Zennio GetFace IP

IP Video Intercom (Basic Unit)

ZVP-CAM/ZVP-WOCAM

User manual version: [2.23]_a
Firmware version 2.23

www.zennio.com

USER MANUAL

CONTENTS

DOCUMENT UPDATES

Version	Changes	Page(s)
[2.23]_a	Fingerprint reader module (ZVP-FINGER) configuration. Up to two cards per user for accessing with the module ZVP-RFSMN.	38 29
[2.22]_a	New section for door configuration: **Hardware / Door.** Minor corrections.	
[2.21]_a	Reset configuration to default state. Clarification about “Phone Number (ID)” Automation Configuration. Accesses E-Mail Configuration. Hardware configuration of the ZVP-RFSMN module Minor text changes.	
[2.20]_a	Bluetooth Module Configuration. Configuration of RFID cards in Hardware section. Minor corrections.	
[2.18]_b	Minor text changes.	

1 INTRODUCTION

Zennio GetFace IP is the video intercom solution from Zennio. In combination with the supported touch panels (such as **Z41 COM**), it provides integration for **video-call** management between the entrance door of a residential environment (like single-family homes, apartment blocks or housing states with a common access) and the interior of the dwelling. Or between the interior of any environment with similar characteristics, as an office building, and the access door.

The most outstanding features of Zennio GetFace IP are:

- High resolution video camera (1280x960 resolution) and IR emitter for darkness situations (ZVP-CAM).
- Operating temperature: -40 to 60 ºC.
- Operating relative humidity: 10 to 95%.
- RJ-45 connector and Fast Ethernet standard support.
- PoE (Power over Ethernet) 802.3af – Class 0 – 12.95W power supply possibility.
- Reset button and pilot lights (yellow, red and green).
- Audio output (Line Out).
- Relay output NO/NC 30V/1A (AC/DC) for opening and closing functions.
- Active or passive input (-30 – 30VDC).
- Active output (12VDC/2A).
- Several Opening Methods.

2 INSTALLATION

2.1 DEVICE WIRING DIAGRAM

Zennio GetFace IP provides several optional modules which can be connected individually to expand the number of the device functions or features.

- Keypad module (ZVP-KEYPAD),
- 5-button module (ZVP-NAME5),
- Touch display (ZVP-TOUCHD),
- Information panel (ZVP-INFOP),
- Access card reader module RFID (ZVP-RFSMN),
- Magnetic induction module (ZVP-ILOOP),
- I/O module (ZVP-INOUT).
- Smart card RFID reader NFC ready (ZVP-RFSMN).
- Bluetooth Module (ZVP-BLUET).

Notes:

- *A reboot of the intercom is necessary after connecting a module prior to accessing its configuration.*
- *Locating a specific module at any time is possible by entering the web Hardware → Extenders section within the web interface (please refer to the next sections of this document).*
- *The video intercom can be powered by a 12V external supply or through the PoE input.*
- *If audio coupling problems are observed during a call, a filter of the acoustic feedback is required (see section 3.2.4.1).*

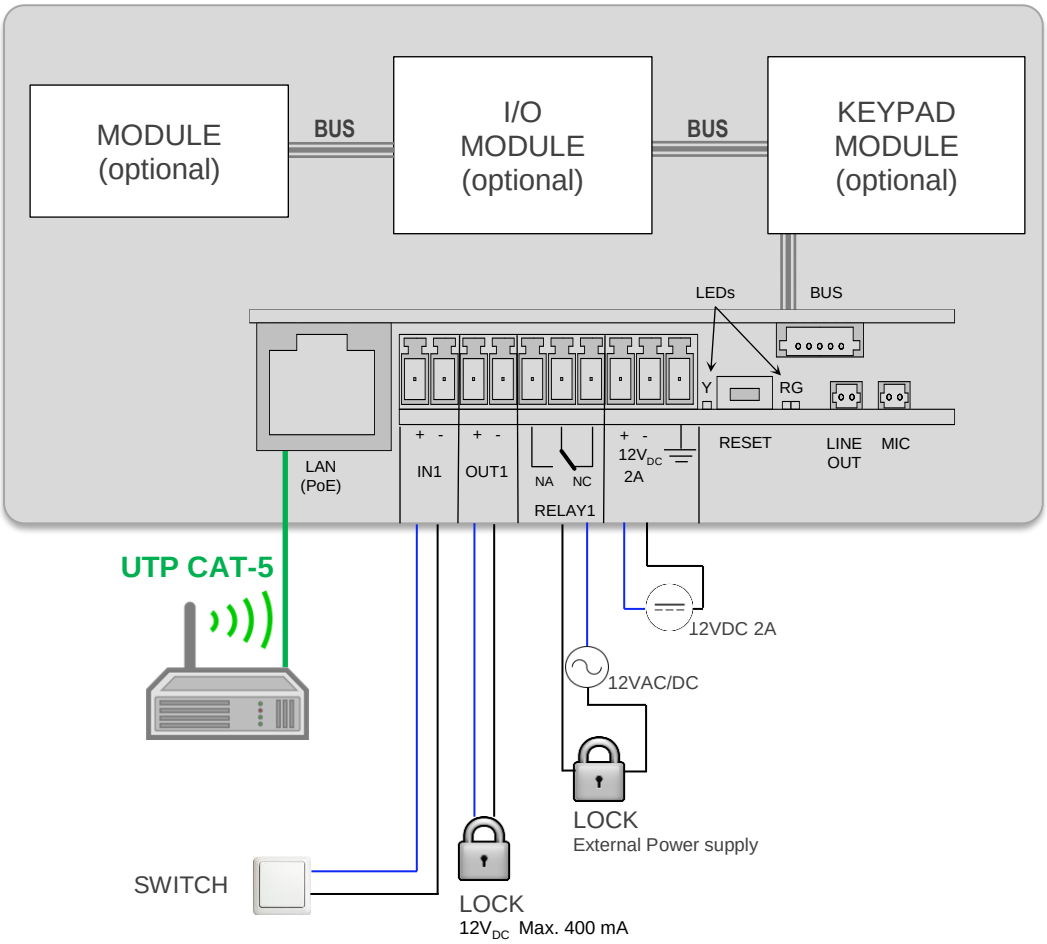

Figure 1 Device wiring diagram.

2.2 APPLICATION CASES

The most typical network topologies where Zennio GetFace IP can be installed are outlined in this section.

2.2.1 SINGLE-FAMILY HOMES

For an individual housing environment that requires completely independent video-call systems, the typical installation will be one of the two shown in Figure 2 -- this will depend on whether direct interconnection between Zennio GetFace IP and the touch panel is possible or, alternatively, on whether both devices are being connected through an indoor router (provided, for example, by the Internet service provider).

If needed, a network switch that expands the number of available LAN interfaces can be connected to the router, so multiple Z41 COM can be incorporated to the system.

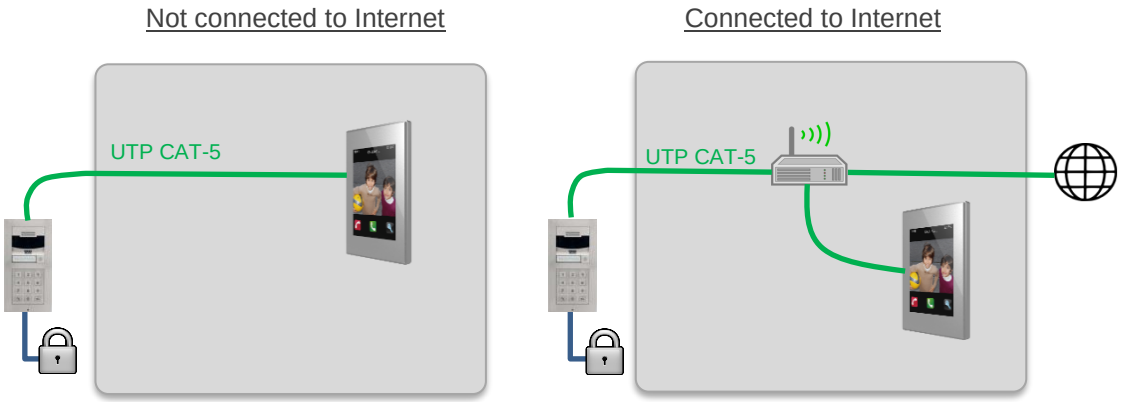

Figure 2 Single-family home installation.

2.3 APARTMENT BLOCK

In the case of an apartment building equipped with a common Zennio GetFace IP intercom for all of them, a community network infrastructure (firewall-managed) will be required to interconnect the video intercom with each apartment. As in 2.2.1, each of aparments may or may not have its own Internet connection router.

Figure 3 shows a good example of this type of topology: VLAN labelling is used as traffic insulation between each dwelling.

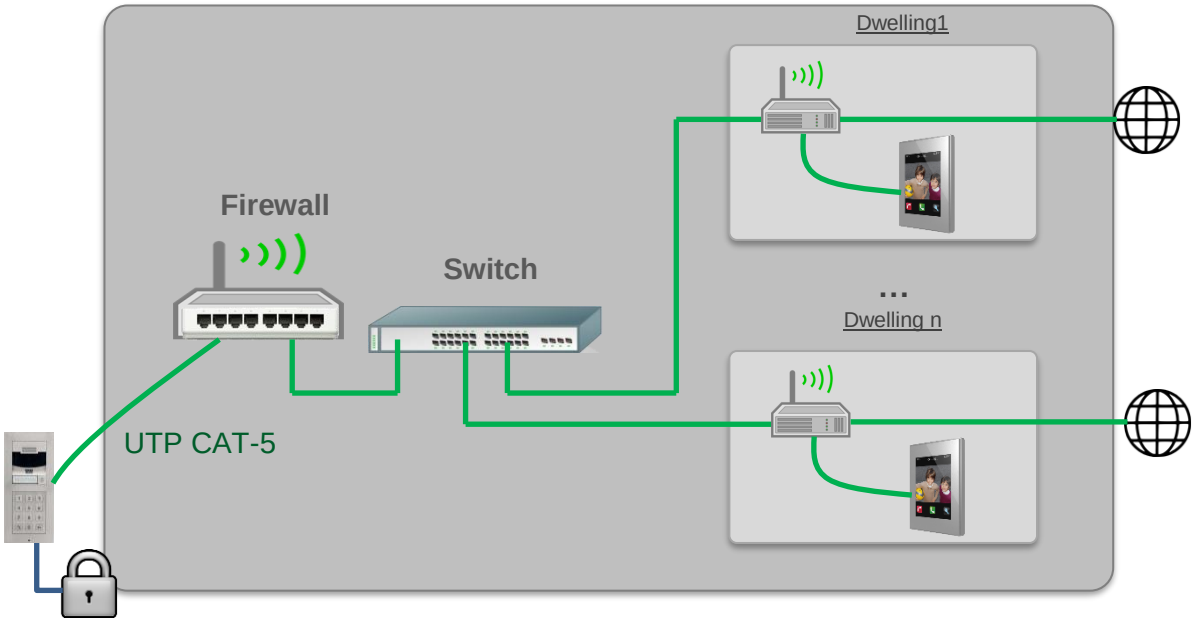

Figure 3 Apartment block installation.

For detailed information about the technical features of Zennio GetFace IP, as well as on security and installation procedures, please refer to the device **Datasheet**, bundled within the device packaging and also available at www.zennio.com.

3 CONFIGURATION

After completion of the installation (please pay attention to the application cases explained above), the device shall be configured. A number of parameters will be provided for the proper, joint operation of Zennio GetFace IP and Z41 COM.

During the first 30 seconds of operation (after supplying power to the video intercom), **the Hardware button should be pressed for 5 times**. This will make **the device say (with its own voice!) its IP address**. To enter the configuration interface, a web browser will be required. The URL address should be in the following format: "**http://192.168.1.100"** (assuming that 192.168.1.100 is the IP address of the device).

The video intercom is configured to work with a DHCP server by default. If no DHCP server is available or network issues are found, the video intercom may take a wrong IP address (0.0.0.0).

The network configuration of the GetFace IP can be modified by **quick pressing the main button of the base unit for 15 times after the start-up**. This will make it reboot again automatically. After each reboot, the device will switch between a dynamic IP (DHCP) and a static IP configuration, being the latter 192.168.1.100.

Authentication is required for access to the web interface. **By default**, it is set to:

- User: **admin**
- Password: **zennio**

Note: *please pay attention to upper and lower case letters.*

Changing the password is recommended after the first access to the device. This is possible by entering **Services → Web Server**. The new password should be eight characters long and should include at least one capital letter, one lowercase letter, and one number.

The main window will look similar to Figure 4.

Figure 4 Configuration menu.

Notes:

- *The default language of the interface is English.*
- *A Save button is provided at the bottom of each configuration page to allow saving any changes made, although a confirmation message will show up if trying to switch to another page without having saved them.*

3.1 GETFACE IP BASIC SETTINGS

The most important fields to be configured so the video intercom can interface with Z41 COM are explained next. Those to be modified from the default configuration are, in short, the following:

- **Phone Number (ID)**: identifier of the video intercom (if intending to link it to a specific box in Z41 COM).
- **HTTP API**: services security settings. Up to 5 different configurations available.
- **Users Phone Number**: should contain the IP address of each Z41 COM.

How these fields should be configured is explained in the following sections.

Notes:

- *Options not mentioned in the present document should be left with their default configuration.*
- *Options showing a prohibition icon when the mouse pointer is placed over them are locked due to license constraints.*
- *It is possible to return the device to its default settings ('hard reset'). To do this, there are two options:*
  - *Pressing the reset button of the basic unit for 30 seconds.*
  - *In the web interface, in the section **System → Maintenance → Configuration → Reset Configuration to Default State**.*

3.1.1 NETWORK CONFIGURATION (SYSTEM)

The Network section allows using a DHCP server or setting up a static network configuration.

Note: *there are cases where the application of a static IP is mandatory*.

- *In single-family homes, with the video intercom connected directly to the indoor unit. It is important to ensure that their network mask is the same while their IPs are different (but belonging to the same range)*.

- *When the video intercom and Z41 COM belong to different networks (depending on the case). In this case it will be also necessary to enable in the application program of Z41 COM in ETS the parameter **The External Unit Is In a Different Network,** and to enter the same fixed IP address that has been configured in the web interface.*

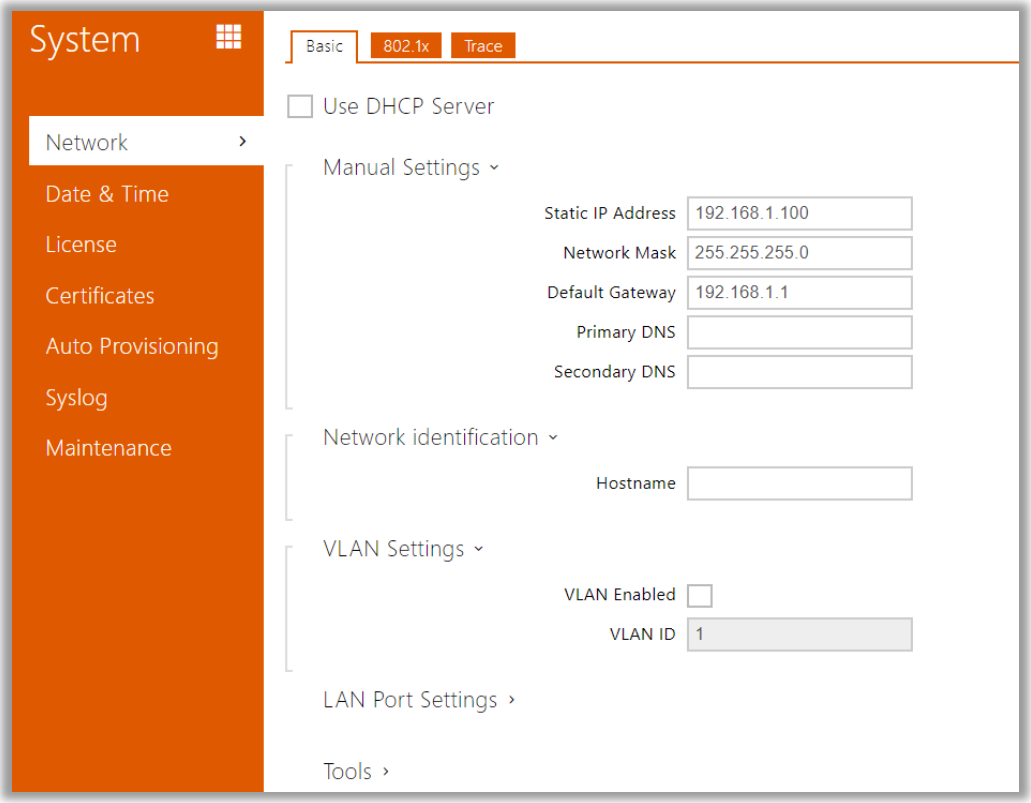

Figure 5 System.

3.1.2 VIDEO-CALL CONFIGURATION (SERVICES)

3.1.2.1 PHONE

Basic video-call functions are configured in this tab.

SIP

SIP is a transmission control protocol used in IP telephony. Up to two SIP profiles can be set up. Each profile should be configured properly according to its own operation network. The following configuration settings allow Z41 COM to connect to Zennio GetFace IP.

- **Intercom identity**: configuration parameters that define the video intercom profile (see section 3.1.3.1):

  - **Display name**: identification name for the video intercom, which is also shown at the start page of the web interface.

  - **Phone Number (ID)**: alphanumerical identifier for the video intercom. This value must match the **Intercom ID** parameter (in ETS) of the particular box of Z41 COM where the video intercom is desired to be linked to. This field is mandatory if the outdoor and indoor unit are in different networks. It is also required when several video intercoms must be distinguished in different boxes in the same Z41 COM.

Notes:

- *Characters > and < are not allowed in the **Display name** field.*
- *The **Phone number (ID)** field must be alphanumeric and no longer than 10 characters. Characters like @ or · are not allowed. However, basic punctuation marks are allowed*.

