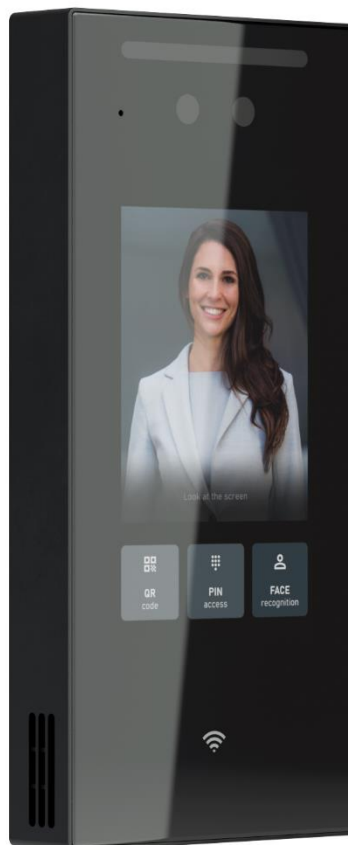


eKinex

CONTROL YOUR LIVING SPACE

Administrator Guide



DICO video intercom with facial recognition

EK-5DP-VI

Contents

1.	Scope of the document.....	7
2.	Product Overview	8
3.	Model Specification.....	9
4.	Access the Device	11
4.1	Access the Device Setting on the device.....	11
4.2	Access the Device Setting on the Web Interface	11
5.	Time and Language Setting.....	13
5.1	Language Setting.....	13
5.2	Time Setting.....	13
5.3	Light setting.....	15
5.3.1	Configure Card Reader LED Setting	15
5.3.2	Configure LED White Light Setting.....	15
5.4	Screen Display configuration	16
5.4.1	Configure Screensaver.....	16
5.4.2	Upload Screensaver	17
5.4.3	Configure the company information display.....	18
5.4.4	Configure the PIN keypad display mode.....	18
5.4.5	Homepage configuration	19
5.4.6	Configure Background display	20
5.5	Volume and Tone Configuration	21
5.5.1	Volume Configuration.....	21
5.5.1.1	Configure Volume on the Device	21
5.5.1.2	Configure Volume on the Web Interface.....	22
5.5.2	Upload Open Door Tone	23
5.5.3	Configure Door Access Prompt Text	24
6.	Network Setting.....	25
6.1	Device Network Connection Setting	25
6.2	Device Deployment in Network.....	26
6.3	NAT Setting.....	27
7.	Intercom Call Configuration	28
7.1	IP call and IP Call Configuration	28
7.1.1	Make IP calls	28
7.1.2	IP Call Configuration	28
7.2	SIP Call and SIP Call Configuration.....	29
7.2.1.1	SIP Account Registration.....	29
7.2.1.2	Configure SIP Account on the Device.....	29
7.2.2	SIP Server Configuration on the Web interface	30
7.2.3	Configure Outbound Proxy Server on the Web interface.....	31
7.2.4	Configure Data Transmission Type.....	31
7.3	Dial Options Configuration	32
7.3.1	Quick Dial By Number Replacement on the Device	32

7.3.2	Quick Dial by Number Replacement on the Web Interface	33
7.4	Auto-answer Configuration	33
7.5	Sequence Call Configuration	34
7.6	Enabling Prevent SIP Hacking.....	36
7.7	Call Settings.....	37
7.7.1	Maximum Call Duration Setting.....	37
7.7.2	Maximum Dial Duration Setting.....	37
7.7.3	Audio / Video Codec Configuration for SIP Calls	38
7.7.3.1	Configure Audio Codec.....	38
7.7.3.2	Configure Video Codec.....	39
7.8	Configure DTMF Data Transmission	40
8.	Contact List Configuration	41
8.1	Contact List Configuration on the Device	41
8.2	Contact List Configuration on the Web Interface.....	42
8.2.1	Managing users on Web Interface	42
8.2.2	Managing Contact Groups on the Web Interface	43
8.2.3	Managing Contact List Display Setting	43
9.	Relay Switch Setting.....	45
9.1	Relay Switch Setting.....	45
9.2	Web Relay Setting	46
9.2.1	Configure Web Relay on the Web Interface	46
9.2.2	Configure Web Relay on the Device.....	48
9.3	Security Relay.....	50
9.4	Relay Schedule.....	51
10.	Door Access Schedule Management.....	52
10.1	Configure Door Access Schedule	52
10.1.1	Create Door Access Schedule on the Web interface	52
10.1.2	Create Door Access Schedule on the Device	54
10.1.3	Import and Export Door Access Schedule in the Web interface.....	54
10.1.4	Edit the Door Access Schedule	55
11.	Door Unlock Configuration.....	57
11.1	Access Authentication.....	57
11.2	Configure PIN Code for Door Unlock	57
11.2.1	Configure Public PIN code	57
11.2.2	Configure Private PIN code on the Device	59
11.2.3	Configure Private PIN code on the Web Interface.....	59
11.2.4	Configure Private PIN Access Mode	61
11.3	Configure RF Card for Door Unlock.....	61
11.3.1	Add RF Card on the Web Interface	61
11.3.2	Add RF Card from Device Setting.....	63
11.3.3	Configure RF Card Code Format	64
11.4	Configure Facial Recognition for Door Unlock.....	64

11.4.1	Enroll Face Data on the Device	64
11.4.2	Upload Face Data on the Web Interface.....	65
11.4.3	Configure Facial Recognition	66
11.5	Configure Door Access Using Configured Files	67
11.5.1	Editing the User(s)-specific Door Access Data	69
11.6	Unlock by QR Code	69
11.7	Unlock by Bluetooth	69
11.8	Unlock by NFC	70
11.9	Unlock by HTTP Command on Web Browser	70
11.10	Unlock by Exit Button by the Door	71
11.11	Unlock by Reception Tab.....	72
11.12	Unlock by DTMF Code	73
11.12.1	Configure DTMF White List.....	74
12.	Security	75
12.1	Tamper Alarm Setting	75
12.2	Emergency Action	76
12.3	Security Notification Setting	77
12.3.1	Email Notification Setting	77
12.3.2	FTP Notification setting	78
12.3.3	TFTP Notification Setting	78
12.3.4	SIP Call Notification.....	79
12.4	Automatic log-out from the web interface	79
12.5	Action URL.....	80
13.	Monitor and Image.....	82
13.1	MJPEG Image Capturing	82
13.2	Live Stream.....	83
13.3	RTSP Stream Monitoring	84
13.3.1	RTSP Basic Setting	84
13.3.2	RTSP Stream Setting	85
13.4	Acquisition in ONVIF standard.....	86
13.4.1	Camera Mode.....	87
14.	Logs	88
14.1	Call Logs	88
14.2	Door Logs	88
15.	Debug	90
15.1	System Log for Debugging.....	90
15.2	PCAP for Debugging.....	90
15.3	Remote Debug Server	91
15.4	Face Recognition Debug	92
15.5	User Agent	92
16.	Firmware Upgrade	93
17.	Backup.....	94
18.	Auto-provisioning via Configuration File.....	95

18.1 Provisioning principle	95
18.2 Configuration Files for Auto-provisioning.....	95
18.3 AutoP Schedule	96
18.4 PNP Configuration	97
18.5 DHCP Provisioning Configuration	97
18.6 Static Provisioning Configuration	99
19. Integration with Third Party Device.....	102
19.1 Wiegand integration	102
19.2 Integration via HTTP API	103
19.3 Lift control.....	104
19.3.1 OSDP integration mode	105
19.3.2 Ekinex integration mode.....	105
19.3.3 KEYRING integration mode	106
19.4 Integrate with third-party Access Control Server	106
20. Password Modification	107
21. System Reboot and Reset.....	109
21.1 Reboot.....	109
21.2 Reset.....	110
22. FAQ.....	112
23. Markings	113
24. Maintenance	113
25. Disposal	113
26. General warnings.....	113
27. Other information	114

Release	Changes	Date	Author	Verified by
1.0	First issue	26/09/2023	G. Schiochet	C. Baldini
1.1	Corrections after first issue of Italian language manual	17/11/2023	G. Schiochet	C. Baldini
1.2	Added references to Ekinex Delégo	22/11/2023	G. Schiochet	C. Baldini
1.3	Added reference to the security relay EK-SR1-VI	01/12/2023	G. Schiochet	C. Baldini
1.4	Cover image updated	02/07/2024	G. Schiochet	I. Panero
2.0	Updated to FW rel. 216.43.100.26	12/07/2024	G. Schiochet	C. Baldini
2.1	Updated to FW rel 216.43.100.31	25/07/2024	G. Schiochet	I. Panero

1. Scope of the document

Thank you for choosing the Ekinex EK-5DP-VI “DICO” device.

This manual is intended for the administrators who need to properly configure the door phone. This manual applies to the 216.43.0.18 version and later, and it provides all the configurations for the functions of EK-5DP-VI “DICO” door phone. Please visit the www.ekinex.com website or contact the technical support at the following e-mail address: support@ekinex.com for any new information or the latest firmware.

2. Product Overview

The Ekinex EK-5DP-VI “DICO” device is a Linux system IP video door phone with a touch screen. It integrates audio and video communications, access control, and video surveillance. The device offers customizable features through its advanced system, Ekinex Delégo, and AI-based communication technology, adapting to your operational preferences. This comprehensive solution ensures holistic control over building entrances and surroundings, providing enhanced security through various access methods such as smart card access, NFC, mobile app, QR code, PIN code, ideal for residential buildings, office buildings, and complexes.

3. Model Specification

Display	5" IPS
Touch Screen	√
Resolution	1280 x 720 pixel
Camera	2M pixel dual-lens, WDR
Relay Out	1
Alarm In	1
Card Reader	13.56MHz
Ethernet port	RJ45, 10/100Mbps adaptive 802.3af Power-over-Ethernet
Wiegand connection	√
Face recognition	√
RS485	√
PoE	√
Brightness	500cd/m ²
RAM	1GB
ROM	8GB
IP Rating	IP65
Wall Mounting	√
Flush Mounting	√
POE Stand by Power	5.5W

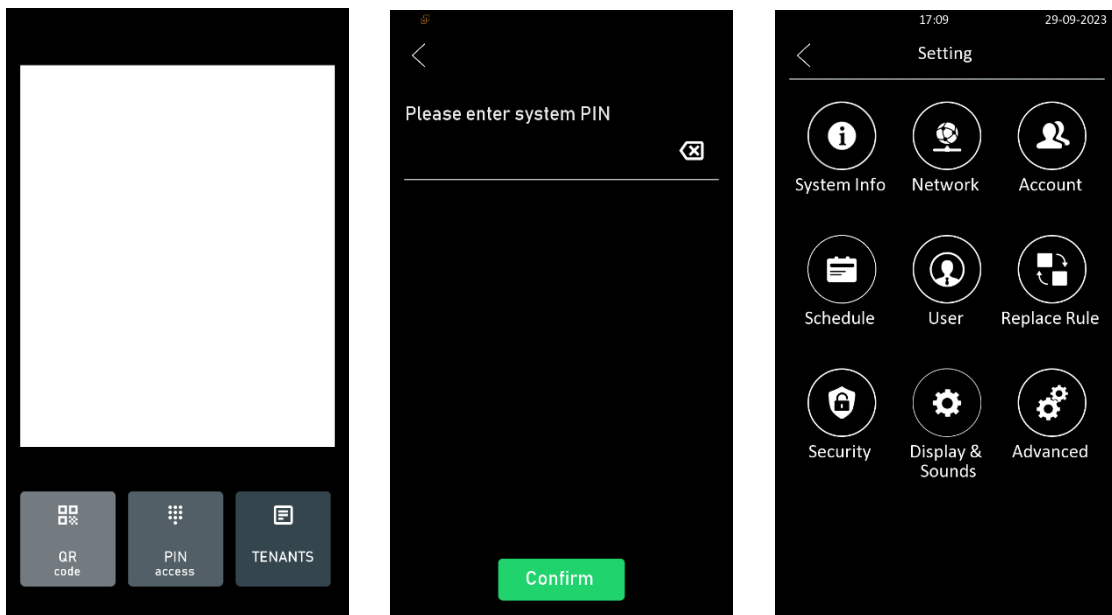
POE Full Load Consumption	9.8W
Power Adapter Standby Power	5.5W
Power Adapter Full Load Consumption	10W

4. Access the Device

DICO device system settings can be either accessed on the device directly or on the device web interface.

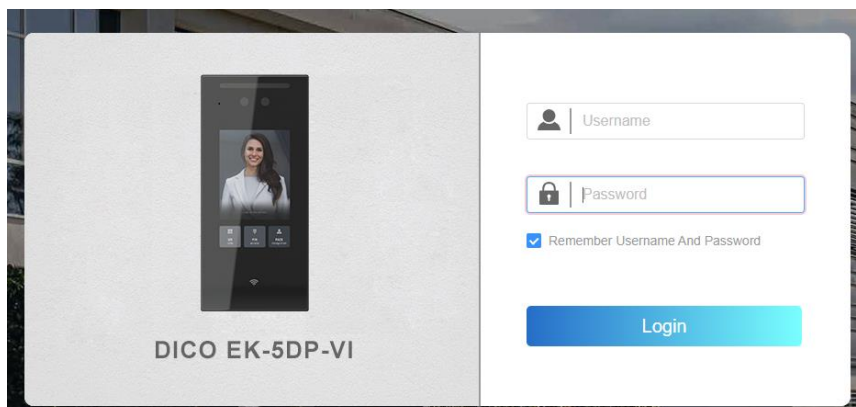
4.1 Access the Device Setting on the device

To access the device setting, you can long press on the initial screen for approximately five seconds, then enter the default PIN code **admin** and press *Confirm*.



4.2 Access the Device Setting on the Web Interface

You can also use a common IP scanner tool in order to search the device's IP address on the same LAN. Then enter the device IP address on the web browser in order to login to the device web interface where you can configure and adjust parameters etc. Then use the IP address to login into the web browser by user name and password **admin** and **admin**.

**Note**

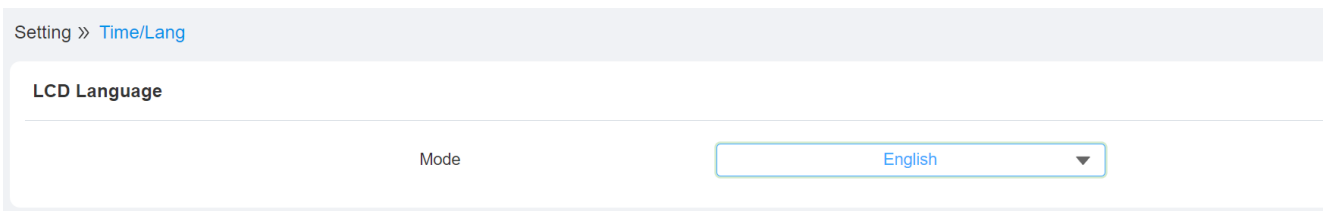
- Google Chrome browser is strongly recommended.
- The initial user name and password are **admin** and please be case-sensitive.

5. Time and Language Setting

5.1 Language Setting

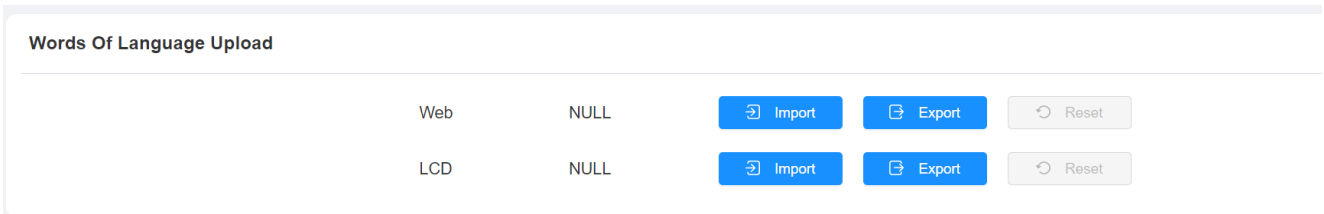
You can select **Device language**, and customize interface text including configuration names and prompt text display on the device and on the web interface.

To select the device language, go to **Setting > Time/Lang > LCD Language** interface.



To customize configuration names and prompt text, you need to export and edit the .json file before uploading the file to the device.

This can be done in the web interface at the following link: **Setting > Time/Lang > Words Of Language Upload**.



5.2 Time Setting

Time setting on the web interface can be done at the following link:

Setting > Time/Lang > Time

This allows the user to set up time and date manually or by adding a NTP server address, to automatically synchronize time and date. As soon as the time zone is selected, the device will automatically notify the NTP server of its time zone so that the NTP server can synchronize the time zone setting in your device.

Time	
Automatic Date&Time Enabled	<input checked="" type="checkbox"/>
Time Zone	GMT+0:00 London
Preferred Server	0.pool.ntp.org

Time	
Automatic Date&Time Enabled	<input type="checkbox"/>
Date	2023-07-11
Time	06:52
Time Zone	GMT+0:00 London
Preferred Server	0.pool.ntp.org

Parameter set-up:

- **Automatic Date&Time Enabled:** enable it if you want the device's date and time to be automatically set up and synchronized with the default time zone and the NTP server (**Network Time Protocol**).
- **Time Zone:** select the specific time zone depending on where the device is used and then press **Submit key** for the confirmation. The default time zone is GMT+0.00.
- **Primary Server:** enter the primary NTP server you obtained in the **NTPServer**.

Note

- When the check box is not ticked, parameters related to the NTP server cannot be edited.

5.3 Light setting

5.3.1 Configure Card Reader LED Setting

You can enable or disable the LED lighting on the card reader area as needed on the web interface. Meanwhile, if you do not want the card reader LED light to stay on, you can also set the timing for the exact time span during which the LED light can be disabled to reduce the electrical power consumption. To setup the configuration on the web interface, please move to **Device > Light > LED Of Swiping Card Area**

Device » Light

LED Of Swiping Card Area

Enabled

Start Time - End Time(Hour) - (0-23)

Parameter set-up:

- **Start Time- End Time (H):** enter the time span for the LED lighting to be valid, e.g. if the time span is from **18-22**, it means the LED light will stay on during the time span from **6:00 pm to 10:00 pm** during one day (24 hours).

5.3.2 Configure LED White Light Setting

LED White Light is used to reinforce the lighting for facial recognition as well as for QR code access in the dark environment. To configure the function on the web interface, go to **Device > Light > White Light**

White Light

Mode

Max White Light Value

Parameter Set-up:

- **Mode:** if you select **Auto**, then the white light will be turned on automatically for face recognition and QR code scan for door opening. If you select **Off**, then the white light will be disabled.
- **Max White Light Value:** set the white light value in the **1-5 range**, where default white light value is **3**. The greater value it is, the brighter the light will be.

Note

- IR LED light should be triggered first before the white light can be valid in the facial recognition, however, IR LED light does not need to be triggered for the white light function in the QR code scan.

5.4 Screen Display configuration

DICO door phone allows you to enjoy a variety of screen displays to enrich your visual and operational experience through the customized setting to your preference.

5.4.1 Configure Screensaver

The Screensaver is mainly a function for screen protection. You can make the device go into idle status for a predefined time span when there is no operation on the device, or no one is detected approaching.

This can be configured via the web interface at **Device > LCD > Standby Interface Display**.

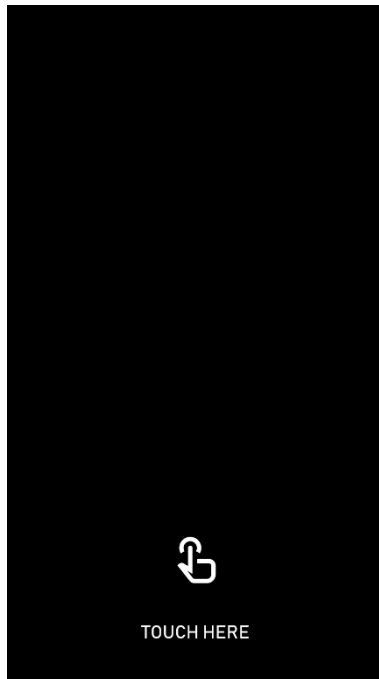
Standby Interface Display

Screensaver Mode	<input checked="" type="checkbox"/>
Screensaver Time	30minutes ▼
Sleep	15seconds ▼
Wakeup Mode	Auto ▼

Parameter set-up:

- **Screensaver Mode:** it allows to enable/disable the Screensaver feature.
- **Screensaver Time (sec):** set how long you expect the screen saver to last before turning off the device's display. This Sleep time can be setup in 5 seconds to 2 hours range.
- **Sleep (sec):** set the screen saver start time from 2 seconds up to 30 minutes after the last activity. For example, if you set the start time as 5 minutes, then the screen saver will start if there is no operation on the device or no one is approaching during the five minutes interval.
- **Wakeup Mode:** select the screen wake-up mode. By choosing **Auto** mode, the screen will wake up when someone approaches without being touched; if you select **Manual** mode, you will need to touch the display to wake it up; if you select **Touch Here Icon** mode, after touching the display you will then

need to click on the “Touch Here” icon (visible on the display in the lower central position) to wake it up.



