# Smart Face Accesss
# User Manual

# 2APLZ-BT100

## 1. PRESENTATION

Versatile, modern and efficient, the FaceAccess access controller provides enhanced security access to restricted environments, and allows monitoring of schedules and access to the site.

Capable of storing up to 5,000 users password, of which 1,200 will have faces for identity verification.

For authentication equipment, different combinations may be used ( face).

## 2. PACKAGE CONTENT

- ✓ 1 Face Access;
- ✓ 1 Power supply: 12Vdc, 1.5A;
- ✓ 1 Harness 9 cables;

## 3. SPECIFICATIONS SOFTWARE & HARDWARE STAND ALONE

### 3.1 Software

| Item | Description or Capacity |
|---|---|
| Storage Capacity of Faces | 1200 |
| Identification Mode | [ [Face]<br>[Face & Password],<br>[Face &Password] |
| Records of User ID | 5000 |
| Number of digits of an ID | 15 digits (000000000000001～999999999999999) |
| General Records count (Input / Output) | 100000 |
| Records of Management | 10000 |

| | |
|---|---|
| Touch screen | yes |
| Communication Interface | Ethernet, WiFi, RS-485 |
| USB | Yes |
| Languages | English and Portuguese |
| Functions Attendance and Access Control | Lock Control |
| | Control by time or time zone |
| | Operation Mode per hour or time zone |
| | Status of service per hour or time zone |
| Power Management | Automatic shutdown |
| Types of Alarms | Open Door Illegally, Time Open Door exceeded |
| Self Test | Yes |
| Detection of Approximation of person | Yes |

**Table. 1 – Software Specification**

### 3.2 HARDWARE

| Item | Description |
|---|---|
| Camera | 2 (RV and IV) |
| Display | Screen 2.8” TFT LCD |
| Keyboard | Touch Screen Panel |
| Proximity Sensor | Supported |
| Entry of exit button | Supported |
| Entrance of Door Sensor | Supported |
| Alarm Relay | Supported |
| Relay of Door | Supported |
| Communication | TCP-IP, WIFI (optional), RS485 |
| U-disk, USB | Supported (USB Optional) |
| Audio Output | Supported (IIS Mode) |
| RTC | Supported |
| Temperature | -10°C~ +60°C |
| Supported humidity (RH) | 20% ~ 80% |

**Table. 2 – Hardware Specification**

## 4. USERS STORAGE CAPACITY

The FaceAccess access controller when in stand alone, is capable of storing up to 5,000 users (password), of which 1,200 users can make use of the face as another access option.

## 5. AUTHENTICATION MODE

The identity verification can be made via Face, PIN (password) or combination of them; supported the verification modes are:

- ✓ **Face;**
- ✓ **PIN (Password)**
- ✓ **Face+PIN (Password);**

## 6. DATASHEET

The following table reports the technical characteristics of FaceAccess access controller.

| **Item** | **Description** |
|---|---|
| Camera | 2 cameras for facial recognition |
| Display | 2.8” Touch Screen |
| Presence Sensor | Presence sensor of approximately 50 cm |
| LED | 4 LEDs |
| Communication | TCP-IP,WIFI,RS485 |
| Connection | USB port |
| Audio Output | One speaker |
| Feed | Output (Voltage DC7.5 ~ 13V) |

| | |
|---|---|
| | (Current: 2A) |
| Temperature | -10º ~ +60º |
| Supported humidity (RH) | 20% ~ 80% |
| Languages | English and Portuguese |

## 7. USER

É possível utilizar o FaceAccess em dois níveis de usuário:

- **Supervisor:** user level with full permission of access to the internal settings of the equipment menu. Among the internal settings, you can c adastrar, remove users, and change any equipment configuration. To access the mode Master User, you must enter the PIN (password) this user, The FaceAccess only recognize the supervisor through their respective password (PIN). For supervisor configuration must be accessed the "Security" menu.
- **User**:. User level with only permitted to make access, this user does not register, remove users or change their usage settings Access this user will be done after / or password (PIN) and / or face .

