
The LAN / WLAN configurations are saved in a file with the filename extension "*. df0".
Here you have the possibility to edit the file, load it into the Datafox device (upload) or read it from the device (download).
When reading the WLAN setting from the device, the currently specified file is overwritten.

In the General tab, first of all, you can set the main communication with which the device is equipped.
- Device with LAN (The first configuration is for LAN connection)
- Device with WLAN
- Device with LAN and WLAN (The first configuration is for the LAN connection)
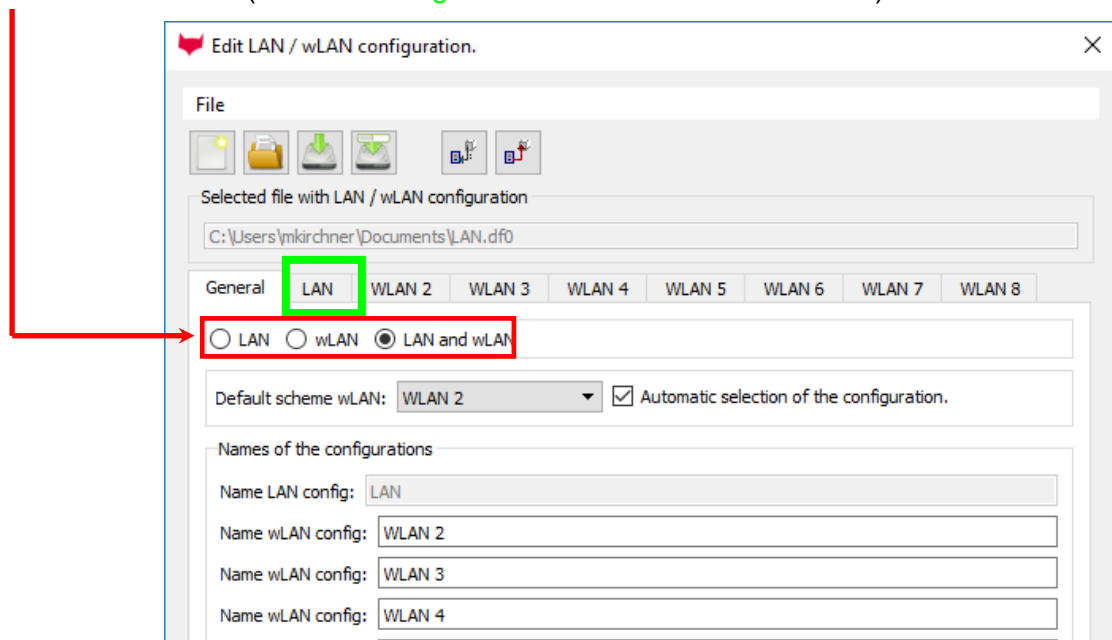
> **Caution:**
> For TimboyIV only this setting (only wLAN) can be used.
>
>

5.7.3.1. Communication TCP / IP via network-cable

You can make the IP settings on the "LAN" tab.

Please enter the desired IP address, subnet and if necessary a gateway.
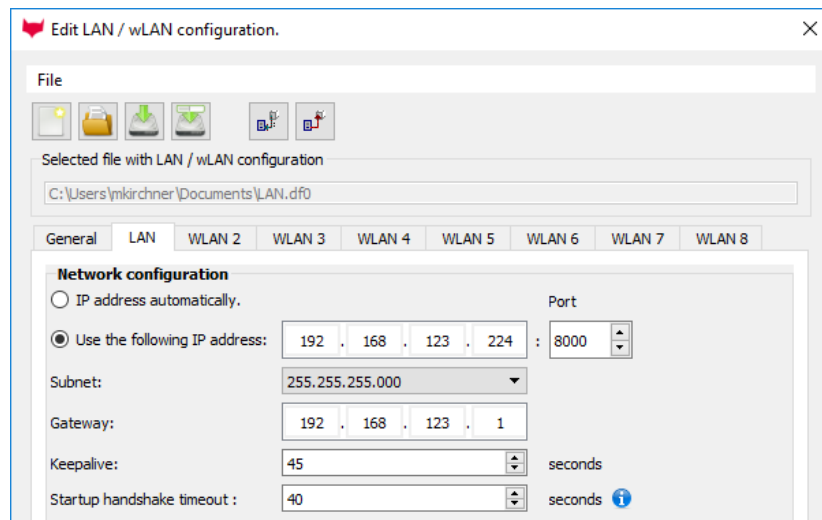
For devices with display, the IP address can also be entered directly on the device. Press ESC and ENTER simultaneously to enter the Bios menu of the device.

More information can be found in the chapter „bios menu".

5.7.3.2. Communication TCP / IP via wLAN / Wifi

General information about the WLAN modules used.

There are 2 different WLAN modules that have been integrated into the Datafox devices.
1.) Redpine – installed in the units since 2013.
2.) Texas Instruments TI-CC3135 - installed in the devices since 2021.03.

Basically, both modules can be set via the DatafoxStudioIV or on the device itself.
The only difference between the modules is that different standards are supported.
You can see what each module supports in detail on the following pages.

You check with the DatafoxStudioIV via Configuration -> Device configuration (Bios):

Standardmodul	014 RS485 + 12V Supply	1	M1	
Standardmodul	012 Digital In-/Output	2	M2	DI 1, DO 1
Standardmodul	WLAN TI CC3135 ML01	4		
Standardmodul	037 Single Serial Port	6		
Transponderleser	TSR32 Reader 125kHz	1		
Standardmodul	014 RS485 + 12V Supply	7	M7	

oder:

Standardmodul	001 WLAN Redpine RS9110	6	-	Vers. 4.5.5, Mac: 88-DA-1A-7F-E6-65, Ip: 192.

You have a delivery note and look at the article number
1.) Redpine: Art.Nr.: xxx112 (generation 1)
2.) Texas Instruments CC3135:   Art.Nr.: xxx112 A   (generation 2)

You are checking the Bios menu of the unit:

Under: System Menu-> System Menu Bios-> Communication
Here you have to set the unit to "WLAN" as the main communication.
Under the settings WLAN parameters you have an info menu „Modul Informationen".

16:36 Do., 07.01.2021		ESC
WLAN-Parameter		
Datafox WLAN 5G	📶	∧
Netzwerk auswählen		
Neues Netzwerk hinzufügen		∨
Modul Informationen		

5.7.3.3.   M111_WLAN ESP32-c3 ML01 (wLAN-Modul DF-WL03)

This overview shows you which WLAN methods are supported.

The WLAN 3 module automatically detects the encryption of the AP. Therefore, only the Security parameter needs to be set. The other parameters (Encryption and Authentication) are detected automatically.

Routers that operate WPA3/WPA2 in mixed mode can already be used now.

Router die WPA3/WPA2 im Mixed Modus betreiben können bereits jetzt genutzt werden.

Supportet is here only the 2.4Ghz.
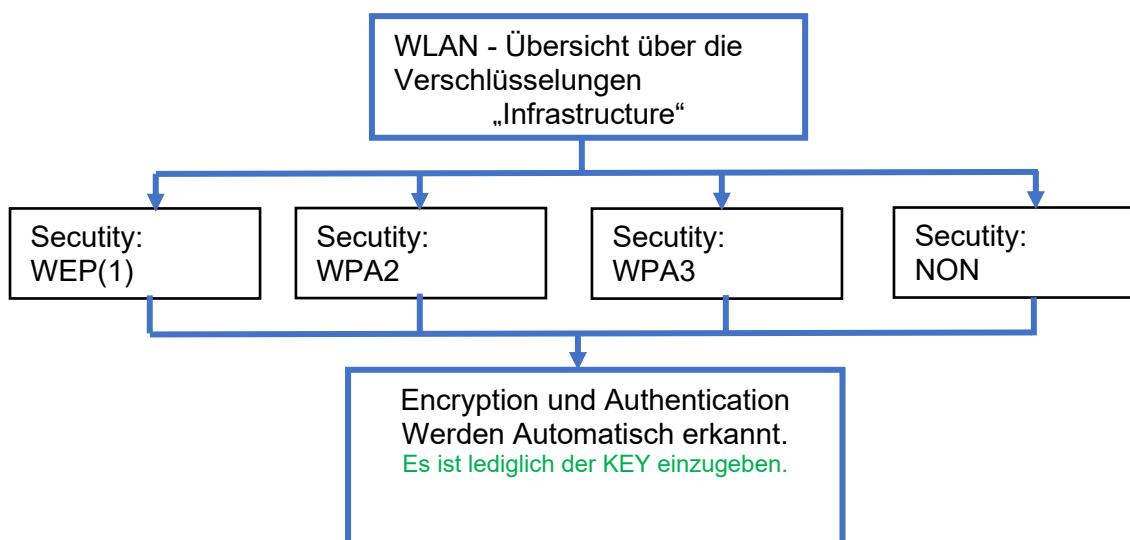
Achtung:
Wir können nicht jeden auf dem Markt befindlichen Acsess-Point Testen.
Daher ist es uns nicht möglich, einen Verbindungsaufbau zu jedem AP zu garantieren.

5.7.3.4. Texas Instruments TI-CC3135 (Generation 2)

This overview shows you which WLAN methods are supported.

The TI-CC3135 module automatically detects the encryption of the AP. Therefore, only the Security parameter needs to be set. The other parameters (Encryption and Authentication) are detected automatically.

Routers that operate WPA3/WPA2 in mixed mode can already be used now.

If the networks in the 5Ghz and 2.4Ghz bands have the same name, the network with the better reception quality is selected. This is usually the network in the 2.4Ghz band.

```
            WLAN - Overview of the en-
            cryptions
                    „Infrastructure"

  Secutity:      Secutity:       Secutity:      Secutity:
  WEP(1)         WPA2            WPA3           NON

            Encryption and Authentication
            Are automatically recognised.
            Only the KEY hast o be entered.
```
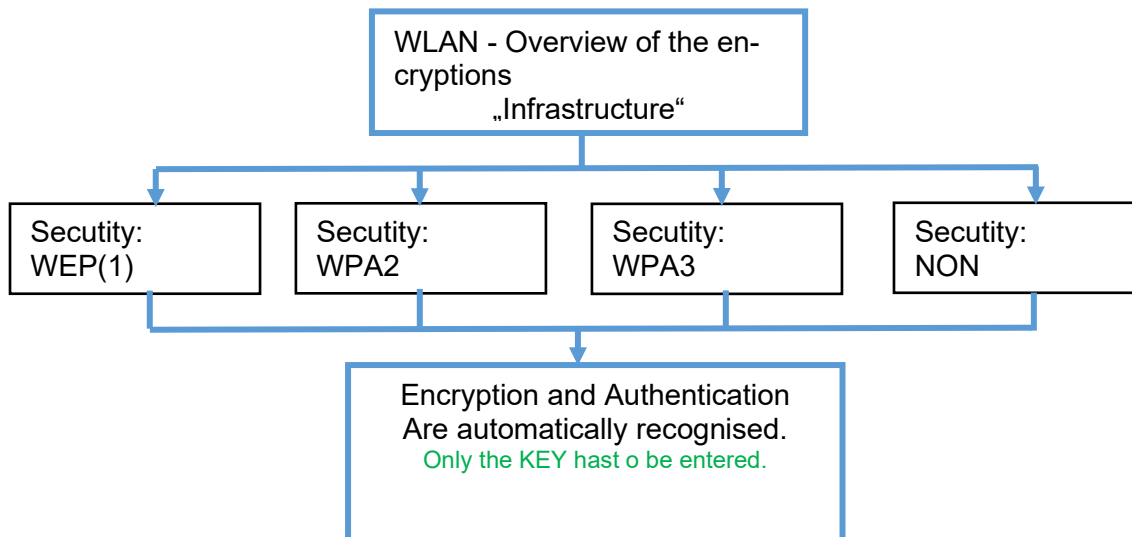
Attention:
We cannot test every Acsess point on the market.
Therefore, it is not possible for us to guarantee a connection to every AP..

Support for WPA3 and WPA2 Enterprise is planned.

5.7.3.5. Redpine (Generation 1)

This overview shows you which WLAN methods are supported.
- **Not supported** is WPA (Predecessor of WPA2).
- **Not supported** is multiple-input multiple-output (MIMO)
- **Not supported** 5 GHz connections and no mixed operation 2.4 GHz / 5 GHz
- **Not supported** Authentication via WPA2 Enterprise according to IEEE 802.1x

```
                    WLAN / Wifi – overview about
                    the encriptions and
                    „Infrastructure"
                              |
        +---------------------+---------------------+
        |                     |                     |
   Security:             Security:             Security:
   WEP(1)                WPA2/802.11i          None (0)
                                               ohne
        |                     |                     |
   Encryption            Encryption              NO Key
        |                     |
      WEP64             AES / CCMP
                        „AES 128"
      WEP128
                        AES / CCMP +
                        WEP
   Authentication       Authentication
   Open/None (0)        Shared/PSK
   Shared/PSK (1)
```
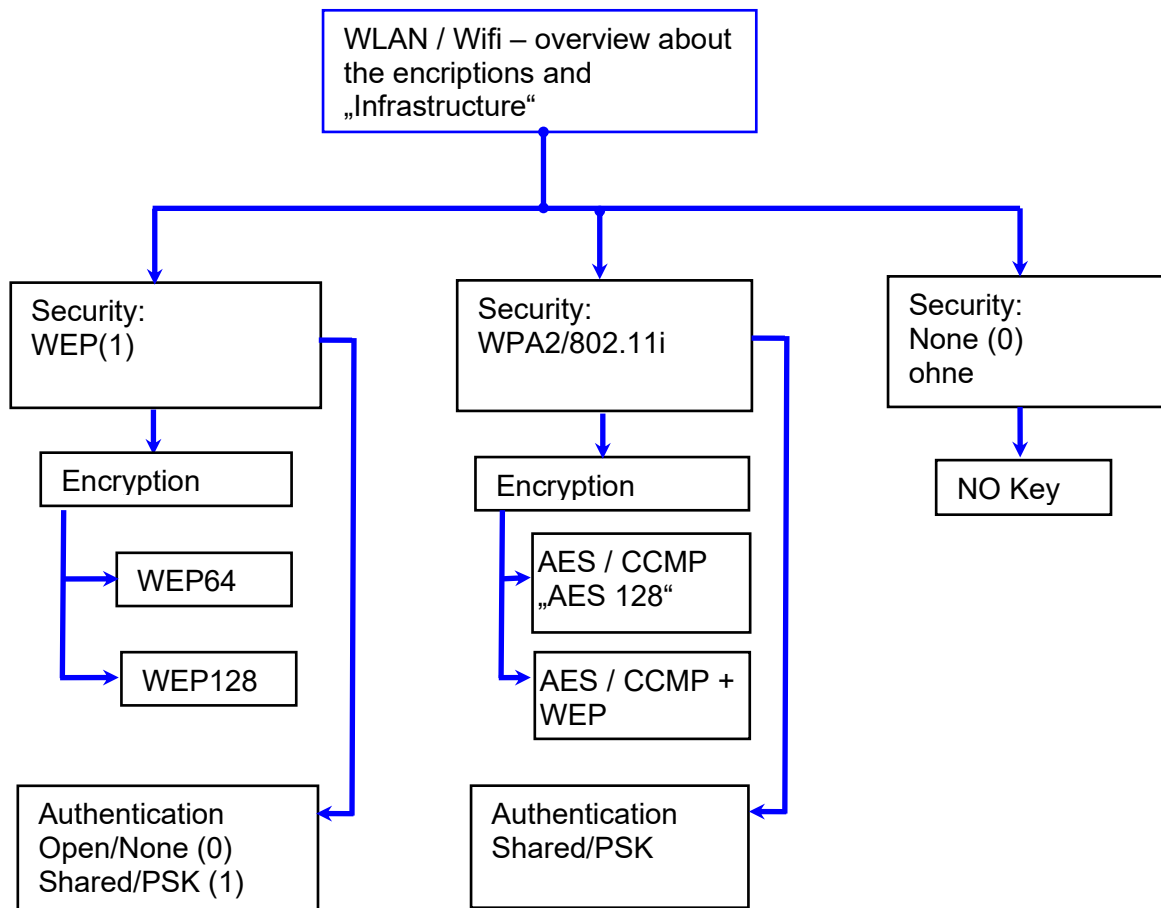
> ⚠ **Attention:**
> We cannot test every available Access-Point on the market.
> Therefore, it is not possible for us to guarantee a connection to any AP.

> ⚠ **Attention:**
> multiple-input multiple-output (MIMO) are not supportet. If you switch the access-Point AP from b/g/n to b/g, use the access-Point only SISO.
> https://en.wikipedia.org/wiki/Single-input_single-output_system

When setting the encryption AES or WEP, only one type is used at a time.
The setting AES+WEP means for some access points that AES encryption is performed first and then additionally encrypted with WEP.
In this case, only set AES.

Select the configuration or location for which you want to set the WLAN parameters.

Enter the IP address for the device here.
This must be the same for every location.

All the settings required for an access point can be made here.

If a key is stored, this will be displayed.

If you check this box, the battery life will be significantly increased if the device is operated with a rechargeable battery. Important for TimeboyIV!

A scan (search) for access points is only carried out after a disconnection after this set time. Please note the following Attention Box!

Attention:
A search for a new access point requires a lot of energy and drains the battery. Avoid a continuous search for an access point when the device is operating at the limit by generously selecting the pause between scans for new access points (80-120s).
At most access points there is the possibility to set the "Beacon Interval". The higher this is set, the less power the TimeboyIV needs. Recommendation: Beacon interval >300ms.

The entire file with all settings is transferred to the device. If the device has a display, the location can be selected in the Bios menu -> Communication -> WLAN. Each location has its own configuration for the WLAN connection. The user therefore has no insight into the dial-in parameters at the various locations.
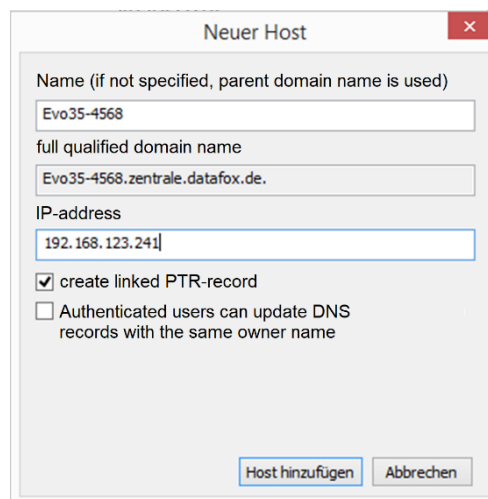
Hint:
With automatic selection of the configuration / location, the first attempt is always made to establish a connection with the default schema.

5.7.3.6. Connection of the Terminals via TCP/IP DNS / DHCP
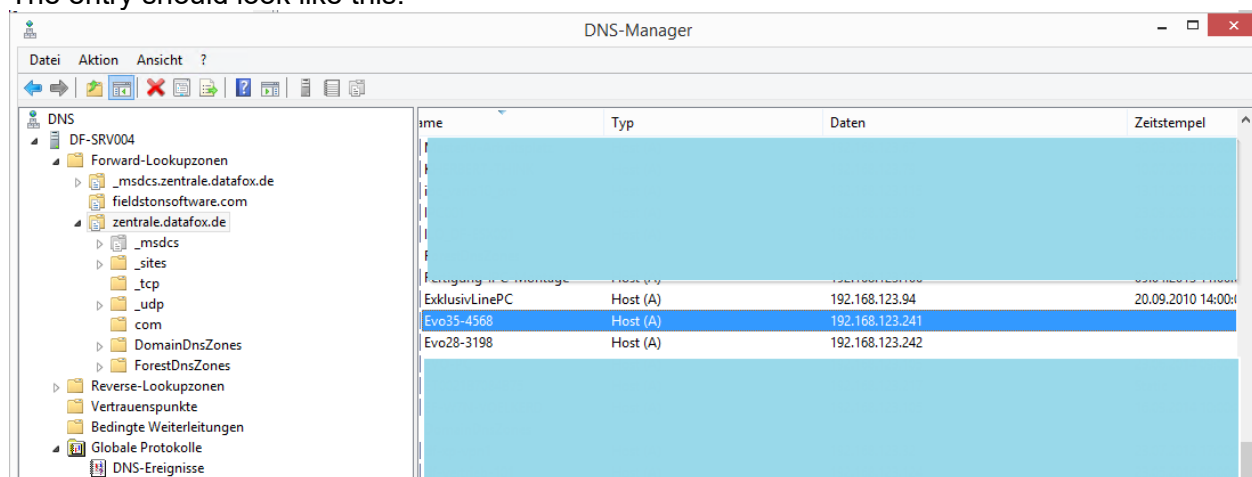
To connect a Datafox EVO-Device with the Hostname it is necessary to set something in the DNS-Server. (In this example Windows-Server 2012)

Create a new Host (A)-value:

Abbreviation	Descripion
Name	Name of the device Contains the device designation and the serialnumber „device*XX*-serialnumber" Example: „Evo28-1652" „EVO43-8552"
full qualified do-main name	This is the host name to be entered later.
IP-address	Here you must enter the IP of the device.
Create linked PTR-record	You must create a linked PTR-record. Just put this hook.

The entry should look like this:

Settings in the DatafoxStudioIV:

| Host name | | Before entering, this checkbox must be set. |

DHCP- entry for Datafox devices

If a device is set to DHCP, the IP address and the entry in the DHCP server can look like this.

The entry contains the following:

device	serial number	domain	DHCP- entry
EVO 2.5	10245	.zentrale.de	Evo25-10245.zentrale.de
EVO 3.5	10246	.zentrale.de	Evo35-10246.zentrale.de
AE-Master	10247	.zentrale.de	AE-10247.zentrale.de
PZE-Master	10248	.zentrale.de	PZE-10248.zentrale.de
EVO 4.3	10249	.zentrale.de	Evo43-10249.zentrale.de

5.7.4. Communication via RS485

5.7.4.1. Connecting the terminal via RS485 to PC

RS 485 to PC
up to 1000m

B
A
GND

RS 485 - HK

A
B
GND

RS 485 connection at the Terminal

USB - RS485 Adapter at the PC
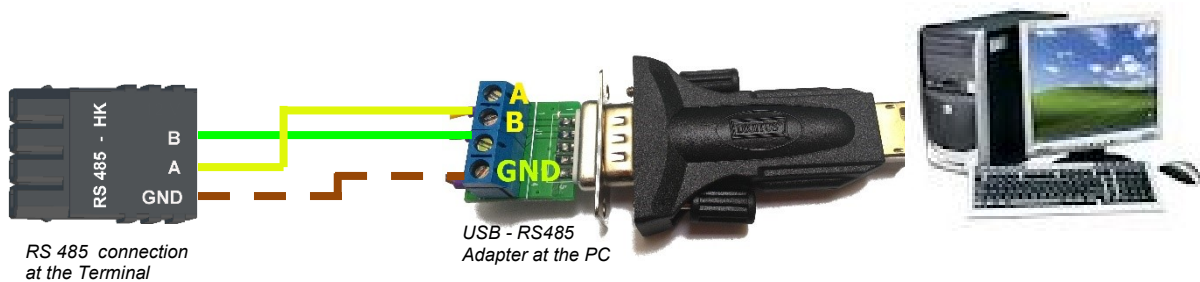
Setting for communication in the DatafoxStudioIV for connection via RS 485:
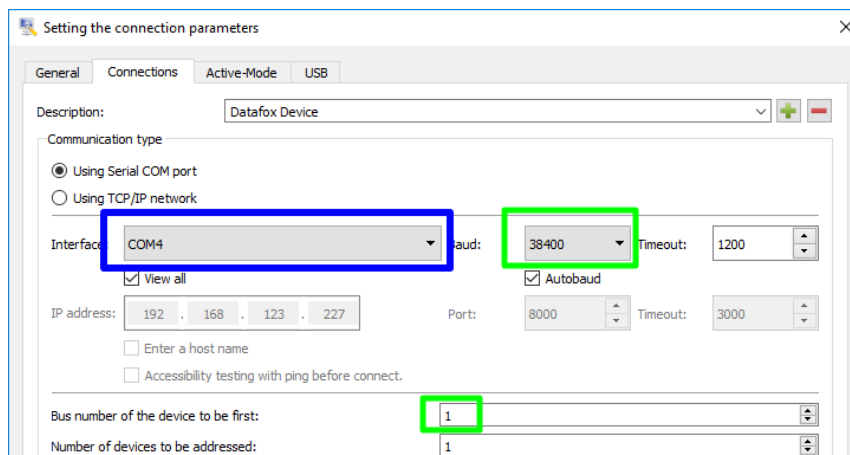
Com-Port
See in the device manager on your PC

Baud rate 38400 and Bus number are to set in the device bios menu

5.7.4.2. Connecting the Terminal via RS485 with a Comserver Lantronix

TCP/IP   RS485

plug
Pin 15 - BUS B
Pin 14 - BUS A
Pin 7 - GND

plugr 4 Pol.
BUS A
BUS B
Pin 1 - GND

plug 4 Pol.
BUS A
BUS B
Pin 1 - GND

120 Ohm
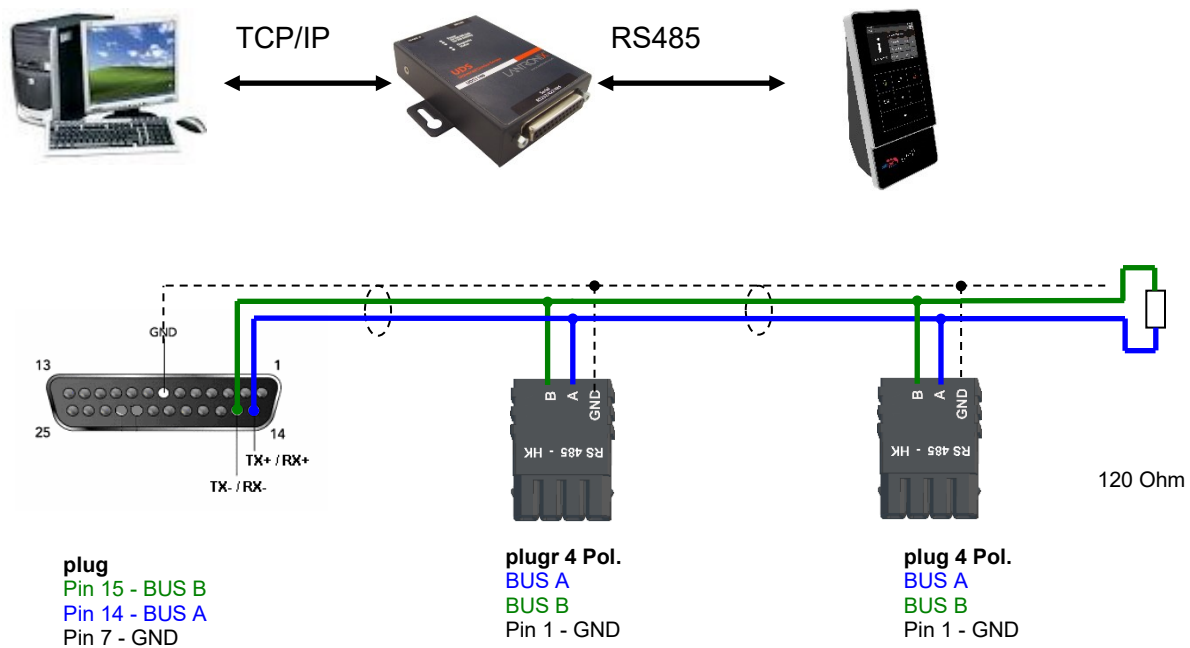
Setting for communication in the DatafoxStudioIV for connection via RS 485:
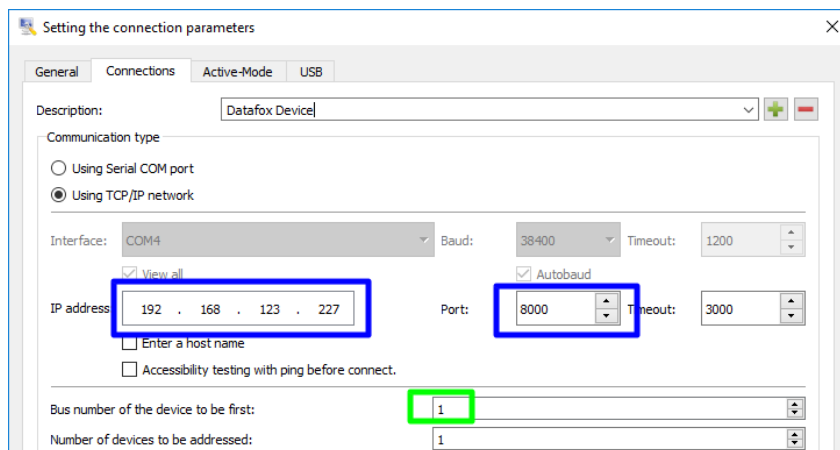
IP and Port must set in the comserver.

Baud rate 38400 and Bus number are to set in the device bios menu

Setting in the Comserver for connection via RS 485:

Port: for example 8000

IP: for example 192.168.123.224

5.7.5. Communication via Cellular Network (GPRS)

The EVO 2.8 Pure can be equipped with a cellular network modem. It enables the communication via cellular network. The antenna is located in the connection compartment of the device and can optionally be replaced by an external antenna if reception is bad.
The SIM card is inserted via the connection compartment of the EVO 2.8 Pure.

Inserting the SIM-Card at the EVO 2.8 Pure.

Inserting the SIM-Card at the EVO 4.3/4.6.
Ins

ed. Take care that

For removing, the SIM card has to be pushed in a bit. After releasing it, the SIM card protrudes a bit and can be removed.

☞ **Note:**
We recommend to use T-Mobile or Vodafone as provider for mobile networks! Our experience shows that with other providers you have to reckon with more frequent dial-ups and thus delayed data transmission and possibly higher costs.

Information for M2M:
http://www.t-mobile.de/business/machinetomachine/m2m-im-einsatz/0,23219,26762-_,00.html

5.7.5.1. Communication state in the Display

The state of GPRS-/GSM-connection you can always see in the state bar on the display.
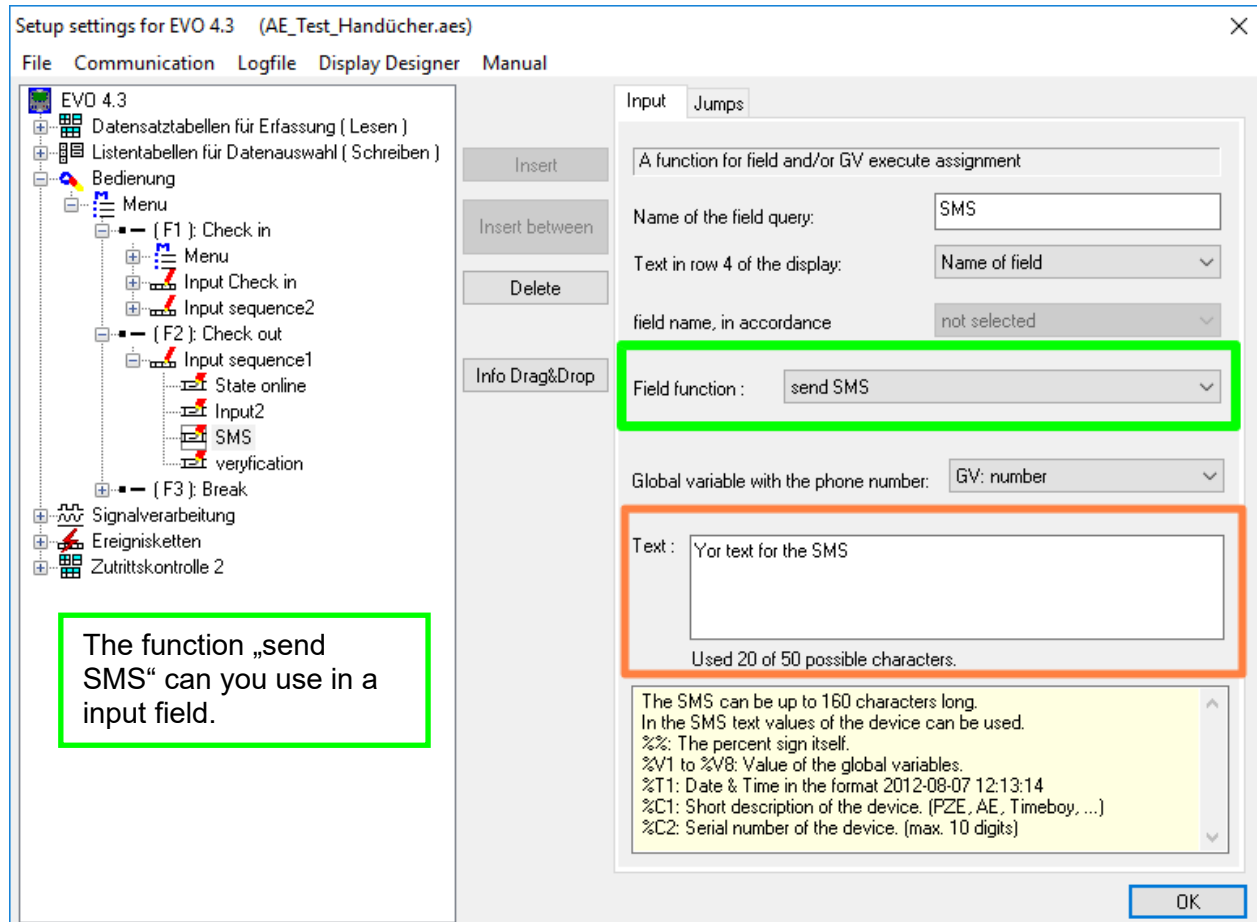
Pin	Bez.
0	Modem is off
1	Initialization of the software
2, 3	Start of the modem
4, 5	Initialization of the modem and SIM-card check
6	if PIN necessary, sending of the PIN
7	if PUK necessary, sending of the PUK
8	dilated initialization of the modem
10	Modem in standby mode
11	Call recognized
12	take calls
14	GSM connection activ
15, 16	GSM connection closed
20	GPRS Standby, Initialization of the GPRS connection after the first records
25	connection to Provider (Attach)
30	GPRS standby (waiting for next data/records)
31	Server (Open)
32	connect to server
33	send data to Server (HTTP)
34	Wait for quitting from server (HTTP)
35	recive data from server (TCP/IP)
36	send data to server (TCP/IP)
37	close connection
38	Braek between tries to connect the server, active mode
40	timeout after failed connection, to 15 minutes
41[1)	timeout after failed connection Provider, to 15 minutes.
42[1)	count of the connection attempt is end
43	on the Device is the encryption active, but not on the server
44	battery is down, to disable Modem.
45	impossible connect to the provider or Roaming impossible
50	close connection
55	Turn modem off

5.7.6. Communication via SMS

5.7.6.1. Send a SMS

With the EVO 2.8 Pure, it's possible to send a SMS. Condition for this is, an integrated GPRS-Modem (communication via Cellular Network). The main communication must be set on GSM or GPRS/GSM.
To send an SMS you must use the Field Function "send SMS" in the device Setup.

The maximum length of the SMS is 160 characters.
The text can integrated device value:
%%: The percent signs self.
%V1 to %V8: value of global variable.
%T1: date and time 2012-08-07 12:13:14
%C1: Short device description. (PZE, AE, TIMEBOY, ...)
%C2: Serial number of the device. (max. 10 Stellen) %1 für GV 1, %2 für GV2 usw..

The call number if you want send an SMS must be saved in a GV.

! Caution:
Enter the phone number always with a country code.
Example.: +49161458✱✱✱✱✱

The device can save 128 SMS. Then there is additional as follows to clear the oldest SMS.

5.7.6.2. Receive a SMS

The follows functions are possible:
- ► View the SMS on the display. The same action you find in the „DFCComSendMessage" or the answer via HTTP.
- ► to order an service connection (the same how in the HTTP- answer)
- ► start in the signal processing an input sequence
- ► Output an acoustic signal

Condition to receive a SMS is a KEY include in the device an in the text from the SMS.
The Key for the device can set in the GPRS/HTTP .ini file.
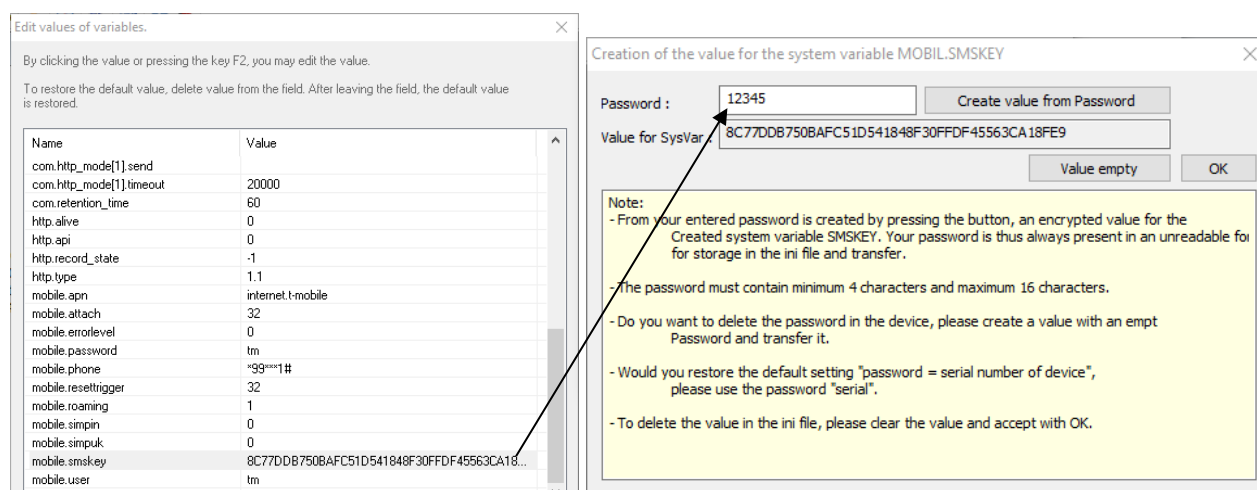
Text message
The keyword must be included in the SMS-text is:
message=text1↵ text line2 ↵ line3 etc.
&delay=10&key=12345

The 10, is the time how long to display the message.
After the character ↵ gives a line break (carriage return).
If not a key in the device, you can use the serial number as a key (default setting). Save you an empty Key, then receive the device every SMS. The last received SMS can you see in the Bios-Menu under „general information Bios (Menu)".