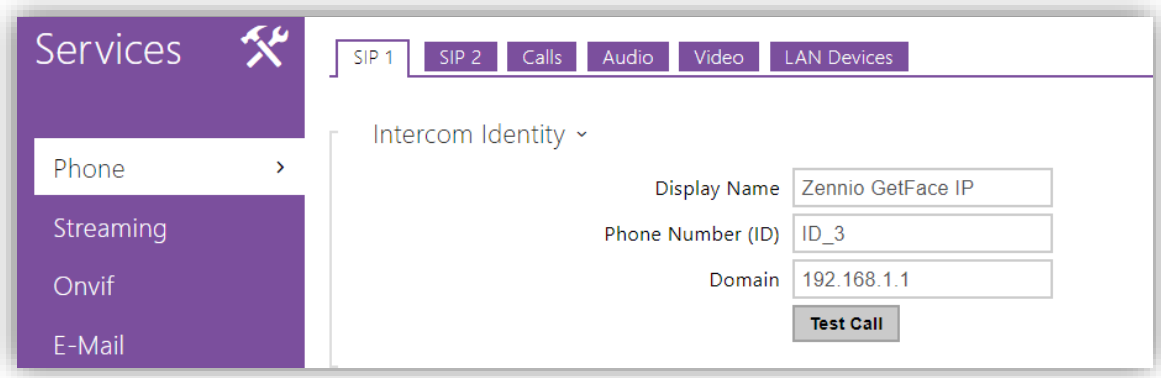

Figure 6 SIP.

CALLS

The **Calls** tab allows setting up the parameters related to the video-calls. The intercom's response to an incoming call is parameterised under **Incoming calls**. As the video intercom is designed for one-way calls, this field is set to "Always busy" by default.

Under **Outgoing calls**, the timing of the calls can be defined:

- The **Ring Time Limit** is the unanswered call maximum duration. It is advisable to set a length longer than 20 seconds.

- **Call Time Limit** sets the maximum duration of the call. After this time, the call is finished automatically. The end of this call will be warned by Zennio GetFace IP by beeping 10 seconds in advance. In such case, the call can be extended by simply pressing on any button from the touch display module (ZVP-TOUCHD) or from the keypad module (ZVP-KEYPAD), if configured.

- **Dial Cycles Limit** sets the maximum dial call repetitions to avoid deadlock in case that the User is not accessible and the User Deputy has the same phone number on the Phone Book.

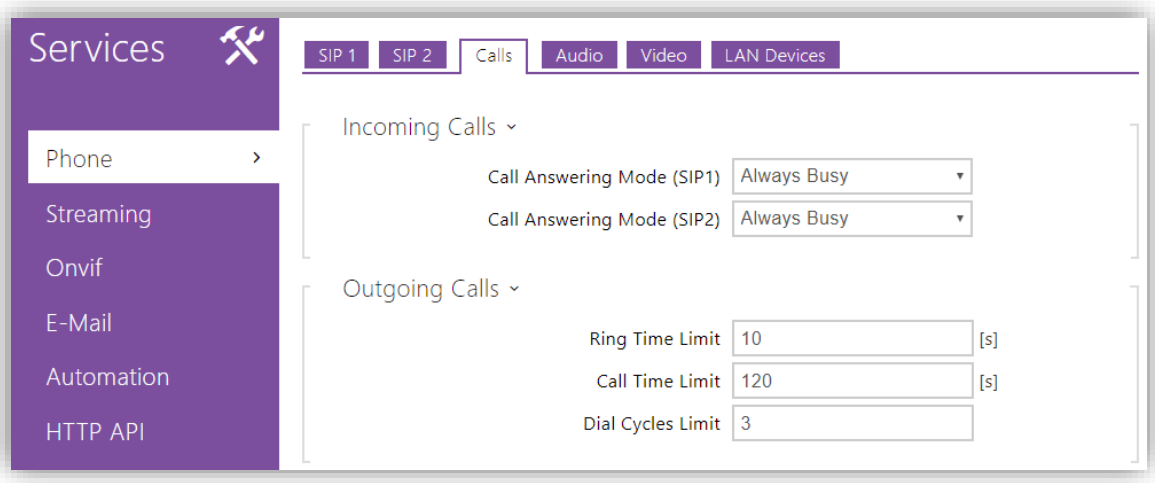

Figure 7 Calls.

AUDIO

Audio output settings can be configured in the **Audio** tab. It consists of:

- **Audio Codecs: Services → Phone → Audio.** Giving the highest priority to the G.722 codec is encouraged, as show in in Figure 8.

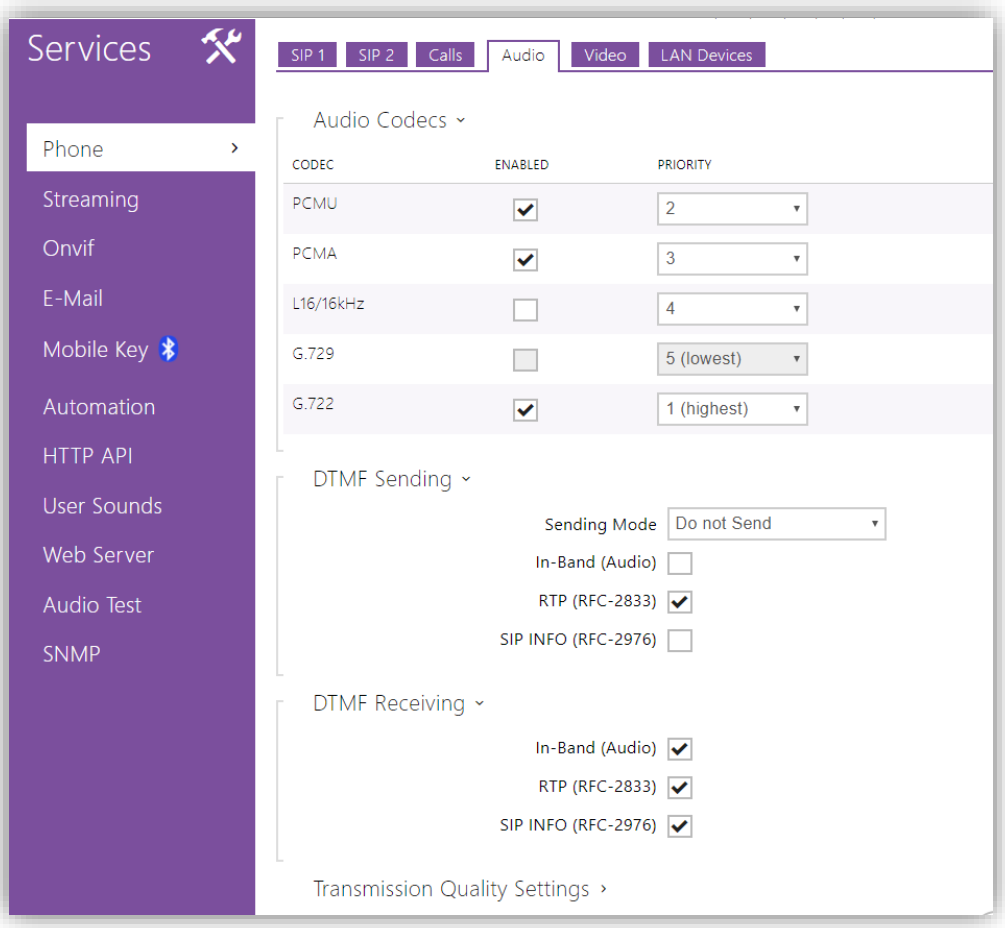

Figure 8 Audio.

- **Transmission Quality Settings**:

  - **Quality of Service DSCP Value**: sets the priority of the RTP packages in the network. The value set here will be sent under the ToS (Type of Service) field of the IP package header.

  - **Jitter Compensation**: sets the buffer storage capacity to compensate the jitter effect in the audio package transmission. The greater the capacity, the better the transmission stability. However, the sound delay will be longer either.

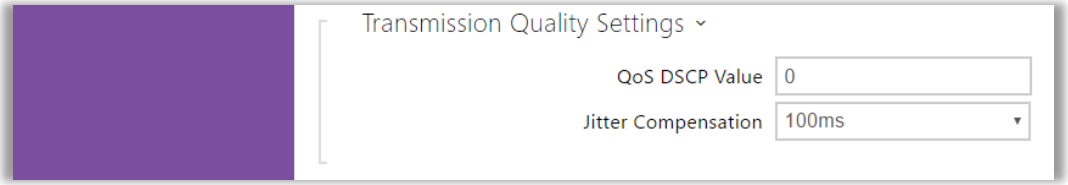

Figure 9 Transmission Quality Settings.

VIDEO

The video output settings can be configured under the **Video** tab.

- **Video Codecs**: It is advisable to change the H.264 video resolution for a smooth video transmission. This is possible under **Services** → **Phone** → **Video**, as shown in Figure 10.

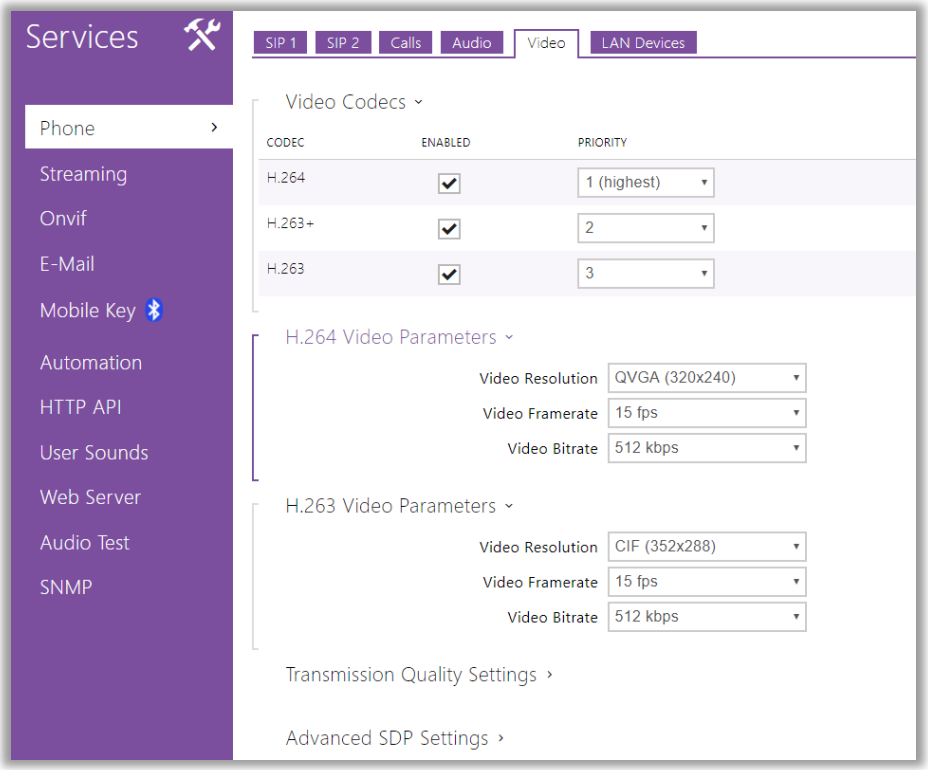

Figure 10 Video.

3.1.2.2 HTTP API

This section allows controlling IP functions via HTTP.

SERVICES

This tab allows setting up the services, the transport protocol and the authentication procedure for each service (for details on the configuration of the advanced services, please refer to section 3.2.3**)**. It is also necessary to parameterise the **System API**[1], the **Switch API** and the **Camera API**.

[1] *API: Application Programming Interface.*

To that end, the aforementioned parameters are configured as detailed below, under **Services → HTTP API → Services**.

- **System API**: **"**Unsecure (TCP)", with no authentication.
- **Switch API**: "Secure (TLS)" with "Digest" authentication.
- **Camera API**: "Unsecure (TCP)". If a camera preview is required, the authentication should be set to "None".

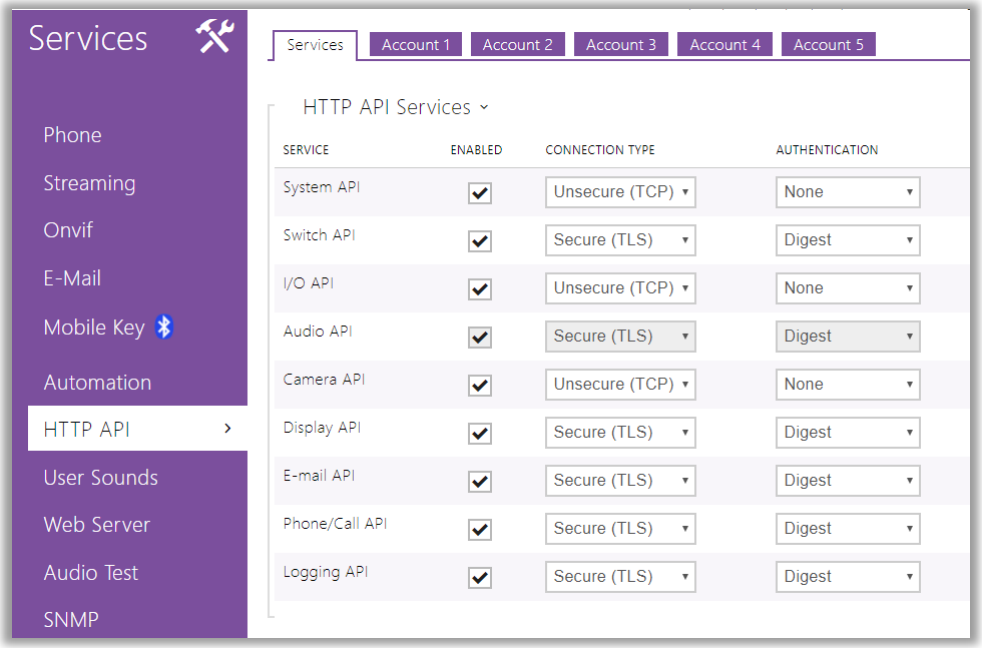

Figure 11 HTTP API Services.

ACCOUNTS

The **Account n** tabs allow setting up user configuration profiles that restrict certain actions depending on the username and password. Up to five accounts are possible, each with a username and a password and with different access privileges, either monitor or control privileges. These accounts allow a higher security level, as authentication with Z41 COM is required.

If Z41 COM is configured with a username and a password through the **Opening Method** parameter, then an analogous configuration should be performed in the **Accounts** tab to allow the opening of the door lock system.

Moreover, the **Switch Access** checkbox should be activated. Otherwise, the door unlocking will not work successfully. If this configuration is not desired, the username and password fields should be left blank in both devices.

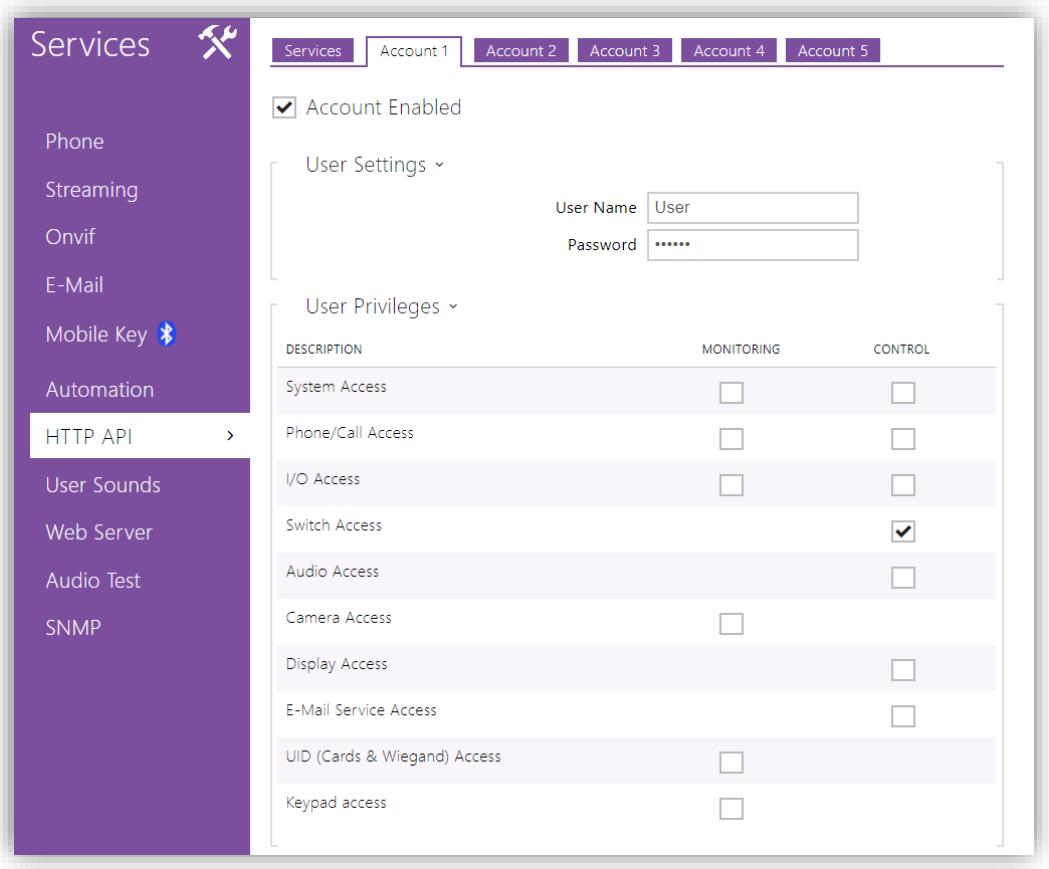

Figure 12 HTTP API Account.

Note: *The maximum size for user and password fields is 10 characters. This limit is given by the corresponding ETS fields in Z41 COM, which are limited by 10 bytes (if special characters of more than 1 byte are included is possible the maximum size would be less than 10 characters).*

3.1.3 HOUSING CONFIGURATION & Z41 COM (DIRECTORY)

Homes connected to the video intercom system must be configured from **Directory**. The following features can be set up from this window.

3.1.3.1 USERS

It is necessary to configure, at least, as many positions as dwellings that may be called from the video intercom. For each of these positions, the corresponding **User Phone Number** should be established according to the IP of the corresponding Z41 COM. These settings are performed from **Directory → Users → Number.**

For a single user, it will be also possible to set up as many telephone numbers as Z41 COM devices existing within the dwelling. This requires activating **Parallel call to the following number**.

In case there are more than three Z41 COM within a home, it will be possible to call to all of them in parallel if more than one user is defined for that home. In such case, it will be necessary to activate not only **Parallel call to following number** but also **Parallel call to following deputy**. In short, a single dwelling can have several users assigned, however all the Z41 COM defined for a user must belong to the same dwelling.

