

# User's manual



eng

## NVAC-C300CKF

# NOVUS®


## EMC (2004/108/EC) and LVD (2006/95/EC ) Directives CE Marking

**CE** Our products are manufactured to comply with requirements of the following directives and national regulations implementing the directives:

- Electromagnetic compatibility EMC 2004/108/EC.
- Low voltage LVD 2006/95/EC with further amendment. The Directive applies to electrical equipment designed for use with a voltage rating of between 50VAC and 1000VAC as well as 75VDC and 1500VDC.


## WEEE 2002/96/EC Directive

### Information for users who want to get rid of electrical and electronic appliances

 This product is marked according to the European Directive on Waste Electrical and Electronic Equipment (2002/96/EC) and further amendments. By ensuring this product is disposed of correctly, you will help to prevent potential negative consequences for the environment and human health, which could otherwise be caused by inappropriate waste handling of this product. The symbol on the product, or the documents accompanying the product, indicates that this appliance may not be treated as household waste. It shall be handed over to the applicable collection point for the waste electrical and electronic equipment for recycling purpose. For more information about recycling of this product, please contact your local authorities, your household waste disposal service or the shop where you purchased the product.

## 2002/95/EC RoHS Directive

### Information concerning limitation of the use of dangerous substances in the electrical and electronic appliances.

 Out of concern for human health protection and friendly environment, we assure that our products falling under RoHS Directive regulations, regarding the restriction of the use of hazardous substances in electrical and electronic equipment, have been designed and manufactured in compliance with the above mentioned regulation. Simultaneously, we claim that our products have been tested and do not contain hazardous substances whose exceeding limits could have negative impact on human health or natural environment.

## Information

The device, as a part of professional AC system used for control, is not designed for self installation in households by individuals without technical knowledge.

Prior to undertaking any action that is not provisioned for the given product in its user's manual and other documents delivered with the product, or that arises from the normal application of the product, the manufacturer must be contacted or the responsibility of the manufacturer for the results of such an action shall be excluded.

## **ATTENTION!**

THE KNOWLEDGE OF THIS USER'S MANUAL IS AN INDESPENSIBLE CONDITION OF A PROPER CONTROLLER OPERATING. YOU ARE KINDLY REQUESTED TO FAMILIARIZE YOURSELF WITH THIS MANUAL BEFORE STARTING THE DEVICE.

THE MANUAL SHOULD BE KEPT FOR FUTURE USE.



## **CAUTION!**

ALL REPAIRS CAN BE EXECUTED ONLY BY QUALIFIED STAFF OF THE AUTHORISED NOVUS SERVICE.

## **ATTENTION!**

PRIOR TO UNDERTAKING ANY ACTION THAT IS NOT PROVISIONED FOR THE GIVEN PRODUCT IN ITS USER'S MANUAL AND OTHER DOCUMENTS DELIVERED WITH THE PRODUCT, OR THAT ARISES FROM THE NORMAL APPLICATION OF THE PRODUCT, ITS MANUFACTURER MUST BE CONTACTED OR THE RESPONSIBILITY OF THE MANUFACTURER FOR THE RESULTS OF SUCH AN ACTION SHALL BE EXCLUDED.

eng

## **IMPORTANT SAFEGUARDS AND WARNINGS**

1. Read, keep, and follow these instructions. All the safety and operating instructions should be read before the product is operated;
2. Follow all the safety instructions in this manual. Improper installation and controller operation may have impact on operator's safety as well as controller operational reliability and working life;
3. All the controller installations and operations should be done according to this user's manual;
4. Please unplug the unit from the power before starting maintenance procedures.
5. You mustn't use attachments / accessories that are not specified by the manufacturer.
6. Mounting the device in places where proper ventilation cannot be provided (e. g. closed lockers etc.) is not recommended since it may lead to heat build-up and damaging the device itself in consequence.
7. Do not mount the controller on unstable surface or do not use mounts that are not recommended by manufacturer.
8. Device should be supplied only from power sources which parameters are in accordance to one's pointed out by the producer in controller technical datasheet. Therefore it is forbidden to supply the controller from power sources with their parameters unknown, unstable or not meeting the producer's requirements.
9. Cables to the device should be placed in a way excluding the possibility of damaging them by accident. Special attention must be paid to cables going out of the controller and connecting power supply;
10. Electric installation supplying the device should be designed to meet the specifications given by the producer in such a way, that overloading it is impossible.
11. Camera should be protected from water and objects that may get inside it.
12. User cannot repair or upgrade equipment himself. All maintenance actions and repairs should be done only by the qualified service personnel.
13. Unplug the camera from the power source immediately and contact the proper maintenance department when the following occurs:
  - ◆ Damages to the power cord or to the plug itself;
  - ◆ Liquids getting inside the device or exposure to strong mechanical shock;

- ◆ Device behaves in a way not described in the manual and all adjustments approved by the manufacturer, and possible to apply by user himself, seem not to have any effect;
- ◆ Controller is damaged;
- ◆ Atypical behavior of the controller components may be seen (heard).

14. In case of repairs please pay attention to using only original replacement parts (with their parameters in accordance to those specified by the producer) should be paid.

Non-licensed service and non-genuine replacement parts may cause fire or electrocution.

15. After maintenance activities tests should be run to ensure proper work of all the device's functional components.

eng

## **INFORMATION**

Data included in the following user's manual is up to date at the time of printing.

Novus Security Sp z o.o. holds exclusive rights to modify this manual. The producer reserves the rights for device specification modification and change in the design without prior notice.

## Contents

1. Forward.....	6
2. Start Menu.....	10
3. Enroll Users.....	14
4. Edit Users.....	19
5. View Users.....	23
6. Delete Users.....	26
7. System Setup.....	27
7.1 Date and Time.....	27
7.2 Operating Mode.....	27
7.3 Re-lock Time.....	29
7.4 Address.....	29
7.5 Communication Password.....	30
7.6 Wiegand Format.....	30
7.7 System Reset.....	31
7.8 Event Reset.....	31
7.9 Communication Speed.....	32
7.10 Door Relay.....	32
7.11 Two Users.....	33
7.12 Antipassback.....	33
7.13 Duress.....	34
7.14 Date Format.....	34
7.15 Custom Display.....	35
7.16 LCD Display.....	36
7.17 Conceal PIN.....	36
7.18 Lockdown.....	37
7.19 Time and Attendance.....	37
7.20 Network Setup.....	37
7.21 Delete Event.....	40
7.22 Wiegand Type.....	40
7.23 Wieganda Time.....	40
7.24 RS Port On.....	41
7.25 Select Language.....	41
8. Scanner Setup.....	42
9. Sensor Setup.....	44
10. Alarm Setup.....	46
11. Installation Guide.....	48

## 1. Foreword

Functionality: This “all-in-one solution” integrates biometric reader, proximity reader and a PIN PAD device. NVAC-C300CKF controller offers very convenient and safe technology that verifies a user on the basis of biometric features.

Advanced Sensor Technology: ability to recognize fingerprints even in unfavorable conditions such as dirt makes it useful not only in offices but also in factories where it has previously been impossible to implement.

### Features

- Innovative technology of fingerprint reading and analysis (1st place in FVC2004).
- 1:1 and 1: Many verification in less than one second (processing speed: 1 sec for every 1000 templates).
- Possibility to assign one user with 2 or 4 templates.
- Multiple work modes: 11 to choose from.
- User name (after positive verification) and client info display (i.e. company name) in the standby mode.
- Integrated LCD display and numeric keypad with luminescent back light.
- Built-in sensor inputs and relay outputs.
- Ability to cooperate with an external relay module for enhanced security (available in the future).
- Port for output reader connection.
- Standalone or network communication via TCP/RS232 ports
- Two program modes for Access Control and Time & Attendance (available in the future)
- 512 time zones
- 365 holidays

eng

## Specification

### Controller

User Registration:	4096 cards, 1910 templates
Transaction Buffer:	16 000 with complete description
Communication:	Wiegand 26/34 bits, RS232 and TCP
Indicators:	3 LEDs and buzzer
Power Supply:	12VDC 1A
Dimensions:	125 x 125 x 22 mm ABS Housing
Operating Conditions:	Temperature 0 : +50C Humidity: 10% - 90%
Sensor Inputs:	3
Control Outputs:	2 Relay Optional: Remote Relay Module

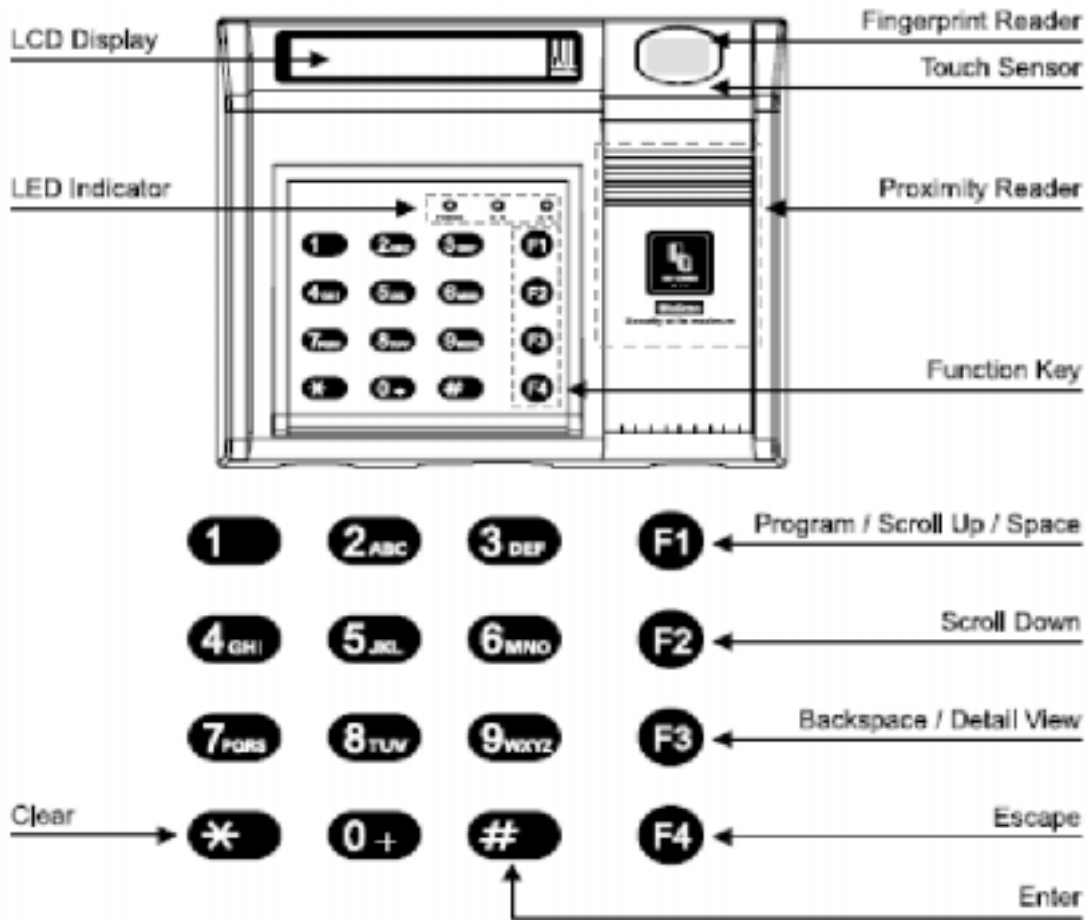
### Fingerprint Scanner

CPU	400 MHz DSP
FLASH Memory	1 MB (4 MB, option)
FAR	0,00008%
FRR	0,09%
Template Size	256 - 384 bytes (configurable, 384 default)
Encryption	256 bit AES
Dimensions	55 x 40 x 8 mm (L x W x H)
Sensor Type	Optical
Resolution	500 dpi
Scanning area	16 x 19 mm
Image Size	280 x 320 pixels

### Card Module

Card Type	Mifare, iClass (HID, Unique option)
Frequency	13,56 MHz (125 kHz option)
Antenna Type	Coil
Frequency Type	A1D
Modulation Type	Amplitude Modulation
Antenna Dimensions	45 x 55 mm

## 1.2 About Controller



## 1.3 Using the Scanner

How much pressure is required for a good-quality fingerprint?

