

# USER MANUAL

## CM1000 EMV

CM1000 EMV is a flexible keypad and Mifare reader in one unit for many different applications. This device supports EMV (Europay, MasterCard, and Visa) cards or mobile wallets as access control devices (not payment transactions supported).

Mykey - Art. Nr: 480040 (black), 480042 (white)  
Classic - Art. Nr.: 482040 (black), 482041 (white)

[www.conlan.eu](http://www.conlan.eu)


## CM1000 EMV

**CONLAN**

A **SALTO** GROUP COMPANY



# CONTENT

<b>1. Installation</b>	Page 3
<b>2. Access</b>	Page 3
2.1 Using the device	Page 3
<b>3. Fixed user PIN codes management</b>	Page 4
3.1. Adding user PIN codes	Page 5
3.2 Adding NFC tags	Page 5
3.3 Deleting user PIN codes and NFC tags	Page 6
3.4 Assigning an Output behavior for a user	Page 7
3.5 Smart enroll	Page 9
<b>4. Configuration</b>	Page 10
4.1 Change User Configuration code	Page 10
4.2 Change Service Configuration code	Page 11
4.3 LED's and Buzzer Feedback Configuration	Page 12
4.4 Outputs Configuration	Page 13
4.4.1 Configuring Output activation time	Page 14
4.4.2 Configuring Output activation flank	Page 15
4.5 Special functions	Page 17
4.5.1 Service Configuration Code Timeout	Page 17
4.5.2 Change User Configuration Code without Service Configuration Code	Page 17
4.5.3 Mute	Page 18
4.5.4 exBuzzer Function	Page 18
4.5.5 Software Enable High Security Function	Page 18
4.5.6 Bell Key  Function	Page 18
4.6 High Security	Page 19
4.7 Backup Card	Page 19
4.7.1 Cloning	Page 20
4.7.2 Loading	Page 20
<b>5. Hardware factory reset</b>	Page 21
<b>6. REX Input</b>	Page 22
<b>7. Technical specifications</b>	Page 22

# 1. INSTALLATION

For instructions on the installation, please check the installation guide.

## 2. ACCESS

The keypad is totally Stand Alone and can grant access to open a lock by inserting a custom user PIN code or swiping a NFC tag or EMV (Europay, MasterCard, and Visa) cards.

### 2.1. Using the device

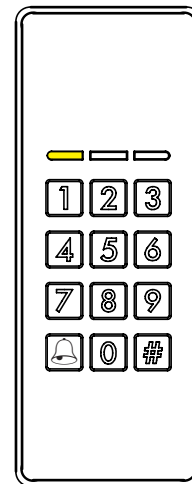
User PIN's and NFC tags ID's are allocated in the internal device memory. The CM1000 can retain up to 190 fixed codes from 1 to 8 digits long or NFC tag ID's. Each individual user has their own PIN code or NFC tag to operate the lock. This permits also to share one lock between different users.

1234 is a default fixed PIN code configured at position 1 under fabrication and can be used to test the device. Check '3. Fixed User PIN Codes and NFC Tags Management' section at page 4 to manage the fixed PIN's and NFC Tags.

#### Idle State

The yellow light is always ON in idle state, the keypad is waiting for a user interaction.

Back-lights are OFF as default, but turns on when a key is touched.



#### Opening and Closing

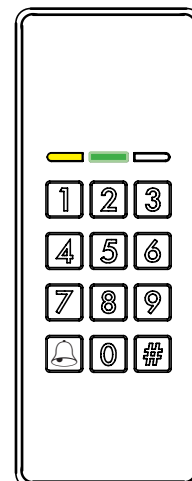
Example: **1** **2** **3** **4** **#**

OR

Swiping a valid NFC card



Upon entering a **VALID** user PIN code, or swiping a **VALID** NFC tag, a confirmation beep will sound and the green LED will blink one time. Output2 is activated.

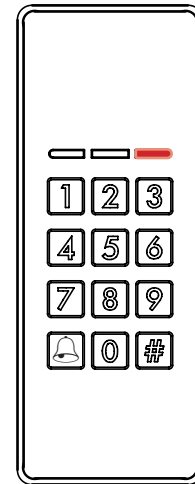


### Wrong Code

Example: **0 0 0 0 #**

OR

Swiping a wrong NFC card



In case of **WRONG** code inserted or swiping an **INVALID** NFC tag, a rejection beep will sound and the Red LED will blink one time.

**After 4 successive wrong tries, the keypad will lockout for 60 seconds.**

## 3. FIXED USER PIN CODES AND NFC TAGS MANAGEMENT

User PIN codes and NFC tags can be changed, added, and deleted. Each user PIN code or NFC tag is stored in a specific addressed internal memory position (from 1 to 190). We recommend to keep a record of the position numbers and user names to future management.

To add or delete user PIN codes or NFC tags, is necessary to access the User Configuration Menu:

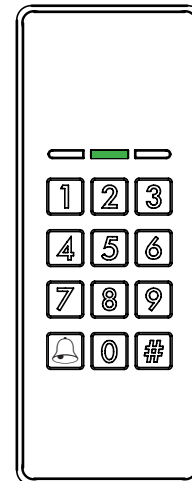
### User Configuration Menu

Insert the User Configuration Code  
(4711 is factory default)

Enter: **4 7 1 1 #**

The yellow LED will turn OFF and the green LED will turn ON.

The keypad is ready to add or delete fixed user PIN's.



