Security

This menu item can be used to configure security settings for access control and between wired Kentix devices.

General

To increase the security of communication between wired Kentix devices, a communication key can be entered. This means that communication between the devices is additionally protected by Kentix-specific encryption. The key must be the same on all communicating Kentix devices (main device and satellite devices).

Each user can be assigned their own PIN under the ACCOUNT MANAGER menu item. This allows bookings to be made on SmartAccess components with an integrated keypad with the user's corresponding authorizations. Greater security can be achieved by using a longer PIN. This can be set under this menu item from PIN length 4 to PIN length 10.

The DoorLock-RA4 rack lock only supports the digits 1 to 4.

RFID settings

The Kentix SmartAccess components use RFID tokens (Radio-Frequency Identification) for contactless access control. Each token is characterized by a globally unique UID (Unique Identifier) and encryption technology. The standard technology used is MIFARE®DESFire®.

Under KentixONE, you can now specify for each user whether and which RFID encryption should be used. If no encryption is used, the UID can be read and copied with any MIFARE®DESFire® reader. The UID then easily serves as the basis for cloning identification media, giving people access to areas they would not normally be allowed to enter. If you do not want to use encryption, this must be selected accordingly in the menu.

All SmartAccess components are supplied with Kentix-specific encryption as standard.

Only tokens delivered after 06/2018 contain the Kentix-specific encryption.

You can also use your own encryption. To do this, a configuration file must be uploaded to KentixONE. A template for the configuration file can be downloaded after selecting "Custom encryption".

Tokens with a Kentix-specific encryption cannot be used in conjunction with your own encryption.