Service-connection (active-mode)
The content of the SMS is similar to that of HTTP-Answer from the WEB-Server.
Actually supported are 3 keywords: **service**, **host** and **port**. The keyword must follow
an "=" character with corresponding value. The individual fields are separate with the character "&".
With the KEY „**service=1**", open the device a Service-connection. The connection Parameters
(Host, Port) are saved in the "active.ini" file from the device.
An option is, to give the device the Parameters for the connection via SMS (→**host=**, **port=**). Then
use the device this parameters from the SMS and not the saved from the "active.ini" (active mode).

"**&service=2**"
Coution ! this funktion first supportet with the hardware version V4 GPRS(Mobilfunk) and FW 04.03.06.XX.
When using parameter 2, the service connection is established immediately.

Beispiele:
   a) **service=X**&key=12345
   b) **service=X&host=www.datafox.de**&key=12345
   c) **service=X&host=123.123.123.123**&key=12345
   d) **service=X&host=www.datafox.de&port=4711**&key=12345

a) Connection to the server with the saved parameters in the „active mode".
b) and c) Connection on Port 8000 to the server (www.datafox.de/123.123.123.123).
d) Connection to the server "www.datafox.de" and port "4711".

Start an input sequence in the device signal processing

The keyword, if you need in the SMS is:
ek=name&key=ja   (the name of the input sequence).

The name of the input sequence must match completely, otherwise it will not run.
Recieve the device an SMS with this text, then start the input sequence.

If save a SMS Key, the must include the SMS this Key (&key=ja).

With this are many different variants are possible.
Here some example:

Open a door via SMS.

check   open the door

SMS
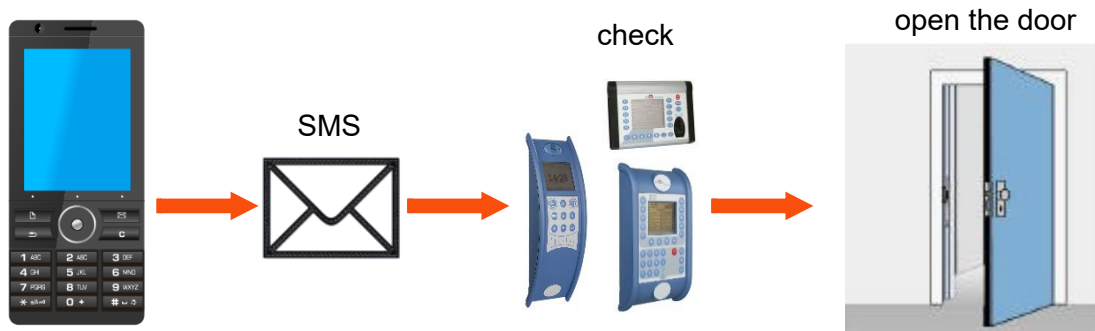
Control a technical system and send a SMS in trouble:

If the level of regulation from the system is not correct, then there is a report via SMS.
The Datafox MasterIV is not the regulator here. He gives only a report in trouble.
If necessary, a procedure also can be done.

Füllstand

oversize the level

Standhöhe

SMS from device to you

The Datafox-device switch on a pump.

SMS to the device

you can activate a action
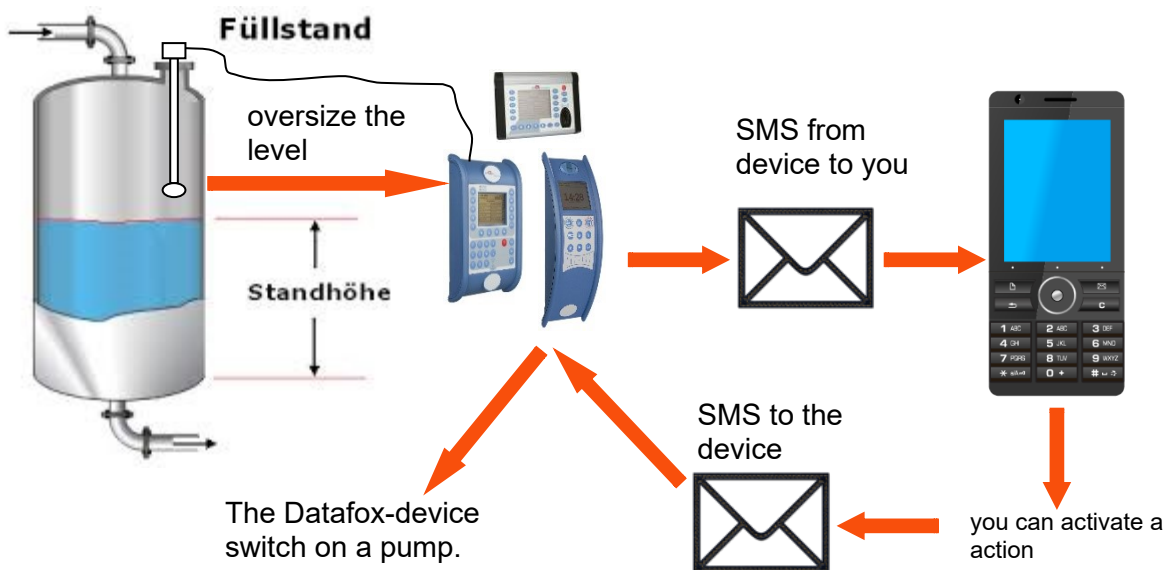
> **! Caution:**
> There is no 100% guarantee that a sent text message reaches the receiver. This is only an example which is intended to represent the possibilities.

5.8. Connection and wiring of the access control

5.8.1. Configuration and structure of the Access control

The basis of the access control II are tables. They store all information about the hardware configuration of the access control system, access right of the employees, periods of time (activation, blocking times, holidays,...). The tables are connected as follows:
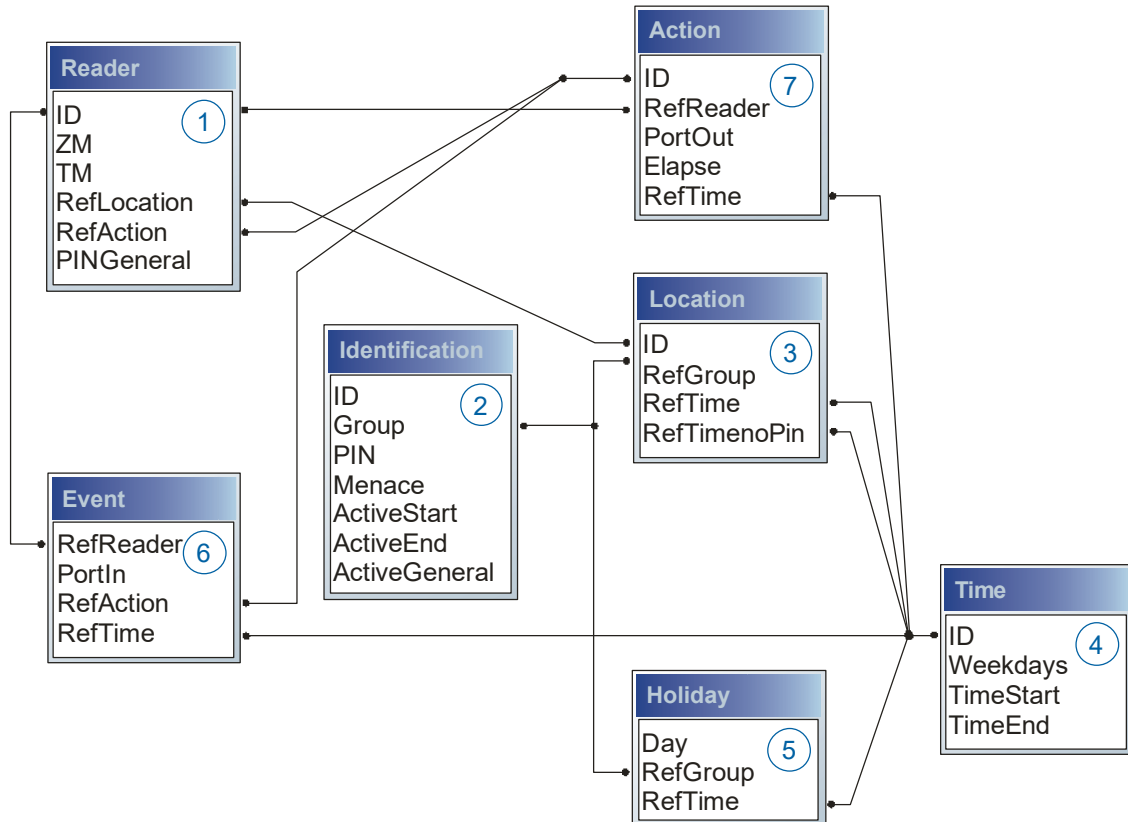
The tables are created as text files. For an easier administration you can add comments within the files.

When adding comments, you have to notice that in a comment line no field values can be given and that the comment line has to start with a semicolon.

The table Reader.txt might look like this:

ID	ZM	TM	RefLocation	RefAction	PinGeneral
1	1	320	0	1	0
2	1	000	1	2	0
3	1	010	2	3	0

Holiday Control

It is now possible for ZK-II to consider holidays at switching the relay. In order to achieve compatibility with older versions, the function consider Holidays for the Time Control of Relays has to be activated at the setup page Access Control 2. In the column Group, you specify the Action ID of the switched relay output instead of a Group ID. Thus, it is not necessary to alter the table structure of the holiday list. The column RefTime provides the time model applicable that day. A minus sign must be inserted in front of the Action ID in order that the MasterIV terminal can differentiate between Action ID and Group ID. As a result, these Action IDs must be three-digit numbers.

Example:

Action

ID	RefReader	PortOut	Elapse	RefTime
1	10	1	25	0
2	11	1	25	0
3	12	1	0	0

Holiday

Day	RefGroup „Action-ID"	RefTime
2012-05-01	1	3
2012-05-01	2	4
2012-05-01	-3	5

In the action list above, the door module with the ID 12 was assigned the time model 2 which switches port 1 of the module. If separate holiday control has been activated in the setup, time model 2 is not applied to the relay output at May 1, 2012, but time model 5.

Extended Parameterization ZK-II

The value range of the parameter 'ActiveGeneral' has been extended by the value 8. Additionally to the general permission (value 9), a PIN request is executed - if defined so for the user and activated for the reader. Furthermore, at both configurations of the ID cards with the ActiveGeneral value 8 and 9, the validity period of the ID card is checked.

For ZK-II the operation modes online, offline or online/offline after time-out are available. In online mode, configuration lists stored in the device are not considered. A data record is read from the server, analyzed and an action triggered. In offline mode, the configuration lists of the terminal are used to grant or deny access to a person. Online / offline after time-out is a combination. If the server is unavailable, the terminal can decide on basis of its lists whether to grant access to a person or not.

Timing of the Digital Outputs for the MasterIV Device Series:

It is possible to time the digital outputs of the MasterIV device series via tables. Thus, for example turning down the heating system at night, a buzzer control and much more can be realized.
Switch Relays via time table:

The following tables must be configured:
  ►Action
  ►Reader
  ►Time

Description:

Each action that is to be activated must be entered in the table Action. The table Action refers to the tables Reader and Time. In the table Reader the module is provided on which the relay or the Open Collector is to be switched. The reference to the table Time indicates when the switch is to be done. If start and stop time are entered, the relay is switched on when exceeding the start time and switched off when exceeding the stop time. The entry of the duration Elapse in the table Action is ignored. If the relay is only to be activated for a few seconds, e.g. for a buzzer control, the stop time has to be set on "'00 : 00'". If the start time is exceeded, the respective output will be switched for X seconds (RefTime in Action table). The entry Elapse in the table Action now indicates the on-time.

Example:
  ► A buzzer is to be activated for **3** seconds from Monday to Friday at **10.00** am and 4 pm (**16.00**). The buzzer is controlled by the internal relay of the PZE-MasterIV.
  ► The heating system is to be set to the "'day mode'" at **07.00** am and to the "night mode" at 7 pm (**19.00**) on all weekdays. The corresponding relay is at the door module with the bus number **2**.

Reader.txt

ID	ZM	TM	RefLocation	RefAction	PinGeneral
1	1	320	0	0	0
2	1	020	0	0	0

Time.txt

ID	Weekdays	TimeEnd	TimeEnd
3	12345	**10:00**	00:00
4	12345	**16:00**	00:00
5	1234567	**07:00**	**19:00**

Action.txt

ID	RefReader	PortOut	Elapse	RefTime
6	1	1	15	**3**
7	1	1	15	4
8	2	1	0	5

5.8.1.1. Description of Tables for Access Control 2

Table **Reader** (List of all devices installed in the system)

Name	Data type	Length	Description
ID	Number (int)	4	Unique Key (value>0) of the Reader table.

ZM	Number (int)	4	In our example, it has number 1. If there are several PZE-MasterIVs in an access system, they can be depicted in one table connection and it is not necessary to have a separate string for each PZE-MasterIV. If several RS485 bus lines are used on a device, each additional line must be entered with Master ID + 1.
TM	Number (int)	3	Contains two information in one number. Both figures on the left (010) indicate the bus number of the door module, the figure on the right (010) contains information about the type of connection. A 0 means a connection via RS485, a 1 stands for a connection via RS232 or RS485 as stub.
RefLocation	Number (int)	4	Indicates which room is supervised by the reader.
RefAction	Number (int)	4	Indicates which action is worked through after a successful check.
PinGeneral	Number (int)	8	Can contain a numerical sequence by which a person without a card gets access.

Table **Identification** (list of all devices installed in the system - master and door modules)

Name	Data type	Length	Description
ID	Text (ASCII)	20	Contains the ID card no. which is read at the TMR33 device or terminal. An ID card can occur several times (is assigned to several authority groups).
Group	Number (int)	4	Assigns the ID card to an authority group.
Pin	Number (int)	8	Activates a PIN request if not equal 0. Please note that a PIN must not start with zero. 0815 would be invalid.
Menace	Number (int)	4	Activates (if not equal 0) a "'menace-PIN'" that can be added to the PIN. If entered, the system sends a data record that can be analyzed by software developed for this purpose and sets off the alarm.
ActiveStart	Text (Date)	10	The tag entered here indicates the start date of the validity of the ID card. (for example 2007-07-12 = yyyy-mm-dd)
ActiveEnd	Text (Date)	10	The tag entered here indicates the end date of the validity of the ID card. (for example 2007-07-12 = yyyy-mm-dd)
ActiveGeneral	Number (int)	1	Activates or deactivates this card record. 0 = card blocked 1 = card active 2= virtual card (use only via DLL) 3 = access only by entering the PIN; field ID are now only a PIN for access. 4 = pin = threat code i.e. the threat code is used instead of the Pin entered. 5 = The value for Duress / threat code is not transferred to the PIN adds up to form the threat code (ex: Pin = 1234, Duress = 1 -> threat code = 1235; Pin = 1234, Duress = 6 -> threat code = 1230) 6 = permanent opening for U & Z cylinders 7 = Burglary alarm system, allowed to switch on/off 8 = general authority (with PIN request) 9 = general authority (no PIN request)

Table **Location** (defines which card groups get access to which room at which time)

Identifier	Data type	Length	Description
ID	Number (int)	4	ID of the room. All other tables refer to this data line via this number, if necessary.
RefGroup	Number (int)	4	Reference to the identification table. Labels the access authorized group. All cards of this group have access to this room.
RefTime	Number (int)	4	The time model in which authorized persons get access. (0 = not used)
RefTimeNoPin	Number (int)	4	The time model for which entering an additional PIN is not necessary (at peak times etc.).

Table **Time** (grouping of single time zones (weekday from to) as a time model number)

Name	Data type	Length	Description
ID	Number (int)	4	ID of the time model. All other tables refer to this data line via this number, if necessary.
Weekdays	Number (int)	7	Indicates the weekdays on which the following period of time should be applied (form: 7 digits at most 1-7 e.g. 134567 = Monday, Wednesday till Sunday)
TimeStart	Text (Time)	5	The start point for the period of time. (form: 24h HH:MM)
TimeEnd	Text (Time)	5	The end point for the period of time.

Table **Holiday** (setting blocking days like holidays or company holidays)

Name	Data type	Length	Description
Day	Text (Date)	10	Date of the blocking day. (form: YYYY-MM-DD)
RefGroup	Number (int)	4	Indicates the authorization group to which the blocking day is applied. Zero defines a global validity for all groups.
RefTime	Text (Time)	4	Indicates the assigned time model. (0 = not used) During this time access is granted. Thus, also "'half holidays"' like New Year's Eve can be realized.

Table **Event** (assigning an action to a signal at the digital input)

Name	Data type	Length	Description
RefReader	Number (int)	4	Module (door module or master) where the digital input is.
PortIn	Number (char)	1	Number of the digital input on the module. Possible values: 1 ... 9 & A ... W corresponds to port 1-32 (digital in)
RefAction	Number (int)	4	Reference to the action that should be carried out (e.g. switch relay).
RefTime	Number (int)	4	The time model which indicates when the digital input is checked. (0 = not used).

Table **Action** (list of all workable actions in the access control system; an action group, i.e. all actions with the same action number, can switch several relays)

Name	Data type	Length	Description
ID	Number (int)	4	Action number, it can occur several times due to several actions that have to be worked through.
RefReader	Number (int)	4	Module (door module or master) on which an output(relay) is switched.
PortOut	Number (char)	1	Indicates the number of the output on the module. Possible values: 1 ... 9 & A ... W corresponds to port 1-32 (digital out)
Elapse	Number (int)	3	The duration of the switching of the relay (0 = permanently). Unit 200 ms
RefTime	Number (int)	4	The time model indicates when the output may be switched. (0 = not used) This is a function to switch relays directly via time (table) Please not mix this function with the normal access actions. !!! By a time-table setting "1234567 00:00-23:59" is the relay permanent on.

5.8.2. Access-control with Intera 2

The following hardware is available to set up an access control intera 2 modules. The devices can be combined in different ways according to their hardware requirements.

EVO 2.8 Pure

If the device MasterIV is used for access control, door supervision or remote monitoring, one device can supervise up to 8/16 doors.

EVO Intera

with PIN and without PIN
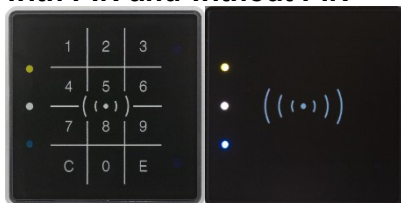
dimensions: 81 x 81 x 19 mm (wxhxd)
The EVO Intera access reader can be used with 125 kHz, Legic or Mifare. It is available for in-wall or on-wall mounting with or without keyboard. Each reader has a sabotage recognition, three lamps for visualizing the state, a buzzer for the acoustic signaling and a proximity sensor.
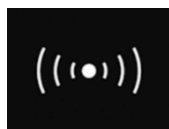
Backlight signaling:
Glowing white = reader ready for use
Flashing white = reader not recognized
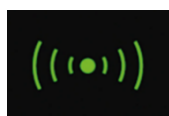
Backlight signaling:
green = access allowed

Backlight signaling:
red = Access denied or reader is currently being configured by the master. Or Reader was recognized but not entered in the reader.

LED – Yellow RFID-Tac in the field

LED – white = sleepmode (deactivatet via proximity sensor.)
LED – off -> reddy to read and the background LED is on.

LED – **Blau** (no function)

Anschlussbelegung:

Anschlussbelegung

PTSM 5-polig   DIP switch   PTSM 4-polig   Mikro-USB
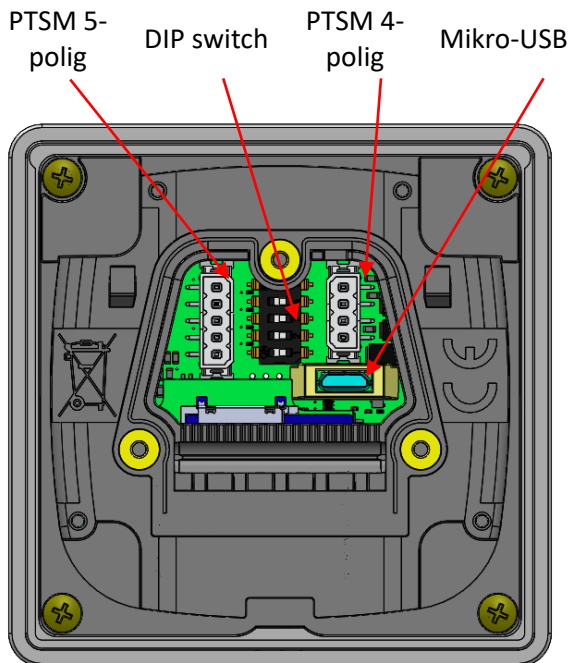
Anschluss an die PTSM Steckverbinder
Connection to the PTSM connector

The EVO Intera II is supplied with the 4-pin or 5-pin mating connector for connecting the reader. These are protected against polarity reversal and are supplied by Datafox with printed assignment.

Stecker 4 polig

10-30V DC

RS485-B

RS485-A

GND

Stecker 5 polig

DGND

D IN1

Relais
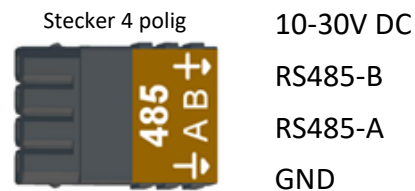
DIP - Schalter	Off	On
1 – Adresse Bit 0	+ 0	+ 1
2 – Adresse Bit 1	+ 0	+ 2
3 – Adresse Bit 2	+ 0	+ 4
4 – Adresse Bit 3	+ 0	+ 8
5 – end resistor 120R	no-activ	activ

Beispiel	5-4-3-2-1
Adress 2, with active end resistor	1-0-0-1-0
Adress 3, no active end resistor	0-0-0-1-1
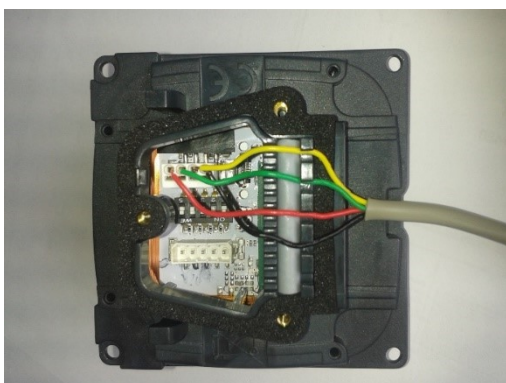
wiring
The EVO Intera II has an integrated cable comb to accommodate single wires up to d=1.5mm incl. suspension for strain relief. Lay the cores as shown.

Settings for proximity sensor:

The proximity sensor are on rigth side on the reader:
The settings are include in the SW DatafoxStudioIV
Configuration -> proximitiy-sensor:
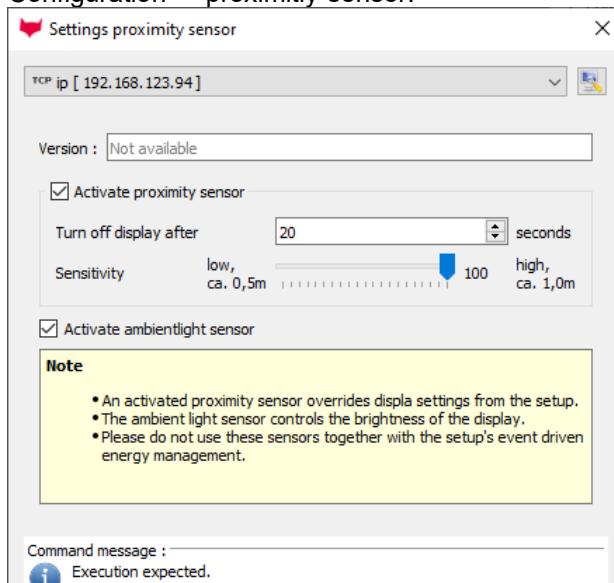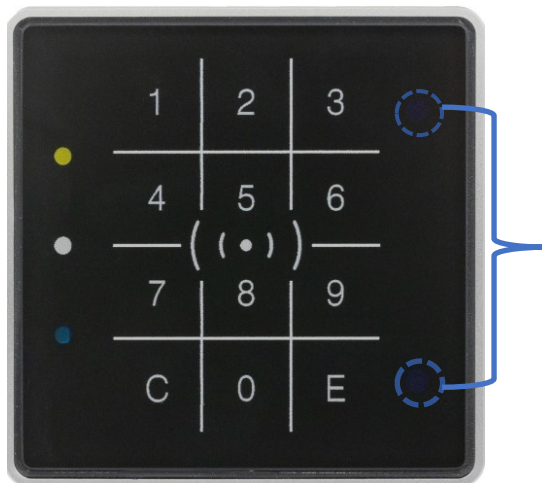
example Reader Table,:

ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	1	1	0	Leser an RS485 Modulplatz 1 = Bus ID 1
4	1	320	0	1	0	ZK-Box V4 (Mastergerät)

wire plan for one reader, Intera 2:

Bus Nr. 1
EVO-ZK-Leser

plug 4 poles
for access

Uv >max. 200 m bei 0.6mm^2

plug 5 poles
digital in-/output

+ **-** max. 30V; 2A
Power supply for door electic door opener
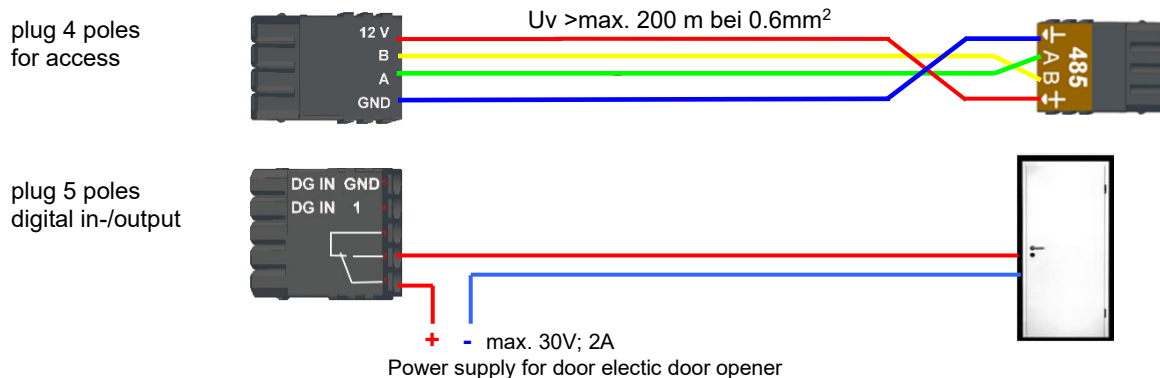
5.8.2.1. EVO Intera II, Individual settings

The mask for setting the EVO Intera II configuration can be accessed in the Datafox Studio via the configuration menu:
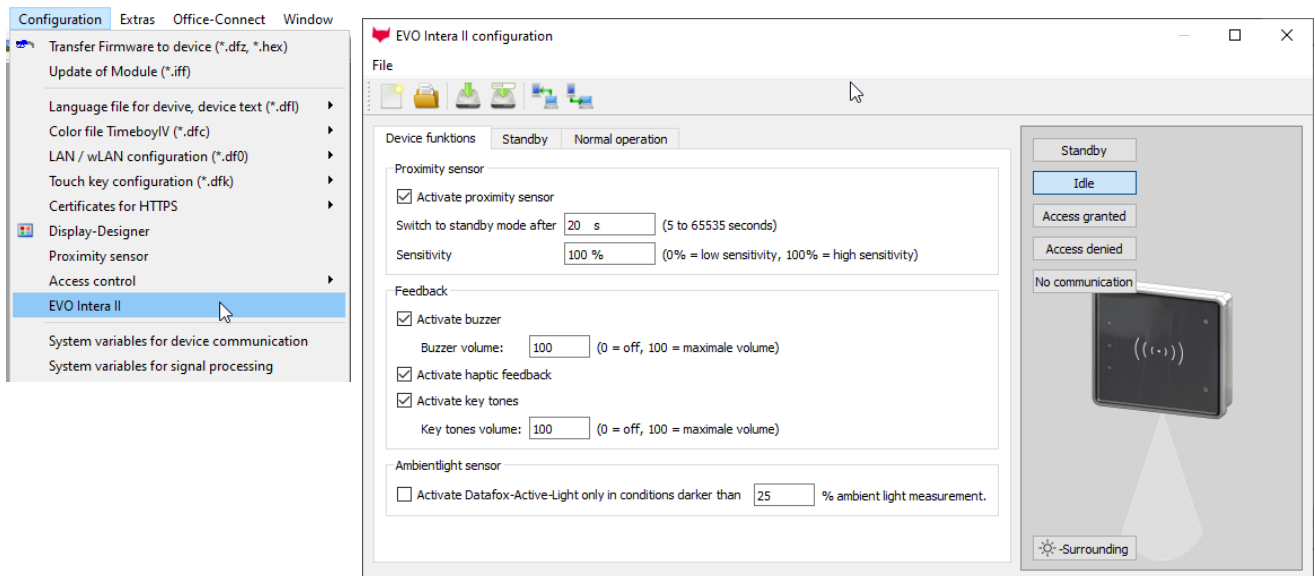
The mask allows setting / adapting the behavior of the EVO Intera II. These settings are divided into 3 areas:
- Configuration of the device sensors and actuators (device functions tab))
- Configuration of the standby configuration (sub-configuration of the proximity sensor)
- Configuration of normal operation (Standard Operation tab)

In addition, a preview of the reader signaling is shown based on a selected operating status.

5.8.2.2. Functionality of the EVO Intera II

The EVO Intera II is an RFID reader for use in access control. As such, it is designed for operation on an RS485 bus and uses the phg_crypt communication protocol, which is used as a de facto standard in large parts of the industry.

The reader differs from many competing products in terms of its features:
- It can project indirect lighting
- It has sensors for ambient light and proximity detection.
- It can be used as a pin reader and then generate haptic feedback in addition to the acoustic feedback.

The EVO Intera II also has three programmable LEDs on the left. Functions can be assigned to these LEDs, such as signaling an ID in the field of the RFID reader or a person nearby. There are also other functions such as permanently on / off or switched by the access controller.

The Datafox Studio dialog described in this chapter is used to set up these features. The configuration is transferred via the USB interface of the reader.

5.8.2.3. Global function

From left to right, the mask offers functions for

- Creation of a new standard configuration
- Reading in a configuration file
- Save the configuration file
- Save the configuration file under a new name
- Transfer of the configuration file to an EVO Intera II
- Reading the configuration file from an EVO Intera II

These actions are also available from the File menu.

5.8.2.4. Einstellung der Gerätefunktionen
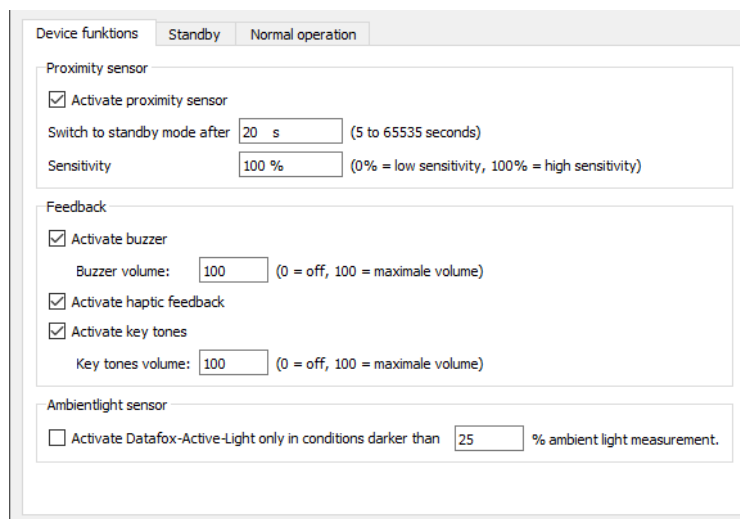
The EVO Intera II has a proximity sensor - if this is activated, the standby lighting can be set. The standby mode is activated if no person is detected in the vicinity of the reader for an adjustable period of time (20 seconds as standard).

Depending on the structural situation, it may be necessary to limit the sensitivity of the proximity sensor, for example if it is used in narrow aisles and the opposite wall is supposedly recognized as a person nearby.

As feedback are next to the
• Buzzer for access events still
• Haptic and sound feedback ready for PIN readers.

You can set the maximum volume for all acoustic feedback so that the reader can also be adapted to quiet office environments.
The reader can adjust its brightness - e.g. in order not to shine too brightly at night - to the brightness of the surroundings. If this function is desired, activate the ambient light sensor.

5.8.2.5. Settings for standby
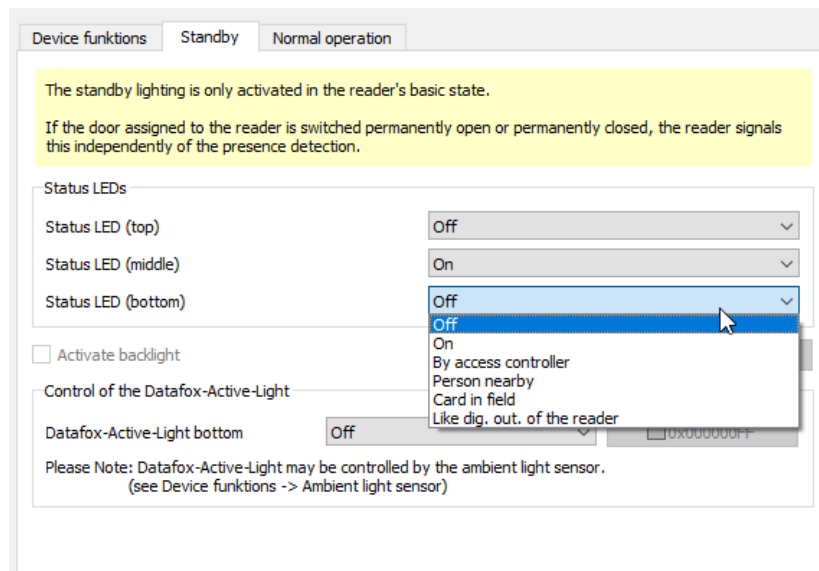
The standby mode of the EVO Intera II is activated if the proximity sensor has not detected a person in the vicinity for an adjustable period. In this operating mode, the 3 LEDs can be assigned functions that differ from the normal operating mode. In addition, the Datafox Active Light can be switched if it is built into the reader.

5.8.2.6. Setting for standard operation
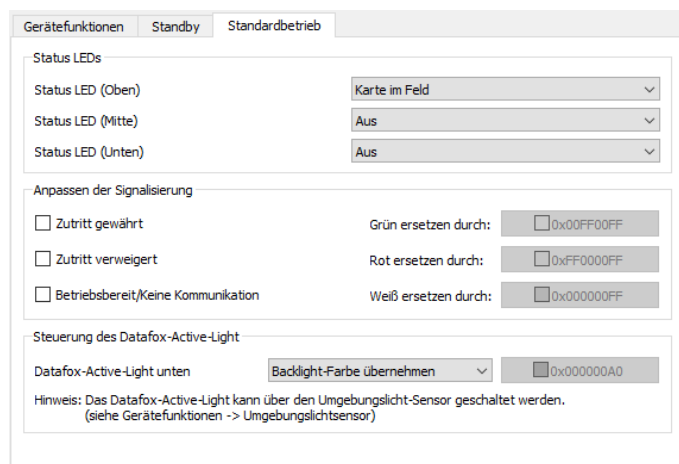
In standard operation, the EVO Intera II fulfills the normal functions of an access reader - the reader is controlled via the access bus by an access controller. In the simplest case, the reader transmits the read RFID data to the access controller and is then switched to access granted ("green") or access denied ("red"). If no access signaling is active, the reader normally lights up white.

In addition to assigning functions to the three programmable LEDs, you can adjust the colors used for green, red and white. You can also - if built into the device - set the color and brightness of the Datafox Active-Light.

5.8.2.7. Preview of reader behavior

An EVO Intera II is shown on the right-hand side of the configuration mask. This changes - based on the currently loaded configuration - its appearance. Use one of the five buttons to select the operating status to be displayed.
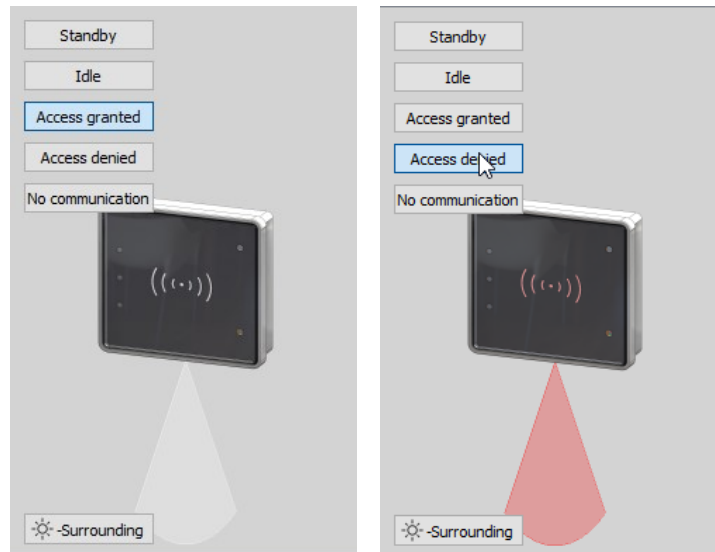
„Zutritt gewährt" und „Zutritt verweigert" mit Datafox Active-Light im Modus „Backlight-Farbe übernehmen"

You can use the button at the bottom left in the preview area to explicitly switch the reader to day or night operating mode.