If too much pressure is applied to the sensor window, the fingerprint ridges move away from each other and the user is not verified. If too little pressure is applied the scanner cannot read the fingerprint and the resulting image resembles dirty finger. A correct scan requires a number of attempts and can be easily mastered - it is best to compare a proper fingerprint scan to pressing a button. It gives information-rich picture and allows for easy identification.

1. Position - placing your finger far from the sensor center results in negative verification. The finger has to be touching the touch sensor that is located below the sensor and that activates the sensor.
2. Movement - Finger movement during scanning should be reduced to minimum.
3. Pressure - should be in accordance with the suggestions describe above.



Figure 1: Improper Alignment Causes Problems

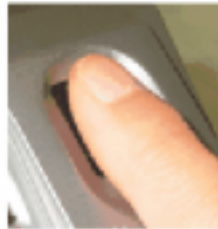


Figure 2: Proper Alignment

eng

## Finger Position

It is best when your finger covers the scanner area. Your fingertip should slightly extend beyond the length of the upper part of the sensor. Apply pressure lightly and evenly without moving the finger during the scanning process. Figure 2 shows the correct position of the finger during scanning. Figure 1 shows most common mistakes during the initial phase of the scanning process.

After placing your finger the scanner starts emitting red light. The finger should be placed on the sensor until the light goes off.

## Getting users fingerprints

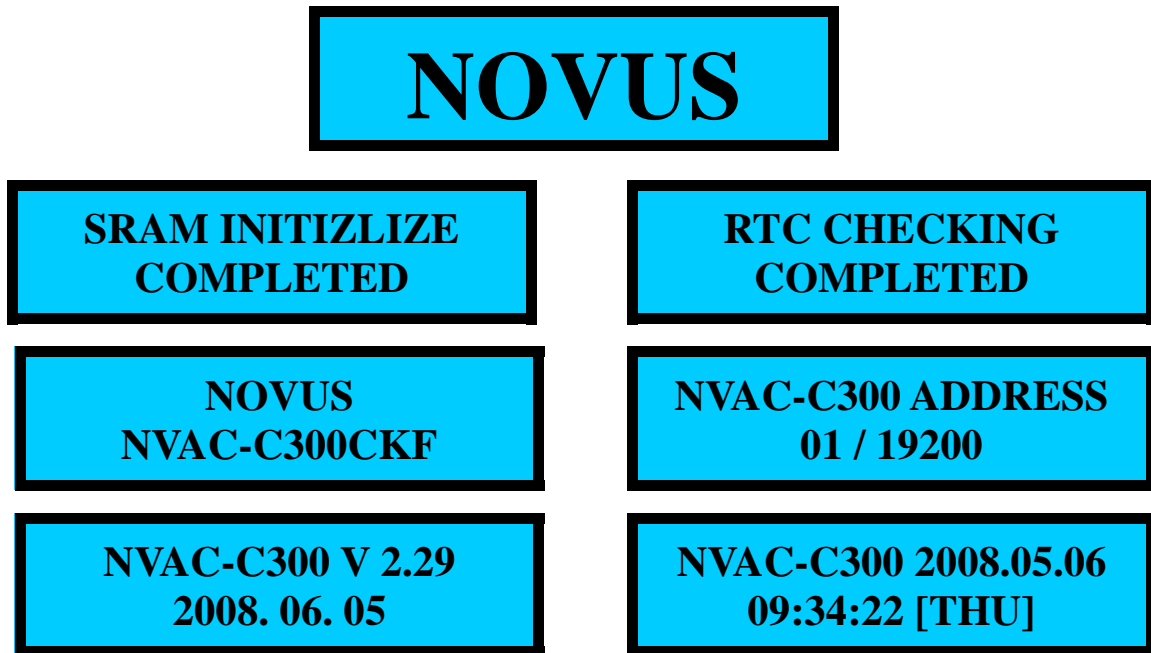
The process of getting users fingerprints should be carried out very thoroughly as the quality of templates will have influence on verification process during a day-to-day controller utilization. Finger during scanning should be clean and dry. User should pay special attention during placing the finger on the sensor and during the scanning process itself. The number of details determines much easier verification process. Every time that you place the finger on the sensor in a different way the device generates a number string and compares the similarity of this string with the template according to a special algorithm. If the similarity is higher than a predefined minimum a positive verification takes place.

## 2. Start Menu

Before starting the device make sure that the power supply is connected in the same way (block scheme) as it is described at the end of this user's manual.

### 2.1 Starting Sequence

After turning the power on the controller generates starting sequence which can be observed on the LCD display:



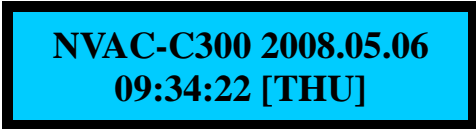





### 2.2 Program mode - before creating Admin account

If the device is powered on, then after the starting sequence a welcome sign is displayed (description of client Info Menu configuration is described in the following chapters). If Admin account has not been created every user can access the menu by pressing F1.



## 2.3 Program mode - after creating Admin account

If the Admin account has been created (in the way described in the following part of this manual) the order of actions connected with the program mode is the following:

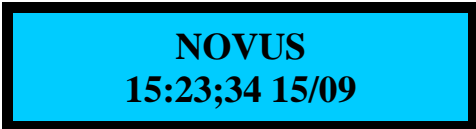


- |   |   |
|---|---|
| <p>1. Press F1</p>  <p>2. Enter Admin ID 1~16 digits, followed by the # key.</p>  <p>3. Admin touches the scanner with a finger (advised method) presents proximity card.</p>  | <p>4. The scanner is turned on.</p>  <p>5. After positive verification Admin</p>  <p>To exit program mode F4/Esc till the above appears.</p>  |
|---|---|

eng

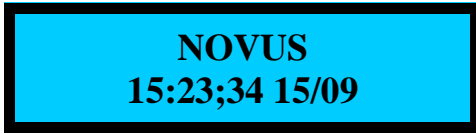
## 2.4 Controller utilization

To start utilization of NVAC-C300CKF controller after creating Admin account you have to create user accounts. To add a new user please assign him with unique ID (1 to 16 digits). Next, add 2 or 4 fingerprints and/or card number. Such a user, depending on the set identification mode, can be granted access either by scanning his finger or by presenting his proximity card to the controller. After placing a finger on the sensor, the scanner starts emitting red light. After the light goes off you may remove your finger. Next, a message, whether you have been granted access or not, appears on the display. User identification can be done in one out of the three ways: ID, card, finger) or their combination. Altogether, the controller can be set in 1 out of 11 work modes.

### 2.4.1 Operating with User PIN (ID)

- |   |  |
|---|--|
| <p>1. Enter ID in the standby mode.</p>  <p>2. Enter ID and press the # key.</p>  | <p>3. After successful verification, welcome message appears.</p>  |
|---|--|

### 2.4.2 Operating with User card

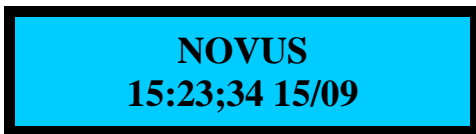


1. Present the card to the reader in the standby mode



2. After successful verification, welcome message and User ID or name appear.

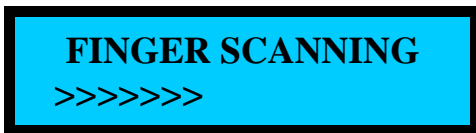
### 2.4.3 Operating with User fingerprint



1. Touch the scanner with your



3. After successful verification, welcome message and User ID or name appear.

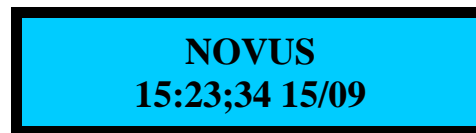


2. If the scanner doesn't turn on automatically press the # key to turn it on manually.



In case of negative verification controller displays the above message.

### 2.4.4 Operating with PIN (ID) and fingerprint



1. Enter ID in the standby mode.



3. Once the scanner has been turned on touch it with your finger.



2. Once the user ID has been entered press #



4. After successful verification, welcome message and User ID or name appear.

### 2.4.5 Operating with User card and fingerprint

**NOVUS**  
**15:23;34 15/09**

1. Present the card to the reader in the standby mode. After successful

**FINGER SCANNING**  
**>>>>>>**

2. Touch the scanner with your finger.

**WELCOME**  
**JONES**

3. After successful verification, welcome message and User ID or name appear.

eng

### 2.4.6 Operating with User PIN (ID), card and fingerprint

**NOVUS**  
**15:23;34 15/09**

1. Enter ID in the standby mode.

**ENTER USER ID**  
**123456789**

2. Enter ID and press the # key.

**PRESENT CARD**

3. After the above message appears, present the card to the reader. After positive verification the scanner is turned on.

**FINGER SCANNING**  
**>>>>>>**

4. Touch the scanner with your finger.

**WELCOME**  
**JONES**

5. After successful verification, welcome message and User ID or name appear.

If the controller is set to double or triple verification mode (ID, card, fingerprint) you need to make sure the verification goes in the right order. If the order is wrong a message stating controller work mode and the required verification order is displayed. i.e. if the controller is set in the ID & Card & Fingerprint mode you need to enter PIN first, next present the card to the reader and then touch the scanner with your finger. If the order is wrong the following messages are displayed:

**NVAC-C300CKF**  
**ID & CD & FP**

**PLEASE TRY AGAIN**  
**ID & FP**

### 3. Enroll Users

#### 3.1 Enroll users with fingerprints templates

The following procedure is used to add a user who will only use fingerprints to gain access to a location guarded by the reader. The NVAC-C300CKF controller in its basic version can have up to 1910 fingerprint templates and this means that you can add 955 users with 2 fingerprint templates each or 477 users with 4 fingerprint templates each (including Administrators).

Before adding a user make sure Admin account need to be created (Admin account is created in the same way as User account). The only difference lies in assigning Admin with SA access level (explained in the following part of this chapter).

Below you can find the procedure of adding a new fingerprint user. It is done by the Admin in the setup mode.

