

FaceSentry6

AN / Mini

Standard/Micro controller

Hello!

Quick Start Guide

FCC Note

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.

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, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following

measures:

- 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.

Note: The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. such modifications could void the user's authority to operate this equipment

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

CE Note

Manufacturer: IWT Limited.

Address: 2503 Skyline Tower, 39 Wang Kwong Road, Kowloon Bay, Hong Kong

Hereby, IWT Limited. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU
A copy of the declaration of conformity can be obtained with this user manual;
This product is not restricted in the EU.

The wireless operation frequency

RFID: 13.56MHz; Max H-Field Strength: -4.2dBuA/m at 10m

The device has been evaluated to meet FCC/CE general RF exposure requirement. The device can be used without restriction

Table of contents

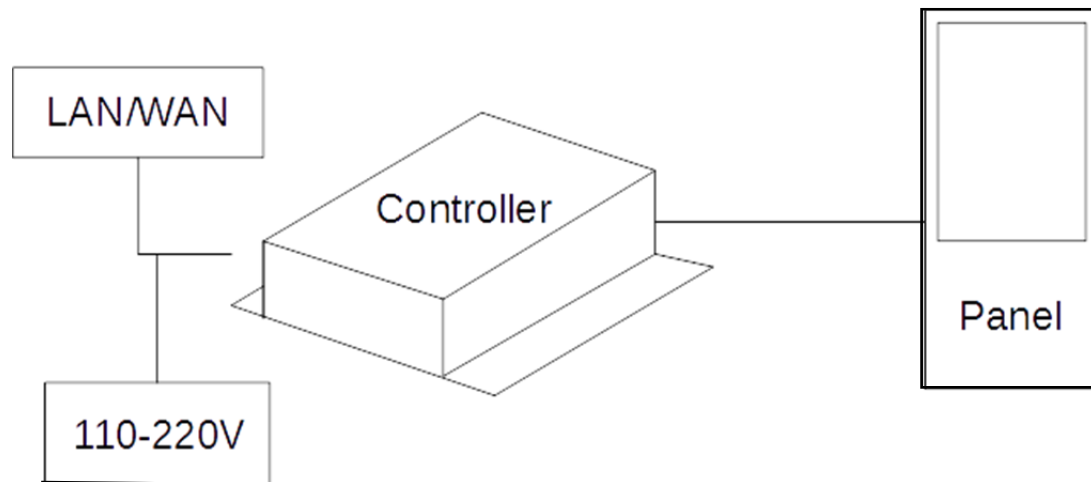
1	LOGIN FACEENTRY6 WEB PAGE	6
2	FACEENTRY INTERNET MANAGEMENT TOOL.....	7
3	ADD NEW USER	8
4	USER REGISTRATION.....	13
5	CHECK ACCESS LOG.....	15
6	HOW TO OPEN 1:N IDENTIFY MODE	18
7	HOW TO USE FASENTRY6 FOR DOOR OPENING	20

Welcome to FaceSentry6 AN and Mini. Let me introduce:



Cable connection

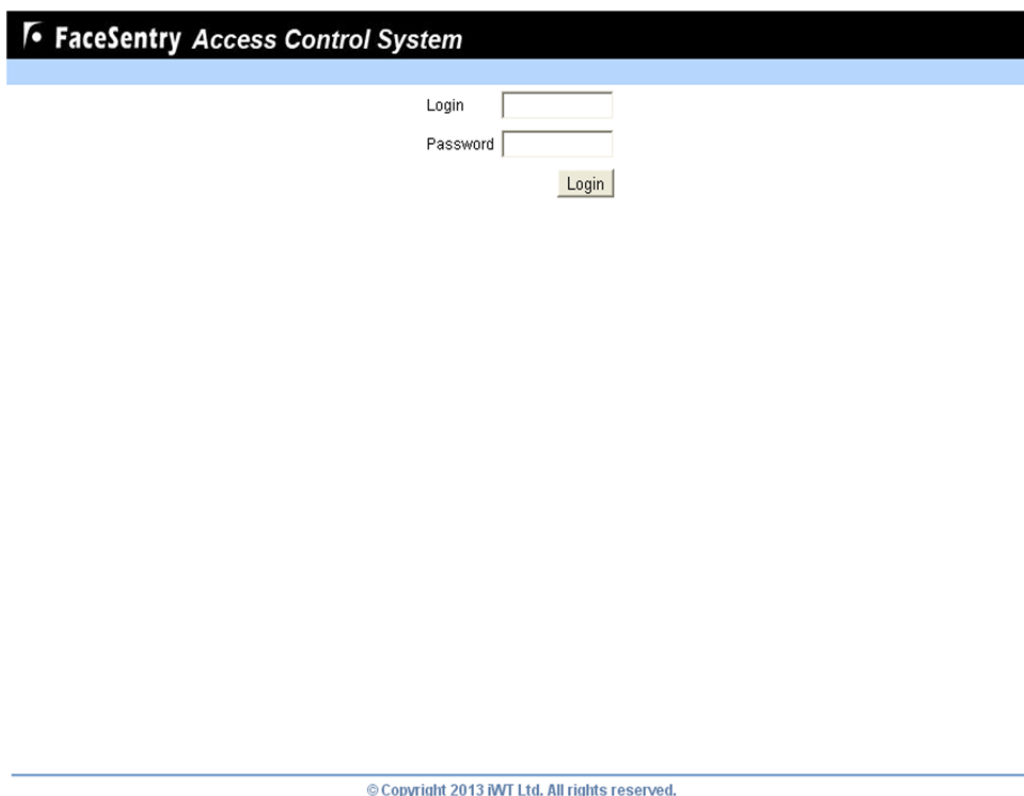
Please set up the device like the following picture, turn the power on then we could start using it.



1. Getting Start

Firstly, launch your Internet browser (e.g. Internet Explorer 8.0 or later, Firefox, Safari or Google Chrome), fill in the IP address of FaceSentry6 AN device in the Address (URL) field, and press ENTER key.

You should be able to see the Administration Web Tool, like the screen shot below:



FaceSentry Access Control System

Login

Password

Login

© Copyright 2013 IWT Ltd. All rights reserved.



Default factory settings are

IP address: 172.16.1.252

Username: administrator (case sensitive)

Password: 123456

2. FaceSentry Web Administration Tool

Front page of FaceSentry Web Administration Tool shall be displayed after correct username and password were entered:

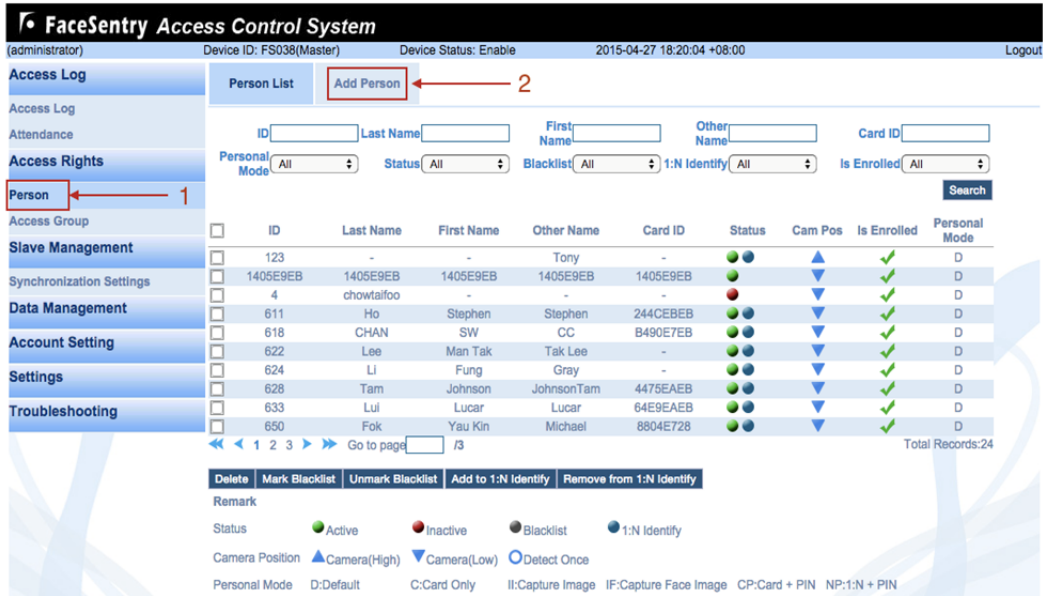
The screenshot shows the FaceSentry Access Control System web administration tool. The title bar at the top displays the user 'administrator', the device ID 'FS234/Master', the device status 'Enable', the date and time '2014-06-05 23:20:57 +08:00', and a 'Logout' button. The main menu on the left includes options like Access Log, Attendance, Access Rights, Person, Access Group, Slave Management, Synchronization Settings, Data Management, Account Setting, Settings, Sentry Info, User Management, Application Setting, Network Setting, System Setting, Multimedia Settings, Device Operation, and Troubleshooting. The main content area is titled 'Sentry Info' and shows various settings for the device, including General Information, Network, Application Setting, and Card Format.

