

# System technical manual for the installer



**iPer**  
com | INTEGRATED IP  
VIDEO DOOR PHONE  
SYSTEMS

IF YOU LOVE YOUR BUILDING

**urmet**

<b>1</b>	<b>Introduction .....</b>	<b>12</b>
1.1	<i>IPerCloud mode.....</i>	14
1.2	<i>Configuration of an IPerCom system .....</i>	18
1.3	<i>IT security of the IPerCom system.....</i>	20
<b>2</b>	<b>IPerCom devices and features offered by the system.....</b>	<b>22</b>
2.1	<i>Server 1060/1.....</i>	26
2.2	<i>Call Module 1060/12-13-17-18.....</i>	26
2.3	<i>Call Module 1060/23 .....</i>	27
2.4	<i>Modular calling station with 1060/48 .....</i>	27
2.4.1	<i>Call module.....</i>	28
2.5	<i>Entry Panel 1060/71-74-75-78.....</i>	28
2.6	<i>Entry Panel 1060/21 .....</i>	29
2.6.1	<i>Villa Kit with Entry Panel 1060/21 in IPerCloud mode.....</i>	29
2.7	<i>Entry panel Mikra Plus 1060/33 .....</i>	29
2.8	<i>Entry panel Mikra Digital 1060/34 .....</i>	29
2.9	<i>Private Call Module 1060/22.....</i>	30
2.10	<i>Video door phone 7" VOG<sup>7</sup> 1761/31-32-33 .....</i>	30
2.11	<i>Video door phone 7" VOG<sup>7</sup> 1761/31U-33U.....</i>	30
2.12	<i>Video door phone 5" VOG<sup>5+</sup> 1761/15-16-18-19 .....</i>	31
2.13	<i>Video door phone 5" VOG<sup>5+</sup> 1761/15U-16U.....</i>	31
2.14	<i>Video door phone 5" VOG<sup>5</sup> 1761/6.....</i>	31
2.15	<i>Video door phone 7" MAX 1717/31-32-33-34-41 .....</i>	32
2.16	<i>Video door phone 10" MAX 1717/21-22-23 .....</i>	32
2.17	<i>Video door phone 10" MAX 1717/21U-22U-23U.....</i>	32
2.18	<i>Video door phone 7" Basic 1741/1-2-3 .....</i>	33
2.19	<i>IPerCom Client video door phone 1060/43.....</i>	33
2.20	<i>Miro door phone 1160/3.....</i>	33
2.21	<i>Relay actuator 1060/84 v. 2.07 .....</i>	33
2.22	<i>Relay actuator 1060/84 v. 3.04 .....</i>	34
2.23	<i>Relay actuator 1060/84 v. 4.05 .....</i>	34
2.24	<i>Key Reader 1060/86 .....</i>	34
2.25	<i>Key Reader 1060/45 .....</i>	34

2.26	<i>Switchboard 1060/41</i>	35
2.27	<i>IPerCom Clock Module 1060/85</i>	35
2.28	<i>Lift Interface 1060/37</i>	35
2.29	<i>Gateway IPerCom-2Voice 1083/59</i>	36
2.30	<i>IPassan controller</i>	36
2.31	<i>IPerTALK Server</i>	36
2.32	<i>RTSP Cameras</i>	37
2.32.1	<i>RTSP Cameras (NVR)</i>	37
3	<i>Basic concepts</i>	38
3.1	<i>Topology</i>	38
3.2	<i>Topological path and topological group</i>	39
3.3	<i>Applications of the concepts of topological path and topological group</i>	40
3.3.1	<i>Automatic display of residents in the address book of calling stations with display</i>	40
3.3.2	<i>Propagation of contacts in address book of apartment station</i>	40
3.3.3	<i>Propagation of activation rules</i>	41
3.3.4	<i>Default view of apartments on the CallMe app linked to the Switchboard application</i>	41
3.3.5	<i>Practical example of application of the topological group concept</i>	41
3.3.6	<i>Resident access (with key code and door code) to doors/gates of the system</i>	42
3.3.7	<i>Competence Switchboards</i>	42
3.3.8	<i>Creation of the camera directory for the video door phone indoor stations for auto-on function</i>	42
3.3.9	<i>Practical example of application of the topological path concept</i>	43
3.3.10	<i>Summary table</i>	44
3.4	<i>Main and secondary calling stations</i>	44
3.5	<i>Security level of an IPerCom system</i>	45
4	<i>System installation</i>	48
4.1	<i>Minimum requirements for the installation of an IPerCom system</i>	48
4.2	<i>IP network structure</i>	49
4.3	<i>Maximum distances and sections cables</i>	50
4.4	<i>Device/application firmware upgrade</i>	51
5	<i>System commissioning</i>	53
6	<i>Commissioning a system through IPerCom Installer Tools</i>	55
6.1	<i>Introduction to IPercom Installer Tools</i>	55
6.2	<i>IPerCom Installer Tools: functions</i>	56

6.3	<i>Automatic update to the latest available version</i>	57
6.4	<i>Starting the Launcher</i>	59
6.5	<i>Automatic detection of the IPerCom version</i>	59
6.5.1	<i>System upgraded to the last version</i>	61
6.5.2	<i>System not upgraded to the last released version</i>	63
6.5.3	<i>Mixed system</i>	64
6.6	<i>Launch a certain version of IPerCom Installer Tools</i>	65
6.7	<i>First run of IPerCom Installer Tools</i>	67
6.7.1	<i>Urmet Cloud authentication</i>	69
6.7.1.1	<i>Pre-activation license bundle and pre-activation license bundle history</i>	73
6.7.2	<i>Urmet Cloud authentication not performed</i>	76
6.7.3	<i>Project and site</i>	78
6.7.4	<i>Creating a new project</i>	79
6.7.5	<i>Opening a project</i>	81
6.7.6	<i>Importing a project</i>	83
6.7.6.1	<i>Use a same project on another PC</i>	83
6.7.6.2	<i>Import a project on a version of IPerCom 2.1.1 or higher</i>	85
6.7.7	<i>Deleting one or more projects</i>	86
6.7.8	<i>Closing the application</i>	87
6.8	<i>Project and site parameters</i>	87
6.9	<i>How to use IPerCom Installer Tools for the configuration of a system</i>	90
6.9.1	<i>Mode 1: system installed but not configured, creation of configuration associated to the project without connection to the system</i>	90
6.9.2	<i>Mode 2: system installed but not configured, creation of configuration associated to the project with connection to the system</i>	90
6.9.3	<i>Mode 3: system installed but not configured, creation of configuration associated to the project by importing it from external file</i>	91
6.9.4	<i>Creating the project and the related configuration file</i>	91
6.9.5	<i>“Save backup”: how to create one or more backups of a project</i>	96
6.9.5.1	<i>How to restore a backup</i>	100
6.9.6	<i>Connecting to the system and transferring the configuration</i>	102
6.9.7	<i>How to set date and time on the system</i>	104
6.9.8	<i>Transferring the system configuration</i>	105
6.9.9	<i>Creating the configuration file with import from external file</i>	109

6.10	How to use IPerCom Installer Tools to edit the configuration with system already installed and configured.....	111
6.11	System modified locally by MAX, VOG <sup>7</sup> or Basic video door phone .....	115
6.12	Importing configuration files with different IDs .....	119
6.13	Systems with two configurations .....	124
6.14	System remote access.....	125
6.15	Other functions of IperCom Installer Tools.....	129
6.15.1	“Urmnet Cloud” tab .....	130
6.15.1.1	Urmnet Cloud access.....	130
6.15.1.2	Urmnet cloud access performed .....	132
6.15.1.3	Urmnet Cloud access and opening of a project.....	133
6.15.1.4	Urmnet Cloud access, opening of a project and connection to a site .....	134
6.15.1.5	CallMe Manager support enabled with or without IPerCloud apartments.....	135
6.15.1.6	Site authorization management.....	137
6.15.1.6.1	Transfer of the ownership of the site from installer to a building manager .....	137
6.15.1.6.2	Transfer of the site ownership to another installer.....	142
6.15.1.7	IPerCloud Test Mode.....	148
6.15.2	Security.....	152
6.15.2.1	Modifying the installer password .....	153
6.15.2.2	System block.....	154
6.15.2.3	Unlocking the system.....	156
6.15.3	Date/Time .....	157
6.15.3.1	Configuring date and time from PC.....	157
6.15.3.2	Obtaining date and time from IPerCom system.....	158
6.15.4	Diagnostics .....	161
6.15.5	System Logs .....	164
6.15.5.1	How to filter System Logs: basic and advanced filters .....	168
6.15.5.2	Filter on Calls event.....	171
6.15.6	System backup.....	175
6.15.7	Maintenance .....	178
6.15.8	Devices not aligned to the same IPerCom or software development platform (UPTK) version.....	186
6.15.8.1	IPerCom Installer tools application not aligned to the same IPerCom or software development platform (UPTK) version.....	192
7	The configurator.....	193

<b>7.1</b>	<b><i>Creating or editing the configuration file from IPerCom Installer Tools.....</i></b>	<b>193</b>
7.1.1	<i>Selecting the system topology (model) and the configurator structure.....</i>	194
7.1.1.1	<i>Villa Kit (one-household) systems.....</i>	201
7.1.1.2	<i>Single Stair systems .....</i>	202
7.1.1.3	<i>Multiple Stairs systems.....</i>	203
7.1.1.4	<i>Multi Block systems.....</i>	204
7.1.2	<i>Adding devices.....</i>	206
7.1.2.1	<i>Adding a Gateway IPerCom-2Voice on a stair node .....</i>	215
7.1.2.2	<i>Adding a Lift Interface 1060/37 on a stair node .....</i>	219
7.1.2.2.1	<i>Lift interface mode.....</i>	219
7.1.2.2.1.1	<i>Creating the path .....</i>	220
7.1.2.2.1.2	<i>Control Relay Assignment.....</i>	221
7.1.2.2.1.3	<i>Assignment in Floor mode .....</i>	222
7.1.2.2.1.4	<i>Assignment in Apartment mode .....</i>	224
7.1.2.2.2	<i>Access for non-residents.....</i>	225
7.1.2.2.3	<i>Lift interface-RS485 mode .....</i>	226
7.1.2.2.4	<i>Relay Actuator Mode .....</i>	226
7.1.3	<i>System IPerCom in IPerCloud mode.....</i>	227
7.1.3.1	<i>Addition in configuration of a Server 1060/1 on an IPerCom system in IPerCloud mode ....</i> <i>.....</i>	227
7.1.3.2	<i>How to set up an apartment in IPerCloud mode .....</i>	230
7.1.3.2.1	<i>Hybrid apartments.....</i>	232
7.1.4	<i>Contacts .....</i>	233
7.1.4.1	<i>How to call MAX video door phones and Miro door phones from MAX video door phones, Miro door phones and/or call modules.....</i>	234
7.1.4.1.1	<i>How to call an IPerCloud apartment.....</i>	244
7.1.4.2	<i>How to call the Switchboards from MAX video door phones, Miro door phones and/or call modules .....</i>	246
7.1.4.3	<i>Auto-on function on Door Speaker Units, Call Modules and RTSP cameras from MAX video door phones outside their competence.....</i>	251
7.1.5	<i>Activations.....</i>	257
7.1.5.1	<i>Activation for events on Entry panel 1060/33-34-71-74-75-78.....</i>	262
7.1.5.2	<i>Activation for events on Entry panel 1060/21.....</i>	267
7.1.5.3	<i>User recognition event .....</i>	270
7.1.5.4	<i>Activation for events on Floor Entry panel 1060/22 .....</i>	271

7.1.5.5	Activation for events on Call Module.....	273
7.1.5.6	Activation for events on Entry Panel with 1060/48 .....	276
7.1.5.7	Key Reader activations .....	277
7.1.5.8	Activations for topological events .....	279
7.1.5.8.1	Topological events for Relay Actuator .....	281
7.1.5.8.1.1	Addition of a user activation on video door phones / door phones / CallMe application .....	286
7.1.5.8.2	Topological events Lift Up and Lift Down .....	290
7.1.5.8.3	Events Open Door and Open Gate .....	294
7.1.5.8.4	Switchboard Activations .....	295
7.1.5.8.5	Activations for topological events with 2Voice audio/video apartment stations ...	297
7.1.5.9	Automation events: input/output association .....	299
7.1.5.9.1	Input-output activation on two different relay actuators .....	300
7.1.5.9.2	Creating a scenario .....	309
7.1.5.9.3	Adding a time profile to the activation .....	314
7.1.5.9.4	Sending alarms to the Switchboard via relay actuator inputs .....	318
7.1.5.9.5	Creation of relay actuator activations and alarms.....	322
7.1.5.9.6	Schedules .....	325
7.1.6	Gate contact used as output of a Relay Actuator.....	332
7.1.7	Remote relay functions, remote entrance hall button and remote sensor.....	335
7.1.8	User management .....	339
7.1.8.1	Residents .....	339
7.1.8.2	Not residents.....	344
7.1.8.3	Groups.....	349
7.1.8.4	Switchboards .....	352
7.1.9	Access control .....	354
7.1.9.1	Access profiles.....	356
7.1.9.2	Time Profiles .....	360
7.1.9.3	Holidays.....	365
7.1.9.4	Door groups .....	369
7.1.9.5	Door profiles .....	372
7.1.9.6	Trade .....	376
7.1.10	System parameters .....	378
7.1.10.1	Global Settings .....	379

7.1.10.2	<i>Door/Gate Settings</i> .....	383
7.1.10.3	<i>Call Forwarding Settings</i> .....	385
7.1.10.4	<i>Call divert settings</i> .....	388
7.1.10.5	<i>Network settings</i> .....	389
7.1.10.6	<i>CUSTOM NETWORK SETTINGS</i> .....	391
7.1.10.7	<i>Maintenance Settings</i> .....	392
7.1.10.8	<i>Sunrise/Sunset Settings</i> .....	394
7.1.11	<i>Call addressing mode</i> .....	395
7.1.12	<i>Setting of call forwarding function in IPerCom system not in IPerCloud mode</i> .....	401
7.1.12.1	<i>Configuring call forwarding function with CallMe Manager application support</i> .....	403
7.1.12.2	<i>Configuring call forwarding function without CallMe Manager application support</i>	424
7.1.13	<i>Configuring the call forwarding function in IPerCom systems in IPerCloud mode</i> .....	441
7.1.14	<i>Search function</i> .....	469
7.1.15	<i>How to save the configuration</i> .....	472
8	<i>Commissioning a system through MAX, VOG<sup>7</sup> or Basic video door phones: the configuration menu</i> ....	473
8.1	<i>Mode 1: Access to the configuration menu from the start screen page of non-configured MAX, VOG<sup>7</sup> or Basic video door phones</i> .....	474
8.1.1	<i>Date and time setting</i> .....	477
8.1.2	<i>Configuration menu</i> .....	479
8.2	<i>Access to the configurator from the MAX, VOG<sup>7</sup> or Basic video door phone</i> .....	482
8.2.1	<i>The configurator on Android tablets</i> .....	486
8.3	<i>System first configuration</i> .....	494
8.3.1	<i>Creation of a new configuration: definition of the system topology</i> .....	495
8.3.2	<i>Adding devices to the system using the MAX video door phone and/or the Android tablet app</i> .....	498
8.3.2.1	<i>Mode 1: installer uses only MAX video door phones for the system configuration</i> .....	498
8.3.2.2	<i>Mode 1.1: The installer creates the configuration in the laboratory on the MAX video door phone/PC/Android tablet and adds the devices to the configuration via the MAX video door phone</i> .....	504
8.3.2.3	<i>Mode 2: The installer creates the configuration in the laboratory on the MAX video door phone/PC/Android tablet but adds the devices via Android tablet</i> .....	505
8.3.2.4	<i>Mode 3: The installer creates the configuration in the laboratory on the MAX video door phone/PC/Android tablet and adds at the same time the devices that are not yet installed</i> .....	507



8.3.2.5	<i>Mode 3.1: The installer creates the configuration in the laboratory on the MAX video door phone/PC/Android tablet and adds at the same time the previously installed devices ..</i>	508
8.3.2.6	<i>Mode 4: One MAX video door phone with configurator in "Acquisition" mode .....</i>	509
8.4	<i>Configuration distribution.....</i>	512
8.5	<i>Exporting the configuration to an SD card .....</i>	515
8.6	<i>Securing the system.....</i>	516
8.7	<i>Changing the system configuration .....</i>	517
8.7.1	<i>Unlocking a system .....</i>	518
8.7.2	<i>How to change the configuration .....</i>	519
8.7.3	<i>Changing the administrator password .....</i>	521
8.7.4	<i>Changing the installer password.....</i>	522
8.7.5	<i>Devices not aligned to the same IPerCom version or UPTK software development platform .</i>	524
9	<i>Integration with the iPerTALK system.....</i>	530
9.1	<i>Configuration and installation sequence for integration of the iPerTALK system into the IPerCom system with the switch Ref. 1375/701.....</i>	531
9.1.1	<i>iPerTALK system configuration .....</i>	531
9.1.2	<i>IPerCom system configuration .....</i>	532
9.2	<i>Configuration and installation sequence for integration of the iPerTALK system into the IPerCom system without the switch Ref. 1375/701.....</i>	535
9.2.1	<i>IPerCom system configuration .....</i>	535
9.2.2	<i>iPerTALK system configuration .....</i>	537
9.3	<i>Auto-on function on iPerTALK RTSP cameras from IPerCom video door phones .....</i>	538
10	<i>Restoring the factory settings.....</i>	541
10.1	<i>Factory reset of MAX, VOG<sup>7</sup>, Basic video door phone and IPerCom Client app.....</i>	542
10.2	<i>Factory reset of video door phone VOG<sup>5+</sup> .....</i>	543
10.3	<i>Factory reset of video door phone VOG<sup>5</sup> .....</i>	545
10.4	<i>Factory reset of Door Phones Miro .....</i>	547
10.5	<i>Factory reset of Call Modules 1060/12-13-17-18-23.....</i>	548
10.6	<i>Factory reset of the Modular Entry Panel with 1060/48 .....</i>	551
10.6.1	<i>Factory reset via the Outdoor Audio and Video IP Station 1060/48 .....</i>	551
10.6.2	<i>Factory reset via the Display Module 1168/1 .....</i>	553
10.7	<i>Factory reset of the Entry panels 1060/71-/74-75-78 .....</i>	554
10.8	<i>Factory reset of IPerCom 2Voice Gateway .....</i>	555
10.9	<i>Factory reset of the lift interface 1060/37 .....</i>	556

10.10	Factory reset of the Entry panel 1060/33-34.....	557
10.11	Factory reset of Entry Panel 1060/21 .....	558
10.12	Factory reset of Floor Entry Panel 1060/22 .....	559
<b>APPENDIX A: Configuration parameters of IPerCom devices .....</b>		<b>560</b>
	Server 1060/1.....	560
	Call Module 1060/12-13-17-18.....	561
	Call Module 1060/23 .....	568
	Modular Calling Station with 1060/48.....	575
	Entry Panel 1060/71-74-75-/78.....	585
	Entry panel 1060/33 .....	592
	Entry panel 1060/34.....	599
	Entry Panel 1060/21.....	605
	Private Call Module 1060/22.....	610
	Switchboard 1060/41 .....	613
	Video door phone 7" VOG <sup>7</sup> 1761/31-32-33 .....	615
	Video door phone 5" VOG <sup>5+</sup> 1761/15-16-17-18 .....	616
	Video door phone 5" VOG <sup>5</sup> 1761/6.....	617
	Video door phone 7" MAX 1717/31-32-33-34-41 .....	619
	Video door phone 10" MAX 1717/21-22-23 .....	620
	Video door phone 7" Basic 1741/1-2-3 .....	621
	IPerCom Client 1060/43 .....	622
	Miro door phone 1160/3.....	623
	Key Reader 1060/45 or 1060/86.....	625
	Relay actuator 1060/84 v. 2.07 / 3.04 / v. 4.05 .....	628
	IPerTAlk Server / IPerTAlk Server V1.....	631
	IPassan controller.....	632
	IPerCom-2Voice Gateway 1083/59.....	633
	IperCom Clock Module 1060/85 .....	634
	Lift interface 1060/37.....	635
	RTSP Camera.....	637
	RTSP Camera (NVR).....	639
<b>APPENDIX B: Differences of functions between 2Voice and IPerCom apartment station .....</b>		<b>641</b>
<b>APPENDIX C: Differences of functions between 2Voice and IPerCom devices with IPerCom Switchboard .....</b>		<b>642</b>

<i>APPENDIX D: IPerCom priority calls.....</i>	<i>643</i>
<i>APPENDIX E: Type of proximity keys that can be read by IPerCom devices with access control function</i>	<i>644</i>
<i>APPENDIX F1: How to use customized network settings in IperCom system.....</i>	<i>645</i>
<i>APPENDIX F2: Custom network settings and editable static IP addresses for IPerCom devices .....</i>	<i>656</i>
<i>APPENDIX G: Changing the network settings of IPerCom Installer Tools.....</i>	<i>659</i>
<i>APPENDIX H: Date and time incorrectly set in the future. ....</i>	<i>662</i>
<i>APPENDIX I: Modular entry panel with 1060/48 Alpha .....</i>	<i>663</i>
<i>APPENDIX L: Alpha call module 1168 .....</i>	<i>715</i>
<i>APPENDIX M1: Streaming video from IPerCom calling stations to NVR Urmet.....</i>	<i>743</i>
<i>Software requirements.....</i>	<i>743</i>
<i>Display of the software version.....</i>	<i>744</i>
<i>Software update of the Urmet NVR device .....</i>	<i>749</i>
<i>Connection of the Urmet NVR device to the IPerCom system.....</i>	<i>750</i>
<i>Enabling the RTSP streaming during calls from Modular Calling Station with 1060/48.....</i>	<i>752</i>
<i>Association of an IP channel with the RTSP streaming of a calling station .....</i>	<i>753</i>
<i>Viewing the streaming video .....</i>	<i>756</i>
<i>APPENDIX M2: RTSP Cameras with NVR Urmet device .....</i>	<i>761</i>
<i>APPENDIX N: “Site name” and “Global site ID” field definition.....</i>	<i>765</i>
<i>APPENDIX O: IPassan integration with IPerCom .....</i>	<i>769</i>
<i>APPENDIX P1: How to properly turn 1060/1 Server on and off. ....</i>	<i>770</i>
<i>APPENDIX P2: Connection between 1060/1 Server and UPS device. ....</i>	<i>771</i>
<i>APPENDIX P3: Replacing a 1060/1 Server that is no longer working.....</i>	<i>773</i>
<i>APPENDIX Q: First upgrade of a system via Server 1060/1 .....</i>	<i>774</i>
<i>APPENDIX R: Call to several Switchboard applications each connected to a CallMe app .....</i>	<i>776</i>
<i>APPENDIX S: CallMe contacts .....</i>	<i>780</i>
<i>APPENDIX T: Consumption in watts of IPerCom devices.....</i>	<i>783</i>
<i>APPENDIX U: Types of system/performance for which the presence of the 1060/1 Server is required....</i>	<i>784</i>
<i>APPENDIX V: Device compatibility table.....</i>	<i>786</i>
<i>APPENDIX W1: RTSP Cameras supported by IPerCom video door phones .....</i>	<i>789</i>
<i>APPENDIX W2: Auto-on on RTSP Cameras.....</i>	<i>790</i>
<i>APPENDIX X: CallMe operating mode for VOG<sup>7</sup>, MAX 1717/3x and 1717/2x video door phones.....</i>	<i>791</i>
<i>APPENDIX V: Template of the list of devices installed in the system .....</i>	<i>793</i>

## 1 Introduction

**IPerCom 3.1.0** is an IP video door phone system with the following features:

1. it supports small and medium-sized systems with a maximum number of 1000 IP devices and a maximum number of 1000 users without having to use any system server <sup>1</sup>;
2. it supports small and medium-sized systems with a maximum number of 4000 IP devices and a maximum number of 10000 users if the system is equipped with one or more system servers;
3. allows you to receive calls on a smartphone/tablet via the CallMe app, even without having a door phone or a video door phone in the apartment (for further details see the following [IPerCloud mode](#) paragraph);
4. increase in IT security relating to passwords used in system applications and devices;
5. it does not have single vulnerability points both in case of systems without servers and in case of systems with several servers<sup>2</sup>;
6. it can be configured via the *configurator* (integrated in the *IPerCom Installer Tools* app released for the Windows operating system and in the video door phones) and via the *IPerCom Configurator* app released for Android tablets;
7. it allows the System Logs to be displayed on the *Switchboard*<sup>3</sup> and *IPerCom Installer Tools* (in this case only if there is at least one system server in the system), i.e. the events relating to system operation (e.g. call log, access point activity, user activity, alarms and so on);
8. it allows displaying on *Switchboard* and *IPerCom Installer Tools* the system diagnostic, i.e. a set of information that allow understanding if all the devices connected to the system work properly and if they have been correctly updated and configured;
9. it can work on an existing network with other already installed devices;
10. all communications between devices are encrypted using a proprietary algorithm to prevent attacks to the system;
11. provides 2 levels of security for each system model chosen in the *configurator*;
12. it is not necessary for the installer to have in-depth knowledge of IP networks: it is sufficient to have a basic knowledge of network equipment (switches, routers and PoE ports) and their connections;
13. the remote technical support benefits from the fact that the configuration of the system is in a single small file (usually < 1 MB), it allows the System Logs to be displayed on the *Switchboard*<sup>4</sup> and *IPerCom Installer Tools* (in this case only if there is at least one system server in the system), i.e. the events relating to system operation (e.g. call log, access point activity, user activity, alarms and so on) this is a great advantage compared to other systems, where it is necessary to back up the database, which can reach over 100 MB and to be analysed requires a physical server on which to import the backup configuration;

---

<sup>1</sup> The presence of a server is however recommended for systems with more than 500 devices to better optimize the workload of the system and make the use of the IP network by the system more efficient.

<sup>2</sup> In systems with up to 1000 IP devices and/or 1000 users and only one server, there will only be a 15-minute downtime if it stops operation. With more than 1000 IP devices and/or 1000 users and only one server the disruption would be permanent; therefore, in these conditions, it is recommended to have more servers (at least 2) in the system, so that any malfunction of one of the servers is compensated for by the presence of the others, and this does not cause any disruption to the system.

<sup>3</sup> The *Switchboard* is a software application (Switchboard application) designed to allow the concierge staff of a building to manage all the typical functions of a switchboard station.

14. in systems with at least one system server, the configuration file can also be backed up periodically (automatic mode) to a USB stick (connected to the server) using *iPerCom Installer Tools*;
15. in systems with at least one system server, the firmware update of all devices can take place automatically via the server itself (appropriately configured).

## 1.1 IPerCloud mode

The IPerCloud mode, integrated into the IPerCom system starting from version 3.0.0, allows to receive calls on the “Urmet CallMe 2023 ed.” app (for smartphones/tablets) without the need for a door phone or video door phone in apartment: in this mode, the apartments are defined as **IPerCloud apartments**.

The “Urmet CallMe 2023 ed.” app is available for both Android (minimum version 8) and iOS (minimum version 13) and in this manual it will simply be called the *CallMe* app.



*In general, the CallMe app can be used with IPerCom systems with a minimum version of 2.1.0. For versions below 2.1.0, it is necessary to use “Urmet CallMe” app available for both Android (minimum version 5) and iOS (minimum version 12.5).*



*The call forwarding to a smartphone/tablet is also possible with versions of IPerCom prior to version 3.0.0, with the only difference that a door phone or a video door phone is required in the apartment.*

The IPerCloud mode requires the use of licenses to function. These licenses have a duration of 5 years or 15 years and are distributed in versions from 1 to 200 users. Licenses can be renewed for one year through *CallMe* in-app purchase.

The *CallMe* app naturally requires an Internet connection on your smartphone/tablet to function correctly. In cases where Internet coverage is absent or unstable, it is possible to forward the call over the GSM (smartphone/tablet) or landline phone network, thus avoiding potential disruptions and making the system more reliable.



*The call to the GSM or landline phone network, if enabled, is forwarded both in the presence and absence of an Internet connection. In the first case, the call arrives approximately 10 seconds after the call forwarded through the CallMe application. If the user answers the call via the app, the call forwarded to the GSM or landline phone network is cancelled.*

The call forwarding service to the GSM or landline phone network is linked to licenses and has a duration of 30 days for 15-year licenses and a duration of 5 years for 5-year licenses. In both cases, renewal can be done through *CallMe* in-app purchase and is valid for one year.