Example:

*The **format** should be:*

- ***sip:irrelevant_identifier@IP_of_the_Z41_COM_device***

*A valid example would be: **sip:555@192.168.1.101**, being 192.168.1.101 the IP address of the Z41 COM.*

Note: *if a keypad (ZVP-KEYPAD) or a touch-display (ZPV-TOUCHD) is added to the video intercom, the **Virtual Number** field should contain the number to be dialled on the keypad for the call.*

Before accessing the Users configuration, is required to click on **Add** in every user's tab. Once the user is added, this button will switch to **Remove.**

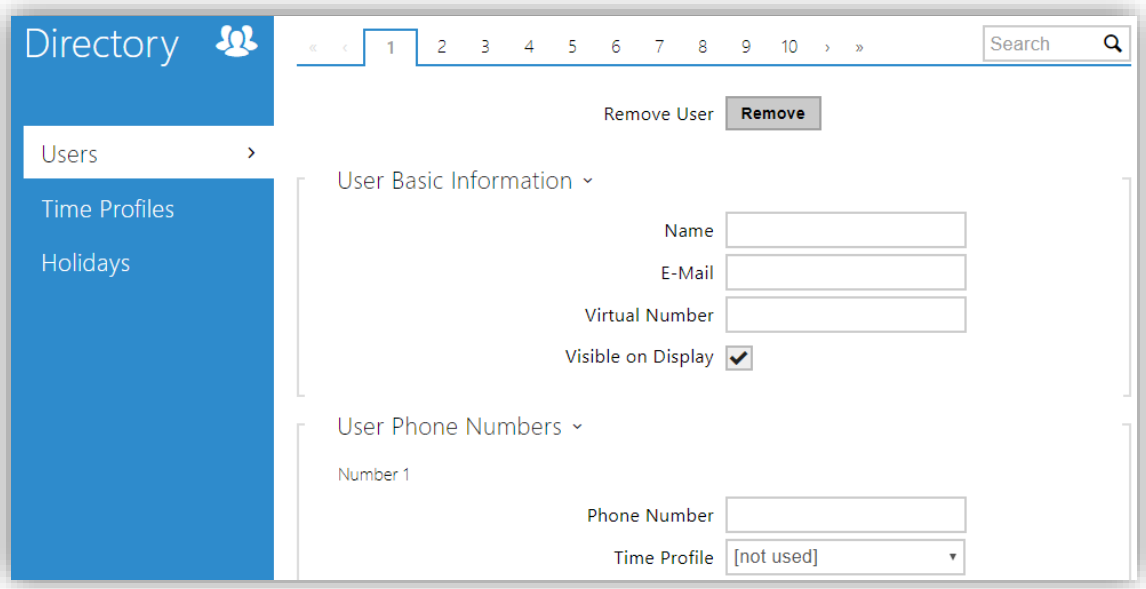

Figure 13 Users.

The **Users** section defines the following parameters:

- **Name**, which will identify the housing or the owner.
- **E-Mail** contact address (optional; see section 3.2.3.1)
- **Virtual Number**: number to be entered into the keypad in order to call the user. It must contain from 2 to 4 digits. Only for the ZVP-KEYPAD module.

  Note: *this field is enabled provided that "Virtual number" has been selected in Dial by Numeric Keypad (see section 3.2.4.3).*

- **User Phone Numbers**:
  - **Phone Number**: string with the already described format.
  - **Time Profile**: time range in which call reception is allowed.
  - **Parallel call to following number**: if parallel calling to another number is required (i.e., in case of more than one Z41 COM in the same house), this checkbox should be enabled.
  - **User Deputy**: user the calls should be redirected to in the event of not being the current user available. If **Parallel to following deputy** is enabled, all calls will be transmitted in parallel to both the current user and the deputy. This option can be useful when there are more than three Z41 COM in the same house.
- **User activation**: user activation / deactivation code and current status (only for the ZVP-KEYPAD module).
- **Access Settings:** (simple by default), which is based on combining an RFID card along with a code to be typed for the door opening (for the ZVP-KEYPAD, ZVP-RFSMN or ZVP-TOUCHD modules). Time profiles are allowed for activation / deactivation.
- **User Codes**: user private code for the switch opening. Time profiles can be established to restrict its application. Only for the ZVP-KEYPAD module.

  Note: *the corresponding switch must be enabled in **Hardware → Switches** (see section 3.1.4)*.

- **User Cards**: ID of the user access card and time profile that will remain active. One card is allowed per user. Only for the ZVP- RFSMN module (see section 3.1.9).

3.1.4 DOOR CONFIGURATION

The section **Hardware → Door** groups the configuration parameters needed to control the door opening and its access rules.

DOOR

This tab contains the general configuration of the door, which will be applied regardless of the access direction.

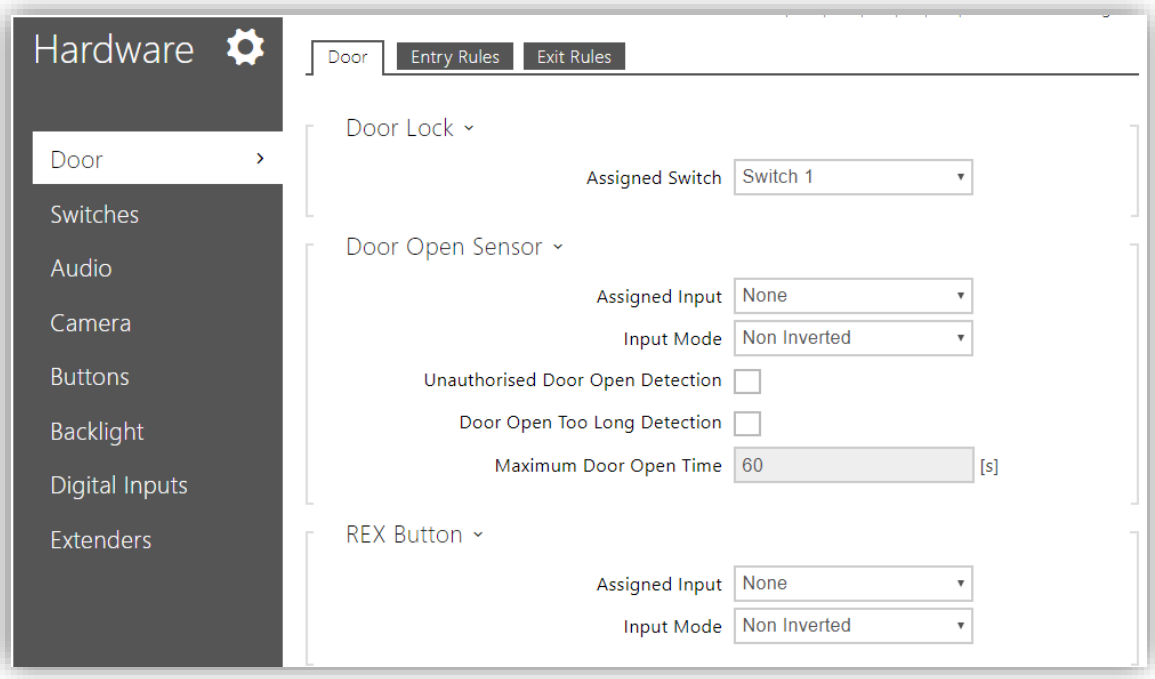

Figure 14 Door.

- **Door Lock**: assignation of the switch to be controlled. Its configuration is explained in the next section.

- **Door Open Sensor**: an input can be assigned to monitor the door's state. It is possible to detect unauthorised openings and excessively long opened times, where the time can be parameterised.

- **REX Input Control** section allows configuring one of the GetFace IP inputs to function as an output button, so that when this input is activated the output associated with the gate will be opened. This feature will be useful if required an indoor switch to activate the door opening.

ENTRY / EXIT RULES

This two tabs have the same parameters but each one referring to one access direction.

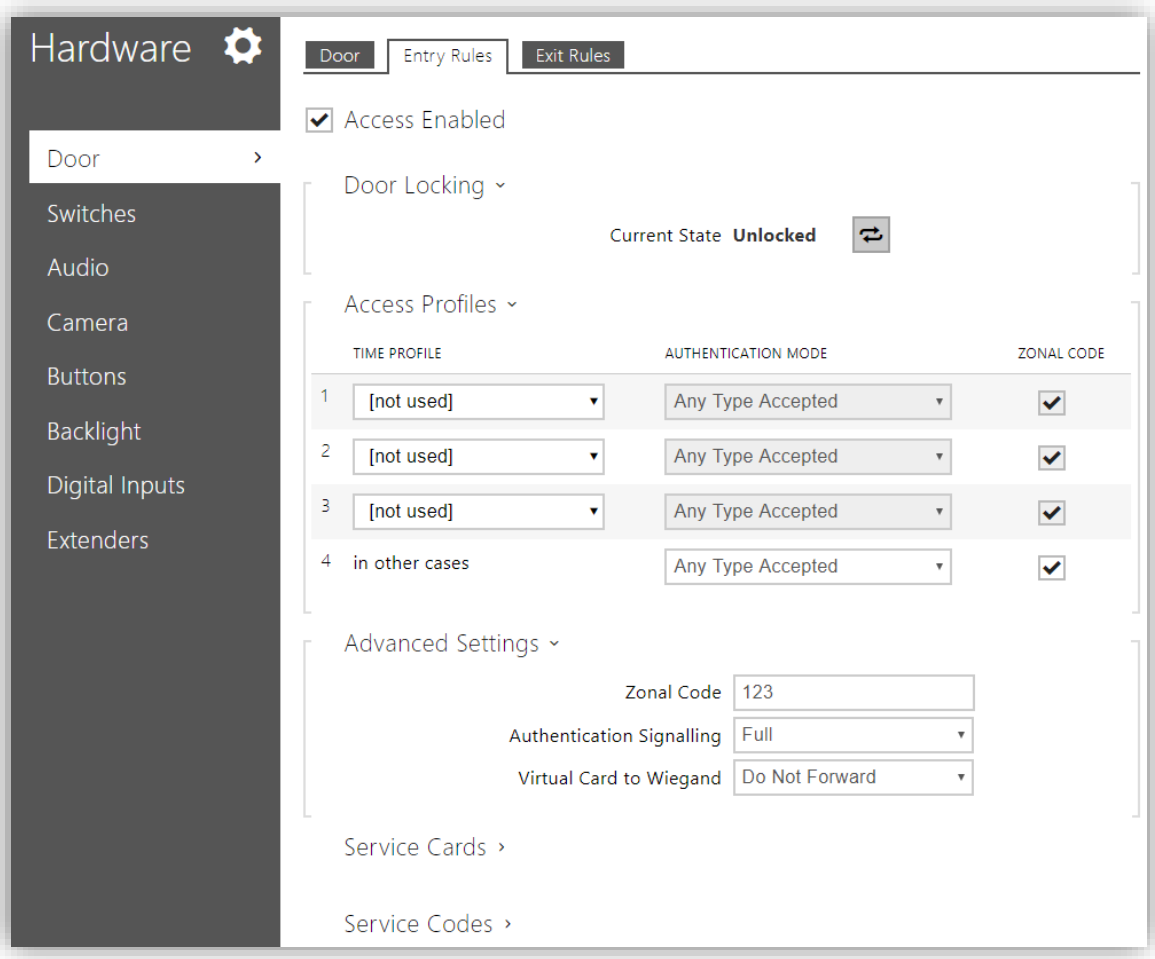

Figure 15 Door. Entry / Exit Rules

- **Door Locking**: this button allows to block every access in that direction. The current status is displayed.

- **Access Profile**: links the authentication modes available with the time profiles configured in **Directory → Time Profiles** and whether the Zonal Code is enabled.

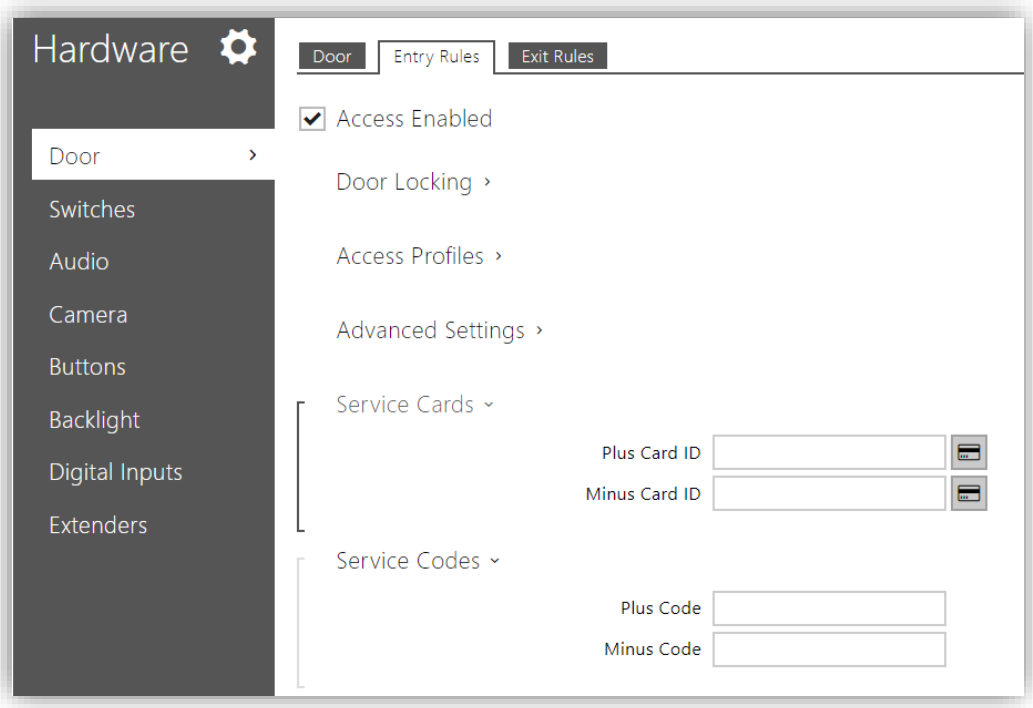

Figure 16 Door. Entry / Exit Rules.

- **Advanced Settings**: configuration of the Zonal Code, the authentication signalling and whether the card ID will be sent to a Wiegand output group.

- **Service Cards**: determine the ID of the cards used to add or delete user cards. The card reader module is required (ZVP-RFSMN).

  - Once the ID of the Plus Card and Minus Card are added, , it is enough to swipe the master card over the card reader module and, afterwards, the user card to be activated/deactivated.
  - The user cards added will be saved as new users, named *"!Visitors #n"*, where n will be the first user available.

- **Service Codes**: determine the codes used to add or delete user codes, but in this case through the keyboard module (ZVP-KEYPAD).

  - These service codes will be used to add or delete user codes. The user codes added will be saved as new users, named *"!Visitors #n"*, where n will be the first user available.
  - The codes must have 2 characters minimum, but is recommended to use at least a 4-charater code.
  - The procedure to add or delete a code is:

- Enter Plus Code and press the key button ( ).
- If a new user code is being added, enter the number of the switch to be controlled and press the key button.
- Enter the new code to add or an existent code to delete, and press the key button.

After each of these steps, a visual and acoustic notification will be given if the step has been successfully completed.

3.1.5 SWITCHES CONFIGURATION

It is possible to configure the opening of electric locks linked to Zennio GetFace IP. This allows controlling them from Z41 COM (up to three electric lock can be enabled).

For instructions on how to wire the lock system to Zennio GetFace IP please refer to section 2 and to datasheet of the device.

Regarding the configuration, it is necessary to enable the switch in the top side box and to set the page options according to the provided lock system.

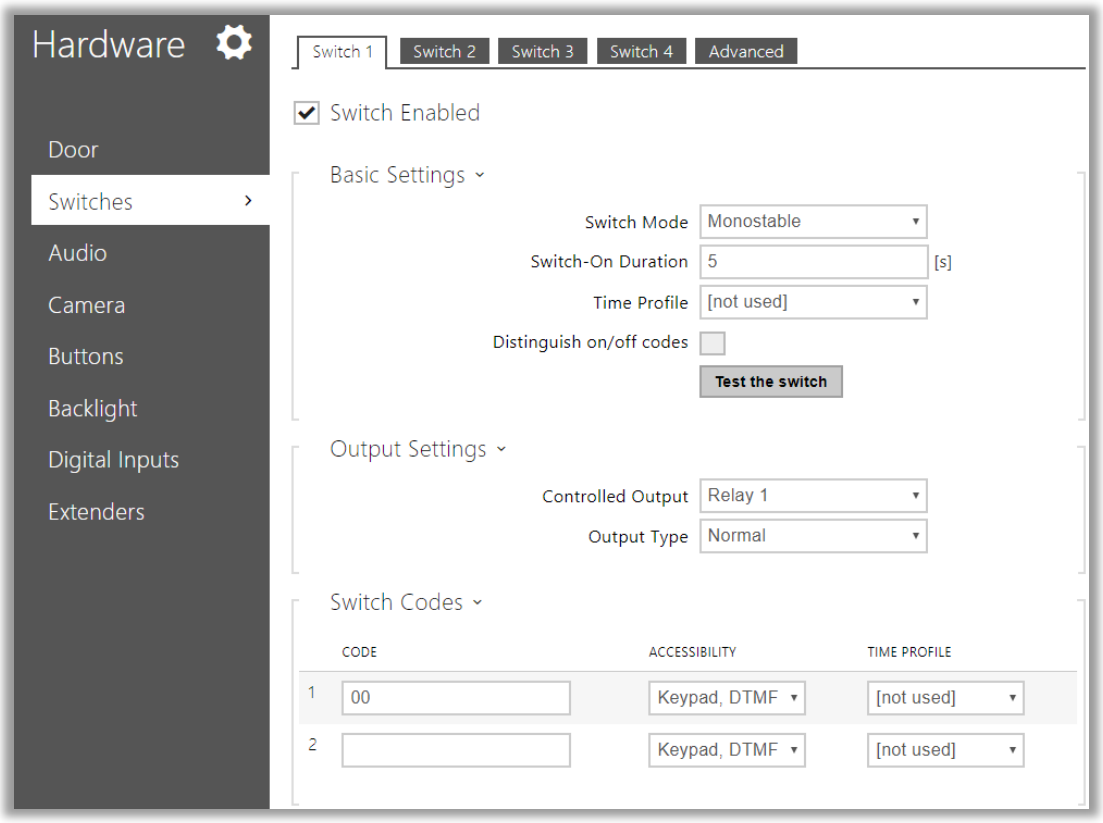

Figure 17 Switches.

