



Triplow



F-MA300 ACCESS CONTROL TECHNICAL MANUAL



Introduction

The F-MA300 is a standalone access control by fingerprint and card that uses advanced reading technology, it is ideal for using in circumstances that require high security levels.

It uses a management software with different functions, attendance control, user management, access control, and so on.

Programming is carried out by the management program in English. This equipment has a 10000 user capacity.

Functions

- Standby function
Energy saving system by means of an on/off automatic control of the equipment. In standby, the energy consumption is lower than 0,2 w.
- Programming by the management program
The entire programming is carried out by means of a command.
- Closing timer
Door closing timer setting is between 0-99 (0s equals to 50ms).
- Anti-vandal alarm
Anti-vandal protection system that activates a sound alarm when there is an attempt to open the equipment by force.
- Connection by using a network cable (RJ45) on to the computer or TCP/IP connection.





Triplow W

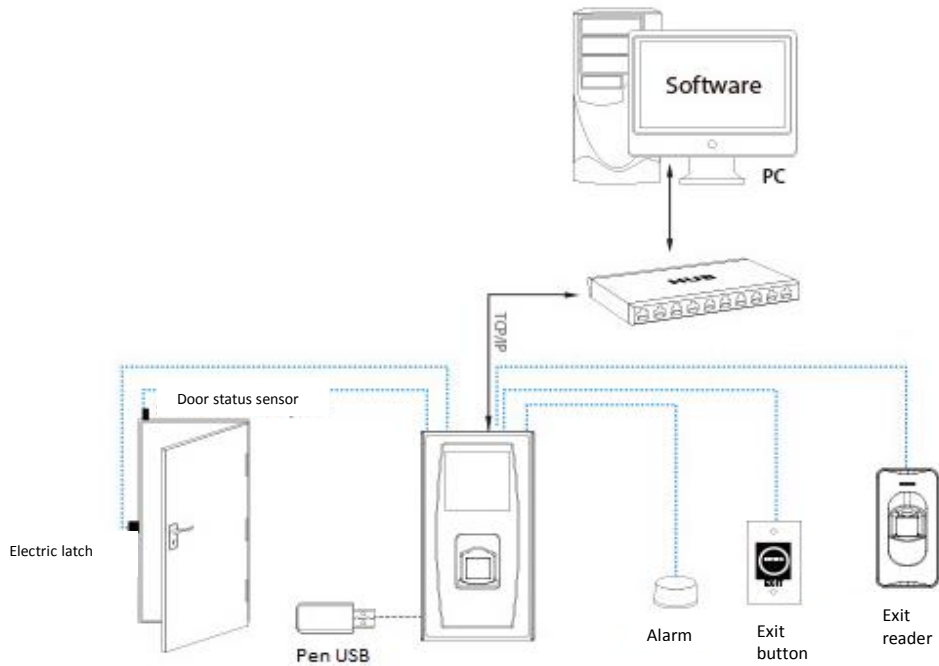
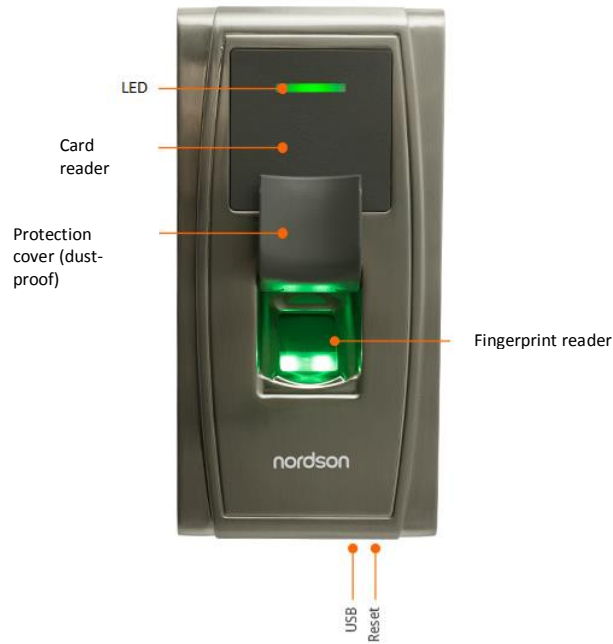
CE FC

F-MA300



Installation

- Installation and mounting





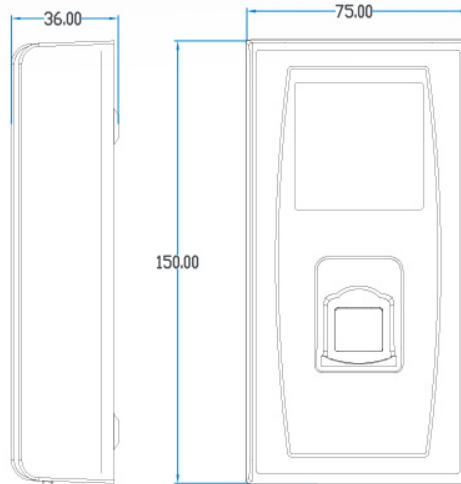
Triplow W

CE FC

F-MA300



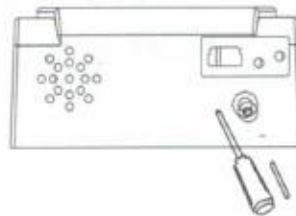
Dimensions



Installation



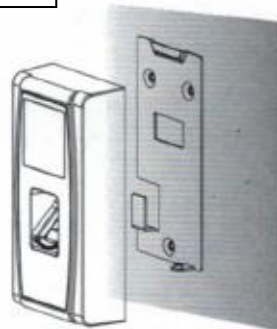
Use the drilling template to mark screw holes.



Untighten the screw at the bottom of the device.



Remove the device's back panel and mount according to template marks.



Mount the device in place.



Tighten back the screw at the bottom of the device.





Triplow



Contents

1. Operating Instructions	5
1.1. Hardware requirements.....	5
1.2. Basic operations.....	5
1.3. Management program initialization	5
1.4. Add a new device to the F-MA300.....	6
1.5. Create privilege levels for access	9
1.6. Door settings.....	11
1.7. Add a new user to the software.....	12
1.8. Add user fingerprint.....	14
1.9. Time Zone	18
1.10. Monitoring	20
1.11. Reports.....	20
1.12. Anti-Passback.....	21
1.13. Change the F-MA300 device IP	22
2. Additional Functions Performed Directly on the Equipment	244
2.1. Add administrator card.....	244
2.2. Reset factory settings	244
3. Technical Specifications	244





1. Operating Instructions

1.1. Hardware requirements

- Memory: 1G minimum
- Storage: 10G minimum
- Windows XP or later

1.2. Basic operations

- Management program initialization
- Add a new device
- Create privileges levels for access
- Add users
- Define privileges for users
- Time Zones
- Monitoring

1.3. Management program initialization

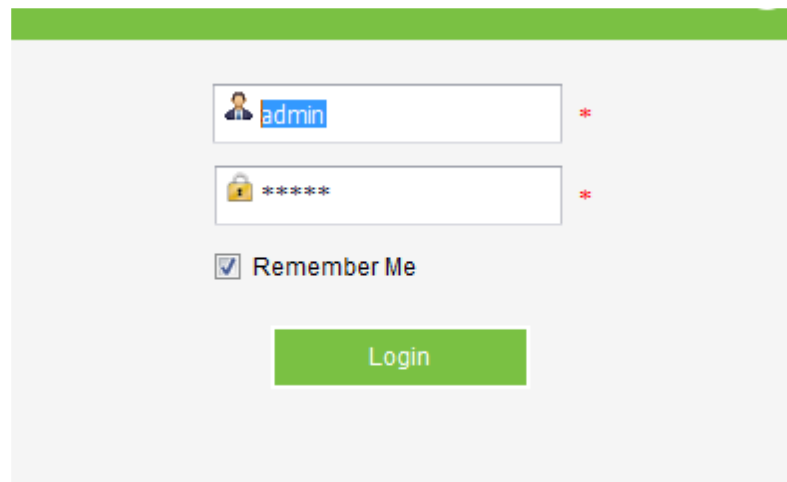


Image 1 – Login

After opening up the software, it will be necessary to log into the application.

Default credentials are:

- User: admin
- Password: admin

It is recommended to change access credentials after the first initialization, you just need to click on **System -> Change Password**.





Triplow

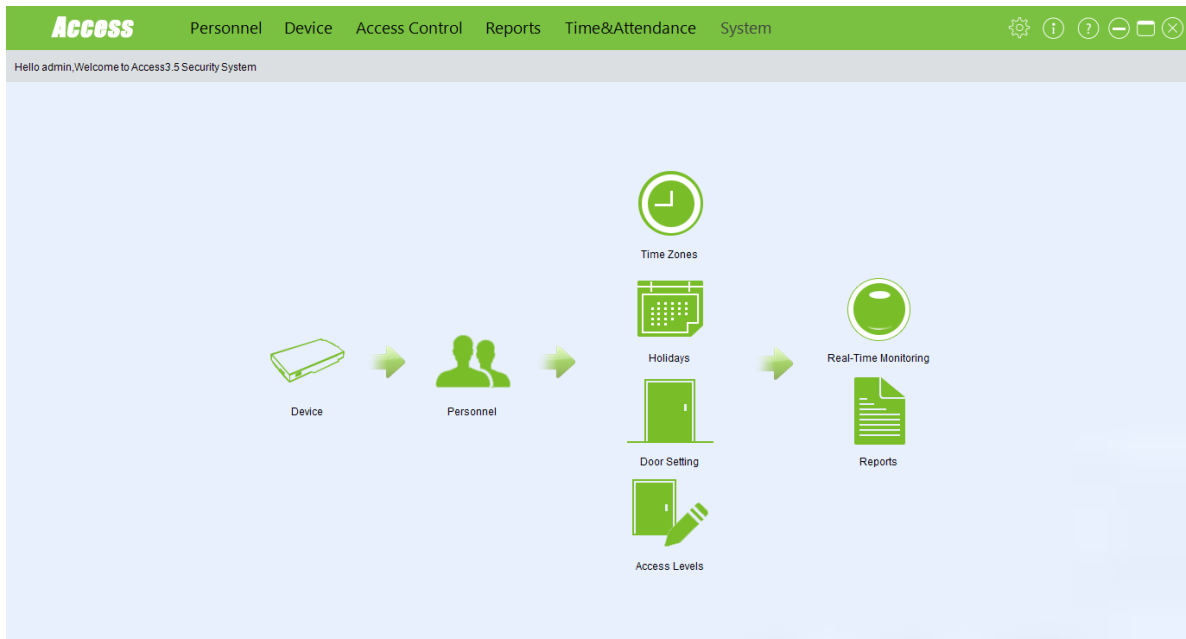


Image 2 – Main screen

After logging in, the application's main screen will initialize (**Image 2**).

