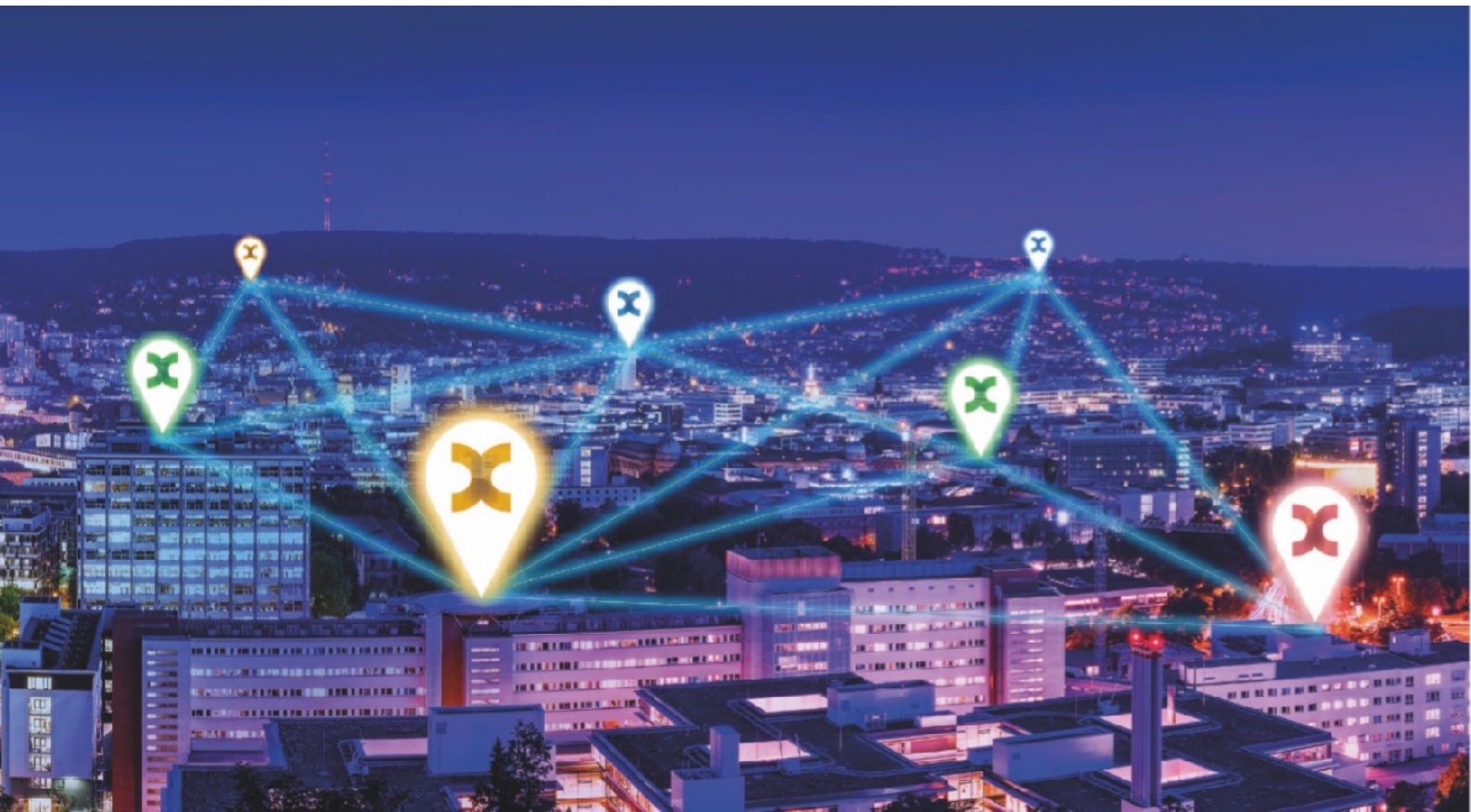


User-Manual



360° Smart Building Security for Pros

SMART MONITORING



SMART ACCESS



SMART METERING



SMART VIDEO



KENTIX360CLOUD



1. Introduction - About this manual	6
2. Smart Monitoring - Introduction	7
1. Features	7
2. Operations	7
3. Safety instructions	7
3. Connection examples and installation notes	8
3.1. StarterSet-BASIC	8
3.2. StarterSet-PRO	8
3.3. StarterSet with optional equipment	9
3.4. Alarm-inputs	10
3.5. Switching outputs	10
3.6. Power supply	10
4. Overview KENTIX System Topology	11
5. AlarmManager-BASIC/PRO	12
5.1. Connections of the AlarmManager	12
5.2. Inserting a SIM card	12
5.3. Settings factory settings	13
5.4. Reset to factory settings	13
5.5. Establish Connection to AlarmManager	13
5.6. Communication / network ports	14
5.7. Configuration in 8 steps	15
5.8. Visual and acoustic signaling	16
5.9. Configuration - Dashboard / Logbook / Time profiles	17
5.9.1. Add / edit MultiSensors	17
5.9.2. Manage alarm zones	18
5.9.3. Quitting alarms	19
5.10. User accounts	20
5.11. Kentix360 Cloud	21
5.12. Configuration	21
5.12.1. General	21
5.12.2. Network	21
5.12.3. E-Mail	21
5.12.4. SNMP - Monitoring	21
5.12.5. GSM	23
5.12.6. SMS Gateway function	23
5.12.7. SMS Limit	23
5.13. System	24
5.13.1. Logbook	24
5.13.2. System functions	24
5.13.3. License management	24
5.13.4. Wireless settings (ZigBee)	24
5.13.5. SD card	24
5.14. Further devices / sensors	25
5.15. Execution of Firmware Updates	26
6. MultiSensors	27
6.1. Mounting instructions for MultiSensor-RF / -LAN / -LAN-RF	27
6.2. Coverage of the integrated PIR movement detector	27
6.3. Calibration of the temperature / humidity sensor	28
6.4. Kentix system port on MultiSensor-RF / -LAN / -LAN-RF	28
6.5. MultiSensor-RF	28

6.5.1. MultiSensor-RF teach-in	28
6.6. MultiSensor-LAN	29
6.6.1. Default settings / Factory defaults	29
6.6.2. Software function MultiSensor-LAN	29
6.6.3. Sensors (sensors and alarming)	31
6.6.4. Users	32
6.6.5. Konfiguration	32
6.6.6. System	34
6.7. MultiSensor-Door	35
6.7.1. Mounting instructions	36
6.7.2. Usage of the reed contact	37
6.7.3. Opening of the casing / replacement of battery	38
6.7.4. Adding a MultiSensor-Door	38
6.7.5. Settings	38
6.7.6. Test of the settings	39
7. KeyPad-Touch (KKPT)	40
7.1. Adding a KeyPad	40
7.2. Operation KeyPad	41
8. Enhancements	42
8.1. Leakage sensor (KLS03)	42
8.2. Leakage sensor rope (KLS03-ROPE)	44
8.3. Kentix Power-Adapter (KIO1) with digital input clips	45
8.4. Kentix Power-Adapter (KIO2) for powering a MultiSensor	46
8.5. Kentix Power-Adapter (KIO3) with digital I/O clips	47
8.6. Overview and application examples for Power-Adapters (KIO1-3)	48
8.7. Kentix Alarm siren (KFLASH1)	49
8.7.1. Configuration	49
8.8. Kentix IO-Modules	50
8.9. MultiSensor-LAN-RF (LAN-ZigBee Repeater)	51
9. Smart Access - Introduction	52
9.1. Product features	52
9.2. Application areas	52
9.3. Safety instructions	52
9.4. Components	53
9.4.1. Online knob (DoorLock-DC) and profile cylinder	54
9.4.2. Online door lever (DoorLock-LE)	54
9.4.3. Online wall reader (DoorLock-WA)	54
9.4.4. Online cabinet lock (DoorLock-RA)	54
9.4.5. IP Wall Reader and network relay module	55
9.4.6. Master card set	56
9.4.7. AccessPoint	56
9.4.8. Accessories	56
9.5. Installation & Programming (installation)	57
9.5.1. Online knob	57
9.5.2. Online door lever	58
9.5.3. Online wall reader	61
9.5.4. Online cabinet lock	65
9.5.5. IP Wall Reader and network relay module	69
9.5.6. AccessPoint	73
9.6. Configuration and operation modes	74
9.6.1. DoorLock-device without AccessPoint (offline-mode)	74
9.6.1.1. Initial setup - insert / activate batteries	74

9.6.1.2.	Initial setup - Master card set	75
9.6.2.	DoorLock-devices with AccessPoint (online-mode)	77
9.6.2.1.	Default settings / factory defaults	77
9.6.2.2.	Communication ports	77
9.6.2.3.	Dashboard - Access logbook	78
9.6.2.4.	Dashboard - DoorLock control	78
9.6.2.5.	Access - Users	79
9.6.2.6.	Teach-in of RFID-media in the online-mode	80
9.6.2.7.	Access - Access profiles	81
9.6.2.8.	Access - Time profiles	81
9.6.2.9.	Access - DoorLocks	81
9.6.2.10.	Access - General	83
9.6.2.11.	Access - DoorLocks - Switching alarm zones	83
9.6.2.12.	Configuration - General	84
9.6.2.13.	Configuration - Network	85
9.6.2.14.	Configuration - Communication	85
9.6.2.15.	Configuration - Master/Slave Mode	86
9.6.2.16.	Configuration - Network cameras	86
9.6.2.17.	Configuration - LDAP Configuration	87
9.6.2.18.	Kentix360	88
9.6.2.19.	System - Logbook	88
9.6.2.20.	System - System settings	88
9.6.2.21.	System - SD card	88
9.6.2.22.	System - Import/Export	89
9.6.2.23.	System - Help	89
9.6.3.	Master-Slave-mode (Compound operation with multiple AccessPoints)	89
9.6.4.	Reset of components	89
9.6.5.	Battery replacement	90
9.6.6.	Emergency opening	91
9.6.7.	Dismantling	91
10.	Smart Metering - Introduction	92
10.1.	Product features	92
10.2.	Application areas	92
10.3.	Safety instructions	92
10.4.	Components	93
10.4.1.	PowerManager	93
10.4.2.	Wireless SmartMeter	93
10.4.3.	Wireless Inline-Meter	93
10.5.	Assembly & Programming (commissioning)	94
10.5.1.	Installation Wireless SmartMeter	94
10.5.2.	Installation Wireless InlineMeter	95
10.5.3.	PowerManager	95
10.5.4.	Configuration	95
10.5.4.1.	Settings delivery state / factory settings	95
10.5.4.2.	Communication ports	96
10.5.4.3.	Dashboard - Measurement data	96
10.5.4.4.	Smartmeter - Smartmeter	97
10.5.4.5.	Smartmeter - General	98
10.5.4.6.	User	98
10.5.4.7.	Configuration - General	99
10.5.4.8.	Configuration - Network	100
10.5.4.9.	Configuration - Communication	100
10.5.4.10.	System - logbook	101
10.5.4.11.	System - system functions	101

10.5.4.12. System - ZigBee	101
10.5.4.13. System - Help	101
11. Kentix AlarmManager Smartphone-App	102
11.1. The Profile menu	102
11.2. AlarmManager	103
11.3. MultiSensor-LAN	103
11.4. AccessPoint	104
12. Kentix360 Cloud	105
12.1. Setup	105
12.2. Manage Devices	106
13. Kentix SIM card	107
13.1. Setup	107
13.2. Telephone number and PIN	107
14. Data sheets	108
14.1. Data sheet AlarmManager-BASIC/PRO (KAM-BASIC/PRO)	108
14.2. Data sheet MultiSensor-RF (KMS-RF)	109
14.3. Data sheet MultiSensor-LAN (KMS-LAN)	110
14.4. Data sheet MultiSensor-LAN-RF (KMS-LAN-RF)	111
14.5. Data sheet MultiSensor-Door (KMS-Door)	112
14.6. Data sheet KeyPad (KKPT)	113
14.7. Data sheet AccessPoint (KXP-16)	114
14.8. Data sheet Online Door knob DoorLock-DC (KXC-KN1/2/3)	115
14.9. Data sheet DoorLock-LE (KXC-LE)	116
14.10. Data sheet DoorLock-WA (KXC-WA)	117
14.11. Data sheet DoorLock-RA1 (KXC-RA1)	118
14.12. Data sheet IP wall reader with network relay module (KXC-WA3-IP1)	119
14.13. Data sheet PowerManager (KPM-RF-B)	120
14.14. Data sheet SmartMeter (KSM-DR60-RF / KILM-x-xx)	121
14.15. Data sheet digital I/O expansion-module (KIO7052)	122
14.16. Data sheet digital I/O expansion-module (KIO7053)	123
14.17. Data sheet analogue I/O expansion-module (KIO7017)	124
14.18. Data sheet leakage sensor (KLS03, KLS03-ROPE10/20)	125
15. Checklist - Acceptance report	126
16. Support	129

1. Introduction - About this manual

This document contains general installation, configuration and operation instructions for installing Kentix products.

The installation is explained by topologies, quick manuals and important points. The devices are connected via Plug&Play via network (PoE) or power plugs respectively.

If further steps for installation are necessary, e.g. DoorLock components, these will be explained in detail. Follow the overview in the table of contents.

Configuration

This Manual explains required points for commissioning Kentix products.

Further information or hints and explanations respectively to certain configuration points can also be found on the Web Interface of the respective device.

2. Smart Monitoring - Introduction

Thank you for your decision to buy a KENTIX monitoring solution based on the KENTIX MultiSensor technology.

1. Features

The KENTIX AlarmManager-BASIC/PRO is the central system unit, where all the information of the MultiSensors are collected. The AlarmManager is installed in the server room or rack. It controls and forwards all alarm and fault messages to the responsible persons. The configuration is done using a browser directly via the AlarmManagers web interface. The connection and installation of the devices is done plug&play with external power supplies and RJ45 cabling.

2. Operations

- Industry and Trade
- Banks
- Authorities and hospitals
- Telecommunications
- Law firms and medical practices
- Energy and water utility

3. Safety instructions

The installation of the AlarmManager must be run by a competent person.

The sole responsibility for protection against misuse of the SIM card is the card owner. The device allows the use of a PIN number.

In case of a power failure, the settings of the AlarmManager are not lost. Energized relays drop out and go back when the power returns in the unswitched output state.

The device sends power outages directly via SMS. The internal energy supply can protect short-term power failures for 3-5 minutes. To bridge a longer downtime, use a suitable UPS system.

Installation

To ensure the security and integrity of the operator and the correct operation of the KENTIX AlarmManager, the execution of the installation only has to be done by an expert. There must also be ensured, that the relevant requirements are met.

Environment

The installation must be such that the KENTIX AlarmManager and all associated cables are not affected by the environmental conditions listed here: *dust, humidity, excessive heat, direct sunlight, heat sources, devices that build strong electromagnetic fields, liquids or corrosive chemicals.*

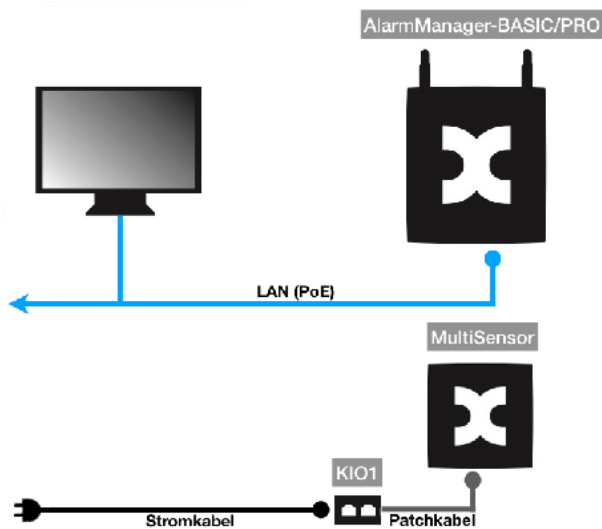
See the technical data sheet for more technical data and environment conditions.

Protection

During the installation of the AlarmManager, certain degrees of protection must be guaranteed. Observe the relevant regulations for installation in certain environments such as industrial or residential and commercial buildings.

3. Connection examples and installation notes

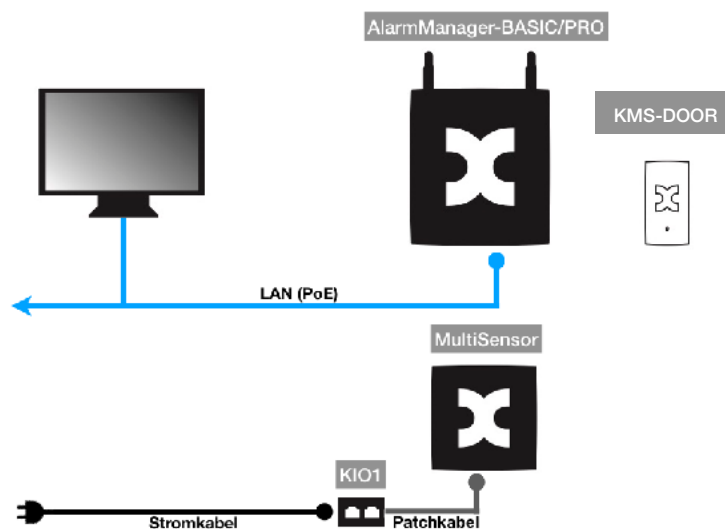
3.1. StarterSet-BASIC



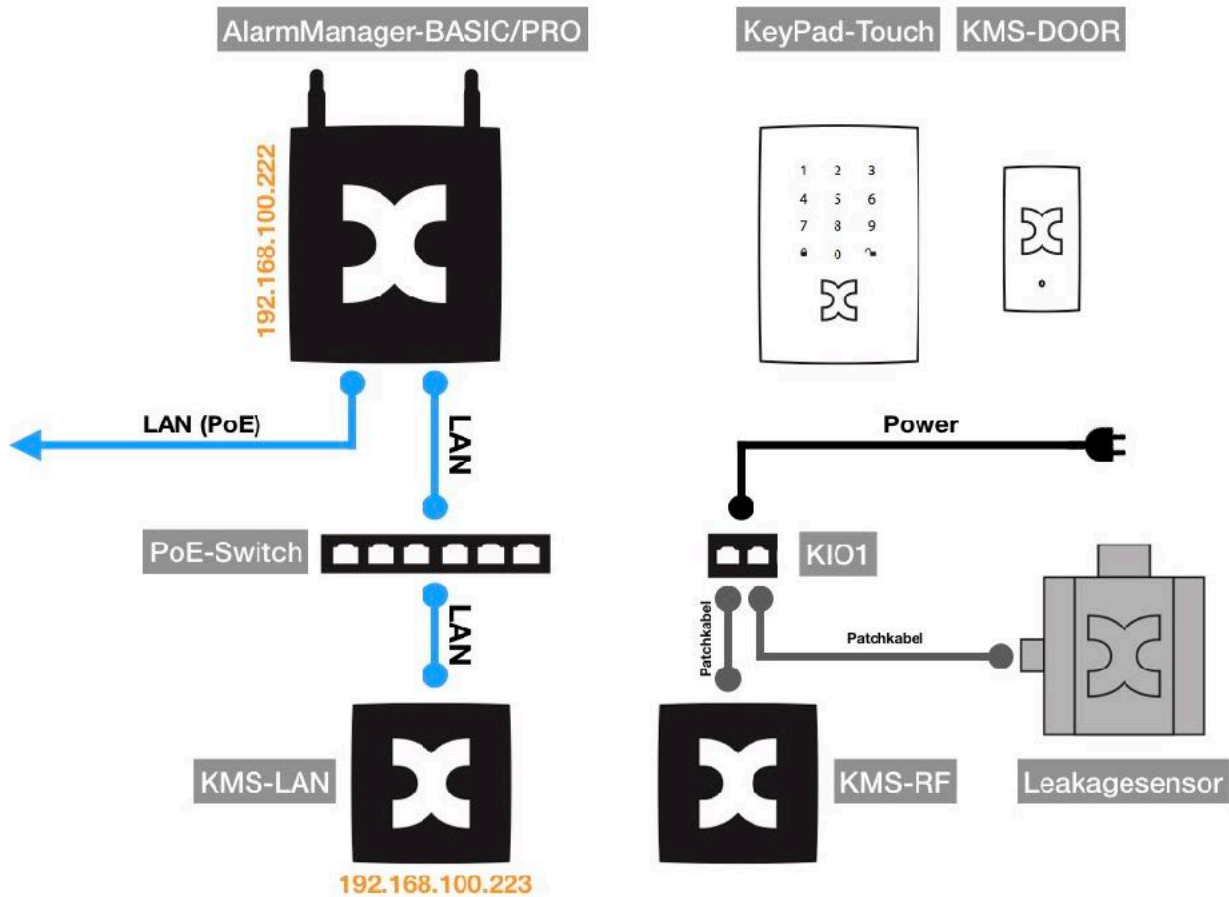
1. Connect AlarmManager to PoE enabled switch.
2. Connect MultiSensor-RF to KIO2 power adapter and power plug.
3. Enter Kentix-Default-IP-Address **(192.168.100.222)** into your web browser.
4. Enter default user (admin/password) and click Login (pay attention to your own IP settings)
5. Adjust IP address of AlarmManager in settings.
6. Add wireless sensor in dashboard.
7. Make own individual settings.

3.2. StarterSet-PRO

1. Follow the steps like described for „StarterSet-Basic“.
2. The MultiSensor-Door is added in the configuration similar to a MultiSensor-RF. Please note the description further down in the manual.



3.3. StarterSet with optional equipment



1. MultiSensor-LAN:

Establish network connection and external power supply, if needed.
Connect to the sensor via browser by entering the Default-IP (**192.168.100.223**).
Press „Login“ to reach configurations menu (Username: „**admin**“, Password: „**password**“).
Activate AlarmManager communication in the communication settings.
After saving the settings the MultiSensor can be added to the AlarmManager configuration.

2. Leakage-Sensor:

The connection of a Leakage-Sensor is realized either by a direct connection to an AlarmManager, MultiSensor-LAN or with a KIO1-Power-Adapter (required for a connection to a MultiSensor-RF). The configuration is then done on the device to which the leakage sensor is connected.
Enter a name in the „External sensors“ section and switch the alarming of the input to „Alarm when open“ and „Always-Active“.

3. MultiSensor-Door:

Please follow the the instructions for adding new sensors as described in this manual. Also note that there are differences in procedure depending on the type of MultiSensor.

3.4. Alarm-inputs

When installing the device follow the instructions in this manual. Please note polarity and technical data of the inputs.

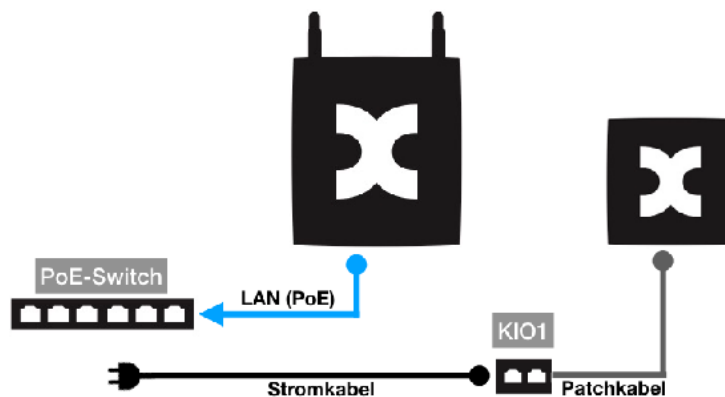
3.5. Switching outputs

When installing the device follow the instructions listed in this manual.

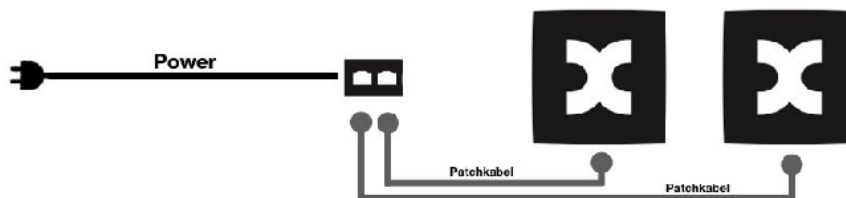
Connected devices must installed properly following the specifications in this manual. Pay particular attention to the allowed supply voltages and services for the various consumers in the technical data-sheet.

3.6. Power supply

The devices are power supplied via PoE or with a DC voltage between 10-32VDC. Use only recommended power supplies or listed power supplies in this document. The polarity of the cable must not be interchanged.



Example 1: Power supply of one MultiSensor via the system jack of the AlarmManager



Example 2: Power supply of two MultiSensors via Power Adapter (KIO1) and plug power supply



Electronic equipment is not domestic waste - in accordance with directive 2002/96/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL dated 27th January 2003 concerning used electrical and electronic appliances, it must be disposed of properly. At the end of its service life, take this unit for disposal at a designated public collection point.



Spent batteries are special waste!

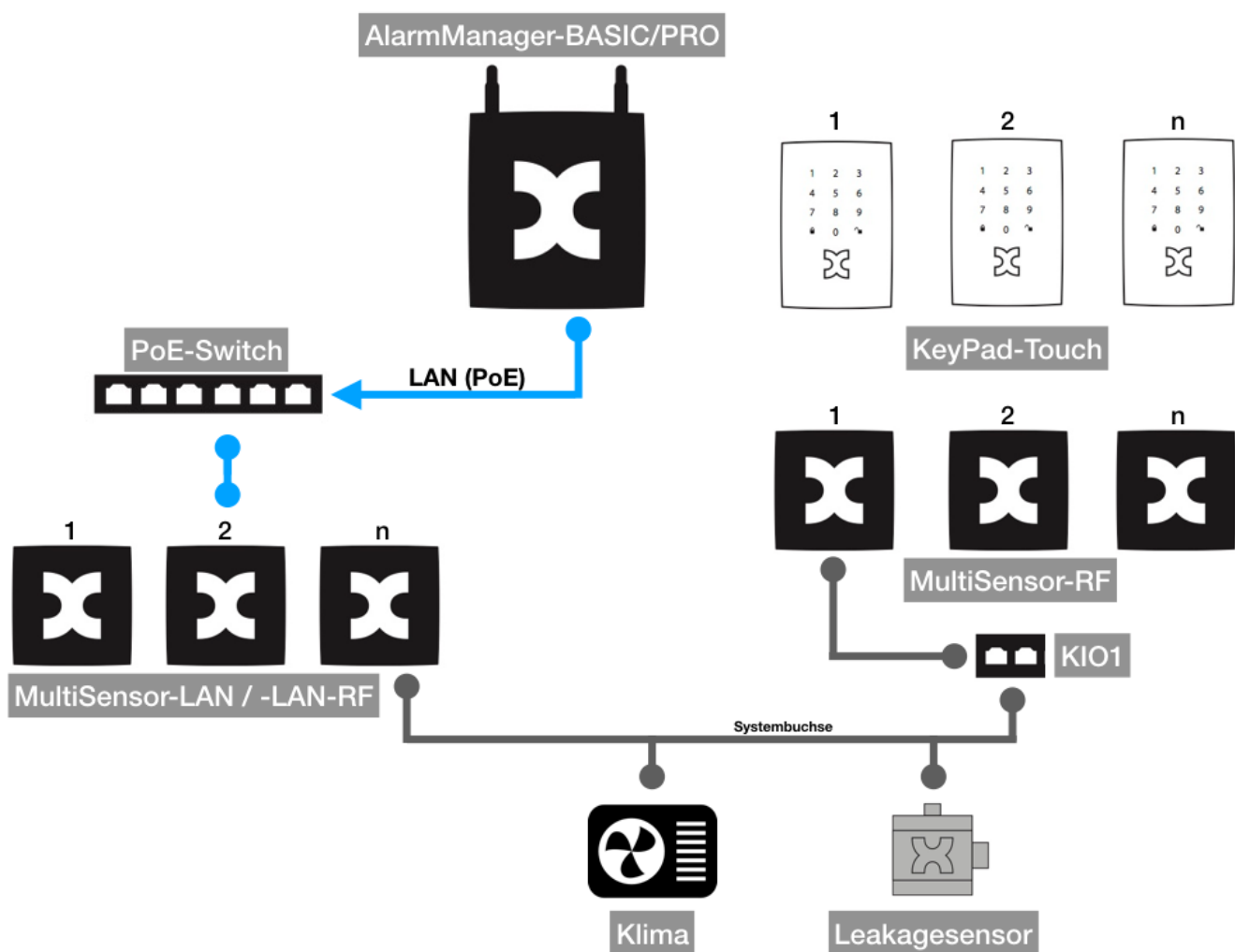
Do not throw spent batteries into your domestic waste; take them to a collection point for spent batteries.



The products complies with applicable European standards and directives and is confirmed by the CE mark.
The CE conformity declaration is available on request.

4. Overview KENTIX System Topology

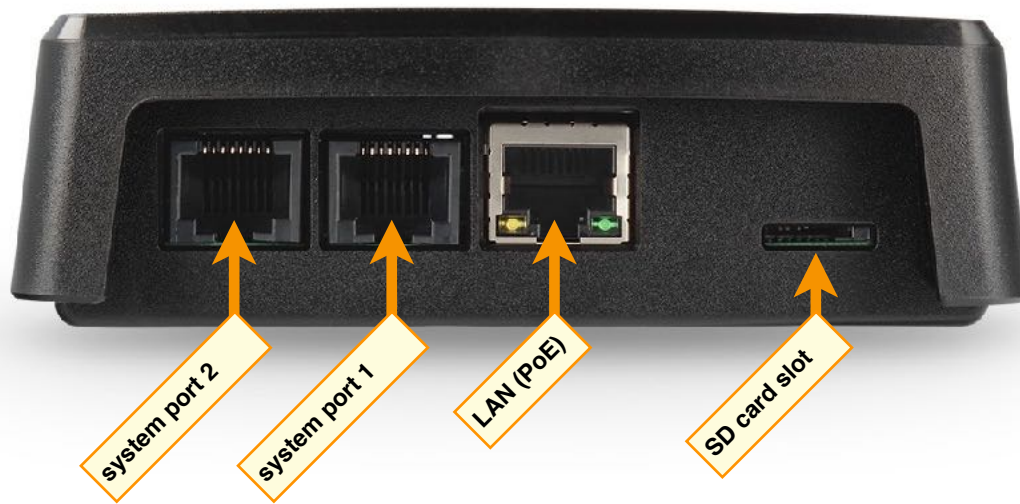
- ✓ The AlarmManager is the central unit.
With the **BASIC-Version** up to 200 MultiSensors (only MultiSensor-RF) and other devices can be connected. The **PRO-Version** supports up to 500 devices.
- ✓ The Kentix RF-components communicate via (ZigBee®) radio in the 2.4GHz ISM Band.
The wireless MultiSensors work in a mesh network and communicate via each other.
- ✓ Always start each new project with a CompleteSet. The Sets include everything you need for a Plug'n'Play installation.



5. AlarmManager-BASIC/PRO

5.1. Connections of the AlarmManager

Below you can see an overview of the connections of the AlarmManager



5.2. Inserting a SIM card

The SIM tray is positioned on the backside of the case below the mounting bracket. The bracket can be removed without any tool by lifting the latch. Afterwards the tray can be unlocked and opened. The SIM card is placed inside the opened part of the holder.

IMPORTANT!

The SIM card has to be inserted that way, so that the recess on the card is pointing down-right with closed holder.

5.3. Settings factory settings

The configuration of the AlarmManager and all other connected MultiSensors is done via the web interface. For initial configuration enter the IP address printed on the backside of the AlarmManager in your browser. Please pay attention to your own network settings of your PC.

Default IP-Adresse: 192.168.100.222
Subnet mask: 255.255.255.0
User: admin
Password: password

5.4. Reset to factory settings

Reset to factory settings

To reset the AlarmManager back to factory settings restart the device.

As soon as the internal status LED is active, press the RESET-button on the backside of the device. Hold the button for 15 seconds until you hear an acoustic signal.

The device is reset to factory settings and restarts. The AlarmManager is accessible via the default settings after approximately 60 seconds.

5.5. Establish Connection to AlarmManager

Connection with PC: Connect the LAN interface of the AlarmManager via the supplied LAN cable to a PoE enabled switch. Connect your PC to the same switch.
Set the IP address of your PC for example to "192.168.100.123".

IMPORTANT!

Always check the entered IP data of the network configuration before saving. If the IP configuration is forgotten or the AlarmManager is no longer reachable via the web interface, a factory reset would be required.

After entering the IP address in your web browser a login screen will open.

Enter the user data to log in.

For initial configuration use:

Default-IP-address 192.168.100.222, user name „admin“ and password „password“.

NOTICE!

Only users with the permission „Administrator“ are allowed to make changes to the AlarmManager.