- **Basic Settings** of the switches:
  - **Switch Mode**: sets the opening mode (**monostable**, in case it gets automatically deactivated some time after the opening order; or **bistable**, if a manual deactivation is required).
  - **Switch-On Duration**: delay for monostable switches.
  - **Time Profile** to be applied to the switch (see section 3.2.2.1).
  - **Distinguish on/off codes**, in case of a bistable switch.
- **Output Settings**: regarding the output type, it can be configured as a relay or as an electric output. In case of selecting "None", the switch will be controllable through HTTP commands.

  The output behaviour can be configured as one of the following types:
  - **Normal**: to perform the door opening, the output needs to be activated.
  - **Inverted**: to perform the door opening, the output needs to be deactivated.
  - **Security**: the output works in inverted mode but a security relay module has been installed and therefore a specific pulse sequence is necessary for the door opening (this requires the ZVP-ACSR module).
- **Switch Codes**: codes that will allow activation of the switches by typing them into the keypad (only for the ZVP-KEYPAD or ZVP-TOUCHD modules). Code activation time profiles can also be applied (see section 3.2.2.1).
- **State Signalling**: sets the type of the acoustic feedback to be performed on the activation of the relay. Either a short or long beep can be configured.
- **Synchronisation**: enables switch synchronisation so that, when one of the switches is activated and after a parameterised delay, another switches gets activated as well.

3.1.6 BUTTONS MODULE CALL CONFIGURATION

The section **Hardware → Buttons** defines the buttons and the dwelling linked to each one of them, in case a buttons module has been attached to the system (reference ZVP-NAME5).

Basic Settings:

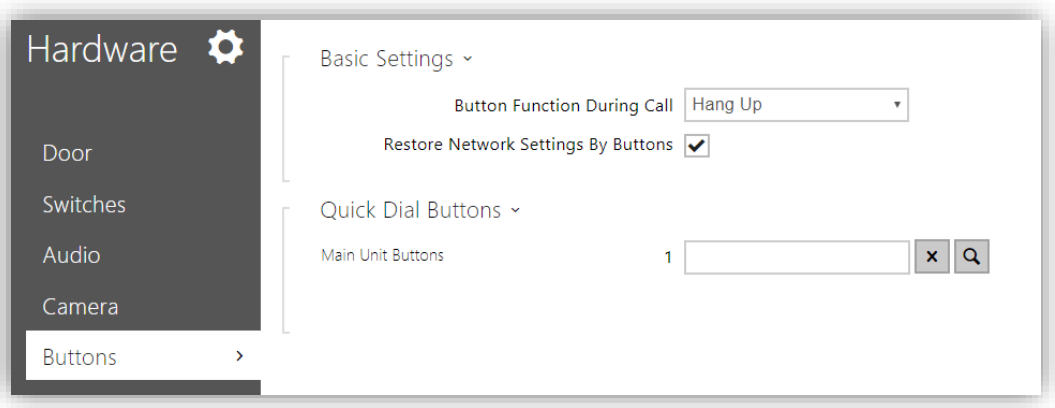

Figura 18 Buttons.

- **Button Function During Call**: configures the function of the quick dial button during a call. This only applies to the button the call was started with. It is recommended to leave this button non-functional during calls, otherwise the calls may be finished by mistake.

- **Restore Network Settings By Buttons**: this option allows restoring the network default settings through a quick dial buttons sequence (see section 3 for more information).

In **Quick Dial Buttons** will appear all available direct dial buttons, depending on the number of five-button modules connected (up to 29 modules), together with the button incorporated in the video intercom. Each button must correspond with the user associated to a particular dwelling (see section 3.1.3.1 for more information).

3.1.7 TAMPER SWITCH CONFIGURATION

The **tamper switch** does not require extra configuration. The function of this accessory is warning when the video intercom is being manipulated. For that purpose, it must be connected to a KNX input or any monitoring system. That connection will remain closed

after the Zennio GetFace IP frame has been installed. On the other hand, it will be open once the frame gets removed.

3.1.8 ACCESS CONFIGURATION WITH TOUCH-DISPLAY

The Touch Display module (ZVP-TOUCH) allows making phone calls an opening the lock. To configure this module is necessary to enter the **Hardware → Display** section of the web interface.

DISPLAY

The basic settings are configured in this section.

- **Language Settings**: sets the main language for the on-screen controls.
- **Phone Book Displayed**: allows providing an orderly user phone book through the Touch Display.
- **Keypad Displayed**: enabling this option activates the keypad that allows making phone calls and opening the lock. The configuration of the directory is analogous to that for the ZVP-KEYPAD module (see section 3.1.3.1).
- **Dial Numbers by Keypad**: allows calling users by dialling their virtual numbers on the keyboard. If no virtual numbers have been configured please leave this option disabled.
- **Slideshow Screen Activation Timeout**: time in seconds the Touch Display should be inactive before the screensaver slideshow stars.
- **Slideshow Transition Time**: time between slides.

PHONE BOOK

The appearance of the phone book is configured in this section. Users can be distributed into groups ordered into levels, up to four levels including the main group.

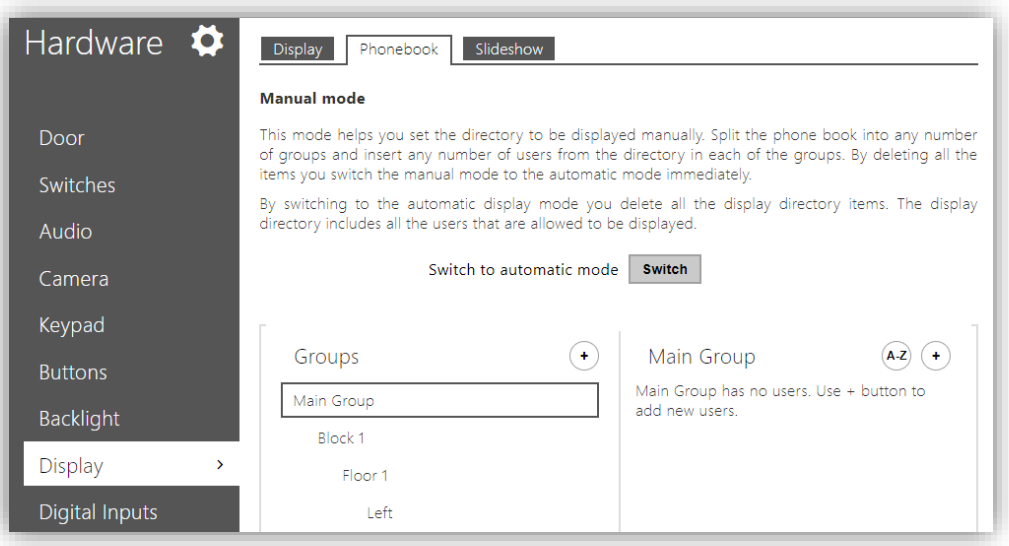

Figure 19 Display.

Once the levels have been defined, the users can be included into them through the configuration area on the right side.

Note: *one user cannot be assigned to more than one group*.

The Switch button toggles between the two user organization modes: manual, from the screen you can change the display of users, and automatic,

Through the button **Switch**, the user displayed mode change between manual, which allows manual configuration of the user's visualization in the directory of the display, and automatic, where the user's visualization will be governed by the configuration option of each of the contacts.

On the other hand, once users have been added up, they can be rearranged by dragging them. If alphabetical order is required, the **A-Z** button can be pressed.

SLIDESHOW

The Touch Display module allows showing a screensaver or a custom slideshow after a time count. For the latter, it is possible to upload up to 8 images from the PC. Once uploaded, they can be rearranged by dragging each of them to the desired position. The images will be scaled to the Touch Display resolution automatically.

3.1.9 ACCESS CONFIGURATION WITH RFID CARD

The ZVP-RFSMN module allows reading RFID access cards. To that end, it is possible to assign cards to the users (up to two cards per user). Moreover, ten additional cards can remain unassigned while two more cards will be aimed for service (one for adding unassigned cards and one for deleting).

There are two ways to configure these cards:

- **By automating the process through an RFID card reader for PC (ZVP-RFUSB)**. This requires installing the card reader driver, available at http://www.zennio.com, and entering the web interface of a Zennio GetFace IP with the ZVP-RFSMN module installed. By pressing on the icon shown in Figure 20, the field will be directly filled in with the code of the card being read by the reader (a green LED will be turned on to indicate that the card can be placed over the reader).

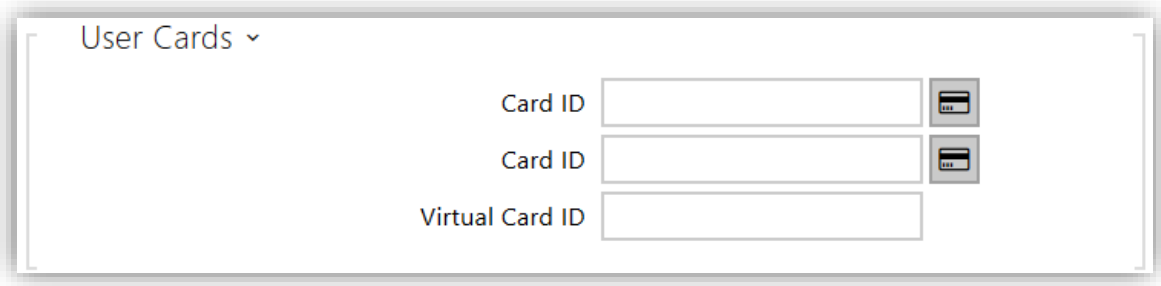

Figure 20 Card reading.

- If no RFID card reader is available for the PC, the assignment can still be performed manually. For adding up a new card, it is necessary to provide its ID. This card ID can be obtained by swiping the card over the reader module and consulting the card reading log in **Status → Access Log**:

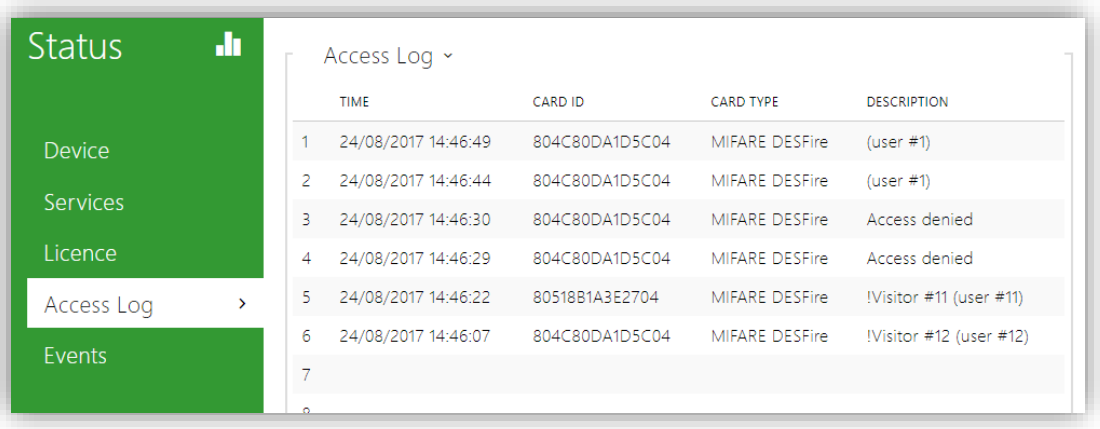

Figure 21 Access Log.

User card registration must be done in **Directory → Users**. The ID just obtained should be entered into the corresponding textbox.

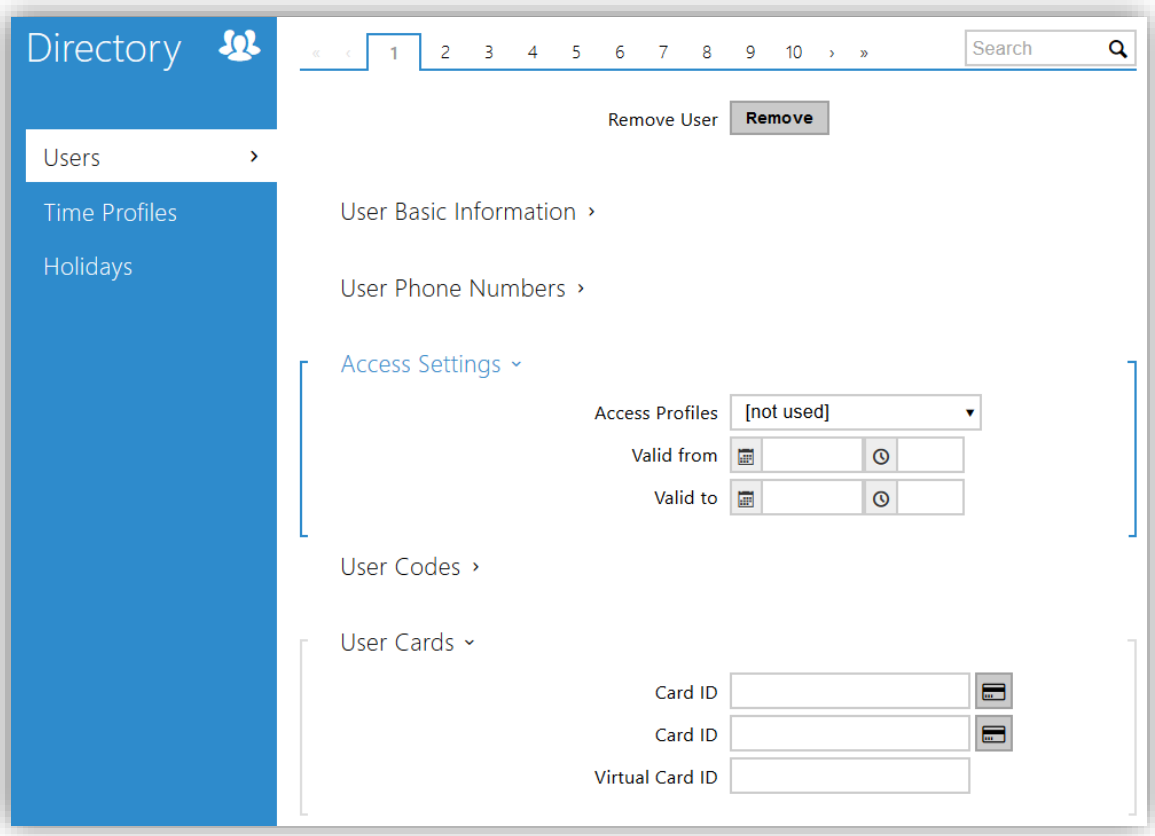

Figure 22 User cards.

Virtual Car ID is the value to resend to Wiegand Group configured.

Card activation time profiles can be configured in **Directory → Time Profiles** (see section 3.2.2.1). If no time profile is configured, make sure that in section **Users → Access Setting**, the access profile **[not used]** is selected.

On the tab **Hardware → Extenders** will be more options for the module configuration.

- **Module name**: sets the module name for logging events from the Bluetooth module.
- **Door**: sets the reader direction (None, Door Entry, Door Exit).
- **Associated switch**: sets the Door Lock Switch or the number of the switch to be activated after user authentication via this module.

  Each RFSMN module can only be associated with one switch, but with 'Automation' it is possible to create a function that allows the activation of other switch based on some criteria. For this purpose, the option "None" of this field could be useful, and thus a concrete switch would not be always activated.
- **Allowed Card Types**: sets the card types supported by the module.
- **Forward to Wiegand output** – set a group of Wiegand outputs that will receive the virtual card IDs configured.

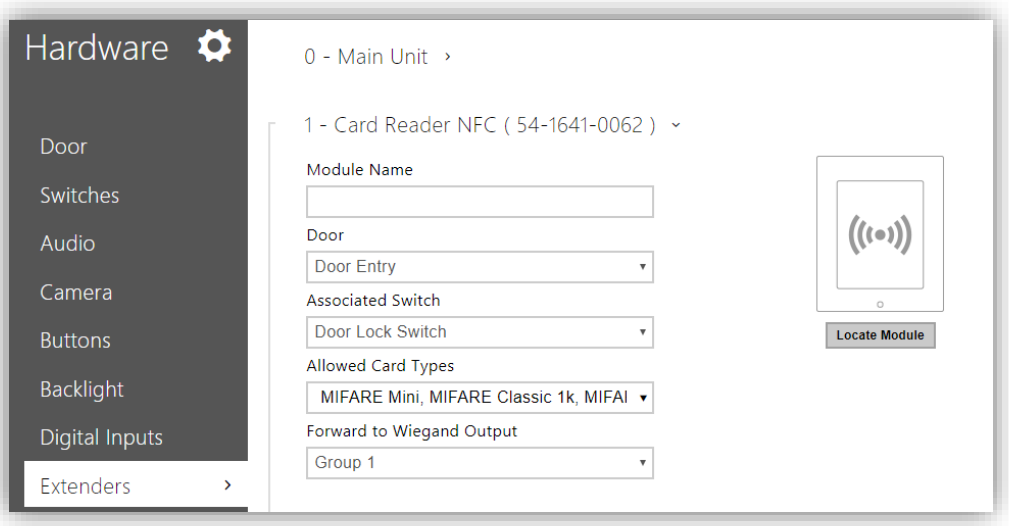

Figure 23 Bluetooth Module Hardware Configuration

3.1.10 ACCESS CONFIGURATION WITH BLUETOOTH MODULE

The module **ZVP-BLUET** provides a safe and convenient way to open doors using mobile devices with Bluetooth technology through **GetFace Key** application. This application is available for Android (version 4.4 or higher) and iOS (version 11.0 or higher) on Google Play and the App Store respectively.

The use of this module is very simple, only needs to be connected to a GetFace IP and paired with a mobile device. For security reasons, the bluetooth communication is **encrypted** using several keys for authentication and pairing.

3.1.10.1 PAIRING PROCESS

Pairing consist on transmission of user access data in GetFace IP to a user personal mobile device.

The pairing is done by introducing the PIN number on the mobile application. The PIN number is generated by the GetFace IP web configuration interface in the tab **Directory → Users → User Mobile Key**.