Example of user tracking:

Position	User	PIN
1	Carlos	148954
17	Torbjörn	94830132
23	Juan	1111

The next sections uses Juan as example to add and delete fixed PIN codes on the device.

### 3.1 Adding user PIN codes

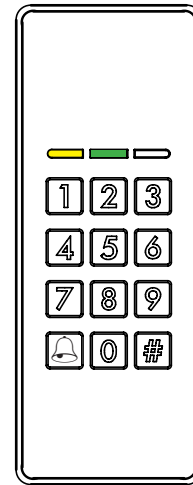
To add users, first insert a position to place the new PIN code (between 1 and 190).

Example: **2** **3** **#**

If a valid position is inserted, the yellow and green LED's will light solid until the fixed user PIN code is entered. The fixed user PIN must be a number of 1 to 8 digits.

Example: **1** **1** **1** **1** **#**

All positions can be overwritten, so be aware to keep a register of all the configured PIN codes and their positions.



Note that the first 9 positions must always be inserted as one digit numbers, without a zero '0' in front. It means, insert '1' not '01', insert '2' not '02', etc. Numbers that starts with zero '0' are reserved to Special functions (check 4.5 Special Functions, page 17).

### 3.2 Adding user NFC tags

To add users, first insert a position to place the new NFC tag (between 1 and 190).

Example: **2** **3** **#**

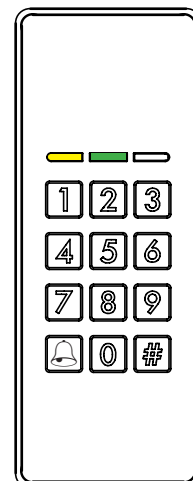
If a valid position is inserted, the yellow and green LED's will light solid until a valid NFC card is swiped in front of the reader.

Swiping a valid  
NFC card



A confirmation beep will sound, once if a normal Mifare NFC tag is registered, twice if a EMV (Europay, Master-Card, and Visa) card is registered.

All positions can be overwritten, so be aware to keep a register of all the configured PIN codes and their positions.



### 3.3 Deleting user PIN codes and NFC tags

Deletion is a simple process that can be performed just by knowing the PIN code(s) or NFC tag(s) position to be deleted.

#### Deleting a specific PIN code or NFC tag

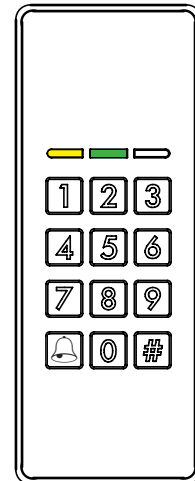
Insert the position of the user PIN or NFC tag that you want to delete (a number between 1 and 190).

Example:

If a valid position is inserted, the yellow and green LED's will light solid until the deletion is confirmed. Push # to confirm the deletion

Enter:

The keypad go back to User Configuration Menu and is ready to perform another user PIN handling action.



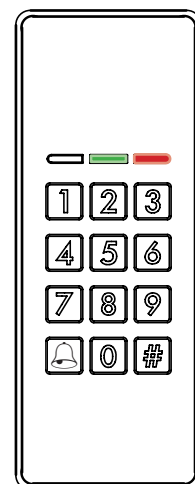
#### Deleting all user PIN codes and NFC tags

Insert 2500, to clear the user PIN's memory on the device.

Enter:

The red and green LED's will blink. All the stored PIN codes are now deleted.

The keypad go back to User Configuration Menu and is ready to perform another user PIN handling action.



### 3.4 Assigning an Output behavior for a user

When adding users to the device, it is possible to specify the corresponding Output behavior for every specific PIN code or NFC tag.

There are four configurable Output modes:

**Normal Mode:** The inserted PIN code or NFC tag, changes the corresponding Output state to **Active** and remains in this state until the configured Output Timeout (4.4.1 Configuring Output activation time, page 13) expires. The output then changes its state to **Inactive**.

All user PIN codes or NFC tags are configured in Normal Mode as default.

**Toggling Mode:** The inserted PIN code or NFC tag, changes the corresponding Output state to **Active** and remains in this state until a new or the same valid PIN code or NFC tag, configured in Toggling Mode, is used again; the Output then changes state to **Inactive**. The Output toggles its state every time a PIN code or NFC tag configured as Toggling Mode is used.

To configure a PIN code or NFC tag with this Output Mode, add the same PIN code or NFC tag at the same position **twice**.

**Switch Only to Active Mode:** The inserted PIN code or NFC tag, changes the corresponding Output state to **Active** and remains in this state.

To configure a PIN code or NFC tag with this Output Mode, add the same PIN code or NFC tag at the same position for **three times**.

**Switch Only to Inactive Mode:** The inserted PIN code or NFC tag, changes the corresponding Output state to **Inactive** and remains in this state.

To configure a PIN code or NFC tag with this Output Mode, add the same PIN code or NFC tag at the same position **four times**.

Example: Configuring a NFC tag to **Toggling Mode**.

To add users, first insert a position to place the new NFC tag (between 1 and 190).

Example:

If a valid position is inserted, the yellow and green LED's will light solid until a valid NFC card is swiped in front of the reader.

Swiping a valid NFC card



A confirmation beep will sound, once if a normal Mifare NFC tag is registered, twice if a EMV (Europay, Master-Card, and Visa) card is registered.

The keypad go back to User Configuration Menu.

Insert the same position again.

Example:

If a valid position is inserted, the yellow and green LED's will light solid until a valid NFC card is swiped in front of the reader.