5.4.2 Upload Screensaver

The user can upload custom screensaver pictures to the device. This setting can be configured on web interface at the following link: **Device > LCD > Upload Screensaver**. A maximum of 5 pictures can be uploaded, and each picture will be displayed in rotation according to the ID order with a specific time duration (**Interval**) set.

Upload Screensaver

Screensaver1

Screensaver ID	File Status	Interval(Sec)	Delete
1	File Exists	<input type="text" value="5"/>	<input type="button" value="Delete"/>
2	File Exists	<input type="text" value="5"/>	<input type="button" value="Delete"/>
3	File Exists	<input type="text" value="5"/>	<input type="button" value="Delete"/>
4	File Exists	<input type="text" value="5"/>	<input type="button" value="Delete"/>
5	File Exists	<input type="text" value="5"/>	<input type="button" value="Delete"/>

NOTE:

- The pictures uploaded should be in **JPG** or **PNG** format with 2M pixels maximum size.
- Previously saved images with a specific Screensaver ID will be overwritten when next loading of images with the same ID occurs.

5.4.3 Configure the company information display

You can configure company information for the welcome page from the web interface by selecting **Device > LCD > Company Information**.

Company Information

Company Name	<input type="text" value="Ekinex S.p.A."/>
Street Number	<input type="text" value="37"/>
Company Address	<input type="text" value="Via Novara Vaprio d'Agogna"/> ?
Working Hours	<input type="text" value="8:30 - 12:30 / 14:00 - 18:00"/>

Parameter Set-up:

- **Company Name:** allows you to enter the company name.
- **Street number:** the street number of the address, up to 5 digits;
- **Company Address:** can be configured on two lines, using the "|" character to separate them;
- **Working Hours:** to enter any opening hours of the company.

5.4.4 Configure the PIN keypad display mode

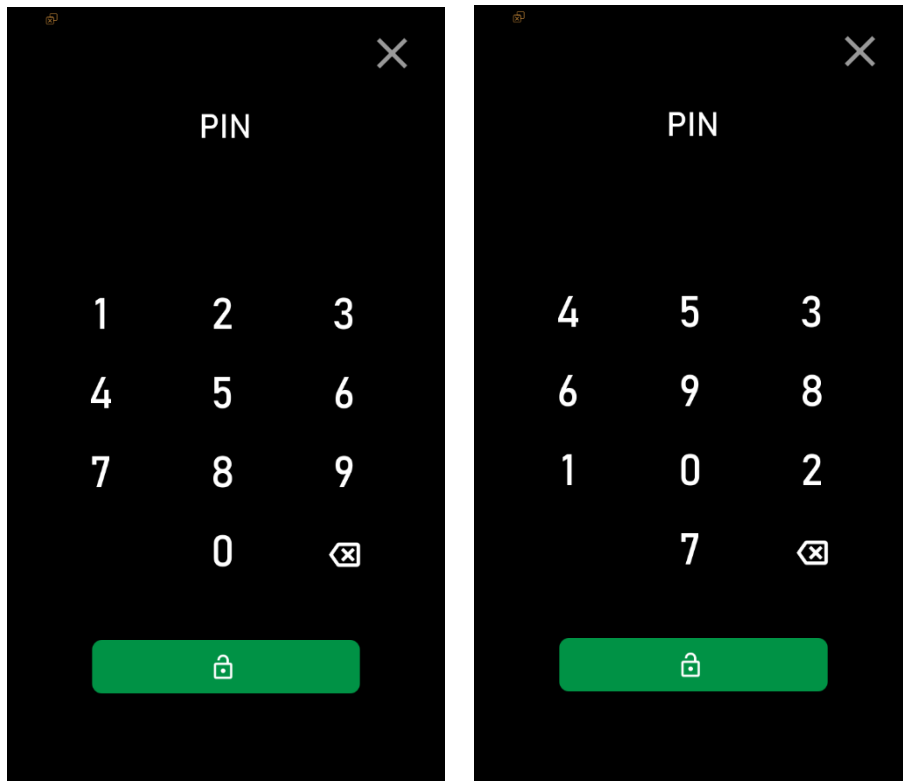
There are two types of keypad display modes that can be selected for PIN input; **Normal** mode or **Random** mode. On the web interface, this can be configured in **Device > LCD > Keypad Display Mode of PIN interface**.

Keypad Display Mode Of PIN Interface

Mode	<input type="text" value="Normal"/>
------	-------------------------------------

Parameter set-up:

- **Normal:** the sequence of numbers is ordered from 0 to 9;
- **Random:** the numbers are displayed randomly: this allows to increase security, as there is no correspondence between the numbers and any digital imprints left by an authorized user.



5.4.5 Homepage configuration

You can change the display of the home page by configuring the name of the virtual keys (from 1 to 3 buttons) and their arrangement. Path: **Device > LCD > Key in Homepage**

Key In Homepage

Display Type

Speed Dial Tenants Display Company ...

QR Code Recognition Interval(Sec)

ID	Name	Type	Value
1	<input type="text" value="Use '[' for line breaks"/>	<input type="text" value="QR Code"/>	<input type="text"/>
2	<input type="text" value="Use '[' for line breaks"/>	<input type="text" value="PIN"/>	<input type="text"/>
3	<input type="text" value="Use '[' for line breaks"/>	<input type="text" value="Tenants"/>	<input type="text"/>

Parameter set-up:

- **Display Type:** Select among **four display types: Company information, Face, QR code, Speed Dial Tenants.** By choosing QR code, the DICO camera is available to frame a login QR code.

NOTE: By choosing **Speed Dial Tenants**, users are displayed in the Homepage if a number has been entered in the contact details and **Type = Speed Dial Tenants** has been selected in the web interface at **Directory > User > Contact details**.


- **Speed Dial Tenants Display Company information:** allows you to display the Company information in the homepage, even by choosing “**Speed Dial Tenants**” as type for the Contact details.
- **QR code recognition interval (Sec):** it allows to set, in seconds, the time interval for recognition between two QR codes.
- **ID:** key identifier.
- **Name:** enter a new name to replace the original one, without changing the type attribute. You can enter up to 2 lines, separated by the “|” character.
- **Type:** select the tab type corresponding to the index number which indicates the tab position. For example, if you want to make the **Speed Dial Tenants** tab be displayed in position one, you can change the type in index number 1 to **Speed Dial Tenants**. And you can change another tab position accordingly.
- **Value:** enter the IP or SIP number to be attached to the reception icon for the speed dial. The number entered will be dialed out as you press the **Reception** icon on the home screen. This field is only valid for speed dial. You can type in five-speed dial numbers maximum and every two of the number must be separated by “;”. You can also select a contact group to be called by pressing the **Reception** icon.


5.4.6 Configure Background display

You can upload a background for the Company Information page, from the **Device > LCD > Upload Background** interface.

Upload Background

Company Info Page Background

 Import

 Reset

Parameter Set-up:

By clicking on **Import** button, you can select an image file to use as a background. The maximum size allowed is 200 kB, the format can be .jpg, .jpeg, .bmp, .png.

X

File(Max Size: 200KB, Format: .jpg, .png, .bmp, .jpeg, Recommended resolution: 720*1280)

Not selected any files

Select File

Reset

Cancel

Upload

5.5 Volume and Tone Configuration

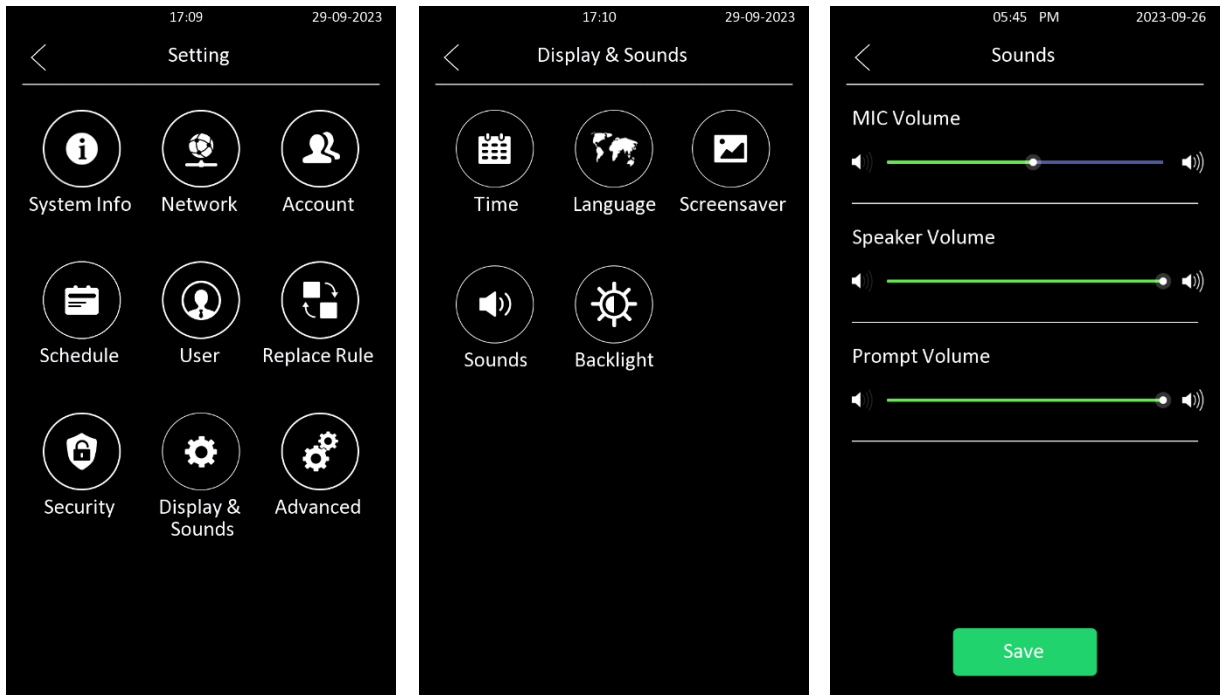
Volume and tone configuration in DICO door phone refers to the call volume (speaker), Mic volume, and prompt volume (eg. open door tone). Moreover, you can upload the tone you like to enrich your personalized user experience.

5.5.1 Volume Configuration

You can configure the microphone volume, speaker volume, and tamper alarm volume according to your need for intercom-based audio/video communication. Moreover, you can also set up the tamper alarm volume when unwanted removal of the door phone occurs.

5.5.1.1 Configure Volume on the Device

You can adjust the microphone volume, speaker volume, and prompt volume on the device. Starting from the Setting page, move to **Display & Sounds > Sounds**.



Parameter set-up:

- **MIC Volume:** adjust the microphone volume.
- **Speaker Volume:** adjust the internal speaker volume.
- **Prompt Volume:** adjust the prompt volume, which includes various types of prompt sound for door open success and failure, ringback, temperature measurement sound (where available), etc.

5.5.1.2 Configure Volume on the Web Interface

On the web interface, you can set the tamper alarm volume, Mic volume, speaker volume, and prompt volume.

Path: **Device > Audio > Volume Control.**

Device » [Audio](#)

Volume Control

Mic Volume	<input style="width: 90%;" type="text" value="8"/>	(1~15)
Speaker Volume	<input style="width: 90%;" type="text" value="15"/>	(1~15)
Tamper Alarm Volume	<input style="width: 90%;" type="text" value="15"/>	(1~15)
Prompt Volume	<input style="width: 90%;" type="text" value="15"/>	(0~15)
Allow Adjustment During Call	<input checked="" type="checkbox"/>	

Parameter set-up:

- **Mic Volume:** to adjust the volume of the microphone.
- **Speaker Volume:** to adjust the volume of the internal speaker.
- **Tamper Alarm Volume:** to adjust the volume for the tamper alarm.
- **Prompt Volume:** adjust the prompt volume, which includes various types of prompt sound for door open success and failure, ringback, temperature measurement sound, etc.
- **Allow Adjustment During Call:** to enable/disable the adjustment while a call is in progress.

5.5.2 Upload Open Door Tone

You can upload the Open-Door Tone on the device web interface. The path to follow on the web interface is **Device > Audio > Open Door Tone Setting**.

Open Door Tone Setting

Open Door Tone Enabled

Open Door Succeed Tone Upload

Note

- The open door tone file should be in .wav format and the file size should be smaller than 200KB.

5.5.3 Configure Door Access Prompt Text

You can enable or disable the door access prompt to be shown on the access control terminal screen for door open failure and success. This parameter can be configured on the web interface at **Access Control > Relay > Door Setting General**.

Door Setting General

Open Door Succeeded Text Prompt	<input type="checkbox"/>
Open Door Failed Text Prompt	<input type="checkbox"/>
Display User Info	<input type="checkbox"/>

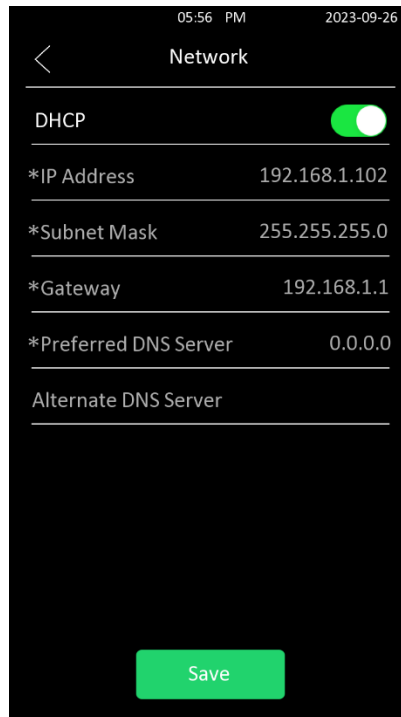
Parameter set-up:

- **Open Door Succeeded Text Prompt:** tick the check box if you want to see the text prompt after the door opening success.
- **Open Door Failed Text Prompt:** tick the check box if you want to see the prompt words after the door open failure.
- **Display User Info:** tick the check box if you want to see the detected user information.

6. Network Setting

6.1 Device Network Connection Setting

You can select **DHCP** (Dynamic Host Configuration Protocol) mode or **static IP** connection. When you select static IP connection, you can manually set up IP address, Subnet Mask, Default Gateway, and DNS servers.



Parameter set-up:

- **DHCP:** select the **DHCP mode** by moving the toggle switch to the right. DHCP mode is the default network connection. If the DHCP mode is turned on, then the door phone will be assigned by the DHCP server with IP address, subnet mask, default gateway, and DNS server address automatically.
- **Static IP:** select the **static IP mode** by checking off the DHCP check box. When static IP mode is selected, then the IP address, subnet mask, default gateway, and DNS server address have to be manually configured according to your actual network environment.
- **IP Address:** set up the IP Address if the static IP mode is selected.
- **Subnet Mask:** set up the subnet Mask according to your actual network environment.
- **Gateway:** set up the correct gateway default gateway according to the IP address of the default gateway.
- **Preferred&Alternate DNS Server:** set up a preferred or alternate DNS Server (**Domain Name Server**) according to your actual network environment. Preferred DNS server is the primary DNS server address

while the alternate DNS server is the secondary server address, and the door phone will connect to the alternate server when the primary DNS server is unavailable.

To configure the device network on the web interface, go to **Network > Basic > LAN Port**.

LAN Port

Type	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP
IP Address	<input type="text"/>
Subnet Mask	<input type="text"/>
Default Gateway	<input type="text"/>
Preferred DNS Server	<input type="text"/>
Alternate DNS Server	<input type="text"/>

6.2 Device Deployment in Network

DICO door phone should be deployed before it can be properly configured in the network environment in terms of their location, operation mode, address, and extension numbers as opposed to other devices for device control and the convenience of the management.

To setup the parameters in the web interface, go to **Network > Advanced > Connect Setting** interface.

Connect Setting

Server Mode	None
Discovery Mode	<input checked="" type="checkbox"/>
Device Address	<input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="1"/>
Device Extension	<input type="text" value="1"/>
Device Location	<input type="text" value="Stair Phone"/>

Parameter set-up:

- **Server Mode:** it is automatically set up according to the actual device connection with a specific server in the network such as **ACMS, Cloud** and **None**. **None** is the default factory setting indicating the device is not in any server type, therefore you are allowed to choose Ekinex Delégo in discovery mode.
- **Discovery Mode:** check *Enabled* to turn on the discovery mode of the device so that it can be discovered by other devices in the network, or check *Disabled* if you want to conceal the device so as not to be discovered by other devices.
- **Device Address:** specify the device address by entering device location information from the left to the right: **Community, Unit, Stair, Floor, Room** in sequence.
- **Device Extension:** enter the device extension number for the device you installed.
- **Device Location:** enter the location in which the device is installed and used.

6.3 NAT Setting

Network Address Translation (NAT) is what is used to map multiple local private addresses to legal public ones before transferring the information. To facilitate data transmission between the door phone and the SIP server, you will need to set up NAT. This can be done in the web interface at the following link: **Account > Advanced > NAT**.

NAT

UDP Keep Alive Messages	<input checked="" type="checkbox"/>	
UDP Alive Messages Interval	<input style="width: 100px;" type="text" value="30"/>	(5-60Sec)
RPort Enabled	<input type="checkbox"/>	

Parameter Set-up:

- **UDP Keep Alive Messages:** if enabled, the device will send out the message to the SIP server so that the SIP server will recognize if the device is in online status.
- **UDP Alive Messages Interval:** set the message sending time interval from 5-60 seconds, the default is 30 seconds.
- **RPort:** enable the RPort when the SIP server is in WAN (Wide AreaNetwork).

7. Intercom Call Configuration

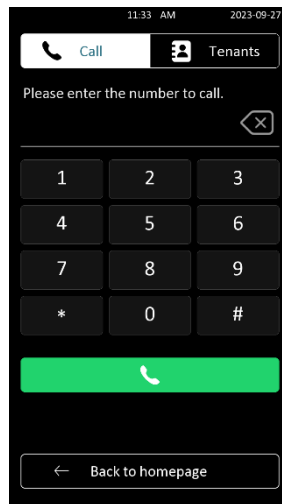
The intercom call in the device can be configured to allow you to perform a variety of customized intercom calls such as IP call and SIP call for different application scenarios.

7.1 IP call and IP Call Configuration

IP calls can be made directly on the intercom device by entering the IP number on the device. And you can also disable the direct IP call if you allow no IP call to be made on the device.

7.1.1 Make IP calls

To make a direct IP call on the device, you can press the **Dial**  icon, then enter the IP or SIP number and press the **Call**  icon to call out.



7.1.2 IP Call Configuration

To configure the IP call on the web interface, go to **Intercom > Basic > Direct IP** interface.

Direct IP	
Enabled	<input checked="" type="checkbox"/>
Port	<input type="text" value="5060"/> (1-65535)

Parameter set-up:

- **Enabled:** to enable/disable the IP direct calls.
- **Direct IP Port:** the direct IP Port is **5060** by default with the port range from **1-65535**. If you enter any values within the range other than 5060, you are required to check if the value entered is consistent with the corresponding value on the device you wish to establish a data transmission with.

7.2 SIP Call and SIP Call Configuration

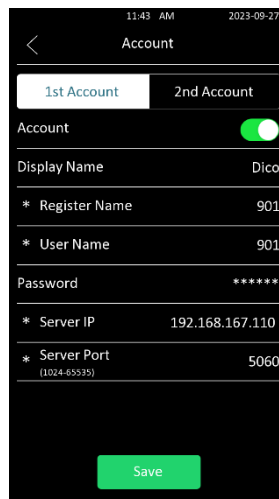
You can make a SIP call (Session Initiation Protocol) in the same way as you do for making the IP calls on the device. However, SIP call parameters related to its account, server, and transport type need to be configured first before you can make calls on the device.

7.2.1.1 SIP Account Registration

DICO device supports two SIP accounts that can all be registered according to your applications. You can, for example, switch between them if any one of the accounts failed and become invalid. The SIP account can be configured on the device and on the web interface.

7.2.1.2 Configure SIP Account on the Device

On the device **Setting** screen, select **Account**.



Parameter set-up:

- **Status:** check to see if the SIP account is registered or not.
- **Display Name:** configure the name, for example, the device's name to be shown on the device being called to.

- **Register Name:** enter the SIP account register Name obtained from the SIP account administrator.
- **Username:** enter the user name obtained from the SIP account administrator.
- **Password:** enter the password obtained from the SIP account administrator.

7.2.2 SIP Server Configuration on the Web interface

SIP servers can be set up for devices in order to achieve call sessions through SIP servers between intercom devices. To set up a SIP server, you can go into the Web interface and select **Account > Basic > Preferred SIP Server**.

Preferred SIP Server			
Server Address	<input type="text"/>		
Sip Server Port	<input type="text" value="5060"/>	(1024-65535)	
Registration Period	<input type="text" value="1800"/>	(30-65535 Sec)	

Alternate SIP Server			
Server Address	<input type="text"/>		
Sip Server Port	<input type="text" value="5060"/>	(1024-65535)	
Registration Period	<input type="text" value="1800"/>	(30-65535 Sec)	

Parameter set-up:

- **Preferred SIP Server:** enter the primary server IP address number or its IP address or domain.
- **Alternate SIP Server:** enter the backup SIP server IP address or domain.
- **SIP Port:** set up a SIP server port for data transmission.
- **Registration Period:** set up SIP account registration time span. SIP re-registration will start automatically if the account registration fails during the registration time span. The default registration period is **1800**, ranging from **30-65535s**.