*For 5-year licenses, renewing the license for one year also includes the renewal of the call forwarding service to the GSM or landline phone network for one year. For 15-year licenses, after 30 days, it is possible to renew only the call forwarding service to the GSM or landline phone network for one year.*

The configuration of the IPerCloud mode requires the mandatory use of the following applications to be used in the following order:

- *IPerCom Installer Tools* (Windows application) for the installer ([registration on Urmet Cloud is required](#)),
- *CallMe Manager* (Windows application) for the installer and building manager ([registration on Urmet Cloud is required](#)),
- *CallMe* (Android or iOS smartphone/tablet application) for the end-user ([registration on Urmet Cloud is required](#)).

The first two applications are available on the [www.urmet.com](http://www.urmet.com) website, the third is available on the respective app stores.

Below is the list of actions to be carried out by the installer, building manager and end-user for correct configuration of an IPerCom system in IPerCloud mode.

## INSTALLER

The installer uses the *IPerCom Installer Tools* application to:

- create an Urmet Cloud account and authenticate on *IPerCom Installer Tools* with this account,
- create a system configuration with IPerCloud apartments,
- enable the *test mode* (from the *configurator*) and then verify that the call to a test IPerCloud apartment from any calling station reaches the *CallMe* application without pre-activating (and therefore wasting) any license,
- disable the test mode (from the *configurator*),
- pre-activate license bundles.

The installer uses the *CallMe Manager* application (authenticating with the same account as *IPerCom Installer Tools*) to:

- activate the licenses and apply them to the IPerCloud apartments,
- transfer the property of the site to the building manager via invitation sent via email.

All these features will be explained in detail in the relevant paragraphs.



*Creating the configuration in IPerCom systems in IPerCloud mode must be done exclusively by IPerCom Installer Tools. Any changes must also always be made by IPerCom Installer Tools starting from the relevant project (see paragraph [How to use IPerCom Installer Tools for the configuration of a system](#)).*

## **BUILDING MANAGER**

The building manager must first accept the invitation sent by the installer, then use the *CallMe Manager* application to:

- create an Urmet Cloud account and authenticate on *CallMe Manager* with this account,
- acquire the site created by the installer,
- generate letters (pdf format) with the QR-code,
- send letters via email or post to users.



*Printing the letters in PDF is an activity that the installer could also do via the CallMe Manager application, after assigning the licenses. Once printed, the installer can send them via email to the building manager, who forwards them to the various apartment residents.*

The point of union between the two apps is the transfer of the ownership of the site from the installer to the building manager, meaning by site the topological structure of the system. The transfer takes place, as already mentioned, by means of an invitation sent via email from the installer to the building manager via the *CallMe Manager* application.



*The topological structure (of the system) is intended as a simplified map of the various elements that compose it (blocks, stairs, floors, and apartments) and their relative positioning.*



*For further details on the use of the CallMe Manager app, see paragraph [Configuring the call forwarding function in IPerCom systems in IPerCloud mode](#), where the main steps to activate the license bundles, associate the licences to an apartment and print the relevant QR codes are shown. For more detailed information, please refer to the app user manual which can be downloaded from the website [www.urmet.com](http://www.urmet.com).*



## END-USER

The end-user uses the *CallMe* application to:

- create an Urmet Cloud account and authenticate on *CallMe* with this account,
- scan the QR code sent by the building manager to associate the account (created in the previous point) with the apartment.

Once this is done, you can receive the call to an IPerCloud apartment on your smartphone/tablet.



For further details on using the *CallMe* app, see the paragraph [Configuring the call forwarding function in IPerCom systems in IPerCloud mode](#), where the fundamental steps to follow to receive a call from an IPerCloud apartment will be illustrated. For more detailed information, please refer to the app user manual which can be downloaded from the website [www.urmet.com](http://www.urmet.com).

The various points reported above can be summarized as follows:

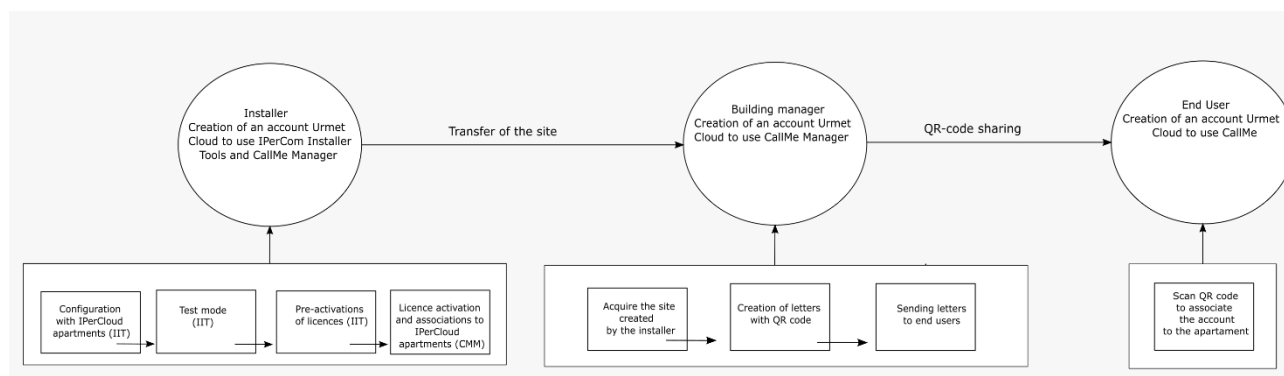


Figure 1: IPerCloud mode configuration

Since the IperCloud mode is integrated into the IPerCom system, it is important to underline that all the IPerCom functions are also available for the IPerCloud apartments (for example access control and activations); therefore, everything written for the Ipercom system also remains valid for the Ipercloud mode, except where explicitly indicated.

## 1.2 Configuration of an IPerCom system

It is advisable to use the *IPerCom Installer Tools* application as configuration tool for an IPerCom system. The tool allows to:

- automatically update to the latest version available (if there is an Internet connection);
- detect the version of IPerCom installed on a system;
- select which version of IPerCom you want to work with when starting the application and then automatically start the compatible version of *IPerCom Installer Tools*;
- create a **project** to be associated with a system (**site**);
- save and edit a project;
- import a project from PC and export a project to PC;
- set the time of an IPerCom system or retrieve its time;
- distribute the configuration associated with a project to the system;
- lock or unlock an IPerCom system;
- view the system diagnostics, that is view if all the devices are aligned with the same version of IPerCom, if they are correctly connected to the system and if the configuration is aligned across the entire system;
- view the event history, for example list of calls, access to gates, alarms (this function is only available if there is at least one 1060/1 *Server* in the system);
- carry out a backup of the system configuration directly on your PC or in automatic mode on a USB stick connected to the 1060/1 *Server* (the performance of the backup on the PC is in any case linked to the presence of a 1060/1 *Server* in the system);
- import a project to a higher IPerCom version (import is possible for projects created starting from IPerCom 2.0.0);
- connect to Urmet Cloud (after registering) to:
  - save projects on Urmet Cloud so as not to lose them (for example if the data on your PC is no longer available);
  - transfer the configuration of a project with IPerCloud apartments to a system;
  - use the *CallMe Manager* application to configure call forwarding;
  - modify the configuration of a system even remotely (if at least one 1060/1 *Server* is present on the remote system);
  - transfer a project to another installer/administrator;
  - pre-activate the licenses for IPerCloud mode;
  - view the history of pre-activated licenses;
  - run the test mode for IPerCloud mode.

All these features, which will be explained in detail in this manual, make *IPerCom Installer Tools* a useful and versatile tool for the installer. The configuration of a system will be explained also with reference to the video door phones of the IPerCom system and the *IPerCom Configurator* app.



*The system technical manual for the installer is intended as a manual for setting up an IPerCom system, so for the use and the detailed installation of the single devices and software applications please refer to the relevant user and installation manuals, available on the website [www.urmet.com](http://www.urmet.com).*




*In this manual, calling station means a generic call module or entry panel of the system, while an apartment station means a video door phone or door phone in an apartment.*

### 1.3 IT security of the IPerCom system

To increase IT security, starting from version 3.1.0 the following has been introduced regarding the passwords used by the applications and devices of the IPerCom system.

1. The complexity of new passwords must meet the requirements below:


- minimum length: 8 characters,
- maximum length: 19 characters,
- presence of at least one uppercase character,
- presence of at least one lowercase character,
- presence of at least one numeric character,
- presence of at least one special character.


 *If your password does not meet these requirements, a dialog box listing all the above requirements is displayed.*


Therefore, there must be no fixed passwords, which can easily be recovered by attackers to carry out attacks on the system

The passwords subject to this change are detailed below:

- installer password, both when it is entered when creating the configuration of a new project and when it is modified (from *configuratore* or *IPerCom Installer Tools*);
- password to start the *Switchboard* application (entered from the *configurator*);
- administrator password to block the system (entered by *IPerCom Installer Tools*);
- password to enable RTSP streaming video of one or more calling stations;
- password to change the date and time from the video door phones *MAX*, *Basic* and *VOG*<sup>7</sup>.

 *This manual will explain in detail where the passwords listed above appear and their use.*

 *In the case of IPerCom systems created with versions prior to version 3.1.0, the old passwords continue to be valid even if they do not satisfy the above requirements. However, it is advisable to modify them as previously written.*

 *The Urmet Cloud registration passwords for the IPerCom Installer Tools, CallMe Manager and CallMe applications already meet the above requirements in versions prior to 3.1.0.*

2. Because of point 1), the fixed password "1937" (where present) has been removed from the applications and devices of the IPerCom system.

3. Protection against "*brute force*" attacks aimed at discovering passwords in use.

To protect applications and software from possible "*brute force*" attacks, it is necessary to wait 5 seconds to enter a new password (if the previous one was wrong). This delay, combined with the new password security requirements, makes this type of attack practically impractical for an attacker.

## 2 IPerCom devices and features offered by the system

IPerCom system 3.1.0 supports the devices indicated below<sup>5</sup>:

- Server:
  - *IPerCom Server 1060/1*
- Switchboards:
  - *Switchboard (software application) 1060/41<sup>6</sup>*
- Calling stations:
  - *Call module soft touch 1060/12-13 and vandal-proof 1060/17-18*
  - *Vandal-proof call module 1060/23*
  - *Modular entry panel with 1060/48*
  - *Entry panel 1060/71-74-75-78*
  - *Entry panel 1060/33*
  - *Entry panel 1060/34*
  - *Entry panel 1060/21*
  - *Floor entry panel 1060/22*
- Apartment stations:
  - *7" VOG<sup>7</sup> video door phone 1761/31-32-33*
  - *7" VOG<sup>7</sup> video door phone 1761/31U-33U*
  - *5" VOG<sup>5+</sup> video door phone 1761/15-16-18-19*
  - *5" VOG<sup>5+</sup> video door phone 1761/15U-16U*
  - *5" VOG<sup>5</sup> video door phone 1761/6*
  - *7" MAX video door phone 1717/31-32-33-34-41*
  - *10" MAX video door phone 1717/21-22-23*
  - *10" MAX video door phone 1717/21U-23U*
  - *7" Basic video door phone 1741/1-2-3*
  - *IPerCom Client 1060/43 (software application)*
  - *Miro door phone 1160/3*
- Key Readers:
  - *Key reader 1060/45*
  - *Key reader 1060/86*
- Relay Actuators:
  - *Relay Actuator 1060/84 v. 2.07*
  - *Relay Actuator 1060/84 v. 3.04*
  - *Relay Actuator 1060/84 v. 4.05*
- Integration Devices:
  - *IPerTalk Server / IPerTalk Server V1*
  - *IPassan Controller*
  - *2Voice Gateway 1083/59*

<sup>4</sup> IPerCom supports a maximum of 20 devices among MAX monitors and Audio Apartment Stations per apartment and a maximum of 10 Switchboards.

<sup>5</sup> The Switchboard supports event log and diagnostic functions. For further details see the installation and user manual of the [Switchboard](#) downloadable from [www.urmet.com](http://www.urmet.com)

- Other Devices:
  - IPerCom Clock Module 1060/85
  - Lift Interface 1060/37
  - RTSP Camera
  - RTSP Camera (NVR)



*It is recommended to have a maximum of 200 devices in an IPerCom system including Key Reader 1060/45, Key Reader 1060/86, Relay Actuators 1060/84, and Lift Interface 1060/37.*



*In [APPENDIX V: Device compatibility table](#) the set of supported devices is reported for each version of IPerCom officially released.*

IPerCom system 3.1.0 supports the following services:

- Audio/video communication on calls from calling station to an apartment station and on intercom calls,
- Opening of the main door and gate from apartment stations during call and conversation with calling stations,
- Auto-on on all calling stations and *RTSP Cameras* from all video door phones of the system (for *VOG<sup>5</sup>* and *VOG<sup>5+</sup>* video door phones, see the list of supported *RTSP Cameras* in [APPENDIX W1: RTSP Cameras supported by IPerCom video door phones](#)),
- Access control,
- Addition of 2Voice type columns to the IPerCom system through the *2Voice Gateway 1083/59*,
- Display of the system logs (if there is at least one *Server 1060/1* in the system) and the diagnostic through the *IPerCom Installer Tools* application (both services are available on the *Switchboard* even without the presence of a *Server 1060/1* in the system),
- Activation of *Relay actuator 1060/84* outputs through:
  - system events,
  - events on *Relay actuator* inputs (starting from firmware version 3.04),
  - scheduling.
- Calling station gate contact configurable as *1060/84 Relay Actuator* output,
- System alarm generation through events on *Relay actuator 1060/84* inputs (starting from firmware version 3.04),
- “*User recognition*” function, that is the passage of a proximity key or the entering of an opened door key code associated with a resident or non-resident, in addition to opening the access point, also activates one or more outputs of a *Relay Actuator* depending on the user,
- Remote relay function, remote entrance hall button and remote door open sensor (from *relay actuators* with firmware version 4.05),
- Control of one or more lifts through the *Lift Interface 1060/37*,
- Call divert to another apartment or to the switchboard,
- Centralised firmware upgrade via *IPerUpgrade* application for Microsoft Windows (available at [www.urmet.com](http://www.urmet.com)) or via *Server 1060/1*,
- IPassan advanced access control and IPerTalk systems integration,
- IPerCloud mode integration,
- Floor call button on apartment station configurable as an alarm button,
- Hall button configurable as *Switchboard* call button,



- Call forwarding on smartphone/tablet Android and iOS via CallMe app with these additional features:
  - Auto on on IPerCom calling stations,
  - Intercom calls to apartment stations,
  - Display of missed calls with snapshot from calling stations,
  - Opening of main doors and gates during and outside calls,
  - Sending commands to activate the outputs of one or more relay actuators,
  - Alarm history display with emergency call,
  - Renewal of licenses with in app purchase (IPerCloud mode),
  - Callback to a landline or GSM telephone network if Internet coverage is absent (only in IPerCloud mode),
  - Sharing of the service with up to 10 users,
  
- Concierge service with the following features:
  - Day mode to intercept calls,
  - Night mode,
  - Stand-by with divert function on other switchboards,
  - Door opening,
  - Display of active calls on the system,
  - Visual and acoustic signalling of alarms with log of received and reset alarms,
  - Auto-on function on calling stations and *RTSP cameras*,
  - System logs displayed in 2 different modes,
  - Diagnostic function,
  - Activation of *Relay actuator* 1060/84 outputs (even through code),
  - *Lift Interface* relay activation 1060/37,
  - Call forwarding to Android and iOS smartphones/tablets via app *CallMe*,
  - Alarm, apartment call and door opener services available also via maps.

IPerCom system 3.1.0 supports the following licences for the IPerCloud mode:

- *5 years 1 user license (5Y) 1065/001,*
- *5 years 10 users license (5Y) 1065/010,*
- *5 years 50 users license (5Y) 1065/050,*
- *5 years 100 users license (5Y) 1065/100,*
- *5 years 200 users license (5Y) 1065/200,*
- *15 years 1 user license (LT) 1065/601,*
- *15 years 10 users license (LT) 1065/610,*
- *15 years 50 users license (LT) 1065/650,*
- *15 years 100 users license (LT) 1065/700,*
- *15 years 200 users license (LT) 1065/800.*



*The 5Y license includes the callback service on the landline/GSM network for a period of 5 years while for the LT license the same service has a duration of 30 days.*

## 2.1 Server 1060/1

The *Server 1060/1* is a device required to manage large installations (with more than 1000 IP devices and/or 1000 users) and to have the System Logs available on *IPerCom Installer Tools*. It is possible to configure up to 4000 IP devices and 10000 users with at least one *Server 1060/1* in the system. The *Server 1060/1*, properly configured, can also update independently the various devices of the system: this means that through *IPerUpgrade* it is sufficient to upgrade only the *Server 1060/1*, which will upgrade the rest of the system.

It is mandatory that all servers connected to the system are configured (and therefore added to the configuration) via *IPerCom Installer Tools*: if this is not the case (i.e. servers connected but not configured) the system will not work properly.

It is strongly recommended to connect a UPS (uninterruptible power supply) device to the *Server 1060/1*, to avoid irreparable damage caused by possible voltage drops and sudden power outages. The UPS models currently supported are BK350EI/BK500EI/BK650EI. *IPerCom Installer Tools* be used to obtain information about the UPS parameters, including the battery charge level. Appendices P1, P2 and P3 contain detailed information on how to properly turn 1060/1 *Server* on and off, how to connect it to the UPS device and how to replace it in case of failure.



For details on the operation of the *IPerUpgrade* app, please refer to the relevant manual available at the site [www.urmet.com](http://www.urmet.com).



For the correct system configuration see the paragraph [The configurator](#).

## 2.2 Call Module 1060/12-13-17-18

The *Call Module 1060/12-13-17-18* is a call station with 3.5" colour display and alphanumeric keyboard.

The graphic display allows access to various functions (such as the residents' address book, direct call to the relevant switchboard, door opening via numeric code) and the display of a welcome message (the display is switched on automatically by means of a proximity sensor).

The Call Module can independently control two different outputs. The first is used to open a pedestrian door, the second to control the gate opening control unit of a possible garage gate.

The device allows access to the pedestrian door and to the driveway also by means of an integrated proximity key reader (with 125KHz technology) or by typing a user code on the alphanumeric keypad; in the latter case it also allows managing the anti-coercion function through which a silent alarm is sent to the gatekeeper lodge exchange at the same time as the door is opened.

It is also possible to set access to the pedestrian door and the driveway through both the reading of a key and the typing of a code (both enabled).

The version 1060/12-13 features a soft-touch alphanumeric keypad and glass panel, while the version 1060/17-18 features a vandal resistant steel front panel.

It can be used in both 50Hz (1060/13-18) and 60Hz (1060/12-17) systems.

### 2.3 Call Module 1060/23

The *Call Module 1060/23* is a call station with 3.5" colour display, alphanumeric keyboard, and steel vandal resistant front panel.

The graphic display allows access to various functions (such as the residents' address book, direct call to the relevant switchboard, door opening via numeric code) and the display of a welcome message (the display is switched on automatically by means of a proximity sensor).

The *Call Module* can independently control two different outputs: the first one used to open a pedestrian door, the second one to control the gate of a driveway.

The device allows access to the pedestrian door and to the driveway also by means of an integrated proximity key reader (with MiFare Plus technology) or user code on the alphanumeric keypad; in the latter case, it also allows managing the anti-coercion function through which a silent alarm is sent to the gatekeeper lodge exchange at the same time as the door is opened.

It is also possible to set access to the pedestrian door and the driveway through both the reading of a key and the typing of a code (both enabled).

It can be used in both 50Hz and 60Hz systems.

### 2.4 Modular calling station with 1060/48

*Modular calling station with 1060/48* is a calling station consisting of an *IP audio and video outdoor station 1060/48* with 2 call buttons, based on model Alpha with single-module mechanics. The calling station can be extended up to a maximum of 45 buttons on one row or 90 buttons on two rows by means of proper expansion modules 1168/4 and 1168/8.

The *Modular calling station with 1060/48* can independently control two different outputs: the first one used to open a pedestrian door, the second one to control the gate opening control unit of a possible driveway.

On the *IP audio and video outdoor station 1060/48* there are 3 LEDs for signalling the system status (call in progress, line busy, door open and other). System status can also be signalled via vocal messages.

For more detail on configuration of the *Modular Entry Panel with 1060/48*, see [APPENDIX I: Modular entry panel with 1060/48 Alpha](#)

It can be used in both 50Hz and 60Hz systems.

### 2.4.1 Call module

The *IP audio and video outdoor station 1060/48* together with the *Display Module 1168/1* and the *Numeric Keypad 1168/46* make up the standard configuration of a call module.

The *Display Module 1168/1* allows access to various functions (such as the residents' address book, direct call to the relevant switchboard, door opening via numeric code) and the display of a welcome message.

The *IP audio and video outdoor station 1060/48* can independently control two different outputs: the first one used to open a pedestrian door, the second one to control the gate opening control unit of a possible driveway.

On the *IP audio and video outdoor station 1060/48* there are 3 LEDs for signalling the system status (call in progress, line busy, door open and other). System status can also be signalled via vocal messages.

The call module allows access to the pedestrian door and the driveway also by entering a user code on the *Numeric Keypad 1168/46*. In the latter case, it is also possible to manage the anti-coercion function through which a silent alarm is sent to the concierge switchboard at the same time as the door is opened.

Using the extended configuration like call module it is possible to integrate a *Proximity Key Reader module 1168/45* (with MiFare Plus technology) for access control.

For more detail on configuration of the *Alpha Call Module*, see [APPENDIX L: Alpha call module 1168](#).

It can be used in both 50Hz and 60Hz systems.

### 2.5 Entry Panel 1060/71-74-75-78

The *Entry Panel 1060/71-74-75-78* is a calling station with 2 push buttons (only 1 for 1060/71).

By means of special add-on modules it is possible to extend the buttons up to a maximum number of 32.

The *Entry Panel* can independently control two different outputs. The first is used to open a pedestrian door, the second to control the gate opening control unit of a possible garage gate.

It can be used in both 50Hz (1060/74) and 60Hz (1060/75) systems.

The one-button version 1060/71 is to be used in 50Hz systems.

The *Entry Panel 1060/78* It can be used in both 50Hz and 60Hz systems.

## 2.6 Entry Panel 1060/21

The *Entry Panel 1060/21* is a vandal-proof calling station with a single push button with weather-proof zama front.

It can independently control two different outputs. The first is used to open a pedestrian door, the second to control the gate opening control unit of a possible driveway.

The *Entry Panel* integrates a proximity key reader (with MiFare technology) for access control only for the pedestrian door.

It can be used in both 50Hz and 60Hz systems.

### 2.6.1 Villa Kit with *Entry Panel 1060/21* in IPerCloud mode

The villa kit with Mikra entry panel 1060/21 in IPerCloud mode is aimed at a single-family unit and does not require the use of the *IPerCom Installer Tools* and/or *CallMe Manager* applications for the initial configuration. All configuration operations can be performed by simply scanning a specific QR-code with the *CallMe* app. The license automatically provided on the *CallMe* application (via the previously scanned QR-code) is of the LT type (15 years) with 1 month of fallback service on landline/GSM included. For further information, consult the [relevant booklet](#).

## 2.7 Entry panel Mikra Plus 1060/33

The *Entry panel 1060/33* is a call station with a 3.5" display and weatherproof zamak faceplate.

The graphic display allows accessing a directory with 4 names (the display switches on automatically thanks to a proximity sensor).

It can independently control an output to open a pedestrian door and a second output to control the gate of a possible driveway.

Visual and acoustic (vocal messages) signalling of system status (call in progress, line busy, door open, etc.).

It can be used in both 50Hz and 60Hz systems.

## 2.8 Entry panel Mikra Digital 1060/34

The *Entry panel 1060/34* is a call station with a 3.5" display and weatherproof zamak faceplate.

The graphic display allows accessing the resident directory (the display switches on automatically thanks to a proximity sensor).

It can independently control an output for pedestrian door and a second output to control the gate of a possible driveway.

Visual and acoustic (vocal messages) signalling of system status (call in progress, line busy, door open, etc.).

It can be used in both 50Hz and 60Hz systems.

## 2.9 Private Call Module 1060/22

The *Private Call Module* 1060/22 is a one-push button call station to be installed directly outside the main door of the apartment.

It can only call the apartment station of the apartment to which the call station is associated.

Apartment station can make auto-on on the *Private Call Module*.

## 2.10 Video door phone 7" VOG<sup>7</sup> 1761/31-32-33

The video door phone *VOG<sup>7</sup> 1761/31-32-33* is a hands-free video door phone apartment station with a 7" touch-screen.

The video door phone allows call forwarding to smartphones / tablets through the CallMe app (for Android and iOS), as well as allowing normal video door phone functions (also via gesture or voice commands).

Versions 1761/31-33 also integrate light and shutter automation (via integrated Yokis remote control), intrusion detection and video surveillance functions.

Version 1761/32 integrates only intrusion detection and video surveillance functions.

## 2.11 Video door phone 7" VOG<sup>7</sup> 1761/31U-33U

The video door phone *VOG<sup>7</sup> 1761/31U-33U* is a hands-free video door phone apartment station with a 7" touch-screen.

The video door phone allows call forwarding to smartphones / tablets through the CallMe app (for Android and iOS), as well as allowing normal video door phone functions (also via gesture or voice commands).

Versions 1761/31U-33U also integrate light and shutter automation (via integrated Yokis UP remote control), intrusion detection and video surveillance functions.

For further details on Yokis UP, see the Urmet web page relating to the [Smart Home](#).




*The 7" VOG<sup>7</sup> 1761/31U-33U video door phones, apart from the light and shutter automation functions, are like the 1761/31-33 video door phones and therefore in this manual we will always refer to the versions without U.*

## 2.12 Video door phone 5" VOG<sup>5+</sup> 1761/15-16-18-19

The video door phone VOG<sup>5+</sup> 1761/15-16-18-19 is a hands-free video door phone indoor station with a 5" display and soft-touch keys.

The video door phone allows call forwarding to smartphones/tablets via the *CallMe* app (for Android and iOS), as well as enabling normal video door phone functions (also via gesture or voice commands).

Versions 1761/15-16 also integrate light and shutter automation (via integrated Yokis remote control).

 *The video door phone VOG<sup>5+</sup> 1761/15-16-18-19 does not allow you to configure the IPerCom system or export the configuration file to an SD-card.*


## 2.13 Video door phone 5" VOG<sup>5+</sup> 1761/15U-16U


The video door phone VOG<sup>5+</sup> 1761/15U-16U is a hands-free video door phone indoor station with a 5" display and soft-touch keys.

The video door phone allows call forwarding to smartphones/tablets via the *CallMe* app (for Android and iOS), as well as enabling normal video door phone functions (also via gesture or voice commands).

Versions 1761/15U-16U also integrate light and shutter automation (via integrated Yokis UP remote control).

For further details on Yokis UP, see the Urmet web page relating to the [Smart Home](#).


 *The video door phone VOG<sup>5+</sup> 1761/15U-16U does not allow you to configure the IPerCom system or export the configuration file to an SD-card.*

 *The 7" VOG<sup>7</sup> 1761/15U-16U video door phones, apart from the light and shutter automation functions, are like the 1761/15-16 video door phones and therefore in this manual we will always refer to the versions without U.*

## 2.14 Video door phone 5" VOG<sup>5</sup> 1761/6

The video door phone VOG<sup>5</sup> 1761/6 is a hands-free video door phone apartment station with a 5" display and soft-touch buttons.

The video door phone allows call forwarding to smartphones / tablets through the *CallMe* app (for Android and iOS), as well as allowing normal video door phone functions (also via gesture commands).

 *The video door phone 1761/6 does not allow you to configure the IPerCom system or export the configuration file to an SD-card*

## 2.15 Video door phone 7" MAX 1717/31-32-33-34-41

The video door phone MAX 1717/31-32-33-34-41 is a hands-free video door phone apartment station with a 7" touch-screen display.

The video door phone allows call forwarding to smartphones / tablets through the CallMe app (for Android and iOS), as well as allowing normal video door phone functions (also via gesture or voice commands for 1717/3x versions).