If it is necessary to change the language, just click on the icon . It is recommended the use of the English language because all other language options are still in the update stage.

1.4. Add a new device to the F-MA300

The first setting step is to add the F-MA300 to the software. After carrying out all the corresponding connections, the device can be added by clicking on **Device** on the main screen (**Image 3**).

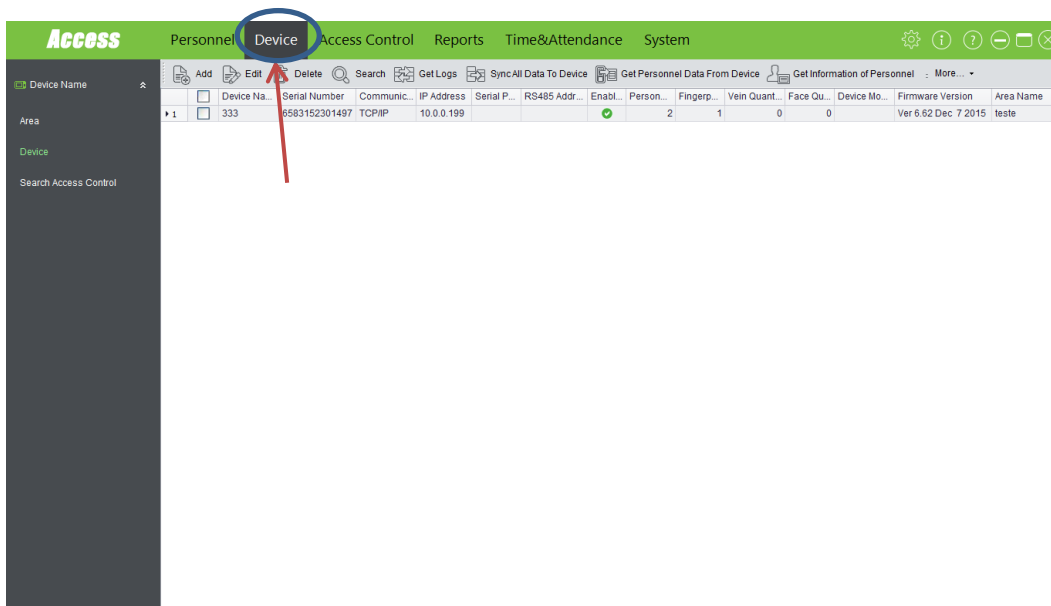


Image 3 – Screen to add the device



Next, a new window will pop out (**Image 4**), click on **Add** to add a new device.

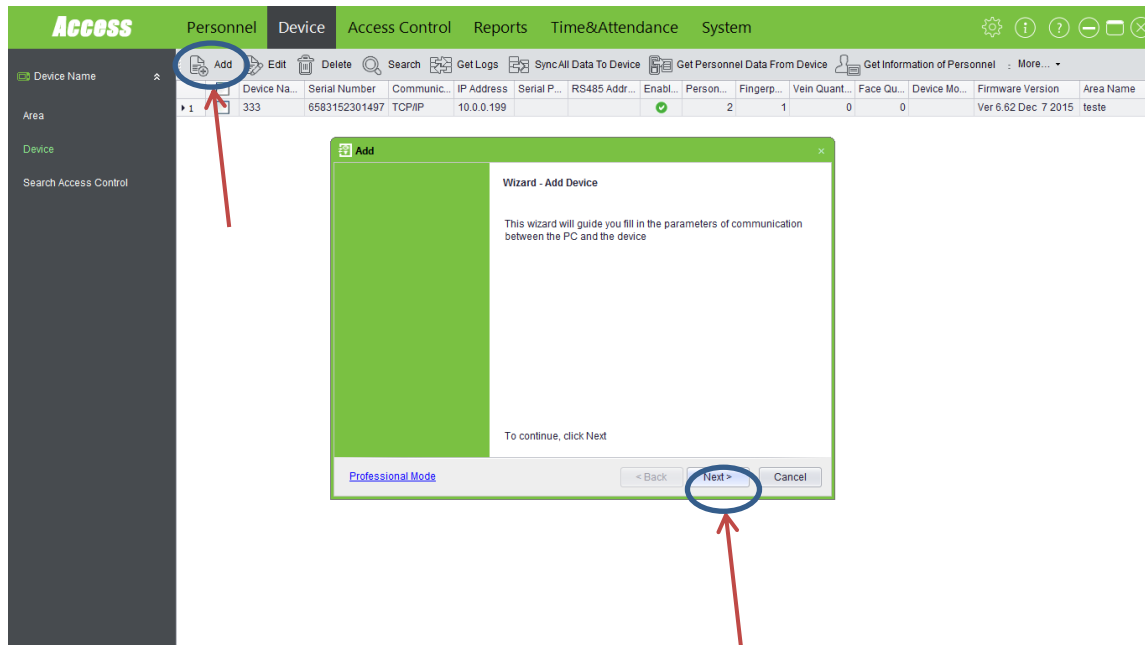


Image 4 – Setting window for the new device

Then, another window will pop out (**Image 4**), click on **NEXT** to add a new device to the system, fill in all the device data in this window (if the window looks different, click on **Wizard Mode** on the bottom left corner of this window, when clicking, the window will turn to a similar window as shown in **Image 4**).

Communication Type: TCP/IP.

IP Address: 192.168.1.201 (factory default IP).

IP Port Number: 4370 (by default every TCP/IP connection uses the 4370 port).

Note: If the device stays directly connected to the computer, it is not necessary to change the device IP, but if it is necessary to change it due to the device being connected to a router/switch, the IP will have to be changed for a free static IP within the router network (**See point 0**).

Click on **NEXT**.





Triplow

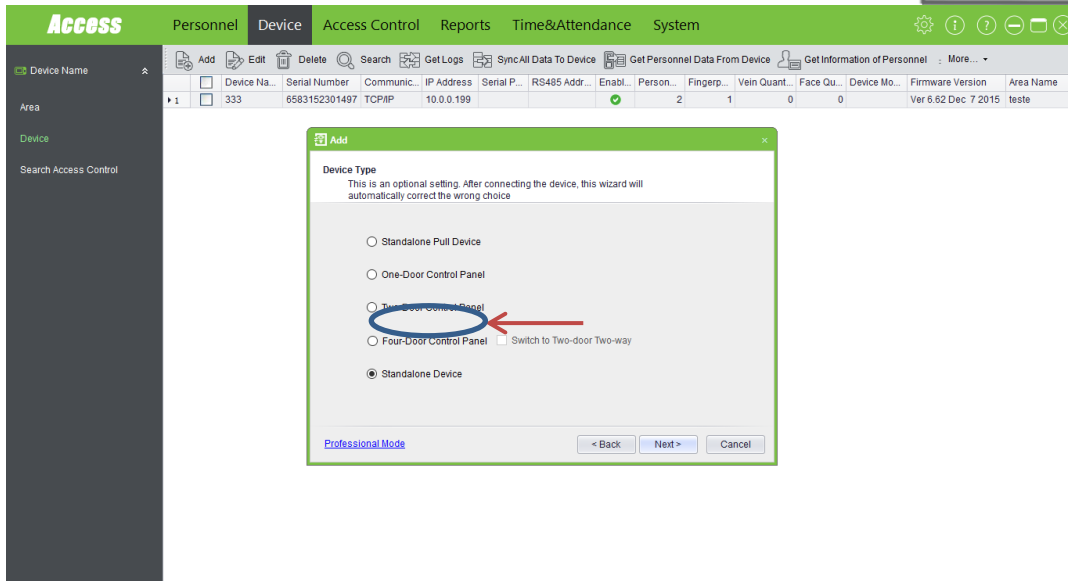


Image 5 – Add new device

On the **Image 5** select the option **Standalone Device**.
Click on **NEXT**.

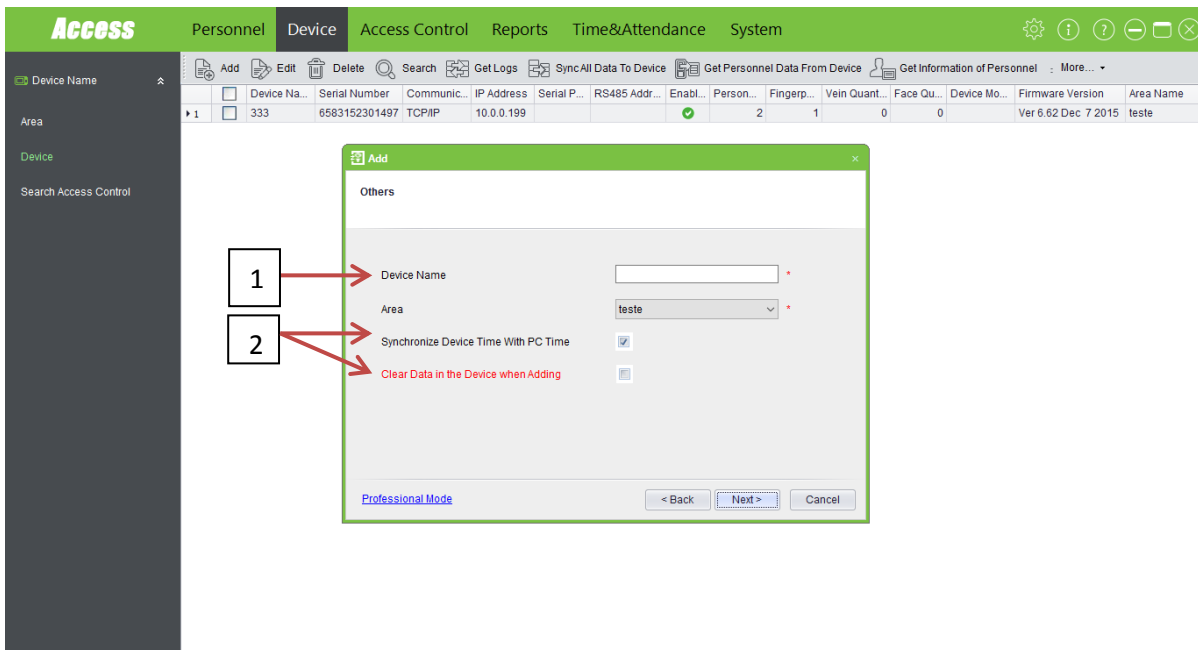


Image 6 – Add a new device

On **Device Name (1)** fill in with the desired name, for example: entry door.
Select **Synchronize Device Time with PC Time** and **Clear data in Device When Adding (Image 6)**.
Click on **NEXT** on the following windows.





