

# Maxx Access Management System

e-Kontos 6000

User's manual

# Index

<b>Introduction</b> .....	2
<b>Lock Features</b> .....	2
<b>Using an RFID Keycard</b> .....	6
<b>Deadbolt and Privacy feature</b> .....	7
<b>Programming Locks</b> .....	8
<b>Low Battery Warning</b> .....	9
<b>Reset Lock to Factory Default Settings</b> .....	9

# Introduction

This manual is intended for people who program and troubleshoot locks. It covers the use of special keycards, programming and interrogating locks, and lock maintenance. Before reviewing this section, you should first become thoroughly familiar with the material covered in the Maxx Access Management System User's Manual. The e-Kontos is a grade 1 heavy duty electronic lock with the security afforded by using Maxx Access Management System for an offline access management solution. The lock accepts encrypted Mifare credentials for enhanced functionality to simplify the management of the lock.

## Lock Features

### **Automatic Inhibiting**

Normally, a guest room lock will be set up to operate with more than one guest keycard type (Guest, Alternate, backup, one shot). The lock is programmed to automatically activate inhibiting between these keycard types. When a new keycard is used from one of the types, it will prevent previously used keycards for the other keycard types from activating the lock.

### **Checkout Keycard**

The checkout keycard is used to prevent the current Guest keycards from entering a room. When this keycard is used in the lock the current keys of these types will not activate the locking mechanism. This feature prevents guests who have checked out of a room from later reentering the room, and is normally used by housekeeping after the room has been cleaned.

### **Block/Unblock Keycards**

These keys can be used to temporarily prevent a specific key ID from accessing a lock or multiple locks. A specific key ID can be blocked allowing remaining key ID's in the same key group to remain functioning. The block and unblock key can be assigned to both guest and master level key groups.

## **Passage mode schedules**

A lock can be programmed to automatically unlatch or latch at specified times for each day of the week. A keycard is not required to perform the unlatching and latching activities. When a lock is unlatched, a key is not required to open the door. The lock may have up to three different unlatch/latch times per week.

## **Passage mode**

A keycard can be programmed to latch and/or unlatch the lock. When a lock is unlatched, a keycard is not required to open the door. If a keycard is used, the lock will display the normal lights and will function normally. When the lock is once again latched, a valid keycard is required to release the locking mechanism.

## **Dead Bolt/Privacy Override**

Each type of keycard can be programmed to indicate whether or not it will override the dead bolt/privacy function. Usually, one emergency keycard type is programmed with the capability, and is used only in emergency situations.

## **Block only/Block except**

When this feature is set, the lock will be electronically locked from the outside, and valid keycards will be unable to activate the lock. The indicated type(s) of keycard will be affected by the block only/block except keycard. Two levels are available, and there can be one keycard to lock out only one type of keycards and another to lock out all types of keycards except one.

## **Internal Clock and Calendar**

The lock contains a clock crystal that maintains actual date and time. The time is updated every minute and the crystal automatically adjusts for changes due to daylight savings and leap year.

## **Time zone in keycards**

Certain personnel keycards can be programmed to work only during certain hours of the day. When the keycard is made, the user specify the start and end times of the shift. A keycard can have only three shifts specified. If the keycard is used outside the shift times, it will not work.

## **One shot**

A guest keycard type can be programmed to limit the number of times a valid keycard will activate the lock to one use. This determination is made in advance, and the number of times the keycard will work cannot be varied. You can also program a keycard expiration date and time when a keycard is made. The keycard will cease to activate the lock when it has been used or when it expires at the specified date and time, whichever comes first.

## **Areas**

This feature is used for special locks such as pool doors, elevators or limited access doors. Locks can be programmed as areas allowing certain keycards with permissions to activate the locking mechanism. This permissions to the areas can be selected during the creation of the keycards. Both, personnel and guest keycards can have permissions to areas.

## **LED indicators**

If a keycard does not work in a lock the light indicators to display the red LED that indicates the keycard did not work. If the keycard is a valid keycard, the indicator lights will display the green LED and the keycard will work normally. LED can also be used to display a lock that has the privacy function activated.

## **Low Battery**

If the lock's batteries are low a red indicator light will flash when a correct keycard is used before displaying the green LED and unlocking.

The low battery indicator will only be displayed when a personnel keycard is used and will not affect guest keycards.

## **Property entries**

This feature is used for special locks such as perimeter entrances, elevators or limited access doors. Locks can be programmed as property entries which allow valid keycards to activate the locking mechanism. This feature can be programmed in several ways: Hotel gate – These locks will allow any keycard made at the property to function in the locks. Building gate –These locks will allow any keycard made for the specified building to function in the locks. Floor gate –These locks will allow any keycard made for the specified floor to function in the locks. The feature is programmed and functions automatically without requiring the users to set any permissions on keycards.