5.8.2.8. Transfer to the device

To transfer to or from a reader, please connect it to your PC via USB. After pressing one of the buttons for transfer, you will see the file transfer dialog of the Datafox Studio:
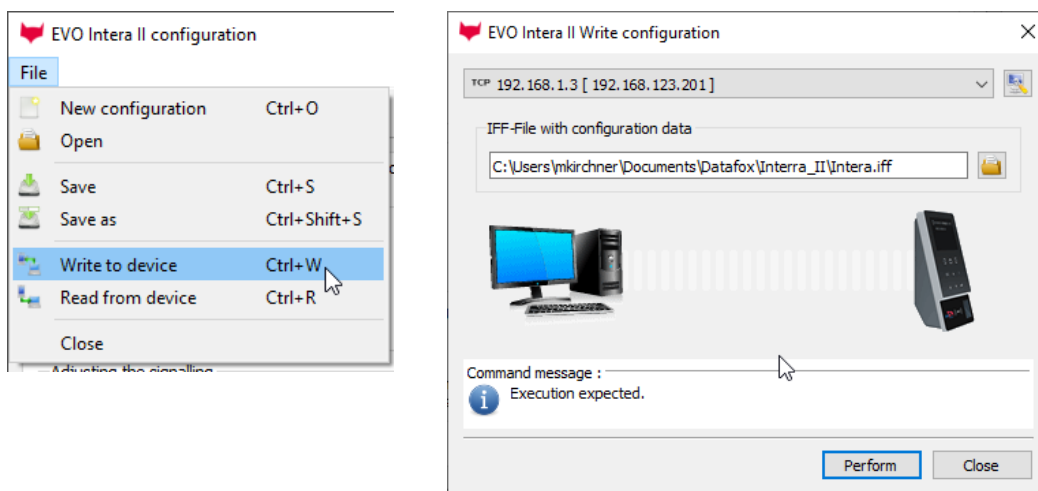
Here you can select the configuration file to be transferred - the version opened in the editor is the standard assignment of the transfer dialog via the transfer button to the device. By pressing the "Execute" button, the configuration file is transmitted to the reader (or read from there).

5.8.3. Access control II with PHG-Modules

The following hardware is available to set up an access control with PHG modules. The devices can be combined in different ways according to their hardware requirements.

EVO 2.8 Pure

If the device MasterIV is used for access control, door supervision or remote monitoring, one device can supervise up to 8 doors and control 12 doors at most.

VOXIO & (T-Z)

Flush-mounted: 81 x 81 x 11 mm (WxHxD)
Surface-mounted: 81 x 81 x 40 mm (WxHxD)

The VOXIO can be used with Legic or Mifare. It is available for in-wall or on-wall mounting with or without keyboard. Each reader has a sabotage recognition, three lamps for visualizing the state and a buzzer for the acoustic signaling.

Relino & Relino B

50 x 50 x 43 mm (WxHxD)

The RELINO (B) reader can be used with Legic or Mifare. It is available for in-wall mounting. Each reader has three lamps for visualizing the state and a buzzer for acoustic signaling.

Siedle

100 x 100 x 20 mm (WxHxD)

The Siedle reader can be used with 125 kHz, Legic bzw. Mifare. It can be mounted in the Siedle Vario 611 housingsand is available with and without keyboard. Each reader has three lamps for visualizing the state and a buzzer for the acoustic signalling.

IO-Box

51 x 48 x 22 mm (WxHxD)
The I/O box as equipment for the RFID wall reader or RELINO reader has two digital inputs and two digital outputs. The I^2C bus is used as interface.

From firmware
version of the access reader 69806D of the PHG readers the autologin function for Mifare is supported. Here for 5 of the max. 6 keys can be used in the setup.

> **Attention:**
> Technical data for the PHG access modules can be found on the Datafox DVD or in our download area. Please note the power consumption of the modules and the voltage drop at long cable lengths.
> The responsibility for calculating the maximum cable lengths lies with the installer.

5.8.3.1. Connecting of PHG-reader

In order to connect the PHG modules, please note the PHG documentation on the Datafox CD:
    <Datafox-Geräte- Datafox-Zutritt-Module PHG *.pdf>

In the PHG documents for the single modules, the pin assignment and configuration via the DIP switches are described. In order to carry out an access control with theEVO 2.8 Pure the option "'access"' has to be integrated (Datafox art. no. 105201). The following figure shows the possibilities for connecting the PHG devices to a. The following figure shows the possibilities for connecting the PHG devices to a EVO 2.8 Pure for access control.
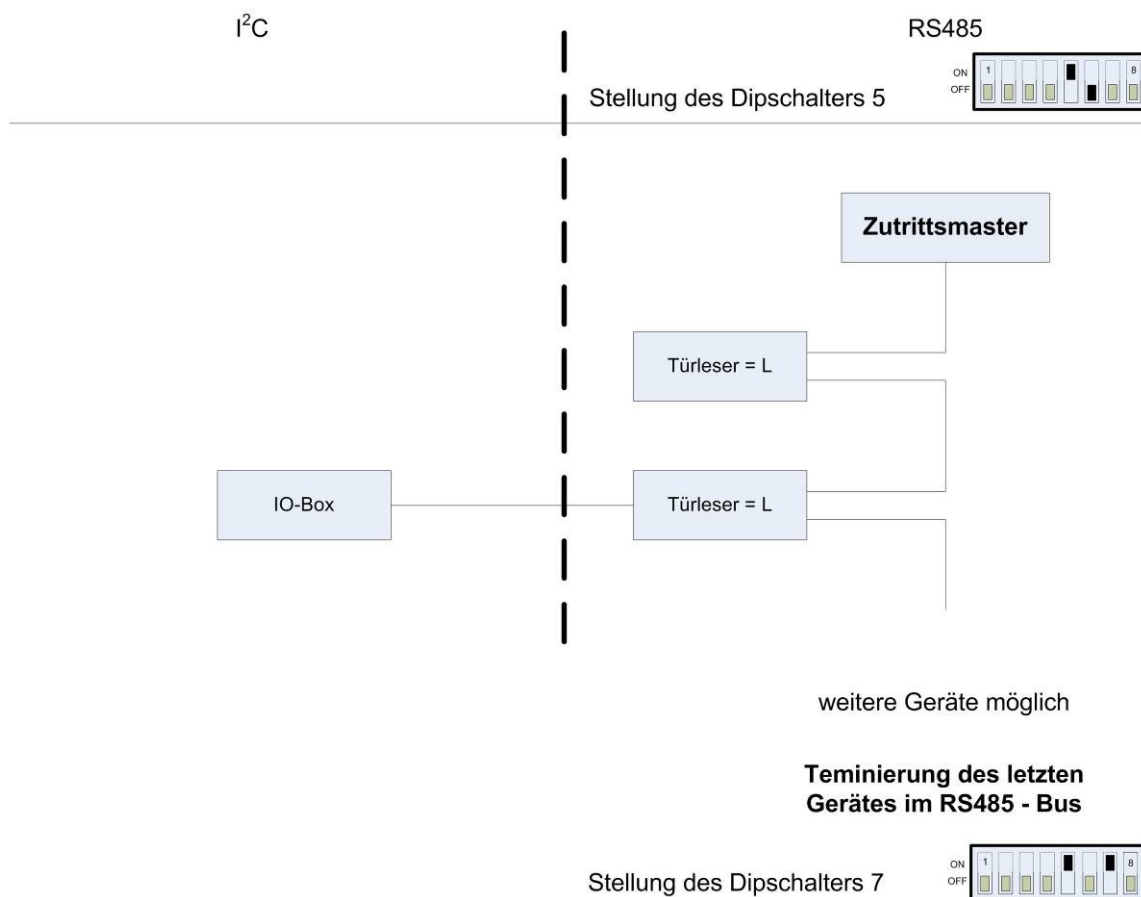
The bus number of the module is set via the DIP switches 1 - 4. The DIP switch 5 always must be set to "ON". The DIP switches 6 and 8 always must be set to "OFF". With the DIP switch 7 = "ON" the RS485 bus is terminated at the last module, otherwise always "'OFF"'.
If a door-opener is to be controlled additionally via a relay, the IO-box must be used.
With the IO-box two digital outputs as relays are available.

Connection example one door and I/O Box:

Reader   I/O-Box

RS485
max. 1000 m

I²C
max. 5 m

floating relay
contact

Reader   I/O-Box

Power supply 12 V DC for reader

-   +   3A

12 V
B
A
GND

ST 1

ST 3

I²C   max. 5m
ISTY 2x2x0,8

+ /
~
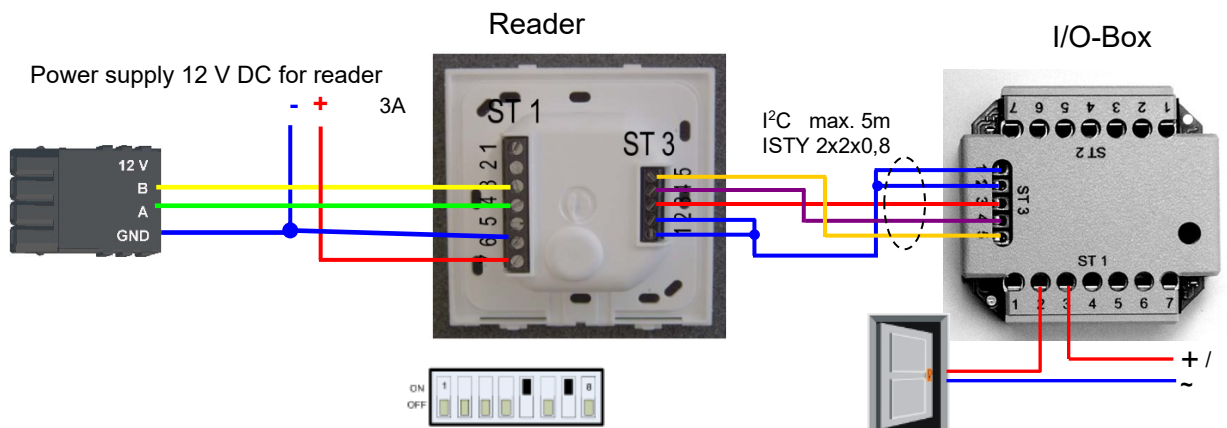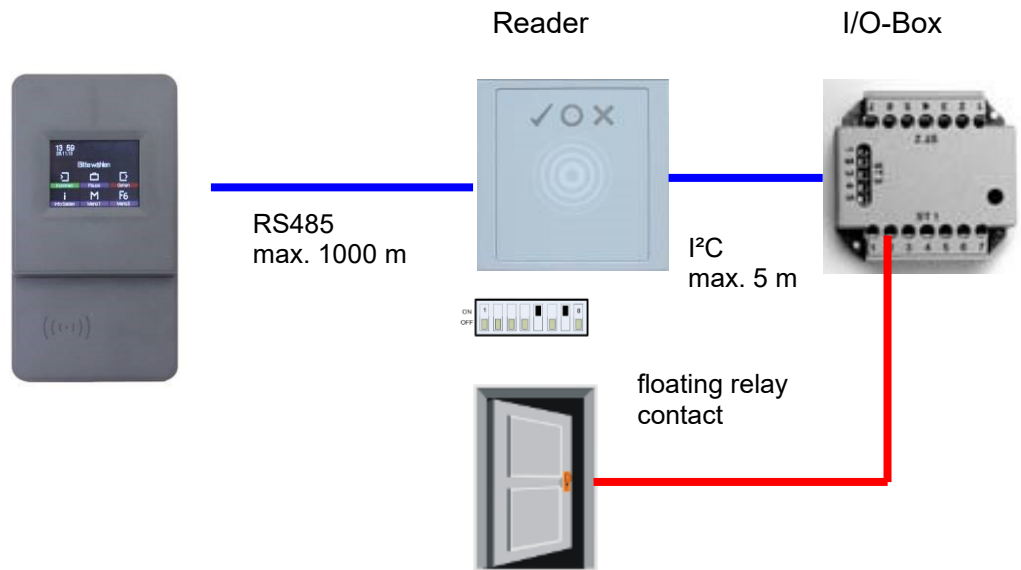
Connecting example with one door and without I/O-Box:

RS485

TCP/IP

Türöffner

Busadresse

Wire plan:

ST 1

ST 3

12 V
B
A
GND

max. 30 V; 2A
Power supply for door opener

DG IN GND
DG IN 1

Bus Nr. 1
Siedle-access reader
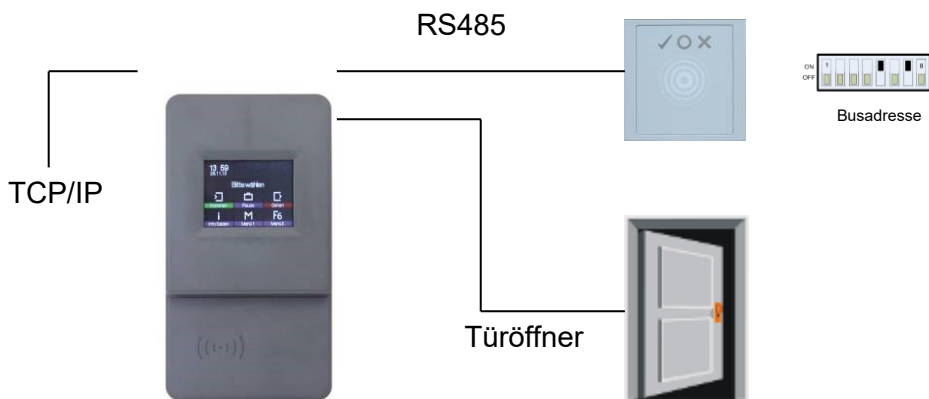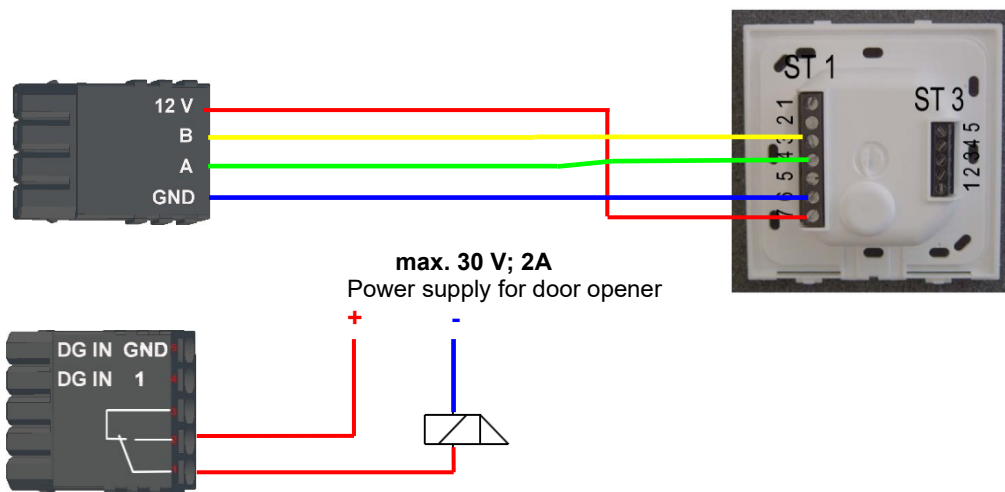
Wire plan for Siedle access reader:

Power supply 12 V DC for reader
3A

12 V
B
A
GND

DG IN GND
DG IN 1

+   **-** max. 30V; 2A
Power supply for door opener
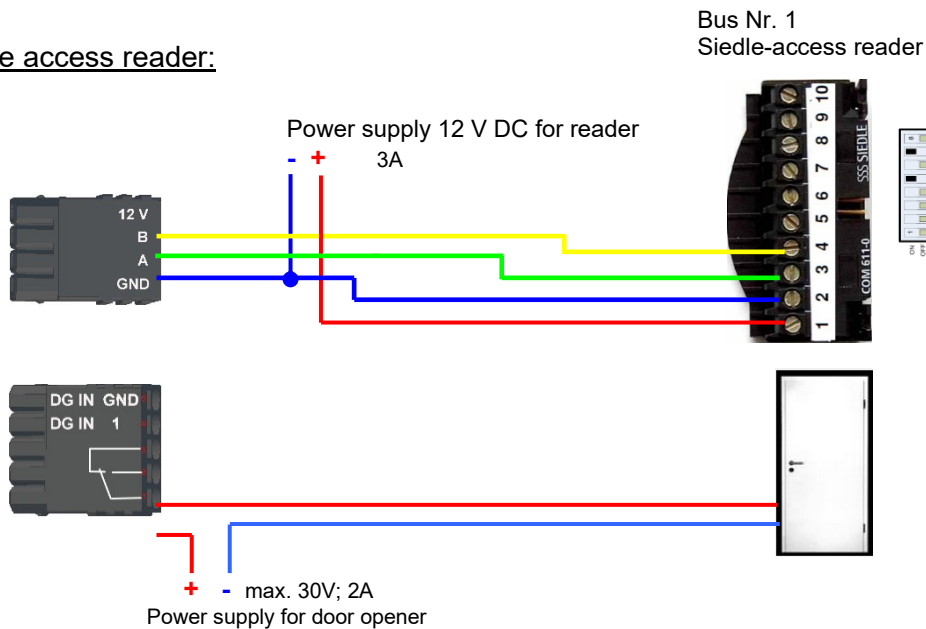
Wiring plan for a PHG Relino-B-reader:
! The reader type is supported as of FW 04.03.09.17.

PHG reader Relino-B

Power supply 12 V DC for AC-reader

- + 3A

12 V
B
A
GND

DG IN GND
DG IN 1

+ - max. 30V; 2A
Power supply for door opener
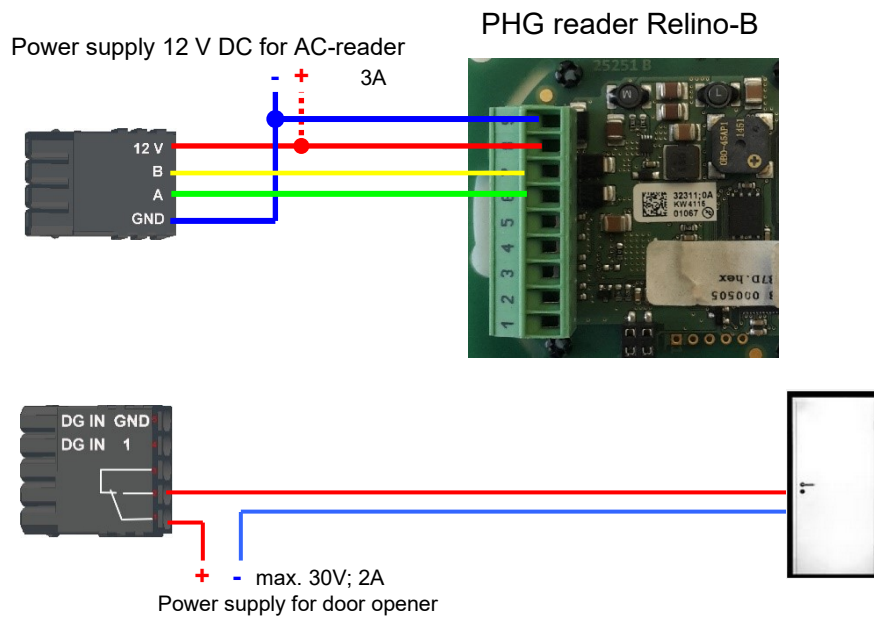
Wiring plan for a VOXIO-T-Z reader:
The reader type is supported as of FW 04.03.12.xx

PHG reader VOXIO-T-Z

Power supply 12 V for DC AC-reader

- + 3A

12 V
B
A
GND

DG IN GND
DG IN 1

+ - max. 30V; 2A
Power supply for door opener
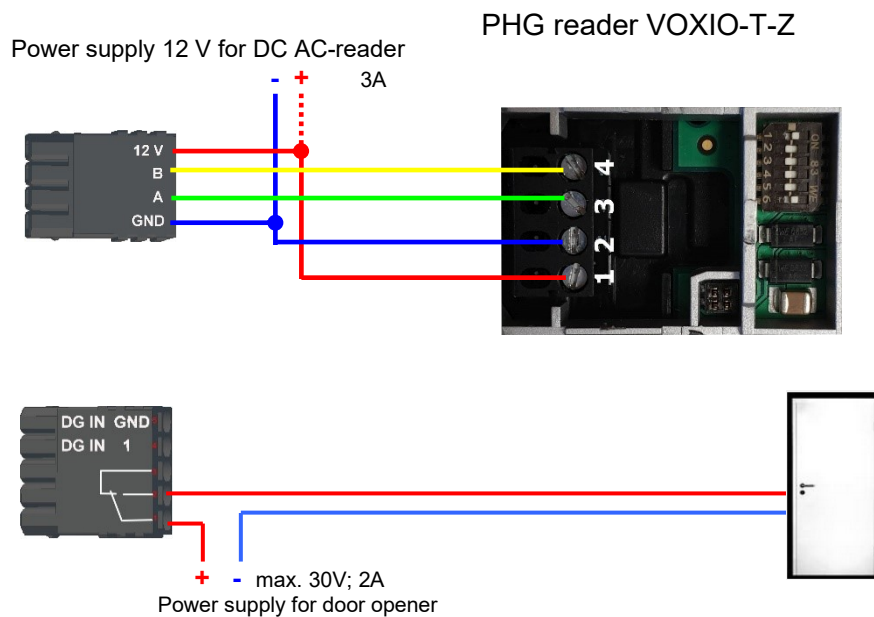
RS485 bus diagram for access control with 3 PHG-modules:

TCP/IP and
AC 100-230 V

DIP-switch setting

12 V DC

RS485

Reader 1

I²C
max. 5 m

potential-free
contact for door

RS485

Reader 2

I²C
max. 5 m

potential-free
contact for door

RS485

Reader 3

I²C
max. 5 m

potential-free
contact for door

more reader

Last reader
end resistor
switch 7 → on

last reader
max. 1000 m
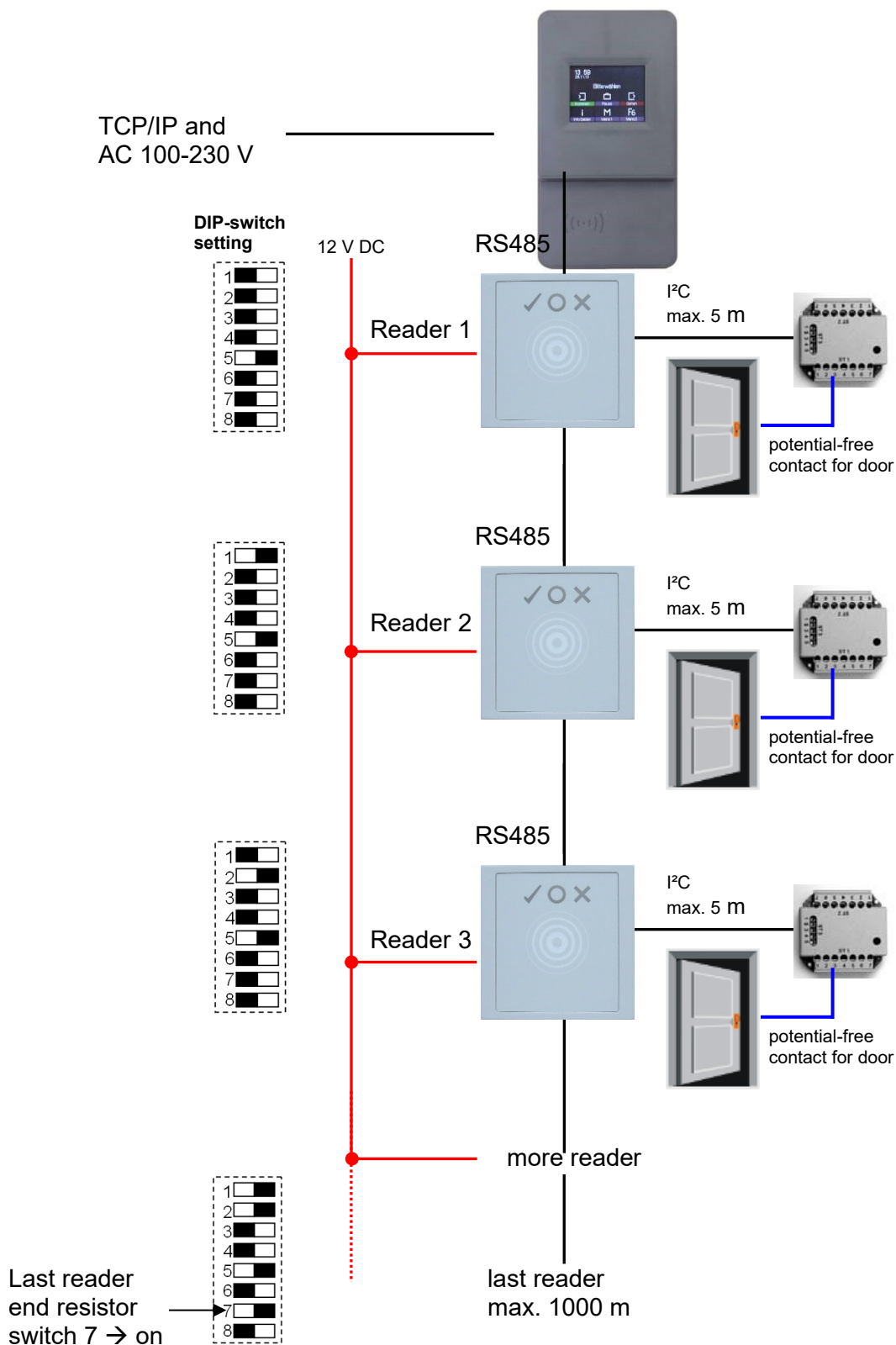
Wiring plan for several PHG-reader:

supply
12V 3A/DC
+   **−**

I²C   max. 5m
ISTY 2x2x0,8

Door opener

+ / ~
− / ~

I²C   max. 5m
ISTY 2x2x0,8

Door opener

+ / ~
− / ~

I²C   max. 5m
ISTY 2x2x0,8

Door opener

+ / ~
− / ~

+   GND   A B
further reader
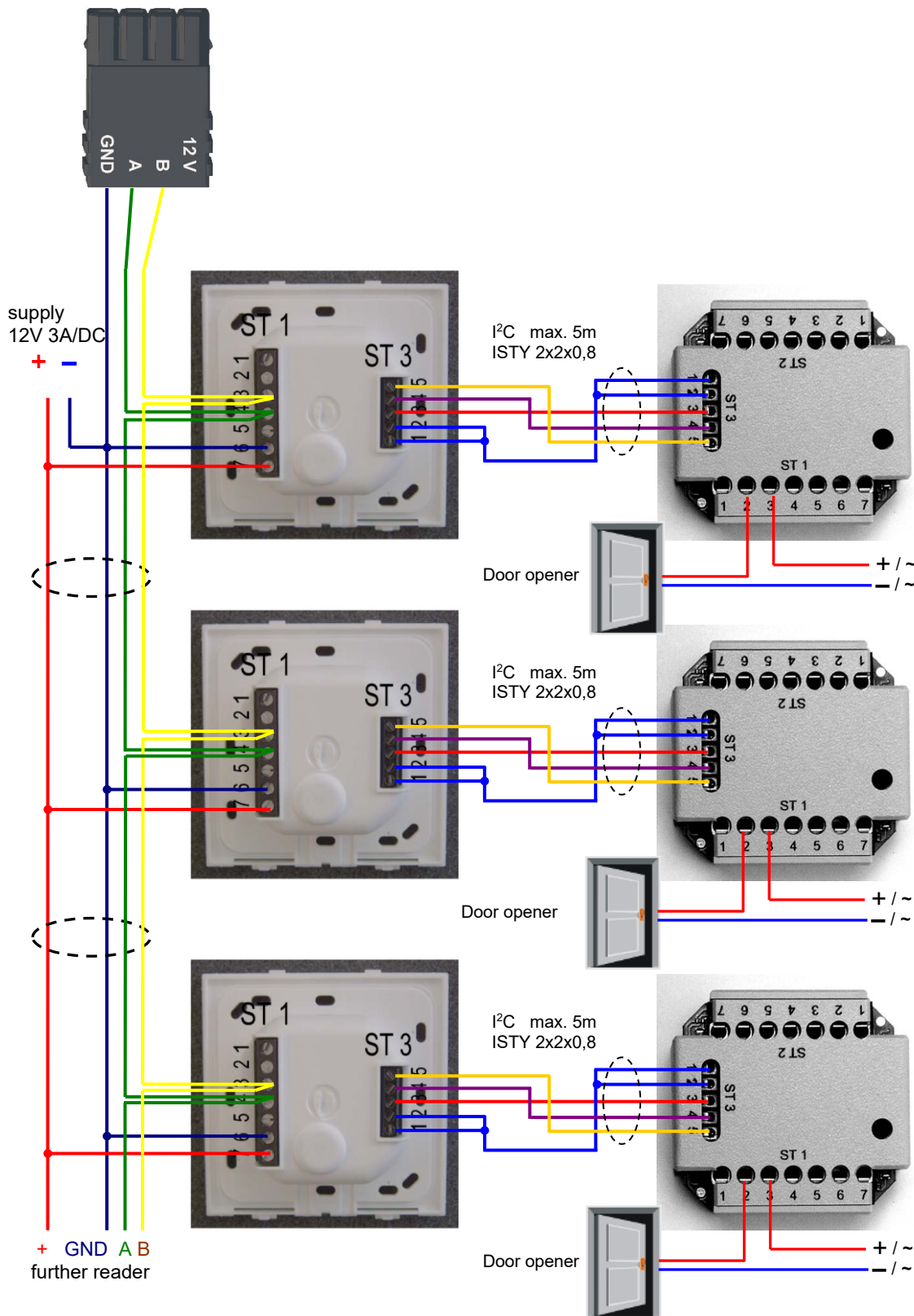
In any case, a protection circuit should be integrated when connecting the door-opener.
A freewheeling diode for DC and an RC element for AC.

Connecting the IO-Box:

Anschluss (ST1,2,3)	Klemme Nr.	Beschreibung
ST1	1	Relais 1→ normally close
	2	Relais 1→ common
	3	Relais 1→ normally open
	4	free
	5	free
	6	digital in 1 Signal
	7	digital in 1 ground
ST2	1	Relais 2→ normally close
	2	Relais 2→ common
	3	Relais 2→ normally open
	4	free
	5	free
	6	digital in 2 Signal
	7	digital in 2 ground
ST3	1 und 2	ground
	3	U+ 8…..30V
	4	SCL
	5	SDA
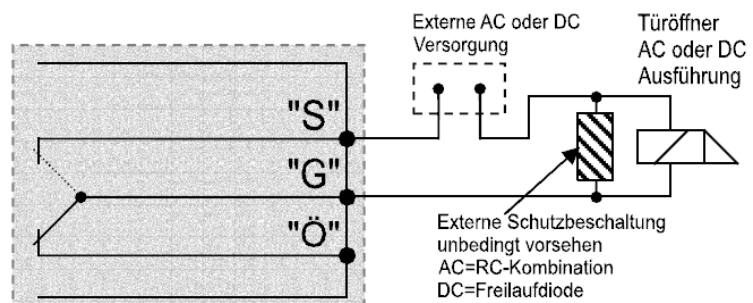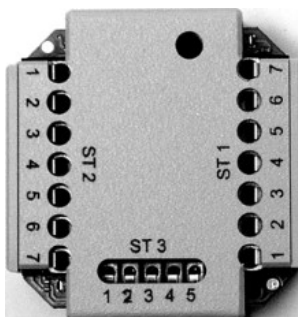
ST 1   Circuit diagram
3   =   "S" normally open
2   =   "G" common
1   =   "Ö" normally close

5.8.3.2. Configuration

The access modules work with internal encryption. The key is stored in the DatafoxStudioIV but not visible.
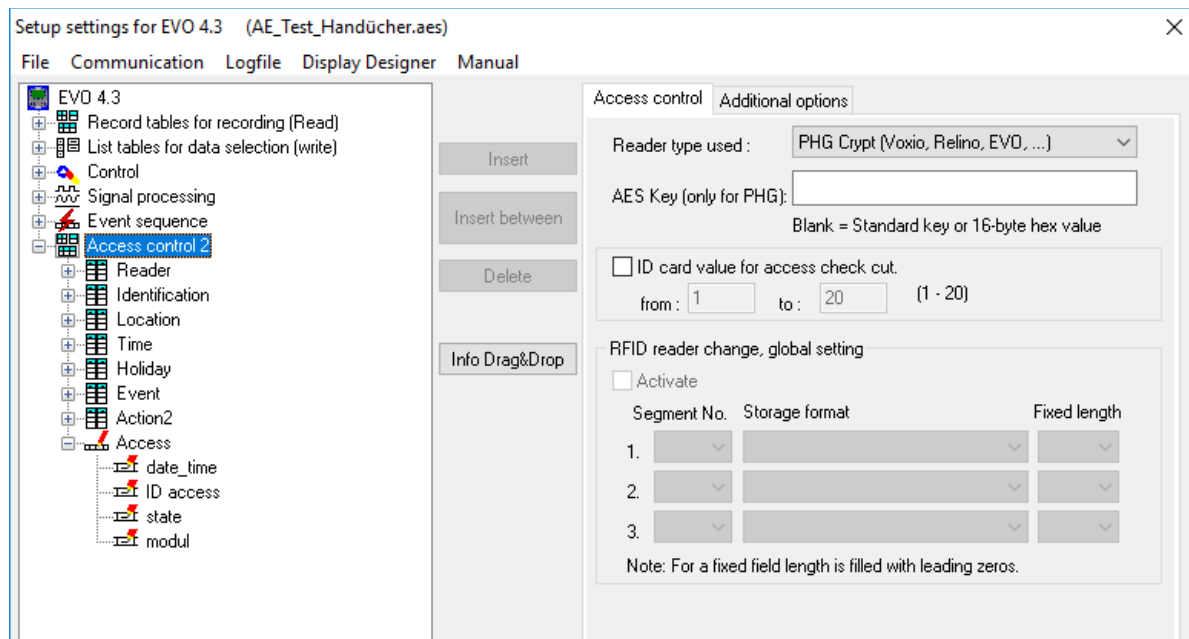
If no key is provided under "AES Key" (PHG only), the default key is used.

> **!** **Caution:**
> The key must only be changed at a fully installed access control. If you changed the key and forgot it, the modules must be sent in. Restoring the default key is <u>subject to a charge</u>.

All door modules that are compiled in the reader table have to be available in the RS485 network in order to guarantee that the code can be changed in all modules if a new setup with a different code is loaded. If a door module from the list in the bus is missing, the key is not changed. The old setup with the old key has to be reloaded; otherwise, after rebooting the device, it is not possible to communicate with the door modules until the right key is used again.

If a defective reader is replaced by a new reader that has not been used yet, it is recognized by the firmware automatically at the start and the encryption is set up. The reader can also be replaced during operation, the firmware automatically integrates it.

Contrary to GIS readers, PHG readers always have 2 digital inputs and a sabotage contact. The firmware regards input 1 and input 2 as normal inputs with the number 1 and 2 and the sabotage contact as number 3. The sabotage contact is integrated in the reader. The PHG reader has no analog-switch-input for door monitoring.

Additionally, the PHG reader can be extended by an IO box. The IO box has two digital inputs and two relay outputs. The IO box is accessed via the same address like the reader. The two digital inputs have port number 4 and 5, the digital outputs port number 1 and 2. In case of discontinuity or sabotage, port no. 6 is used.

PHG modules and firmware:

If you want to use the PHG modules, you have to set it in the Additional Options.

After changing over to the access readers of the PHG series, the firmware must be transferred again.
The device then selects the respective firmware from the DFZ-file.
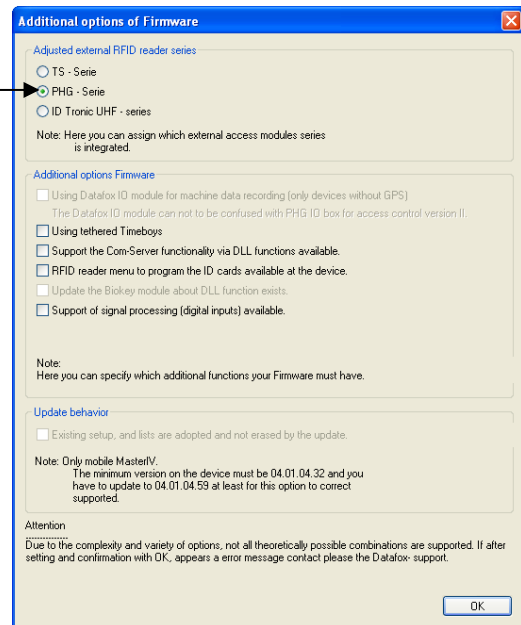
All configurations like tables etc. are to be configured in the same way as for the access readers of the TS series.
Only exception:
The IO box is not specified in the reader table. Thus, information regarding the modules which are connected via the I^{2}C bus, is omitted.