Category	Parameter	Value
General Information	Device ID	FS234
	Device Role	Master
	Hardware Key	2fa431c20cca00f15209ae910661df
	FN HardwareKey	000459de70c: 12634211
	Firmware Version	5.6.0-pre build-151
	Algorithm	A14
	Maximum Person Number	500
	Maximum Identify Number	100
	Maximum Access Log Number	20000
	Total Up Time	1175190.94
Sentry Service Status	Sentry Service Status	Started
	NTP Service Status	Started
	DHCP Service Status	Started
	SNMP Service Status	Started
Network	IP Address	192.168.0.234
	Subnet Mask	255.255.255.0
	Subway IP	192.168.0.1
	Panel Network Range	192.168.11.x/255.255.255.0
	DNS IP	192.168.0.94
	Time Server Address	192.168.0.94
	HTTPS	Not In Use
Application Setting	Admin Mode	Default
	Main Mode(Panel 1)	Card Keyboard Identify
	Main Mode(Panel 2)	Card Keyboard Identify
Card Format	Input Setting	
	Reader Type	MIFARE
	Wiegand Format	32 bits
Output Setting	Card Format	HEX
	Wiegand Output	None
	Wiegand Format	32 bits

1. Title bar: to display current user login ID, Device ID, Device status, current date and time, followed by Logout button.
2. Main Menu: to launch all types of menu options and settings
3. Option Tab: to display all sorts of functions under the current menu option
4. Content pane: to display the content and settings of the current selected option tab

3. Adding Person

To add a new enrollee, select “Person” menu option,



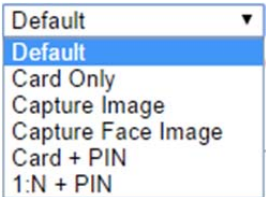
and then click “Add Person” tab as screen shot shown below:

The screenshot shows the 'Add Person' form. The form has the following fields and options:

- ID:** 0005 (Max. 10 char.)
- Last Name:** Zhang (Max. 10 char.)
- First Name:** San (Max. 10 char.)
- Other Name:** Sam (Max. 10 char.)
- Card ID:** B44EF7EB
- Status:** Active Inactive
- Camera Position:** Lower Camera
- Personal Mode:** Default
- PIN:** (4 to 10 digits)
- 1:N Identify:** Enable Disable
- Threshold:** (Decimal from 0 to 1)
- Accessgroup:** Super Group (), Test Group 01 (1), 23123 (12SHR), 1RES (1PSR), 3RBB (3RB)
- Schedule Status:** Active Inactive Delete
- Schedule Date:** (YYYY/MM/DD)
- Schedule Time:** (HH:mm:ss)
- TEMP1 Display:** (Empty field)
- TEMP2 Display:** (Empty field)
- TEMP3 Display:** (Empty field)
- TEMP4 Display:** (Empty field)

At the bottom of the form is an 'Add Person' button.

