APPENDIX LIST

IPer com

INTEGRATED IP
VIDEO DOOR PHONE
SYSTEMS

IF YOU LOVE YOUR BUILDING

urmet

APPENDIX A: 2Voice and IPerCom apartment station features

Below is a table with the features supported and not supported by the IPerCom and 2Voice apartment stations. Remember that adding a riser column of 2Voice apartment stations to an IPerCom system is only possible through the *IPerCom-2Voice Gateway* Ref. 1083/59.

Function	2Voice apartment station	IPerCom apartment station
Call from IPerCom calling station	**Yes**	**Yes**
Call from 2Voice calling station	**Yes**	**No**
Call from IPerCom apartment station	**Yes**	**Yes**
Call from 2Voice apartment station	**Yes (*)**	**No (**)**
Call to IPerCom *Switchboard*	**Yes**	**Yes**
IPerCom calling station auto-on	**Yes**	**Yes**
2Voice calling station auto-on	**Yes**	**No**
RTSP camera auto-on	**No**	**Yes**
Relay activation on Ref. 1060/84	**Yes (#)**	**Yes**
Relay activation on Ref. 1083/80	**Yes**	**No**
Call forwarding to smartphone	**Yes (with 1083/58-58A-83)**	**Yes**
Panic alarm	**Yes (on compatible apartment stations)**	**Yes**
Emergency call	**Yes (##)**	**Yes**
Address book	**No**	**Yes**

Table 1: differences of functions between IPerCom and 2Voice Door Phones

(*): only if the calling and called apartment stations are on the same stairs of the gateway and if the apartment stations are appropriately programmed. On different stairs, it is necessary to pass through the IPerCom *Switchboard*.

(**): only through the IPerCom *Switchboard*.

(#): only with some apartment station buttons and in particular conditions (see booklets for individual 2Voice apartment station).

(##): unlike IPerCom apartment stations, 2Voice apartment stations ring when an emergency call is sent from the IPerCom *Switchboard*.

It is also remembered that:

- if an audio apartment station (IPerCom or 2Voice) with call forwarding function enabled is called from an IPerCom calling station, the streaming video of the calling station is sent to the smartphone/tablet;

- if a smartphone/tablet via the *CallMe* app calls an apartment station (IPerCom or 2Voice) with the call forwarding function enabled, the call is not forwarded to other smartphones / tablets.

APPENDIX B: 2Voice and IPerCom calling station features with *Switchboard*

The following table shows the differences in functions between the 2Voice and IPerCom devices with an IPerCom switchboard.

Function	**2Voice device**	**IPerCom device**
Auto-on from *Switchboard*	2Voice secondary calling stations (connected to the IPerCom Gateway): **No**	IPerCom calling stations (any): **Yes**
Interception of calls from IPerCom *Switchboard* located on 2Voice stairs node	Calls from 2Voice secondary calling stations (connected to the IPerCom Gateway): **No**	Calls from IPerCom secondary calling stations: **Yes**

Table 2: differences of functions with IPerCom Switchboard

APPENDIX C: IPerCom priority calls

Calls within an IPerCom system are shown in ascending order of priority:

- auto-on;
- intercom (call between two apartments);
- call from calling stations/*Switchboard* to apartment or from apartment to *Switchboard*;
- emergency call.

Each call has two basic parameters (which can be set from the "*System*" tab of the *configurator*):

- Maximum answer response time, after which the call ends (if the user does not answer). Default setting: 60s.
- guaranteed conversation time, after which the call can be interrupted by a call with the same priority (higher priority calls can interrupt calls already in progress at any time). Default setting: 30s.

In the absence of interruptions, the conversation phase of a call lasts a maximum of 10 minutes.

Even an auto-on without interruptions has a maximum duration of 10 minutes (even if two-way audio is activated within 10 minutes).

About call management, maximum answer response time, guaranteed conversation time and busy status in the 2Voice system, please refer to the applicable system manual available on the website ***www.urmet.com***

Remember that if the *Switchboard* has already established a conversation with a 2Voice apartment station and you want to call another 2Voice apartment station on the same column (stairs), having put the first conversation on hold, this is not possible even after the guaranteed conversation time. You need to close the first call and then make the second, otherwise an engaged message will continue to appear on the *Switchboard*.

APPENDIX D: Proximity keys compatible with IPerCom devices

The following table shows, for each IPerCom device which integrates a proximity key reader, the types of keys compatible with the reader:

	125KHz	MIFARE	125KHz/MIFARE	MIFARE PLUS
Call Module 1060/12-13-17-18	Yes	No	Yes (*)	No
Call Module 1060/23	No	Yes	Yes (***)	Yes
Modular Entry Panel with 1060/48	No	Yes	Yes (**)	Yes
Modular Entry Panel with 1060/48 Touch	No	Yes	Yes (**)	Yes
Call Module 1060/16	No	Yes	Yes (***)	Yes
Entry panel 1060/21	No	Yes	No	No
Key Reader 1060/86	No	Yes	Yes (***)	Yes
Key Reader 1060/45	No	Yes	Yes (***)	Yes

Table 3: types of keys recognized by the various IPerCom devices

(*): with dual technology keys (125KHz/Mifare), only the 125KHz component is read;

(**): with dual technology keys (125KHz/Mifare), both 125KHz and Mifare components are read;

(***): with dual technology keys (125KHz/Mifare), only the Mifare component is read.

The product codes of the keys are as follows:

- 1125/50, 10 125Khz keys,
- 1125/52, 10 125KHz/Mifare keys,
- 1125/53, 10 Mifare Plus keys,
- 1125/54, 4 Mifare keys.

APPENDIX E: How to use customized network settings in IperCom system

The "*Custom Network Settings*" section is present in the "*System*" tab, as shown below:

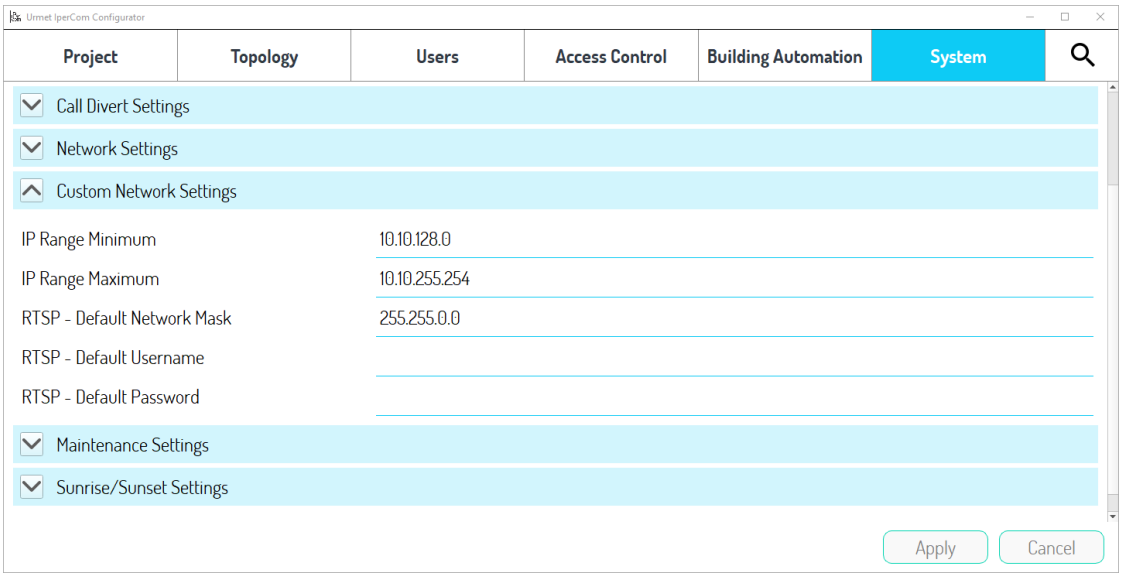

Figure 1: "System" tab - "Custom Network Settings"

In this section it is possible to define a range of IP addresses (between the "*IP Range Minimum*" and "*IP Range Maximum*" fields) with the relative mask defined by the "*RTSP - Default Network Mask*" field. The default values of these fields are shown in ***Figure 1***.

The IP address range and the related netmask must have compatible values.

The IP addresses defined in this way are automatically used by the *configurator* if the installer needs to:

- add devices such as *RTSP Cameras* (not IPerCom devices),
- enable RTSP streaming (streaming video) of one or more calling stations.

*If you enable RTSP streaming of the calling stations in the configurator, the related "User Name" and "Password" fields are automatically filled in with the values set in the "RTSP - Default User Name" and "RTSP - Default Password" fields in **Figure 1**).*

In doing this, you must ensure that the IP addresses statically assigned to the *RTSP Cameras* and video streaming of the calling stations are not among those already assigned to the various IPerCom devices.

To avoid this, three ways of proceeding are reported (for simplicity we will refer only to *RTSP Cameras*, but what is written also applies to RTSP streaming from calling stations, except where explicitly indicated).

In all three cases reported below, the network infrastructure and any configuration of the routers must be carried out by specialized personnel for the correct functioning of the system.

CASE 1: IPERCOM SYSTEM WITH DYNAMIC ADDRESSING, RTSP CAMERAS AND IPERCOM DEVICES IN THE SAME SUBNET

To implement this case, we recommend following the diagram displayed below, where the IP addresses shown are purely by way of example:

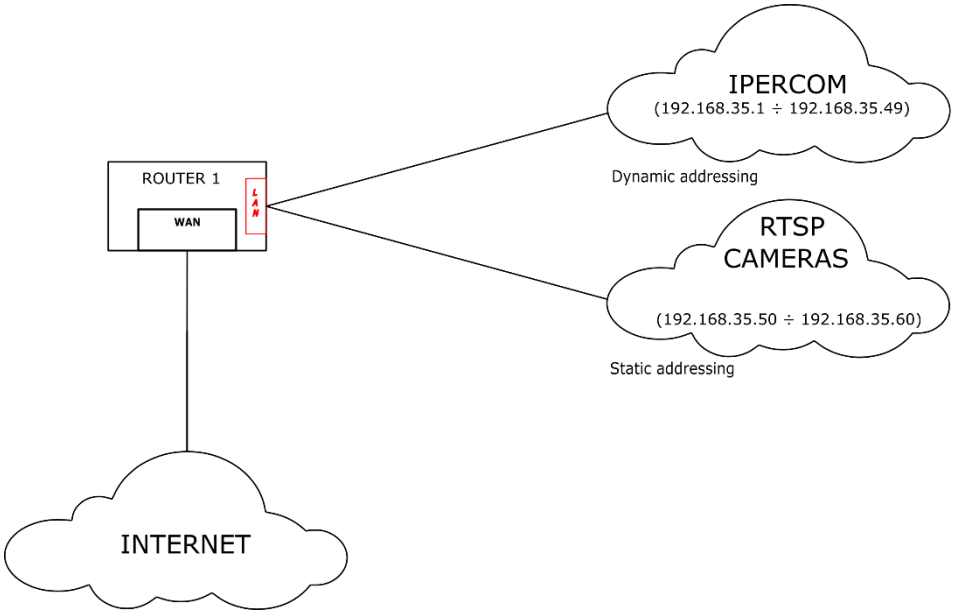

Figure 2: connection diagram for RTSP cameras and IPerCom devices

To create the diagram in ***Figure 2***, follow the instructions below.

1. **ROUTER 1**
   - Enable the DHCP Server and ensure that it assigns addresses of the 192.168.35.x/24 type, in detail from 192.168.35.1 to 192.168.35.49;
   - Connect the WAN port to Internet (optional).

2. **RTSP CAMERAS**
   - Set the *RTSP Cameras* addressing in static mode with addresses ranging from 192.168.35.50 to 192.168.35.60

In this way the IPerCom devices connected to ROUTER 1 via LAN have IP addresses of the 192.168.35.x/24 type, from 192.168.35.1 to 192.168.35.49; the *RTSP Cameras* connected to the LAN ports of ROUTER 1 will have IP addresses from 192.168.35.50 to 192.168.35.60 (set statically).

As regards the IPerCom *configurator*, follow the points below.

1. Dynamic addressing of IPerCom devices

In the "*System*" tab in the "*Network Settings*" section, choose the "*Dynamic*" item regarding the way in which IPerCom devices receive IP addresses:

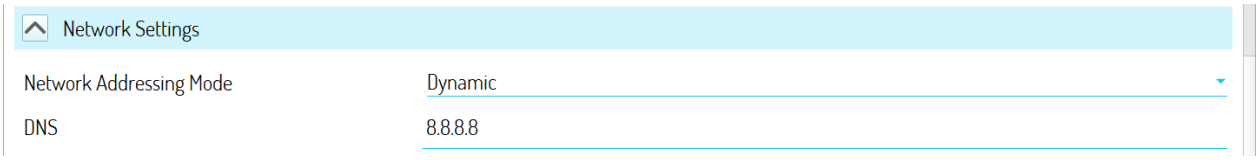

Figure 3: dynamic network settings for IPerCom devices

2. Static addressing of *RTSP Cameras*

For *RTSP Cameras*, choose a 192.168.35.x/24 subnet in the "*Custom Network Settings*" section, as shown below:

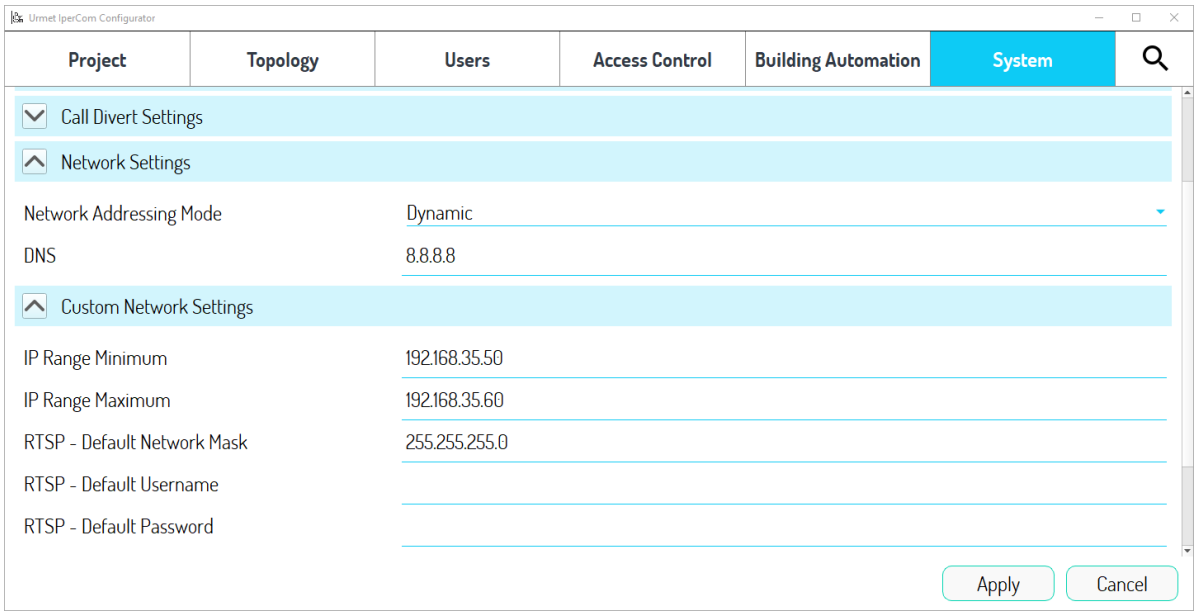

Figure 4: custom IP address range

3. Adding an RTSP Camera

If you add an *RTSP Camera* to the system, the following screen appears:

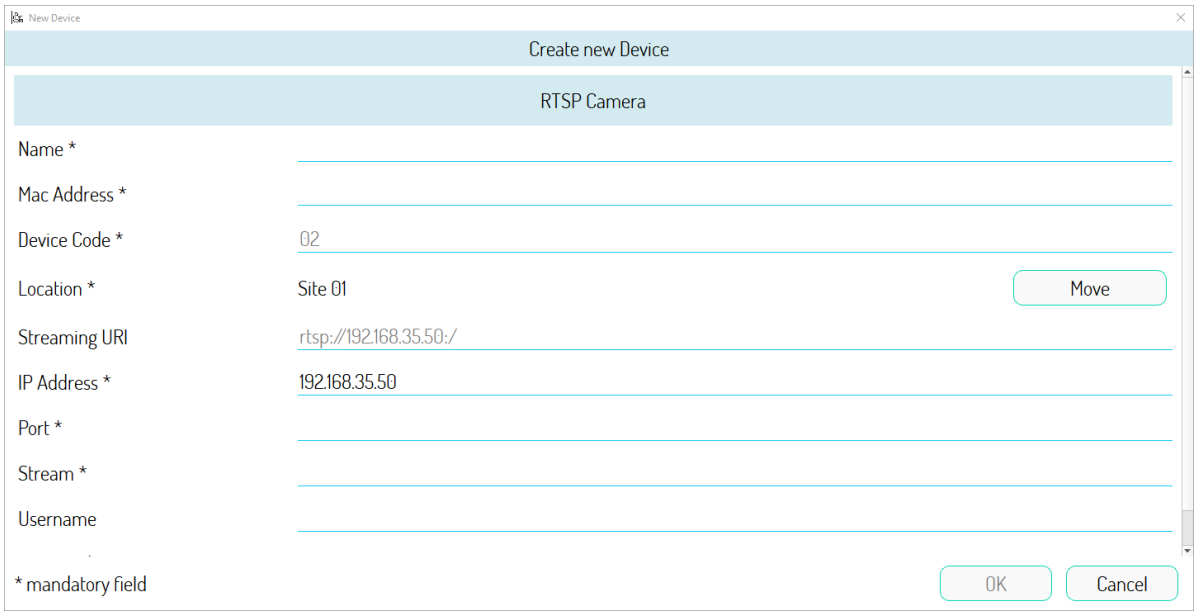

Figure 5: adding an RTSP camera to the IPerCom system

The "*IP Address*" field automatically reports the first available IP address among those present in the range of IP addresses defined in ***Figure 4***.

The proposed IP address must be the same as the one manually set in the *RTSP Camera* that you are adding into the configuration: if this is not the case, simply change it in the *configurator*.

*The proposed IP address can be changed to another IP address even outside the range set in **Figure 4** (provided it has not already been used).*

Similarly, if RTSP streaming of a calling station is enabled, the IP address assigned will be included in the range of ***Figure 4***. This can be modified with another value which in this case, however, must be included in the range set and must not have already been used.

CASE 2: IPERCOM SYSTEM WITH STATIC ADDRESSING, RTSP CAMERAS AND IPERCOM DEVICES IN THE SAME SUBNET

This case is like the previous one with the only difference that the IP addresses of the IPerCom devices are not assigned by the DHCP server of a router but by the *configurator*.

To implement this case, we recommend following the diagram displayed below, where the IP addresses shown are purely by way of example:

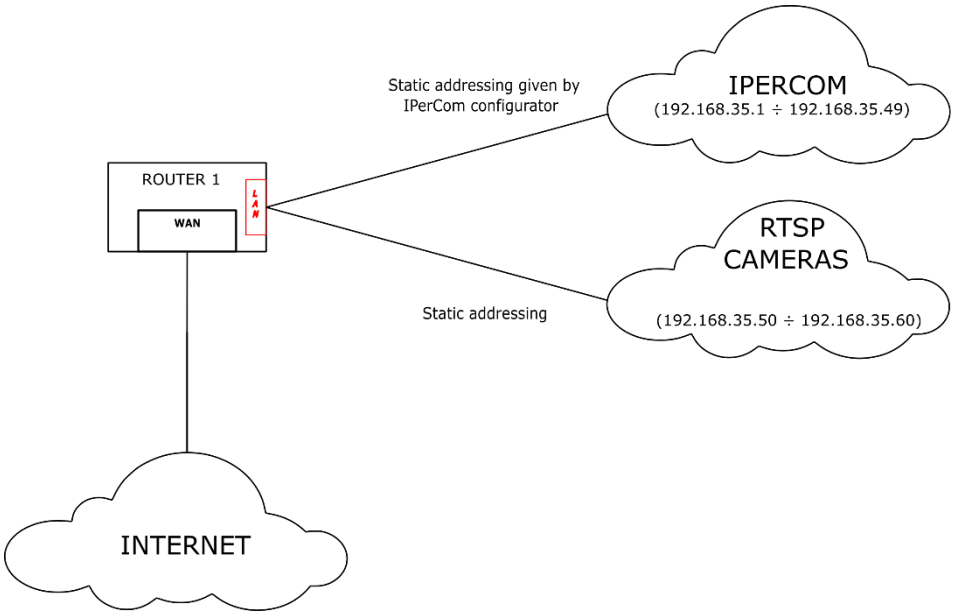

Figure 6: connection diagram for RTSP cameras and IPerCom devices

To create the diagram in ***Figure 6***, follow the instructions below.

1. **ROUTER 1**
   - Connect the WAN port to Internet (optional).

2. **RTSP CAMERAS**
   - Set the *RTSP Cameras* addressing in static mode with addresses ranging from 192.168.35.50 to 192.168.35.60.

In this way the IPerCom devices connected to ROUTER 1 via LAN have IP addresses of the 192.168.35.x/24 type, from 192.168.35.1 to 192.168.35.49 (assigned by the *configurator*); the *RTSP Cameras* connected to the LAN ports of ROUTER 1 will have IP addresses from 192.168.35.50 to 192.168.35.60 (set statically).

As regards the IPerCom *configurator*, follow the points below.

1. **Static addressing of IPerCom devices**

   In the "*System*" tab in the "*Network Settings*" section, choose the "*Static*" item regarding the way in which IPerCom devices receive IP addresses:

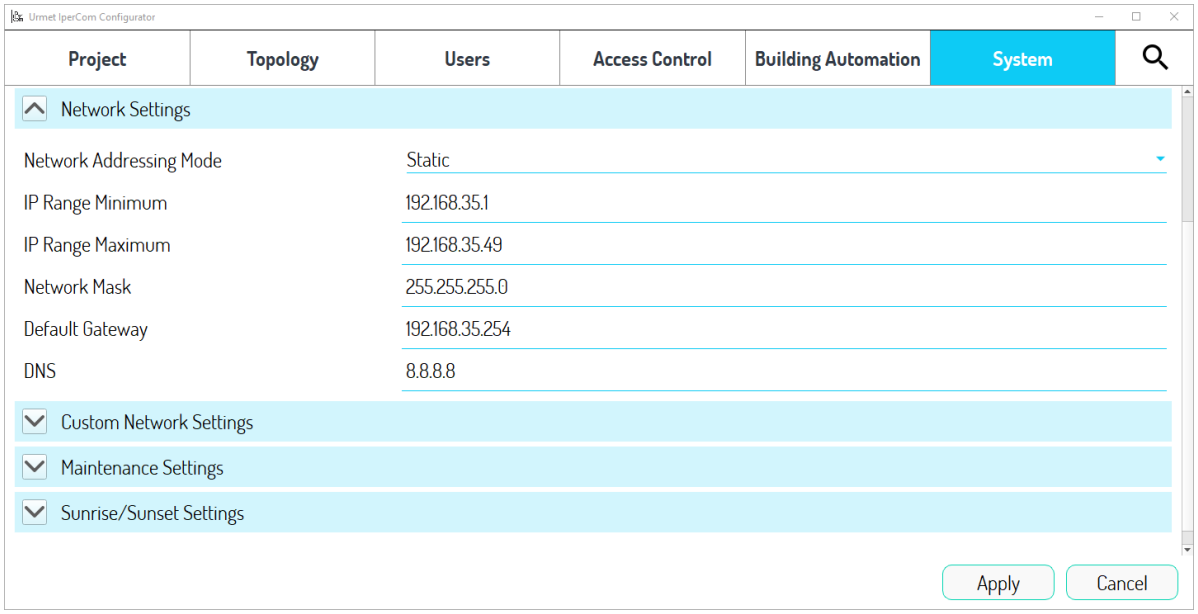

Figure 7: static network settings for IPerCom devices

2. **Static addressing of RTSP Cameras**

   For *RTSP Cameras*, choose a 192.168.35.x/24 subnet in the "*Custom Network Settings*" section, as shown below:

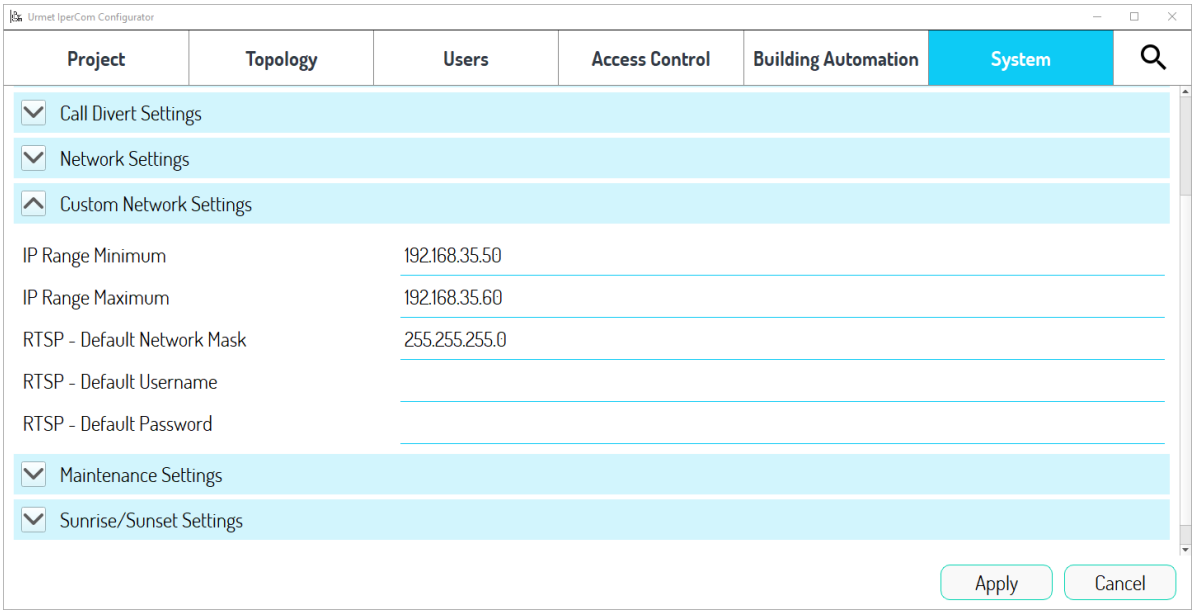

Figure 8: custom IP address range

3. Adding an RTSP Camera

If you add an *RTSP Camera* to the system, the following screen appears:

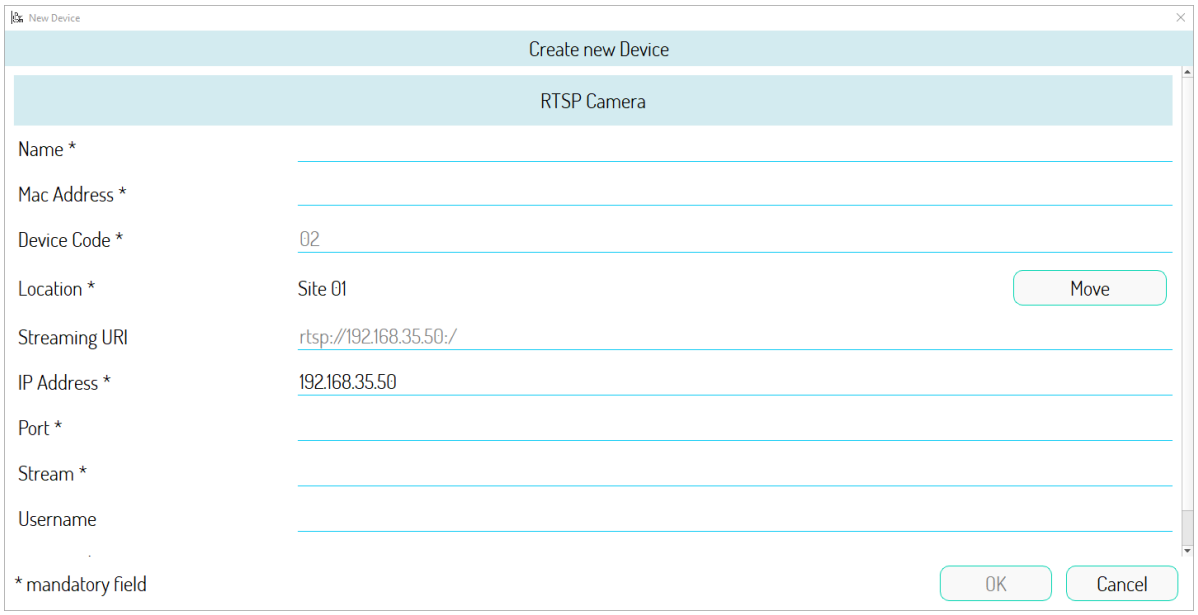

Figure 9: adding an RTSP camera to the IPerCom system

The "*IP Address*" field automatically reports the first available IP address among those present in the range of IP addresses defined in ***Figure 8***.