Triplow

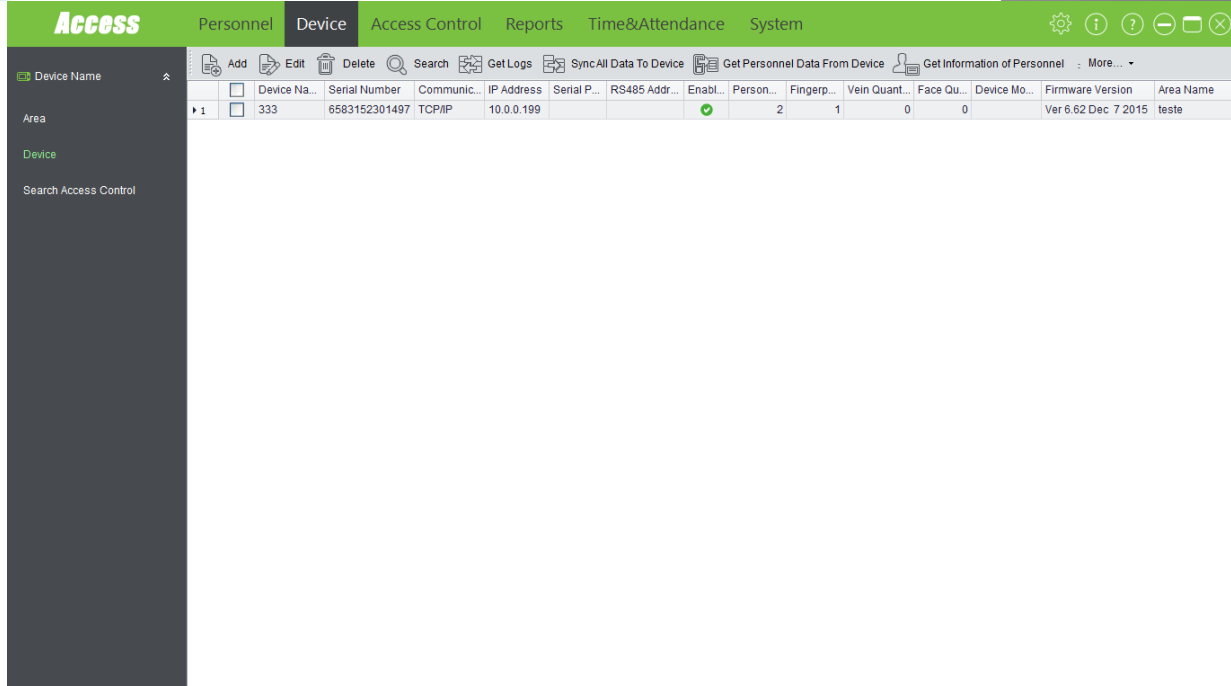


Image 7 – Add the new device successfully

If the device is added successfully, the window in **Image 7** will pop out.

In this window, click on **Sync All Data to Device** and on **More**, click on **Synchronize Time**.

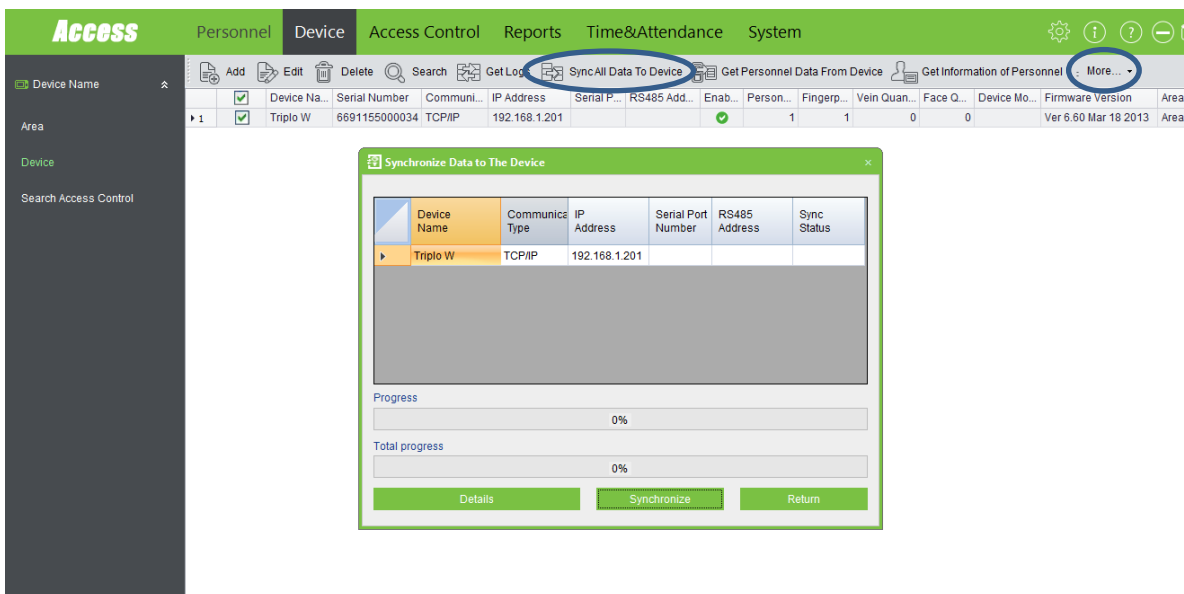


Image 8 – Synchronize software data to the F-MA300

1.5. Create privilege levels for access

Before creating new users, it is necessary to create privilege levels that are going to be available for the door. By default, there is only the option to set the door for a 24 h opening. Access shifts can be created in **Access Control ->Time Zones->Add**.





Triplow



Set access levels on **Access Control (1)**->**Access Levels (2)**->**Add (3)** (Image 9).

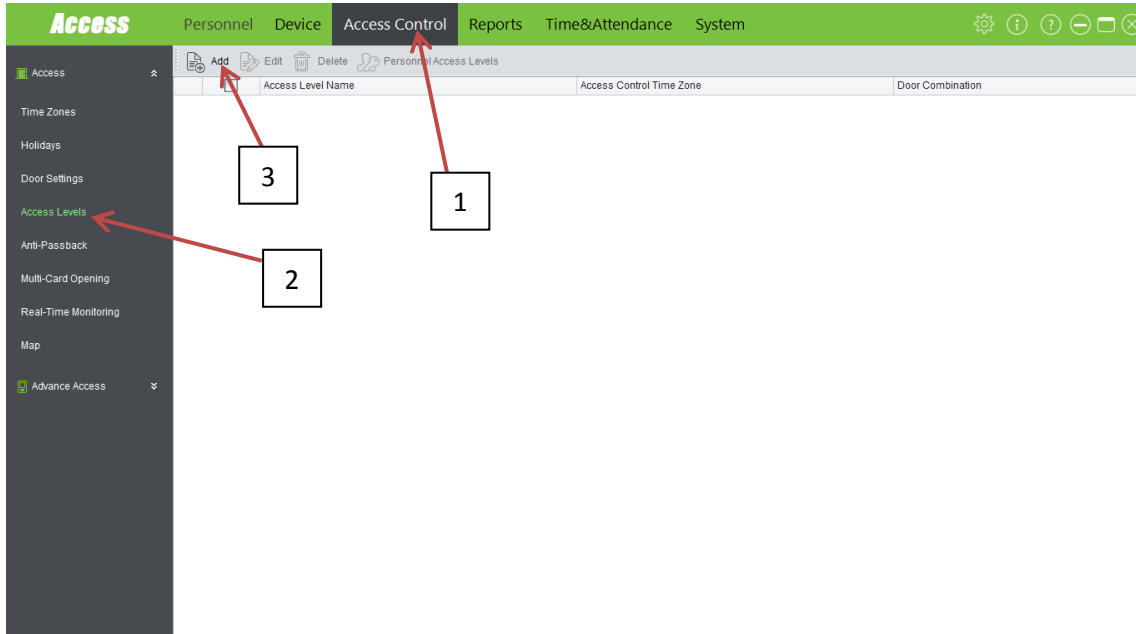


Image 9 – Privilege levels

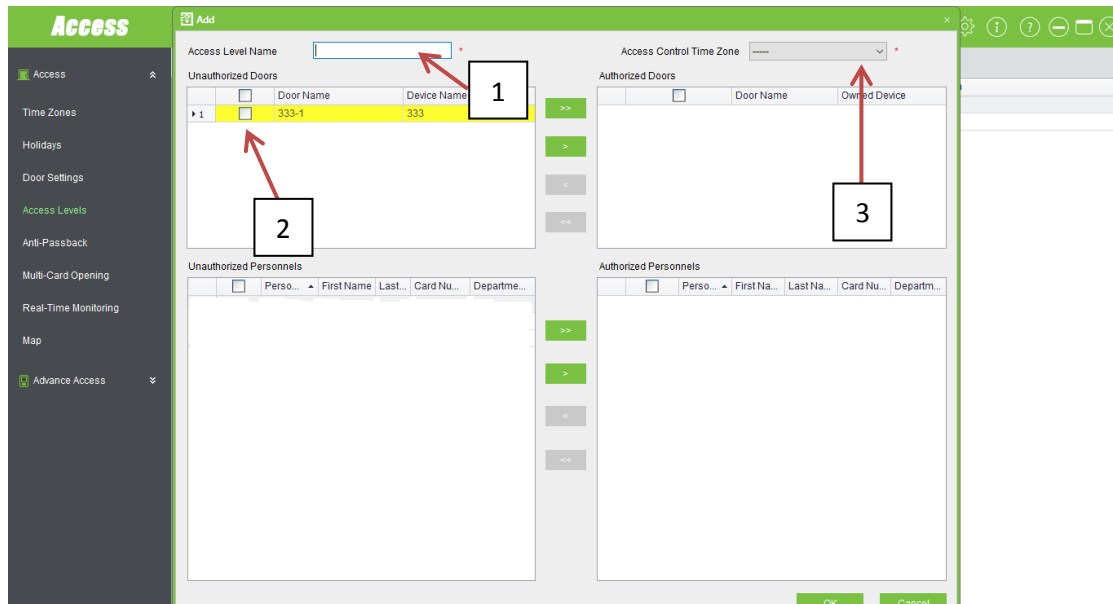


Image 10 - Privilege levels

Click on **Add**, a new window will pop out (Image 10) where desired access levels can be created.

- 1- Name de type of access level (Example: Management, Employees).
- 2- Door (in this case the F-MA300).
- 3- Time zone access type (To create different access schedules, see point 1.9).

Click on **SYNC NOW**.