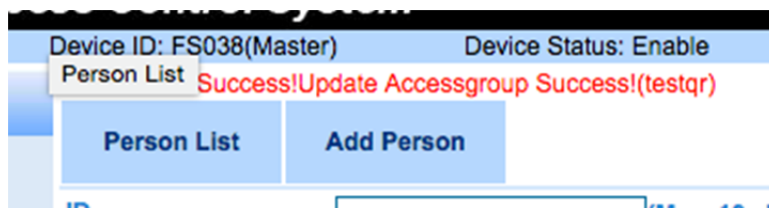
Fill in the fields as prompt below:

Field	Description
ID	Unique identifier (ID) of the enrollee
Last name	Last name
First name	First name
Other Name	Short name to display on the screen after match
Smart Card ID	Smart Card ID (in your case, the ID represented by the QR code)
Status	<p>Either Active or Inactive.</p> <p>Enrollee with Inactive radio button selected will be blocked from being 1:1 verified, even though his/her smart card ID or QR code ID was read.</p> <p>Under 1:N identification mode, if inactive enrollee was being identified, a warning message will be shown at the end to notify the user, and no door strike action will be done.</p>
Personal Mode	<p>Default mode is 1:1 Verification (QR code scan first, follow by facial verification)</p> 
1:N Identify	To toggle on/off of 1:N Identification mode

Personal Threshold	To input threshold setting for the current enrollee: a floating point number range from 0 to 1. If this field was blank, system threshold will be in effect. The priority of this personal threshold will override the system threshold if it is not null.
#Access Group	To set access privilege of the current enrollee
*Schedule status	To set a schedule (date forward) task by selecting required radio button
Schedule date	To set the execution date of the current schedule task
Schedule time	To set the execution time of the current schedule task

Please be reminded that: at least one access group should be selected for any enrollee. For new/novice operator, please leave “SuperGroup” selected to avoid “No Right” error message because of the enrollee does not belong to any access group, and get rejected by the device.

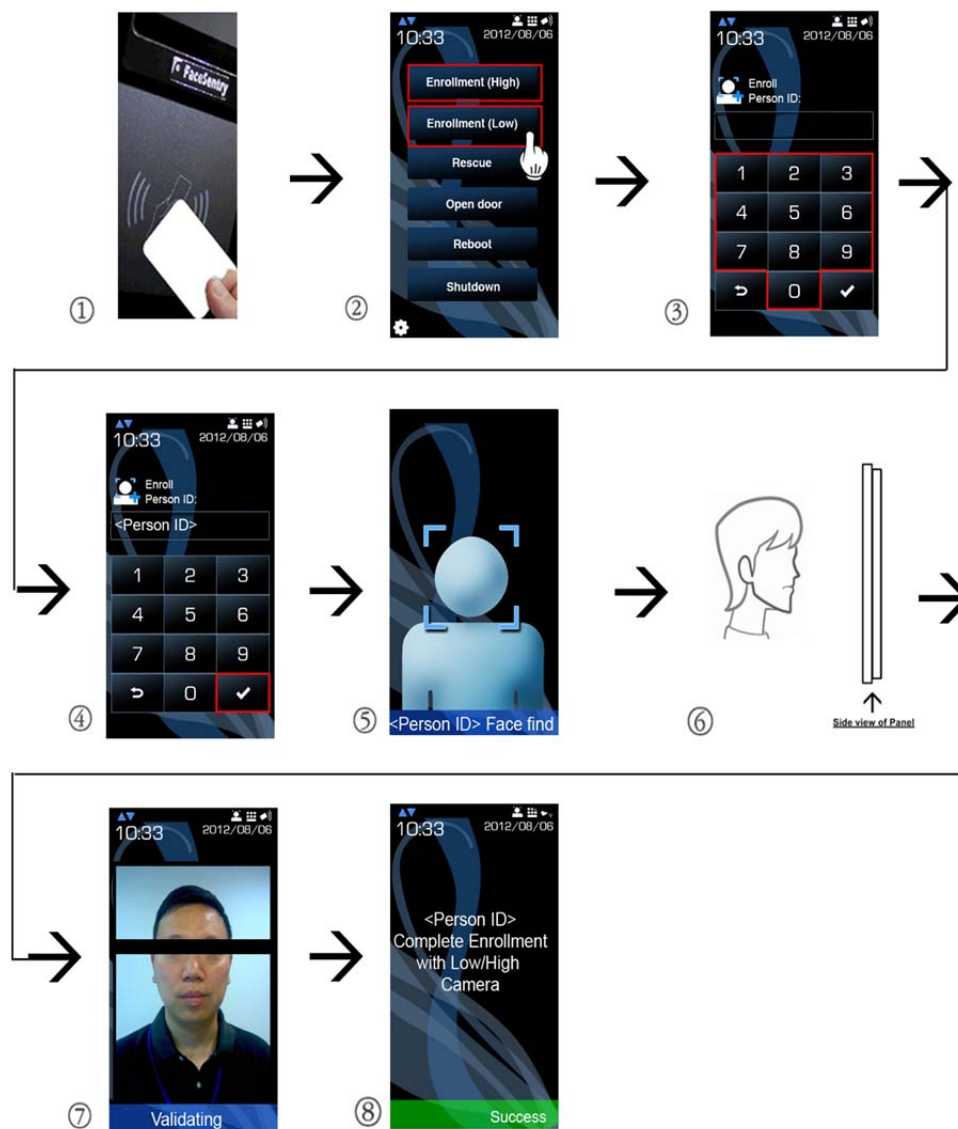
Finally, press “Add Person”, and you can expect this confirmation message:



That's all to complete an Add Person task.

4. Enrolling a Person

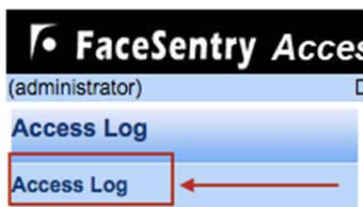
Photo-capture and enrolment is the final step to get a new person enrolled with the device. Please perform these steps on the front panel of the FaceSentry device:



Step	Description
1	Scan the “Special Card” smart card or QR code with the reader
2	Tap “Upper Camera” or “Lower Camera” button on the touch screen. We recommend to user lower camera for enrollee not taller than 1.7m
3	Scan the smart card or QR code of the current enrollee If no smart card or QR code to be used, tap on the on-screen keypad to input ID instead
4	Tap the OK ✓ button
5	Stand still and get ready for the photo capture
6	Look straight at the screen of the panel
7	Wait for 2 photo shootings and you should be able see yourself on the screen. First photo will be used to enroll, and the second photo to be used to make a test verification.
8	Enrolment done successfully

5. View access log

From FaceSentry web administration tool, select “Access Log” option as screen shot illustrated below:



Access log main page will be displayed, like screen shot below:

Access Log List Add Access Log

Date From Date To Person ID Card ID Search

Device ID Access Status All Cam Pos All Direction All

Time	Person ID	Card ID	Device ID	Panel#	Direction	Cam Pos	Operation	Access Status	Input Mode
2014-07-11 15:19:50	0001	-	FS234	0	In	▼	Identify	Unauthorized	Auto Face Find
2014-07-11 14:51:29	-	-	FS234	0	In	▲	Identify	Unauthorized	Auto Face Find
2014-07-05 18:56:00	-	-	FS234	0	In	▼	Identify	Unauthorized	Auto Face Find
2014-06-21 16:14:07	-	-	FS234	0	In	▲	Identify	Unauthorized	Auto Face Find
2014-06-21 16:13:28	-	-	FS234	0	In	▼	Identify	Unauthorized	Auto Face Find
2014-06-21 15:14:34	0001	-	FS234	0	In	▼	Identify	Success	Auto Face Find
2014-06-20 22:28:34	0001	-	FS234	0	In	▲	Identify	Unauthorized	Auto Face Find
2014-06-20 18:15:45	-	-	FS234	0	In	▼	Identify	Unauthorized	Auto Face Find
2014-06-20 17:55:33	0001	-	FS234	0	In	▼	Identify	Success	Auto Face Find
2014-06-20 17:55:20	0001	-	FS234	0	In	▲	Identify	Unauthorized	Auto Face Find
2014-06-20 17:55:03	-	-	FS234	0	In	▲	Identify	Unauthorized	Auto Face Find
2014-06-20 17:28:56	0001	-	FS234	0	In	▲	Identify	Unauthorized	Auto Face Find
2014-06-20 17:28:34	0001	-	FS234	0	In	▼	Identify	Success	Auto Face Find
2014-06-20 17:28:27	0001	-	FS234	0	In	▼	Identify	Success	Auto Face Find
2014-06-20 17:28:20	0001	-	FS234	0	In	▼	Identify	Success	Auto Face Find