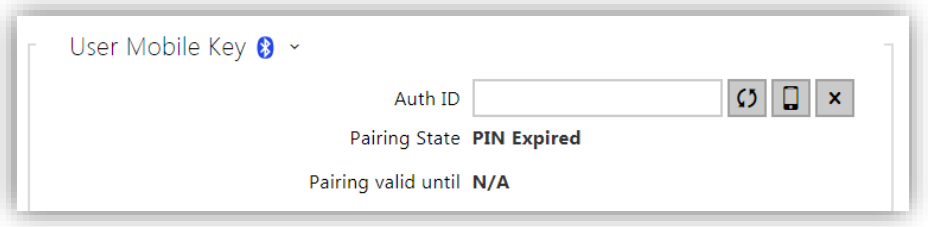

Figure 24 User Mobile Key.

Parameter list:

- **Auth ID**: sets a unique mobile device/user identifier. It is automatically generated for pairing. It can be moved to another user or copy it to another device in the same location.
- **Pairing state**: displays the current pairing state (Inactive, Waiting for pairing, PIN validity expired or Paired).
- **Pairing valid until**: displays the date and time of the generated authorisation PIN validity end.

Pairing process:

1. Click  next to Auth ID to start pairing for the selected user account.
2. A dialogue window with the PIN code is displayed.

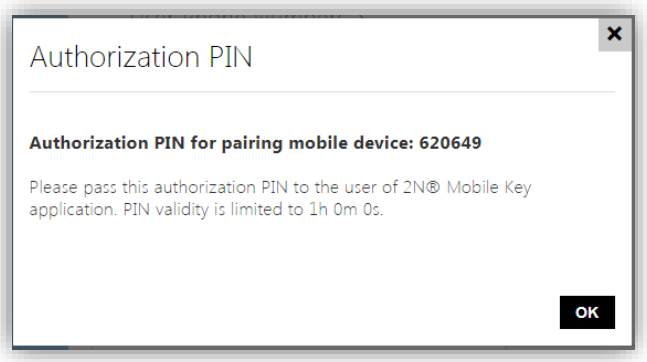

Figure 25 PIN dialogue window

3. Find the appropriate reader in the GetFace Key application and press Start pairing.

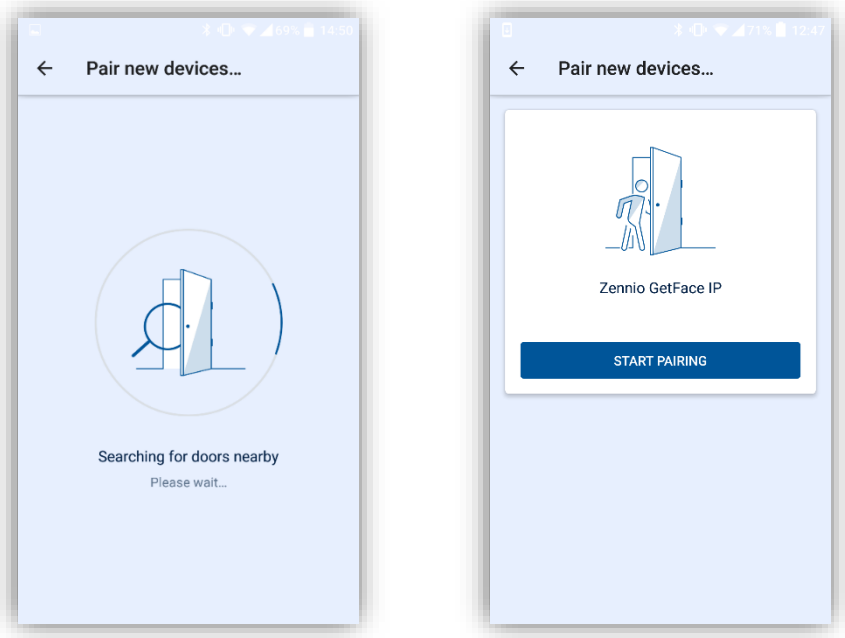

Figure 26 Device searching

4. Enter the code obtained in step 2 into the input field.

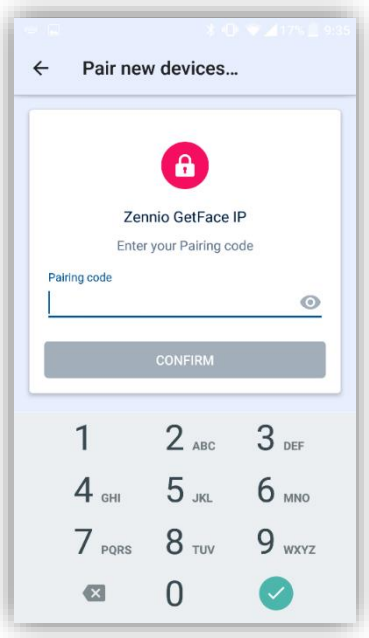

Figure 27 Introduction of the PIN number

5. Pairing is completed.

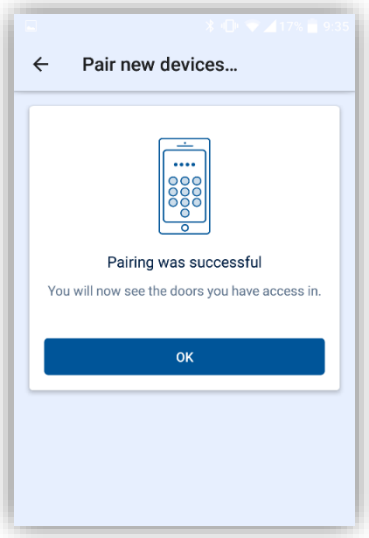

Figure 28 Device paired

The following data is transmitted to a mobile device for pairing:

- Location identifier (see section 3.1.10.2 for details).
- Location encryption key (see section 3.1.10.2 for details).

- User Auth ID.

Once they have been paired, when the device is within the Bluetooth module range, it will appear on the application and just tapping on the button showed on Figure 29, the door will open.

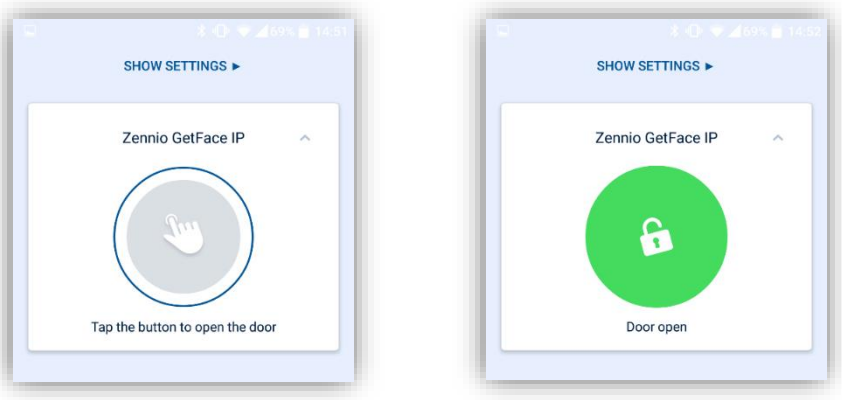

Figure 29 Authentication and opening process

3.1.10.2 OTHER CONFIGURATIONS

On the tab **Services → GetFace Key** there are more options related to the interaction of the mobile application and the Bluetooth module.

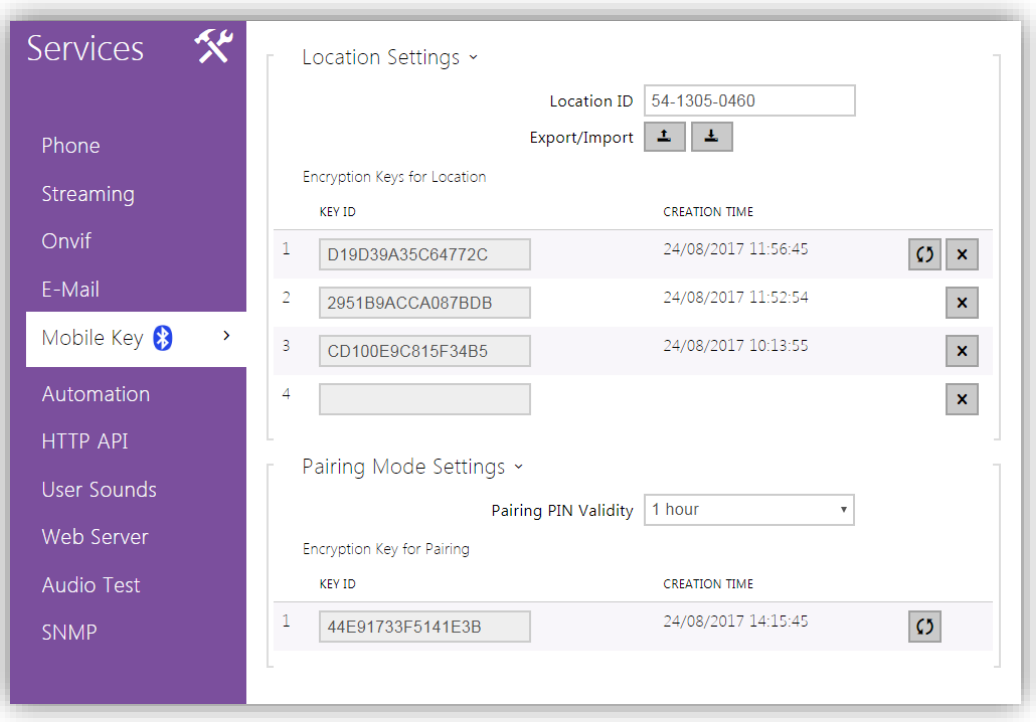

Figure 30 Location and Pairing Mode settings

As already mentioned, Bluetooth communication between GetFace IP and the GetFace Key application is encrypted. To this end, a primary key and up to three secondary keys are available, valid for a certain location.

The primary key is generated automatically upon the intercom first launch and transmitted to the mobile device during pairing.

It is possible to export/import the encryption keys and location identifier to other intercoms. Intercoms with identical location names and encryption keys form so-called **locations**. A user Auth ID can be copied from one intercom to another within a location and it would not be necessary to pair it.

Location Settings:

- **Location ID**: set a unique identifier for the location in which the encryption key set is valid.
- **Export**: push the button to export the location ID and current encryption keys into a file. Subsequently, the exported file can be imported to another device. Devices with identical location IDs and encryption keys form a so-called location.
- **Import**: push the button to import the location ID and encryption keys from a file exported from another intercom. Devices with identical location IDs and encryption keys form a so-called location.

The options for encryption keys are:

- **Restore primary key**  : the original primary key becomes the first secondary key, the first secondary key becomes the second secondary key and so on (if there were 3 secondary keys the oldest is deleted).
- **Delete primary/secondary key**  : delete the corresponding key to prevent the users that still use this key from authentication.

If the key stored on a mobile device is one of the secondary keys, access is allowed and after valid access the key is updated to the primary key in the device.

If the key stored on a mobile device does not match any of the keys (primary or secondary) access is not allowed.

Important: *in the case of loss or theft of a mobile device with access data, proceed as follows:*

- *Delete the Auth ID (see section 3.1.10.1) to prevent access.*
- *Re-generate the primary key (optionally) to avoid misuse of the encryption key stored in the mobile device.*

Pairing Mode Settings:

- **Pairing PIN validity**: set the authorisation PIN validity for user mobile device pairing with the intercom.
- **Encryption key for pairing**: shows the actual key and allows to re-generate it.

3.1.10.3 HARDWARE OPTIONS

On the tab **Hardware → Extenders** will be more options for the module configuration.

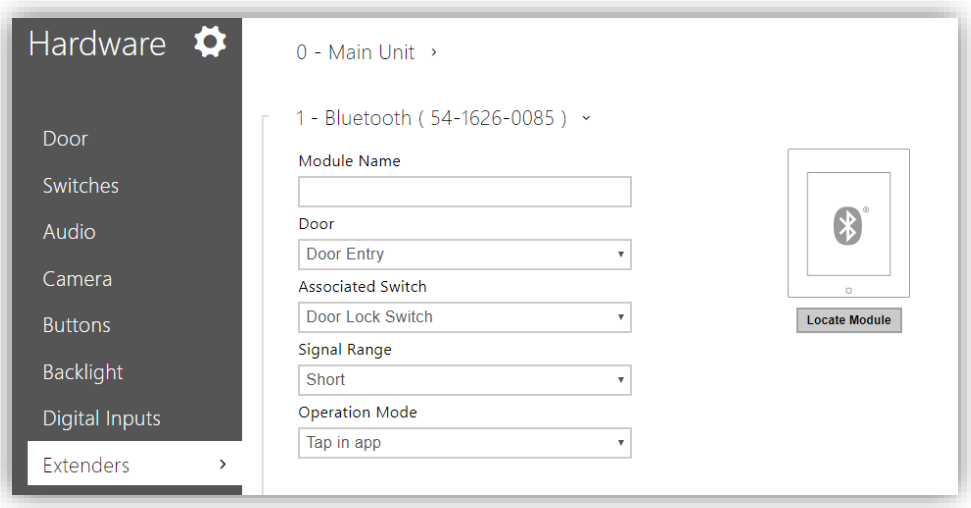

Figure 31 Bluetooth Module Hardware Configuration

- **Module name**: sets the module name for logging events from the Bluetooth module.
- **Door**: sets the reader direction (Door Entry, Door Exit).
- **Associated switch**: sets the Door Lock Switch or the number of the switch to be activated after user authentication via this module.
- **Signal range**: sets the maximum signal range, i.e. the distance within which the Bluetooth module can communicate with the mobile phone.

- **Operation mode**: authentication method for a mobile phone:
  - Tap in app: authentication has to be confirmed by tapping on an icon in the application running in a mobile phone.

3.1.11 ACCESS CONFIGURATION WITH FINGERPRINT MODULE

The ZVP-FINGER module offers a secure and convenient way of authentication and access by reading user fingerprints.

The fingerprint registration for each user can be done on the tab **Directory → Users → User Fingerprints**.

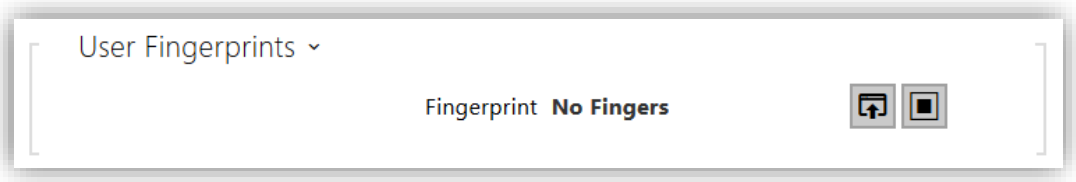

Figure 32 User Fingerprints.

The steps to follow are:

1. Press one of the two buttons:
   a. Press  to enter the fingerprint using a USB reader.
   b. Press  to enter the fingerprint using the ZVP-FINGER module itself. This option is only available for firmware versions 2.23 or higher.
2. Select the finger and press “Scan Finger”.

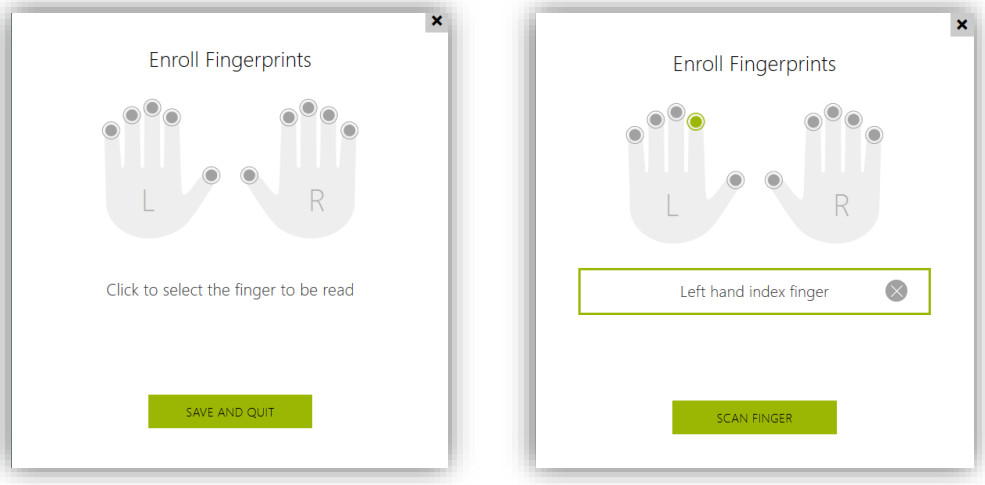

Figure 33 Fingerprint selection.

3. Place the selected finger on the reader. This process is repeated three times for greater precision.
   If the reading is correct, the fingerprint appears in green. If it is wrong it appears in red and step 2 must be repeated.

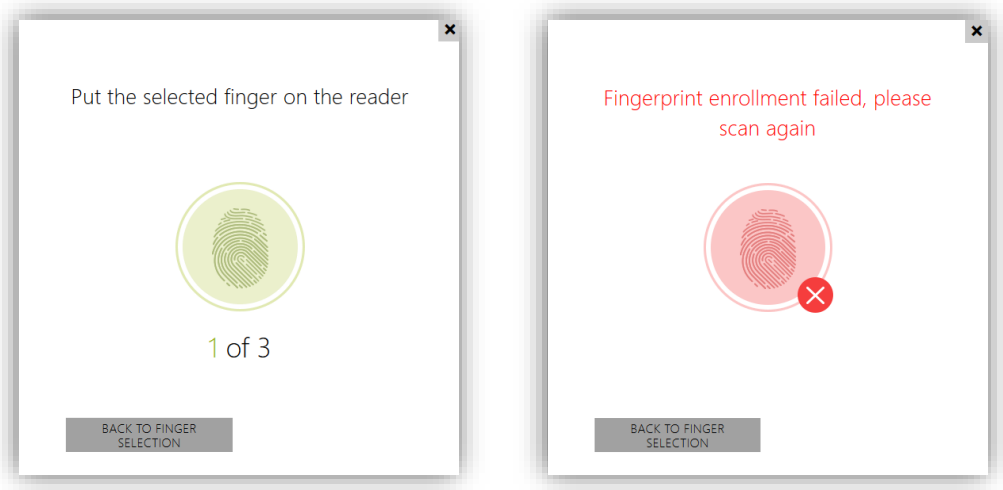

Figure 34 Fingerprint reading.