**1> ENROLL USER  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**1> ENROLL USER  
F1:UP F2:DN**

2. Press F1 to go to the next menu

**1. FINGER  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**LEVEL 1:USER  
2:RA 3:AA 4:SA**

4. Select user level access (explained in the following part of this point)

**1 - 16 DIGTS  
ENTER USER ID**

5. Enter user ID followed by the # key.

**ENTER USER ID  
123456789**

6. Press the # key to go to the next

**SELECT ENROLL  
1:2-FP 2:4:FP**

7. Select 1 for 2 templates or 2 for 4 templates - controller will ask you to scan the required number of fingertips

**FINGER SCANNING  
FIRST >>>>>**

**FINGER SCANNING  
FOURTH >>>>>**

8. Scan 2 or 4 fingertips.

**TRY AGAIN  
>>>>>**

**ENROLL TIME OUT  
CONT. # STOP: ANY**

During the scanning process you may be asked to rescan or after to long delay time out.

**ENROLL COMPLETED  
CONT. # STOP: ANY**

To exit the menu press any key apart from # and then press F4/Esc

Recommendations regarding fingertip templates scanning:

- Position the finger where the first joint meets the edge of the sensor
- Do not apply too much pressure
- Keep the finger on the sensor until the red light turns off.
- Use thumb, index or middle fingers.
- Don't use small finger as it is inconvenient and it has the small finger has a small area to be scanned.
- During scanning try to cover the whole scan area with your finger.
- 

**NOTE:**

There are four levels of administration:

- **User (Level 1)** - assigned to a regular user who wants to access a restricted area or location.
- **RA (Level 2)** - assigned to Admin who will have the right to add users. This admin doesn't have access to other administrative functions.
- **AA (Level 3)** - assigned to Admin who will have the right to administer user database.
- **SA (Level 4)** - assigned to Admin who will have access to all the controller functions as the main administrator.
- 

eng

**3.2 Enroll Card Users**

The following procedure is used to add a user who will only use a card to gain access to a location guarded by the reader. The NVAC-C300CKF controller in its basic version can have up to 4096 card numbers. If we save 500 fingerprint templates there will be 3596 free slots left for card numbers. Fingerprint users are automatically assigned with a card slot in the system memory even if they do not use or add any cards.

Below you can find the procedure of adding a new card user. It is done by the Admin in the setup mode.



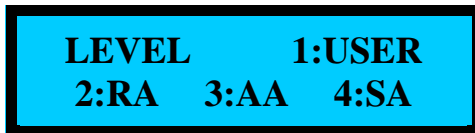
1. Press the # key to go to the next menu level.



3. Press the # key to go to the next menu level.



2. Press F1 to go to the next menu level.



4. Select user level access (explained in the following part of this point).

**1 - 16 DIGITS  
ENTER USER ID**

5. Enter user ID followed by the # key.

**ENTER USER ID  
123456789**

6. Press the # key to go to the next menu level.

**PRESENT CARD**

7. Present card to the reader.

**USER CARD EXIST  
PRESENT CARD**

If this card has already been assigned to somebody else, the controller displays the above message.

**ENROLL COMPLETED  
CONT. # STOP: ANY**

8. To exit the menu press any key apart from # and then press F4/Esc

### 3.3 Enroll users with cards and fingerprints

The following procedure is used to add a user who will only use a card and/or fingerprints to gain access to a location guarded by the reader.

Below you can find the procedure of adding a new card and fingerprint user. It is done by the Admin in the setup mode.

**1> ENROLL USER  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**LEVEL 1:USER  
2:RA 3:AA 4:SA**

4. Select user level access (explained in the following part of this point).

**1> ENROLL USER  
F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**1 - 16 DIGITS  
ENTER USER ID**

5. Enter user ID followed by the # key.

**3. FINGER+CARD  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**ENTER USER ID  
123456789**

6. Press the # key to go to the next menu level.

**SELECT ENROLL**  
**1:2-FP 2:4:FP**

7. Select 1 for 2 templates or 2 for 4 templates - controller will ask you to scan the required number of fingertips as a next step.

**FINGER SCANNING**  
**FIRST >>>>>**

**FINGER SCANNING**  
**FOURTH >>>>>**

8. Scan 2 or 4 fingertips.

**PRESENT CARD**

9. Present card to the reader.

**ENROLL COMPLETED**  
**CONT. # STOP: ANY**

10. To exit the menu press any key apart from # and then press F4/Esc

eng

### 3.4 Enroll V1 block of card users

The following procedure is used to add block user. This procedure is very useful when we have a large quantity of consecutive card numbers to add. Below we have an example of 100 users to be added to the system. We start adding the users starting from ID 1000. It means that User ID 1000 corresponds to card number 1000 and so on.

Below you can find the procedure of adding a block of card users. It is done by the Admin in the setup mode.

**4. CARD BLOCK**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**START USER ID**

2. The following message appears.

**ENTER USER ID**  
**1234**

3. Once finished confirm by pressing #

**START USER CARD**

4. The following message appears.

**USER CARD**  
**1000**

5. Once finished confirm by pressing #

**REG. USER NUM**

6. The following message appears.  
Enter the total number of cards.

**USER COUNT  
100**

7. Once finished confirm by pressing #

**ENROLL CARD 100**

>>>>>>>>

8. After confirmation the system starts  
adding cards number to the memory.

**ENROLL COMPLETED**

9. Once the process has been finished  
controller displays confirmation.

**NOTE:**

This option adds new cards in consecutive empty slots which are searched for during this process. That is why, this process may take more time if some of the controller's memory has been taken up by previously saved card number or fingerprints. If an ID given during adding process is already in use such a card will not be added.

**3.5 Enroll V2 block of card users**

The following procedure is used to add block user. This procedure is very useful when we have a large quantity of consecutive card numbers to add. The difference between V2 and V1 is in way software adds new card numbers. In case of V2 the software adds new card numbers to consecutive slots even though they have the numbers that have already been entered. This option is very useful when we want to add a new database very fast.

Below you can find the procedure of adding a block of card users. It is done by the Admin in the setup mode and is exactly the same as the V1 procedure.

**5. CARD BLOCK 2  
# ENTER F4:ESC**

The next points of the procedure are exactly the same as described above. This process is faster as the software does not search for free slots but overwrites the existing ones.

eng

## 4. Edit Users

### 4.1 Edit User ID

The following procedure is used to edit user ID.

Below you can find the procedure of editing user ID. It is done by the Admin in the setup mode.

**2> EDIT USER  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**2> EDIT USER  
F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**1. USER ID  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**1 - 16 DIGTS  
ENTER USER ID**

4. Enter user ID followed by the # key.

**ENTER NEW ID**

5. Enter new user ID, followed by the # key.

**EDIT COMPLETED  
CONT. # STOP: ANY**

6. Press any key apart from # to end the edition mode.

### 4.2 Edit User Fingerprint

The following procedure is used to edit user fingerprint. Below you can find the procedure of editing user fingerprint. It is done by the Admin in the setup mode.

**2> EDIT USER  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**2> EDIT USER  
F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**2. FINGER  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**ENTER USER ID  
123456789**

4. Enter user ID followed by the # key.

**FINGER SCANNING  
FIRST >>>>>>**

5. Enroll finger the some or new one, followed by the # key.

**EDIT COMPLETED  
CONT. # STOP: ANY**

6. Press any key apart from # to end the edition mode.

### 4.3 Edit User Card

The following procedure is used to edit user card. Below you can find the procedure of editing user card. It is done by the Admin in the setup mode.

**2> EDIT USER  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**ENTER USER ID  
123456789**

4. Enter user ID followed by the # key.

**2> EDIT USER  
F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**PRESENT NEW CARD**

5. Present a new card to the reader.

**3. CARD  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**EDIT COMPLETED  
CONT. # STOP: ANY**

6. Press any key apart from # to end the edition mode.

### 4.4 Edit User Access Level

The following procedure is used to edit user access level. Below you can find the procedure of editing user access level. It is done by the Admin in the setup mode.

**2> EDIT USER  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**ENTER USER ID  
123456789**

4. Enter user ID followed by the # key.

**2> EDIT USER  
F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**(U) 1: USER  
2:RA 3:AA 4:SA**

5. Select the user level followed by the # key.

**4. LEVEL  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**EDIT COMPLETED  
CONT. # STOP: ANY**

6. Press any key apart from # to end the edition mode.

## 4.5 Edit User Name

The following procedure is used to edit user name. Below you can find the procedure of editing user name. It is done by the Admin in the setup mode.

**2> EDIT USER  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**2> EDIT USER  
F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**3. NAME  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**ENTER USER ID  
123456789**

4. Enter user ID followed by the # key.

**1. ENTER NAME  
2. SELECT DISPLAY**

5. Select 1 to enter name.

**ENTER USER NAME  
JONES**

6. You enter a name by means of keyboard in the same way as you write short text messages. Each button needs to be pressed as many times as it is required to displayed a desired sign (see the table on the next page). Each set sign has to be confirmed by pressing F1. Once the whole name has been entered confirm by pressing the # key.

**EDIT COMPLETED  
CONT. # STOP: ANY**

7. Press # to continue.

**ENTER USER ID  
123456789**

8. Enter user ID followed by the # key.

**1. ENTER NAME  
2. SELECT DISPLAY**

9. Select 2 to choose info to be displayed on the LCD display.

**1. DISPLAY USER ID  
2. DISPLAY NAME**

10. You can select user name or user ID to be displayed.

**EDIT COMPLETED  
CONT. # STOP: ANY**

11. Press any key apart from # to end the edition mode.

eng

KEYS	NUMBER OF TIMES KEY IS PRESSED							
	1	2	3	4	5	6	7	8
1								
2	A	B	C	a	b	c		
3	D	E	F	d	e	f		
4	G	H	I	g	h	i		
5	J	K	L	j	k	l		
6	M	N	O	m	n	o		
7	P	Q	R	S	p	q	r	s
8	T	U	V	t	u	v		
9	W	X	Y	Z	w	x	y	z
0								
*	Clear							
#	Enter							
F1	Space							
F2								
F3	Back Space							
F4	Escape							

#### 4.6 Edit AntiPassback

This function prevents more than once person using the same identification method from entering a location.

#### 4.7 Edit ID Option

This function allows user to access a location ID only even when the verification mode is set to Card or Fingerprint.

#### 4.8 Edit Two Users Function

This function allows for accessing an area only when two authorized users enter this area.

#### 4.9 Edit Canteen

This function is devoted to a special utilization connected with canteen operation. It requires writing its own software based on SDK software.

#### 4.10 Edit Canteen - counter

This function is devoted to a special utilization connected with canteen operation. It requires writing its own software based on SDK software.

## 5. View

### 5.1 User List

The following procedure is used to view user list. Below you can find the procedure of viewing user list. It is done by the Admin in the setup mode.

**3> VIEW**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**3> VIEW**  
**F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**1. USER LIST**  
**# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**LIST 12280/00001**  
**F1:UP F2:DN**

4. Controller displays the number of memory slots and the number of used slots. Press F1/F2 to view particular positions.

**12280/00001 (U)**  
**3836767**

5. In the first slot description window, controller displays in brackets the level of access (U) - user or (R) - Admin. In the second line user ID is displayed. To display more details regarding user with the above mentioned ID you need to press F3 on the keyboard.

**FINGER: 4-FP**  
**CARD: 7DA56BC4**

6. In the second slot description window, controller displays the number of scanned fingertips and card ID. If these data have not been assigned "empty slot" info is displayed.