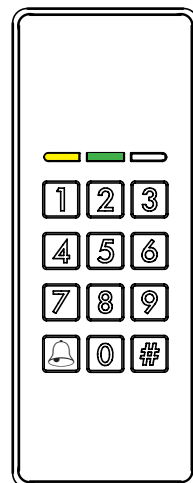
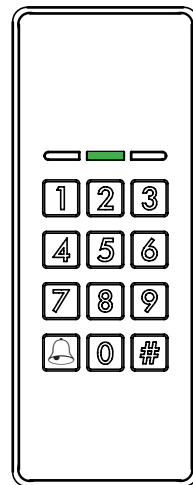
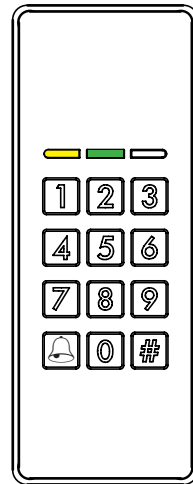
Swiping the same valid NFC card again



A confirmation beep will sound, once if a normal Mifare NFC tag is registered, twice if a EMV (Europay, Master-Card, and Visa) card is registered.

The keypad go back to User Configuration Menu.

Now, this NFC card **Toggles** the corresponding Output every time it is used.





### 3.5 Smart enroll

This function can help when a large number of NFC tags or PIN codes needs to be registered at the same time.

Smart Enroll allows the PIN code or NFC card registration without specify a memory position for every enrollment. It means, just an initial position is needed and all the subsequent registrations are placed automatically at the consecutive next memory position.

Enter: 0 5 #

The yellow LED blinks and the green LED remains ON, the device is waiting for a start position.

To start users enrolling, first insert a start position to place the first PIN code or NFC tag (between 1 and 190).

Example: 2 3 #

If a valid position is inserted, only the yellow LED starts to blink until a user PIN code is entered or a NFC card is swiped (the fixed user PIN must be a number of 1 to 8 digits).

Example: Swiping a valid NFC card



The green LED blinks once, the NFC card is registered at position 23.

Example: Swiping another valid NFC card



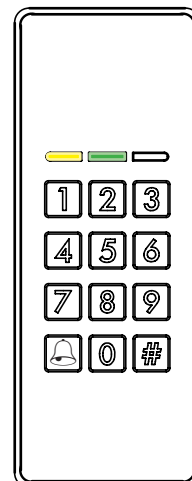
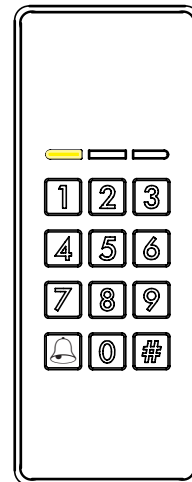
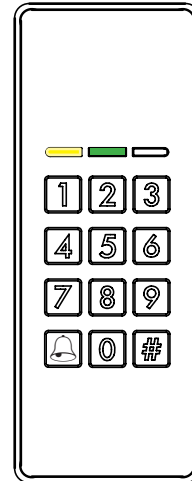
The green LED blinks once, the NFC card is registered at position 24.

Example: Swiping another valid NFC card



The green LED blinks once, the NFC card is registered at position 25.

⋮



## 4. CONFIGURATION

The service configuration code is used to authenticate and access the configuration menu, which is needed to configure the CM1000.

**It is possible to access the Service Configuration Menu within the first 60 seconds after the device has been powered up (connected to a power supply). After this time, the Service Configuration Menu is inaccessible.**

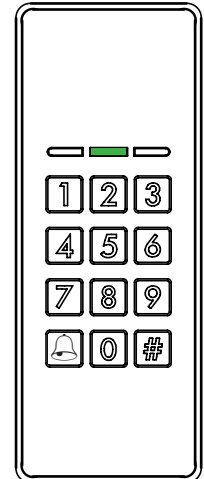
### Service Configuration Menu

**Just after the device has been powered up**, insert the Service Configuration Code (12347890 is factory default)

Enter:



The green LED will turn ON.  
The keypad is now ready to be configured.



Once in Service Configuration Menu, the following actions can be performed:

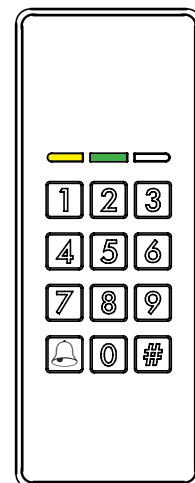
### 4.1 Change User Configuration Code

Enter:   

The yellow and green LED will light solid. The keypad is ready to receive a new User Configuration Code. Insert a code that is between 1 to 8 digits.

Example:     

The User Configuration Code has been changed. The keypad go back to User Configuration Menu and is ready to perform another Service Configuration action.



## 4.2 Change Service Configuration Code

Enter: **0** **1** **#**

The yellow and green LED will turn ON. The keypad is ready to receive a new Service Configuration Code. Insert a code that is between 1 to 8 digits.

Example:

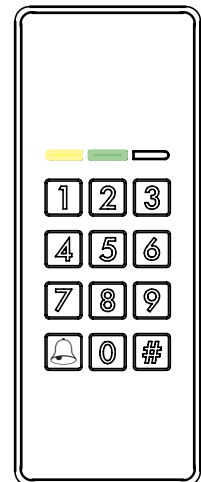
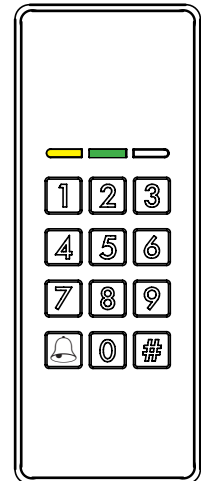
**1** **2** **3** **4** **7** **8** **9** **0** **#**

The yellow and green LED will blink until the new Service Configuration Code is inserted again to confirm the action.  
Insert the same code again.