7.2.3 Configure Outbound Proxy Server on the Web interface

An outbound proxy server is used to receive all initiating request messages and route them to the designated SIP server in order to establish a call session via port-based data transmission. To configure the proxy server, you can go in the Web interface and select **Account > Basic > Outbound Proxy Server**.

Outbound Proxy Server

Outbound Enabled	<input type="checkbox"/>	
Preferred Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024-65535)
Alternate Server IP	<input type="text"/>	
Port	<input type="text" value="5060"/>	(1024-65535)

Parameter set-up:

- **Outbound Enabled:** to enable/disable outbound calls.
- **Preferred Server IP:** enter the SIP address of the outbound proxy server.
- **Port:** enter the Port number for establishing a call session via the outbound proxy server.
- **Alternate Server IP:** set up Backup Server IP for the backup outbound proxy server.
- **Port:** enter the Port number for establishing a call session via the backup outbound proxy server.

7.2.4 Configure Data Transmission Type

SIP messages can be transmitted in four data transmission protocols: **UDP** (User Datagram Protocol), **TCP** (Transmission Control Protocol), **TLS** (Transport Layer Security), and **DNS-SRV**. In the meantime, you can also identify the server from which the data come. To do the configuration, you can go in the web interface and select **Account > Basic > Transport Type**.

Transport Type

Type	<input type="text" value="UDP"/>
------	----------------------------------

Parameter set-up:

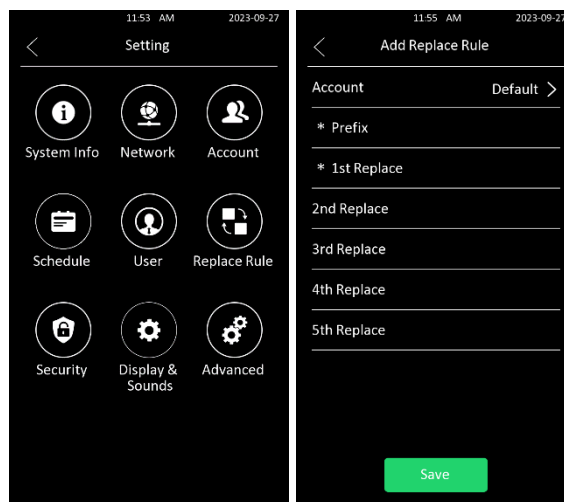
- **UDP**: select **UDP** for unreliable but very efficient transport layer protocol. UDP is the default transport protocol.
- **TCP**: select **TCP** for a reliable but less-efficient transport layer protocol.
- **TLS**: select **TLS** for Secured and Reliable transport layer protocol.
- **DNS-SRV**: select **DNS-SRV** to obtain a DNS record for specifying the location of servers. And **SRV** not only records the server address but also the server port. Moreover, SRV can also be used to configure the priority and the weight of the server address.

7.3 Dial Options Configuration

DICO device offers a variety of Dial options that allows you to have a fast dial experience while relieving you of memory burden due to long and complex dial numbers.

7.3.1 Quick Dial By Number Replacement on the Device

You can replace multiple device dial numbers such as IP addresses or SIP numbers with only one short number. On the device setting screen, select **Replace Rule**, then select **Add**.



Parameter set-up:

- **Account**: select the account to which you want to apply dial number replacement. The account is **Auto** by default (to dial out from the account in which the dialed number has been registered). You can select either account 1 or account 2 from which the number can be dialed out. If you have registered the dialed number in both

Account 1 and Account 2, then the number will be called out from Account 1 by default.

- **Prefix:** enter the short number to replace the dialed number you wish to replace.
- **Replace 1/2/3/4/5:** enter the dialed number(s) you wish to replace. It supports up to 5 numbers maximum for the replacement of the device configuration. For example, if you replace five original dial numbers with a common short number such as **101** then the five intercom devices with the dialed number will be called at the same time when you dial **101**.

7.3.2 Quick Dial by Number Replacement on the Web Interface

You can replace the long SIP/IP number with the short number on the web interface. To configure it, you can go to **Intercom > Dial Plan**.

7.4 Auto-answer Configuration

The auto answer feature allows the door phone to automatically answer the incoming calls, such as, from the resident’s indoor monitor, Smarplus App, and the guard phone. Also, you can select audio or video auto-answer mode based on your need.

To enable Auto-answer mode in the web interface, go to **Account > Advanced > Call**.

To configure Auto-answer function, go to **Intercom > Call Feature > Auto Answer**.

Auto Answer

Auto Answer Delay	<input type="text" value="0"/>	(0-5Sec)
Mode	<input type="text" value="Video"/>	▼

Parameter set-up:

- **Auto Answer Delay:** set up the delay time (**from 0-5 sec.**) before the call can be answered automatically. For example, if you set the delay time as 1 second, then the call will be answered in 1 second automatically.
- **Mode:** set up the **Video** or **Audio** mode you preferred for the automatic call answering.

7.5 Sequence Call Configuration

It is possible to call a targeted group of numbers (e.g. your extension numbers in your kitchen, bedroom, etc.) in sequential order until the call is answered. Sequence call will complete as soon as the call is answered by any of the targeted extension devices.

This feature can be configured in the web interface by going into **Intercom > Basic > Sequence Call**.

Sequence Call

When Refused	<input type="text" value="Do Not Call Next"/>	▼
Call Timeout (Sec)	<input type="text" value="60"/>	▼

Parameter set-up:


- **When Refused:** by selecting **Do Not Call Next**, the call will be stopped as soon as it is refused. By selecting **Call Next**, the call will be transferred to the next one.
- **Call Timeout (Sec):** to check the call time interval in between the sequence call number in a targeted sequence Call group. For example, if you set the time interval as 10 seconds, then the call (if not answered in 10 seconds) will be terminated automatically and be transferred sequentially to the next sequence call number in the targeted sequence call group.

To decide the sequence of calling, in the web interface navigate to **Directory > User > Add or Modify > Contact details**

Directory » User

User

User ID/Name/Code Local ALL

<input type="checkbox"/>	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
 No Data												

Selected: 0/0 Total: 0 1/1 Go To Page

Contact Details

Type

Phone

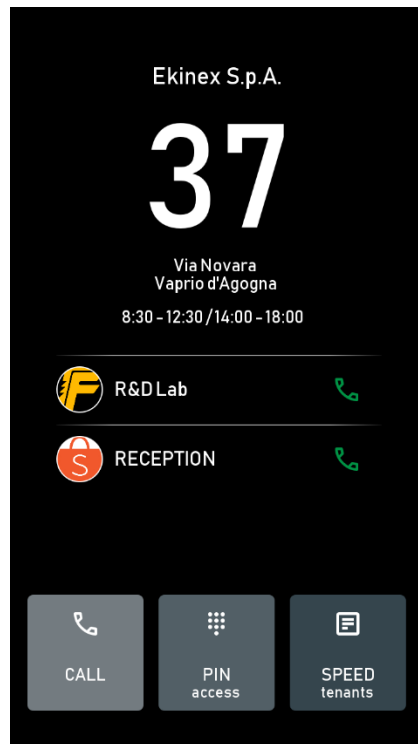
Group

Dial Account

Profile Picture

Parameter set-up:

- **Type:** to insert the contact into the **Tenants** list (therefore with a Group, Call Priority and Call Account), or into the **Speed Dial Tenants** list.
- **Phone:** the number to call;
- **Group:** allows to assign the number to a previously created Group;
- **Priority of call:** it assigns a priority to the call (first, second, last);
- **Dial account:** allows to select the account to dial (automatic, Account 1, Account 2).
- **Profile picture:** to insert a photo of the user. Clicking on Import allows you to select an image file to use as a background. The maximum size allowed is 200 kB, the format can be .jpg, .jpeg, .bmp, .png.



7.6 Enabling Prevent SIP Hacking

You can enable the Prevent SIP Hacking so that the door phone will only receive calls from the SIP numbers registered in the same SIP server, and contacts added locally or synchronized from Ekinex Delégo App.

This feature can be configured in the web interface by going into **Account > Advanced**.

Call

Max Local SIP Port	<input type="text" value="5062"/>	(1024-65535)
Min Local SIP Port	<input type="text" value="5062"/>	(1024-65535)
Auto Answer	<input checked="" type="checkbox"/>	
Prevent SIP Hacking	<input type="checkbox"/>	

Note

The direct IP calls will be blocked if the direct IP is disabled.

7.7 Call Settings

7.7.1 Maximum Call Duration Setting

DICO door phone allows you to set up the call time duration on received calls, as the calling party might forget to hang up the phone. When the call time duration is reached, the door phone will terminate the call automatically.

To personalise the configuration on the web interface, you can go to **Intercom > Call Feature > Max Call Time**.

Max Call Time

Max Call Time	<input type="text" value="5"/>	(2~30Min)
---------------	--------------------------------	-----------

Parameter set-up:

- **Max Call Time:** enter the call time duration as preferred (ranging from 2-30 min.). The default call time duration is 5 min.

Note

- The max call time of the device is also related to the max call time of SIP. If you use a SIP account to dial a call, please pay attention to the max call time of the SIP server. If the max call time of the SIP server is shorter than the max call time of the device, then the SIP server max call time will be applied.

7.7.2 Maximum Dial Duration Setting

Maximum Dial Duration consists of the maximum dial-in time duration and the maximum dial-out time. Maximum dial-in time refers to the maximum time duration before the door phone hangs up the call if the call is not answered by the door phone. On the contrary, maximum dial-out time refers to the maximum time duration before the door phone hangs up itself automatically when the call from the door phone is not answered by the intercom device being called to.

The configuration can be done on the web interface, in **Intercom > Call Feature > Max Dial Time**.

Max Dial Time

Dial In Time	<input type="text" value="60"/>	(5~120Sec)
Dial Out Time	<input type="text" value="60"/>	(5~120Sec)

Parameter set-up:

- **Dial In Time:** enter the dial-in time duration for your door phone (ranging from 5-120 sec). For example, if you set the dial-in time duration as 60 seconds in your door phone, then the door phone will hang up the incoming call automatically if the call is not answered by the door phone in 60 seconds. 60 seconds is the dial-in time duration by default.
- **Dial Out Time:** enter the dial-in time duration for your door phone (ranging from 5-120 sec). For example, if you set the dial-out time duration as 60 seconds in your door phone, then the door phone will hang out the call it dialed out automatically if the call is not answered by the device being called to.

7.7.3 Audio / Video Codec Configuration for SIP Calls

7.7.3.1 Configure Audio Codec

DICO door phone supports four types of Codec (PCMU, PCMA, G729, G722) for encoding and decoding the audio data during the call session. Each type of Codec varies in terms of sound quality. You can select the specific codec with different bandwidths and sample rates flexibly according to the actual network environment.

To configure it on the web interface, you can go to **Account > Advanced > Audio Codecs**.

Audio Codecs

Please refer to the bandwidth consumption and sample rate for the four types of codecs in the table below:

Codec Type	Bandwidth Consumption	Sample Rate
PCMA	64 kbit/s	8kHz
PCMU	64 kbit/s	8kHz
G729	8 kbit/s	8kHz
G722	64 kbit/s	16kHz

7.7.3.2 Configure Video Codec

DICO door phone supports the H.264 codec that provides a better video quality at a much lower bit rate with different video quality and payload. To setup the configuration via the web interface, you can go to **Account > Advanced > Video Codec**.

Video Codec

Name	<input checked="" type="checkbox"/> H264
Resolution	4CIF ▼
Bitrate	320 ▼
Payload	104 ▼

Parameter set-up:

- **Name:** check to select the H264 video codec format for the door phone video. H264 is the video codec by default.
- **Resolution:** select the code resolution for the video quality among five options: **QCIF, CIF, VGA, 4CIF, and 720P** according to your actual network environment. The default code resolution is 720P.
- **Bitrate:** select the video stream bitrate (ranging from 320-2048 bit/s). The greater the bitrate, the data transmitted every second is greater in amount therefore the video will be clearer. While the default code bitrate is 2048 bit/s.
- **Payload:** select the payload type (ranging from 90-118) to configure the video codec. The payload for the door phone and the corresponding intercom device should be identical. The default payload is 104.

7.8 Configure DTMF Data Transmission

In order to achieve door access via DTMF code or some other applications, you are required to properly configure DTMF in order to establish a DTMF-based data transmission between the door phone and other intercom devices for the third-party integration.

To configure the DTMF data transmission via the web interface, you can go to **Account > Advanced > DTMF**.

DTMF	
Mode	RFC2833
How To Notify DTMF	Disabled
Payload	101 (96~127)

Parameter set-up:

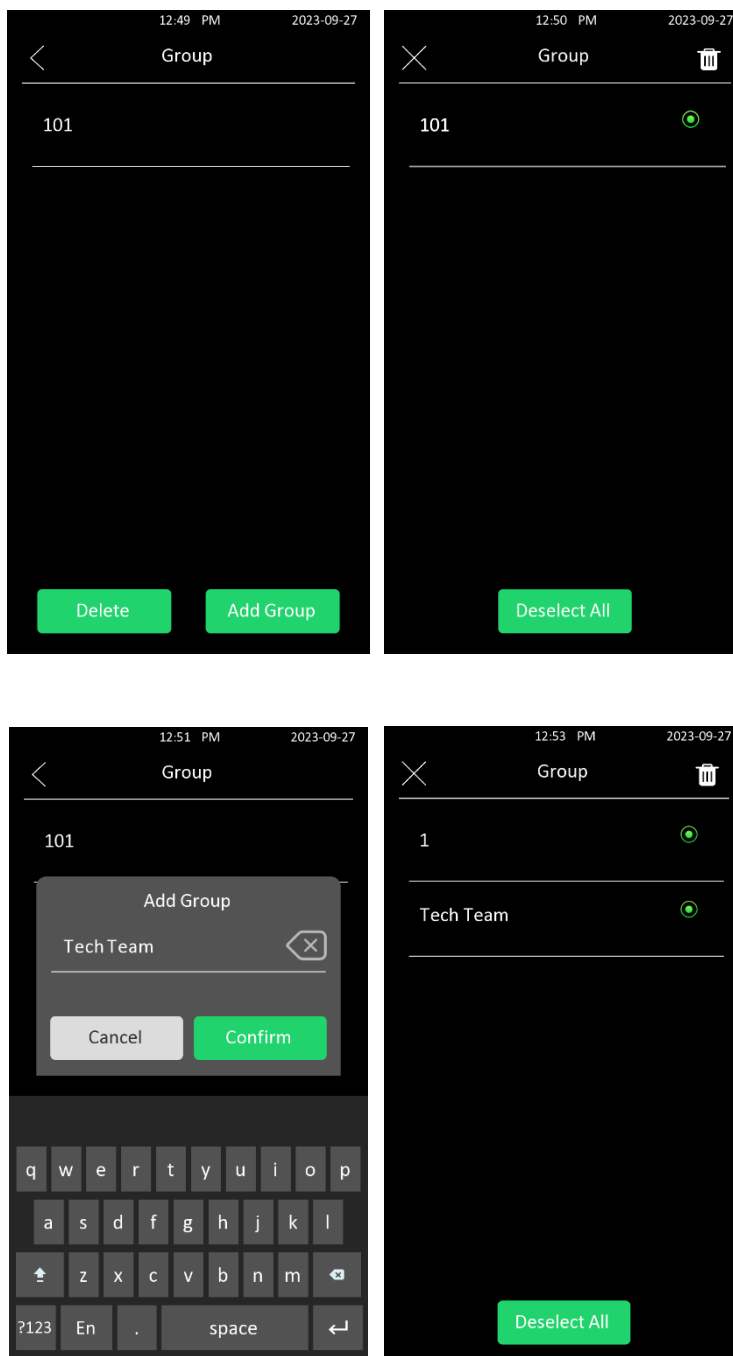
- **Mode:** select DTMF mode among five options: **Inband**, **RFC2833**, **Info+Inband**, **Info+RFC2833** and **Info+Inband+RFC2833** based on the specific DTMF transmission type of the third party device to be matched with as the party for receiving signal data.
- **How to Notify DTMF:** select among four types: **Disable**, **DTMF**, **DTMF-Relay**, and **Telephone-Event** according to the specific type adopted by the third party device. You are required to set it up only when the third-party device mode include an Info option (see the previous parameter).
- **Payload:** set the payload according to the specific data transmission payload agreed on between the sender and receiver during the data transmission.

8. Contact List Configuration

8.1 Contact List Configuration on the Device

DICO allows to configure a contact list in terms of adding and modifying contact groups or contacts on the device directly.

To configure the phone book on the device, enter the **Settings** page and select **User > Group**.



8.2 Contact List Configuration on the Web Interface

8.2.1 Managing users on Web Interface

You can configure individual contacts by adding and editing them on the web interface in **Directory > User > User**

User

User ID/Name/Code														
Local			ALL		Search		Reset		Add		Import		Export	
<input type="checkbox"/>	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit		
<input type="checkbox"/>	1	Local	1	R&D Lab	1111		✘	1111	None	0	1001-1			
<input type="checkbox"/>	2	Local	2	Reception	2222		✘	2222	None	0	1001-1			

Selected: 0/2 Delete Delete All Total: 2 Prev 1/1 Next Go To Page Go

By clicking on “**Add**” button, it is allowed to access the interface to create a new user contact.

In the **Contact Details section**, you can insert the following parameters:

- **Type:** choose between **Tenants** (accessible from the Tenants button on the display) and **Speed Dial Tenants** (the contact will be displayed on the Homepage)
- **Phone:** the contact’s telephone number
- **Profile picture:** to insert a photo of the contact.

Contact Details

Type	<input type="text" value="Speed Dial Tenants"/>
Phone	<input type="text" value="1111"/>
Profile Picture	Import Reset

By selecting *Type = Tenants*, the following parameters are also accessible:

- **Group:** to assign a group to the contact
- **Priority of call:** choose between **Firstly** (the contact will be called first), **Secondary**, or **Lastly**.
- **Dial account:** choose between **Auto**, or an account between **Account1** or **Account2**.

Contact Details

Type	<input type="text" value="Tenants"/>
Phone	<input type="text" value="1111"/>
Group	<input type="text" value="Administration"/>
Priority Of Call	<input type="text" value="Firstly"/>
Dial Account	<input type="text" value="Auto"/>
Profile Picture	<input type="button" value="Import"/> <input type="button" value="Reset"/>

8.2.2 Managing Contact Groups on the Web Interface

You can configure contact and contact groups by adding and editing them on the web interface at **Directory > User > Group**

Group

<input type="checkbox"/>	Index	Name	Edit
<input type="checkbox"/>	1	1	<input type="button" value="Edit"/>

Selected: 0/1 Total: 1 1/1 Go To Page

By clicking on “**Add**”, it is possible to access the interface to create a new group, entering the **Name** and possibly a **Profile Picture** (logo image):

Add Group X

Name

Profile Picture (Max Size: 2...

8.2.3 Managing Contact List Display Setting

If you want to customize your contact list displayed to your desired visual preference, in the web interface you can go to **Directory > Directory Setting > Tenants List Setting**.

Tenants List Setting

Show Local Tenants Enabled	<input type="checkbox"/>
Show Cloud Tenants Enabled	<input type="checkbox"/>
Tenants Sort By	Room No. ▼
Click Tenants To Dial Out	<input checked="" type="checkbox"/>
Contacts Display Mode	Groups Only ▼

Parameter set-up:

- **Show Local Tenants Enabled:** tick or untick the check box to manage the display of the group label. If you untick the check box, then only the group tab will be displayed while the contact tab will be concealed and viceversa.
- **Show Cloud Tenants Enabled:** tick the check box to show the cloud tenants in the tenant's list. And when you untick the check box, the cloud tenants will be hidden.
- **Tenants Sort By:** select among **ASCII Code**, **Room No.** or **Import** options. When you select ASCII Code, the tenants will be listed by their names in the sequence of the ASCII code. When you select Room No., the tenants will be sorted according to their room numbers. This is applicable to the local contacts and contacts synchronized from Ekinex Delégo.
- **Click Tenants to Dial Out:** tick the check box to enable the dial-out by pressing the contact tab. When this function is enabled, you can press anywhere on the contact tab to dial out. This function will be disabled when you untick the check box, and when it is disabled, you need to press the Call icon in the middle of the tab to dial out.
- **Contacts Display Mode:** the options are **Groups Only**, **All Contacts**, or **Group On Entry Page And Their Contacts On Subpage**. If you select **Groups Only**, you can tap the group to call all contacts. The group name is displayed when calling.

9. Relay Switch Setting

9.1 Relay Switch Setting

The relay switch(es) and DTMF for the door access can be configured in the Web interface on **Access Control > Relay > Relay**.