**FINGER: EMPTY**  
**CARD: EMPTY**

7. Press F3 one more time to display name.

**NAME**  
**JONES**

8. Press F1 or F2 to transfer data to the next user. To exit the browser press F4/Esc.

**LIST VIEW EXIT**  
**CONT. # STOP: ANY**

9. Press any key apart from # to end user view.

eng

## View

### 5.2 View Event Data List

The following procedure is used to view event data list. Below you can find the procedure of viewing event list. It is done by the Admin in the setup mode.

**3> VIEW**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**3> VIEW**  
**F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**2. EVENT DATA**  
**# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**EVENT 25600/00173**  
**F1:UP F2:DN**

4. Controller displays the number of memory slots and the number of used slots. Press F1/F2 to view particular positions.

**25600/00173 2008**  
**09. 19. 10:21:43**

**25600/00174**  
**EMPTY EVENT**

5. In the slot description window controller displays the number of memory slots and a consecutive slot number. It also displays event date and time. To display more details regarding the event you need to press F3 on the keyboard.

**ACCESS DENEID**  
**241AFC7F**

6. In the second slot description window, controller displays event description and i.e. card number.

**ACCESS GRANTED**  
**241AFC7F**

7. User ID is displayed when the access has been granted.

**SYSTEM EVENT**  
**ADMIN MODE**

8. It can be also system event - i.e. entering Admin mode.

**EVENT VIEW EXIT**  
**CONT. # STOP: ANY**

9. Press any key apart from # to end event view.

eng

## View

### 5.3 Firmware View

The following procedure is used to view firmware. Below you can find the procedure of viewing firmware. It is done by the Admin in the setup mode.

**3> VIEW**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**3> VIEW**  
**F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**3. FIRMWARE**  
**# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**NVAC-C300 V 2.29**  
**2008. 06. 05**

4. Controller displays firmware version that is currently installed.

**VIEW CLOSED**  
**F1:UP F2:DN**

5. Press any key apart from # to end firmware view.

eng

### 5.4 Scanner Version View

The following procedure is used to view scanner version. Below you can find the procedure of viewing scanner version. It is done by the Admin in the setup mode.

**3> VIEW**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**3> VIEW**  
**F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**4. FINGER VER.**  
**# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**SFM-3020**  
**VER : A1 7C**

4. Controller displays scanner version that is currently installed.

**VIEW CLOSED**  
**F1:UP F2:DN**

5. Press any key apart from # to end firmware view.

## 6. Delete Users

### 6.1 Delete Single User

The following procedure is used to delete single user. Below you can find the procedure of deleting single user. It is done by the Admin in the setup mode.

**4> DELETE USER  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**4> DELETE USER  
F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**1. SINGLE USER  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**1 - 16 DIGTS  
ENTER USER ID**

4. Enter user ID to be deleted.

**ENTER USER ID  
123456789**

5. Once user ID has been entered confirm it by pressing #. The user is deleted.

**DELETE COMPLETED  
CONT. # STOP: ANY**

### 6.2 Delete All Users

The following procedure is used to delete all users. Below you can find the procedure of deleting all users. It is done by the Admin in the setup mode.

**4> DELETE USER  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**4> DELETE USER  
F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**1. ALL USER  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

**DELETE : ' #'  
CANCEL : ' ANY '**

4. Software demands confirmation by pressing # and deleting process starts what last a few seconds.

**DELETETING...  
>>>>>>>**

**DELETE COMPLETED  
F1:UP F2:DN**

eng

## 7. System Setup

### 7.1 Date and Time

This procedure is used to set current date and time. The device has an internal clock for all logged events. Below you can find the procedure of setting date and time. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**5> SYSTEM SETUP**  
**F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**1. TIME**  
**# ENTER F4:ESC**

**YEAR:MON:DAY**  
**20 : :**

3. Enter current date in the following format: YYYY:MM:DD i.e. 2008:01:15. #.

**NOUR:MIN:SEC**  
**: :**

4. Enter current time in the following format: HH:MM:SS. Confirm #.

**1:SUN, , 7:SAT**  
**SELECT 1 - 7**

5. Select day of the week by pressing appropriate number from 1 to 7.

**1:SUN, , 7:SAT**  
**{FRI} ENTER '#'**

6. Confirm by pressing the # key.

### 7.2 Operating Mode

This procedure is used to set work mode. You can set 1 out of 11 work modes. Work modes apply to the way of user identification via:

- entering ID on the keyboard
- presenting the card to the reader
- scanning fingerprints

or combination of these methods.

Below you can find the procedure of setting operating mode. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**2. OPERATING MODE**  
**# ENTER F4:ESC**

2. Press the # key to go to the next menu level.

**SELECT MODE**  
F1:UP F2:DN

3. Press the # key to go to the next menu level.

**CARD / FP**  
F1:UP F2:DN

1. Access with card or fingerprint (1 : many).

**ID&FP / CD**  
F1:UP F2:DN

2. Access with ID and fingerprint (1:1) or with card.

**ID&CARD&FP**  
F1:UP F2:DN

3. Access with ID and fingerprint and card. The highest security mode.

**ID / CARD / FP**  
F1:UP F2:DN

4. Access with ID or fingerprint (1: Many) or with card. The lowest security mode.

**FP (ID&FP)**  
F1:UP F2:DN

5. Access with fingerprint (1: Many). To speed up the process of identification in case of a bigger database you can enter ID first and then scan a finger.

**ID & FP**  
F1:UP F2:DN

6. Access with ID and fingerprint (1:1)

**CD & FP**  
F1:UP F2:DN

7. Access with card and fingerprint (1:1).

**ID & FP / ID & CD**  
F1:UP F2:DN

8. Access with ID and fingerprint or ID and card.

**ID&FP / CD&FP**  
F1:UP F2:DN

9. Access with ID and fingerprint or card and fingerprint.

**ID&CD / CD&FP**  
F1:UP F2:DN

10. Access with ID and card or card and fingerprint.

**ID & CD**  
F1:UP F2:DN

11. Access with ID and card.

& means „AND”

/ means „OR”

After selecting a mode press Enter #, and then Esc.

**OPEN MODE**  
F1:UP F2:DN

Permanent open mode in emergency situations.

**TEST MODE**  
F1:UP F2:DN

Controller test mode.

**CLOSED MODE**  
F1:UP F2:DN

Permanent closed mode to disable access.

**SETUP COMPLETED**  
F1:UP F2:DN

eng

### 7.3 Re-lock Time

This procedure is used to set the activation time of the relay output controlling the electronic lock. You can set the time in the range from 1 to 99 seconds. 0 seconds cannot be set.

Below you can find the procedure of re-locking time. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
F1:UP F2:DN

1. Press F1 to go to the next menu level.

**LOCK TIME SETUP**  
C : 04 S :

4. Enter time range from 1 to 99 seconds. Press the # key to confirm.

**3. RE-LOCK TIME**  
# ENTER F4:ESC

2. Press the # key to go to the next menu level.

**SETUP COMPLETED**  
F1:UP F2:DN

### 7.4 Address

This procedure is used to set device address. You can set the address in the range from 1 to 14. The address is utilized during communication between a controller with a PC. Below you can find the procedure of setting the address. It is done by the Admin in the setup mode. After entering Setup:

**4. ADDRESS**  
# ENTER F4:ESC

3. Press the # key to go to the next menu level.

**1 ... 14 SETUP**  
C : 01 S :

4. Enter address from 1 to 14. Press the # key to confirm.

## 7.5 Communication Password

This procedure is used to set communication password. Its main aim is the protection against unauthorized communication with a controller and system sabotage. The password is used in communication between a controller and a PC.

Below you can find the procedure of setting communication password. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
**F1:UP F2:DN**

1. Press F1 to go to the next menu level.

**0 - 99999999 SETUP**  
**C : FFFFFFFF**

4. Enter 8-digit password.  
Press the # key to confirm.

**5. COMM. PASSWORD**  
**# ENTER F4:ESC**

2. Press the # key to go to the next menu level.

**SETUP COMPLETED**  
**F1:UP F2:DN**

## 7.6 Site code - Wiegand Format

This procedure is used to set Wiegand format which allows for sending information via Wiegand port to an external controller. You can set 1 out of 7 formats. The formats are divided into 3 groups depending on the card technology:

- EMS cards
- HID cards
- Mifare cards

Below you can find the procedure of setting Wiegand format. It is done by the Admin in the setup mode. After entering Setup:

**5> SYSTEM SETUP**  
**F1:UP F2:DN**

1. Press F1 to go to the next menu level.

**1. EM. S. 26 BIT**  
**F1:UP F2:DN**

**6. SITE CODE**  
**# ENTER F4:ESC**

2. Press the # key to go to the next menu level.

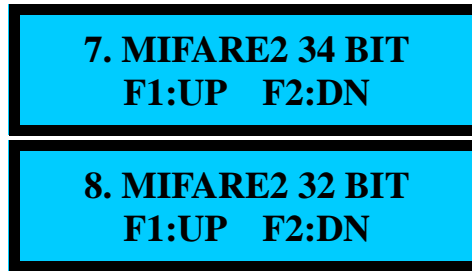
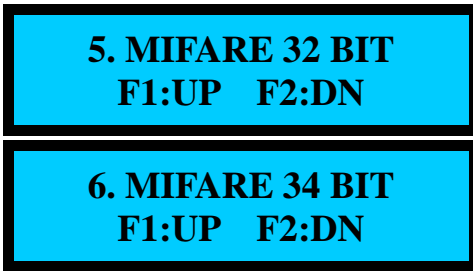
**2. HID. S. 26 BIT**  
**F1:UP F2:DN**

**3. HID. FULL. 26 BIT**  
**F1:UP F2:DN**

**SEL CARD TYPE (8)**  
**F1:UP F2:DN**

3. Press F1 to go to the next menu level. Select position from 1 to 8  
Press the # key to confirm.

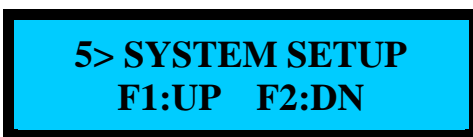
**4. HID. IDTI 34 BIT**  
**F1:UP F2:DN**



### 7.7 System Reset

This procedure is used to reset the system to the default settings. Controller has two memory areas (event and settings). After system reset the second memory area is set to default settings. Below you can find the procedure of system reset. It is done by the Admin in the setup mode.

eng



1. Press F1 to go to the next menu level.



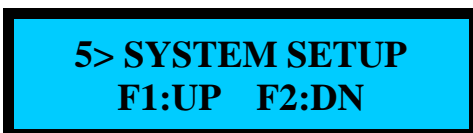
3. Press 1 to confirm or any other key to cancel.



2. Press the # key to go to the next menu level.

### 7.8 Event Reset

This procedure is used to reset events. Controller has two memory areas (event and settings). After system reset the second memory area is set to default settings. Below you can find the procedure of event reset. It is done by the Admin in the setup mode.