For users without the admin permission, only the tab pages „Dashboard - Logbook - Chart“ are available for viewing purposes.

5.6. Communication / network ports

For the configuration and firmware updates and also the communication between MultiSensors (-LAN / -LAN-RF) the following ports are used. These ports eventually have to be taken into account for the configuration of your network.

No	Description	Port number
1	Configuration of AlarmManager and MultiSensors, firmware update	TCP 80, 443 from PC to AlarmManager / MultiSensor
2	Data transfer between MultiSensors and AlarmManager	TCP 80, 443 (bidirectional)
3	Request of measurement values via SNMP (network monitoring) from AlarmManager / MultiSensors	TCP 161 (from SNMP-Tool to AlarmManager or MultiSensor)

In combination with the Kentix360 Cloud additional ports for configuration and connection to the Cloud are required.

No	Description	Port number
1	Configuration of the Kentix360 Cloud	TCP 80, 443 from PC to Internet („mykentix.com“)
2	Communication between AlarmManager/AccessPoint or mobile app to cloud	TCP 5222 to the Internet („mykentix.com“)

5.7. Configuration in 8 steps

No	Step	Comment
Startup		
1	Connect AlarmManager and PC to a PoE-enabled switch. Start your web browser and connect with the default IP-address 192.168.100.222 to the AlarmManager. Login with the default user data (admin/password)	Make sure that your PC is in the same network. Adjust the settings of your network card, if necessary.
Menu item „Configuration“		
2	To change the network configuration open the menu item „Network“ and enter the required data for the integration into your existing network.	The settings are active directly after saving without restart
3	To configure the different notification ways, use the menu items „E-Mail“, „SNMP“ and „GSM“. Enter all necessary data for the different communication ways.	When using a PIN for the SIM card, directly after activation of GSM this PIN should be entered to avoid a locking of the SIM card.
Menu „User“		
4	Edit the existing user account and enter your name, e-mail-address and mobile number in international notation (+49 ...) or simply create a new user profile. Also assign the Alarmzones and ways of notification for the user.	You can test the e-mail and mobile settings by pressing one of the test-buttons. The user password is also the password for the authentication in the Kentix App.
5	Using a KeyPad the PIN also applies to the operation via a KeyPad. Note that the KeyPad allows only 4-digit passwords. To use the internal RFID card inside a KeyPad also enter the RFID card number.	The RFID card number can also be read out via a KeyPad. To do so press the „+“ button next to the field „RFID token“.
Menu „Dashboard“		
6	Press the "+" key to teach-in new devices such as MultiSensor or KeyPad. A selection of all possible sensors is shown. When selecting wireless sensors, a popup with information about the „teach-in“ process appears. With network enabled sensors, the configuration mask depending on the device type appears. Here you can enter e.g. IP data and alarm zone assignment.	When you run the teach-in process for RF-devices a closed wireless network is created, similar to an encrypted wireless PC network. Make sure that the devices are located in radio range close to the AlarmManager / MultiSensor-LAN-RF.
7	The new sensor is assigned to the selected alarm zone. Via the settings button in the line of the sensor these settings can be accessed again.	Via the test functions you can switch also the external outputs on or off.
8	Finally change the alarm settings and alarm assignments (Armed-Active / Always-Active) according to your needs.	Armed-Active: Alarms are only triggered, when the system is in armed state. Always-Active: Alarms are always triggered, independent of the armed/disarmed state of the system
Saving the configuration IMPORTANT! All changes directly become active when the settings are saved.		

5.8. Visual and acoustic signaling

LED-POWER/ALARM:	AlarmManager Lights after connection to the power supply RED/GREEN toggle in case of an alarm
	MultiSensor-RF / -LAN / -LAN-RF Lights if MultiSensor is powered and function is OK RED/GREEN toggle in case of an alarm Constant: MultiSensor is armed
BUZZER:	MultiSensor-RF / -LAN / -LAN-RF and AlarmManager Alternating: Arm delay is running. Delay is depending on configured time in the alarm zone settings. Constant of 1 Second: System has been disarmed. Constant of 3 Seconds: Arming was not executed - alarms are existing. Please check external alarm inputs on AlarmManager or MultiSensor.
	MultiSensor-Door
Normal operation mode:	
LED-RED:	blinking 1x in case of alarm
LED-GREEN:	OFF
BUZZER:	1x short in case of alarm (if acoustic signalization is active)
Teach-In process:	
LED-RED:	OFF
LED-GRÜN:	long blinking: Teach-In process started ON: Teach-In process completed
BUZZER:	1x long when pressing and holding down the teach-in button for approx. 3 seconds (start of teach-in process)

5.9. Configuration - Dashboard / Logbook / Time profiles

Below the steps for configuring the Kentix System via the AlarmManager are described.

For this purpose, the dashboard contains operating elements for editing sensors and alarm zones and operating the system.

The screenshot shows the Kentix AlarmManager dashboard. Annotations with arrows point to specific features:

- add building / alarm zone**: Points to the 'System' menu item in the left sidebar.
- general system state**: Points to the status icons (green checkmark, grey checkmark, red lock) at the top of the main content area.
- add sensors**: Points to the '+' icon in the top right corner of the sensor list table.
- edit sensor settings**: Points to the gear icon in the top right corner of the sensor list table.
- edit building / alarm zone**: Points to the '2 Factory Ikt-Oberstein' item in the left sidebar.

The dashboard displays a tree view of buildings and a table of sensors. The sensor table includes columns for Sensorname, Temperatur, Rel. Luftfeuchte, and various status icons.

5.9.1. Add / edit MultiSensors

New MultiSensors can be added via „+“ in the alarm zone heading. After selection, a list of all possible sensors for the system appears.

IMPORTANT!

Please note the respective device type. An AlarmManager BASIC supports only wireless sensors, cameras and the server Live check.

MultiSensor RF / Door and KeyPad-Touch must be assigned directly to the respective device (AlarmManager or MultiSensor-LAN-RF) during this process. For all other devices this is not necessary. Here, the assignment to an alarm zone suffices. The procedure for adding new sensors can be found in the description of the respective device later in this manual.

5.9.2. Manage alarm zones

Each device connected to the AlarmManager (MultiSensors, cameras, server, IO-Modules) can be allocated to an alarm zone, creating a separation into different logical areas. Each zone can be armed or disarmed independently and alert.

For configuration, add alarm zones to a building in the "System" area by clicking on the „+“. The mask for adding new alarm zones appears.

Existing alarm zones can also be edited by clicking the gear next to the name of the zone.

After creating the alarm zone, a device can be assigned to this zone via its sensor settings.

Alarm behaviour

IMPORTANT!

Also with multiple sensors in one zone an alarm of the type „Armed-Active“ can only be reported once for every zone. After alarming the alarm repetition is activated. If a continuous alarming is desired, the automatic quitting of alarms can be activated in the advanced settings.

With this an armed-active alarm will automatically be quit after the configured time.

Alarm zone settings and signaling

Define here the behavior of the AlarmManager when alarms occur. For active alarms, each alarm zone can be assigned a timer profile for timed activation / deactivation. The arming delay allows you to set a time between arming and first alarm activation.

The acoustic feedback (buzzers of AlarmManager and sensors) and the behavior of the LEDs can be activated or deactivated as required. Exempted from this setting is the CO alarm. Depending on the set buzzer time, an acoustic feedback is always triggered on all buzzers.

5.9.3. Quitting alarms

When an Armed-Active or Always-Active alarm is triggered at the AlarmManager, it has to be quit after the cause has been fixed. This can be done by the web interface, or with the App.

IMPORTANT!

Only when an alarm has been quit, it can be triggered again.

Other following alarms with a different cause from the sensors are still reported without acknowledgement.

The last triggered alarm will be resent every time the set up time for the alarm repetition runs up. With a value of 0 this repetition can be suppressed.

If an existing alarm is quit without the cause being fixed, the AlarmManager stops the alarm repetition. The alarm state stays active.

Additionally the AlarmManager tries for every 6 hours to quit existing alarms. When the cause has been fixed or is no longer present, alarming can be stopped this way, but gives the possibility to be re-triggered again.

5.10. User accounts

In the user accounts the setup of the permissions and the alarming is done.
Only if the required user data is entered, a user can control the AlarmManager or request information.
The list describes the user data required for AlarmManager interaction:

Input field	Description
User Password	Login to the Web-Interface and the Kentix App
E-Mail Address	Destination address for the alarming
Phone number	Destination phone number for the alarming
PIN-Code - RFID-Token	Remote control by SMS and switching via KeyPad
User level	Authorization level for working with the system
Notification	Defines which type of alarms and and ways of alarming are used for this user
Assigned alarm zones	The user can only switch zones assigned to his account. To switch all zones together, every zone has to be assigned to the user.

IMPORTANT!

Only users with the permission „Administrator“ are allowed to make changes to the AlarmManager.
For users without the admin permission, only the tab pages „Dashboard - Logbook - Chart“ are available for viewing purposes.
Power failures and connection interrupts to the sensors are also only reported to users marked as „Administrator“.

Kentix360 cloud access

A mobile access to the AlarmManager via the Kentix360 cloud service can be activated for each user account.
The option „Kentix360 cloud access“ activates a button „Setup app access“ where the users individual cloud ID is displayed.
After the first login with the smartphone alarms are also reported to the user as push notification.
Additionally messages are also send via e-mail and SMS, if activated.

5.11. Kentix360 Cloud

Please read „Kentix360 Cloud“ and „Kentix SIM“.

5.12. Configuration

5.12.1. General

Here, the system name is assigned to the AlarmManager.
German and English language for the configuration are available.

In addition, a communication key is assigned here in the "Security" section.
This is used to encrypt the communication of AlarmManager and MultiSensors.
It is also used to combine the AlarmManager with the "Kentix DoorLock" access system to arm and disarm alarm zones via the Kentix AccessPoint.

The communication key has to be identical in all connected devices.

In the time settings section, up to 2 NTP time servers can be stored for the time synchronization.
If there is an Internet connection, the AlarmManager can request the already preconfigured servers.

5.12.2. Network

Here you change the network configurations of your AlarmManager to integrate it into your network.
In addition to a fixed IP address, DHCP is also available.
To use the Kentix360 cloud and an email configuration with DNS server name, you must have a valid gateway and DNS server.

5.12.3. E-Mail

NOTICE!

If your AlarmManager has been registered for the Kentix360 Cloud, all emails will be sent through the Cloud service. In this case, no SMTP server needs to be configured, but it can be used as redundancy. If the AlarmManager does not reach the Kentix360 Cloud, it will send the e-mails via the configured SMTP server.

For e-mail alerting, an account with or without access data can be specified.
In addition - depending on the e-mail server - an encryption with an associated port must be selected.
When selecting an encryption type (STARTTLS / SSL), the corresponding standard port is automatically entered as well. If necessary, it can be changed to any port.

NOTICE!

With the checkbox next to the field "Password" a test e-mail can be sent. This will be sent to users configured as administrator. If an error occurs, please check whether at least one administrator has stored a valid e-mail address. Please also pay attention to eventually existing restrictions (Routing / Firewalls) in your network and if required check the data like encryption type and communication ports together with the responsible IT administrator.

5.12.4. SNMP - Monitoring

The AlarmManager supports full SNMP functionality. Alarms can be sent as traps. In addition, the AlarmManager can be configured for a polling via network monitoring systems. For this purpose, a MIB (Management Information Base) for the SNMP target system can be downloaded.

MIB for SNMP systems

For Kentix devices a MIB (Management Information Base) file is available, that describes the information that can be queried by a SNMP-System (e.g. PRTG, OpManager oder WhatsUp Gold). The single values are identified and requested via their OID (Object Identifier). Each values has its own specific OID.

The following list shows the structure of the MIB and gives an overview of the available values:

● system

- valuemultiplier
- alarmstate
 - alarm1
 - alarm2
 - ...

system - System state:

Query branch of the general system states.
Returns the current state as displayed in the web interface
(e.g. arm/disarm, alarm1 (armed-active), alarm2 (always-active), fire, server state, ...).

● sensors

- generalTable
- temperaturTable
 - temperatureIndex
 - tempValue
 - tempAlarm
 - tempMin
 - tempMax
- humidityTable
- inputs
 - input1Table
 - input2Table
 - ...
- outputs
- pdus

sensors - MultiSensors / IO-modules / SmartMeter:

Query branch for the values of all connected sensors.
All values are represented as integers, with temperature and dew point increased by a factor of 10 to take into account 1 decimal place.
This must be taken into account / adapted accordingly in the querying SNMP system.

● zones

- zoneTable
 - zoneIndex
 - zoneName
 - zoneArmedState

zones - Alarm zone state:

Query branch for index, name and arm/disarm-state of an alarm zone.

● logbook

- systemLogbookTable
- accessLogbookTable
- eventLogbookTable

logbook - request of logbook entries:

Query branch for system logbook, access logbook or event logbook.

Identification of the necessary OIDs:

To determine the OIDs required for the queries, a MIB Browser can be used to read the MIB file for Kentix devices. Alternatively, you can use the appropriate tools to perform an SNMP walk.
Please note that the respective OID can vary due to the fixed assignment of a sensor to an index. In the AlarmManager and MultiSensor-LAN there is a list of the OIDs in the sensor details and also download option to receive a full CSV list with all OIDs via the SNMP settings.

5.12.5. GSM

Here the phone number and PIN of the SIM card can be entered.

In addition, there are options for changing the PIN, unlocking a SIM card, and switching the PIN request on and off.

5.12.6. SMS Gateway function

External applications such as network monitoring systems can send SMS text messages via the AlarmManager's integrated GSM module. Communication is carried out via the build-in web server and the HTTP protocol. The following HTTP call is necessary for this function:

Replace the variables with your data. You can send a test SMS from any web-browser.

HTTP command structure:

https://AlarmManager-IP/php/sms_gateway.php?
key=password&recipients=+49123456789,+49987654321&message=myText

AlarmManager-IP	IP address of the AlarmManager (Default 192.168.100.222)
key	SMS-Gateway password
+49...	Mobile number in national or international notation To use the character „+“ in the URL please replace it with „%2B“ Exp.: „+49“ replaced with „%2B49“
myText	Text-message with up to 160 characters (Up to 320 characters possible. In this case 2 Messages will be sent)

HTTP return code: 200 when SMS sending was successful
300 when SMS sending was unsuccessful



HTTP Return Codes

To avoid DDoS-attacks from outside, the SMS-Gateway does not react/respond on wrong requests.

It is also not possible to determine whether a SMS has been successfully send or arrived.

In case of an error there are return codes that can be helpful to determine the cause of a failed SMS sending.

403: Wrong SMS Gateway password
404: SMS Gateway not activated
900: SIM card not recognized
901: GSM modem not recognized
902: SIM card is locked

5.12.7. SMS Limit

To avoid sending too many SMS at once (e.g. by a wrong configuration of the Kentix system)

a SMS limit of 100 SMS per 6 hours is defined in the AlarmManager.

If more than 100 alarm messages are triggered the AlarmManager will automatically stop the SMS alarming.

The limit can be reset by the alarm acknowledgement or disarming.

5.13. System

5.13.1. Logbook

Regardless of the event log, all messages relevant to the functionality of the Kentix system are stored here. The logbook contains, for example, messages about log-on to the AlarmManager, configuration changes and alarm notification messages.

With the help of the logbook eventual misconfiguration can be retraced.

5.13.2. System functions

In the section System functions a backup of the configuration can be created and restored.

In addition, a firmware update can be performed here.

Firmware updates are available for download on the Kentix website. A description of how to perform firmware updates can be found later in this manual.

5.13.3. License management

Basically there are two versions of the AlarmManager - AlarmManager-BASIC and AlarmManager-PRO. The devices are identical on the hardware side. A license key defines the respective device variant. An AlarmManager-BASIC can be converted to an AlarmManager-PRO by entering a license key to extend the functionality if required.

For information on the scope of functions or differentiation of the two device types, go to www.kentix.com.

5.13.4. Wireless settings (ZigBee)

This section displays information about the current ZigBee wireless network. In addition, the radio channel can be changed here and the radio network can be reset.

NOTE!

If the radio channel is changed, it may be necessary to re-teach some sensors.

When the radio network is reset, re-teaching of all wireless sensors connected to the AlarmManager is necessary.

5.13.5. SD card

To record video images in case of an alarm, a SD card must be inserted in the AlarmManager.

The card is automatically recognized after insertion and can be formatted here if required. A previous deletion or adjustment of the file system is not required. SD cards with a memory size of up to 128 gigabytes can be used.

5.14. Further devices / sensors

The Kentix AlarmManager offers the possibility to include other network devices into the monitoring as well. These are added to the configuration like a MultiSensor via the dashboard.

To do this, select "+" in the alarm zone header area to add a new device to the respective zone.

Server Livecheck

Define here network devices that are to be monitored for availability using one of the two service types ICMP Ping or Portcheck.

The AlarmManager cyclically checks whether a request on the service provides a positive response.

The polling interval can be freely defined between 60 and 999 seconds. Please note that the alarm is first triggered after at least 2 failed attempts.

Network cameras

When an alarm is triggered, the AlarmManager can control cameras connected to the network and record image data. The images are then linked to the respective alarm event. A camera is always assigned to an alarm zone.

The HTTP command for retrieving the image data can be found in the documentation of the camera manufacturer.

I/O Modules

The AlarmManager-PRO can be expanded with additional modules (KIO7017, KIO7052, KIO7053) with additional digital inputs and outputs.

This makes it possible to have external alarms for monitoring e.g. air conditioning or extinguishing systems and UPS or other alarm systems.

5.15. Execution of Firmware Updates

We are always looking to include innovations of development in our products and to ensure their faultless operation. Therefore regularly updates are released. To execute an update pay attention to the following steps.

No	Step	Comment
1	Download and unpack the actual firmware version for the respective device from the Kentix website. You can find the firmware in the section „Download & Support“, „Software and manuals“.	
2	Log in to the web interface of your device and go to the section „System“ -> „System functions“.	
3	Always create a backup before starting with the update.	A firmware update is only possible after the creation of a backup. The configuration of the device will remain.
4	Now select the firmware file via the file dialog and start the update.	After a reboot the AlarmManager is up-to-date with its complete configuration.

6. MultiSensors



The MultiSensor-RF (ZigBee radio) and MultiSensor-LAN (network) mainly differ in the way of communication. Additionally the MultiSensor-LAN offers the possibility to operate without an AlarmManager stand-alone. Both types of the MultiSensor offer a wide range of integrated sensors and so are the ideal device to completely monitor critical infrastructures.

6.1. Mounting instructions for MultiSensor-RF / -LAN / -LAN-RF

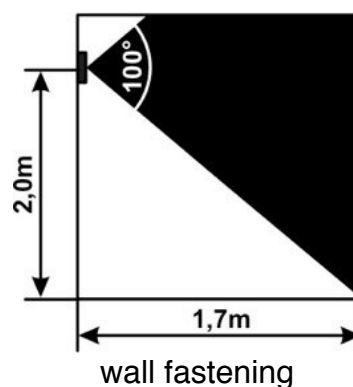
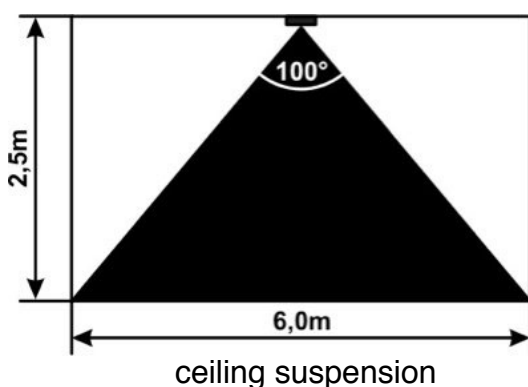
The MultiSensor is equipped with various individual sensors. To get an optimal sensitivity and function of the sensors, please note the following installation instructions.

Note the following instructions:

- Do not install close to heaters or direct heat.
- Avoid detection of moving objects such as fans, plants, trees, flags, etc.
- Don't cover the Sensor. The PIR-Sensor needs inter-visibility for detection.

6.2. Coverage of the integrated PIR movement detector

The range of the MultiSensor is depending on the configured sensitivity about 8m. You get the best results, when objects/persons move past the MultiSensor.



6.3. Calibration of the temperature / humidity sensor

For the MultiSensor-RF / -LAN and -LAN-RF devices, it may be necessary to calibrate the combination sensor for temperature and humidity once after installation and commissioning.

For this, the temperature must be determined in the immediate vicinity of the MultiSensor (for example with an infrared thermometer). The difference between the two measured temperatures (meter and MultiSensor) is then entered as an offset in full degrees in the corresponding field in the sensor configuration.

The correction also has a direct influence on the determined air humidity.

NOTICE!

Depending on the orientation of the MultiSensor (for example, wall mounting, test mode with lateral position or cover upwards) and the conditions (air conditioning) in the room, a correction by several degrees may be necessary.

6.4. Kentix system port on MultiSensor-RF / -LAN / -LAN-RF



The Kentix system socket of the MultiSensor can be used to install system components, such as leakage sensors, door contacts, sirens or external alarms can be connected of UPS or air conditioners. At the MultiSensor-RF the system jack is also required for the power supply of the sensor.

Two adapters are available for connecting external devices or external alarms with inputs or outputs:

- 1) Power-Adapter KIO 1: power supply, 2 digital inputs
- 2) Power-Adapter KIO 3: power supply, 2 digital inputs and 2 relay outputs

6.5. MultiSensor-RF

The MultiSensor RF is configured via the AlarmManager. Perform of updates is not possible or required.

6.5.1. MultiSensor-RF teach-in

1. To add a MultiSensor RF to the AlarmManager configuration, in the alarm zone header area, select "+" in the dashboard and then select "MultiSensor (Radio)".
2. Press the learn button for 3 seconds, which you can access via the recess on the back of the housing.
3. The sensor should be detected within 15-20 seconds. Subsequently, the configuration mask for the sensor is opened directly. The teach-in process is completed.
4. Make the individual settings for configuring the sensor and then save the settings.

6.6. MultiSensor-LAN

In contrast to the MultiSensor RF with radio interface, the MultiSensor LAN can also be operated in stand-alone mode without AlarmManager. For configuration in stand-alone mode, a web server is integrated via which you can configure and operate the device via the network with a web browser. The SNMP software interface makes integration into network management systems easy.

Connection via PC: Connect the LAN jack of the MultiSensor-LAN with a PoE enabled switch. Also connect your PC to the same switch. Set the IP address of your PC to e.g. „192.168.100.123“.

6.6.1. Default settings / Factory defaults

Voltage supply:	PoE (Power over Ethernet). Operation with external power supply possible.
Default IP-address:	192.168.100.223
Subnet mask:	255.255.255.0
User / password:	admin / password

IMPORTANT! - Reset to factory defaults

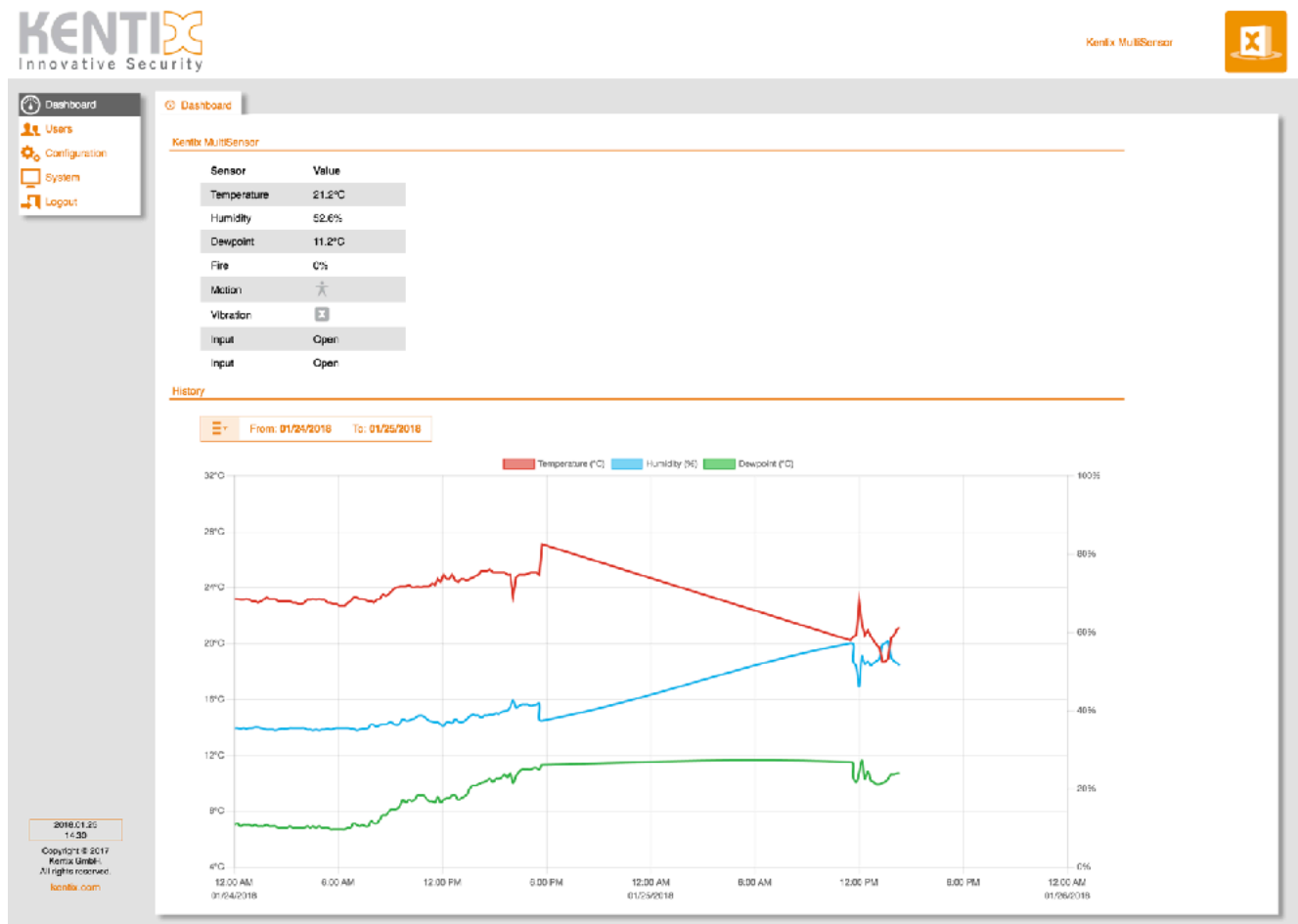
In the case that the IP-address or login data are lost it is possible to reset the MultiSensor-LAN to factory defaults. For this there is a RESET button which can be reached via a hole on the back of the device. Reboot the device and wait until the internal status LED turns green again.

Now press the reset button for about 10 seconds, until there is an acoustic feedback. After about 30 seconds the MultiSensor will reboot and can then be reached again using the default settings.

6.6.2. Software function MultiSensor-LAN

In the following, the stand-alone functionality of the integrated web server is described. For the described functionality no AlarmManager is required. When operating the MultiSensor-LAN with the AlarmManager-PRO, the AlarmManager controls the configuration and monitoring functions.

Dashboard



MultiSensor values and status:

Display of the sensor measurements and alarm conditions. This display will be actualized all 5 seconds.

NOTE!

The Sensor records a value for temperature and humidity every 10 minutes. Additionally the values in an alert case are also recorded.

Navigation

Dashboard	- Starting page with measurement table, graphic history, logbook
Sensors	- Configuration of sensor thresholds, alarm behavior and motion detection
User	- User configuration (Login, E-Mail)
Configuration	- Basic settings, network and notification settings
System	- System log book, configuration management (backup / restore), firmware update, SD card management
Logout	- User logout

6.6.3. Sensors (sensors and alarming)

In the following settings you can set the limit and action values for the alerting.

When an alarm is triggered, an e-mail will be sent to the configured persons and the internal buzzer is activated.

Sensor-Temperature, Humidity, Dew-point

Set the alarm limit values. Alarm will be triggered when the measurements undershot or exceeded the limits. The temperature hysteresis is 1°C, humidity hysteresis 1%.

The dew-point is calculated with the current temperature and the relative humidity from the sensor.

If the room temperature approximates to the difference of the set dew-point hysteresis (2°C default) an alarm will be triggered. Systems and devices can lead to condensation, when the dew point temperature approximates the room temperature.

Sensor-Carbon Monoxide

Alarm settings for the Carbon Monoxide. The sensitivity can be set from 0% to 100% and will be triggered by exceeding. CO is measured from about 10ppm. There is no exact measurement of the CO content. The measurement is construed to the highest sensitivity and can be changed slightly in the adjustment.

Carbon Monoxide concentrations like they emerge in fires are detected even at 100% setting.

10%: Minimal concentration of around 20-50ppm lead to an alarm trigger.

100%: Concentrations of 200ppm and more lead to an alarm trigger.

Sensor-Motion

Limit value for the integrated PIR (passive infra-rot) motion detection. It is triggered when exceeded. Objects which have a temperature difference of about 4°C to the environment temperature and which are bigger than 250x400mm will be detected. For a safe detection of persons, the value should be in the range of 30-50%.

The detection range is about 100°.

Sensor-Vibration

Alarm settings for the sensitivity of the internal vibration sensor. The sensitivity can be adjusted in 3 levels.

If necessary the vibration sensor can also be completely turned of.

Ext. alarm sensors

The MultiSensor has two configureable alarm inputs. At this alarm inputs external signaling devices can be plugged (e.g leakage sensors, door contacts or malfunction messages from external devices). The trigger is set by a potential free contact (opener). The trigger logic can be set to Open or Closed.

Ext. alarm output

With this output external devices or signals can be switched. An additional adapter (KIO3) is required for use. The description can be found later in this manual.

Alarm repeat

Set the time, when a triggered alarm shall be triggered.

The alarm will be sent to the entered e-mail-addresses until all values are in normal range again.

A value of 0 sets the alarm repeating to inactive

Alarm buzzer time

Time in seconds how long the internal buzzer will sound after an alarm.

Alarm relay time

Time in seconds, how long the open collector output is set when an alarm is triggered.

Motion detection - Arm-Disarm time

Switching time for the time-controlled arming and disarming from the integrated motion detection.

To use it, a time server (NTP) must be set in the network settings.

6.6.4. Users

User accounts

You can set up to 5 user accounts with individual passwords. With the first user it is also possible to access the integrated FTP server. For the e-mail alerting, enter the addresses of the recipients.

6.6.5. Konfiguration

Device name

Configuration of the device name, this is freely selectable

Language

Select the display language of the website of the Kentix MultiSensor-LAN.

You can select between German and English language.

Temperature unit

Changes the temperature evaluation and display of the MultiSensor-LAN between Celsius and Fahrenheit.

Communication key

The communication key is used for data encryption when operating with an AlarmManager.

This must also be stored in the AlarmManager.

NTP1/2

Configuring the Time Server (Network Time Protocol). The NTP configuration is required for timed arming and data logging.

Public NTP Server: 0.de.pool.ntp.org or 1.de.pool.ntp.org

IP Address / Netmask / Gateway / DHCP / MAC Address

Network configuration of the MultiSensor. You can enable DHCP for IP configuration, in which case the MultiSensor must always be assigned the same IP address from the DHCP server. The MAC address of the device can be read here. This is required for router or firewall settings.

Changes on network settings are active direct after saving the configuration.

DNS 1/2 (Domain Name Server Addresses)

Depending on the network configuration, e.g. if using an ADSL router, this may also be the gateway address.

Public DNS Server: 8.8.8.8 or 8.8.8.4

AlarmManager communication

Enable communication with a Kentix AlarmManager PRO. Enter the IP address of the AlarmManager and activate the communication by ticking the box.

The AlarmManager-PRO takes over the configuration of the alarm settings of the MultiSensor, the local alarm / threshold values are then inactive.

E-Mail

If the MultiSensor should be able to send e-mails in the case of alarm to a configured user, it is necessary to set an e-mail server (SMTP or ESMTP). When you have set a DNS server, which is configured in the DNS settings, you can use the DNS name of the e-mail server here. With using ESMTP you can here enter the e-mail access data, which you can obtain from your e-mail provider. Depending on the E-mail server, an encryption method might be necessary. When choosing an encryption mode (STARTTLS / SSL) the required port will be set to the default port. The port can be changed to another one when needed.

Pay attention that many mail servers need an existing sender address to send an e-mail correctly.

In the subject of the e-mail the corresponding alarm text can be found and in the mail text all measurements from the MultiSensor are included.

E-Mail Signature

Enter a signature, which is sent with every alarm E-Mail. The signature is limited to 300 signs length.

SNMP settings

Configuration of the Simple Network Management Protocols. The MultiSensor-LAN is able to send alarm messages as SNMP-Traps. Enter **both** SNMP host addresses for this. Further the sensor can be prompted or partially configured via SNMP. The functions which are available for the SNMP communication are specified in the supplied MIB (Management Information Base). It is available on the integrated FTP server or as download from the Kentix website.