**COMMENTS:** It is only permitted the registration of a supervisor equipment by setting a password (PIN) to the supervisor.

## 8. MENU

To access the Device menu, click Home in the upper left corner of the main screen.

Fig. 1 – Home Icon

If there is one or more registered supervisors, the device will require a check. If there are no registered supervisors, the menu is accessed directly.

Fig. 2 – User (PIN) Icon

To do verification by PIN a registered user, click Enter the password located on the top, right of the main screen.

### 8.1. Registration and User Exclusion

Fig. 3 – User

Fig. 4 - Subscribe user

Fig.5 – Delete User

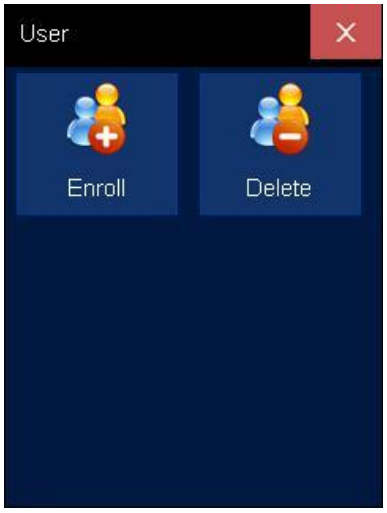



Fig.6 – User Screen

To register new users, access the Menu "User" device and click Subscribe:

Before registering methods of verification and restrictions, determine user data with your ID and name, as shown in the following image:

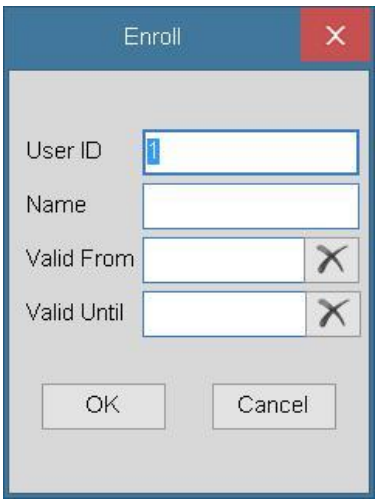



Fig.7 – Registration Screen

When you click Name, will be presented the following screen:


Fig.8 – User name Screen

Here you must enter the user name. The button 

lets you switch between numbers, symbols and special characters.

To enter characters in capital letters, you must select the button 

once, and then the desired letter.

Example: 

+ 

= 

.

To enter "space", you must select the button 
.

### 8.1.1. Add User

To register a new user click "Subscribe". The following options appear:

- ✓ ID- Indicates the number of the user;
- ✓ Name- Indicates the user name;
- ✓ Valid From- This option refers to the date of commencement of validity which will allow access.
- ✓ Valid until- This option refers to the date of expiry to allow access.
- ✓ Face - To register the face, the camera will make your templates automatically.

Click OK , and will be registered.

**Password**: It is recommended that the security password contains at least six (6) numbers; confirm your choice and click "OK".

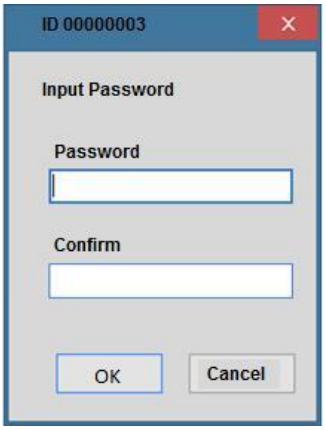



Fig.10 – Password Screen

- ✓ Photograph: You can use a picture to supplement the user 's registration information. However, you must register at least one certificate (Face, card or password) before registering the picture.
- ✓ Access warning: You can tell if someone has been recognized in the device if that user is recognized a message is sent to a registered email.
- ✓ User TimeZone: This menu allows the administrator to control access by Timezones, ie, the user can only access the site at predetermined hours.

To edit the data of a user is necessary to choose the desired user ID and click OK. You can edit all user data.