The proposed IP address must be the same as the one manually set in the *RTSP Camera* that you are adding into the configuration: if this is not the case, simply change it the *configurator*.

*The proposed IP address can be changed to another IP address even outside the range set in **Figure 8** (provided it has not already been used).*

Similarly, if RTSP streaming of a calling station is enabled, the IP address assigned will be included in the range of ***Figure 8***. This can be modified with another value which in this case, however, must be included in the range set and must not have already been used.

CASE 3: RTSP CAMERAS AND IPERCOM DEVICES ON TWO DIFFERENT SUBNETS

To implement this case, we recommend following the diagram displayed below, where the IP addresses shown are purely by way of example:

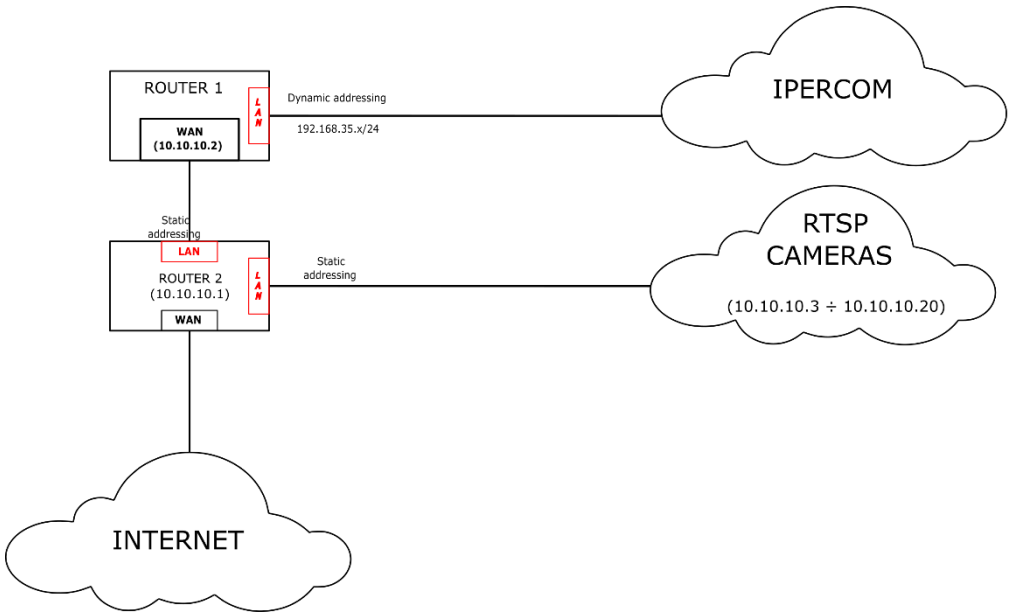

Figure 10: connection diagram for RTSP cameras and IPerCom devices

To create the diagram in ***Figure 10***, follow the instructions below.

1. **ROUTER 1**
   - Enable the DHCP Server and ensure that it assigns addresses of the 192.168.35.x/24 type;
   - Set the WAN port to static addressing with an address compatible with the network settings of ROUTER 2 (for example 10.10.10.2).

2. **ROUTER 2**
   - Disable the DHCP Server and assign to ROUTER 2 an IP address 10.10.10.1;
   - Set a 24-bit netmask;
   - Connect the WAN port to Internet (optional).

3. **RTSP Cameras**
   - Set the *RTSP Cameras* addressing in static mode with addresses (for example) ranging from 10.10.10.3 to 10.10.10.20.

In this way the IperCom devices connected to ROUTER 1 via LAN have IP addresses of the 192.168.35.x/24 type while the WAN port of ROUTER 1 has an IP address of 10.10.10.2. ROUTER 2 has an IP address 10.10.10.1 with a 24-bit network mask: the *RTSP Cameras* connected to the LAN ports of ROUTER 2 will have IP addresses from 10.10.10.3 to 10.10.10.20 (set statically).

As regards the IperCom *configurator*, follow the points below.

1. **Dynamic addressing of IperCom devices**

   In the "*System*" tab in the "*Network Settings*" section, choose the "*Dynamic*" item regarding the way in which IperCom devices receive IP addresses:

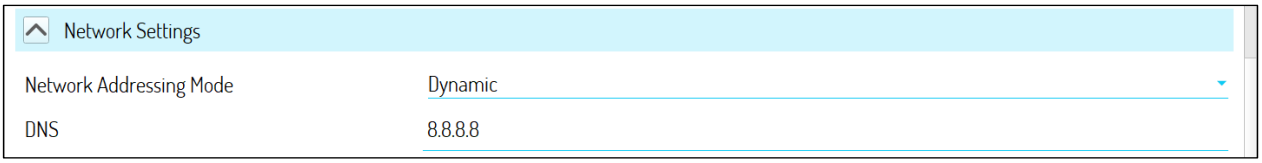

Figure 11: dynamic network settings for IPerCom devices

2. **Static addressing of *RTSP Cameras***

   For *RTSP Cameras*, choose a 10.10.10.x/24 subnet in the "*Custom Network Settings*" section, as shown below:

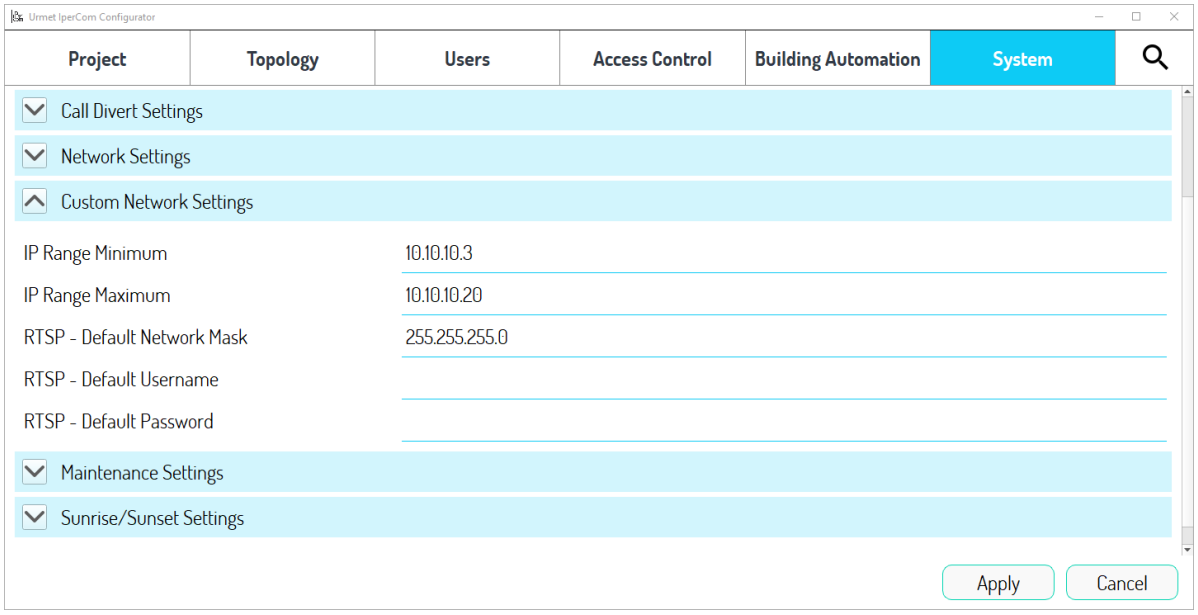

Figure 12: network settings RTSP Cameras

3. Adding an RTSP Camera

If you add an *RTSP Camera* to the system, the following screen appears:

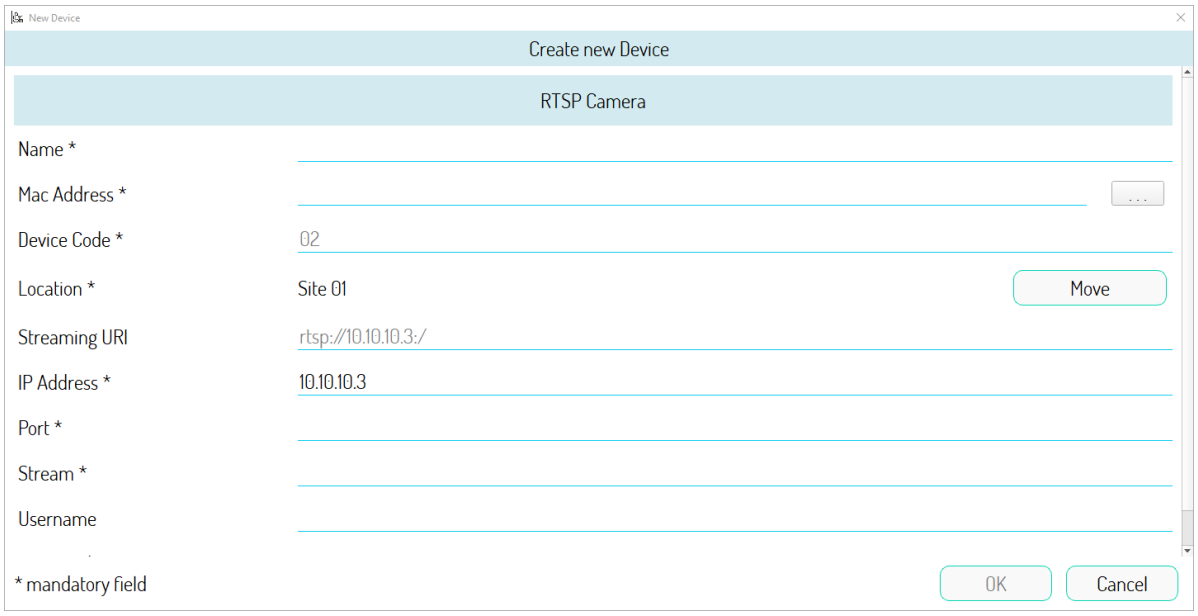

Figure 13: adding an RTSP camera to the IPerCom system

The "*IP Address*" field automatically reports the first available IP address among those present in the range of IP addresses defined in ***Figure 12***.

The proposed IP address must be the same as the one manually set in the *RTSP Camera* that you are adding into the configuration: if this is not the case, simply change it in the *configurator*.

*The proposed IP address can be changed to another IP address even outside the range set in **Figure 12** (provided it has not already been used).*

If you enable RTSP streaming of a calling station, the following screen appears:

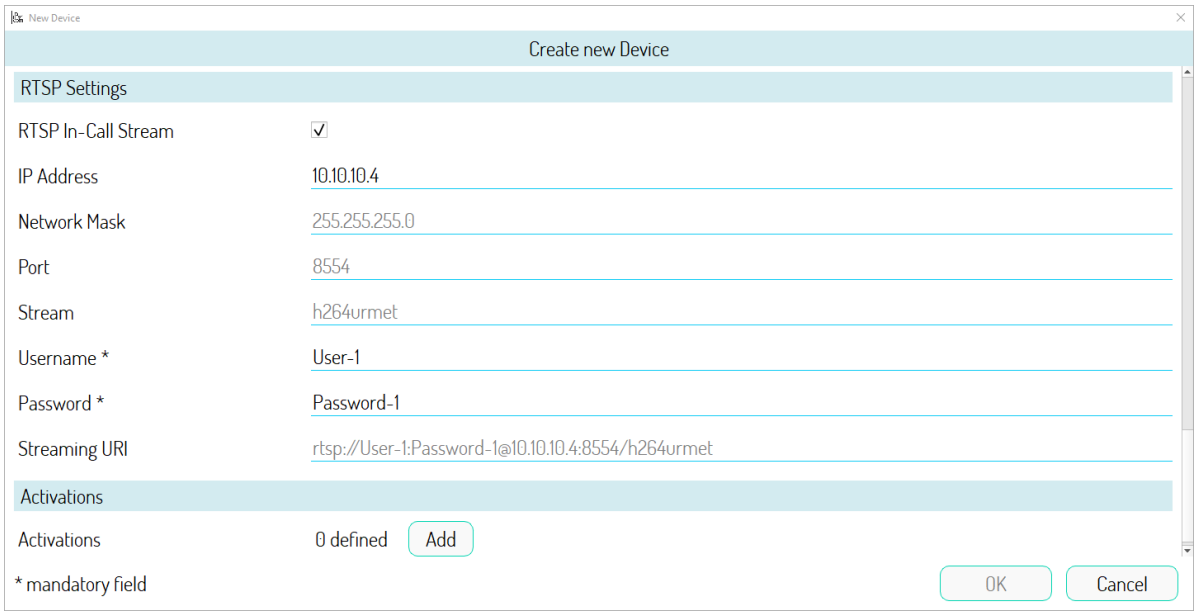

Figure 14: enabled RTSP streaming of a calling station

*As written above, the "IP address" field automatically reports the first available IP address: this can be modified with another value which in this case, however, must be included in the range set in **Figure 12** (and must not already be been used).*

*The above works even if in **Figure 10** the IPerCom devices have static addressing.*

APPENDIX F: Custom network settings and editable static IP addresses for IPerCom devices

If you choose the "*Static*" item in the "*Network Settings*" section of "*System*" tab of *configurator*, it is necessary, as already mentioned, to define a range of IP addresses, a network mask, DNS, and gateway as shown below:

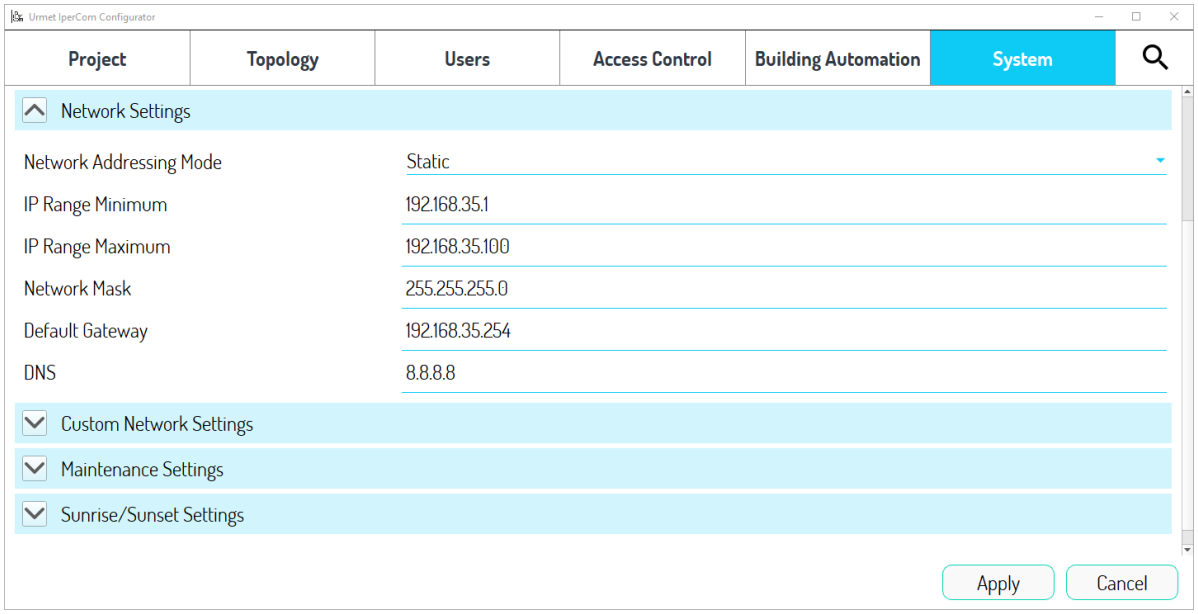

Figure 15: static network settings for IPerCom devices

If you add an IPerCom device, a screen like this appears:

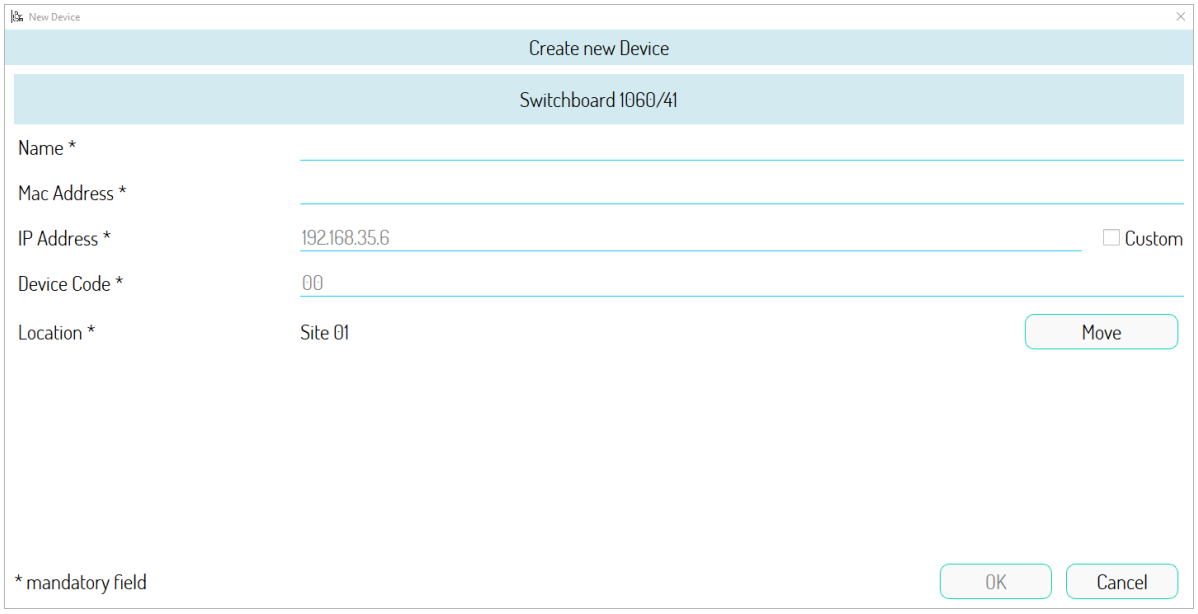

Figure 16: adding an IPerCom device

The "*IP Address*" field automatically reports the first available IP address proposed in the range of IP addresses defined in ***Figure 15***. This IP address can be modified if you select the "*Custom*" item:

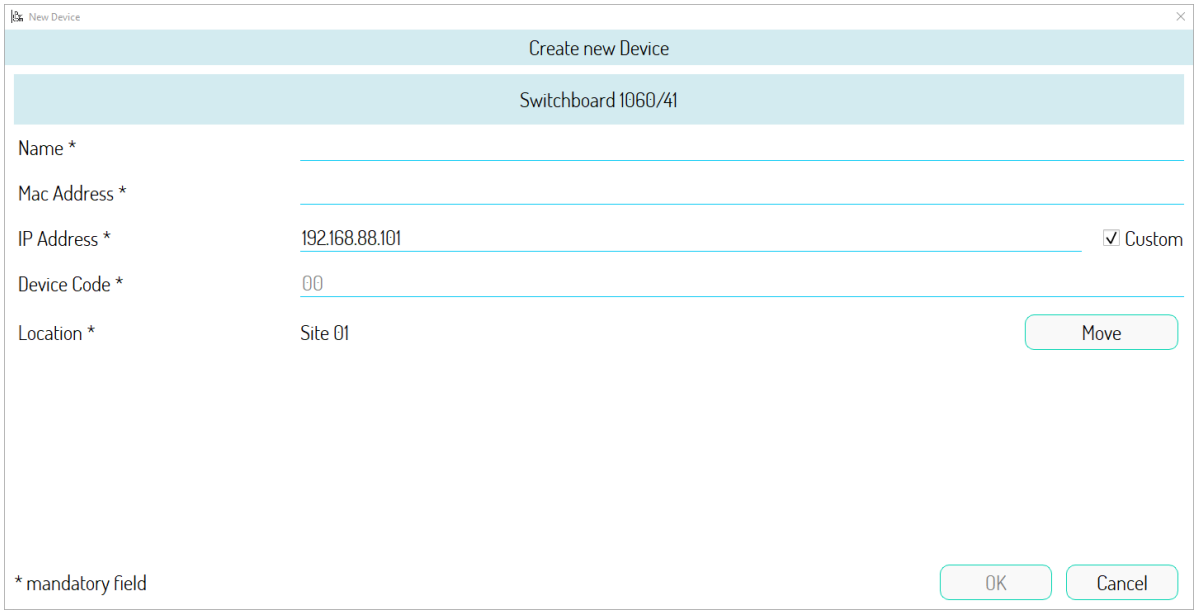

Figure 17: editable IP address

The "*IP Address*" field shows the first available value among those present in the IP address range set in the "*Custom Network Settings*" section:

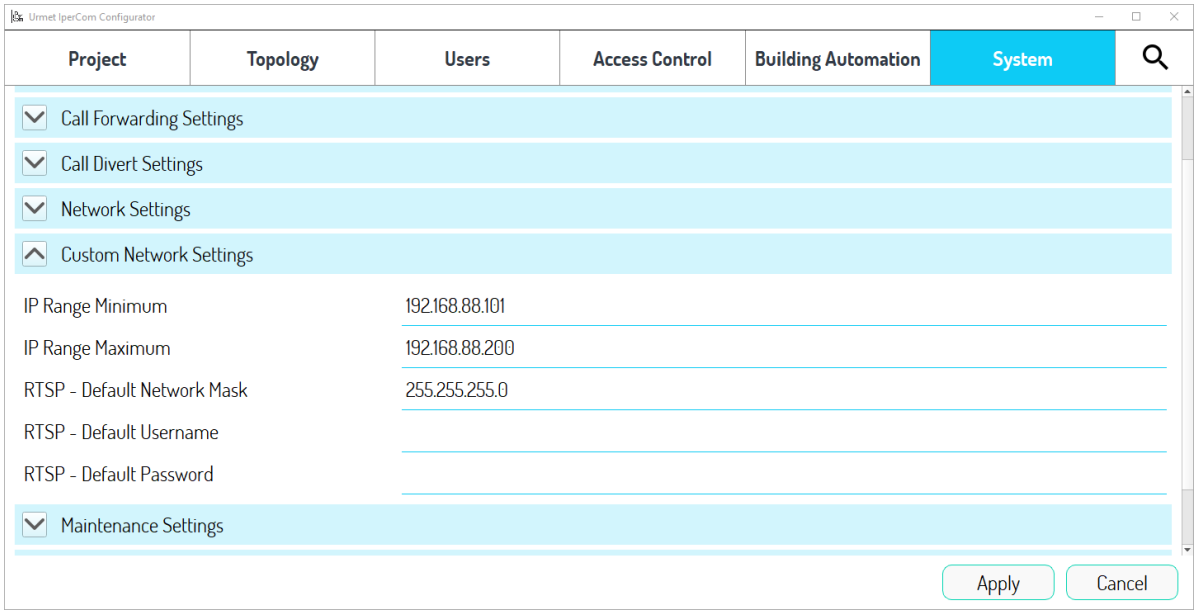

Figure 18: custom IP address range

To be able to modify the "*IP address*" field of ***Figure 17*** it is necessary to choose a value included in the IP address range of ***Figure 18***.

The need to be able to modify the static IP addresses of the IPerCom devices arises from the fact that the *IPerCom Client* and *Switchboard* applications reside on PCs that may have a static IP address already set and consequently this IP address must also be reported in the *configurator* when adding these devices.

Regardless of whether you choose the "Static" or "Dynamic" item in the "Network Settings" section, if you add the iPassan Controller device via the configurator, its IP address must always be within the range set in the "Custom Network Settings" section.

APPENDIX G: Changing the network settings of *IPerCom Installer Tools*

If it is necessary to change the network settings of the system after its commissioning, this is possible in the *configurator* through the **System** tab in the "*Network Settings*" section, which allows you to switch from a dynamic addressing mode (for example if there is a router in the system) to a static addressing mode or vice versa. In both cases the settings of the network card, through which the PC connects to the system where the *IPerCom Installer Tools* application is installed, need some modifications to continue to connect to the system. To make the task easier for the installer, the *IPerCom Installer Tools* application, through an interactive dialogue box, indicates which modifications need to be made.

For example, if you switch from an automatic network setting to a manual network setting with the following parameters:

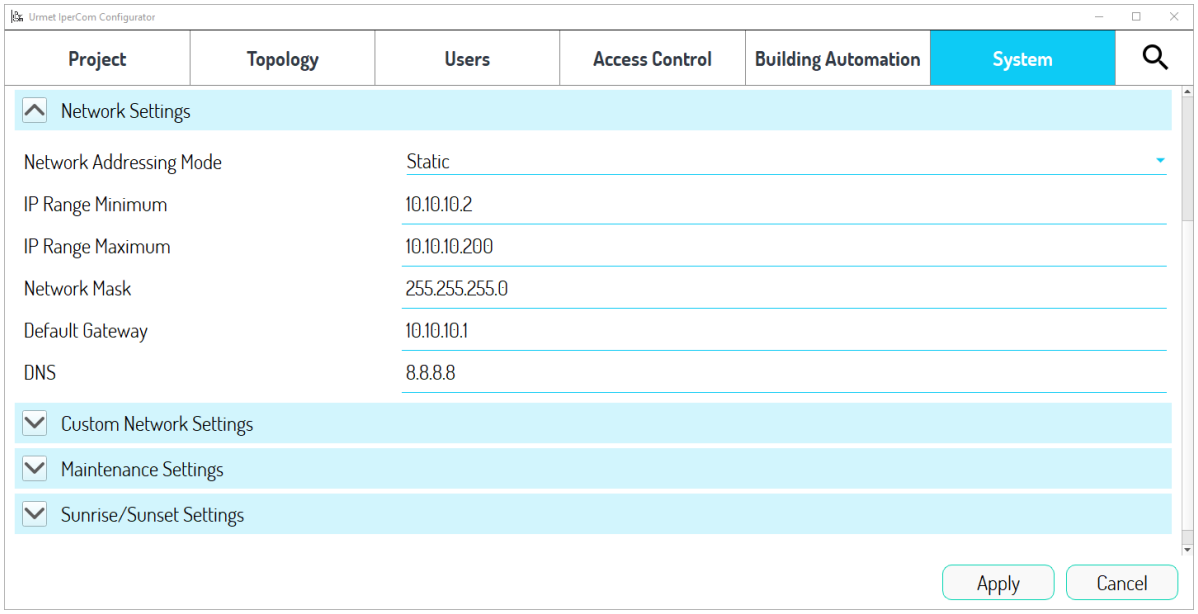

Figure 19: changing the network parameters

After saving the configuration, exiting the *configurator,* and applying the modifications to the system, *IPerCom Installer Tools* shows the following message:

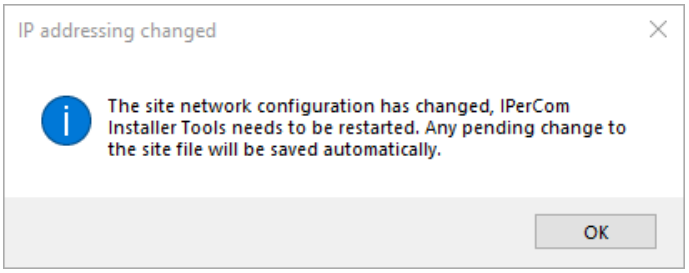

Figure 20: message on the modification of network parameters

At this stage some devices may reboot because of the IP address change.