Network camera

In the event of an alarm, the MultiSensor LAN can retrieve image data from a network camera and save it to an SD card. The image data is then linked to the logbook entry of the alarm. For this purpose, any network camera can be used, where it is possible to pick up pictures via an HTTP command.

Enter a name for the camera (such as installation location), as well as the camera-specific data such as IP address and user data, and select the location of the camera.

The field "HTTP command" contains an example of an AXIS camera. Enter the path to the image source file without specifying the IP address or communication port starting with a slash.

6.6.6. System

Logbook

Regardless of the event log, all messages relevant to the functionality of the Kentix system are stored here. For example, the logbook contains messages about logging in to the MultiSensor, configuration changes, and alarm notification messages.

With the help of the logbook possible misconfiguration can be understood.

System functions

In the section System functions a backup of the configuration can be created and restored.

In addition, a firmware update can be performed here.

Firmware updates are available for download from the Kentix website. For a description of how to perform firmware updates, see later in this guide.

Wireless settings (ZigBee - MultiSensor-LAN-RF)

This section displays information about the current ZigBee wireless network. In addition, the radio channel can be changed here and the radio network can be reset.

NOTICE!

If the radio channel is changed, it may be necessary to re-teach some sensors.

When the radio network is reset, re-teaching all wireless sensors connected to the AlarmManager is necessary.

SD card

To record video images in the event of an alarm, an SD card must be inserted in the MultiSensor LAN.

The card is automatically recognized after insertion and can be formatted here if required.

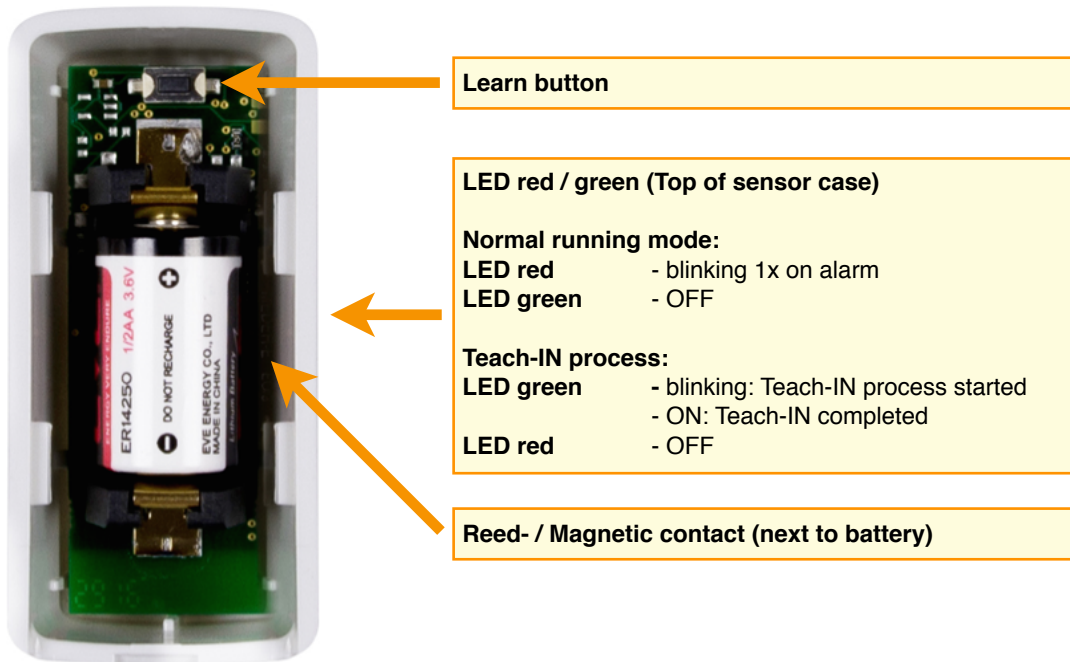
A previous deletion or adjustment of the file system is not required. SD cards with a memory size of up to 128 gigabytes can be used.

6.7. MultiSensor-Door

The MultiSensor-Door is designed for an efficient intrusion detection on doors or windows or for a specific environmental monitoring in a server rack.

The MultiSensor-Door is configured via the ControlCenter.
Updating the device is not necessary / possible.

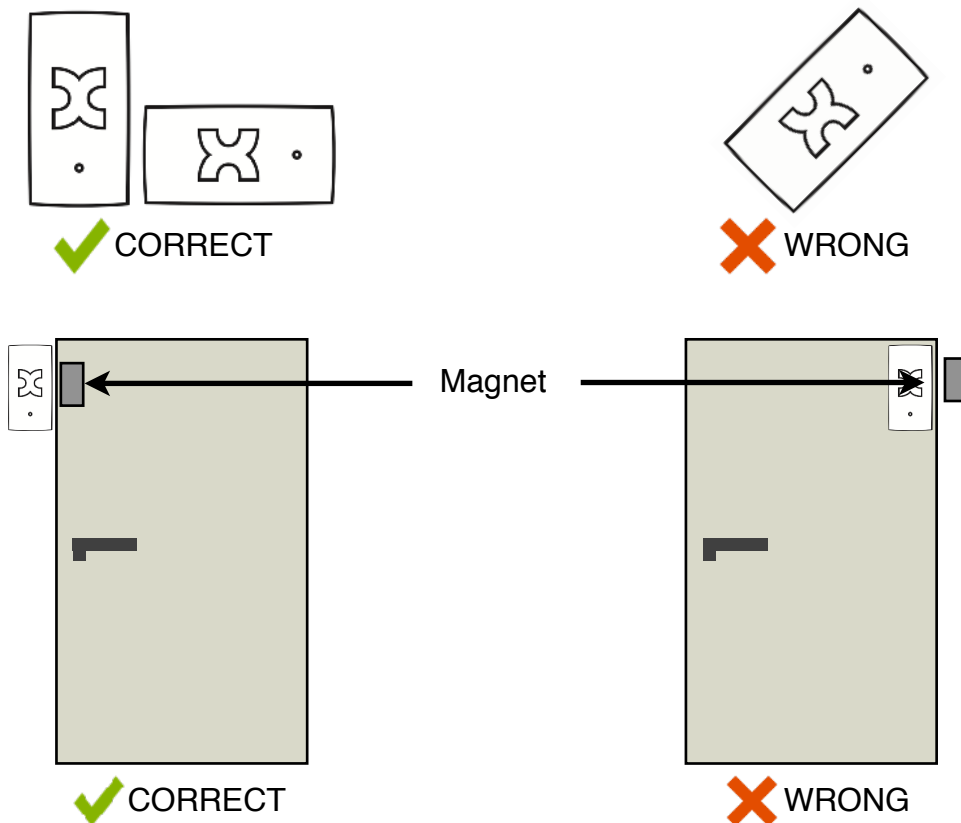
Interior view - MultiSensor-Door



6.7.1. Mounting instructions

The MultiSensor-Door is equipped with several different sensors. To ensure the best evaluation and functioning of the sensors, please note the following **mounting instructions**:

- Only install the MultiSensor in horizontal or vertical direction on the handle's side of the door or window
- to avoid false alarms the MultiSensor can be installed at the door frame or window frame and instead the magnet at the moveable part



- when using the reed contact, keep the distance to the magnet below one centimeter
- only use suitable mounting material (foam tape)
- sensor casing can be fastened with screws on the door frame or window frame, if necessary

ATTENTION!

Kentix is not liable for false alarming or damages on devices due to improper installation.

6.7.2. Usage of the reed contact

The reed contact extends the MultiSensor-Door by an additional alarm contact for the definite open/closed detection of a door or window. The contact reacts to magnetic fields (magnet contained in package). For the installation a wiring is not necessary.

To ensure the functionality of the contact, take care to not exceed the **maximum distance of one centimeter** between magnet and casing and orientated to one side of the casing of the MultiSensor.

Depending on the type of the door or window it might be necessary to place a spacer between surface and magnet to not exceed the maximum distance to the sensor.



6.7.3. Opening of the casing / replacement of battery

The board of the MultiSensor-Door is fixed in the lid of the casing which is placed on the bottom part. To open the casing, press the latching lug on the bottom of the housing downwards and push the casing upwards. It can then be easily taken off.

Take the battery out of the mounting and replace it with an equivalent type (see data sheet).

NOTE!

The battery level of the MultiSensor-Door can be read out with the ControlCenter. At a low battery level an alarm is sent via SMS and E-mail to all administrators. In this case replace the battery as soon as possible.

Please note that an active connection to an AlarmManager is required for the operation of the MultiSensor-Door. If the MultiSensor is not configured on an AlarmManager or the connection is interrupted, the battery in it will discharge much faster.

6.7.4. Adding a MultiSensor-Door

1. For adding a MultiSensor-Door to the AlarmManager's configuration, start the teach-in process in the Kentix ControlCenter. Press the „learn button“ and keep it pressed.
After 3 seconds there will be a short buzzing. The button can then be released.
2. The sensor should appear in the list after approx. 15-20 seconds and is configured automatically.
3. The teach-in process is completed, when the sensor is marked in the list with a green checkmark.
4. For completion click on Apply to add the MultiSensor-Door to the devices list.

NOTE!

The MultiSensor-Door sends its data in a routine message every 5 minutes. Note that it can take up to 5 minutes after saving the data to the AlarmManager, until the sensors measurement values appear in the ControlCenter's dashboard.

6.7.5. Settings

The MultiSensor-Door is configured by 3 simple settings for the door-opener contact, vibration and sabotage:

Magnetic door contact

The default setting is „arming - only if closed“ and „armed-active“.

With this settings an arming is only possible if the door or window is closed and the sensor has detected the magnet. Arming attempts are otherwise directly terminated.

If the equipped door has to be opened during arming, the option „Arming“ must be changed to „Always arm“. During this phase the door can still be opened. After the arming an alarm will be triggered when the door is still open.

Vibration

For vibration a 3-step sensitivity can be selected. The vibration is used for the detection of burglary attempts. Mainly the two levels „High“ and „Medium“ presuppose that there are no external influences on the sensor which lead to false alarms.

Tampering

For the tampering detection the MultiSensor-Door is equipped with a „tilt-sensor“.

This sensor reacts on the change of the sensors angle/orientation - by removing and tilt of the sensor.

Please note that the tilt-sensor will only operate properly if it is installed vertically and not on moving parts (door leaf / window leaf).

6.7.6. Test of the settings

The alarming function of the MultiSensor-Door can be tested by simply opening/closing door or window. This will trigger a direct update of the sensors open/closed state.

NOTE!

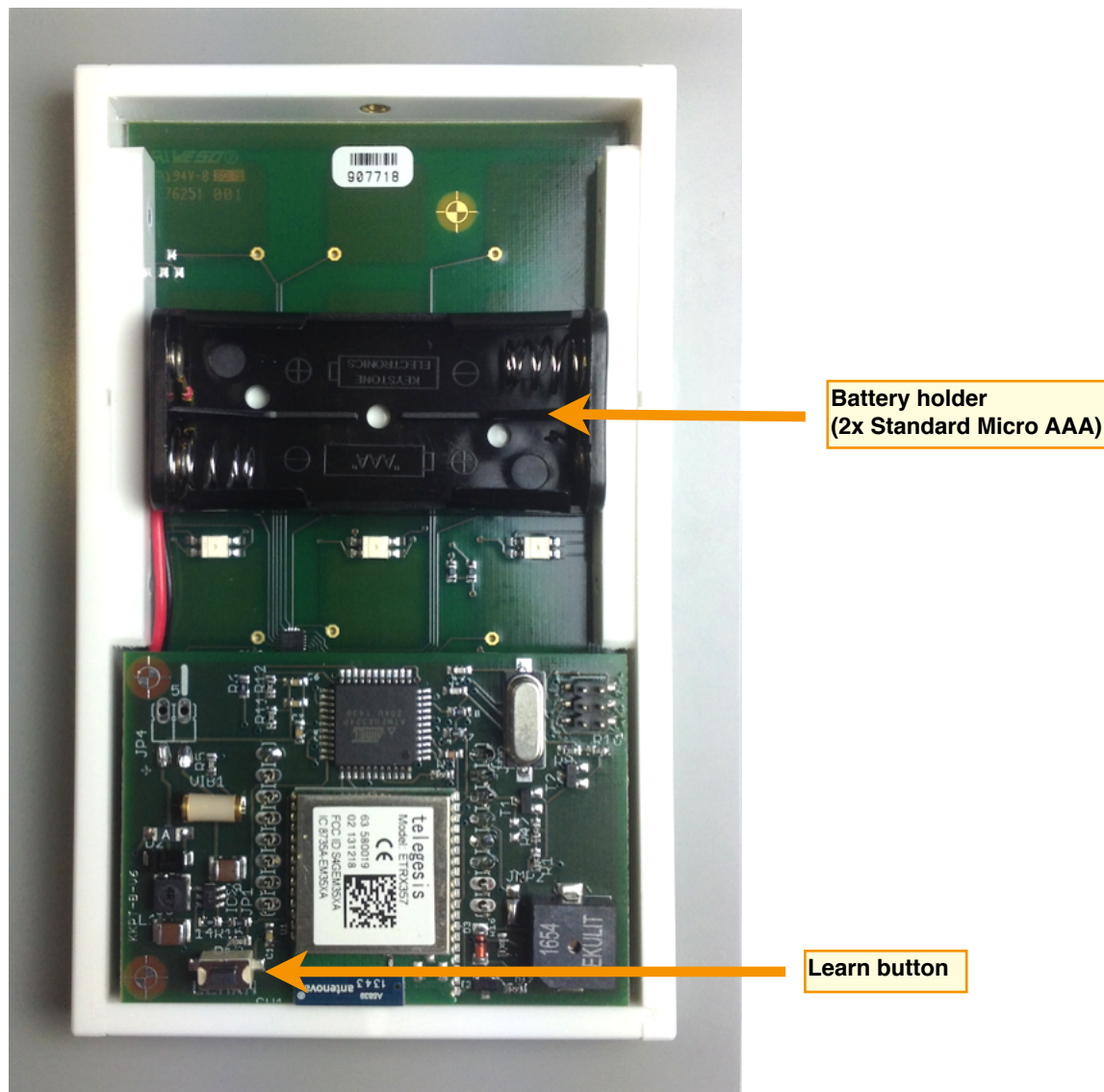
To test the alarming of MultiSensor-Door the sensor has to switch to armed state.

After the arming this can take up to 5 minutes. There will be no alarm triggering before.

7. KeyPad-Touch (KKPT)

The KeyPad is used for arm-disarm switching of the AlarmManager on site. The KeyPad is integrated into the ZigBee® wireless network of the AlarmManager in the same way as a MultiSensor-RF. Please note that the KeyPad does not work as a router and can not extend the network range.

The KeyPad is activated by pressing any button. The duty cycle is then about 10 seconds. During this time you can arm or disarm single alarm zones or the complete system.



7.1. Adding a KeyPad

1. For adding a KeyPad to the AlarmManagers configuration start the teach-in process in the AlarmManagers Dashboard and press the „learn button“ on the back of the KeyPad.
2. The KeyPad's LEDs signalize the running teach-in process.
3. The teach-in process is finished when the KeyPad is found and the configuration mask opens. The LEDs at the KeyPad turn green.
4. To add the KeyPad to the devices list, click on Apply.
5. After saving the configuration the KeyPad is activated in the system.

7.2.Operation Keypad

With the Keypad you have the possibility to switch either the assigned alarm zone or any other alarm zone:



Switch alarm zone

Enter the number of the zone, then press one of the function keys. Now enter your 4 digit PIN to finish the action.

The function will be triggered directly after the input of the last digit. Pressing a button is always signalized by a sound. The selected function is signalized by a LED in the function (arm disarm) button.

Switch pre-assigned zone or all zones together

By simply pressing one of the function keys (arm/disarm) and the entering of your PIN the pre-assigned zone is switched. Please note that a user needs the correct permissions for switching.

	Arming - leave the room <i>OK :</i> 5 seconds acoustic beep signal, LED lights constant, MultiSensors signal acoustically according to the arming buzzer time. <i>Not OK :</i> 3 seconds constant acoustical signal. All LEDs are flashing.
	Disarming - enter the room <i>OK :</i> 1 second constant acoustic signal, LED lights constant, MultiSensors signal also with 1 second acoustic signal.
	RFID reader Select the desired function (arm, disarm, enter zone number) and place the RFID card in front of the reader. The function is executed immediately after the correct read.

Operation via RFID

To operate the Keypad a RFID card can be used instead of the 4-digit PIN.

Activate the Keypad and enter either the zone number or directly press one of the function keys. Now place you RFID card in directly in front of the X.

IMPORTANT!

Via the Keypad only „armed-active“ alarms can be switched. All alarms of the type „always-active“ are always triggered, independent from the armed-disarmed state.

Learn User / RFID cards

New RFID cards are added via the user configuration.

In the user's settings select the „+“ next to the RFID card field and select the Keypad.

Then press one of the buttons „Arming“ or „Disarming“ and hold the user card in front of the RFID reader (X). The number / ID of the card is now transferred to the field „RFID token“.

8. Enhancements

8.1. Leakage sensor (KLS03)

The leakage sensor KLS03 is shipped with a 10m patch cable for a direct connection to Kentix devices via the Kentix system jack. It is also powered by the system jack.

An LED indicates the current state of the sensor (GREEN: no alarm / no humidity; RED: alarm / humidity detected). To test the sensor touch it's bottom of the sensor with a wet cloth. The internal LED should signal the detection by glowing RED.

The detection unit is maintenance-free when detecting normal water. Aggressive or solvent-containing liquids can damage the sensor and cause false alarms. A contamination of the sensor electrodes also leads to incorrect measurements.



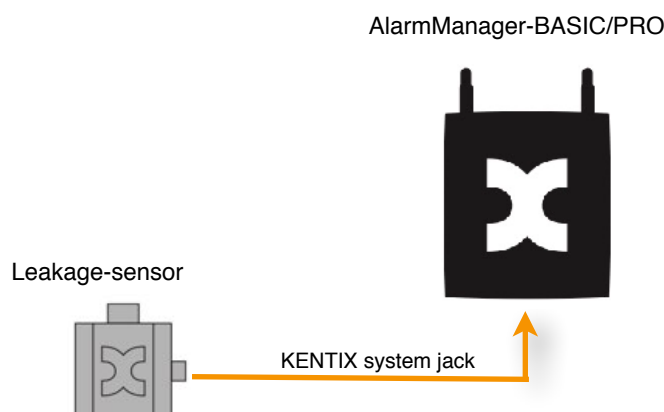
IMPORTANT!

The signaling for a connected leakage-sensor is realized via the external alarm input of the device to which the leakage-sensor is connected (AlarmManager or MultiSensor). For the correct functioning, this input has to be configured correctly (see examples).

Therefor its necessary to test the alert triggering after connection to ensure the correct cabling.

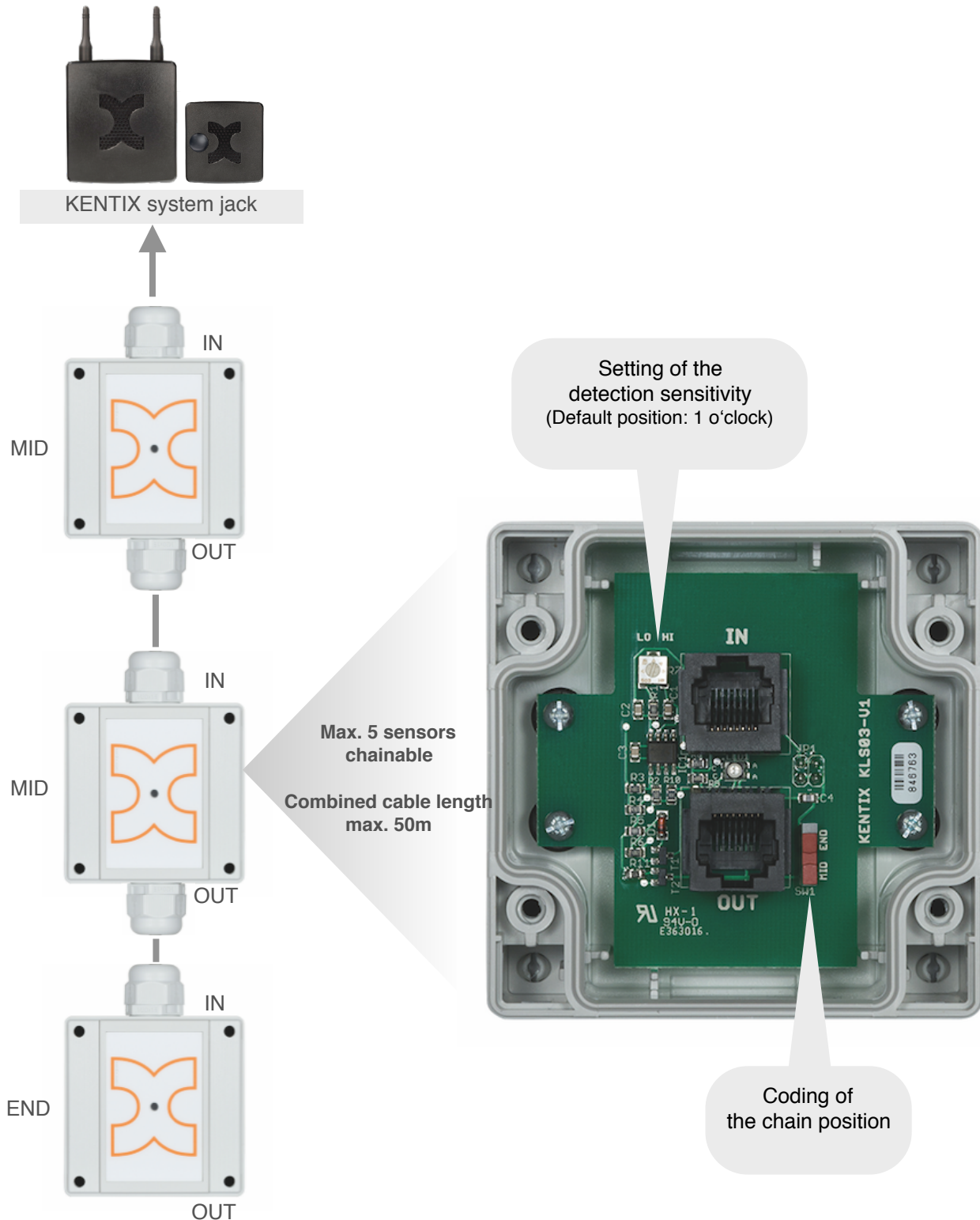
Connection example 1: Leakage-Sensor connected to AlarmManager

Plug the connection cable of the leakage-sensor into one of the System-jacks of the AlarmManager. The powering and alarming is done directly via the AlarmManager. With the ControlCenter enter a suitable name for the external alarm input and set the alarming of the input to „Always-Active“ for a permanent alarming. If the leakage sensor is working with opening the contact on an alarm, additionally change the alarm logic to „Open“.

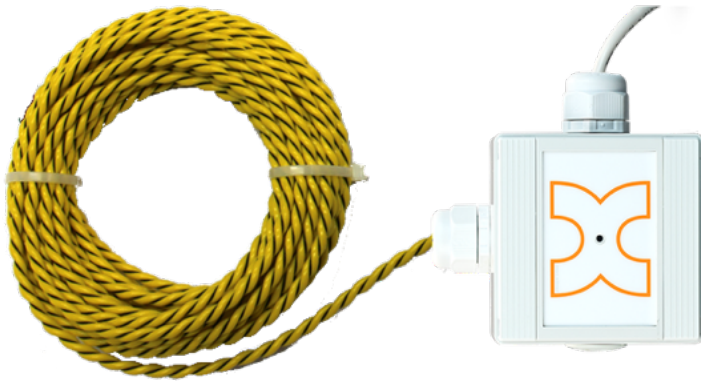


Connection example 2: Daisy chaining leakage sensors

It is possible to chain up to 5 leakage sensors together and connect them to a Kentix system jack via standard patch cables. Therefore they can be patched into structured wirings. The combined cable length should not exceed 50m. It is important to code the according sensors as intermediate or end device. For this purpose a micro switch is located inside the casing.



8.2. Leakage sensor rope (KLS03-ROPE)



The leakage sensor (KLS03) monitors leaks through the sensor electrodes at the bottom of the device. In a room with several locations where leakages could occur, it is possible to cascade up to 5 KLS03 and operate these at one AlarmManager or MultiSensor.

Alternatively a leakage sensor with a 10 / 20 meter rope is available. Here the whole cable serves as a detector to detect leaks with a single sensor over a length of up to 20 meters.

The KLS03-ROPE works in the same way as the standard KLS03. It also has the sensor electrodes at the lower side of the housing and also here a cascading of up to 5 sensors is possible.

The rope of the leakage sensor must be fixed to the floor. Recommended for this is the use of anchoring clamps for single pipes with a drill hole diameter of 6mm and a clamping range of 3-13mm. The distance of the clamps should be between 30cm and 50cm.

8.3. Kentix Power-Adapter (KIO1) with digital input clips

The Kentix I/O Power-Adapter is used to expand your Kentix-solution to include the additional functions:

- Power supply for up to two MultiSensors-RF via an AC adapter
- Connecting of up to two external alarms via dry contacts to a MultiSensor

The adapter is connected directly to the Kentix system jack and offers the possibility to power the MultiSensor with a power plug or a permanently connected AC adapter.

The cable length between MultiSensor and the KIO1 adapter should not exceed the following lengths:

- Power supply only: up to 50m
- Power supply with digital inputs: up to 10m

Important!

When using the input clips for external alarms and simultaneous power supply of two MultiSensors remove the jumpers. Otherwise the external alarms will be indicated on both sensors.

Figure 1: Back of Kentix Power-Adapter (KIO1)

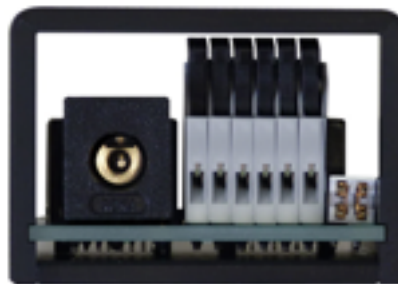
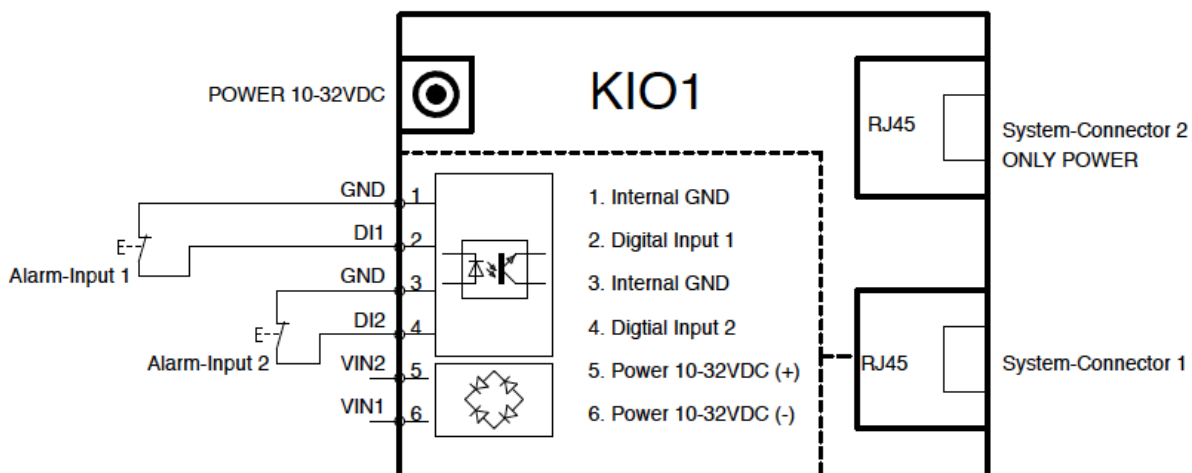


Figure 2: Circuit diagram with external alarms



8.4. Kentix Power-Adapter (KIO2) for powering a MultiSensor

The Kentix I/O Power-Adapter KIO2 is used to expand your Kentix solution by offering the following features:

- Connection of a MultiSensor-RF/-LAN/-LAN-RF for a separate power supplying

The adapter is directly connected to the Kentix system jack and offers the possibility to supply power for one MultiSensor via an external power supply.

This can be necessary e.g. if no PoE-Switch is available for the operation of a MultiSensor-LAN/-LAN-RF or when a MultiSensor-RF shall be connected separately to monitor the external power.

The cable length between MultiSensor and the KIO1 adapter should not exceed 50 meters.

Figure 1: Back view of Kentix Power-Adapter (KIO2)



NOTE!

This adapter can only be used for the power supply of one MultiSensors. The alarm inputs and outputs are not available when this adapter is used.

8.5. Kentix Power-Adapter (KIO3) with digital I/O clips

The Kentix I/O Power-Adapter is used to expand your Kentix-solution to include the additional functions:

- Connecting of up to two external alarms via dry contacts to a MultiSensor
- Controlling resp. switching of up to two external devices via relays by a MultiSensor

The adapter is connected directly to the Kentix system jack and offers the possibility to power the MultiSensor with a power plug or a permanently connected AC adapter.

The cable length between MultiSensor and the KIO3 adapter should not exceed 10m.

The relays are equipped with PDT contacts and can be loaded with up to 60VDC/3A.