Relay

Trigger Delay(Sec)	<input type="text" value="0"/>
Hold Delay(Sec)	<input type="text" value="5"/>
DTMF Mode	<input type="text" value="1 Digit DTMF"/>
1 Digit DTMF	<input type="text" value="0"/>
2~4 Digits DTMF	<input type="text"/>
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> TFTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/> SIP Call
HTTP URL	<input type="text"/>
Relay Status	<input type="text" value="Low"/>
Relay Name	<input type="text" value="Relay"/>

Parameter set-up:

- **Trigger Delay (sec):** set the relay trigger delay timing (ranging from 1-10 Sec). For example, if you set the delay time as 5 sec, then the relay will not be triggered until 5 seconds after you press the unlock button.
- **Hold Delay (sec):** set the relay hold delay timing (ranging from 1-10 Sec). For example, if you set the hold delay time as 5 sec, then the relay will stay triggered for 5 seconds after the door is It means the door will stay open for 5 seconds.
- **DTMF Mode:** select the number of DTMF digits for the door access control (ranging from 1-4 digits). For example, you can select a 1-digit DTMF code or 2-digit DTMF code, etc., according to your need.
- **1 Digit DTMF:** set the 1-digit DTMF code within range from (0-9 and *, #).
- **2~4 Digits DTMF:** set the DTMF code according to the DMTF Mode selected option. For example, you are required to set the 3-digits DTMF code if DTMP Mode is set as “3 Digit DTMF”.

- **Action to Execute:** an action can be selected after the relay is triggered (FTP, email, SIP call, TFTP or HTTP).
- **HTTP URL:** if “HTTP” is selected as “Action to Execute”, then the URL has to be added in this field.
- **Relay Status:** relay status is low by default which means normally closed (NC). If the relay status is high, then it is in normally open status (NO).
- **Relay Name:** name the relay switch according to your need. For example, you can name the relay switch according to where the relay switch is located for convenience.

Note

- Only the external devices connected to the relay switch need to be powered by powered adapters as the relay switch does not supply power.

Note

- If DTMF mode is set as **1 Digit DTMF**, you cannot edit DTMF code in **2~4 Digits DTMF** and if you set DTMF mode from 2-4 in **2~4 Digits DTMF** field, you cannot edit DTMF code in **1 Digit DTMF** field.

9.2 Web Relay Setting

In addition to the relay that is connected to the door phone, you can also control the door access using the network-based web relay on the device and on the device web interface.

9.2.1 Configure Web Relay on the Web Interface

Web relay needs to be set up on the web interface. It is required to fill in such information as relay IP address, and password. And you can fill in a maximum of 50 web relay action commands for different web relay actions, which can later be selected on the device screen for the specific relay action for the door access control.

These settings are available in the web interface at the following path: **Access Control > Web Relay**.

Web Relay

Type

IP Address

Username

Password

Web Relay Action Setting

Action ID	Web Relay Action	Web Relay Key	Web Relay Extension
1	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>

Parameter set-up:

- **Type:** three options are available, **Disabled**, **Web Relay** and **Local Relay+Web Relay**. Select **Web Relay** to enable the web relay. Select **Disable** to disable the web relay. Select **Local Relay+Web Relay** to enable both local relay and web relay. If you select Web relay, then the local relay will not be valid.
- **IP Address:** enter the web relay IP address provided by the web relay manufacturer.
- **User Name:** enter the User name provided by the web relay manufacturer.
- **Password:** enter the password provided by the web relay manufacturer. The passwords are authenticated via HTTP and you can define the passwords using **http get action**.
- **Web Relay Action:** enter the specific web relay action command provided by the web manufacturer for different actions by the web relay.
- **Web Relay Key:** enter the configured DTMF code, when the door is unlocked via the DTMF code, the action command will be sent to the web relay automatically.
- **Web Relay Extension:** enter the related command extension, where available.

After the web relay is set up, you can select the specific web relay action to be carried out.

You can go to **Directory > User**, then click  , then scroll down to **Access Setting**.

User

User ID/Name/Code Local ALL Search Reset Add Import Export

Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
No Data											

Selected:0/0 Delete Delete All Total:0 Prev 1/1 Next Go To Page 1 Go

Access Setting

Relay Relay A

Security Relay Security Relay A

Floor No.

Web Relay

Schedule

1 item Unselected

1002:Never

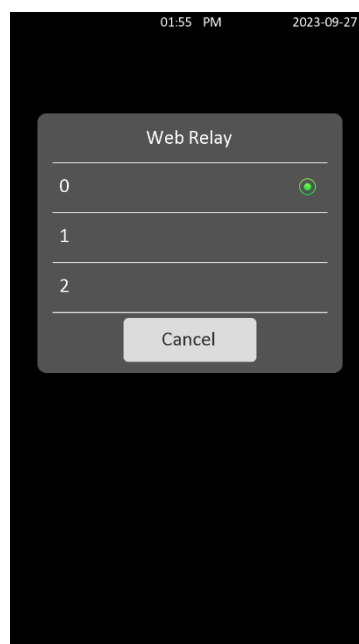
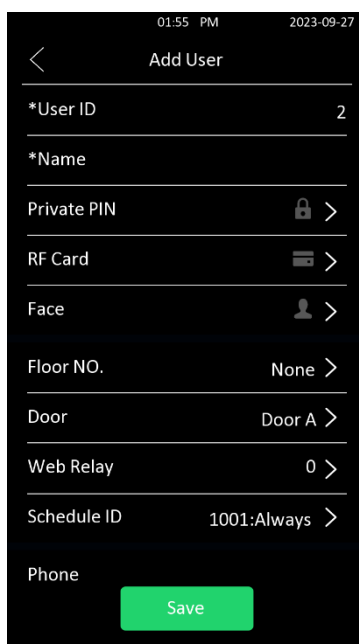
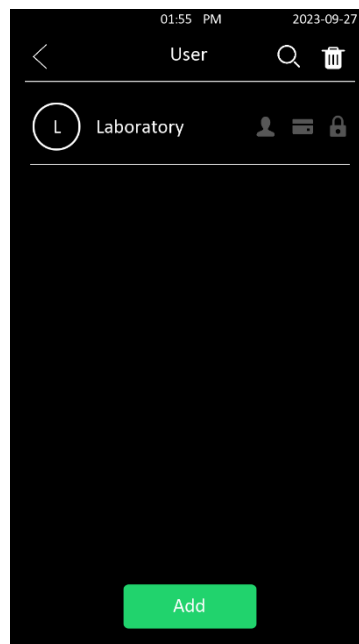
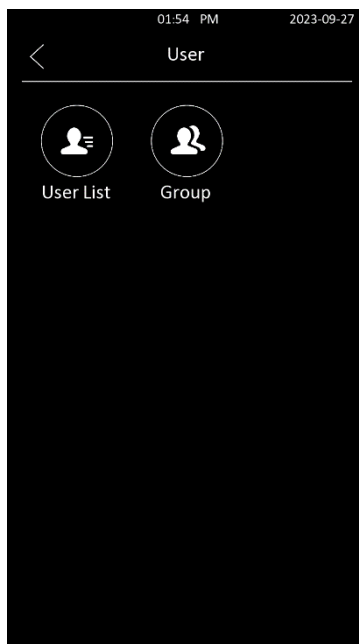
1 item Selected

1001:Always

> <

9.2.2 Configure Web Relay on the Device

After the web relay actions are entered on the web interface, you can now select the specific number of the web relay actions to be carried for the specific resident you added for the door unlock. To configure it, go to the Setting page on the device and select **User > User List**.



9.3 Security Relay

The security relay of the DICO device is connected to the door lock via the DICO door phone itself. It is installed inside the door and serves as extra protection against the forced door unlock through tampering with the door phone. The security relay is applied in applications requiring a higher level of security.

The recommended model is the ekinex **EK-SR1-VI** product, to be connected exclusively to the RS485 port.

To set up the security relay, navigate to **Access Control > Relay > Security Relay** in the web interface

The screenshot shows the 'Security Relay' configuration page. It features several settings:

- Connect Type:** A dropdown menu set to 'RS485'.
- Trigger Delay(Sec):** A dropdown menu set to '0'.
- 1 Digit DTMF:** A dropdown menu set to '2'.
- 2~4 Digits DTMF:** A text input field containing '013'.
- Relay Name:** A text input field containing 'Security Relay A'.
- Enabled:** A checkbox that is currently unchecked.
- Test:** A button with a speaker icon and the text 'Test'.

Parameter set-up:

- **Trigger Delay (sec):** sets the relay trigger delay timing (ranging from 1-10 sec.) For example, if you set the delay time as 5 sec. then the relay will not be triggered until 5 seconds after you press Unlock key. The default is 0 meaning triggering relay right after you press the unlock tab.
- **Hold Delay (sec):** sets the relay hold delay timing (ranging from 1-60 sec.)
- **1 Digit DTMF:** set the 1 digit DTMF code within range from (0-9 and *,#).
- **2~4 Digits DTMF:** set the DTMF code according to the DMTP Option setting. For example, you are required to set the 3-digit DTMF code if DTMP Mode is set as 3- digits.
- **Relay Name:** give a name to the relay if needed. And relay name can be edited on the Ekinex Delégo App.
- **Enable:** this checkbox allows to enable/disable the security relay.
- **Test:** press the button to test the security relay.

9.4 Relay Schedule

It sets the corresponding relay always open at a specific time. This feature is designed for some specific scenarios, such as, the time after school, or morning work time. To configure this feature, navigate to **Access Control > Relay > Relay Schedule** in the web interface.

Relay Schedule

Relay ID

RelayA ▼

Schedule Enabled

2 items Unselected

- 1001:Always
- 1002:Never

>

<

0 item Selected

No Data

Parameter set-up:

- **Relay ID:** choose the relay you need to set up.
- **Schedule Enabled:** it is disabled by default. If enabled, the schedule setting becomes available. For creating the schedule, please refer to the door access schedule configuration (par. 10.1)

Note

- You can refer to **Create Door Access Schedule details** for the relay schedule setting.


10. Door Access Schedule Management

You are required to configure and make a schedule for the user-based door access via RF card, private PIN, and facial recognition.




10.1 Configure Door Access Schedule



You can create door access schedules so that they can be later conveniently applied to the door access control intended for the individual user or a group of users created. Moreover, you can edit your door access schedule if needed.




10.1.1 Create Door Access Schedule on the Web interface

You can create the door access schedule on a daily or monthly basis, and you can also create a schedule that allows you to plan for a longer period of time in addition to running the door access schedule on a daily or monthly basis. To configure the schedule in the web interface, go to **Setting > Schedule**, then click  .

Schedule

Local   

<input type="checkbox"/>	Index	Schedule ID	Source	Mode	Name	Date	Day Of Week	Time	Edit
<input type="checkbox"/>	1	1001	Local	Daily	Always			00:00-23:59	
<input type="checkbox"/>	2	1002	Local	Daily	Never			00:00-00:00	

Selected:0/2  Delete  Delete All Total:2 Prev 1/1 Next Go To Page 

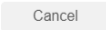
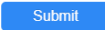
To create a daily schedule, select **Daily** mode.

Add Schedule x

Name

Mode

Date Time -

Parameter set-up:

- **Name:** enter the daily schedule name.
- **Mode:** select daily schedule.
- **Date Time:** set up the time schedule for the validity of the door access during the day.

To create a weekly schedule, select **Weekly** mode.

Add Schedule

Name

Mode Weekly ▾

Day Of Week

<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday
<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input checked="" type="checkbox"/> Saturday
<input checked="" type="checkbox"/> Sunday	<input type="checkbox"/> Check All	

Date Time 00:00 ⌚ - 23:59 ⌚

Cancel
Submit

Parameter set-up:

- **Day of Week:** select the day(s) on which door access can be valid in a week.
- **Date Time:** set up the time schedule for the validity of the door access during the day.

To create a longer period schedule, select Mode = **Normal**:

Add Schedule ✕

Name

Mode Normal ▾

Date Range 2023-07-11 📅 - 2023-07-12 📅

Day Of Week

<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday
<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input checked="" type="checkbox"/> Saturday
<input checked="" type="checkbox"/> Sunday	<input type="checkbox"/> Check All	

Date Time 00:00 ⌚ - 23:59 ⌚

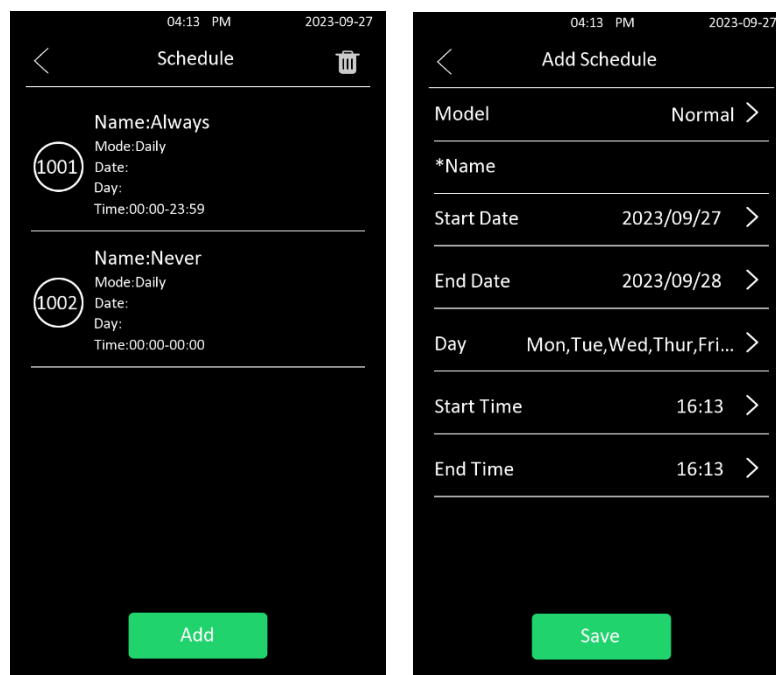
Cancel
Submit

Parameter Set-up:

- **Date Range:** set the date range of the validity of the door access (start date – end date).

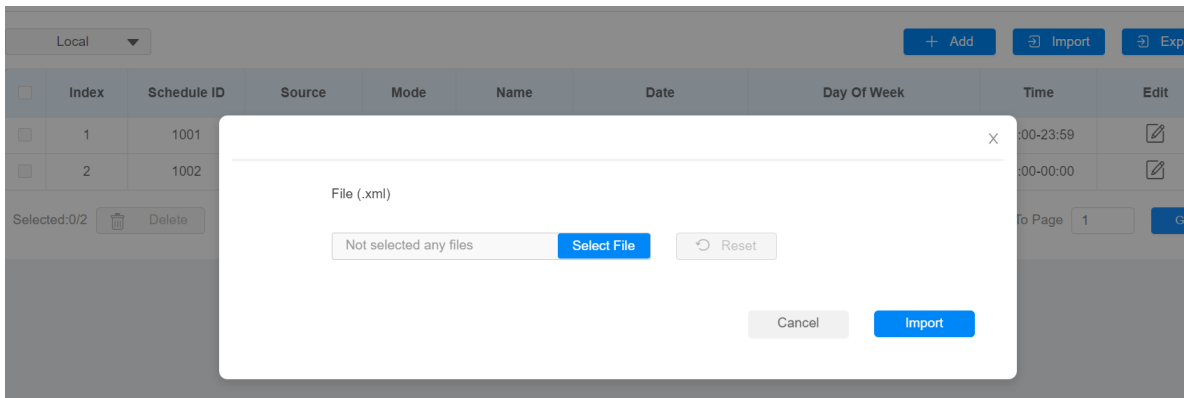
10.1.2 Create Door Access Schedule on the Device

You can also create a door access schedule on the device. It is necessary to open the Setting page, then go to **Schedule > Add**



10.1.3 Import and Export Door Access Schedule in the Web interface

In addition to creating door access schedule separately, you can also conveniently import or export the schedules in order to maximize your door access schedules management efficiency. In the Web interface, it is necessary to go to **Setting > Schedule**, then click **Import**.



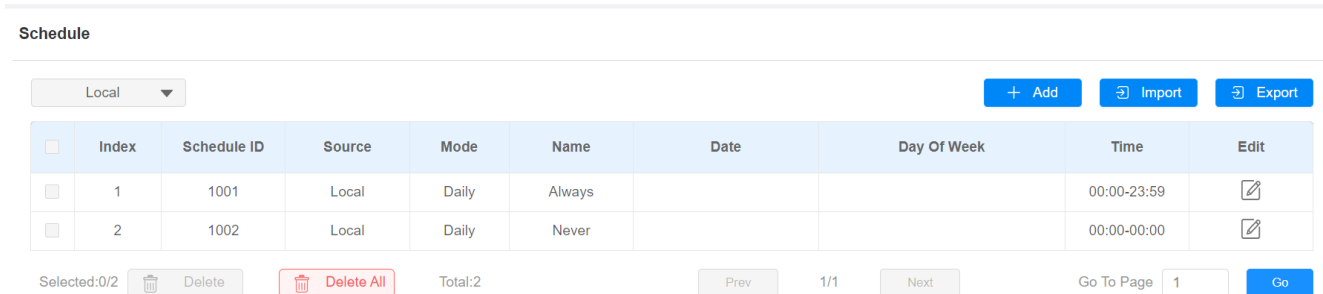
Note

- .xml format files only are supported for importing and exporting the schedule.

10.1.4 Edit the Door Access Schedule

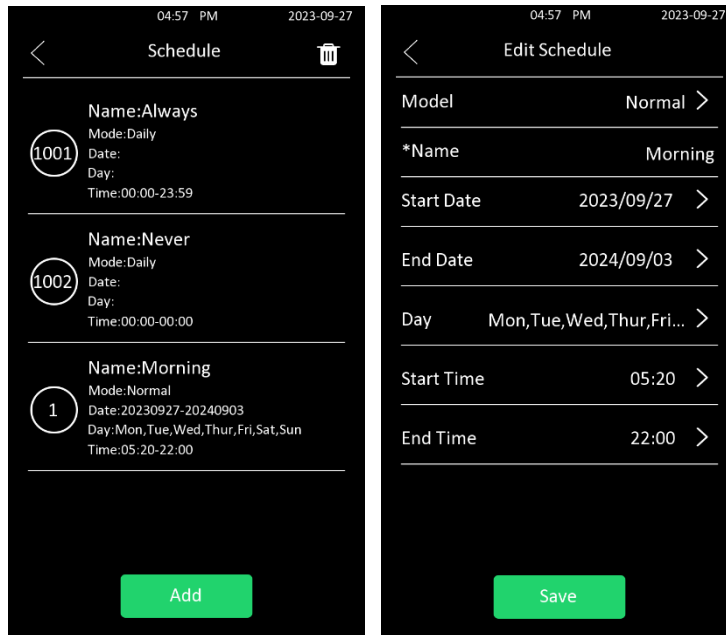
If you want to edit or delete the door access schedule you created, you can edit or delete the configured schedule separately or in batch.

To edit the schedule on the web interface, go to **Setting > Schedule**.



Multiple deletion is allowed by checking the box next to the Index and clicking on “Delete”.

To edit the schedule on the device, click **Schedule** in the Setting page, then choose the schedule you want to edit.



11. Door Unlock Configuration

DICO door phone offers three types of door access: via PIN code, RF card, and facial recognition.

This feature can be configured both on the device and web interface. Moreover, it is allowed to import or export the configured files to maximize the RF card configuration efficiency.

11.1 Access Authentication

It is possible to setup several access authentication modes and set up authentication security as needed. On the web interface, navigate to **Access Control > Relay > Access Authentication Mode**.

Access Authentication Mode

Authentication Mode	<input type="text" value=""/>
Entry Restriction	<input type="checkbox"/>

Parameter set-up:

- **Authentication Mode:** for this parameter, four options are allowed
 1. **Any method** if you allow all the access methods to unlock the door.
 2. **Face + PIN** if you want to apply dual access methods (Face + PIN) for the door unlock.
 3. **Face + RF Card** if both Face and RF Card are possible for the door unlock.
 4. **RF Card + PIN** to allow dual access methods (RF Card + PIN) for the door unlock.
- **Entry Restriction:** enable it to set the time interval of unlocking the door.

11.2 Configure PIN Code for Door Unlock

DICO door phone allows to create and modify both public PIN codes and private PIN codes for door access.

11.2.1 Configure Public PIN code

This options allows to configure and change public PIN codes.

On the web interface, go to **Access Control > PIN Setting > Public PIN**.

Public PIN

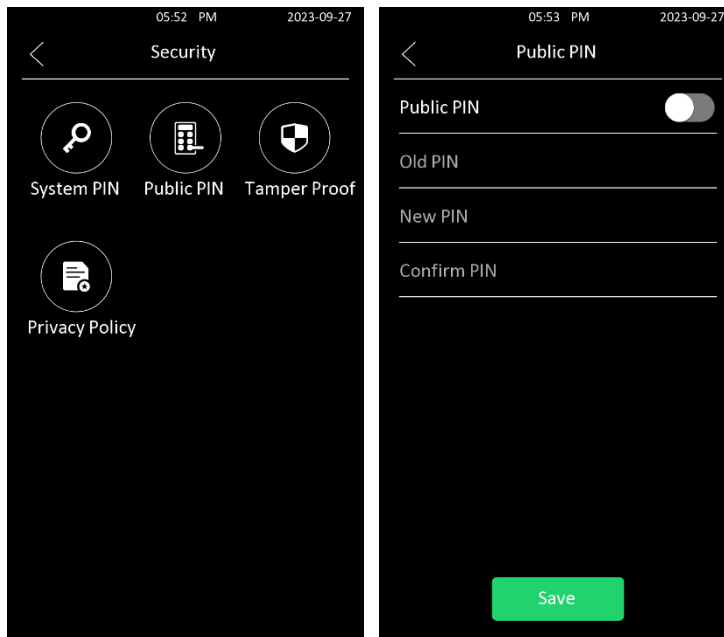
Enabled

PIN Code

Parameter set-up:

- **Enabled:** it allows to enable/disable the Public PIN code management.
- **PIN Code:** set the PIN code with a digit limit ranging from 4 to 8.

