BSC-401

User Manual

Version 1.00 *2014.01.*

IDENTIFICATION DEVICE TECHNOLOGY, INC.

http://www.idti.co.kr

COPYRIGHT

WARNING!

- 15.19:

  THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS: (1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE, AND (2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION.

- 15.21:

  The user manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

- NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT
- EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

WARRANTY

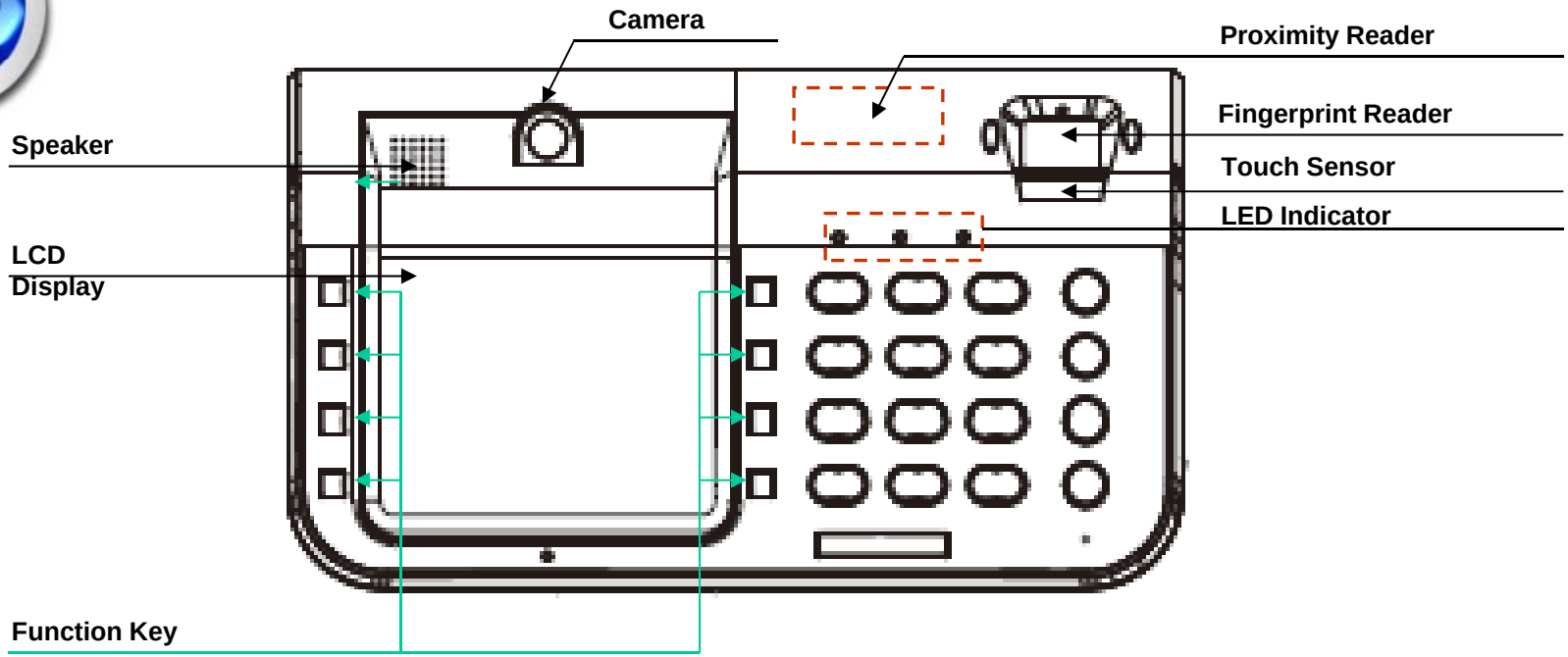
Limited Warranty:

All Products sold to Dealer hereunder shall be subject to IDTi standard warranty for the Product included with the Product by IDTi ("Product Warranty"). The Product Warranty shall be extended to end user purchasers of the Products from Dealer who purchases such Products within twelve (12) months of the date the Products are shipped to Dealer. Provided within the aforementioned time period, the warranty period for a Product shall commence upon the date stated in the Product Warranty. Dealer shall not extend any warranty regarding the Products other than IDTi then standard warranty. The limited warranty statement included in the Product Warranty is the exclusive statement of the controlling terms and conditions of the limited warranties on the Products. Nothing in this Agreement or any other written document or any oral communications with Dealer or other parties may alter the terms and conditions of the Product Warranty. IDTi may, in its sole discretion, revise its limited warranties from time to time, however; no change in limited warranties will affect Product orders already accepted by IDTi. Dealer agrees to only pass on to Dealer's end-users IDTi limited warranties and Dealer will be liable for any greater warranty that Dealer purposely or inadvertently transfers to end-users. Dealer will indemnify, defend and hold IDTi harmless for any damages or other costs that arise because of Dealer's failure to properly inform Dealer's end-users of current limited warranties.

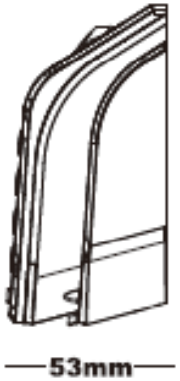
Warranty Disclaimer: IDTi MAKES NO EXPRESS OR IMPLIED WARRANTIES FOR THE PRODUCTS EXCEPT THOSE INCLUDED IN THE PRODUCT WARRANTY. IDTi DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

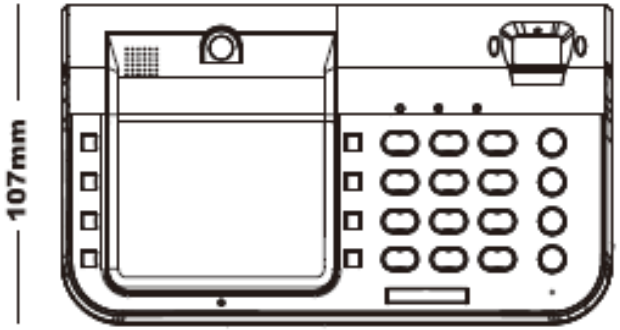
Table of Contents

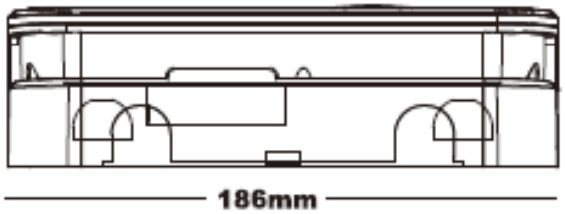
BSC-401 (Layout)



BSC-401 (SPECIFICATION)