Figure 1: Back of Kentix Power-Adapter (KIO3)

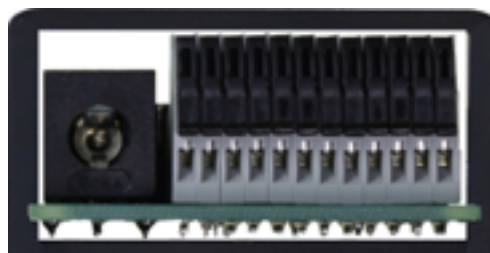
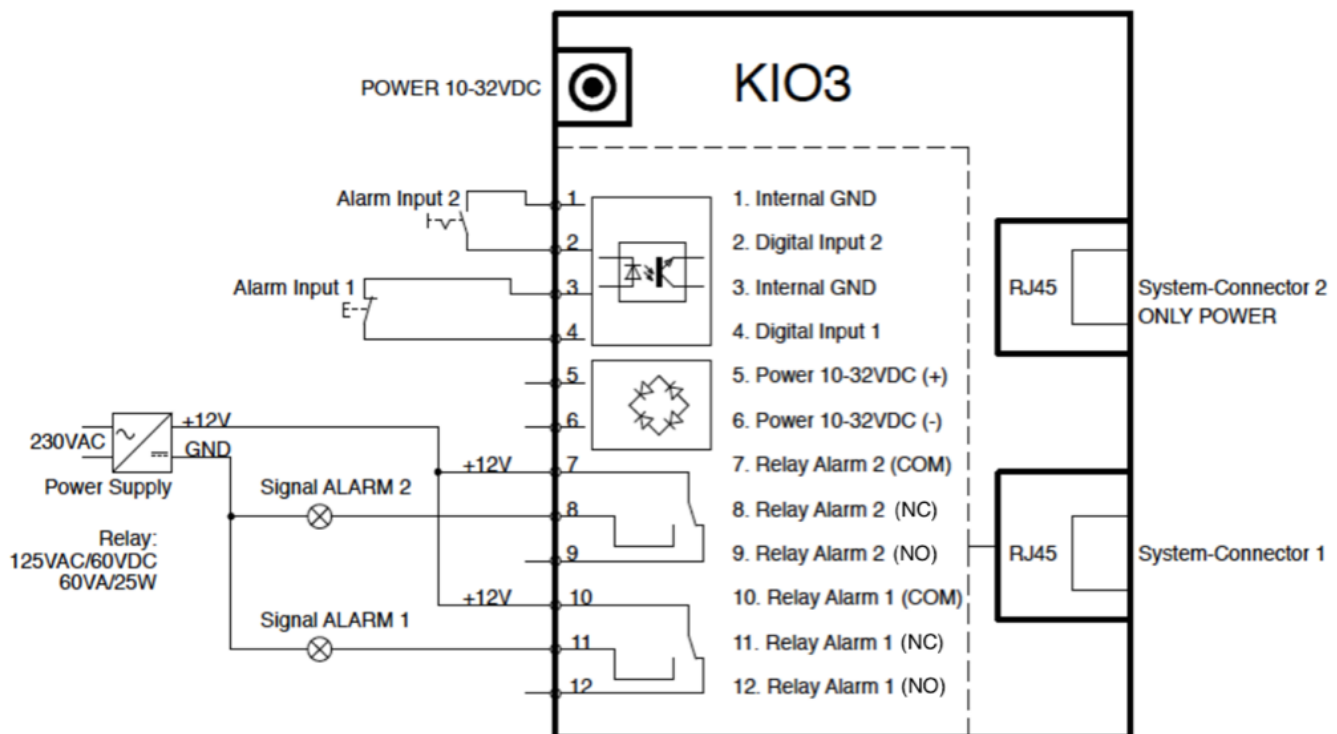
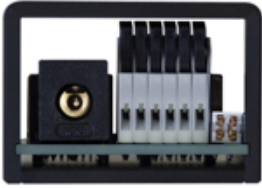

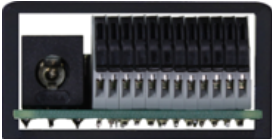


Figure 2: Circuit diagram with external alarms



8.6. Overview and application examples for Power-Adapters (KIO1-3)

Image	Description	Application examples
 <p>KIO1</p>	<p>Power-Adapter with digital I/O clips Adapter block for the connection of 2 MultiSensor-RF to a power supply via the Kentix system jack. Additionally a terminal block for using the alarm inputs at one MultiSensor is available.</p> <p>Terminal block:</p> <ul style="list-style-type: none"> • Digital inputs: 2 • Digital outputs: 0 • Power supply: Terminal block or AC adapter 	<ul style="list-style-type: none"> • Operation of one Kentix leakage sensor at a MultiSensor-RF • Connection of external components to the alarm input of a MultiSensor (e.g. air conditioning, door contact)
 <p>KIO2</p>	<p>Power-Adapter Adapter block with AC adapter for powering one Kentix MultiSensor via the Kentix System jack.</p> <p>Terminal block:</p> <ul style="list-style-type: none"> • Digital inputs: 0 • Digital outputs: 0 • Power supply: AC adapter 	<ul style="list-style-type: none"> • Power supply for one MultiSensor-RF/-LAN/-LAN-RF • Connection of one MultiSensor-RF to monitor the external power supply • Power supply for a Kentix Alarm sirene plus one MultiSensor-RF/-LAN/-LAN-RF via a RJ45 T-Adapter (included with Alarm sirene)
 <p>KIO3</p>	<p>Power-Adapter with digital I/O clips Adapter block with 2 digital inputs and 2 relay-outputs and 2 Kentix System jacks for the connection of MultiSensors.</p> <p>Terminal block:</p> <ul style="list-style-type: none"> • Digital inputs: 2 • Digital outputs: 2 • Power supply: Terminal block or AC adapter 	<ul style="list-style-type: none"> • Connection of external components to the alarm input of a MultiSensor (e.g. air conditioning, door contact) • Connection of a LED to display the arm/disarm state via the 1st sensor output (relay 1) • Connection of a door control to open a door when disarming an alarm zone

8.7. Kentix Alarm siren (KFLASH1)

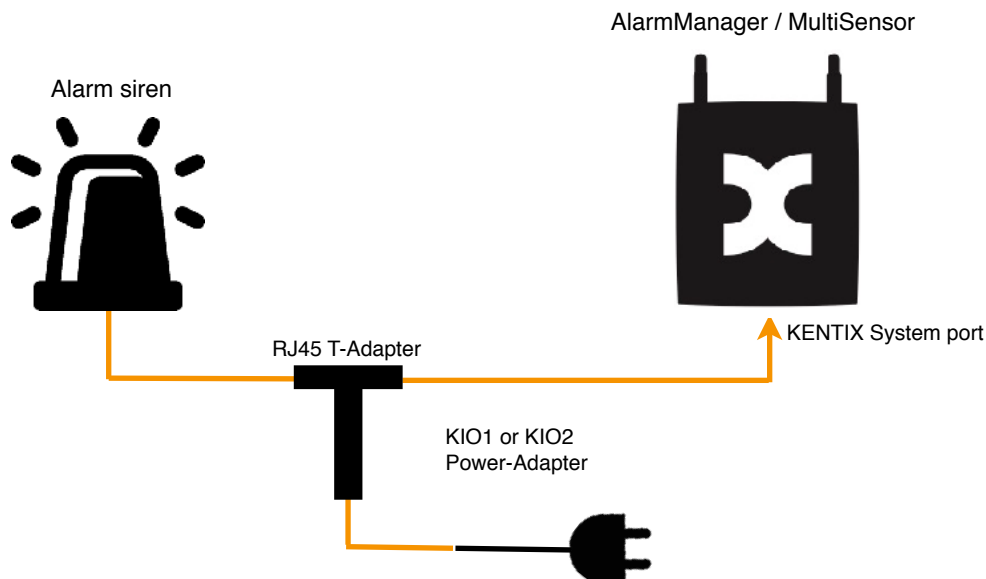
The Kentix Alarm sirene can be used for an acoustical and optical signalization in case of an alarm. It is suitable for an indoor and outdoor installation (protection class IP65).

The Alarm sirene is equipped with a 10 meter patch cable and a RJ45-connector and can be directly connected to the system jacks of an AlarmManager or to all MultiSensor-RF/-LAN/-LAN-RF using an additional adapter (RJ45-T-Adapter). The required adapters are included with the Alarm sirene.

Connection example: Alarm siren at AlarmManager or MultiSensor

Plug in the Alarm sirene into the RJ45 T-Adapter and connect the MultiSensor to the socket next to it using a patch cable. The power supply is done via a Power-Adapter (KIO2), which is connected to the opposite side of the T-Adapter.

When also the alarm input of the connected MultiSensor shall be used (e.g. by connecting a leakage sensor), a KIO2 Power-Adapter can be used instead of the KIO1. In this case all connection cables have to be patch cables.



8.7.1. Configuration

To trigger the Alarm sirene relay times have to be configured in the AlarmManager or the MultiSensor.

For the AlarmManager and all MultiSensors operating in AlarmManager mode the relay timings in the settings of the corresponding alarm zone are also used for the sounder.

Here one time for armed-active alarms and one time for always-active alarms can be defined.

8.8. Kentix IO-Modules

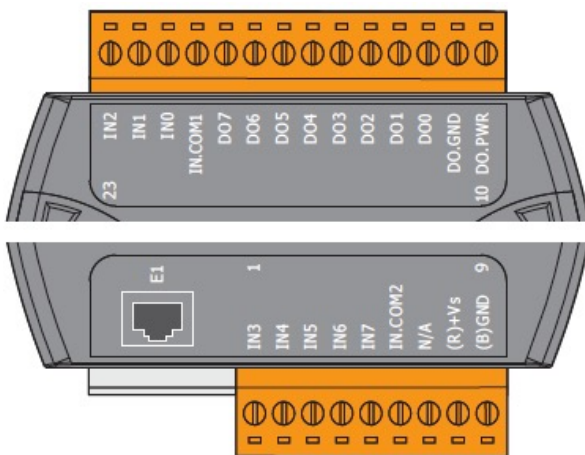
The AlarmManager-PRO can be extended by additional digital Inputs and Outputs via special Expansion modules. For this 2 external modules (KIO7052 with 8 digital Inputs / Outputs and KIO7053 with 16 digital Inputs) are available.

Both modules are configured via a Web browser and are queried by the AlarmManager over the network.

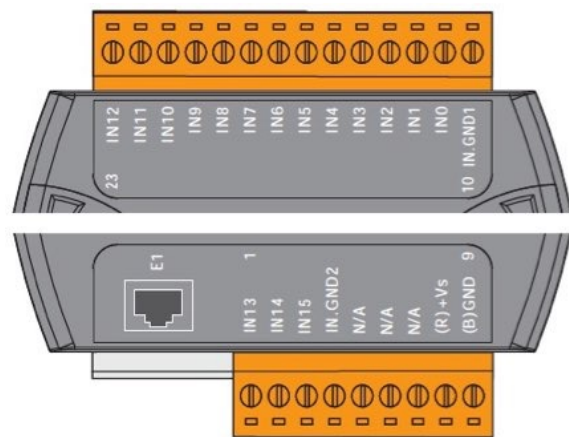
Commissioning and Configuration

Depending on the module type it can be powered via PoE or with an external power supply. Using a power supply it is necessary to regard the information in the data sheet, or only to use a power supply delivered by Kentix. Information for the wiring of the In- and Outputs can also be found in the data sheet.

Terminal assignment KIO7052



Terminal assignment KIO7053



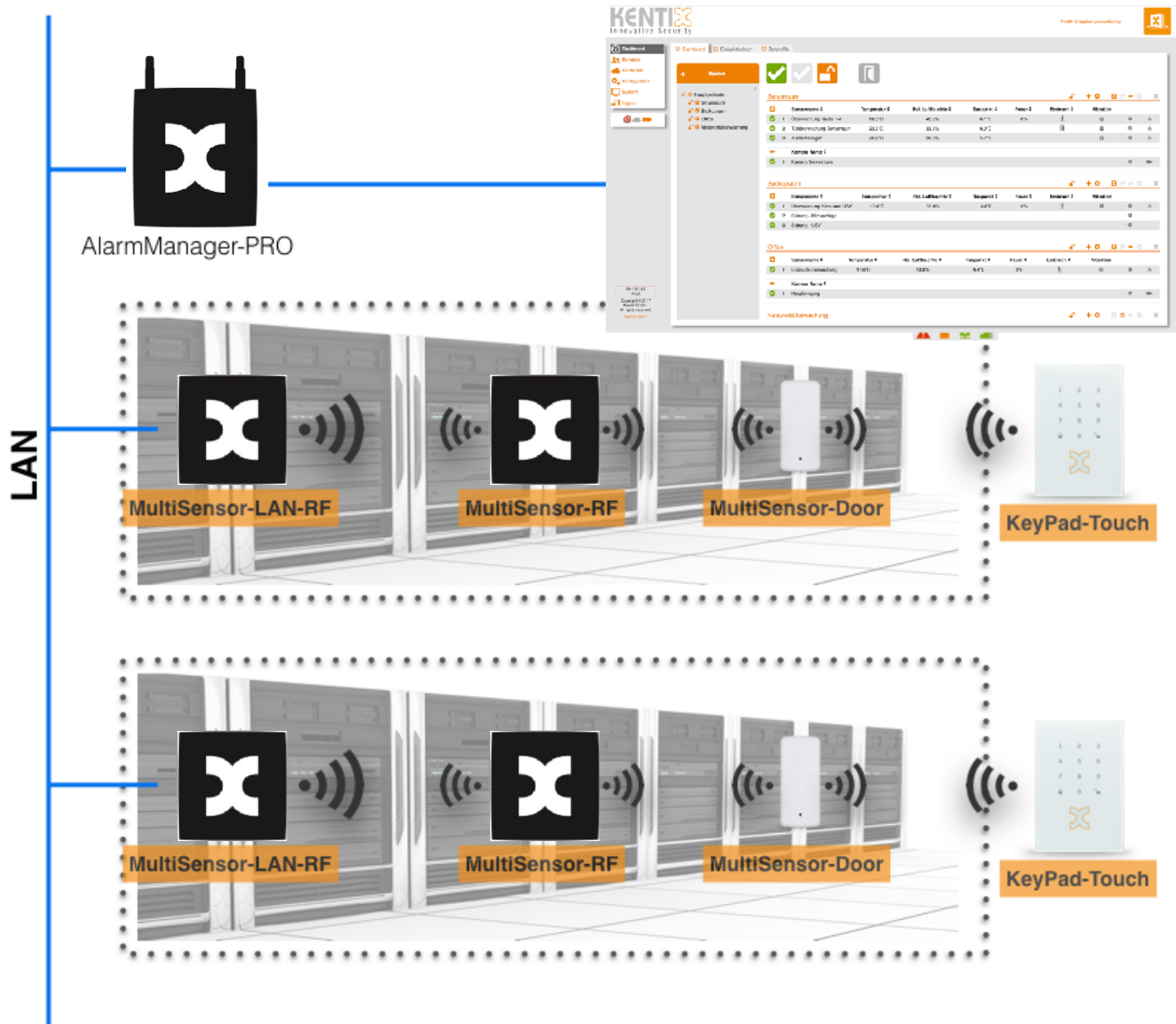
No	Step	Comment
1	Connect the network port E1 to a network switch with PoE support. Connect your PC to this switch respectively establish a network connection.	If you use a switch without PoE establish power supply via the connectors (R)+Vs and (B)-GND. Use the supplied power adapter-cable.
2	Open the Web-Interface of the module via the default IP 192.168.255.1 and change the IP-settings in „Network Settings“ to your required settings. Default username and password: Admin/Admin	In the section „Web HMI“ the Inputs and Outputs of the module can be monitored for test purposes.
3	Connect to the AlarmManagers web interface and add a new IO module via the dashboard.	Select the module type and set the configured IP-address.
4	Proceed with the setup for the wired external Inputs: Enter a name for the alarming and choose alarm assignment and the alarm logic. Eventually enter another alarm delay (default 1 sec.). Also select an alarm zone for every used input.	In the module KIO7052 for each alarming state one of the 8 outputs is switched. The type of alarm can be assigned free (s. data sheet for alarm types).
5	Save the configuration. After this the settings are directly active.	Each active input will be listed up in the dashboard with its state.

8.9. MultiSensor-LAN-RF (LAN-ZigBee Repeater)

The MultiSensor-LAN-RF offers the same functionality as the MultiSensor-LAN.

Moreover it allows the creation of a dedicated radio network. With this option it is possible to realize a connection to distant RF-Components (MultiSensor-RF / -Door / KeyPads) via LAN/WAN. The configuration of the repeater and the connected components is done via the web interface of the AlarmManager.

If the sensor is added as LAN-RF-Repeater, additional sensors can be added via the „+“ for adding new devices to an alarm zone.



9. Smart Access - Introduction

Thank you very much for choosing to purchase a KENTIX access solution based on KENTIX DoorLock.

9.1. Product features

The KENTIX AccessPoint is the central component of the access solution. Door knobs, door handles, wall readers and cabinet locks are connected via radio here. The AccessPoint is connected to the network via a PoE-enabled switch.

The web interface can then be used to change the basic settings, such as IP data, as well as the configuration of user data and profiles.

A description of the configuration can be found later in this guide.

Kentix Smart Access offers a fully networked locking solution that can combine up to 15,000 doors into one system.

The smallest unit is the Kentix Wireless Knob in combination with a mechanical lock cylinder or wireless door handle, wall scanner or cabinet lock. The components can either be operated wirelessly with the Kentix AccessPoint, or Offline (easy setup and management via the programming card set).

The Kentix AccessPoint implements networking of the devices with each other.

9.2. Application areas

- Industry and trade
- Banks
- Authorities and hospitals
- Telecommunication
- Chambers and practices
- Energy and water supplier

9.3. Safety instructions

The installation of the AccessPoint and all DoorLock components must be carried out by a qualified person.

In the event of a power failure, the settings of the AccessPoints are not lost.

To bridge longer downtime, use a suitable UPS.

Installation

To ensure the safety and integrity of the operator as well as the correct operation of the KENTIX DoorLock components, the installation must be carried out by a competent person. In addition, the relevant regulations must be adhered to.

Environment

The installation site must be selected so that the KENTIX AccessPoint and all associated cables are not affected by the following environmental influences:

Dust, moisture, excessive heat; direct sunlight; heat sources; devices that generate strong electromagnetic fields; liquids or corrosive chemicals.

Observe the ambient conditions given in the technical data.

Degree of protection

When installing an AccessPoint, certain degrees of protection must be guaranteed. Observe the relevant regulations for installations in specific environments such as industrial or residential and commercial buildings.

9.4. Components

Equipping a door can be done in combination with the Kentix Online knob and the profile-cylinder or with an online door lever. Additionally a wall reader for the control of motor locks of gates and a cabinet lock is available. The commissioning of the DoorLock-devices is done with the programming card set. This card set is required only once per system. Multiple DoorLock-devices are put into operation with the same card set.

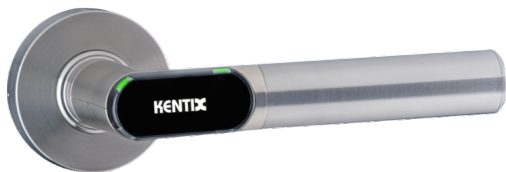
The cross-linking of one or several doors is done via the Kentix AccessPoint. This allows the complete management of users directly from the workstation and extends the functionality of the DoorLock-devices by the configuration of time-level-profiles and access logbooks, camera integration and more.

9.4.1. Online knob (DoorLock-DC) and profile cylinder



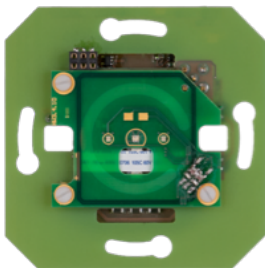
The Online knob is the RFID-Reader unit which is installed on the outer side of the door. Using the Kentix AccessPoint the knob can be linked wireless. The configuration of users and permissions is then done via the AccessPoint. Alternatively a configuration can be made directly at the door using the servicekey-card (Standalone-mode).

9.4.2. Online door lever (DoorLock-LE)



Like the knob the online door lever is equipped with a RFID reader unit. The electronic is completely integrated into the door handle. It can also be operated with or without AccessPoint (online- / offline-mode).

9.4.3. Online wall reader (DoorLock-WA)



The online wall reader expands Kentix DoorLock with additional application fields, such as factory doors, doors with motor control or barriers. It integrates completely into the DoorLock series with Online knob and online door lever. Integration, configuration and operation are completely analogous. Also here online or offline operation is possible. The wall reader is already equipped with a switching relay. In online mode it can also control one of two relays in the connected AccessPoint.

9.4.4. Online cabinet lock (DoorLock-RA)




The radio cabinet lock is a locking solution for the simple equipment or conversion of IT racks or distribution cabinets. The locker lock can also be used online or offline. In online operation with AccessPoint, the lock also seamlessly integrates with existing Smart Access solutions. The lock comes with various adapters and locking levers, making it adaptable to almost any IT rack.

9.4.5. IP Wall Reader and network relay module



The IP Wall Reader enables contact-free unlocking of doors with an RFID medium or alternatively via a pin code (two-factor-authentication also possible). A StarterSet comes with an IP Wall Reader, a network relay module and three RFID tokens. This set can be combined with one additional Extension Reader (only IP Wall reader without network relay module) in order to integrate an extra door into the system. Up to 1.998 IP Wall reader can be integrated with 999 Network relay modules.

9.4.6. Master card set

	<p>With the master card set the DoorLock-devices are prepared for the operation. Only one master card set is required per system / installation, which consists of these 4 cards:</p> <ul style="list-style-type: none"> • System card • Servicekey card • Battery change card • Dismantling card
---	---


NOTE!

Always keep these cards at a safe place. Without them a configuration of the components is no longer possible.

When the Servicekey card (=programming card) is lost, it is possible to order a replacement card with the help of the number printed on the System card.

Battery change card and dismantling card are only required at an Online knob, not for the other DoorLock-devices.

9.4.7. AccessPoint

	<p>The AccessPoint is the central component of the access solution. Online-knobs, door levers, wall readers and cabinet locks are connected wireless to this device. The AccessPoint is then integrated into the network via a PoE-enabled Switch. Now the basic settings like IP-addresses, doors and user data can be done via the web-interface. A description of the configuration can be found later in this manual.</p>
---	---

9.4.8. Accessories

To replace the batteries at an Online knob or cabinet lock a special battery replacement tool is required. The replacement tool for an Online knob is already included in every master card. For the cabinet locks, the tool has to be purchased separately.

For the replacement of the battery in a door lever a matching Allen key is required. This is always supplied together with the door lever.

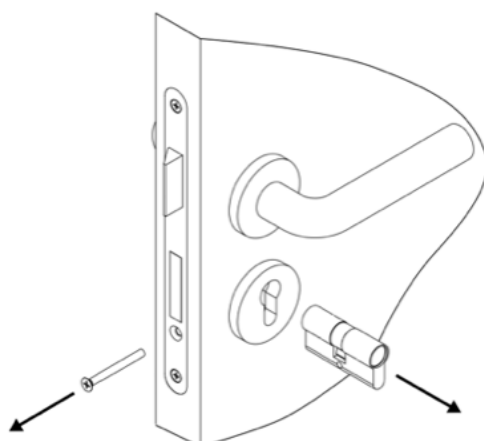
When fully discharged, it is no longer possible to open a Online knob for a battery replacement. For this purpose a „low power adapter“ is available to make single access bookings. A description of this emergency opening can be found later in this manual.

9.5. Installation & Programming (installation)

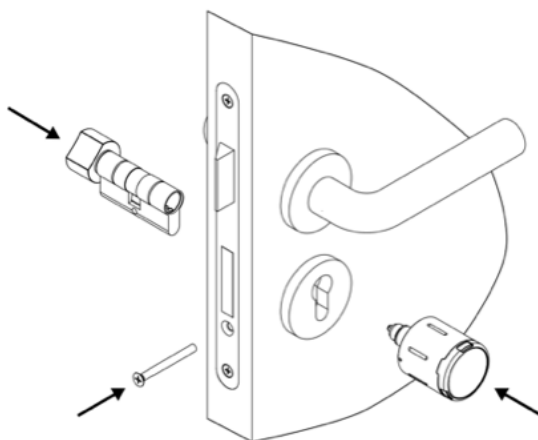
9.5.1. Online knob

For the installation only a few steps are necessary. Please follow the instruction as listed here:

No	Step	Note
1	Remove forend screw and pull the existing cylinder out of the door.	Every Kentix profile cylinder is delivered with a new forend screw.
2	Insert the Kentix profile cylinder into the door. Insert and fix the new forend screw.	The mechanical knob is already mounted at the profile cylinder. Plugging the profile cylinder into the door from the inside does not require additional disassembly work.
3	Plug the RFID Online knob into the cylinder until it clicks into place.	
4	The installation is then finished. If not already done, the knob can now be programmed with the master card set.	The programming of a knob can already be done before the installation at door.



Step 1: Remove forend screw and pull the existing cylinder out of the door.



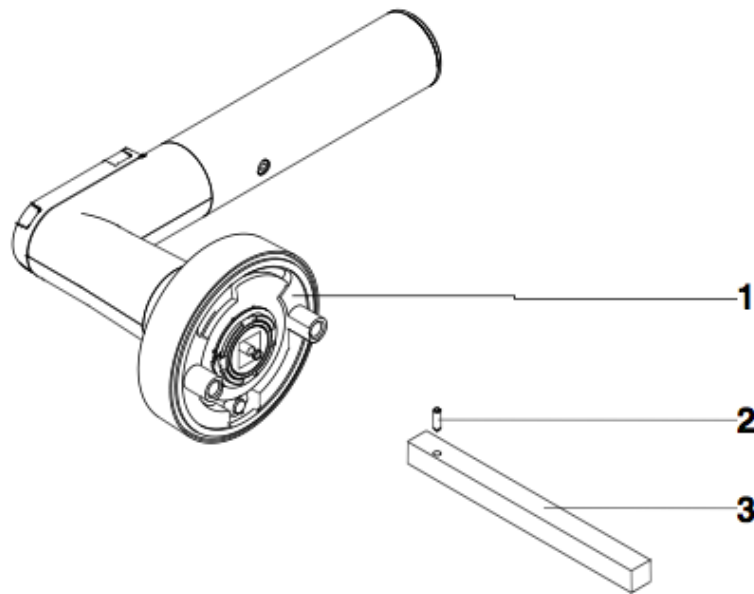
Step 2+3: Insert the Kentix profile cylinder into the door. Insert and fix forend screw.
Plug the RFID Online knob into the cylinder.

9.5.2. Online door lever

To install a Kentix online door lever, proceed as described in the following:

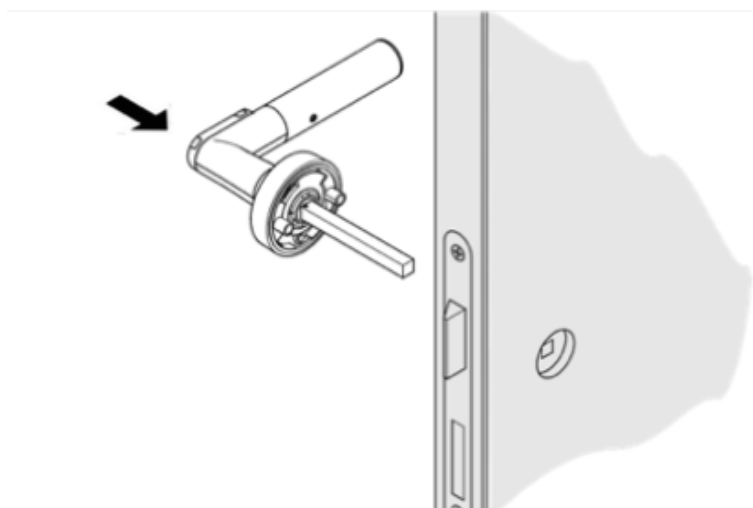
Step 1: Assembly of the square pin

Plug the square pin (3) completely over the fixing pin and into the square pin fixture of the lever (1).
Insert the spiral pin (2) into the square pin and completely press it into it using a pliers.



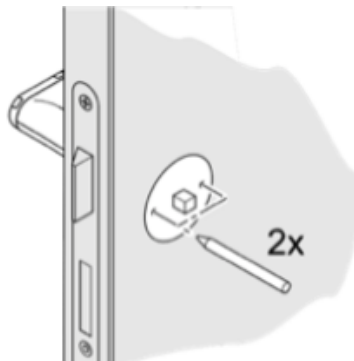
Step 2: Put on square pin

Insert the square pin of the electronic door lever into the square nut of the lock.



Step 3: Mark boreholes

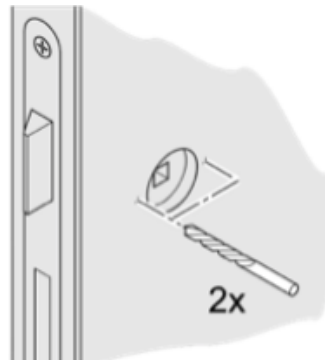
Place the drilling template on the square pin, align horizontally and center punch the hole markings.



Step 4: Drill holes

Remove the square pin again. Drill holes with a diameter of 8 - 8,5 mm at the marked positions.

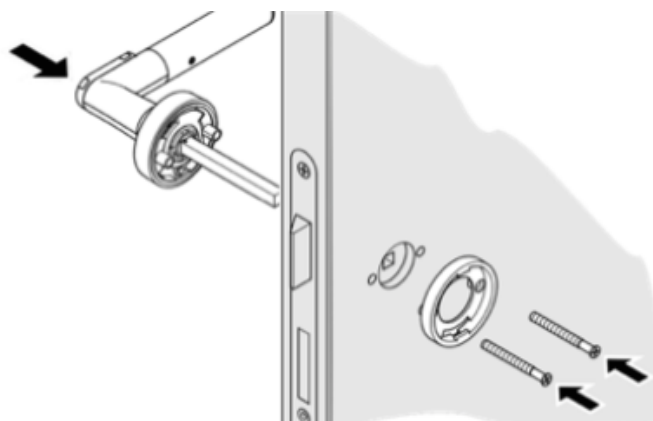
ATTENTION! Do not drill into or through the lock casing!



Step 5: Install electric door lever

Insert the square pin of the electric door lever once again into the square nut of the lock.

Insert the handle holder of the mechanical door lever from the other side and screw it along with the electronic door lever through the door panel using the supplied mounting screws.



ATTENTION!

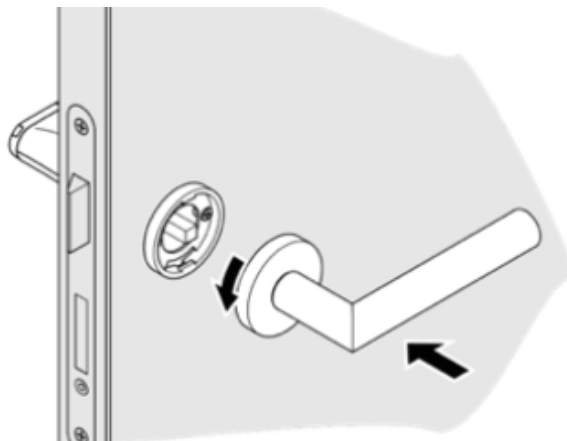
The included mounting screws are designed for doors with a larger door thickness. Before inserting the screws it is important to check whether these have to be shortened before. Otherwise the door rosettes might be damaged.

Step 6: Install mechanical lever

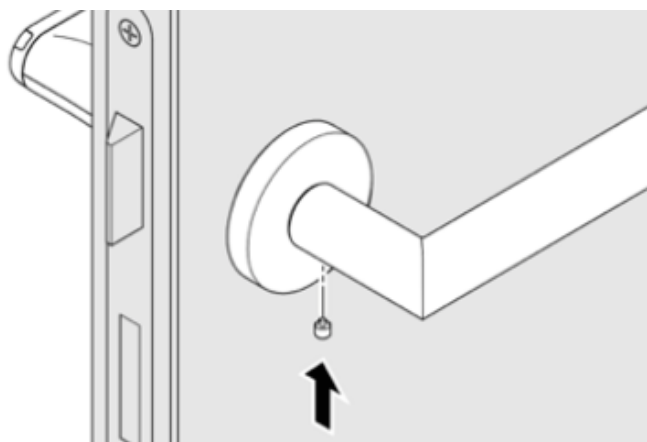
Insert the mechanical door lever keeping it in a horizontal position.

For door levers pointing to the right, tighten the rosette towards the left, guide it over the lever holder and engage the bayonet lock.

Accordingly, tighten the rosette towards the right for door levers pointing to the left.

**Step 7: Fasten mechanical lever**

Insert the locking screw from the bottom of the rosette and tighten it.

**Step 8: Check functionality**

Check the functionality and easy movement of the door lever with the door open.

To do this, hold an authorized key in front of the reading unit.

When engaged, the catch of the lock should be completely inside the lock casing when the latch is pressed down.

9.5.3. Online wall reader

The commissioning of a Kentix online wall reader consists of 2 steps:

The wiring and the installation into the flush-mounted socket at the wall.

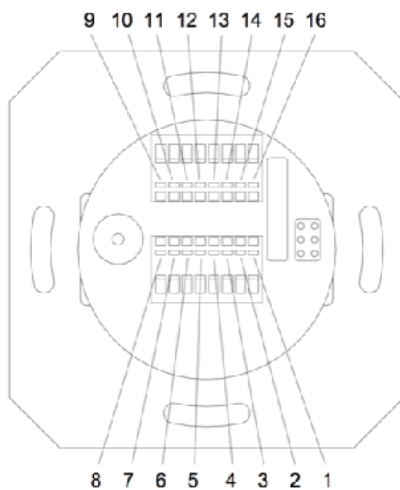
Two modes are available for the wiring and control of external components (factory doors, barriers):

1. Wiring of the relay directly at the wall reader (applications with low safety requirements)
2. Wiring of up to two relays at the AccessPoint (AccessPoint installed in the secure area, application with high security requirements)

The wiring for the desired operating mode is described in the following:

9.5.3.1. Commissioning with wiring of the relay at the wall reader

Power supply and the relay are connected directly to the wall reader. Please follow the PIN assignment as shown on the diagram below.

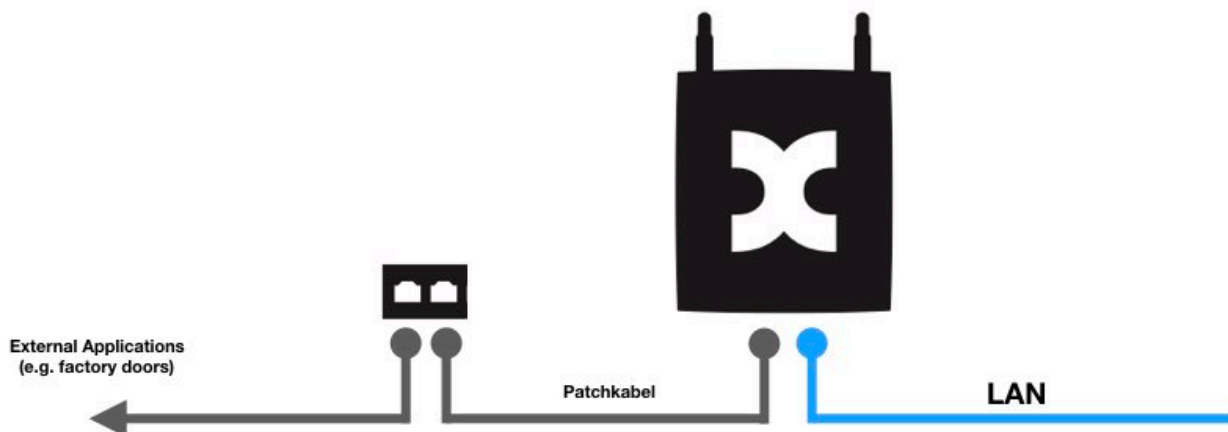


Terminal connector (back of reader unit):

- 1 - Voltage supply 8-40 VDC (polarity: any)
- 2 - Voltage supply 8-40 VDC (polarity: any)
- 9 - Switching relay max. 30 V AC/DC, max. 1,5A (polarity: any)
- 10 - Switching relay max. 30 V AC/DC, max. 1,5A (polarity: any)

9.5.3.2. Commissioning with wiring of the relays via the AccessPoint

The voltage supply is realized as described above. In addition one of the two relays at the AccessPoint is used. For the connection an external adapter (KIO3) is available. This is connected to the system jack of the AccessPoint using a patch cable.