2014-06-20 17:28:11	0001	-	FS234	0	In	▲	Identify	Success	Auto Face Find
2014-06-20 15:08:39	-	-	FS234	0	In	▲	Identify	Unauthorized	Auto Face Find
2014-06-20 15:06:39	0001	-	FS234	0	In	▼	Identify	Success	Auto Face Find
2014-06-20 15:06:30	0001	-	FS234	0	In	▼	Identify	Success	Auto Face Find
2014-06-20 15:06:24	0001	-	FS234	0	In	▲	Identify	Unauthorized	Auto Face Find

◀◀ 1 2 3 4 5 ▶▶ Go to page /7 Total Records:122

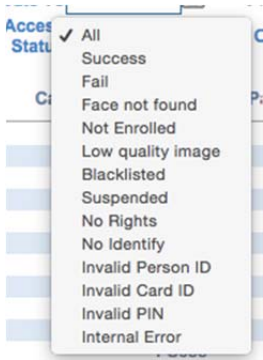
Remark
Camera Position ▲Camera(High) ▼Camera(Low) ○Detect Once

User can navigate by selecting Page Up, Page Down, Top, Bottom, or simply click the page number to jump to required page.



Or, we recommend user to set selection criteria to pinpoint the logs required:

Parameters	Descriptions
------------	--------------


Date From, Date To	To set date range (inclusive) of logs required
Person ID	To display all logs of matching person ID
Card ID	To display all logs of the matching smart card or QR code ID
Device ID	To display all logs of matching device ID
Status	To display all logs of matching status 
Cam Pos	To display all logs of matching camera position: Upper, Lower or show All
Direction	To display all logs of matching direction of the access: In, Out or show All

User can click on “Time” position of each access log record to display a pop-up screen that shows the detail of this selected access log record:


Time	Person ID	Card ID	Device ID	Panel#	Direction	Cam Pos	Operation	Access Status	Input Mode
2013-04-13 09:29:47	626		FS038	0	In	▼	Identify	Success	Auto Face Find
2013-04-13 09:13:15	624		FS038	0	In	▼	Identify	Success	Auto Face Find
2013-04-12 09:12:05			FS038	0	In	▼	Identify	Unauthorized	Auto Face Find
2013-04-12 09:12:05	611		FS038	0	In	▲	Identify	Success	Auto Face Find
2013-04-12 09:06:05			FS038	0	In	▲	Identify	Unauthorized	Auto Face Find
2013-04-11 18:51:42	699		FS038	0	In	▲	Identify	Success	Auto Face Find
2013-04-11 11:25:05			FS038	0	In	▼	Identify	Unauthorized	Auto Face Find

Access Log Detail

Access Log Detail



Enrollment Photo



Access Log ID	0000030062
Time	2015-04-27 15:00:14
Person ID	678
Card ID	
Device ID	FS038
Operation	Identify
Access Status	Success
Score	0.999504
Panel#	0
Direction	In
Input Mode	Auto Face Find
Cam Pos	Lower Camera

Moreover, the device provides a last resort: Add Access Log, to allow administrator to enter an access log manually without facial recognition. But the log will be marked clearly that such access record was entered by Administrator.