Versions 1717/31-33 also integrate light and shutter automation (via integrated Yokis remote control), intrusion detection and video surveillance functions.

Versions 1717/32-34 integrates intrusion detection and video surveillance functions.

Version 1717/41 integrates only the video door phone functions.

## 2.16 Video door phone 10" MAX 1717/21-22-23

The video door phone MAX 1717/21-22-23 is a hands-free video door phone apartment station with a 10" touch-screen display.

The video door phone allows call forwarding to smartphones / tablets through the CallMe app (for Android and iOS), as well as allowing normal video door phone functions (also via gesture or voice commands).

The video door phone MAX 10" also integrate light and shutter automation (via integrated Yokis remote control), intrusion detection and video surveillance functions.

The video door phone MAX 10" 1717/22-23 are to be used for the Chinese market only.

## 2.17 Video door phone 10" MAX 1717/21U-22U-23U

The video door phone MAX 1717/21U-22U-23U is a hands-free video door phone apartment station with a 10" touch-screen display.

The video door phone allows call forwarding to smartphones / tablets through the CallMe app (for Android and iOS), as well as allowing normal video door phone functions (also via gesture or voice commands).

The video door phone MAX 10" also integrate light and shutter automation (via integrated Yokis UP remote control), intrusion detection and video surveillance functions.

The video door phone MAX 10" 1717/22U-23U are to be used for the Chinese market only.

For further details on Yokis UP, see the Urmet web page relating to the [Smart Home](#).



*The MAX 10" 1717/21U-22U-23U video door phones, apart from the light and shutter automation functions, are like the 1717/21-22-23 video door phones and therefore in this manual we will always refer to the versions without U.*



## 2.18 Video door phone 7" Basic 1741/1-2-3

The video door phone *Basic 1741/1-2-3* is a hands-free video door phone apartment station with a 7" touch-screen display.

The video door phone allows call forwarding to smartphones / tablets through the CallMe app (for Android and iOS), as well as allowing normal video door phone functions (also via voice commands).

Version 1741/2 is to be used for the Chinese market only.

## 2.19 IPerCom Client video door phone 1060/43

The video door phone *IPerCom Client 1060/43* is a software application for Windows PCs which integrates with the IPerCom system and implements all the functions of a video door phone apartment station without the need for a dedicated hardware device.

The video door phone allows call forwarding to smartphones / tablets through the CallMe app (for Android and iOS), as well as allowing normal video door phone functions.

Once installed, the application is enabled for operation via a special hardware key.



*The IPerCom Client application and the Switchboard application must be used on 2 different PCs.*

## 2.20 Miro door phone 1160/3

The *Miro* door phone 1160/3 is a hands-free audio apartment station.

It is provided with a door opening button and four buttons for optional functions, two of which are configurable for use in the IPerCom system.

In addition to the normal door phone functions, it also allows call forwarding to a smartphone/tablet via the *CallMe* app (for Android and iOS).

## 2.21 Relay actuator 1060/84 v. 2.07

The *Relay Actuator 1060/84* is an IP device, which can be used to activate two electrical loads via double exchange relay capable of working in bistable or monostable timed mode. The activation of the relays in monostable or bistable mode occurs through events generated by *Call Module, Entry Panel, Modular Entry Panel with 1060/48, Private Call Module, Key Reader, apartment station* or locally through the inputs of the *Relay Actuator* itself.

## 2.22 Relay actuator 1060/84 v. 3.04

The activation of the relays in monostable or bistable mode occurs through events generated by call stations, key readers, and apartment stations or locally through the inputs of the *Relay Actuator*. The same inputs (properly programmed) can activate one or more outputs of several *Relay Actuators* and generate an alarm towards the *Switchboard* application.

## 2.23 Relay actuator 1060/84 v. 4.05

The *Relay Actuator* 1060/84 is an IP device, which can be used to activate two electrical loads via double exchange relay capable of working in bistable or monostable timed mode. The activation of the relays in monostable or bistable mode occurs through events generated by call stations, key readers, and apartment stations or locally through the inputs of the *Relay Actuator*. The same inputs (properly programmed) can activate one or more outputs of several *Relay Actuators* and generate an alarm towards the *Switchboard* application. The *Relay Actuator* 1060/84 with firmware version 4.05 is the only one that supports the remote relay function, remote entrance hall button and door open remote sensor.

## 2.24 Key Reader 1060/86

The *Key Reader* 1060/86 is a 1-module IP device with Sinthesi Steel mechanics used to read proximity keys. The device is equipped with a relay output to control an electric lock and with an input available for a door opener button.

The electric lock is activated by passing a valid proximity key (with MiFare Plus technology) or pressing the door opener button.

When a key is passed, the reader, in addition to opening the relevant door, can activate one or more remote relay outputs (user activation function) depending on the user who passed the key.

## 2.25 Key Reader 1060/45

The *Key Reader* 1060/45 is a 1-module IP device with Alpha mechanics used to read proximity keys. The device is equipped with a relay output to control an electric lock and with an input available for a door opener button.

The electric lock is activated by passing a valid proximity key (with MiFare Plus technology) or pressing the door opener button.

When a key is passed, the reader, in addition to opening the relevant door, can activate one or more remote relay outputs (user activation function) depending on the user who passed the key.

## 2.26 Switchboard 1060/41

The IPerCom system implements the concierge function using a PC and the specific *Switchboard* application software. It is possible to connect the door phone 1060/41 (via a USB port of the PC and the mini-jack audio connectors).



*Switchboard and IPerCom Client applications must be used on 2 different PCs.*



*For details on the operation of the Switchboard app, please refer to the relevant manual available at the site [www.urmet.com](http://www.urmet.com)*

## 2.27 IPerCom Clock Module 1060/85

The *IPerCom Clock Module 1060/85* is a device that provides date and time to an *IPerCom* system if the latter does not include devices with an internal clock (RTC).

The minimum duration of the battery is 3 years.

## 2.28 Lift Interface 1060/37

The *Lift Interface 1060/37* is used to control the lift control units in order to enable the movement to the defined floors according to the apartment called.

The interfacing to the lift control units is typically made by changing the status of one or more inputs of these control units through the 24 control relays of the interface. The device is controlled directly from the system's IperCom system; the relays drive the lift control unit in response to user actions. The lift interface allows enabling the lift to reach the desired floors according to certain system events (e.g. door opening following a call to an apartment, or entering a door opening code, or passing a key, etc.).

Operation can be in floor mode or apartment mode.

In the first mode it is possible to associate the control devices of the interface according to the apartment floor: in this case the apartments on the same floor share the same relay activation layout.

In the second mode, instead, it is possible to associate a different configuration for every single apartment (useful if several apartments are on the same floor with their own dedicated lift).

The events that activate the relays can be of 2 types:

- request for access from the outside to a certain floor or apartment (opening of an access point);
- request for access from the inside to a floor other than the one where you live.

For details on configuring the device, refer to paragraph

[Adding a Lift Interface 1060/37 on a stair](#) node and [APPENDIX A: Configuration parameters of IPerCom devices](#).

## 2.29 Gateway IPerCom-2Voice 1083/59

The *Gateway IPerCom-2Voice 1083/59* allows integrating the 2Voice system with the IPerCom system: in detail, it allows the addition of a riser column (stair) of 2Voice audio / video apartment stations to an IPerCom system.

In this way, it is possible to create systems with an IPerCom common backbone on street side and 2Voice riser columns with only 2 non-polarized wires. Each riser column (associated with a gateway) can manage a maximum of 128 apartment stations, 127 users, 2 secondary door units on 2 backbones. It is therefore possible to have several main door units (*Call Modules* and *Entry Panels*) and switchboards (IPerCom) higher than the known limits of the 2Voice system (for further details, follow instructions in the 2Voice technical manual).

For device configuration details, follow instructions in the "[Adding a Gateway IPerCom-2Voice on a stair node](#)" and in "[APPENDIX A: Configuration parameters of IPerCom devices](#)".

## 2.30 IPassan controller

The *IPassan Controller* allows integrating the IPerCom system with the IPassan access control system. Integration concerns the following aspects:

- sending to the IPassan system a door opening request (pedestrian or driveway) coming from the IPerCom system with consequent access point opening;
- allowing the IPassan system to control any lifts in the system.

The integration is done by exporting from *IPerCom Installer Tools* an xml file (which shows the topology of the system and its devices) and manually importing this file on the IPassan system (for further details see "[APPENDIX O: IPassan integration with IPerCom](#)").

## 2.31 IPerTALK Server

The *IPerTALK Server* allows integrating the iPerTALK system with the IPerCom system. This integration is useful to perform all the main video door phone functions (that is audio-video calls, gate opening and auto-on function) between the two systems.

For the details for the integration of the iPerTALK system with the IPerCom system, see "[Integration with the iPerTALK system](#)".

## 2.32 RTSP Cameras

*RTSP Cameras* are cameras that use the network protocol *Real Time Streaming Protocol* for the video streaming. The auto-on function on *RTSP Cameras* is available from all video door phones of the IPerCom system and from the *Switchboard* and *IPerCom Client* applications for video surveillance functions (in addition to auto-on on calling stations).



*The auto-on function on RTSP cameras for video door phones VOG<sup>5</sup> 1761/6 and VOG<sup>5+</sup> 1761/15-16-18-19 is available on a limited number of RTSP cameras: see the list of supported RTSP cameras in [APPENDIX W1: RTSP Cameras supported by IPerCom video door phones](#).*

*RTSP Cameras* are not “*native*” IPerCom devices but can still be integrated into an IPerCom system by paying particular attention to the assignment of the IP address. For further details, see [APPENDIX F1: How to use customized network settings in IperCom system](#).

### 2.32.1 RTSP Cameras (NVR)

The *RTSP Cameras* can also be integrated into the IPerCom system through Urmet **1098/324P-326P-328P** NVR devices if, for example, the network infrastructure requires having the *RTSP Cameras* on a different subnet from that of the IPerCom devices due to needs. For further details on integration see [APPENDIX M2: RTSP Cameras with NVR Urmet device](#).

### 3 Basic concepts

*IPerCom* is based on the following basic concepts: *topology*, *topological group* and *topological path*.

#### 3.1 Topology

The **topology** of a building (or *site*) is a simplified map that considers the various elements that make it up and their relative positioning.

Typically, the types of elements that make up a building are: blocks, stairs, floors, apartments.

An example of a topology is provided in the following figure:

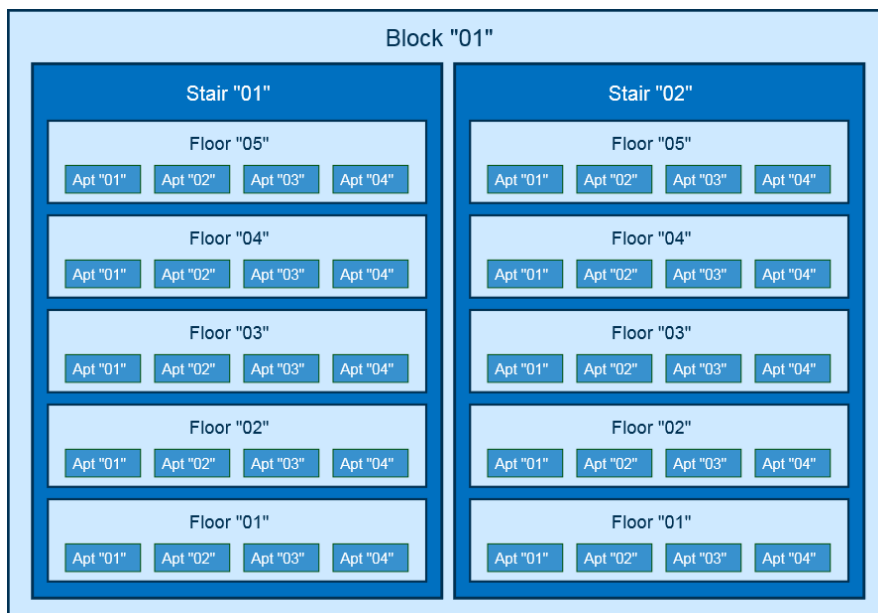


Figure 2: Example of a building topology

where there is a block containing two stairs; in stair "01" and "02" there are five floors with four apartments each: each of these elements is a **topological node** within the topology.

In *IPerCom* each topological node is assigned a two-digit alphanumeric code from "01" to "ZZ", which is automatically assigned by the system when defining the system topology.

In the example given in [Figure 2](#) we will have a block with code "01" and inside of it a stair with code "01" and one with code "02"; inside each stair we will have floors with codes "01", "02", "03", "04" and "05", whereas inside each floor we will have apartments with codes "01", "02", "03" and "04".

Since each node can be associated with two digits, to identify in the entire topology an apartment that is below a floor, a stair, a block and a site, a numeric code of 10 digits is needed. In the example of [Figure 2](#), by assigning to the base site a code equal to “01”, to the block the code “01”, to the second stair “02”, to the third floor of the stair “03” and to the second apartment of such floor “02”, the concerned apartment can be identified by the 10-digit numeric code “0101020302”.

If we decide to use always 10 digits to identify the position of all the topological nodes of the system, to identify the floor of the example above it will not be necessary to enter the numeric code of the apartment; it can be replaced by “##”: therefore, we will have the following 10-digit code “01010203##”. Similarly, the stair, the block and the site of the example will be identified respectively by the following codes: “010102#####”, “0101#####” and 01#####”.

The 10-digit code that identifies the generic topological node in the system topology is called **topological code**.

Each *IPerCom* device must be placed (installed) in a specific topological node (site, block, stair, floor, or apartment).

Apartment station (e.g. *MAX* video door phones) are normally installed in an apartment, call stations or calling stations (e.g. *Call Modules*) and *Switchboards* are generally installed on a unit or block.

### 3.2 Topological path and topological group

The **topological path** is the set of (topological) nodes which start from a certain node and arrive to the site node.

The **topological group** of a node is given by the set of nodes contained in the group itself (the node in question and all the nodes below it).

Considering the topological structure shown in the following figure, we can say that:

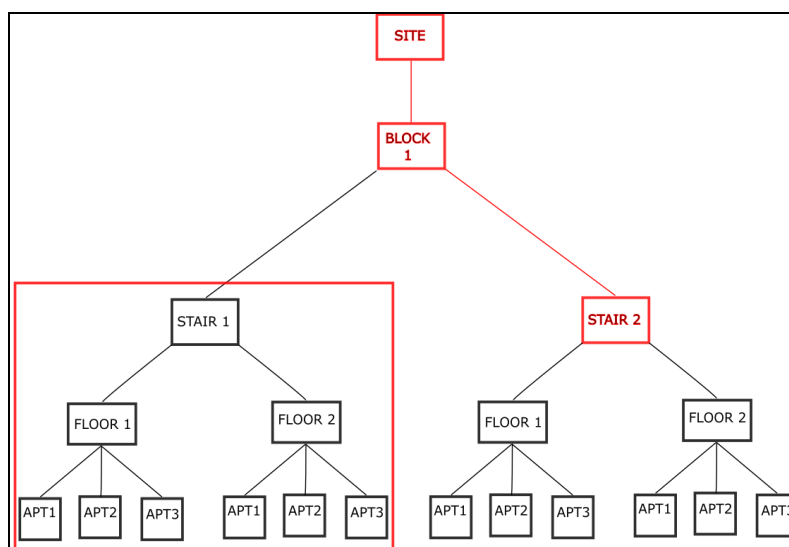


Figure 3: Example of topological path and group

- the path highlighted in red from the “Stair 2” node to the “Site” node is the topological path of the “Stair 2” node: visually speaking the topological path goes from the node considered upwards (“Stair 2 -> Block 1 -> Site”);
- the set of nodes included in the red rectangle is the **topological group** of nodes “Stair 1”: visually speaking the topological group goes from the node considered towards the bottom.

By topological group of a device is meant the node where the device is installed and all the underlying nodes.

By topological path of a device is meant the path from the node where the device is installed to the site node.

### 3.3 Applications of the concepts of topological path and topological group

The above concepts can be applied to quickly and unambiguously define the operation of the main services offered by the IPerCom system.

The following services are linked to the topological group concept:

- display of residents in the directory of outdoor stations with display (*Call Modules 1060/12-13-17-18-23, Alpha Call Modules, Outdoor Station 1060/34*),
- propagation of contacts in the address book of *MAX video door phones* and *Audio Door Phones*,
- propagation of the activation rules on the apartment stations,
- default view of the apartments on the *CallMe* app linked to the *Switchboard* application.

The following services are linked to the topological path concept:

- access of residents to the doors of the system to enter their own apartment,
- competence *Switchboards* definition,
- realisation of the camera address book for the apartment stations.

#### 3.3.1 Automatic display of residents in the address book of calling stations with display

The *calling station with display* show automatically in the address book all the residents of their own topological group. For example, a *Call Module 1060/18* placed on a stair node will automatically show in the address book all the residents (set as visible) of all apartments in its topological group, that is the topological group of stair node.

#### 3.3.2 Propagation of contacts in address book of apartment station

A (public) contact created on a node is propagated on all apartment station contained in the topological group of the node in question. For example, a contact created on a stair node will be automatically propagated in the address books of all apartment station placed within the topological group of that stair.

For all the details on how to create a contact see the dedicated paragraph “[Contacts](#)”.



### 3.3.3 Propagation of activation rules

An activation rule created on a node is propagated on all apartment station contained in the topological group of the node in question. For example, an activation rule created on a stair node will be automatically propagated on all apartment station placed within the topological group in question.

For all the details on how to create an activation rule see the dedicated paragraph “[Activations](#)”.

### 3.3.4 Default view of apartments on the *CallMe* app linked to the *Switchboard* application

The *CallMe* app linked to the *Switchboard* application automatically shows in its address book all the apartments of the topological group of the *Switchboard* application itself (competence apartments). For example, if the *Switchboard* application is placed on a stair node, the related *CallMe* app will automatically show in its address book all the apartments of the topological group of that stair (that is, the topological group of the *Switchboard* application).

### 3.3.5 Practical example of application of the topological group concept

The figure below shows an example of application of the 3 concepts above:

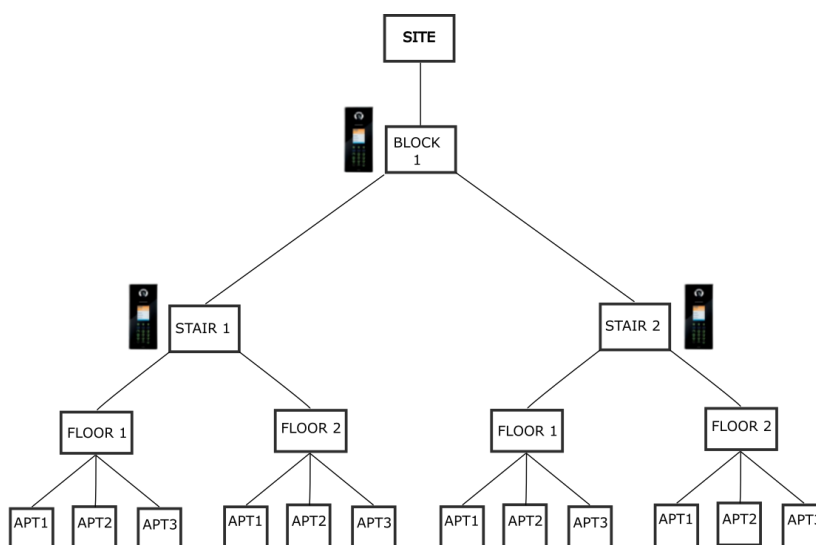


Figure 4: Example of application of topological group concept

The *Call Module* placed on node “Block 1” has in its address book all the residents of the underlying apartments, that is the 12 apartments of its topological group. The *Call Modules* placed on the nodes “Stair 1” and “Stair 2” have in their address book only the apartments of their corresponding topological groups, that is six apartments each.

The contacts and the activation rules created on the “Block 1” node will be propagated on all the underlying apartments, that is those of the topological group of the node in question.

The *CallMe* app linked to the *Switchboard* application placed on the “*Stair 1*” node has in its address book the apartments of the topological group relating to the “*Stair 1*” node.

### 3.3.6 Resident access (with key code and door code) to doors/gates of the system

Residents have automatic access by means of door codes and proximity key codes to all those entrances (pedestrian doors or driveways of Call Modules, Entry Panel and Key readers) that are placed on their topological path, that is on the topological path of their respective apartment nodes.

In this condition, apartment station can open these entrances even if you are not in conversation, that is if the entrances are not under secret.

### 3.3.7 Competence *Switchboards*

The competence switchboards for a device are those found on its topological path.

The competence *Switchboards* for apartment station in day status intercept the calls coming from calling station.

Specific buttons are present on *Call Modules, Modular Entry Panel with 1060/48* and video door phones to be able to call all the relevant switchboards at the same time.

### 3.3.8 Creation of the camera directory for the video door phone indoor stations for auto-on function

Camera address book of video door phone shows the cameras of all *calling station* and *RTSP cameras* that are on their topological path, that is on the topological path of the respective apartment nodes.

### 3.3.9 Practical example of application of the topological path concept

The figure below shows an example of application of the three concepts above:

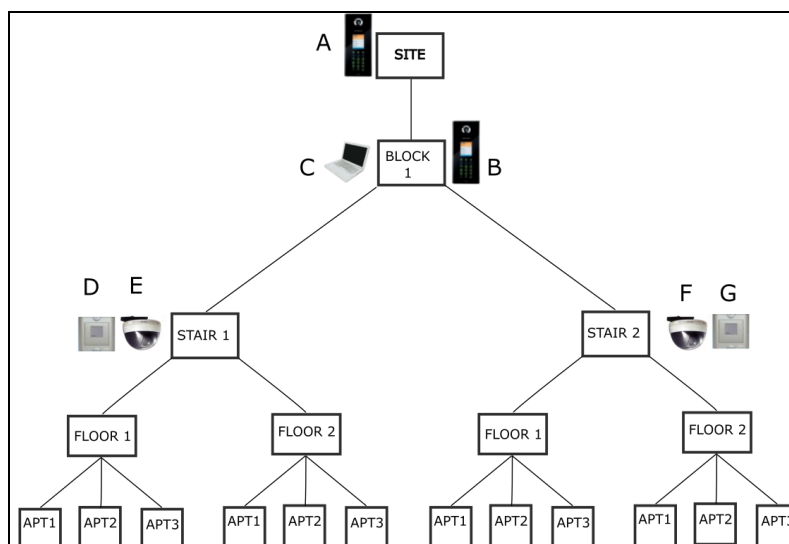


Figure 5: Example of topological path concept application

As for resident access, everyone has access to the entrances of Call Modules A and B (placed on the node "Site" and "Block 1"). Access to the Key Reader D is automatically only allowed to the residents of the left while only those on the right automatically have access to the Key Reader G. The same concept applies for what concerns the address book of the cameras for auto-insertion: all residents can see the images of the cameras A and B. The displays of the camera E are allowed to the residents of the left while only those on the right can see the images coming from the camera F.

Switchboard C is of competence for all apartment stations in apartments and for Call Module B while it is not for Call Module A, as its topological path does not intercept the only Switchboard present in the system. According to what is reported in paragraph "[Competence Switchboards](#)", this means that:

- the Call Module B has a specific button to call the competence Switchboard C;
- the video door phones in apartments have a specific button to call the competence Switchboard C;

Switchboard C (in day status) intercepts calls to video door phones made by both Call Module A and Call Module B.

### 3.3.10 Summary table

Below is a summary table of what has been written above regarding the main services offered by the IPerCom system and which concepts they are connected to (whether topological group or topological path):

<i>Topological Group</i>	<i>Topological Path</i>
Contacts in address book of <i>calling station with display</i> .	Access to resident entrances
Contact propagation in address book of MAX video door phones and Audio Door Phones	Calling stations and <i>RTSP cameras</i> that can be displayed from the video door phones (auto-on)
Activation rule propagation on the apartment station	Competence <i>Switchboards</i>

*Table 1: Services offered by the IPerCom system by group or topological path*

## 3.4 Main and secondary calling stations

The calling stations, according to the topological node where they are positioned, are divided into:

- **main**, if placed on the site or block topological node;
- **secondary**, if placed on the unit or floor topological node.

This difference is reflected in the audio settings of the apartment station, which allow assigning two different ring tones for calls coming from the two different types of calling stations.

The calling station that can be divided into main and secondary are: *Call Modules 1060/12-13-17-18-23*, *Entry panel 1060/21-33-34-71-74-75* and *Modular Entry Panel with 1060/48*.

### 3.5 Security level of an IPerCom system

To guarantee a high level of safety for an IPerCom system it is necessary to comply with what is reported below depending on the type of system model chosen during the configuration phase. The available system models are shown below:

- “Villa kit (one-household)”, for single-family installations,
- “Single Stair”, for small installations with a single stair,
- “Multiple Stairs”, for medium-sized installations with multiple stairs on a single block,
- “Multiple Blocks”, for large installations.



For further details on the 4 system models above, see the paragraph [Selecting the system topology \(model\) and the configurator structure](#).

The instructions to follow are different depending on whether you choose the “Villa kit (one-household)” model or one of the last 3 models listed, as explained below.

#### “SINGLE STAIR” OR “MULTIPLE STAIRS” OR “MULTIPLE BLOCKS” SYSTEM

For these models, the presence of the installer and building manager is required to guarantee the safety of the system. Both play a specific role using specific applications, as shown below:

- *IPerCom Installer Tools* (Windows application) for the installer ([registration on Urmet Cloud is required](#));
- *CallMe Manager* (Windows application) for the building manager ([Registration on Urmet Cloud is required](#)).



Using the IPerCom Installer Tools application to configure the system makes the possibility of creating and modifying the configuration unavailable from the VOG<sup>7</sup>, MAX or Basic video door phones.

The list of actions to be carried out by the installer and administrator is shown.

## INSTALLER

The installer, after installing the system, uses the *IPerCom Installer Tools* application to:

- create an Urmet Cloud account and authenticate on *IPerCom Installer Tools* with this account (see paragraph [6.7.1](#));
- create a new project (see paragraph [6.7.4](#));
- connect to the system (see paragraph [6.9.6](#));
- create a configuration with the related password to access the configuration itself (see paragraph [7](#));
- distribute the configuration to the system (see paragraph [6.9.6](#));
- invite the building manager via email to acquire ownership of the plant site (see paragraph [6.15.1.6.1](#)).



*The email sent by the installer to the building manager contains the links to download the CallMe Manager application and related manual and a third link to acquire ownership of the system site.*



*It is possible to connect to a system via IPerCom Installer Tools only after having accessed Urmet Cloud.*



*Access to Urmet Cloud ensures that only the authorized installer can connect to the system, that is the installer who created the project and the related configuration or a second installer authorized by the first. The transfer of ownership between one installer and another occurs via IPerCom Installer Tools.*

## BUILDING MANAGER

The building manager, after acquiring ownership of the plant site, uses the *CallMe Manager* application to:

- suspend the installer once he has finished the configuration phase and the same configuration has been applied to the system (this is useful to prevent the installer from making changes to the system without the administrator's knowledge);
- re-enable the installer (if you need to make new configuration changes) and suspend it again;
- change installer (if necessary);
- invite a new building manager to transfer ownership of the site (if necessary).



*For further information, consult the [CallMe Manager application booklet](#) in the download area relating to IPercom 3.1.0.*



*The building manager is not required to enter any administrator password by IperCom Installer Tools if the CallMe Manager application is used: even in the case of an unlocked system, in fact, no installer, other than the one authorized by the building manager, can make changes to the system.*

**Managing an IPerCom system with the IPerCom Installer Tools and CallMe Manager applications therefore guarantees a high safety standard for the "Single Stair", "Multiple Stairs" and "Multiple Blocks" system types.**

#### **"VILLA KIT (ONE-HOUSEHOLD)" SYSTEM**

In this case the configuration does not require the use of specific applications and the role of an administrator is not required. In fact, given that the system generally consists of a calling station and one or more video door phones, the configuration can be done by the installer directly from the VOG<sup>7</sup>, MAX or Basic video door phones (after entering the installer password). Once the configuration has been completed, the owner of the apartment **must always block the system** with the VOG<sup>7</sup>, MAX or Basic video door phones using an appropriate password and no one will be able to access the configuration again.