To configure it on the device, enter the Setting page and select **Security > Public PIN**



Note

- The public PIN code will not be valid until the function is turned on.

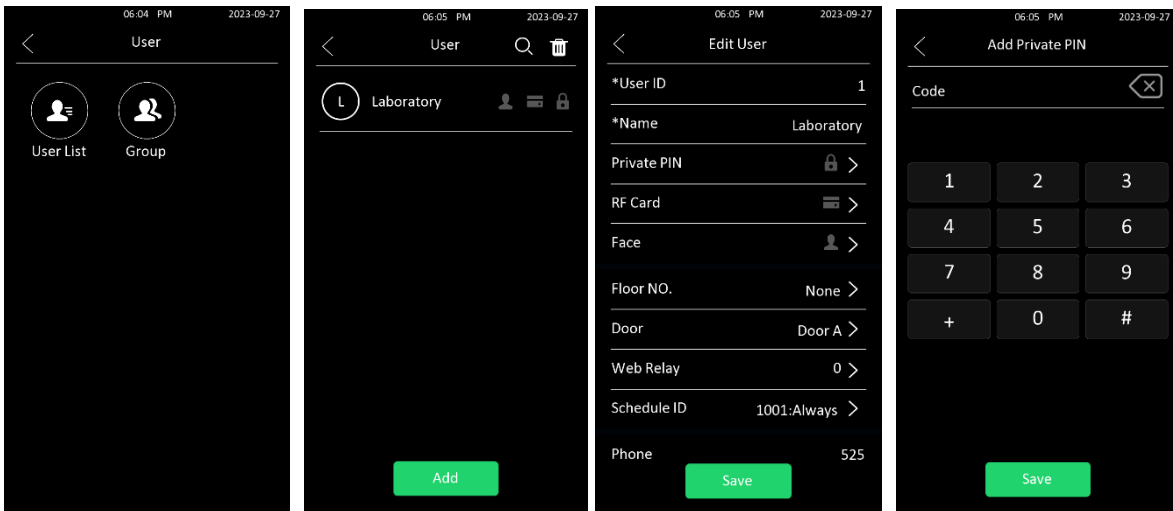
Note

- **APT+PIN** is applicable only when the device is added to the Ekinex Delégo App.

11.2.2 Configure Private PIN code on the Device

You can configure door access via Private PIN code for the resident on the device by entering the user’s name and the PIN code for the door access.

On the device, select Settings and then **User > User List**. By clicking on any user, it is possible to add or edit a Private PIN.



11.2.3 Configure Private PIN code on the Web Interface

On the web interface, you can not only set up a PIN code but also set and select the door access schedule that you created for the validity of the PIN Code access during a certain time span you scheduled. In addition, you can set the limit for the total number of valid PIN code door access.

To configure the PIN code, go to **Directory > User** in the web interface.

User

User ID/Name/Code Local ALL Search Reset Add Import Export

Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
1	Local	1	Laboratory			⊗	525	None	0	1001-1	

Selected 0/1 Delete Delete All Total: 1 Prev 1/1 Next Go To Page 1 Go

Then, press **Edit** symbol for a specific user

User Info

User ID	1
Name	

PIN

Code	
------	--

After user information and PIN code are entered, you can scroll down to **Access Setting** on the same page to set door access schedule with Private PIN code:

Access Setting

Relay	<input checked="" type="checkbox"/> Relay A			
Security Relay	<input type="checkbox"/> Security Relay A			
Floor No.	<input type="text" value="None x"/>			
Web Relay	<input type="text" value="0"/>			
Schedule	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; border: 1px solid #ccc; padding: 5px;"> <div style="text-align: right; font-size: small;">1 item Unselected</div> <input type="checkbox"/> 1002:Never </td> <td style="width: 10%; text-align: center; vertical-align: middle;"> <input type="button" value=">"/> <input type="button" value="<"/> </td> <td style="width: 40%; border: 1px solid #ccc; padding: 5px;"> <div style="text-align: right; font-size: small;">1 item Selected</div> <input type="checkbox"/> 1001:Always </td> </tr> </table>	<div style="text-align: right; font-size: small;">1 item Unselected</div> <input type="checkbox"/> 1002:Never	<input type="button" value=">"/> <input type="button" value="<"/>	<div style="text-align: right; font-size: small;">1 item Selected</div> <input type="checkbox"/> 1001:Always
<div style="text-align: right; font-size: small;">1 item Unselected</div> <input type="checkbox"/> 1002:Never	<input type="button" value=">"/> <input type="button" value="<"/>	<div style="text-align: right; font-size: small;">1 item Selected</div> <input type="checkbox"/> 1001:Always		

Parameter set-up:

- **Relay:** select the relay for the door unlock for the user.
- **Security relay:** it allows to enable the relay for security purposes.
- **Floor No.:** enter the resident's floor number.
- **Web relay:** select the specific number of web relay action commands you have set up on the web interface.
- **Schedule:** select one or more door access schedules previously created and displayed in the left box and move those to be applied to door access with a user-specific private PIN code to the right box.

Note

- This step is also applicable to door access by RF card and facial recognition as they are identical in configuration.

11.2.4 Configure Private PIN Access Mode

DICO device offers two types of access modes for private PIN code access, namely **PIN** and **APT#+PIN**.

On Web interface, go to **Access Control > PIN Setting > Private PIN** to enable/disable Private PIN.

The screenshot shows the 'Private PIN' configuration page. At the top, there is a breadcrumb trail: 'Access Control >> PIN Setting'. Below this, the page title is 'Private PIN'. There are two main settings: 'Enabled' with a checked checkbox, and 'Authorization Mode' with a dropdown menu currently set to 'PIN'.

Parameter Set-up:

- **Authorization Mode:** select access mode between **PIN** and **APT#+PIN**. If you select the **PIN**, then you are only required to enter the PIN code directly for the door access, while if you select **APT#+PIN**, then you are required to enter the Apartment Number first before entering your PIN code for the door access.


11.3 Configure RF Card for Door Unlock

11.3.1 Add RF Card on the Web Interface

To add RF cards, on the Web interface go to **Directory > User**, then click [+ Add](#).

User

User ID/Name/Code Local ALL

<input type="checkbox"/>	Index	Source	User ID	Name	PIN	RF Card	Face	Phone	Floor No.	Web Relay	Schedule-Relay	Edit
 No Data												

Selected: 0/0 Total: 0 1/1 Go To Page

Then scroll the page to **RF Card** tab.

RF Card

Code **+ Obtain**

Add

Then press **+ Obtain** button and hold the RF card close to the DICO device reader for about 5 seconds, so that the card is recognized and associated with the selected user.

Note

- Please refer to PIN code access schedule selection for the RF card user(s)-specific door access.

Note

- For door access, the video intercom considers 13.56 MHz and 125 kHz RF cards

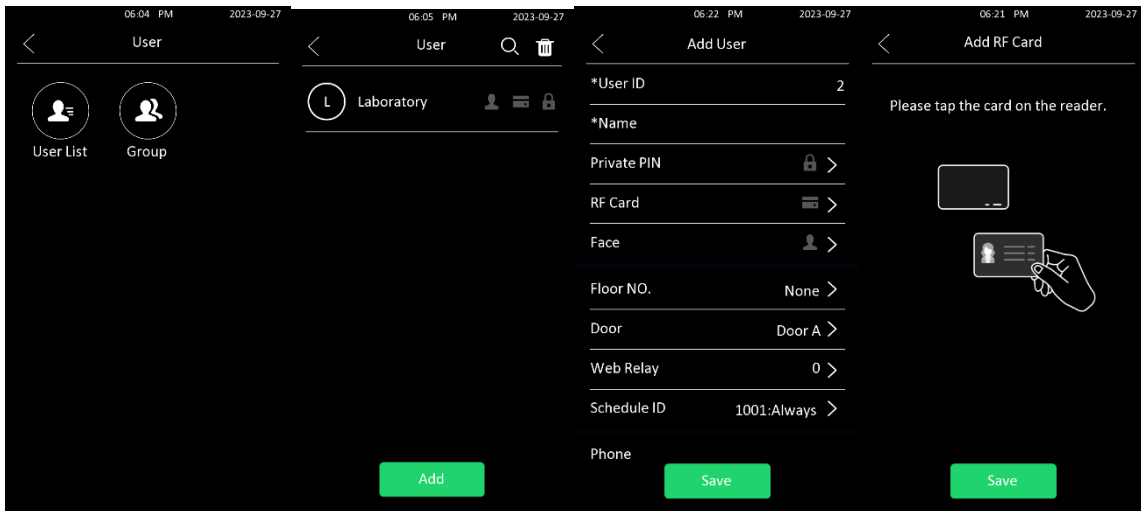
11.3.2 Add RF Card from Device Setting

It is possible to configure the RF card for door access directly from the device, while setting the other access modes (PIN, facial recognition, Web relay, etc.) or the time programming for access for a specific user.

To add an RF card, tap **User**, then **User List**, then **Add**.

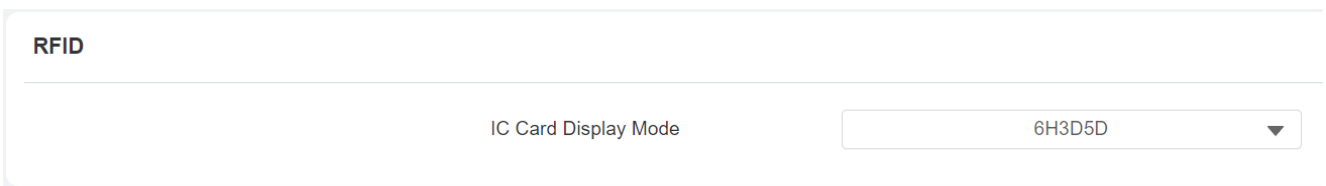
To add an RF card, from the **Settings** page tap **User**, then **User List** and then tap **+ Add** to create a new user, or edit an already registered user.

Finally, tap on **RF Card** entry:



11.3.3 Configure RF Card Code Format

If you want to integrate with a third-party intercom system in terms of RF card door access, it is possible to change the RF card code format. In this way, this can be identical to the one applied in the third-party system. To configure the configuration on the web interface please go to **Access Control > Card setting**.



Parameter set-up:

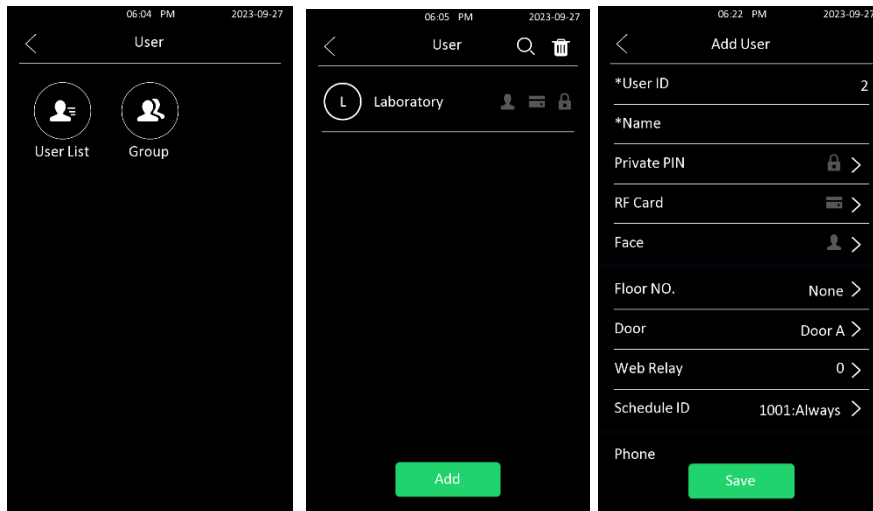
- **IC Card Display Mode:** select the card format for the **IC Card** for the door access among six format options: **8H10D, 6H3D5D(W26), 6H8D, 8HN, 8HR, 8HR10D**. The card code format is 8HN by default in the door phone.

11.4 Configure Facial Recognition for Door Unlock

11.4.1 Enroll Face Data on the Device

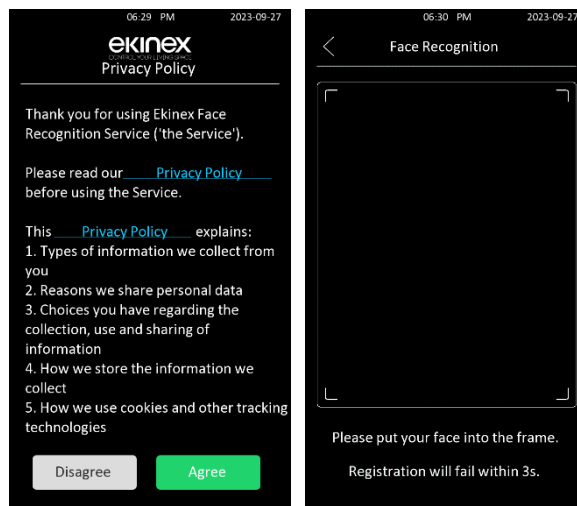
You can configure door access by facial recognition on the device by entering the user's name and registering the facial ID on the device for door access.

On the device, access the Setting page and then tap **User > User List**, then tap **Add**, and **Face**.





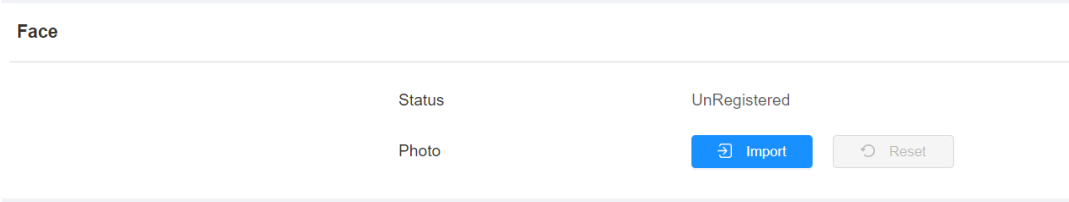
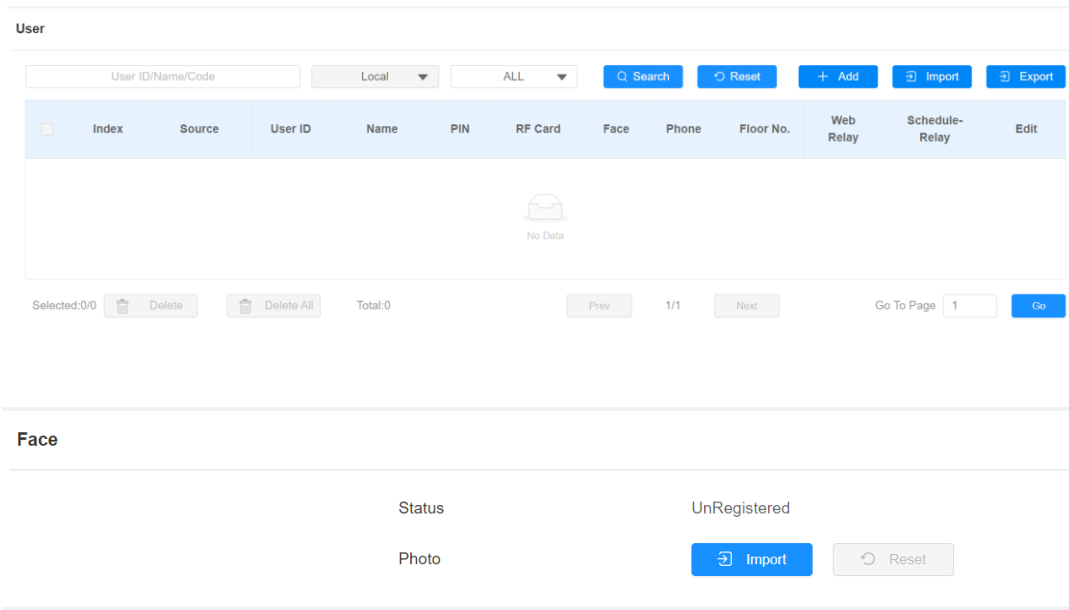
Then the device prompts you a page, where it is possible to accept the Privacy Policy by clicking on “Agree” button.


Finally, the camera will proceed with the face recognition in about 10 seconds.



11.4.2 Upload Face Data on the Web Interface

The user can upload the face data to the device via the web interface. To do so, go to **Directory > User**, then click  or **Edit**  symbol for an already registered user.



After that, upload the face photo by using the  **Import** button.

Parameter set-up:

- **Status:** this field will show **Registered** when the picture uploaded is compliant to the format and standard required. Otherwise it would show **Unregistered** as default. However, the status will be changed back to **Unregistered** if the picture uploaded is cleared when you press the **Reset** button.
- **Photo (jpg/png):** click on **Import** button to select the picture and upload it to the device. By clicking on reset, the picture is deleted from the device.

Note

- Pictures to be uploaded should be in **.jpg** or **.png** format.

11.4.3 Configure Facial Recognition

DICO door phone allows to adjust facial recognition accuracy and recognition intervals according to the user request. It is also possible to improve the recognition quality and user experience through the basic facial recognition setting.

To setup the configuration on the web interface, go to **Access Control > Face Setting** page.

Face Basic

Facial Recognition Enabled	<input checked="" type="checkbox"/>
Offline Learning Enabled	<input checked="" type="checkbox"/>
Facial Recognition Matching Level	<input type="text" value="Normal"/>
Face Living Recognition Matching Level	<input type="text" value="Close"/>
Facial Recognition Interval (sec)	<input type="text" value="18"/>
No Face Detected Interval (sec)	<input type="text" value="23"/>
Face Detection Distance (M)	<input type="text" value="0"/>

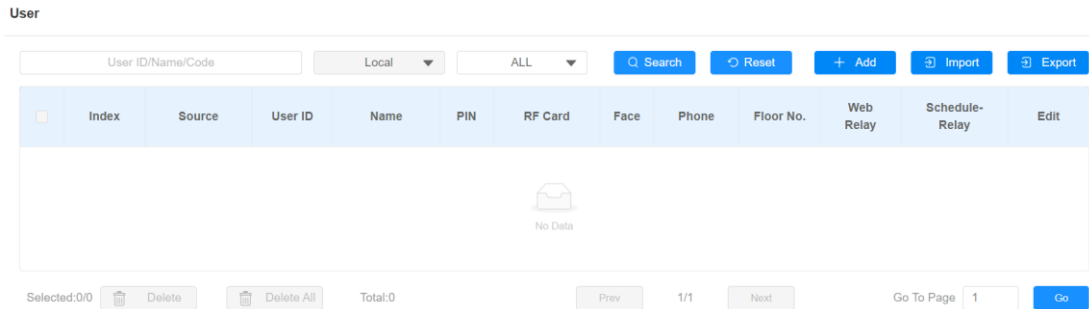
Parameter set-up:

- **Facial Recognition Enabled:** it allows to enable/disable the feature.
- **Offline Learning Enabled:** select **Enable** if you want to improve the device recognizing capability, focusing on the major facial characteristics while sidelining the minor changes that occurred to the face. Facial recognition accuracy improves as the number of successful facial recognitions increases.
- **Facial Recognition Matching Level:** click to select the facial recognition accuracy level among four options: **Low**, **Normal**, **High**, and **Highest**. For example, if you select **Highest**, there will be the least possibility that someone else will be mistaken for you during the facial recognition process.
- **Face Living Recognition Matching Level:** select Anti-spoofing level among five options: **Close**, **Low**, **Normal**, **High**, **Highest**. For example, if you select **Highest** then there will be the least possibility that the device will be fooled by digital images or pictures of any kind.
- **Facial Recognition Interval (sec):** select the time interval between two facial recognitions in a 1-8 minutes timespan. For example, if you select **5** then you have to wait for 5 min. before you are allowed to perform another facial recognition again.
- **No Face Detected Interval (sec):** it sets the maximum amount of time to wait if no face is detected (range 1-8 secs).
- **Face Occlusion Rejection:** if **Enabled**, allows to abort the face recognition in case an image is partially captured or is not fully visible due to overlapping objects, clothing, and body parts.
- **Face Detection Distance (m):** sets the distance for the face recognition. Possible values are 1,2,3 m.

11.5 Configure Door Access Using Configured Files

DICO door phone allows the user to quickly configure user(s)-specific door access in a massive way, by importing the configured all-in-one door access control files incorporating user information, door access type, door access schedule, etc. Thus all the door access settings can be done in a single step, saving time and effort with respect to configure the door access for users separately, especially when users are large in number.

In order to perform this process, the user can access the web interface and the move to **Directory > User**.