Then it is necessary to press the "*OK*" button: the modifications to the site are automatically saved and *IPerCom Installer Tools* restarts, showing, after the login to Urmet Cloud, the following screen:

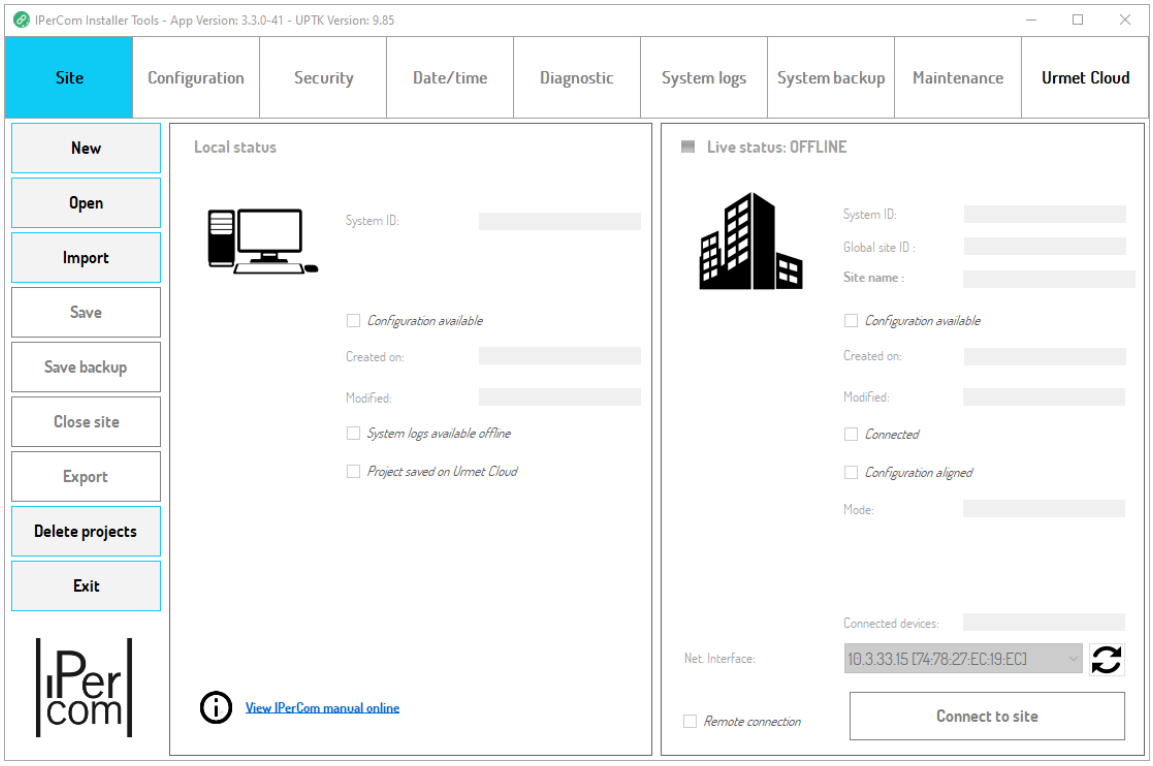

Figure 21: IPerCom Installer Tools screen after restart

Now it is necessary to open the project associated with the system and connect to it. When you press the "*Connect to site*" button, *IPerCom Installer Tools* detects that the network settings of the system are no longer consistent with those of the network card of the PC connected to the system. As a result, the following window is displayed, which shows a list of the network parameters that must be changed to allow a correct connection to the system:

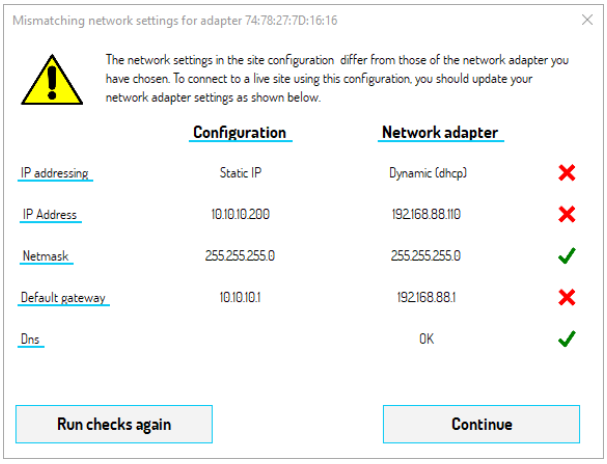

Figure 22: invalid network parameters

If you press the "Continue" button during this step (without changing the network parameters), the IPerCom Installer Tools application is closed.

*To change the IP address and MAC address of the network interface through which you are connected to the IPerCom system, it is necessary to press the **Open Network Connections and Sharing Centre** button on your PC (icon at the bottom right of the screen), then identify the name of the network connected to IPerCom system. Press with the left mouse button on the network item in question, to display a screen with the **Property** button, then press the "Internet Protocol version 4 (TCP/IPv4)" item twice. A mask is displayed where you can enter the required network parameters.*

After changing the various parameters as shown in the dialogue box, press the Recheck button to check what has been changed. If the various parameters have been changed correctly, the Recheck button shows the following screen:

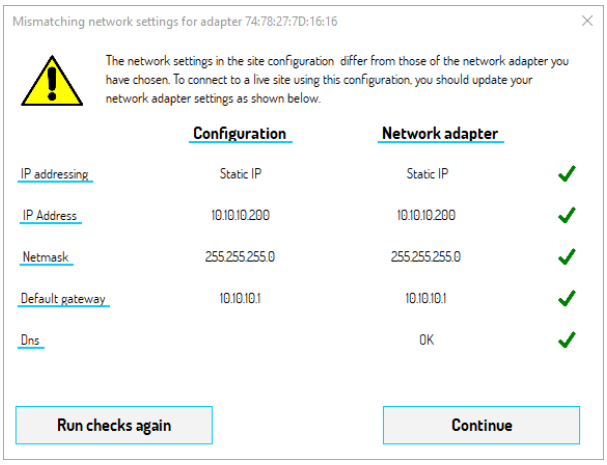

Figure 23: valid network parameters

Now, by pressing the "*Continue*" button, you are prompted to reconnect to the system, as the network settings have changed:

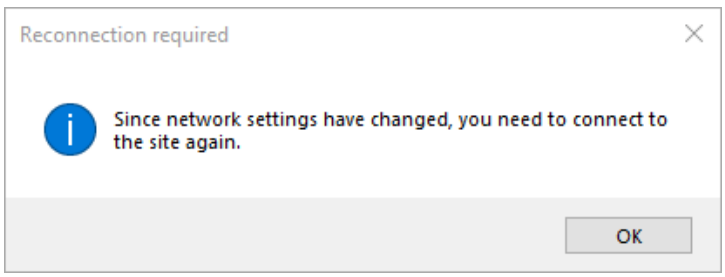

Figure 24: request for new connection to the system

Pressing “*OK*”, in the drop-down menu with the list of network interfaces with MAC and IP addresses you can find the previously modified network interface, i.e. the one with MAC address 74:78:27:7DA:16:16 and IP address 10.10.10.200. Once this interface has been selected, press the “*Connect to site*” button to reactivate the connection to the system.

APPENDIX H: Date and time incorrectly set in the future.

When commissioning an IPerCom system, it is necessary to set date and time correctly: this can be done if at least one device with internal clock is installed in the system.

The devices equipped with an internal clock are the following:

- *Entry Panels* 1060/21-33-34,
- *Modular Calling Station with 1060/48*,
- *Gateway-2Voice* 1083/59,
- *Server* 1060/1,
- *VOG[7], VOG[5], VOG[5+], Basic*, *MAX* and Ref. 1761/23 video door phones.

The initial setting of the date and time of the internal clock is done through *IPerCom Installer Tools* or through *VOG[7]*, *Basic*, *MAX* or Ref. 1761/23 video door phones.

Setting the date and time is essential for the correct functioning of the system, as this allows you to check the alignment status between the on-site configuration and the project configuration (after connecting to the system), highlighting the possible situations:

- **site** configuration aligned with that present in the **project**;
- **site** configuration older than that present in the **project**;
- **site** configuration newer than the one present in the **project**.

If the configuration distribution on a system is mistakenly done from one of the video door phones listed above or from a PC (where the *IPerCom Installer Tools* application is installed) that have a date and time set in the future with respect to the current date, when the date and time are reset correctly, any new configuration will never be applied to the system. This is because IPerCom devices do not accept a configuration file if the one inside them has a date later than the current date (date in the future).

From a visual point of view this means that, after having modified and distributed the configuration (for example with *IPerCom Installer Tools*):

- all configured devices in the system will always have a newer configuration than the one you are trying to distribute;
- the number of devices with the same configuration will always be zero.

To solve the problem, it is necessary to configure the steps below:

- export the project by means of *IPerCom Installer Tools*;
- open the the project, make a change to the configuration, and save: in this way current date and time are set in the project;
- from the **Maintenance** tab of *IPerCom Installer Tools* press "*Erase configuration on all devices*" button;

Once the devices have finished deleting the configuration, distribute the previously saved configuration by means of *IPerCom Installer Tools*.

If the configuration was created from one of the video door phones listed above, simply export the configuration file, create a project in *IPerCom Installer Tools*, import the configuration using the "*From file*" button in the **Configuration** tab, save configuration with the correct date and distribute it to the system, after having deleted the old configuration.

APPENDIX I: Streaming video from IPerCom calling stations to NVR Urmet

The following procedure describes how to display and record the following on Urmet **1098/324P-326P-328P** NVR devices:

- streaming video during calls from IPerCom calling stations to apartments or to a generic apartment station;
- streaming video during auto-on with mono- and bi-directional audio from apartment station or *CallMe* application to IPerCom calling stations.

*About Urmet NVR devices, only the information necessary to view and record the streaming video of the IPerCom calling station is reported; for more detailed information on Urmet NVR devices, download the **relevant booklet**.*

*The procedures below refer to accessing the web interface of the Urmet NVR device via IP address. If access is done via the OSD menu (with HDMI cable and USB port for the mouse), we recommend consulting the **relevant booklet**, as the procedures may be slightly different.*

The procedures below refer to a not configured Urmet NVR device. In case of a device already configured, some points can be skipped.

Software requirements

On Urmet NVR devices the software version must be **V8.2.4.1-20240515** or higher.

Display of the software version

Follow the procedure below to view the software version of the Urmet NVR device.

1. Connect to a switch a PC and the Urmet NVR device (via one of the LAN ports or via the WAN port);

2. Assign the PC a static IP address 192.168.1.101 (for example) with a 24-bit network mask, default gateway 192.168.1.254 and DNS 8.8.8.8, as shown below:

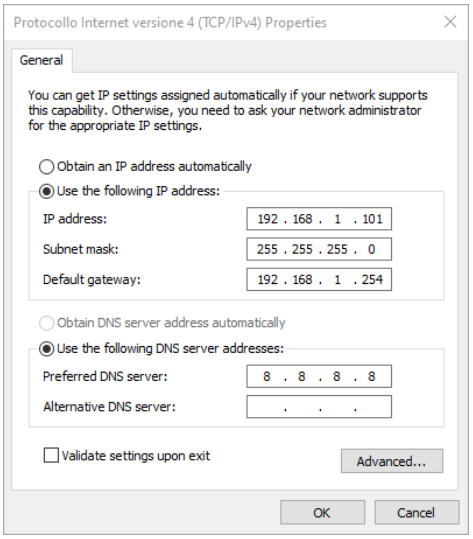

Figure 25: static IP address assignment

3. Enter the IP address 192.168.1.100 into the address bar of your browser and press "*Enter*".

   The following screen appears, where it is necessary to set the language in English, enter the required passwords (access password for the "*admin*" user and password to activate any cameras with private protocol). Then confirm the data entered with the "*OK*" button:

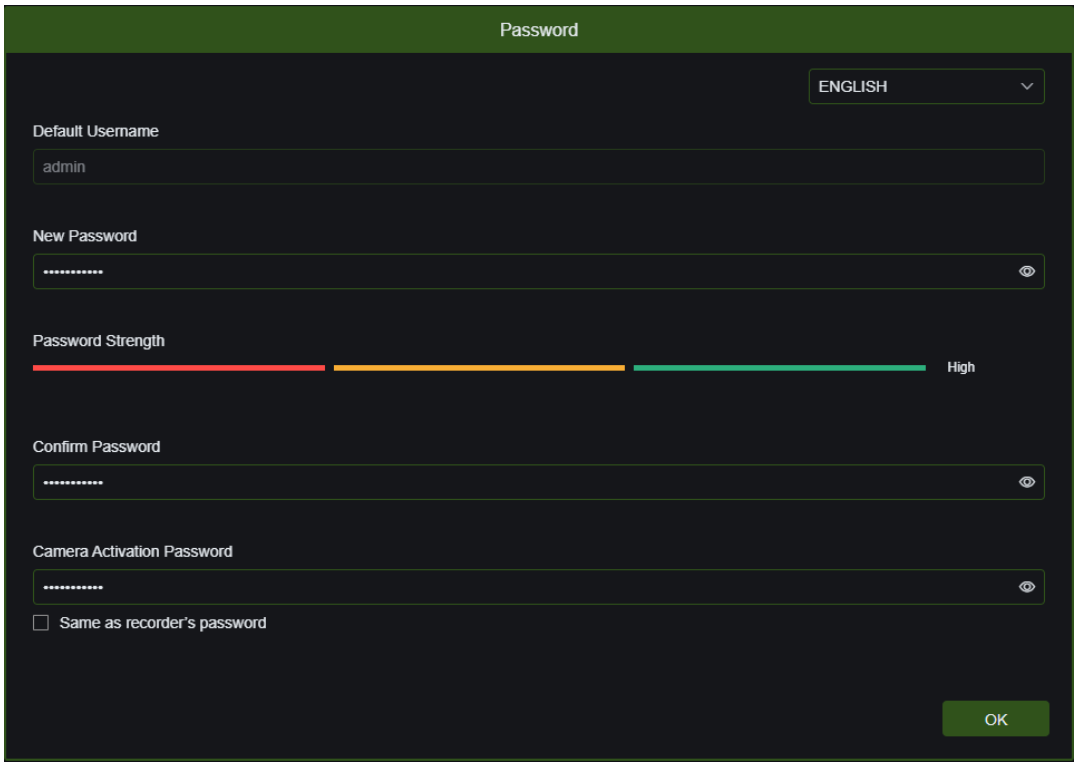

Figure 26: default username and password to access the Urmet NVR device

The username "admin" cannot be changed

At this point a password recovery screen appears with related security questions. The user can fill in this form and press the "*OK*" button or press the "*Cancel*" button. In both cases the following dialog box appears:

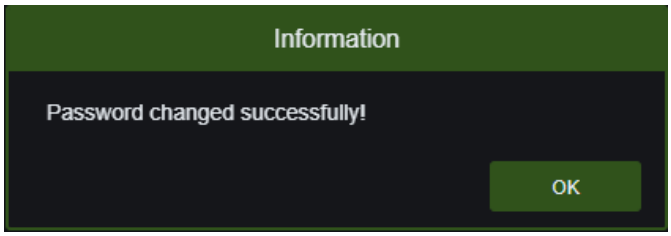

Figure 27: password accepted

After pressing the "*OK*" button, the login window appears:

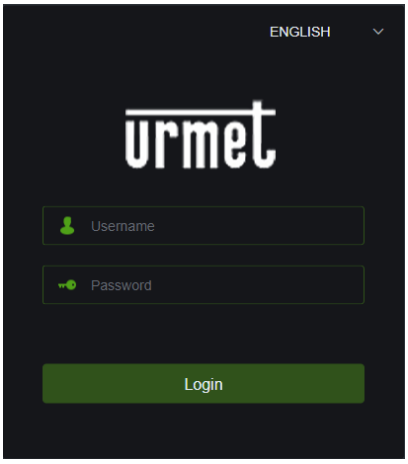

Figure 28: login window

After entering your username ("*admin"*) and password and pressing the "*Login*" button, the following screen appears:

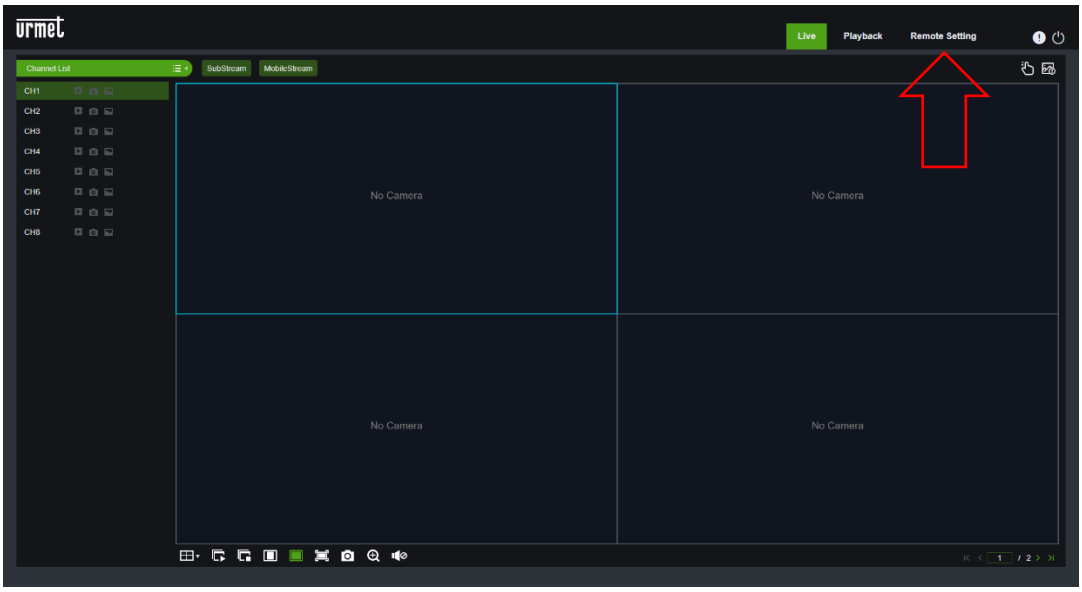

Figure 29: access to the NVR device

By pressing on the "*Remote settings*" item (red arrow), the following screen appears:

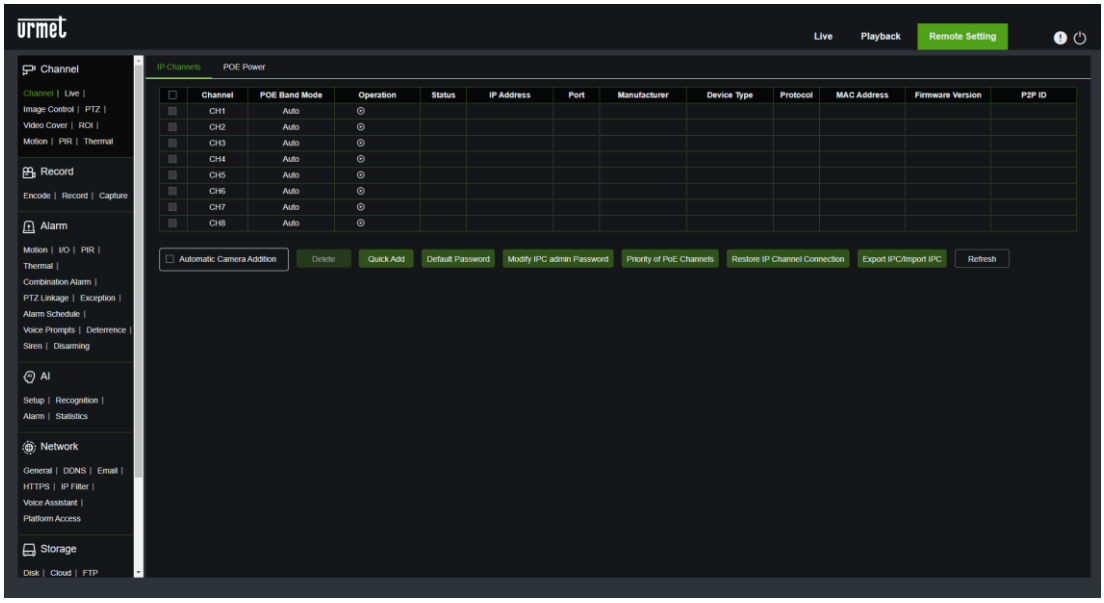

Figure 30: tab "Remote Setting"

On the left side of the screen, move the scroll bar to the bottom until the "*System*" section and the "*Information*" item are displayed (red arrow):

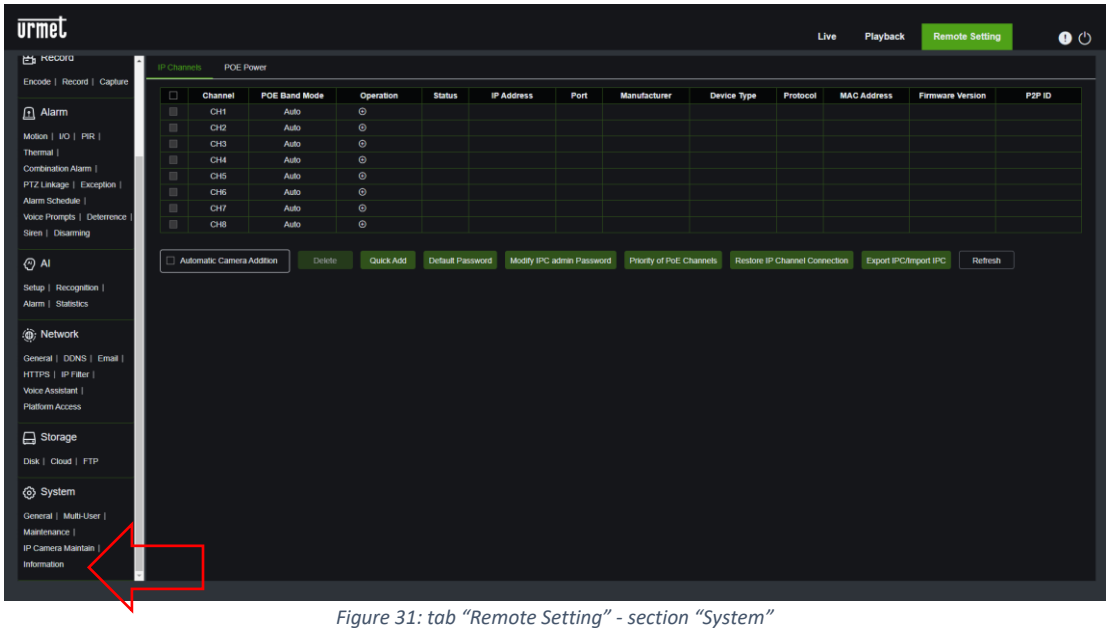

Figure 31: tab "Remote Setting" - section "System"

By pressing on the "*Information*" item, the software version of the Urmet NVR device is displayed (red arrow):

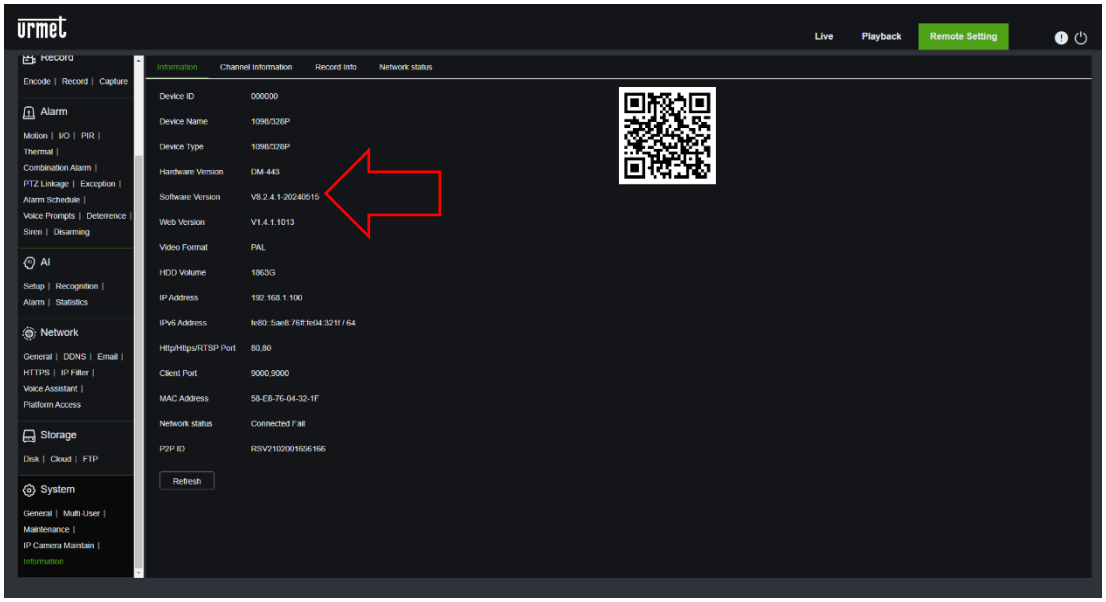

Figure 32: tab "Remote Setting" - section "System" --- > "Information"

Before continuing with the other operations, we recommend extending the time out of the connection via the web page to the Urmet NVR device. In the "System" section, press on the "General" item and then in the "Web Session Timeout" field change the 5 minutes default value.

Software update of the Urmet NVR device

Follow the following procedure to update the software version of the Urmet NVR device.

1. Download the software version **V8.2.4.1-20240515** or higher from the website ***www.urmet.com*** in the **1098/324P-326P-328P** related web page;
2. Press on the "*Remote Setting*" item, then in the "*System*" section press on the "*Maintenance*" item, then on the "*Upgrade*" item; the following screen appears:

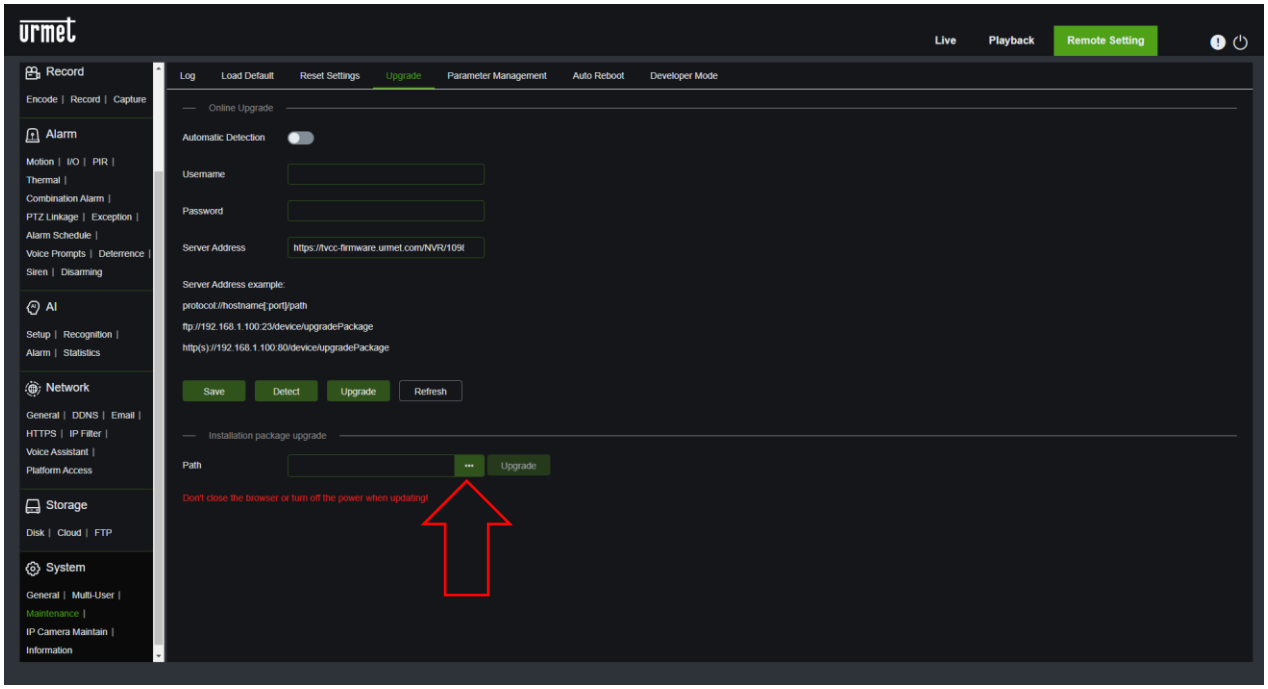

Figure 33: button to upload the software update file

3. Press the button ••• (red arrow) to select the previously downloaded update file;
4. Press the "*Update*" button to confirm the update;
5. Press the "*OK*" button on the relevant dialog box;
6. Enter the administrator password and confirm with the "*OK*" button;
7. Wait for the update to complete;
8. Once the update has been completed, carry out the procedure described in the previous paragraph to verify that the update has been completed.