Example:

**1** **2** **3** **4** **7** **8** **9** **0** **#**

The Service Configuration Code has been changed. The keypad go back to User Configuration Menu and is ready to perform another Service Configuration action.



### 4.3 LED's and Buzzer Feedback Configuration

Light indications can be customized for the following three device states:

**Idle:** Device normal state, nothing to perform, waiting for user interaction. The LED(s) remains in this state until a user interaction is detected.

**Access Granted :** Feedback when a valid PIN code or NFC tag is used to grant access. The LED(s) and buzzer audio indication, remains in this state as long as the Output is Active.

**Key Touched:** Feedback when a key is touched. Buzzer audio indication and LED(s) remains in this state (blinks) for 500ms.

To customiz the LED indications first insert:

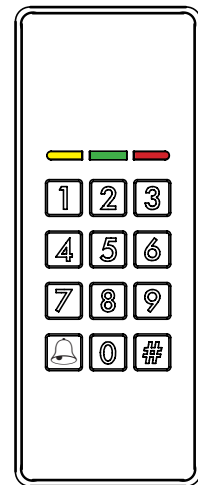
Enter:

All three LEDs will turn ON until a device state to configure is selected:

Enter:   to configure **Idle** user feedback

Enter:   to configure **Access Granted** user feedback

Enter:   to configure **Key Touched** feedback



The device shows the selected state LED's feedback, and for **Access Granted** and **Key Touched** states, also the Buzzer feedback by a constant beep if it's not muted. Now it is possible to customize the state feedback.

To customize a selected state, use the keys 1, 2 and 3 to turn ON or OFF the Yellow, Green and Red LED's respectively. Besides, the buzzer behavior can also be customized for the **Access Granted** and **Key Touched** states by using the key 0, if the buzzer is not muted in this state, a constant beep can be heard.

Use the corresponding key to turn ON or OFF the wanted LED or Buzzer

Values for LED selection:	1	2	3	0
LED's				

Enter:  When the customization is done, push # to save the configuration

The LED indications has been changed. The keypad go back to LED's and Buzzer Feedback Configuration menu, and is ready to chose another state to be customized.

## 4.4 Outputs Configuration

When a valid PIN or NFC tag is used, the corresponding Output (Output1 or Output2) is Activated (GND) for a defined period of time (5 seconds as default). The Output assigned for a user is defined by a User Output Assignment Array with 190 available positions.

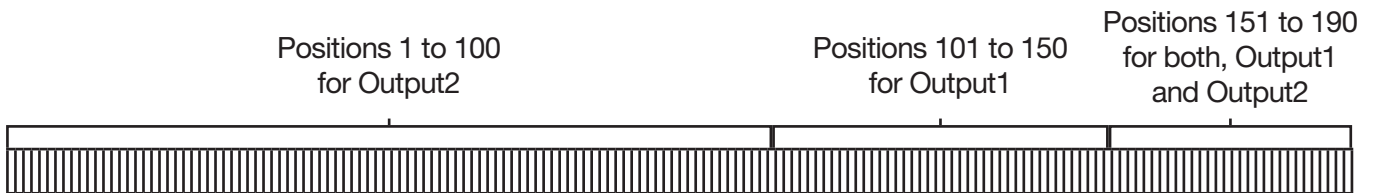
There are 3 configurable parameters for an output:

**Activation time:** 5 seconds as default, but configurable up to 61 hours.

**Activation Flank:** GND as default, the 'polarity' which the output changes to when active. There are only two options:

	Idle State	Active State
Normal	Floating (not connected)	GND
Inverted	GND	Floating (not connected)

**User Output Assignment Array:** As default this array looks like follows:



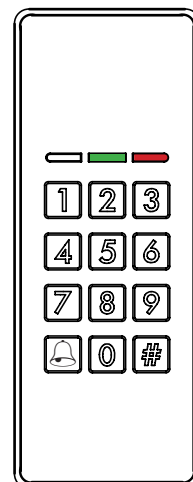
What this User Output Assignment Array means is:

- If a user PIN or NFC tag is registered in a position between 1 and 100 (as default), Output 2 is activated every time this PIN or NFC tag is used to grant access.
- If a user PIN or NFC tag is registered in a position between 101 and 150 (as default), Output 1 is activated every time this PIN or NFC tag is used to grant access.
- If a user PIN or NFC tag is registered in a position between 151 and 190 (as default), both, Output 1 and Output 2 are activated as the same time every time this PIN or NFC tag is used to grant access.

To manage all those configurations:

Enter:

The green and red LED's will light solid until a parameter to be configured is inserted



#### 4.4.1 Configuring Output activation time

Enter: **1** **#** For Output 1

OR

Enter: **2** **#** For Output 2

The yellow LED will turn ON and remain in this state until a time in **hours**, from 0 to 60, is inserted.

Example,  
Configuring 0 hours  
Activation Time: **0** **#**

The green LED will turn ON and remain in this state until a time in **minutes**, from 0 to 60, is inserted.