## **Audit Trail**

Audit trail determines which keycard was used, when an access occurred, who owned the keycard at the time of access and what action was performed. Audit trail is stored in the lock's nonvolatile memory. Displayed in the Maxx Access software in order of most recent event.

**Encryption** - All the data that is written on the keycards is encrypted and can only be read by the Maxx Access software. Also each property will have its own encrypted code to prohibit keycards of working from one property to another.

**MIFARE** - Type of technology used for contactless smart card systems. MIFARE is compliant with the international ISO 14443 Type A standard.

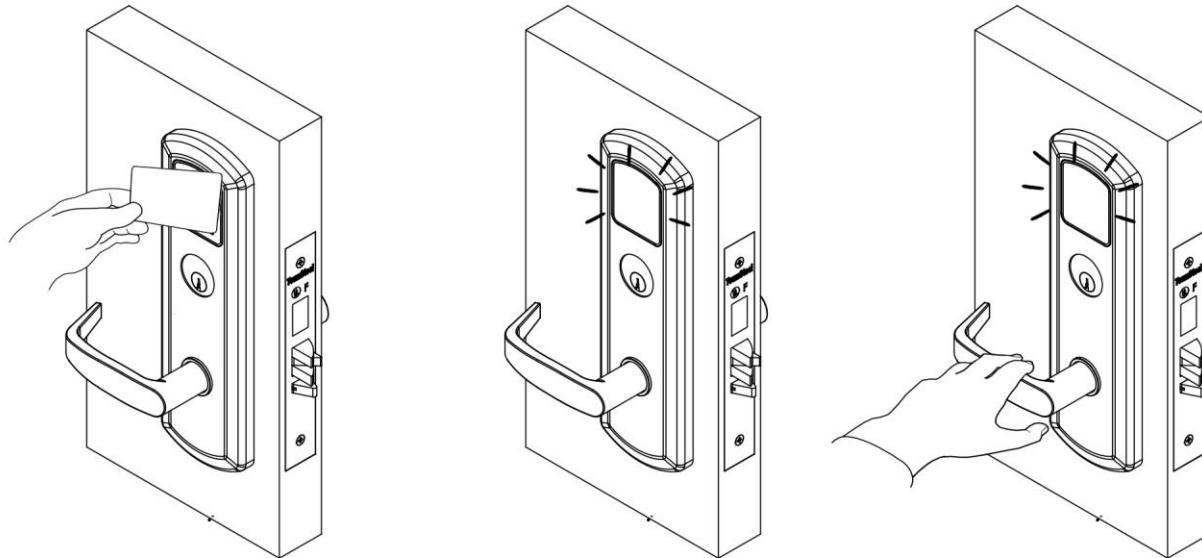
## **Authorization**

Used to register or change the property code when installing the Maxx Access Management System, or if a severe security problem has occurred. The authorization keycard initializes the lock during a first-time installation. After first-time installation the authorization card prepares the lock for communication with parameter cards or DLP device.

**Door Lock Programmer (DLP)** - A handheld device containing the Maxx Access database information downloaded from the system. The DLP is used to program and audit locks and card readers.

## Using an RFID Keycard

1. Bring the flat surface of your keycard near the circular or rectangular RFID reader. When the keycard is close enough to be read, the green LED will flash on the RFID reader. You will hear the lock operate.
2. The green light will begin to flash once access has been granted.
3. Turn the lever and open the door while the green LED is on.



## Deadbolt and Privacy feature

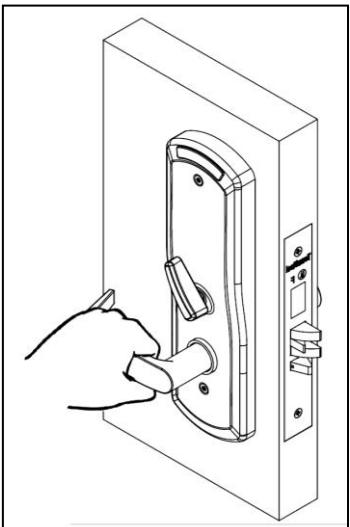
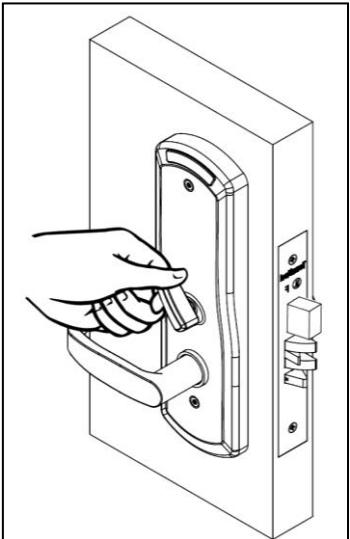
Additionally to the electronic features, the lock is also equipped with a deadbolt. That can be thrown from the inside of the room. The deadbolt is set by turning the deadbolt latch to the locked position.