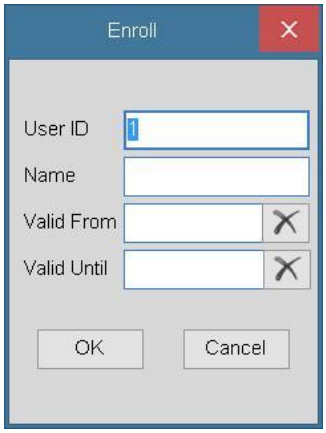



Fig.11 – Registration Screen

### 8.1.2. Delete User

This menu is for the information of users are deleted. After the ID specification, select the information or test methods to be deleted (Face , Password, Photo or All).

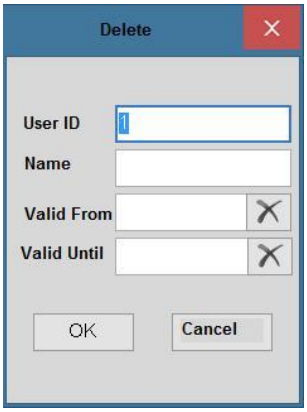



Fig. 12 – Delete User Screen

## 9. SETTINGS

To access the Settings menu, you must access the Main menu and click the Settings button.


Fig. 13 – Settings Screen

### 9.1. BASIC

14 - Basic

Are the basic device information and can give a name to the access site, choose the language used (English or Portuguese), the volume of the sound, the choice of service status, use bells

for a certain time, the amount of times this bell will ring, the desired time to light up the front - lighting LED equipment.

| | |
|---|---|
| Room ID | |
| Language | English |
| Sound | Yes |
| Volume | 10 |
| Auto Change of Time Mode | |
| Bell Setting | |
| Bell Count | 10 |
| Use Camera LED From | 00:00 |
| Use Camera LED Until | 00:00 |

### 9.1.1. ROOM ID (N° EQUIPAMENT)

Equipment for communication identifier number with the software.

### 9.1.2. Language

Select English or Portuguese (PTBR).

### 9.1.3. Sound

Opting for the No option, the device does not emit any sound.

### 9.1.4. VOLUME

The volume can be set on a scale that ranges from the numbers 0 to 10. The volume 0 (zero) will issue no sound and 10 (Ten) is the maximum volume.


Fig. 15 – Volume Screen

### 9.1.5. Control Time Service

This item is used to define how the service time is being used. You can choose the following options: In service, At rest, Extra Time, Real Time, Return.

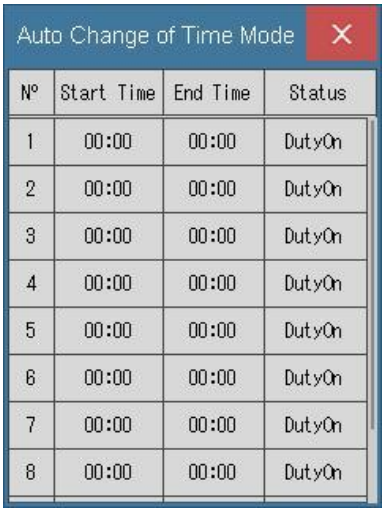



Fig. 16 – Time Service Screen

### 9.1.6. SETTING ALERT

If enabled, this item can be used to set the alert sound of the service time schedule.

.

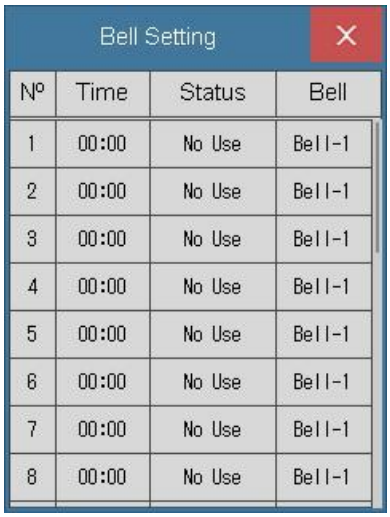



Fig. 17 – Alert Control Screen

### 9.1.7. Counter bell

Number of times the alert will sound 0-255.

### 9.1.8. LED light from

This determines the LED driving time to assist in lighting to identify the face.