1. Press F1 to go to the next menu level.



3. Select 1 to reset all or 2 to reset by index.



2. Press the # key to go to the next menu level.

After selecting 1 in the previous menu

**EVENT RESET ?  
YES : 1 NO : ANY**

5. Press 1 to confirm or any other key to cancel.

**EVENT RESET  
>>>>>>>>**

After selecting 2 in the previous menu

**PUT 0 - 25999**

5. Enter index number to be reset and confirm by pressing the # key.

**EVENT RESET  
>>>>>>>>**

eng

### 7.9 Communication Speed

This procedure is used to set communication speed for RS-232 port. You can select 1 out of 5 baud rates in the range from 4800 to 57600. Below you can find the procedure of setting communication speed. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP  
F1:UP F2:DN**

1. Press F1 to go to the next menu level.

**SEL SPEED 19200  
F1:UP F2:DN**

3. Press the # key to go to the next menu level.

**9. COMM. SPEED  
# ENTER F4:ESC**

2. Press the # key to go to the next menu level.

**1. 4800 B-RATE  
F1:UP F2:DN**

4. Set the speed by pressing F1 and F2 buttons and confirm by pressing #.

### 7.10 Door Relay

This procedure is used to select function 1 and 2 of controller relay. Each of the relays can: control electronic lock after access has been granted, turn the alarm system On/Off or react to sensor inputs alarms. Below you can find the procedure of setting door relays. It is done by the Admin in the setup mode

**10. DOOR (RELAY)  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**RELAY 1 SEL 1. DOOR  
2. ALARM 3. INPUT 3**

3. Select 1 out of 3 relay functionality levels by pressing 1,2 or 3.

**SELECT RELAY 1-2  
1 - DOOR 2 - ALARM**

2. Press 1 or 2 to select the relay.

**RELAY 2 SEL 1. DOOR  
2. ALARM 3. INPUT 3**

4. Analogical function selection for the second relay.

## 7.11 Two Man

This procedure is used to turn on the function of granting access after two card users have presented their card to the reader in a set period of time. Only then can other users access a location individually. The same applies to exiting the location - the last two persons have to leave together. To sum up, the system will not allow one person at the location.

This function applies only to a controller that has the option of connecting exit reader.

Below you can find the procedure of setting two users. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
**F1:UP F2:DN**

1. Press the # key to go to the next

**ENABLE TWO MAN?**  
**1 : YES 2 : NO**

3. Select 1 to enable or 2 to disable.

**11. TWO MAN**  
**# ENTER F4:ESC**

2. Press the # key to go to the next menu level.

**ENTER NUM 1-99**  
**C : 00 S :**

4. After selecting Enable you need to enter the time limit for the second user to verify himself to the reader.

## 7.12 Antipassback

This procedure is used to turn on the function of entrance/exit control - antipassback. This function stops two people from using one card or fingerprint to gain access.

This function applies only to a controller that has the option of connecting exit reader.

Below you can find the procedure of setting antipassback function. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
**F1:UP F2:DN**

1. Press the # key to go to the next

**ENABLE ANTIPASS?**  
**1 : YES 2 : NO**

3. Select 1 to enable or 2 to disable.

**12. ANTIPASSBACK**  
**# ENTER F4:ESC**

2. Press the # key to go to the next menu level.

### 7.13 Duress

This procedure is used to enable the function of secretly signaling security that an authorized person is entering the secure area under "duress" through the implementation of a duress feature; i.e. when somebody makes a user let them in to a secure area.

This function requires user to press a defined function key. The system signals such a situation with a secret alarm. Below you can the duress procedure. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
F1:UP F2:DN

1. Press the # key to go to the next menu level.

**13. DURESS**  
# ENTER F4:ESC

2. Press the # key to go to the next menu level.

**ENABLE DURESS?**  
1 : YES 2 : NO

3. Select 1 to enable or 2 to disable.

**ENTER F2, F4**

3. Press F2 to assign secret entrance key.

**ENTER NUM 0-9**  
F2 :

4. Press a button from 1 to 9, which will activate discrete entrance function and confirm it by pressing the # key.

**SETUP COMPLETED**  
F1:UP F2:DN

### 7.14 Date Format

This procedure is used to set displayed date and time format.

Below you can find the procedure of setting date format. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
F1:UP F2:DN

1. Press the # key to go to the next menu level.

**14. DATE FORMAT**  
# ENTER F4:ESC

2. Press # to go to the next menu level.

**SYSTEM DISPLAY**  
F1:UP F2:DN

3. Press F1 to go to the next menu level. You can select 1 out of 6 positions. Confirm by pressing the # key.

**1 : ASIA**  
YYYY. MM. DD.

**2 : USA**  
MM. DD. YYYY.

**3 : EUROPE**  
DD. MM. YYYY.

**4 : CUSTOM 1**  
MESSAGE DD/MM

**5 : CUSTOM 2**  
MESSAGE MM/DD

**6 : CUSTOM 3**  
BENCO BCI MM/DD

## 7.15 Custom Display

This procedure is used to enter client info to be displayed in the first line of LCD display in the standby mode. If the info consists of two words or one word which has more than 16 characters it is scrolled from right to left on the LCD display.

Below you can find the procedure of entering client info. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
**F1:UP F2:DN**

1. Press the # key to go to the next menu level.

**EDIT DISPLAY**  
**NOVUS**

3. Utilizing keyboard enter the info - up to 16 characters.

**15. CUSTOM DISPLAY**  
**# ENTER F4:ESC**

2. Press the # key to go to the next menu level.  
Entering characters is done in accordance with the below table.

**CONTINUE DISPLAY?**  
**1 : YES 2 : NO**

4. If the info is longer than 16 press 1 to continue entering the message, otherwise press 2.

KEYS	NUMBER OF TIMES KEY IS PRESSED							
	1	2	3	4	5	6	7	8
1								
2	A	B	C	a	b	c		
3	D	E	F	d	e	f		
4	G	H	I	g	h	i		
5	J	K	L	j	k	l		
6	M	N	O	m	n	o		
7	P	Q	R	S	p	q	r	s
8	T	U	V	t	u	v		
9	W	X	Y	Z	w	x	y	z
0								
*	Clear							
#	Enter							
F1	Space							
F2								
F3	Back Space							
F4	Escape							

## 7.16 LCD Light

This procedure is used to set LCD light parameters and the way in which keyboard is lit. LCD display and the keyboard can be illuminated for 5 seconds, can be constantly lit or can be illuminated during a period of time defined by a user. Constant illumination shortens LCD display lifespan.

Below you can find the procedure of setting LCD display. It is done by the Admin in the setup mode.

**5> SYSTEM SETUP**  
**F1:UP F2:DN**

1. Press the # key to go to the next menu level

**2: ALWAYS ON**  
**LCD LIGHT TIME**

5. Position 2. Constant illumination. Shortens LCD display lifespan.

**16. LCD LIGHT**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level

**3: CUSTOMIZE**  
**LCD LIGHT TIME**

6. Position 3. You can define a period of time during which LCD display and keyboard will be illuminated. Press the # key to go to the next menu level.

**SELECT ON LIGHT**  
**F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**S HOUR : MIN : SEC**  
: :

7. Enter the time at which the LCD Display will be illuminated on.

**1: DEFAULT**  
**LCD LIGHT TIME**

4. Position 1. Default illumination time - 5 seconds.

**E HOUR : MIN : SEC**  
: :

8. Enter the time at which the illumination will be turned off.

## 7.17 Conceal PIN

This procedure is used to conceal PIN during entering it on the LCD display. The digits are represented by \*. Below you can find the procedure of concealing PIN. It is done by the Admin in the setup mode.

**17. CONCEAL PIN**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**CONCEAL SETUP?**  
**1 : YES 2 : NO**

1. Press 1 to conceal or 2 to cancel.

## 7.18 Lockdown

This procedure is used to arm/disarm an external alarm system called Lockdown via controller relay output.

Below you can find the procedure of setting alarm system. It is done by the Admin in the setup mode.

**18. LOCKDOWN**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level and then F1 or F2.

**LOCK DN ENABLE?**  
**1 : YES 2 : NO**

2. Press 1 to enable or 2 to disable.

eng

## 7.19 Time and Attendance

**Caution:** T&A software which will be use for generate T&A report will be available in the future. This procedure is used to monitor time and attendance. Below you can find the procedure of setting time and attendance. It is done by the Admin in the setup mode.

**19. ATTENDENCE**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level and then press F1 or F2.

**ATTENDENCE?**  
**1 : YES 2 : NO**

2. Press 1 to enable or 2 to disable.

When this function is enabled controller displays additional functional descriptions F2: WE / F4: W after access has been granted. Detailed description can be found in the user's manual for T&A software. To make T&A reports the reader has to be connected with an appropriate PC software.

## 7.20 Network Setup

**Caution:** Administration software which will be use for programming and monitoring controllers trough the network will be available in the future.

This procedure is used to set parameters allowing for communication between a supervisory software and a controller over TCP/IP protocol via Ethernet network. The controller works in Server mode whereas the software in Client mode. It is an advantage of this mode that when the connection is lost the software automatically tries to reestablish the connection with the controller. The controller has a network socket allowing for computer network connection.

Below you can find the procedure of setting these parameters. It is done by the Admin in the setup mode.

**20. NETWORK SETUP**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**1 : VIEW 2 : SETUP**  
**NETWORK CONFIG**

2. Press 1 to display settings or 2 to set parameters.



After selecting 2 you can start entering computer and controller IP parameters.

Computer address

**1 : HOST (PC) IP**  
**2 : DEVICE IP**

1. Press 1 to set computer IP address or 2 to set controller parameters. If you have selected 1 you will find the following parameters.

**HOST (PC) IP**  
**192.168.050.001**

2. Enter computer IP address on which NAM (Novus Access Manager) software is installed. Exemplary address is shown on the display.

**HOST (PC) PORT**  
**05000**

2. Enter computer port address and confirm by pressing the # key. Default address is shown on the display.

**COMPLETED**  
**F1:UP F2:DN**

Controller address

**NETWORK MODE**  
**1 : SERVER 2 : CLIENT**

1. Press 1 to set Server mode or 2 to set controller into Client mode. To work

**1 : DHCP DISABLE**  
**2 : DHCP ENABLE**

2. Press 1 to disable DHCP mode or 2 to enable. To work with NAM select 1.

**DEVICE IP**  
**192.168.050.105**

3. Enter controller address and confirm by pressing the # key. Exemplary address is shown on the display. Next proceed as below.

**SUBNET MASK**  
**255.255.255.000**

**GATEWAY**  
**192.168.050.254**

**CONTROLLER PORT**  
**05000**

**COMPLETED**  
**F1:UP F2:DN**

eng

After selecting 1 you can display and check set parameters.

View by pressing F1 or F2.

Additionally, MAC address of the device is displayed at the end.

The same parameters have to be set in controller configuration menu software.

<b>DEVICE IP</b> <b>192.168.050.105</b>
<b>SUBNET MASK</b> <b>255.255.255.000</b>
<b>GATEWAY</b> <b>192.168.050.254</b>
<b>CONTROLLER PORT</b> <b>05000</b>
<b>HOST (PC) IP</b> <b>192.168.050.001</b>
<b>HOST (PC) PORT</b> <b>05000</b>
<b>DHCP DISABLE</b>
<b>MAC ADDRESS</b> <b>1A:22:BC:FF</b>

eng

## 7.21 Remove Event

This procedure is used to delete identical events (type) from controller memory and compress it in one event to decrease transmit time and increase free memory size.