Connection of the Urmet NVR device to the IPerCom system

The procedure below refers to an IPerCom system with dynamic addressing via a DHCP Server.

In the "*Network*" section, press on the "*General*" item, then in the "*WAN*" section, check that the DHCP option is enabled.

Connect the Urmet NVR device to the IPerCom system via its WAN port.

To identify the IP address of the WAN port of the Urmet NVR device, follow the instructions below:

- press on the following ***link***;
- in the "*Technical documents and resources*" section ---> "*Software*" download the "*Software Tools*" software package;
- install the "*Device Config Tool_1.0.2.64_2023_09_27.exe*" software.

At the first start, the Windows operating system may notify the user of the need to *unlock* the communication ports on the IP network used for communication between the Urmet NVR device and the *Device Config Tool* application. This operation is necessary for the correct functioning of the application. If protection is entrusted to the *Windows Firewall* module, a warning like the one shown in the following figure will be shown to the user:

Figure 34: Windows Firewall block for Device Config Tool application

You must select both types of networks and press the "*Allow access*" button to continue. The screen that appears is the following:

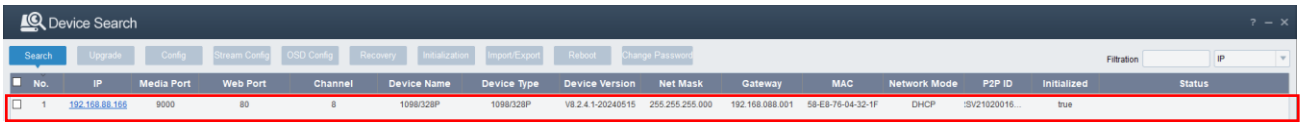

Figure 35: IP address of the Urmet NVR device

The IP address of the Urmet NVR device is shown in the red box in the *"IP"* column.

At this point, from a PC with an IP address in the same subnet as the IPerCom system, enter the IP address reported in the *Device Config Tool* application in the address bar of the browser. After entering the username and password, you can connect to the Urmet NVR device again.

In the "*Network*" section, press on the "*General*" item to view the IP address of the WAN port, network mask and gateway (like what is reported by the *Device Config Tool* application):

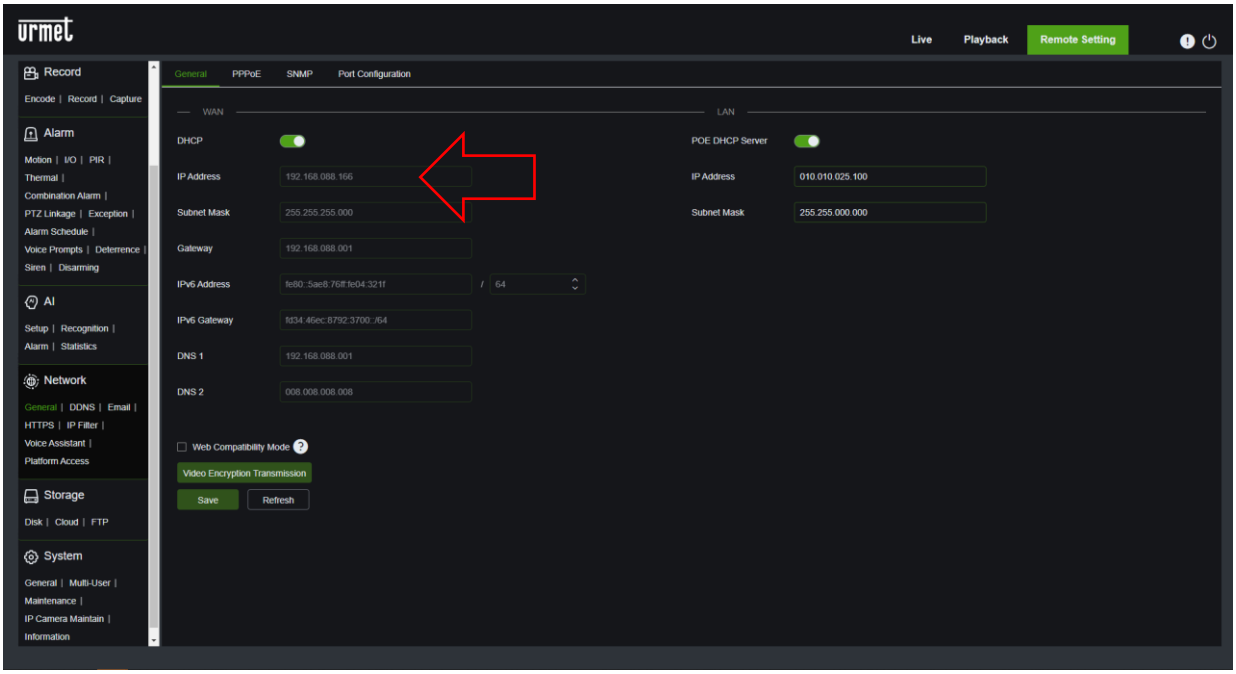

Figure 36: tab "Remote Setting" - section "Network" --- > "General"

Enabling the RTSP streaming during calls from Modular Calling Station with 1060/48

1. Access the configuration page of an IPerCom calling station (for example the *Modular Calling Station with 1060/48*) via the *configurator*;
2. Enable the "*RTSP In-Call Stream*" item by selecting the relevant box:

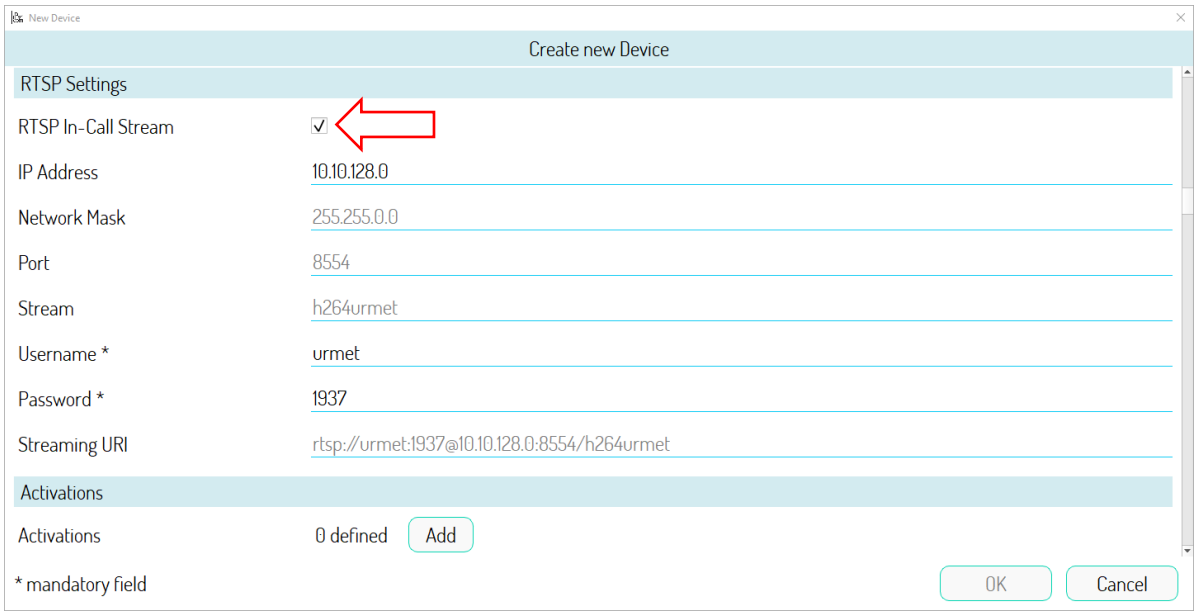

Figure 37: enabling of the RTSP streaming from the configurator for the Modular Entry Panel with 1060/48

3. Press "*OK*" to save the configuration then apply the configuration.

   Some of the parameters shown in the previous figure are predefined in the "*System*" tab in the "*Custom Network Settings*" section, as shown below:

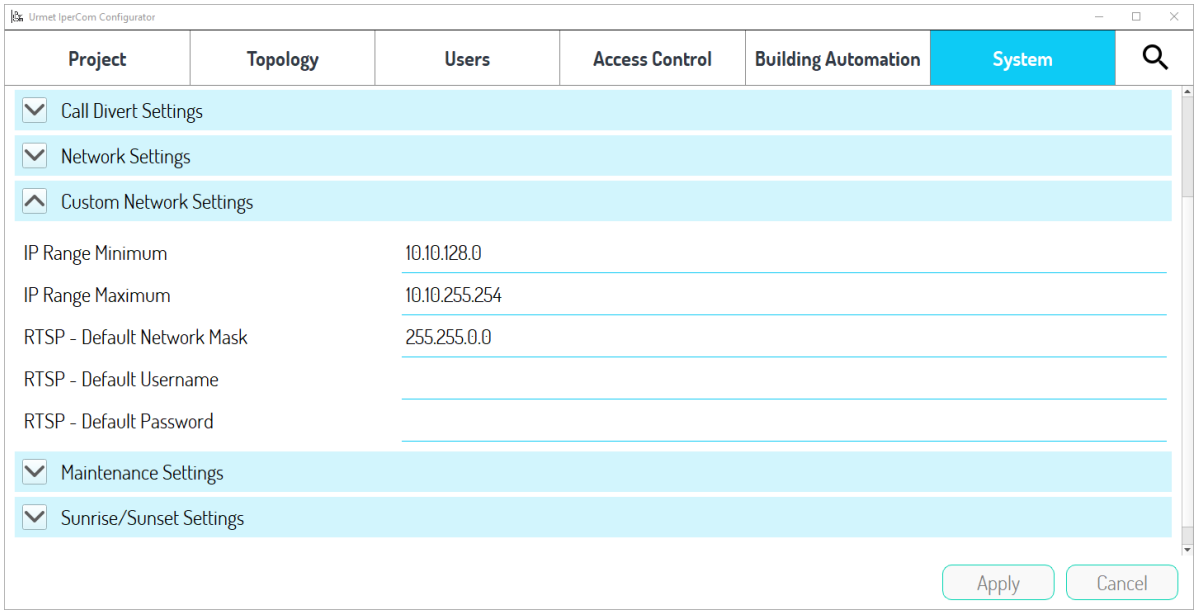

Figure 38: custom network settings

The above values can be modified and saved by pressing the "*Apply*" button.

Every time you enable the RTSP streaming of a calling station, the first available IP address within the range of IP addresses set in the previous figure is proposed in the relevant "*IP address*" field.

The IP address range and the related netmask must have compatible values.

Association of an IP channel with the RTSP streaming of a calling station

In the "*Channel*" section, press on the "*Channel*" item. The following window appears:

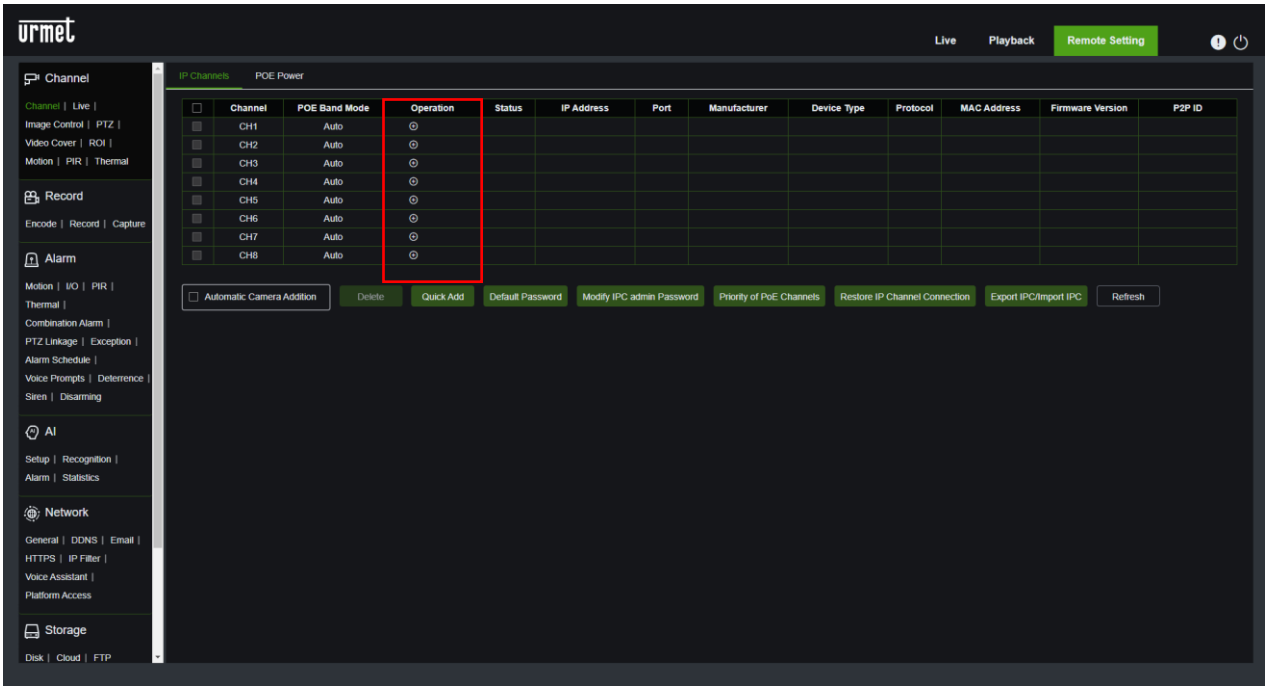

Figure 39: tab "Remote Setting" - section "Channel" --- > "Channel"

Press the button  ("*Operation*" column in the red box) relating to channel 1 (CH1). The following screen appears:

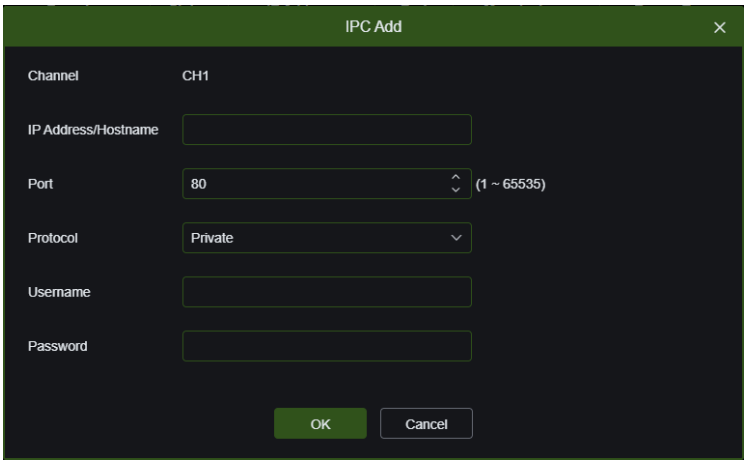

Figure 40: parameters for setting the channel

In the "*Protocol*" field, select the "*RTSP*" item. The following screen appears:

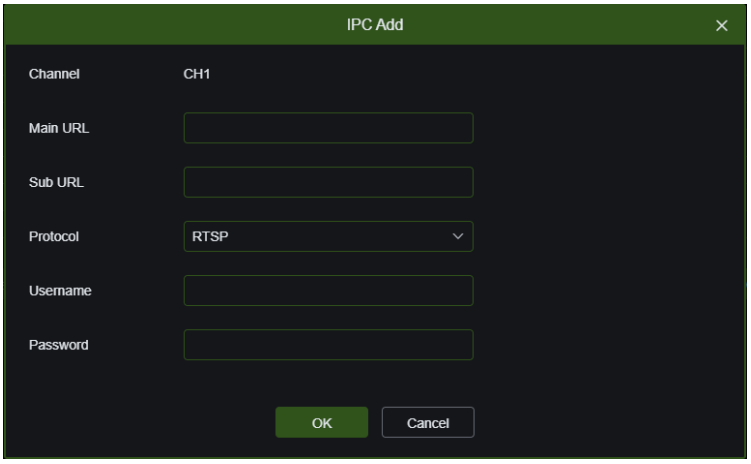

Figure 41: RTSP protocol setting on CH1 channel

Then fill in the other fields as shown below, assuming that the default values of the RTSP streaming have not been changed:

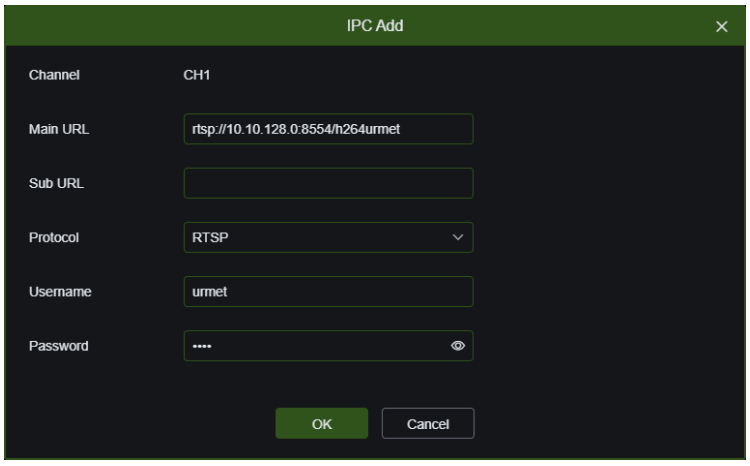

Figure 42: URL, username, and password settings on CH1 channel

The string for RTSP streaming to be entered is the following: **rtsp://10.10.128.0:8554/h264urmet**; username and password must be entered separately.

Press the "*OK*" button to confirm. The following screen appears, where channel 1 of the Urmet NVR device appears in the red box correctly configured:

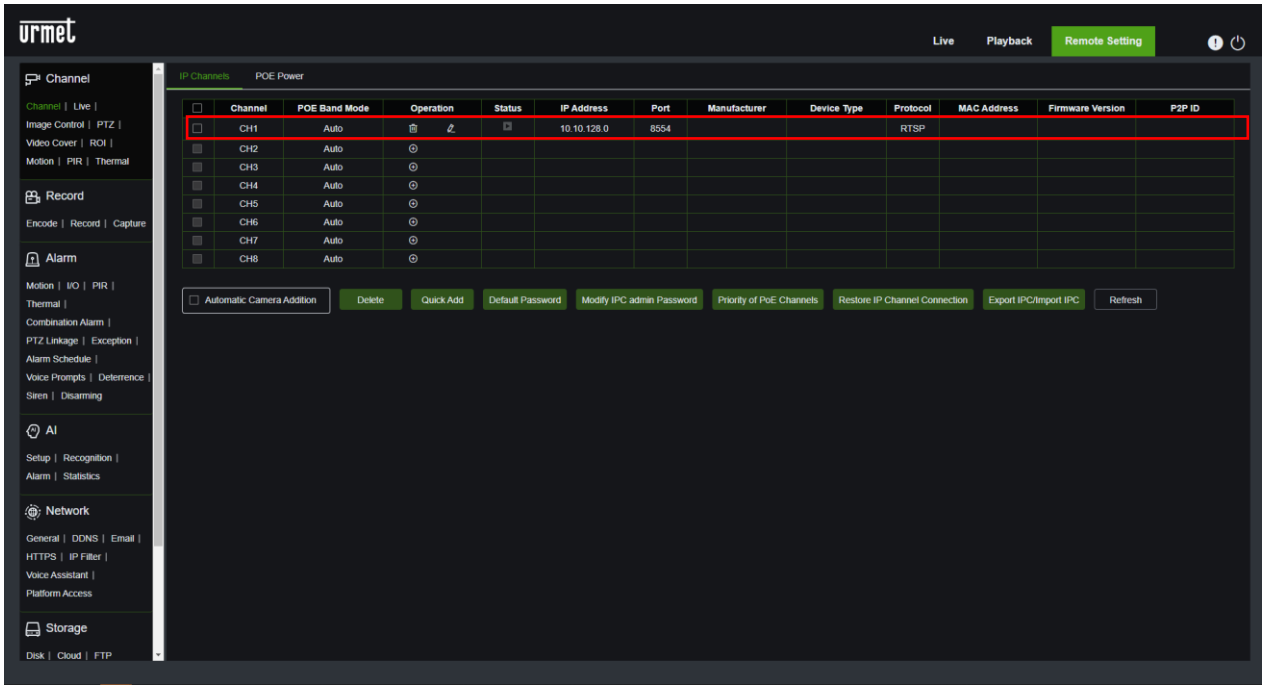

Figure 43: CH1 channel correctly configured

Viewing the streaming video

To view the streaming video, you need to press on the "*Live*" item. The following screen appears:

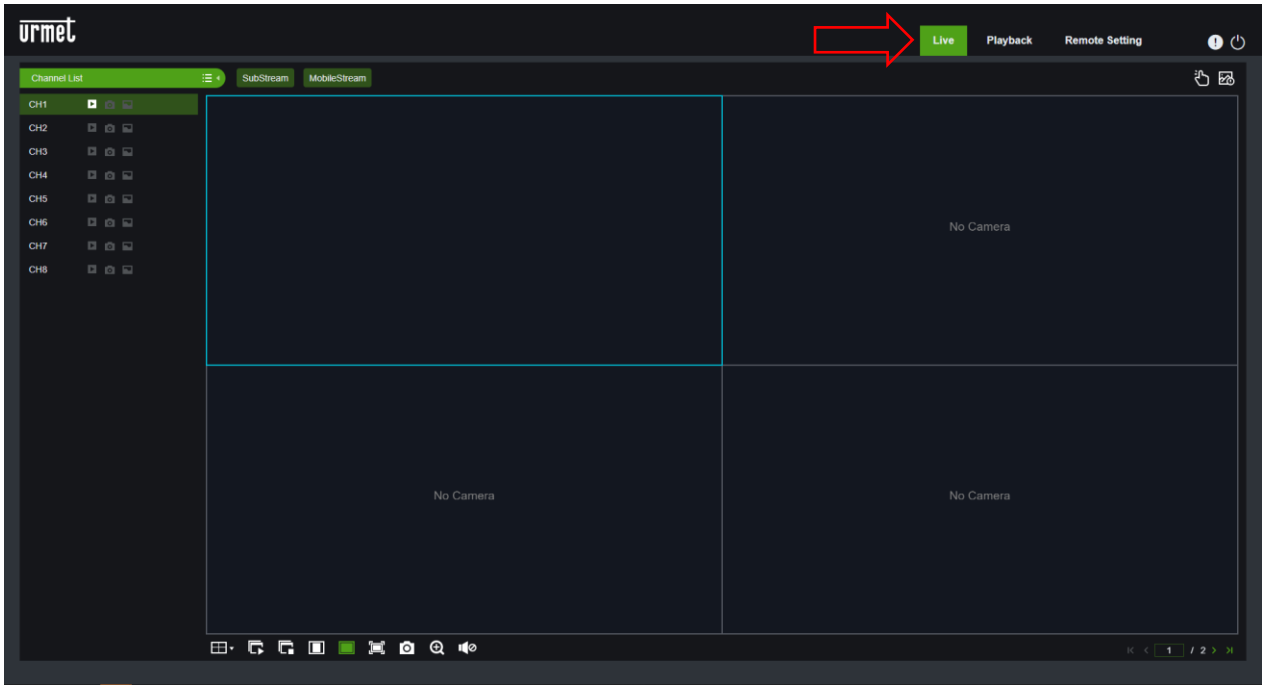

Figure 44: "Live" tab to view the streaming video

If on the IPerCom system no call from the *Modular Calling Station with 1060/48* is in progress or if no auto-on towards the *Modular Calling Station with 1060/48* is being performed from any video door phone, no streaming video is displayed.

On the contrary, if an apartment/resident is called from the *Modular Calling Station with 1060/48* or an auto-on is made from a video door phone towards the *Modular Calling Station with 1060/48*, the corresponding video streaming is displayed on the Urmet NVR device:

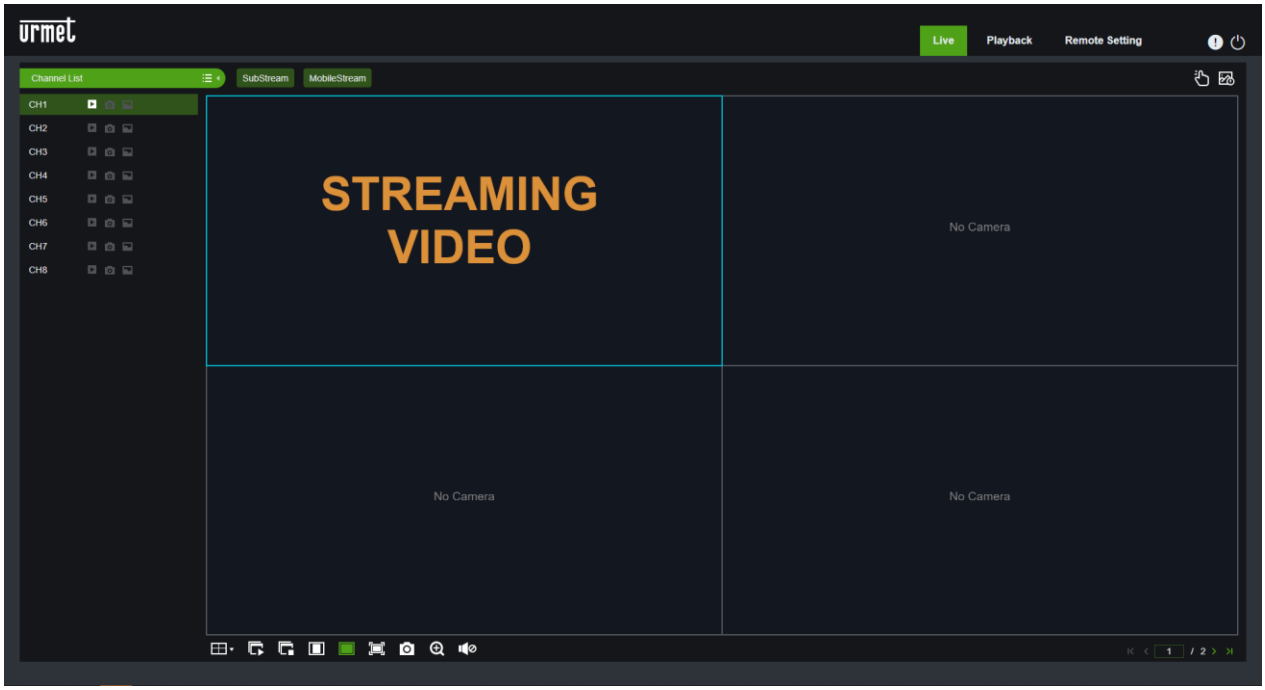

Figure 45: streaming video during calls from the calling station or auto-on from the video door phone

What is written above applies to any other calling station present on the IPerCom system.