### 9.1.9. Keep LED lights up

This determines how long the LED should be kept lit to assist in lighting to identify the face.

## 9.2. Advanced

| | |
|---|---|
| Verification Mode | FACE l CD l PWD |
| Date and Time | |
| Manager Email | |
| Device Email | |
| Photo Setting | Enrolled Photo |
| Upgrade Firmware | |
| Factory Reset | |
| Clear All Time Log | |
| Clear All Management Log | |
| Clear All User Database | |

### 9.2.1. Verification mode

Set the default mode of system check.

- ✓ **Face**
- ✓ **PWD**
- ✓ **Face+PWD**

### 9.2.2. Date and time

Clicking this option, the following screen appears:


Modify the options you want, and then click OK.

### 9.2.3. Email Manager

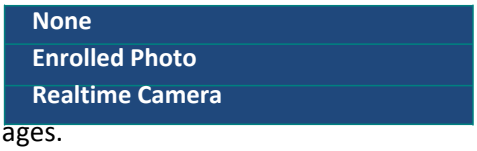
In this menu you can submit an email for which a recognition in the device notice will be sent.

### 9.2.4. Email device

In this menu , you can register the device email.

### 9.2.5. Photo setting

When performing an access in FaceAccess, it may be shown a photo of the registered person, or who take a picture of who is trying to access.




- ✓ **None -** not show any images.
- ✓ **Photo registered** - Uses a picture already registered.
- ✓ **Camera Real** - Time - Take a picture in real time.

### 9.2.6. Firmware Update

With this item, you can update the firmware version of the device.

### 9.2.7. Factory Reset

This item restores the default settings with the following message on the menu:


Fig. 18 – Restore Settings Screen

### 9.2.8. Clear All Time Log

This item performs the cleaning of all time records (records relating to access validation attempt).

### 9.2.9. Clear All Management log

This item performs the cleaning of all records management (records relating to the maintenance of the information on the machine 's display).

### 9.2.10. Delete All user Database

This item performs the exclusion of users of the database.

## 9.3. Energy

Fig. 19 - Energy

### After hibernating

In this menu you can configure the device to the power saving mode. Thus, it is possible to determine a range in minutes for the device to stay connected and, after this interval, hibernate automatically. May be a value reported from 1 minute to 9999 minutes. To disable this feature, inform the value 0.

| Sleep After | No |
|---|---|

This item saves energy during the period of non - use of the equipment, determining the time that the equipment will enter standby.

## 9.4. Communication

Fig. 20 - Communication

It allows you to change the device communication settings. You can also enter a search with a dynamic network address, enable the connection by Wi-Fi, choose the TCP port, choose the RS485 communication speed, change the port and server address.

| | |
|---|---|
| TCP/IP Settings | |
| WiFi | |
| TCP Port | 5005 |
| RS485 Speed | 115200bps |
| Server Address | 115200bps |
| Server Port | 500 |

### 9.4.1. TCP/IP Settings

In this menu you can configure the Ethernet system, ie the devices on the network interconnection architecture.

| | |
|---|---|
| DHCP | Yes |
| IP Address | 000.000.000.000 |
| Subnet mask | 000.000.000.000 |
| Gateway | 000.000.000.000 |
| MAC Address | 00.13:8f:28:47:f2 |

#### 9.4.1.1 DHCP

It allows you to set whether to allow enable DHCP or not. If this feature is enabled, the FaceAccess will acquire an IP address automatically so that you can establish communication equipment.

#### 9.4.1.2 IP Address

If DHCP is enabled, the IP address acquired will be displayed. Otherwise, you must enter the desired IP address.

#### 9.4.1.3 Subnet Mask

If DHCP is enabled, the mask acquired subnet will be displayed. Otherwise, you must inform the mask desired subnet.

#### 9.4.1.4 GATEWAY

If the DHPC protocol is enabled, the Gateway acquired will be displayed. Otherwise, you must enter the number of the desired Gateway.

#### **9.4.1.5** MAC Address

It will be presented the physical address of FaceAccess Ethernet interface.