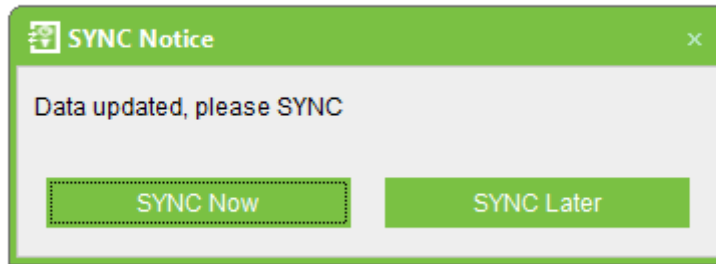


Image 11 – Synchronization between software and device

Image 11, this window is going to open up every time the software detects new entered data that needs to be transferred to the device, so that the software and the device are synchronized.

1.6. Door settings

In this tab, it can be set the time the door remains open and the type of verification necessary to open up the door (card, card + fingerprint, only fingerprint).

To enter door settings:

Click on **Access Control (1)** -> **Door Setting (2)** -> **Edit (3)** (Image 12).

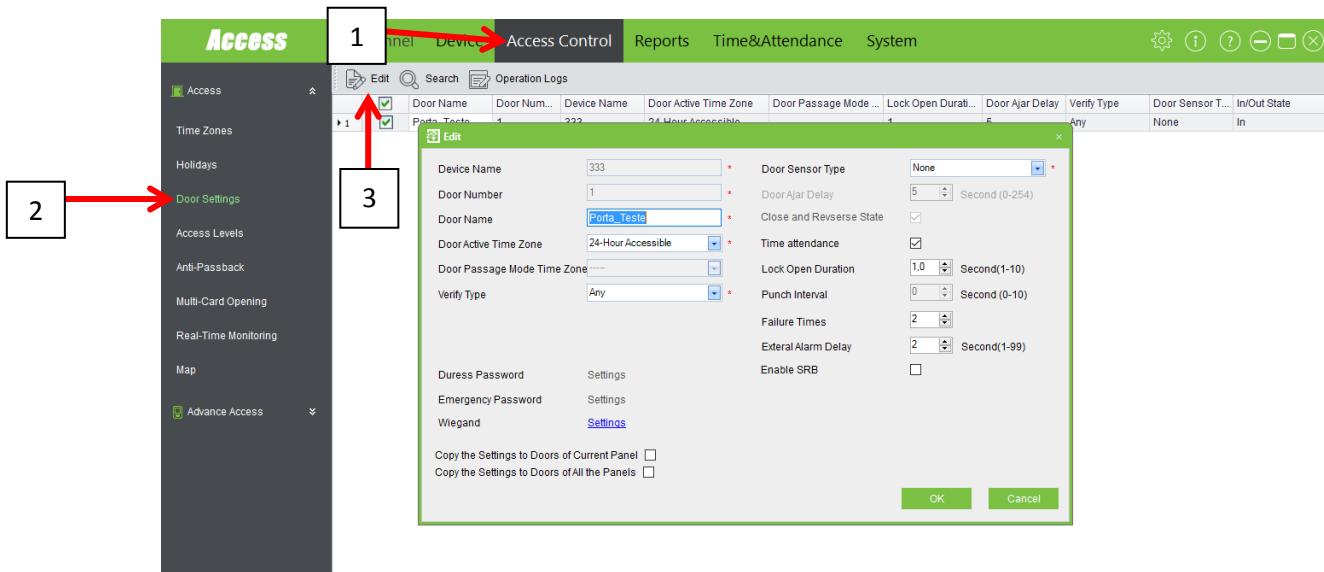


Image 12 – Door settings

When clicking on **Edit**, a window will open where all door settings are be found:

- **Door Name**
- **Door Active Time Zone:** It is recommended to leave the door with a 24 h availability.
- **Verify Type:** In this field, it can be set how the user is going to open de door, for example:
 - **Any:** Door opens by card or fingerprint.
 - **Only Fingerprint:** Door opens only by fingerprint.
 - **Only Card:** Door opens only by card.
 - **Card and Fingerprint:** Door opens by card + fingerprint.
 - Etc.
- **Door Sensor:** If the door has a status sensor, it can be selected. If it does not have it, select **None**.



- **Lock Open Duration:** Time the door stays open (In order for the door to work properly, it is recommended to change the time for a minimum of 3 seconds).

The **WIEGAND** option is for when the door or exit terminal has the F-MA300 to open the door and another WIEGAND terminal inside for exits. In this case, the terminal can be set in the **WIEGAND** option.

1.7. Add a new user to the software

To add new users, click on **Personnel (1)** -> **Add (2)** (Image 13).

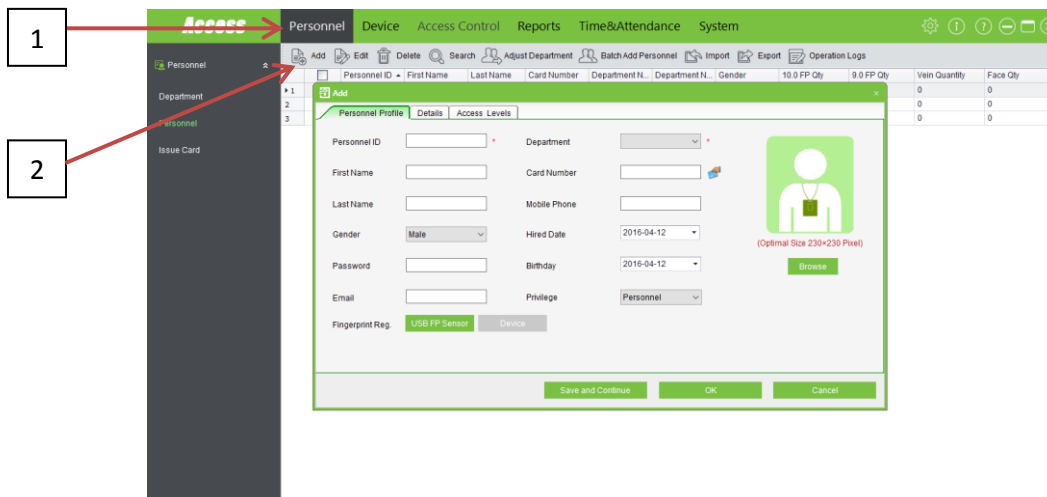


Image 13 – Add new users

On the **Image 14** window, the complete new user data can be filled in.

If it is necessary to assign a department to each user, then first a department has to be created on **Personnel** -> **Department**.





Personnel ID * Department Company Name *

First Name Card Number

Last Name Mobile Phone

Gender Hired Date

Password Birthday

Email Privilege

Fingerprint Reg.

Image 14 – User data

Card Number: Enter the access card number (Image 15).

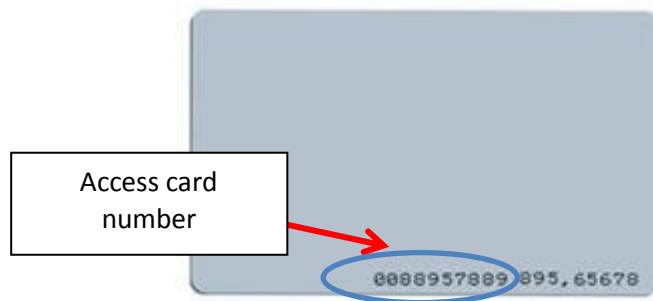


Image 15 – RFID card

Fingerprint Reg.: For adding a user fingerprint (See point 1.8).

Access Levels: Assign an access level for the user (Image 16). This option will assign the access level for the user. Access levels were created on point 1.5 (this is a mandatory step for the proper operation of the device, without this setting, users will not be able of opening the door).



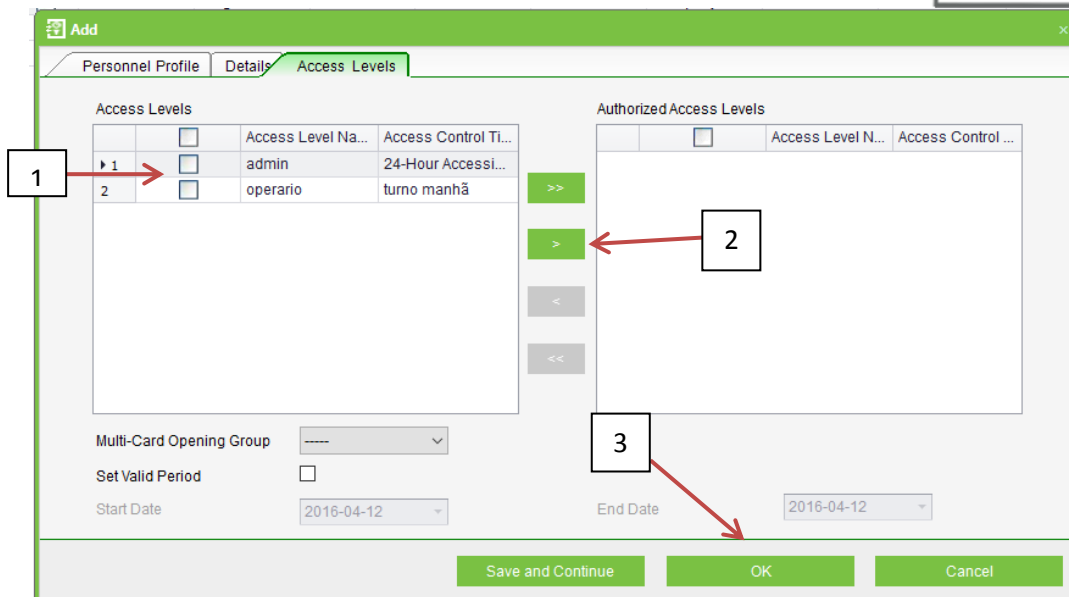
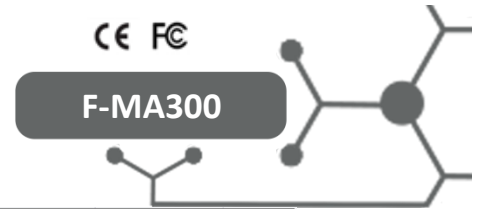


Image 16 – Access level

To define user access is necessary to (Image 16):

- 1- Select access type.
- 2- Add authorization type.
- 3- Confirm add/edit user settings.

Click on **SYNC Now**.

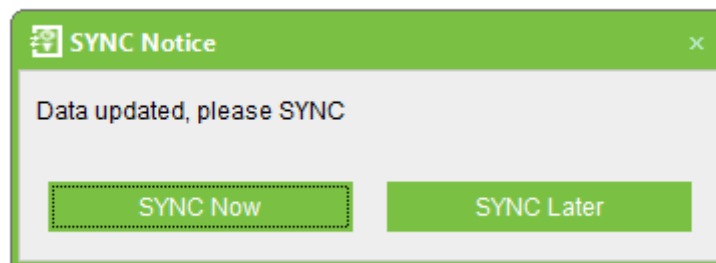


Image 17 – New data synchronization to device

If the software detects new data updates, such as new users, privileges, time zones, etc., the text box shown in **Image 17** is going to pop out to synchronize the software data to the device, so that both systems have the same information.