In this page, click on **Import** button and upload an archive file with the users information. Allowed formats for such file are .tgz and .zip.

Note

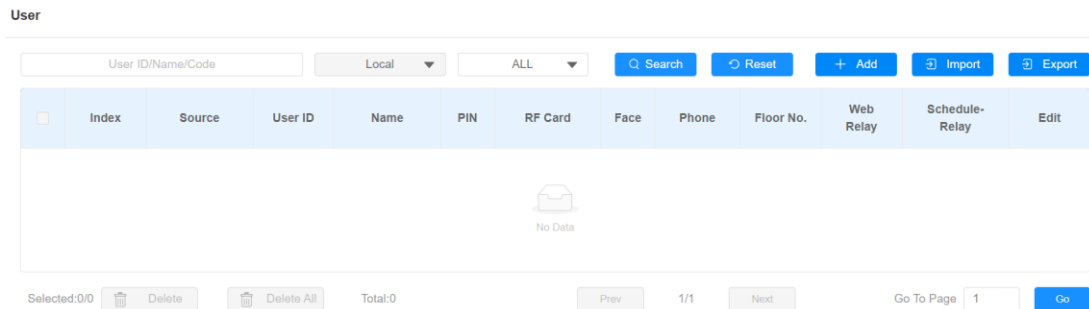
- Configured files for facial recognition and the other types of configured door access files are separated with different file forms.

11.5.1 Editing the User(s)-specific Door Access Data

User-specific port access data can be searched and door access data modified from the web interface.

It is necessary to open the **Directory > User** page and click on

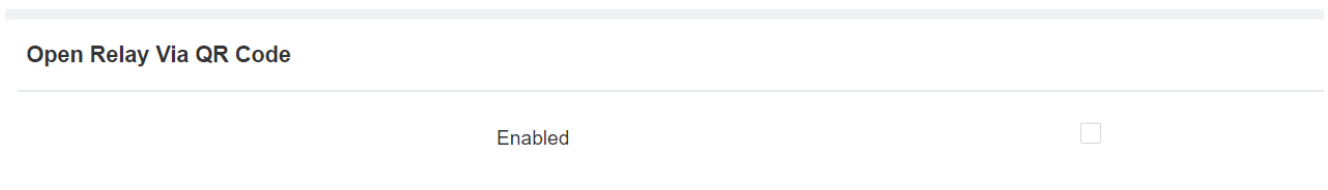
- **Search**, providing a UserID, name or code in the upper left field;
- **Edit**, by clicking on the icon at the end of an entry.



11.6 Unlock by QR Code

QR code is another option for door unlock.

To use it, it is necessary to enable the QR code function from the web interface by clicking on **Access Control > Relay > Open Relay via QR Code**.



Note

- The function should work with Ekinex Delégo App.

11.7 Unlock by Bluetooth

The user can also gain the door access by mobile phone with Bluetooth function.

The function is activated by moving the smartphone near the access control terminal and allows access to the door. To configure it on web interface, please enable the feature in the **Access Control > BLE > BLE** webpage.

BLE

Enabled	<input type="checkbox"/>
RSSI Threshold	<input type="text" value="0"/> (-85~-50db)
Open Door Interval(Sec)	<input type="text" value="0"/> ▼

Parameter set-up:

- **RSSI Threshold:** it selects the signal receiving strength in the -85~-50db interval. The higher value is, the greater strength it has. The default value is 72db.
- **Open Door Interval (sec):** it selects the time interval between two door accesses via Bluetooth.

11.8 Unlock by NFC

You can also gain door access by mobile phone with NFC which is used with Ekinex Delégo App. It is enough to keep the mobile phone close to the door phone for door access.

To enable the feature via the web interface, go to **Access Control > Card Setting > NFC**.

NFC

Enabled

11.9 Unlock by HTTP Command on Web Browser

It is possible to unlock the door remotely without approaching the DICO device physically

In this case, the user can type the created HTTP command (URL) on a web browser, in order to trigger the relay when he's not available by the door for the door access.

To setup the configuration on web interface, please go to **Access Control > Relay > Open Relay via HTTP**.

Open Relay Via HTTP

Enabled	<input type="checkbox"/>
Username	<input type="text" value="0"/>
Password	<input type="password" value="*****"/>

Parameter set-up:

- **Enabled:** to enable/disable the door unlock via http request
- **Username:** enter the user name of the device web interface, for example, **admin**.
- **Password:** enter the password for the HTTP command. For example, **12345**.

Please refer to the following example, with the parameters set as above:

http://YOUR_DEVICE_IP/fcgi/do?action=OpenDoor&UserName=admin&Password=12345&DoorNum=1

Note

- **DoorNum** in the HTTP command above refers to the relay number #1 to be triggered for the door access.

11.10 Unlock by Exit Button by the Door

When the user needs to open the door from inside a building using the exit button installed on the door, it is possible to configure the **Input** function of the DICO video intercom to trigger the relay for the door access.

To setup such configuration on web interface, please go to **Access Control > Input > Input**.

Input

Enabled	<input type="checkbox"/>
Trigger Electrical Level	<input type="text" value=""/>
Action To Execute	<input type="checkbox"/> FTP <input type="checkbox"/> TFTP <input type="checkbox"/> Email <input type="checkbox"/> HTTP <input type="checkbox"/> SIP Call
HTTP URL	<input type="text" value=""/>
Action Delay	<input type="text" value="0"/> (0~300Sec)
Action Delay Mode	<input type="text" value="Unconditional Execution"/>
Execute Relay	<input type="text" value=""/>
Door Status	High

Parameter set-up:

- **Enabled:** it allows to enable/disable the feature.
- **Trigger Electrical Level:** select the trigger electrical level options between **High** and **Low** according to the desired operation on the exit button.
- **Action to Execute:** select the method to carry out the action among five options: **FTP, Email, SIP Call, HTTP** and **TFTP**.
- **HTTP URL:** enter the URL if you select the http mode to carry out the action.
- **Action Delay:** set up the delay time when the action is carried out, in a range 0-300 seconds. For example, if you set the action delay time at 5 seconds, then the corresponding actions will be carried out 5 seconds after you press the button (input is triggered).
- **Action Delay Mode:** if you select **Unconditional Execution**, then action will be carried out when the input is triggered. If you select **Execute If Input Still Triggered**, then the action will be carried out if the input stays triggered. For example, if the door stays open after triggering input, an action such as an email will be sent to notify the receiver.
- **Execute Relay:** set up relays to be triggered by the input.

11.11 Unlock by Reception Tab

On the device's home screen, the DICO door phone provides residents and visitors quick door access by pressing the **Reception** tab at the bottom of the home screen.

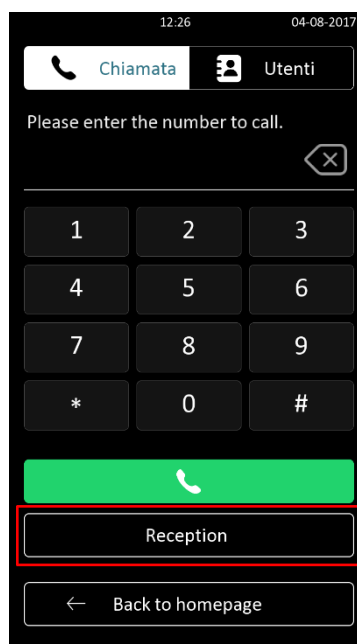
To setup the configuration, please access the web interface and go to **Intercom > Basic > Key Setting**.

Key Setting

Reception Enabled	<input type="checkbox"/>
Name	<input type="text" value="0"/>
Number	<input type="text" value="3"/>

Parameter set-up:

- **Reception Enabled:** it allows to enable/disable the Reception tab.
- **Name:** enter the name for the **Reception** icon on the home screen.
- **Number:** enter the SIP/IP number to be called after pressing the **Reception** icon for the door access.



11.12 Unlock by DTMF Code

DTMF codes can be configured on the intercom web interface. By setting identical DTMF codes on intercom devices connected to the same network (e.g., an indoor monitor), you can allow users to enter the DTMF code on the virtual keypad or press the attached DTMF code to unlock the door for visitors, etc., during a call.

To enable the extra DTMF configuration on the web interface, you can go to the web interface at **Account > Advanced > DTMF**.

DTMF

Mode	<input type="text" value="RFC2833"/>
How To Notify DTMF	<input type="text" value="Disabled"/>
Payload	<input type="text" value="101"/> (96-127)

Parameter set-up:

- **Type:** select DTMF type among six options: **Info**, **Inband**, **RFC2833**, **Info+Inband**, **Info+RFC2833** and **Info+Inband+RFC2833** as desired.
- **How to Notify DTMF:** this option is enabled only if Type option includes **Info** and it allows to select among four values: **Disable**, **DTMF**, **DTMF-Relay**, and **Telephone-Event** as desired.
- **DTMF Payload:** select the payload in the 96-127 range for data transmission identification. Default value is 101.

Note

- Please refer to the chapter *7.8 - Configure DTMF Data Transmission* for the specific DTMF code setting.
- Intercom devices involved must be consistent in the DTMF type otherwise DTMF code cannot be applied.

11.12.1 Configure DTMF White List

In order to secure the door access via DTMF codes, you can set up the DTMF whitelist on the web interface at **Access Control > Relay > Open Relay Via DTMF** so that only the caller numbers designated in the door phone can use the DTMF code to gain door access.

Open Relay Via DTMF

Assigned The Authority For	<input type="text" value="Only Tenants List"/>
----------------------------	--

The options are: **Only Tenants List** (default), **none** and **All numbers**.

12. Security

12.1 Tamper Alarm Setting

The tamper alarm function serves as a protection against any unauthorized removal of the device by triggering off the tamper alarm on the device. To setup the configuration on web interface, please go to **System > Security > Tamper Alarm** interface.

Tamper Alarm			
Enabled	<input checked="" type="checkbox"/>		Disarm
Key Status		High	

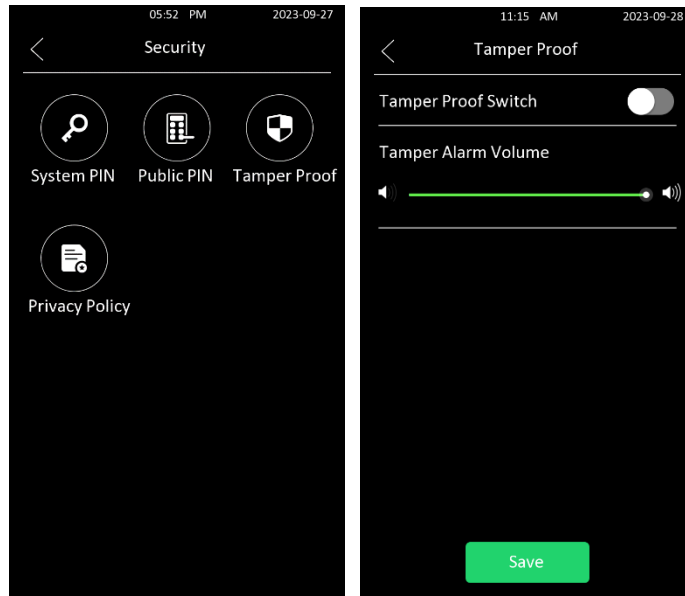
Parameter set-up:

- **Enable:** tick the check box to enable the tamper alarm function. When the tamper alarm goes off, you can press the **Disarm** tab beside the check box to clear the alarm.
- **Key Status:** when the tamper alarm button pops up, then the status will be changed from low to high. The normal state is high.

Note

- **Disarm** tab will turn gray when the tamper alarm is cleared.
- The round rubber button at the back of the device must be in press-down status otherwise the tamper alarm function will not be activated.

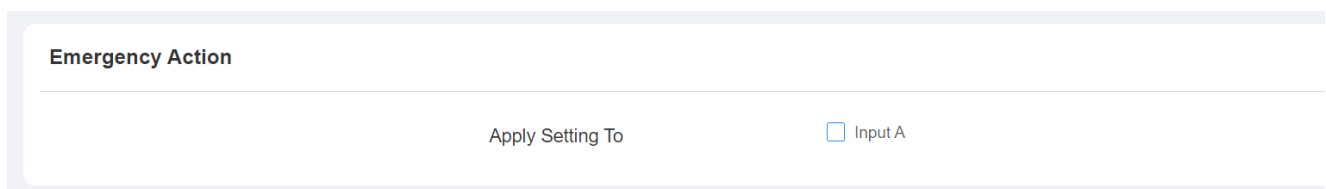
To turn on the tamper-proof function on the device, just enter the **Setting** page and tap **Security > Tamper Proof**.



12.2 Emergency Action

It is possible to keep the door open when emergency happens, so that people can get out.

In the web interface, go to **System > Security > Emergency Action**.



Note

- This function needs to work with Ekinex Delégo App.

12.3 Security Notification Setting

Several security notifications are available on the DICO door phone. The next paragraphs describe how to set them.

12.3.1 Email Notification Setting

In order to receive the security notification via email, it is necessary to configure the Email notification on the web interface properly. This can be done at the following path: **Setting > Action > Email Notification**

Email Notification

Sender's Email Address	<input type="text"/>
Sender's Email Name	<input type="text"/>
Receiver's Email Address	<input type="text"/>
Receiver's Email Name	<input type="text"/>
SMTP Server Address	<input type="text"/>
Port	<input type="text"/>
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password" value="....."/>
Email Subject	<input type="text"/>
Email Content	<input style="height: 40px;" type="text"/>
Email Test	<input type="button" value="📧 Test Email"/>

Parameter set-up:

- **Sender's Email Address:** enter the sender's email address from which the email notification will be sent out.
- **Sender's Email Name:** enter the name of the email sender.
- **Receiver's Email Address:** enter the receiver's email address.
- **Receiver's Email Name:** enter the name of the email receiver.
- **SMTP Server Address:** enter the SMTP server address of the sender.
- **Port:** enter the port number from which the email is sent out.
- **SMTP User Name:** enter the SMTP user name, which is usually the same as the sender's email address.

- **SMTP Password:** configure the password of the SMTP service, which is the same as the sender's email address.
- **Email Subject:** enter the subject of the email.
- **Email Content:** compile the email contents according to your need.

12.3.2 FTP Notification setting

It is also possible to receive the security notification via FTP. In this case, it is necessary to configure the FTP notification on the web interface by going to **Setting > Action > FTP Notification**

FTP Notification

FTP Server	<input type="text"/>
FTP User Name	<input type="text"/>
FTP Password	<input type="password" value="*****"/>
FTP Path	<input type="text"/>

Parameter set-up:

- **FTP server:** enter the address (URL) of the FTP server for the FTP notification.
- **FTP User Name:** enter the FTP server user name.
- **FTP Password:** enter the FTP server password.
- **FTP Path:** enter the folder name you created in the FTP server.

12.3.3 TFTP Notification Setting

If the user wants to receive the security notification via TFTP, it is necessary to configure the TFTP notification on the web interface at **Setting > Action > TFTP Notification**

TFTP Notification

TFTP Server	<input type="text"/>
-------------	----------------------

Parameter set-up:

- **TFTP Server:** enter the address (URL) of the TFTP server for the TFTP notification.

12.3.4 SIP Call Notification

If you want to receive the security notification via SIP call, you can configure the SIP call notification on the web interface at **Setting > Action > SIP Call Notification**.

SIP Call Notification	
SIP Call Number	<input style="width: 100%;" type="text"/>
SIP Caller Name	<input style="width: 100%;" type="text"/>

Parameter set-up:

- **SIP Call Number:** enter the SIP call number.
- **SIP Caller Name:** enter the name of the caller party.

12.4 Automatic log-out from the web interface

The administrator can set up the web interface automatic log-out timer. After this expires, it is required a re-login by entering again the user name and the passwords. This can be useful for security purposes or for the convenience of operation.

This timer can be configured on the web interface at the following path: **System > Security > Session Time Out**

Session Time Out	
Session Time Out Value	<input style="width: 100%; text-align: center;" type="text" value="300"/> (60~14400Sec)

Parameter set-up:

- **Session Time Out Value:** set the automatic web interface logout timing ranging from 60 seconds to 14400 seconds. The default value is 300.

12.5 Action URL

DICO door phone allows to set up some specific HTTP URL commands that will be sent to the HTTP server to run predefined actions. Relevant actions will be initiated depending on any changes in the relay status, input status, PIN code, and RF card access for security purposes.

These action URLs can be set up in the web interface at the following link: **Setting > Actions URL.**

Note

- Action URLs and the specific format are provided by a third-party manufacturer. DICO door phone sends the URL to the third-party devices only.

Action URL	
Enabled	<input type="checkbox"/>
Make Call	<input type="text"/>
Hang Up	<input type="text"/>
Relay Triggered	<input type="text"/>
Relay Closed	<input type="text"/>
Input Triggered	<input type="text"/>
Input Closed	<input type="text"/>
Valid Code Entered	<input type="text"/>
Invalid Code Entered	<input type="text"/>
Valid Card Entered	<input type="text"/>
Invalid Card Entered	<input type="text"/>
Tamper Alarm Triggered	<input type="text"/>
Valid Face Recognition	<input type="text"/>
Invalid Face Recognition	<input type="text"/>

For example:

[http://YOUR_DEVICE_IP/help.xml?mac=\\$mac:ip=\\$ip:model=\\$model:firmware=\\$firmware:card_sn=\\$card_sn](http://YOUR_DEVICE_IP/help.xml?mac=$mac:ip=$ip:model=$model:firmware=$firmware:card_sn=$card_sn)

DICO door phone supports the following parameter format for the events listed in the table below.

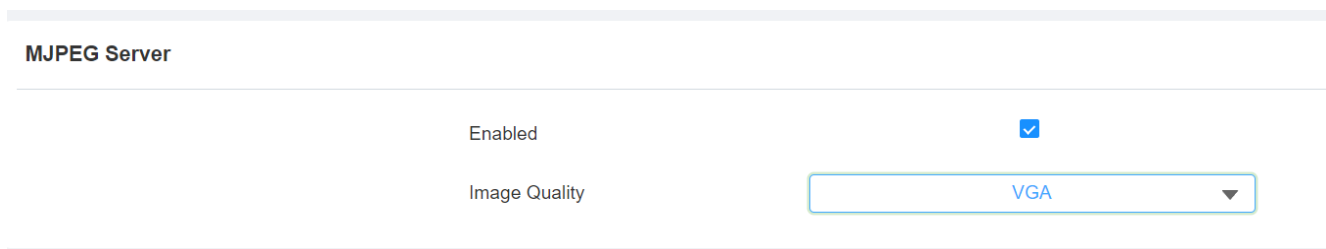
No.	Event	Parameter format	Example
1	Make Call	\$remote	http://server_ip/Callnumber=\$remote
2	Hang Up	\$remote	http://server_ip/Callnumber=\$remote
3	Relay Triggered	\$relay1status	http://server_ip/relaytrigger=\$relay1status
5	Relay Closed	\$relay1status	http://server_ip/relayclose=\$relay1status
6	Input Triggered	\$input1status	http://server_ip/inputtrigger=\$input1status
7	Input Closed	\$input1status	http://server_ip/inputclose=\$input1status
8	Valid Code Entered	\$code	http://server_ip/validcode=\$code
9	Invalid Code Entered	\$code	http://server_ip/invalidcode=\$code
10	Valid Card Entered	\$card_sn	http://server_ip/validcard=\$card_sn
11	Invalid Car Entered	\$card_sn	http://server ip/invalidcard=\$card_sn
12	Tamper Alarm Triggered	\$alarm status	http://server ip/tampertrigger=\$alarm status

13. Monitor and Image

13.1 MJPEG Image Capturing

DICO door phone has a feature to capture the MJPEG format monitoring images if needed.

It is possible to enable this MJPEG function and set the image quality on the web interface. To configure it, please go to **Surveillance > MJPEG > MJPEG Server**.



MJPEG Server	
Enabled	<input checked="" type="checkbox"/>
Image Quality	VGA

Parameter set-up:

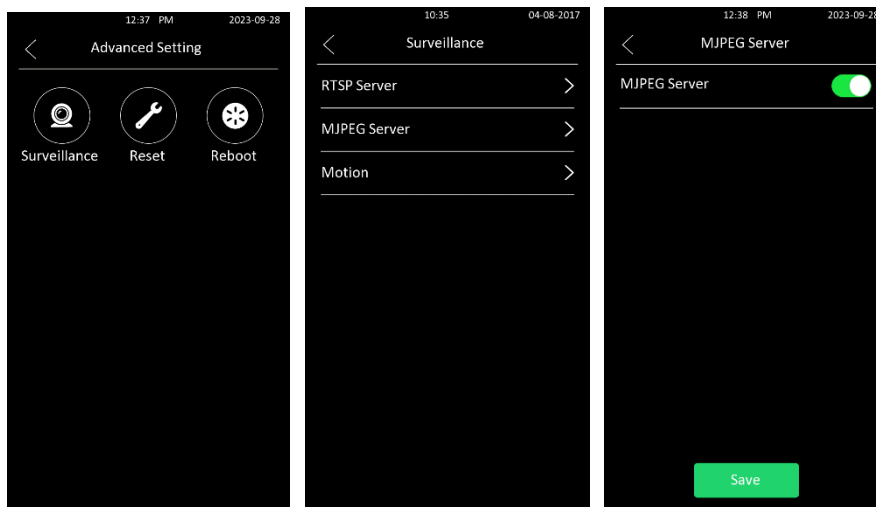
- **Enabled:** it allows to enable/disable the MJPEG capture function
- **Image Quality:** select the quality for the image capturing among seven options: **QCIF, QVGA, CIF, VGA, 4CIF, 720P, 1080P**.