4. When the reading has been successful, press "Done" to confirm.

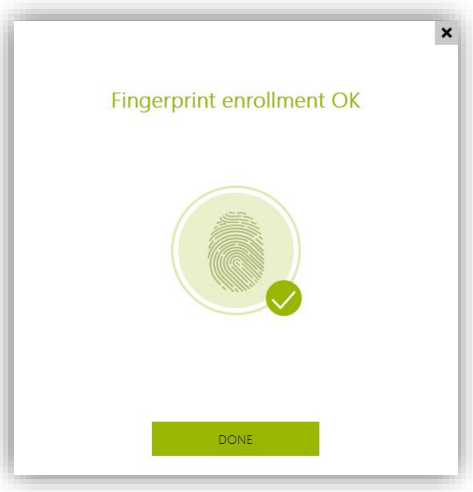

Figure 35 Fingerprint reading successful.

5. Next, press for selecting the acction to be executed with the finger. The available options are:

   - Open door.
   - Silent Alarm.
   - F1 automation.
   - F2 automation.

Several funtions can be selected for each fingerprint.

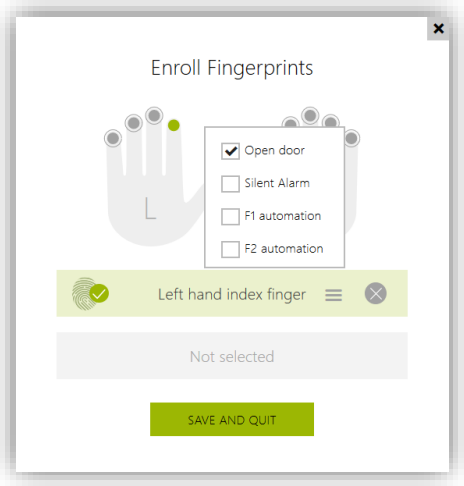

Figure 36 Function associated with the fingerprint.

Up to two fingerprints per user can be registered.

On the tab **Hardware → Extenders** will be more options for the module configuration.

- **Module name**: sets the module name for logging events from the Bluetooth module.
- **Door**: sets the reader direction (Door Entry, Door Exit).
- **Associated switch**: sets the Door Lock Switch or the number of the switch to be activated after user authentication via this module.

3.1.12 MAGNETIC INDUCTION LOOP CONFIGURATION

ZVP-LOOP is a module designed for people with hearing impairment. It allows transmitting an audio signal directly to a hearing aid device through a magnetic loop. It also shows oversize visual signals to improve the communication.

This module can be configured in **Hardware → Extenders**, where the signal power level should be adjusted to the required value.

3.2 ADVANCED SETTINGS

These fields are not mandatory for a standard configuration, but they are detailed in case the end requires any of the extra features.

3.2.1 STATUS

The **Status** window shows status information concerning Zennio GetFace IP. It consists of the following sections.

3.2.1.1 DEVICE

Shows the main aspects about the device tab, including hardware, firmware and bootloader versions, as well as **Product Name**, **Serial Number**, **Up Time** and **Power Source**. There is also a button to **Locate Device**. By clicking on it, the device reproduces a short beep and blinks.

The **Device Features** drop-down section details the module features and whether the base unit incorporates a camera.

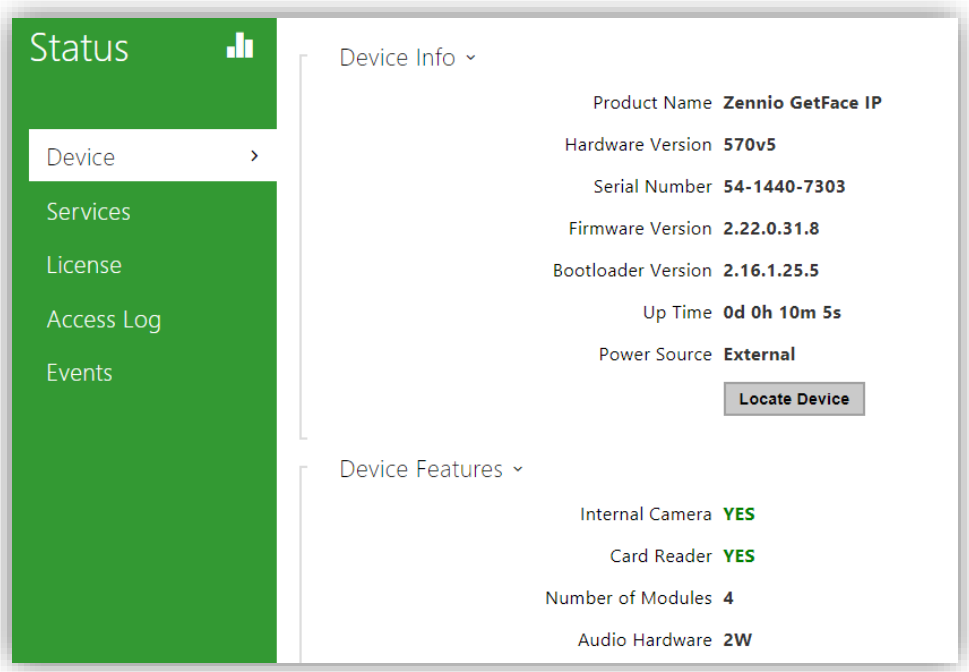

Figure 37 Device.

3.2.1.2 SERVICES

It shows basic information about the device network and the service status.

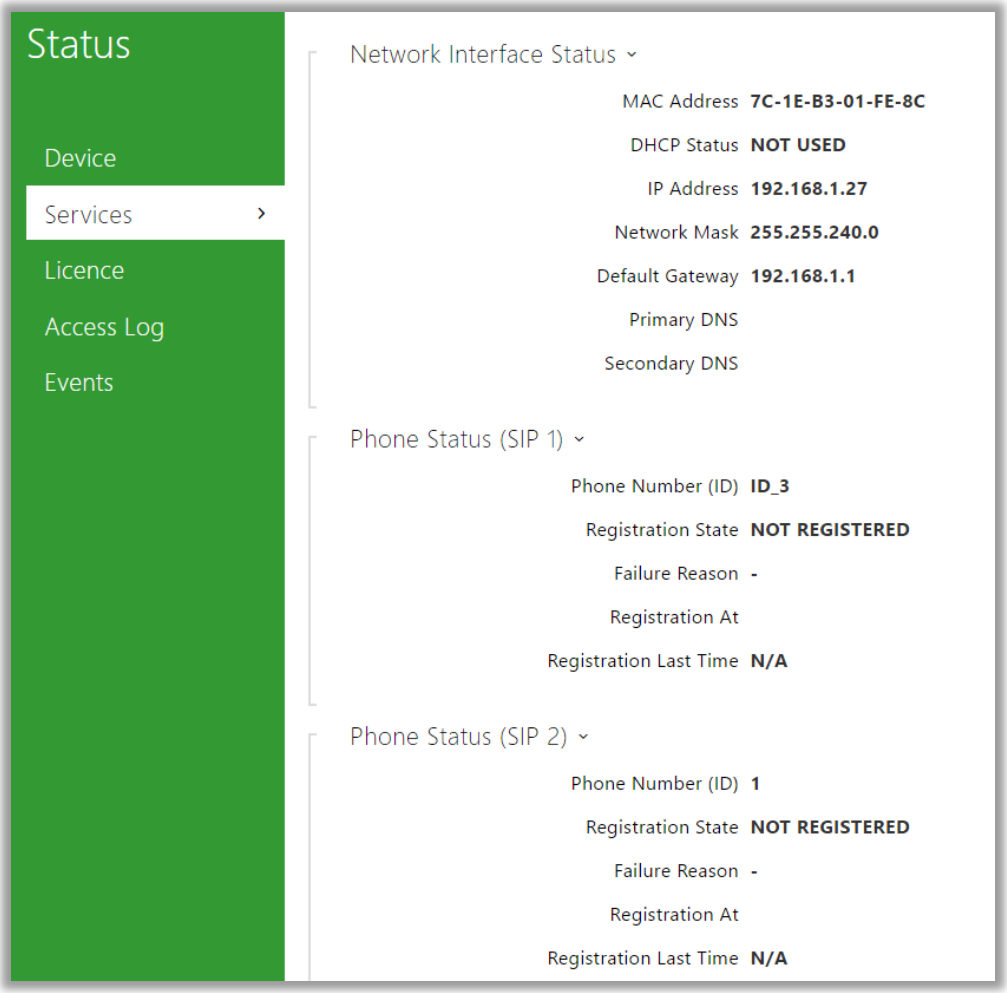

Figure 38 Services.

3.2.1.3 EVENTS

It shows a date-ordered register of the last events that have taken place.

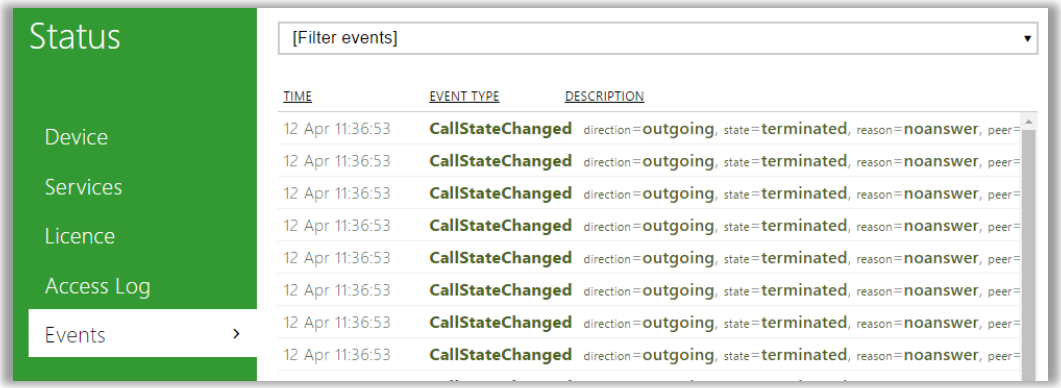

Figure 39 Events.

3.2.2 DIRECTORY

Homes connected to the video intercom system are configured in **Directory.** The following advanced features can be set up from this window:

3.2.2.1 TIME PROFILES

Time profiles allow restricting the use of the RFID cards and the numeric codes. In particular, it is possible to define time bands for:

- Locking all incoming calls for a specific user.
- Locking the door opening.
- Locking access via RFID cards.

Up to 20 different profiles with different active hours for each day of the week can be set. The following parameters must be set:

- **Profile Name** (optional).
- **Profile Time Sheet** for each day of the week (holidays included).

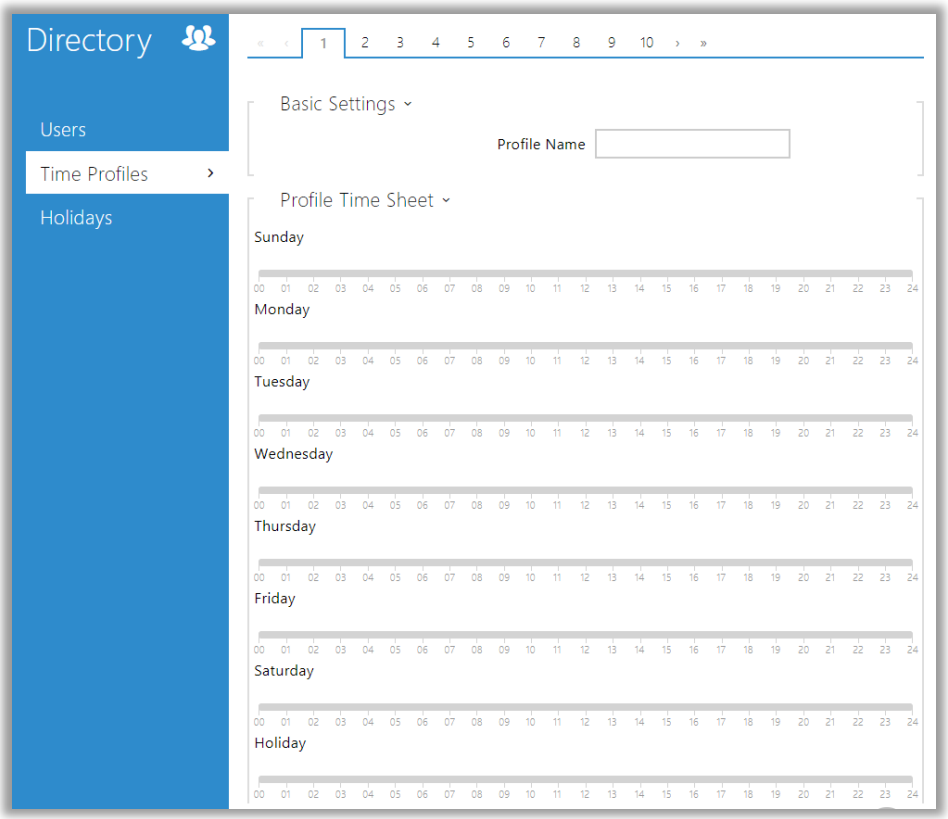

Figure 40 Time Profiles.

3.2.2.2 HOLIDAYS

Fixed (yearly) and variable holiday dates are configured in the **Holidays** tab so date-depending time profiles can be defined.

By clicking on a specific day, the box will be highlighted in green colour, which shows it is a **fixed holiday**. By clicking on the box again, it will be highlighted in blue colour, thys showing it is a **variable holiday**. A third click on the box will discard the current configuration as a holiday.

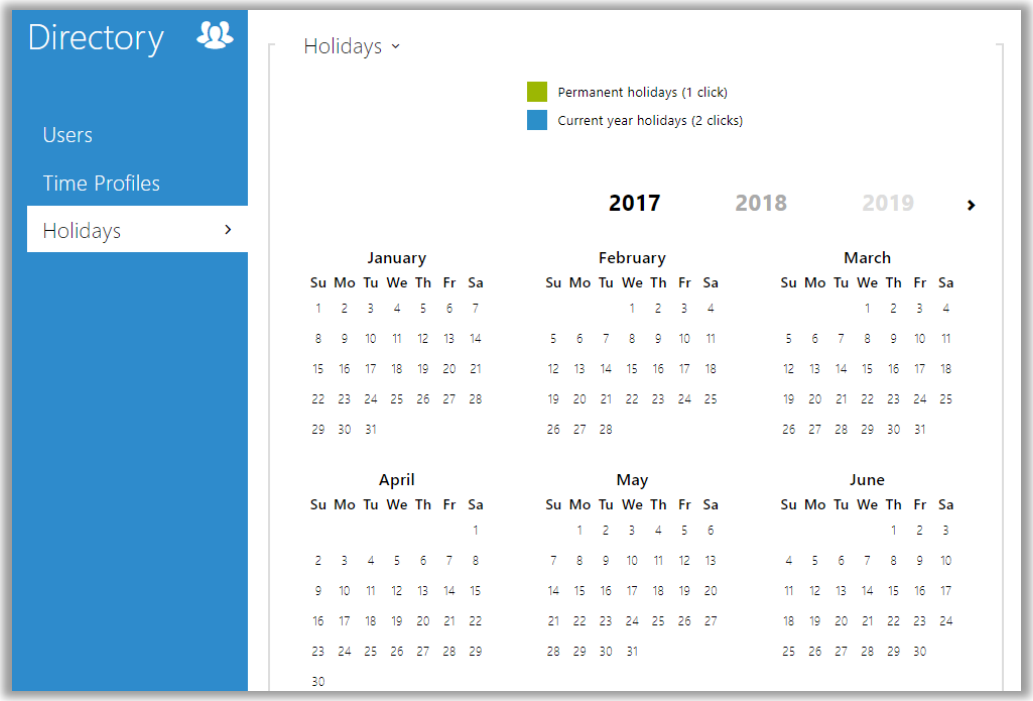

Figure 41 Holidays.

3.2.3 SERVICES

The **Services** section provides the following advanced settings:

3.2.3.1 E-MAIL

Zennio GetFace IP users can be notified of all missed or successful calls via e-mail, provided that an Internet connection is available (e-mails about accesses can also be sent when using the module ZVP-RFSMN). Also, if the video intercom is camera-equipped, one or more snapshots taken during the call or the ringing can be attached.

The video intercom sends e-mails to each user for whom a valid e-mail address has been included in the user list. If the **E-Mail** field is blank in the user list, e-mails are sent to the default address.

SMTP

This section allows configuration of the SMTP server.

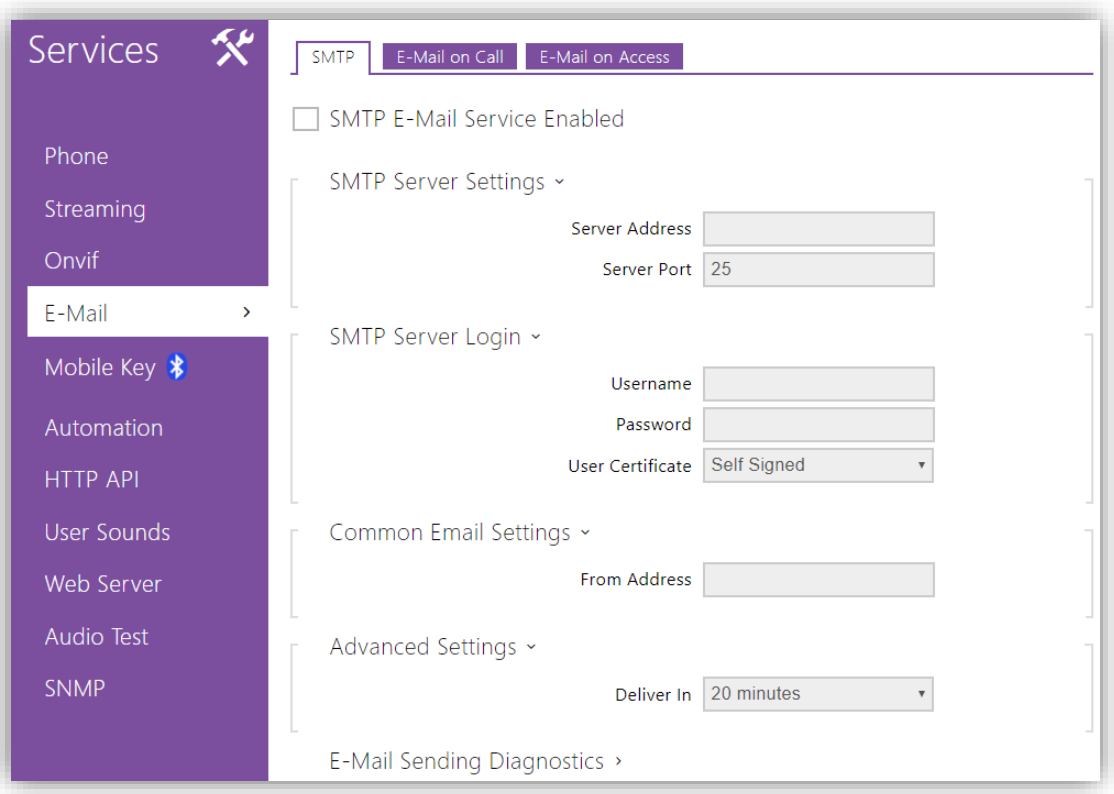

Figure 42 SMTP.