1.8. Add user fingerprint

To add a user fingerprint is necessary to create a user or edit a user data **Personnel (1)** -> **Select user (2)** -> **Edit (3)** (Image 18).



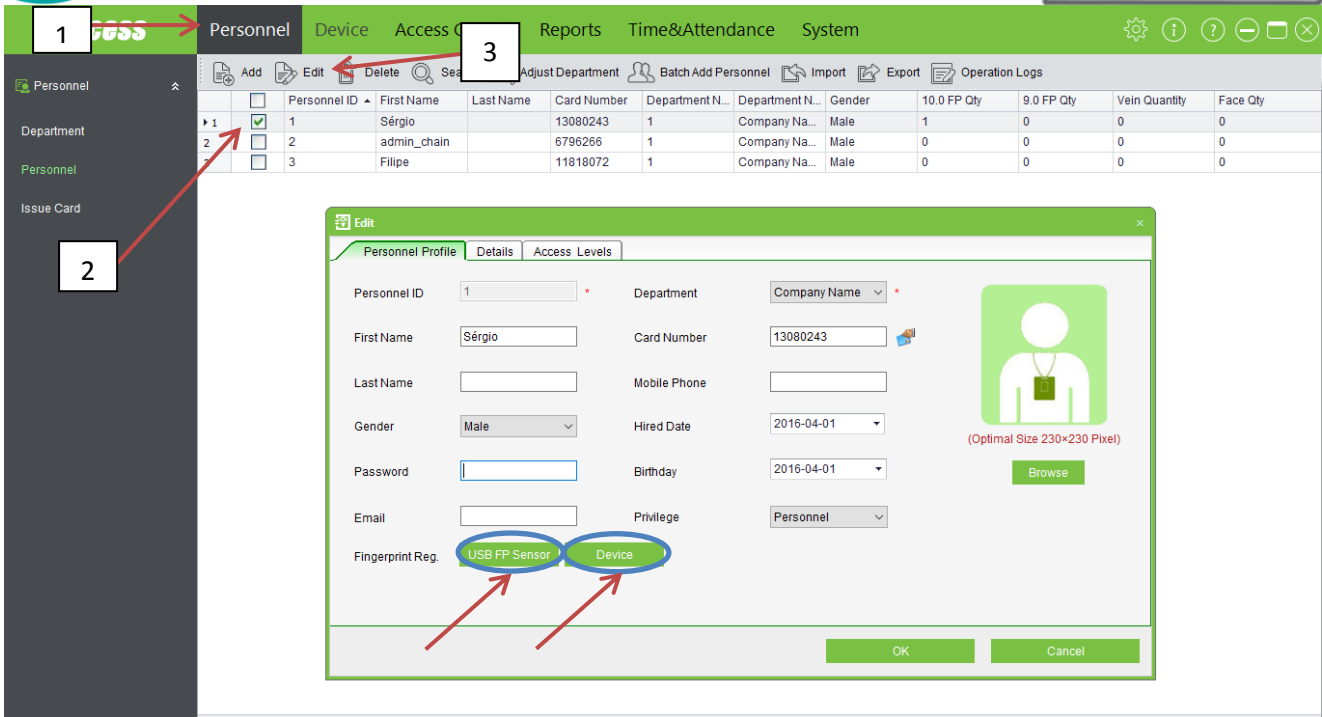


Image 18 – Add fingerprint

Select (Image 18):

- **Device:** If fingerprints need to be added using the F-MA300:

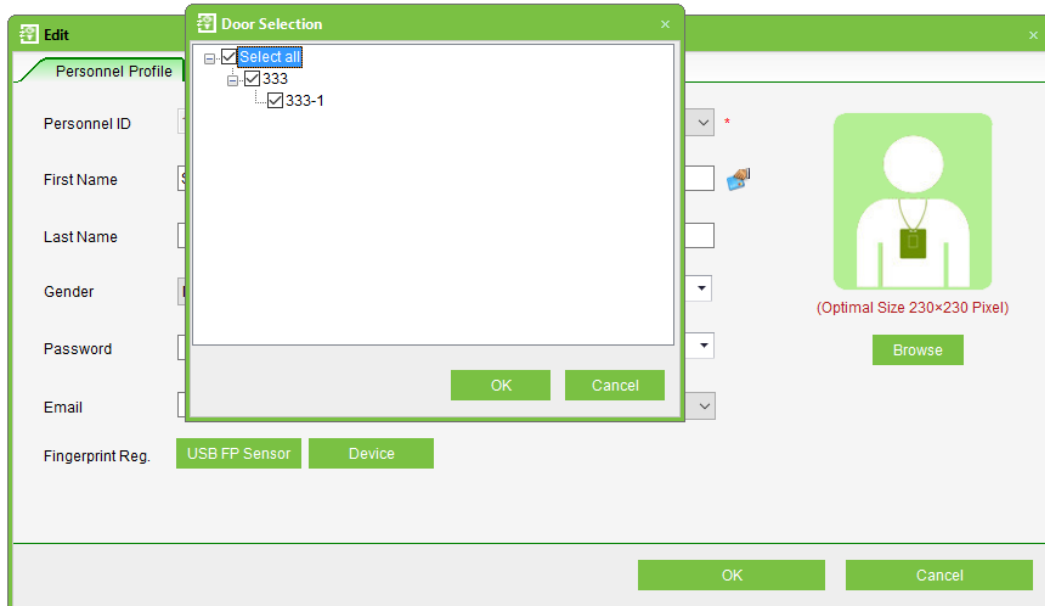


Image 19 – Add fingerprint

Click on **Select all** -> **Ok** (Image 19).

On the following window (Image 20) two hands are shown, in order to add fingerprints you have to:

- 1- Pick the user's finger to be added by clicking on the corresponding finger as shown in Image 20.





Triplow

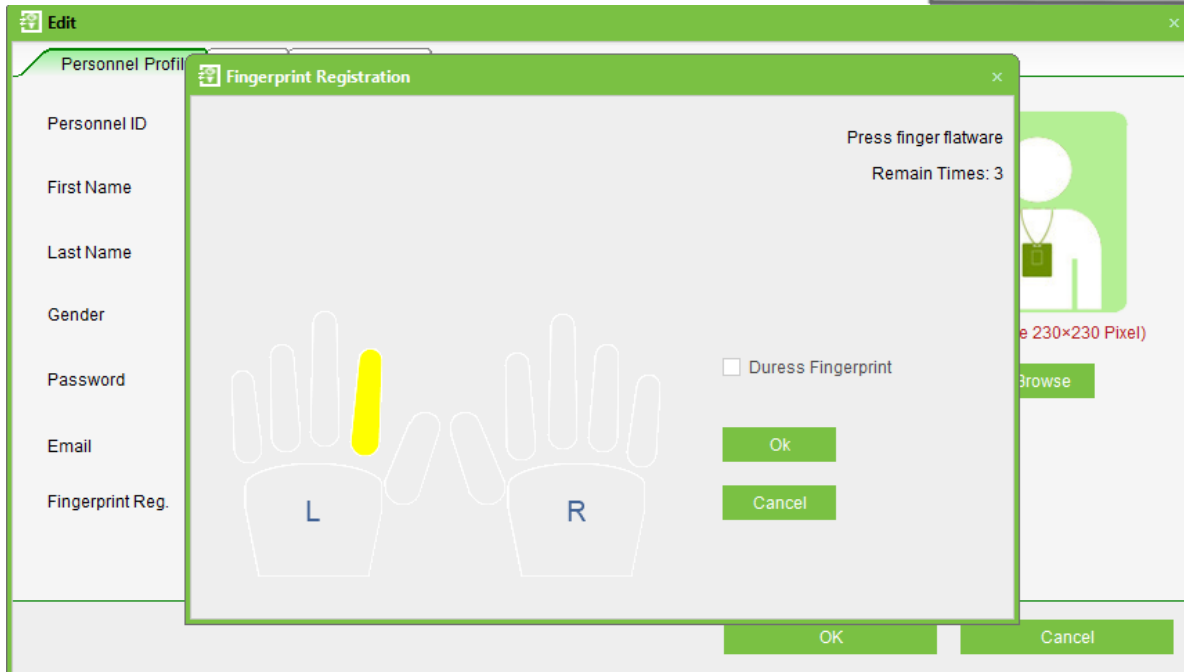


Image 20 – User's finger selection

- 2- When selecting the finger on the software (**Image 20**) the device is going to show the instructions to add fingerprints correctly.
- 3- If the user's fingerprint is added correctly to the software, the selected finger will turn green (**Image 21**). It can be added as many fingers as desired from the same user (it is recommended to at least add two fingers).

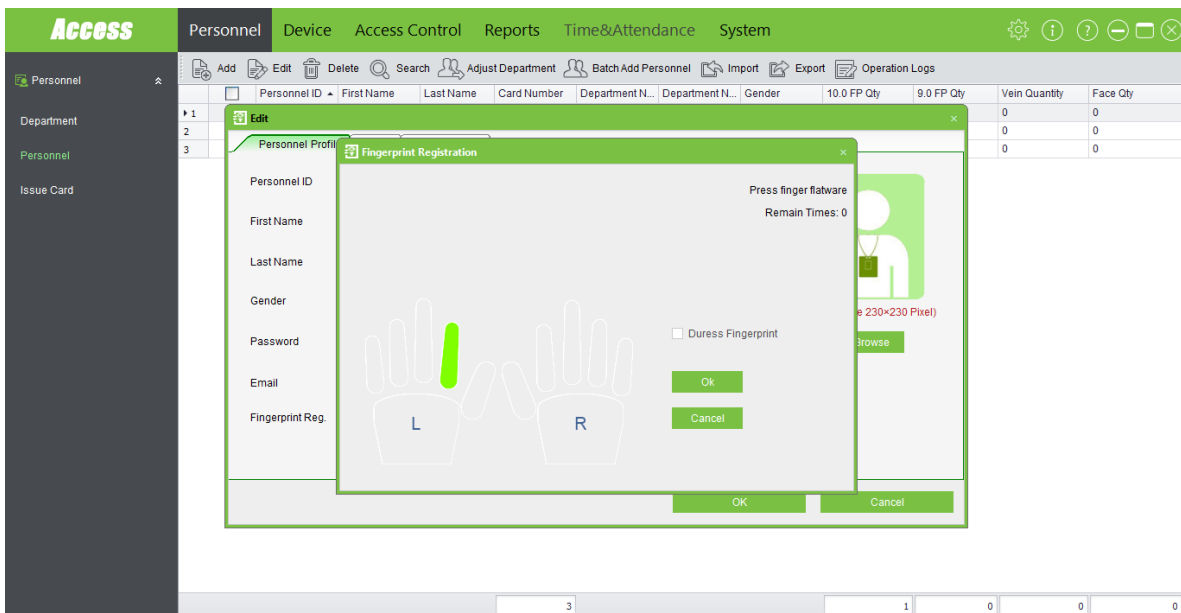


Image 21 – Add fingerprint

Click on **Ok** on the following windows to confirm changes.
Click on **SYNC Now** (**Image 22**).