Recording of the streaming video

To view the recording settings, press on the "*Remote Setting*" item, then in the "*Record*" section select the "*Record*" item, as shown below:

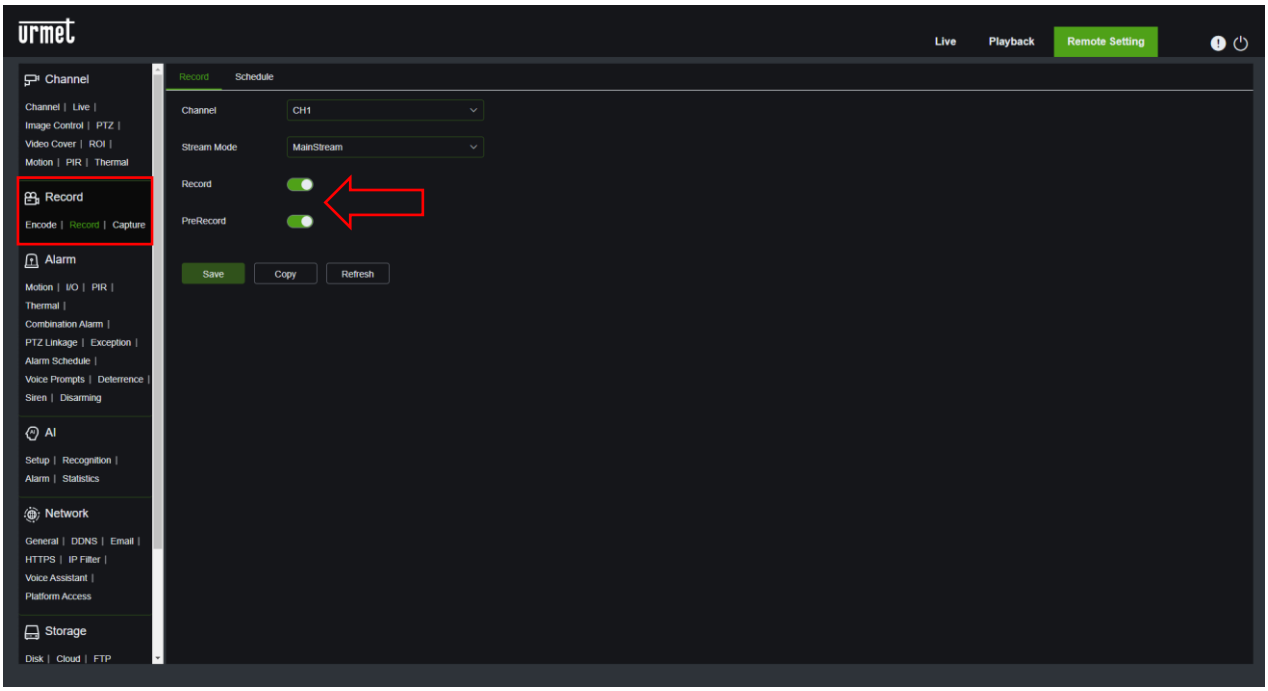

Figure 46: tab "Remote Setting" - section "Record" --- > "Record"

The "*Record*" item is already enabled (as indicated by the red arrow in the figure) for all channels.

To view the recording, press on the "*Playback*" item, as shown below:

Figure 47: "Playback" tab to view the recording

In the "*Channel List*" section, select the channel for which you want to play the recording of the streaming video (you can select one channel at a time). If you select channel 1 and press the "*Search*" button, the following screen appears:

Figure 48: channel selection in the "Playback" tab

The vertical green bars in the red box indicate the time intervals of when the recording occurred.

By pressing the button  (highlighted by the red arrow), you can play the recording, which starts at the first green bar. Simply press the mouse on a subsequent green bar to play the recording corresponding to another time interval.

Enable the acoustic signal for streaming video loss

To enable the acoustic signal of streaming video loss on the Urmet NVR device, press on the "*Remote setting*" item, then in the "*Alarm*" section select the "*Exception*" item, as shown below:

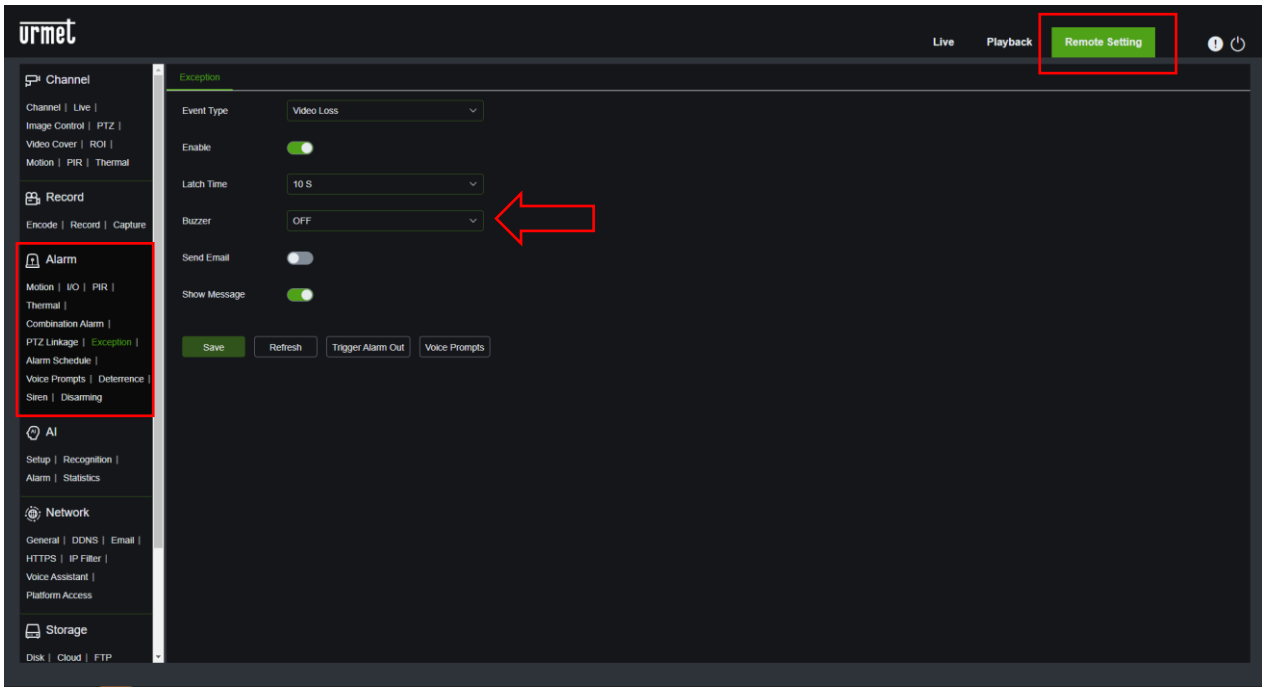

Figure 49: enable the acoustic signal in case of video loss (tab "Remote setting" - section "Alarm" --- > "Exception")

The "*Buzzer*" item (next to the red arrow) allows you to enable the acoustic signal for a period of 10s, 20s, 40s or 1min (via the relevant drop-down menu).

The default value is OFF, that is acoustic signal disabled.

APPENDIX L: RTSP Cameras with NVR Urmet device

Below is a short procedure for integrating the *RTSP Cameras* into the IPerCom system through the Urmet **1098/324P-326P-328P** NVR devices connected in turn to the IPerCom system.

In this way the streaming video of the *RTSP Cameras* will be visible from the system's video door phones (in auto-on, in call both during the unhook time and during the conversation time), from the *Switchboard* application and can also be recorded (and displayed) by the Urmet NVR device.

To implement what is written above, it is recommended to have 3 different subnets: one for the IPerCom devices, one for the Urmet NVR device and a third for the *RTSP Cameras*. In general, you can follow the scheme displayed below, where the IP addresses shown are purely by way of example, as is the type of addressing:

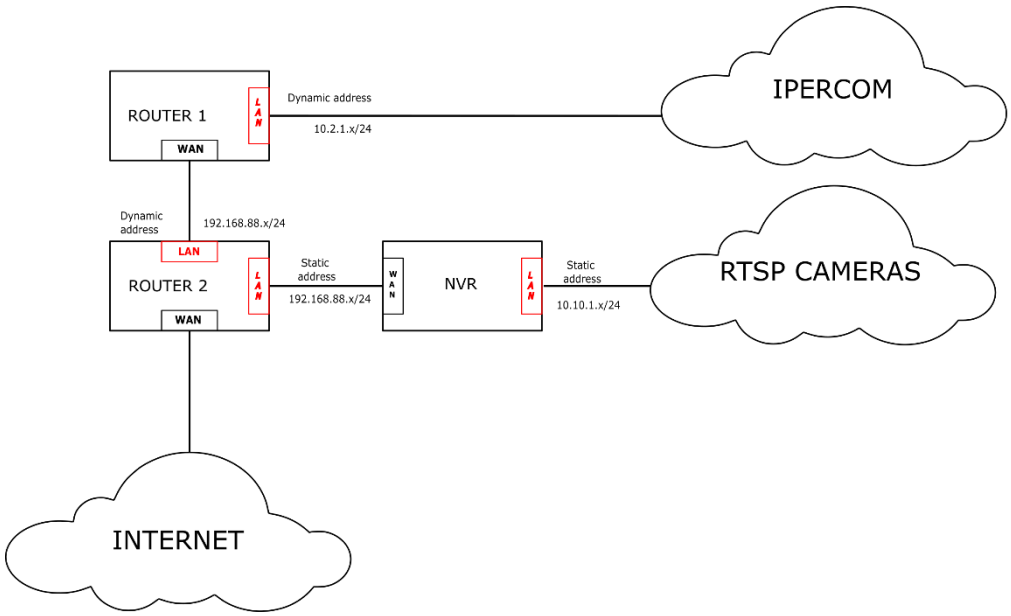

Figure 50: connection diagram for RTSP cameras and Urmet NVR device

The network infrastructure and any configuration of the routers must be carried out by specialized personnel for the correct functioning of the system.

To create the above diagram, follow what is written below.

1. **ROUTER 1**
    - Enable the DHCP Server and ensure that it assigns addresses of the 10.2.1.x/24 type;
    - Set the WAN port in DHCP.

2. **ROUTER 2**
    - Enable the DHCP Server and ensure that it assigns addresses of the 192.168.88.x/24 type;
    - Connect the WAN port to Internet (optional).

3. **NVR Urmet device**
    - Set the WAN port in DHCP;
    - Disable the DHCP Server on PoE interface.

4. **RTSP Cameras**
    - Set the *RTSP Cameras* addressing in static mode with addresses of type 10.10.1.x/24.

In this way the IPerCom devices connected to ROUTER 1 via LAN will have addresses of the type 10.2.1.x/24 while the WAN port of ROUTER 1 and the WAN port of the Urmet NVR device will have IP addresses of the type 192.168.88.x/24. Furthermore, the *RTSP Cameras* connected to the LAN ports of the Urmet NVR device will have static IP addresses of the 10.10.1.x/24 type.

From the *configurator*'s point of view, for each *RTSP Camera* physically connected to the Urmet NVR device it is necessary to add a device of the "*RTSP camera (NVR)*" type from menu "*Other Devices*", as shown below:

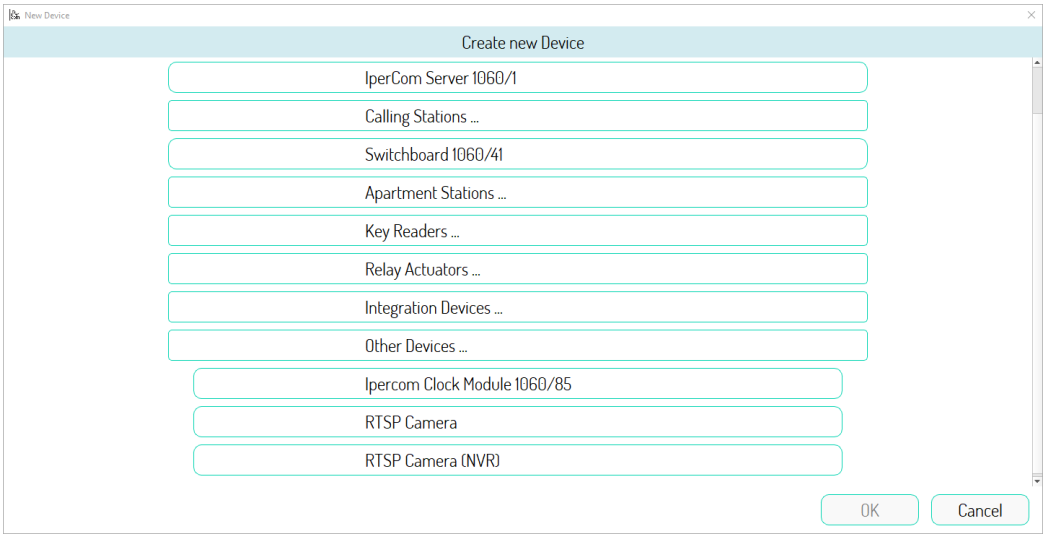

Figure 51: "RTSP Camera (NVR)" device

The following screen appears:

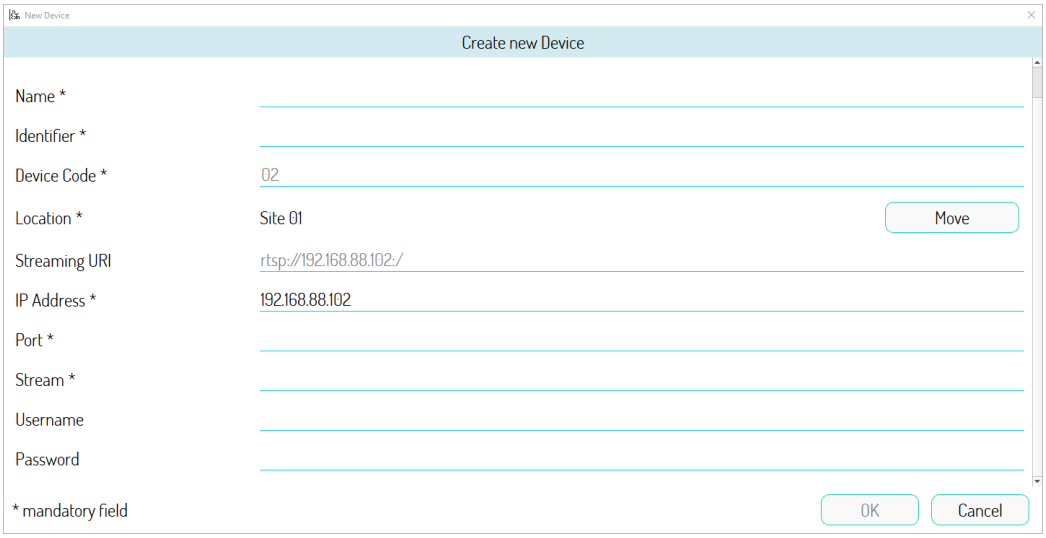

Figure 52: "RTSP Camera (NVR)" device configuration page

The following table shows the meaning of the fields for the "*RTSP Camera (NVR)*" device:

General Settings	
Name	*Meaningful name to be assigned to the RTSP Camera connected to the Urmet NVR device*
Identifier	*Unique identifier of the NVR device (serial number or other)*
Device Code	*Non-editable value*
Location	*Position in the system topology: it is possible to move the device to another topological node by pressing the "Move" button.*
Streaming URI	*Full URI of the streaming video. Non-editable value. It is built automatically by filling in the fields below respecting the following syntax:* *rtsp://[<username>:<password>@] <IP Address>:<port>/<stream>* *The part in square brackets may not be present if the username and password are not defined*
IP Address	*NVR Urmet device IP address (depends on your network configuration)*
Port	*Port through which the Urmet NVR device performs RTSP streaming (variable depending on the Urmet NVR device)*
Stream	*Streaming channel (variable depending on the Urmet NVR device)*
Username	*Username for accessing the Urmet NVR device*
Password	*Password for accessing the Urmet NVR device*

Table 4: parameters for "RTSP Camera (NVR)" device

For Urmet 1098/324P, 1098/326P or 1098/328P NVR devices use as port the port 80 and as stream the string "rtsp/streaming?channel=01&subtype=0". Parameter "01" varies depending on the channel being configured.

An example URI for streaming is as follows:

rtsp://admin:Password1!@192.168.88.158:80/rtsp/streaming?channel=01&subtype=0

where:

- ***<admin>: username for accessing the Urmet NVR device,***
- ***<Password1!>: password for accessing the Urmet NVR device,***
- ***<192.168.88.158>: Urmet NVR device IP address,***
- ***<80>: RTSP streaming port,***
- ***<rtsp/streaming?channel=01&subtype=0>: stream for channel 1.***

APPENDIX M: "*Site name*" and "*Urmet Cloud System ID*" field definition

The **site** represents the system you want to configure, meaning for system the entire network, devices and IPerCom software applications. It is possible to **assign a name to the site** and this is a fundamental data because it allows the site to be uniquely recognized in all the possible applications in which it is involved.

The applications in question are the following:

- the *configurator*, where when creating a new project, you must enter the name of the site;
- *IPerCom Installer Tools*, where the name of the site given in the *configurator* is visible in the "*Site*" tab on the right side of the screen,
- *CallMe Manager*, where the name of the site appears in the list of sites managed by the building manager.

Below are the right steps to fill in the "*Site name*" field.

When creating a new project, *IPerCom Installer Tools* shows the following screen (after connecting to the system to be configured):

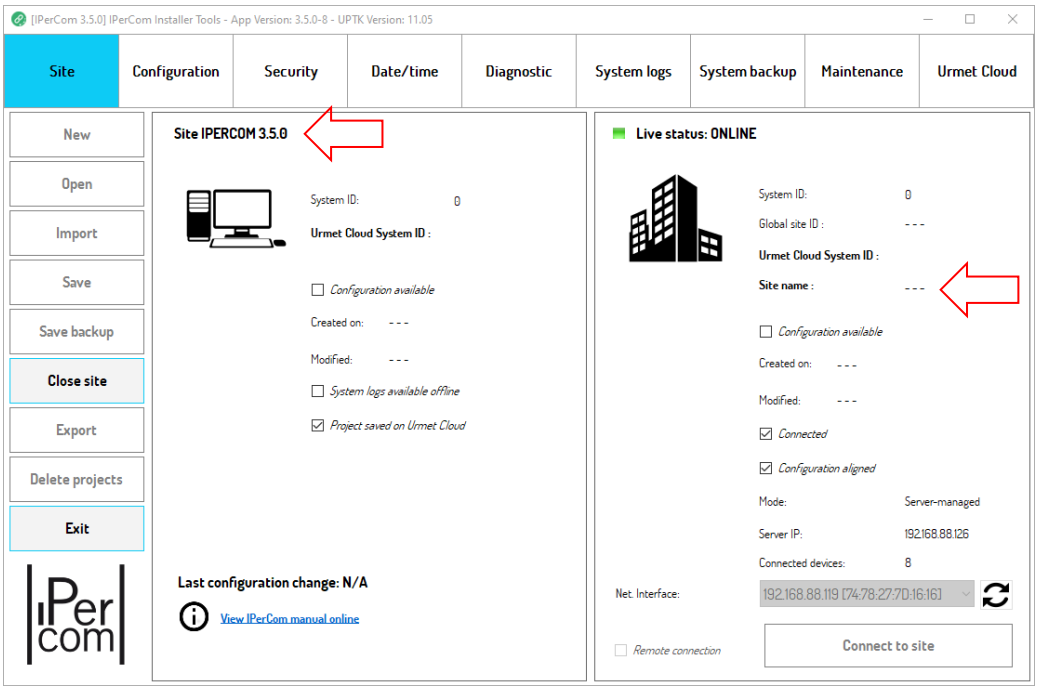

Figure 53: "Site name" field not filled in yet

The "*Site name*" field has not yet been filled in and at the top right the name of the project is used as the site name (red arrows).

In this phase it is necessary to create a new configuration via the "*Create*" button in the "*Configuration*" tab:

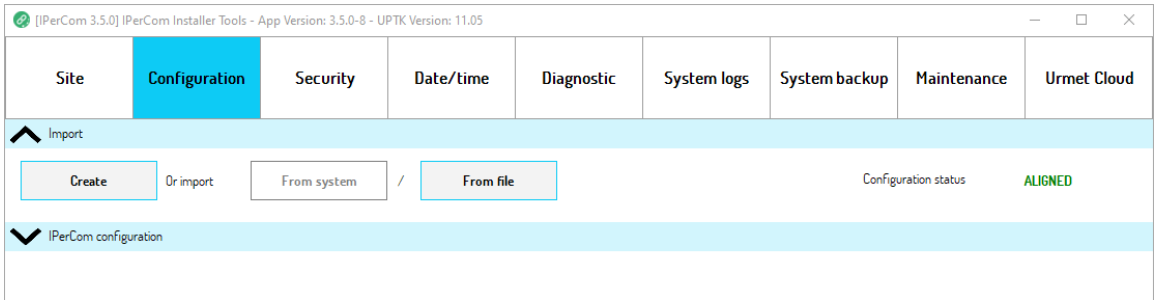

Figure 54: creation of a new configuration

The screen that appears is the following:

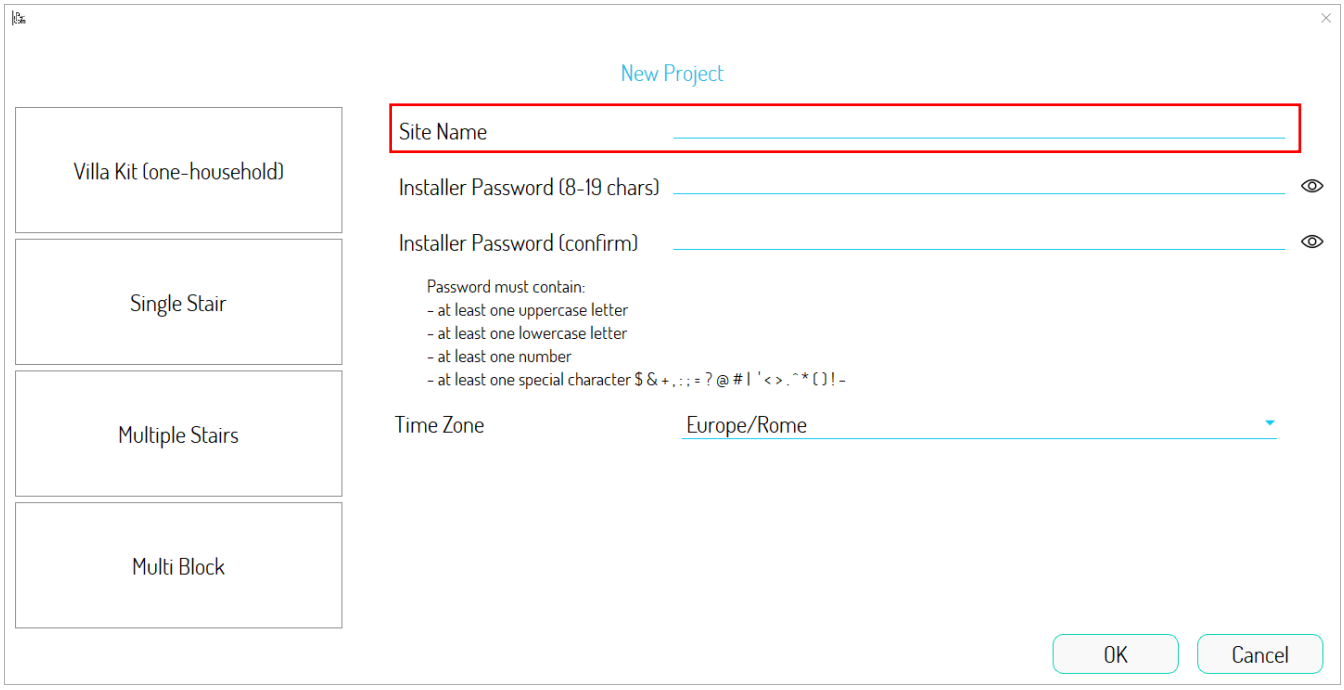

Figure 55: "Site Name" field when creating a configuration

The first data to enter is the site name (red box).

After entering the name of the site (for example "*Turin via Bologna 188C*"), *IPerCom Installer Tools* shows this data on the right and left side of the screen (after having applied the configuration to the site):

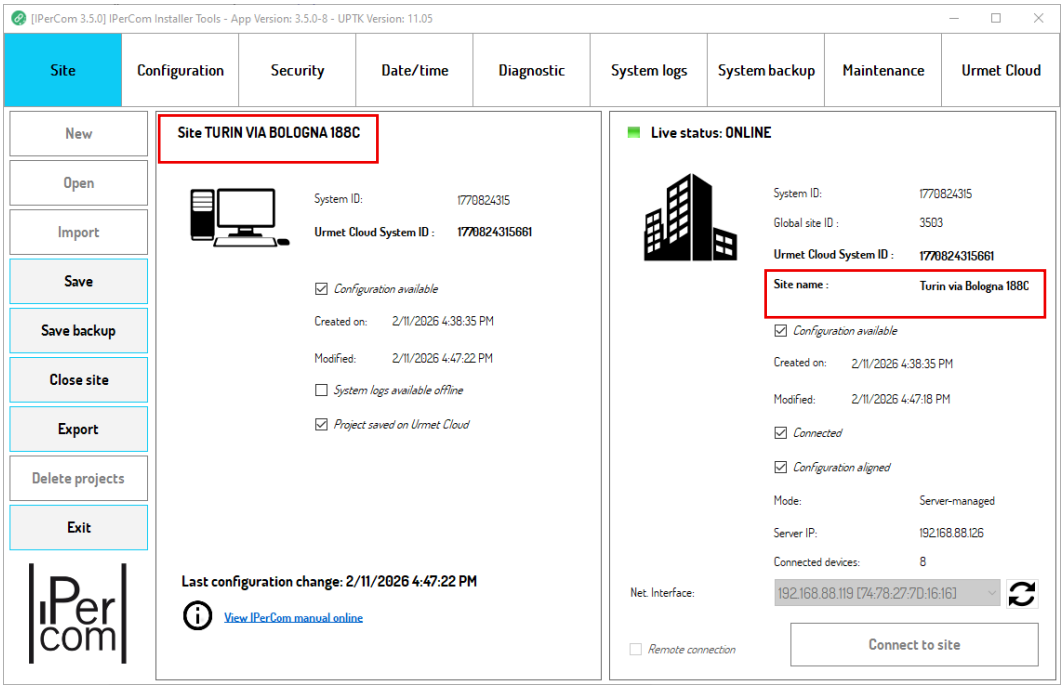

Figure 56: "Site name" field filled in in IPerCom Installer Tools

The site name can subsequently be changed from the *configurator* and *IPerCom Installer Tools* will always show the aligned data (after having applied the configuration).

After applying the configuration, the "*Urmet Cloud System ID*" field, the "*Global site ID*" field and the "*System ID*" field are also filled in:

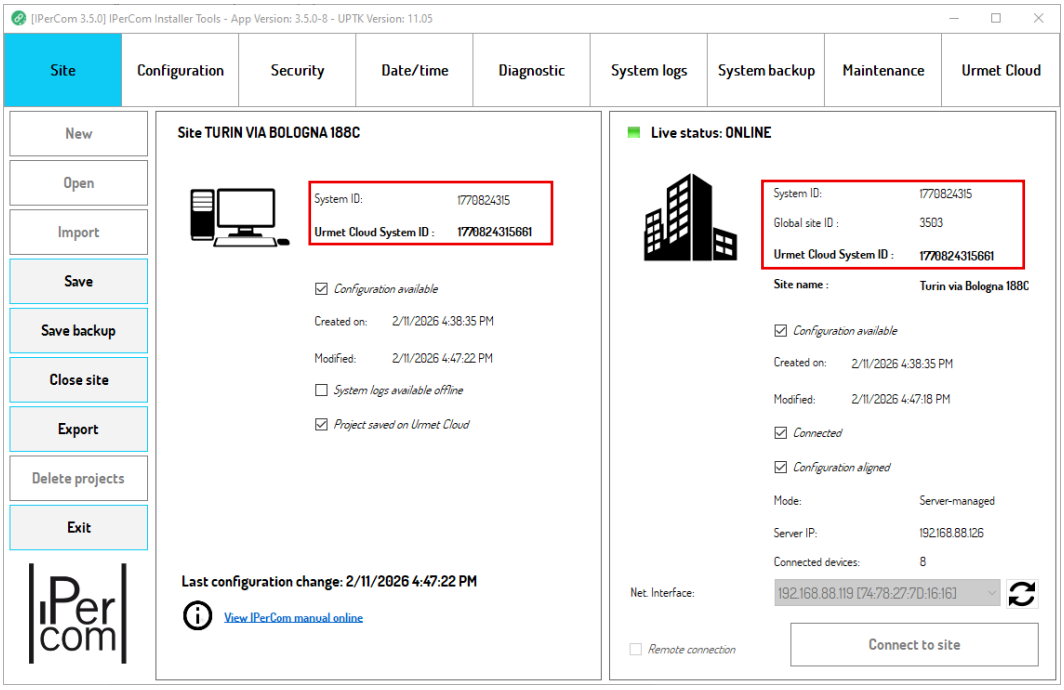

Figure 57: different IDs fields filled in

If the site is imported into the *CallMe Manager* application, to ensure that the correct site has been imported, it is advisable to check that:

- "*Site Name*" fields in *CallMe Manager* app and *IPerCom Installer Tools* app are the same;
- "*ID*" field reported in *CallMe Manager* app and "*Urmet Cloud System ID*" field reported in *IPerCom Installer Tools* app are the same.