For further information, see the paragraph [Commissioning a system through MAX, VOG7 or Basic video door phones: the configuration menu.](#)

The owner can unlock the system to allow access to the installer (when it is necessary to make substantial changes to the configuration): once the installer has made changes to the system, the owner can lock it again.

Changing the installer password does not require knowing the previous one. This means that if the owner decides to change installer, the new installer can enter his own password without knowing that of the previous installer. Similarly, if the installer has more simply forgotten the password, he can enter a new one without entering the previous one.

Finally, the owner can change the installer password if necessary.

**The management of an IPerCom system of the "Villa kit (one-household)" type therefore guarantees a high safety standard if the system itself is blocked by the owner of the apartment after the installer has finished the configuration part.**

## 4 System installation

The installation of the system can be carried out independently of the system configuration.

All IPerCom devices are uniquely identified by their MAC address (physical address of the network interface connected to IPerCom, e.g. 00:1E:E0:01:02:03).

The video door phone *MAX*, *VOG<sup>7</sup>*, *Basic* and *Ipercom Client 1060/43* are equipped with QR codes which are useful for acquiring devices in one of the configuration modes (see "[Adding devices to the system using the MAX video door phone and/or the Android tablet app](#)").



Figure 6: Example of QR code of an IPerCom device

It is recommended to take note of the association between the position of the installed device and its physical MAC address.



*When the system is installed but not configured, all the devices with display show that the device is not configured.*

### 4.1 Minimum requirements for the installation of an IPerCom system

*IPerCom* can be added to **any IP network where the IGMPv2 or IGMPv3 Multicast service is enabled.**

The network must offer an available bandwidth compatible with the number of simultaneous conversations expected on the system (the maximum bandwidth during a single video call session is 2 Mb/s).

The prerequisite for IPerCom system correct operation is that **at least one device with internal clock is installed in the system.**

The *Outdoor Stations 1060/21-33-34*, the *IPerCom Clock Module*, the *Modular Entry Panel with 1060/48*, the *IPerCom-2Voice Gateway*, the *Server 1060/1* and *MAX*, *VOG<sup>7</sup>*, *VOG<sup>5</sup>*, *VOG<sup>5+</sup>*, *Basic* video door phones are devices equipped with an internal clock.

The initial setting of the date and time of the internal clock is done through *IPerCom Installer Tools* or through the *MAX*, *VOG<sup>7</sup>* or *Basic* video door phones (see paragraphs "[Date/Time](#)" or "[Date and time setting](#)" respectively).



*The life of the IPerCom Clock Module and the Server 1060/1 batteries is 3 years in the event of a long power failure. In contrast, the batteries of other devices last a few days.*



## 4.2 IP network structure

Although no knowledge of IP networks and their configuration is required for the installation of the system, it is recommended to refer to the wiring diagram shown in the following figure:

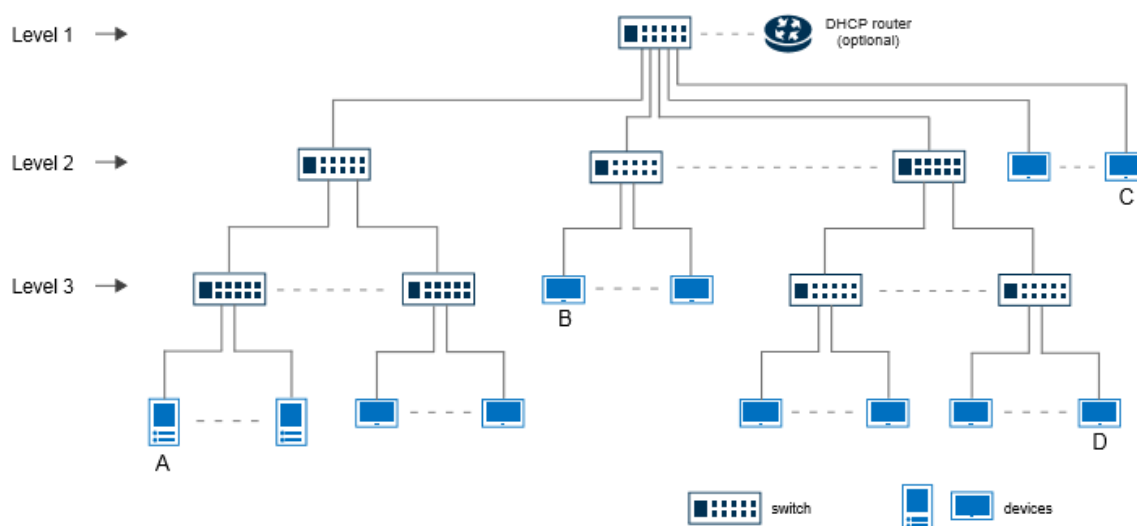


Figure 7: Recommended network topology

The shown network structure is of the “tree type”, in which the switches are arranged on different levels of the network: if you use switches with 24 POE ports, **just 3 levels are sufficient** to reach the maximum number of 1000 devices.


In large systems it is important to pay attention to the fact that the number of switches can greatly reduce the passband of the network. In this case, ask an experienced network administrator.

All IPerCom devices (except Server 1060/1, IPassan Controller and IPerTalk Server) must be connected to a PoE port on the system switches.

For a correct operation of the system, it is necessary that the network ports shown below are not blocked:

- UDP ports: 5060, 5061, 6060, 6061 (SIP protocol), 68 (BOOTP and DHCP protocols) and 69 (TFTP protocol), 1024÷65535 (RTP protocol);
- TCP ports: 5060, 5061, 6060, 6061 (SIP protocol), 13451÷13500, 18759, 27015 and 51234 (proprietary protocols);
- group UDP Multicast 238.0.0.200: port range from 55000 to 55100;
- group UDP Multicast 239.255.0.200: port range from 55000 to 55100.

 **Only one IPerCom system can be installed on the same network infrastructure.**

 *The correct operation and IT security of the TCP-IP networks on which Urmet products are installed are the full responsibility of those who manage the network infrastructure (consisting of switches, routers, firewalls, etc.) and cannot be charged either to the products or to Urmet. It is recommended to use certified personnel specialized in IT network security to properly configure the network infrastructure.*


### 4.3 Maximum distances and sections cables

To ensure correct operation of IPerCom system, the following installation prescriptions must be respected; they will be described in this chapter. However, besides this specific information, standard rules for a “good” installation must be followed, for ensuring a sufficient protection against noise and a good system reliability. All devices must be correctly installed and wired, according to national installation standards. Pay special attention to wiring operations and particularly to crimp operations of connectors on CAT5 cable, in order to ensure a correct and reliable electric connection, that is fundamental for correct operation of the system. In detail, the following must be respected:

Type of connection	Max distance	Max distance
LAN	100m (*)	CAT5e (#)

*Table 2: Maximum distance and cable cross section by type of LAN connection*

- (\*) The max. allowed distance is that defined by IEEE 802.3 standards for Fast Ethernet networks (100 Mb/s), connected with UTP CAT5 cable: according to these standards, the distance between two Ethernet devices must not be longer than 100 m.
- (#) To ensure longest-range door phone operation, the cable must be a class 5e device and the twisted pairs’ cross section must be AWG24.

 *The maximum resistance of the individual wires must not exceed 10ohm / 100m.*

*The connection between the door phone and POE switch must be ensured by a single cable without any extra patch cords.*

*The cable must be up to the following standards: EIA/TIA 568-B.2 o EIA/TIA 568-C.2, EN50288 3-1, IEC 61156-5.*

In presence of a *Gateway IPerCom-2Voice 1083/59* for the maximum distances and cable section of the 2Voice side, follow the instructions in the 2Voice technical manual, section 7 “*Gateway Ipercom-2Voice*” (available on website [www.urmet.com](http://www.urmet.com)).

## 4.4 Device/application firmware upgrade

After the installation of the system, it is necessary to **upgrade the firmware** of all devices and the software of any applications.

The upgrade files (available at [www.urmet.com](http://www.urmet.com)) allow having one of the officially released IPerCom versions on the system.

There can be 2 different upgrade modes if there is at least 1 *Server 1060/1* in the system. Otherwise, there is only one possible upgrade mode.

### SYSTEM WITHOUT SERVER 1060/1


The system is upgraded using the *IPerUpgrade* application for Windows operating systems. There is no need to configure the system before the upgrade.


The *IPerUpgrade* application and its user manual are available at [www.urmet.com](http://www.urmet.com).

### SYSTEMS WITH AT LEAST ONE SERVER 1060/1

In addition to the method described above, it is also possible to upgrade via *IPerUpgrade* only the *Server 1060/1* (disconnected from the system) which will then independently update all the other devices.

This upgrade mode is only available from IPerCom version 2.1.

 *In systems with several Servers 1060/1, all servers must be upgraded to the same firmware version using IPerUpgrade.*

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

After upgrading the *Servers* on the system (via the *IPerCom Installer Tools configurator*):


- configure all *Servers 1060/1* via the *configurator*;
- select the option "*Automatic Server Upgrade*" in the *configurator*.


At this point, after connecting the *1060/1 Servers* to the system, one of these will autonomously update the other system devices.

In "[APPENDIX Q: First upgrade of a system via Server 1060/1](#)" are described in detail.

The advantages of this mode of operation are shown below:

- if a new device is added to the system, it is automatically upgraded by the *Server 1060/1*;
- if it is necessary to upgrade the entire system to a version later than 2.1.2, it is sufficient to upgrade only the *Server 1060/1* (via *IPerUpgrade*), which will then upgrade all the other devices.

 In both above cases, the Switchboard and IPerCom Client applications, assuming they are each running on different PCs, are automatically upgraded (by IPerUpgrade or by Server 1060/1). From version 3.1 the update of the IPerCom Client application is performed correctly even if you do not have administrator rights on the PC.

 In both the above-mentioned cases the firmware of the following devices does not require an upgrade: Relay Actuators, Key Readers, Lift Interface, iPassan Controller, IPerTalk Server and RTSP Cameras.

It is essential that all devices and/or applications (IPerCom Installer Tools and Switchboard) are aligned to the same IPerCom version, otherwise the proper system operation is not guaranteed.


The possible presence of a misalignment between the IPerCom versions of the devices and/or applications is signalled by the IPerCom system via:

- IPerCom Installer Tools application,
- video door phone,
- iPerCom Client application,
- Switchboard application.

The check is not actually done on the IPerCom version but on the software development platform version (UPTK) incorporated into the same IPerCom version: in general, the presence of different UPTK versions implies the presence of devices/applications with different IPerCom versions in the same system.

In all the three cases mentioned above a list of software devices/applications whose UPTK version is not aligned with the local UPTK version of the device/application that reported the misalignment is shown.

The mode in which this is reported is explained in detail in the dedicated paragraphs [\(Devices not aligned to the same IPerCom or software development platform \(UPTK\) version\)](#) and [\(Devices not aligned to the same IPerCom version or UPTK software development platform\)](#) in the sections relating respectively to IPerCom Installer Tools and to the video door phones of the IPerCom system. As regards the IPerCom Client and Switchboard applications, please refer to the relevant manual available on the website [www.urmet.com](http://www.urmet.com).

 If there are no video door phones in the system, the IPerCom Installer Tools or Switchboard or IPerCom Client application must be used to detect the presence of devices and/or applications with misaligned IPerCom versions.

## 5 System commissioning

The **commissioning of a system** essentially involves:

- setting the date and time;
- the creation of the **project**, which also includes **configuration**;
- the application (distribution) of the **configuration** to the system;
- securing the system.

To commission a system, the installer can use:

- the *IPerCom Installer Tools* application for Windows,
- the configuration menu on the *MAX*, *VOG<sup>7</sup>* and *Basic*.

We recommend using the *IPerCom Installer Tools* application, whose new features will be explained in detail in the paragraph [Commissioning a system through IPerCom Installer Tools](#).



*For IPerCom systems in IPerCloud mode it is mandatory to use the IPerCom Installer Tools application.*

The date and time setting on *IPerCom Installer Tools* and *MAX video door phone* is carried out in different ways. In both cases it is essential to set the correct date and time on the system to avoid malfunctions related to the configuration distribution. In this way the devices in the system equipped with internal clock have the date and time set correctly and can distribute it to the rest of the system.

The creation (or change) of the configuration on *IPerCom Installer Tools*, *MAX*, *VOG<sup>7</sup>* or *Basic* video door phones is done by calling the *IPerCom Configurator* application (or more simply *configurator*).

The creation (or the change) of configuration can only be done by one user at a time and the system prevents two open configuration sessions on the same system (on *IPerCom Installer Tools* and on a *MAX*, *VOG<sup>7</sup>* or *Basic* video door phone).

*MAX*, *VOG<sup>7</sup>* or *Basic* video door phones, via the *configurator*, allow to create and saving the configuration (file with *ccf* extension) within the *project*. The configuration is then distributed to the various devices in the system. The configuration files can be imported to the *configurator* (or exported from the *configurator*) using a micro-SD card.

*IPerCom Installer Tools*, via the *configurator*, allows saving the configuration associating it to a *project*. The configuration is then transferred to the various devices in the system. *IPerCom Installer Tools* too allows importing a configuration file (with *ccf* extension) from PC and associating it to a project previously created. A generic project can be exported to PC and imported to other PCs. These concepts will be explained in detail in paragraph [Commissioning a system through IPerCom Installer Tools](#).

The *configurator* is also available on Android tablets through the *IPerCom Configurator* app, to provide the installer with all the flexibility possible in the creation/change of system projects only.

The securing of a system on *IPerCom Installer Tools* and *MAX*, *VOG<sup>7</sup>* or *Basic* video door phone is done in different ways.

This manual describes how to commission the system from both the *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* and the *IPerCom Installer Tools* and describes also how to create the configuration using the tablet application.



*In IPerCom systems with Door phone 1160/3 only, IPerCom Installer Tools must be used for configuring the system if you do not want to use a MAX, VOG<sup>7</sup> or Basic video door phone as a configuration tool.*



*The IPerCom Installer Tools application is available from version 1.1.0 of IPerCom.*

## 6 Commissioning a system through IPerCom Installer Tools

### 6.1 Introduction to IPercom Installer Tools

The *IPerCom Installer Tools* application can be downloaded from [www.urmet.com](http://www.urmet.com) in the download area (*Software -> Technical software -> Communication -> IPerCom system*). To access the software, download area, registration to the website is required.

Hardware and software minimum requirements for installation are the following:

- Windows 7, 8, 10, 11 operating system with quad core CPU and frequency greater than 2GHz;
- SSD disk with 512GB or higher capacity (no hard disk);
- 8GB or higher RAM memory;
- 10/100/1000 Mbit/s network card.

For each officially released version of IPerCom (starting from version 1.1.0) there is the corresponding version of *IPerCom Installer Tools*, as the versions of a system and *IPerCom Installer Tools* must always be aligned.

The application allows the commissioning of an IPerCom system and at the same time features a set of additional functions which make it an indispensable tool for system configuration and maintenance. All these functions will be explained in detail later in this manual: in this introductory chapter it is sufficient to underline that in *IPerCom Installer Tools* the system you want to configure (by system meaning the entire network, devices and IPerCom software applications) is called a **site**.

It is possible to **assign a name to the site** (via the configurator of *IPerCom Installer Tools*). 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 *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.



The 3 points above are illustrated in detail in [APPENDIX N: "Site name" and "Global site ID" field definition](#).

On *IPerCom Installer Tools* in the "Site" tab, it is possible to check the alignment status between the configuration relating to a project and the configuration present on the site (plant), highlighting the following possible situations:

- site configuration aligned with that present in the project (same date and time);
- site configuration older than that present in the project;
- site configuration newer than the one present in the project.

The *IPerCom Installer Tools* application represents a significant evolution of the previous versions 1.1.0, 1.2.0, 1.3.0 and 1.4.0. The manuals of these versions can be downloaded from the website [www.urmet.com](http://www.urmet.com) in the relevant sections of IPerCom. This manual will only describe the operation of version 3.0.0 with all its functions, new and inherited from previous.

## 6.2 IPerCom Installer Tools: functions

All the main functions of the *IPerCom Installer Tools* application are described below:

- automatically update to the latest version available (if there is an Internet connection);
- detect the version of IPerCom installed on a system;
- select which version of IPerCom you want to work with when starting the application and then automatically start the compatible version of *IPerCom Installer Tools*;
- create a **project** to be associated with a system (**site**);
- save and edit a project;
- import a project from PC and export a project to PC;
- set the time of an IPerCom system or retrieve its time;
- distribute the configuration associated with a project to the system;
- lock or unlock an IPerCom system;
- view the system diagnostics, that is view if all the devices are aligned with the same version of IPerCom, if they are correctly connected to the system and if the configuration is aligned across the entire system;
- view the event history, for example list of calls, access to gates, alarms (this function is only available if there is at least one 1060/1 *Server* in the system);
- carry out a backup of the system configuration directly on your PC or in automatic mode on a USB stick connected to the 1060/1 *Server* (the performance of the backup on the PC is in any case linked to the presence of a 1060/1 *Server* in the system);
- import a project to a higher IPerCom version (import is possible for projects created starting from IPerCom 2.0.0);



- connect to Urmet Cloud (after registering) to:
  - save projects on Urmet Cloud so as not to lose them (for example if the data on your PC is no longer available);
  - transfer the configuration of a project with IPerCloud apartments to a system;
  - use the *CallMe Manager* application to configure call forwarding;
  - modify the configuration of a system even remotely;
  - transfer a project to another installer/administrator;
  - pre-activate the licenses for IPerCloud mode;
  - view the history of pre-activated licenses;
  - run the test mode for IPerCloud mode.

All these features will be described in detail in the following paragraphs.

### 6.3 Automatic update to the latest available version

At the first start, the application checks if there is a more up-to-date version than the one installed, as shown below:

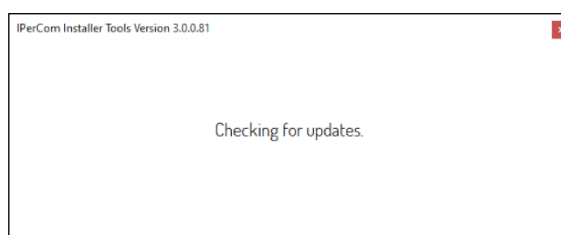


Figure 8: upgrade presence check

If the PC is connected to the Internet and the application is not updated to the latest available version, a message like the one below is displayed:

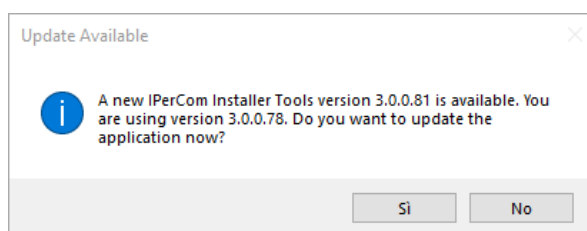


Figure 9: upgrade available

Press the “Yes” button to start downloading the new version:

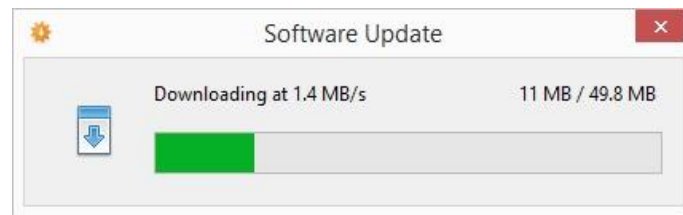



Figure 10: upgrade download in progress

As soon as the upgrade is finished, the installation starts.

 *Upgrades can be optional or mandatory: in this case if the upgrade is not performed, it is impossible to start the application.*

If there is no Internet connection, the application displays the following screen:

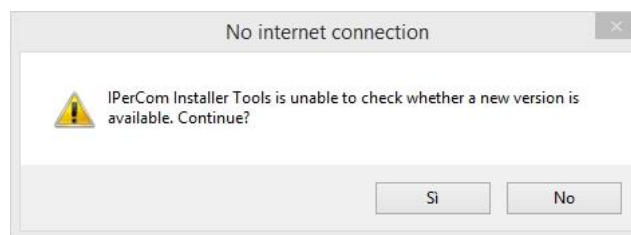


Figure 11: no Internet connection

Press "Yes" to start the application without upgrading it, otherwise, press "No" to close the application.

If you are not able to check the availability of upgrades for a period longer than 6 months, the application will not start, except with an available (if not with an available Internet connection). In this case a window like the one below is displayed:

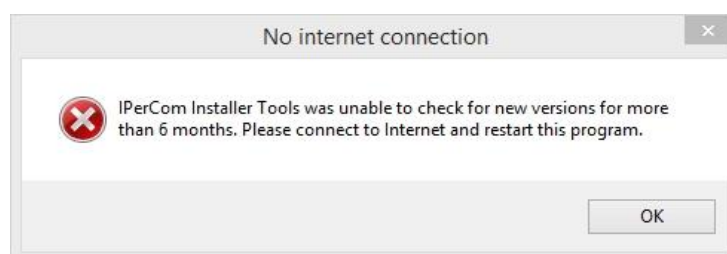


Figure 12: failure to check for updates for more than 6 months

## 6.4 Starting the Launcher

Once the search for a more up-to-date version and the possible upgrade step have been completed, the following "launcher" is displayed:

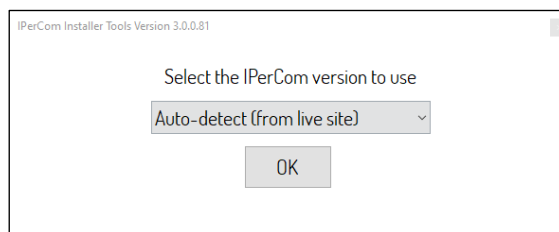


Figure 13: launcher di IPerCom Installer Tools

Depending on the selected item, the drop-down menu of the above screen allows you to:

- detect which version of IPerCom is installed on a system (if the PC on which the *IPerCom Installer Tools* application is installed is connected to the system);
- directly select an IPerCom version (among those officially released) with which you want to work.

Depending on the detected or selected version, it is possible to launch (through the same screen shown above) the corresponding version of *IPerCom Installer Tools* so that the configuration file of a project distributed to the system site is compatible with the IPerCom version installed on the system. In this way it is possible to choose from a single application which version you want to work with (thus avoiding having different versions of the same application installed on the same PC).

The 2 operating modes are now described in more detail.

## 6.5 Automatic detection of the IPerCom version

To detect the IPerCom version of a system to which the PC is connected, it is possible to use the "Auto-detect (from live site)" item:

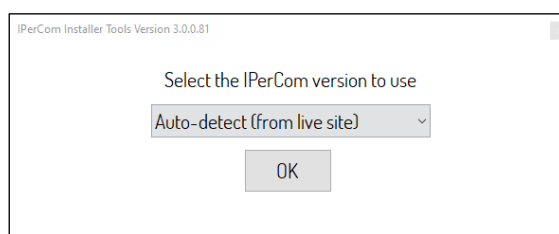


Figure 14: detect the IPerCom version from the site

Press "OK" to select the network interface through which the PC is connected to the IPerCom system, as shown in the following screen:

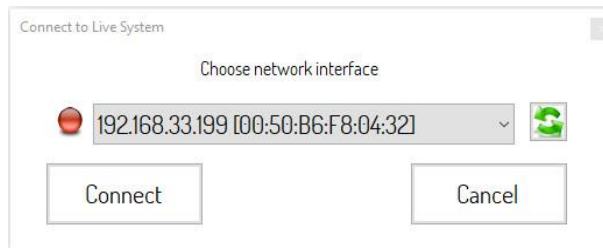






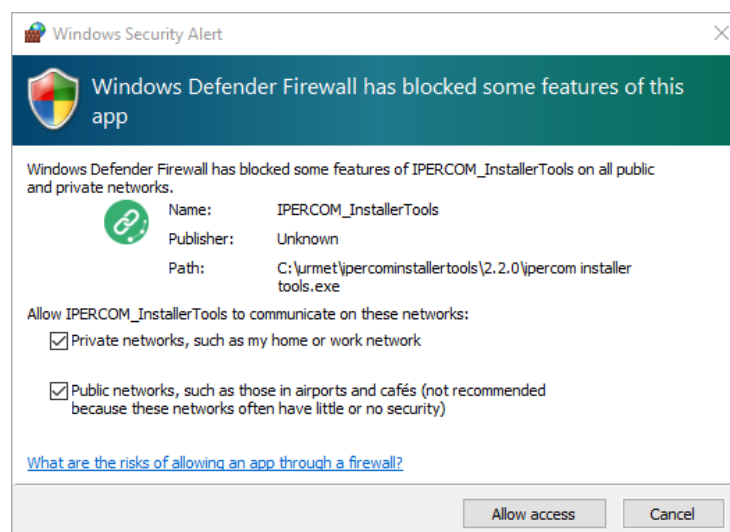
Figure 15: selecting the network interface

The  button allows updating the list of available network interfaces.

 To know the IP and MAC addresses 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 the left mouse button on the network item in question, to display a screen with the "Details" button, where the IP address and MAC address are shown.

After selecting the correct network interface, the "Connect" button detects the IPerCom devices connected to it with their firmware version (after checking if the system is with or without server).

 After pressing the "Connect" button, the Windows operating system can notify the user of the need to unlock the communication ports on the IP network used for communication between the IPerCom system and the IPerCom Installer Tools application. This operation is required for proper application operation. If this operation is carried out by Windows Firewall, a warning like the one below is shown to the user:



You must select both kind of networks and press the "Allow access" button.

Depending on the firmware version detected on the various devices, 2 different cases can occur:

- the system **is updated** to one of the officially released versions;
- the system **is not updated** to one of the officially released versions.

### 6.5.1 System upgraded to the last version

If the version installed on the system coincides with the latest released version (that is 3.0.0 version), you will see a screen of this type, where in bold (red box) the IPerCom version detected is shown:

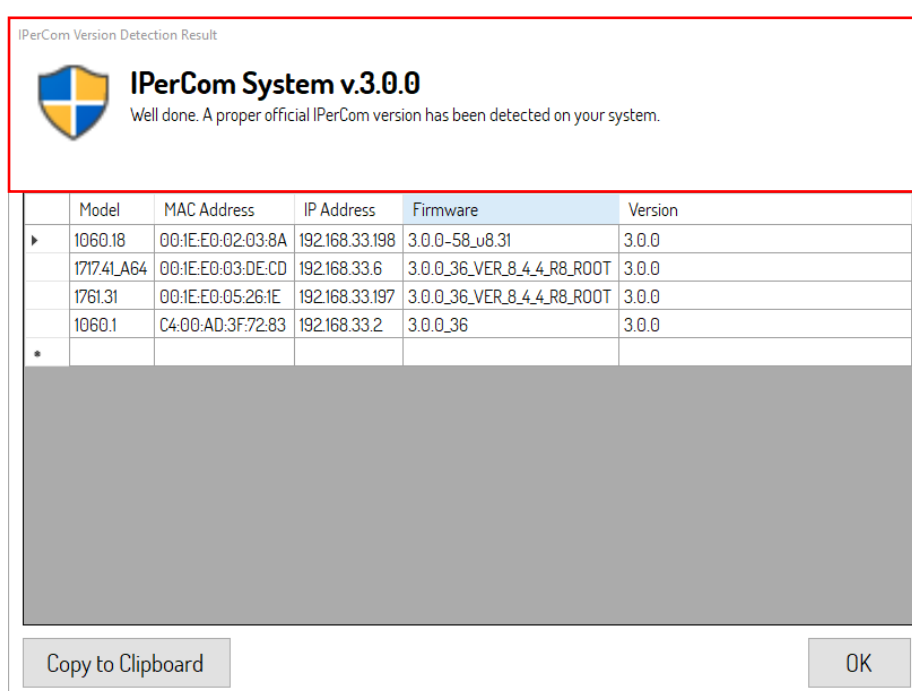


Figure 16: system aligned to latest released version 3.0.0

The following information about the devices on the system is shown in this order:

- the model (whether apartment station, calling station or other);
- the MAC address;
- the IP address;
- the internal firmware version;
- the IPerCom version corresponding to the internal firmware version.

The "Copy to Clipboard" button allows copying the table displayed above to a text or Excel file.