Triplow

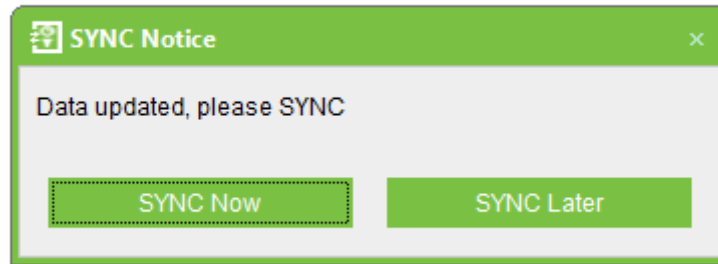


Image 22 – Synchronize new data

- **USB FP Sensor:** If fingerprints are to be added by using the USB F-4500:

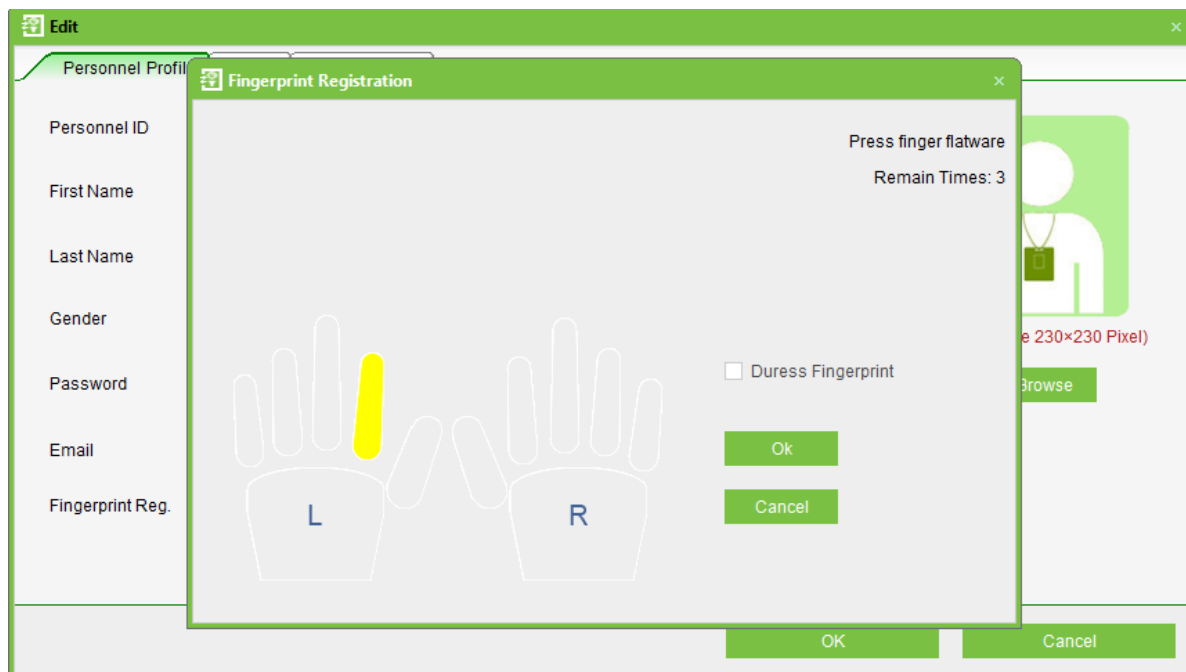


Image 23 – Selection of user's finger

- 1- When selecting the finger on the software (**Image 23**) the device will show the instructions to add fingerprints correctly.
- 2- If the user's fingerprint is added correctly on the software, then the selected finger will turn green (**Image 24**). It can be added as many fingers as desired from the same user (it is recommended to at least add two fingers).



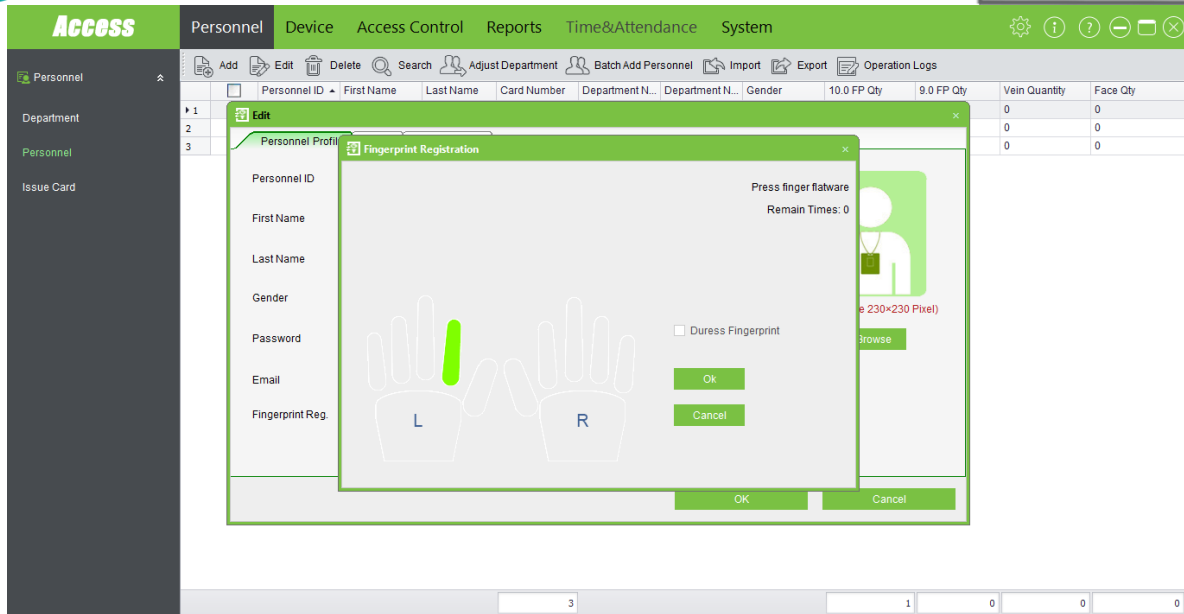


Image 24 – Add fingerprint

Click on **Ok** on the following windows to confirm all changes.
Click on **SYNC Now** (Image 25).

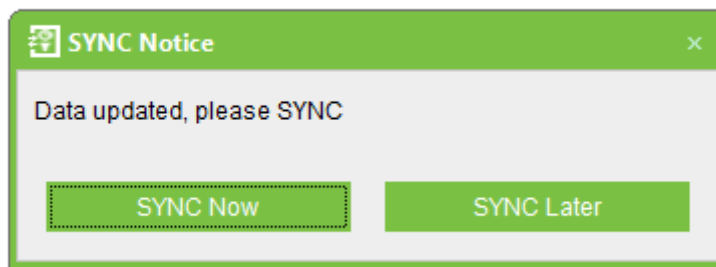


Image 25 – Synchronize new data

1.9. Time Zone

The Time Zone function is used when it is necessary to create schedules where the user is able to open the door by using his access credentials. This function is used for example, for employee shifts, for access to certain areas at specific times, etc.

To create a **Time Zone** click on **Access Control (1)** -> **Time Zone (2)** -> **Add (3)** (Image 26).

As factory default, there is already a predefined time zone of 24h accessibility. This Time Zone has a 24h access setting, which means the door is available for opening 24hs a day.