### 9.4.2. WIFI

In this menu item, you can set the Wi-Fi mode FaceAccess.

| | |
|---|---|
| **Use WiFi** | **Yes** |
| **Select WiFi Hub** | |
| **DHCP** | **Sim** |
| **IP Address** | |
| **Subnet mask** | |
| **Gateway** | |
| **Link Information** | |

#### 9.4.2.1 Using WiFi

It allows to enable Wi-Fi communication feature.

#### 9.4.2.2 Select WiFi network

It lets you select a Wi-Fi network equipment for communication.


Fig. 21 – Wifi

#### 9.4.2.3 DHCP

It allows you to set whether to allow enable DHCP or not. If this feature is enabled, the FaceAccess will acquire an IP address automatically, so you can establish communication equipment.

.

#### 9.4.2.4 IP Address

If DHCP is enabled, the IP address acquired will be displayed. Otherwise you must enter the desired IP address.

#### 9.4.2.5 Subnet Mask

If DHCP is enabled, the mask acquired subnet will be displayed. Otherwise, you must inform the mask desired subnet.

#### 9.4.2.6 GATEWAY

If the DHPC protocol is enabled, the Gateway acquired will be displayed. Otherwise, you must enter the number of the desired Gateway.

#### 9.4.2.7 Link Information

- ✓ Disconnected state: This function refers to the state of the used connection (connected or not). Has the following shortcut use: Setup menu. -> News -> WiFi -> Link information -> State
- ✓ SSID: This function refers to the connection name used. Has the following shortcut use: Setup menu. -> News -> WiFi -> Link information -> SSID
- ✓ Sensitivity: This feature refers to the link-level internet On Time. Each link-level varies from 1 to 5 layers. Has the following shortcut use: Setup menu. -> News -> WiFi -> Link information -> Sensitivity
- ✓ Speed: This function refers to the speed of the Internet used by the machine: Setup menu. -> News -> WiFi -> Link information -> Speed.
- ✓ MAC Address: This function displays the physical address of the WiFi interface: Setup menu. -> News -> WiFi -> Link Information -> MAC address.

### 9.4.3. TCP PORT

In this menu you set the port to be used, allowing a TCP / IP communication device with the software that will be installed on your computer in case of integrated network use.

The PC software must use the TCP port to communicate with the FaceAccess.

### 9.4.4. Server address:

The IP address of the server that has the communication software with FaceAccess is set.

### 9.4.5. Server port:

The port used to perform communication with the communication software is set.

## 9.5. LOG

Fig. 22 - Logs

This item has an alert that tells you when the device memory is full. When the log memory space is less than the chosen number, the device will alert you to download the log data to a USB device (USB flash drive).

The limit for Notices Log Management (logs relating to access to the equipment interface) is 200 records, while the limit for registration Time Advisory (log for the record attempts in the equipment) is 2000 records. To bypass this function, simply put 0 (zero).

Check the time used to prevent generation of unnecessary records. By doing facial recognition, the device will continue to capture his face, and the set time will not be computed the record for rechecking.

| | |
|---|---|
| Management Log Warning | 50 |
| Time Log Warning | 500 |
| Re-verification Time | 5Min |

### 9.5.1. Management Log Warning

Used to set the generation of a warning in the event of display of memory for records management equipment. When the chosen number is 50, it means that when he arrived in 9950 (equipment has a storage limit for Log Management 10,000 records), a warning will be issued to be made the collection of USB device via records (Pen Drive) or via communication management records.

### 9.5.2. Time Log warning

Used to set the generation of a warning in the event to present full memory for validation attempt records on the equipment. If the storage memory validation attempts records exceed a certain storage limit, this menu will allow the definition of a warning. In this case, a "minimum clearance" is set, and if the free memory space is below the set point , the device will generate a warning

### 9.5.3. Re- Verification Time

Which are not used for validation attempts stored in the machine unnecessarily. The face authentication means is performed continuously, thus could be generated by trial duplicate records and validation access authentication. If it is informed to this menu 1 min for one minute they will not be generated records in memory regarding the same release.