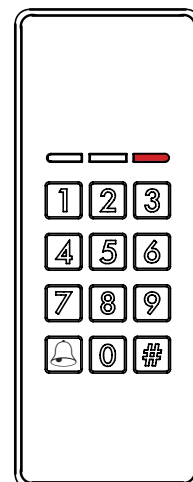
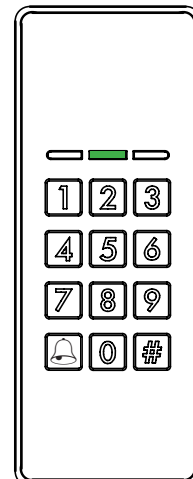
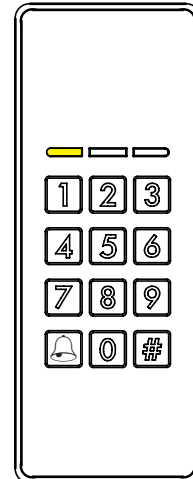
Example,  
Configuring 0 minutes  
Activation Time: **0** **#**

The red LED will turn ON and remain in this state until a time in **seconds**, from 0 to 60, is inserted.

Example,  
Configuring 15 seconds  
Activation Time: **1** **5** **#**

The selected Output is configured to remain Active for 15 seconds when a valid PIN code or NFC tag is used to grant access.

The keypad go back to Outputs Configuration Menu and is ready to perform another action.





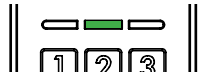

#### 4.4.2 Configuring Output activation flank

Enter: **5** **#**

THEN

Enter: **1** To toggle Output1  
Activation Flank  
OR

Enter: **2** To toggle Output2  
Activation Flank

	Normal	Inverted
Enter: <b>1</b> To toggle Output1 Activation Flank		
Enter: <b>2</b> To toggle Output2 Activation Flank		

Enter: **#** When the customization is done  
to save the configuration

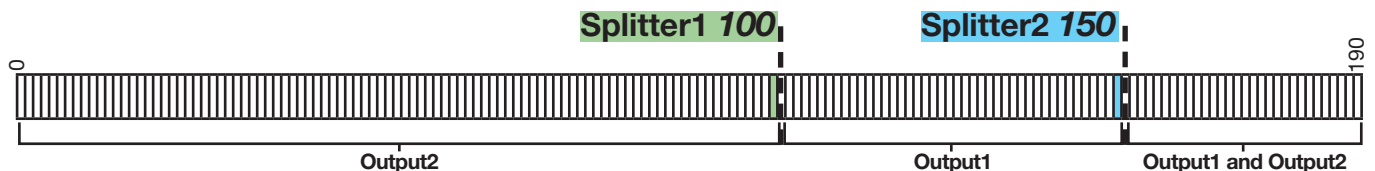
The keypad go back to Outputs Configuration Menu and is ready to perform another action.

#### 4.4.3 Configuring User Output Assignment Array

This function uses a User Output Assignment Array to assign a defined Output to a group of user PIN's or NFC tags.

We assume the User Output Assignment Array is separated in user groups by two **Splitter**:

- **Splitter1**: All users registered at positions behind it, inclusive the **Splitter1** itself activates Output2.
- **Splitter2**: All users registered at positions behind it, inclusive the **Splitter2** itself, and back to the **Splitter1**, activates Output1. Besides, all users registered at positions in front of the **Splitter2** up to the last position of the array (position 190), activates both, Output1 and Output2, at the same time.



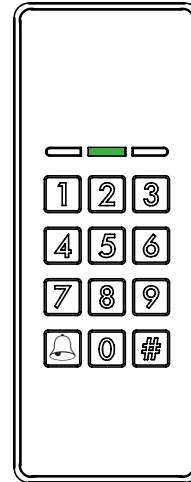
In this example, all users from 0 to 100 activates Output2, all users from 101 to 150 activates Output1 and all users between 151 and 190 activates both, Output1 and Output2.

Note that **Splitter2** value must always be greater than **Splitter1** value, otherwise, the configuration will be rejected and an error beep will sound.

Example: Configuring users from 1 to 50 to activate Output2, users from 51 to 100 to activate output1 and the remaining positions to activate both Output1 and Output2:

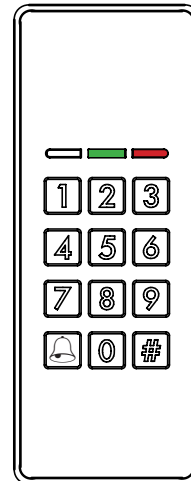
Enter: **4** **#** For Splitter 1

The green LED will turn ON and remains in this state until **Splitter1** position is inserted.



Example: **5** **0** **#**

The Splitter1 has been set. The keypad go back to Outputs Configuration menu, the red and green LED's turns ON and is ready to chose another parameter to be customized.

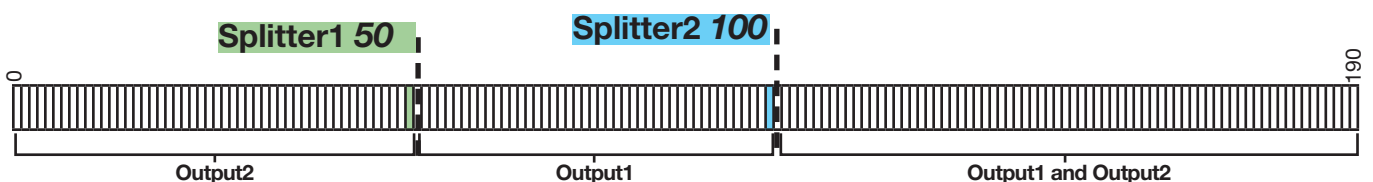
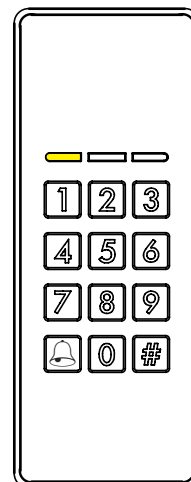


Enter: **3** **#** For Splitter 2

The yellow LED will turn ON and remains in this state until **Splitter2** position is inserted.