Below you can find the procedure of setting alarm system. It is done by the Admin in the setup mode.

**21. REMOVE EVENT**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**REMOVE EVENT?**  
**1 : YES 2 : NO**

2. Press 1 to remove or 2 to cancel.

eng

## 7.22 Wiegand Type

This procedure is used to set the type of info sent via controller Wieganda output. You can send user ID or user card number.

Below you can find the procedure of enabling this function. It is done by the Admin in the setup mode.

**22. WIEGAND TYPE**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**WIEGAND SELECT**  
**1 : ID 2 : CARD**

2. Press 1 to send ID or 2 to send card number.

## 7.23 Wieganda Time

This procedure is used to set the time of impulses sent via controller Wieganda output. You are advised to use the default settings.

Below you can find the procedure of enabling this function. It is done by the Admin in the setup mode.

**23. WIEGAND TIME**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level

**TIMING 50uS\*2**  
**50uS \* PUT [1\*5]**

2. Enter from 1 to 5 to et Wiegand time.

## 7.24 Display COM

This procedure is used to enable RS port for the printer or display. Below you can find the procedure of enabling this function. It is done by the Admin in the setup mode.

**24. DISPLAY COM**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**ENABLE SERIAL?**  
**1 : YES 2 : NO**

2. Press 1 to enable or 2 to disable.

eng

## 7.25 Language

This procedure is used to select a language in which messages are displayed on the LCD display. Below you can find the procedure of enabling this function. It is done by the Admin in the setup mode.

**25. LANGUAGE**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**SELECT LANGUAGE**  
**1. ENGLISH**

2. Press F1 or F2 to select a language:
  1. English
  2. Polish
  3. German
  4. Russian
  5. Spanish

## 8. Scanner Setup

### 8.1 Rescanning

This procedure is used to set scanning parameters. You can decide how many times fingerprints are scanned during the process of user identification and verification. Default is 3 time.

Below you can find the procedure of setting scanner parameters. It is done by the Admin in the setup mode.

**6> SCANER SETUP**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**1. RE-SCANNING**  
**# ENTER F4:ESC**

3. . Press the # key to go to the next menu level.

**6> SCANER SETUP**  
**F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**NUMBER SETUP 1-9**  
**C : 3 S :**

4. Enter digit from 1 to 9 . Confirm by pressing the # key.

### 8.2 Scanning Level

This procedure is used to set scanning parameters. You can decide which security level will be used during the process of user identification and verification. Higher access level need higher security level. Below you can find the procedure of setting scanner parameters. It is done by the Admin in the setup mode.

**2. LEVEL**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**SELECT LEVEL 1-7**  
**C : 5 S :**

2. Enter digit from 1 to 7.

### 8.3 Lightning Conditions

This procedure is used to set scanning parameters. Here we can select lightning conditions in which scanner and controller will work. Correct settings greatly reduce rejection rate.

Below you can find the procedure of setting lightning conditions. It is done by the Admin in the setup mode.

**3. LIGHTING CON.**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**SELECT CONDITION**  
**<OUT> 1:OUT. 2:IN**

2. Select 1 for indoor operation or 2 for outdoor operation. You can see the current settings displayed in brackets.

## 8.4 Enroll Mode

This procedure is used to set scanning parameters. Here you can select the number of enrolling per one templates per each finger.

Below you can find the procedure of setting the number of enrolling. It is done by the Admin in the setup mode.

**4. ENROLL MODE**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**SEL. ENROLL MODE**  
**<1> 1 : 2FP 2 : 1FP**

2. Select 1 to generate 2 templates or 2 to generate 1 template. Default setting is shown in brackets - 1 for 2 templates.

eng

## 8.5 Identification Speed

This procedure is used to set identification speed. In case of small database (up to 100 templates) identification speed is not significant.

Below you can find the procedure of setting identification speed. It is done by the Admin in the setup mode.

**5. IDENT. SPEED**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**SELECT SPEED 1-6**  
**C : 5 S :**

2. Select any value from 1 to 6. Default value - 5.

## 9. Sensor Setup

### 9.1 Input Type

This procedure is used to set sensor input parameters.

Below you can find the procedure of setting sensor input parameters. It is done by the Admin in the setup mode.

**7> SENSOR SETUP  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**SELECT SENSOR  
ENTER NUM 1-3**

4. Enter digit from 1 to 3.

**7> SENSOR SETUP  
F1:UP F2:DN**

2. Press F1 to go to the next menu level.

**SENSOR 1 N/O  
1NO 2:N/C**

5. Select 1 for NO type or 2 for NC type.

Set the input type for the other sensors in the same way.

**1. INPUT TYPE  
# ENTER F4:ESC**

3. Press the # key to go to the next menu level.

### 9.2 Function

This procedure is used to set sensor input parameters.

Below you can find the procedure of setting sensor input parameters. It is done by the Admin in the setup mode.

**2. FUNKTION  
# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**SENSOR 1 1. EXIT  
1 SETUP 2 : CANCEL**

3. Select 1 to go to setup or 2 to cancel

**SELECT SENSOR  
ENTER NUM 1-3**

2. Select sensor from 1-3.

**SELECT FUNKTION  
F1:UP F2:DN**

4. Press F1/F2 to select function.

5. Press F1/F2 to select function.

<b>0. INACTIVE</b> F1:UP F2:DN	<b>5. DOOR CONTACT</b> F1:UP F2:DN
<b>1. EXIT</b> F1:UP F2:DN	<b>6. INTRUSION</b> F1:UP F2:DN
<b>2. ALRM</b> F1:UP F2:DN	<b>7. LOCK DOWN</b> F1:UP F2:DN
<b>3. FIRE ALARM</b> F1:UP F2:DN	<b>8. F. KEY - F2</b> F1:UP F2:DN
<b>4. LOCK</b> F1:UP F2:DN	<b>9. F. KEY - F4</b> F1:UP F2:DN

Sensors are used with conjunction with alarm setups. Once the sensor is made active, go to alarm setup and configure to output setup.

### 9.3 Line Fault

This procedure is used to set sensor input parameters. Below you can find the procedure of setting sensor input parameters. It is done by the Admin in the setup mode.

**3. LINE FAULT**  
# ENTER F4:ESC

1. Press the # key to go to the next menu level.

**DO NOT SUPPORT**

2. This feature is not support in this version now.

### 9.4 Bell active

This procedure is used to set sensor input parameters. Below you can find the procedure of setting sensor input parameters. It is done by the Admin in the setup mode.

**4. BELL ACTIVE**  
# ENTER F4:ESC

1. Press the # key to go to the next menu level.

**SENSOR 1: 0**  
ENTER NUM:

3. Enter number from 1 – 5

**SELECT SENSOR**  
ENTER NUM 1-3

2. Select sensor from 1-3.

**ENTER NUM: 0-5**  
ENTER NUM: 4

4. Press the # key to confirm.

## 10. Alarm Setup

### 10.1 Alarm Setup

This procedure is used to set sensor alarm functions.

The controller, depending on the version, have 3 sensor inputs, 2 relays and a built-in buzzer. One of the relays is most often used to control the lock whereas the second one can be used for announcing alarms. When an alarm takes place the controller can:

- Activate buzzer and relay
- Activate only buzzer
- Activate only relay
- Do nothing

The list of events that are monitored and can trigger the alarm can be found below in the alarm menu. Below you can find the procedure of setting alarm parameters. It is done by the Admin in the setup mode.

**8> ALARM SETUP**  
**# ENTER F4:ESC**

1. Press the # key to go to the next menu level.

**8> ALARM SETUP**  
**F1:UP F2:DN**

2. Press F1 to go to the next menu level. Using F1/F2 buttons you can scroll the list of 13 positions. 10 positions apply to alarm situations. The other 3 apply to alarm time, activating alarm system and siren.

**1. CASE OPEN**  
**# ENTER F4:ESC**

8.1. Alarm from the housing sabotage detector. Press the # key to go to the next menu level.

**2. INTRUSION**  
**# ENTER F4:ESC**

8.2. Alarm from motion detector - assigned to sensor. Press the # key to go to the next menu level.

**3. FORCE OPEN**  
**# ENTER F4:ESC**

8.3. Alarm from door status detector - assigned to sensor 1 or 5. Press the # key to go to the next menu level.

**4. ALARM SENSOR**  
**# ENTER F4:ESC**

8.4. Alarm from motion detector - assigned to sensor 2. Press the # key to go to the next menu level.

**5. FIRE**  
**# ENTER F4:ESC**

8.5. Alarm from fire detector - assigned to sensor 3. Press the # key to go to the next menu level.

**6. DURESS**  
**# ENTER F4:ESC**

8.6. Forced entrance discrete alarm. This function has to be enabled in the system setup menu. Press the # key to go to the next menu level.

**7. LINE TROUBLE**  
**# ENTER F4:ESC**

8.7. Sensor alarm.  
 Press the # key to go to the next menu

**8. BOLT OPEN**  
**# ENTER F4:ESC**

8.8. Bolt open alarm. Press the # key to go to the next menu level.

**9. DOOR HELD**  
**# ENTER F4:ESC**

8.9 Door held alarm. Press the # key to go to the next menu level.

**10. LOCK HELD**  
**# ENTER F4:ESC**

8.10. Lock held alarm. Press the # key to go to the next menu level.

**11. ALARM TIME**  
**# ENTER F4:ESC**

8.11. Alarm duration setup.  
 Press the # key to go to the next menu level. After selecting 11 you can set alarm duration time.

**ALARM TIME SETUP**  
**C : 03 S :**

**12. ALARM OFF**  
**# ENTER F4:ESC**

8.12. Alarm Off. Press the # key to go to the next menu level.

**ALARM OFF ?**  
**YES : 1 NO : ANY**

Press 1 to turn the alarm off or any key to cancel.

**13. ALARM BELL**  
**# ENTER F4:ESC**

8.13. Activation of bell control.  
 Press the # key to go to the next menu level.

After selecting 1 out of the first 10 positions on the list as or position 13, press the # key to go to the below

**ALARM SETUP ?**  
**1 : SETUP 2 : CANCEL**

Select 1 to enter setup or 2 to cancel.

**SELECT FUNKTION**  
**F1:UP F2:DN**

Press F1 or F2 to select buzzer activation. Current setting is displayed in the upper line.

**1. BUZZER + RELAY**  
**F1:UP F2:DN**

**2. BUZZER ONLY**  
**F1:UP F2:DN**

**3. RELAY ONLY**  
**F1:UP F2:DN**

**1. INACTIVE**  
**F1:UP F2:DN**

Confirm your selection by pressing the # key.