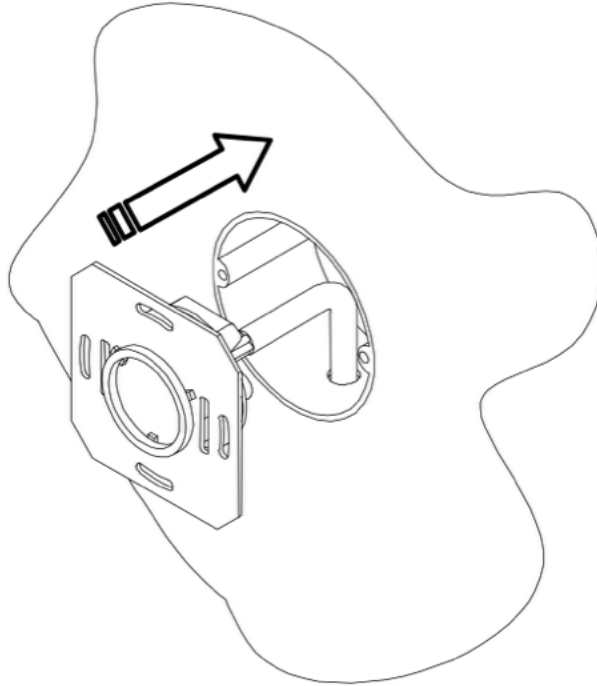


9.5.3.3. Installation of the wall reader

For the installation of a Kentix online wall reader please proceed as described in the following:

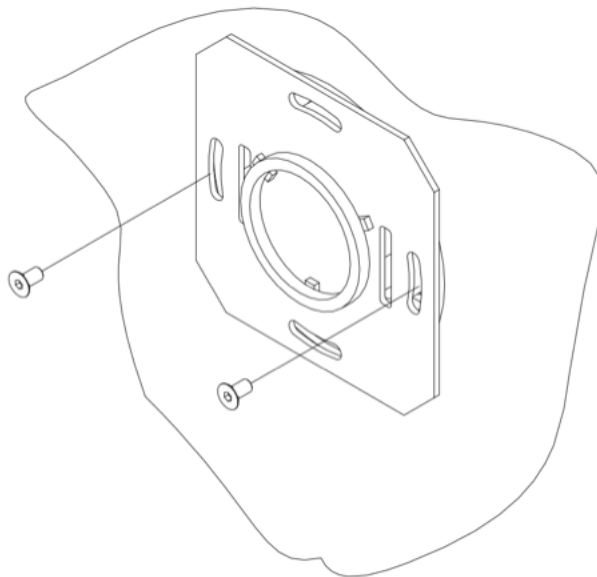
Step 1: Installation in the flush box

Connect the wall reader to the flush-mounted socket. Ensure that no cable is pinched or squeezed.



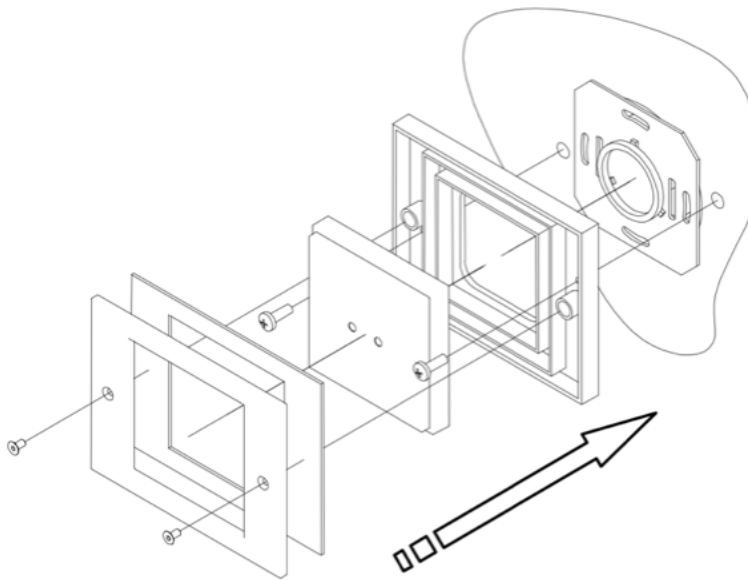
Step 2: Fasten wall reader

Align the wall reader in the flush box fasten the screws.

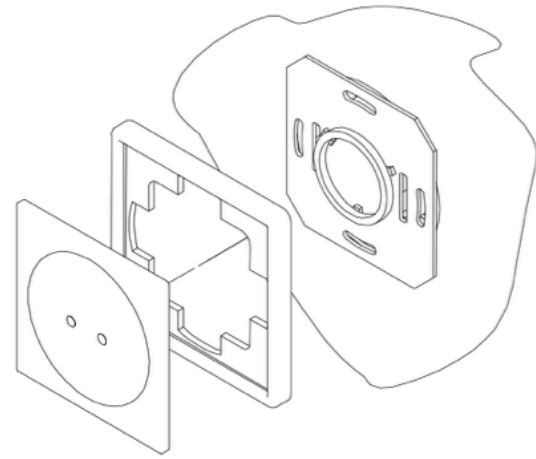


Step 3: Fasten cover

Attach the cover to the wall reader. Please note that the cover eventually must be screwed (depending on the version).



TX-44



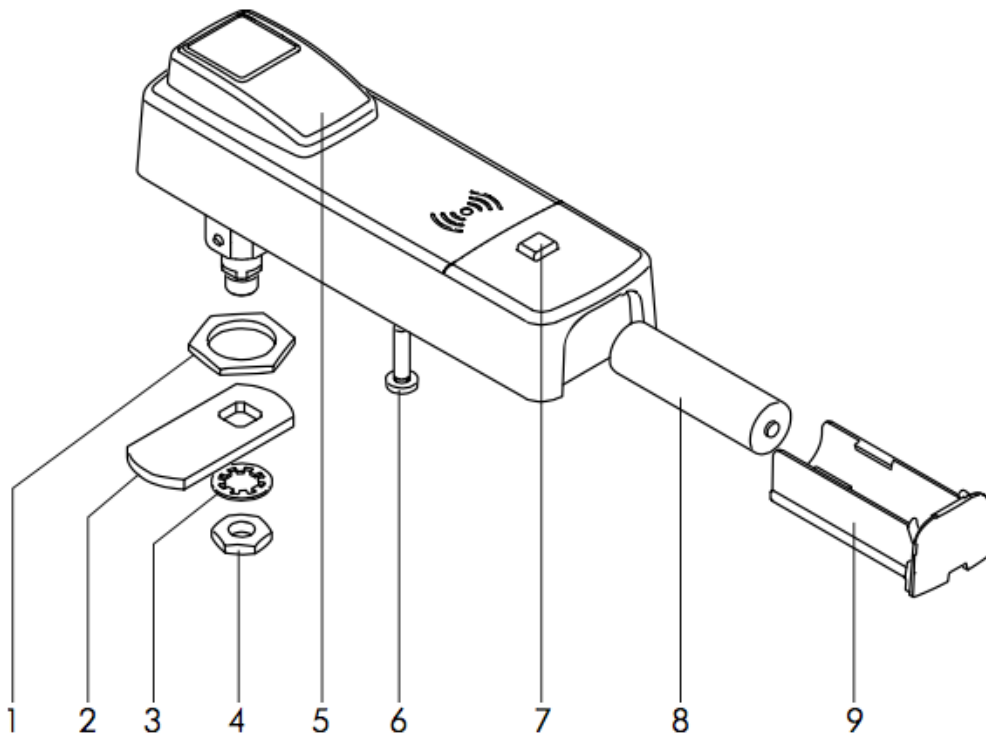
S-Color

9.5.3.4. Installation of the wall reader (surface mounted)

With the surface mounted version the wall reader is already preassembled in a 2-part surface-mounted housing. The lower housing part is mounted on the wall using the supplied screws. Then the connection cable is inserted through the cable inlet and then connected to the wall reader. The screwed connection can then be closed and the upper housing part screwed to the lower part.

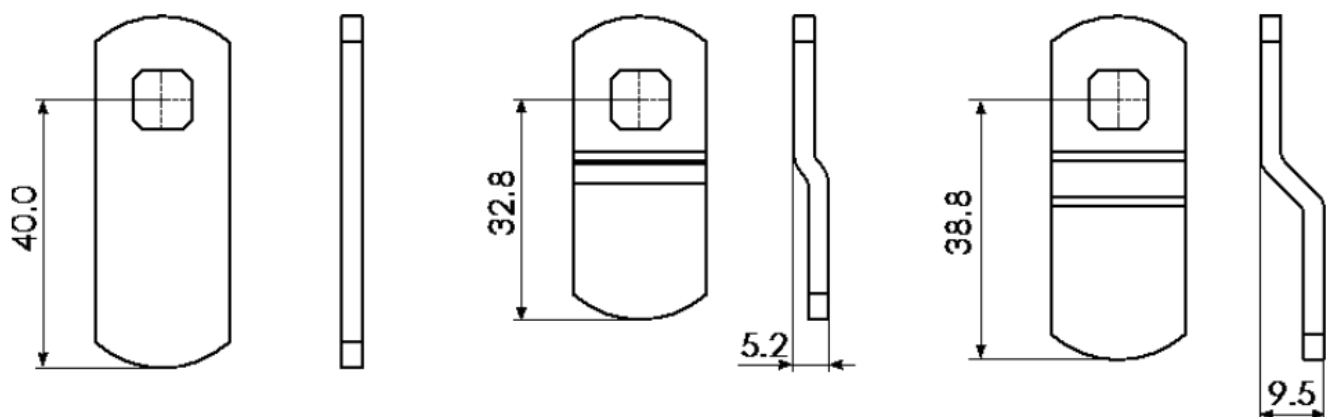
9.5.4. Online cabinet lock

The Online cabinet lock consists of the following components:



1. Locking nut for the cabinet lock on the door
2. Locking lever (various variants available, included)
3. Safety washer
4. Locking nut for the closing lever
5. Operating lever
6. Mounting screw
7. Wakeup-button
8. Battery
9. Battery compartment

To open the battery compartment a special key is required, which is available separately.
For the different types of locks 3 different locking levers are included.

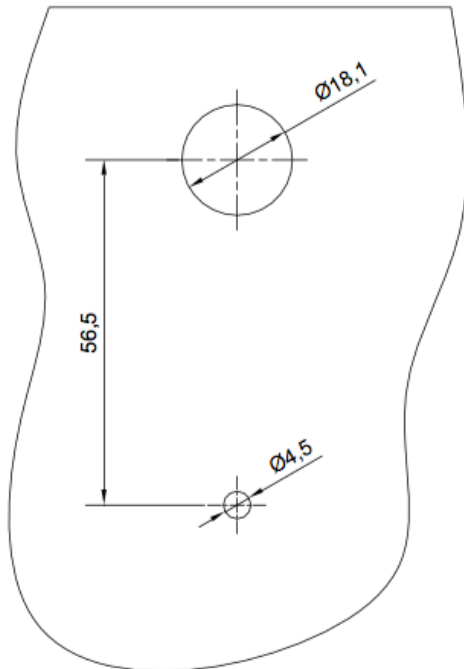


After the installation of the fitting at the door frame it has to be checked which of the variants fits the best.

For the installation of a Kentix online cabinet lock please proceed as described in the following:

Step 1: Drilling

To fix the cabinet lock holes are required in the door as shown in the following drawing.

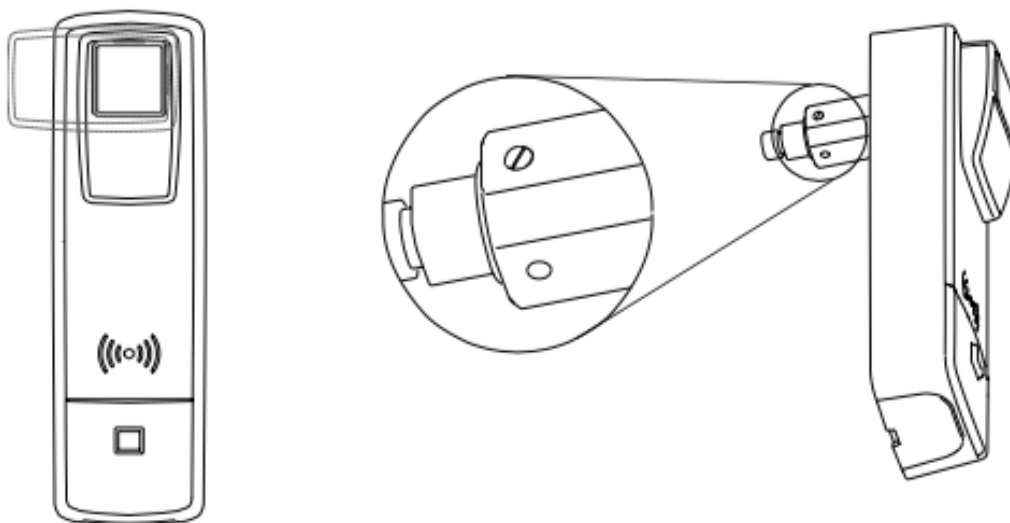


NOTE!

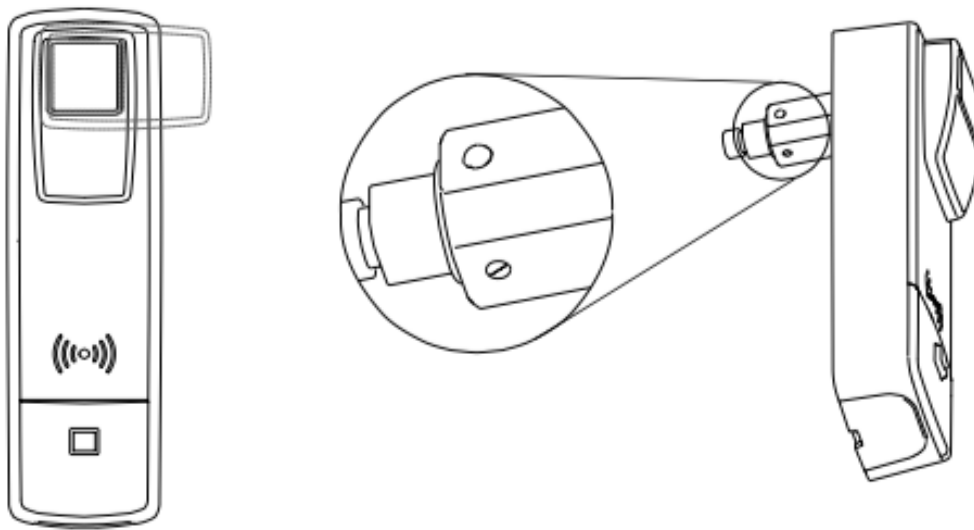
Depending on the type of cabinet, a drilling at the door is not required. For cabinets that already have an opening after the removal of the existing closing lever, matching profiles for the inside of the door are included.

Step 2: Setting of the opening direction

The levers rotation direction is determined by the position of the small screw at the mounting thread.



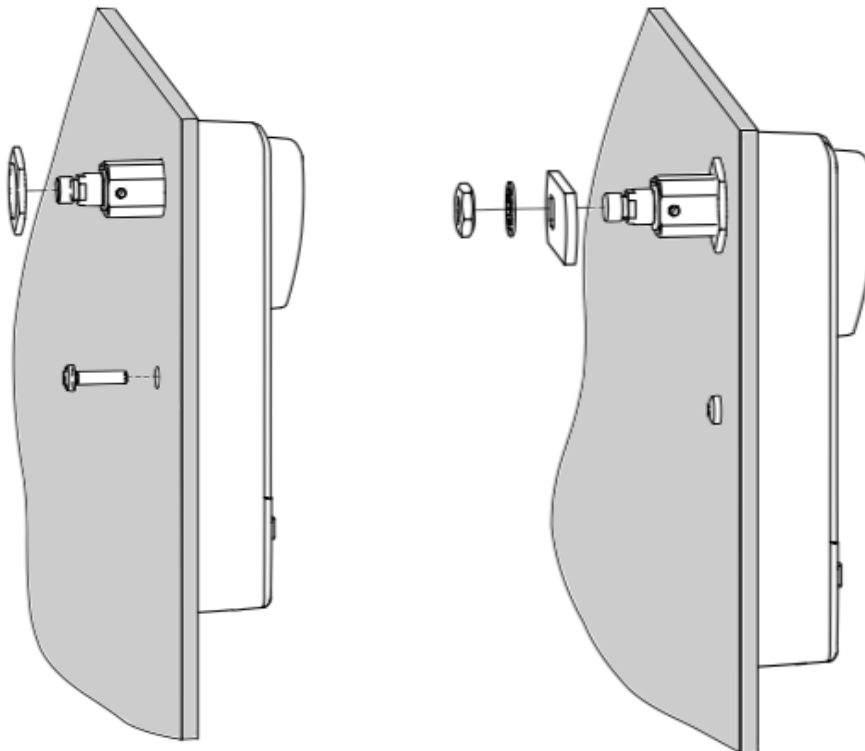
Screw at the side of the mounting thread. Opening by turning the lever to the left.



Screw at the bottom if the mounting thread. Opening by turning the lever to the right.

Step 3: Installation

Push the cabinet lock through the hole in the door and fix it with the fastening nut and fastening screw. Then install and fasten the locking lever and safety washer with the locking nut.

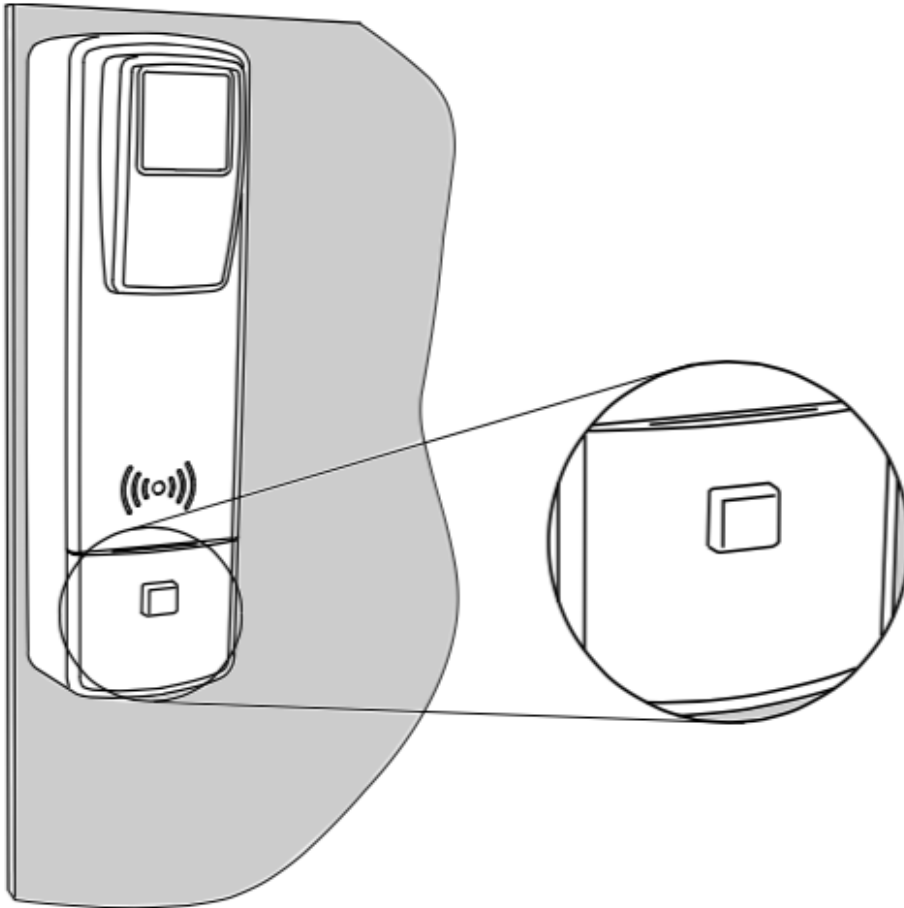


NOTE!

If necessary, place the two profiles at the inside of the door. The profiles are included in the delivery.

Wakeup of the online cabinet lock

In contrast to the other DoorLock devices, the cabinet lock must be activated by pressing the button at the lock. This is necessary for the initial setup and also the normal operation. Press the button until the LED lights up. Then hold the RFID-key in front of the reading unit.



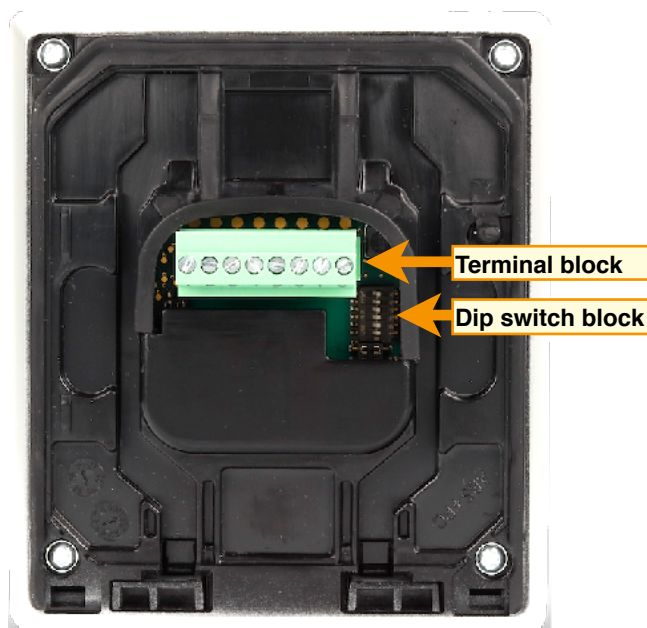
9.5.5. IP Wall Reader and network relay module

The IP Wall Reader consists of the following components:

1. IP Wall Reader
2. Surface-mounted housing (optional)
3. Network relay module

9.5.5.1. Terminal assignment / DIP switch at IP wall reader

On the back of the reader there is a terminal block for the wiring and a dip switch for setting the device address of the reader.



Terminal block	
PIN	Function
1	RS485 Data „A“
2	RS485 Data „B“
3	-
4	-
5	-
6	-
7	GND
8	8-30 V/DC

Dip switch block	
DIP switch	Function
1	Address 1
2	Address 2
3	-
4	-
5	Baud rate
6	-

On the terminal block 4 PINs are required, 2 for data communication and 2 for powering. The connection is done using the pinning in the table one the right.

On the dip switch block the first two switches are required for the addressing.

The first IP Wall Reader connected to a network relay module always has the device address 1.

So here dip switch no. 1 has to be set to ON.

Using a second reader the reader requires address 2. Dip switch no. 2 has to be set to ON here.

Dip switch no. 5 sets the baud rate / communication speed. The default position is ON.

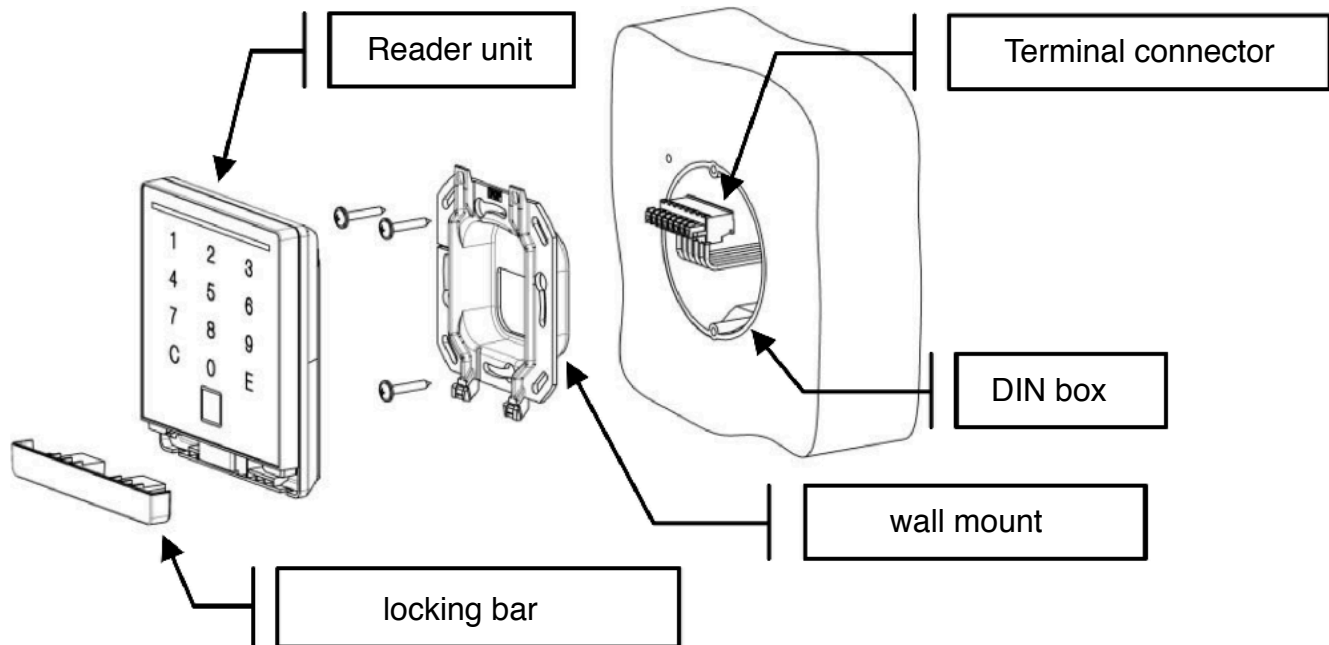
IMPORTANT!

The wiring must be done in unpowered state. The operating voltage must only be switched on after the reader has been completely installed.

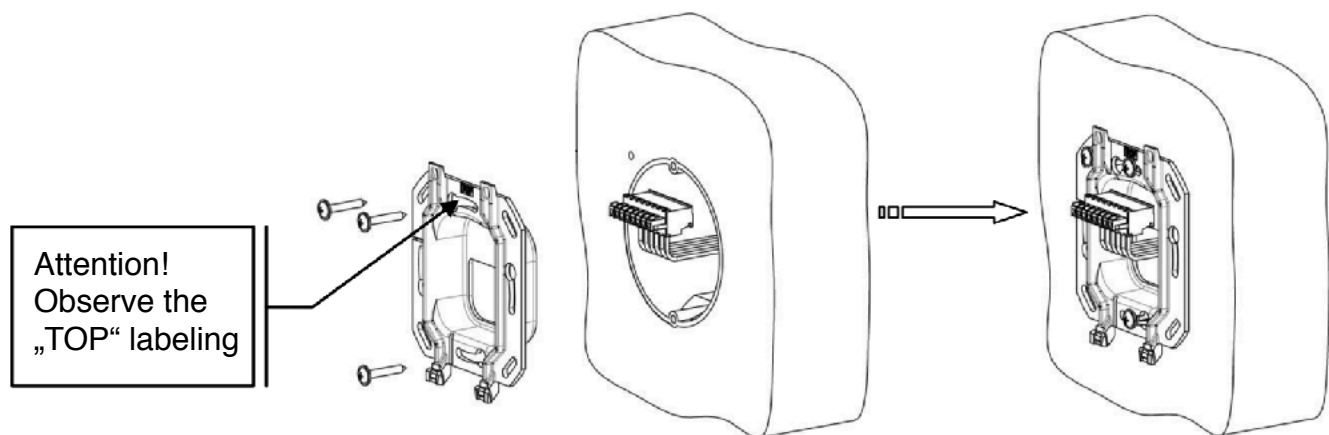
9.5.5.2. Installation of IP wall reader

For the reader unit two ways of installation are possible:

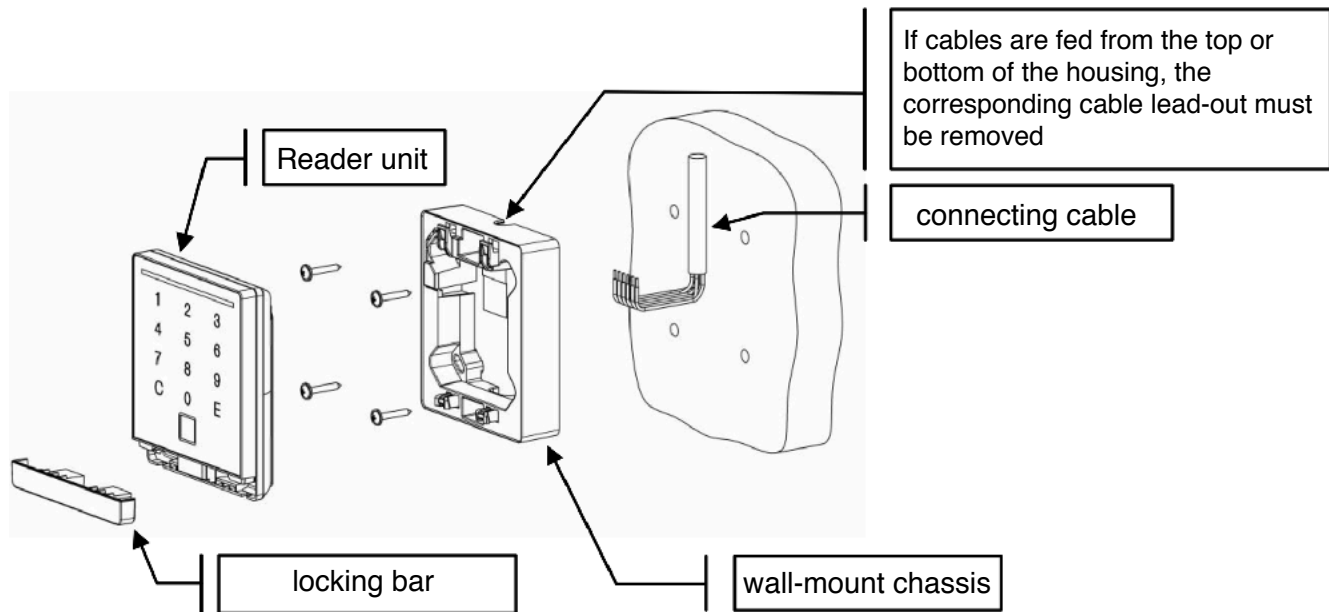
Flush-mounted installation



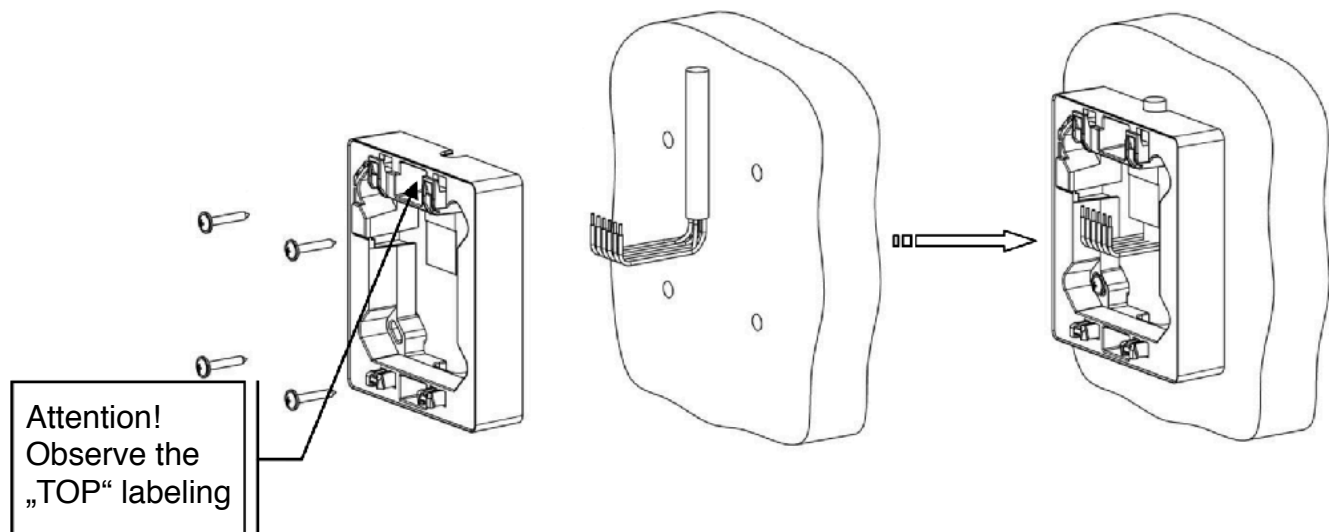
Screw the wall bracket onto a DIN device box with a screw distance of 60mm using the supplied screws.