Access Log List
Add Access Log

Person ID (Max. 10 char.)

Date (YYYY/MM/DD)

Time (HH:mm:ss)

Type In Out

Add

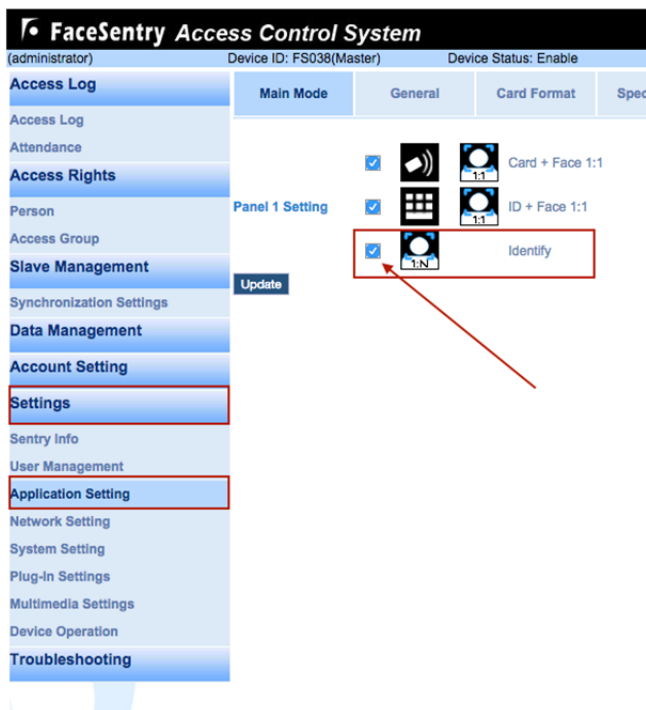
6. How to open 1:N recognition mode

The operation needs to execute on 2 levels:

1. Open 1:N recognition mode on FaceSentry 5 equipment
2. Open 1:N recognition rights on registration level

Then, below are the operating steps.

First, find “Settings | Application Setting | Main Mode”, ensure the frame in front of “1:N identify” is already ticked, shows below:



Second, find menu through “Access Rights | Person” to choose ID for running 1:N recognition mode.

Click "Edit" button, then ensure "1:N Identify" "Enable" is chosen, shows below:

FaceSentry Access Control System

(administrator) Device ID: FS038(Master) Device Status: Enable 2016-02-25 1

Person List Add Person

ID: Last Name: First Name:

Personal Mode: All Status: All Blacklist: All

ID	Last Name	First Name	Other Name	Card ID
<input type="checkbox"/>	123	Lau	Tony	Tony
<input type="checkbox"/>	6000	HseKeeping	1	-
<input type="checkbox"/>	6001	HseKeeping	2	-
<input type="checkbox"/>	6003	HseKeeping	3	-
<input type="checkbox"/>	611	Ho	Stephen	Stephen 244C
<input type="checkbox"/>	618	CHAN	SW	Carl B490
<input type="checkbox"/>	622	Lee	Man Tak	Tak Lee 3609
<input type="checkbox"/>	624	Li	Fung	Gary
<input checked="" type="checkbox"/>	628	Tam	Johnson JohnsonTam	4475E
<input type="checkbox"/>	63	Lui	Lucar	Lucar 64E9

Go to page: /3

Delete Mark Blacklist Unmark Blacklist Add to 1:N Identify Remove from 1:N Identify

Remark:

Status: Active Inactive Blacklist 1:N Identify

Camera Position: Camera(High) Camera(Low) Detect Once

Personal Mode: D:Default C:Card Only II:Capture Image IF:Capture

Person Detail

628
Last Name: Tam
First Name: Johnson
Other Name: JohnsonTam
Card ID: 4475EAEB
Status: Active
Camera Position: Lower Camera
Personal Mode: Default
1:N Identify: Enable
Threshold:

Accessgroup: Super Group ()

Enrollment Time: 2014/05/07 11:26:17
Schedule Status: Active

TEMP1 Display
TEMP2 Display
TEMP3 Display
TEMP4 Display

Edit

FaceSentry Access Control Sy

https://192.168.0.38/personDetail.php

Person Detail

ID: 628

Last Name: Tam (Max. 10 char.)