**SETUP COMPLETED**  
**CONT. # STOP: ANY**

eng

## 11. Installation Guide

### Connector Layout

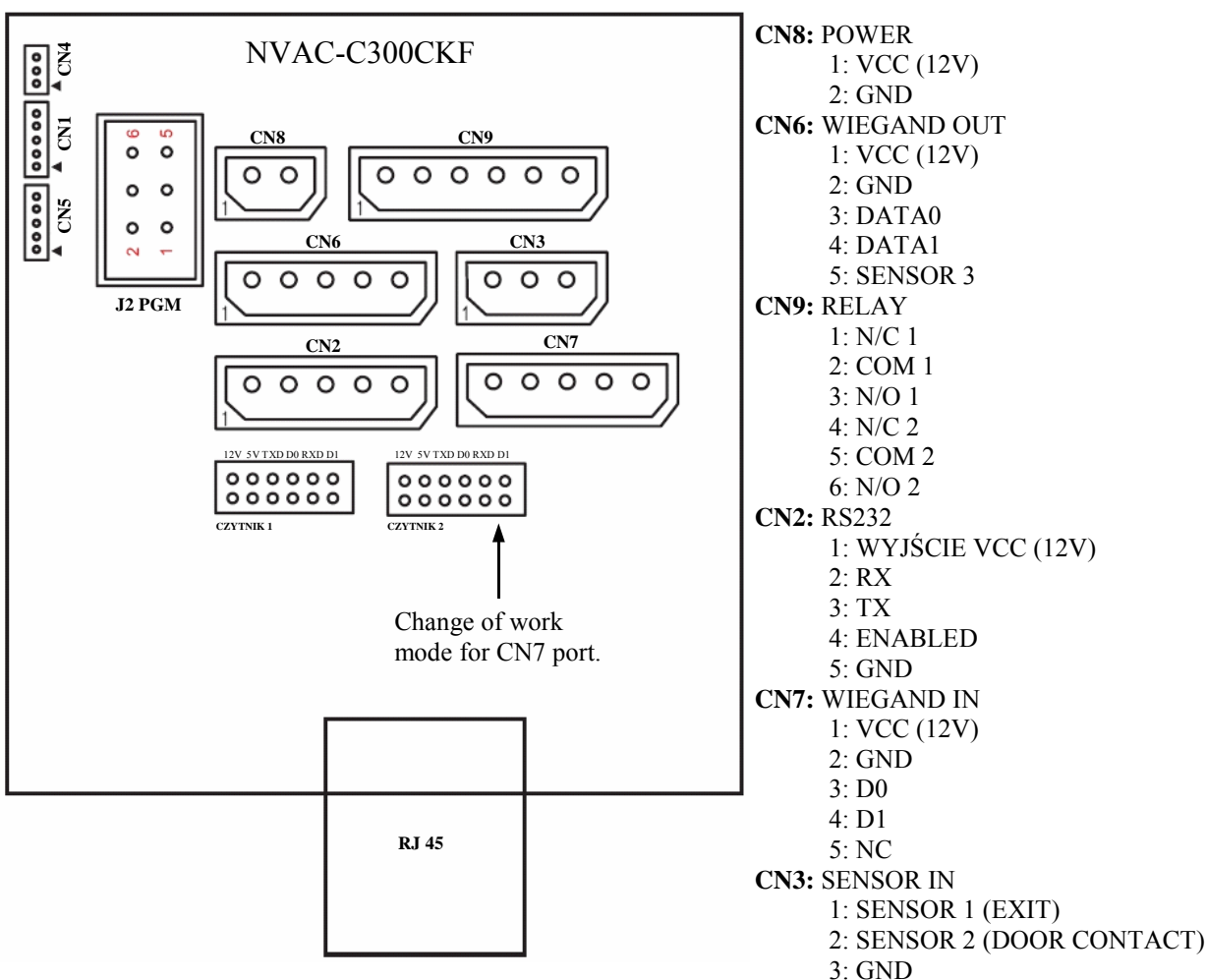
For testing purposes in the autonomic mode use to connectors:

- CN8 12VDC/1A power connector .
- CN9 relay connector that can be used for lock control.

Programming and user registration in the autonomic mode is done from the level of the controller itself utilizing LCD display, keyboard, scanner and a built-in (13,56 MHz) Mifare card.

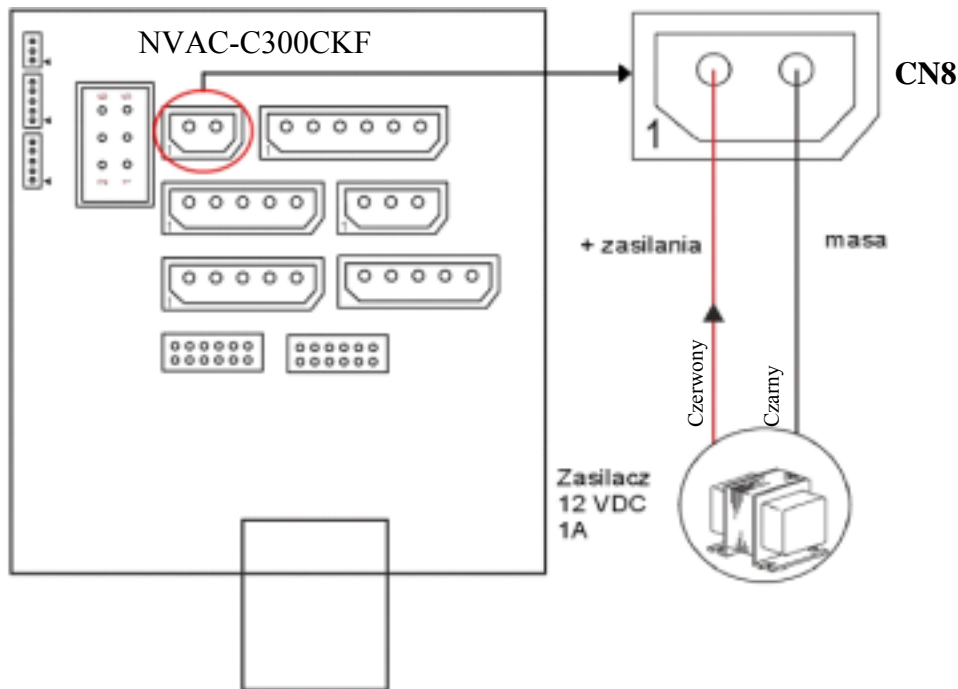
Below you can find the installation procedure.

**ATTENTION:** After tests have been finished delete all the users in accordance with the procedure described in the user's manual so that you can access setup menu.



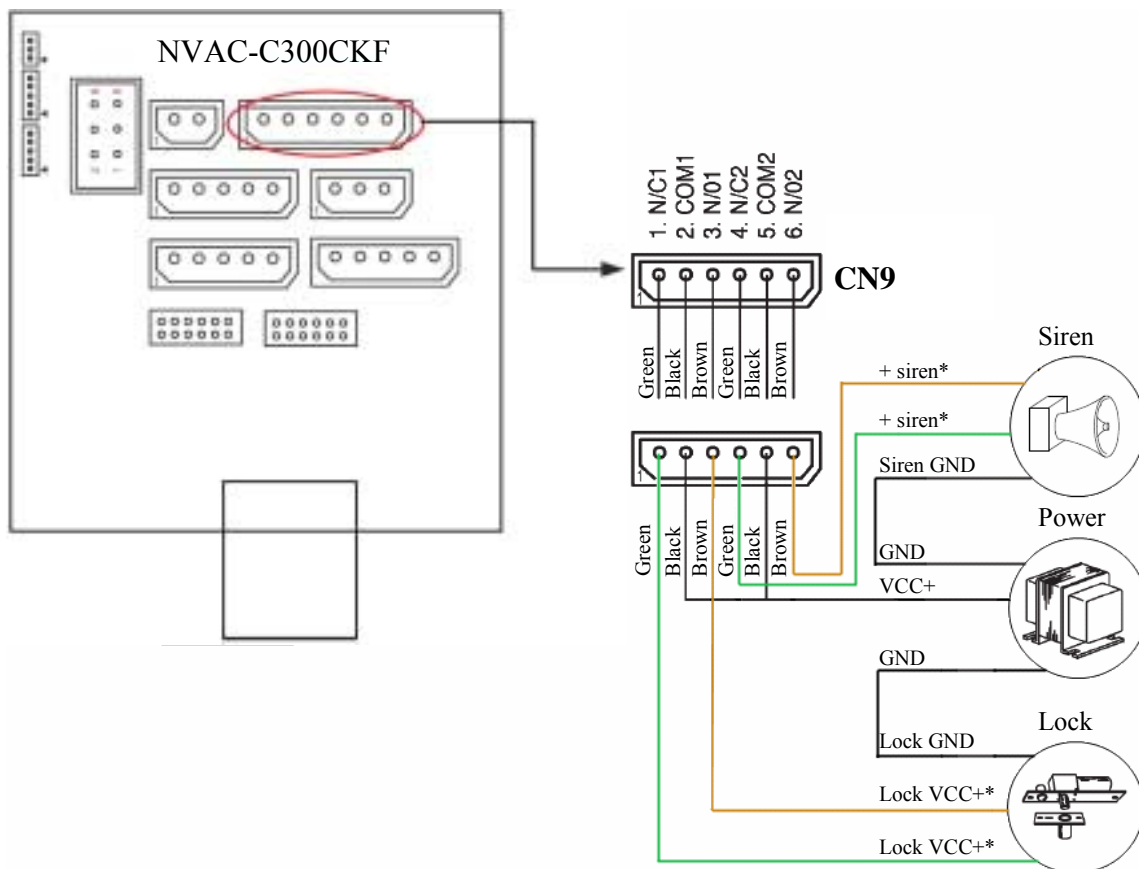
RJ45 connector should be used in network application with NAM (Novus Access Manager) which will be available in the future. In this case remember to set network settings.

## Power Connection



eng

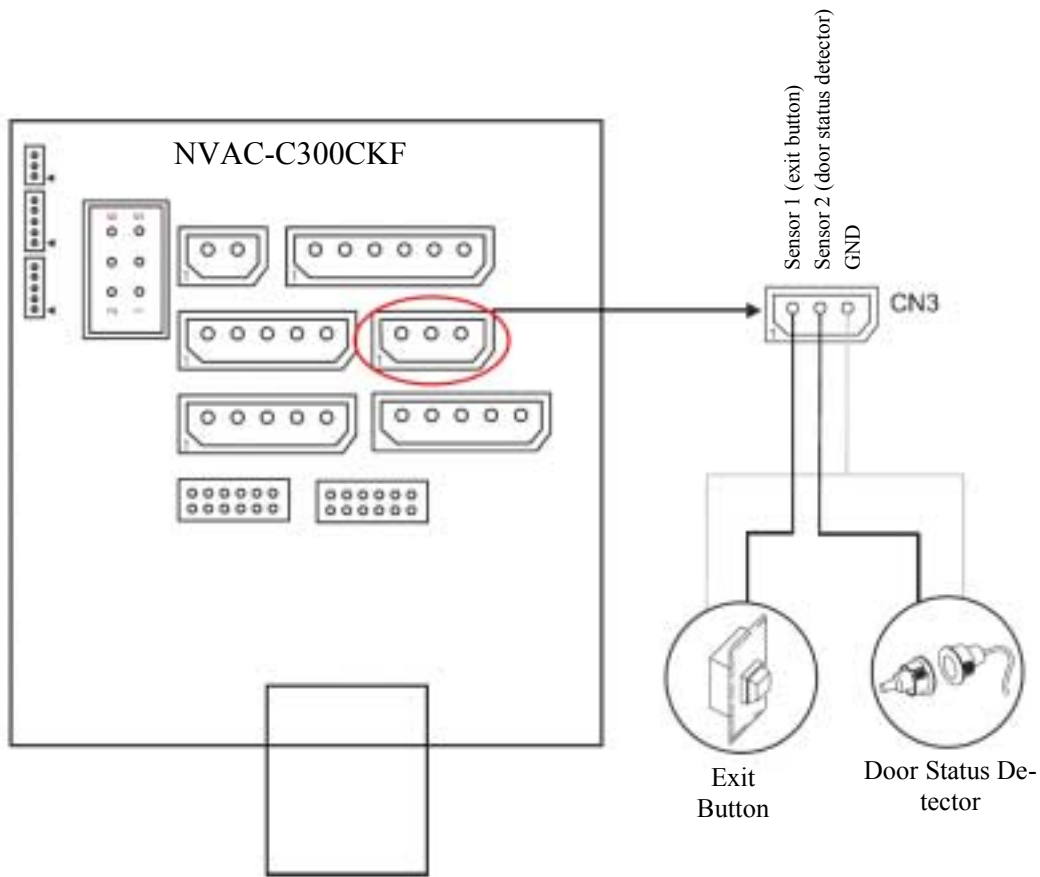
## Relay connection.