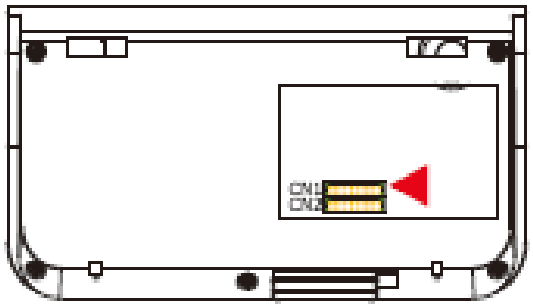


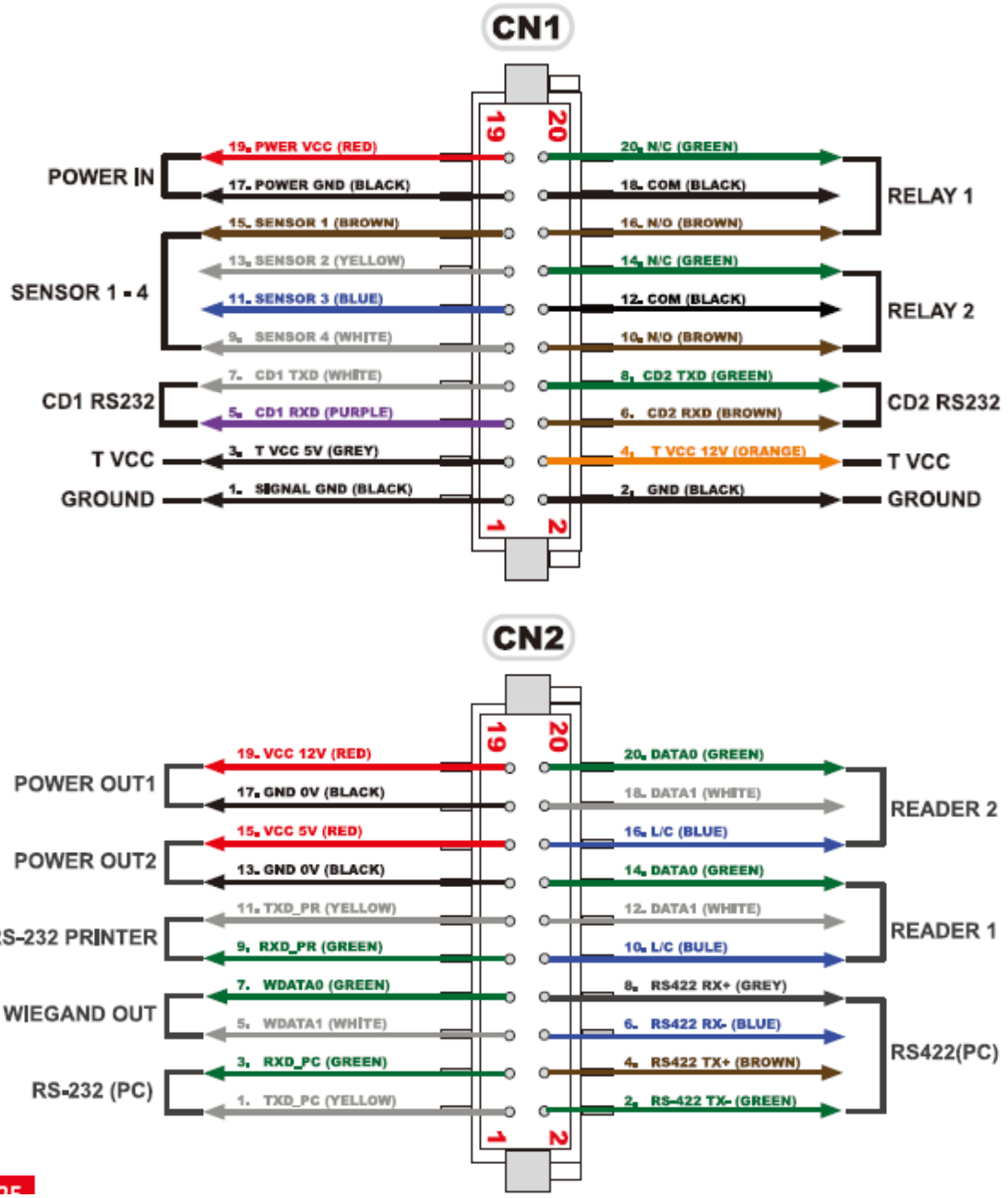
BSC-401 Specification

- ► USER : 131,072
  BSM200 12,000 (48,000-Templete)
  SFM3020 1M – 1900-Templete
  SFM3020 4M – 9590-Templete
- ► Log Data : 1,000,000 (Upto 2,000,000)
  Log Image : 10,000 Upto 20,000
- ► Time Zone : Controller:1024,
  Reader Per 1024
- ► Holiday : 365
- ► User Level : 254
- ► User Group : 1024

- ► FAR = 0.00008 %
- ► FRR = 0.09 %
- ► CPU :
  ARM11 32bit,
  ARM 32-bit Cortex™-M3 CPU
- ► POWER : 12V DC 1A
- ► SIZE :
  - H107 X W186 X D53mm
- ► Temperature : -10℃~50℃
- ► Humidity : 10%~90%
- ► RF Card : ~10 cm
- ► Communication : RS-232 , TCP/IP,
  Option RS-422(1.2 Km),
- ► IN/OUT : 4 In / 2 Out
- ► Material : ABS (Polycarbonate)

Connector Layout





USING THE FINGERPRINT SCANNER

How Much Pressure is Required For a Good-Quality Fingerprint?
If too much pressure is applied to the sensor window, the ridges adhere to each other and are rendered indistinguishable. In this case, the net effect is similar to the hard-to-find minutiae of the wet fingerprint image. Alternatively, if too little pressure is applied the resulting image is similar to the dry fingerprint. Issues related to pressure are easily addressed however. A little practice is all that is needed for users to get the feel of it. Touching the sensor as if pressing a button creates an image that lacks information-rich fingerprint data.
1. Position: Placing your finger far from the center of the sensor will increase the rejection rate. Ridge of the finger must me touching the touch sensor to turn on the fingerprint sensor. Touch sensor is located just below the sensing area.
2. Rotation: Finger rotation should be kept to a minimum during enrollment and verification
3. Pressure: Apply moderate pressure when making contact with the sensor. Too much pressure may cause smudging of the fingerprint. Too little pressure may not allow the sensor to recognize the presence of a finger. The ideal amount of pressure would be similar to a firm grip used to hold a pen

Figure: Improper Alignment Causes Problems

Figure2: Proper Alignment

Position of the Finger
In order to capture the most minutiae, maximize the surface area of the fingerprint on the fingerprint input window by covering the sensor completely. It is okay for the fingertip to extend beyond the length of the sensor to center the fingerprint. Apply pressure lightly and evenly without moving it during the capturing process. Figure2 shows the correct positioning of the fingerprint on the input window. Figure1 shows the most common mistakes made during the initial phase of enrollment.
When the Red light (Fingerprint Scanner) is on, slide the finger across the scanner.
1. Position the finger where the first joint of the finger meets the edge of the sensor.
2. Lower the finger onto the sensor and apply moderate pressure.
3. Keep the finger on the sensor until the Red light (fingerprint scanner) turns off. You may then remove the finger
Getting Good Fingerprint Images
The quality of a fingerprint image is relative to the number of minutiae points captured. If the number and locations of the minutiae remain consistent whenever an individual's fingerprint image is scanned and captured, the fingerprint image is successfully matched to the template of the registered finger. Fingerprint images that do not contain adequate minutiae data are not acceptable as personal credentials, and are therefore invalid. Figure 3 shows poorquality fingerprints, characterized by smudged, faded, or otherwise distorted areas on the fingerprint. Conditions like these may be attributable to a number of factors, including excessively dry or wet skin, or scarring.
1. Use index, middle or ring fingers
2. Avoid using thumb and pinky fingers since they are typically awkward to consistently position on the sensor
3. Completely covering the area of the sensor with the fingerprint will provide the best performance

ENTERING THE SYSTEM MENU

When the reader is powered on with no fingerprint templates enrolled in the unit, anyone can enter the system menu by pressing the F1/p key. If you are enrolling the first administrator card via the reader's keypad, you must first determine the 1~16 digit PIN that the administrator will use. Once this PIN is determined, the administrator must be present to enroll their card into the reader. Note that this operation is not valid if there are administrator card in the reader.