## 9.6. ACCESS

Fig. 23 - Acess

| | |
|---|---|
| Define Time Zone | |
| Door Open Time | 5s |
| Door Open Timeout | 20s |
| Door Sensor Type | Open |
| Watch Tamper | No |
| Wiegand Type | Wiegand-34 |

### 9.6.1. Define Time Zone

In this menu you can create time zones for access control After clicking on this menu will appear in the image below.:

In this menu you can set each daily each zone access time, the zones will 1 to 50.

### 9.6.2. Door Open time

It is possible to determine the activation time of the relay after a check (or in case of activation by pushbutton). The standard stipulated time will be five (5) seconds.

### 9.6.3. Door open Timeout

This sets the warning alarm that will be triggered if the door is open for longer than determined. The determined standard time is 20 seconds.

### 9.6.4. Door Sensor type

You can set the detection of the state in three ways door sensor:

a) None
The device does not detect the status of the door.

b) Open
The device detects the change of always open sensor signal for closed (NA => NC)

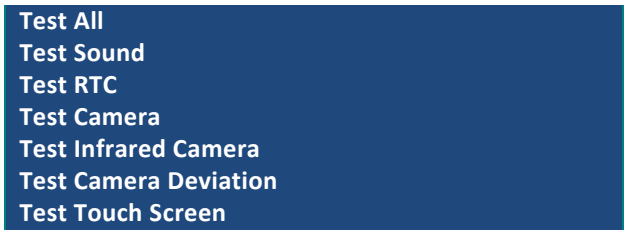
c) Closed

The device detects the change from closed to open whenever sensor signal (NF => NO)

- ✓ Watch Tamper - Enables alarm violation opening the equipment..
- ✓ Note: To disable the alert, go to the main menu, which will be available Alarm option. By accessing this option, the questions asked for it to be turned off until there is another warning.

## 9.7. TEST

Fig. 25 – Test




### 9.7.1. All test

This menu allows performing sequentially all the testing device.

### 9.7.2. Sound test

This menu allows make the device sound test.

### 9.7.3. Test RTC

In this menu you can perform the test RTC (real time clock), viewing the device's date and time.

### 9.7.4. Test Camera

This menu area tests the device camera.

### 9.7.5. Test Infrared Camera

This item tests the infrared camera device.

### 9.7.6. Test Camera Deviation

This item enables test the color camera and infrared camera, and test and detect possible deviations from these cameras capture.

## 10. SECURITY

Fig. 26 - Security

This menu is used to configure the supervisor has the following options.:


- ✓ Master PIN - Enroll PIN (password) master card with up to 31 digits;
- ✓ Encryption Key - Register the key and the encryption of the Master Card (supervisor password), and is also used in communication for firmware update;

 NOTE: The PIN is only valid to the supervisor quan be an encryption key, otherwise the PIN will not be considered.

 OBSERVAÇÃO: NOTE: Do not register an encryption key without Master Password. If done, it will need assistance from technical support to change the settings of FaceAccess.

### 10.1. RESET

The button on the device controller card enables the administrator FaceAccess, in case of loss of password, delete the security settings, such as administrator passwords, encryption and database. Pressing the button will appear on the screen the following options:

**Remove privileges:** Deletes all passwords and encryption;
**Erase all data:** Removes all data;
**Cancel:** Cancels the operation.

## 11. QUICK CONFIG

Clicking this option, you receive the following message:

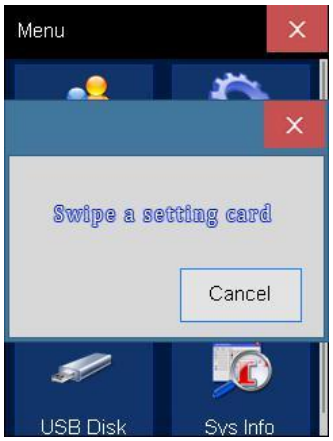



Fig. 28 – Quick config

It is a technical feature that allows, through a customized programming card, make the change automatically the encryption key, password (PIN) supervisor, server IP address, and server connection port.