Example: **1** **0** **0** **#**

The Splitter1 has been set. The keypad goes back to Outputs Configuration menu. The User Output Assignment Array has been configured as follows:






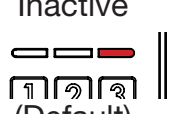
## 4.5 Special functions

Enter: **0** **4** **#**

Six options can be chosen, every time an option key is touched, the configuration toggles its state between ON/Active and OFF/Inactive:



### 4.5.1 Service Configuration Code Timeout

As default, the Service Configuration Menu can be accessed only for the first 60 seconds after the device is powered. If this configuration is turned OFF, the timeout is ignored and the Service Configuration Menu can be accessed anytime.

Enter: **1** ||  ||  ||  
(Default)

### 4.5.2 Change User Configuration Code without Service Configuration Code

Allows to change the User Configuration Menu Code under User Configuration Menu in stead of only under Service Configuration Menu.

Enter: **2** ||  ||  ||  
(Default)

Example when this option is enabled. First, access User Configuration Menu

Insert the User Configuration Code (4711 is factory default)

Enter: **4** **7** **1** **1** **#**

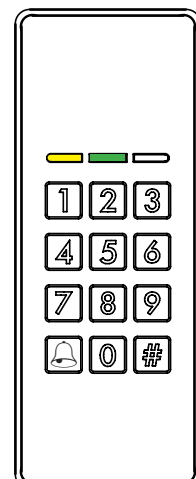
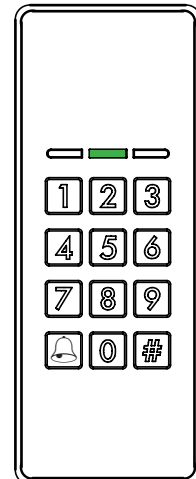
The yellow LED will turn OFF and the green LED will turn ON.  
The keypad is ready to add or delete fixed user PIN's.

Enter: **0** **0** **#**

The yellow and green LED will light solid. The keypad is ready to receive a new User Configuration Code. Insert a code that is between 1 to 8 digits.

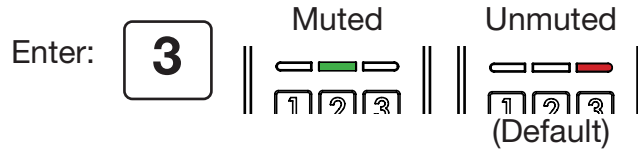
Example: **4** **3** **2** **1** **#**

The User Configuration Code has been changed. The keypad go back to User Configuration Menu and is ready to perform another Service Configuration action.



### 4.5.3 Mute

Used to mute (buzzer OFF) or unmute(buzzer ON) the device.



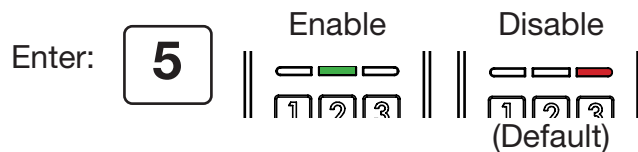
### 4.5.4 exBuzzer Function

This wire is used to activate the buzzer on the device externally, by connecting exBuzzer input (brown wire) to GND. Besides, it can be configured to physically enable or disable a High Security function (check High Security Function at page 19).





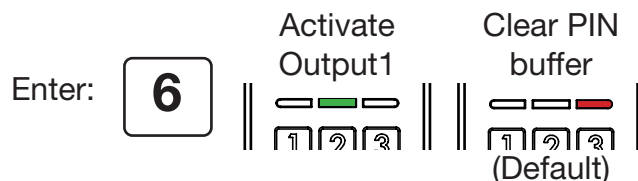
### 4.5.5 Software Enable High Security Function

Enables the High Security Function as mandatory, it means, independent of exBuzz (brown wire), (check High Security Function at page 19).



### 4.5.6 Bell Key Function

When this option is enabled, the Bell Key  activates Output1 (no PIN code required).  
When disabled, the Bell Key  function is just to clear the PIN buffer.



When the customization is done, use # to save the configuration:






The keypad go back to Outputs Configuration Menu and is ready to perform another action.

## 4.6 High Security

This function improves devices security by requiring 2 authentications before to activate an Output. PIN codes, NFC tags or a combination of both can be used as authentication pair.

This function, also affects the user registration procedure, that is mandatory to register PIN's or/ and NFC tags to grant a unique user access. **The positions used to registration must be always consecutive for every user:**

User	Position	PIN Code/ NFC tag	Case
Carlos	1	148954	Carlos may insert a PIN code and swipe a NFC card to grant access.
	2		
Torbjörn	15	94830132	Torbjörn may insert two PIN codes to grant access.
	16	1111	
Juan	101		Juan may swipe two NFC cards to grant access.
	102		

This special function can be activated by software, in which case is always mandatory to use two authentication methods (check 4.5.5 Software Enable High Security Function at page 18). Or by hardware in which case the exBuzzer input must be connected to GND to activate the function (check 4.5.4 exBuzzer Function at page 18).