Corresponding reader table:

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Description
1	320	1	0	1	0	Master device
2	010	1	1	1	0	Reader at RS485 (PHG)
~~3~~	~~011~~	~~1~~	~~1~~	~~1~~	~~0~~	~~IO-Box at I^{2}C-Bus~~
4	020	1	2	2	0	Reader at RS485 (LTM)
~~5~~	~~021~~	~~1~~	~~2~~	~~2~~	~~0~~	~~IO-Box at I^{2}C-Bus~~

5.8.4. Access control with EVO Intera Reader

The following hardware is available to set up an access control with EVO Intera. The devices can be combined in different ways according to their hardware requirements.

EVO 2.8 Pure

If the device MasterIV is used for access control, door supervision or remote monitoring, one device can supervise up to 8/16 doors.

EVO Intera Reader

dimensions: 81 x 81 x 19 mm (wxhxd)

The EVO Intera access reader can be used with 125 kHz, Legic or Mifare. It is available for in-wall or on-wall mounting with or without keyboard. Each reader has a sabotage recognition, three lamps for visualizing the state and a buzzer for the acoustic signaling.

IO-modul for EVO Intera reader

Relay
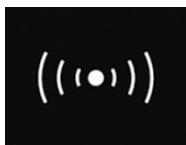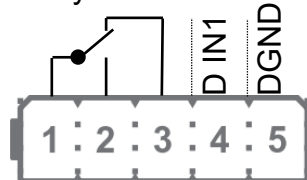
Signals from the backlight:
white permanent = Reader found an ready
white flashing   = reader not found and not connection to the master
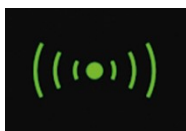
Signals from the backlight:
green = access accept

Signals from the backlight:
red = access denied or the master configured the reader currently.

Display	Backlit transponder symbol		3-coloured white, green, red	
Individualization	Integrated backlight		Individual printable front glass with backlight 56 x 37mm	
			Colour always like transponder symbol	
power supply	10 - 30V DC, max. 120mA			
Environment values	Ambient temperature, Protection		-20 ° C to +70 ° C, IP65	
Transponder systems	**125kHz**		**Mifare**	**Legic**
	Hitag 1+2+S		Mifare Classic	Legic prime
	Unique EM4102		Mifare Desfire	Legic advant
	Titan EM4450		Mifare Ultralight	

Connectors of EVO Intera:

DIP-switch:

switch number	Off	On
1 – address Bit 0	+ 0	+ 1
2 – address Bit 1	+ 0	+ 2
3 – address Bit 2	+ 0	+ 4
4 – address Bit 3	+ 0	+ 8
5 – terminate resistor 120 ohm	not activ	activ

example	5-4-3-2-1
address 2, with terminate resistor	1-0-0-1-0
address 3, without terminate resistor	0-0-0-1-1

Connector for IO-module
Relay + digital in

pin Number.	description
1	+10V bis +30V DC **! new**
2	RS 485-Data „B"
3	RS 485-Data „A"
4	GND ground
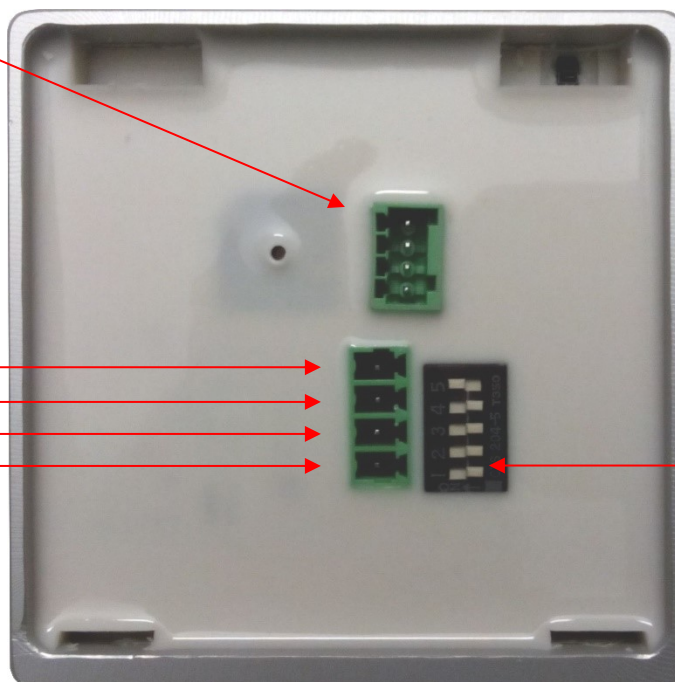
DIP-switch

5.8.4.1. Connecting of the EVO Intera reader examples

Cable plan for one door, 1 Relay in the EVO 2.8 Pure:

TCP / IP (LAN)

12V vom Master

RS 485 ZK Bus-ID 1

Bus Nr. 1

Türöffner Relais 1 der ZK-Box

Bus Nr. 1
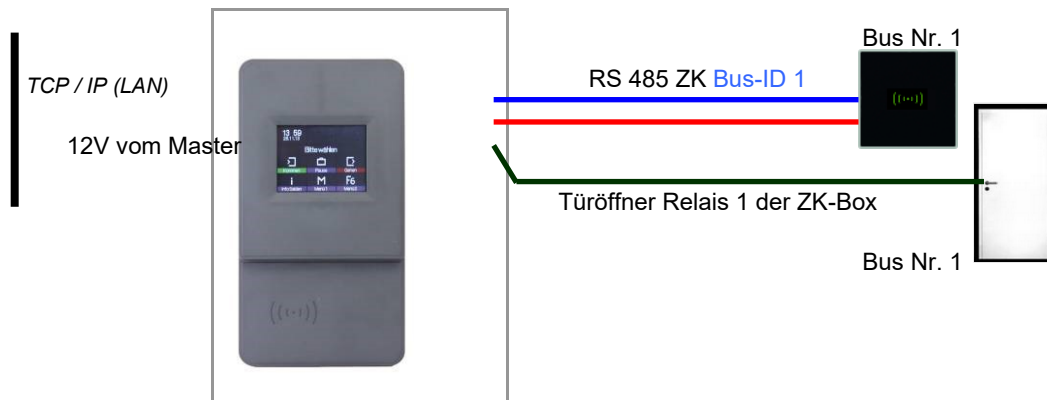
Reader Tabelle, for this example:

ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Beschreibungstext
1	1	010	1	1	0	Reader on RS485 Module place 1 = Bus ID 1
4	1	320	0	1	0	access-Box V4 (Masterdevice)

Wire plan for one EVO Intera:

Bus Nr. 1
EVO Intera

Connector 4 pole for Access Bus

12 V
B
A
GND

+ 1
B
A
GND

connector 5 pole for digital in and out

DG IN GND
DG IN   1

+   **-** max. 30V; 2A
Power supply for door opener
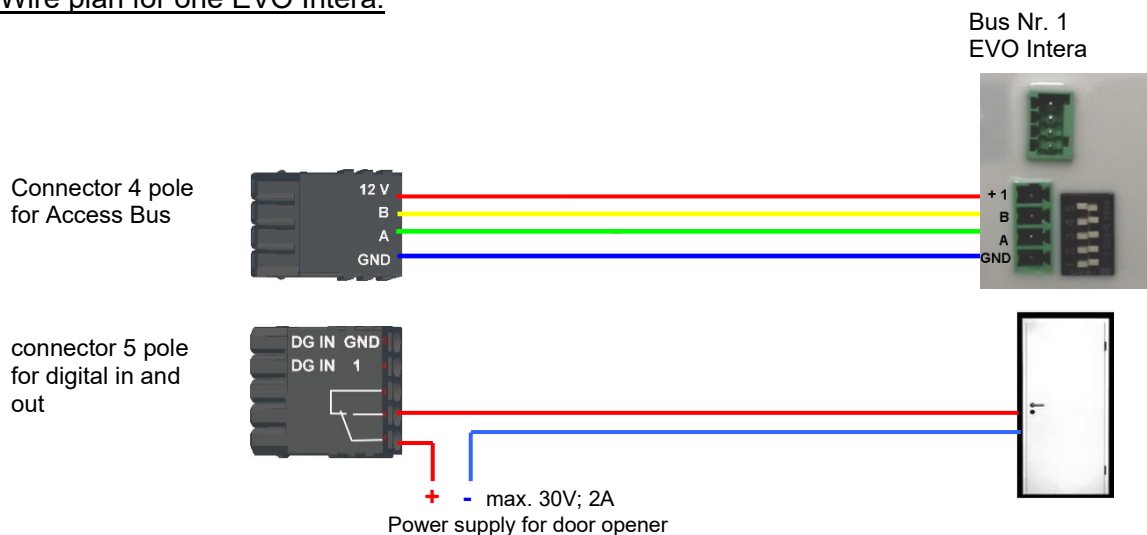
5.8.5. Access control II with EVO Agera

5.8.5.1. Display and operation

The reader has a capacitive touch.
All images displayed by the reader and marked as standard below can be exchanged.
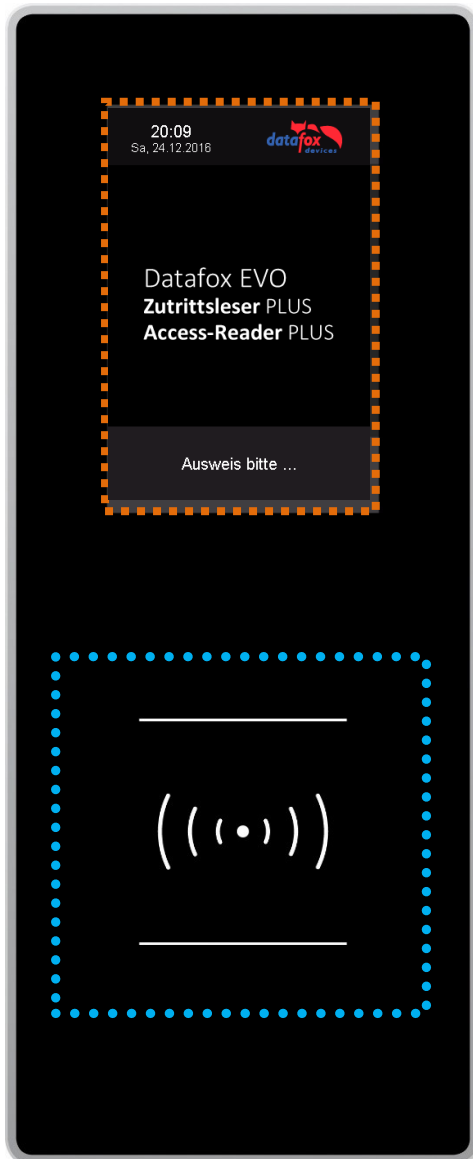
Display:
The entire display area is backed by a touch screen.

With the DatafoxStudioIV, images can be stored here for a gallery display and for the necessary inputs/outputs.
See → Configuration → Display Designer.

Reading range of the transponder with backlight in RGB colours.
The control of the LED is controlled exclusively by the readers firmware.

Access denied   = red   -

Access permitted = green -

Bios activated   = blue -

5.8.5.2. Display for state of access control

Currently there are 2 displayed states for:
granted access: access denied:

Datafox standard image   *Datafox standard image*

5.8.5.3. Display the number keypad

If an additional PIN is requested for access, the keypad will be displayed automatically. For access only by entering a PIN, it is sufficient to briefly touch the display to activate the PIN display.

Datafox standard image
Picture 1 of the gallery
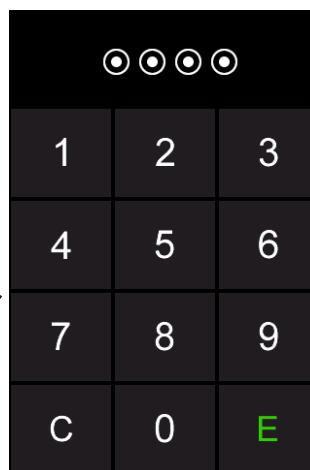
Datafox standard image
PIN normal
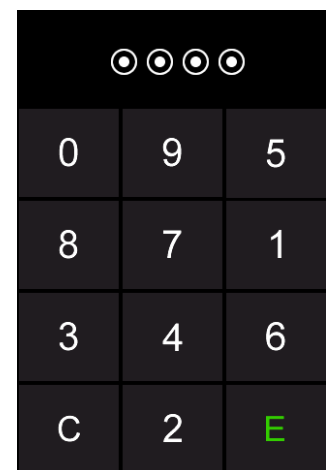
Datafox standard image
PIN randomization

5.8.5.4. Error message

The reader is in constant communication with the master.
If communication is interrupted, this is indicated by the text "Communication error" on the reader.

error
communication
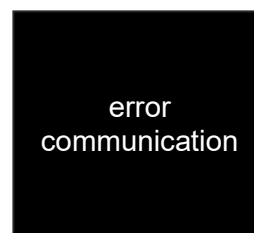
5.8.5.5. Bios-menu

Connect the reader to the 12V power supply with the connecting cable.
As soon as it is started, connect the reader via USB to a PC or a small battery (power bank).
The Bios menu can only be accessed when the USB port is powered.

| Power bank USB |

| USB port on the back of the reader |
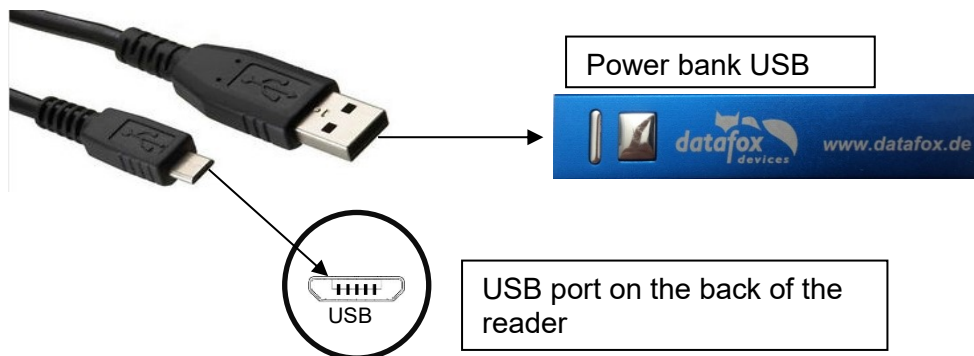
Tap both top left and bottom right at the same time.
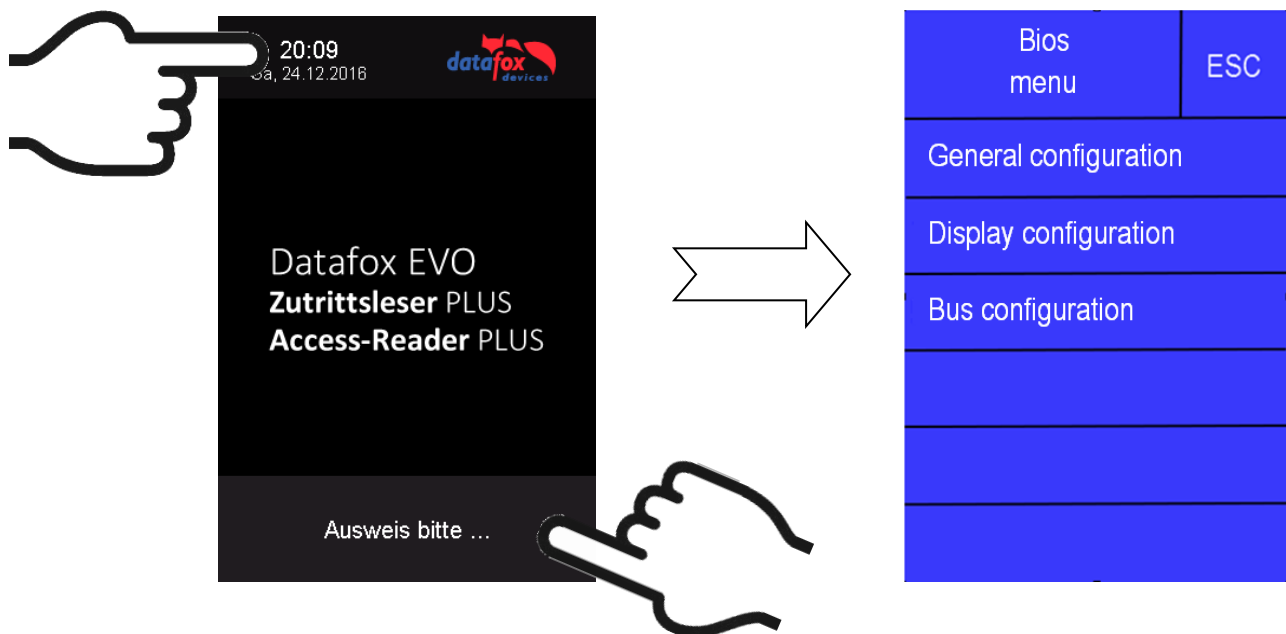
5.8.5.6. General configuration

The following information can be called up in the general configuration:
- Installed firmware, serial number
- Memory allocation for the image memory
- Transponder test for the transponder configured in the master setup.
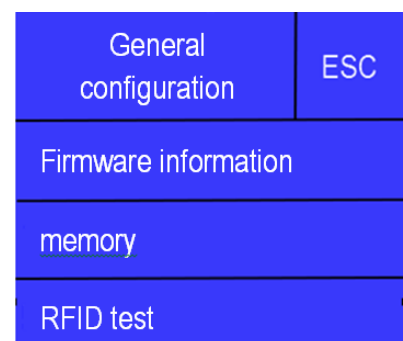
5.8.5.7. Display configuration

The following parameters can be set in the display configuration:

- The brightness of the device
- Random number keys - arrangement of the pin and keyboard
- The basic activation of the pin - keyboard

Display configuration	ESC
Brightness	100%
Random keyboard	
Display Touch Pin	

5.8.5.8. Bus configuration

In the bus configuration, the initial parameters that are used for the setup of the reader must be set.

Bus Configuration	ESC
Bus number	
End resistor	

5.8.5.9. Setting the bus address of the reader for RS485 bus

The bus address is defined in the bus configuration under "Bus number".
Note that only bus addresses between 1 and 16 are possible.

The input of the bus number is confirmed with the "Enter" key (bottom right).

With the Escape button (bottom left) the process can be aborted.

Bus Nummer

0

1	2	3
4	5	6
7	8	9
ESC	0	↵
	←	

5.8.5.10. Activate the termination resistor of the bus

The bus terminating resistor of 120 Ω is switched on or off in the bus configuration under "Terminating resistor".

Note: If it is the last or only reader in the RS485 bus, the terminating resistor must be switched on.

End resistor	ESC
On	
Off	

5.8.6. Online functions for the access control

The access control mechanism offers the functionality to control every configuration and action in your software-solution.
So you can

This allows you to react to all requests from the access control in real time.

Activate the online function in the setup
under the basic settings tab.

There are 2 options:
- Offline Mode (the device always waits for the answer from the server)
- In the option Online/Offline the terminal waits a defined time before switching to the offline functionality. If this happens the terminal will use the access lists in its memory.
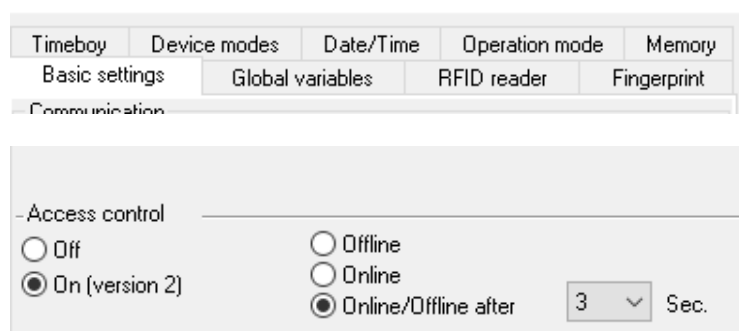
5.8.6.1. Online via http-protocol

The communication with http is very quick and easy to set up. Therefore the webserver has an easy job to react to the requests in a very short period of time.

Requirements:
Hardware:
- TCP/IP
- GPRS (1-2 seconds delay)

Software:
- Active Script with a logic for the access control and specially designed to suit the connected hardware (access reader)

With the answer from the server you are able to perform specific actions with the access readers.

The following examples will give you an insight in what is possible with the functions and actions.
All parameters correspond the online functions with the dll.

Example 1:

The following data is going to be received
table=access&date_time=2013-07-05_07%3A48%3A11&
Master_ID=1&Modul_ID=010&Chip_Nr=2058&Status=34&checksum=2461

Master_ID=1   Master-ID
Modul_ID=010   bus adress of the reader / TM
Ausweis_Nr=2058   ID of the read Chip
Status=34   Online (34)

Fitting answer to grant access:
status=ok&checksum=2461&**access**=010&**mask**=8&**type**=1&**duration**=1

With firmware-version 04.03.04 and up also possible is:

status=ok&checksum=2461&**master**=1&**module**=010&**mask**=8&**type**=1&**duration**=1

access=010   bus adress, on which the action will take place (FW 04.03.03 and lower)
module=010   bus adress on which the action action will take place
master=1   rs485-bus on which the action action will take place
mask=8   relais Nr.1
type=1   turn-on
duration=1   for 1 second

Fitting anser to deny the access => Red-LED:
status=ok&checksum=2482&**access**=010&**mask**=5&**type**=1&**duration**=2
 ab der Firmware 04.03.04 ebenfalls möglich ist:
status=ok&checksum=2461&**master**=1&**module**=010&**mask**=8&**type**=1&**duration**=1

access=010   bus adress, on which the action will take place (FW 04.03.03 and lower)
module=010   bus adress on which the action action will take place
master=1   rs485-bus on which the action action will take place
mask=5   red LED + buzzer
type=1   turn-on
duration=2   for 1 second

Several bus strings can be controlled with the new hardware V4. In order to be able to execute actions on the corresponding bus string, the bus string ID must be transferred with the response as well.

For this, the new keywords "module" and "master" were implemented. These must be used together, replacing the keyword "access".

! **Attention:**
The order "**access→mask→typ→duration**" or **master→module→mask→typ→duration** must be strictly adhered to.

status=ok&checksum=2482&**access**=010&**mask**=5&**type**=1&**duration**=2
status=ok&checksum=2482&**master**=1&**module**=010&**mask**=5&**type**=1&**duration**=2

Overview of the possible parameters for the keywords:

keyword	value / Bit Nr.	description
access= or **module**= function for 1x Bus RS485	000 010 011 … 081 usw.	The value of the string must follow the format of the "TM" field of the "Reader" list. He must therefore always include 3 digits.
master =	1-3 1 2	Id for the RS485 bus ZK, represents the ZK- rs485-bus. RS485 Bus ID 1 RS485 Bus ID 2… „**master**" has to be set together with „**module**" and so replaces the function „**access**"
mask	1 / 0	this bit will trigger the buzzer.
	2 / 1	this bit will trigger the green LED.
	4 / 2	this bit will trigger the red LED.
	8 / 3	this bit will trigger the first relay.
	16 / 4	this bit will trigger the second relay.
	32 / 5	this bit will trigger the third relay.
	64 / 6	this bit will trigger the fourth relay.
	128 / 7	this bit will trigger the fifth relay.
	256 / 8	this bit will trigger the sixth relay.
	….	unused. always set to 0
type	0	Off
	1	On
	2	change (600ms on, 600ms off)
	3	3 times on for 500ms
duration	Sekunden / 0	Is a period of time and only at =1 active. meaning: 0 = always on, 1 - 40 = seconds on.

☞ **Hint:**
You can also perform multiple actions on the access control in one response. However, the total length of the response must not exceed 254 characters.

! **Attention:**
A automated switch between online and offline mode is not possible in http mode

5.8.6.2. Online via DLL connection

The dll offers the function to directly access the external access reader. With the function "DFCEntrance2OnlineAction"you are able to trigger the buzzer, the LEDs and the relays.

In the case of an access booking, the access master generates a data record. This must be picked up immediately and forwarded to the application on the server. The application then decides whether access is granted and returns a command to control the relay in the door module or lets the buzzer sound and issues a visual message via the LEDs.

More dll functions are documented in the "Datafox SDK" on our website
https://www.datafox.de/downloads-datafox-kyo-inloc.de.html?file=files/Datafox_Devices/Downloads_Geraete_Zubehoer/001_MasterIV-Software/Datafox_SDK_Windows_04.03.12.zip

5.8.7. Function extention for access control II

5.8.7.1. General description

The access control has been extended to some functionality. To the table "Action 2" was introduced. This table replaces the previously known "Action". On the end of this chapter you find a description for the table „Action2". Due to a lot of additional references many scenarios are now possible.

The entire logic of the access control lies in the links between the access lists. Here is an overview of the links between the access lists:
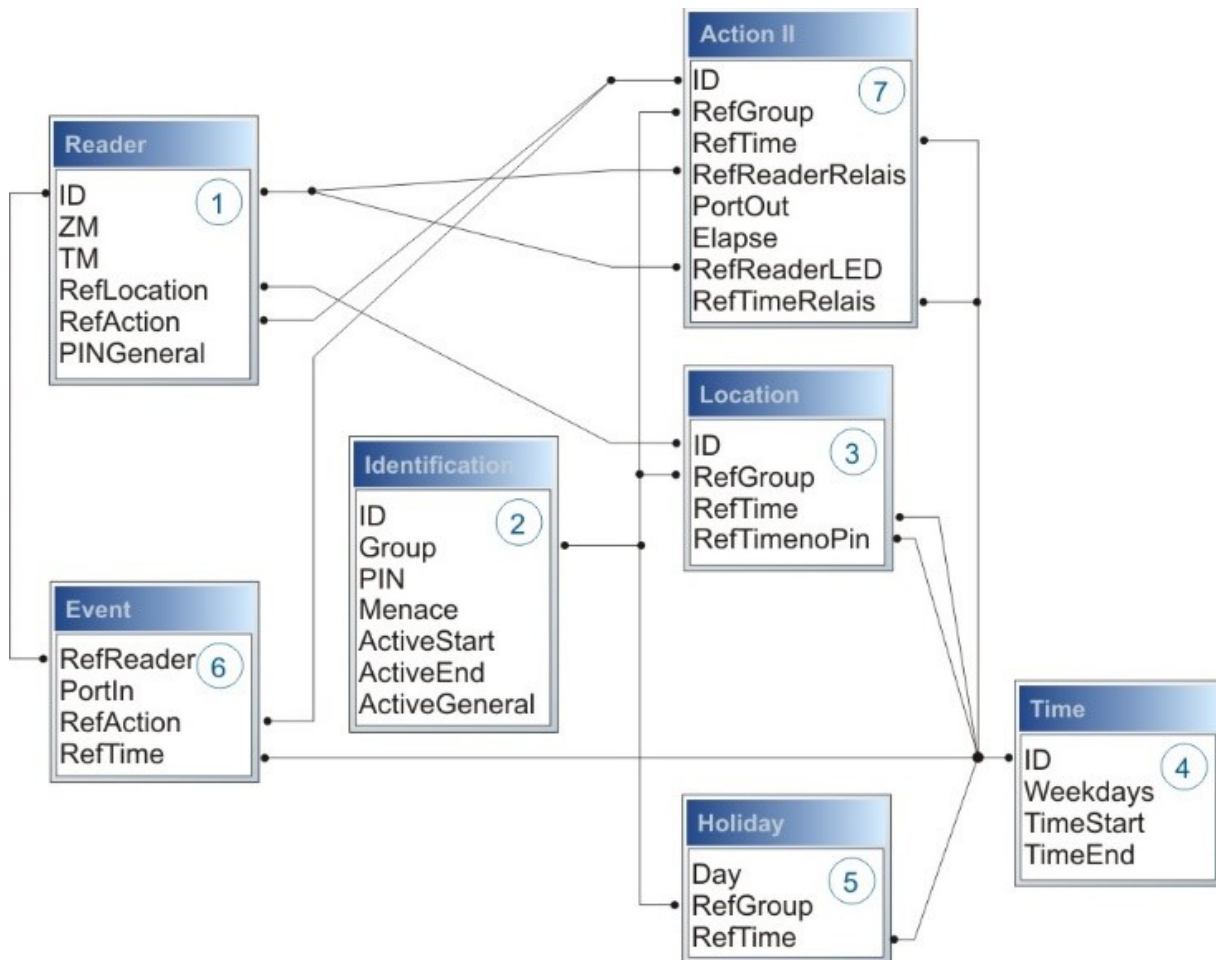
The following example gives an overview:

5.8.7.2. Examples

Example - Garage:

The facility manager comes in the morning at 7.00 o´ clock and uses the Entry 1.
- with his RFID-chip he opens the door 1 for 5 seconds.
- with the same action he gives the door 3 free, the opening is now possible with a switch, until 4 o´ clock pm.
- entry 2 is now open until 4 o´ clock pm for the other person.
  the closing is possible with:
  - 1 – one RFID-chip registry on group 40
  - 2 – double read of a normal RFID-chip
  - 3 - Automatic at 4 o´ clock pm (define in the time table, see in row 2 „RefTime")
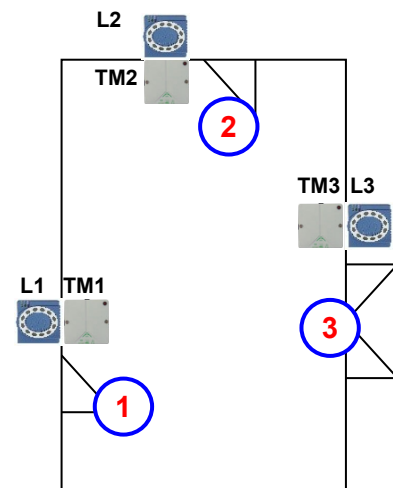
Construct of Reader-, Location- , Action2- and Identification-table looks maybe at follows

Table *Reader*

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Description text
1	1	320	0	0	0	Master device
2	1	010	100	0	0	Door-module on RS485 wire (TM1) only relays include Need not a listing in the table „action"
3	1	011	100	1000	0	RFID-reader on RS232 wire (L1) only reader All readings of RFID on this reader make all actions in the table "action", with the ID 1000.ID 1000.
4	1	020	200	0	0	Door-module on RS485 wire (TM2) only relays include Need not a listing in the table „action"
5	1	021	200	2000	0	RFID-reader on RS232 wire (L2) only reader All readings of RFID on this reader make all actions in the table "action", with the ID 2000.
6	1	030	300	0	0	Door-module on RS485 wire (TM3) only relays include Need not a listing in the table „action"
7	1	031	300	3000	0	RFID-reader on RS232 wire (L3) only reader All readings of RFID on this reader make all actions in the table "action", with the ID 3000.

Table *Time*

ID	Weekdays	TimeStart	TimeEnd	Description text
1	1234567	00:01	23:59	24houers opening possible
2	1234567	07:00	16:00	Time for special action

Table *Action2*

ID	RefGroup	RefTime	RefReader Relais	PortOut	Elapse	RefReader LED	RefTime Relais	Description
... Read an RFID chip on reader 1								
1000	10	0	2	1	5	3	0	Opening normal for 5s. Group (10; 20; 30) have always entrance
1000	20	0	2	1	5	3	0	
1000	30	0	2	1	5	3	0	
1000	30	2	4	1	32400	5	0	door 2 open for 9h (max. 16:00)
1000	30	2	6	1	32400	7	0	door 2 open for 9h (max. 16:00)
1000	40	0	2	1	-1	3	0	command door open, return
1000	40	0	4	1	-1	5	0	command door open, return
Read an RFID chip on reader 2								
2000	10	0	4	1	5	5	0	Opening normal for 5s. Group (10; 20; 30) have always entrance
2000	20	0	4	1	5	5	0	
2000	30	0	4	1	5	5	0	
2000	30	2	4	1	32400	5	0	door 3 open for 9h (max. 16:00)
2000	30	2	6	1	32400	7	0	door 3 open for 9h (max. 16:00)
2000	40	0	4	1	-1	5	0	command door open, return
2000	40	0	6	1	-1	7	0	command door open, return
Read an RFID chip on reader 3								
3000	0	0	6	1	5	0	0	This action is for all Groups are listed in the table "*Location*".

Table *Location*

ID	refGroup	refTime	refTimeNoPin	Description
100	10	1	0	Group 10, 20, 30 and 40 have access on this reader.
100	20	1	0	
100	30	1	0	
100	40	1	0	
200	10	1	0	Group 20 can not use this entrance 2.
200	30	1	0	
200	40	1	0	
300	10	1	0	The Master of Garage and the facility manager can open this door.
300	30	1	0	

Table *Identification*

ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Description
1111	10	0	0	2005-01-01	2015-12-31	1	Master of Garage
2222	20	0	0	2005-01-01	2015-12-31	1	Skilled workers
3333	30	0	0	2005-01-01	2015-12-31	1	Facility manager
4444	40	0	0	2005-01-01	2015-12-31	1	Facility manager second RFID-chip, only for closing the door

Example - elevator
The goal is to allow users only to exit at the allowed floor.
Then tenant uses the transponder to activate only the switch for his floor.

In the cabin of the elevator the RFID-reader is installed. The Datafox-Device is on the top of the cabin.

- RS485 Bus to the reader in the cabin

Relay for floor 1

Relais for floor 2

Relay for floor 3

Relay for floor 4

Relay for floor 5

Relay for floor 6

… Relay for floor 12
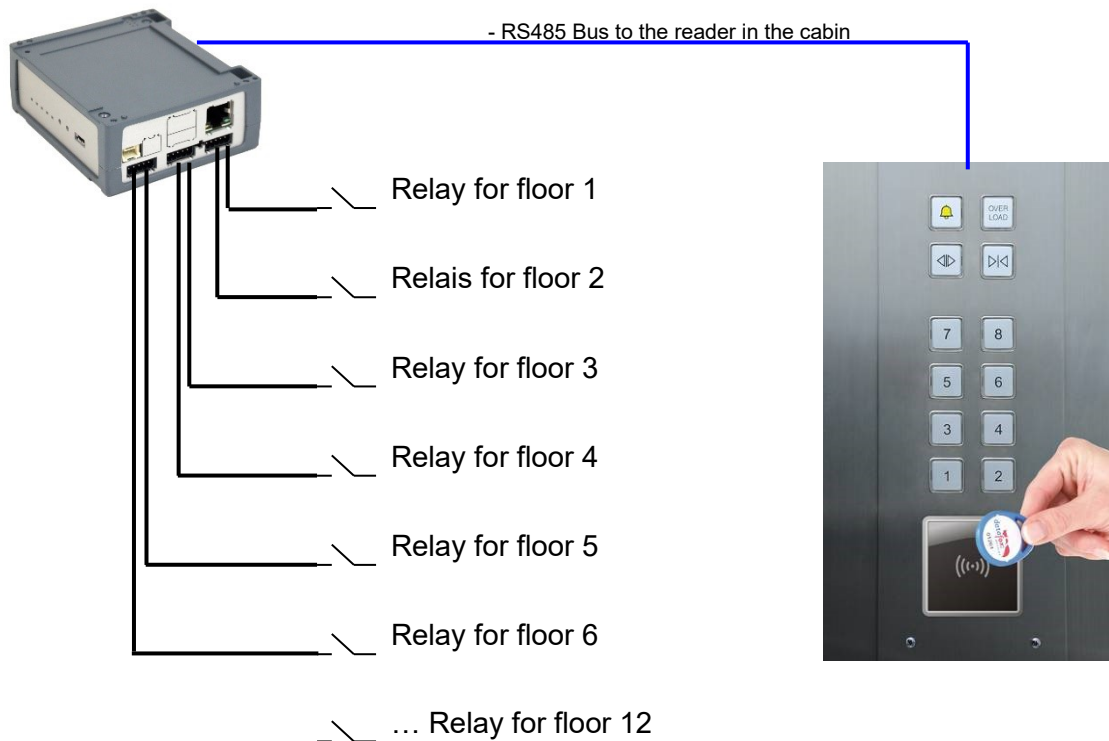
Wiring plan for the EVO-Access reader:

Bus Nr. 1
EVO-access-reader

Connector for
RS485 Bus
On the Mod-
ulplace 1

12 V
B
A
GND

+ 1
B
A
GND

Relay 2 for floor
normaly close

relay 2

Relay 1
With no/nc contact

relay 1

Connector 5 poles
for 2 digital out
free potential

Elevator Con-
trol Center

+ **-** max. 30V; 2A
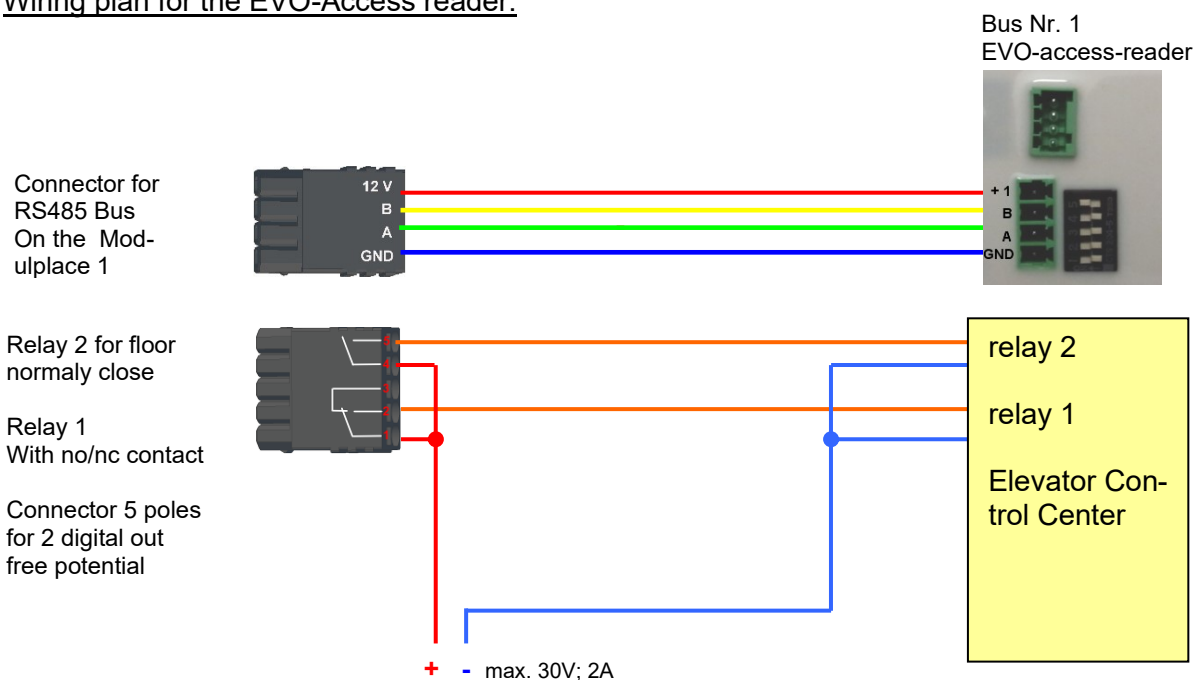
The content of Reader-, Location- , Action2- and Identification- might look like follow:

Table *Reader*

ID	ZM	TM	RefLocation	RefAction	PinGeneral	Description
1	1	320	0	0	0	Master device
2	1	000	100	1000	0	Reader on RS485 wire

Table *Action2*

ID	RefGroup	RefTime	RefReader Relais	PortOut	Elapse	RefReader LED	RefTime Relais	Description
Buchungen am Leser in der Kabine								
1000	10	0	1	1	20	2	0	Group10 only for floor 1.
1000	20	0	1	2	20	2	0	Group 20 only for floor 2.
1000	30	0	1	3	20	2	0	Group 30 only for floor 3.
1000	40	0	1	4	20	2	0	Group 40 only for floor 4.
1000	50	0	1	5	20	2	0	Group 50 only for floor 5.
1000	60	0	1	6	20	2	0	Group 60 only for floor 6.
1000	102	0	1	1	20	2	0	Group 102 moving to floor 1 and 2
1000	102	0	1	2	20	2	0	
1000	104	0	1	1	20	2	0	Group moving to floor 1, 2 and 3.
1000	104	0	1	2	20	2	0	
1000	104	0	1	3	20	2	0	

Table *Location*

ID	refGroup	refTime	refTimeNoPin	Note
100	10	1	0	
100	20	1	0	
100	30	1	0	
100	40	1	0	All Groups 10, 20, 30, 40, 50, 60,102 and 104 must listed in the location for this reader.
100	50	1	0	
100	60	1	0	
100	102	1	0	
100	104	1	0	

Table *Identification*

ID	Group	Pin	Menace	ActiveStart	ActiveEnd	Active	Description
1111	10	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 1
2222	20	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 2
3333	30	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 3
4444	40	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor4
5555	50	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 5
6666	60	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 6
1102	102	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 1 and 2
1104	104	0	0	2005-01-01	2099-12-31	1	Tenant of an apartment on the floor 1, 2 and 3

5.8.7.3. Description of the table „Action2"

The switching from „Action" to „Action2" it's a setting in the StudioIV.