Triplow W

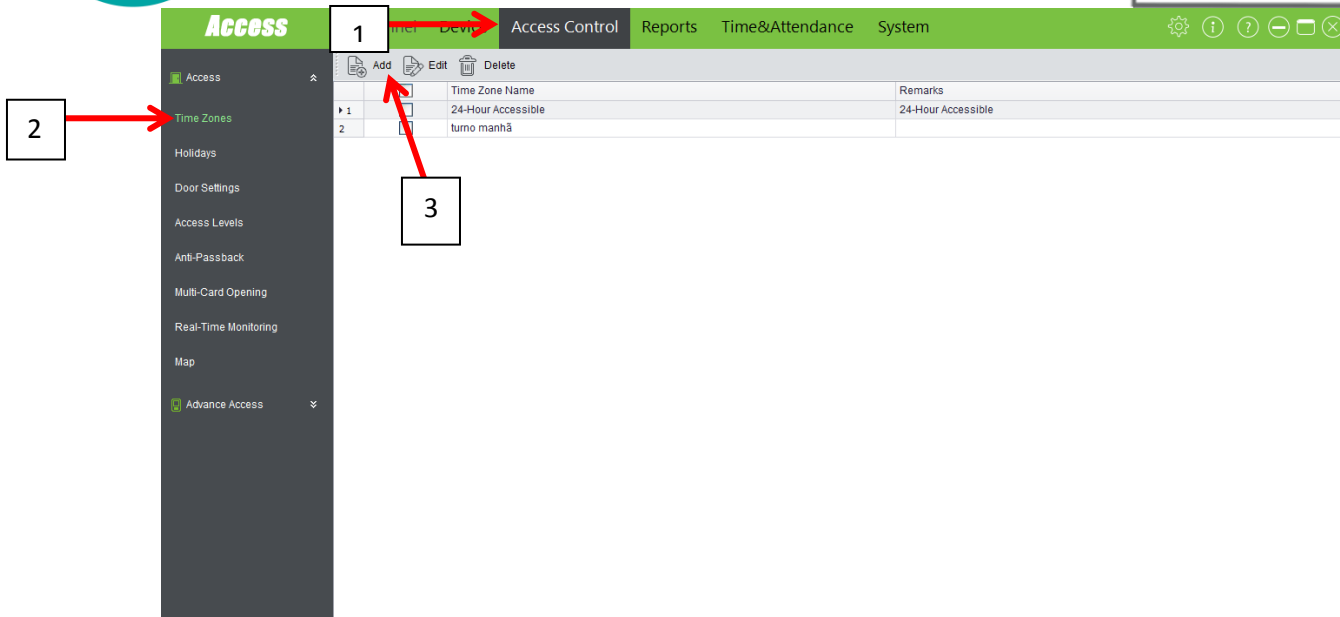


Image 26 - Time Zones

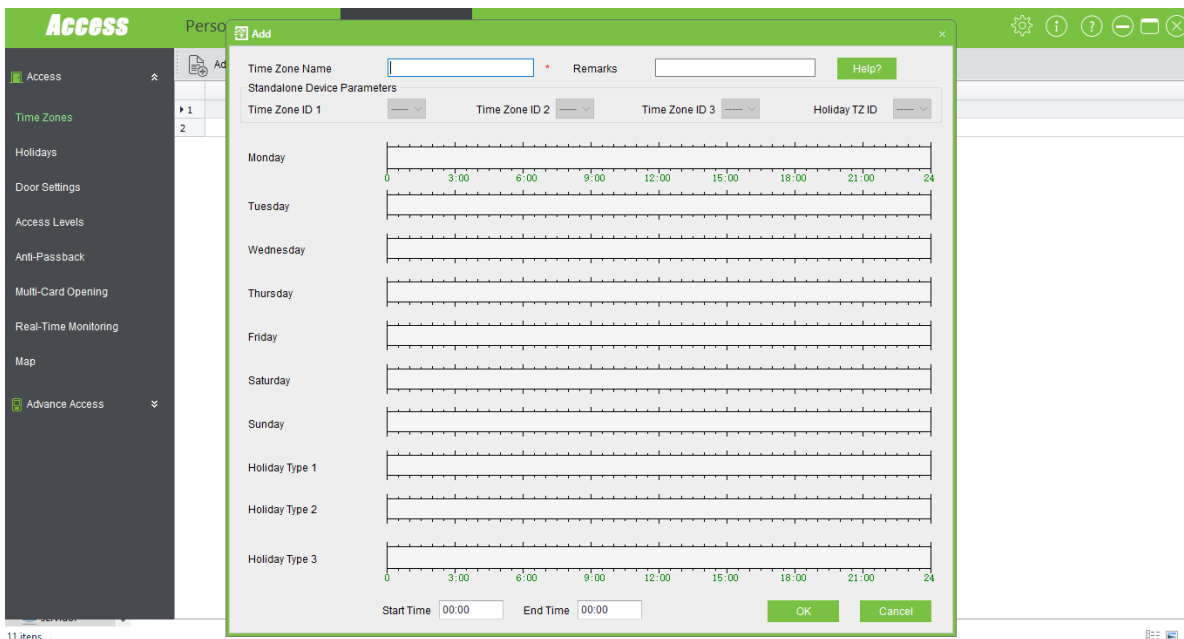
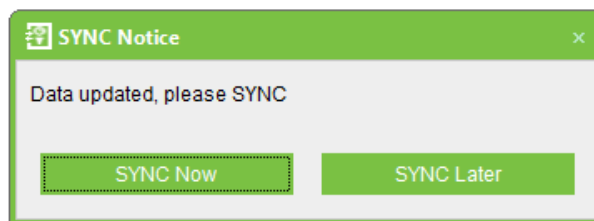


Image 27 - Time Zones

The window on **Image 27** is going to pop out to create a new Time Zone, where it can be created a weekly schedule for the door opening availability.

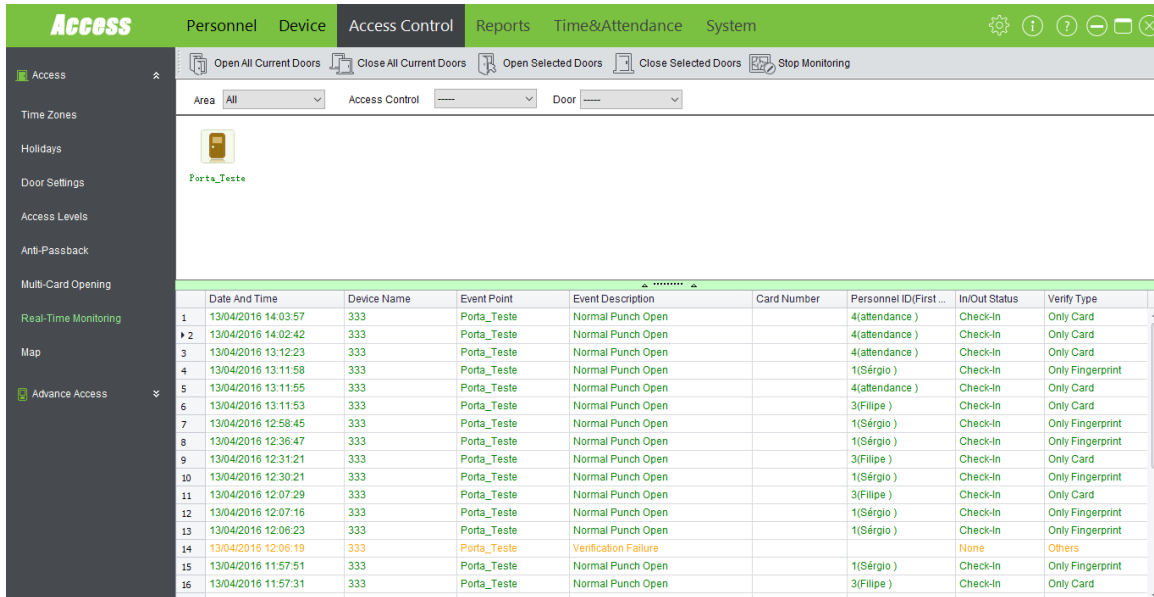


Click on **SYNC Now**.



1.10. Monitoring

In this menu, times made and the remote door opening can be controlled in real time.
Click on **Access Control** -> **Real Time Monitoring**.

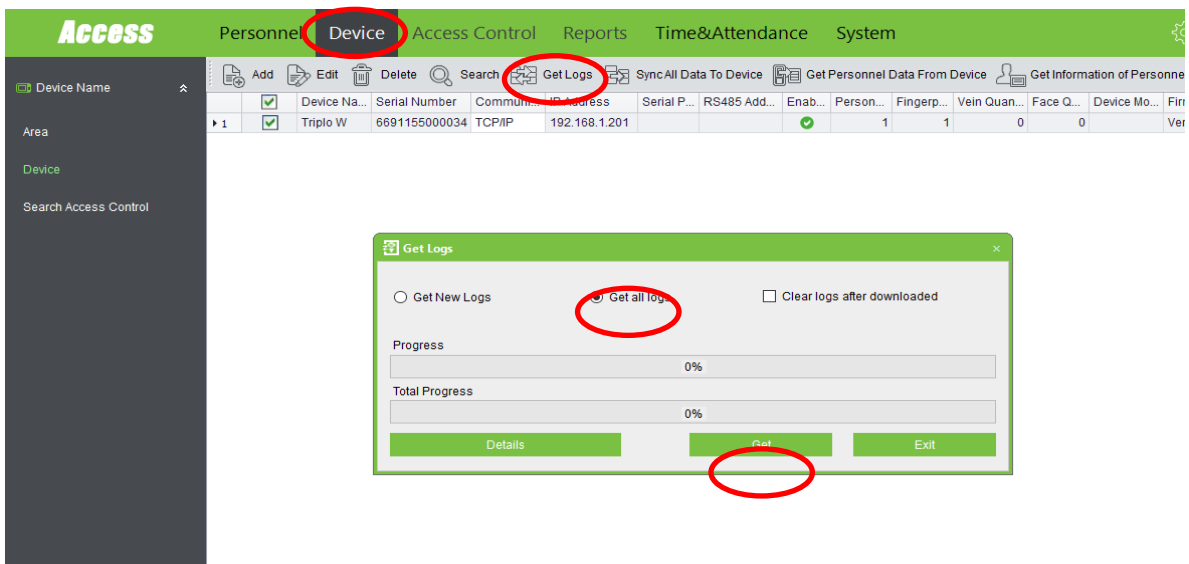


	Date And Time	Device Name	Event Point	Event Description	Card Number	Personnel ID(First ...	In/Out Status	Verify Type
1	13/04/2016 14:03:57	333	Porta_Teste	Normal Punch Open		4(attendance)	Check-In	Only Card
2	13/04/2016 14:02:42	333	Porta_Teste	Normal Punch Open		4(attendance)	Check-In	Only Card
3	13/04/2016 13:12:23	333	Porta_Teste	Normal Punch Open		4(attendance)	Check-In	Only Card
4	13/04/2016 13:11:58	333	Porta_Teste	Normal Punch Open		1(Sérgio)	Check-In	Only Fingerprint
5	13/04/2016 13:11:55	333	Porta_Teste	Normal Punch Open		4(attendance)	Check-In	Only Card
6	13/04/2016 13:11:53	333	Porta_Teste	Normal Punch Open		3(Filipe)	Check-In	Only Card
7	13/04/2016 12:58:45	333	Porta_Teste	Normal Punch Open		1(Sérgio)	Check-In	Only Fingerprint
8	13/04/2016 12:36:47	333	Porta_Teste	Normal Punch Open		1(Sérgio)	Check-In	Only Fingerprint
9	13/04/2016 12:31:21	333	Porta_Teste	Normal Punch Open		3(Filipe)	Check-In	Only Card
10	13/04/2016 12:30:21	333	Porta_Teste	Normal Punch Open		1(Sérgio)	Check-In	Only Fingerprint
11	13/04/2016 12:07:29	333	Porta_Teste	Normal Punch Open		3(Filipe)	Check-In	Only Card
12	13/04/2016 12:07:16	333	Porta_Teste	Normal Punch Open		1(Sérgio)	Check-In	Only Fingerprint
13	13/04/2016 12:06:23	333	Porta_Teste	Normal Punch Open		1(Sérgio)	Check-In	Only Fingerprint
14	13/04/2016 12:06:19	333	Porta_Teste	Verification Failure			None	Others
15	13/04/2016 11:57:51	333	Porta_Teste	Normal Punch Open		1(Sérgio)	Check-In	Only Fingerprint
16	13/04/2016 11:57:31	333	Porta_Teste	Normal Punch Open		3(Filipe)	Check-In	Only Card

Image 28 – Monitoring

1.11. Reports

Click on **Device** -> **Get Logs** -> **Get all logs** -> **Get**.