- **SMTP Server Settings**: defines the address and the port of the SMTP server the e-mails will be sent to.
- **SMPT Server Login**: allows entering a valid log-in user name if the SMTP server requires authorisation. Otherwise, the field should remain blank. A **user certificate** and a **private key** can be defined to encrypt the communication between the video intercom and the SMTP server.
- **Common E-mail Settings**: configures the sender address for all outgoing e-mails.
- **Advanced Settings**: defines the e-mail delivery timeout in case the SMTP server is not available.

- **E-Mail Sending Diagnostics**: allows testing the e-mail sending functionality and the current configuration by sending a test e-mail to a defined address. Please enter an e-mail address and click on the **Apply and Test** button. The current sending status is then shown to allow the detection of issues.

E-MAIL ON CALL

This tab shows the configuration of the e-mail to be sent in the event of a call:

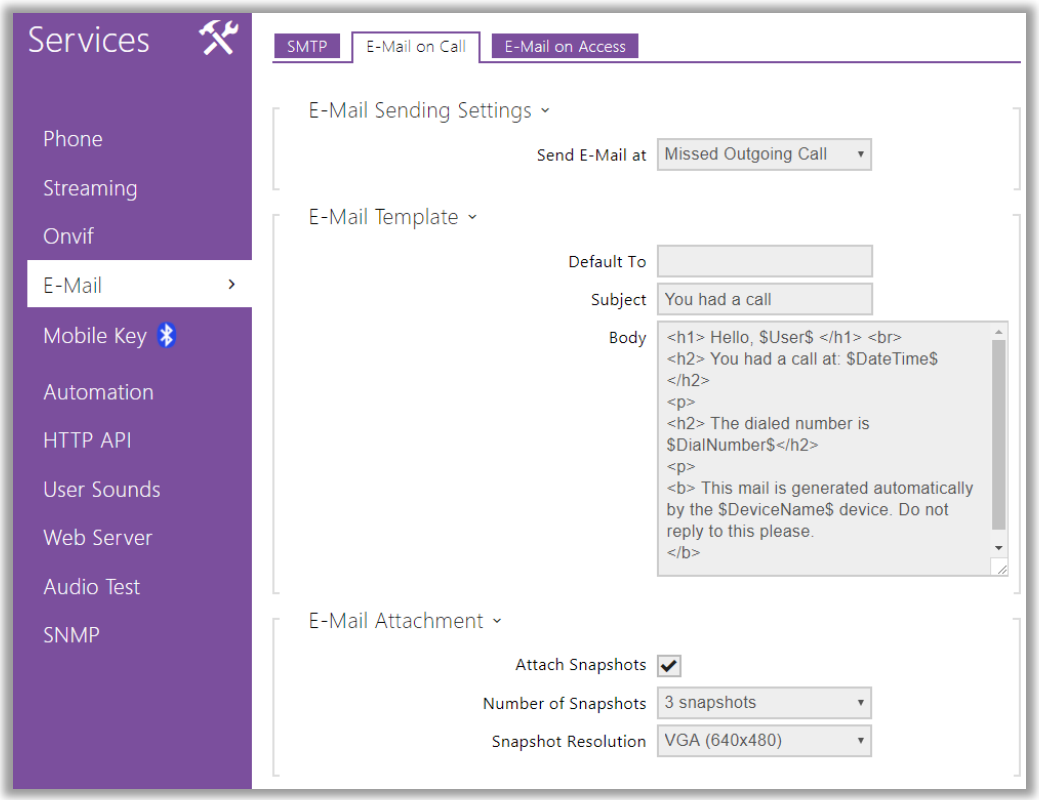

Figure 43 E-Mail on Call.

- **E-Mail Sending Settings**: sets the sending type.

- **E-Mail Template**: determines the message recipient, subject and body.

  Although the video intercom sends these e-mails to the address defined in the user phone list, in case such field is blank, the mail will be sent to the **Default to** address (empty by default). In case this field is also blank, the e-mail will eventually not be sent. It is possible to configure multiple e-mail addresses by separating them by commas or semicolons.

The e-mail body can contain **HTML tags** as well as special symbols to represent the username, date, time, video intercom ID or called number, which will be replaced by the actual values before sending.

- **$User$**: user name.
- **$DateTime$**: current date and time.
- **$DialNumber$**: dialled number.

- **E-Mail Attachment**: enables attaching pictures taken by the video intercom during the dial or in the course of the call. The number of shots and their resolution can be parameterised.

E-MAIL ON ACCESS

This tab shows the configuration of the e-mail to be sent in the event of an access.

The parameters are similar to the ones in the previous tab.

3.2.3.2 AUTOMATION

Automation allows associating system events (key presses, RFID card readings, changes in a digital input, etc.) with specific actions (digital output activations, user audio playback, calls, etc.). Moreover, the action execution can be restricted by selected conditions (time profiles, input status, etc.).

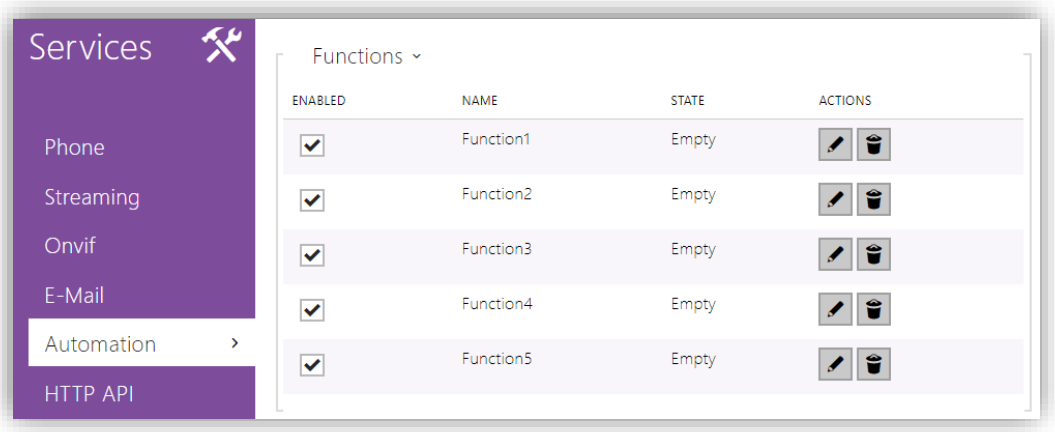

Figure 44 Automation.

Up to **five functions** can be set, which can be configured in an interface available by clicking on the 'Edit' button of the corresponding function (represented by a pencil icon). Each function combines events, actions and conditions. Up to 30 conditions can be configured.

Note: *After the device initialization, the status of the inputs will be automatically checked in the Automation.*

3.2.3.3 WEB SERVER

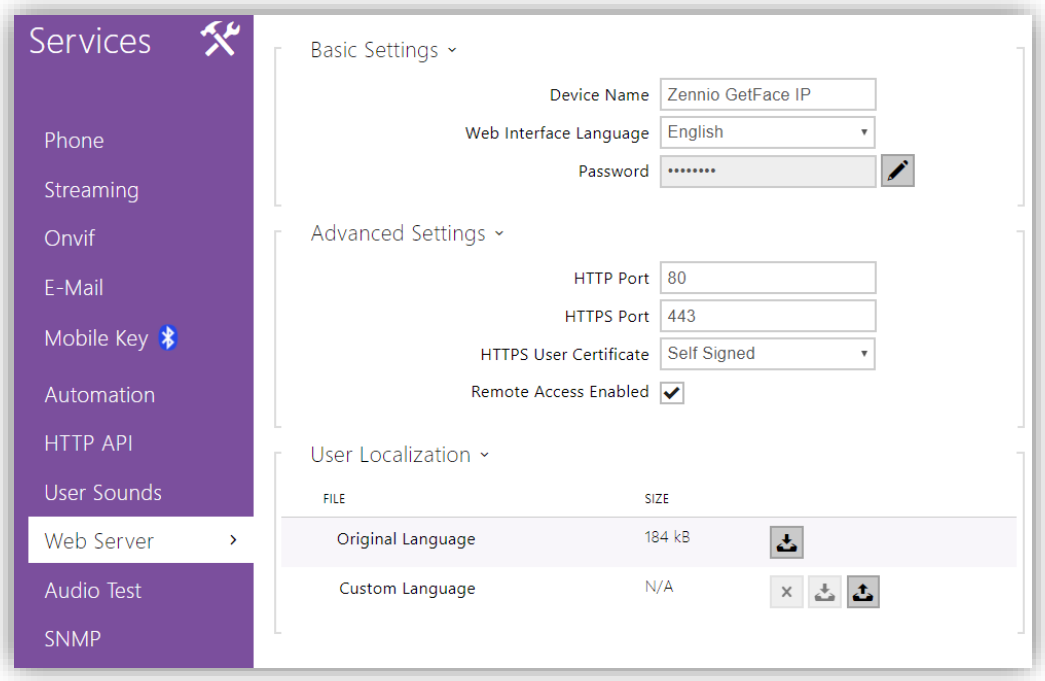

Figure 45 Web Server.

The login username and password of the Zennio GetFace IP web interface (by default, **admin** and **zennio** respectively) can be modified from this section. The language of the interface can be customised too.

3.2.4 HARDWARE

The following items can be configured in the **Hardware** section:

3.2.4.1 AUDIO

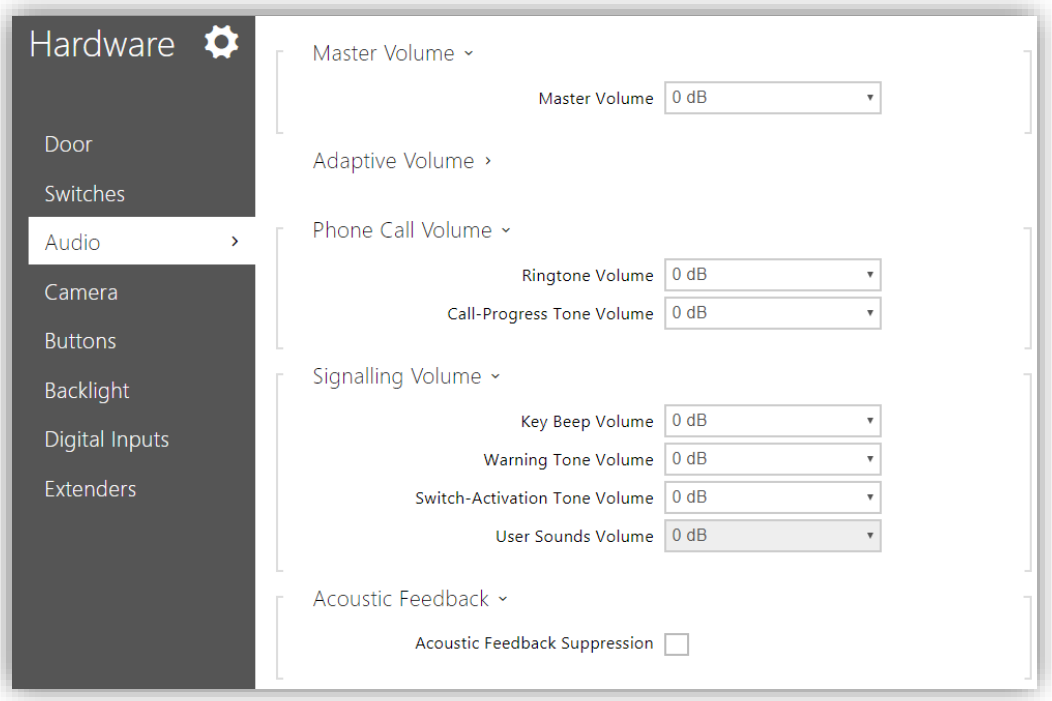

Figure 46 Audio.

- **Master Volume**: audio volume level for both calls and signals (ringtones).
- **Adaptive Volume**: if enabled, a **Maximum Gain** and a **Sensitivity Threshold** can be parameterised. The latter defines the volume level that will trigger the adaptive volume increase. On the other hand, even if this option is left disabled, the **Current Noise Level** and the **Current Adaptive Gain** can be consulted here.
- **Phone Call Volume**: defines the volume of the ringtones as well as of the call-progress tones, i.e., of the dial and busy-line tones.
- **Signalling Volume**: sets the volume of the key beeps, the warning tones and the switch-activation tone, as well as the user sounds to be played back.

- **Acoustic Feedback**: allows eliminating feedback between the intercom speaker and the internal unit. It is recommended to have this parameter active only when occurring sound coupling problems.

3.2.4.2 CAMERA

The Zennio GetFace IP video source can be configured in this section, together with the video output settings.

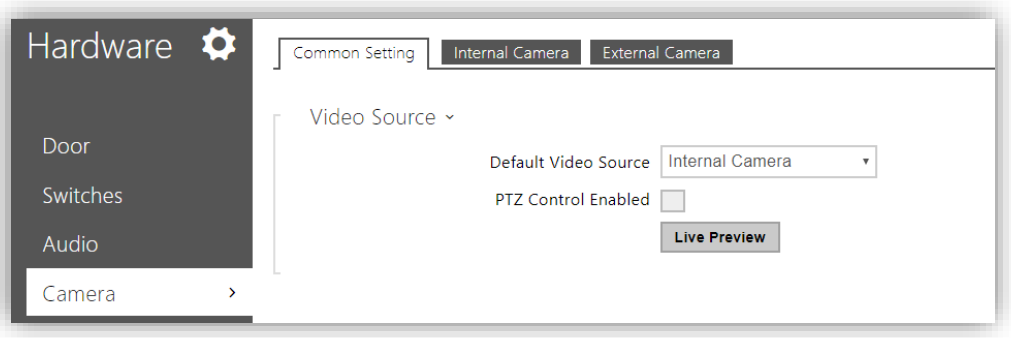

Figure 47 Camera.

COMMON SETTINGS

The default video source is set in this tab: either an **internal** camera (the on-board camera of Zennio GetFace IP) or an **external** IP camera can be configured. Once the default video source is selected and the configuration has been set, a **live preview** can be performed.

Note: *in case the device does not include its own camera (ZVP-WOCAM model), setting an internal camera will not be possible.*

INTERNAL CAMERA

The video output image settings are configured in the following section:

- **Brightness Level**.
- **Colour Saturation**.
- **Camera Mode**: allows reducing the effect of direct sun light or artificial light sources over the image, depending on where Zennio GetFace IP will be installed (indoor or outdoor).

- **Day/Night Mode**: sets the day/night modes of the camera. It is possible to set one particular (fixed) mode or let the device automatically switch between them depending on the ambient light level.

- **Current Mode**: displays the currently selected camera mode (day/night).

- **IR LED Brightness Level**: defines the brightness level of the infrared LED in the range 0-100% with steps of 25%. If set to automatic, the infrared light will be activated by Zennio GetFace IP in case the ambient light is low and the camera is being used.

- **Current IR LED Brightness Level**: displays the current IR LED brightness level. This level may drop below the configured value in the event of an excessive power consumption (usually when multiple extenders are connected –see section 3.2.4.6– and the PoE source is used).

- **Live Preview**: shows the video camera images with the current configuration.

3.2.4.3 KEYBOARD

The numeric and telephone keypads are configured in this section.

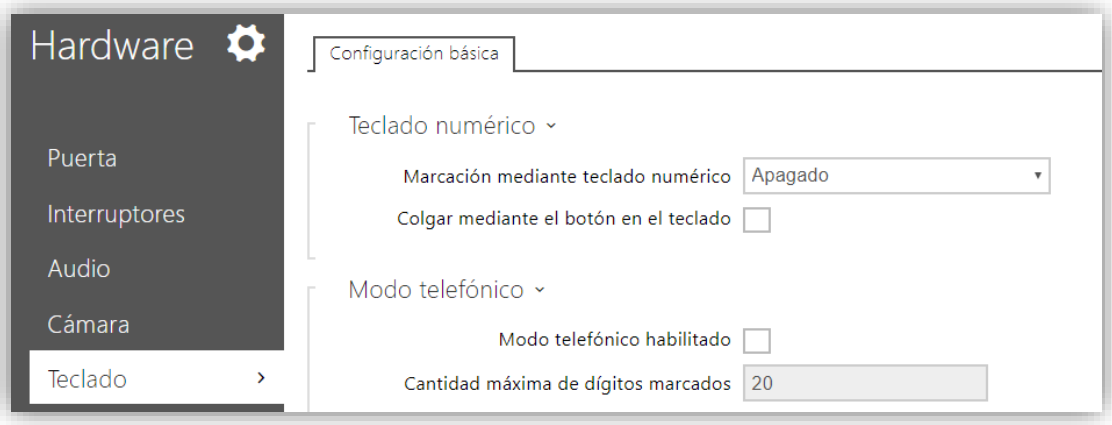

Figure 48 Keyboard.

- **Dial by Numeric Keypad**: allows calling users from the phone book by either dialling their position number or by using their virtual number. Pressing the * (**asterisk**) key is required for confirmation.

- **Hangup by Numeric Keypad**: allows termination of the active call by pressing the # (**pad**) key. If the call was started by a quick dial button, the same button needs to be pressed again.

3.2.4.4 BACKLIGHT

Zennio GetFace IP allows restricting the level of the device lower light and of the signalling LED depending on whether it is day-time or night-time. Also, the current value can be verified in this section.