If Administrator has been enrolled

1. Press F1/P key to enter system mode.

Press PRO to enter system mode

2. Key in administrator ID followed by the # key Input fingerprint or Card

3. Present either finger or card which ever administrator has been enrolled with. For now we will use the fingerprint.

4. Now you're into system mode.
Press F1 key to scroll up the main menu
Press F2 key to scroll down the main menu

If no Administrator has been enrolled

1.Press F1/P key to enter system mode

2. Now you're into system mode.
Press F1 key to scroll up the main menu
Press F2 key to scroll down the main menu

Main Menu List

F1/P↑

1. 'F1/P' or 'F2' Key '#' Key.
or Touch Screen

F2 /↓

USER MANAGEMENT

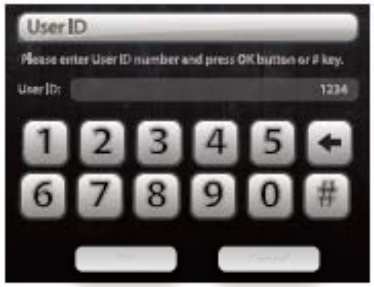
User Enroll

This command is used to add typical fingerprint only users to the reader so that they will be able to gain entry to the location guarded by the reader. The system has an option to enroll either 2 or 4 templates per user. The following key sequence performs this action:

1. Press F1/P key to enter system mode.
   Press PRO to enter system mode

2. Press '#' Key USER MEMAGEMENT Select.

3. Press F1/P(UP) or F2 Key Add-menu Select or Press LCD  Icon



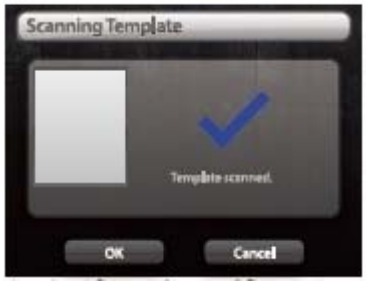
4. Key in user ID from 1 to 16 digits as shown in next figure

5. Key in user ID followed by the # key

6. System has an option to enroll 1~4 fingerprint templates per each user. For now we will select number 1~4 key by enrolling 1~4 templates

 Enroll Fingerprint

 Enroll Card



7. Present first finger to the scanner. Remove the fingerprint when the red light turns off. You can either enroll same fingerprint or different fingerprint after the first. Repeat this process until the last fingerprint

8. Enroll completed. Press the # key to continue enrolling another user fingerprint or press any others to exit off the sub-menu

NOTE :
There are 2 levels of administration,
1. USER (Level 1) - Corresponds to an ordinary user. They may verify, but are not allowed to access any
administrative functions.
2. ADMIN (Level 4) - This is an system administrator level and has full rights to configure the reader.

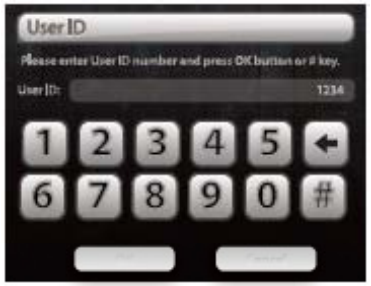
Edit User

This command is used to edit existing users ID by accessing the user ID. When editing, Administrators have the ability to make changes to user ID only in this menu.

1. Press F1/P key to enter system mode.
   Press PRO to enter system mode

2. Press '#' Key USER MEMAGEMENT Select.

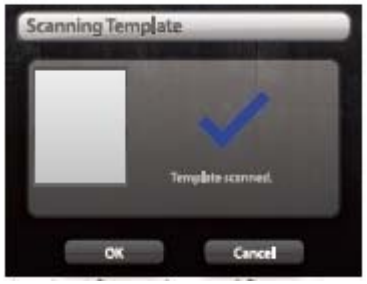
3. Press F1/P(UP) or F2 Key Edit-menu Select or Press LCD  Icon



4. Key in user ID from 1 to 16 digits as shown in next figure

5. Key in user ID followed by the # key

6. System has an option to enroll 1~4 fingerprint templates per each user. For now we will select number 1~4 key by enrolling 1~4 templates



7. Present first finger to the scanner. Remove the fingerprint when the red light turns off. You can either enroll same fingerprint or different fingerprint after the first. Repeat this process until the last fingerprint

8. Enroll completed. Press the # key to continue enrolling another user fingerprint or press any others to exit off the sub-menu

Delete User

Deleting a fingerprint template from a reader will prevent that template from being granted access to the location via the reader. Any fingerprint template can be removed from a fingerprint reader, including administrative and the last remaining fingerprint template on the reader. Templates can be deleted by a single user or all users including administrative templates.

1. Press F1/P key to enter system mode.
   Press PRO to enter system mode

2. Press '#' Key USER MEMAGEMENT
   Select.

3. Press F1/P(UP) or F2 Key Delete-menu Select or Press LCD Icon

4. Key in user ID from 1 to 16 digits as shown in next figure

5. Key in user ID followed by the # key

Deleting a all user will erase all template from a reader, including administrative and the last remaining fingerprint template on the reader.

1. Press F1/P key to enter system mode.
   Press PRO to enter system mode

2. Press '#' Key USER MEMAGEMENT
   Select.

3. Press F1/P(UP) or F2 Key Delete All-menu Select or Press LCD Icon

4. Press 'OK' or Press the # key to confirm delete all
Press any other key to cancel

View User

At any time, you can view a list of all users of the system. The list can be an overall enrollment list of all users in the system, or it can be a list of the individual users that are physically enrolled on any individual fingerprint reader.