If the firmware versions of the various devices all coincide with those of an officially released version ("3.0.0" in this case), the system is aligned with an officially released IPerCom version. When the "OK" button is pressed, the following screen is displayed:

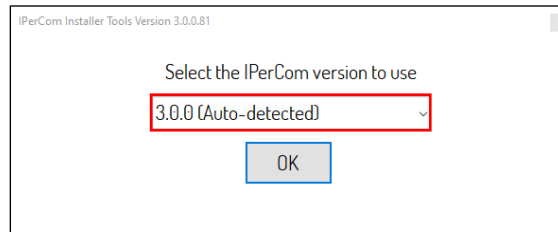


Figure 17: auto-detected version 3.0.0

This means that a version 3.0.0 of IPerCom has been detected (referred to the above example) and therefore the version of *IPerCom Installer Tools* to use is 3.0.0 version; if the "OK" button is pressed, the corresponding version of *IPerCom Installer Tools* is launched:

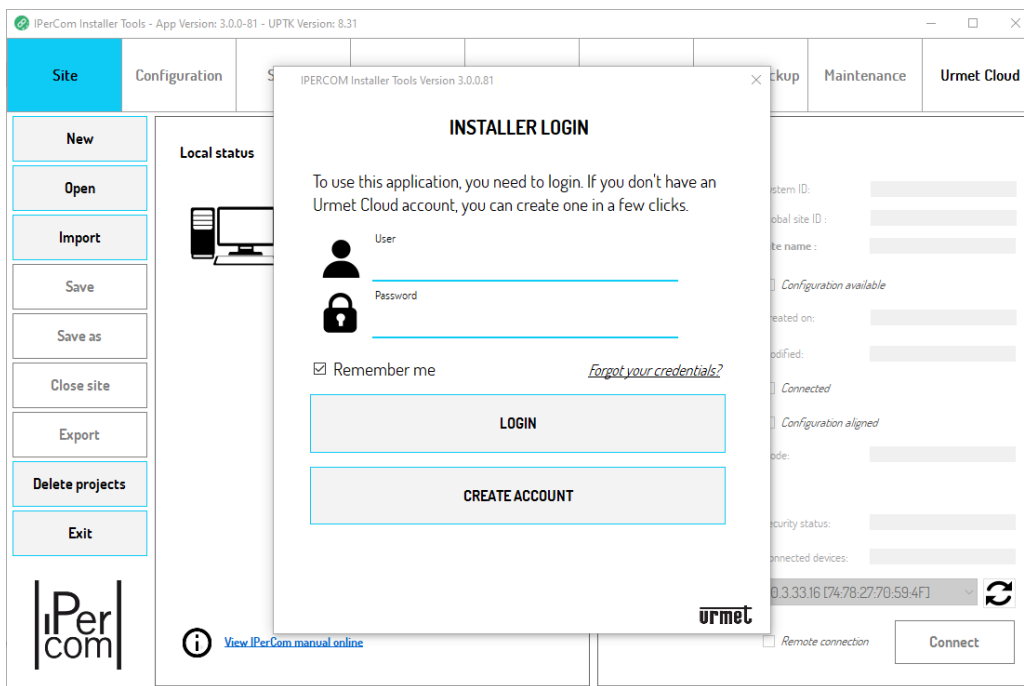


Figure 18: start screen page of IPerCom Installer Tools version 3.0.0

The operation of this user interface will be explained in detail in paragraph "[First run of IPerCom Installer Tools](#)".

### 6.5.2 System not upgraded to the last released version

If the version installed on the system does not coincide with the latest released version, a screen of this type is displayed:

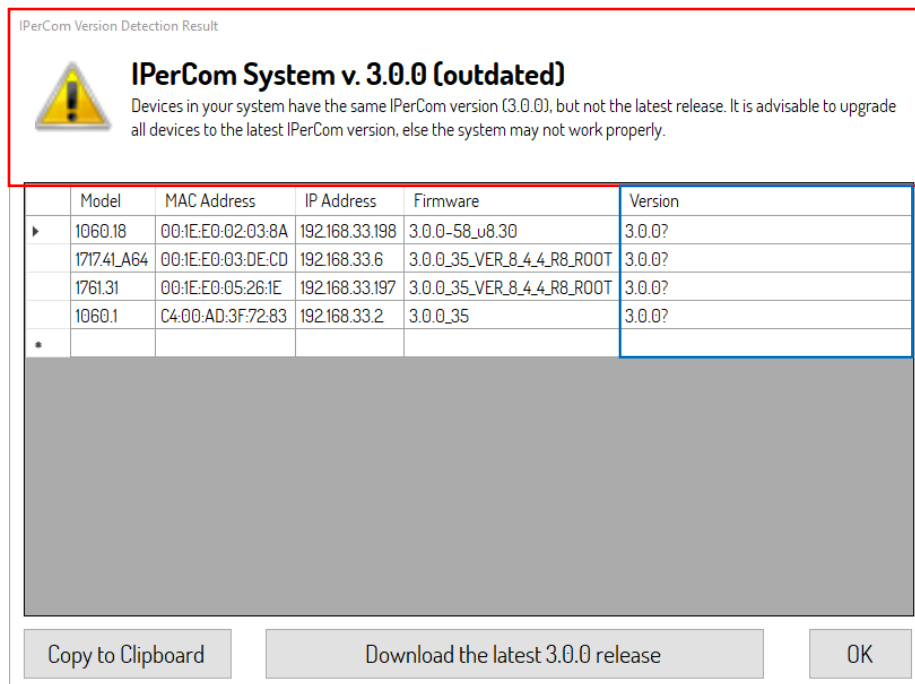


Figure 19: system not aligned to the latest version 3.0.0

The red box shows that an IPerCom 3.0.0 version has been detected on the system, but it is not the latest released one.

The information shown is the same as for a system upgraded to the latest version. However, it should be noted (blue box) that the data in the "Version" column do not coincide with the data "3.0.0": in fact, it is shown "3.0.0?" for the devices whose firmware is not aligned with the latest version.

In this case **it is recommended to upgrade** the system to the latest version: the "Download the latest 3.0.0 release" button allows downloading the latest upgrade and installing it through the *IPerUpgrade* application (downloadable from the website [www.urmet.com](http://www.urmet.com)).

After upgrading the system, it is possible to repeat the procedure described in paragraph [Automatic detection of the IPerCom version](#) and check that the latest version 3.0.0 of IPerCom is detected. Now it is possible to launch the corresponding version 3.0.0 of *IPerCom Installer Tools*.

**For version 3.1.0 of IPerCom there will be two update files: the installer will be able to choose whether to download the update file with the YnO application for the MAX and VOG<sup>7</sup> video door phones or the one with the YnO UP application for the same video door phones. The YnO application is compatible with Yokis V5 devices while the YnO UP application is compatible with Yokis V6 devices.**

In the figure above, the "Copy to Clipboard" button allows copying the displayed table to a text or Excel file whereas the "OK" button simply returns to the initial screen (in case the system is not upgraded to the latest version):

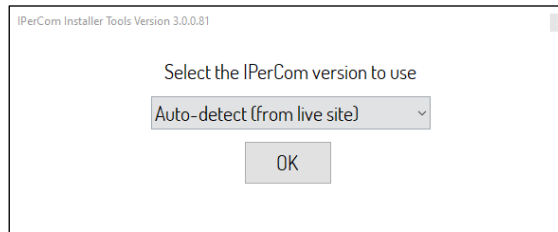


Figure 20: IPerCom Installer Tools launcher



In reference to a generic released IPerCom version, If the detected version does not correspond to the latest one, it is always possible to update the system to the latest release. For example, if a system has an obsolete version 1.2.0, it is possible to upgrade it to the latest version 1.2.0. If the detected version is the latest version 1.2.0 (for example), no upgrade is required.

### 6.5.3 Mixed system

If in the system devices are upgraded to different versions among those released, a screen of this type is displayed:

IPerCom Version Detection Result

**Mixed IPerCom System**

Your system has devices with multiple Ipercom versions: [2.2.0?,3.0.0?].  
It is advisable to upgrade all devices to the same firmware version.

	Model	MAC Address	IP Address	Firmware	Version
▶	1160.3-1139.3	00:1E:E0:01:D3:B5	192.168.33.5	ipercom-2.2.0-18	2.2.0?
	1060.18	00:1E:E0:02:03:8A	192.168.33.198	3.0.0-58_u8.31	3.0.0?
	1717.41_A64	00:1E:E0:03:DE:CD	192.168.33.6	3.0.0_36_VER_8.4.4_R8_ROOT	3.0.0?
	1761.31	00:1E:E0:05:26:1E	192.168.33.197	3.0.0_36_VER_8.4.4_R8_ROOT	3.0.0?
	1060.1	C4:00:AD:3F:72:83	192.168.33.2	3.0.0_36	3.0.0?
*					

Copy to Clipboard
Download the latest 3.0.0 release
OK

Figure 21: system with devices upgraded to different IPerCom versions



The information shown is always the same as in the previous screen: you can immediately see that the "Version" column indicates the presence of devices not upgraded to the latest version 2.2.0 ("2.2.0?") and devices not upgraded to the latest version 3.0.0 ("3.0.0?").

In this case, **it is necessary to upgrade** the system to the latest released version: the "Download the latest 3.0.0 release" button allows downloading the most recently released upgrade (in this case the one related to version 3.0.0) and installing it through the *IPerUpgrade* application (downloadable from the website [www.urmet.com](http://www.urmet.com)).

After upgrading the system, it is possible to repeat the procedure described in paragraph "[Automatic detection of the IPerCom version](#)" and check that latest version 3.0.0 of IPerCom is detected. Now it is possible to launch the corresponding version 3.0.0 of *IPerCom Installer Tools*.

The "Copy to Clipboard" and "OK" buttons have the same functions as described in the previous paragraph.

## 6.6 Launch a certain version of *IPerCom Installer Tools*

If you already know which version of IPerCom you want to work with (that is if you already know which version of IPerCom is installed on a system), simply select one of the versions already released from the drop-down menu:

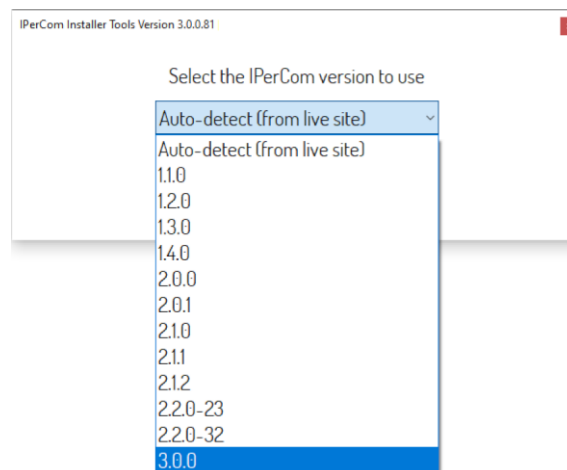


Figure 22: selecting the iPerCom version

If you choose the latest officially released version, after pressing the "OK" button, the corresponding *IPerCom Installer Tools* application is launched.

Otherwise, the other applications are downloaded from the Internet and subsequently installed. For example, if you choose to work with IPerCom version 2.0.0, after pressing the "OK" button, the following screen will appear:

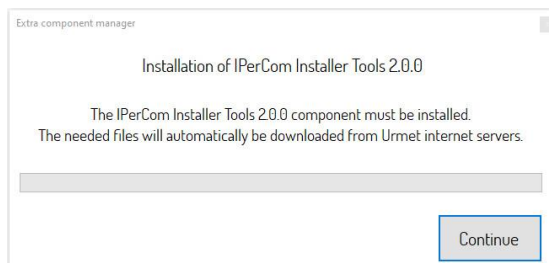


Figure 23: request to install version 2.0.0 of IPerCom Installer Tools

By pressing the "Continue" button, the download of the *IPerCom Installer Tools* version 2.0.0 application starts.

When the download ends, the following windows appears:

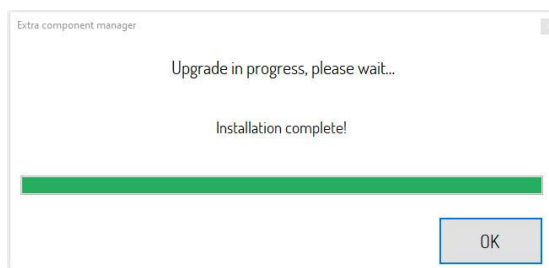





Figure 24: Version 2.0.0 of IPerCom Installer Tools installed

By pressing the "OK" button, the 2.0.0 version of *IPerCom Installer Tools* is started.

-  *If a version of IPerCom Installer Tools 1.1.0 or 1.2.0 or 1.3.0 or 1.4.0 has already been installed on your PC, by updating the application to version 3.0.0, what written above is no longer valid if the version of IPerCom selected is the one previously installed.*
-  *If a version of IPerCom Installer Tools 2.0.0 or 2.0.1 or 2.1.0 has already been installed on your PC by updating the application to version 3.0.0, what written above is no longer valid for any selected IPercom version.*
-  *After downloading and installing a specific version of IPerCom Installer Tools, if this is updated online, the next time you start up you are prompted to update the version in question.*

The next paragraph describes the operation of the user interface corresponding to version 3.1.0.

## 6.7 First run of IPerCom Installer Tools

If the detected IPerCom version is 3.1.0 or you want to work with an IPerCom 3.1.0 version, the situation below occurs:

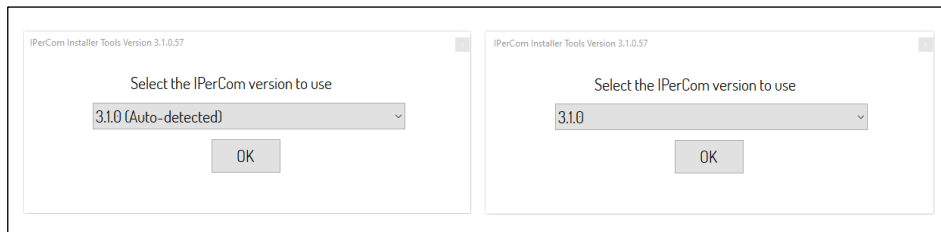


Figure 25: auto-detected or directly selected 3.1.0 IPerCom version

In both cases, press the "OK" button to display the following screen:

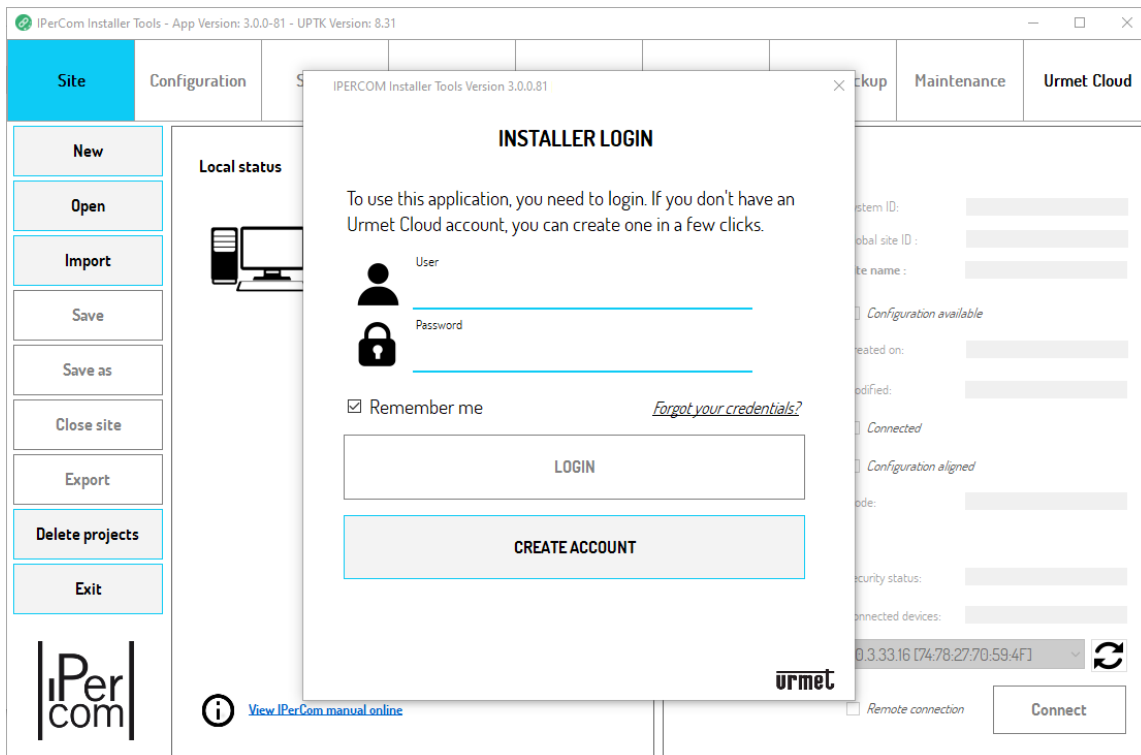




Figure 26: start screen page of IPerCom Installer Tools

The first thing the installer is asked to do is to authenticate to Urmet Cloud, creating the relevant account (if it has never been created previously).



The icon  indicates that authentication will take place on the European Urmnet cloud; if you press the mouse once on the icon in question, it turns into , indicating that the authentication will take place on the Chinese Urmnet cloud. At the first start IPerCom Installer Tools automatically shows one or the other icon based on the first response received following a ping to the European and Chinese Urmnet cloud. The setting in question is however memorized and maintained at subsequent program starts.

Urmnet Cloud authentication is useful as it allows you to:

- save projects on Urmnet Cloud so that you always have them available (even if, for example, the data on your PC is no longer available);
- transfer the configuration of a project with IPerCloud apartments to a site (system);
- use the *CallMe Manager* application to configure call forwarding function;
- modify the configuration of a system even remotely;
- transfer a project to another installer/administrator;
- pre-activate the licenses for IPerCloud mode;
- view the history of pre-activated licenses;
- run the test mode for IPerCloud mode.



***Urmnet Cloud authentication is not mandatory but it is recommended to take advantage of the above services.***

Below is a description of what to do to authenticate or not authenticate to Urmnet Cloud.

### 6.7.1 Urmet Cloud authentication

Creating an account is done by pressing the “Create Account” button.

The following window opens where it is necessary to fill in the fields marked with an asterisk:

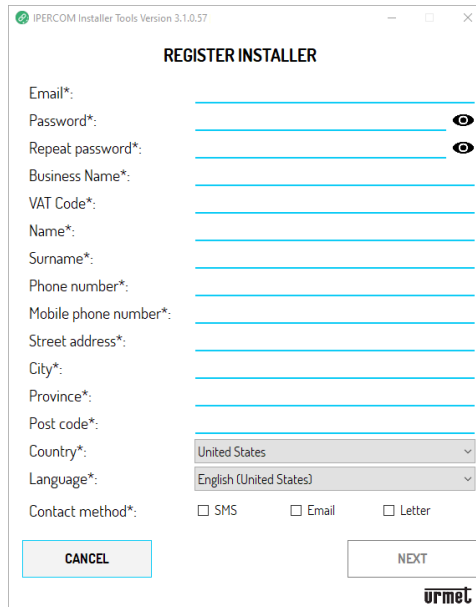


Figure 27: new account registration window

After filling in all the fields correctly, the “Next” button is enabled and, after pressing it, the following screen appears:

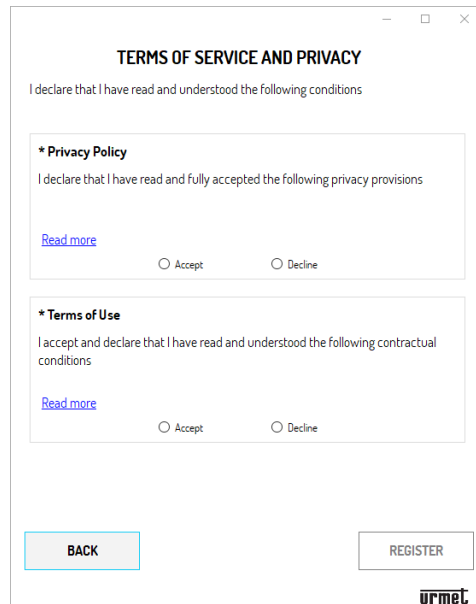


Figure 28: terms of service and privacy

At this point, after accepting the general conditions of use and the privacy policy, you can press the “Register” button to complete the registration, as confirmed by the following dialog box:

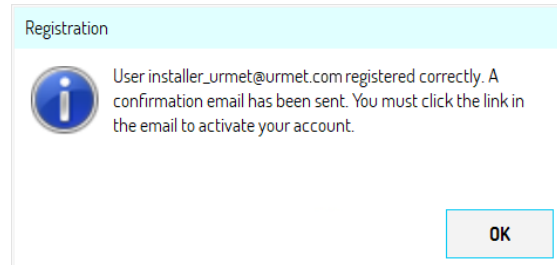


Figure 29: registration successful

The last step to do is to go to your email inbox and click on the account activation link. You are then transferred to a web page which confirms that activation was successful:

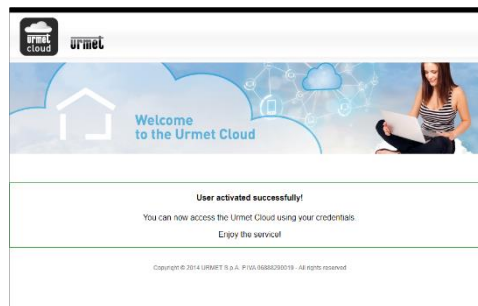


Figure 30: account activated successfully

Once the account has been activated, access to Urmet Cloud occurs by entering the username and password in the authentication window (red box):

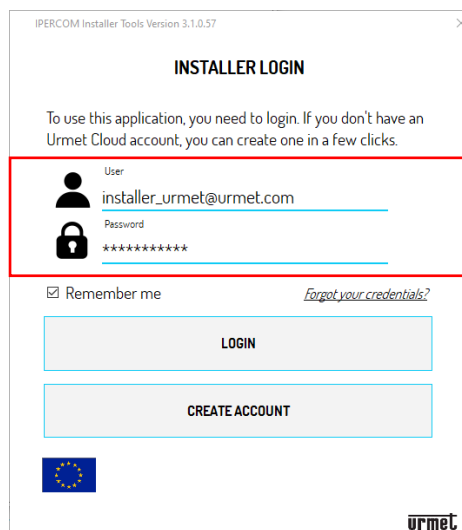


Figure 31: login window

The "User" field must be filled in with the e-mail address entered during registration, just as the password is the one entered during registration.

At this point, simply press the **"LOGIN"** button to authenticate on Urmet Cloud.

Correct access is indicated by the following pop-up window:

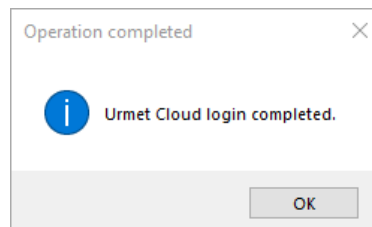


Figure 32: correct access to Urmet Cloud

In [Figure 31](#) if you select the **"Remember me"** field, the next time you log in to Urmet Cloud, you will no longer be asked to enter your username and password as they are automatically pre-loaded by *IPerCom Installer Tools*.

If you have forgotten your password, you can set it again pressing **"Forgot your credentials?"** (still in [Figure 31](#)). The window that appears is the following:

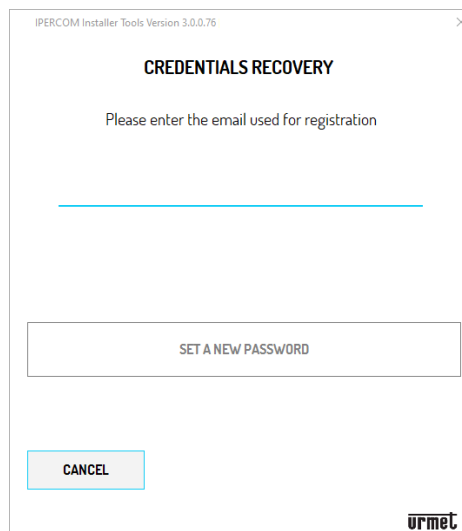


Figure 33: credentials recovery

After entering your registration email address, simply press the **"Set a new password"** button. An email is sent to the address entered through which you can set a new password.

After logging in, the screen that appears is the following:

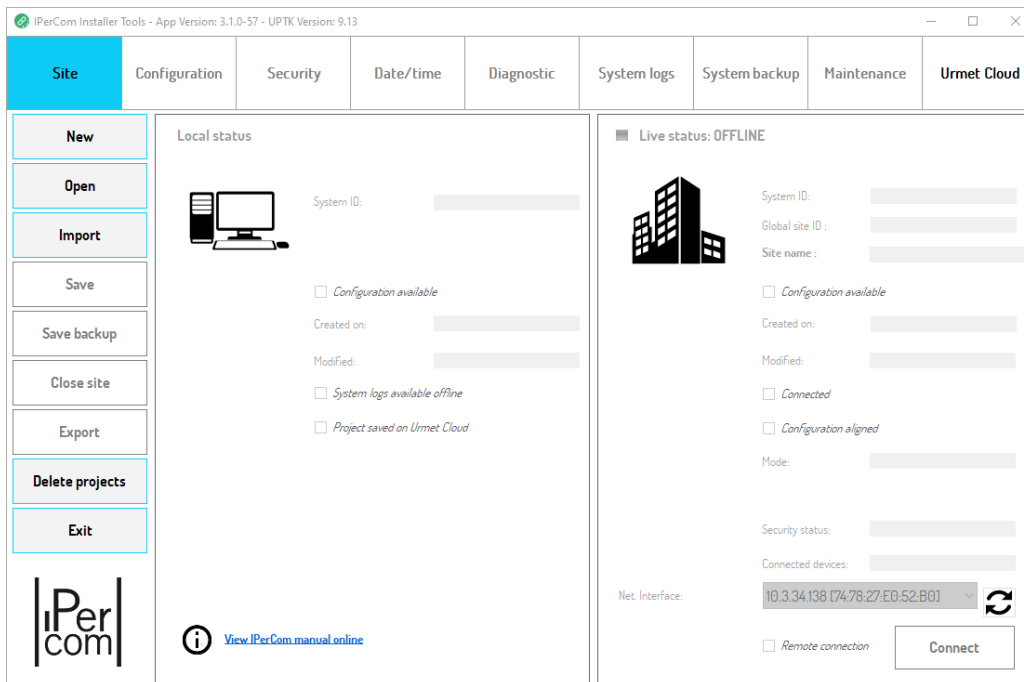


Figure 34: IPerCom Installer Tools screen after cloud authentication



Pressing the "Urmet Cloud" tab displays the screen shown below:

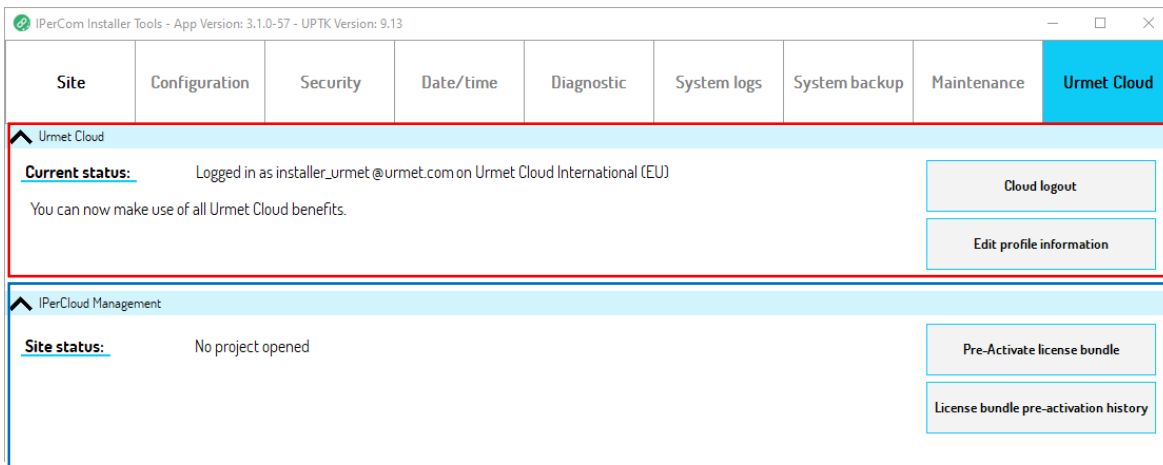


Figure 35: screen of the Urmet Cloud tab after cloud authentication

The **Urmet Cloud** section (red box) presents the "Cloud logout" and "Edit profile information" buttons, which respectively allow you to exit Urmet Cloud and modify the data entered when creating the account.