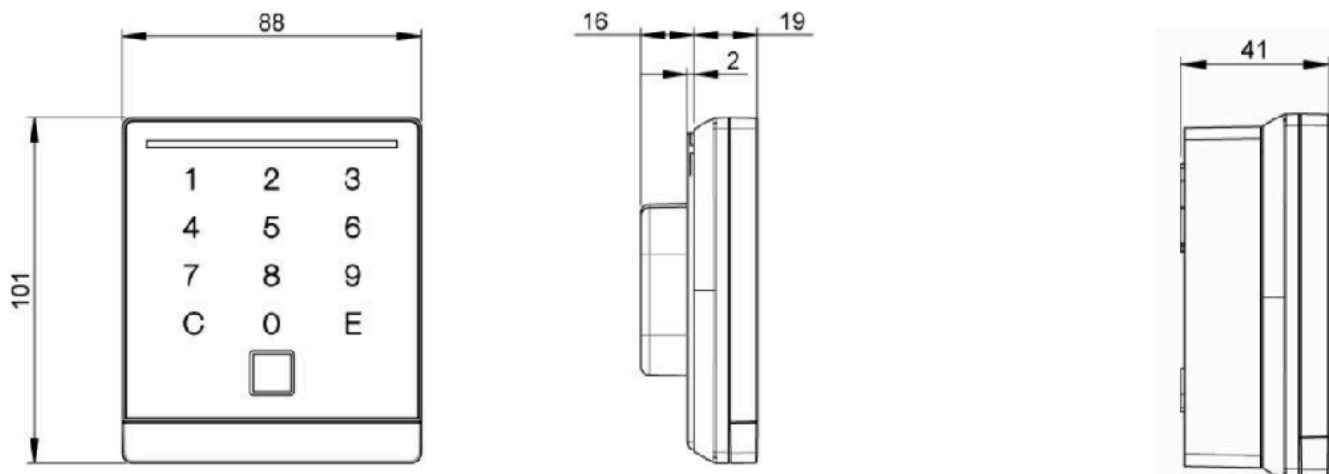
Surface-mounted installation



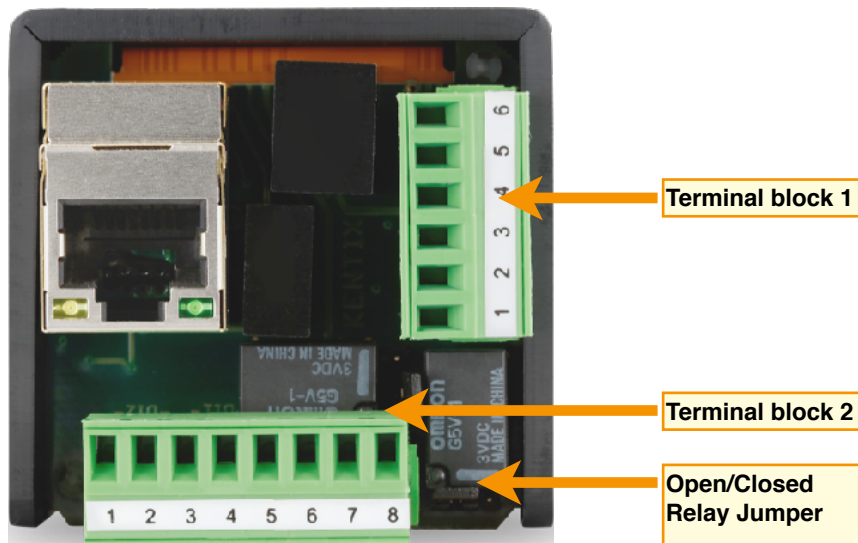
Screw the wall-mount chassis to the wall using suitable screws



Dimensions (in millimeters)



9.5.5.3. Installation of network relay module



The network relay module can be installed in two ways:

1. Installation into a DIN wall device connection box below the IP Wall Reader. This variant requires either a connection box with a higher depth, or the use of the wall-mount chassis.
2. Installation into a separate DIN wall device connection box or to a DIN rail bracket.

The module has two terminal blocks. The PINs are connected as shown in the following:

Terminal block 1	
PIN No.	Function
1	24V/DC Out
2	GND
3	24V/DC Out
4	GND
5	RS485 Data „B“
6	RS485 Data „A“

Terminal block 2	
PIN No.	Function
1	GND
2	DI-IN2
3	GND
4	DI-IN1
5	DO2-NO
6	DO2-CO
7	DO1-NO
8	DO1-CO

9.5.5.4. Switching between „normally open“ (NO) and „normally closed“ (NC) mode

The network relay module has two jumpers to define the operating mode of the internal relays. By default the relays/outputs of the module work a so-called „normally open“ mode. On an access with a valid authentication the relay closes to trigger the connected application (door) for the configured time.

This can be switched to a permanently closed state („normally closed“). On a valid access the relay/output is then opened.

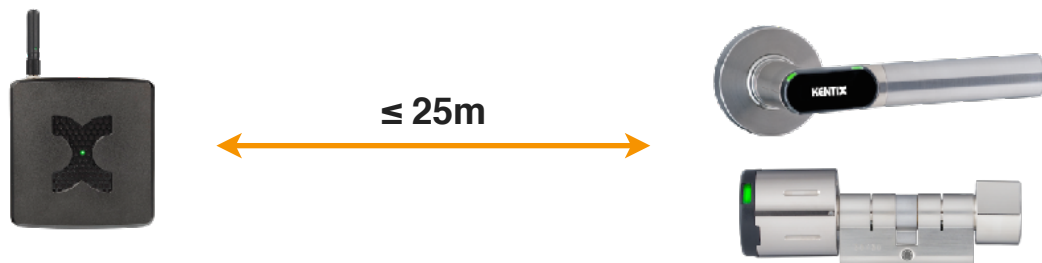
9.5.5.5. Configuration of IP Wall Reader and network relay module

The configuration of the two devices is done via the web interface of the network relay module. This configuration is based on the same structure as on the Kentix AccessPoint. To configure reader and module please follow the steps as described later in this manual.

9.5.6. AccessPoint

To mount the AccessPoint simply fix the supplied mounting bracket to wall or ceiling and attach the AccessPoint to it. Connect the AccessPoint to a PoE-enabled switch.

Please note that the maximum distance to the DoorLock-devices must not exceed 25 meters. Otherwise the radio connection is not guaranteed.



9.6. Configuration and operation modes

The access system Kentix DoorLock can be operated in an online- and offline-mode. In the offline-mode the complete programming is done at each DoorLock-device separately. Time profiles cannot be configured in this mode. The offline-mode is suitable for small installations with only a few doors and up to 10 users.

In the online-mode the programming of DoorLock-devices is done via the web-interface of the AccessPoints. Here only the master card set (Servicekey) has to be programmed directly at the device.

9.6.1. DoorLock-device without AccessPoint (offline-mode)

The programming basically consists of two steps:
the initial setup and the programming of the RFID cards for the users.

NOTE!

Each action is confirmed by visual and acoustic notifications.

9.6.1.1. Initial setup - insert / activate batteries

Online knob and door lever and cabinet lock are battery operating devices. For the commissioning the batteries must be inserted or activated first.

The **Online knob** is delivered in opened state with the a loosely mounted knob cover.

The cover can be easily pulled down from the knob. One of the two batteries is blocked by a plastic lock. This lock has to be pulled out to activate the knob. The knob then signalizes the activation by multiple short tones.

At the **Online door lever** the required battery is not installed, but delivered with the additional equipment.







To insert the battery, the allen screw on the electronic side must be **screwed into** the lever using the enclosed Allen key. The front part can then simply be removed.

Insert the battery with the negative pole first into the front part. Then put it back onto the lever and fasten it. The activation is then signalized by a short tone.

At the **Online cabinet lock** the battery is also delivered separately. It has to be inserted into the battery compartment which is then pushed into the lock from below.

For the opening a special key is required which has to be purchased separately.

9.6.1.2. Initial setup - Master card set

No	Step	Note / Signalization
1	Servicekey card (yellow) in front of knob to activate This step is only required once during initial startup.	 3x longer Ton
1	Present Servicekey card (yellow) in front of DoorLock-devices reading unit. This step has to be performed only one time at the initial setup. At a door lever, wall reader or cabinet lock the initial setup is completed with this step.	 2x short sound, 1x long sound then wait for 5 seconds
2	Present Servicekey card (yellow) again in front of knob to start programming mode.	 1x short sound, 1x long sound
3	Present Battery replacement card (green) in front of knob.	 2x short sound, LEDs light up green then wait for 5 seconds
4	Present Disassembly card (blue) in front of knob.	 2x short sound, LEDs light up green then wait for 5 seconds
5	Present Servicekey card (yellow) in front of knob to leave programming mode.	 1x short sound, 1x long sound




NOTE!

For the initial setup of door levers, wall readers or cabinet locks the teaching of battery changing and dismantling card is not required. The door lever has to be woken up by presenting any RFID card in front of the reader unit. Then the servicekey card must be held in front of it for one time. After this the process is finished. As the wall reader is permanently powered a wakeup with a RFID card is not necessary.




At a cabinet lock the wakeup button has to be pressed before holding the Servicekey card in front of the reader.

If the initial programming leads to an error, a DoorLock-device can be reset using the Servicekey card. Please read the chapter „Reset of components“ later in this manual.

The RFID-cards for the users are also added with the programming mode in the offline-mode:

No	Step	Note / Signalization
1	Present Servicekey card (yellow) in front of DoorLock-devices reader unit to start the programming mode.	 1x long sound, 1x short sound wait for 5 seconds
2	Present RFID user card in front of the reader unit.	 2x short sound, LEDs light green wait for 5 seconds, then the next card can be directly learned
3	Present Servicekey card (yellow) in front of the reader unit to leave programming mode.	 1x short sound, 1x long sound

It is also possible to remove single RFID user-cards by presenting them again during programming mode:

No	Step	Note / Signalization
1	Present Servicekey card (yellow) in front of DoorLock-devices reader unit to start the programming mode.	 1x long sound, 1x short sound wait for 5 seconds
2	Present RFID user card in front of the reader unit.	 2x long sound, LEDs light red wait for 5 seconds, then the next card can be directly learned
3	Present Servicekey card (yellow) in front of the reader unit to leave programming mode.	 1x short sound, 1x long sound

NOTE!

In offline mode a DoorLock-device must be reset to delete lost RFID user cards.
For a description please read the chapter „Reset components“ later in this manual.

9.6.2. DoorLock-devices with AccessPoint (online-mode)

For the initial setup please proceed as described in the chapter „DoorLock-devices without AccessPoint“. The following configuration is then done via an AccessPoint.

For the configuration a web-server is integrated in the AccessPoint, to configure and control the device via the network using a web-browser.

Connection to PC: Connect the LAN interface of the AccessPoints to a PoE-enabled switch using a standard patch cable. Establish a network connection between this switch and your PC. Configure the IP-address of your PC to e.g. „192.168.100.123“.

9.6.2.1. Default settings / factory defaults

Power supply: PoE (Power over Ethernet).
 Default IP-address: 192.168.100.224
 Subnet-mask: 255.255.255.0
 Username / Password: admin / password

IMPORTANT! - Reset to factory defaults

In case of loss of the IP or login data of your AccessPoint it is possible to reset the device to factory defaults. For this there is a RESET button located at the antenna side. The device is then completely reset and performs a restart. After approx. 30 seconds it can be accessed again using the default settings.

For safety reasons the reset of the AccessPoint is only possible after the device has been restarted for the duration of 1 minute. The AccessPoint can be restarted by unplugging the network cable for a few seconds. After the reset please wait for about 30 seconds until the device is in its normal operation mode (signalized by the internal green LED). Now press the RESET button.
 Press and hold the button for 15 seconds until the reset process is confirmed by a long tone.

9.6.2.2. Communication ports

The configuration of the AccessPoints and communication with each other is done via the default HTTP(S)-Ports. For the Kentix360 cloud service an additional port is required.

The following ports are used/required:

Nr	Beschreibung	Port-Nummer
1	Configuration of AccessPoint and firmware update via web-browser	TCP 443 (HTTPS), 80 (HTTP - redirected to 443) from PC to AccessPoint
2	Communication / configuration of multiple AccessPoints with each other („Master/Slave“-mode)	TCP 443 (HTTPS) from „Master“ to „Slave(s)“ both directions required
3	Communication between AccessPoint (Master only) and Kentix360 cloud service	TCP 5222 from „Master“ to „mykentix.com“

9.6.2.3. Dashboard - Access logbook

Zutrittsbuchungen

#	Datum und Uhrzeit	DoorLock	Benutzer	Buchungsstatus	Detail
1	2018-01-29 10:22:57	Serverraum		X	RFID eingelernt: 9'0015c1
2	2018-01-29 10:19:52	Serverraum	Administrator	Key	Fernschaltung
3	2018-01-29 10:14:50	Serverraum		X	Keine Türberechtigung
4	2018-01-29 10:14:19	Serverraum		X	Buchung außerhalb des Zeitprofils
5	2018-01-29 10:09:47	Serverraum		Key	
6	2018-01-29 10:06:45	Serverraum		Key	
7	2018-01-29 09:48:58	Serverraum		Key	
8	2018-01-29 09:29:52	Serverraum		Key	

Overview of all bookings done (door openings)

The access logbook shows the bookings of all DoorLock-devices connected to the system with date, time and the respective user.

Via the magnifying glass icon in the upper right different filter functions can be applied to the logbook.

9.6.2.4. Dashboard - DoorLock control

DoorLocks

#	Aktiv	Türstatus	Name	Gerätetyp	Batterie	Eingelernt an
1	✓	Offen	Office	DoorLock-LE	✓	Kentix AccessPoint
2	✓	Offen	Schrankschloss	DoorLock-RL	✓	Kentix AccessPoint
3	✓	Offen	Serverraum	DoorLock-DC	✓	Kentix AccessPoint

Overview of all available doors for remote opening

Navigate to the tab „DoorLock control“ to control single DoorLock-devices remotely.

NOTE!

To use the remote opening the DoorLock-device must be put into an active state by the person on the spot. At a knob it is sufficient to move it as soon as the button for remote opening has been pressed in the AccessPoint.

At a door lever any Mifare RFID card has to be held in front of the reading unit. This may also be an identity card or credit card.

The cabinet lock has to be woken up by pressing the button at the lock.

At a wall reader not interaction of the person at the door/reader is required.

9.6.2.5. Access - Users

Here the users are created and managed. Up to 5,000 users can be configured per system.

Username

Assign a unique name for the user. It is required for the login to the AccessPoint and may be used only once in the complete system.

Name

In addition to the username the full name of the users should be entered here. This is only for informational purposes and has no functionality for the operation with the system.

User password

All users that shall have access to the AccessPoints web-interface additionally require a user password for the login.

E-mail address

When an e-mail address is entered, the user will be informed about critical system states, e.g. exhausted batteries in an online-cylinder.

RFID-Token

For each user one RFID-token number / RFID-card number can be assigned. This number can be entered either manually or directly at an online-cylinder or door lever.

Description

Enter a description for the user, if necessary.

Permissions - Userlevel

There are 3 user permission levels available:

Userlevel	Description
Remote Access Only	Access to bookings of assigned doors in the logbook. Remote controlling of the assigned doors.
Access Administrator	Restricted administrative access. The Access Administrator has the permissions to manage users and doors in the access section. Additionally permissions to edit the time and access profiles are given.
Super-Administrator	Unrestricted access to the system. The Super-Administrator also has permissions to change the basic configuration (e.g. IP data) in the AccessPoint.

The user level has no effect on the access permissions at the doors.

Permissions - Emergency access

When the option „Emergency access“ is activated, the card data of the user are transferred into the DoorLock-devices. The user then has the permission to open these doors even if the connection to the AccessPoint is interrupted.

To trigger the transfer of users card data to the respective device, at least one booking of the user at each of the doors is required.

Permissions - Receive notifications

The user will be informed by e-mail about critical system conditions - for example batteries in a knob that require a replacement. It is important that a valid e-mail address has been entered in the user data.

Access profiles

Sets the access authorization for the user. The times for the access authorization are defined in the respective access profile.

9.6.2.6. Teach-in of RFID-media in the online-mode

In the online-mode the user cards are added to the AccessPoint by reading them directly at a DoorLock-device. To read a RFID-card for the actual selected user, select „+“ and choose the door at which the card shall be read. Click on the arrow next to the door selection.

Now present the card in front of the device. After being read it will appear in the user data.

9.6.2.7. Access - Access profiles

An access profile always consists of a time profile and one or several doors. In combination with the user management the permissions for each door can be assigned here.

The tab „Access profiles“ shows an overview of all configured profiles. With „+“ new profiles can be created. Existing profiles can be edited by clicking on the pencil.

Each access profile always consists of a name and a time profile.
Assign a unique name for each profile and select a previously configured time profile.
Then assign the desired doors to the profile.

The settings can be saved by clicking the corresponding button on the right.

9.6.2.8. Access - Time profiles

The time profiles define the weekdays and times, to which users are allowed to get access to the doors assigned in the access profiles.

The tab „Access profiles“ shows an overview of all configured profiles. With „+“ new profiles can be created. Existing profiles can be edited by clicking on the pencil.

Each time profile always consists of a name and a week plan.
Enter a unique name for each profile and mark the times to which the user shall have permission to access the assigned doors.
The week plan can be edited in 15 minute steps. Single fields can be selected by clicking, a range of fields can be marked by clicking and dragging.

9.6.2.9. Access - DoorLocks

In the tab „DoorLocks“ the DoorLock-devices connected to the AccessPoint are managed.
The overview shows the devices that have already been added. New online-components can be added by clicking „+“.
Via the info-button („i“) additional information about the selected device can be received.

NOTE!

Please note, that the new device has to be in range of the corresponding AccessPoint (25m max.).

Present the Servicekey-card in front of your new DoorLock-device. By clicking „+“ the search for available devices is started. On a „Master-Slave“ system additionally the corresponding AccessPoint has to be selected.

After about 10-20 seconds the DoorLock-device will respond by ending the programming mode.
The configuration interface of the device will be shown.
If this is not the case, please wait until the AccessPoint stops the search-mode (60 seconds) and repeat the process.
When the device is found it can directly be configured. This can also be done later by clicking on the pencil next to the corresponding device.

The single settings of a DoorLock's configuration interface are described here:

Default teach-in DoorLock

When learning new RFID-Tokens for the users this device is always displayed at first in the selection.

Double authentication (IP Wall Reader only)

At an IP Wall Reader doors can be opened using a PIN code or RFID media.

Activating the option double authentication, both types of authentication will be required for a successful opening.

Name

Enter a name for the DoorLock-device. Typically this corresponds to the installation place.

Couple Time

Select the desired time (3 / 6 / 12 seconds), for which a device shall stay engaged after a valid booking.

Booking switches Alarmzone

If desired, an arm-/disarm-switching of a Kentix alarm system can be triggered by a booking.

The AlarmManager communication has to be activated for this in the „Configuration“ section.

Choose the desired Alarmzone here. If no Alarmzone is displayed, press the refresh-button to update the zone selection. The usage of the function is described on the next page.

Time control Active

A Kentix DoorLock component can be configured to stay permanently engaged. The door can then be opened without a booking at the RFID reader.

For this operating mode a time profile can be chosen here which determines the times to which the door can be opened without additional authorization. The time control mode is activated automatically without any authorization.

Time control requires booking

When this option has been activated the time control function always has to be activated by a valid booking.

Otherwise an opening of the door is not possible.

Switch output on booking

The Kentix AccessPoint has 2 relay outputs. These can be switched/activated by a booking (e.g. in combination with a wall reader), to control external components (motor locks, barriers).

You can choose between two switching outputs at the AccessPoint.

Assigned Network Camera

Configured network cameras can be assigned to a door. Each time a RFID card is read at this door, an SD card recording of several images is triggered and linked to the logbook entry.

The settings for network cameras can be found in „Configuration“ -> „Network cameras“.

Access profiles

In the settings of a DoorLock-device a direct assignment to one or multiple access profiles can be made, if profiles have already been configured.

9.6.2.10. Access - General

Logbook data - Remove user related data after

Defines for how long user accesses / bookings will be stored in the AccessPoints database. Several periods are available here. „Store all“ will provide space for up to 200.000 bookings.

Security - PIN Length

Defines the number of digits when using IP wall readers with PIN.

Security - Mifare Desfire

Kentix DoorLock can request application data from the users RFID media. By default this feature is inactive, so that only the cards ID is requested and compared.

NOTE!

This option will only work together with RFID tokens prepared by Kentix. The application data already has to be present on the card and cannot be written during operation.

9.6.2.11. Access - DoorLocks - Switching alarm zones

The following requirements must be fulfilled for switching an alarm zone on the AlarmManager:

1. The same communication key must be entered in AccessPoint and AlarmManager.
2. In the AccessPoint (section „Configuration“ -> „Communication“) the AlarmManager must be entered with IP-address and a valid user.
3. An alarm zone must be selected for the Online knob / door lever or wall reader in the section „Access“ -> „DoorLocks“.
4. The option „Time control“ for the permanently engaged mode must not be active.

For booking and simultaneous switching please proceed as follows:

- | | |
|----------|---|
| DISARMED | - One-off booking disarms the assigned alarm zone |
| ARMED | - Booking twice at a maximum of 15 seconds will activate the alarm zone. For the second booking, the RFID card must also be held in front of the knob until the arming is signaled visually and acoustically at the knob. |

9.6.2.12. Configuration - General

These are the basic settings of the AccessPoint.

Name

Enter a unique name for each AccessPoint. As a recommendation the place of installation can be used here.

Language

Select the language for the web-interface of the AccessPoint. German and english language are available.

Security - Communication Key

The communication key is the password for the encryption of the communication between Kentix-devices. It is required for the „Master-Slave-mode“ between multiple AccessPoints and also for the connection of an AlarmManager.

The key must be identical on all devices and should comply with certain guidelines (length, upper / lower case, numbers, special characters).

NTP 1 / NTP 2

In the fields „NTP 1“ and „NTP 2“ the time servers for the time synchronization are defined. This can be servers in the own network or public time servers (default settings).

The time is required for time profiles and the correct reporting of bookings and events in the logbooks.

Public NTP Servers: 0.de.pool.ntp.org or 1.de.pool.ntp.org

Timezone

Select the time zone in which the AccessPoint is located. This will ensure that the time profiles match the booking times.

Current system time

Saves the current time of the PC in the AccessPoint. This function can be used if no time server is available. In the display the time of the switching to the „General“ settings is shown.

9.6.2.13. Configuration - Network

This are the network settings of the AccessPoint. The device is delivered with a default configuration.

Default IP-address: 192.168.100.224
Subnet-mask: 255.255.255.0
Username / password: admin / password

This data can be altered for an operation in the own environment after commissioning.

IPv4-address, subnet mask, gateway

Network configuration of the AccessPoints. DHCP can be optionally activated. In this case always the same IP-address has to be assigned to the AccessPoint. For this the MAC-address is displayed here. Alternatively manual network settings can be entered.

The changes in the network settings are directly active after saving.

DNS server address 1 / 2 (Domain Name Server Addresses)

Depending on the network configuration (e.g. in combination with a DSL router) this can also be the gateway address.

Public DNS Servers: 8.8.8.8 or 8.8.8.4

9.6.2.14. Configuration - Communication

E-Mail Data

To send e-mails to the configured users (e.g. to warn about a low battery level), an e-mail server (SMTP or ESMTP) has to be configured in the AccessPoint.

When a valid DNS server is configured, the DNS name of the E-Mail server can be used. With ESMTP it is also possible to work with public e-mail servers which require a user authentication. Also the selection of an encryption method (STARTTLS / SSL) is possible. The communication port can be changed, if necessary. Please note, that often e-mail servers also require a valid sender address to forward e-mails.

E-Mail signature

Enter a signature, which will be appended to each e-mail. The signature is limited to a length of 1000 signs.

SNMP Settings

The AccessPoint supports SNMP V2 to call up the access log.

For this a MIB (Management Information Base) is available.

Alarms can also be sent in the form of SNMP traps to up to 2 hosts. To do this, enter the destination IP addresses for the hosts and the corresponding communication port (default: 162).

For call ups, a name must additionally be entered in the field "Public Community".

AlarmManager-Communication

Here the AlarmManager-Communication for a remote arm-/disarm-switching of a Kentix alarm system is configured.

Enter the IP-address of your AlarmManager and an AlarmManager-user and password.

This user must exist in the configuration of the AlarmManagers and have the authorization „Administrator“.

In the AlarmManager also the communication key of the AccessPoint must be configured.

9.6.2.15. Configuration - Master/Slave Mode

Multiple AccessPoints can be connected together to one system for the exchange of configuration data (users, doors, permissions). This compound operation mode is also called „Master/Slave“ mode. Here one of the AccessPoints is configured as „Master“, all other AccessPoints as „Slaves“.

The „Slaves“ receive the configuration data from the „Master“ AccessPoint. With this operating mode changes of the configuration have to be made only on one device.

Master/Slave Mode

Determines whether the AccessPoint works as „Master“ or „Slave“. When set to „Slave“, the IP address of the „Master“ AccessPoint has to be entered.

The address is required for the synchronization. Configuration data is also only accepted from this IP address.

When operating as „Master“, all slaves in the system have to be configured/listed in the „Master“ AccessPoint. All „Slaves“ are listed with name and IP address.

By pressing „+“ additional slaves can be added, existing profiles can be edited with the pen.

In the profiles a unique name (place of installation) and the IP address for the slaves has to be entered.

NOTE!

Prerequisite for the "master / slave" operation is the availability of all access points via an existing network. If necessary, contact the responsible administrator to discuss the requirements for the operation of the access system.

Please also refer to the point "Communication Ports" earlier in this manual.

9.6.2.16. Configuration - Network cameras

One network camera can be assigned to each Kentix-DoorLock component, to request multiple pictures from the camera and link these to the corresponding logbook entry. For this purpose any network camera can be used which is able to deliver pictures via a HTTP command.

Enter a name for the camera (for example the installation place) as well as the camera-specific data (IP address, user data) and select the camera location.

The field „HTTP Command“ contains an example for an AXIS camera. Enter the path to the image source file here without specifying the IP address or communication port beginning with a slash.

Camera location	Description
Inside	The camera is installed in the room, which is entered after the door is opened. The recording begins at the moment of the booking. 10 pictures are saved.
Outside	The camera is installed in front of the room. 3 pictures are pre-buffered and 7 additional pictures are stored beginning from the moment of the booking.

NOTE!

The image data are stored on the respective local AccessPoint. In Master-Slave-operation with several AccessPoints, SD cards must also be used in the slaves depending on the configuration.

The HTTP command for the request of images can be found in the documentation of your network camera.

Note that the image size of 200 kilobytes per image must not be exceeded. This may have to be taken into account when entering the HTTP command.

9.6.2.17. Configuration - LDAP Configuration

The Kentix AccessPoint has the possibility to synchronize user data with LDAP servers. This allows to avoid duplicate data maintenance by having to edit user data on two systems separately.

LDAP Server Settings

Specify IP-address, network port and Base DN for the connection to the LDAP server here.

Authentication

Specify distinguished name (Bind DN) and password of a LDAP administrator. The administrator must have full access to all organization units (OU) that shall be read out for import.

System Permissions

Here 3 organization units (OU) can be defined for the available user levels of the AccessPoint. Specify a path for each of the levels „Access Only“, „Access Administrator“ and Super-Administrator.
The required paths are individual depending on the LDAP servers structure.

Attributes

Here the LDAP attributes for the user import have to be entered. The most important value here is the Username which has to match with the username on the LDAP server.
If available, also access profiles can be transferred. With this a separate assignment of access profiles would not be necessary.

Synchronization interval

Define an interval for the synchronization with the LDAP server. The minimum/default values is „1 hour“.
The synchronization of the user data can also be triggered manually here.

9.6.2.18. Kentix360

Like the Kentix AlarmManager also the AccessPoint can be connected to the Kentix360 cloud service. If you already have a Kentix360 account, you can simply add the AccessPoint to this account. Only the Master-AccessPoint has to be configured for the cloud operation.

Otherwise a new account can be created using the „Register now“ button.

After the registration the account data can still be changed later.
Devices registered for the cloud service can be administrated here.

For information on features and pricing of the Kentix360 cloud service please visit www.kentix.com

9.6.2.19. System - Logbook

This is the system log of the AccessPoint. All events except the bookings at doors are listed here. The logbook contains e.g. warnings about critical system states (low battery charge level).

9.6.2.20. System - System settings

Create / Restore Backup

Here a complete backup of the configuration can be created and also restored. It is recommended to create a complete backup after the final setup of all doors, profiles and users.

NOTE!

The backup always consists of the complete configuration including all DoorLock-devices in the system. As long as none of the components in the system has been replaced or reset to factory defaults, the complete system can be recovered using the backup.

Firmware update

New firmware updates for the AccessPoint can be uploaded here, if necessary.
Select the firmware-image file via the file-dialog and press „Start update“.

ATTENTION!

Please also note the information in the release notes attached to each firmware image.

9.6.2.21. System - SD card

This is the administration for an SD card inserted in the AccessPoint.
An SD card is required to store images from network cameras.

A newly inserted card can also be formatted directly for a usage in the AccessPoint.
Any SD card with form factor "microSD" can be used in the AccessPoint. The capacity should be at least 8 gigabytes minimum and 128 gigabyte maximum.

NOTE!

In a system with multiple AccessPoints a SD-card has to be inserted in any AccessPoints, at which cameras are assign to doors of these AccessPoints.

9.6.2.22. System - Import/Export

Here the user profiles can be exported or imported as CSV file. If user data can be provided by another system, it can easily be imported here, which can be interesting especially on new systems with many users.

The export function will provide something like a template having at least the admin user in the file.

9.6.2.23. System - Help

Contains information for the support and version information of the AccessPoint.

9.6.3. Master-Slave-mode (Compound operation with multiple AccessPoints)

Multiple AccessPoints can be connected together to one system.

For the one of the AccessPoints is configured as „Master“ via the web interface, all other AccessPoints as „Slaves“. The advantage is, that configuration changes only have to be done on the „Master“ AccessPoint. The master distributes the configuration to all slaves in the system.

The description for the setup of the Master-Slave-mode can be found under „DoorLock-devices with AccessPoint“ earlier in this manual.

9.6.4. Reset of components




In case of misconfiguration DoorLock-devices and AccessPoints can be reset to factory defaults.

DoorLock-devices

The reset deletes all configured RFID-cards except the Servicekey-card.

A deletion of the Servicekey-card is not possible.

For the reset please proceed as described here:

Nr	Step	Note / Signalization
1	<p>Present Servicekey-card (yellow) in front of the DoorLock-device to start the programming mode.</p> <p>Leave the Servicekey-card in front of the RFID-reader until it quits the programming mode (after approx. 15 seconds).</p>	 <p>1x long sound, 1x short sound</p> <p>Wait for 5 seconds</p>
2	<p>Present Servicekey-card in front of the device again to start the programming mode a second time.</p> <p>Leave the card in front of the RFID-reader.</p>	 <p>1x long sound, 1x short sound</p>
3	<p>The deletion process is signalized by multiple short sounds. During the complete process the card has to be held in front of the reader unit. Otherwise the process will stop and has to be repeated.</p>	 <p>Multiple short sounds signalize the running deletion process.</p>

After the reset the DoorLock-device can be configured again.

At the online-cylinder at first the battery changing and dismantling card have to be read (follow the steps for the initial setup in: „DoorLock-devices without AccessPoint“) .

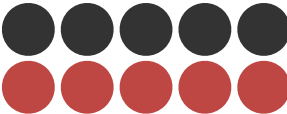


AccessPoint

For a factory reset the AccessPoint is equipped with a reset-button. To perform the factory reset, please proceed as described in the chapter „Default settings / factory defaults“ earlier in this manual.

9.6.5. Battery replacement

In the online-mode the AccessPoint receives the battery charge level of every connected DoorLock-device. On a low charge level an e-mail is sent to all users that have the notification option activated. The device can then still be used, but the batteries should be replaced soon. About 1000 bookings can then be made. The DoorLock-device (online- and offline-mode) optically and acoustically signalizes that a replacement of the batteries is necessary during the last 1000 bookings.