First Name: Johnson (Max. 10 char.)

Other Name: JohnsonTam (Max. 10 char.)

Card ID: 4475EAEB

Status: Active Inactive

Camera Position: Lower Camera

Personal Mode: Default

PIN: (4 to 10 digits)

1:N Identify: Enable Disable Threshold:

Accessgroup: Super Group ()
Lunch (Lunch)
normal group (NO)
OfficeHour (OfficeHour)

Schedule Status: Active Inactive Delete Schedule Da
Schedule Tir

TEMP1 Display
TEMP2 Display
TEMP3 Display
TEMP4 Display

Update Cancel

7. How to use FaceSentry for door opening

It is easy but you need to connect a few wires. Following steps are for preparation before operating.

7.1 FaceSentry standard controller

1. Find FaceSentry 5 control box
2. Prepare the key of FaceSentry 5 control box because the control box is locked. You can find the key from the accessory bag in the package.
3. Confirm the message of your electric lock, latch, magnetic lock, revolving door or automatic door with the supplier, to confirm for whether there is door lock connector. You can find the door lock connector from the electric lock power source or the control board. These connectors have different label, e.g. NC, NO, GND. You need to confirm which connector is used for receiving the door open message from machine with the supplier.
4. Connect the suitable connector with compatible cable at the end of the electric lock. The other side of the electric lock should be connected with the controller box of FaceSentry 5.
5. Under default setting, door open signal should be connected with the first relay module on the top right-hand corner (count from the top to bottom). As picture below, NC connects with the universal relay module 1, universal relay module 2 will also be connected.



6. Check the relay setting configuration from “Settings | System Setting”.
As picture below, relay module 1 setting as open door, relay module 2 setting as rang doorbell. You can choose from the menu to change for the configuration.

FaceSentry Access Control System

(administrator) Device ID: FS038(Master) Device Status: Enable 2016-02-25 11:58:4

Access Log Device Setting Date & Time Panel Setting **Relay Setting**

Access Log

Attendance

Access Rights

Person

Access Group

Slave Management

Synchronization Settings

Data Management

Account Setting

Settings

Sentry Info

User Management

Application Setting

Network Setting

System Setting

Plug-In Settings

Multimedia Settings

Device Operation

Troubleshooting

Relay Setting

Function Name	I/O Board ID	Relay ID
Panel1Open Door	1	1
Panel1DoorBell	1	2
Panel1Anti-Duress	1	3

Period Setting

Open Door	0.5	(second(s))
DoorBell	0.5	(second(s))
Anti-Duress	0.5	(second(s))

7.2 FaceSentry6 with a microcontroller

1. Find the microcontroller box of FaceSentry AN or Mini



Software default settings from the network management page:

Function Name	I/O Board ID	Relay ID
Panel1Open Door	1	1
Panel1DoorBell	1	2
Panel1Anti-Duress	1	3

Open Door	<input type="text" value="0.5"/>	(second(s))
DoorBell	<input type="text" value="0.5"/>	(second(s))
Anti-Duress	<input type="text" value="0.5"/>	(second(s))

2. NC1+Com1: Lock signal export
3. NC2+Com2: Doorbell signal export
4. Confirm the message of your electric lock, latch, magnetic lock, revolving door or automatic door with the supplier, to confirm for whether there is door lock connector. You can find the door lock connector from the electric lock power source or the control board. These connectors have different label, e.g. NC, NO, GND. You need to

confirm which connector is used for receiving the door open message from machine with the supplier.

- End of Quick Start Guide –
Renewal date: 2018/09/12