1. Press F1/P key to enter system mode.
   Press PRO to enter system mode

2. Press '#' Key USER MEMAGEMENT Select.

3. Press F1/P(UP) or F2 Key View-menu Select or Press LCD Icon

4. View Enrolled User / Total User.

5. Press F1(UP) or F2(DN) Key.

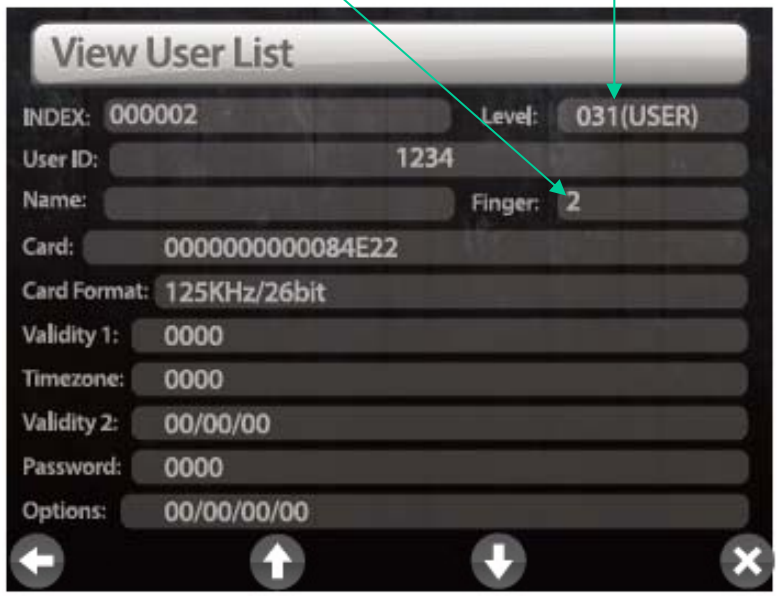
Memory Index

User Id

User Name

Card Number

Fingerprint Count **USER LEVEL**

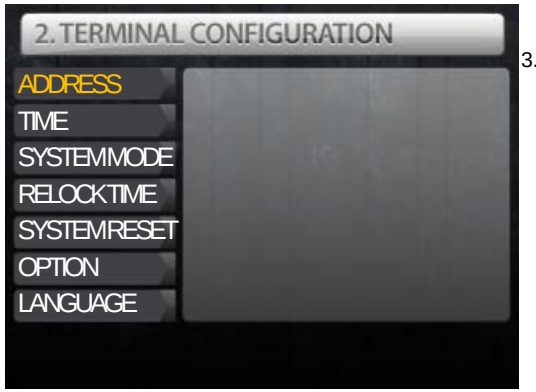


CHAPTER 2

DEVICE SETTING

System setup

1. Press F1/P key to enter system mode.
   Press PRO to enter system mode
2. Press '#' Key TERMINAL Select



3. Press F1/P(UP) or F2 Key or Press Touch LCD Menu Select

ADDRESS

1. LOCAL ADDRESS : 1~32
2. SYSTEM ADDRESS : 0~65535

TIME

System Time Setup

SYSTEM MODE

Device Access Mode Setup
CARD / FINGER
CARD/ ID&FINGER
ID&CARD&FINGER
ID / CARD/ FINGER
FINGER(ID&FINGER)
ID&FINGER
CARD&FINGER
ID&FINGER ID&CARD
ID&FINGER CARD&FINGER
ID&CARD CARD&FINGER
ID / CARD
ID&CARd
CARD
OPEN
CLOSE

SYSTEM RESET

RELOCK TIME

Lock Time Setup
1~99 Sec

OPTION : Access Option Setup

ANTIPASS BACK
KEY SECURE
LOCK DOWN
FUNCTION KEY
DAY DISPLAY TYPE
DURESS

LANGUAGE : Display Language Setup

Log

1. Press F1/P key to enter system mode.
   Press PRO to enter system mode
2. Press '#' Key SYSTEM LOG Select

3. Press F1/P(UP) or F2 Key or Press Touch LCD Menu Select

LOG VIEW

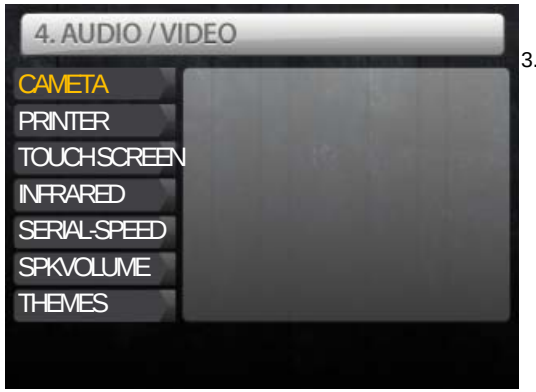
INDEX CHANGE

LOG FORMAT

PHOTO FORMAT

AUDIO/VIDEO

1. Press F1/P key to enter system mode.
   Press PRO to enter system mode
2. Press '#' Key AUDIO/VIDEO Select



3. Press F1/P(UP) or F2 Key or Press Touch LCD Menu Select

CAMETA

- CAMERA ENABLE/DISABLE
- EVENT MODE ENABLE/DISABLE
- BRIGHTNESS
- ANGLE
- FRAME RETE
- DENIED SAVE

PRINTER

TOUCH SCREEN

- TOUCH Calibration

INFRARED

- INFRARED ENABLE/DISABLE
- FINGER MODE
- DETECT LEVEL

SERIAL-SPEED

- PC
- PRINTER
- EXTERNAL 1
- EXTERNAL2

SPKVOLUME

THEMES

Network

1. Press F1/P key to enter system mode.
   Press PRO to enter system mode
2. Press '#' Key NETWORK Select

3. Press F1/P(UP) or F2 Key or Press Touch LCD Menu Select

NET VIEW

NET SETUP

System can operate either as Server or Client. If set as Server then the software must be set as Client and if set as Client then the software must be set as Server.

Static/DHCP
IP Address
Gateway
Subnet mask
Port

Server IP Address
Server Port

NET SPEED

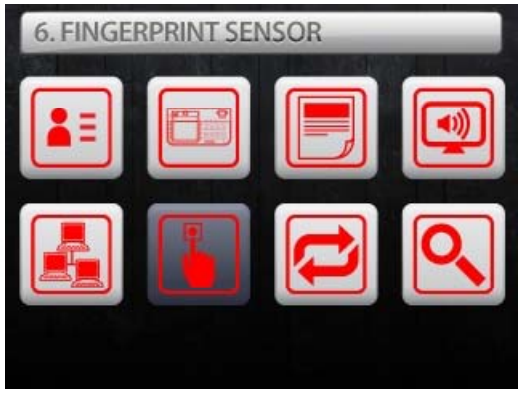
0: Auto-negotiation enable with all capabilities
1: Auto-negotiation with 100 BASE-TX FDX/HDX ability
2: Auto-negotiation with 10 BASE-T FDX/HDX ability
3: REV(0-Auto-negotiation enable with all capabilities)
4: Manual selection of 100 BASE-TX FDX
5: Manual selection of 100 BASE-TX HDX
6: Manual selection of 10 BASE-T FDX
7: Manual selection of 10 BASE-T HDX

CALL SERVER

intercom PC server Setup.

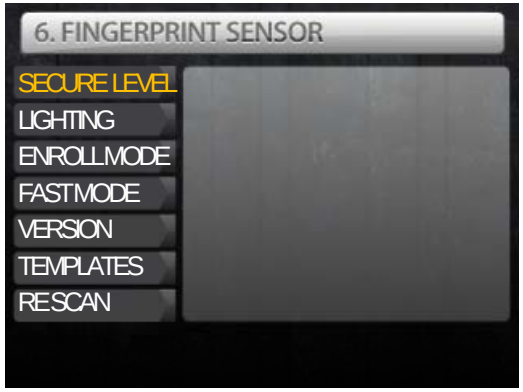
Finger print Sensor

BSC-401 Only .



1. Press F1/P key to enter system mode.
   Press PRO to enter system mode

2. Press '#' Key FINGERPRINT SENSOR Select



3. Press F1/P(UP) or F2 Key or Press Touch LCD Menu Select

SECURE LEVEL

This command sets both the security level that the reader will use when verifying fingerprints and when identifying fingerprints. Security level ranges from 1 to 7, with 3 being the normal value for verification. The highest security setting is 7 and the lowest security setting is 1. Higher security access would normally require a higher security setting.

LIGHTING

This is an operational mode whereby the scanner sets the environment condition. There are 2 conditions available, OUTDOOR and INDOOR. Depending on the mode, scanner automatically adjust it self to the surrounding environment to enhance the scanning ability. Setting the right mode will greatly reduce the false rejection rate(FRR).

ENROLL MODE

There are 2 types of enrollment procedures. By default system is setup to use mode 1 which scans 1 template per finger. Mode 2 scans 2 templates per finger.