When the deadbolt is in the locked position, a flashing red LED will appear every 15 seconds. If a keycard is used on the reader a red LED will flash and beep, and the door will remain locked. A keycard with the override option enabled will produce a green LED and will override the deadbolt and allow access to the room.

To unlock the lock from the inside while the deadbolt is thrown, turn the door handle. This action will retract both the latch and the deadbolt.

Select models of the e-Kontos have an automatic deadbolt feature that automatically projects the 1" deadbolt when the door is closed. This feature provides latching security against forced entry. Keycards require to have the DND override option enabled in order to gain access.

To open the door from the inside after the deadbolt has been thrown, simply depress the door handle. This action will override the privacy feature and allow the guest to exit.



## Programming Locks

When the locks are shipped from the factory, the batteries are not installed. The locks will be fully functioning when four AA batteries are installed on a lock. After installing the batteries the locks will only be operable via construction cards since all locks are initially on factory default settings. To program the locks to accept other keycards, you must use the **Door Lock Programmer (DLP)**, along with the computer that has the Maxx Access Client.

### Door Lock Programmer

The Door Lock Programmer is a handheld device containing the Maxx Access database information downloaded from the system. The DLP acts an interface between the lock and the Maxx Access Client and is used to enter lock code information directly from the computer into the lock. It is also used to interrogate locks and obtain an audit trail of keycards that were used in the lock, lock status information and keycard information.

The DLP connects to the computer and downloads information using a micro-USB mini-b cable. The DLP communicates with the locks using NFC communication.

### Programming locks using the Door Lock Programmer

To program the locks using the DLP, you must first download the database information from the Maxx Access Client. For more information regarding downloading the database information please review the Maxx Access Management System User's Manual.

Once the database information is downloaded from the client to the DLP, you can disconnect the DLP from the cable and transport the DLP to the lock.

In order to program the lock you will need to have the Authorization keycard that was delivered with your copy of the Maxx Access Management System. Follow the steps for lock programming:

From the DLP's main menu, select option 2. Lock Functions. Four new options will appear onscreen, select 1. Program Room. The list of possible room numbers that can be programmed into the lock will appear. These room are based off of the user's database information that was downloaded into the DLP. Select the room number and press set and follow the onscreen instructions

## **Setting Date and Time**

The lock's embedded system maintains the actual date and time. The time is automatically updated every minute and the clock is automatically adjusted for changes due to Daylight Saving Time, and Leap Year. The date and time are initially updated when the DLP is used to program the door lock and it is updated when the DLP is used to interrogate the lock for audit trials. The time can be manually updated using the DLP if there are any changes needed.

For example: if the lock's batteries are disconnected for a period of time.

If the lock experiences a low battery condition.

If the lock's clock has not been updated via the DLP for a 12-month period.

## **Low Battery Warning**

Each lock contains batteries, which are used to power the lock's circuit board and to release the locking mechanism. The lock uses four AA alkaline batteries. Lithium batteries although long lasting, are not recommended to be used due to their lower voltage output.

The lock's batteries may need to be replaced when one of the following symptoms appear:

- A Standard keycard alternately flashes the red LED 5 times before the green LED flashes on the RFID reader and the lock operates.
- The DLP report indicates that the batteries are low.

If the low battery warning is displayed follow the step-by-step procedures for replacing lock batteries on each type of lock are provided in the Lock Installation Manual.

## **Reset Lock to Factory Default Settings**

### **Steps**

1. Bring the flat surface of your Authorization keycard near the circular or rectangular RFID reader. When the keycard is close enough to be read, the green LED will flash on the RFID reader and beep.
2. Leave the Authorization keycard in that same position for 7 seconds. The green LED will remain solid on the RFID reader and the lock will beep two more times.

**CAUTION: RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.**

**FCC Warning:**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- o Reorient or relocate the receiving antenna.
- o Increase the separation between the equipment and receiver.
- o Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- o Consult the dealer or an experienced radio/TV technician for help.

**Caution:** Any changes or modifications to this device not explicitly approved by manufacturer could void your authority to operate this equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

The device has been evaluated to meet general RF exposure requirement. The device can be used in portable exposure condition without restriction.

*Visit [www.TownSteel.com](http://www.TownSteel.com) for more.*

17901 Railroad Street  
City of Industry, CA 91748

Toll Free: 877-858-0888

Tel: 626-965-8917

Fax: 626-965-8919