The signalization has 3 stages:

Nr	Stage	Note / Signalization
1	Battery warning phase 1: The online-cylinder / door lever can still be used, batteries should be replaced soon.	 5x short sound, LEDs flash red simultaneously
2	Battery warning phase 2: The online-cylinder / door lever can still be used, the engaging is delayed. Batteries must be replaced.	 5x short sound, LEDs flash red simultaneously 5s delay of the engagement, LEDs flash green
3	Battery warning phase 3: Opening of the door is no longer possible. The batteries must be replaced. The knob unlocks the locking pins for the battery change. The cover of the knob can be taken off with the battery replacement tool.	 5x short sound, LEDs flash red simultaneously no engagement / opening of the door

When reaching a low battery charging level the batteries should be replaced as soon as possible. For the replacement of the batteries the cover of the knob has to be removed. If the batteries are fully discharged, the opening of a knob is only possible using a low-power-adaptor (see also the chapter „emergency opening“).

To remove the cover, hold the battery changing card in front of the knob. The knob then releases the locking pins. Now the cover can be taken off by pressing the two pins with the battery replacement tool and pulling the cover back.

The batteries can then be taken out. After the exchange the cover has to be put over the knob again. The locking pins can be pushed down easily with thumb and forefinger.

To complete the process, the battery changing card has to be held in front of the knob once again.

To replace the batteries at a door lever, the Allen screw has to be opened on the electronic side of the lever. The front part of the lever can then be pulled off. The battery is located inside the lever and can now be simply taken out.

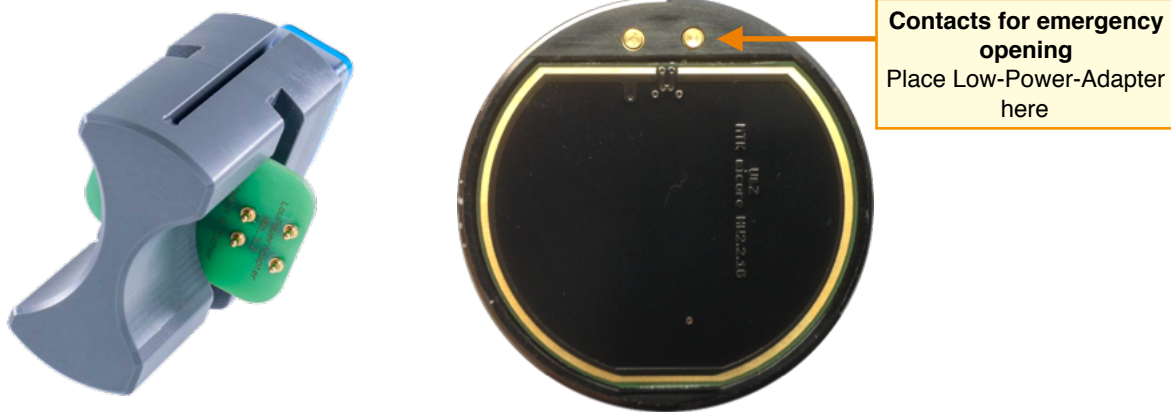
ATTENTION!

The Allen screw has to be screwed clockwise into the lever to open it.

For the battery replacement at a cabinet lock the battery compartment has to be pulled out after inserting the battery changing tool. The battery can then be exchanged and then inserted again together with the compartment.

9.6.6. Emergency opening

If the batteries have not been replaced during the three warning stages, an emergency opening with the help of the low-power-adaptor is required at an online knob.



Low-Power-Adapter

Online knob without cover

For this purpose the front cover (Kentix logo) at the knob is removed using the supplied suction cup. Now the low-power-adaptor can be put onto the contacts at the knob. Single bookings can then be made.

Perform a booking with the battery changing card and replace the batteries as described above.

9.6.7. Dismantling

Using the dismantling card, the knob can be pulled off from the profile cylinder. There are no extra tools required.

To remove the knob, hold the dismantling card in front of it. The knob goes into the dismantling position. By simultaneous turning and slight pulling the knob can be pulled off the cylinder.

To quit the dismantling position, the dismantling card has to be held in front of the knob once again.

NOTE!

The removal of the knob is only possible in one position. To reach this position slowly turn it to left or right. Depending on the position, a full turning of 360° might be necessary.

10. Smart Metering - Introduction

Thank you very much for purchasing a KENTIX energy monitoring solution based on the KENTIX PowerManager.

10.1. Product features

The KENTIX PowerManager is the central component of the solution. Online SmartMeter and InlineMeter as well as alternatively via serial interface (RS485) a Power Analyser and electricity meter can be connected. The PowerManager is connected to the network via a PoE-enabled switch.

The web interface can then be used to change the basic settings, such as IP data and user configuration, as well as the configuration of all measuring devices (SmartMeter).

A description of the configuration can be found later in this guide.

10.2. Application areas

- Industry
- Hospitals
- Telecommunication
- Energy and water supplier
- Data centers

10.3. Safety instructions

Installation

In order to ensure the safety and integrity of the operator as well as the correct operation of KENTIX Smart Metering components, the installation must be carried out by a competent person. In addition, it must also comply with the relevant regulations.

Environment

The location of the installation must be such that the PowerManager and SmartMeter and all associated cables are not affected by the following environmental factors:

Dust, moisture, excessive heat; direct sunlight; Heat sources; Devices that generate strong electromagnetic fields; Liquids or corrosive chemicals.

Please observe the ambient conditions given in the technical data.

Degree of protection

When installing PowerManager and SmartMeter, certain degrees of protection must be guaranteed. Observe the relevant regulations for installations in specific environments such as in industry or data center.

10.4. Components

Depending on the requirements, the equipment for energy monitoring can be carried out with the Kentix SmartMeters via radio or, alternatively, wired with ModBus meters.

ModBus counters are either wired directly or integrated over the network depending on the version.

The Kentix SmartMeter connect via ZigBee radio with the PowerManager and can also network with each other, for example, to equip larger areas.

Up to 32 SmartMeters can be operated using one PowerManager.

10.4.1. PowerManager



The PowerManager is the central component of the solution. Here, the SmartMeter or ModBus counters are connected via radio or RS485.

The PowerManager is connected to the network via a PoE-enabled switch.

The web interface can then be used to change the basic settings, such as IP data, as well as the configuration of user data and counter settings.

A description of the configuration can be found later in this guide.

10.4.2. Wireless SmartMeter



Radio extension meter for the integration of consumers in the IT infrastructure or technical rooms. Ideal for measuring rack PDUs, UPSs, air conditioning systems or building services. The meter is installed on the standard DIN rail in the electrical distribution or can be used directly as a so-called InlineMeter. In the event of a power failure, a last message can be sent to the PowerManager. Thus, network and phase failure are optimally monitored.

10.4.3. Wireless Inline-Meter



Inline meters are ready-made SmartMeters. These are available ready for connection in 4 versions::

Online Inline-Meter 16A, 1-phase

Online Inline-Meter 16A, 3-phase

Online Inline-Meter 32A, 1-phase

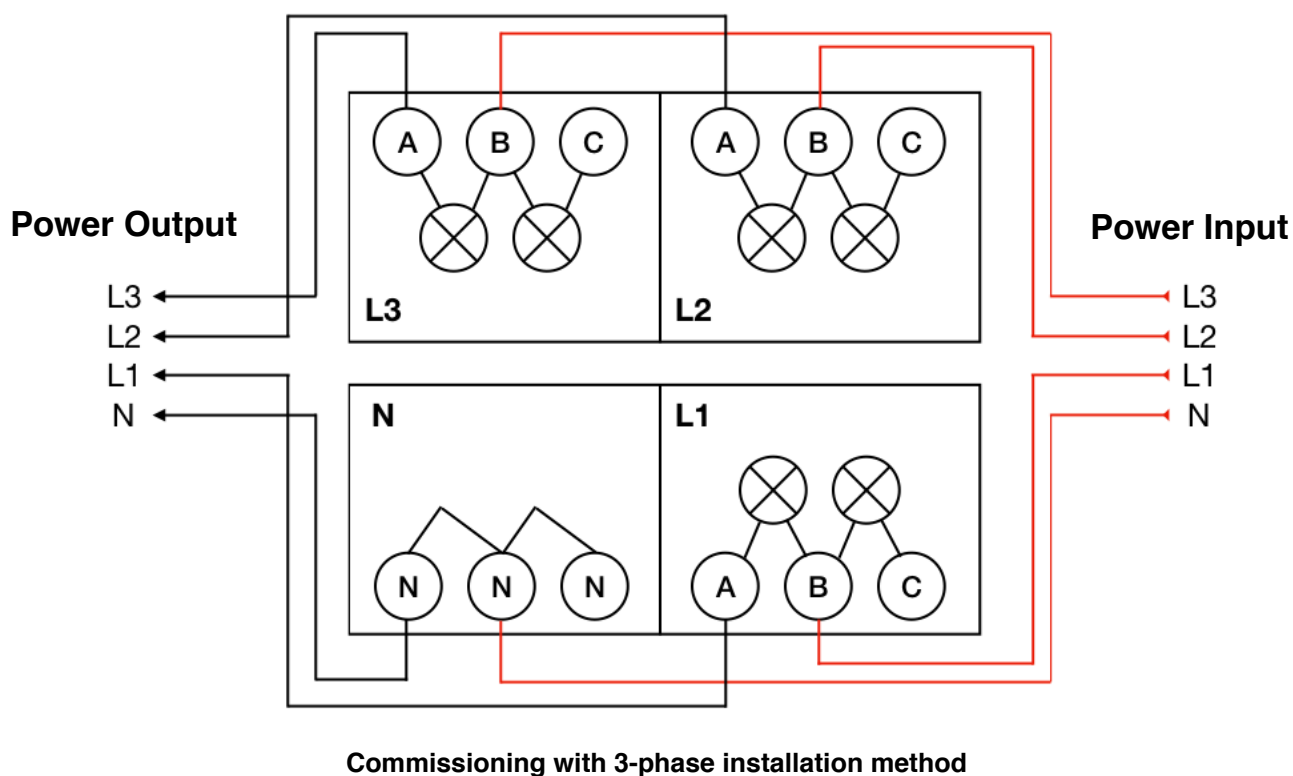
Online Inline-Meter 32A, 3-phase

10.5. Assembly & Programming (commissioning)

10.5.1. Installation Wireless SmartMeter

The installation is done in following steps:

No	Description
1	Interrupt power supply. For the duration of the electrical work, the power supply for the entire work area must be disconnected by switching off the corresponding fuses.
2	Place the radio smart meter on the DIN rail. Make sure that it engages correctly.
3	Remove 11mm of the cable insulation at the supply and output lines with a suitable wire stripper.
4	Connect the cables to the Wireless Smart Meter according to the following wiring diagram.
5	Mount the antenna.
6	Restore power.



NOTE!

For a single-phase installation, it is always necessary to establish a connection between L1, L2 and L3 via connection B. Otherwise, no metering takes place.

10.5.2. Installation Wireless InlineMeter

The installation is done in following steps:

No	Description
1	Interrupt power supply. For the duration of the electrical work, the power supply for the entire work area must be disconnected by switching off the corresponding fuses.
2	Plug the radio InlineMeter between the supply voltage and the load. Please make sure that the plug is completely connected.
3	Restore power.

10.5.3. PowerManager

To install the PowerManager, simply attach the supplied mounting bracket to the wall or ceiling and attach the PowerManager. Then establish a network connection to a PoE switch.

Make sure that the maximum distance between PowerManager and the SmartMeters or InlineMeters must not exceed 30 meters, otherwise the wireless connection is not guaranteed.

10.5.4. Configuration

For configuration purposes, a web server is integrated in the PowerManager in order to be able to configure and operate the device via the network using a web browser.

Connection with PC: Connect the LAN jack of the PowerManager to a PoE-enabled switch using a LAN cable. Also establish a network connection between your PC and this switch. Set the IP address of your PC to eg "192.168.100.123".

10.5.4.1. Settings delivery state / factory settings

Power supply: PoE (Power over Ethernet).
 Default IP-Adress: 192.168.100.224
 Subnet-Mask: 255.255.255.0
 User / password: admin / password

IMPORTANT! - Reset to factory settings

For security reasons, resetting the PowerManager is only possible immediately after the system has been started for a period of 1 minute.

You can restart the PowerManager by briefly unplugging and reconnecting the connected network cable. Then wait about 30 seconds until the device is ready for operation (green LED active) and press the button.

Press and hold the button for 15 seconds until the reset process is confirmed by a long tone.

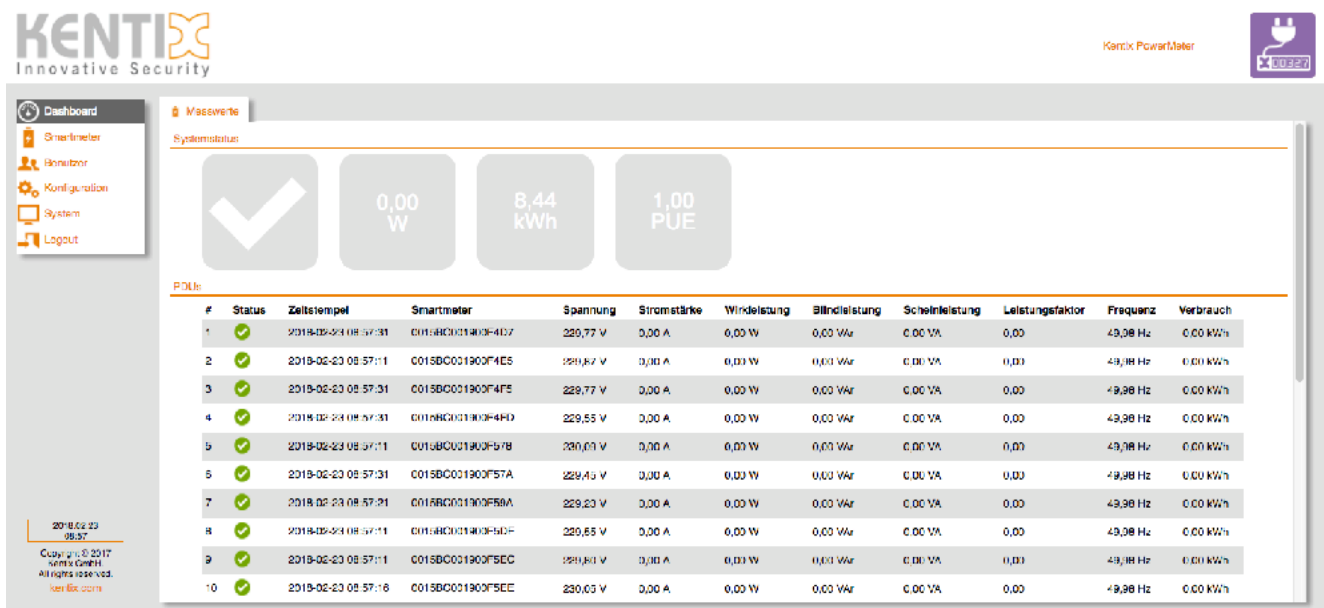
The device is reset to factory settings and restarts. After approx. 30 seconds, the PowerManager can be reached again via the standard settings.

10.5.4.2. Communication ports

The configuration of the PowerManager is done via standard HTTP (S) ports:

No	Description	Port Number
1	Konfiguration PowerManager und Firmwareupdate über den Webbrowser	TCP 443 (HTTPS), 80 (HTTP - will be directed to 443) from PC to AccessPoint

10.5.4.3. Dashboard - Measurement data



Overview of all configured smart meters

In the overview, the dashboard displays the measured values of all connected smart meters, including the current consumption.

The system status above indicates whether there are currently alarms - e.g. Threshold exceeded - pending, as well as the current torque consumption, total consumption and PUE value (Power Usage Effectiveness).

NOTICE!

Consumption always indicates the total consumption since commissioning the meter, but not monthly or annual consumption.

10.5.4.4. Smartmeter - Smartmeter

In the tab "Smartmeter" the Smart Metering devices are managed, which are connected to the PowerManager. In the overview you will see already learned devices. With "+" you can add more smart meters. The info button ("i") also gives you additional information such as the device address and the current firmware version.

NOTICE!

Note that to learn new Smart Metering devices, you must be within range of the respective PowerManager (up to 30m).

Teach-in of new Smartmeters

To teach in a new smart metering device, click on the "+". Then select the counter type and the number of phases.

In addition, a name must be assigned and the smartmeter address entered which is similar to the serial number printed on the Smartmeter.



Then click on the arrow next to the Smartmeter address. This starts the search for new smart meters on the PowerManager.

On the smartmeter, the teach-in button "LEARN" must then be pressed and held down until the "INFO" LED flashes permanently. This takes about 20 seconds.

The smartmeter should then be recognized after about 10-20 seconds and added to the list of already configured smart meters.

Then continue with the configuration of the device by clicking on the edit pen.

10.5.4.5. Smartmeter - General

Transmission cycle (Sec)

Sets the transmission cycle of the smartmeter in seconds.

Connection timeout (Sec)

Sets the time interval for a connection timeout. If a smartmeter has not sent data to the PowerManager within this time, the device will be marked in the Dashboard with an interrupted connection.

Sending reports

This option enables an automatic monthly report with consumption data that is sent to all users who have an e-mail address enabled.

NOTICE!

The values set here for transmission cycle and connection timeout are based on empirical values. Changing the values can lead to failures or connection interruptions.

10.5.4.6. User

Here, users can be added and managed. Up to 1,000 users per system can be configured.

User name

Assign a unique user name for the user. This is required to log in to the PowerManager and may only be used once in the system.

Full Name

As a supplement to the user name, the full name of the user must be entered here. This has no function for the operation of the system.

User password

All users who should have access to the PowerManager require a login user password in addition to the user name.

E-mail address

If an e-mail address is stored, the user is informed about critical system states - e.g. Threshold exceeded for current or voltage informed.

Description

Enter a description for the respective user, if required.

System permissions - user level

Users have 2 permission levels to choose from:

"Display only" allows you to log in to the system for viewing the dashboard.

"Super Administrator" allows full access to the PowerManager.

System permissions - receive notifications

Defines whether the user should be informed about critical system states.

10.5.4.7. Configuration - General

These are the basic settings of the PowerManager.

Name

Assign a unique name for each PowerManager, e.g. the installation site for better identification of the respective device.

Language

Select the language for the web interface of the PowerManager.
As languages German and English are available.

Safety - Communication key

The communication key is the password used to encrypt communication between Kentix devices.
The key must be identical on all devices and should conform to certain guidelines (length, upper / lower case, numbers, special characters).

NTP 1 / NTP 2

In the fields "NTP 1" and "NTP 2" the time servers are set to synchronize the time. These can be servers in your own network as well as public time servers (default).

The time is needed to use the time profiles and the correct logging of bookings and events in the logbook.

Public NTP Server: 0.de.pool.ntp.org oder 1.de.pool.ntp.org

Time zone

Select your time zone, in which the PowerManager is located. This is the only way to ensure that the timestamps of the measured value update and any alarm entries match the actual time.

Current system time

Saves the current time from your workstation to the PowerManager. This feature can be used if no time server is available.

The field displays the time in the PowerManager when the "General" tab is called.

10.5.4.8. Configuration - Network

These are the network settings of the PowerManager. The device is delivered with a standard configuration.

Default IP Address: 192.168.100.224
Subnet-Mask: 255.255.255.0
User / password: admin / password

This data can be adapted after commissioning for your own environment.

IPv4 address, subnet mask, gateway

Network configuration of the PowerManager. You can enable DHCP for IP configuration. In this case, the PowerManager must always be assigned the same IP address from the DHCP server. The MAC address of the device can be read here. Alternatively, manual network data can be specified.

The changes to the network settings are directly active after saving.

DNS server address 1 / 2 (Domain name server address)

Depending on the network configuration, e.g. if using an ADSL router, this may also be the gateway address.

Public DNS Server: 8.8.8.8 or 8.8.8.4

10.5.4.9. Configuration - Communication

E-mail Settings

In order for the PowerManager to be able to send e-mails to the configured users (for example, if the threshold is exceeded), an e-mail server (SMTP or ESMTP) must be configured here. If you have configured a DNS server in the DNS settings, you can use the DNS name of the e-mail server here. By using ESMTP, you can enter the e-mail credentials provided by your e-mail provider. In addition - depending on the mail server - an encryption with an associated port must be selected.

When selecting an encryption type (STARTTLS / SSL), the corresponding standard port is automatically entered as well. If required, it can be changed to any port.

Note that many mail servers require existing sender addresses for proper mail delivery.

E-mail signature

Enter a signature that will be sent with each e-mail. The signature is limited to a length of 1000 characters.

SNMP settings

The PowerManager supports SNMP V2 to query the readings of all connected SmartMeters.

For this a MIB (Management Information Base) is available. Alarms can also be sent in the form of SNMP traps to up to 2 hosts. To do this, enter the destination IP addresses for the hosts and the corresponding communication port (default: 162).

For queries, a name must additionally be entered in the field "Public Community".

10.5.4.10. System - logbook

This is the system logbook of the PowerManager. All important system events are listed here. Among other things, the logbook contains warnings about critical system conditions such as Threshold violations or connection interruptions to SmartMeters.

10.5.4.11. System - system functions

Create backup / restore

The buttons can be used to create a complete backup of the configuration data and also to restore it. After setting up Smartmeter and users, it is recommended to create a corresponding backup.

NOTICE!

The backup always includes the complete configuration including all devices configured in the system. If no component has been replaced in the system or reset to factory settings, the entire system can be restored with a backup.

Firmware update

Firmware updates for the PowerManager can be loaded here, if required.
Select the firmware image file via the displayed file dialog and then click on "Start update".

ATTENTION!

Please note the notes of the respective release notes of the downloaded update!

10.5.4.12. System - ZigBee

Contains information about the current wireless network of the PowerManager. In addition, the current radio channel can be changed and the radio network can be reset here.

ATTENTION!

If there are connection problems between PowerManager and SmartMeter, it is possible to change the radio channel. This may be necessary if there are other devices in the area that communicate over 2.4 GHz (for example, Wi-Fi access points).

When changing the channel, the PowerManager notifies the SmartMeters of the new radio channel before the change. If a SmartMeter can not be reached during this time, it must be re-taught.

The function "reset network" creates a new wireless network. If this is done, all SmartMeters must be re-taught!

10.5.4.13. System - Help

Contains support information and version information about PowerManager.

11. Kentix AlarmManager Smartphone-App

With the Kentix Mobile app a monitoring and control of a Kentix System via IOS or Android devices is possible. In the following, functions and control of the app are described.

11.1. The Profile menu

When starting the app the profile selection menu is displayed.
With the „+“ Button in the upper right edge a new profile is created.
Now select the device type.

NOTE!

Connections to the Kentix360 cloud only work together with an AlarmManager (BASIC or PRO) or an AccessPoint.
A local connection (WLAN profile) is not provided.

Make sure the app is allowed to access the camera. Otherwise, data such as the personal Kentix360 ID must be entered manually.

If the camera is active, this data can be recorded in the form of a QR code.
The code can be found in the user settings on the respective device.

After photographing the code, assign a unique name to differentiate multiple profiles / devices and enter your user password.

NOTE! - Disable and delete devices from a cloud account!

A deactivated AlarmManager or AccessPoint can be added again to the cloud at any time.
On deleting the device is first only marked for the deletion. The final deletion will be processed after 24 hours.
Only after expiry of this period, the device is completely removed from the cloud account.
It can then be added again using the same or a new account.
All recorded data (sensor readings, logbook) will be deleted.
AlarmManager for which the Kentix360-SIM has been activated can **not** be deleted from the cloud profile!

11.2. AlarmManager

Dashboard

Similar to the AlarmManagers web interface, the Dashboard if the app gives an overview of the AlarmManager with the general building state and an overview of the alarm zones.

Here the zones can also be switched and alarms can be acknowledged.

Selecting a zone will open the overview for the devices configured in this zone.

Here the alarm zone can be switched separately.

Logbook

Tapping the menu icon opens the selection menu.

There the logbook can be accessed. The logbook of the app provides the same information as the event log of the AlarmManager.

11.3. MultiSensor-LAN

The MultiSensor LAN currently does not support cloud communication.

A corresponding firmware update is available from Q3 / Q4-2018.

11.4. AccessPoint

Door Control

In the view „Door Control“ single doors can be accessed for a remote opening. Select the desired door and then press the button „Open door“. The person at the door can open it now for the next 15 seconds.

For the remote opening a knob (DoorLock-DC) must be turned to wake it up.

At a door lever (DoorLock-LE) a booking with any RFID media (Mifare) is required.

At a wall reader the assigned relay of the AccessPoint is triggered.

The cabinet lock also has to be woken up by pressing the button at it.

Favorites

The view „Door Control“ always shows all DoorLock-devices / doors configured in the system.

In order to be able to directly access frequently used doors for a remote opening, these doors can be marked as favorites here.

To do so, press the „+“ and select the desired doors for this view.

The favorites view will then automatically become the first view after selecting the AccessPoint-profile.

Logbook

The logbook shows the last 100 bookings made at the DoorLock-devices in the system.

If necessary older entries can also be called up.

NOTE!

The Kentix360 security key stored in the AccessPoint is required for the accessing the logbook. Without this key the reading of logbook entries is not possible.

12. Kentix360 Cloud

The Kentix360 Cloud expands your Kentix system by essential improvements in availability, alerting, data recording and accessibility. Advantages of the Kentix360 Cloud are:

- Safe remote access via smartphone app without complicated setup
- PUSH messages and redundant e-mails without configuration
- Backup of the AlarmManager's configuration
- Hourly routine checkup of the AlarmManager / AccessPoint availability
- SIM card with a startup bonus of 600 ALARM-SMS for the first year (optional, only for AlarmManager)
The card will be automatically recharged after 600 sent ALARM-SMS and the latest after 12 months with up to 600 ALARM-SMS.
- 12 month recording of data and logbook
- Remote control of the Kentix DoorLock-components via App

12.1. Setup

The activation of the Kentix360 Cloud is done via the web interface of the AlarmManager or the AccessPoint. Activation via telephone support or e-mail is **not possible**.

To use the cloud, an AlarmManager-BASIC/-PRO or an AccessPoint is required. MultiSensor-LAN is not intended for operating with cloud access in stand-alone mode. A corresponding firmware update is available from Q3 / Q4-2018.

To activate the cloud usage on your Kentix system login to your AlarmManager via the web interface and go to Kentix360 in the menu bar.

Click the button „Create new Kentix360 account“ and fill out the personal data form. This information is required for the billing by Kentix.

Please note that for the password some policies have to be followed. These policies are:

- 6 signs minimum length
- at least one upper-case and one lower-case letter
- at least one digit and one special character

Now click on „Apply“ to transmit the data.

The account becomes active directly after applying.

You can now login to the cloud using the previously entered e-mail-address and password.

12.2. Manage Devices

After logging in the 3 tabs **Registered Devices**, **Kentix360 SIM (only AlarmManager)** and **Kentix360 Account** are available.

Registered Devices

Here the AlarmManager or AccessPoint, to which you are connected, can be added to the cloud.

To add it, click the „+“ button. A message appears showing that the service entails costs which has to be confirmed.

The AlarmManager now appears in the list as „not connected“ (red cloud icon). To complete the process, save the settings. The active connection to the cloud will be signalized in the icon bar at the bottom of the ControlCenter window.

In the section „Registered Devices“ of the cloud configuration all AlarmManagers assigned to the Account are displayed, which are connected with Kentix360 Cloud.

The "Edit button" (pen) can be used to define a routine time for each device. In addition, the AlarmManager or AccessPoint with which you are currently connected can be temporarily deactivated or deleted completely.

Kentix360 Account

In the section „Account“ the data of your Kentix360 cloud account and the corresponding user data is administrated. Except for the company name the data can be changed as required.

The entered data will be transmitted to the Kentix360 service after applying and is active directly.

Kentix360 SIM

To setup the Kentix SIM card please continue reading further down: „Kentix SIM card“.

NOTE - Deactivating and deleting devices from a cloud account

A deactivated AlarmManager or AccessPoint can be added again to the cloud at any time.

On deleting the device is first only marked for the deletion. The final deletion will be processed after 24 hours.

Only after expiry of this period, the device is completely removed from the cloud account.

It can then be added again using the same or a new account.

All recorded data (MultiSensor values, logbook) will be deleted.

AlarmManager with an activated Kentix360 SIM card can not be deleted from the cloud profile!

13. Kentix SIM card

All AlarmManagers are shipped together with a SIM card of the Deutsche Telekom. This card is an integral part of the Kentix360 cloud (chargeable). When activating the card via the cloud configuration a startup bonus of 600 ALARM-SMS is granted.

The use of the SIM card is chargeable. The exact price can be found in our conditions.

Activation of the card is only possible in Germany, Austria and Switzerland.

It is possible to use any other SIM card with the AlarmManager.

13.1. Setup

The SIM card is included with your AlarmManager and must be plugged into the SIM card holder of the AlarmManager for activation.

Activation of the card takes place exclusively via the AlarmManager web interface, but not via telephone support or via e-mail.

For activating your Kentix360 SIM card login to your AlarmManager and go to „Kentix360“.

Login with your account data or create a new Kentix360 account. Then register your AlarmManager for the cloud service (chargeable, charged by Kentix).

Click the tab „Kentix SIM“ and there the button „Activate SIM card“.

Your card data is now transmitted to Kentix and the SIM card will be activated within the next 2 working days. A message about the activation and your new telephone number and billing information will be sent to the e-mail-address used during the Kentix360 account creation.

13.2. Telephone number and PIN

When shipped the Kentix SIM does not have a telephone number and PIN. It can only be activated and used in combination with an AlarmManager.

For safety reasons we recommend to enter a PIN after the insertion.

To assign a PIN login to your AlarmManager and select „Configuration“ -> „GSM“ -> „Change PIN“.

Now enter a 4-digit PIN. Use „0000“ as value for the old PIN.