Name	Data type	Length	Description
ID	Number (int)	4	Action number, it can occur several times due to several actions that have to be worked through.
RefGroup	Number (int)	4	Only work this action for the listed Group. 0 = for all groups work this action.
RefTime	Number (int)	4	Give a time, and only works this action to this time. (0 = works ever) ! Not mixed with times in RefTimeRelais!
RefReader Relais	Number (int)	4	Reference to the list reader, action to switch a relay on this listed reader in table reader.
PortOut	Number (char)	1	Indicates the number of the output on the module. Possible values: 1 ... 9 & A ... W corresponds to port 1-32 (digital out)
Elapse	Number (int)	6	Specifies the period of time a relay is switched ! The time is in seconds! When **(-1)** is specified, the relays are reset directly. With **(0)** the relays switch for the duration specified for the relay with RefTime. "**FRA**" activates Free Access "**BLA**" activates Blocked Access = permanent red signal "**STD**" returns to Standard mode.= Deactivate from FRA or BLA
RefReaderLED	Number (int)	4	This is a reference to the table Reader to switch the LED on other modules
RefTimeRelais (only for automatic time switch)	Number (int)	4	The time model indicates when the output may be switched. (0 = not used). (Automatic time control) ! Action how here work with automatic times, be not mixed with action from the access!

> **!** **Caution:**
> By transferring the table "Action 2" to the unit, the table "action" is replaced. Thus, only entries in the table "Action 2" will be considered.

> **!** **Caution:**
> If you would like to continue working with the "action" table, the table "Action 2" may not be transferred to the device.
> A table "Action 2" has already been transferred to the device, it must be cleared by loading a new setup.

5.8.7.4. Additional functions for Access Control

All functions described below are only supported in conjunction with the Action 2 table.
Possible functions:
- Logging, in an internal list, in which room each employee is located.
- Hard antipassback
- Soft antipassback (= only the software is informed that an ID card has entered a room 2 times = status message 251)
- BDS
- Type associated to the supervised door unctionality.

The table "ReaderProps" must be created under the table structure of the operation:

Name	Data type	Length	Description
Name	Data type	Length	Description
RefReader	Number (int)	4	Reference to the ID of the Reader whose properties should be specified
Type	Number (int)	2	Type of the Property 1 = anti-passback 2 = BDS-System 3 = BDS 4 = BDS 5 = Type associated to the supervised door unctionality.
Mode	Number (int)	1	Mode for details of the type above 1 - Only protocol the attendance of persons in a room (in list "presence"). 2 - Hard anti-passback (no entry when conflict detected, status code 250) 3 - Soft anti-passback (entry allowed when conflict detected, status code 251).
Duration	Number (int)	10	Access is permitted again after the duration time has elapsed. Value in seconds. 0 = no end time. It is necessary to enter another room necessarily

The table **"ReaderProps"** is created in the setup:

Protocol - Function
Essentially serves to ensure that when several access managers are used, they know in which room a person is located.
Via your software, this information is distributed between the access managers or can be read out if required.
See the documentation DFComDLL
- DFCTable.......
- DFCPresence....

Soft antipassback
A status message 251 is issued here if one and the same badge enters the same room more than once. Admission is still permitted!

Hard antipassback
A reader is always assigned to a room. This room may then only be entered once with the same ID.
If the same ID card is used again for access to this room, it will be rejected. Status 250 is output in the data record during access control.
Here you can choose whether the reject is limited in time or whether Hard remains active.
In the case of Hard Active, access is not permitted again until another room ID has been accessed.
This corresponds to leaving the previous room.

5.8.7.5. List Presence

This list is created by the access controller itself.
This makes it possible to enable the tracking of people and rooms via several access controllers.
If the Antipassback function is to be used via several access controllers, this list must always be updated by the software to all access controllers.

Example:
A room (example room ID 10) has several doors that are managed by different access control boxes. If a person enters this room, an entry is created in the Presence list of this box that this person is in the room.

The other access control boxes can now also be informed that the person with ID X is in room 10.
To do this, an entry in the Presence list must be created in the other boxes via your software (with DLL).
This is done using the method DFCTableAppendRowData Append Data Row to the table.
The same applies if a person leaves the room, this entry must be deleted in the Other Access Control Boxes.

Name	Data type	Length	Description
ID	Number (int)	20	ID of the person that is stored in the presence list.
RefLocation	Number (int)	4	Reference to the ID of the room, defined in the table "Location", where this person currently stays
TimeStamp	Number (int)	10	Time stamp when the person entered the current room Integer in seconds, starting 01.01.2000.

5.8.8. Integration of a Burglar Detection System (BDS)

Integration of a Burglar Detection System (BDS)
Starting with firmware version 04.03.12 the integration of a BDS into the access control system is possible.

You may control the state of up to five BDS sections using PIN readers and arm or disarm them.

In the presence of a BDS the access controller checks, that the BDS section is not armed. If armed, it will reject transponder events leading to opening the door of an armed section due to the armed BDS. Access transponder events will be evaluated according to the normal access control rules and only be granted if the reader is either part of no BDS section or part of a disarmed BDS section. An access control event rejected to an armed section will result in a dataset with "BDS armed" state.

You may (try to) arm or disarm a BDS section any time using a PIN reader associated to it.
As second attempt to either arm or disarm a BDS section will result in "BDS already armed" or "BDS already disarmed" status passed to dataset.

5.8.8.1. Configuring up the BDS

In order to activate the BDS inside the access control sub system, the setup list „ReaderProps" is required. Up to now this list was required to configure "AntiPassBack" only. To configure BDS the ReaderProps requires twelve columns.

> ☞ **Please note:**
> - If you are transferring list data using the DatafoxStudioIV it is not possible to transfer "empty" columns. Please fill these columns using "0" values.
> - The width of the ReaderProps' columns may be chosen arbitrarily. However, it is important that the required information fit into the columns!

To setup the BDS three types of entries are required. Firstly the relay(s) to active the BDS is/are required as well as inputs to query the BDS's current status. Additionally PIN readers of the access control system are required to allow activating / deactivating the BDS sections. Finally the PIN readers will have to associate to one or more BDS sections.
The sequence of the entries inside the "ReaderProps" list does not matter.

5.8.8.2. Relays and digital inputs for controlling the BDS (Type 2)

The relays associated to arming or disarming the alarm sections are set up according the entries described in this chapter. Additionally the digital input to indicate the readiness to be armed and the armed-state of the BDS section is configured here.

Column	Name I the Setup	Data type	Length	Description
1	RefReader	Number (int)	4	Not required, leave empty
2	Type	Number (int)	variable 10	Type 2 = BDS – definition entry for relay and digital input
3	Area	Number (int)	variabel max. 10	Number associated to the BDS section
4	OutArmReader	Number (int)	4	Reference to the device (controller or bus member) that contains the relay for arming the BDS.
5	OutArmPort	1-9; A…	1	Nummer den Ausgangs
6	OutUnarmReader	Number (int)	4	Reference to the device (controller or bus member) that contains the relay for disarming the BDS.
7	OutUnarmPort	1-9; A…	1	Number of the relay on the device column 6
8	InRdyReader	Number (int)	4	Reference to the device (controller or bus member) that contains the digital input that signals the BDS section to be ready to be armed (through "high" voltage level).
9	InRdyPort	1-9; A…	1	Number of the relay on the device column 8
10	InArmedReader	Number (int)	4	Reference to the device (controller or bus member) that contains the digital input signalling that the BDS section is armed (through "high" voltage level).
11	InArmedPort	1-9; A…	1	Number of the relay on the device column 8
12	OutElapse	Number (int)	4	0 -> The relay for arming / disarming is continuous active, otherwise duration of the relay's closing time in seconds.
13	Timeout for activate/deactivate	Number (int)	4	Adjustable timeout for EMA arming/disarming. If the column does not exist or the value =0, the default value of 5 seconds is applied. The value can be between 3000-30000 ms. Valid from firmware 04.03.21.08!

Description ReaderProbs für (Type=2) in- and output Definition!

> **Please note:**
> - If arming and disarming is using the same relay, the values in columns OutUnarmReader and OutUnarmPort have to be identical to OutArmReader and OutArmPort. If the relay then is closed, the BDS is meant to be armed, the opened relay indicates the disarmed BDS.
> - If no digital input is set as „InRdyRead", the BDS is considered to be ready to be armed any time.

5.8.8.3. Assigning codes for arming and disarming (Type 3)

In order to use a PIN reader for arming or disarming a BDS section the following entry is required.

Spalte	Name In the setup	Data type	Length	Description
1	RefReader	Number (int)	4	Reference (ID) to the PIN reader inside the reader
2	Type	Number (int)	variabel max. 10	Type assigned to this entry, 3 = BDS PIN code to "arming or disarming"
3	Area	Number (int)	variabel max. 10	BDS section
4	CodeOn	Number (int)	2	Code (max. 2 digits) to start arming mode. If these digits are entered, the reader starts the arming process.
5	CodeOff	Number (int)	2	Code (max. 2 digits) to start disarming mode. If these digits are entered, the reader starts the disarming process.
6	RefGroup	Number (int)	4	In order to allow arming or disarming a privileged tag has to be presented to the reader after entering the prefix code. After the tag the reader waits for a legitimation code (this field) before actually arming or disarming the BDS section (see Privileging transponders to control the BDS)). If you enter "0" here, no PIN is enquired and any BDS privileged transponder may arm or disarm the BDS section.
7				
8				
9	Not required, leave empty			
10				
11				
12				

Hinweise:

Please note:
- If a reader controls more than just one BDS section, you will need one entry per BDS section.
- Operating codes are not interpreted numerically, so "0" or "00" are different prefix codes!
- If a BDS section is only to be armed or disarmed by the reader, enter a Minus "-" into the other operation's prefix code because "0" would be a valid code.
- Please ensure that no operating code is used more than once – the system behaviour is not defined then.

5.8.8.4. Associating BDS sections to readers (Type 4)

In order to be able to reject door openings when a BDS section is armed, the readers have to be associated to BDS sections.

Spalte	Name im Setup	Data type	Length	Description
1	RefReader	Number (int)	4	Reference (ID) to the reader definition in the Reader list
2	Type	Number (int)	variabel max. 10	Type assigned to this entry 4 = Association of reader and BDS section
3	Area	Number (int)	variabel max. 10	Definition of the BDS section
4				
5				
6	Not required, leave empty			
7				
8				
9				
10				
11				
12				

☞ **Please note:**
- A reader may be part of more than one BDS section. Every section requires an entry inside the list ReaderProps.
- Readers not associated to any BDS section may be used to gain access any time using the normal access control rules.

5.8.8.5. Privileging transponders to control the BDS

To enable BDS control using an RFID transponder, this transponder has to be part of the Identification table. The corresponding group (see section [Assigning codes for arming and disarming (Type 3)](#), Column 6 „Group") has to be entered as "Group" inside the Identifiaction as well. Final requirement will be Column „ActiveGeneral" to be set to „7".

Should you require the RFID transponder to be enabled for all BDS sections, use "0" as "Group" value. This will enable the transponder to control all BDS sections, even if a "Group" is entered into the code definition (see [Assigning codes for arming and disarming (Type 3)](#), Column 6).

Once the operating code and "E" (Enter) have been entered at the PIN reader, the reader will start flashing red and green. Within the 5 seconds timeout a privileged RFID transponder has to be presented to the reader, then the PIN has to be entered. Depending on the validity of PIN and transponder, the BDS section will be reconfigured correspondingly (green signal) or left unchanged (red flashing three times).

Examplefor the table Identification:

The RFID-Number 59780 can switch the BDS-System and have standard access.

ID	Group	Pin	Duress	ActiveStart	ActiveEnd	ActiveGeneral
51044	1	0	0	2018-01-01	2099-12-31	1
59780	1	0	0	2018-01-01	2099-12-31	1
59780	8	0	0	2018-01-01	2099-12-31	**7**

5.8.8.6. Statuscodes

The following status codes have been added in order to document the BDS state:

BSD/ EMA	Discription/ Beschreibung
258[1]	The access control system awaits legitimation through RFID transponder and/or PIN after starting a BDS control event due to entering the operating code.
259	The access control system awaits legitimation through RFID transponder and/or PIN after starting a BDS control event due to entering the operating code.
260	During a BDS control event a non-privileged RFID transponder has been presented to the reader. This transponder is either not contained within the Identifiaction table or does not have ActiveGeneral set to 7. See Privileging transponders to control the BDS.
261	The specified BDS section is not configured correctly.
262	There are no concurrent BDS control events supported while a BDS control event is currently being processed.
263[1]	The BDS signals that is ready to be armed.
264[1]	The BDS signals that is not ready to be armed.
265	The relay to arm the BDS section has been set.
266	The relay to disarm the BDS section has been set.
267	The BDS section to be armed is already armed. The reader signals "green" anyway so that the operator knows that the BDS section is armed.
268	The BDS section to be disarmed is already disarmed. The reader signals "green" anyway so that the operator knows that the BDS section is disarmed.
269[1]	The BDS section is armed now.
270[1]	The BDS section is disarmed now.
271	The BDS section could not be armed within five seconds. The digital input pin associated to the BDS section state still reports the section as disarmed.
272	The BDS section could not be disarmed within five seconds. The digital input pin associated to the BDS section state still reports the section as armed.
273	The access request was denied due to the BDS section being armed.
274	Identification requires an additional PIN.
275	The PIN entered does not match the stored one.
276	The PIN entered matches the stored one.
277	Timeout while waiting for the PIN to be entered.

[1] This status code contains the BDS section [1..5] as property „ID number".

5.8.8.7. Pre-checked online processing graph
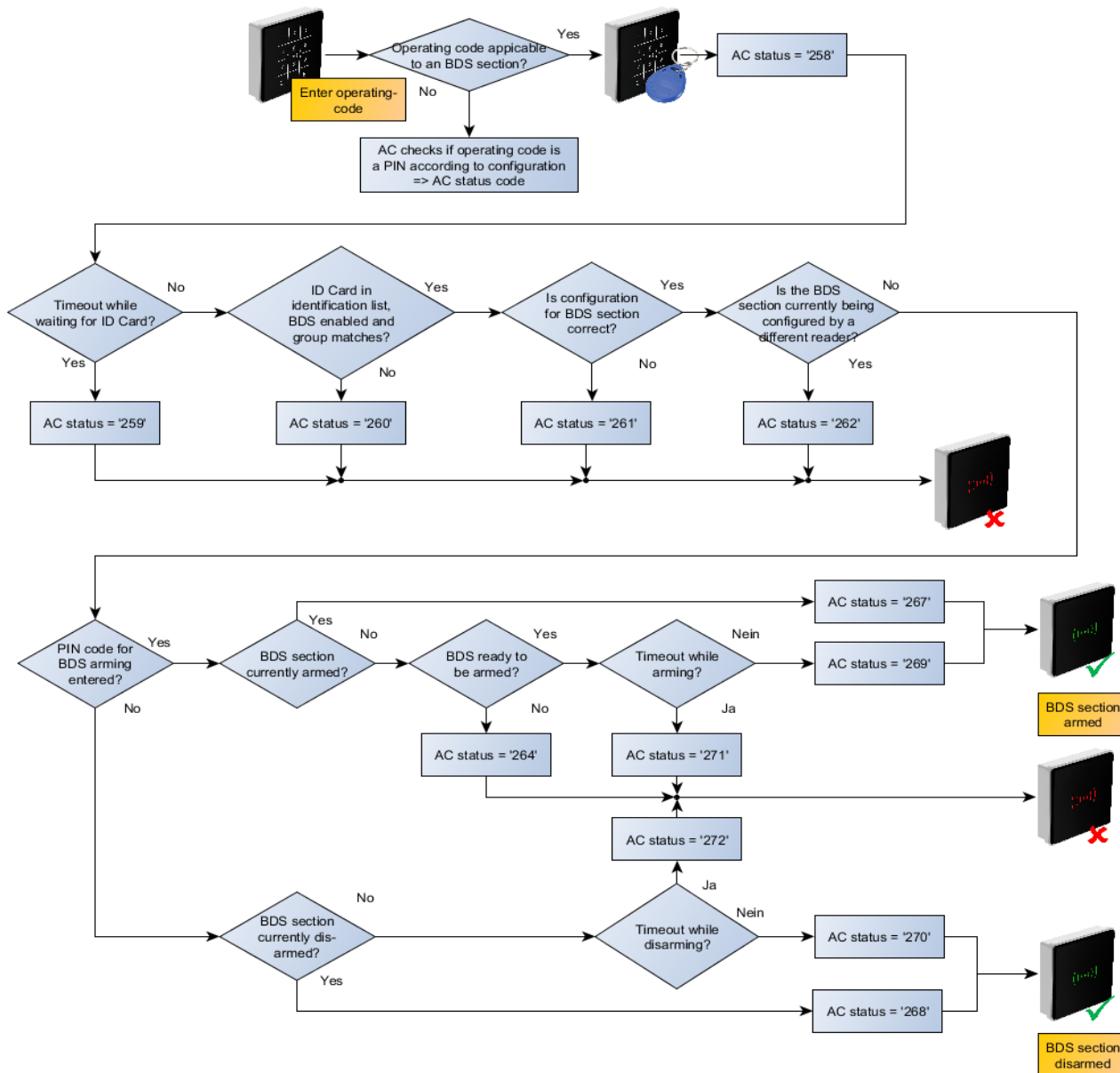
5.8.8.8. Example for the BDS integration

The following sections contains an example configuration for including a BDS:
The BDS section "2" is being configured in the example below. The AC controller's third relay is used to request arming a section, the fourth relay of the AC controller to request disarming. Digital input 1 of the AC controller indicates that the BDS is ready to be armed. Digital input 2 of the AC controller indicates that the BDS section is currently armed.
Using the operating code "11+E" the BDS section can be armed, the code "22+E" is used to disarm the section. RFID-cards associated to group 8 may change the BDS configuration of section "2". There are two AC readers with IDs "104" and "105" associated to the BDS – these readers allow normal access control identification when the BDS is disarmed.

Example ReaderProps-table

The ReaderProps table associates digital inputs and relays to the BDS section.

;Ref Reader	Type	Area	Out Arm-Reader	Out Arm-Port	Out Unarm-Reader	Out Unarm-Port	In Rdy-Reader	In Rdy-Port	In Armed-Reader	In Armed-Port	Out-Elapse
0	2	2	999	3	999	4	999	1	999	2	2
;Ref Reader	Type	Area	Code On	Code Off	Group	----	----	----	----	----	---
104	3	2	11	22	8	0	0	0	0	0	0
;Ref Reader	Type	Area	----	----	----	----	----	----	----	----	----
104	4	2	0	0	0	0	0	0	0	0	0
105	4	2	0	0	0	0	0	0	0	0	0

Reader-table

The reader table contains both readers and the controller "999"

ID	ZM	TM	Location	Action	Pin	Ref-Time
104	1	040	1		1004	0
105	1	050	1		1005	0
999	1	320	0		0	0

Action2-Tabelle
The action2 table defines the relays 1 and 2 for opening doors – this is not really necessary for configuring the BDS section.

;ID	RefGroup	RefTime	RefReaderRelais	PortOut	Elapse	RefReaderLED	RefTimeRelais
1004	0	0	999	1	3	0	0
1005	0	0	999	2	3	0	0

Examplefor the table Identification:
The RFID-Number 59780 can switch the BDS-System and have standard access.

ID	Group	Pin	Duress	ActiveStart	ActiveEnd	ActiveGeneral
51044	1	0	0	2018-01-01	2099-12-31	1
59780	1	0	0	2018-01-01	2099-12-31	1
59780	8	0	0	2018-01-01	2099-12-31	**7**

5.8.9. Automatic relay release upon opening of the door

Access control:
The amount of time for which a door is being opened is defined by the "Action" table's "Elapse" property. The door is opened for the amount of time defined by "Elapse" continuously.

With the enhancements of 04.03.13 firmware release, the relay opening the door can now be deactivated ("release") as soon as a door-open sensor is trigger. This sensor has to present and connected to the access control system when using this function.

5.8.9.1. Supervised doors
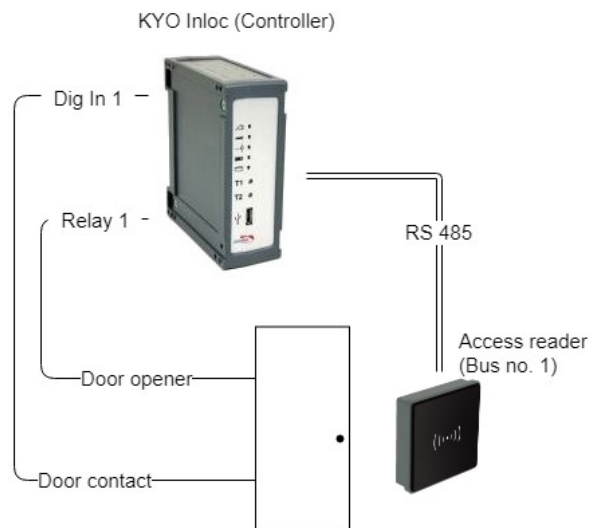
Figure 1 Diagram of a supervised door

A supervised door is a feature of the access controller that allows to lock a door as soon as it has been opened. The supervised door functionality that each door is associated to a digital input that detects if a door is opened. The digital input is assigned using the ReaderProps list.

If the opening of a door is detected, then the associated reader is determined and all realis associated to the reader are deactivated. For this, all actions associated to the reader are checked.

> **Please Note:**
> The supervised door functionality will only release relays that have been set for a defined time interval. Doors that are opened by a time model or set to free access will remain opened.

> **Caution:**
> All action entries associated to the reader will be checked and released. A check concerning the group is not implemented.

5.8.9.2. Configuration

Implementing supervised door using the Datafox Access Control modules requires the setup using the ReaderProps list. This list is required for BDS and anti-passback as well. The following specification of the ReaderProps thus contains minimal field length specifications.

5.8.9.3. Requirements for the ReaderProps entry

The ReaderProps list requires at least 5 columns when used for supervised doors.

Name	Type	Length	Description
RefReader	Number	4	Reference number of the reader, where the relay to be released is placed.
Type	Number	2	Type associated to the supervised door (5) functionality.
Mode	Number	1	Mode used for interpreting the digital input 0 (Input low) = The door is opened 1 (Input high) = The door is opened
RefReaderInput	Number	4	Reference to the reader (or door module or access controller) that provides the digital input for the supervised door.
Input	Number	2	Id of the digital input that changes upon opening of the door. 0 = the door is not supervised. 1-32 = Digital input wired to the door contact

5.8.9.4. Logical conditions implemented by the access controller
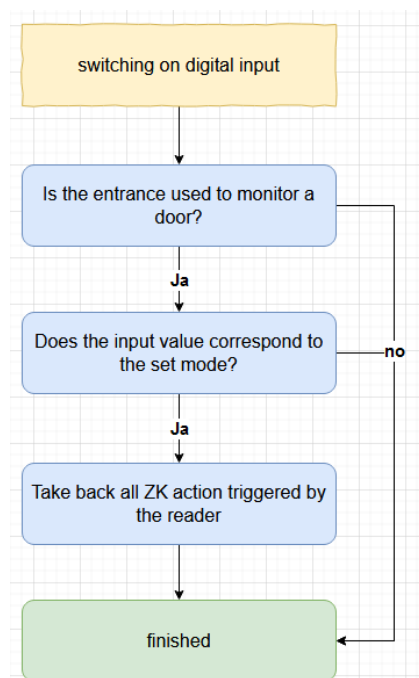
The following conditions are checked by the access controller:

(1) The check of supervised doors is started upon the change of a digital input.

(2) Next it is checked, if the digital input ("Input") and the reader ("RefReaderInput") are present within the same a supervised door entry of the ReaderProps list.

(3) If so it is checked, if the input's state matches the mode ("Mode"). If the Mode is set to 1, the input's state has to be High (1) has well, for the Mode being 0 the input has to Low (0). If the Mode matches the input's state, the state of the relay is checked.

(4) Next all relays associate to the referenced reader ("RefReader") that are set for a finite amount of time are being released. If the relay has be set to free access (FRA), blocked access (BLA) or due to a time model associated, it is not released.

5.8.9.5. Special case: Relays operated by time model

Despite a time model being active, the RFID reader will detect and read RFID transponders. The Elapse time associated to the action may overlap with the time model's activity period.
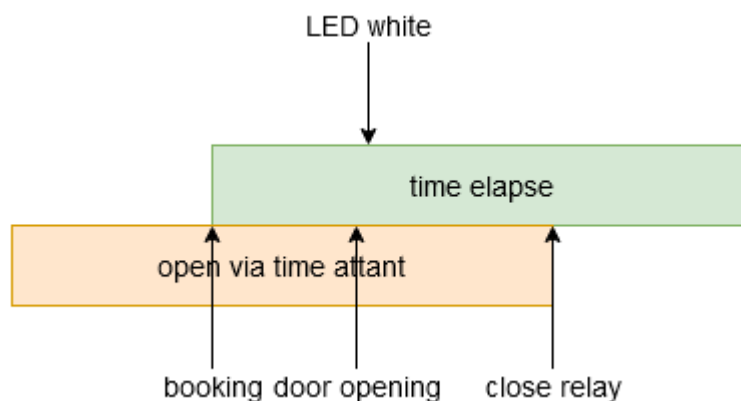
A conflict will occur if the door is opened before the time model expires. I this case the reader's LED is set to white. The relay does not toggle there and switches when the time model expires.

> **Please Note:**
> The reader's LED is not set to green if a time model sets the relay. When granting access due to an RFID transponder the LED is set to green only for 3 seconds, not for the elapse time associated to the action. This is the standard behaviour for granting access.

5.8.9.6. Configuration sample

The sample configuration explained here is associated to Figure 1. The digital input 1 is used to detect the opening of the door. A low voltage on the digital input indicated that the door is open.

5.8.9.7. Access control lists

First the two devices are declared by entries to the Reader list. ID 10 is associated to the RFID reader, which is present next to the door. ID 99 identified the access controller.

Reader.txt

ID	ZM	TM	RefLocation	RefAction	PinGeneral
10	1	010	1	100	0
99	1	320	1	0	0

The list Action2 contains the operations for opening the door. Entry 100 will be evaluated when reader ID 10 identified an RFID transponder that is allowed to open the door. The action sets relay 1 at the access controller for 10 seconds. Simultaneously the green LED is activated at reader ID 10.

Action2.txt

ID	Ref Group	Ref Time	Ref Reader Relais	PortOut	Elapse	Ref Reader Led	Ref Time Relais
100	0	1	99	1	10	10	0

The list Time contains time model 1. This time model is active 24/7.

Time.txt

ID	Weekdays	TimeStart	TimeEnde
1	1234567	00:00	23:59

The Location list must contain an entry. This entry associated the time model, so that access using the reader is possible always.

Location.txt

ID	RefGroup	RefTime	RefTimeNoPin
1	0	1	0

In order to open the door, the Identification list must contain an entry that is allowed to open the door.

Identification.txt

ID	Group	Pin	Menace	ActiveStart	ActiveEnd	ActiveGeneral
2059FB3A	0	0	0	2005-04-01	2020-04-01	1

5.8.9.8.   Additional lists

As explained earlier, the ReaderProps list is needed in addition to the access control list. If digital input 1 changes to low voltage, all doors being unlocked for a finite time will be locked again. The entry to the ReaderProps list is as follows:

ReaderPorps.txt

RefReader	Type	Mode	RefReaderInput	Input
10	5	0	99	1

5.8.10. Status messages of the access control

Display /online	Pre-checked mode for online/offline ac-cess	Assigned status message
0		module detected everything OK
3		module not in the list defined but found in the bus rs485
4		module in the list reader added but not found in the bus rs485
5		wrong Encryption password
6		login password is wrong
7		RFID-typ (Mifare, Legic, Unique, etc.) wrong
8		Failed to configure the module
9		No modules
10		the Key for communication with PHG-Modules was chonged
11		the Key for communication with PHG-Modules was not chonged
12		battery-level of the doorlock phase 0 (full)
13		battery-level of the doorlock phase1
14		battery-level of the doorlock phase 2
15		battery-level of the doorlock phase 3 (empty)
16		Doorlock in mode to change battery
17		Modul Update readdy, important applies to EVO Agera and Interra 2)
18		Reboot after update
19	519	Access denied, because BLA (blocked Access) is activate on this reader
20	520	ID ok, accses succesful
21	521	ID is not in the list identification.
22	522	ActiveGeneral not correct.
23	523	Validity period does not fit.
24	524	Could not find the room. (group definitions)
25	525	Could not find am Time in time-table.
26	526	wait for PIN-input.
27	527	Pin wrong
28	528	threat code was input.
29	529	the PIN is right, accses successful.
30	530	the Master-PIN was input, accses successful.
31	531	PIN-Timeout.
32	532	Master-ID right, accses successful.
33	533	accses successful with PIN input.
34		Online-TP.
35		Online-PIN.
36	536	Make Action closing
37	537	Free access on this reader
38	538	Permanent blocked access
39		Online-result from the server, no access allowed
	256	The server rejects the preliminary test
	257	The server agrees with the preliminary check

Digital	output
40	digital output 1 is low (off)
41	digital output 1 is HIGH.(on)
42	digital output 1 is for the time ELAPSE, HIGH.
43	digital output 2 is low (off)
44	digital output 2 is HIGH.(on)
45	digital output 2 is for the time ELAPSE, HIGH.
46	digital output 3 is low (Off).
47	digital output 3 is HIGH.(On).
48	digital output 3 is for the time ELAPSE, HIGH.
49	digital output 4 is low (Off).
50	digital output 4 is HIGH.(On).
51	digital output 4 is for the time ELAPSE, HIGH.
52 #	digital output 5 is low (Off).
53 #	digital output 5 is HIGH.(On).
54 #	digital output 5 is for the time ELAPSE, HIGH.
55 #	digital output 6 is low (Off).
56 #	digital output 6 is HIGH.(On).
57 #	digital output 6 is for the time ELAPSE, HIGH.

Status messages of the access control

display	Assigned status message digital output
120#	digital output 7 is low (Off).
121#	digital output 7 is HIGH.(On).
122#	digital output 7 is for the time ELAPSE, HIGH.
123#	digital output 8 is low (Off).
124#	digital output 8 is HIGH.(On).
125#	digital output 8 is for the time ELAPSE, HIGH.
126#	digital output 9 is low (Off).
127#	digital output 9 is HIGH.(On).
128#	digital output 9 is for the time ELAPSE, HIGH.
129#	digital output 10 is low (Off).
130#	digital output 10 is HIGH.(On).
131#	digital output 10 is for the time ELAPSE, HIGH.
132#	digital output 11 is low (Off).
133#	digital output 11 is HIGH.(On).
134#	digital output 11 is for the time ELAPSE, HIGH.
135#	digital output 12 is low (Off).
136#	digital output 12 is HIGH.(On).
137#	digital output 12 is for the time ELAPSE, HIGH.
138#	digital output 13 is low (Off).
139#	digital output 13 is HIGH.(On).
140#	digital output 13 is for the time ELAPSE, HIGH.
141#	digital output 14 is low (Off).
142#	digital output 14 is HIGH.(On).
143#	digital output 14 is for the time ELAPSE, HIGH.
144#	digital output 15 is low (Off).
145#	digital output 15 is HIGH.(On).
146#	digital output 15 is for the time ELAPSE, HIGH.
147#	digital output 16 is low (Off).
148#	digital output 16 is HIGH.(On).
149#	digital output 16 is for the time ELAPSE, HIGH.
300#	digital output 17 is low (Off).
301#	digital output 17 is HIGH.(On).
302#	digital output 17 is for the time ELAPSE, HIGH..
303#	digital output 18 is low (Off).
304#	digital output 18 is HIGH.(On).
305#	digital output 18 is for the time ELAPSE, HIGH..
306#	digital output 19 is low (Off).
307#	digital output 19 is HIGH.(On).
308#	digital output 19 is for the time ELAPSE, HIGH..
309#	digital output 20 is low (Off).
310#	digital output 20 is HIGH.(On).
311#	digital output 20 is for the time ELAPSE, HIGH..
312#	digital output 21 is low (Off).
313#	digital output 21 is HIGH.(On).
314#	digital output 21 is for the time ELAPSE, HIGH..
315#	digital output 22 is low (Off).
316#	digital output 22 is HIGH.(On).
317#	digital output 22 is for the time ELAPSE, HIGH..

digital	input
160#	digital input 7 is Low
161#	digital input 7 is HIGH
162#	digital input 8 is Low
163#	digital input 8 is HIGH
164#	digital input 9 is Low
165#	digital input 9 is HIGH
166#	digital input 10 is Low
167#	digital input 10 is HIGH
168#	digital input 11 is Low
169#	digital input 11 is HIGH
170#	digital input 12 isLow
171#	digital input 12 is HIGH
_____	____continuously until:
210#	digital input 32 is Low
211#	digital input 32 is HIGH

for new devices hardware version 4

BSD/ EMA	Discription/ Beschreibung
258[1]	The access control system awaits legitimation through RFID transponder and/or PIN after starting a BDS control event due to entering the operating code.
259	The access control system awaits legitimation through RFID transponder and/or PIN after starting a BDS control event due to entering the operating code.
260	During a BDS control event a non-privileged RFID transponder has been presented to the reader. This transponder is either not contained within the Identification table or does not have ActiveGeneral set to 7. See Privileging transponders to control the BDS.
261	The specified BDS section is not configured correctly.
262	There are no concurrent BDS control events supported while a BDS control event is currently being pro-cessed.
263[1]	The BDS signals that is ready to be armed.
264[1]	The BDS signals that is not ready to be armed.
265	The relay to arm the BDS section has been set.
266	The relay to disarm the BDS section has been set.
267	The BDS section to be armed is already armed. The reader signals "green" anyway so that the operator knows that the BDS section is armed.
268	The BDS section to be disarmed is already disarmed. The reader signals "green" anyway so that the operator knows that the BDS section is disarmed.
269[1]	The BDS section is armed now.
270[1]	The BDS section is disarmed now.
271	The BDS section could not be armed within five seconds. The digital input pin associated to the BDS section state still reports the section as disarmed.
272	The BDS section could not be disarmed within five seconds. The digital input pin associated to the BDS section state still reports the section as armed.
273	The access request was denied due to the BDS section being armed.
274	Identification requires an additional PIN.
275	The PIN entered does not match the stored one.
276	The PIN entered matches the stored one.
277	Timeout while waiting for the PIN to be entered.