As soon as the MJPEG service is enabled, the user can capture the image from the door phone using the following three types of URL format:

- http://device_ip:8080/picture.cgi
- http://device_ip:8080/picture.jpg
- http://device_ip:8080/jpeg.cgi

For example, in order to capture the jpg format image of a door phone with the IP address: 192.168.1.104, the user can type the following URL on a web browser: <http://192.168.1.104:8080/picture.jpg>.

The MJPEG server function can be enabled also on the device directly. From the Setting window, it is necessary to tap on **Advanced > Surveillance > MJPEG server**.

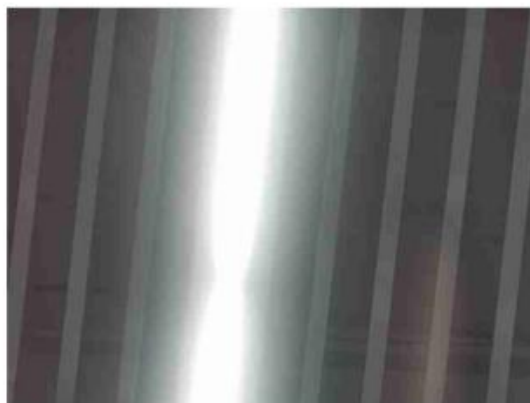


13.2 Live Stream

To check the real-time video from the DICO door phone, the user can open the web interface and obtain the real-time video. Alternatively, it is possible to enter the correct URL on a web browser and get it directly.

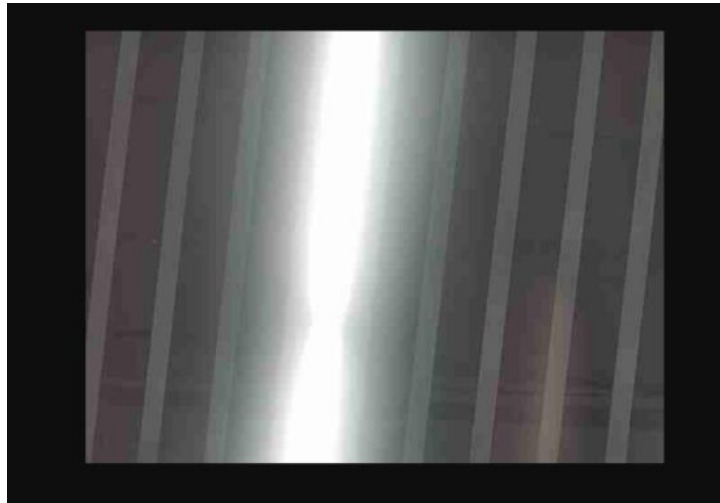
From the web interface, the user has to go to **Surveillance > Live Stream**

Live Stream



To check the real-time video using a URL, the user can Enter the correct URL on a web browser (http://IP_address:8080/video.cgi).

For example: <http://192.168.2.5:8080/video.cgi>



13.3 RTSP Stream Monitoring

DICO door phone supports RTSP stream, that allows intercom devices (such as an indoor monitor or the monitoring unit from a third party) to monitor or obtain the real-time audio/ video (RTSP stream) from the door phone using the properURL.

13.3.1 RTSP Basic Setting

The RTSP function has to be configured in terms of RTSP Authorization, authentication, password, etc. before using it. To setup this function from the web interface, the user has to go to **Surveillance > RTSP > RTSP Basic**

RTSP Basic

Enabled	<input checked="" type="checkbox"/>
Authentication Enabled	<input type="checkbox"/>
Authentication Mode	<input type="text" value="Digest"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="*****"/>

Parameter set-up:

- **Enabled:** to enable/disable the RSTP function.
- **Authorization Enabled:** tick the check box to enable/disable the RTSP authorization. If you enable the RTSP Authorization, you are required to enter RTSP Authentication Type, RTSP Username, and RTSP Password on the intercom device such as an indoor monitor for authorization.
- **Authentication Mode:** select RTSP authentication type between **Basic** and **Digest**. **Basic** is the default authentication type. The difference is that “*Basic*” Authentication mechanism sends credentials in 'clear text'. Whereas, “*Digest*” Authentication sends credentials in MD5 hashed form.
- **Username:** enter the name used for RTSP authorization.
- **Password:** enter the password for RTSP authorization.

13.3.2 RTSP Stream Setting

It is possible to select the video codec format of the RTSP stream for the monitoring activity, and configure video resolution, bitrate and other parameters based on the actual network environment.

On the web interface, this settings can be done via **Surveillance > RTSP > H.264 Video Parameters**

H.264 Video Parameters

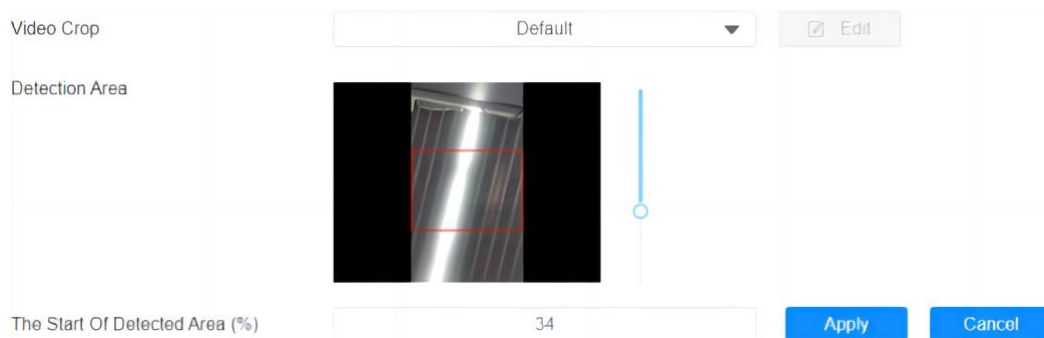
Video Resolution	4CIF	▼
Video Framerate	25 fps	▼
Video Bitrate	2048 kbps	▼
2nd Video Resolution	VGA	▼
2nd Video Framerate	25 fps	▼
2nd Video Bitrate	512 kbps	▼
Video Crop	Default	▼

✎ Edit

Parameter set-up:

- **Video Resolution:** this can be selected among seven options: **QCIF**, **QVGA**, **CIF**, **VGA**, **4CIF**, **720P**, and **1080P**. The default video resolution is **720P**, and the video from the door phone might not be able to be shown on the indoor monitor if the resolution is set higher than **720P**.
- **Video Framerate:** **25fps** is the video frame rate by default.

- **Video Bitrate:** select video bit-rate among six options: **128 kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps, and 4096 kbps** according to the network environment. The default video bit rate is **2048 kbps**.
- **2nd Video Resolution:** select video resolution for the second video stream channel. The default video resolution is **VGA**.
- **2nd Video Framerate:** select the video frame rate for the second video stream channel. The default value is **25fps**.
- **2nd Video Bitrate:** allows the selection of the video bit rate among six options for the second video stream channel: **128 kbps, 256kbps, 512 kbps, 1024 kbps, 2048 kbps, and 4096 kbps** according to the network environment. Default value is **512 kbps**
- **Video Crop:** select **Original** for the full-screen video display, or **Default** if you only want to select the specific area on the video to be displayed. With this choice, you can click **Edit** to start video cropping.



Note

- DICO door phone supports two video stream channels for H.264 codec video stream.

13.4 Acquisition in ONVIF standard

The real-time video captured by the DICO access control terminal camera can be viewed by third-party devices such as NVR (Network Video Recorder). You can configure the ONVIF function in the access control terminal so that other connected devices can view the video stream. You can enable this function in the **Surveillance > ONVIF** tab.

Surveillance » ONVIF

Basic Setting

Discoverable	<input checked="" type="checkbox"/>
Username	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>

Parameter set-up:

- **Discoverable:** tick the check box to turn on the ONVIF mode. If you select a video from the door phone camera, this can be searched by other devices. ONVIF mode is Discoverable by default.
- **Username:** enter the user name. The user name is **admin** by default.
- **Password:** enter the password. The password is **admin** by default.

After the setting is complete, you can enter the ONVIF URL on the third-party device to view the video stream.

For example: **http://indirizzo IP:80/onvif/device_service**

Where IP_address is the specific IP address of the DICO door phone.

13.4.1 Camera Mode

You can select the camera mode for better video quality, depending on where the DICO video intercom has been installed. The options allowed are **Indoor**, for a better video image (RTSP, ONVIF and Mjpeg) if the intercom is positioned in an internal space. On the contrary, if the video intercom has been installed outdoors, it is advisable to select the **Outdoor** mode.

Camera

Mode	<input style="width: 60%;" type="text" value="Indoor"/>
------	---

14. Logs

14.1 Call Logs

It is possible to check the calls (dial-out, received and missed calls) in a certain period of time, by opening and searching the call log on the device web interface. Moreover, it is possible to export the call log from the device if needed. To check the call log, please go to **Status > Call Log** in the web interface.

Call Log

Save Call Log Enabled

<input type="checkbox"/>	Index	Type	Date	Time	Local Identity	Name	Number
<input type="checkbox"/>	1	Dialed	2023-07-10	10:05:07	192.168.35.122@192.168.35.122	192.168.33.51	192.168.33.51@192.168.33.51
<input type="checkbox"/>	2	Dialed	2023-07-10	09:52:02	192.168.35.122@192.168.35.122	192.168.33.51	192.168.33.51@192.168.33.51
<input type="checkbox"/>	3	Dialed	2023-07-10	09:08:12	192.168.35.122@192.168.35.122	192.168.33.51	192.168.33.51@192.168.33.51

Parameter set-up:

- **Save Call Log Enabled:** check the box to enable the call log saving function.
- **Call History:** select call history among four options: **All**, **Dialed**, **Received**, and **Missed** for the specific type of call log to be displayed.
- **Start Time ~ End Time:** select the specific time span of the call logs you want to search, check, or export.
- **Local Identity:** it displays the door phone's SIP account or IP number that receives incoming calls.
- **Name/Number:** select the **Name** and **Number** options to search call log by the name or by the SIP or IP number.

14.2 Door Logs

In addition to call logs, the user can search and check the door access history.

If it is necessary to search and check the door logs, go to **Status > Access Log** in the web interface.

Door Log

- Save Door Log Enabled
- Save Picture Enabled
- Export Picture Enabled
- Remote Door Log Enabled

-

<input type="checkbox"/>	Index	User ID	Name	Code	Door ID	Type	Date	Time	Status	Action
<input type="checkbox"/>	1	-	Visitor	-		Face	2023-07-10	10:04:57	Failed	Picture
<input type="checkbox"/>	2	-	Visitor	-		Face	2023-07-10	08:24:48	Failed	Picture
<input type="checkbox"/>	3	-	Visitor	-		Face	2023-07-10	08:24:46	Failed	Picture
<input type="checkbox"/>	4	-	Visitor	-		Face	2023-07-10	08:24:45	Failed	Picture
<input type="checkbox"/>	5	-	Visitor	-		Face	2023-07-10	08:24:42	Failed	Picture

Parameter set-up:

- **Save Door Log enabled:** check the box to enable the door access log saving function.
- **Save Picture enabled:** check the box to enable the function of saving the image taken during door access (successful or not).
- **Export picture enabled:** check the box to enable the export function of images saved in the door access log.
- **Remote Door Log Enabled:** to enable or disable saving door accesses to a remote log.
- **Status:** select among **All**, **Success** and **Failed** options to search for successful door accesses, Failed door accesses or both.
- **Start Time ~ End Time:** select the specific time span of the door logs you want to search, check, or export.
- **Name/Code:** select the **Name** and **Code** options to search door log by the name or by the PIN code.
- **Action:** click to display the picture captured.

15. Debug

15.1 System Log for Debugging

System log feature of the DICO door phone can be used for debugging purposes. If you want to export the system out to a local PC or to a remote server for debugging, you can set up the function on the web interface at **System > Maintenance > System Log**

System Log

Log Level	<input type="text" value="3"/>
Export Log	<input type="button" value="Export"/>
Remote System Log Enabled	<input type="checkbox"/>
Remote System Server	<input type="text"/>

Parameter set-up:

- **Log Level:** select log levels from 0 to 7 levels. The default log level is **3**, the higher level is **5**, the more complete level for the log is **7**.
- **Export Log:** go to the **Export** tab to export a temporary debug log file to a local PC.
- **Remote System Log Enabled:** select **Enable** or **Disable** if you want to enable or disable the remote system log.
- **Remote System Server:** enter the remote server address to receive the device log.

15.2 PCAP for Debugging

PCAP is a service used to capture the received and transmitted data packages in real time on the network for the DICO door phone, for debugging and troubleshooting purposes.

The PCAP service can be set up properly via the web interface at **System > Maintenance > PCAP** before using it.

PCAP

Specific Port	<input type="text"/>	(1~65535)
PCAP	<input type="button" value="Start"/> <input type="button" value="Stop"/> <input type="button" value="Export"/>	
PCAP Auto Refresh Enabled	<input type="checkbox"/>	

Parameter set-up:

- **Specific Port:** select the specific ports from 1-65535 so that only the data packet from the specific port can be captured. You can leave the field blank by default.
- **PCAP:** go to the start tab and **Stop** tab to capture a certain range of data packets before going to the **Export** tab to export the data packets to your Local PC.
- **PCAP Auto Refresh:** the checkbox allows to turn on or turn off the PCAP auto fresh function. If you set it as **enabled** then the PCAP will continue to capture data packets even after the data packets reached their 1 MByte maximum in capacity. If you set it as **disabled** the PCAP will stop data packet capturing when the data packet captured reached the maximum capturing capacity of 1 MByte.

15.3 Remote Debug Server

The user can set up a remote debug server so that the Ekinex support team will be able to obtain the log remotely for debugging. To configure the server via the web interface, go to **System > Maintenance > Remote Debug Server**.

Remote Debug Server

Enabled	<input type="checkbox"/>
Connect Status	Disconnected
IP Address	<input type="text" value="/cdor.cgi?open=0&door=\$floor"/>
Port	<input type="text" value="/cdor.cgi?open=8"/> (1024~65535)

Parameter set-up:

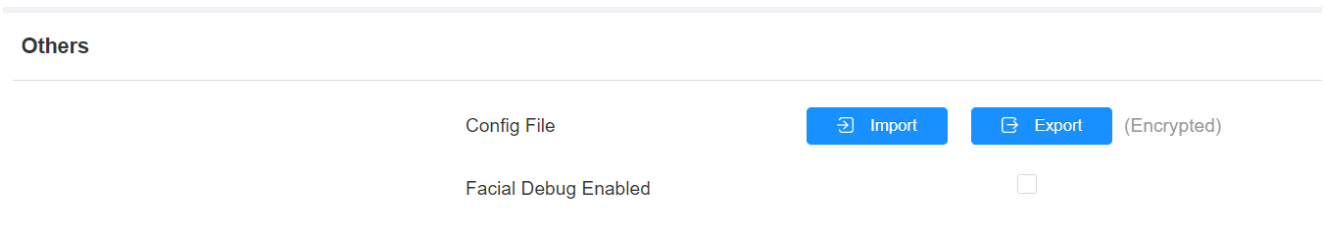
- **Enabled:** to enable/disable remote debug server function.

- **Connect Status:** display the remote debug server connection status (connected or disconnected).
- **IP Address:** enter the remote debug server IP address. Please ask Ekinex technical support team for the server IP address.
- **Port:** type in the remote debug server port.

15.4 Face Recognition Debug

As soon as a face recognition problem arises, it is possible to debug it if the related debug function has been enabled before.

To enable it in the web interface, please go to **System > Maintenance > Others**.



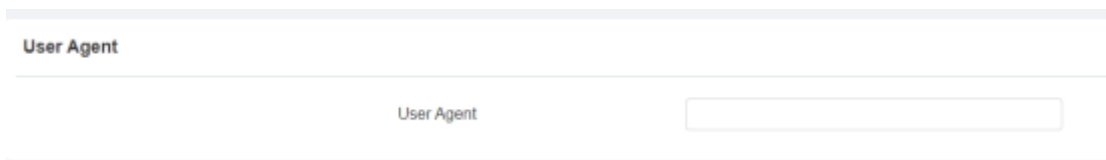
Parameter set-up:

- **Config File:** to import/export a configuration file for the facial recognition debug service
- **Facial Debug Enabled:** to enable/disable the debug function

15.5 User Agent

SIP user agent (UA) is an endpoint device that supports SIP, which is used to establish connections and enable sessions between two endpoint devices. And a UA is comprised of UAC (User Agent Client) and UAS (User Agent server) with the UAC used to issue requests and UAS used to issue responses.

UA acts as a SIP service provider for the specific user (device). You can customize the user agent field in the SIP message. If the user agent is set to a specific value, users can see the information from PCAP. If a user agent is blank, by default, users can see the company name “Ekinex”, model number, and firmware version from PCAP. The UA can be set up at the following link in the web interface: **Account > Advanced > User Agent**







Parameter set-up:

- **User Agent:** support to enter another specific value, Ekinex is by default.

16. Firmware Upgrade

DICO door phones firmware can be upgraded via the device web interface.

This feature is available at the following link: **System > Upgrade**.

Basic	
Firmware Version	216.30.0.67
Hardware Version	216.0.9.0.0.0.0.0
Upgrade	 Import
Reset Configuration To Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot

Note

- Firmware files should be available in **.zip** format.

Parameter set-up:

- **Firmware version:** displays the current FW version hosted in the device.
- **Hardware version:** displays the current HW version of the device.
- **Upgrade:** it allows to upload a new FW version into the device
- **Reset Configuration To Default State (Except Data):** restores the default state of the device
- **Reset to Factory Setting:** it restores the device data with the predefined factory values.
- **Reboot:** performs a reboot of the device.

17. Backup

If you want to import or export encrypted configuration files to your Local PC, go to the following link of the web interface: **System > Maintenance > Others**.

Others

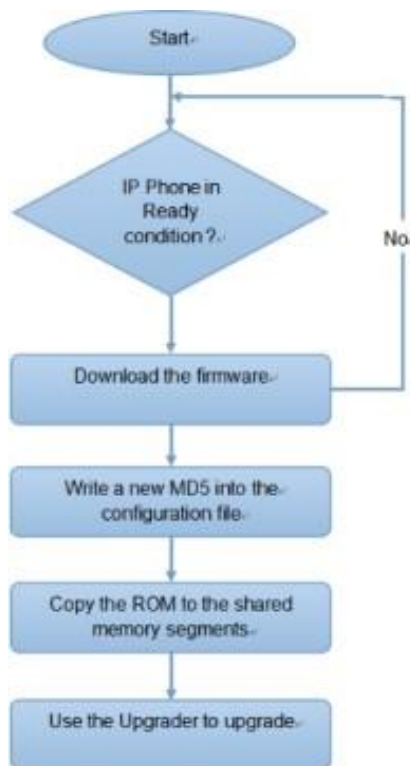
Config File	↻ Import	↻ Export (Encrypted)
Facial Debug Enabled	<input type="checkbox"/>	

18. Auto-provisioning via Configuration File

Configurations and upgrading on the DICO door phone can be done on the web interface via one-time auto-provisioning and scheduled auto-provisioning via configuration files, thus saving you from setting up configurations needed one by one manually on the door phone.

18.1 Provisioning principle

Auto-provisioning is a feature used to configure or upgrade the devices in a massive way via third-party servers. **DHCP, PNP, TFTP, FTP, and HTTPS** are the protocols used by the Ekinex DICO intercom device to access the URL of the address of the third-party server which stores configuration files and firmware. These files will then be used to update the firmware and the corresponding parameters on the door phone.



18.2 Configuration Files for Auto-provisioning

Configuration files have two formats for auto-provisioning. One is the general configuration files used for the general provisioning and another one is the MAC-based configuration provisioning.

The difference between the two types of configuration files is shown below:

- **General configuration provisioning:** a general file is stored in a server from which all the related devices will be able to download the same configuration file to update parameters on the devices. For example, .cfg files.
- **MAC-based configuration provisioning:** MAC-based configuration files are used for auto-provisioning on a specific device as distinguished by its unique MAC number. The configuration files named with the device MAC number will be matched automatically with the device MAC number before being downloaded for the provisioning on the specific device.

Note

- If a server has these two types of configuration files, then IP devices will first access the general configuration files before accessing the MAC-based configuration files.

18.3 AutoP Schedule

Ekinex provides you with different AutoP methods that enable the door phone to perform provisioning for itself at a specific time according to your schedule. You can go to **System > Auto Provisioning** in the web interface.

Automatic Autop	
Mode	Power On
Schedule	Sunday
	22 (0~23Hour)
	0 (0~59Min)
Clear MD5	Clear
Export Autop Template	Export

Parameter set-up:

- **Mode:** the available options are:
 1. **Disabled**, if the service is not active.