The **IPerCloud Management** section instead concerns more directly the configuration of the IPerCloud mode and is explained in detail in the next paragraph.

#### 6.7.1.1 Pre-activation license bundle and pre-activation license bundle history

The **IPerCloud Management** section (blue box) presents the buttons "Pre-Activate license bundle" and "License bundle pre-activation history": both functions are useful for configuring an IPerCom system in IPerCloud mode.

Pressing the "Pre-activate license bundle" button, the following screen opens:

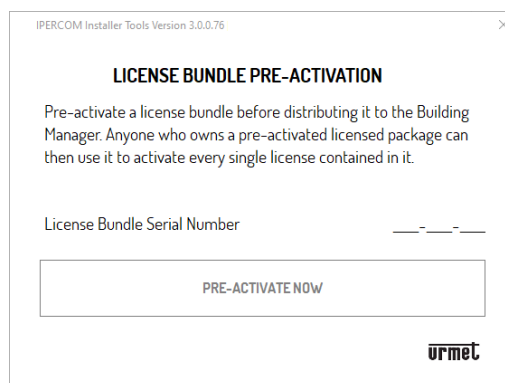


Figure 36: license bundle pre-activation

In the "License bundle serial number" field it is necessary to enter the serial number of the license bundle for pre-activation by the installer. The number is shown on the license card with the abbreviation "S/N" as shown in the following example figure:



Figure 37: serial number of license bundle

After entering the serial number and pressing the "PRE-ACTIVATE NOW" button, the following window is shown, through which the installer can accept (or reject) the license agreement relating to the IPerCloud software (End User License Agreement):

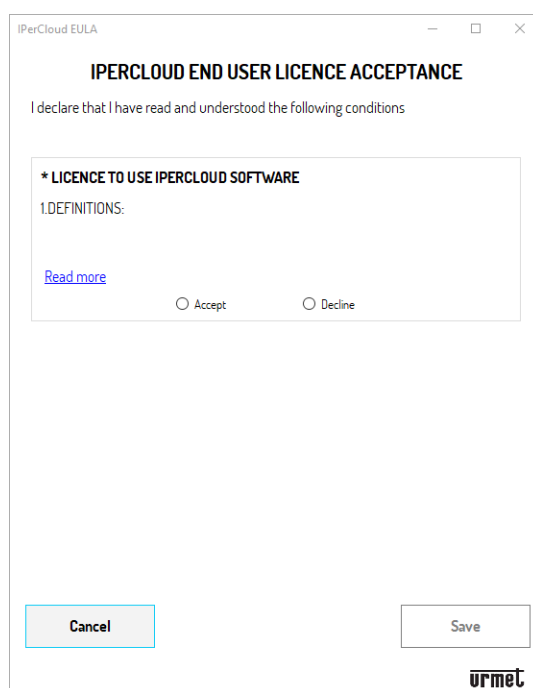


Figure 38: viewing of the IPerCloud user license agreement

It is required to select the "Accept" item and then press the "Save" button to proceed with the procedure of license bundle pre-activation. Once this is done, the positive outcome of the pre-activation is confirmed by the following message:

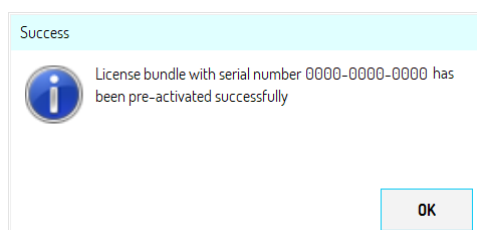


Figure 39: license bundle pre-activation

If a license bundle has already been pre-activated, this is indicated by the following message:

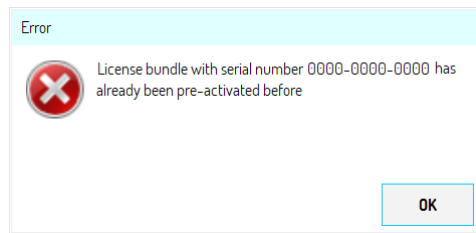


Figure 40: license bundle already pre-activated

The "License bundle pre-activation history" button allows you to view all the license bundles already pre-activated with pre-activation date and time and serial number, as shown below:

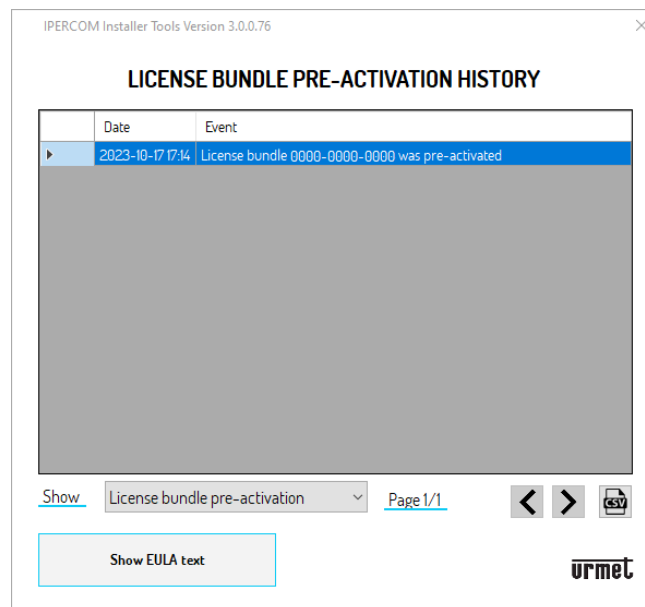


Figure 41: License bundle pre-activation history

The "Show EULA text" button allows you to view the text of the license agreement accepted during pre-activation.

### 6.7.2 Urmet Cloud authentication not performed

If you do not want to authenticate to Urmet Cloud, simply close the log in window that appears when *iPerCom Installer Tools* is started, as shown below:

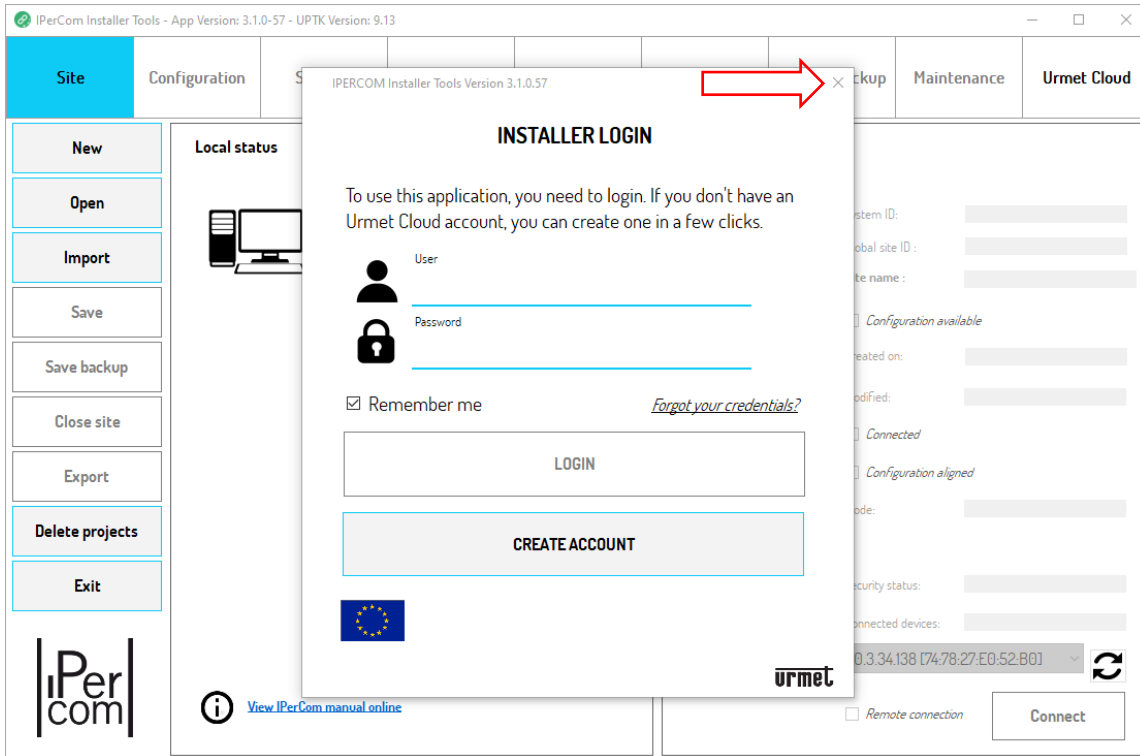


Figure 42: Cloud authentication rejected

The following dialog box is shown, which summarizes the main benefits of connecting to the cloud:

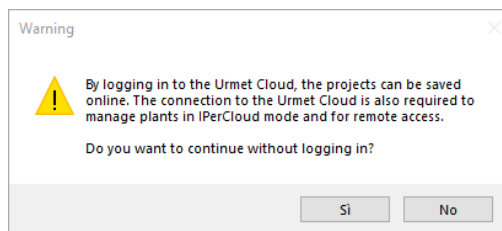


Figure 43: message following cloud authentication refusal

By pressing the "Yes" button the following screen appears, like the one when connecting to the cloud:

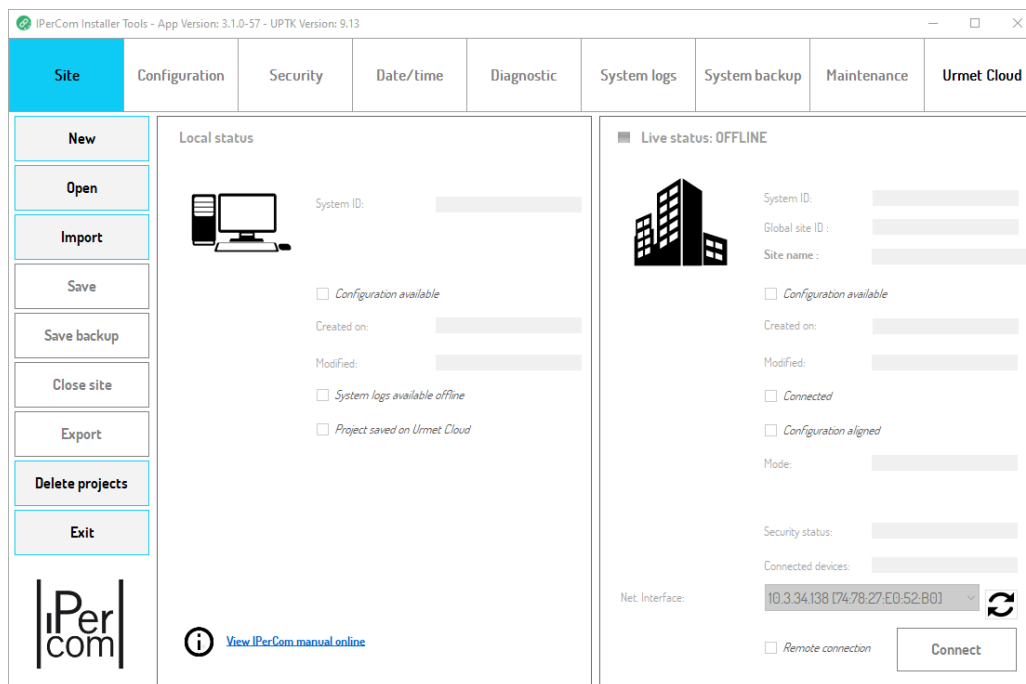


Figure 44: IPerCom Installer Tools screen after not authenticating to the cloud

The difference lies in the "Urmnet Cloud" tab, which appears as shown in the following screen:

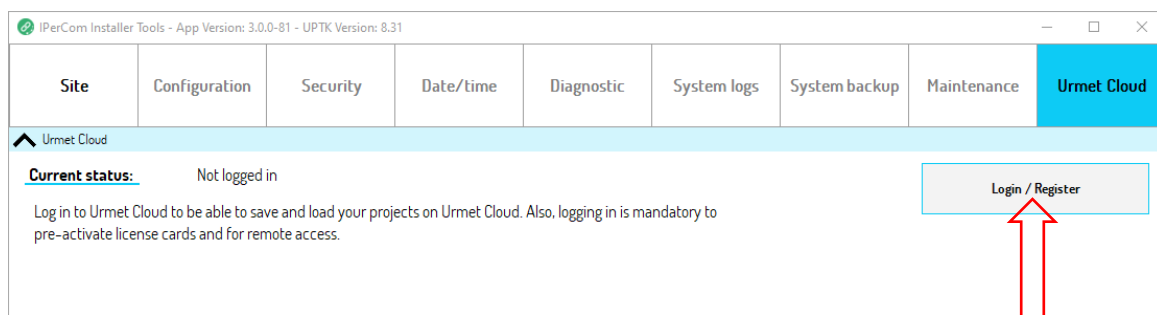


Figure 45 "Urmnet Cloud" tab without access to the cloud

Instead of the "Logout from the Cloud" and "Edit profile" buttons, the "Login/Register" button appears to access the cloud, if you already have an account, or after creating a new one according to the methods explained previously.



Given the additional features offered by access to Urmnet Cloud, in the following paragraphs it is assumed that registration to the cloud has been performed: the unsupported features will still be highlighted if registration to Urmnet Cloud is not performed.

### 6.7.3 Project and site

*IPerCom Installer Tools* is based on the **project** and **site** concepts, highlighted in tab “Site”.

The **site** represents the system you want to configure (meaning for system the entire network, devices and IPerCom software applications).

The configuration of a **site** occurs by creating a **project** with the related configuration, for example definition of the system topology, addition of devices on the topological nodes, addition of apartments (IPerCloud or non-IPerCloud), definition of any address books and activation rules, creation of residents and not residents, configuration of system and call forwarding parameters.

The creation (or modification) of the configuration relating to a **project** takes place from *IPerCom Installer Tools* by launching the *IPerCom Configurator* application or simply the *configurator* (see the relevant paragraph [The configurator](#)).

Through the *configurator* it is also possible to assign within the **project** a significant name to the **site** you want to configure and therefore associate the **project** with the **site** (system).

On *IPerCom Installer Tools*, after connecting to the system, it is possible to transfer the project configuration to the site and check the alignment status by highlighting the following 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**.

As soon as the configuration of a project is created, the “System ID” field is uniquely defined (numerical value calculated starting from the date of creation of the configuration file) (for further information see paragraph [Project and site parameters](#)).

It is possible to associate a project and several backups with the same “System ID” to a site (see [“Save backup”](#): *how to create one or more backups of a project*).

However, it is absolutely forbidden to associate projects with the same “System ID” to different sites.

All these concepts will be explained in more detail in the following paragraphs.

Having defined the concepts of **project** and **site**, it is now possible to explain in more detail the items in the screen below and how they work:

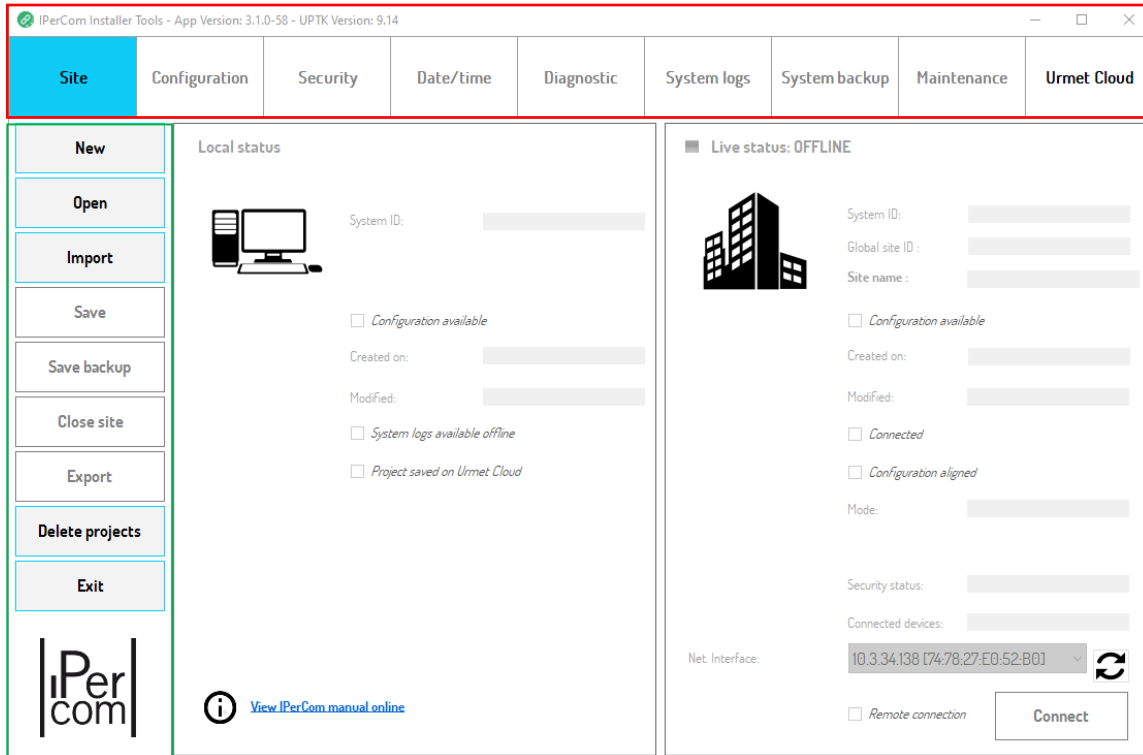


Figure 46: IPerCom Installer Tools startup screen

After starting the *IPerCom Installer Tools* application, all the tabs in the red box at the top are disabled apart from the “Site” and “Urmet Cloud” tabs. The only operations possible in this phase are those that can be performed using the buttons inside the green box and shown below.



The “Open” button is active if projects have already been saved.

#### 6.7.4 Creating a new project

To create a new project, press the “New” button. The following window opens where you can enter the name of the project and then confirm with “OK” button or cancel with “Cancel” button:

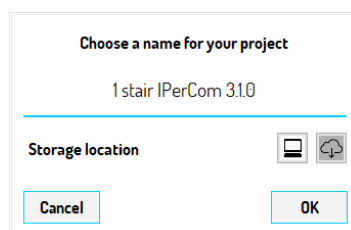








Figure 47: creation of a new project with access to Urmet Cloud

The “*Storage location*” option allows you to choose whether to save the project on your PC (icon ) or on the Urmet cloud (icon  if selected). Saving to PC is the default option.

 If you are not logged in to Urmet Cloud, the icon for this saving mode is as follows: . The icon is always grey and the "X" means that it is not possible to save the project on the cloud.

 The project name must be unique among those already present on your PC or those already present on Urmet Cloud and cannot contain the following special characters: \* : < > ? / \ |.

 Using the configurator, it will be possible to associate the **project** with its configuration to a plant site (for further information see paragraph [How to use IPerCom Installer Tools for the configuration of a system](#)).



### 6.7.5 Opening a project

To open a project, you need to press the “Open” button. The following window opens where **the projects associated with a specific site** are displayed:

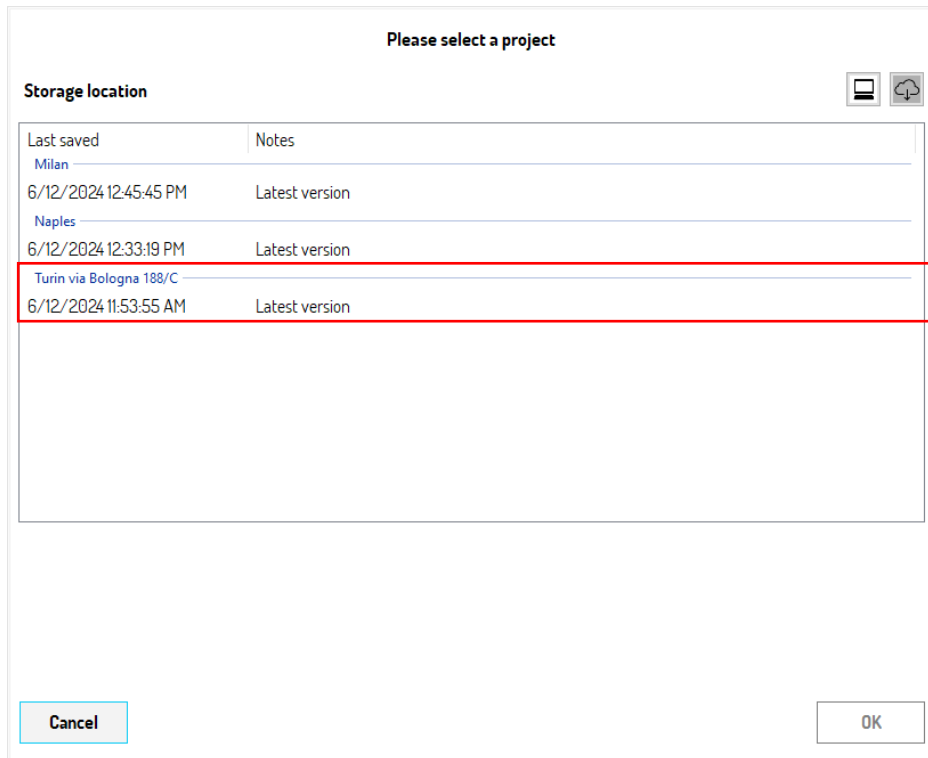


Figure 48: opening already saved projects

The names of the sites are highlighted in blue and immediately below is the **date and time of the last modification of the project** (as shown in the red box). If you select with the mouse the date and time of the last modification of the project, the following screen appears:

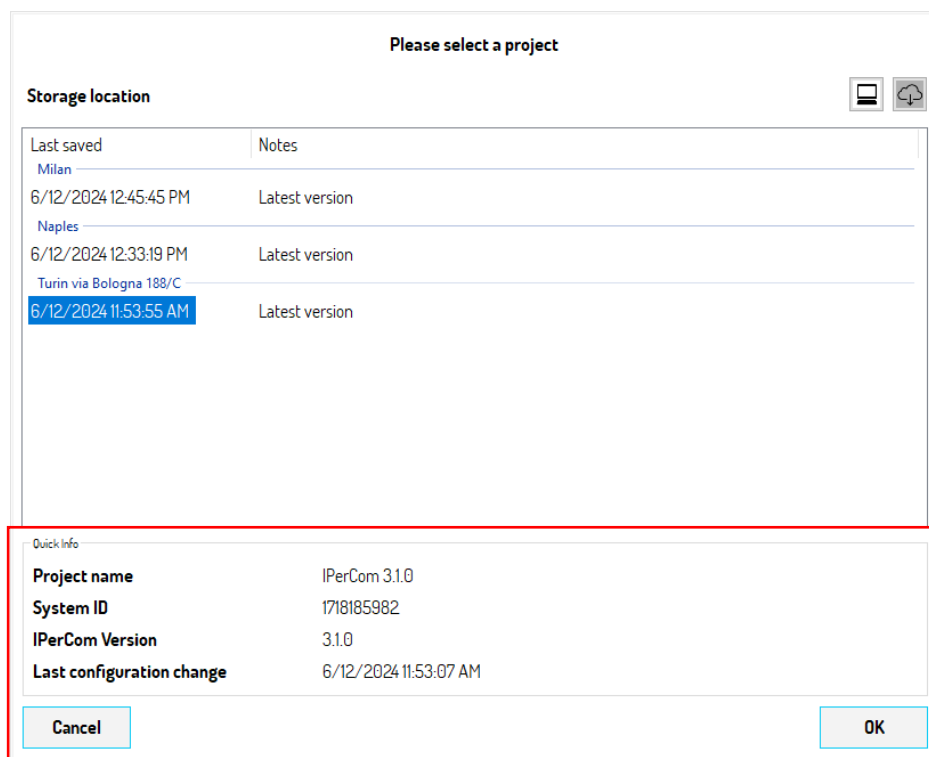






Figure 49: project associated to the site "Turin via Bologna 188/C"

In the **Quick Info** section (red box) the following data relating to the "Turin via Bologna 188/C" site appear in sequence, namely:

- "Project name": name given to the project when creating the project itself (via the "New" button);
- "System ID": unique identifier of the site calculated from the date and time of creation of the configuration file of the relevant project;
- "IPerCom version": IPerCom version with which the configuration file was created;
- "Last configuration change": date and time of the last modification of the configuration file.

The "Notes" column shows the indication "Latest version", as there is only one project associated with the site in question. If there is a need to associate a project and multiple backups of the project with the site, see the paragraph ["Save backup": how to create one or more backups of a project.](#)


The “Storage location” option allows you to choose whether to open the project from your PC (icon ) or from the Urmec cloud (icon  if selected). Opening the project from PC is the default option.

 If you are not logged in to Urmec Cloud, the icon for this opening mode is as follows: . The icon is always grey and the "X" means that it is not possible to open the project from the cloud.

### 6.7.6 Importing a project

To import a project, you need to press the "Import" button. There are 2 import methods and they allow you to:

- use the same project on another PC other than the one where it was created and saved,
- use a project created with old versions of *iPerCom Installer Tools* on a newer version (the oldest version allowed is 2.0.0).

 The second import mode is useful if, after updating a system, you want to use the project already created with the previous version of *iPerCom*.

The 2 import modes are now described in more detail.

#### 6.7.6.1 Use a same project on another PC

To import a project on another PC it is necessary to press the "Import" button. The following screen opens:

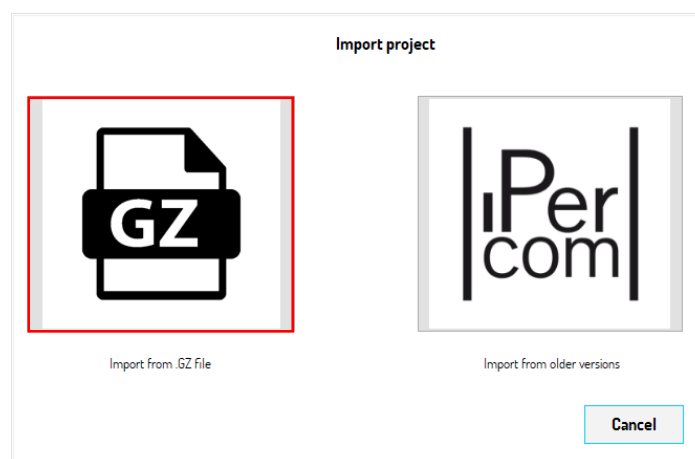






Figure 50: "Import project" window

Then press the button . A window opens through which you can import .gz files or .sbz files.


The .gz files are files previously generated on another PC by *IPerCom Installer Tools* with the "Export" button, after having opened the project to be exported. The .gz file thus generated must be copied to the PC where it is to be imported, so that the related project is available in *IPerCom Installer Tools*.

**The import operation (both for .gz and .sbz files) does not open the project directly but makes it available through the "Open" button.**

**From the installer's point of view, this operation is equivalent to transferring the project to another installer.**

-  *If a project is exported and then imported to the same PC, this operation returns an error, because a project with the same name already exists.*
-  *If a project is exported to a PC, then modified on a second PC through *IPerCom Installer Tools* and finally you want to import it on *IPerCom Installer Tools* from the first PC, the operation is possible only if on *IPerCom Installer Tools* of the first PC the previously created project is deleted.*
-  *In the import operations it is recommended to use *IPerCom* versions equal to or greater than the one used in the project export phase.*

The .sbz files (server backup zipped files) are files generated via the "System Backup" tab and are backup files that contain the site configuration. Importing a .sbz file is equivalent to locally importing the site configuration from which the backup was generated. For further details see the [System backup](#) paragraph.


-  ***If you import a project onto another PC, whose configuration has already been applied on a system, it is absolutely forbidden to transfer the same configuration to another system. The import function is to be used only to pass a project from one installer to another, assuming that both installers work on the same system.***

### 6.7.6.2 Import a project on a version of IPerCom 2.1.1 or higher

To import a project (already created) on an IPerCom version, you need to press the "Import" button. The following screen opens:



Figure 51: "Import project" window

Then press the button . A screen opens with the drop-down menu "IPerCom version", which allows you to choose the IPerCom version from which to import the project:

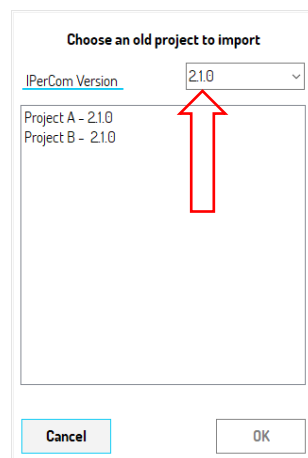


Figure 52: choice of the IPerCom version from which you want to import the project



The minimum IPerCom version from which it is possible to import a project is 2.0.0. The import function is available from version 2.1.1.