FAST MODE

The use of a Identification Speed can accelerate the identification speed up to 10 times at normal speed with relatively small degradation of authentication accuracy. The Identification Speed has 7 different levels from mode 1 to 7.

VERSION

TEMPLATES

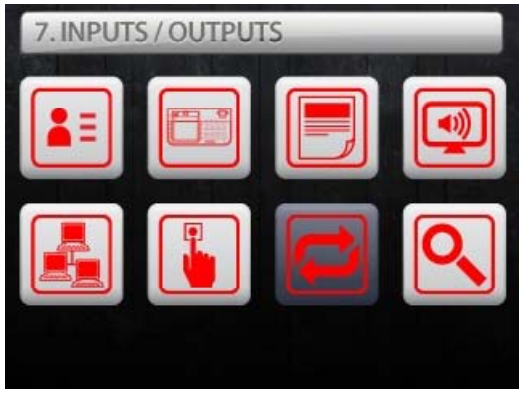
RE SCAN

TEMPLATE TYPE

FAKE DETECT

LATENT DETECT

INPUT / OUTPUT



1. Press F1/P key to enter system mode.
   Press PRO to enter system mode

2. Press '#' Key INPUT/OUTPUT
   Select

3. Press F1/P(UP) or F2 Key or Press
   Touch LCD Menu Select

SENSOR

These are the senor inputs found in device control panel that control external devices. There are 4 sensor inputs in device and all of them can be programmed to handle different types of external sensors from the system menu.

RELAY

The relay output is Normally Open (N.O.), and toggles shorted when triggered by an event, such as an authentication or ID failure. The relay can be used to send power to switched items like electric door strikes, door handles, magnetic hold locks. The alarm can be used to send signals to a alarm panel, controllers or indicators.

ALARM

There are six sensor inputs and 2 relays outputs in the system. Either one or two relays are used for the lock, depending on the configuration, and the spare relays can be used for annunciating alarms or other form of control. There is no programming function for alarms what you program is what happens when a specific alarm occurs. There are two things that can happen as a result of an alarm:
an alarm may result in a message to the speaker (Buzzer).
an alarm may also cause a relay to come on (Relay).
Device has an output to activate a sounder but also equipped with relays that can be controlled from a command station, by some type of system activity. These sensor inputs & relays can allow you to perform many functions such as motion sensor or as a means of interfacing with a home automation system. Only the internal sensors will be activated unless other sensors are connected and configured in Sensor Setup. Relay must be connected to use the alarm. Refer to Relay Connector.

CARD TYPE

1: EM Standard 26bit Card
2: HID Standard 26bit Card
3: HID Full Binary 26bit Card
4: HID IDTi 34bit Card
5: Mifare 32bit UID Card
6: Mifare 34bit iClass
7: Mifare 34bit iClass2
8: Mifare 32bit UID 2
9: Mifare 64bit UID