1) This status code contains the BDS section [1..5] as property „ID number".
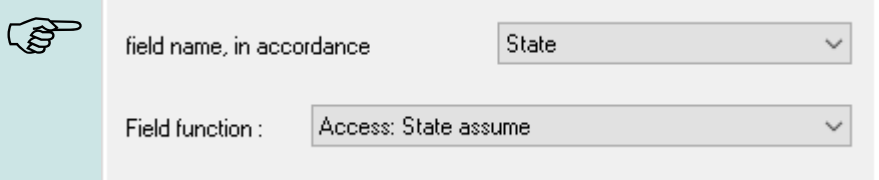
Status messages of the access control

display	Assigned status message		
100	the access-control is off.		
101	server not online (online accses-control)		
102	the device have no lists.		
103	Type not correct in setup settings (GIS, PHG).		
display	Assigned status message		
	Master (ZK-Box / ZK Master)	GIS / TS-Series reader	PHG / EVO-ZK-reader
60	Digital input 1 Master Low	Digital input 1 Reader Low	Digital input 1 (IO-Box is closed)
61	Digital input 1 Master High	Digital input 1 Reader High	Digital input 1 (IO-Box is open)
62	Digital input 2 Master Low	Digital input 2 Reader Low	Digital input 2 (IO-Box closed)
63	Digital input 2 Master High	Digital input 2 Reader High	Digital input 2 (IO-Box open)
64	Digital input 3 Master Low	Digital input 3 Reader Low	Digital input 3 low
65	Digital input 3 Master High	Digital input3 Reader High	Digital input 3 high
66	Digital input 4 Master Low	Digital input 3 wurde unterbrochen	PHG not used
67	Digital input 4 Master High	Digital input 3 wurde kurz geschlossen	PHG not used
68	Digital input 5 Master Low	not used	not used
69	Digital input 5 Master High	not used	not used
70	Digital input 6 Master Low	not used	digital input 1 the Reader Low nicht bei der Voxio-E-Serie
71	Digital input 6 Master High	not used	didigital input 1 on the Reader High nicht bei der Voxio-E-Serie
72		not used	digital input 2 on the Reader Low nicht bei der Voxio-E-Serie
73		not used	digital input 2 am Reader High nicht bei der Voxio-E-Serie
74		not used	tamper switch ➔ OK
75		not used	tamper switch ➔ device manipuliert
display	Assigned status message		
80	alarm-input 1		
81	alarm-input 2		
82	alarm-input 3		
83	alarm-input 4		
84	alarm-input 1		
85	alarm-input 6		
220#	alarm-input 7		
221#	alarm-input 8		
_____	_____ continuously until:		
245#	alarm-input 32		

for new devices hardware version 4

Status message of the access control in a record:

Note:
Do you want see the status from access control, to choose this settings in the Setup.

field name, in accordance	State
Field function :	Access: State assume

5.8.11.   State signals of reader modules via LEDs

Gelb	Grün	Rot	Zustand des TS TMR33-xx
off	off	off	No supply voltage is present
on	off	off	A supply voltage is present,
on	on (ca. 1 s)	on (ca. 1 s)	Reader recognized and configured by master
on	off	on (ca. 10 s)	Status after module test = status "OK
on	off	on (permanent)	Acoustic signal by buzzer (approx. 1s) signals module test
flash	off	off	The lists of the access master are updated
on	on (ca. 1 s)	off	Configuration error via the access lists (Checking of the
on	on	on 3 x short	status messages necessary.)
on	flash	off	Signals readable card in the area,

## 5.8.12. Function for access control U&Z (locking cylinders)

5.8.12.1. Design example

The radio locking cylinders are set up and integrated via the standard Datafox access control system. The PHG crypt protocol is used. All data is thus securely encrypted.

Functionality:
The electronic locking systems read an RFID chip / card and transmit the read information to Datafox access control. The Datafox access control then decides on the basis of the access logic whether the door is opened or not.

Design example with integrated radio module in the KYO Inloc.
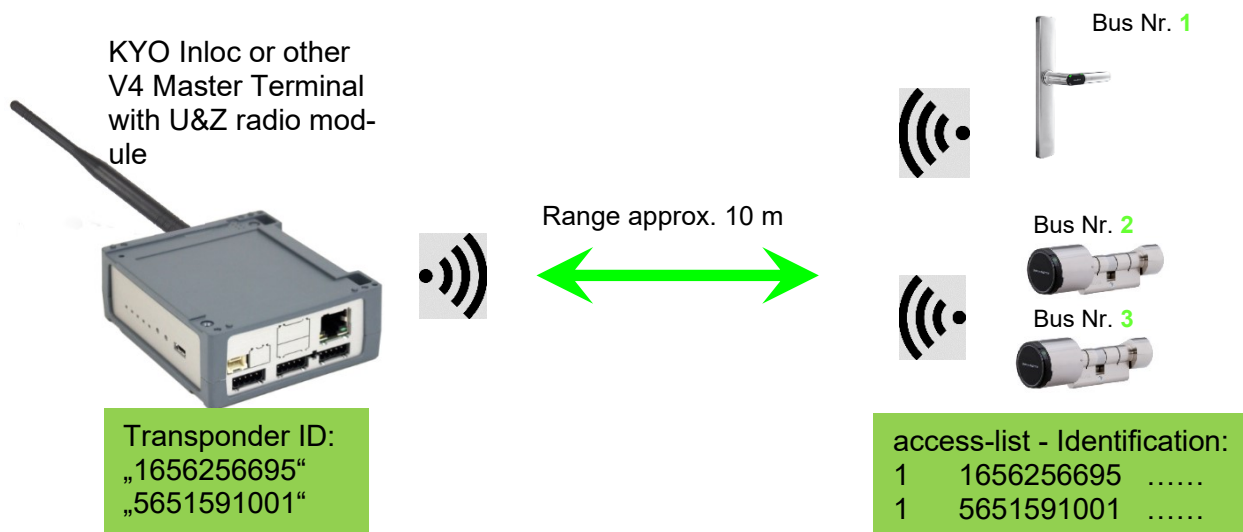
Entsprechende Reader Tabelle, Beispiel:

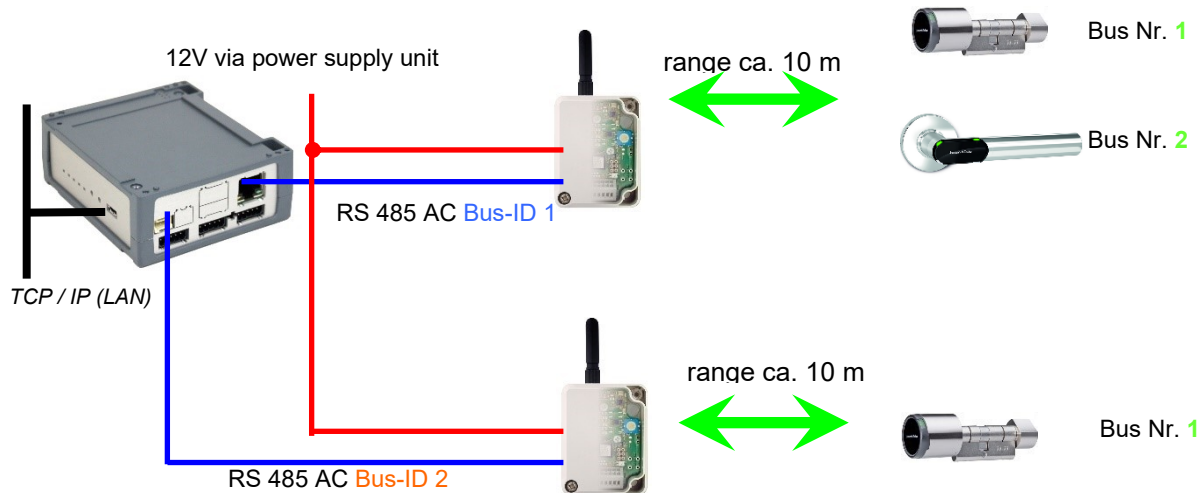| ID	ZM / Bus-ID	TM (Busadresse)	RefLocation	RefAction	PinGeneral	Description-text
1	1	010	1	1	0	Reader - RS485 module slot 1 = Bus ID 1
2	1	020	2	2	0	Reader - RS485 module slot 3 = Bus ID 1
3	1	030	3	3	0	Reader - RS485 module slot 7 = Bus ID 2

> ☞ **Note:**
> The transponders are read by the cylinder and the ID is transferred to the ZK-Box. It then decides whether the ID access is granted and sends a corresponding signal to the cylinder.

> ☞ **Note:**
> Only one radio lock cylinder can be used at a time!
> From booking to termination of the radio connection we need approx. 2 seconds for a rejection. With an opening approx. 1 second.
> If ID cards are held on two or more doors at exactly the same time, the first locking cylinder has the connection with the FSM for approx. 2 seconds. If a radio lock cylinder does not receive a radio connection after 1 second, it performs an offline check. If no ID cards have been deposited, they will no longer respond to the ID card. The badge is then stored in the reader and the system no longer reacts to this badge (repeat posting block) until another badge is available.

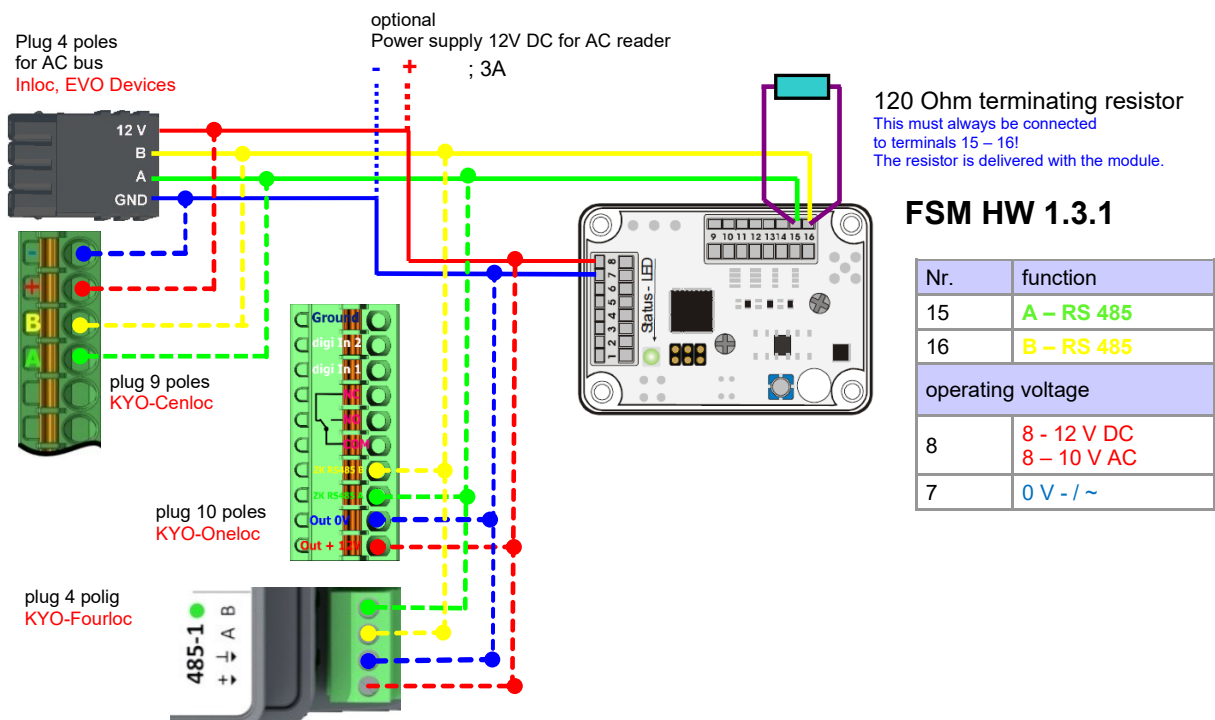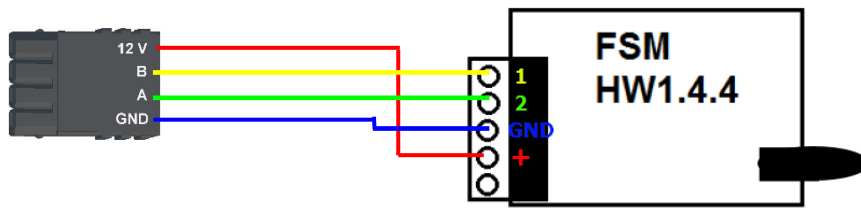## Construction example KYO Inloc with two external radio- or BLE- modules.

12V via power supply unit

range ca. 10 m

Bus Nr. **1**

Bus Nr. **2**

RS 485 AC Bus-ID 1

TCP / IP (LAN)

range ca. 10 m

Bus Nr. **1**

RS 485 AC Bus-ID 2

Corresponding reader table, example:

ID	ZM / Bus-ID	TM (Bus-address)	RefLocation	RefAction	PinGeneral	Description-text
1	**1**	0**1**0	1	1	0	reader RS485 module slot 1 = Bus ID 1
2	**1**	0**2**0	2	2	0	Reader RS485 module slot 3 = Bus ID 1
3	**2**	0**1**0	3	3	0	reader RS485 module slot 7 = Bus ID 2
4	1	320	0	1	0	KYO Inloc (Master-device)

Wiring diagram of the different bus connections with external radio module:
(In this case, the same structure applies per access control string or ZM / Bus-ID)
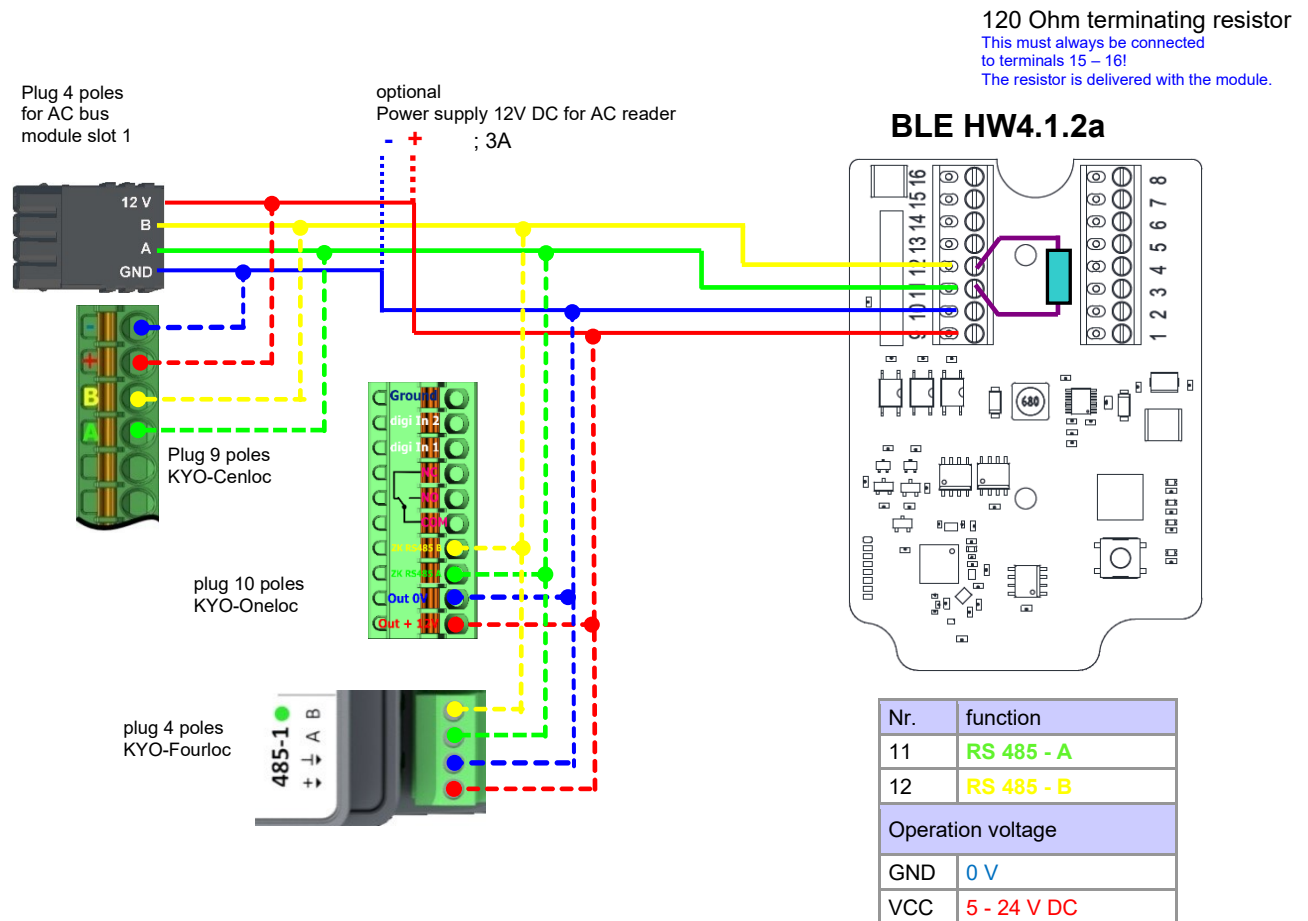

Plug 4 poles
for AC bus
Inloc, EVO Devices

optional
Power supply 12V DC for AC reader
; 3A

120 Ohm terminating resistor
This must always be connected
to terminals 15 – 16!
The resistor is delivered with the module.

12 V
B
A
GND

plug 9 poles
KYO-Cenloc

plug 10 poles
KYO-Oneloc

plug 4 polig
KYO-Fourloc

FSM HW 1.3.1

Nr.	function
15	A – RS 485
16	B – RS 485
operating voltage	
8	8 - 12 V DC 8 – 10 V AC
7	0 V - / ~

Nr.	function
1	B – RS 485
2	A – RS 485
Operation voltage	
GND	0 V + / ~
VCC	8 - 12 V DC 8 – 10 V AC

Wiring diagram of the different bus connections with external BLE-Modul:
In this case, the same structure applies per access control string or ZM / Bus-ID

120 Ohm terminating resistor
This must always be connected
to terminals 15 – 16!
The resistor is delivered with the module.

Plug 4 poles
for AC bus
module slot 1

optional
Power supply 12V DC for AC reader
; 3A

BLE HW4.1.2a

Plug 9 poles
KYO-Cenloc

plug 10 poles
KYO-Oneloc

plug 4 poles
KYO-Fourloc

Nr.	function
11	RS 485 - A
12	RS 485 - B
Operation voltage	
GND	0 V
VCC	5 - 24 V DC

5.8.12.2. First start with locking cylinders

The scope of delivery always includes a service card.
To install the cylinders, you also need a disassembly card.
These have not yet been created in their as-delivered state.

Hold the service key in front of the knob module. (A)
An optical/acoustic signal indicates that the programming mode is active (possibly before this step, the wake-up function of the knob module may be required by turning it)

With firmware 2.7.0, there is only an acoustic signal about activation of the service mode!

Teaching:
1) The first card that is held = battery exchange card
2) The second card becomes the = disassembly card

5.8.12.3. Assembly and disassembly of the cylinders

1) Hold the disassembly card in front of the knob module (A)
(Possibly the knob module may need to be woken up by turning the knob before this step).

2) Knob module enters disassembly mode.

3) Turn the knob module until the emergency power contacts are in the 9 o' clock position. (B)

4) Remove the knob by slightly turning it back and forth and pulling it lightly at the same time. (C+D)
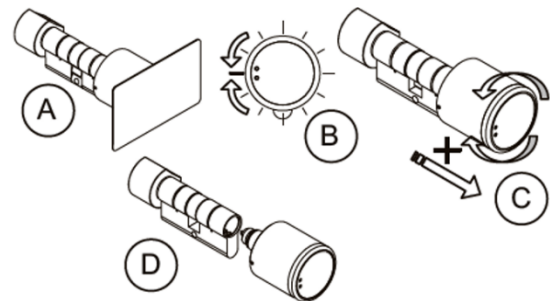
1) Carry out steps 1 and 2 as described in the point above (not necessary if the knob module is still in disassembly mode).

2) The knob module is mounted in the cylinder housing by inserting and simultaneously rotating it. (A+B)

3) To reset the disassembly mode, hold the disassembly card or an authorized transponder in front of the knob module. (C)
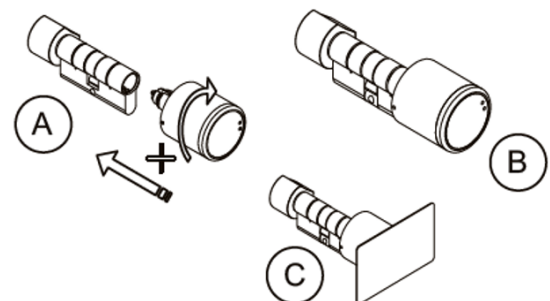
5.8.12.4. Set up the wireless network for cylinder

For setup, DatafoxStudioIV can be used in conjunction with the service key card. To do this, select "Configuration→Access control→Configure U&Z locking cylinder" in DatafoxStudioIV. With "Update data" the current configuration is read from the FSM.
In connection with the BLE module, only addresses 000 - 070 can be used.
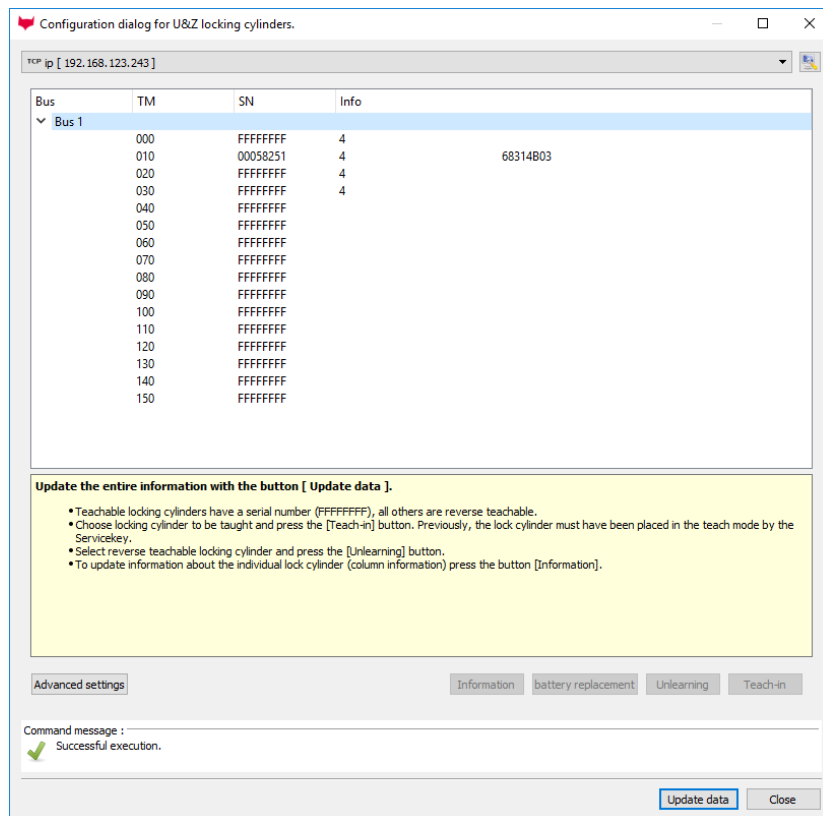
Steps of teaching-in the cylinders:

1. Hold service key to cylinder
(Service = 20 seconds active (activate cylinder by turning it briefly!))

2. Refresh data in DatafoxStudioIV!
Free addresses are displayed with FFFFFFFFFF, the serial number of the radio lock cylinder and the status of the modules are displayed for the assigned addresses, as in the dialogue Status of the access modules.
The "Configuration dialog for U&Z locking cylinders" dialog allows different things to be done.
Advanced settings:
- Setting the ZK-Master ID for the device
- KnobActiveTime: Time that the cylinder tries to reach the FSM after activation until it goes back to standby.
- Update information on individual locking cylinders (column "Info")
- Changing the battery puts the radio lock cylinder into a mode that allows the cover to be removed and the battery to be changed. To do this, brief communication with the FSM is required. This is achieved by turning the knob or holding a transponder in front of it.
- Teach out: The cylinder is removed from the FSM and can be taught in to another FSM.
- Teach-in: To connect a radio lock cylinder to the FSM (the radio lock cylinder then only communicates with this FSM)

5.8.12.5. Battery state and live time
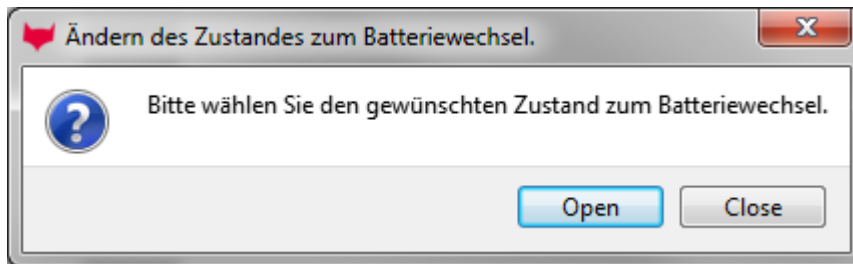
With "Open" the command to open is sent to the FSM. This stops the command until a radio connection is established. This can be achieved by turning or holding a transponder in front of it. The locking pins of the hood are then unlocked.

With "Close" the command for locking the hood bolts is sent back to the FSM. However, the lock is only established after a good entry / opening.

The three phases of battery management
Phase 1
If an authorized ID card is held in front of the knob module, the locking authorization is granted in accordance with the programming. However, the door opening is accompanied by 5x red flashing (LED) and 5 short acoustic signals at the same time.

Phase 2
If an authorized ID card is held in front of the knob module, the locking authorization is only granted after approx. 5 seconds according to the programming. During these 5 seconds the LED flashes green. The door opening is accompanied by 5x red flashing (LED) and 5 short acoustic signals.

Phase 3
The knob module no longer responds to authorized ID cards. Replace the battery immediately. This is now only possible using the service key and the service device or the battery replacement card.

Please also note the corresponding status messages from the access control system:

display	Assigned status message
0	Module detected, everything's OK.
12	Battery status of the radio lock cylinders in phase 0 (full)
13	Battery status of the radio lock cylinders in phase 1
14	Battery status of the radio lock cylinders in phase 2
15	Battery status of the radio lock cylinders in phase 3 (empty)
16	Radio lock cylinder set to battery change mode

5.8.12.6. Change the access control master ID and knob Active Time

To change the access control master ID, the "Configuration dialog for U&Z locking cylinders" dialog must be used. It contains "Advanced settings" and with a click on it this dialog opens.
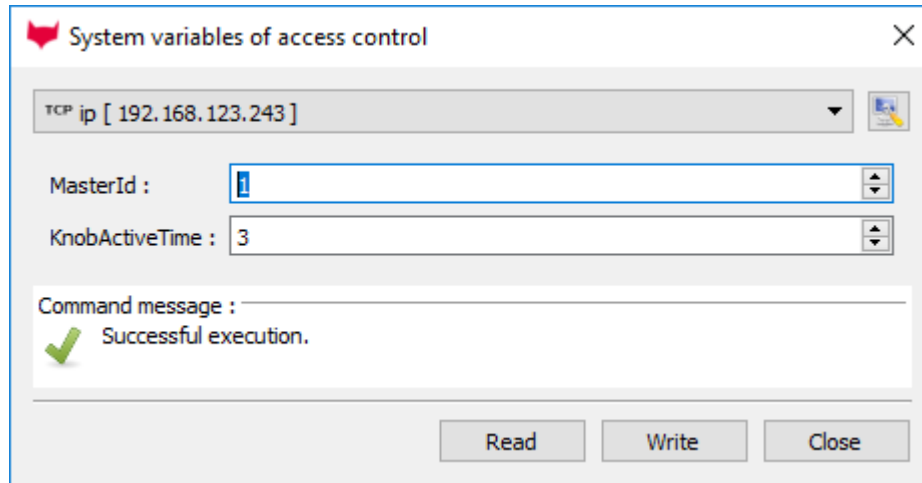
Master ID can be set in the range from 1 to 9999. If a device has more than one access control bus, the access control master ID is the ID of the first bus. The second bus access-control-Master ID + 1 etc.

The Knob Active Time is for presetting how long a radio lock cylinder maintains radio communication with the FSM when activated. When a transponder booking is made, the access control master automatically closes the connection after signaling and opening. If the Knob Active Time is less than required for the transponder booking, the radio lock cylinder switches off and an opening fails. This happens at e. g. Knob Active Time = 1 (1s). If someone turns the knob of the radio lock cylinder, the radio connection to the FSM is established and the connection remains active as long as the Knob Active Time is active. Useful values are between 2 and 10 seconds. By default, this time is set to 3 seconds.
It makes sense to increase the value if three or more radio participants are connected to a radio module. Recommendation: KnobActiveTime = 6 seconds

5.8.12.7. Optical and acoustic signals of the U&Z locking cylinder

function	sounds	Optical signals
sleep mode		
Start programming mode	**- O**	🟢 (except with FW 2.7.0)
badge trained	**O O**	🟢
Badge deleted	**- -**	🔴
warning signal Delete all badges	**O O O O O** 15 sek.	🟢
End of programming mode	**O -**	
After wake-up - Read mode		🟢
Badge not authorized	**- - -**	🔴
badge authorized	**O**	🟢
After battery change	**- - -**	🟢🔴
No radio link (out of range)	No sound	🔴 **long** 🔴 **short** 🔴 **short**

🔴 **=** red lights up   🔴**=** red flashing
🟢 **=** green lights up   🟢**=** green flashing

- = long low tone
O = short beep

### 5.8.12.8. Optical and acoustic signals of the U&Z door handle

function	sounds	Optical signals
Sleep mode		
Begin programming mode	– O	
End programming mode	O –	
Badge trained	O O	🟢
Badge deleted	– –	🔴
After wake-up - read mode		🔴 (red flashing)
Badge not authorized	– – –	🔴
Badge authorized	O	🟢
Reset	–	🟢🔴
Battery warning Phase1	O O O O O	🔴🔴🔴🔴🔴
Battery warning Phase2	O O O O O	🔴🔴🔴🔴🔴🟢

🔴 **=** red lights up 🔴**= red flashing**

🟢 **=** green lights up 🟢**= green flashing**

- = long low tone

O = short beep

5.8.12.9. Resetting the U&Z locking cylinder

1.) The knob module must have been taught out in the radio module.
2.) Hold the service key in front of the knob module for the duration of a programming mode (15 seconds) and repeat the procedure within 60 seconds. At the end of the second programming mode, this deletes all badges (incl. battery change and disassembly card) except for the Servicekey. (A+B)
3.) The existing badges can then be re-learned as described in section 9.1. **Here, the first ID card held is used for the battery change card and the second to the disassembly card.**

A 🔘 grün + 2x 🔊

Innerhalb
60 Sek.

B 🔘 grün
+
15 Sek. 🔊
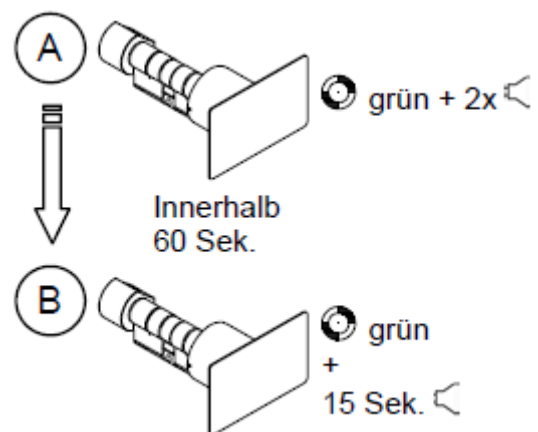
5.8.12.10. Supported transponder technologies

Transponder for 125kHz
Supported is
- read Unique
- read Hitag1
- read Hitag2 only serial number

Not supported is
- reading of Hitag2 segments
- reading of Titan, Q5 und ATA5577

Mifare Classic
Supported is
- read UID
- read Sector/Block
Not supported is
- Autologin (for reading all passwords)

Mifare Plus
Supported is only Security Level 1
- read UID
- read Sektor/Block
Not supported is
- Autologin (Use the default passwords for reading)
- Random UID (Read true UID at Random UID badges)

Mifare Desfire
Supported is
- read UID
- Read file (max. 220Byte)
Not supported is
- Random UID (Read true UID at Random UID badges)

Legic Prime and Legic Advant
currently no restrictions are known.

1.1.1.1 Service key broken / lost

In the case that an authorization medium is damaged or lost, a replacement service key (CX2352) can be ordered from U&Z with the system card.
The system card must therefore be kept safe and inaccessible to unauthorised persons.

1.1.1.2 Replace service key

The service key can be replaced by another one.
Method:

1. Hold the current service key in front of the knob module until the programming mode is active.
2. Hold the new service key in front of the knob module until an optical/acoustic signal indicates that the service key is taught in.

1.1.1.3 Technical data of the radio module

Technical data CX 6932	
dimensions radio module without antenna: 65x50x40 mm radio module with antenna: 111x50x40 mm	**Environmental conditions** Operating temperature: -20°C to 65°C Storage temperature: -40°C to 85°C
Power supply Supply voltage: 8-20V= or 8-16 V~ Power consumption: Typ. 10mA (standby), max. 50mA (send/receive)	Installation location: Indoor and outdoor areas (depending on the product design). Avoid shading! When used outdoors, the external conditions must be checked.

5.9. RFID Reader

The RFID reader is built-in the EVO 2.8 Pure If this option is available, see the type label and the label on the backside. By DatafoxStudioIV you can enable the RFID reader. For more information see the manual of DatafoxStudioIV.

For reading a transponder you must hold it in front of the device. The reading area is marked with the corresponding icon.

The following transponder readers can be built-in the EVO 2.8 Pure :

EVO 2.8 Pure with 125 kHz: Unique EM4102, Hitag1, Hitag2, HitagS, Hewi EM4450
LRW 8 cm R/W (LeseReichWeite "Read range" with card)

EVO 2.8 Pure with Legic-Prime/Advant: LRW 4 cm   R/W

EVO 2.8 Pure with Mifare-Desfire: LRW 4 cm   R/W für MifarePlus / 7 Byte UID necessary

EVO 2.8 Pure with i-Button-Leser: Touchmemory only reading

EVO 2.8 Pure with HID 125kHz: LRW 4 cm   only reading   ProxPoint Plus 4065

EVO 2.8 Pure with HID-iCLASS: LRW 4 cm   only reading   13,56MHz

EVO 2.8 Pure with Nedap: LRW 4 cm   only reading

EVO 2.8 Pure with SimonsVoss Smart-Relais: LRW optimum at approx. 20 cm! If the transponder is too close, it might be not recognized. (interface Siemens: CLS-Signal=Yes).

☞ **Note:**
More information you found in the manual from DatafoxStudioIV chapter „The RFID Technology"

5.10. Data on Card

5.10.1. General Infomation

With the Data on Card - function it is possible to write data with an individual structure on a transponder.
These data are provided in the form of a list of your application.
This list is loaded onto the terminal, and if you´re holding the transponder in front of the terminal the data will be written and saved.
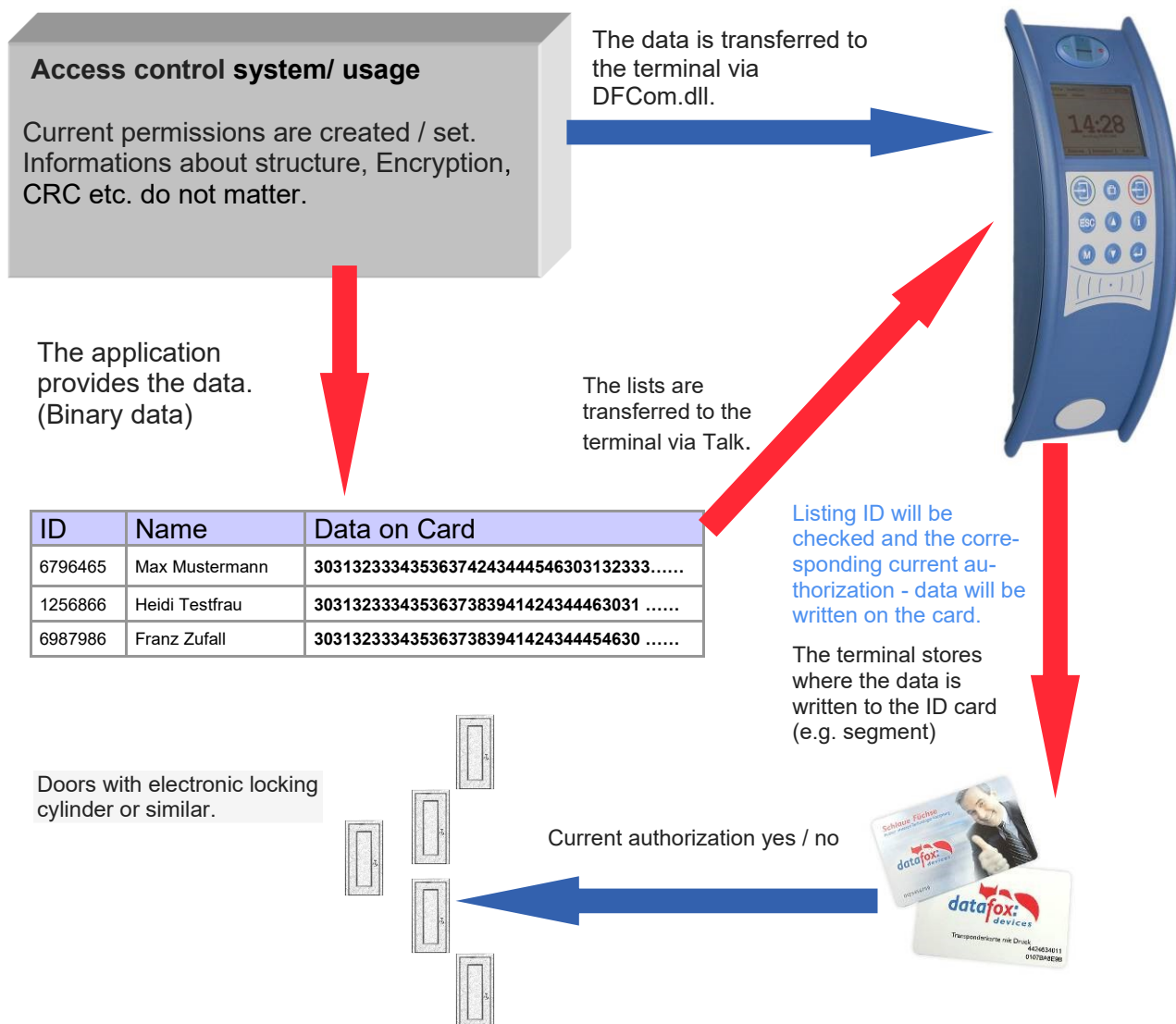The following transponder-procedures support the Data on Card-function:

- Mifare
- Legic
- iCode
- MyD

For instance:
In buildings with an electronic closing cylinder should the actual daily authorization for the access be wrote down on a transponder card.
The Personal ID will be checked and the corresponding current authorization - data will be written on the card.The terminal stores where the data is written to the ID card (e.g. via segment).