14. Data sheets

14.1. Data sheet AlarmManager-BASIC/PRO (KAM-BASIC/PRO)

Number of MultiSensor (KAM-BASIC) Number of MultiSensor (KAM-PRO)	KAM-BASIC: max. 200 (only ZigBee) KAM-PRO: max. 500
Internal Buzzer	85dB, 2.3kHz
Sensor - temperature	range -20 to 99°C / -3 to 210°F (exactness $\pm 0,5^{\circ}$)
Sensor - relative humidity	range 0 to 100% (exactness $\pm 3\%$)
Dew point	calculated in °C/°F
External alarm inputs	4 x alarm input (e.g. Armed-Active, Always-Active alarms) for external potential-free contacts via separately available KIO1/KIO3 power adapter
External outputs	4x alarm output (e.g. Armed-Active, Always-Active alarm) connection via separately available KIO3 power adapter
Internal temper sensor	Internal vibration sensor (high sensitive)
LED	RUN/POWER (green), ALARM (red)
Radio	ZigBee® 2,4GHz ISM Band +3dBm output power, IEEE802.15.4, encryption AES 128 Bit
LAN	10/100Mbit
Integrated GSM Modem	Quad Band (GSM/3G) 850/900/1800/1900MHz integrated SIM card holder
SD card	Integrated micro SD card holder as additional storage for image recording, up to 128 GB
Power supply	PoE Class 3 or via external I/O-module KIO3 12-32VAC/DC, power consumption approx. 5W
Integrated UPS	4 minutes up time by internal high capacitor. Control of external power supply.
Kentix system jack	2 pc. RJ45, for external plug'n play modules
Chassis	Material: PS 130 x 120 x 45 mm Weight approx. 300g Color: White, Black
Environmental conditions	Temperature 0 - 50°C / 32 - 122°F Humidity 5-95%, not condensing
Types	KAM-BASIC/PRO-B = Chassis black KAM-BASIC/PRO-W = Chassis white
Content of delivery	2 pc of antennas (ZigBee, GSM), mounting bracket and material, slim line cable 3m
Accessories	Leakage sensor (KLS03), External antennas for ZigBee and GSM, Power adapter KIO1, KIO3
Approvals	CE



14.2. Data sheet MultiSensor-RF (KMS-RF)

Connectable devices	AlarmManager-BASIC (KAM-BASIC) AlarmManager-PRO (KAM-PRO)
Sensor - temperature	range -20 to 99°C / -3 to 210°F (exactness $\pm 0,5^{\circ}$)
Sensor - relative humidity	range 0 to 100% (exactness $\pm 3\%$)
Dew point	calculated in °C/°F
Sensor - motion	PIR sensor, trigger sensitivity configurable detection cone: approx. 110° range: approx. 8m
Sensor - vibration	3 axes vibration sensor (adjustable)
Sensor - carbon monoxide (CO)	0-10.000ppm measurement $\pm 10\%$ Internal resolution: 20-200ppm (0-100%) lifetime 10 years
Buzzer	85dB, 2.3kHz
Sensor - external alarm input	2 x alarm input (e.g. Armed-Active, Always-Active) Both for external dry contacts via separately available KIO1/KIO3 power adapter
Ext. output	2x alarm output (e.g. Armed-Active, Always-Active), connection via separately available KIO3 power adapter
LED	ALARM (red) RUN (green)
Radio	ZigBee® 2,4GHz ISM band +3dBm output power, IEEE802.15.4, encryption AES 128 Bit
Power supply	12-32VAC/DC power consumption. approx. 1.5W
Integrated UPS	3 minutes up time by internal high capacitor. Control of external power supply.
Kentix System-jack	RJ45, for supply and connection of external IO-modules (KIO1/KIO3)
Chassis	Material: PS 90 x 90 x 45 mm, Weight: approx. 100g Color: White, Black
Environmental conditions	Temperature 0 - 50°C / 32 - 122°F Humidity 5-95%, not condensing
Types	KMS-RF-B (Chassis Black) KMS-RF-W (Chassis White)
Content of delivery	Mounting bracket and material, KIO2, Power supply 24V
Accessories	PowerAdapter with power supply (KIO1, KIO3) Leakage sensor (KLS03)
Approvals	CE



14.3. Data sheet MultiSensor-LAN (KMS-LAN)

Connectable devices	Stand-Alone operation (integrated web server) AlarmManager-PRO
Sensor - temperature	range -20 to 99°C / -3 to 210°F (exactness $\pm 0,5^{\circ}$)
Sensor - Relative humidity	range 0 to 100% (exactness $\pm 3\%$)
Dew point	calculated in °C/°F
Sensor - motion	PIR sensor, trigger sensitivity configurable detection cone: approx. 110° range: approx. 8m
Sensor - vibration	3 axes vibration sensor (adjustable)
Sensor - carbon monoxide (CO)	0-10.000ppm measurement $\pm 10\%$ Internal resolution: 20-200ppm (0-100%) lifetime 10 years
Buzzer	85dB, 2.3kHz
Sensor - external alarm input	2 x alarm input (e.g. Armed-Active, Always-Active) Both for external dry contacts via separately available KIO1/KIO3 power adapter
External alarm output	2x alarm output (e.g. Armed-Active, Always-Active), connection via separately available KIO3 power adapter
LED	ALARM (red), RUN (green) LINK/ACT at the LAN jack
LAN	10/100Mbit LAN connection integrated web server
SD card	Integrated micro SD card holder as additional storage for image recording, up to 128 GB
SNMP (Simple Network Management Protocol)	SNMP V2 (write/read) SNMP Traps
power supply with PoE	12-72VAC/DC power consumption ca. 1.5W, PoE class 1
power supply with power supply unit	12-32VAC/DC power consumption ca. 1.5W over system jack
KENTIX system jack	RJ45, for supply and connection of external IO-modules (KIO1/KIO3)
Chassis	Material: PS 90 x 90 x 45 mm, Weight: approx. 100g Color: White, Black
Environmental conditions	Temperature 0 - 50°C / 32 - 122°F Humidity 5-95%, non-condensing
Types	KMS-LAN-B (Chassis Black) KMS-LAN-W (Chassis White)
Content of delivery	Mount bracket, Mount material, slim line cable 3m
Accessories	PoE Injector (KPOE150S) PowerAdapter with power supply (KIO1, KIO3) Leakage sensor (KLS03)
Approvals	CE



14.4. Data sheet MultiSensor-LAN-RF (KMS-LAN-RF)

Connectable devices	Stand-Alone operation (integrated web server) AlarmManager-PRO
Sensor - temperature	range -20 to 99°C / -3 to 210°F (exactness $\pm 0,5^\circ$)
Sensor - Relative humidity	range 0 to 100% (exactness $\pm 3\%$)
Dew point	calculated in °C/°F
Sensor - motion	PIR sensor, trigger sensitivity configurable detection cone: approx. 110° range: approx. 8m
Sensor - vibration	3 axes vibration sensor (adjustable)
Sensor - carbon monoxide (CO)	0-10.000ppm measurement $\pm 10\%$ Internal resolution: 20-200ppm (0-100%) lifetime 10 years
Buzzer	85dB, 2.3kHz
Sensor - external alarm input	2 x alarm input (e.g. Armed-Active, Always-Active) Both for external dry contacts via separately available KIO1/ KIO3 power adapter
External alarm output	2x alarm output (e.g. Armed-Active, Always-Active), connection via separately available KIO3 power adapter
LED	ALARM (red), RUN (green) LINK/ACT at the LAN jack
LAN	10/100Mbit LAN connection integrated web server
Radio	ZigBee® 2,4GHz ISM band +3dBm output power, IEEE802.15.4, encryption AES 128 Bit
SNMP (Simple Network Management Protocol)	SNMP V2 (write/read) SNMP Traps
power supply with PoE	12-72VAC/DC power consumption ca. 1.5W, PoE class 1
power supply with power supply unit	12-32VAC/DC power consumption ca. 1.5W over system jack
KENTIX system jack	RJ45, for supply and connection of external IO-modules (KIO1/KIO3)
Chassis	Material: PS 90 x 90 x 45 mm, Weight: approx. 100g Color: White, Black
Environmental conditions	Temperature 0 - 50°C / 32 - 122°F Humidity 5-95%, non-condensing
Types	KMS-RF-B (Chassis Black) KMS-RF-W (Chassis White)
Content of delivery	Mount bracket, Mount material
Accessories	PoE Injector (KPOE150S) Power-Adapter with power supply (KIO1, 2, 3) Leakage sensor (KLS03)
Approvals	CE



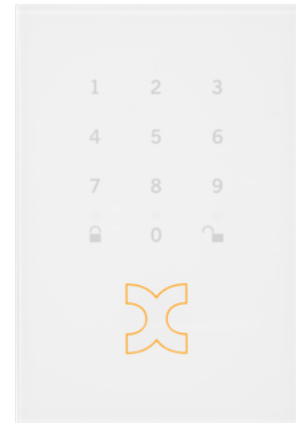
14.5. Data sheet MultiSensor-Door (KMS-Door)

Connectable devices	AlarmManager-BASIC (KAM-BASIC) AlarmManager-PRO (KAM-PRO)
Sensor - temperature	range -20 to 99°C / -3 to 210°F (exactness $\pm 0,5^{\circ}$)
Sensor - Relative humidity	range 0 to 100% (exactness $\pm 3\%$)
Sensor - Dew point	calculated in °C/°F
Sensor - Vibration	3 axes, adjustable sensitivity
Sensor - Sabotage	sabotage alarm on disassembly
Sensor - Magnetic contact	magnetic sensor for door position (distance approx. 1cm)
Buzzer	65dB, 2.3kHz
LED	Multicolor-LED (Red/Green) ALARM (Red) Teach-in (Green)
Radio	ZigBee® 2,4GHz ISM band +3dBm output power, IEEE802.15.4, encryption AES 128 Bit
Power supply	Battery: 1x Lithium Ion 1/2 AA 3,6V (1200 mAh) Battery life up to 4 years
Chassis	Material: PS 63 x 29 x 28 mm, Weight approx. 50g Color: white, black
Environmental conditions	Temperature 0 - 45°C / 32 - 113°F Humidity 5-95%, non-condensing
Types	KMS-Door-W (casing white) KMS-Door-B (casing black)
Content of delivery	1x Li-Battery 3,6V/1200mAh Mounting material Magnet for REED-contact
Approvals	CE



14.6. Data sheet KeyPad (KKPT)

Connectable devices	AlarmManager-BASIC/PRO MultiSensor-LAN-RF
Buzzer	70dB, 2.3kHz
LED	Arm (RED/GREEN) Disarm (RED/GREEN)
Radio	ZigBee® 2,4GHz ISM band +3dBm output power, IEEE802.15.4, encryption AES 128 Bit
Power supply (battery)	Battery 2 pc. 1.5V/AAA Battery life approx. 2 years depending on the number of switching cycles
Chassis	Material: PS 135 x 90 x 19 mm Weight ca. 100g Color: High-White Protection class: IP40
Environmental conditions	Temperature 0 - 45°C / 32 - 113°F Humidity 5-95%, not condensing
Types	KKPT - Integrierter RFID Leser (13.56MHz); ISO14443A/B, ISO15693, ISO18092/NFC (MIFARE® DESFire®, Legic-Advant®)
Content of delivery	KKPT, 2x AAA battery, 2 pc. of Mifare RFID Token
Accessories	Battery KeyPad 1.5V/AAA, 1000mAh
Approvals	CE



14.7. Data sheet AccessPoint (KXP-16)

Connectivity	Stand-Alone or in connection with AlarmManager
Number of profile cylinders	Up to 16 profile cylinders connectable
Networking	Up to 999 AccessPoints in Master-Slave mode linkable. Control via master AccessPoint.
Internal memory	5.000 persons - Access permissions 100 door profiles 100 time profile (daytime, weekday)
SD card	Integrated Micro SD card holder as additional memory for video recording, up to 128 GB
Internal buzzer	85dB, 2.3kHz
LED	ALARM (red), RUN (green), LINK/ACT at LAN interface
LAN	10/100 Mbit LAN interface, integrated Web-Server Ports: 80 (HTTP), 443 (HTTPS)
Wireless DoorLock	868MHz, Encryption AES 128 Bit, Distance up to 25m up to 16 DoorLock-devices per AccessPoint
Power supply (PoE)	12-72VAC/DC Power consumption approx. 3W PoE class 2
Power supply (System connector)	12-32VAC/DC Power consumption approx. 3W via system connector
KENTIX System connector	RJ45, for the connection of external Kentix Plug'n Play modules
Chassis	Material: PS 90 x 90 x 45 mm, weight approx. 100g Color: Carbon black
Environmental conditions	Temperature 0 to 50°C, humidity 5-95%, non condensing with outdoor chassis up to -20°C possible
Types	KXP-16-B (chassis Black) KXP-16-W (chassis white)
Content of delivery	mount bracket, mount material, antenna, SlimLine cable 3m
Accessories	PoE Injector (KPOE150S) Power Adapter with power supply(KIO1, KIO3)
Approvals	CE



14.8. Data sheet Online Door knob DoorLock-DC (KXC-KN1/2/3)

DoorLock-DC	Online door knob according to DIN15684
Connectivity	DoorLock AccessPoint KXP-16
RFID Reader	13.56MHz Mifare Classic, DESfire
Internal buzzer	70dB, 2.3kHz
LED	red, green
Wireless	868MHz, Encryption AES 128 Bit distance approx. 25m up to 16 Online profile cylinders per AccessPoint
Usage	Inside and outside doors suitable for fire and smoke protection doors
Low-Power-opening	with external power supply/adapter
Assembly / disassembly	Via master card set
Permanent engagement	Permanent engagement possible without additional power consumption
Power supply	2 x batteries CR2 Lithium (3V)
Battery life	up to 45.000 operations or up to 4 years
Dimensions knob	KXC-KN1 (IP55): length = 42,7mm, diameter = 40,0mm KXC-KN2 (IP66): length = 20,0mm, diameter = 45,0mm KXC-KN3 (IP66 outside, IP55 inside): length: 44,3mm outside, 42,7mm inside diameter: 31,4mm outside, 40mm inside
Material	nickel-plated brass, antenna: hard plastic
Zylinder lengths	30/30mm to 70/70mm (Special lengths up to 200/200mm) for profile cylinders of type DIN 18252 or circular cylinders (Switzerland)
Environmental conditions	Temperature -25°C to 65°C
Types	KXC-KN1 (IP55) for interior installations KXC-KN2 (IP66) for exterior installations KXC-KN3 (IP66/IP55) KXC-KN3-OD (IP66/IP55)
Content of delivery	Knob, 2 batteries (CR2)
Accessories	EURO Profile cylinder, circular cylinder (Switzerland), Low-Power adapter for emergency powering
Approvals	CE



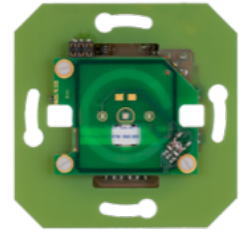
14.9. Data sheet DoorLock-LE (KXC-LE)

DoorLock-LE	Online door lever with one side RFID-reader
Connectivity	DoorLock AccessPoint KXP-16
RFID reader	13.56MHz Mifare Classic, DESfire
Internal buzzer	70dB, 2.3kHz
LED	red, green
Wireless	868MHz, encryption AES 128 Bit, distance approx. 25m up to 16 Online door levers per AccessPoint
Usage	Inside and outside doors fire and smoke protection doors (with door fitting)
Permanent engagement	Permanent engagement possible without additional power consumption
Power supply	Battery CR123A Lithium (3V)
Battery life	up to 100.000 operations or up to 6 years
Dimensions door lever	Compatible with all current European standards
Dimensions round rosette	55mm
Dimensions oval rosette	length=66mm, width=36mm
Door thickness - square pin	length: 30-110mm thickness: 8mm, 8,5mm (anti panic door), 9mm (fire protection door)
Material	nickel-plated brass, antenna: hard plastic
Environmental conditions	Temperature -20°C to 65°C
Types	KXC-LE
Content of delivery	Door lever, 1xbattery (CR123A), mount material
Approvals	CE



14.10. Data sheet DoorLock-WA (KXC-WA)

DoorLock-WA	Online RFID-wall reader for installation in flush-mounted boxes
Connectivity	DoorLock AccessPoint KXP-16 or KXP-16-RF
RFID reader	13.56MHz Mifare Classic, DESfire
Internal buzzer	70dB, 2.3kHz
LED	red, green
Wireless	868MHz, encryption AES 128 Bit, distance approx. 25m up to 16 Online wall readers per AccessPoint
Usage	Installation in flush-mount box or exposed
Power supply	10-32VDC or 10-24VAC Power consumption typ. 0.8W, max. 5W
Switching relays	max. 30V AC/DC, max. 1.5A
Dimensions	length=71mm, width=71mm, Höhe=26mm diameter=60mm for flush-mount box
Material	Plastic / epoxy
Environmental conditions	Temperature -20°C to 65°C for inside use
Types	KXC-WA1, KXC-WA1-OUTDOOR
Content of delivery	wall reader
Accessories	KIO3 Power adapter for relay control at AccessPoint
Chassis	KXC-WA1 for flush mount installation (choose cover) KXC-WA1-Outdoor for surface mouting, IP66, housing size: 90x90x40mm
Approvals	CE



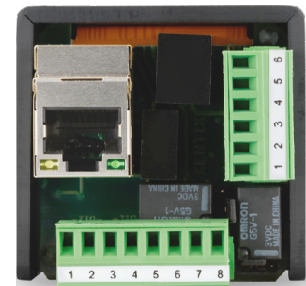
14.11. Data sheet DoorLock-RA1 (KXC-RA1)

DoorLock-RA1	Online RFID-cabinet lock
Connectivity	DoorLock AccessPoint KXP-16
RFID Reader	13.56MHz Mifare Classic, DESfire
Dimensions	Height=148,4mm, Width=44,6mm Depth=35,9mm+37,5mm
LED	RED, GREEN
Wireless	868MHz, encryption AES 128 Bit, distance approx. 25m up to 16 Online cabinet locks per AccessPoint
Usage	Installation in cabinets with a door thickness of up to 20mm suitable for wooden, steel and aluminium doors different locking levers included
Power supply	1 Battery AA Lithium 3,6V Up to 100.000 operations with one battery or 8 years
Material	Plastic
Environmental conditions	Temperature -10°C to 55°C, for inside use
Types	KXC-RA1
Content of delivery	Cabinet lock, 3x locking lever, mounting material, battery
Accessories	Replacement battery AA Lithium 3,6V Battery replacement tool
Approvals	CE



14.12. Data sheet IP wall reader with network relay module (KXC-WA3-IP1)

KXC-WA3-IP	IP wall scanner for mounting in switch box or surface-mounted housing with network relay module
Connectivity	Network relay module, can be networked with the Wireless AccessPoint, up to 999 pieces can be networked together
RFID Reader	MIFARE® DESFire® 13,56MHz, MIFARE® Classic, LEGIC prime, LEGIC advant, ISO14443A (CSN / UID), ISO15693 (CSN / UID), Sony FeliCa (CSN / UID), Inside Secure (CSN / UID)
Dimensions	88 x 99 x 27 mm (Surface Mounting) 88 x 99 x 40 mm (Flush Mounting)
Dimensions Relay Module	47 x 48 x 33 mm, Installation in switch box or on DIN rail
LED	RED, GREEN, BLUE
Signaling, LED	Acoustic signal, RGB illuminated field
Connection Wall Reader	Via relay module 4-wire, length up to 500m, up to two wall readers can be connected
Connection electric door opener / lock	24VDC / 500mA (short term 1A) via integrated PoE splitter or external, 2 pieces relay: 125VAC / 60VDC, 1A, changeover contact
Operating temperature	Wall Reader -25°C to +60°C Relay Module 0°C to +60°C, not condensing
Protection	Wall reader IP54, Relay Module IP20
Configuration	Integrated Webserver (HTTP/HTTPS)
Delivery	Wall Reader with PIN, Network Relay Module, 1x RFID-Token, 3m SlimLine cable
Accessories	Extension reader (KXC-WA3-IP2) PoE injector (KPOE150S)
Approvals	CE



14.13. Data sheet PowerManager (KPM-RF-B)

Connectivity	Stand-Alone operation (Integr. Webserver)
Connection radio counter	Up to 32 wireless meters can be connected
Connection RS485	Up to 128 RS485 (Modbus RTU, Modbus IP) counter KIO3 Adapter required
Internal Storage	1.000 User
Internal Signal	85dB, 2.3kHz
LED	RUN (Green), LINK/ACT on LAN Port
LAN	10/100 Mbit LAN Port, Integrated Web-Server Ports: 80 (HTTP), 443 (HTTPS)
Radio	2,4 GHz, encoding AES 128 Bit reach up to approx. 30m
Power supply (PoE)	12-72VAC/DC input approx.. 1,5W PoE class 1
Power supply (system port)	12-32VAC/DC input approx.. 1,5W via system port
KENTIX system port	RJ45, for connecting external Kentix Plug'n Play Modules (KIO3) for ModBus meters
Chassis	Material: PS 90 x 90 x 45 mm Weight: ca. 100g Color: Black, Protection IP20
Environmental conditions	Temperature 0 to 50°C, Humidity 5-95%, not condensed
Types	KPM-RF-B (Chassis Black)
Delivery	Mounting bracket, mounting material
Accessories	PoE Injektor (KPOE150S) Power Adapter (KIO3)
Approvals	CE



14.14. Data sheet SmartMeter (KSM-DR60-RF / KILM-x-xx)

Connectivity	Kentix PowerManager
Number radio counter	Up to 32 radio counter on one PowerManager
Power supply	1/3 x 230/400V (Neutral) +/-10%, input approx. 1,5W
Power metering	60A per Phase
Metering Accuracy	< 2%
Resolution	1 W
Frequency	45 - 65 Hz, 0,01 Hz
Measured values	Voltage (U), current (I), apparent power (S), active power (P), reactive power (Q), active factor, consumption (kWh)
LED	Teach signaling
Radio	2,4 GHz, encoding AES 128 Bit reach up to approx. 30m
Clamps	Screws, diameter 5,5mm (up to 16 mm ²)
Casing	DIN rail mounting, 4HP, protection class IP2071 x 97 x 70 mm, color: RAL7035
Environmental conditions	Temperature -10°C to 50°C, Humidity 5-95%, not condensed
Types	KSM-DR60-RF (Online SmartMeter) KILM-1-16 (Online InlineMeter 16A, 1-phase) KILM-3-16 (Online InlineMeter 16A, 3-phase) KILM-1-32 (Online InlineMeter 32A, 1-phase) KILM-3-32 (Online InlineMeter 32A, 3-phase)
Delivery	SmartMeter, magnetic antenna
Approvals	CE



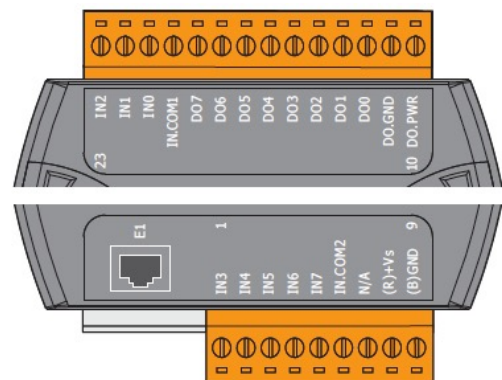
14.15. Data sheet digital I/O expansion-module (KIO7052)



Front



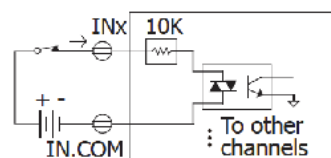
Back



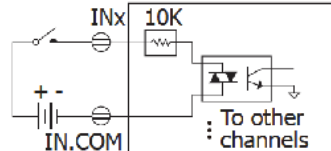
Pin assignment KIO7052

Description	Expansion module for connection to the AlarmManager-PRO. This module extends the external inputs and outputs of AlarmManager on additional 8 digital inputs and 8 digital outputs. Communication is via Ethernet, so the module can be mounted anywhere. The configuration is done in the software interface of the AlarmManager-PRO. The module provides a built-in web-server for simple IP configuration and testing of the inputs and outputs without any additional software.
Connectivity	Connection to Kentix AlarmManager-PRO External Alarms of existing system equipment (HVAC, UPS systems, generators, alarm systems, etc.)
Configuration	Built-in Web-Server (HTTP), Default IP: 192.168.255.1 (Admin/Admin)
Protocols	KAM-IO communication via IP-PORT: 502 (Default)
Security	ID, Password and IP-Filter
Terminals	Plug-able screw-terminal for cables up to 1mm ²
Inputs	Digital wet inputs ON: +10–50VDC, OFF: +4DC Input impedance: 10kOHM Over voltage protection: 70VDC
Outputs	Open-Collector outputs 10–40VDC Current 650mA (bis 1.1A Over current protection) Over voltage protection: 47VDC
Fixed output assignment	DO1-DO8: Armed-Active, Always-Active, Sabotage, General-Alarm, Arm-Zone1, Arm-Zone2, Arm-Zone3, Arm-General
Isolation	Ethernet 1,5kVDC, I/O 3,7kVrms
Environment	Operation temperature 0°C to +45°C, Rel. humidity 10–90%
Network	LAN 10/100 Base-TX
Power supply	PoE (Class 1) or external power supply 12–30VDC, 4.3Watt
Chassis	72 x 123 x 35 mm (DIN-rail mounting)
Content of delivery	KIO7052, 3m patch-cable, power-cable, manual
Approvals	CE

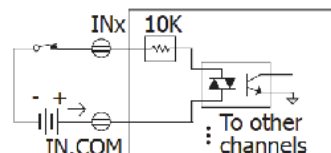
INPUT sink signal (High=1)



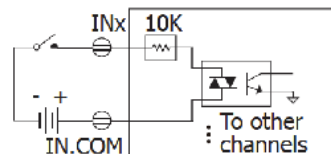
INPUT sink signal (Low=0)



INPUT sink signal (High=1)



INPUT source signal (Low=0)



OUTPUT relay



OUTPUT sink (resistive)



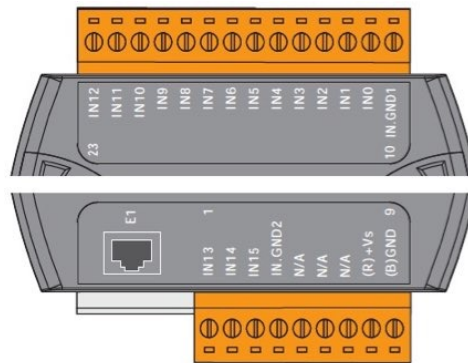
14.16. Data sheet digital I/O expansion-module (KIO7053)



Front



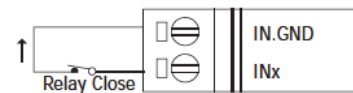
Back



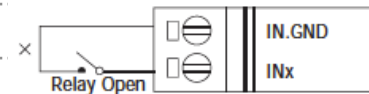
Pin assignment KIO7053

Description	Expansion module for connection to the AlarmManager-PRO. This module extends the external inputs of the AlarmManager on additional 16 digital alarm inputs. Communication is via Ethernet, so the module can be mounted anywhere. The configuration is done in the software interface of the AlarmManager-PRO. The module provides a build in web-server with for simple IP configuration and testing of the inputs and outputs without any additional software.
Connectivity	Connection to Kentix AlarmManager-PRO External Alarms of existing system equipment (HVAC, UPS systems, generators, alarm systems, etc.)
Configuration	Build in Web-Server (HTTP), Default IP: 192.168.255.1 (Admin/Admin)
Protocols	KAM-IO communication via IP-PORT: 502 (Default)
Security	ID, Password and IP-Filter
Terminals	Plug-able screw-terminal for cables up to 1mm ²
Inputs	Digital dry contacts for potential-free wiring ON: Open OFF: Close to GND
Isolation	Ethernet 1,5kVDC, I/O 3,7kVrms
Environment	Operation temperature -25°C to +75°C, Rel. humidity 10–90%
Network	LAN 10/100 Base-TX
Power supply	PoE (Class 1) or external power supply 12–30VDC, 4.3Watt
Chassis	72 x 123 x 35 mm (DIN-rail mounting)
Content of delivery	KIO7053, Power supply 24VDC, manual
Approvals	CE
Accessories	Power-supply or PoE injector if no PoE supply is available

INPUT dry contact (High=1)



INPUT dry contact (Low=0)



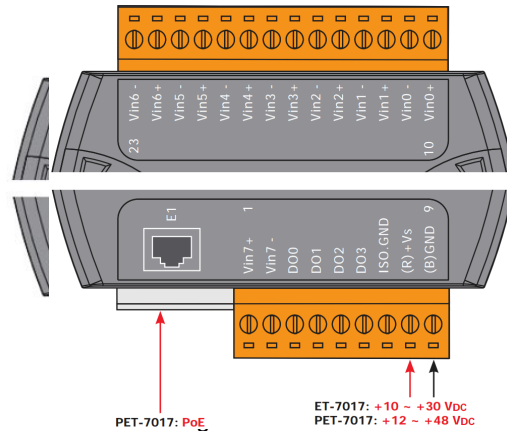
14.17. Data sheet analogue I/O expansion-module (KIO7017)



Vorderseite



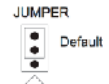
Rückseite



Klemmenbelegung KIO7017

Description	Expansion module for connection to the AlarmManager-PRO. This module extends the external inputs of the AlarmManager on additional 8 analogue alarm inputs. Communication is via Ethernet, so the module can be mounted anywhere. The configuration is done in the software interface of the AlarmManager-PRO. The module provides a build in web-server with for simple IP configuration and testing of the inputs and outputs without any additional software.
Connectivity	Analog sensors with active power (4–20mA) or Power outlet (0–10V)
AlarmManager	Connection to Kentix AlarmManager-PRO
Configuration	Build in Web-Server (HTTP), Default IP: 192.168.255.1 (Admin/Admin)
Protocols	KAM-IO communication via IP-PORT: 502 (Default)
Security	ID, Password and IP-Filter
Terminals	Plug-able screw-terminal for cables up to 1mm ²
Inputs	8 differentially analog inputs with 16 bit resolution Sampling rate 10 Hz and current input 0-10V or Power input 4-20mA, accuracy 0,1%
Isolation	Ethernet 1,5kVDC, I/O 3,7kVrms
Environment	Operation temperature 0°C to +45°C, Rel. humidity 10–90%
Network	LAN 10/100 Base-TX
Power supply	PoE (Class 1) or externes power supply 12–30VDC, 4.3Watt
Chassis	72 x 123 x 35 mm (DIN-rail mounting)
Content of delivery	KIO7017, 3m patch cable, Power supply 24VDC, manual
Approvals	CE
Accessories	Power-supply or PoE injector if no PoE supply is available

Current Input 0–10V



Power Input 4–20mA



14.18. Data sheet leakage sensor (KLS03, KLS03-ROPE10/20)

Connectivity	AlarmManager-BASIC (KAM-BASIC) AlarmManager-PRO (KAM-PRO) MultiSensor-RF (KMS-RF) (with KIO1 Power-Adapter) MultiSensor-LAN (KMS-LAN) MultiSensor-LAN-RF (KMS-LAN-RF)
Chassis sensor	Ni/Au, sensitivity 1ml water
Rope sensor	Conductive polymeric cable, sensitivity: 10ml water on 20cm length
LED	ALARM LEAKAGE (Red) STATE OK (Green)
Connectors	2 x RJ45 for standard patch cables
Power supply	Via Kentix system jack (RJ45)
Daisy chaining - linking	Up to 5 sensors, max. 50m combined cable length
Chassis	Material: PS 80 x 80 x 80 mm Weight: ca. 200g (KLS03), 0,75kg (KLS03-ROPE-10), 1kg (KLS03-ROPE-20) Color: RAL7035 Protection class: IP65
Cable glant	M20
Environment	Temperature -25°C - 70°C Humidity 5-85%, non condensing
Types	KLS03, KLS03-ROPE-10, KLS03-ROPE-20
Protection class	IP65
Content of delivery	10m patch cabel Additional fitting for chaining (Cable glant M20)
Approvals	CE



15. Checklist - Acceptance report

After the successful installation, we implicitly recommend to do a function-check of all components, to ensure the clean operation. For AlarmManager and MultiSensors the following check-list can be used. It can also be used as an acceptance report for the system handover to the customer.

IMPORTANT!

To ensure full functionality, we recommend to repeat this check periodically (about all 6 months).

AlarmManager-BASIC/PRO
☐ **Acceptance report**
☐ **Maintenance report**

Device	Function	
AlarmManager BASIC+PRO	Actual firmware version - check www.kentix.com	<input type="checkbox"/>
	All sensors / servers available in dashboard	<input type="checkbox"/>
	Actualization of sensor values in dashboard	<input type="checkbox"/>
	Arm/disarm switching (manual / time controlled)	<input type="checkbox"/>
	Vibration alarm from AlarmManager and MultiSensors (when used)	<input type="checkbox"/>
	E-mail / SMS alarming / Push notification	<input type="checkbox"/>
	External alarm inputs on AlarmManager	<input type="checkbox"/>
	External switching outputs AlarmManager	<input type="checkbox"/>
	SNMP functionality (trap sending, values in NMS)	<input type="checkbox"/>
	Network monitoring (Test by opening network connection)	<input type="checkbox"/>
	SMS Gateway	<input type="checkbox"/>
	Camera Recording (Test by triggering alarm)	<input type="checkbox"/>
		<input type="checkbox"/>
AlarmManager-PRO	IO-Module (In- / Outputs - test when used)	<input type="checkbox"/>
	Alarm forwarding to alarm control centers	<input type="checkbox"/>
		<input type="checkbox"/>
		<input type="checkbox"/>

 Date

 Customer

 Technical service

KeyPads / Leakage-sensor
☐ **Acceptance report**
☐ **Maintenance report**

Device	Place of installation	Function	
Keypad #1		Test arm/disarm	<input type="checkbox"/>
Keypad #2		Test arm/disarm	<input type="checkbox"/>
Keypad #3		Test arm/disarm	<input type="checkbox"/>
Leakage-sensor #1		Fluidity contact -> alarm trigger	<input type="checkbox"/>
Leakage-sensor #2		Fluidity contact -> alarm trigger	<input type="checkbox"/>
Leakage-sensor #3		Fluidity contact -> alarm trigger	<input type="checkbox"/>

MultiSensors

No.	Type	Place of installation	Temp./Humidity/Dewp	Motion	Carbon monoxide	Ext. alarm inputs	Ext. switching outputs	Measured temp.	Dashboard readings
			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
2			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
3			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
4			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
5			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
6			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
7			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
8			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
9			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
10			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

 Date

 Customer

 Technical service

16. Support

For technical questions about the products please contact our support team by e-mail or via the Kentix website. Send an e-mail with your questions and all the important details of your application and used versions to our support address.

KENTIX GmbH
Autenbornstrasse 2
D - 55743 Idar-Oberstein

support@kentix.com

The manual has been prepared with great care. The correctness and completeness of data, pictures and drawings is not guaranteed.

Regard to protected brand names and logos:

The use of protected trademarks, trade names, designs and brand logos in this manual is not a copyright violation, but serves as an illustrative reference. Even if these are not at the appropriate places marked as such, the relevant statutory provisions. The trade names and logos are the property of the manufacturer and subject to copyright laws. Information about that, please refer to the instructions of the manufacturers websites.

Copyright Notice:

All rights reserved. Any text, images, graphics, animations and videos as well as content and structure of this manual are protected by copyright and other laws protecting intellectual property. Your copy, modification, commercial use, use in other media or transfer to third parties is prohibited or requires the prior express permission of such KENTIX GmbH.