Once the project has been selected, by pressing the "OK" button, it is imported into the same IPerCom version selected in the IPerCom Installer Tools launcher (see paragraph [Starting the Launcher](#)).

The correct outcome of the operation is indicated by the following dialog box:

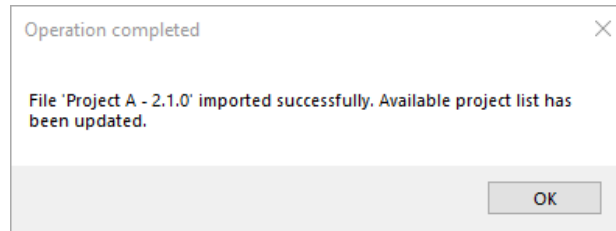


Figure 53: import successful

Through the "Open" button it will be possible to open the project just imported.

### 6.7.7 Deleting one or more projects

To delete one or more projects, you need to press the "Delete projects" button. The following window opens:

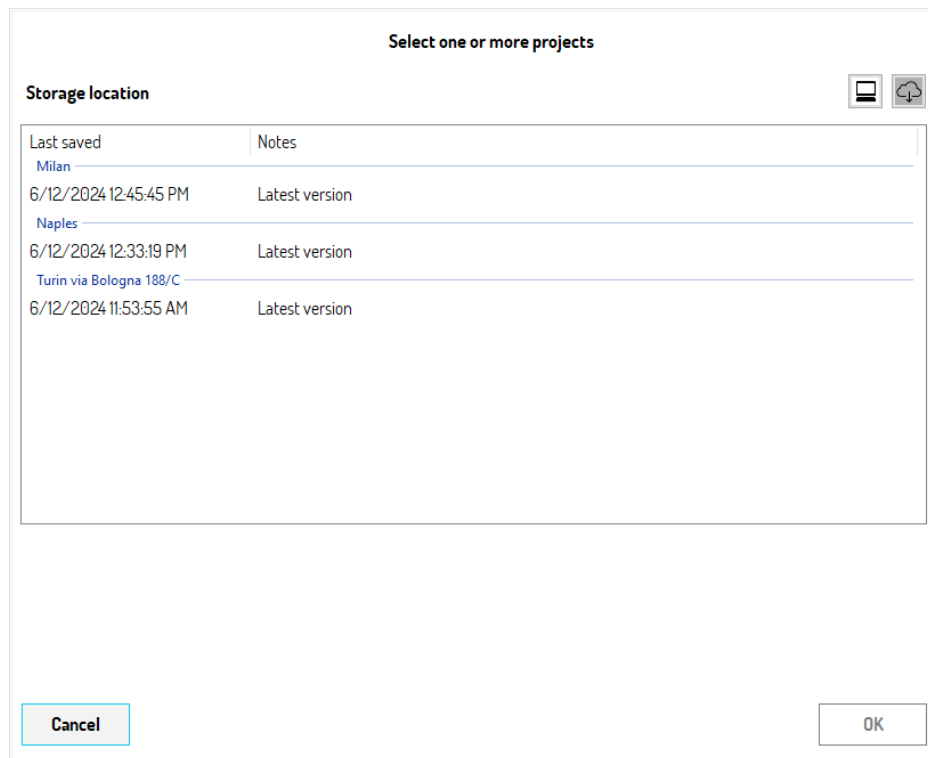


Figure 54: deleting one or more projects



To select a project, simply press the left mouse button on the relevant date and time or on the name of the site to which the project has been associated.



To select more projects, simply do the above and simultaneously hold down the "CTRL" key on the keyboard.

To select all the projects of a site (see paragraph [“Save backup”: how to create one or more backups of a project](#)), simply press the left mouse button on the name of the site in question.

To delete the selected projects, press the “OK” button.

To cancel the operation, press the “Cancel” button.

“Storage location” option allows you to choose whether to delete the project on your PC (icon ) or on the Urmet cloud (icon  if selected). Deleting from PC is the default option.

 If you are not logged in to Urmet Cloud, the icon for this deleting mode is as follows: . The icon is always gray and the "X" means that it is not possible to delete the project on the cloud.

### 6.7.8 Closing the application

To quit the application, you need to press the "Exit" button.

## 6.8 Project and site parameters

After logging in to Urmet Cloud, this screen appears:

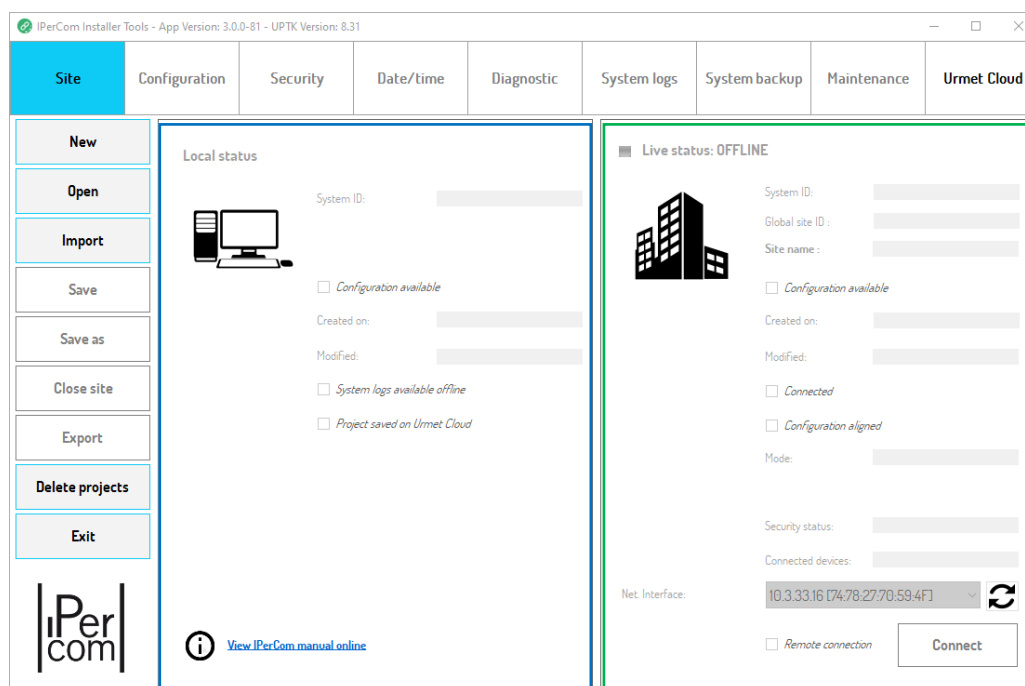


Figure 55: IPerCom Installer Tools screen after cloud authentication

In the box highlighted in blue all the information related to the project is loaded, whereas in the box highlighted in green all the information related to the site is loaded. In both boxes all information is shown in “read-only” mode.

To understand how and when the above parameters vary, some cases of practical use of a system configuration will be described.

Before doing this, a table with the information available in the "Local status" section (related to the project) with their meaning is shown:

Fields	Meaning
System ID	Unique identifier calculated from the date of creation of the configuration file of the relevant project.
Configuration available	Selected if the project has a configuration file, otherwise it is not selected.
Created on	Date of creation of the project configuration file.
Modified	Date of the last modification of the project configuration file.
System Logs saved locally	Selected if the project contains a copy of the System Logs, otherwise it is not selected (for further details see the relevant paragraph " <a href="#">System Logs</a> ").
Project saved on Urmet Cloud	Selected if the project was saved to the Urmet cloud instead of your PC.
View IPerCom manual online	Link to consult the IPerCom manual for the installer online.

Table 3: Meaning of the fields in the "Local Status" section



The above fields are assigned a value when creating a configuration file or opening an existing project.



A table with the information available in the "System status" section with their meaning is shown:

Fields	Meaning
System ID	Unique identifier calculated from the date of creation of the configuration file of the relevant project.
Global site ID	Unique identifier to identify the site in the <i>CallMe Manager</i> application, if related support is enabled.
Site name	Name to be associated with the site via the <i>configurator</i> .
Configuration available	Selected if the site has a configuration file, otherwise it is not selected.
Created on	Date of creation of the site configuration file.
Modified	Date of the last modification of the site configuration file.
Connected	Selected if you are connected to the site, otherwise it is not selected (to connect to the system see below).
Configuration aligned	Selected if the modification date of the project and the site configuration file coincide.
Mode	Shows the operating mode of the site, "Server" mode or "No server" mode.
Security status	Shows the security status of the site if "Blocked" or "Unlocked".
Connected devices	Shows the number of devices connected to the site (present or not present in the configuration file).
Network interface	It allows selecting the network interface through which to connect to the site (in local or remote mode).
Remote connection	Selected if connecting to a remote site.

Table 4: Meaning of the fields in the "Live Status" section



The above fields are assigned a value when you connect to a system and when the system has a configuration file. The last 2 are set manually by the installer.

Regardless of whether the project is saved on a PC or on Urmet Cloud, all the operations described in the following paragraphs are valid (for example transfer of the configuration to the system, export of the configuration and more).

## 6.9 How to use *IPerCom Installer Tools* for the configuration of a system

Below is the description of the various steps to follow to configure a site (system) with *IPerCom Installer Tools* and how the application parameters listed in the previous paragraph vary. The most common ways to configure an IPerCom system are shown below (assuming the system has already been installed and wired).

### 6.9.1 Mode 1: system installed but not configured, creation of configuration associated to the project without connection to the system

The various devices that make up the system have been installed and wired but have not been configured, that is the system has no configuration file. The steps to configure the system are described below:

- create a new project and the related configuration;
- connect to the system;
- set the proper system date and time;
- apply the newly created configuration to the system.

This is a practical example of use, as the installer usually creates the configuration in the laboratory, then goes to the system, where the devices have already been installed, connects to the system, and distributes the configuration. It is necessary to know the MAC addresses of the devices to be added to the configuration and the system topology, that is to know on which nodes the devices must be positioned.

### 6.9.2 Mode 2: system installed but not configured, creation of configuration associated to the project with connection to the system

The various devices that make up the system have been installed and wired but have not been configured, that is the system has no configuration file. The steps to configure the system are described below:

- create a new project and the related configuration, being connected to the system itself;
- set the proper system date and time;
- apply the newly created configuration to the system.

In this way of proceeding, it is not necessary to know the MAC addresses of the various devices (when creating the configuration) as these are automatically suggested by the *configurator*, which is not the case if you are not connected to the system. This will be described in more detail in paragraph “[The configurator](#)”. Instead, it is always necessary to know the system topology, that is to know on which nodes the devices must be positioned.

### 6.9.3 Mode 3: system installed but not configured, creation of configuration associated to the project by importing it from external file

The various devices that make up the system have been installed and wired but have not been configured, that is the system has no configuration file. The steps to configure the system are described below:

- create a new project;
- import from external file the configuration to associate to the project;
- connect to the system;
- set the proper system date and time;
- apply the newly created configuration to the system.



*In the last case there may be the variant in which you are already connected to the system while importing the configuration file.*

The first 2 ways of proceeding are now described in more detail, which are almost the same, since the only difference is the creation of the configuration file from the *configurator* (for more details see paragraph [“The configurator”](#)).

### 6.9.4 Creating the project and the related configuration file

When *IPerCom Installer Tools 3.1.0* is started, this screen appears:

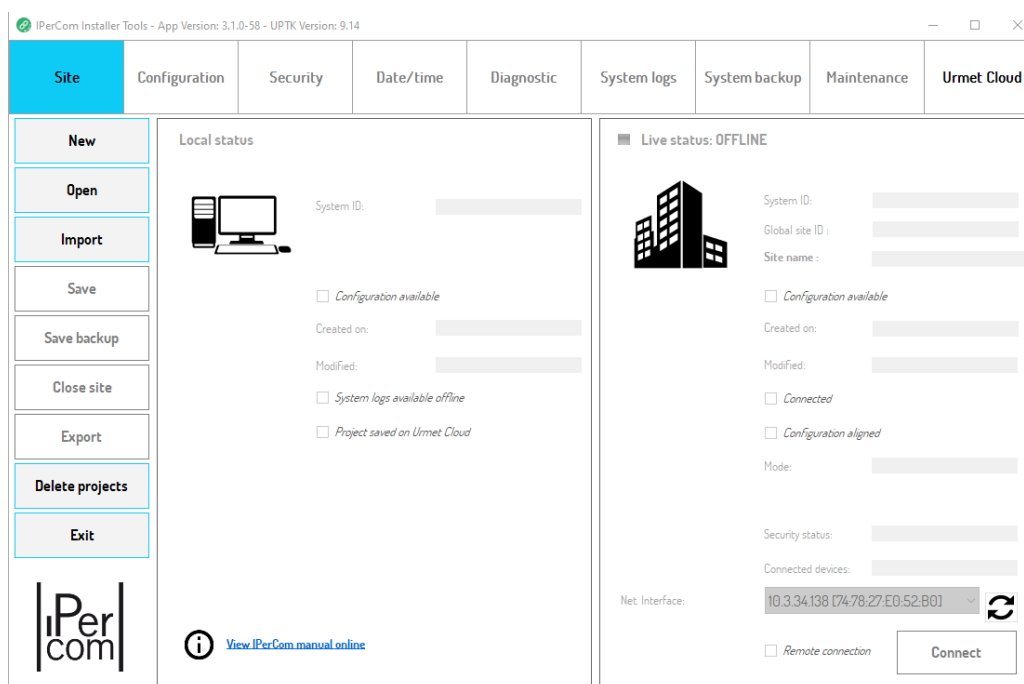


Figure 56: IPerCom Installer Tools startup screen

The "Open" button is active if projects have already been saved.

The starting point is to create a new project: to do this it is necessary to press the "New" button. The following screen opens, where it is necessary to enter the name of the project (to be associated with a site):

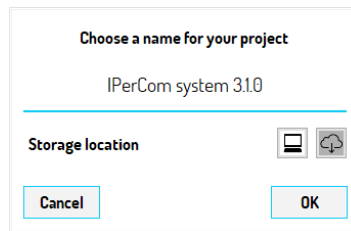


Figure 57: name assigned to the project

Pressing the "OK" button, the start screen of *iPerCom Installer Tools* becomes as follows:

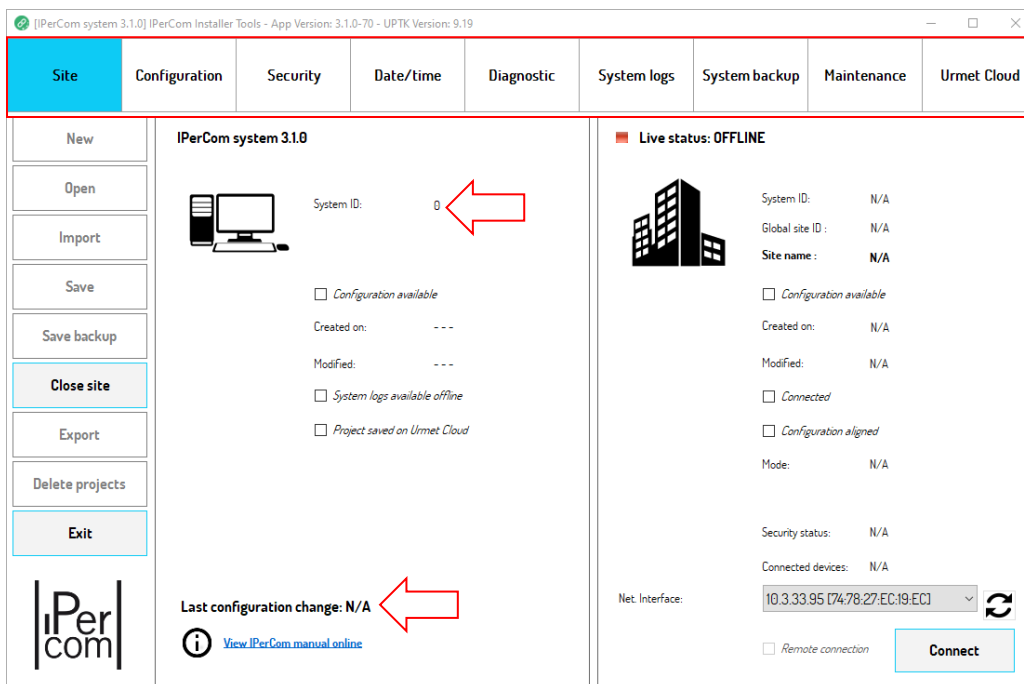


Figure 58: project created ("Site" tab)

The "New", "Open", "Import", "Save", "Save backup", "Export" and "Delete projects" buttons are disabled while the "Close site" and "Exit" buttons are enabled. All the tabs in the red box are enabled, even if the useful tabs for configuring a system are "Site" and "Configuration". The other tabs (except the tab "Urmet Cloud") cannot be used until you connect to the system and until the configurations associated to the project and site are aligned.

The “Close site” and “Exit” buttons are used respectively to:

- close the site (to which you want to associate a project) without exiting the *IPerCom Installer Tools* application;
- exit the *IPerCom Installer Tools* application.

After creating a new project but not yet the related configuration file, the “System ID” field is forced to zero (red arrow). The “Created on” and “Modified” fields are not filled in, as they are linked to the date of creation and last modification of the configuration file. These 3 fields will take on a non-zero value when creating a configuration file.

Similarly, the indication “Last configuration change: N/A” (red arrow) does not report any value as the project has not yet been associated with a configuration file and consequently a last modification date is not available.

To create a configuration file associated to a project, press the “Configuration” tab. The following screen opens:

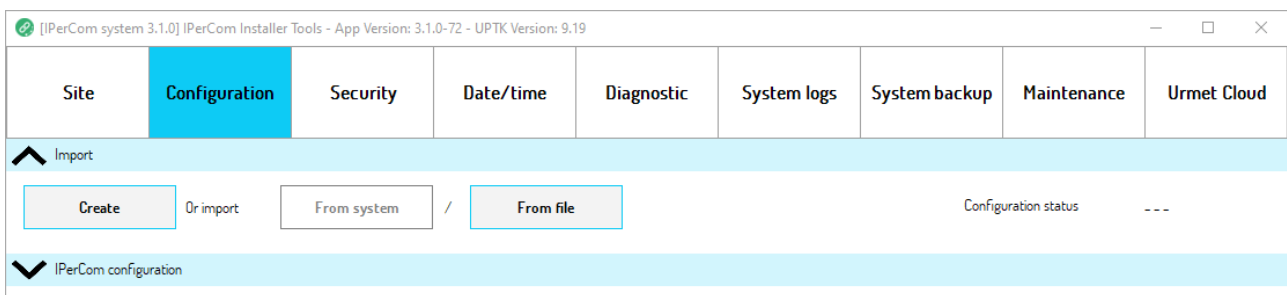


Figure 59: “Configuration” tab

The “Create” button allows creating and associating a configuration file to the project through the application *IPerCom Configurator* or simply *configurator*.

The “From File” button, instead, allows associating a configuration file to the project by importing it from an external file previously saved on PC. This way of importing the configuration will be described in detail later in paragraph [Creating the configuration file with import from external file](#).

As you can see, if you are not connected to any system yet, the only active buttons are “Create” and “From file”.

To create a new configuration, it is necessary to press the “Create” button, which opens the *configurator*. The screen displayed is as follows:

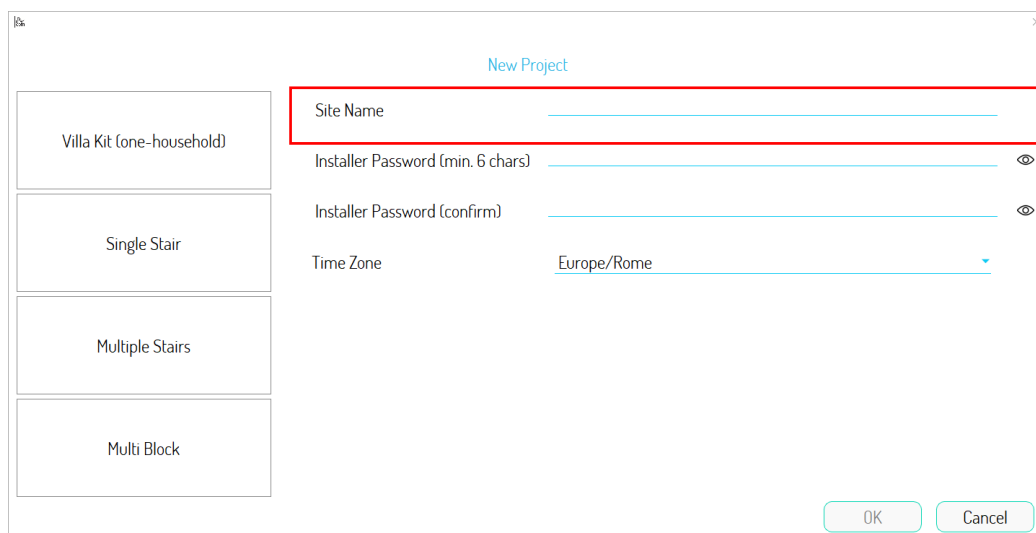


Figure 60: configurator start screen

The steps to follow to create a new project associated to a configuration file are described in paragraph [The configurator](#).

The *configurator* allows you to create (and subsequently modify) the configuration of a project, which will then be applied to the system. The main configuration points are listed below:

- topology definition (whether small, medium, or large system) ([Selecting the system topology \(model\) and the configurator structure](#));
- adding devices to the configuration ([Adding devices](#));
- definition of address books ([Contacts](#));
- creation of activations ([Activations](#));
- creation of residents and non-residents ([User management](#));
- access control setting ([Access control](#));
- setting system and call forwarding parameters ([System parameters](#)).

Each of the points listed above is described in a specific paragraph (in brackets).

Since the topics concerning the *configurator* are many, in order not to lose track of what we are describing about *IPerCom Installer Tools* features, we suppose at this stage to have already created and saved a configuration file associated to the project, referring to paragraph “[The configurator](#)” and to those listed above for all the relevant details.

At this point it is important to underline the presence of the “Site Name” field (red box), which is the significant name that is assigned to the site and which will also appear in the *IPerCom Installer Tools* and *CallMe Manager* applications.

Then, after creating and saving a local configuration, the following screen is displayed:

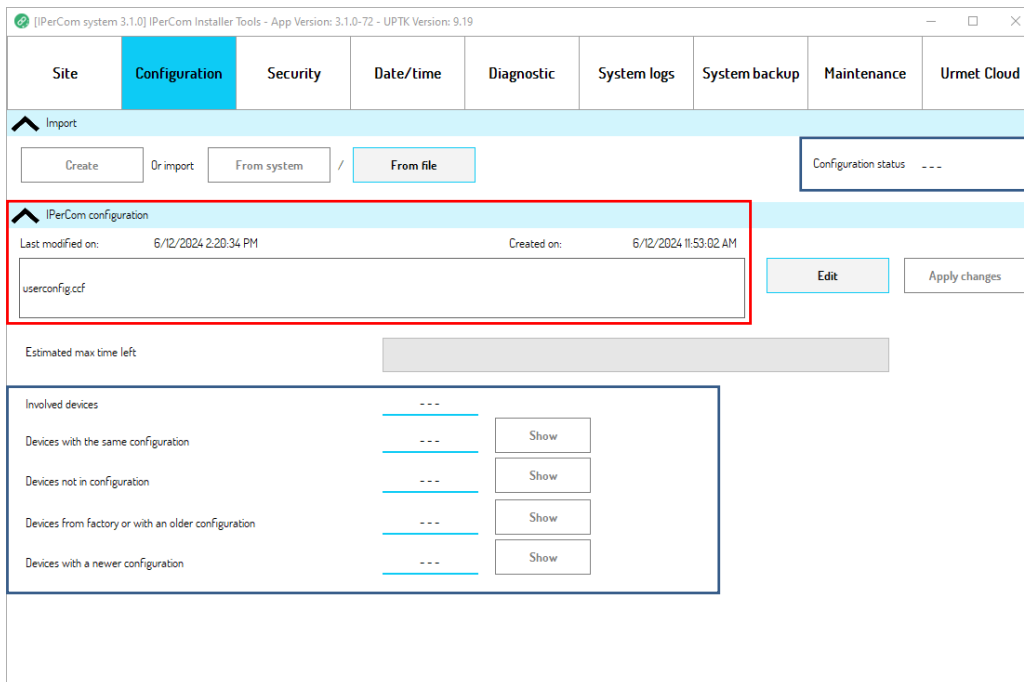


Figure 61: "Configuration" tab after creating the local configuration

The newly created configuration file is named *userconfig.ccf* and the date of last modification and the date of creation (red box) are displayed on this file.

The data in the blue boxes are not assigned a value because you are not connected to any system yet: their meaning will be explained below.

The "Edit" button allows editing the configuration file just created: the *configurator* opens again, and it is possible to make the desired modifications and close the *configurator*.

Now, by pressing the "Site" tab, the "System ID", "Created on" and "Modified" fields are assigned a value as a configuration file associated to the project is present and the "System ID" value is linked to the creation date of this file. The "Configuration available" field is also selected as there is a local configuration associated with a project.

**At this stage the name of the project displayed at the top of the left panel of *IPerCom Installer Tools* (see [Figure 58](#)) is replaced by the name of the site, as this field is available (it was filled in following the creation and saving of the configuration).**

The above is displayed in the following screen:

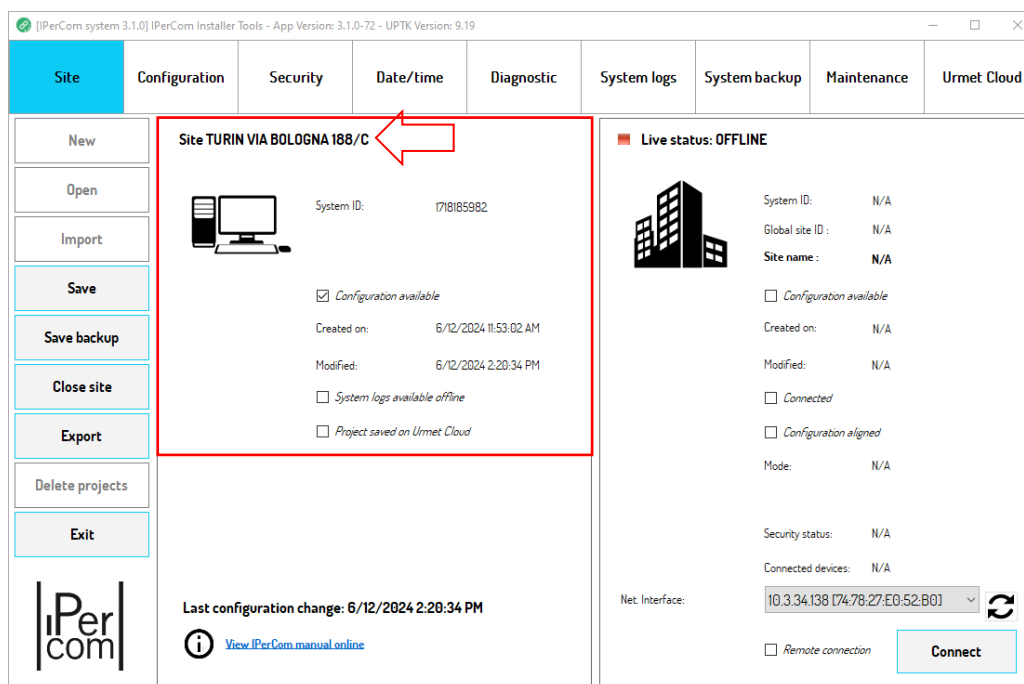


Figure 62: "Site" tab with local configuration created

At the bottom right (blue box) the last modification date of the configuration file is shown.

If during the installation phase the configuration requirements change and at the same time you do not want to lose what was done before any requested changes, it is possible to make a backup of the project (and therefore also of the configuration) and then make the changes. In this way it will always be possible to restore the situation prior to the changes themselves. How to do this will be seen in detail in the next paragraph.