To do this, when you start the *CallMe Manager* application, immediately after the login phase, in the site list window, check that the two fields in question are consistent:

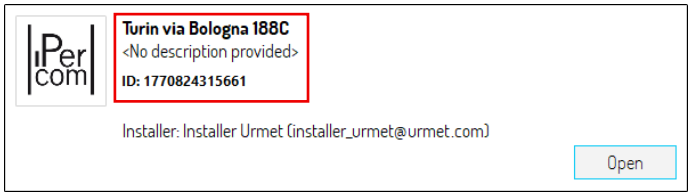

Figure 58: first check of site name and "Urmet Cloud System ID" field

After pressing the "*Open*" button, do the same check on *CallMe Manager* application home page:

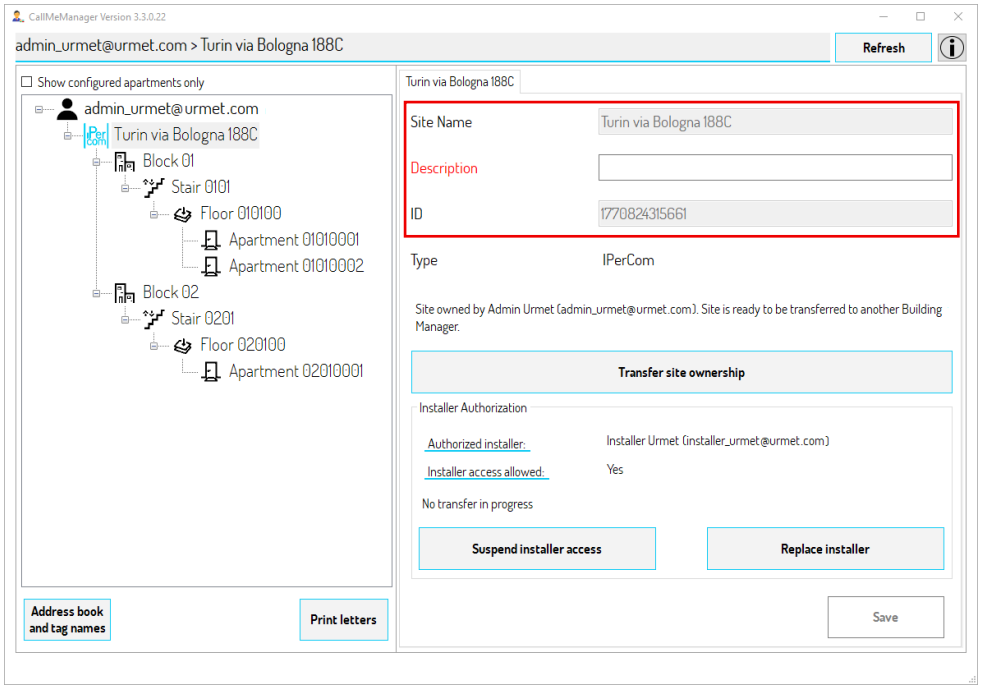

Figure 59: "Global site ID" and "Site name" fields in CallMe Manager

In this way, through the name of the site and the "*Urmet Cloud System ID*" field, you have common and unique references between the *IPerCom Installer Tools* and *CallMe Manager* applications in relation to a site.

APPENDIX N: IPassan integration with IPerCom

The integration of the IPassan system with the IPerCom system is carried out as follows.

Use the *configurator* to:

- create the topological structure of the system (blocks, stairs, floors and apartments);
- add the calling stations and enable the respective passages (pedestrian door and/or driveway gate);
- add any switchboards;
- add the *IPassan Controller* devices in the predetermined topological nodes (site node, block node or other);
- select the "*Lift Control*" option in the configuration page if you want the IPassan Controller to also manage the lift interfaces of the system.

The *IPassan Controller* acts on all passages within its topological group.

At this point, in the *IPerCom Installer Tools* configurator, go to the "*Project*" tab, then to the "*Export*" tab:

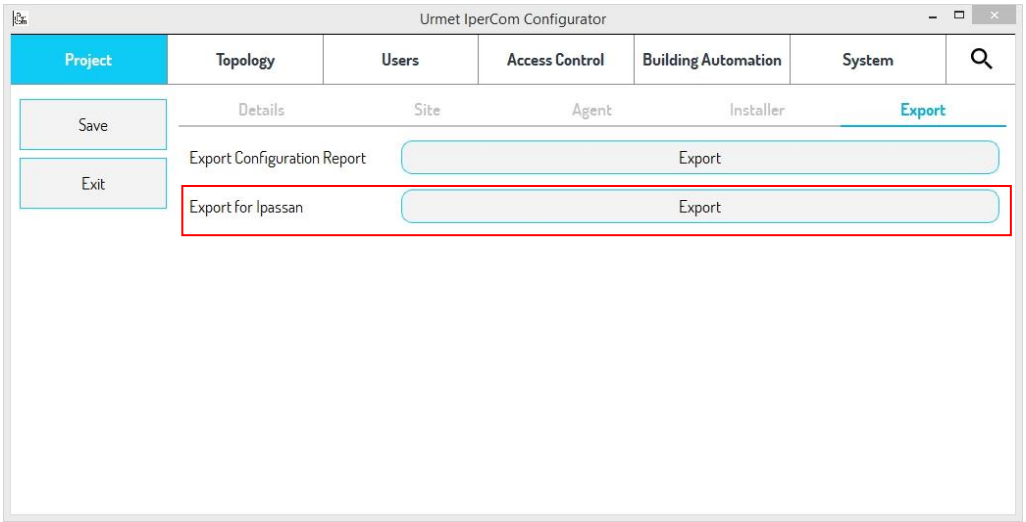

Figure 60: iPassan export

Corresponding to the label "*Export for IPassan*", press the "*Export*" button: an xml file is generated.

The saved xml file must then be imported via the *IPassan Manager* application. The integration can then be completed by adding users, access profiles and other useful to manage advanced access control.

APPENDIX O: How to properly turn 1060/1 *Server* on and off.

The 1060/1 *Server* should never be turned off by directly disconnecting the power cord, as this can cause irreversible damage to the internal memory. The correct way to turn it on and off is shown below.

Switching on the 1060/1 *Server*

After connecting the 1060/1 *Server* to the power supply, the on/off key LED is yellow, as shown below:

Figure 61: button ON/OFF

Briefly press the button shown in the figure and wait for the LED to turn green: the 1060/1 *Server* is on.

Switching off the 1060/1 *Server*

With the LED green, briefly press the button shown in the figure above and wait for the LED to turn yellow. The 1060/1 *Server* is off and only now you can disconnect the power cord.

APPENDIX P: Connection between 1060/1 *Server* and UPS device.

This appendix applies to UPS devices model BK350EI/BK500EI/BK650EI. The correct connection of a UPS device and the 1060/1 Server is required:

- a power cable between the UPS device and the 1060/1 *Server* (not supplied with the product);
- an "*RJ45 to USB*" cable between the UPS device and 1060/1 *Server* (supplied with the UPS device product).

The power cord must be as shown below (input type C14 and socket type C15):

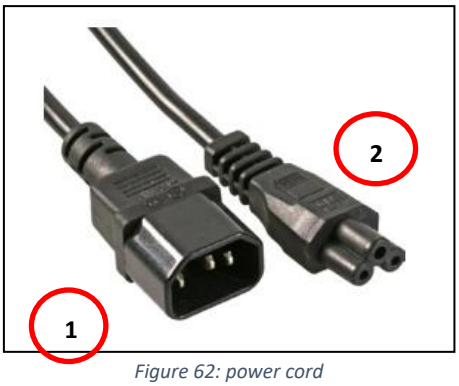

Figure 62: power cord

Input type C14 (1) must be connected to the UPS device while socket C15 (2) must be connected to the power transformer supplied with the 1060/1 *Server*.

For the "*RJ45 to USB*" cable the end with the RJ45 connector must be connected to the UPS device and the end with the USB connector must be connected to one of the three USB inputs of 1060/1 Server.

In this way, on the **Diagnostics** tab of *IPerCom Installer Tools* by selecting 1060/1 *Server* from the devices in the system and pressing button  , a screen with a series of detailed information about the UPS operating status appears, as shown below:

Figure 63: UPS information

APPENDIX Q: Replacing a 1060/1 *Server* that is no longer working.

The procedure for correctly replacing a 1060/1 *Server* that is no longer working is as follows:

1) in a network separated from the IPerCom system, upgrade the new *server* 1060/1 to the IPerCom version in the system, using *IPerCom Installer Tools*;

2) disconnect the malfunctioning *Server* 1060/1 from the system;

3) if the configuration associated to the project is not up-to-date with the system site configuration, import it from the system using the *IPerCom Installer Tools* (if *IPerCom Installer Tools* does not detect any devices, wait some minutes; if this procedure does not work, in the "*Maintenance*" tab of *IPerCom Installer Tools* press the "*Force serverless mode*" button);

4) replace the MAC address of the malfunctioning *Server* 1060/1 with the MAC address on the packaging of the new one, save the project and close the *IPerCom Installer Tools*.

5) connect the new *Server* 1060/1 to the system;

6) open *IPerCom Installer Tools* and then the project, connect to the system and distribute the new configuration.

APPENDIX R: First upgrade of a system via Server 1060/1

To upgrade a system (just installed and not configured) to version 2.1.2 via *Server* 1060/1, follow the steps below:

- using *IPerCom Installer Tools*, upgrade the *Server* 1060/1 (or *Servers* 1060/1) to the required IPerCom firmware version;

  The Servers 1060/1 are upgraded on a network where, in addition to the Servers, there is only one PC where the IPerCom Installer Tools application is installed.

- use *IPerCom Installer Tools* to create a project and connect to the system;
- from the "*Configuration*" tab press the "*Create*" button to create a new configuration and choose the system topology;
- add the *Servers* 1060/1 to the configuration via the "*Devices*" tab and the "*Add new device*" button;
- in the *Server* configuration page assign a name to the device and associate the MAC address through the button in the red box:

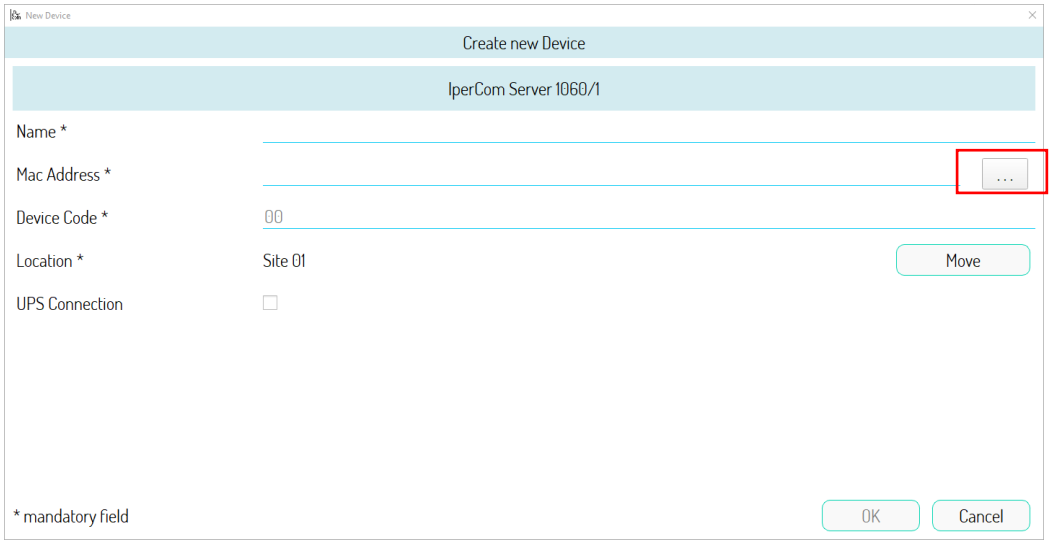

Figure 64: IperCom Server 1060/1

- in the "*System*" tab under the "*Maintenance Settings*" section, enable the "*Automatic Server Upgrade*" item:

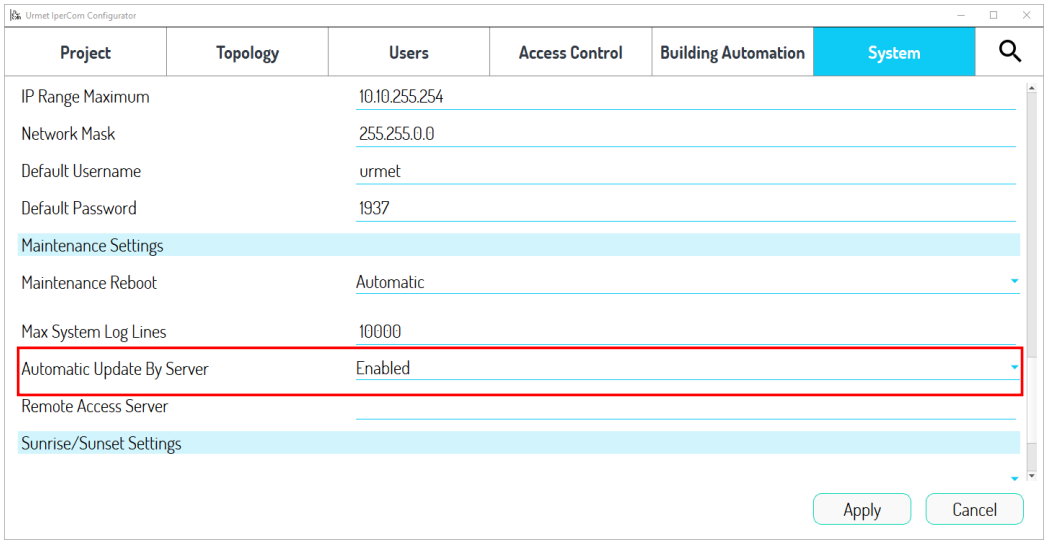

Figure 65: automatic update via IperCom server

- press the "*Apply*" button, save the configuration, and then distribute it.

At this point, after connecting the *Servers* 1060/1 to the IPerCom network, one of them will upgrade the rest of the system to the same version to which it was upgraded. For subsequent upgrades, it will only be necessary to upgrade the system *Servers* 1060/1. Any new devices connected to the system will be automatically upgraded via *Server* 1060/1.

Devices/applications to be upgraded may also have firmware/software versions lower than IPerCom version 2.1.1

To upgrade the devices/applications of an IPerCom system via Server 1060/1, they must be reachable via the network from the same server.

APPENDIX S: Call to several Switchboard applications each linked to a CallMe app

The following applies to both the 1060/41 and 1060/42 Switchboards.

Call to competence Switchboard

If an apartment (or a calling station) calls more than one competence switchboard (each with the call forwarding function enabled) the only **CallMe** app that receives the call is the one linked to the switchboard placed on the lowest node of the topological path of the calling device.

Considering as an example a system with a topological structure like the one shown below:

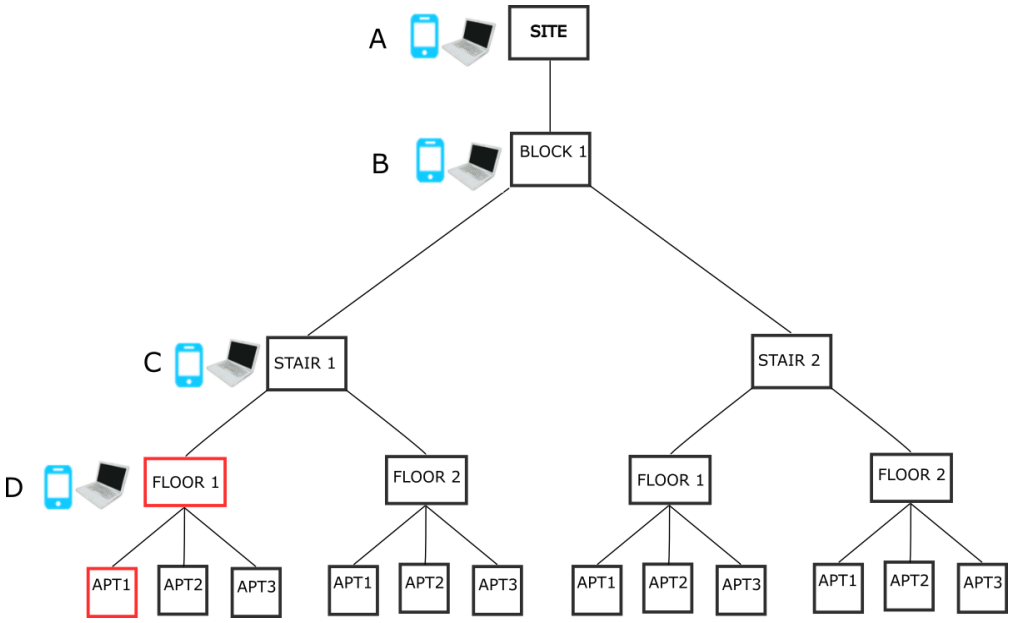

Figure 66: Topological structure with several switchboards

APT1 apartment (in red) has as competence switchboards those placed on the nodes "*Floor 1*", "*Stair 1*", "*Block 1*" and "*Site*". If APT1 apartment calls competence switchboards, they ring at the same time. If all are connected to their own **CallMe** app, the only one that receives the call is that of the switchboard placed on the lowest node of the topological path of the apartment, that is (in the case shown in the figure) the **CallMe** app linked to the **Switchboard** application of the "*Floor 1*" node (in red).

*If on the lowest node the **Switchboard application** is not linked to any **CallMe** app, the application that receives the call is the first one found on the nodes immediately higher (in the example above, the "Stair 1" node).*

If on the lowest node of the topological path of the calling device (or in those immediately above) there are several **Switchboard** applications (each with the call forwarding function enabled), it is possible to establish through the *configurator* which **CallMe** app should receive the call.

For example, if on the "*Floor 1*" node in the figure above there are 3 switchboards with the call forwarding function enabled, the list of switchboards present on the topological node in question appears on the configuration page of any of the 3 in the **CallMe Priority** section:

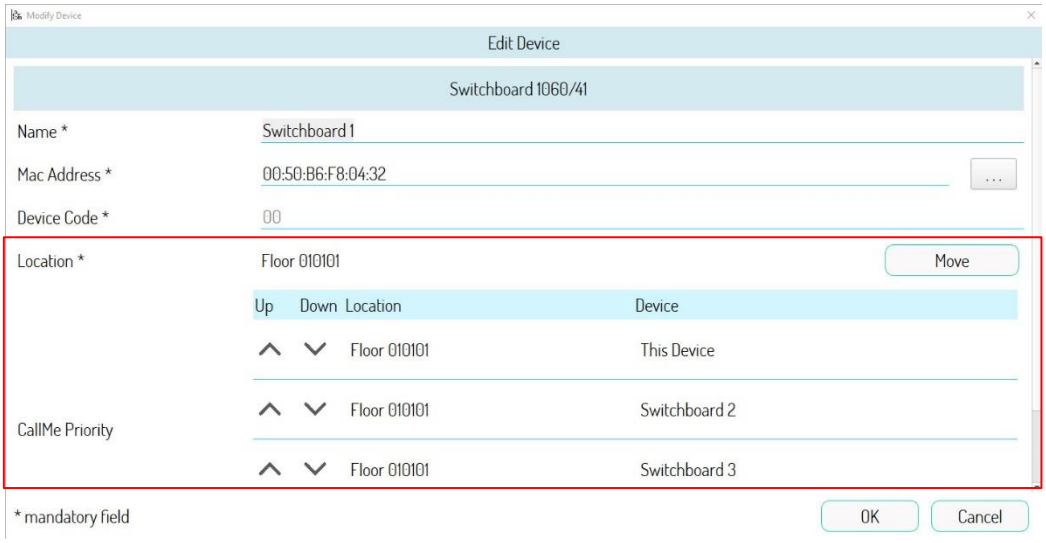

Figure 67: Configuration page with several Switchboard applications on the plant

The list can be modified using the ^ and v buttons.

*"This Device" represents Switchboard 1, i.e. the **Switchboard** application whose configuration page has been opened via the configurator.*

The **CallMe** app associated with the first **Switchboard** application in the list (box in red) is the one that will receive the call if the APT1 apartment calls the competence switchboards. If you want that another **CallMe** app receives the call, you need to reorder the list and enter the **Switchboard** application connected to the **CallMe** app that you want to ring in the first place.

*In the event that not all **Switchboard** applications of the same node are connected to the **CallMe** app, the **CallMe** app that rings is the one related to the first **Switchboard** application found in the list.*

*Any other **Switchboard** applications present on the other nodes of the same level (floor, stair, or block) will also appear in the list. These are not to be considered as they are not on the topological path of the calling device.*

CALL TO ALL SWITCHBOARDS

If an apartment (or a calling station) calls from address book all switchboards of the plant (each one with the call forwarding function enabled) the only **CallMe** app that receives the call is the one linked to the switchboard placed on the highest node of the topological structure.

Considering as an example a system with a topological structure like the one shown below:

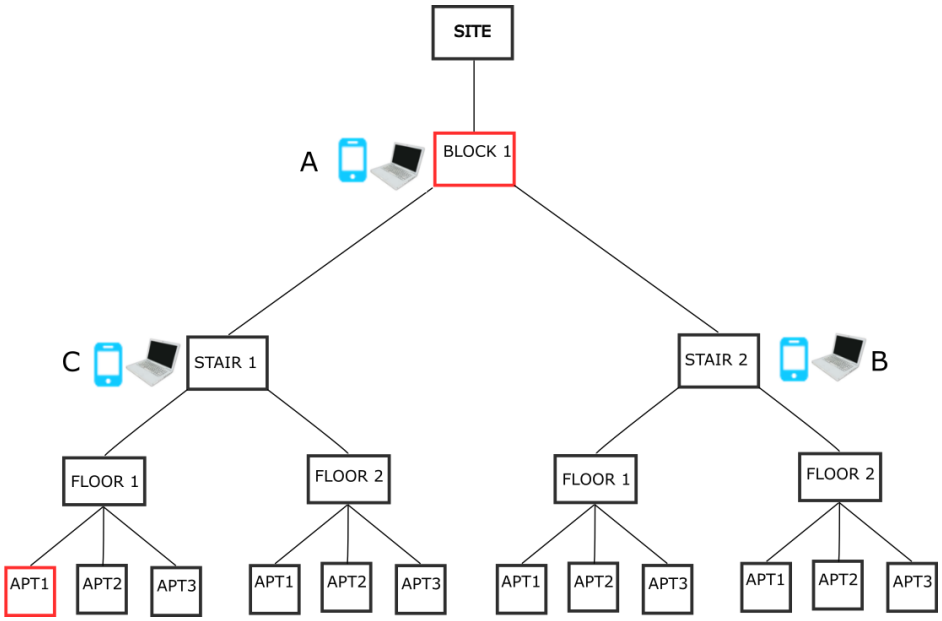

Figure 68: Topological structure with several switchboards

the APT1 apartment (in red) can call all the switchboards in the system from address book, i.e. those on the "*Stair 1*", "*Stair 2*" and "*Block 1*" nodes. These will ring simultaneously but if all are connected to their own **CallMe** app, the only one that receives the call is that of the switchboard placed on the highest node, i.e. (in the case shown in the figure) the **CallMe** app linked to the **Switchboard** application of the "*Block 1*" node (in red).

If on the highest node there are several **Switchboard applications** (each with the call forwarding function enabled), it is possible to establish through the *configurator* which **CallMe** app shall receive the call.

If there are 3 switchboards with the call forwarding function enabled on the "*Block 1*" node in the figure above, the list of switchboards present on the topological node in question appears on the configuration page of any of the 3 in the **CallMe Priority** section:

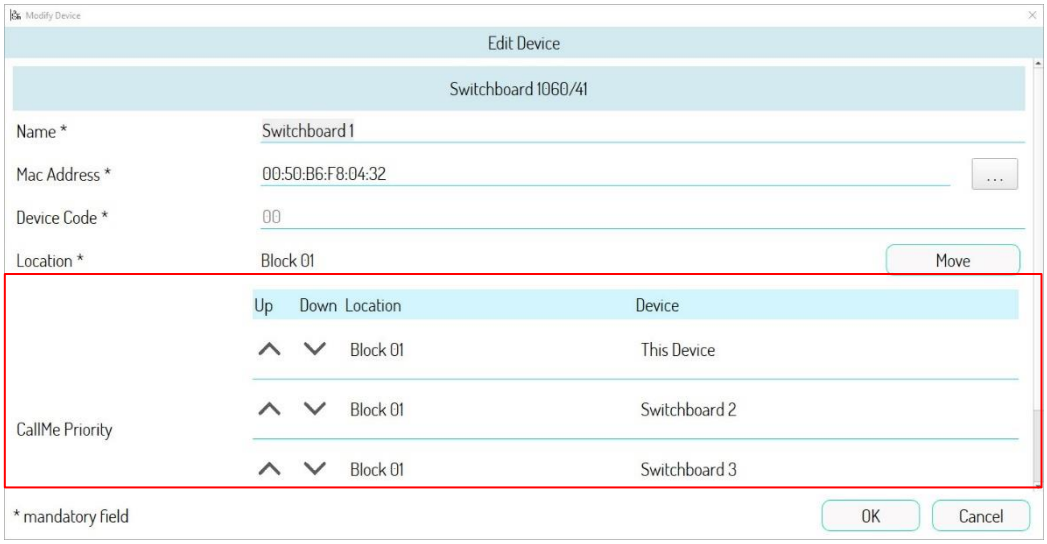

Figure 69: Configuration page with several Switchboard applications on the plant

The list can be modified using the ^ and v buttons.

*"This Device" represents Switchboard 1, i.e. the **Switchboard** application whose configuration page has been opened via the configurator.*

The **CallMe** app associated with the first **Switchboard** application in the list (box in red) is the one that will ring after a call to all switchboards. If you want another **CallMe** app to ring, you need to reorder the list and put the **Switchboard** application connected to the **CallMe** app you want to ring in the first place.

*In the event that not all **Switchboard** applications of the "Block 1" node are connected to the **CallMe** app, the **CallMe** app that rings is the one relating to the first **Switchboard** application found in the list and connected to the app.*

*In general, any other **Switchboard** applications present on the other nodes of the same level (floor, stair and block) will also appear in the list. These (if connected to a **CallMe** app) are to be taken into consideration as the call is directed to all switchboards in the system.*

APPENDIX T: *CallMe* contacts

To ensure that the contacts in the address book of your video door phone also appear in your **CallMe** app, they must have the relevant box selected in the *configurator*.