Access control system/ usage

Current permissions are created / set. Informations about structure, Encryption, CRC etc. do not matter.

The data is transferred to the terminal via DFCom.dll.

The application provides the data. (Binary data)

The lists are transferred to the terminal via Talk.

ID	Name	Data on Card
6796465	Max Mustermann	3031323334353637424344454630313233……
1256866	Heidi Testfrau	3031323334353637383941424344463031 ……
6987986	Franz Zufall	3031323334353637383941424344454630 ……

Listing ID will be checked and the corresponding current authorization - data will be written on the card.

The terminal stores where the data is written to the ID card (e.g. segment)

Doors with electronic locking cylinder or similar.

Current authorization yes / no

5.10.2. Settings for using DataOnCard

Data on Card is an option of the device where data can be written to a transponder from a data list. This option needs to be stated and said while you ordered your product. Those devices who don´t offer this option, an error message will be displaying when it´s executed.
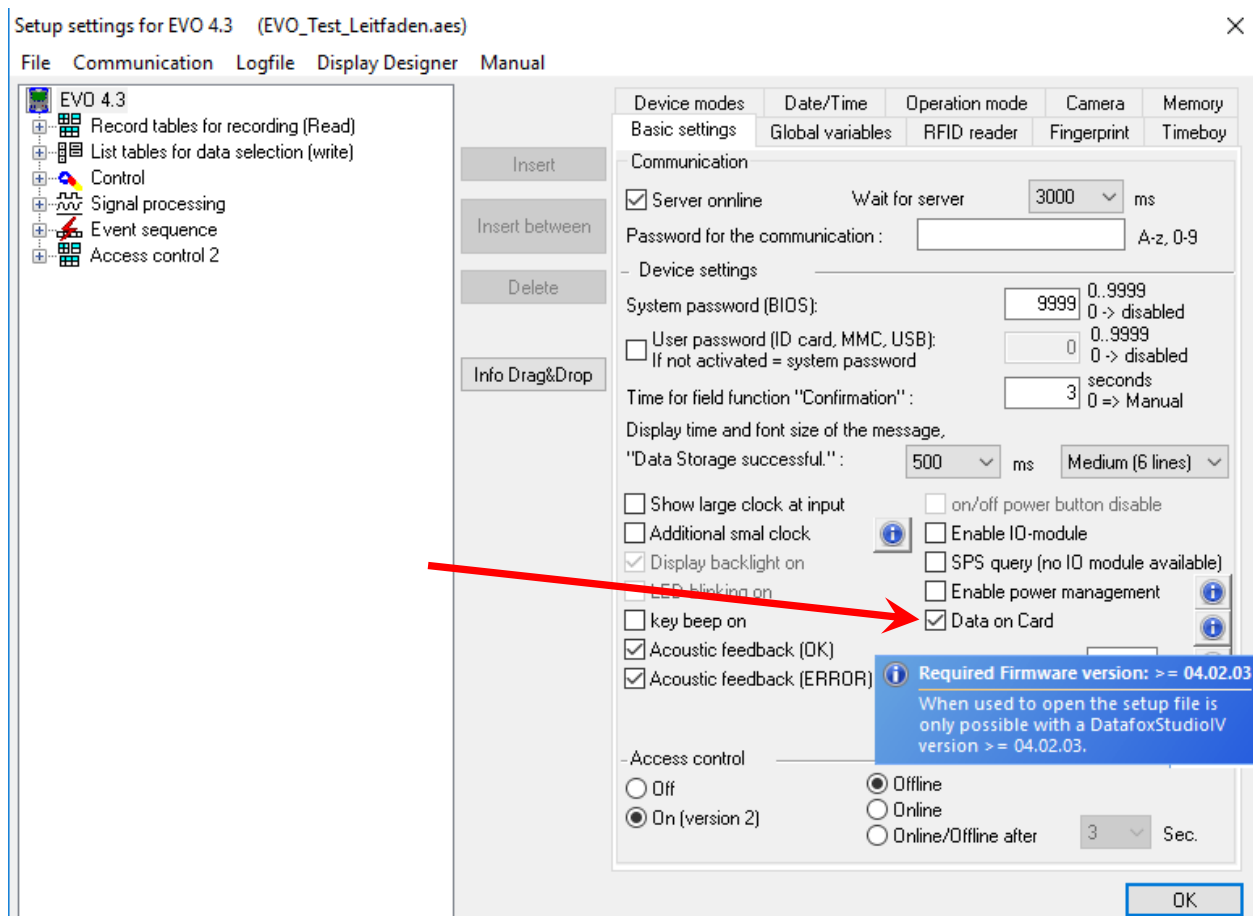
Data on Card works in 3 steps:

- reading a value from the transponder, e.g. Serial number
- the value is used to select a binary field list to read the binary data
- the binary data is written to the transponder

The return value of the Data on Card function for GV or data record field is the value from the first step "Reading a value from the transponder".
For errors like "the value is not found on the list" or the "writing to the ID failed" the function generates an ESC.
The side steps can then be used to decide how the work continues in the input chain.
The binary field data within the file that the DatafoxStudioIV imports and transmits is to be specified as a hex string. When importing via the DLL, the data needs to be passed on as binary data.
Using the DFC GetField, DFC GetField list functions, you are working with strings, while the firmware converts the hexstrings to and from the binary data.

Settings for Data on Card

1.) RFID Configurations for the RFID reader

The transponder configuration for the reading can be freely selected. However, firstly it needs to be defined in the basic transponder settings.

2.) List / binary file structure

By the list configuration the list who has a binary field will be selected.
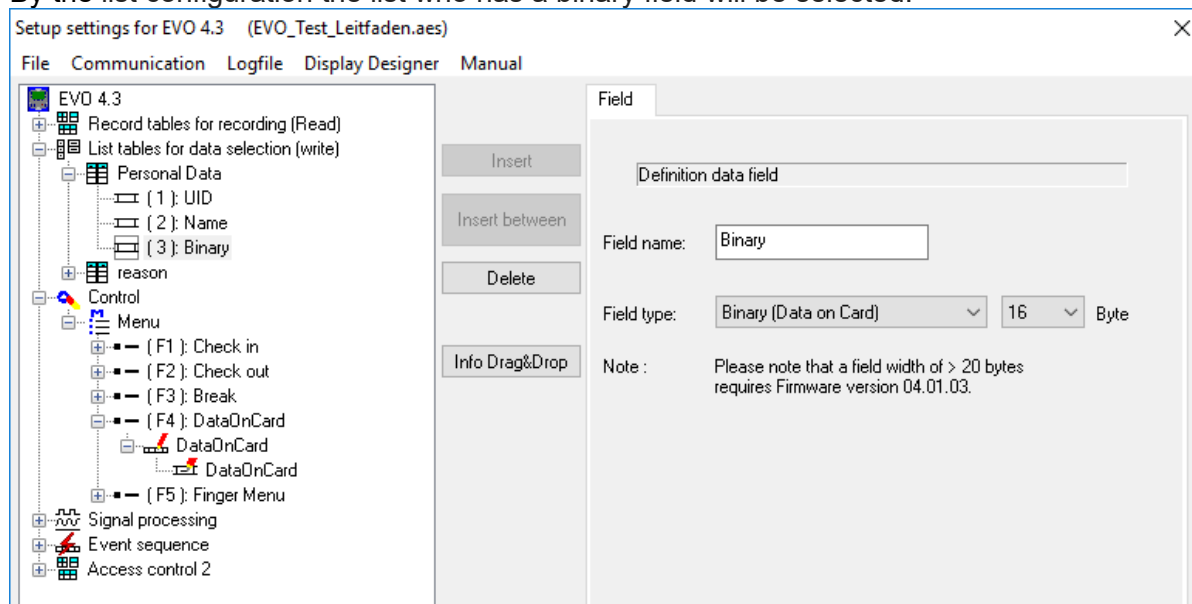
In this example, the value of the transponder reading, who is wanted in the list in the ID field. The data that needs to be written is binary on the Data on Card field. The maximum field size is not allowed to exceed more than 220 bytes. After this, the further procedure can be set for list errors.

3.) RFID configuration for „write on a RFID tag"
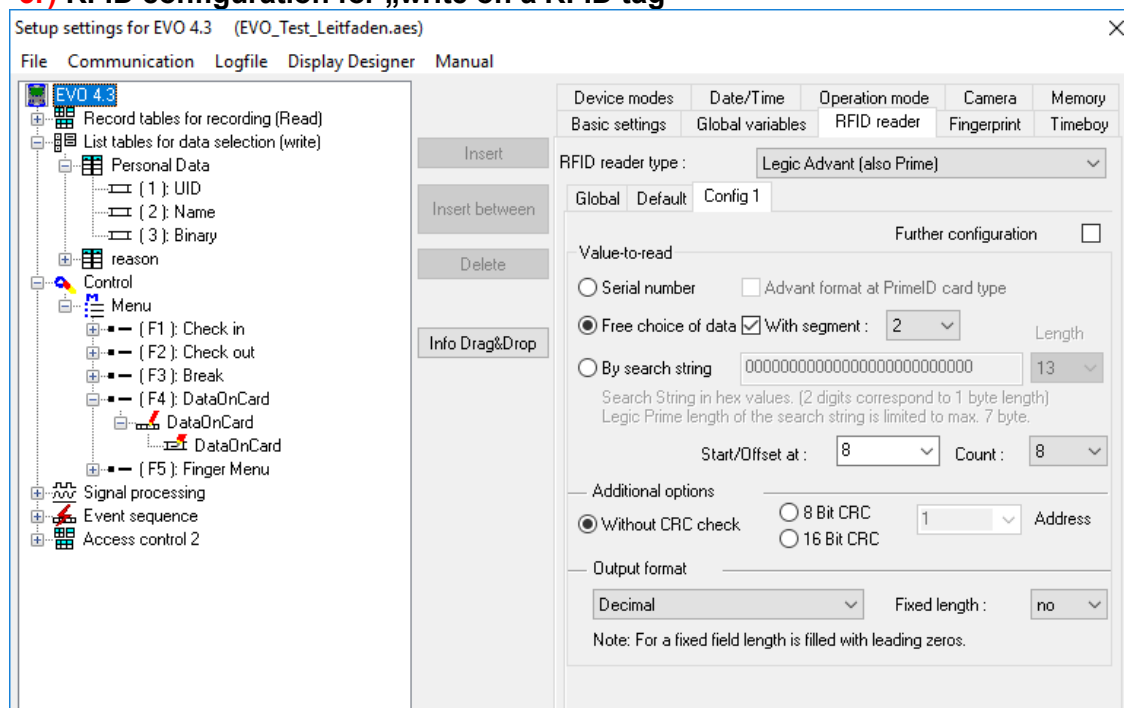
The transponder configuration for the reading can be freely selected. However, firstly it needs to be defined in the basic transponder settings.

☞ **Please note:**
First, complete the transponder configuration, then create the list with the binary field and finally parameterize the field function Data on Card.

Example for Data on Card:

ID with serial number: **1848989745**

List entry for **1848989745** in the file before transferring to the device
Field ID   Field Data (binary field) here as hex bytes
1848989745   30313233343536373839414243444546303132333435363738394142434445463031323334353637383941 ......

Data after conversion or within the device
Field ID Field Data (binary field) is binary here
1848989745   0123456789ABCDEF0123456789ABCDEF0123456789A .....

The following data will be written on the ID card:
0123456789ABCDEF0123456789ABCDEF0123456789A .....
Binary the data looks like this:
0x30, 0x31, 0x32, 0x33, 0x34 ……

Please note:
When a 3-tone sequence is signaled, the Data-On-Card option is not available on this device. The option has to be purchased afterwards.
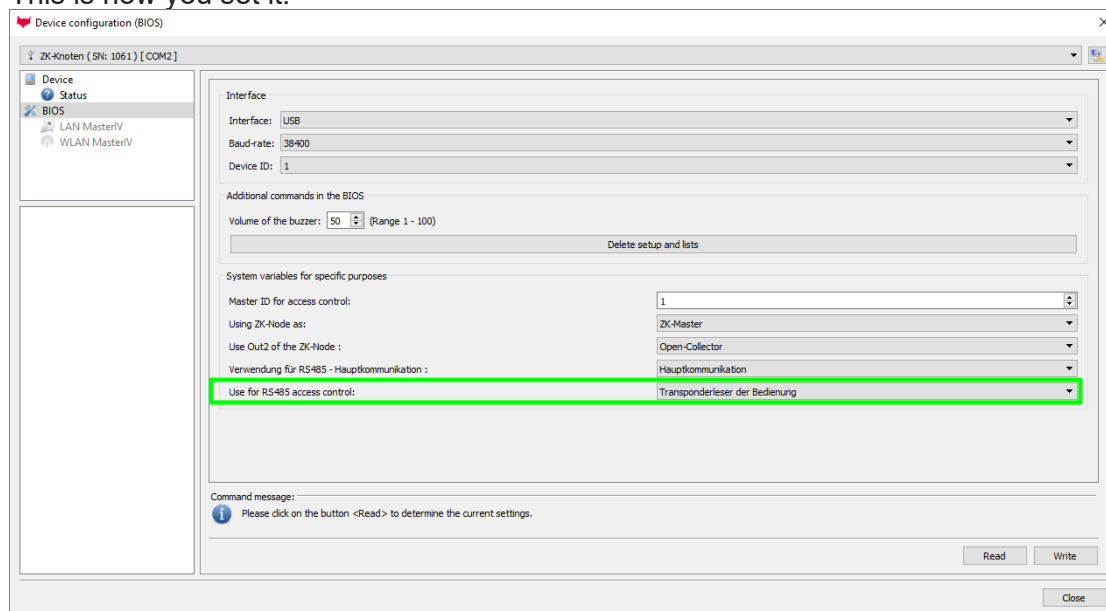
5.10.3. DataOnCard on the access control reader

In order to be able to use on a standard ZK reader of the EVO or the PHG series, the following settings must be made.

The functions for DataOnCard described in the previous chapters can only be set in the setup under Control menu.
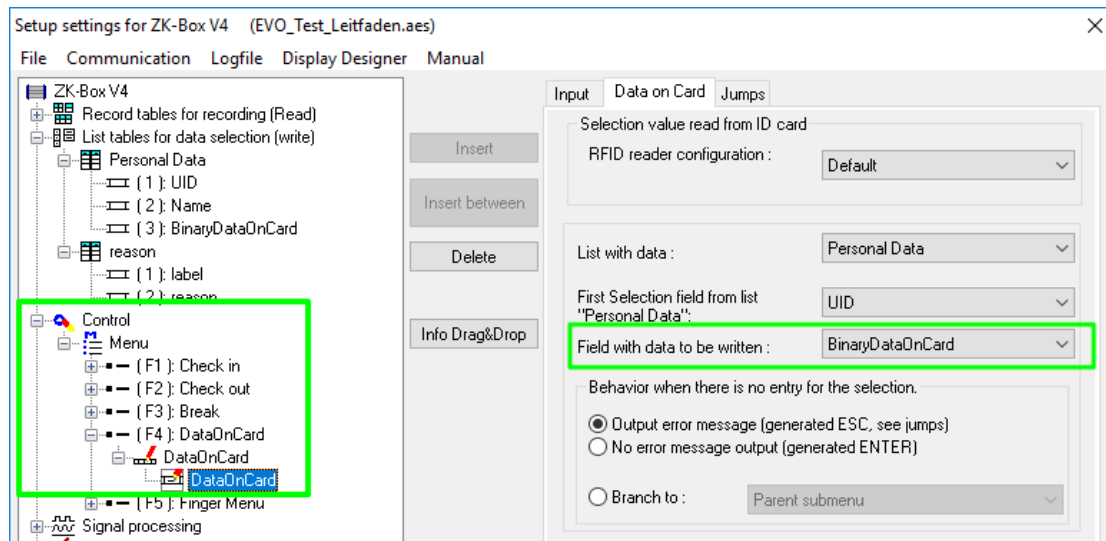
Now it is necessary to be able to access the *access control reader* under the control.
This is how you set it:

The reader on the *access control reader* (ZK) bus (RS485) is now activated via the Control menu (Operation transponder reader)

> **Please note:**
> ☞ Only one *access control reader* (ZK) can be connected to the bus at any time.
> Dip switch 1 and the termination of the bus must be set to "ON"
> (Bus address 1).

5.10.4. DataOnCard and a access control reader - wiring

5.11. Barcode Reader

You can use a internal barcodereader 2d or 3d and
you can connect any barcode reader with a RS232 port to the EVO 2.8 Pure. Observe the following
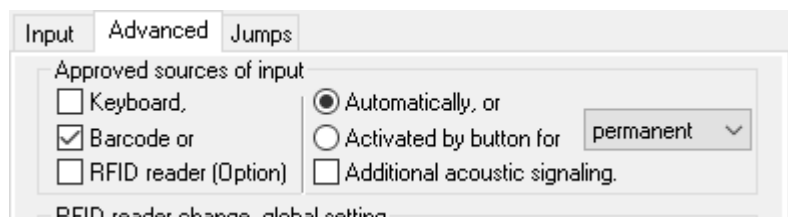pin assignment of the RS232 interface.
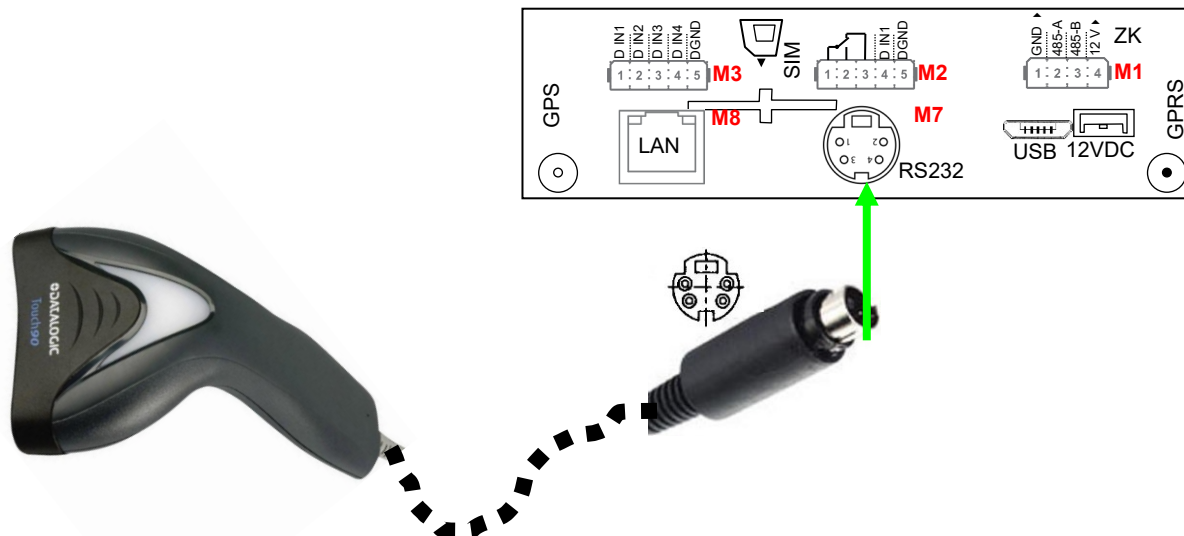
Description	Modulplace	PIN	Function
RS 232 Mini-DIN M004	Here an exa- mple on **M7**	1	TXD
		2	RXD
		3	+ 5 V
		4	Ground / GND

Barcodes that are read in can be up to 255 characters long. This is supported by the field function
"Normal (value transfer from ID card, etc ...)".

From this 255 characters can you coppy maximum 60 in a global variable.
More information about cut a value find you in the manual DatafoxStudioIV in the chapter "Normal
(value transfer from ID card, etc ...)".

Setting in the DatafoxStudioIV:

Cable attachment of the barcode reader:

Place the cable of the barcode reader in the wall bracket approximately in this way or fix the cable with a cable tie.
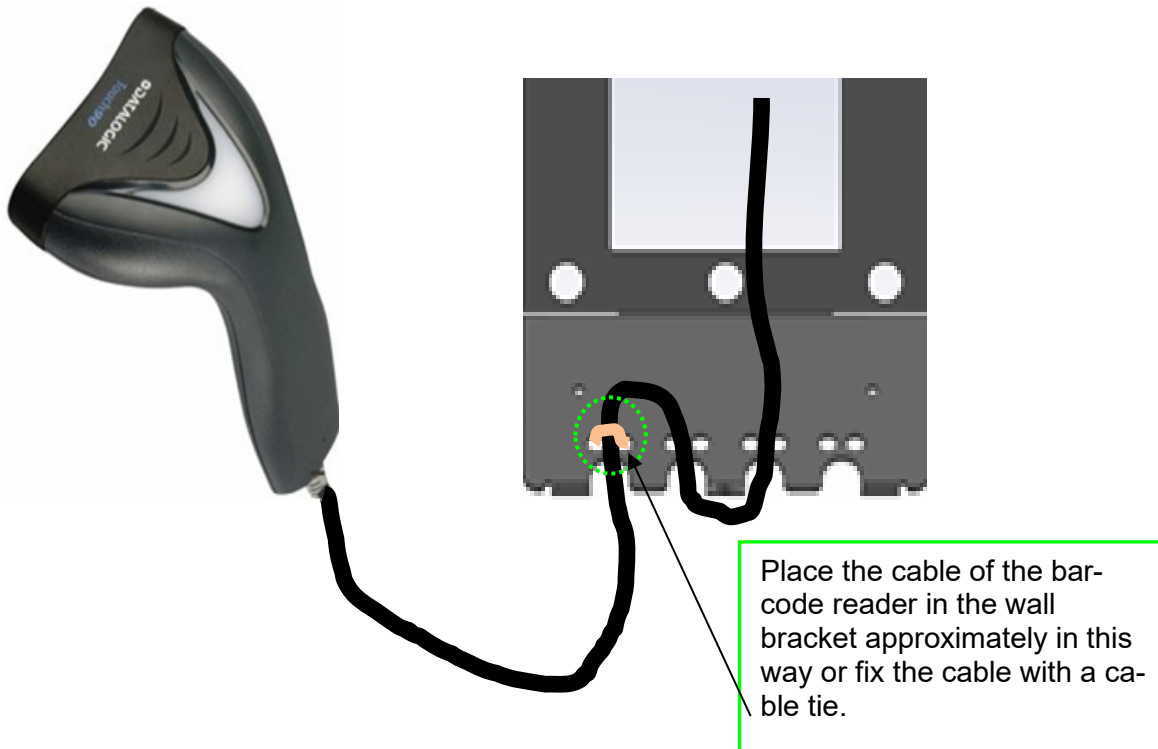
5.12. Fingerscanner optical sensor

In response to many customer requests, we have added a new finger sensor to our product range. This is an optical surface sensor.

RGB LED
The LED is controlled by the setup of the device.
See field function
"Switch the backlight."

Optical area sensor.

Advice:
The background LED illumination is only on when a finger is placed on the sensor.

With the sensor, a new menu navigation was also introduced for teaching in and deleting the fingers. The menu is called up automatically when the Administration field function is called up in the setup (device configuration).
The menu contains 6 pages: **Check fingers, teach fingers, train fingers; delete individual fingers and delete all fingers. In addition, Finger Writing on Card can be active.**

You can select the individual menu items!

You can also watch the handling of the new finger sensor in our video.
https://www.datafox.de/video-verwendung-und-einlernen-einer-fingerprintloesung-mit-optischen-flaechensensor.de.html

5.12.1. Menu Page - Check Finger

This page is used to find out which finger provides the best scan result and how the finger should best be placed on it. To do this, place your finger as straight as possible with light pressure on the sensor. The most important area is the middle of the foremost finger link.
Take your time to select the fingers that provide the best possible image. Please observe the pictures and instructions below.
If the overall picture is too pale, this could be due to the dryness of the finger. Slight rubbing or breathing on the fingertip improves this considerably, see also the example pictures below.

If the finger is scanned, the corresponding image is displayed here.

Please compare with the pictures next to it whether the picture offers sufficient quality.

Once you have selected the appropriate fingers, press the arrow ,
to move to the next page.

5.12.2. Menu page - "Teach in" fingerprints

Select the finger you want to teach in by simply tapping on the corresponding finger shown in the display! The dark grey fields symbolize the two hands, the thumbs are in the middle.

For EVO 2.8/3.5 devices this range is equal to the "ENTER" key.
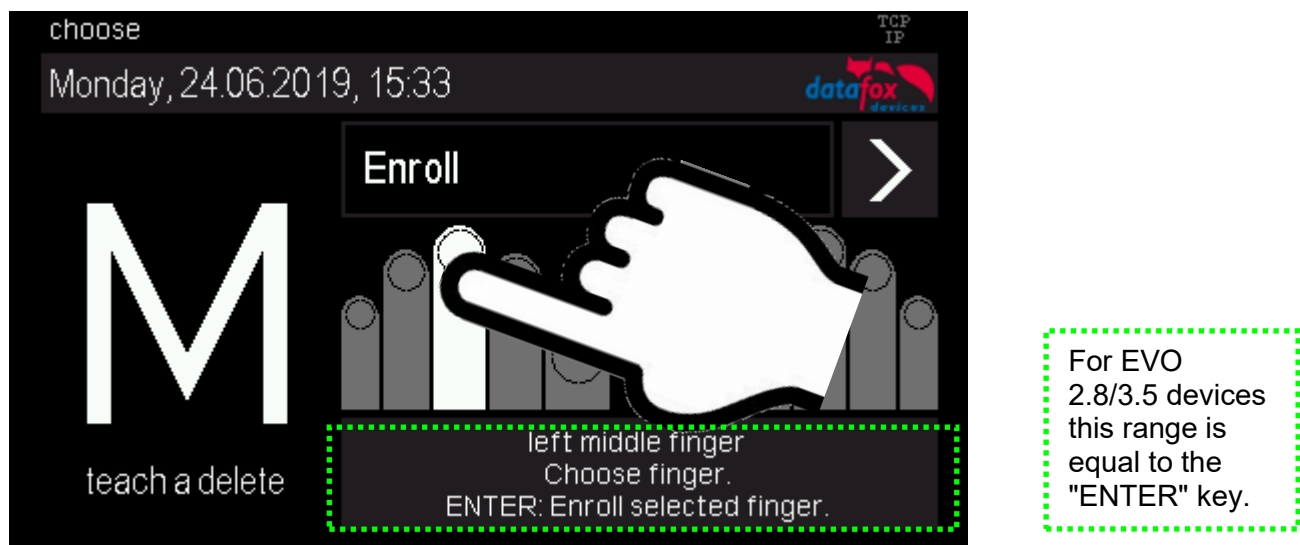
Follow the instructions on the display.
The finger must be scanned 3 times. After each beep, briefly lift your finger off the scanner and replace it.
The successful teach-in is indicated by a green field which also contains a quality value. With a quality value of 85 and more, the teach-in was very successful.

If the values are lower, the teach-in can be repeated directly in order to achieve a better result.
Teaching-in should be completed with the highest possible quality value, as this is the basis for later recognition.
Of course, there are fingers that can only reach lower values. In this case, however, other fingers of this person should also be tested.

We recommend to teach in at least two fingers for each user if a finger is not recognizable due to injury.
If you select a different finger symbol, you can then learn additional fingers directly.

5.12.3. "Training" menu page

This step fulfils two tasks, on the one hand a functional check that the taught-in fingers are actually recognized, on the other hand the system can be further optimized, i.e. trained.

To optimize, the fingers should now be deliberately moved or twisted a little.
This way a larger area of the finger will be recognized bit by bit and the saved template will be optimized. An optimization is indicated by the green bar. Good for the system is, if several such optimizations can take place to a finger.
If no more green feedback comes, the training can be stopped.

The fingers that have already been taught-in are marked with „X"
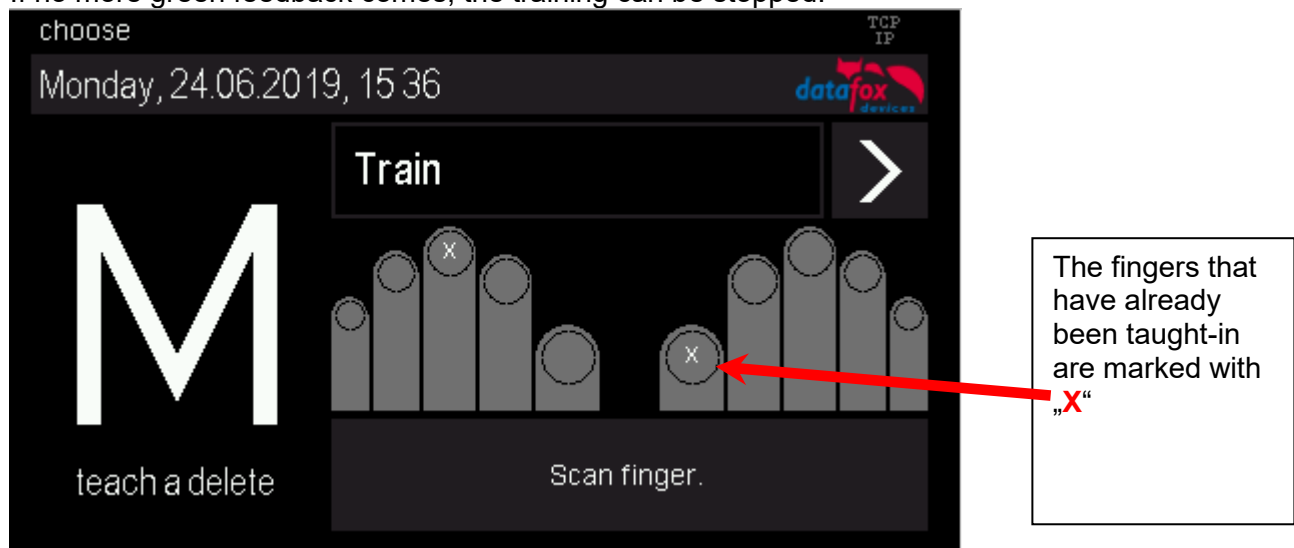
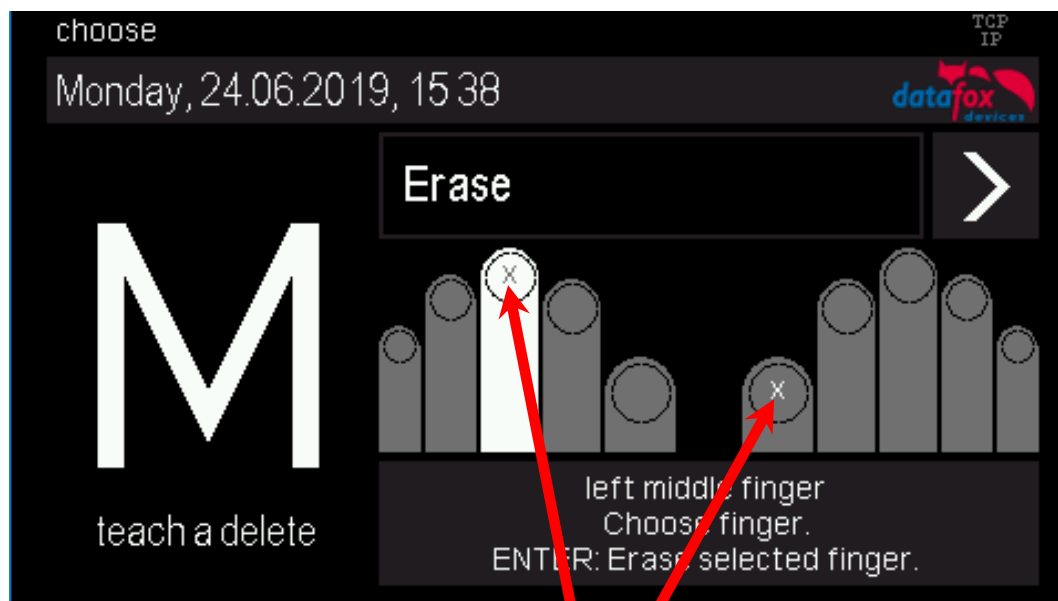### 5.12.4. Menu page - Delete

Delete individual fingers:

The taught-in fingers are marked with "**X**". Tap on the finger you want to delete and confirm with "Enter".

Delete all fingers of a person:

On the next menu page "Delete all fingers of a person", all taught-in fingers of the person are high-lighted. When you confirm with Enter, all the person's fingers are removed from the fingerprint sensor.

5.12.5. Menu page - "Exit

Menu page - "Exit

For EVO 2.8 and 3.5 there is a separate page for exiting the finger administration menu.
Simply click on the center of the screen and exit the menu.

With the EVO 4.3 you can exit the administration menu by pressing the "ESC" key.

Hinweise zur Verwendung des Fingerprint-Flächensensors
Hints for using the fingerprint area sensor

Dieser Abschnitt zeigt anhand von Fingerprint Bildern, wie sie auch beim „Finger check" angezeigt werden, wie ein Bild aussehen sollte und welche Auswirkungen durch schlechte Position, falschen Druck oder ungünstige Finger erkennbar sind.
This chapter shows with images, as they are also shown in the function "Finger check" how a good image should look like and how they could look with respect to bad positions, bad pressure or difficult fingers.

- Der Finger muss mit leichtem Druck auf den Sensor gelegt werden.
  The finger must be put onto the sensor with light pressure.
- Der wichtigste Bereich ist die Mitte des vordersten Fingerglieds, da dort die meisten Eigenschaften vorhanden sind.
  The most important area is the middle of the front finger link, because there are the most characteristics.
-

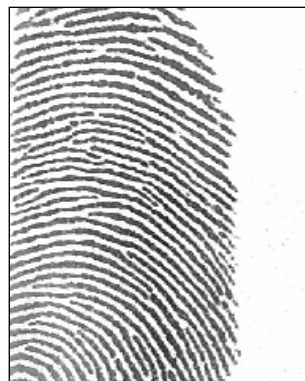**Gutes Bild / good image**

Schlechte Positionen / Bad positions

| Zu weit unten | Zu weit oben | Zu weit links | Zu weit rechts |
| Too far down | Too far up | Too far left | Too far right |

Schlechter Andruck / Bad pressure on the sensor

Zu wenig Druck
Too little pressure
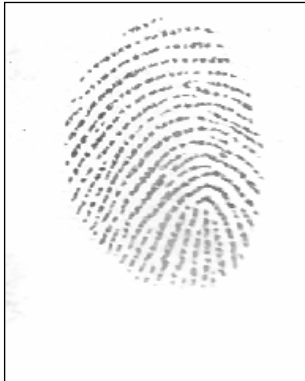
Zu viel Druck
Too much pressure

Finger verdreht / Finger twisted

Zu steil, nur Finger-
spitze
Too steep, only finger-
tip

Nach links verdreht
Twisted to left

Nach rechts verdreht
Twisted to right

Schräg rechts /
Diagonally right

Trockene Finger / dry fingers

Finger sehr trocken
Finger very dry

Trockenen Finger kurz
gerieben
Dry finger shortly
rubbed

Trockenen Finger an-
gehaucht
Dry finger breathed on

Trockenen Finger ein-
gecremt
Dry finger with cream

Schwierige Finger / Difficult fingers

Falten / Wrinkels	Unterbrechungen / Interruptions	Falten, unscharf Wrinkels, diffuse	Unscharf / Diffuse

Schwierige Finger / Difficult fingers

Generell Undeutlich / Generally unclear

Fingerprint Flächensensor Saturn01

| Templates	5000 Templates à 640 Byte, ISO19794-4; ANSI-378	In the module 5000 fingers can be managed, a template has 640 Bytes.
Resolution	500 dpi	The sensor-resolution is 500 dpi.
Active area	14 x 18mm	The active area of the sensor is 14 x 18 mm.