WIEGAND TIME

Wiegand data output time setup

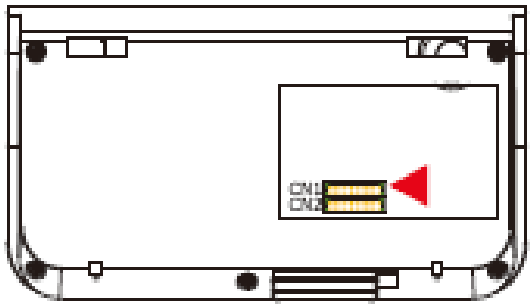
WIGAND TYPE

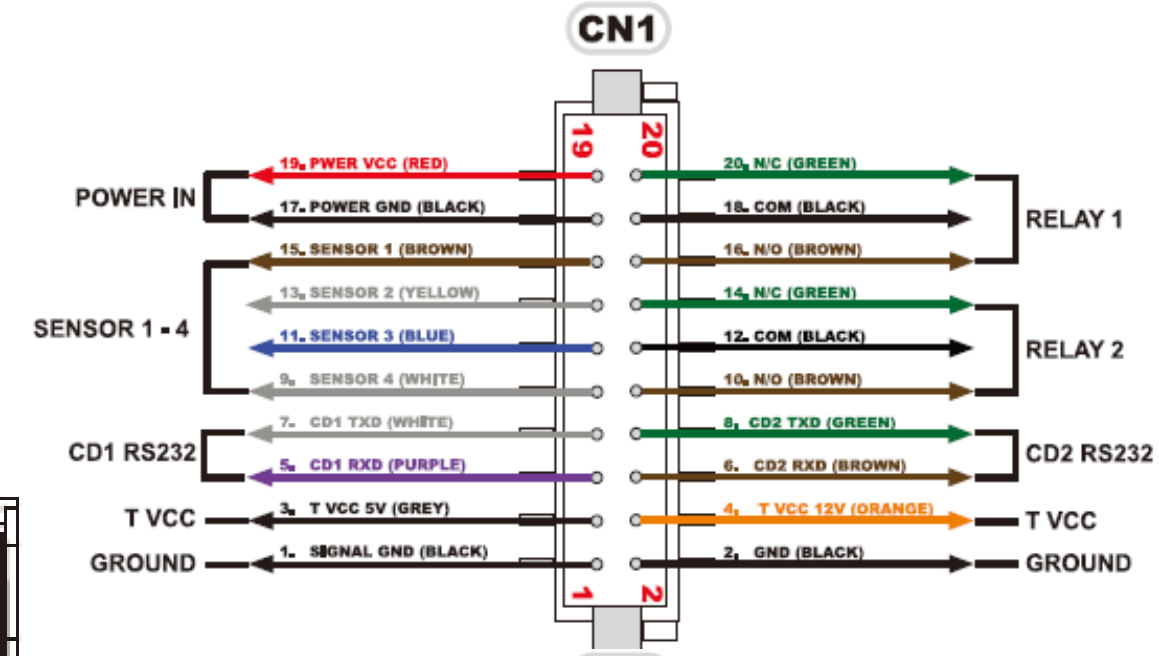
1: USER ID
2: USER CARD
3: CARD READER DIRECT OUTPUT

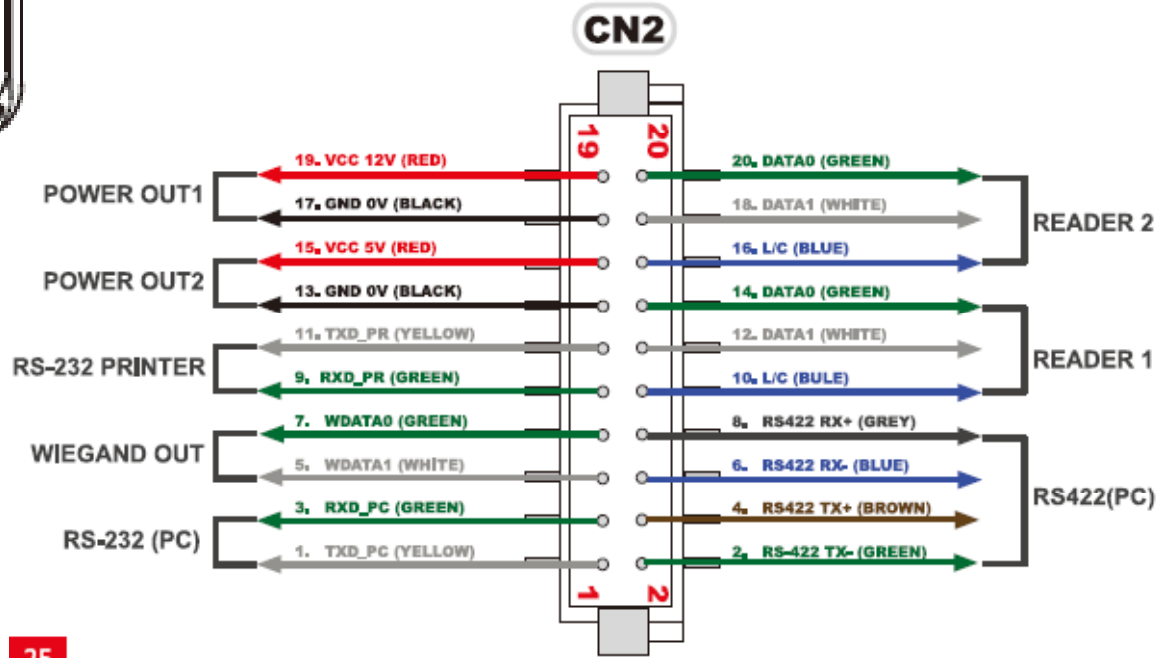
CHAPTER 3

INSTALL

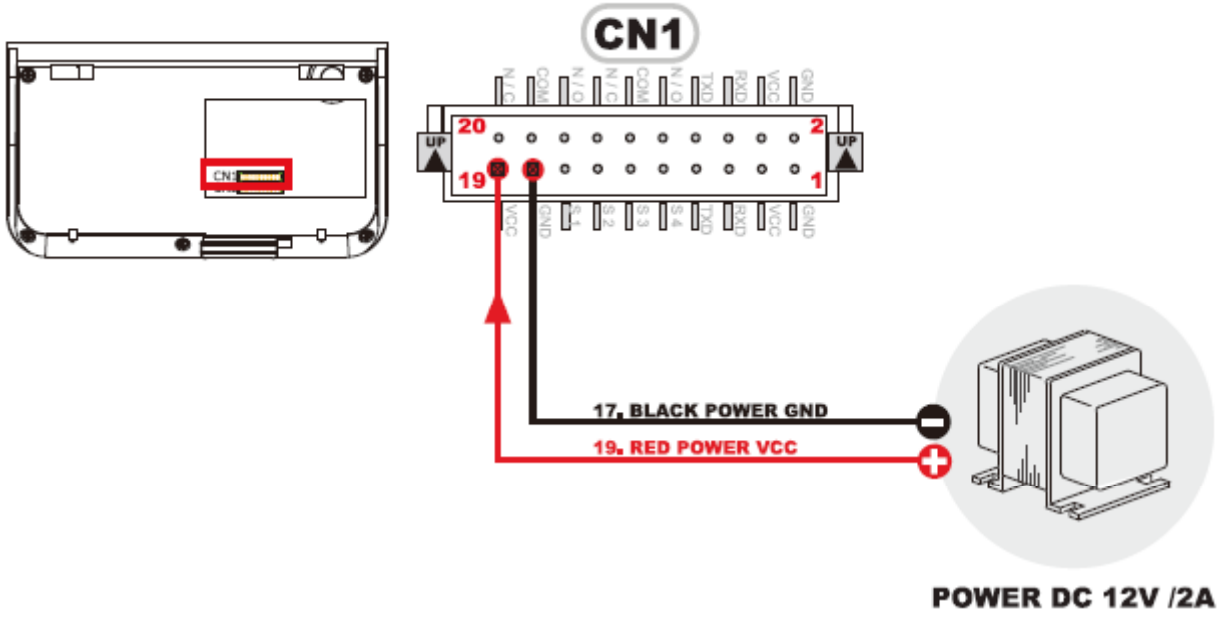