To do this, the following example is shown with 3 apartments on the same floor:

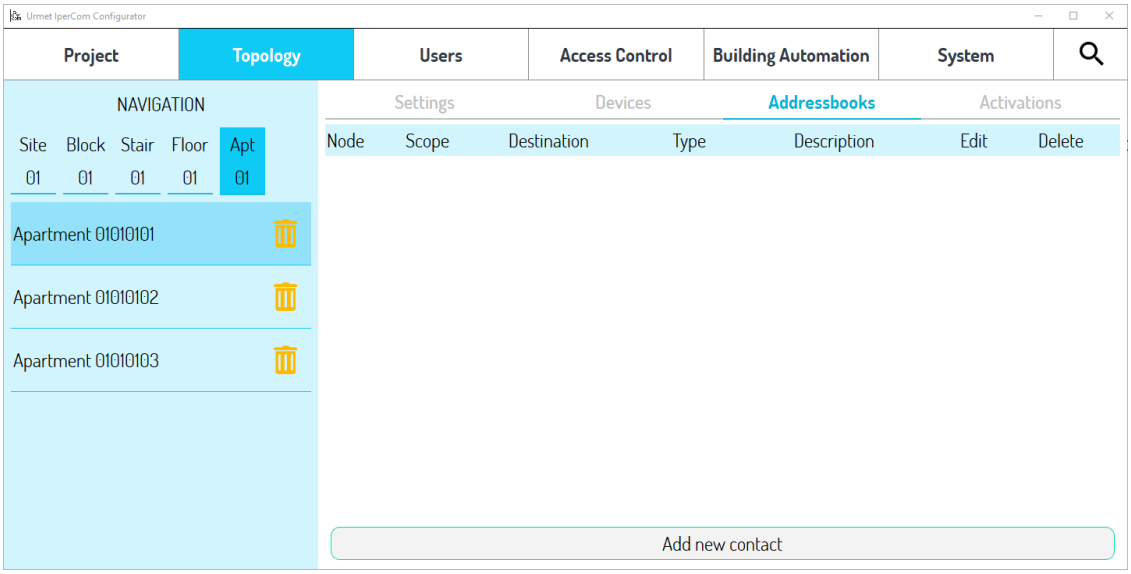

Figure 70: Topological structure with tab "Addressbooks"

The resident of the apartment "*01010101*" wants to have both the apartment "*01010102*" and the apartment "*01010103*" in the address book of his video door phone, while on his own *CallMe* application he only wants to have the apartment "*01010102*". This means that when creating contacts via the *configurator*, the contact relating to apartment "*01010102*" has the "*CallMe*" box selected (in addition to the "*Video door phone with address book*" box):

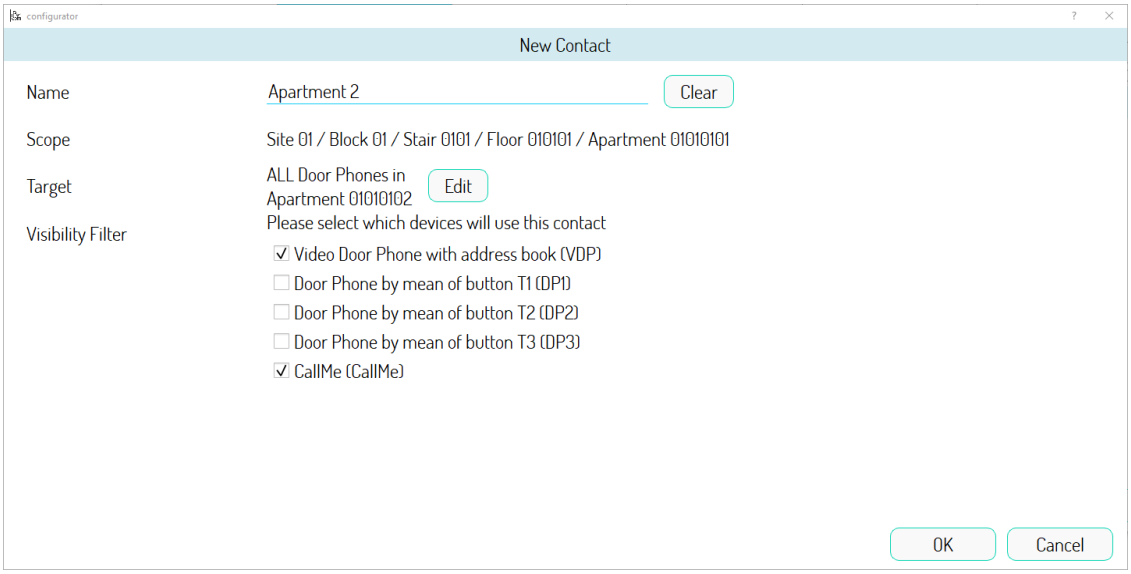

Figure 71: checkbox "CallMe" selected

Instead, the contact relating to the apartment "*01010103*" has the "*Video door phone with address book*" box selected but not the "*CallMe*" box selected:

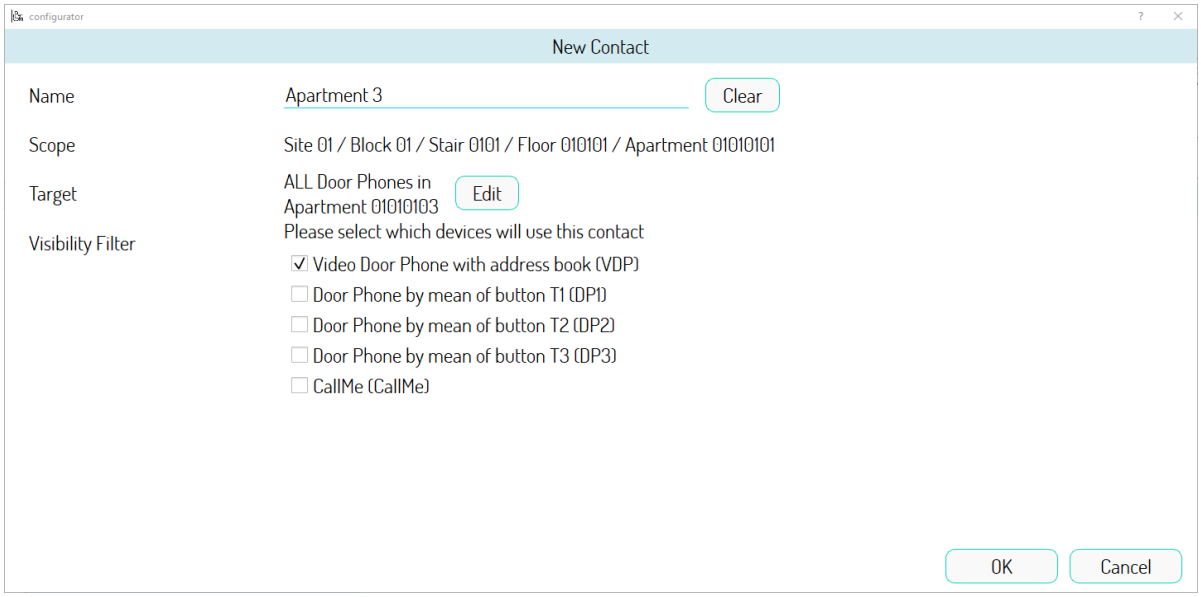

Figure 72: checkbox "CallMe" not selected

The result of this configuration is that both contacts are present on the 7 '' *MAX* video door phone (for example):

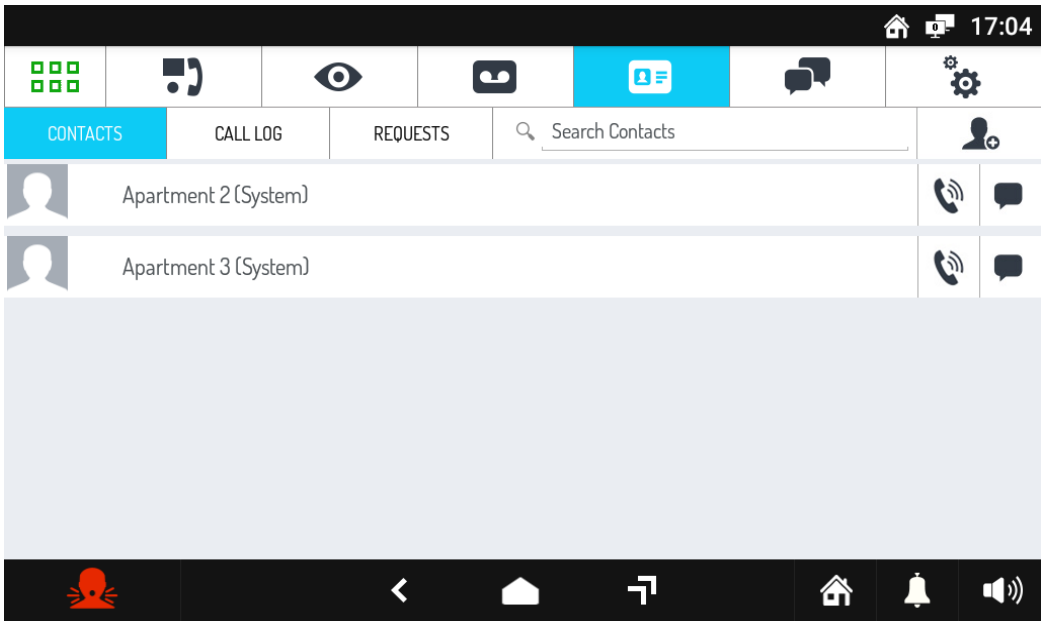

Figure 73: contacts on video door phone

Instead, on the relevant *CallMe* app, only the contact relating to the apartment "*01010102*" appears in the **Address Book** section:

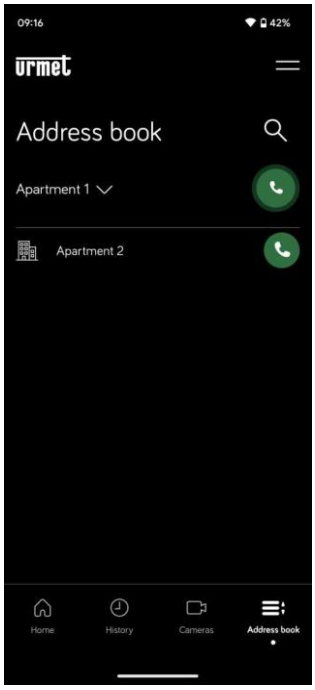

Figure 74: app CallMe contacts

The contacts generated by the video door phones with address book (MAX, VOG7, Basic and IPerCom Client 1060/43) by means of an "invitation" (and not via the configurator) appear directly on the ***CallMe*** *app.*

APPENDIX U: IPerCom device consumption

A table is shown where next to each IPerCom device the relative consumption in Watt referred to the PoE power supply is reported:

Reference	Description	Consumption [W]
1060/12-13	Call Module Soft Touch	7,6
1060/17-18-23	Call Module Vandal Proof	9,6
1060/16	Call Module with face recognition	12,2
1060/48	Modular Calling Station Alpha	12 (*)
1060/48T	Modular Calling Station Alpha Touch	12 (*)
1060/71-74-75-78	Entry Panel Sinthesi S2	9,6 (*)
1060/21	Entry Panel Mikra	3,5
1060/22	Private Call Module	3,5
1060/33-34	Entry Panel Mikra Plus/Digital	12 (*)
1761/31-32-33	7'' VOG^{7} Video Door Phone	12 (**)
1761/6	5'' VOG^{5} Video Door Phone	4,5
1761/15-16-18-19	5'' VOG^{5+} Video Door Phone	4,5 (**)
1717/31-32-33-34-41	7'' MAX Video Door Phone	12
1717/21-22-23	10'' MAX Video Door Phone	11 (**)
1761/23	10'' Video Door Phone	11
1741/1-2-3	7'' Basic Video Door Phone	10
1160/3	Miro Door Phone	6
1060/86	Key Reader	4,8
1060/45	Key Reader	5
1060/84	Relay Actuator	2,4
1083/59	Gateway IPerCom – 2Voice	4
1060/85	Clock Module	6
1060/37	Lift Interface	7,2

Table 5: IPerCom devices and their consumption

The IPerCom devices not listed in this table have a consumption equal to 0W.

(*): these values refer to the configuration that absorbs the most;

(**): the corresponding U-version devices have the same consumption.

APPENDIX V: Features for which 1060/1 Server is mandatory

Depending on the type of system required and/or on the performance that the system must support, the presence of at least one 1060/1 *Server* may be mandatory.

As regards the type of system, we can distinguish the cases in which the system is not in IPerCloud mode and the case in which it is. Regarding the first case, the line highlighted in yellow requires the presence of at least one 1060/1 *Server* in the system:

Apartment number	Device number	Resident and non-resident number
≤ 1000	≤ 1000	≤ 1000
> 1000 (max 4000)	> 1000 (max 4000)	> 1000 (max 10000)

Table 6: presence of a Server 1060/1

Regarding the second line, it is sufficient for only one of the 3 conditions above to occur for Server 1060/1 to be mandatory.

In addition to the above, in the case of IPerCom systems in IPerCloud mode, the 1060/1 *Server* is necessary if at least one of the conditions reported below is verified on the system:

- at least one calling station other than *Call Module* 1060/16, *Modular Calling Station with 1060/48*, *Modular Calling Station with 1060/48 Touch, Entry Panel* 1060/33-34, *Entry Panel* 1060/21;
- several IPerCloud apartments greater than 200;
- only *Entry Panels* 1060/33-34 with several IPerCloud apartments greater than 32;
- only *Entry Panels* 1060/21 with several IPerCloud apartments greater than 20.

The performances that require the presence of a 1060/1 *Server* are the following:

- display of system logs on *IPerCom Installer Tools*;
- modification of the system configuration remotely (*Server* 1060/1 is required on the remote system whose configuration is to be modified);
- saving the system configuration (backup) manually or automatically in periodic mode;
- centralized update of devices (via *Server* 1060/1).

The same 1060/1 *Server* is sufficient to cover one or more conditions among those listed above and one or more performances among the 4 listed above. The presence of multiple 1060/1 *Server* on a system is dictated by requests on the same system.

APPENDIX W: Devices supported by IPerCom versions

A table is shown where for each officially released version of IPerCom the set of supported devices is indicated. This table is of fundamental importance for installers as:

- in case of replacement or addition of a new device, this may not be compatible with the version currently installed on the system, and this would require an update of the entire system;
- if the firmware version of an IPerCom system is updated, a device that has already been installed and configured may no longer be supported.

Legend:

VDP = Vide Door Phone

CM = Call Module

EP = Entry Panel

Supported devices	Ref.	Ver.	IPERCOM versions												
			1.0.0 dec-18	1.1.0 dec-18	1.2.0 apr-19	1.3.0 sep-19	1.4.0 nov-19	2.0.0 dec-20	2.1.0 oct-21	2.1.1 apr-22	2.1.2 may-22	2.2.0 dec-22	3.0.0 oct-23	3.1.0 oct-24	3.2.0 dic-24
VDP IP 7"	1717/3x	A31S	yes	yes	yes	yes	yes	yes	no	no	no	no	no	no	no
VDP IP 7"	1717/4x	A31S	yes	yes	yes	yes	yes	yes	no	no	no	no	no	no	no
KEY READER	1060/82		yes	yes	yes	yes	yes	yes	yes	yes	yes	no	no	no	no
CM ELEKTA	1060/1x		yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
EP SINTHESI	1060/7x		yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
SWITCHBOARD	1060/41		yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
VDP IP 7"	1717/3x	A64	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
VDP IP 7"	1717/4x	A64	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
RELAY ACTUATOR	1060/84	2.07	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
RTSP CAMERAS			yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
DOOR PHONE	1160/3		no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
CLOCK MODULE	1060/85		no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
EP MIKRA2	1060/21		no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
PRIVATE EP MIKRA2	1060/22		no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
RELAY ACTUATOR	1060/84	3.04	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
GATEWAY IP-2VOICE	1083/59		no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
SERVER	1060/1		no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes
EP ALPHA	1060/48		no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes
KEY READER	1060/86		no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes
RELAY ACTUATOR	1060/84	4.05	no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes
SERVER iPerTAlk	1375/1x		no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes
CONTROL. IPASSAN			no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes
LIFT INTERFACE	1060/37		no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes
CM ELEKTA STEEL	1060/23		no	no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes
VDP 7'' IP VOG[7]	1761/3x		no	no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes
VDP 5" VOG[5]	1761/6		no	no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes
VDP MAX 10''	1717/2x		no	no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes
VDP 7" BASIC	1741/1-2		no	no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes
VDP 7" BASIC	1741/3		no	no	no	no	no	no	no	no	no	no	yes	yes	yes
IPERCOM CLIENT	1060/43		no	no	no	no	no	no	yes	yes	yes	yes	yes	yes	yes
1060.WIN			no	no	no	no	no	no	no	yes	yes	yes	yes	yes	yes
EP MIKRA PLUS	1060/33		no	no	no	no	no	no	no	no	no	yes	yes	yes	yes
EP MIKRA DIGITAL	1060/34		no	no	no	no	no	no	no	no	no	yes	yes	yes	yes
VDP IP 5" VOG[5+]	1761/1x		no	no	no	no	no	no	no	no	no	yes	yes	yes	yes
SERVER iPerTAlk	1375/1x	V1	no	no	no	no	no	no	no	no	no	yes	yes	yes	yes
VDP 7'' IP VOG[7]	1761/3xU		no	no	no	no	no	no	no	no	no	no	no	yes	yes
VDP MAX 10''	1717/2xU		no	no	no	no	no	no	no	no	no	no	no	yes	yes
VDP IP 5" VOG[5+]	1761/1xU		no	no	no	no	no	no	no	no	no	no	no	yes	yes
KEY READER	1060/45		no	no	no	no	no	no	no	no	no	no	no	yes	yes

Supported devices	Code	Ver.	IPERCOM versions											
			1.0.0	1.1.0	1.2.0	1.3.0	1.4.0	2.0.0	2.1.0	2.1.1	2.1.2	2.2.0	3.0.0	3.1.0	3.2.0
			dec-18	dec-18	apr-19	sep-19	nov-19	dec-20	oct-21	apr-22	may-22	dec-22	oct-23	oct-24	jan-25
SWITCHBOARD	1060/42		no	no	no	no	no	no	no	no	no	no	no	no	yes
VDP 10''	1761/23		no	no	no	no	no	no	no	no	no	no	no	no	yes

Table 7: device compatibility with IPerCom versions (first part)

Supported devices	Ref.	Ver.	IPERCOM versions													
			3.3.0 July-25	3.4.0 Dic-25	3.5.0 Feb-26											
VDP IP 7"	1717/3x	A31S	no	no	no											
VDP IP 7"	1717/4x	A31S	no	no	no											
KEY READER	1060/82		no	no	no											
CM ELEKTA	1060/1x		yes	yes	yes											
EP SINTHESI	1060/7x		yes	yes	yes											
SWITCHBOARD	1060/41		yes	yes	yes											
VDP IP 7"	1717/3x	A64	yes	yes	yes											
VDP IP 7"	1717/4x	A64	yes	yes	yes											
RELAY ACTUATOR	1060/84	2.07	yes	yes	yes											
RTSP CAMERAS			yes	yes	yes											
DOOR PHONE	1160/3		yes	yes	yes											
CLOCK MODULE	1060/85		yes	yes	yes											
EP MIKRA2	1060/21		yes	yes	yes											
PRIVATE EP MIKRA2	1060/22		yes	yes	yes											
RELAY ACTUATOR	1060/84	3.04	yes	yes	yes											
GATEWAY IP-2VOICE	1083/59		yes	yes	yes											
SERVER	1060/1		yes	yes	yes											
EP ALPHA	1060/48		yes	yes	yes											
KEY READER	1060/86		yes	yes	yes											
RELAY ACTUATOR	1060/84	4.05	yes	yes	yes											
SERVER iPerTAlk	1375/1x		yes	yes	yes											
CONTROL. IPASSAN			yes	yes	yes											
LIFT INTERFACE	1060/37		yes	yes	yes											
CM ELEKTA STEEL	1060/23		yes	yes	yes											
VDP 7'' IP VOG[7]	1761/3x		yes	yes	yes											
VDP 5" VOG[5]	1761/6		yes	yes	yes											
VDP MAX 10''	1717/2x		yes	yes	yes											
VDP 7" BASIC	1741/1-2		yes	yes	yes											
VDP 7" BASIC	1741/3		yes	yes	yes											
IPERCOM CLIENT	1060/43		yes	yes	yes											
1060.WIN			yes	yes	yes											
EP MIKRA PLUS	1060/33		yes	yes	yes											
EP MIKRA DIGITAL	1060/34		yes	yes	yes											
VDP IP 5" VOG[5+]	1761/1x		yes	yes	yes											
SERVER iPerTAlk	1375/1x	V1	yes	yes	yes											
VDP 7'' IP VOG[7]	1761/3xU		yes	yes	yes											
VDP MAX 10''	1717/2xU		yes	yes	yes											
VDP IP 5" VOG[5+]	1761/1xU		yes	yes	yes											
KEY READER	1060/45		yes	yes	yes											

Supported devices	Code	Ver.	IPERCOM versions												
			3.3.0	3.4.0	3.5.0										
			July-25	Dic-25	Feb-26										
SWITCHBOARD	1060/42		yes	yes	yes										
VDP 10''	1761/23		yes	yes	yes										
CM FACE RECOGNITION	1060/16		no	yes	yes										
EP ALPHA TOUCH	1060/48T		no	yes	yes										

Table 8: device compatibility with IPerCom versions (second part)

APPENDIX X: *RTSP Cameras* supported by IPerCom video door phones

VOG^{5+} 1761/15-16-17-18 e *VOG*^{5} 1761/6

Below is the list of supported *RTSP Cameras*:

- Camera IP 5M 2.8-13mm Bullet ECO 2 Ref. 1099/501A;
- Camera IP 5M 2.8mm Dome PLUS AI Ref. 1099/550B;
- Camera IP 5M 2.8mm Bullet NEIUS PLATINUM Ref. 1099/420.

For the first 2 cameras the streaming video is displayed correctly if the parameters below are set as follows:

- Resolution: 640x480 pixel,
- Frame rate per second: 10fps,
- CODEC: H264,
- Code level: baseline,
- Bitrate control: CBR,
- Bitrate: 768 Kbps,
- iFrame interval: 10s.

For the third camera it is necessary to set a resolution of 352x288 pixels (the values of the other parameters remain unchanged).

VOG^{7}, *MAX*, *Basic* video door phones and *IPerCom Client* application

There are no restrictions on supported *RTSP Cameras* other than setting a resolution that does not exceed 1920x1080 pixels.

APPENDIX Y: Auto-on on *RTSP Cameras*

In general, the auto-on function on compatible *RTSP Cameras* is available on video door phones and *Switchboard* / *IPerCom Client* applications in the conditions shown below:

- by means of the auto-on button of the video door phones and *IPerCom Client* application (for the *Switchboard* application there is a dedicated item in the *Tools* menu);
- during the unhook time of the call pressing the dedicated buttons (up and down arrows) on the video door phones and *IPerCom Client* application (for the *Switchboard* application there is a dedicated item in the *Tools* menu);
- during the conversation time of the call pressing the dedicated buttons (up and down arrows) on *VOG*[7]*, MAX* and *Basic* video door phones and *IPerCom Client* application (for the *Switchboard* application there is a dedicated item in the *Tools* menu).

APPENDIX Z: *CallMe* operating mode

VOG[7] 1761/3x and *MAX* 1717/2x, 3x video door phones can work in *CallMe* mode.

The *CallMe* mode allows you to have a new application like *CallMe* on the video door phone with the following features:

- receive calls from calling stations (simultaneously with the *CallMe* app on smartphone/tablet),
- open door and gate opening (on call and outside the call);
- make auto-on;
- make intercom calls;
- send user activation commands.

These functions can be obtained without connecting the video door phone to the Ipercom IP network, but connecting it to the apartment Internet router (via cable or Wi-Fi). The video door phone must be also powered locally by a power supply.

This new operating mode can be set when the video door phone is not configured and switched on. The screen that appears in this case is shown in the figure below:

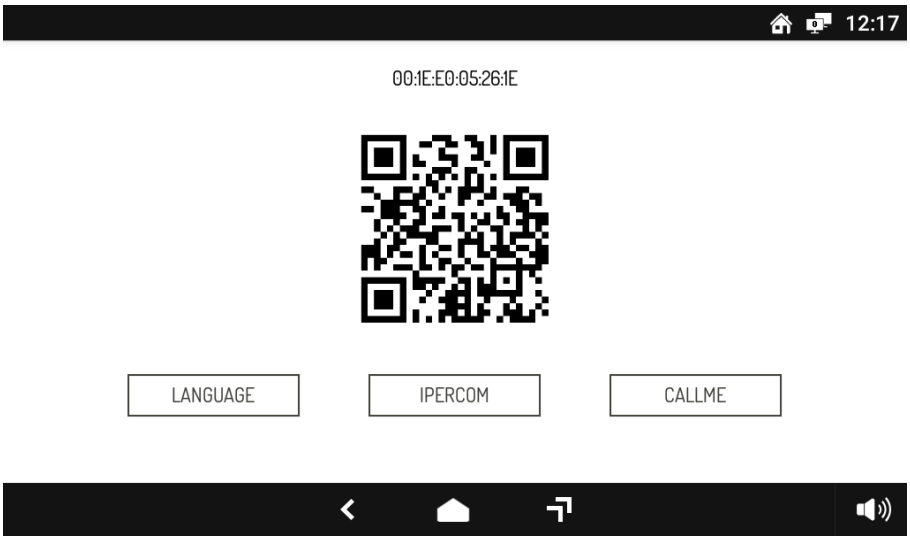

Figure 75: CallMe operating mode

The "*CallMe*" button allows you to set the video door phone in *CallMe* mode, while the "*IPerCom*" button allows you to set the video door phone in IPerCom mode, that is the normal use of the video door phone in an IPerCom system.

Press the "*CallMe*" button and confirm the choice on the relevant dialog box, then set the time zone and local date and time.

After this, the following window appears:

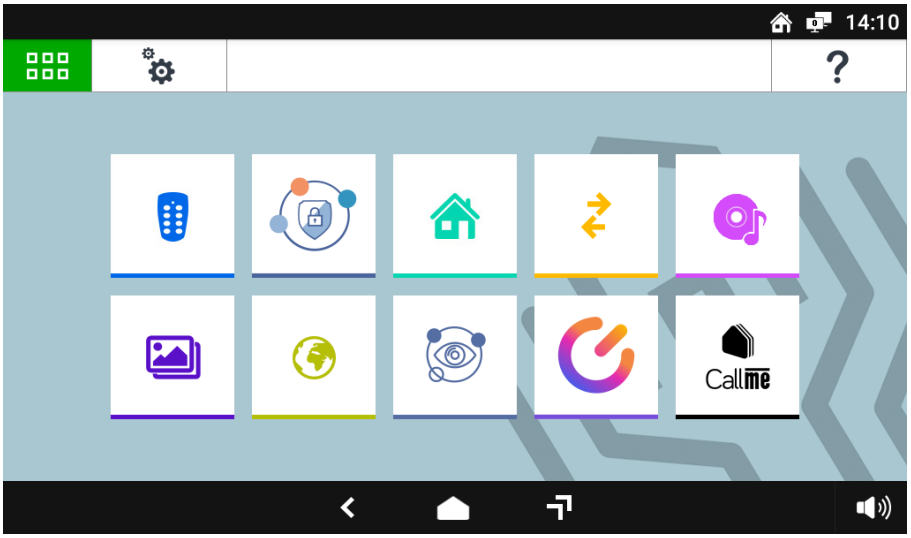

Figure 76: Top Page in CallMe Mode

Press the icon in the red box, then go to the login window and enter the same credentials used in the *CallMe* app on your smartphone/tablet.

The *CallMe* on video door phones *VOG*[7] and *MAX* supports IPerCom and IPerCloud apartments.

The *VOG*[7] and *MAX* video door phones in *CallMe* mode do not have any video door phone function.

APPENDIX A1: Custom video door phones

In addition to the officially released update files for the IPerCom system (files with .smup or .xmup or .mup extension), it is possible to create other update files called *custom*. These update files (always with .smup or .xmup or .mup extension) allow you to customize the following video door phones:

System	Device	Ref.
IPerCom	Video door phone 7'' MAX	1717/3x-4x
	Video door phone 10'' MAX	1717/21-21U-22-22U-23-23U
	Video door phone 7'' *VOG*[7]	1761/31-31U-32-33-33U
	Video door phone 7'' Basic	1741/1-2-3
	Video door phone 10''	1761/23

Table 9: list of video door phones that can be customized

The customizations mainly concern the graphic interface and the addition/deletion of apps. Video door phones upgraded through customized upgrade files are referred to as *custom* video door phones.

*The custom IPerCom system update files (with .mup or .xmup extension) contain within them the relevant custom update file of one or all of the video door phones listed in **Table 9**.*

For creation of custom IPerCom system update files and custom video door phone upgrade files contact Urmet Technical Service.

If there are *custom* video door phones in the IPerCom system, to update the system the 2 points below must be taken into consideration:

- for the same type of video door phones (among those listed in ***Table 9***) the IPerCom system update file can contain either the custom file or the non-custom file;
- *Server* 1060/1 cannot always update *custom* video door phones.

The first point implies that if the customizations are not the same for a specific type of video door phone, it is necessary to carry out multiple updates.

The second point implies that updating the system from *Server* 1060/1 is not always possible and you need to use application *IPerCom Installer Tools*.

These points will be highlighted later.