### \*NOTE!

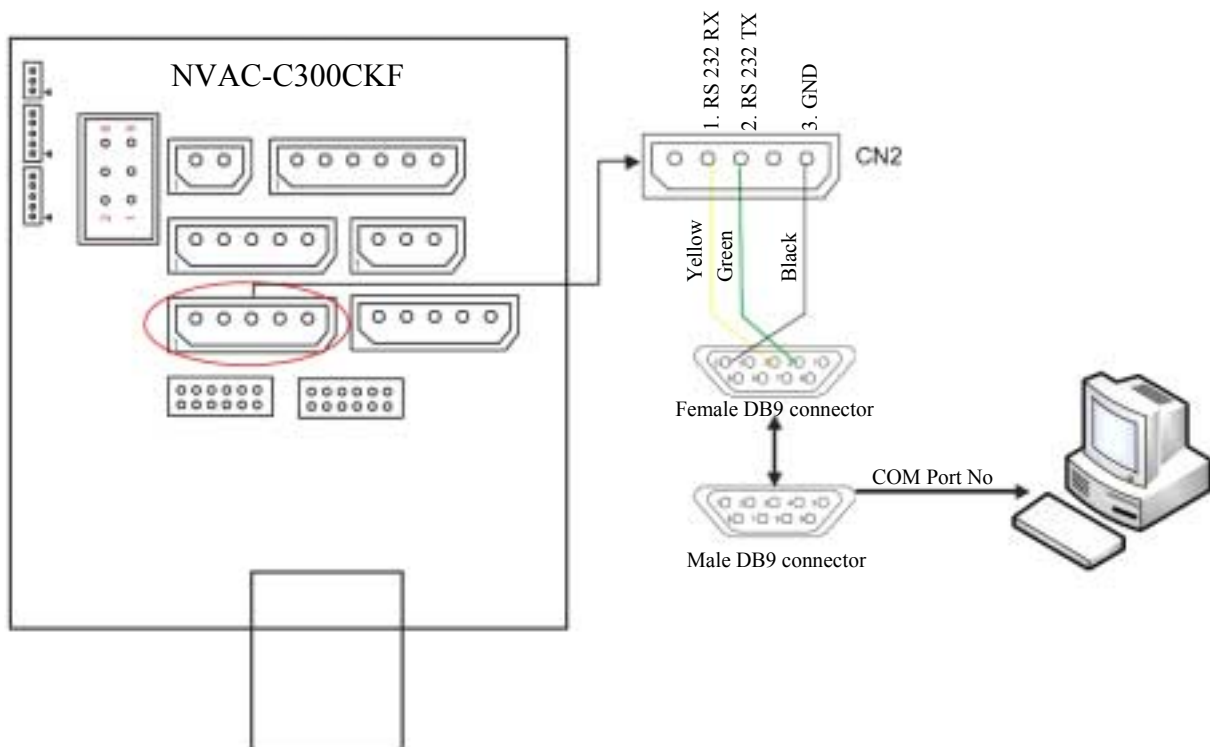
Devices should be connected to relay output utilizing a cable marked as COM and one of the cable marked as N/O or N/C (depending on the type of connected device).

**Connection of door status detector and exit button.**

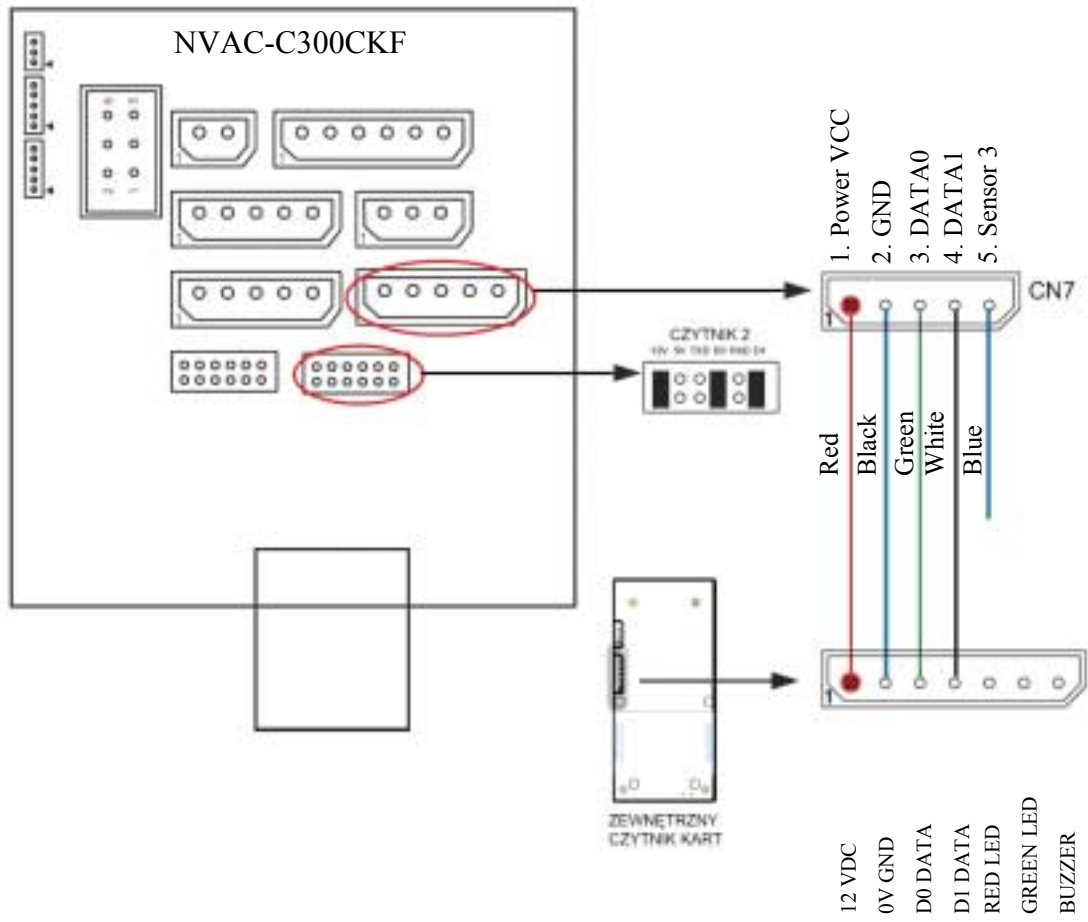


eng

**RS 232 Connection**

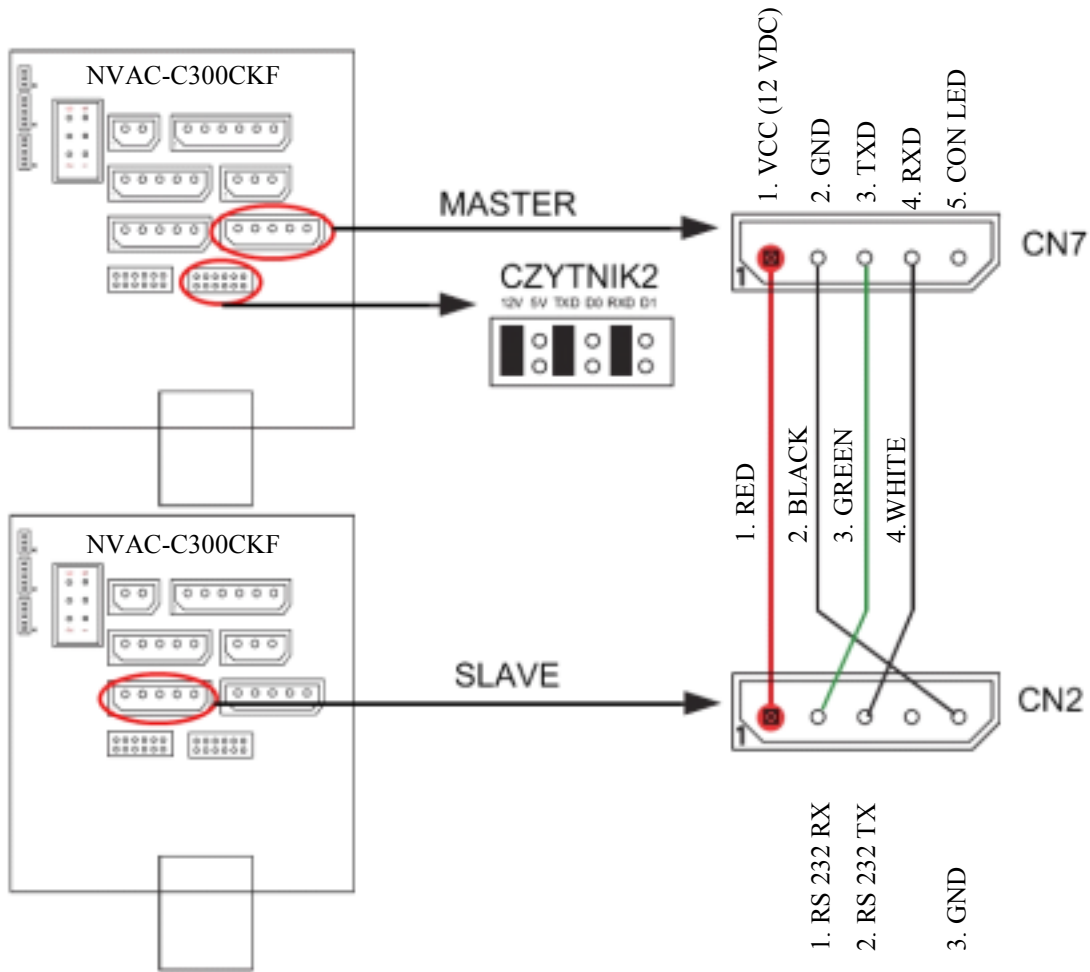


### External Reader Connection



eng

## Two readers connection via RS232



eng

**NOTATKI:**

eng

**NOTATKI:**

eng

**NOTATKI:**

eng

**NOVUS<sup>®</sup>**

**NOVUS Security Sp. z o.o.**

ul. Puławska 431, 02-801 Warszawa  
tel.: (22) 546 0 700, fax: (22) 546 0 719  
[www.novuscctv.com](http://www.novuscctv.com)