CONNECTOR LAYOUT



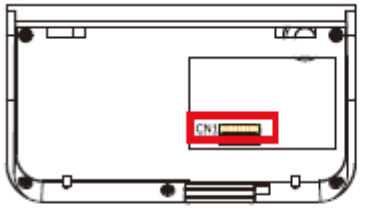


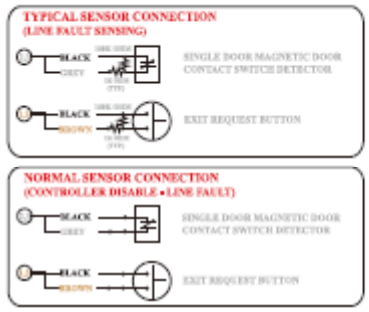


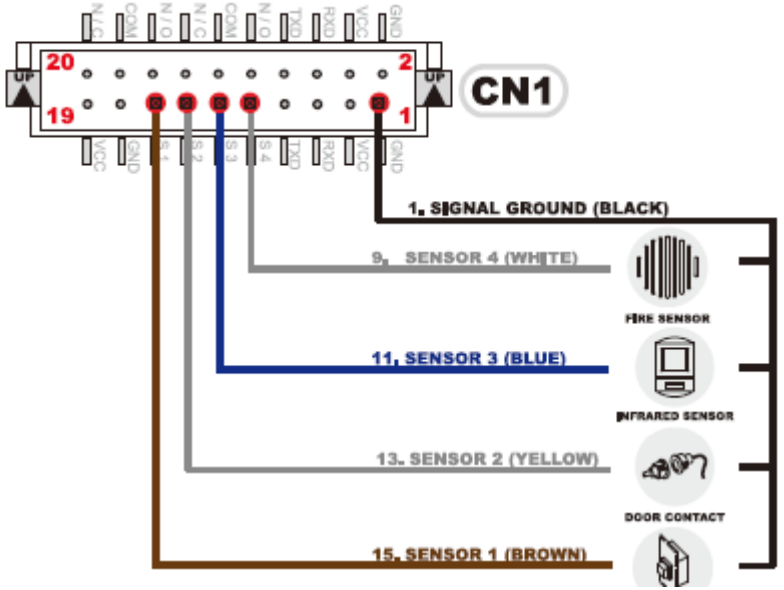
POWER CONNECTOR



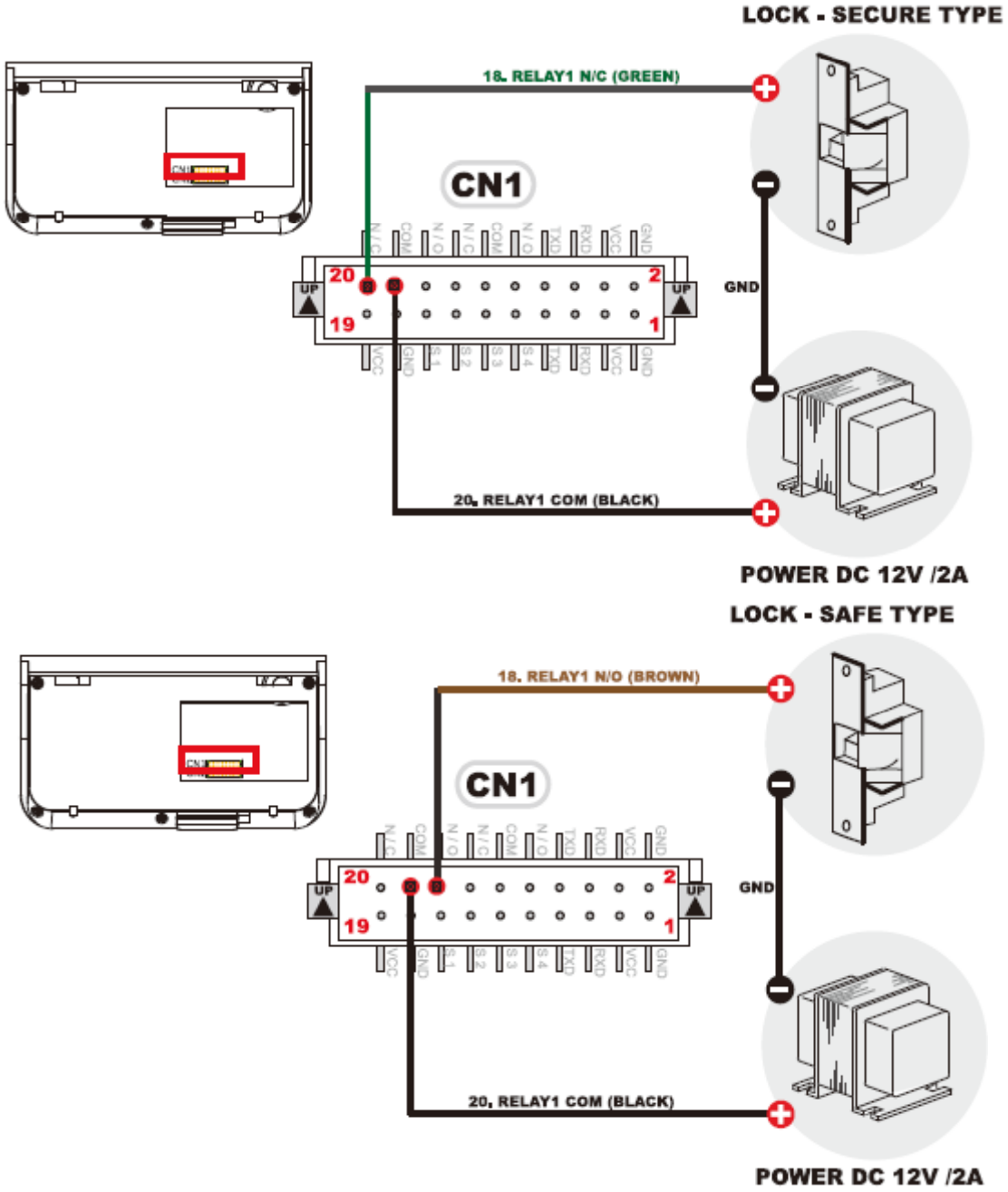
SENSOR CONNECTOR



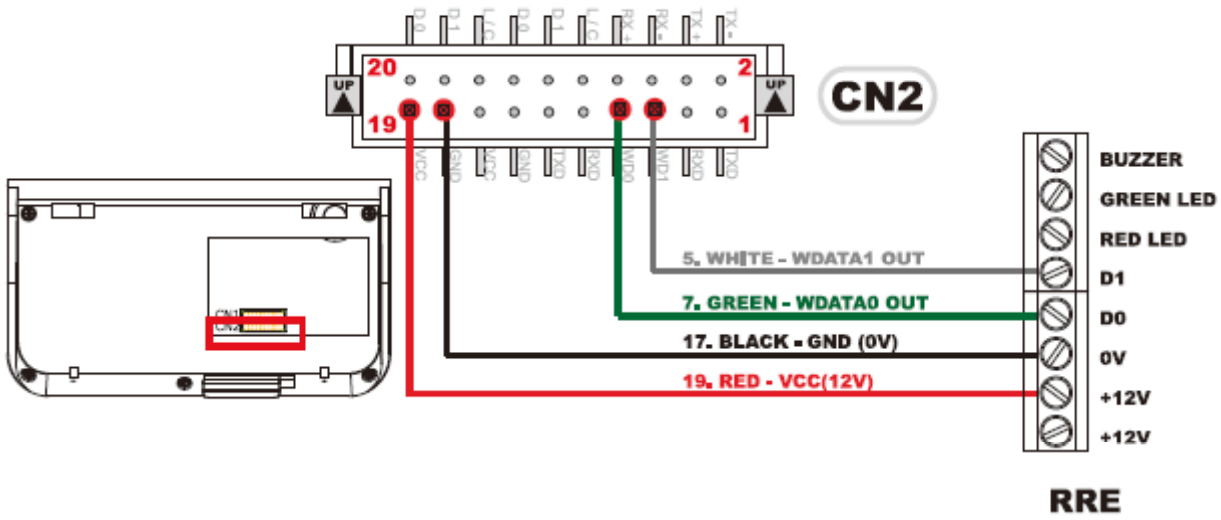




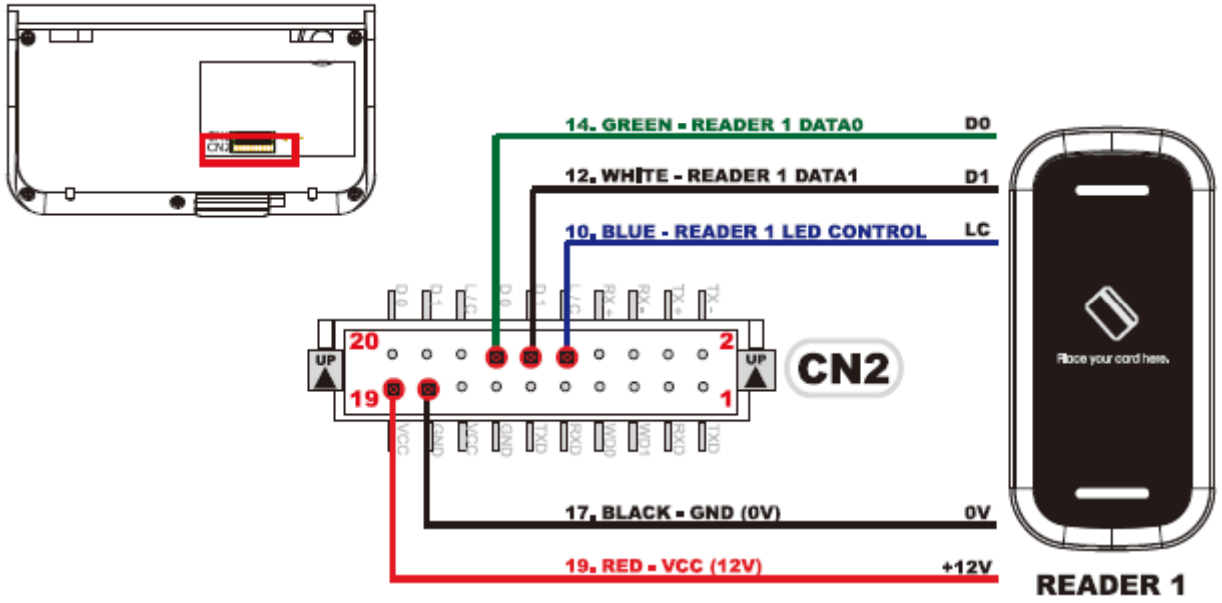