*Once the IPerCom system update file has been imported (with .mup or .xmup or .smup extension), if this is not custom, the video door phone update files in **Table 9** are marked with the ROOT suffix; otherwise they are marked with a suffix (identifier) assigned during the creation of the video door phone custom update file. This can be seen from the figure below:*

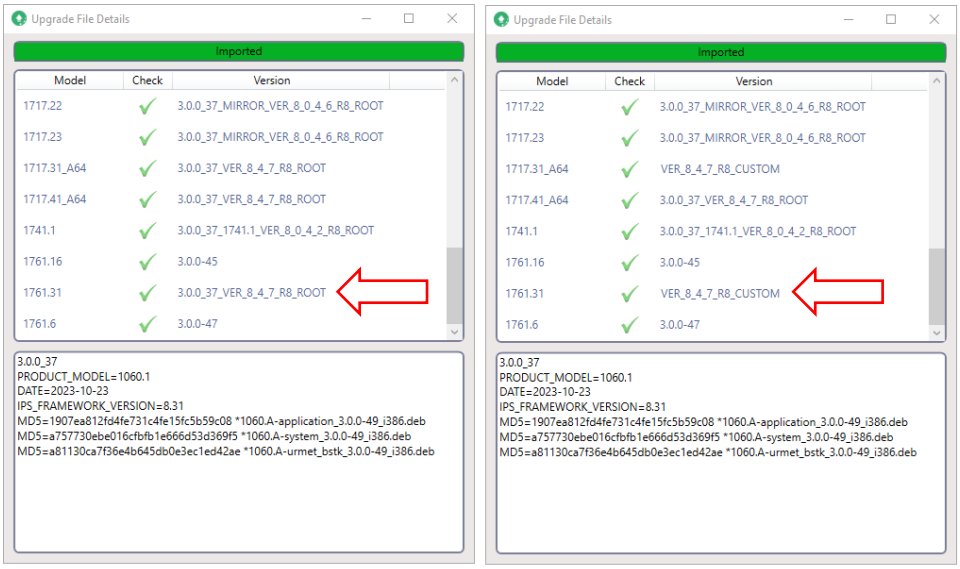

Figure 77: video door phone update files with ROOT and CUSTOM suffixes

It is important to underline that for the Server 1060/1 to be able to update the custom video door phones, the identifiers of the current version and the version you want to install must be the same.

The following 2 common cases can occur in a system:

1. customizations required are the same for all video door phones (or more generally, for the same video door phone model, customizations are the same);

2. for the same model of video door phone, different customizations are required (for example, some video door phones are *custom* and others not).

The 2 different cases are represented in the following figure:

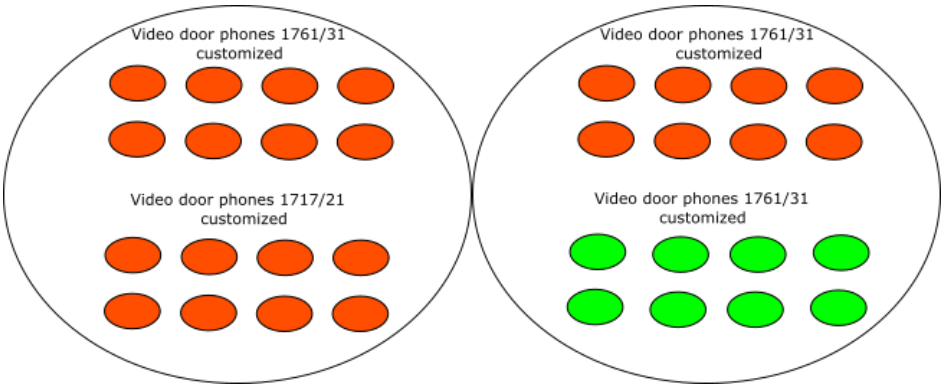

Figure 78: similar (left) and different (right) customizations

For each of the 2 cases indicated above it is advisable to proceed as described below depending on whether the system has a *Server* 1060/1 configured to update the other devices.

Same customizations for all video door phone models: no Server in the system configured to update devices

The update must be always done via *IPerCom Installer Tools* in **FULL MODE** using the custom IPerCom system update file (mup or xmup or smup file): in this way the video door phones listed in ***Table 9*** are made custom (one or more models). Once made custom, *IPerCom Installer Tools* can make them non-custom again or update them with an update file with a different identifier from the previous one. This means that *IPerCom Installer Tools* has no restrictions on updating video door phones.

For further details on the identifier of an upgrade file, contact Urmet Technical Service.

The procedure is summarized in the following figure:

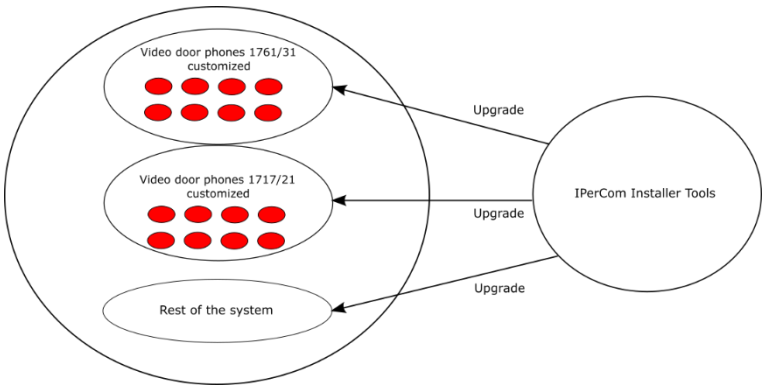

Figure 79: update of the system with no Server 1060/1

Any other video door phones or devices added later must be updated via *IPerCom Installer Tools*.

Once the custom update of a video door phone has been completed, the firmware version with the relevant identifier appears in the "*Version*" column. If not custom, identifier *ROOT* appears.

Same customizations for all video door phone models: at least one Server configured to update devices in the system

It is possible to proceed in one of the following ways depending on whether the system is configured or not.

SYSTEM INSTALLED AND ALREADY WORKING

The update can be done via *IPerCom Installer Tools* in **ACTIVE MODE** and **PASSIVE MODE**.

Since in **ACTIVE MODE** it is *IPerCom Installer Tools* that takes care of updating the video door phones, as seen before, there are no restrictions on updating them, that is *IPerCom Installer Tools* can make them non-custom again or update them with an update file with a different identifier from the previous one.

The procedure is summarized in the following figure:

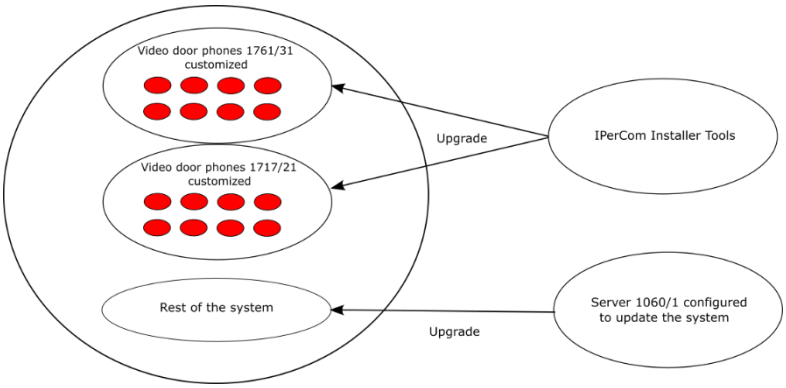

Figure 80: update of the system with IPerCom Installer Tools and Server 1060/1 configured to update devices

SYSTEM JUST INSTALLED BUT NOT CONFIGURED YET

You can follow the steps below as an alternative to the procedure above:

- using the *IPerCom Installer Tools* application, upgrade the *Server* 1060/1 (disconnected from the system) with the required custom system update file;
- create a basic IPerCom configuration that includes only the *Server* 1060/1 by means of the IPerCom *configurator*;
- configure the *Server* 1060/1 so that it can upgrade the other system devices (by means of the IPerCom *configurator*);
- distribute the configuration thus created to *Server* 1060/1;
- connect the *Server* 1060/1 to the system.

In this way the *Server* 1060/1 will be able to update the other devices present in the system and customize the video door phones. The procedure is summarized in the following figure:

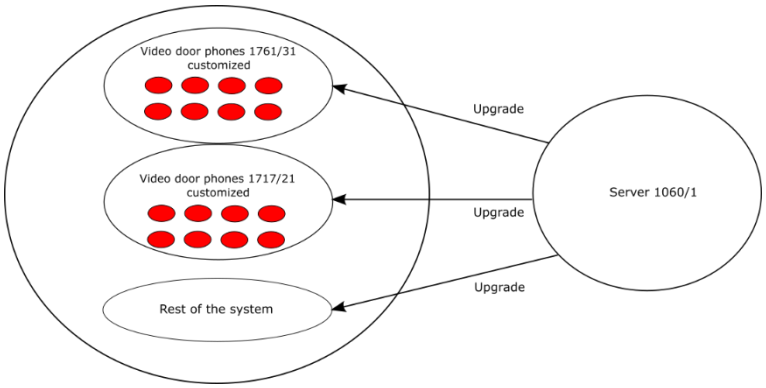

Figure 81: update of the system with Server 1060/1 configured to update devices

Any other devices added later can be updated via *IPerCom Installer Tools* or *Server* 1060/1. The only exception is represented by the addition of custom video door phones whose identifier is different from that present in the mup or xmup or smup file already installed on the system: in this case the update must be carry out from *IPerCom Installer Tools*.

Once the custom update of a video door phone has been completed, the firmware version with the relevant identifier appears in the "*Version*" column. If not custom, identifier *ROOT* appears.

Same video door phones with different customizations: no Server configured to update devices in the system

The update must be done in multiple sessions via *IPerCom Installer Tools* in **FULL MODE** with the button "*Selective Update*".

This is because for each customization request it is necessary to:

- select the video door phones for which the customization in question has been requested;
- import the required custom mup or xmup file into *IPerCom Installer Tools* and upgrade.

In the last update session, it is also possible to update the rest of the system.

In this way the video door phones listed in ***Table 9*** are made custom. Once made custom, *IPerCom Installer Tools* can make them non-custom again or update them with an update file with a different identifier from the previous one. This means that *IPerCom Installer Tools* has no restrictions on updating video door phones.

The procedure is summarized in the following figure:

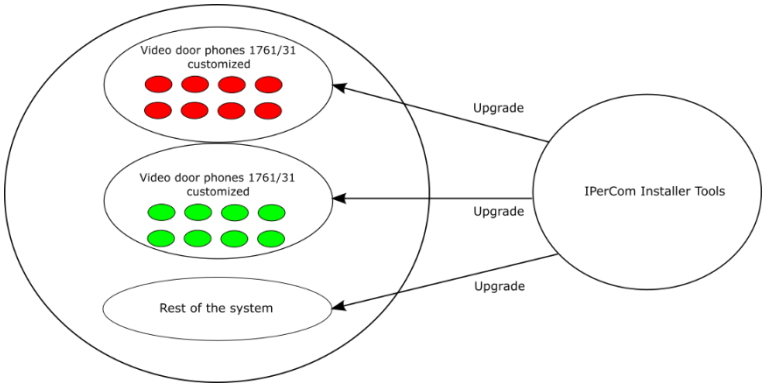

Figure 82: update of the system with no Server 1060/1

Any other video door phones or devices added later must be updated via *IPerCom Installer Tools*.

Once the custom update of a video door phone has been completed, the firmware version with the relevant identifier appears in the "*Version*" column. If not custom, identifier *ROOT* appears.

Same video door phones with different customizations: at least one Server configured to update devices in the system

The procedure is like what was seen in the case of a system without *Server* 1060/1 with the only difference that the selective update is done in **ACTIVE MODE**.

Once the Server 1060/1 has been updated, it will not update the custom video door phones updated previously with IPerCom Installer Tools because identifiers are different.

Any other devices added later can be updated via *IPerCom Installer Tools* or *Server* 1060/1. The only exception is represented by the addition of custom video door phones whose identifier is different from that present in the mup or xmup or smup file already installed on the *Server* 1060/1: in this case the update must be carry out from *IPerCom Installer Tools*.

Once the custom update of a video door phone has been completed, the firmware version with the relevant identifier appears in the "*Version*" column. If not custom, identifier *ROOT* appears.

The following table shows the cases in which a *custom or non-custom* video door phone can be updated by *IPerCom Installer Tools* or by the Server via a custom or non-custom update file:

Type of mup/xmup/smup upgrade file	**Type of upgrade file present on the video door phone**	**Identifier on mup/xmup/smup file == Identifier present on video door phone**	**Can *IPerCom Installer Tools* upgrade the video door phone?**	**Can *Server* 1060/1 upgrade the video door phone?**
Custom	*Non-custom*		Yes	Yes
Custom	*Custom*	Yes	Yes	Yes
Custom	*Custom*	No	Yes	No
Non-custom	*Non-custom*		Yes	Yes
Non-custom	*Custom*		Yes	No

Table 10: upgrade custom and non-custom video door phones

It is not relevant whether the video door phones are configured or not.

APPENDIX B1: Flex options

The "*Apply Flex Options*" button is linked to the use of customized IPerCom system update files, more specifically it concerns the forcing of the homepage and wall paper on custom the video door phones according to what was done in the custom update.

When the *custom* update phase is finished, the homepage and wall paper of custom video door phones can be the following, according to what reported below:

- if before the custom update the homepage and wallpaper were the default ones, these are forced to what was set in the custom update;

- if before the custom update the custom homepage and wallpaper were different from the default ones, they remain as they are.

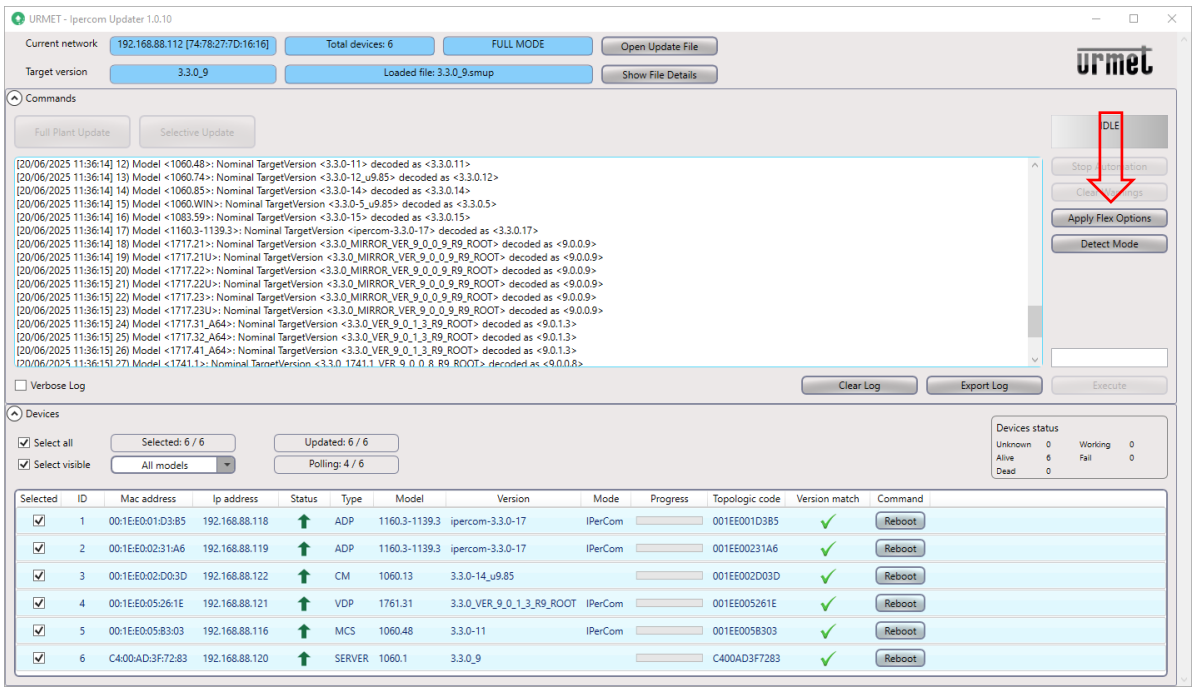

Figure 83: custom update ended

If button "*Apply Flex Options*" (red arrow) is pressed after the custom update, homepage and wallpaper of selected custom video door phones are forced to what selected in the custom update.

APPENDIX C1: Failure to upgrade all devices

During the update phase (both **FULL MODE** and **ACTIVE MODE**), there is a default automatic mechanism for restoring any errors and repeating the update cycle (for maximum 5 times) if one or more devices fail to update.

If at the end of the 5 update cycles *IPerCom Installer Tools* is unable to update one or more devices, a screen like the one below appears:

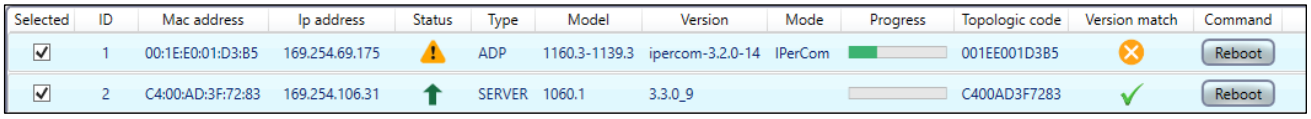

Figure 84: devices not upgraded

The not upgraded devices are marked with symbol  in the "*Status*" column.

This can happen for various reasons, the most frequent of which are:

- upgrade time is longer than normal time (systems with many devices),
- there is no connection between the PC and the IPerCom system,
- devices displaying the symbol in question do not work properly.

In one of these cases, the following dialogue box is displayed:

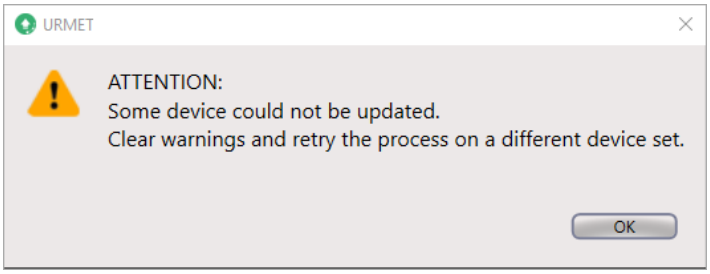

Figure 85: dialogue window on device upgrade failed

After pressing the "*OK*" button, the dialogue window disappears and before trying to update the system you need to press the "*Clear Warnings*" button:

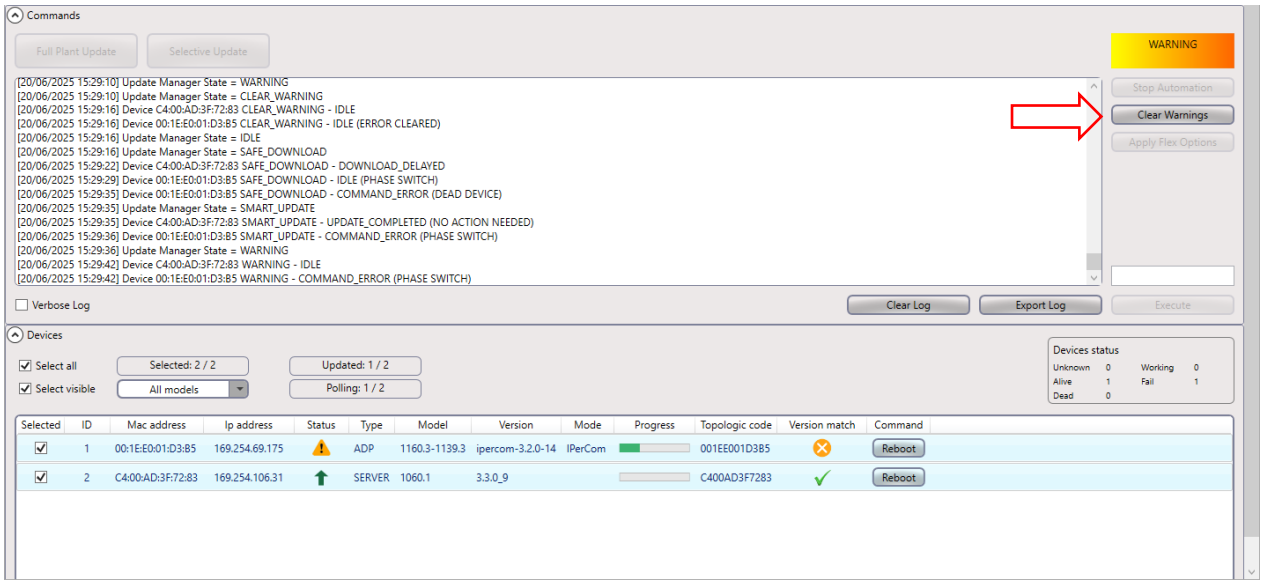

Figure 86: clear warning button

In this way *IPerCom Installer tools* application shows the symbol  in the "*Status*" column:

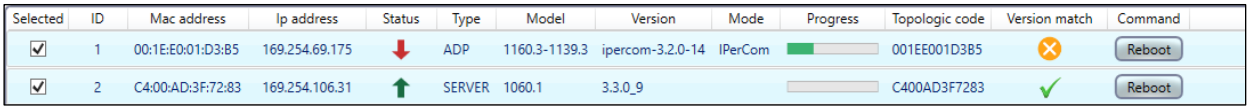

Figure 87: device that does not communicate with IPerCom Installer Tools

Buttons "*Full Plant Update*" and "*Selective Update*" are now available for a new update attempt:

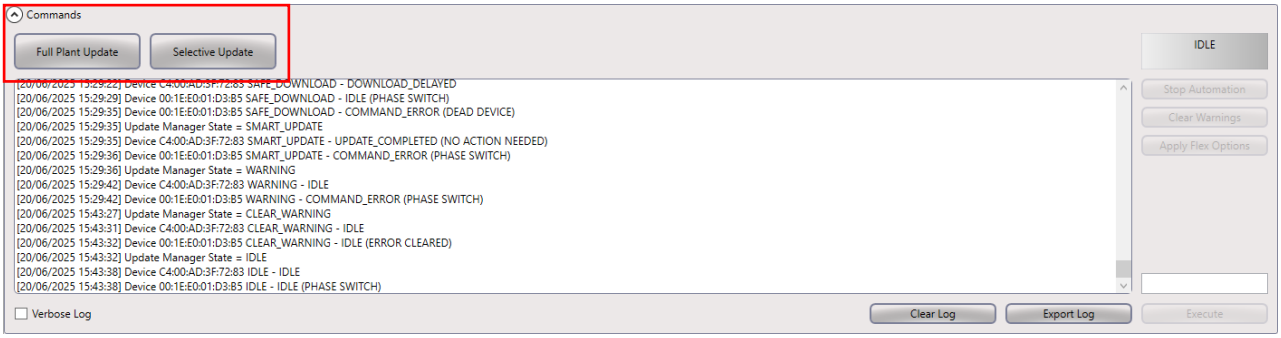

Figure 88: update buttons available

*During the update phase (both in **FULL MODE** and **ACTIVE MODE**) the "Stop Automation" button allows you to block the automatic repetition of the update and error recovery cycle. If you press" Yes" on the relevant dialog box, any failed update messages on one or more devices must be manually deleted and a second update cycle must be started manually.*

APPENDIX D1: Disabled mode

If two instances of *IPerCom Installer Tools* (running on two different PCs) try to connect to the same IPerCom system, the last of the two instances which connects, starts in **DISABLED MODE**, that is, it displays the following message:

Figure 89: disabled mode

Pressing the button "*OK*", the related instance of *IPerCom Installer Tools* closes.

APPENDIX E1: Logs

In the "*Commands*" section there is a box (highlighted in red) where the *IPerCom Installer Tools* logs are displayed, that is the history of the operations carried out by the application is shown, as reported in the figure below:

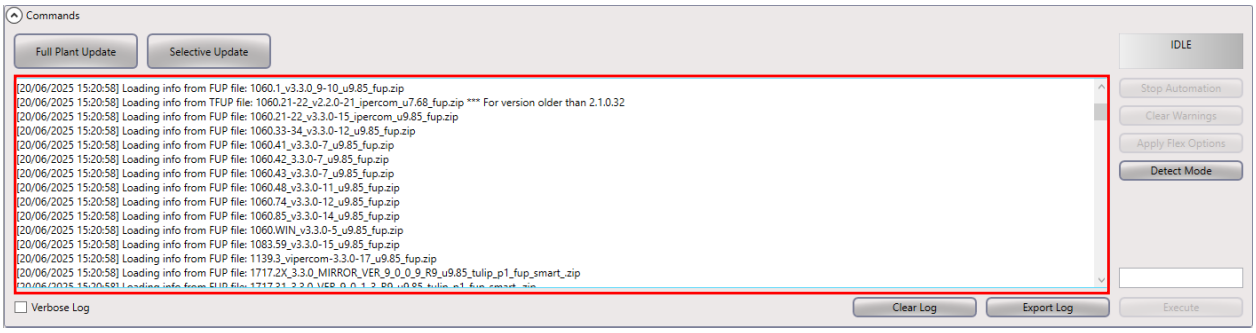

Figure 90: IPerCom Installer Tools logs

The logs can be:

- deleted with the "*Clear log*" button;
- exported to a file with the "*Export log*" button (the file path is written on the logs);
- more detailed by selecting "*Verbose log*" checkbox.

APPENDIX F1: IPerCom devices that can be updated by *IPerCom Installer Tools*

The *IPerCom Installer Tools* application allows updating the firmware of IPerCom system devices. The list of devices that can be updated is shown in the following table:

System	Device	Ref.
IPerCom	Call Module (Elekta)	1060/12-13
	Call Module (Elekta Steel)	1060/17-18-23
	Call Module with face recognition	1060/16
	Modular Calling Station with 1060/48	1060/48 (*)
	Modular Calling Station with 1060/48T	1060/48T (*)
	Entry Panel (Sinthesi Steel)	1060/71-74-75-78
	Entry Panel (Mikra2)	1060/21-33-34
	Private Call Module (Mikra2)	1060/22
	Switchboards (software application and device)	1060/41-42
	Video door phone 7'' *VOG*^{7}	1761/31-31U-32-33-33U
	Video door phone 5'' *VOG*$^{5+}$	1761/15-15U-16-16U-18-19
	Video door phone 5'' *VOG*^{5}	1761/6
	Video door phone 10'' MAX	1717/21-21U-22-22U-23-23U
	Video door phone 7'' Basic	1741/1-2-3
	Video door phone 7'' MAX	1717/3x-4x
	Video door phone 10'' (for Chinese market only)	1761/23
	IperCom Client (software application)	1060/43
	Door phone Miro	1160/3
	Server	1060/1
	Gateway 2Voice	1083/59
	Clock Module	1060/85
	IPerCom Gateway for Windows (software application for Chinese market only)	---

Table 11: list of IPerCom devices that can be updated by IPerCom Installer Tools

*(*): 1060/48 and 1060/48T are the reference codes of the audio/video IP module. For the other reference codes that make up the push button panel, see the relevant booklets on the website **www.urmet.com** or the **system technical manual for the installer**. 1060/48, 1060/48T and 1168/1 (display module) are the only modules that can be updated.*

APPENDIX G1: Device types and models

IPerCom Installer Tools can upgrade the firmware of device types listed below. Each type of device can match several models. Device types and models are displayed in "*Type*" and "*Model*" columns, respectively, in the "*Devices*" section.

The possible types and models are shown in the following table:

Type	**Model**
SERVER (*Server*)	1060.1
CM (*Call Module*)	1060.13, 1060.18, 1060.23, 1060.16
MCS (*Modular Entry Panel with 1060/48*)	1060.48
MCS (*Modular Entry Panel with 1060/48 Touch*)	1060.48T
PEIP (*Entry Panel*)	1060.21, 1060.33, 1060.34, 1060.74
PACM (*Private Call Module*)	1060.22
SWB (*Switchboard*)	1060.41
SWB (*Switchboard*)	1060.42
VDP (*Video door phone*)	1761.31
VDP (*Video door phone*)	1761.16
VDP (*Video door phone*)	1761.6
VDP (*Video door phone*)	1717.31_A64
VDP (*Video door phone*)	1717.41_A64
VDP (*Video door phone*)	1741.1
VDP (*Video door phone*)	1717.21
VDP (*Video door phone*)	1060.43
VDP (*Video door phone*)	1717.31 (No longer supported by IPerCom version 2.1.0)
VDP (*Video door phone*)	1717.41 (No longer supported by IPerCom version 2.1.0)
VDP (*Video door phone*)	1761.23
ADP (*Door phone*)	1160.3-1139.3
GATEWAY (*2Voice Gateway*)	1083.59
CLOCK (*IPerCom Clock Module*)	1060.85

Table 12: list of device types and models

All devices listed in ***Table 11*** can be associated to one of the types and models listed above.