- 2. **Power on** if you want the device to perform Autop every time it boots up;
- 3. **Repeatedly**: if you want the device to perform Autop according to the schedule you set up;
- 4. **Power On + Repeatedly**: if you want to combine Power On mode and Repeatedly mode. This will enable the device to perform Autop every time it boots up or according to the schedule you set up;
- 5. **Hourly Repeat**: if you want the device to perform Autop every hour.

18.4 PNP Configuration

Plug and Play (PNP) is a combination of hardware and software support that enables a computer system to recognize and adapt to hardware configuration changes with little or no intervention by a user.

To set up the PNP configuration on the web interface, go to **System > Auto Provisioning > PNP Option** section.

PNP Option

PNP Config Enabled

Parameter set-up:

- **PNP Config Enabled**: to enable/disable the PNP configuration feature.

18.5 DHCP Provisioning Configuration

Auto-provisioning URL can also be obtained using the DHCP option, which allows the device to send a request to a DHCP server for a specific DHCP option code.

If the user wants to use **Custom Option** as defined by users with option code ranging from 128-255, he is required to configure **System > Auto Provisioning > DHCP Custom Option** on the web interface.

DHCP Option

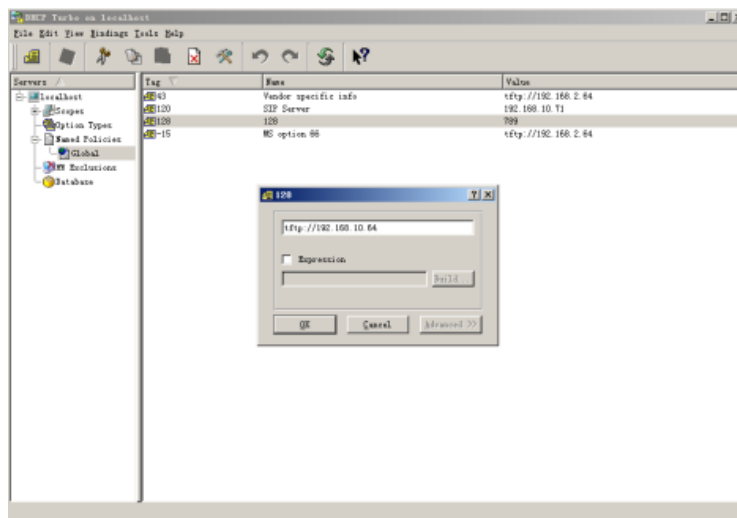
Custom Option (128-254)

(DHCP option 66/43 is enabled by default.)

To set up DHCP AutoP with “Custom Option” and “Power on” mode, please follow the link **System > Auto Provisioning > Automatic Autop** on the web interface. Then click **Export** tab in **Export Autop Template** to export Autop template. Then set up DHCP Option on DHCP server.

Automatic Autop

Mode	<input style="width: 90%;" type="text" value="Power On"/>
Schedule	<input style="width: 90%;" type="text" value="Sunday"/>
	<input style="width: 80%; margin-right: 10px;" type="text" value="22"/> (0-23Hour)
	<input style="width: 80%; margin-right: 10px;" type="text" value="0"/> (0-59Min)
Clear MD5	<input style="width: 80%; background-color: #007bff; color: white;" type="button" value="Clear"/>
Export Autop Template	<input style="width: 80%; background-color: #007bff; color: white;" type="button" value="Export"/>



Note

- The custom Option type must be a The value is the URL of the TFTP server.

Parameter set-up:

- **Custom Option:** the available options are:
 1. **Custom option:** enter the DHCP code that matches the corresponding URL so that the device will find the configuration file server for the configuration or upgrading.
 2. **DHCP Option 66:** if none of the above is set, the device will automatically use DHCP Option 66 for getting the upgrade server URL. This is done within the software and the user does not

need to specify this. To make it work, you need to configure the DHCP server for option 66 with the updated server URL in it.

- DHCP Option 43:** if the device does not get an URL from DHCP Option 66, it will automatically use DHCP Option 43. This is done within the software and the user does not need to specify this. To make it work, you need to configure the DHCP server for option 43 with the updated server URL in it.

Note

- The general configuration file for batch provisioning is in the **rcfg** format. For example, with E16 it becomes r00000000116.cfg (9 zeros total). Instead, the MAC-based configuration file for provisioning the specific device has the format MAC_Address of the device with a .cfg extension, for example **0C110504AE5B.cfg**.

18.6 Static Provisioning Configuration

You can manually set up a specific server URL for downloading the firmware or configuration file. If an Autop schedule is set up, the door phone will perform the auto-provisioning on a specific timing according to the previously configured Autop schedule. In addition, TFTP, FTP, HTTP, and HTTPS are the protocols that can be used for upgrading the device firmware and configuration.


To download the Autop template, please follow **System > Auto Provisioning > Automatic Autop** on the web interface, and setup Autop server on **System > Auto Provisioning > Manual Autop** interface.

Automatic Autop

Mode	<input type="text" value="Power On"/>
Schedule	<input type="text" value="Sunday"/>
	<input type="text" value="22"/> (0-23Hour)
	<input type="text" value="0"/> (0-59Min)
Clear MD5	<input type="button" value="Clear"/>
Export Autop Template	<input type="button" value="Export"/>

Manual Autop

URL	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password" value="....."/>
Common AES Key	<input type="password" value="....."/>
AES Key(MAC)	<input type="password" value="....."/>

 AutoP Immediately

Parameter set-up:

- **URL:** set up TFTP, HTTP, HTTPS, and FTP server addresses for the provisioning.
- **User Name:** set up a user name if the server needs a user name to be accessed otherwise leave it blank.
- **Password:** set up a password if the server needs the password to be accessed otherwise leave it blank.
- **Common AES Key:** set up AES code for the intercom to decipher the general Auto Provisioning configuration files.
- **AES Key (MAC):** set up AES code for the intercom to decipher the MAC-based auto provisioning configuration file.

Note

- AES is one type of encryption, it should be configured only when the config file is encrypted with AES, otherwise leave the field blank.

Note

Server Address format:

- TFTP: tftp://192.168.0.19/
- FTP: ftp://192.168.0.19/ (allows anonymous login)
- ftp://username:password@192.168.0.19/(requires a user name and password)
- HTTP: http://192.168.0.19/ (use the default port 80)
- http://192.168.0.19:8080/ (use other ports, such as 8080)
- HTTPS: https://192.168.0.19/ (use the default port 443)

Note

- Ekinex does not provide user specified server.
- The user is invited to setup TFTP/FTP/HTTP/HTTPS server on his own.

19. Integration with Third Party Device

19.1 Wiegand integration

The DICO device allows you to configure a Wiegand connection, a standard protocol commonly used in access control systems.

If you want to integrate the DICO video intercom with third-party devices via Wiegand, you can set the parameters from the **Device > Wiegand** web interface.

Device » [Wiegand](#)

Wiegand

Wiegand Display Mode	8HN ▼
Wiegand Card Reader Mode	Wiegand-26 ▼
Wiegand Transfer Mode	Input ▼
Wiegand Input Data Order	Default ▼
Wiegand Output Data Order	Default ▼
Wiegand Output CRC Enable	<input checked="" type="checkbox"/>

Parameter set-up:

- **Wiegand Display Mode:** select Wiegand Card code format among **8H10D**, **6H3D5D**, **6H8D**, **8HN**, **8HR**, **RAW** and **8HR10D**.
- **Wiegand Card Reader Mode:** set the Wiegand data transmission format among three options: **Wiegand-26**, **Wiegand-34** and **Wiegand-58**. The transmission format should be identical between the door phone and the device to be integrated.
- **Wiegand Transfer Mode:** set the Transfer mode between **Input**, **Output** or **Convert to Card NO. Input**, depending on whether the video intercom is used as a receiver or as a transmitter.
- **Wiegand Input Data Order:** set the Wiegand input data sequence between **Default** and **Compatible**. In the second case, the input card number will be reversed.
- **Wiegand Output Data Order:** set the Wiegand output data sequence between **Default** and **Compatible**. In the second case, the output card number will be reversed.
- **Wiegand Output CRC enable:** this function is used for Wiegand data inspection. It is turned on by default. If it is not activated, the integration of the video intercom with third-party devices may not be possible.

If you select **Wiegand Transfer Mode = Output**, then you can set the code for input/output conversion:

Convert To Wiegand Output

PIN

Disabled

- **PIN:** sets the encoding type for the conversion, which can be **Disabled**, **8 bits per digit**, **4 bits per digit**, or **All at once**.

19.2 Integration via HTTP API

HTTP API is designed to achieve a network-based integration between the third-party device with the Ekinex DICO intercom device. You can configure the HTTP API function on the web interface at **Setting > HTTP API**

HTTP API

HTTP API Enable



Authorization Mode

Allowlist

Username

admin

Password

.....

1st IP

2nd IP

3rd IP

4th IP

5th IP

Parameter set-up:

- **HTTP API Enable:** enables or disables the HTTP API function for third-party integration. For example, if the function is disabled, any request to initiate the integration will be denied and HTTP 403 forbidden status will be returned.
- **Authorization Mode:** select among five options: **None**, **AllowList**, **Basic**, **Digest** and **Token** for authorization type.

- **Username:** enter the user name when **Basic** and **Digest** authorization mode is selected. The default user name is Admin.
- **Password:** enter the password when **Basic** and **Digest** authorization mode is selected. The default user name is Admin.
- **1stIP- 5th IP:** enter the IP address of the third-party devices when the “*AllowList*” option is selected as Authorization Mode.

19.3 Lift control

It is possible to connect the DICO door phone with an Ekinex lift controller or third-party lift controllers, in order to manage a lift control. You can summon the lift to go down to the ground floor when you are granted through various types of access methods on the door phone. To set up the lift control, go to **Device > Lift Control**.

Device » [Lift Control](#)

Lift Control List

Lift Control List None ▼

Parameter set-up:

- **Lift Control List:** select the integration mode among the following options: **None**, **OSDP**, **Ekinex**, **KEYKING**. The detail for the options will be provided in the following table:

#	Integration mode	Description
1	None	If you select None then the RS485 integration will be disabled.
2	OSDP	If you select OSDP Mode, then the integration communication between the DICO door phone and the third-party device is via OSDP protocol. You are required to check for the device integration protocol and make sure that they use the same integration protocol.
3	Ekinex	Select Ekinex if you want to connect the device to the Ekinex lift controller.
4	KEYRING	Select KEYKING if you want integration with KEYKING elevator controller.

Depending on the selected integration mode, the following additional parameters need to be set.

19.3.1 OSDP integration mode

If the selected integration mode is OSDP, then the user has to set-up some advanced setting:

OSDP Advanced Setting

Connect Status	Disconnected
Output With	<input style="width: 100%;" type="text" value="OSDP"/>

- **Connect Status:** the available options are **Connected** or **Disconnected**
- **Output with:** the options are **OSDP** or **None**.

19.3.2 Ekinex integration mode

If the selected integration mode is Ekinex, then the the following parameters are available:

Ekinex Advance Setting

Server IP	<input style="width: 95%;" type="text"/>	
Port	<input style="width: 95%;" type="text"/>	(1~65535)

Parameter set-up:

- **Server IP:** the IP address of the server where the controller is connected
- **Port:** the communication port of the controller

Ekinex Action

User Name	<input style="width: 95%;" type="text"/>
Password	<input style="width: 95%;" type="password" value="....."/>
Floor No. Parameter	<input style="width: 95%;" type="text"/>
URL To Trigger Specific Floor	<input style="width: 95%;" type="text"/>
URL To Trigger All Floors	<input style="width: 95%;" type="text"/>
URL To Close All Floors	<input style="width: 95%;" type="text"/>

- **User Name:** the user name to connect to the lift service

- **Password:** the password for the service
- **Floor No. Parameter:** the parameter to identify the floor number
- **URL to trigger specific floor:** insert here the server URL for a specific floor number
- **URL to trigger all floors:** insert here the server URL to make all plans reachable
- **URL to close all floors:** insert here the server URL to configure the inaccessible floors.

19.3.3 KEYRING integration mode

If the selected integration mode is KEYRING, then the the following parameters are available:

Keyring Advanced Setting

Address

0

Parameter set-up:

- **Address:** select here the address for KEYRING integration.

19.4 Integrate with third-party Access Control Server

It is possible to access the door phone using the QR code or access card generated by a third-party server. For example, when you use the QR code on the door phone, the QR code will be sent to the third-party server for verification. The user will be granted access if the QR code passes the verification.

To configure it, you can go to **Access Control > Relay > Third Party Integration** on the web interface.

Third Party Integration

List

General

HTTP URL

3

Device ID

Parameter set-up:

- **List:** it allows to select the integration modes.
 1. If you want to disable the function, select **None**.
 2. If you want to use QR code only, select **General**.

3.If you want to select between a QR code and an access card with customized features, select **Customize**.

• **HTTP URL:**

1.For General mode: enter the **HTTP URL** provided by the third-party service provider. After scanning the QR code, the HTTP URL will carry the dynamic QR code information automatically before sending it to the QR code server for verification.

See the example below:

<http://wxqapi.kerryprops.com.cn:8090/api/vistor/scan?codeKey={QRCode} &deviceId={DeviceID}>

2.For Customize mode: select the **QR code** or **Card** verification.

3.For QR code verification: enter the QR code HTTP URL provided by the third-party service provider. See the example below:

<http://www.server.com/<base>/hs/ACS/checking/QRCode/{DeviceID}/{Card}>

4.For Card verification: enter the access card HTTP URL, provided by the third-party service provider. See the example below:

<http://www.server.com/<base>/hs/ACS/checking/{QRCode}/{DeviceID}/Card>

- **Prompt On LCD:** select **Default**, if you want to adopt the Ekinex door phone prompt for the door access. Select **Return** value, if you want to use the return value from the third-party server as the prompt.
- **Remote Verification:** select **QR code** or **Card** verification.
- **Device ID:** enter your device ID, which will be added to the HTTP URL automatically when you use a QR code or card for access.

20. Password Modification

The user is allowed to set and change both the System PIN Code for accessing the device setting and the login password for accessing the web interface. In addition, he can also select the user role when setting passwords.

To set the password, in the web interface go to **System > Security > Web Password Modify**

System » Security

Web Password Modify

Username

Account Status

admin	Enabled
user	<input type="checkbox"/>

By pressing on **Change Password** button, the user will be prompted to enter the information as below:

Change Password
×

The password must be at least eight characters long and contains at least one uppercase letter, one lowercase letter, and one digit.

Username	admin
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

Cancel
Change

To set up the system PIN code, the user can refer to the **system PIN** section.

System PIN

PIN Code

21. System Reboot and Reset

21.1 Reboot

To restart the device system, the user can operate it on the device web interface as well.

Moreover, it is possible to set up a schedule for the device to be restarted.





To set up the device reboot schedule, in the web interface go to **System > Auto Provisioning > Reboot Schedule**.

Reboot Schedule

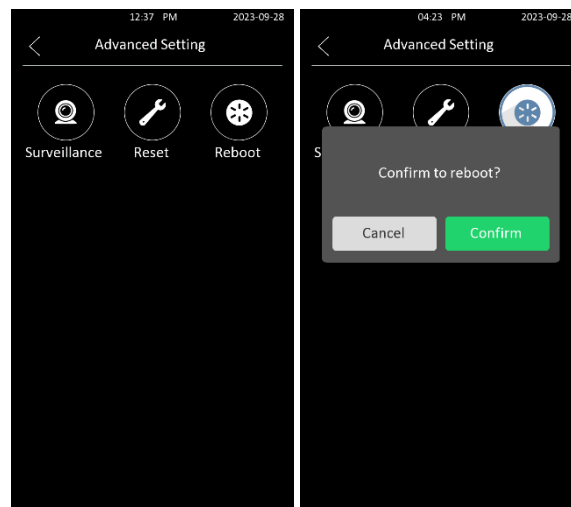
Mode	<input type="checkbox"/>
Schedule	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Every Day ▼</div> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block; width: 150px;">0</div> (0~23Hour)

To reboot the device manually, go to **System > Upgrade > Basic** in the web interface and click on **Reboot** button.

Basic

Firmware Version	216.30.0.67
Hardware Version	216.0.9.0.0.0.0.0
Upgrade	 Import
Reset Configuration To Default State(Except Data)	 Reset
Reset To Factory Setting	 Reset
Reboot	 Reboot

To reboot from the device itself, enter the Setting page and tap **Advanced > Reboot**.



21.2 Reset

The user can select **Reset To Factory Setting** in order to reset the device and therefore delete both configuration data and user data, such as RF cards, face data, and so on.

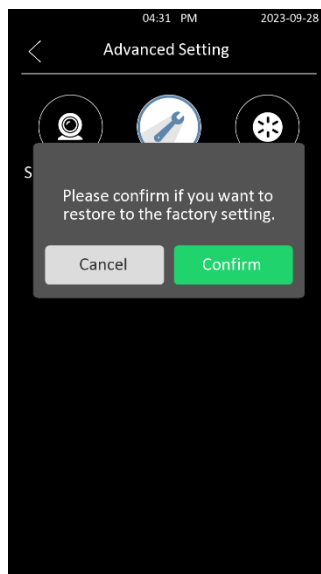
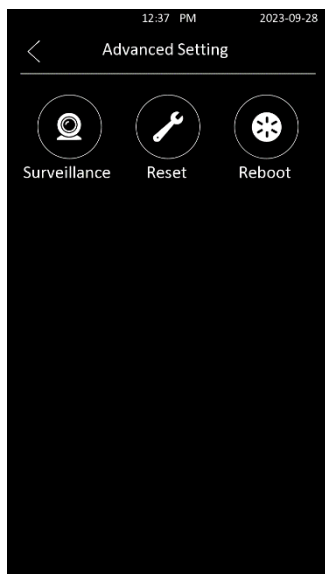
In case **Reset Configuration to Default State (Except Data)** is selected, then the device is reset but the user data are kept stored.

To reset the device, go to **System > Upgrade** in the web interface.

Basic

Firmware Version	216.30.0.67
Hardware Version	216.0.9.0.0.0.0.0
Upgrade	Import
Reset Configuration To Default State(Except Data)	Reset
Reset To Factory Setting	Reset
Reboot	Reboot

To reset the device to the factory setting on the device, enter the Setting page and go to **Advanced > Reset**.



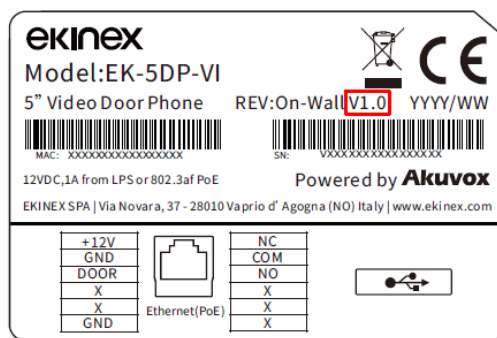
22. FAQ

Q: How to confirm whether my device is hardware version 1.0 or a later version?

A: This can be done in 2 ways:

1. Check the label on the device

- **Hardware version 1.0**



2. Go to **Status > Info > Product Information** on web interface and check firmware and hardware version.

Firmware Version	216.30.0.67
Hardware Version	216.0.9.0.0.0.0.0

- **Firmware Version**

The firmware is different between hardware version 1.0 and later versions.

- 216.X.X.X is hardware version 1.0.

- **Hardware Version**

If the hardware version is 216.X, then the device is the hardware version 1.0.

23. Markings

CE: the device complies with the Low Voltage Directive (2014/35/EU) and the Electromagnetic Compatibility Directive (2014/30/EU).

Tests carried out according to following regulations:

- EN 61000-3-2
- EN 61000-3-3
- IEC/EN 61000-6-1
- IEC/EN 61000-6-3
- EN 55014
- EN 50491

24. Maintenance

The device is maintenance-free. To clean it, use only a dry cloth; please avoid the use of detergents, solvents or other aggressive substances, particularly on the lens.

25. Disposal



At the end of its useful life the product described in this datasheet is classified as waste from electronic equipment in accordance with the European Directive 2002/96/EC (WEEE), and cannot be disposed together with the municipal undifferentiated solid waste.



Warning: *Incorrect disposal of this product may cause serious damage to the environment and human health.*

Please be informed about the correct disposal procedures for waste collecting and processing provided by local authorities.

26. General warnings

- Installation, electrical connection, configuration and commissioning of the device can only be carried out by qualified personnel in compliance with the applicable technical standards and laws of the respective countries.
- In case of tampering, the compliance with the essential requirements of the applicable directives, for which the device has been certified, is no longer guaranteed.
- Ekinex® KNX defective devices must be returned to the manufacturer at the following address: EKINEX S.p.A. Via Novara 37, I-28010 Vaprio d'Agogna (NO) Italy.

27. Other information

This datasheet is aimed at administrators of the system.

For further information on the product, please contact the ekinex® technical support at the e-mail address: support@ekinex.com or visit the website www.ekinex.com.

© EKINEX S.p.A. 2023 - The company reserves the right to make changes to this documentation without notice.