## 12. USB DISK

Fig. 29 – USB Disk

**Download New time Log**
**Download All Time**
**Download New Management log**
**Download All Management Log**
**Download User Database**
**Upload User Database**

To use this function, connect a USB device (Pen Drive) on FaceAccess.

### 12.1. Download New time Log

This item allows you to download accesses records unread for a USB device.

### 12.2. Download All Time Logs

This item enables downloading of all access records to a USB device (USB drive).

### 12.3. Download New Management log

This item enables downloading of managements records unread for a USB device (USB drive).

### 12.4. Download All Management Log

This item enables downloading of all records management to a USB device (USB flash drive).

### 12.5. Download user database

This item enables to download the entire user database to a USB device (USB flash drive). ENROLLDB.DAT one file to be used to load other equipment is generated.

### 12.6. Upload user database

This item enables users to upload a database to a USB device (USB flash drive) to the equipment. Through the "Download User Database" option is stored in the Pen Drive ENROLLDB.DAT the file to be imported into the machine's memory . NOTE: the file is encrypted.

## 13. INFOR. SYSTEM

### 13.1. Enroll Info

| | |
|---|---|
| User | 0/5000 |
| Face | 0/1200 |
| Card | 0/5000 |
| Password | 0/5000 |
| Time Log | 0/100000 |
| Management Log | 0/100000 |
| Photo (User+Log) | (0+0)/5000 |

#### 13.1.1. User

This menu displays the registered users count on the device.

#### 13.1.2. Face

This menu displays the face count registered on the device.

### 13.1.3. Password

This menu displays the password count registered on the device.

### 13.1.4. Time Log

This menu displays the access attempt count of records stored on the device.

### 13.1.5. Management Log

This menu displays the records management count written to the device.

### 13.1.6. Photo (User+ Log)

This menu displays the photo count users and photo records of users recorded in the device.

### 13.2. INFO. DEVICE

| | |
|---|---|
| Release Date | YYYY.MM.DD |
| Serial Number | |
| Manufacturer | INTTELIX BRASI |
| Product Name | FaceAccess |
| F/W Version | |
| Board Version | |

### 13.2.1. Release Date

In this area you can view the update date of the product.

### 13.2.2. Serial Number

In this area you can view the product serial number.

### 13.2.3. Manufacturer

In this area you can view the product manufacturer (INTTELIX BRASIL).

### 13.2.4. Product Name

In this area you can view the product name (FaceAccess).

### 13.2.5. F/W Version

In this area you can view the firmware version of the device.

### 13.2.6. Board Version

Revision of the physical board equipment.

### 13.3. ADVANCED


#### 13.3.1. View Time Log

In this menu you can search time records (hits) for specific periods and user ID.

#### 13.3.2. View management Log

This menu allows you to search records management for specific periods and ID.

#### 13.3.3. View User List

This item enables users of information display from the availability of their respective ID.

- NOTE: To view all the records in each option, just click Search / OK

### 14. CLEAR ALARM

When an alarm is triggered, the alarm item will automatically appear on the Main menu; the selection and confirmation of this item will stop the alarm immediately.

### 15. OTHER SPECIFICATIONS

#### 15.1. Open Door illegally

If the door is opened in a manner that is not valid (validation or buttonhole) the device will issue an alarm signal. This alarm can be disabled as follows:

- Click on the Alarm and turn off the option. The option appears on the main menu as soon as the alarm is triggered.

- Keep the door closed and make access again (use valid ways, for example: check face and drive buttonhole).

- NOTE: For this feature to be valid, it will be necessary to have a sensor on the door, identifying its status (open / closed).

#### 15.2. Equipment Violation Alarm

If the device cover is open, this sounds an alarm due to violation (unauthorized opening of the device).

This alarm will only stop when a supervisor click the Alarm option, which, as stated earlier, will appear as soon as the alarm is triggered, the Main menu.

**FCC Statement**

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.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user’ s authority to operate the equipment.

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

**FCC RF Radiation Exposure Statement**

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment.

And Customers can view more product certification information from the website (https://www.fcc.gov/)