Device Name	Area	Device
1	Triplow	Search Access Control

Get Logs

Get New Logs
 Get all logs
 Clear logs after downloaded

Progress: 0%

Total Progress: 0%

Image 29 – Reports

After downloading reports from the F-MA300, click on **Reports**





Access Personnel Device Access Control Reports Time&Attendance System

Report

Export Clear All Logs

Search

Time Period: 2016-04-13 00:00 -- 2016-04-13 23:59 Personnel ID:

Card Number: Device Name: First Name:

In/Out Status: Event Description: Verify Type:

	Date And Time	Personnel ID	First Name	Last Name	Card Num...	Device Name	Event Point	Verify Type	In/Out Sta...	Event Description	Remarks
1	2016-04-13 14:37:07					333	Porta_Teste	Others	None	Disconnected	
2	2016-04-13 14:08:03					333	Porta_Teste	Others	None	Disconnected	
3	2016-04-13 14:03:57	4	attendance			333	Porta_Teste	Only Card	Check-in	Normal Punch O...	
4	2016-04-13 14:02:42	4	attendance			333	Porta_Teste	Only Card	Check-in	Normal Punch O...	
5	2016-04-13 13:12:23	4	attendance			333	Porta_Teste	Only Card	Check-in	Normal Punch O...	
6	2016-04-13 13:11:58	1	Sérgio			333	Porta_Teste	Only Finge...	Check-in	Normal Punch O...	
7	2016-04-13 13:11:55	4	attendance			333	Porta_Teste	Only Card	Check-in	Normal Punch O...	
8	2016-04-13 13:11:53	3	Filipe			333	Porta_Teste	Only Card	Check-in	Normal Punch O...	
9	2016-04-13 13:03:04					333	Porta_Teste	Others	None	Disconnected	
10	2016-04-13 12:58:45	1	Sérgio			333	Porta_Teste	Only Finge...	Check-in	Normal Punch O...	
11	2016-04-13 12:36:47	1	Sérgio			333	Porta_Teste	Only Finge...	Check-in	Normal Punch O...	
12	2016-04-13 12:31:21	3	Filipe			333	Porta_Teste	Only Card	Check-in	Normal Punch O...	
13	2016-04-13 12:30:21	1	Sérgio			333	Porta_Teste	Only Finge...	Check-in	Normal Punch O...	
14	2016-04-13 12:07:29	3	Filipe			333	Porta_Teste	Only Card	Check-in	Normal Punch O...	
15	2016-04-13 12:07:16	1	Sérgio			333	Porta_Teste	Only Finge...	Check-in	Normal Punch O...	
16	2016-04-13 12:06:23	1	Sérgio			333	Porta_Teste	Only Finge...	Check-in	Normal Punch O...	
17	2016-04-13 12:06:19					333	Porta_Teste	Others	None	Verification Failure	
18	2016-04-13 11:57:51	1	Sérgio			333	Porta_Teste	Only Finge...	Check-in	Normal Punch O...	
19	2016-04-13 11:57:31	3	Filipe			333	Porta_Teste	Only Card	Check-in	Normal Punch O...	
20	2016-04-13 11:57:28					333	Porta_Teste	Others	None	Button Pressing...	

Image 30 – Reports

In this menu, all accesses performed in a time frame can be seen and exported (days, weeks, months).

1.12. Anti-Passback

The anti-passback is a function that can be used as a security booster and as an entry and exit control. This function consists of ensuring that the user always registers every entry and every exit, that is, if the user registers an entry and leaves without registering the exit, this same user will not be able of entering again because he did not register the exit and the system understands that this user is still inside the building.

This function is also used for the attendance control system.

In order for the anti-passback to work correctly, an exit device with a card or biometric reader has to be coupled up to the F-MA300.

To activate the anti-passback click on **Access Control (1)** -> **Anti-passback (2)** -> **Add (3)**

Image 31 – Anti-passback



A window is going to pop out to set the anti-passback function (**Image 32**).

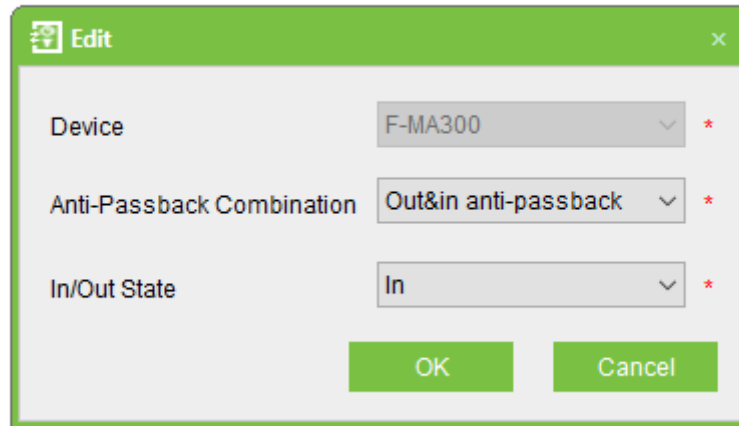


Image 32 – Anti-passback setting window

Device: Choose the device.

Anti-Passback Combination: Out&in anti-passback.

In/Out State: Select In or Out depending on where the F-MA300 is installed, if it is installed on the inner side of the door (out, for entries) or if it is on the outer side (in, for exits).

1.13. Change the F-MA300 device IP

In case it is necessary to change the device IP for an IP within the local network where the F-MA300 was installed, you will have to:

- Have the information regarding the network IP.
- Have the information of a free IP within the network.

After collecting the information previously mentioned, the F-MA300 needs to be directly connected to a computer by using a network cable (RJ45).

First, the device needs to be added to the program with its original IP (point 1.4).

After adding successfully the device to the software, in order to change its IP you need to click on:

Device (1) -> Select device (2) ->More (3) ->Modify IP Address (4)





Triplow

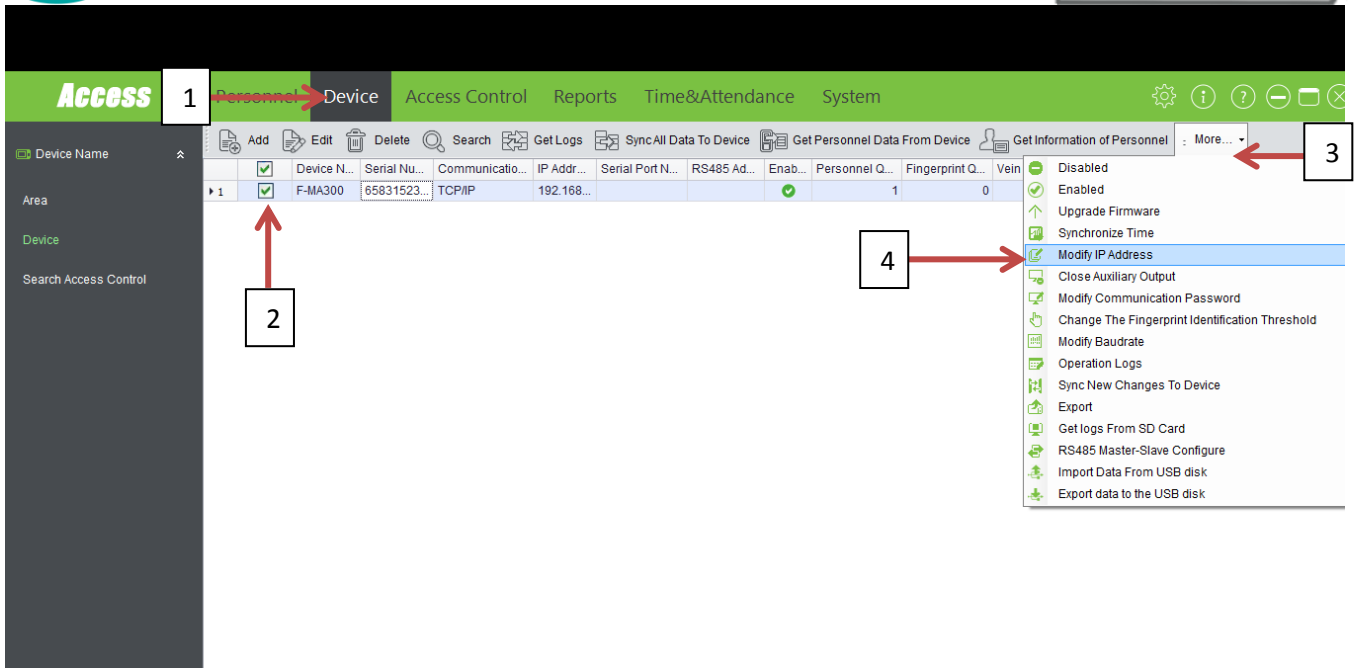
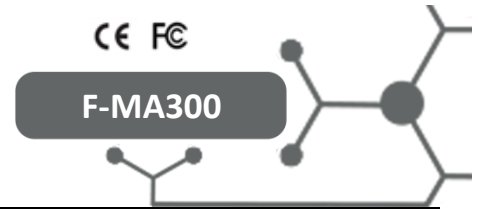


Image 33 – Modify original device IP

A setting window is going to open up to modify the device IP.

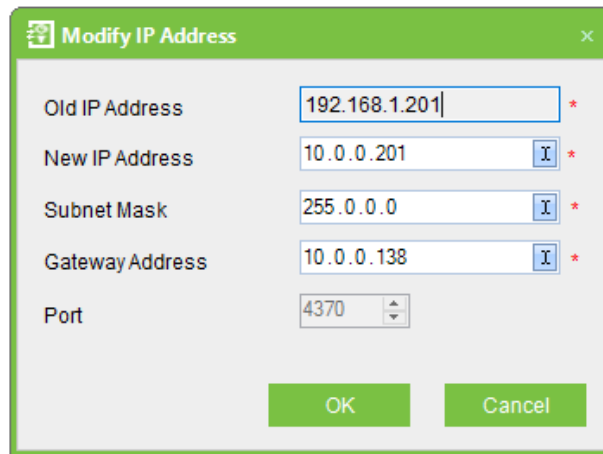


Image 34 – Modify the device IP

On the **Image 33** window, the device IP can be modified for the one desired within the internal network, and so, the device can be directly connected to a router/switch.

Note: If you do not have access to the internal network IP range, then it is recommended to contact the service provider or someone specialized in networks.



2. Additional Functions Performed Directly on the Equipment

Door opening
Press the fingerprint for 1s or present the access card.

2.1. Add administrator card

The administrator card is acquired along with the device (key chain, card).

If the equipment asks for the administrator card (**Please register the management card**) (*please register the administrator card*), present the requested card.

2.2. Reset factory settings

In order to reset factory settings you need to:

1. Disconnect the device from the power supply.
2. Connect the adapter included on the purchase, to the micro-usb port at the bottom of the device.
3. Connect a computer keyboard to the adapter.
4. Present the administrator card.
5. Press 3+Enter+3+Enter on the keyboard.
6. Next, you will hear: **"Restore to default settings. The operation is successful. The system returns to verification state"**.
7. Disconnect the equipment for 60 seconds.
8. Connect the equipment.

3. Technical Specifications

Power supply	12V DC
Relay (output)	3A
Memory	10000 Users
Access log memory	100000
Identification time	<1s
Communications	TCP/IP
Dimensions	150 x 75 x 36 mm
LED	Multicolour (red/green)