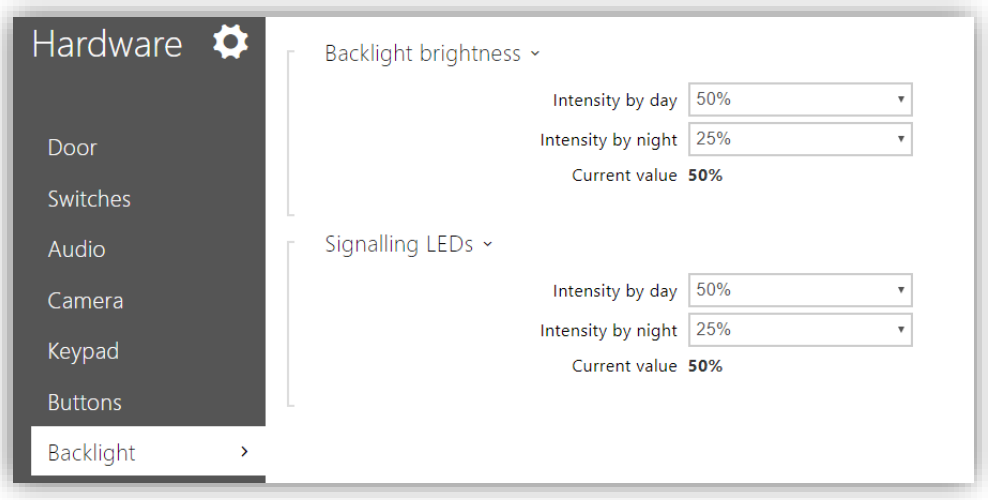

Figure 49 Backlight.

3.2.4.5 DIGITAL INPUTS

Parameters associated with the digital inputs are configured in this section.

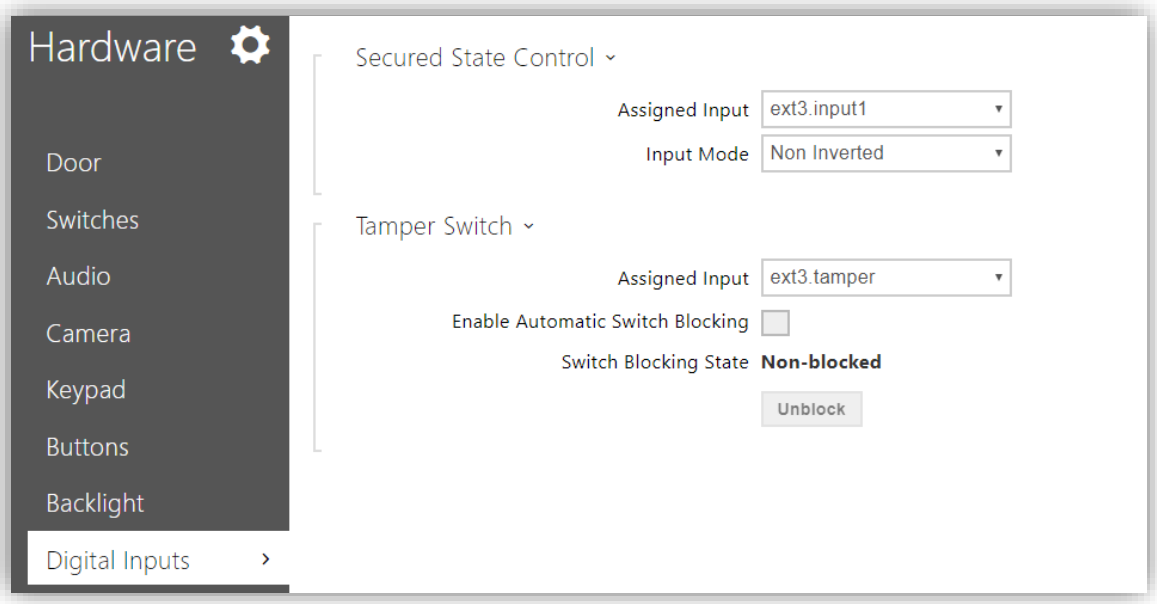

Figure 50 Digital inputs.

- **Secured State Control**: defines which of the inputs will be used for the secured state detection, which is indicated by Zennio GetFace IP through a LED. This

parameter can be applied to pushbuttons for door opening. **Input Mode** allows setting whether this input is inverted or not.

- **Tamper Switch**: defines which ZVP-INOUT module inputs will be used as the tamper switch.

- **Door State**: sets which of the inputs will define the door state. It is possible to detect unauthorised door openings as well as when the door remains open for too long by defining a custom timeout.

3.2.4.6 EXTENDERS

Modules connected to the base unit are shown in this window. These modules are connected in series so each of them has its own number according to its position in the line. The base unit, as a special module, will have number 0.

3.2.5 SYSTEM

The main system configuration is established in the following sections.

3.2.5.1 NETWORK

Parameters related to the device network interfaces are set in this section.

BASIC

Zennio GetFace IP works by default with a static IP. However, it is possible to configure it to work with a DHCP server.

Being the DHCP option deactivated, it is possible to configure the following options:

- **Manual Settings**: allows setting a static IP address, the network mask and the default gateway. Also, a primary and a secondary DNS server can be configured.

- **Network identification**: sets the device hostname (optional).

- **VLAN Settings**: allows enabling a virtual local area network (VLAN).

- **LAN Port Settings**: sets the desired port mode ("Autonegotiation" or "Half Duplex").

- **Tools**: allows monitoring the network and device status, as well as the latency of the responses.

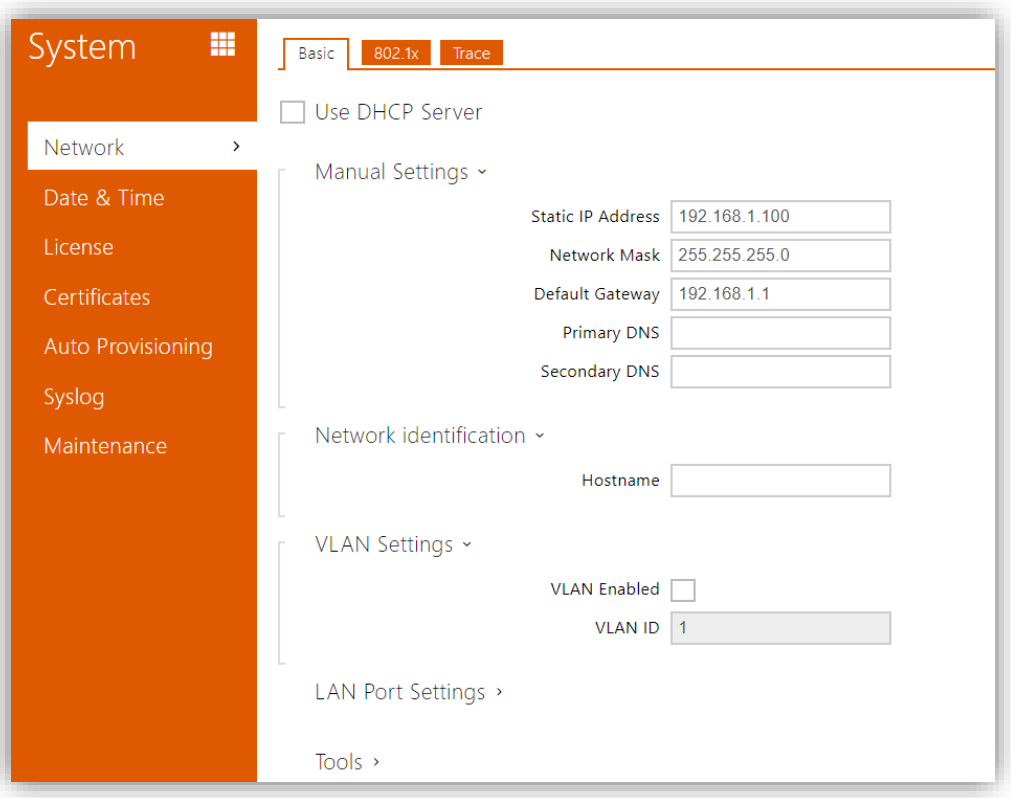

Figure 51 Network.

In case of **enabling the DHCP server**, the manual network settings will not be available.

3.2.5.2 DATE & TIME

Date and time can be configured from this section.

It is possible to synchronise the date and time according to those from the PC (browser). Once synchronised, the **Time Zone** must be set, so winter/summer time shifts are performed according to the Zennio GetFace IP time zone.

It is also possible to define the time zone rules manually through the **Time Zone Rule** parameter.

Finally, a **NTP server** can be defined so the device date and time get synchronised by means of an Internet NTP server, whose URL or IP must be specified.

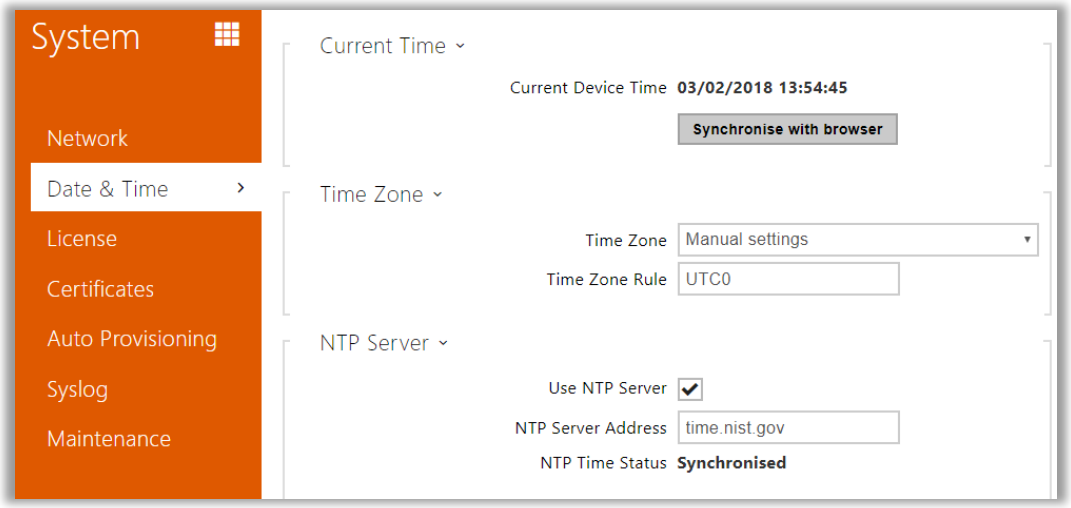

Figure 52 Date and Time.

3.2.5.3 AUTO PROVISIONING

Firmware and configuration updates in Zennio GetFace IP can be performed either manually or automatically, from a TFTP / HTTP.

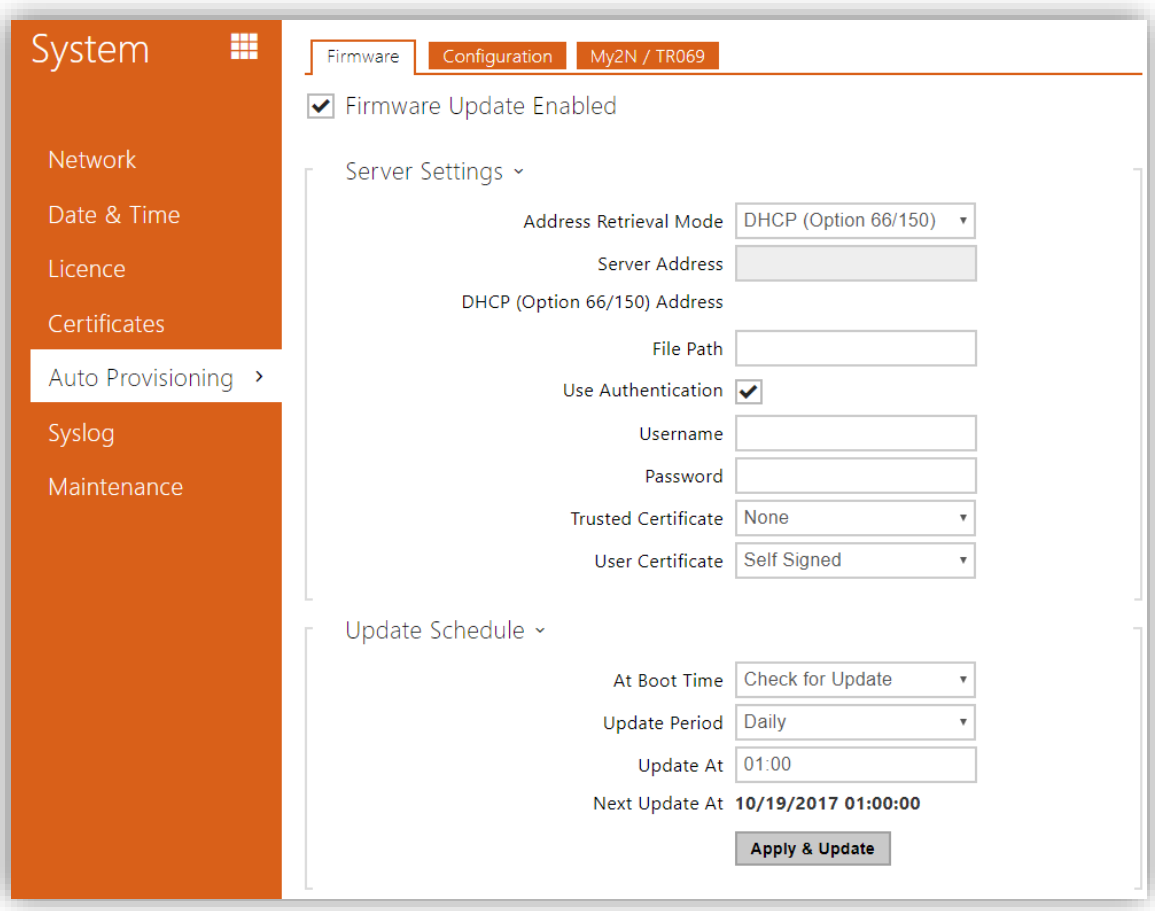

Figure 53 Auto Provisioning.

FIRMWARE

This tab configuring automatic firmware updates.

- **Server Settings**: parameters for connecting to the server.
- **Update Schedule**: frequency of the updates. This section also shows when the next update is expected.
- **Update Status**: date of the last update.

CONFIGURATION

This section includes quite the same settings as the **Firmware** section, but referred to device configuration updates.

3.2.5.4 MAINTENANCE

This section allows performing general maintenance operations. It also provides general information about it.

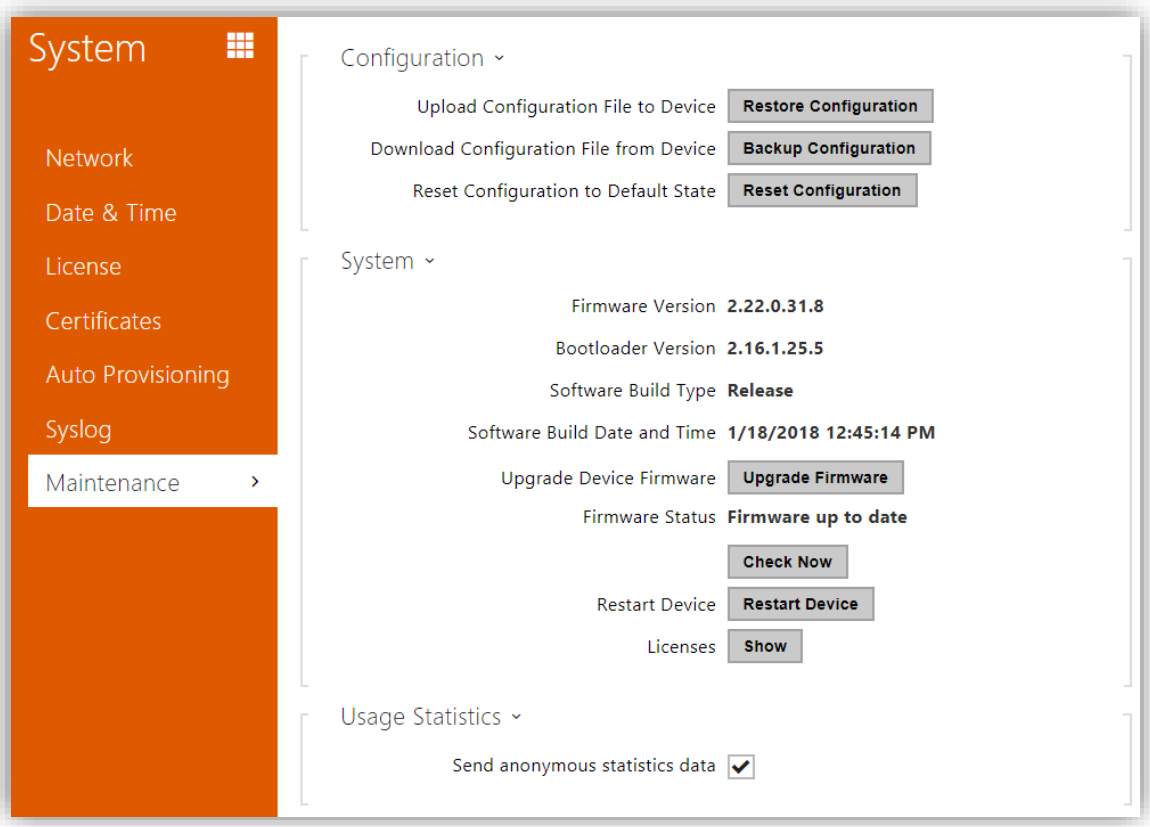

Figure 54 Maintenance.

- The **Configuration** tab allows:
  - Uploading a configuration back-up file to the device.
  - Downloading a configuration back-up file from the device.
  - Resetting the Zennio GetFace IP configuration to the default state.
- The **System** tab allows verifying and managing the firmware and system versions:
  - Firmware Version.
  - Bootloader Version.
  - Software Build Type.
  - Software Build Date and Time.

  In addition, this section allows **manually upgrading the device firmware** by uploading a firmware file, as well as looking for available firmware updates and **restarting the device**.

Join and send us your inquiries
about Zennio devices:
http://support.zennio.com

Zennio Avance y Tecnología S.L.
C/ Río Jarama, 132. Nave P-8.11
45007 Toledo. Spain.

Tel. +34 925 232 002.

www.zennio.com
info@zennio*.com*