RELAY (LOCK) CONNECTOR



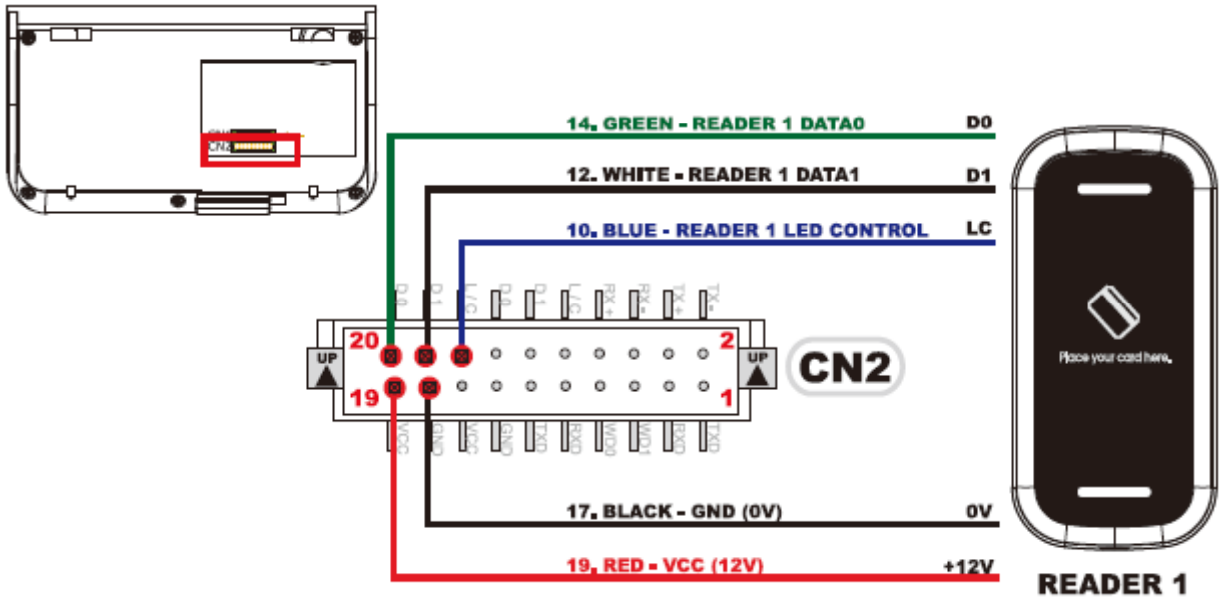
RRE CONNECTOR



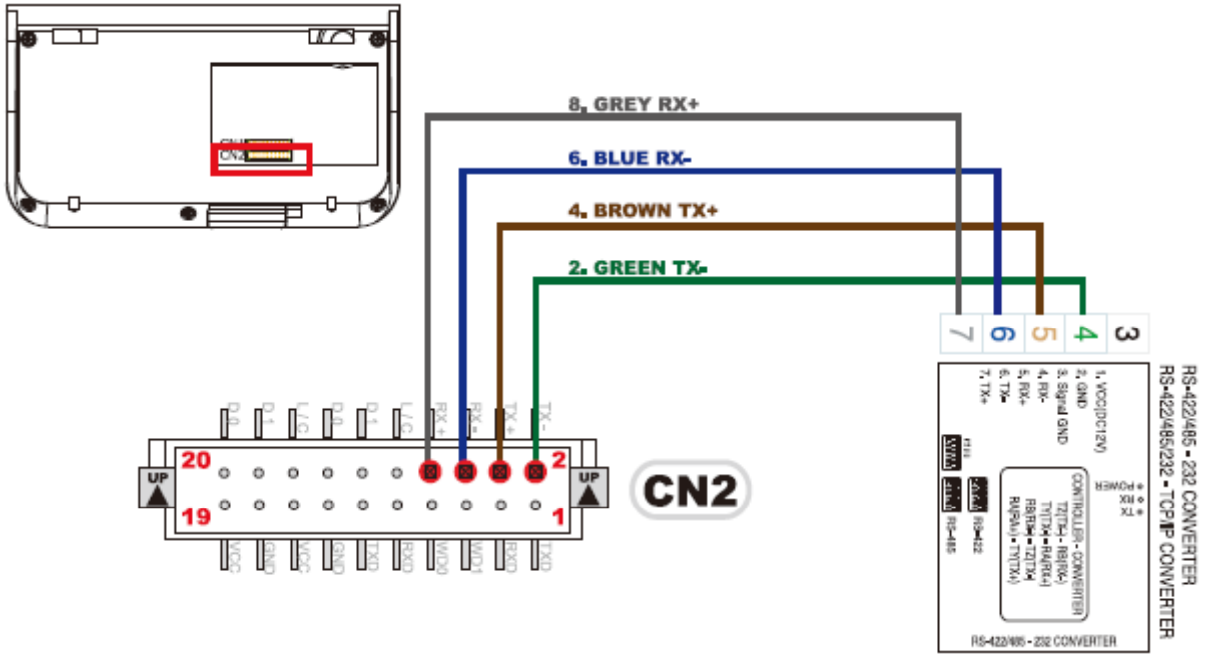
Card Reader 1 Connection



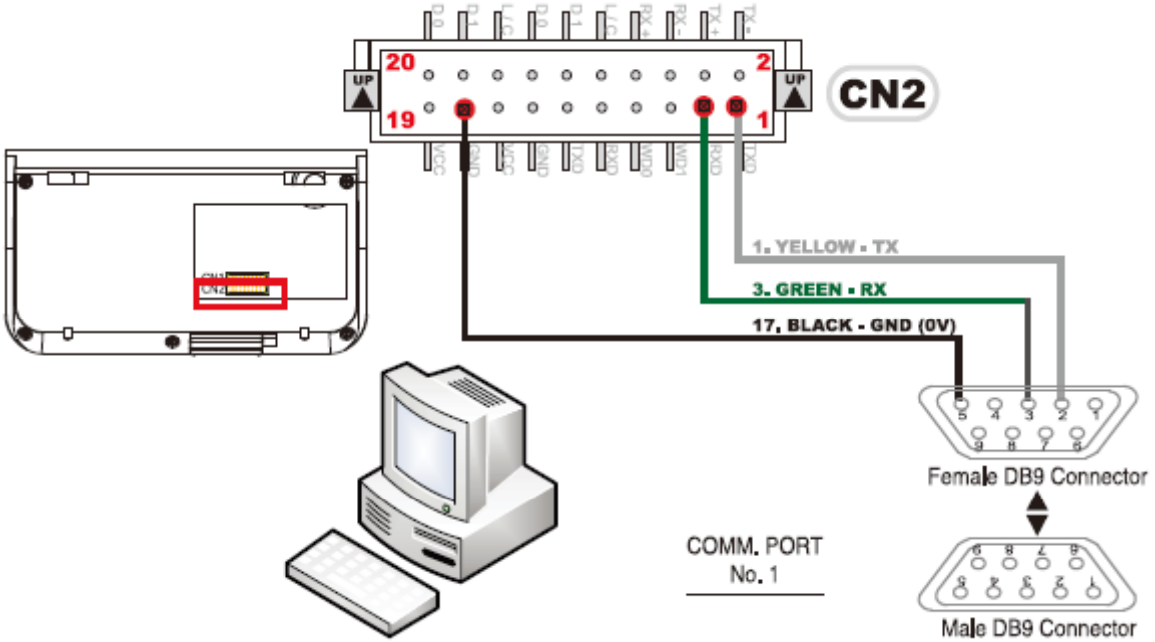
Card Reader 2 Connection



RS422 NETWORK DIAGRAM



RS-232 CONNECTOR



INSTALLATION DIAGRAM