5.13. Operation Finger Scanner Line Sensor

The fingerprint reader's readiness to scan is indicated by the flashing green LED.
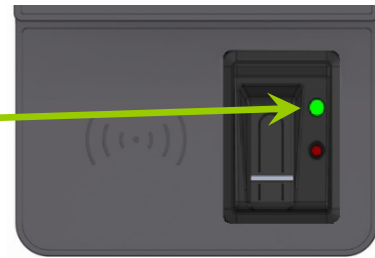
1.) Place the finger with the area of the first finger segment.
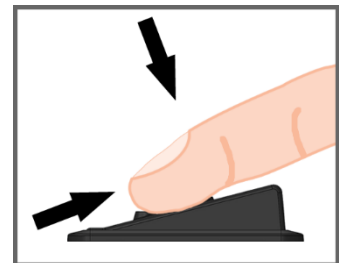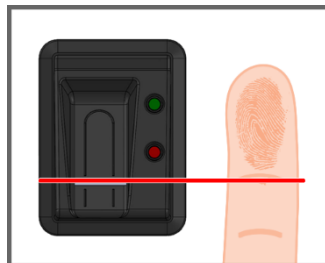
2.) Lay the finger flat. Caution, do not place your fingers on the edge, otherwise only a part can be detected.
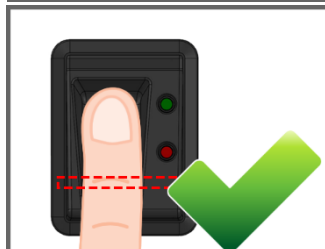
3.) Pull the finger over the scanner with a little pressure on the scanner. In order to allow a good detection of the finger, the fingers must be clean!
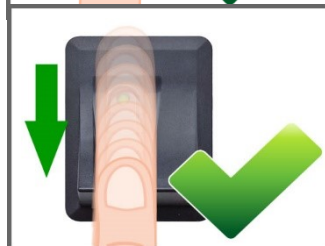
Section view

Attention!
This small strip, shown here red, is the actual line scanner. Pull the finger over the sensor with light pressure. The contact from the finger to the scanner must not be interrupted.
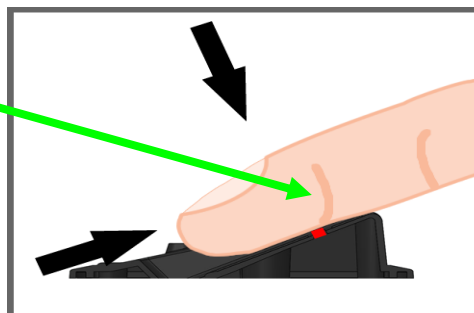
How to scan correctly - video   guide:
http://www.datafox.de/videothek.html

!	All terminals should be mounted in such a way that the finger sensor is at the same height so that the handling can be carried out identically.
!	In no case may be components on the finger, which have an abrasive effect. These use the protective layer of the line sensor and thus significantly reduce the service life.

5.13.1. General infomation

Biometrics offers the possibility of identification and verification by the body's characteristics. Data-fox supports finger detection with the fingerprint module. ID cards and PINs are no longer necessary and thus cannot be forgotten. Reading the fingerprint replaces reading the ID card. Of course, all functions which are available when reading an ID card are also supported for fingerprints. This data sheet is an addition to the respective product sheet.

Basically, you have to differentiate between the following information:

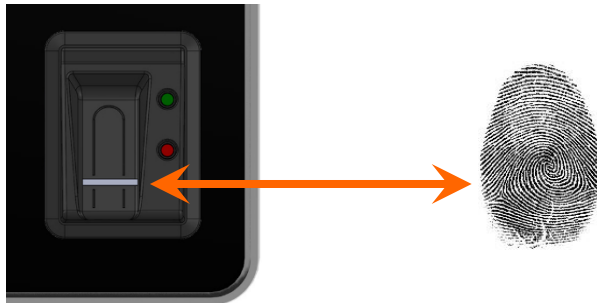The "PID" is the person identification number, also called employee number. 10 finger templates can be assigned to one PID at most. The PID should be a decimal number; when using transponders the corresponding format (decimal n digits) must be selected.

> **!** **Caution:**
> The PID must not exceed the decimal value of 4294967295 (2^{32} -1).
> We recommend working with a 9-place PID.

The "finger template" consists of the PID and the finger characteristics of a person. The finger characteristics are the feature points (minutiae) which are determined from the image after scanning a finger.

The "security level" (false acceptance rate / false rejection rate) defines when a read finger is accepted or rejected. 60 means that 60% of the minutiae of the scanned template must match 60% of the reference template, in order to declare the detection as valid. We recommend setting the value not lower than 55 and not higher than 75. It is best to use 60.

Image quality is the number of usable finger lines in relation to the number of available finger lines. We recommend setting the value not higher than 40.

The "count of minutiae" defines how many minutiae must be determined from the image so that a template for a matching can be created or declared as valid.
We recommend setting the value not lower than 7, better set to 10.

> **!** **Caution:**
> For image quality the recommended value is 40. For older models with Biokey 3000 with a firmware version 04.12, the recommended value is 70. Biokey 3000 with firmware 61.00, the image quality must necessarily be less than 70. The recommended value of 40 offers an optimum for learning the fingers.

> ☞ **Note:**
> Recoment settings:
> **Security level 60%, quality: 40% minimum of minutien: 15**

Difficult fingers can be detected by decreasing the parameters, but this can lead to false detection. The behavior must be checked in each individual case, since it is very dependent on the group of people.
In such cases, one should switch to another finger, because not every human finger is suitable for the Minutien method.

5.13.2. Teach-In

In order to use fingerprint, the persons must be taught-in at the terminal at first.

4 steps to teach-in the Finger

Step 1
Read the PID

Chip number   or   choosing on a list   → PID

personnel data
- (1): ID Number
- (2): Name

ID-number	Name
00799611485215	M. Mustermann
05597861113494	M. Musterfrau

Step 2
Scan finger

Fingerprint: scanning.

Step 3
PID and finger characteristics to combinate

Field funktion: Fingerprint: fingerprint to train.

PID   +   finger characteristics   =   Template

Step 4
Save Template

on Biokey-Module   on Mifare Transponder   on Server

5.13.3. Procedure

Identification

The finger characteristics are recorded via the fingerprint module. Then, the data pool is checked for matches. If a match is found, the PID of the person is returned, otherwise an error. The matching threshold is determined by the security level.

Verification

An employee identifies himself via a transponder. The PID (employee number) is read from the ID card. Then the employee has to swipe his finger across the scanner of the fingerprint module. In the data pool of the fingerprint module, all primary keys (combination of PID and template) with this PID are determined (up to ten assignments are possible) and checked for matches with the scanned finger characteristics.

Advantage: faster detection, higher security
Disadvantage: further detection medium needed, e.g. transponder

Identification with Data Storage of Finger Templates in the Fingerprint Module

The terminal polls the fingerprint regularly whether someone has read their finger. If so, the fingerprint transfers to the terminal, who has read their finger and whether the finger was valid. PID and validity are transferred. The task in the terminal for the fingerprint triggers an input sequence and access control - if defined in the setup. If no person is detected, the fingerprint returns a PID = 0.

Verification with Data Storage of Finger Templates in the Fingerprint Module

The terminal polls a transponder reader regularly whether a transponder was detected. If so, the serial number or a memory block of the transponder is transferred to the fingerprint module. The fingerprint module waits for the reading of the finger. After reading, it is checked whether the finger stored in the fingerprint module with the serial number or the transponder data matches the read finger. The fingerprint module transfers PID and validity to the terminal. The task in the terminal for the fingerprint triggers an input sequence and access control - if defined in the setup.

Verification with Data Storage of Finger Templates at a Transponder

The terminal polls a transponder reader regularly whether a transponder was detected. If so, the serial number or a memory block of the transponder and the finger data stored in the transponder are transferred to the fingerprint module. The fingerprint module waits for the reading (scanning) of the finger. After reading (scanning), it is checked whether the finger transferred by the ID card matches the read (scanned) finger. The fingerprint module transfers PID and validity to the terminal. The task in the terminal for the fingerprint triggers an input sequence and access control - if defined in the setup.

5.13.4. Process Variants

Teach-in for identification/verification with data storage in the fingerprint module
1.) Determine PID (read from ID card or via list selection)
2.) Scan finger (determine finger characteristics)
3.) Teach-in (amalgamate PID and finger characteristics and save in fingerprint module)

or

1.) Scan finger
2.) Determine PID
3.) Teach-in fingerprint module

Teach-in for verification with data storage on a Mifare card
1.) Determine PID (read from ID card or via list selection)
2.) Scan finger (determine finger characteristics)
3.) Teach-in (amalgamate PID and finger characteristics and save on Mifare card)

or

1.) Scan finger
2.) Determine PID
3.) Teach-in and save on Mifare card

Identification via fingerprint module
1.) Scan finger
2.) Identification via fingerprint module

Verification via BIO key
1.) Determine PID (read from ID card)
2.) Scan finger
3.) Verification via fingerprint module or
1.) Scan finger
2.) Determine PID (read from ID card)
3.) Verification via fingerprint module

Verification via Mifare card
1.) Read template from Mifare card
2.) Determine PID (read from ID card)
3.) Scan finger
4.) Verification by fingerprint module

or

1.) Scan finger
2.) Read template from Mifare card
3.) Determine PID (read from ID card)
4.) Verification by fingerprint module

Deleting a template from a fingerprint module by identification
1.) Scan finger
2.) Delete template from fingerprint module or
1.) Determine PID (read from ID card or via list selection)
2.) Delete template from fingerprint module

Deleting a template from a fingerprint module by verification

1.) Determine PID (read from ID card or via list selection)
2.) Scan finger
3.) Delete template from fingerprint module or
1.) Scan finger
2.) Determine PID (read from ID card or via list selection)
3.) Delete template from fingerprint module

Deleting a template from a Mifare card

1.) Read Mifare card
2.) Delete template from Mifare card

> **Note:**
> For more information on possible settings see the manual DatafoxStudioIV, chapter "Functions in the Setup → Fingerprint".

5.13.5.   Technical Data of the Fingerprint Module

- ATMEL FingerChip
- ATMEL ARM9 Controller
- Storage capacity of 2000 fingers
- Power consumption ca. 120 mA at 3.3 volts, sleep 1 μA
- Temperature -20 to + 85 °C (-4 to +185 °F)
- Template: Idencom compact format 216 Byte
- Teach-in time 1.2 seconds + processing time terminal
- Matching time: 0.014 seconds
- False Rejection Rate (FRR): $1{,}4 \times 10^{-2}$
- False Acceptance Rate (FAR) $1{,}0 \times 10^{-4}$
- From 100 fingerprints onwards, we recommend verification only. Combination with PIN via keyboard or ID card.
- Experience shows that not for all employees the fingers can be recorded in sufficient quality.
- Depends on the state of the fingers. For those persons the ID card or PIN has to be recorded.

5.14. Fever measurement on the wrist

			EVO 4.3/4.6	EVO 2.8/3.5	Unive rsal	Agera ZK	Inloc	Mobil Box	IO-Box	Oneloc			EVO-PC
			☒	☒									

The temperature measurement option on Datafox terminals measures the skin temperature behind the wrist at a distance of 3-10 cm. This measurement can give an indication of whether the person at the terminal may have a fever. Fever is often an early sign of contagious infectious diseases, as it is the case with Covid-19.
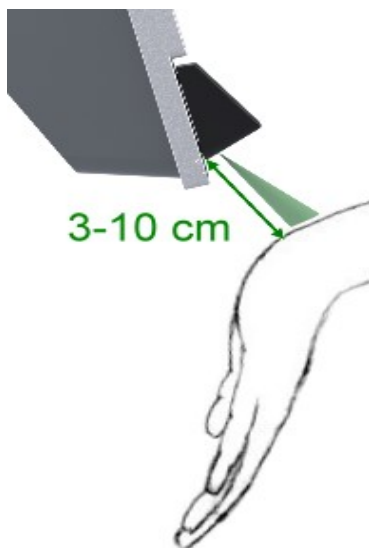
> **!** **Attention:**
> The temperature measurement of the terminals is only an indication. If an increased temperature is detected here, this must be repeated by another measurement with a medical thermometer.
> Which steps are then taken in the individual case must be regulated by the operator, Datafox only offers the technical possibility to measure the skin temperature.

> **!** **Attention:**
> As with all infrared thermometers, only the surface temperature of the skin is measured. This provides a good indication of the body temperature inside.
> However, the temperature can also deviate significantly due to external influences, for example:
> - Cold outside temperature
> - Resting the arms on cold surfaces
> - Cold hands
> - Poor blood circulation
> - Solar radiation
> - Sweat
>
> It is recommended to have a few minutes of acclimatisation before the measurement so that the external influencing factors are reduced.

5.14.1. Operating sequence of the measuring process

To make operation easier for the user, instructions are given on the display and an LED is also used in the sensor.

1. Start of the procedure by the field function.

2. Notice on the display to hold the wrist under the sensor.

3. The LED flashes. The light indicates where the measurement will take place.

4. When the wrist is close enough to the sensor, ideally 3-10 cm, the LED lights up continuously. At a greater distance it flashes slowly, at a smaller distance it flashes quickly, accompanied by a rapid beep.

5. The measurement takes place and lasts about 2-3 seconds. The arm should be held still during this time.

6. The end of the measurement is signalled by a short beep and the LED switching off.

7. The measured value is shown on the display in different colours depending on the status of the result, see table below.

5.14.2. Results oft he measurement

The temperature measurement can be integrated into the booking procedure on the unit via a field function. The temperatures described are the default values, they can be adjusted in the field function
Based on the measured temperature, 4 result states are determined:

Status	Range	Colour	Description
1	< 30,0°C	Blue	The temperature is too low, it should not be a human body temperature. Display of the temperature value in blue.
2	30,0°C bis 37,9°C	Green	Body temperature is fine.
3	38,0°C bis 42,0°C	Red	The temperature indicates a fever.
4	> 42,0°C	Purple	The temperature is too high, it should not be a human body temperature.

Either the temperature value itself can be used for further processing. The status is also available and facilitates conditional jumps in the further input chain.

Result status oft he evaluation:

In addition to the measured value, the field function provides a corresponding "result status of the evaluation". This can be used in the further course of the input chain in input chain fields to display information messages or to perform other actions (e.g. green or red light).

The value of the result status can be assigned to a record description field or also to a "global variable" for a subsequent evaluation.

5.14.2.1. Description of the field function

With the new field function, it is possible to carry out a temperature measurement.
At the same time, a limit value can be set, which is then used for evaluation.

The measured temperature can be displayed in a GV and saved in a Data set

Setting range for the result evaluation.

If the result of the evaluation is to be saved in a GV, you can select it here.

If the result of the evaluation is to be saved in a data record, you can select the corresponding data field here.

The measured temperature is stored in the record description field "Temperature" after successful completion of the function in this example.

The following settings are made in the "Temperature measured value of fever control" area:

- The measured temperature can be written to a "Global Variable".

- The unit of measurement can be selected between Celsius and Fahrenheit, and the measured value is then displayed accordingly. The unit is also written into the record description field and possibly into the "Global Variable".

- The valid measuring range can be adjusted within its limits if necessary. Below 30°C and above 42°C it is to be assumed that no valid body temperature was measured. Elevated temperature and thus suspected fever is indicated from 38.0°C. Which status value is assigned to the result depends on these limits and has already been explained above.

- After a valid or only after an invalid measurement, a query can be activated to be able to repeat the measurement. This gives the user the possibility to perform measurements again by one or more repetitions, e.g. if there were still clothes in the measuring range.
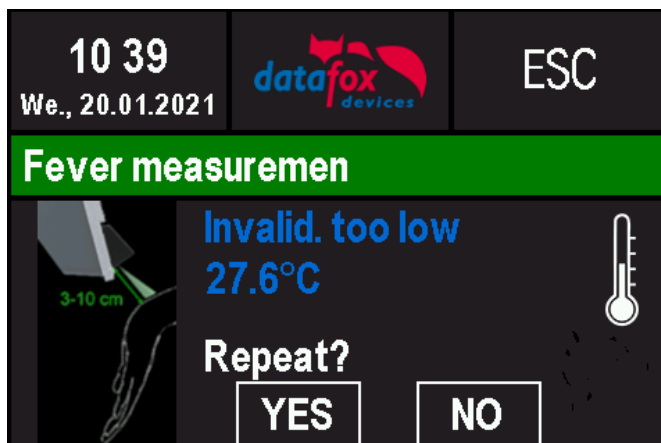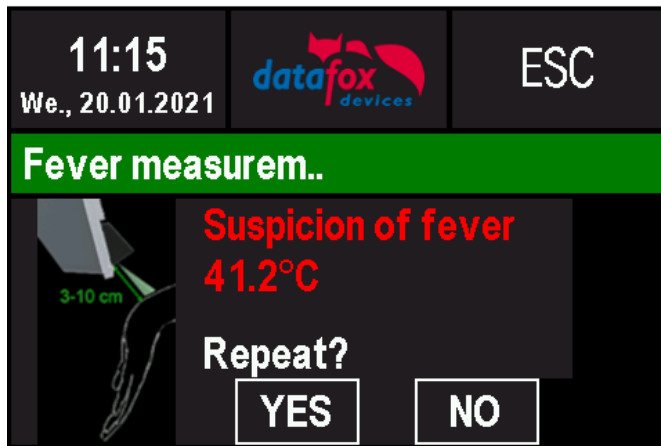
5.14.2.2. Operation on the unit
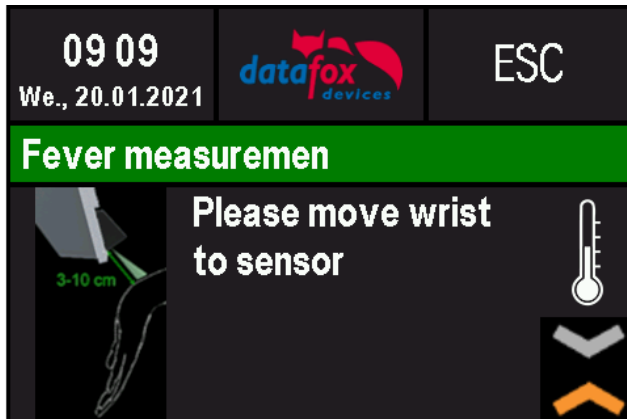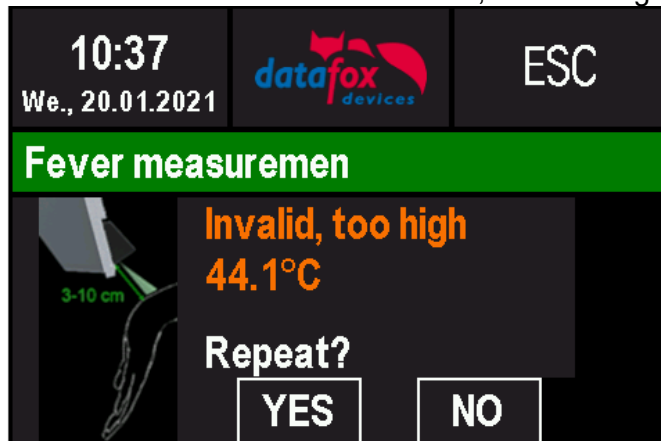

In this case the wrist is too far from the sensor.
sensor.
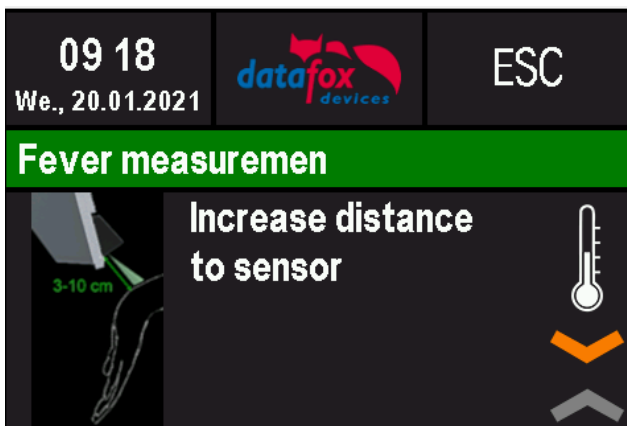
In this case the wrist is too close to the sensor.
sensor away.

If the maximum set value is reached, this message appears.

5.14.3. Description of the field function in the Display Designer

You can adapt the images and symbols that are displayed during fever measurement to your own wishes.
On the page "Additional images" you can decide whether the "Images for the field function for fever control" are displayed and also transferred to the device if the hardware is present.
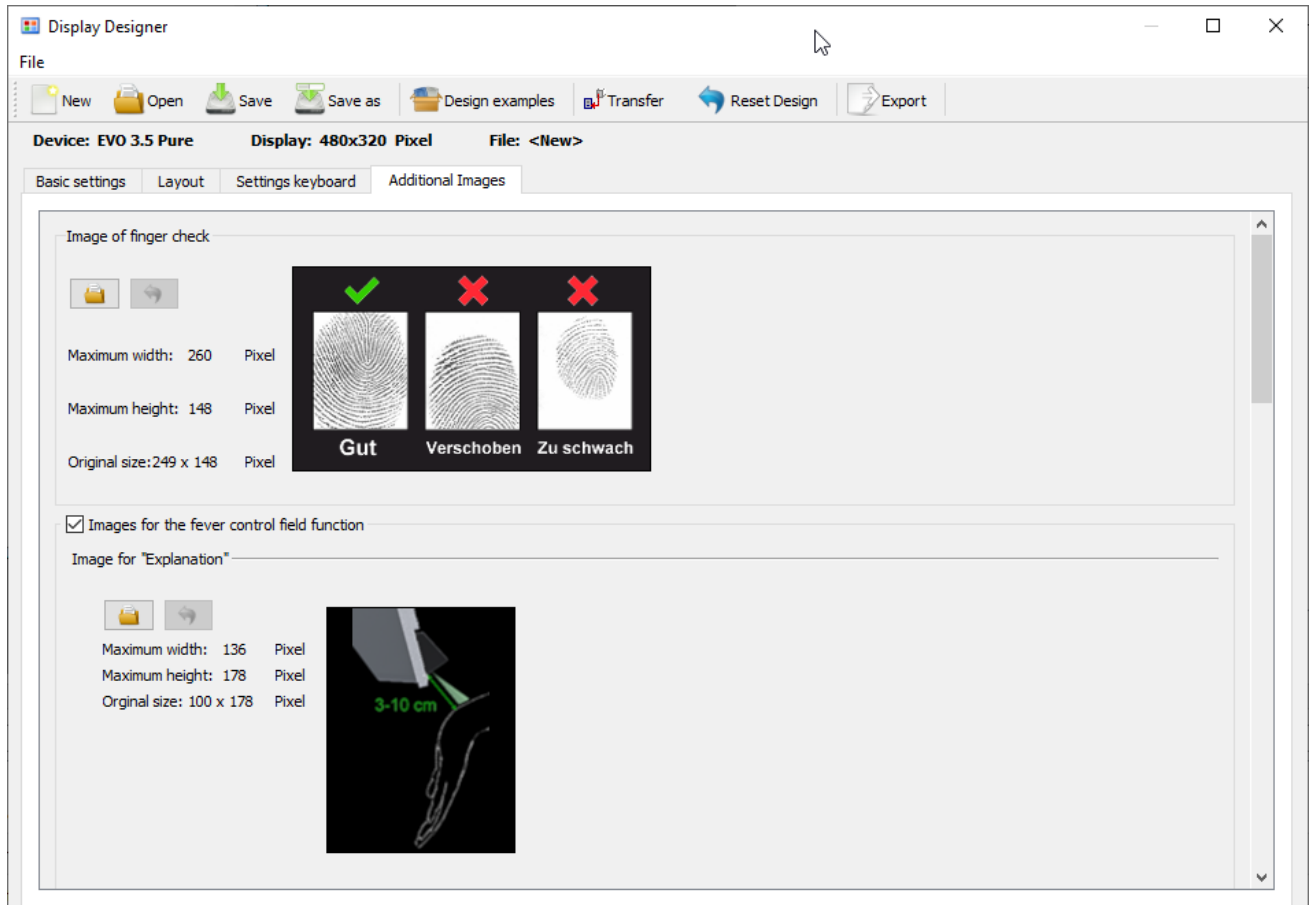
If the option "Images for the field function for fever control" is not selected, the images will not be transferred to the unit, even if a corresponding fever control function has been installed in the unit. If the option is selected, the images are only transferred to devices with a built-in fever control function.

Example of the display layout of an EVO 3.5 Pure during measurement.
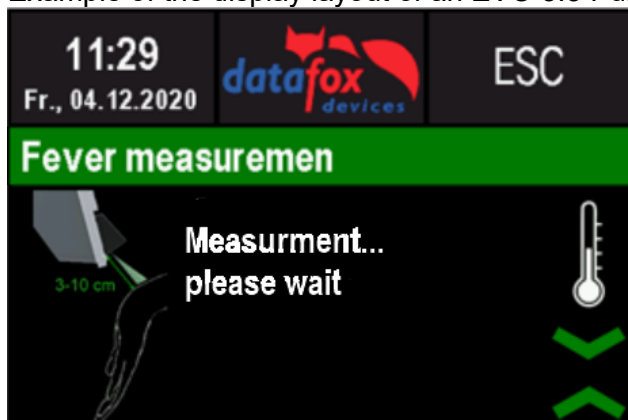
In the display designer, the images are to be specified as follows if the option is selected. Firstly, the image for the explanation (in the left-hand area) and for the thermometer (in the right-hand area).
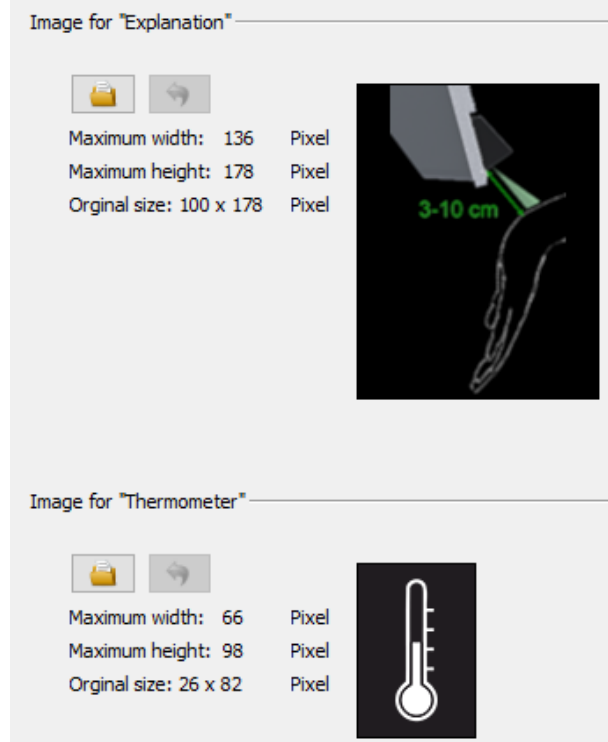
The combination of arrow symbols for the three possible distance states.

- Guide the wrist towards the sensor.
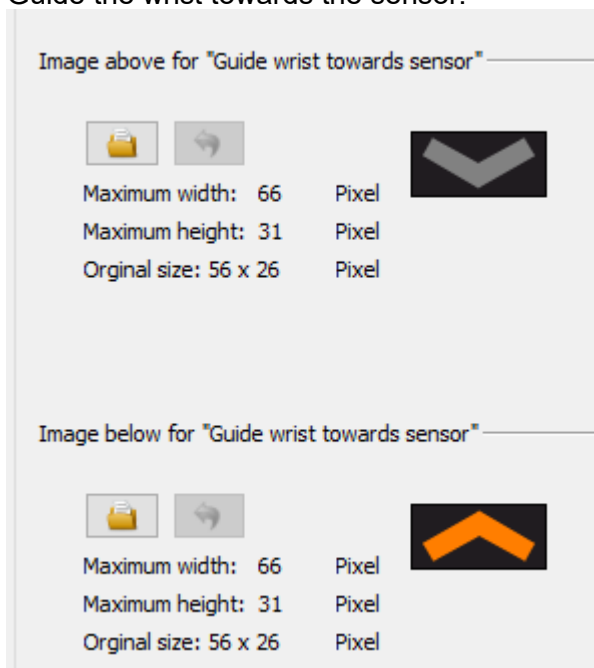
- Guide wrist away from sensor.

- Wrist in the measuring range.

Please note the maximum image sizes when specifying. Images that are too large will be scaled down to the maximum possible size. Smaller images will be aligned in the centre.

6. Technical specifications EVO 2.8 /3.5 /5.0 Pure

EVO 2.8 Pure Terminal V4.X

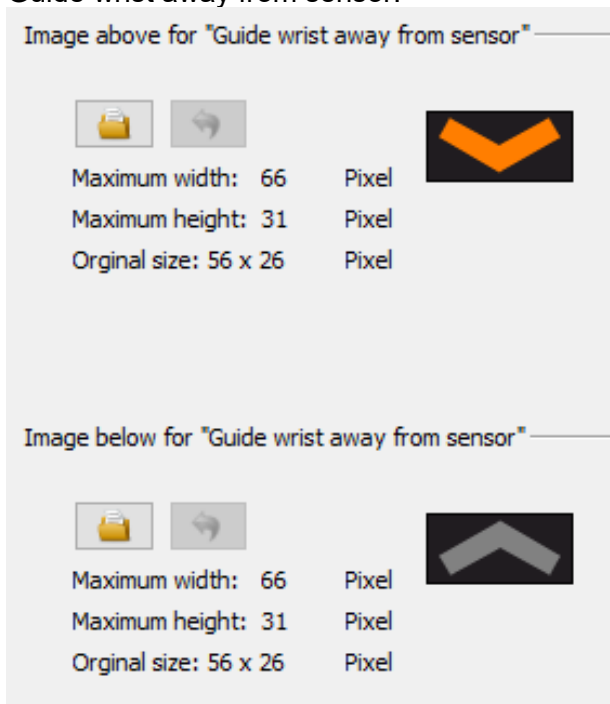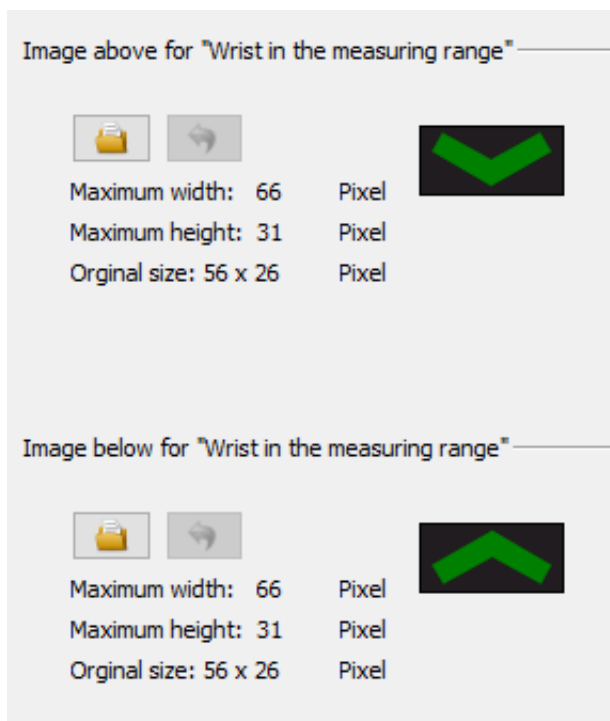|		
Housing	Structure, Dimensions (w x h x d)	Plastic: PC/ABS UL94-V0 // 109 mm x 200 mm x 85 mm
	Weight (Without power supply)	base unit 0,35kg, plus wall mount plate 0,125kg
System	Clock	Real-time clock
Data storage	Flash / Memory expansion (optional)	16 MB, 100.000 write cycles / SD card, max 2 GB
Display	LCD	EVO 2.8 TFT: 320 x 240 Pixel, active area 57,6 x 43,2 mm with LED-Backlight EVO 3.5 TFT: 480 x 320 Pixel, active area 73,4 x 49,0 mm with LED-Backlight EVO 5.0 TFT: 800 x 480 Pixel, active area 108 x 64,8 mm with LED-Backlight
Keys	Type, size	EVO 2.8 Keyboard on touch screen (resistive), touch area 57,6 x 43,2mm Life time according to manufacturer specification: 1 Mio. hits EVO 3.5 Capacitive touch screen, touch area 73,4 x 49,0mm, touch wearless EVO 5.0 touch capacitive (wearless) / resistive (1 Mio. hits): touch area 108 x 64,8mm
Sensors (only EVO 3.5 / 5.0 Pure)	Proximity sensor	Activates the devices when the user comes close to it, distance ca. 0,8m
	Ambient light sensor	Reducing the backlight of the display in a dark environment
Power	Power Supply / PoE	12 V DC / PoE: 802.3af Class 0
	Power	Base unit 3 watts, depending on the equipment up to max. 10 W
	Clock / RAM buffering	Goldcap, securing the time up to one week
Environment values	Ambient temperature	-20°C to +60°C (PoE -20°C bis +50°C)
	Protection	IP 54
Software	Configuration program	Setup program (Datafox-Studio) to configure without programming effort
	Communication tools	HTTP(S), library (DLL, so) or C++ source code for integration in the application
Module extensions	For the extension to a variety of functions such as communication, inputs/outputs, sensors are 5 expansion slots for modules	
Data transmission to PC/Server	USB	Micro USB integrated
	TCP / IP (optional)	TCP / IP operating with integrated TCP / IP stack, 10/100 Mbit
	WLAN (optional)	integrated wireless LAN module, WLAN 802.11 bg and 802.11 n (only 2.4GHz)
	Mobile Radio (optional)	online via mobile module 2G, 3G or 4G
	RS485 (optional)	RS485 2-wire bus
	USB host (optional)	for data transfer via USB stick, protection IP22
	Bluetooth (optional)	Bluetooth module integrated; range up to max. 100 m
Readers Connection	RS232 external (optional) (ML01-RS232)	Connection of bar code readers, magnetic card readers via mini-DIN connector
Access Options	RS485 external (ML01-RS485)	Connection of up to 3 busses with up to 16 external door modules / access readers in total
	Door lock relay with Door Monit. (ML01-DR1)	1 relay changeover , 30 V AC, 30 V DC, 2 A, max. 60W, 1 digital input (elect. Isol.) for door monitoring, …
MDE Options	Module digital inputs (ML01-D01)	4x digital input, electrically isolated, up to 100kHz, or 250Hz, Low 0,0…1,5V; High 3,5…30,0V
	Module relay outputs (ML01-R01)	1 x NO, 1 x changeover contact, 30 V AC, 30 V DC, 2 A, max. 60 W
	Module analog inputs voltage (ML01-A1) / current (ML01-A2)	4 x input, 15-bit resolution, accuracy ± 2% measuring range 0-10 V / 0-25mA, other ranges and functional insulation 230 V on request

Module digital transistor outputs (ML01-T1)

4x output	per output	per module	per device, 40°C	per device, 60°C
Aktiv 12V (Power in):	max. 0,8A	max. 0,8A	max. 1,4A	max. 1,0A
Active GND: (< 30V)	max. 1,4A	max. 2,0A	max. 4,0A	max. 2,0A

Additional Options	Fingerprint	Fingerprint module integrated; sensor on the right below
	Integrated transponder reader	125kHz, for example Unique, titanium, Hitag 13.56 MHz, e.g. Legic, Mifare, ISO14443, ISO15693, Simon Voss, iButton, Nedap
	GPS receiver / receiver	50 Channels, GPS L1 frequency C / A, Galileo Open Service L1
	Bar code scanner integrated	1D/2D/QR bar code scanner
	Column	Column for free mounting
	Fever control at wrist	Only at room temperature +15 - +35°C, no wind, no direct sunlight. Mounted on the side of the device.

6.1. communication modules

LAN (TCP / IP)	Width 20mm	10 / 100Mbit, IPv4, IPv6
WLAN	Width 20mm	Standard 802.11.b/g, encryption WEP, WPA2 802 / 11i
GPRS	Width 40mm	GPRS class 10, quad band, mini-SIM socket
RS485	Width 20mm	RS485 connections, up to 30 participants

6.2. access modules

RS485	Width 20mm	RS485 connection for the access reader, relay modules, ... power supply from 1 external reader when using Datafox power supplies with 12V
Access Control-IO	Width 20mm	1 relay changeover, 42 V AC, DC 60 V, 2 A, max. 60 W; 1 digital input for monitoring door, ...

6.3. Module digital in and out

Digital inputs	20mm	4 x digital input, functional insulation 230V, depending on the device type, up to 250kHz, Low 0.0 ... 1.0 V; High 3,5 ... 30,0V
Digital outputs relay	20mm	1 x NO contact, 1 x change-over contact, 30 V AC, 30 V DC, 2 A, max. 60 W
Digital outputs Open Coll.	20mm	4 x open collector output, 2A, 30V (in preparation)
Analog inputs voltage	20mm	4 x input, 15-bit resolution, accuracy ± 2%, range 0-10 V, other ranges and functional insulation 230 V on request

6.4. Modules miscellaneous

RS232-Modul	Width 20mm	RS232 interface, with MiniDIN connector or spring terminal 5V-output max. 0,5A, with USB supply max. 100mA.
GPS	Width 20mm	50 Channels, GPS L1 frequency C/A, GALILEO Open Service L1
Micro-SD Card	Width 20mm	Micro-SD Card max. 2GB, depending on device accessible from outside the device
Mobil-Box-Modul	Width 40mm	Central connector for power supply, (8-30V DC), 1 relay, 2 digital inputs and connection for Mobile-Dockingstation with Timeboy
Acceleration sensor	Width *20mm*	*3D acceleration sensor in preparation*

7. FAQ

An extensive collection of FAQs can be found on our homepage:
http://www.datafox.de/faq-de.html

8.   Index

A

Access 74
Access with PHG reader 89

B

Bios 19

D

Device 16
DHCP 19
DNS 63

F

FAQ 182
For your Safety 1

G

GPRS 68
graphic on display 29

H

Holiday Control 74
Holiday control ZK 74

I

Image for the key area 34
Integration of a Burglar Detection System
     (BDS) 117
Intended Use and Environmental Protection 5
introduction 2

K

Kommunikation 51
  Umschalten 51

L

Lautstärke 19

M

Mobilfunk Verbindung Status 69

P

power supply 41
  POE 41

S

SMS 70
Switch Relays via time table: 74
System Requirements / Hardware 10

T

TCP/IP 56
Technical specifications EVO 2.8 /3.5 /5.0
     Pure 181
Touchkalibrierung 19

U

UPS 12
USB 51, 53