## 4.7 Backup Card

In case of use the same configuration, user PIN codes and NFC tags, for different devices, is possible to 'clone' a main configuration from one device to another by using a Conlan Backup card (Art. No.: 480080).

To clone a configuration:

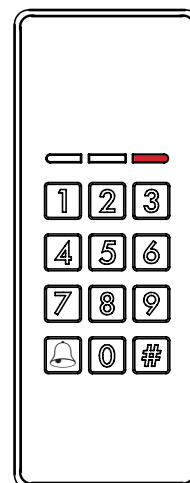
Enter:

The red LED's will light solid until an option is chosen.

For Clone

OR

Enter:   For Load



### 4.7.1 Cloning

It is possible to clone a CM1000 configurations or all registered users PIN codes and NCF tags, or both, making a total copy of the original CM1000.

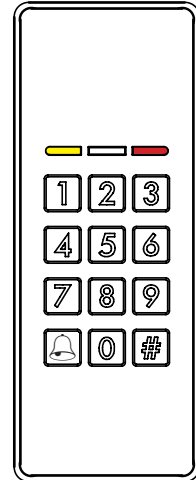
Enter: **1** **#** For Clone

The yellow and red LED's will light solid until an option is chosen.

Enter: **1** **#** To Clone ALL  
OR

Enter: **2** **#** To Clone PIN codes and NFC tags register  
OR

Enter: **2** **#** To Clone CM1000 configurations



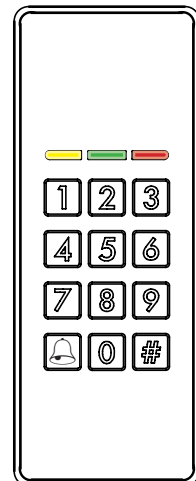
All LED's will blink until a Conlan Backup Card is held in front of the reader.

Holding a Conlan Backup Card in front of the reader.



If the information is successfully cloned, a confirmation beep will sound.

A Conlan Cloning card is made with the current CM1000 reader configurations and/or users register.



### 4.7.2 Loading

To load information from a Conlan Backup Card:

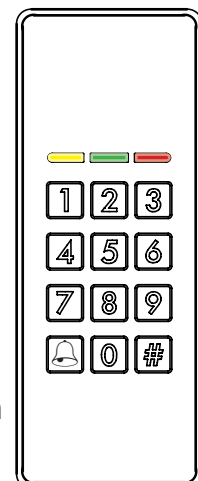
Enter: **2** **#** For Load

All LED's will blink until a Conlan Backup Card is held in front of the reader.

Holding a Conlan Backup Card in front of the reader.



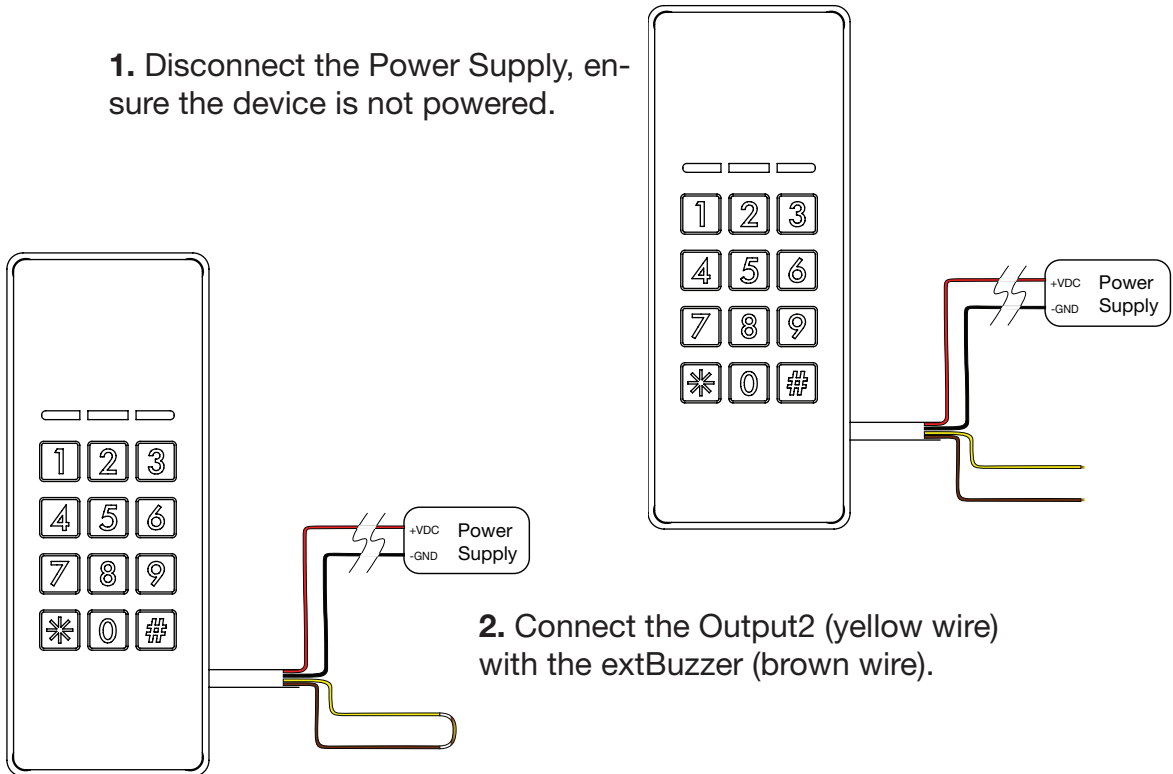
All the information from the Conlan Backup Card is loaded in the CM1000, a confirmation beep will sound.



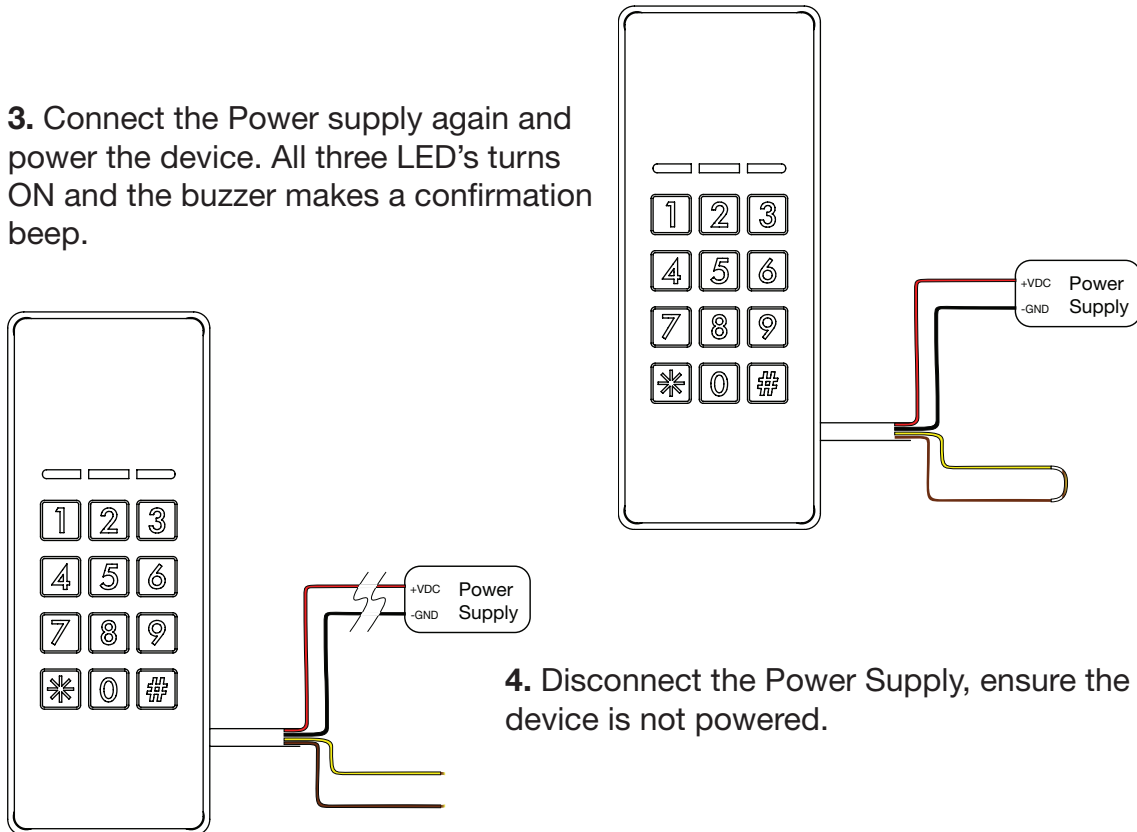
## 5. HARDWARE FACTORY RESET

To reset the hardware to factory default, please follow the below steps:

1. Disconnect the Power Supply, ensure the device is not powered.



3. Connect the Power supply again and power the device. All three LED's turns ON and the buzzer makes a confirmation beep.



5. Disconnect the Output2 (yellow wire) and the extBuzzer (brown wire). The device is now ready to be used again and all configurations are set as factory default.

## 6. REX INPUT

REX means **R**equest to **EX**it. In the CM1000, the REX input will produce Output2 activation as a consequence of someone attempting to egress through a door.

REX is used for three primary reasons:

First, access control systems may control doors which are also being monitored for security management, to indicate exception conditions on remote monitoring equipment.

Second, access control systems may utilize electrically actuated bolts, electromagnetic lock, shear locks, or a combination of locking devices which do not provide an integral means of manually unlocking the door to allow free egress. For the majority of applications, building and Fire Codes will mandate that any door along the path of egress (and most internal doors) allow free egress at all times.

There are exceptions, but these exceptions generally apply to institutional applications (such as detention facilities or psychiatric wards), government high security and special locking arrangements (such as delayed egress). Suitability of an opening for anything other than Free Egress will always be ultimately determined by the AHJ (Authority Having Jurisdiction). There may be times when more than one AHJ may be involved, in which case conflicts between them have been known to occur, as each may interpret the code differently. The bottom line is that for those situations where the electric locking device does not have any integral means of unlocking it for free egress, the REX input becomes a critical elements to the system behavior.

## 7. TECHNICAL SPECIFICATIONS

Device measures:	Classic 50x 130x 8 mm Mykey 50x 77 x 8 mm
Power source:	9 to 24 VDC ( <b>12VDC Recommended</b> )
Power consumption on Idle:	14 mA at 12VDC
Inputs:	ExtGreen, ExtRed and ExtBuzzer [Active LOW (-/GND)]
Outputs:	Output1 and Output2, Open Collector [Active LOW (-/GND)]
Protection rate:	IP67
Environmental conditions:	Temperature: -35°C to +66°C
Color:	White or Black.