### 6.9.5 "Save backup": how to create one or more backups of a project

If the system requirements change during the installation phase and at the same time you do not want to lose what was done before any required changes, it is useful to make a backup of the project using the "Save backup" button.

With reference to [Figure 62](#), the "Turin via Bologna 188/C" site is associated with a single project with the date of last modification of the configuration "06/12/2024 2:20:34 PM". If you need to make changes to the project but do not want to lose what you have done before, once you have opened the starting project, simply press the "Save backup" button.



The following screen appears:

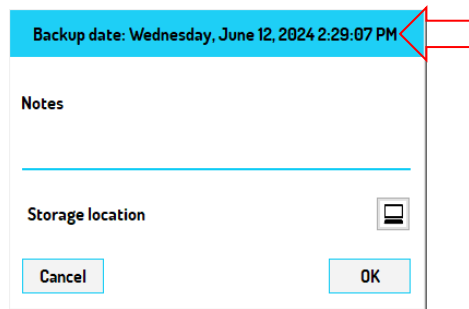


Figure 63: backup of a project

The date and time in which the project backup is being created is highlighted (red arrow) and, if necessary, an identifying note can be associated with the same backup: in this way the installer creates a restore point of his project which he can access at any time if the changes made are no longer necessary.

The location in which the backup is saved cannot be changed, in the sense that if the original project was saved on your PC, all the various backups will be saved on your PC, on the contrary if the original project was saved on Urmet Cloud, all the various backups will be saved on Urmet Cloud.

After entering any notes and pressing the “OK” button, the correct outcome of the operation is confirmed by the following dialog box:

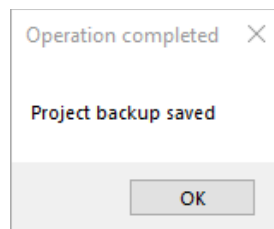


Figure 64: backup saved successfully

After making a backup copy, you can make the required changes to the current project and save with the “Save” button. The “Close site” button allows you to close the site you are working on without closing the *iPerCom Installer Tools* application.

After creating the backup, if you press the “Open” button, a screen like the one shown below appears for the “Turin via Bologna 188/C” site:

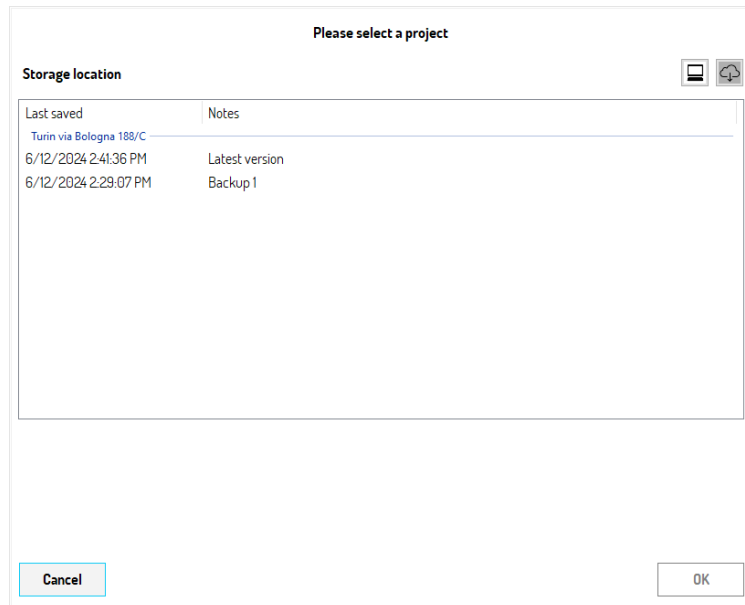


Figure 65: site with 2 projects (one of which is backup)

In detail, the project identified with the note “Latest version” indicates the most recent version of the project.

The project identified with the note “Backup 1” indicates, however, the backup created previously with respect to the latest changes to the most recent version.



The “Last saved” column shows the date and time of the last save of the project or backup creation date and time.

By selecting the most recent project (red box) or the backup (blue box), the following data relating to the selected object is displayed in the **Quick Info** section (red and blue box):

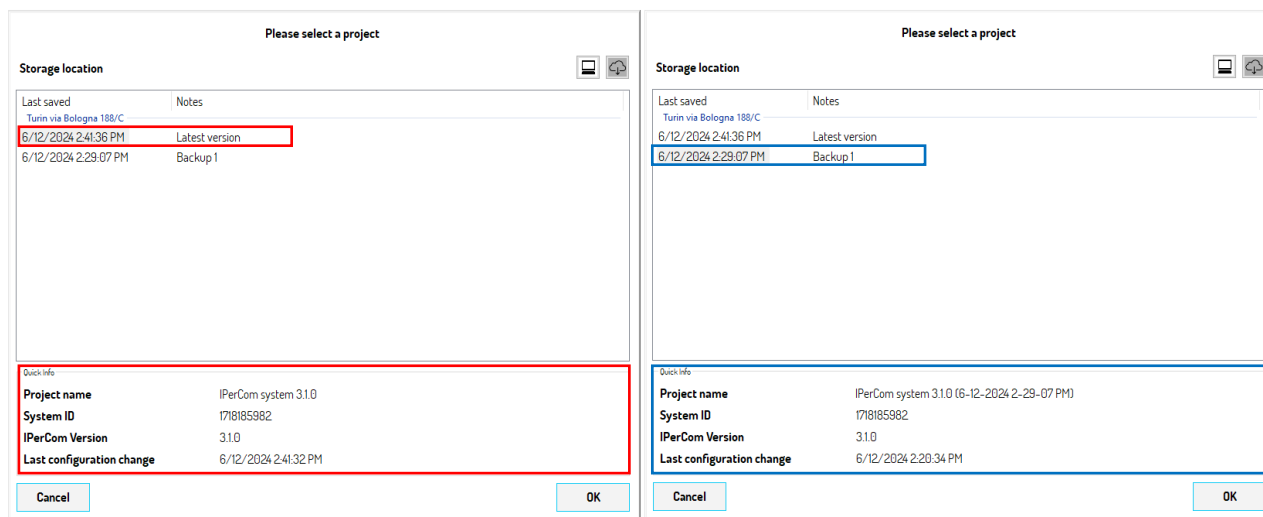


Figure 66: project and related backup associated with the site "Turin via Bologna 188/C"

In details:

- **"Project name"**: name given to the project when creating the project itself (via the "New" button) (in the case of backups, the date and time of backup creation is added in brackets to the project name).
- **"System ID"**: unique identifier of the site calculated from the date and time of creation of the configuration file of the relevant project; the data coincides for both the most recent version and the backup.
- **"IPerCom version"**: IPerCom version with which the configuration file was created; the data coincides for both the most recent version and the backup.
- **"Last configuration change"**: date and time of the last modification of the configuration file and related backups.

If a backup is selected and the “OK” button is pressed, *iPerCom Installer Tools* shows the following screen:

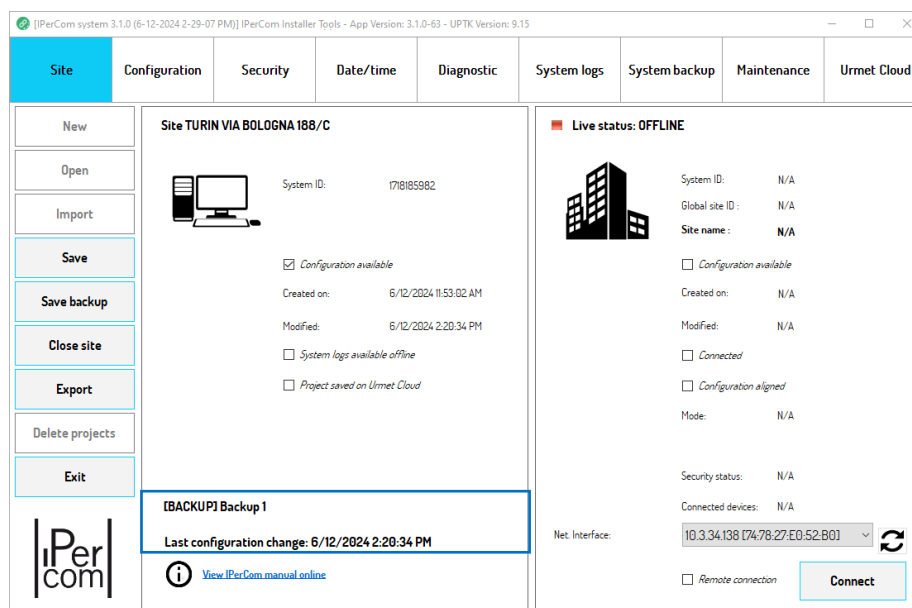


Figure 67: opening a backup

In detail, the following information is shown in the blue box:

- the [BACKUP] identifier to indicate that the open project is a backup;
- the note entered when creating the backup (“Backup 1”);
- date and time of the last configuration change.

### 6.9.5.1 How to restore a backup

To restore a backup, simply do the following after opening *iPerCom Installer Tools*:

- press the button “Open”;
- identify the site for which you want to restore a backup;
- identify the backup to restore from the notes entered when creating the backup itself;
- select the backup and press the “OK” button;
- press the “Save” button.

The effect will be as follows:

- the project identified with the note “Latest version” shows in the “Last saved” column the date and time of the saving just made,
- date and time of modification of the configuration file are those of the project identified as “Backup 1”, i.e. the backup configuration has been transferred to the “Latest version” project.

The following figure shows the above:

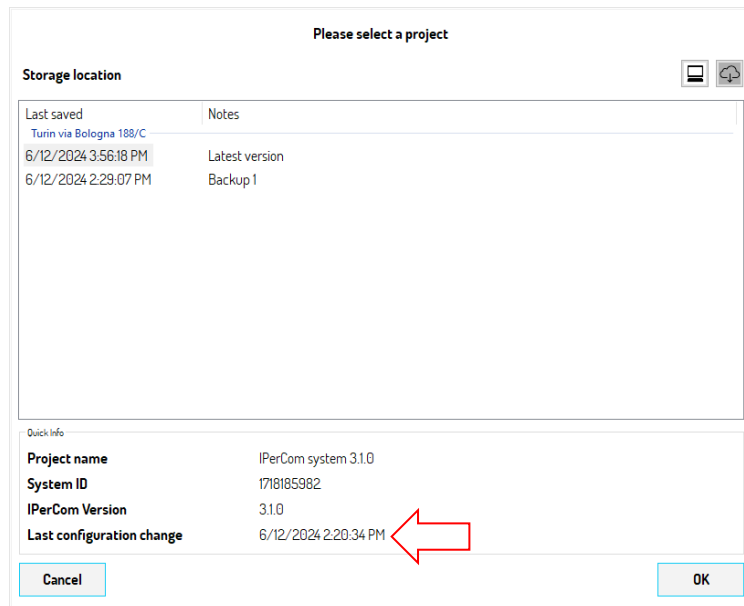


Figure 68: restore of a backup

It is important, therefore, to keep in mind that:

- the “Save” button saves the current project as latest version (regardless of whether the current project is the latest version or a backup copy)
- the “Save backup” button instead creates a non-editable backup copy that can be used as a restore point and at the same time saves the most recent version of the project with the current date.

## 6.9.6 Connecting to the system and transferring the configuration

Once the configuration associated with the project has been created and defined (backup or the most recent one), the next step is to connect to the system site and apply the newly created configuration to it, to configure the system. The relevant box on the “Site” tab shows values that are all unavailable because the system status is still offline (🔴), that is you are not connected yet:

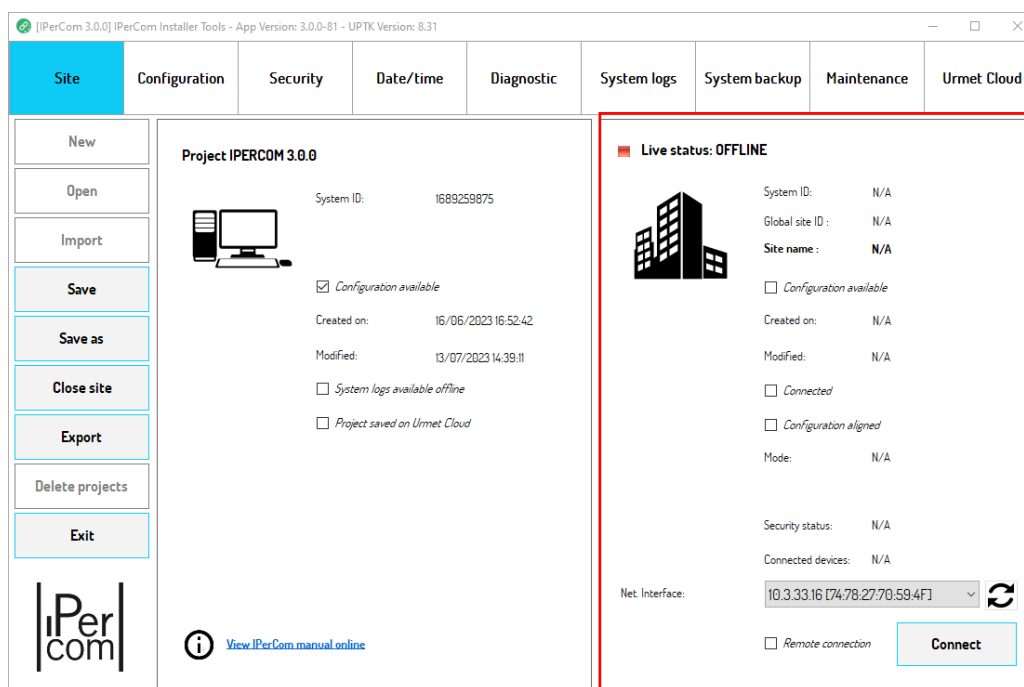



Figure 69: “Site” tab with local configuration created and no connection to the system

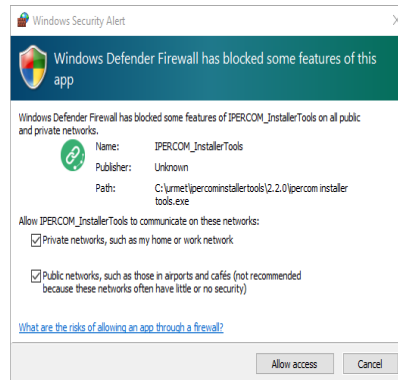
To connect to the system, select the network interface through which the PC is connected to the IPerCom system in the lower part of the red box and then press the “Connect” button.



To find out the IP and MAC addresses of the network interface through which you are connected to the IPerCom system, you need to click on the item “Open Network and Internet settings”, which appears by pressing the right mouse button the icon  at the bottom of right on your PC monitor. A screen opens with the list of available networks. After pressing the corresponding “Properties” item, you can view the IP address and MAC address.



After pressing the "Connect" button, the Windows operating system can notify the user of the need to unlock the communication ports on the IP network used for communication between the IPerCom system and the IPerCom Installer Tools application. This operation is required for proper application operation. If this operation is carried out by Windows Firewall, a warning like the one below is shown to the user:



You must select both kind of networks and press the "Allow access" button.

A progress bar is displayed, during its progress it is detected whether the system is with Server 1060/1 or without it, then the number of devices connected to the system is detected. At the end, the following window is displayed:

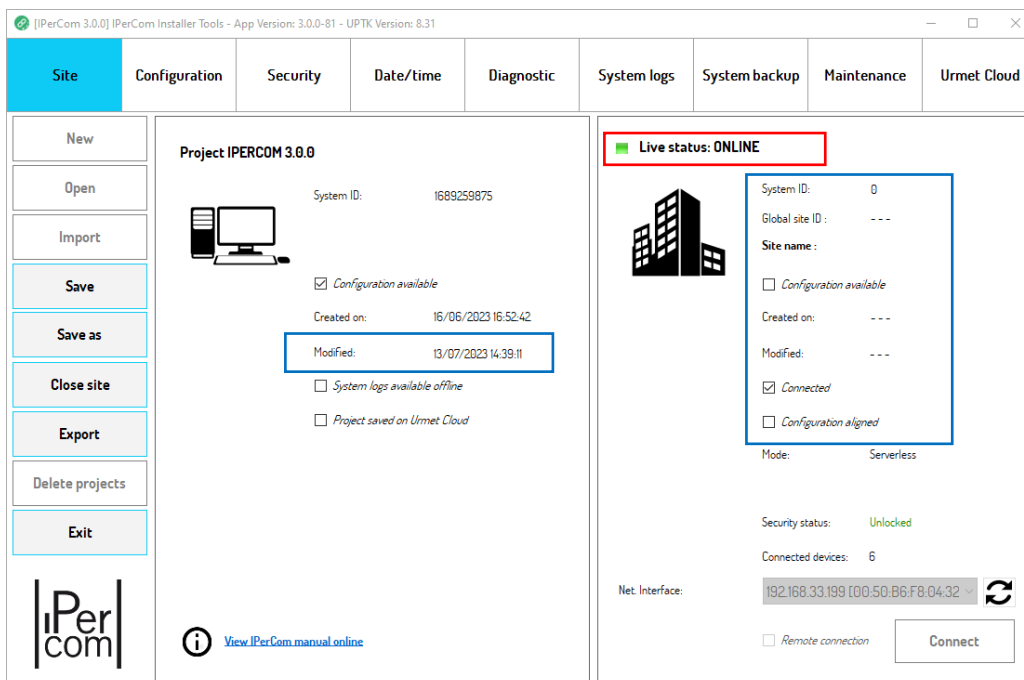



Figure 70: "Site" tab with local configuration created and connection to the system

In the system site box, the system status is now available (ONLINE) (red box), as indicated by the relevant icon . The system ID is zero, since the system does not have a configuration yet: therefore, also the “Created on” and “Modified” fields are not assigned a value since they are linked to the creation date and the last modification of the configuration file. The “Connected” field is selected, because the system is online.

The configuration is not aligned because the modification date of the configuration associated with the project and that associated with the site are different, that is the project has a modification date while the plant site still has none (blue boxes).

The other fields contain the following information:

“Mode”: “Server-managed” or “Serverless”, depending on whether the system is with or without a Server;

“Server IP”: IP address of the Server (if any);

“Security Status”: “Unlocked” or “Blocked”, depending on whether the system is blocked or unlocked;

“Connected devices”: indicates the number of all devices connected to the system (present and not present in the configuration).

### 6.9.7 How to set date and time on the system

Before transferring the configuration to the system, it is necessary to correctly configure the date and time on the system. To do this, press the “Date/Time” tab. The screen displayed is as follows:

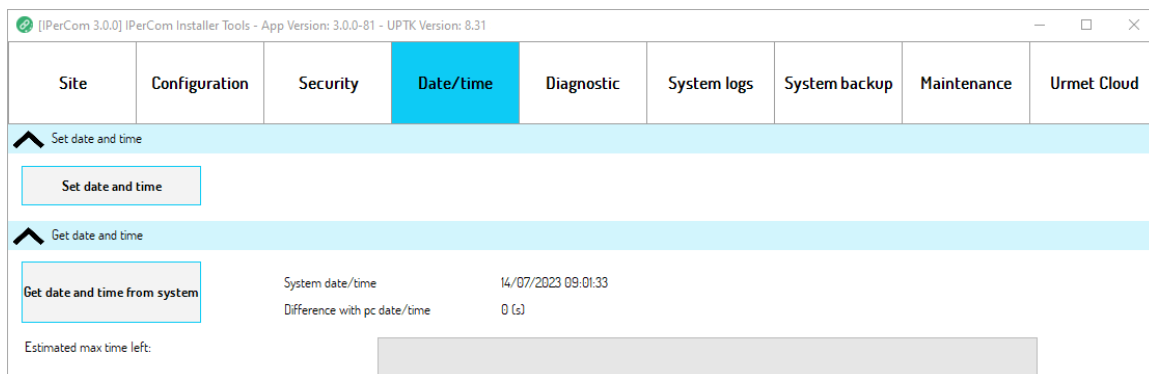


Figure 71: “Date/Time” tab



Now it is necessary to press the "Set Date/Time" button. Press "Yes" on the relevant dialogue box, date and time of the devices will be aligned with those of your PC. An additional dialogue box indicates that the operation has been completed correctly:

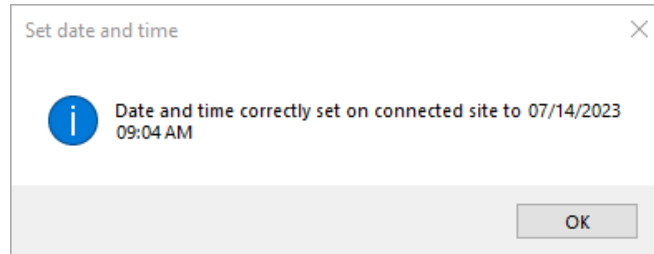


Figure 72: date and time aligned with those of the PC



When setting the date and time of the system, it is recommended to check that the date and time of your PC are correct.



If the system is connected to a router with an Internet connection, the correct date and time are already provided by the NTP (Network Time Protocol) service.

### 6.9.8 Transferring the system configuration

After configuring date and time, to apply the configuration to the system, simply go to the "Configuration" tab. The screen displayed is as follows:

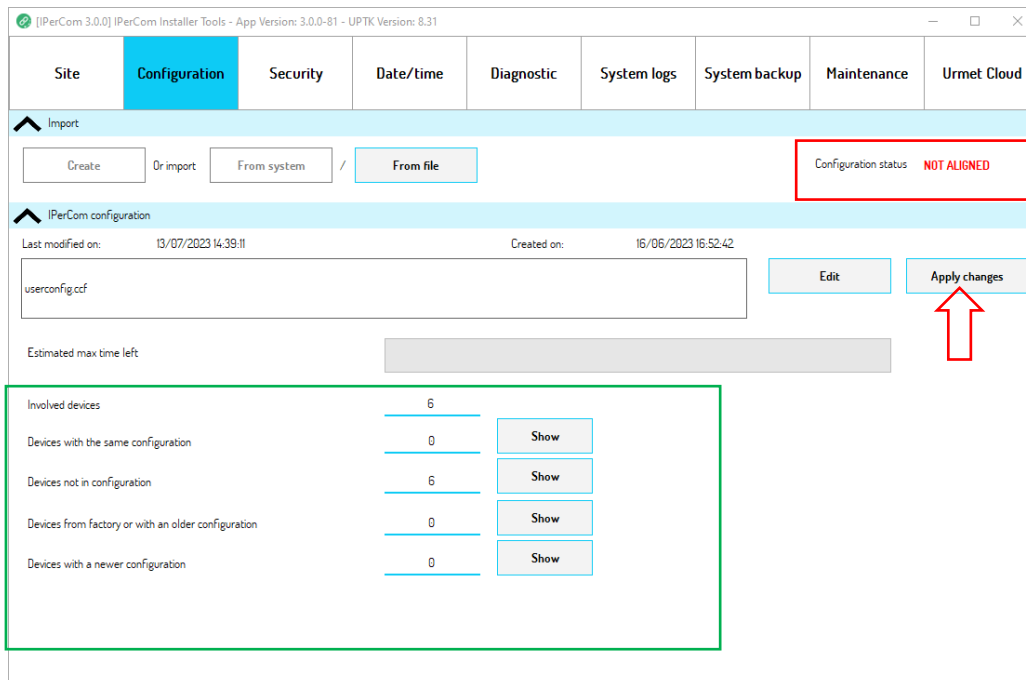


Figure 73: local configuration not yet transferred to the system

The green section shows schematically the condition of all the devices connected to the system. The example in question shows that:

- the number of devices connected to the system (*"Involved devices"*) is 6;
- the number of devices not in configuration is 6.

The configuration status is not aligned (red section), as explained above.

To apply the previously created configuration to the devices of the system, it is necessary to press the *"Apply Changes"* button.

The following pop-up window appears:

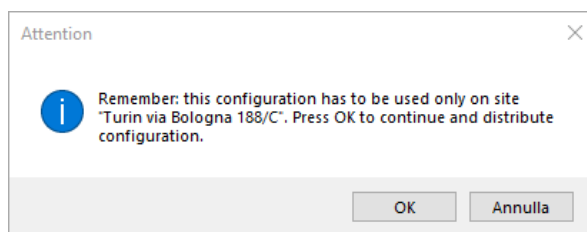


Figure 74: pop up window after pressing the *"Apply changes"* button

**This window only is useful to remind the installer that a project must be associated with only one site and cannot be associated with other sites, as this could cause malfunctions on the systems themselves. Therefore, projects with the same "plant ID" must not be associated with different sites.**

After pressing the “OK” button, the configuration associated with the project is applied on the plant site. Correct transfer of the configuration is highlighted by a progress bar which turns green once the transfer has taken place correctly, as shown below:

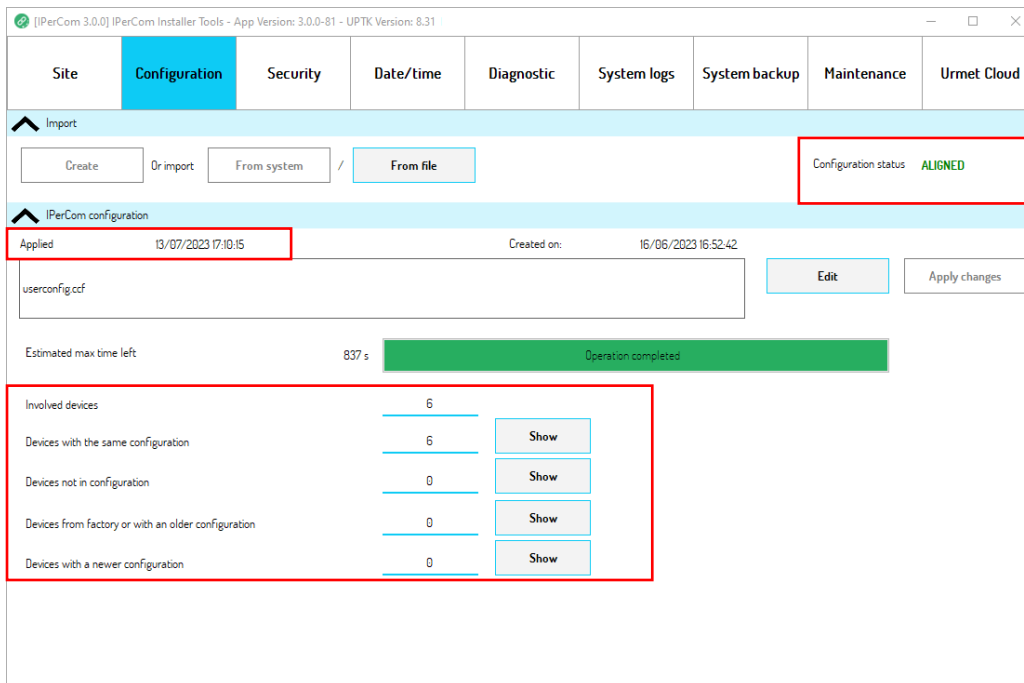


Figure 75: local configuration transferred to the system

The red boxes indicate that the configuration transfer has taken place correctly, i.e.:

- all devices in the system have the same configuration (“Devices with the same configuration” item);
- the configuration status is aligned.



Once the configuration has been applied, the “Last modified” field is renamed to “Applied” and shows the date and time in which the configuration was applied (or modified) to the system.



By pressing the “Apply changes” button, the error shown below is shown if CallMe Manager support is enabled in the configuration but authentication to Urmet Cloud has not been carried out:

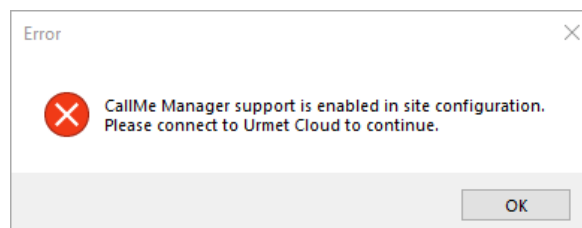


Figure 76: request for access to Urmet Cloud with CallMe Manager support enabled when deploying the configuration

The "Show" button displays a table with the list of devices with the same configuration, their MAC and IP address and the last modification date of the configuration file, as shown below:

Model	IP	MAC address	Configuration
171731A64	192.168.33.196	00:1E:E0:01:3F:45	13/07/2023 15:46:18
11603-11993	192.168.33.193	00:1E:E0:01:D3:B5	13/07/2023 15:46:18
106018	192.168.33.198	00:1E:E0:02:03:8A	13/07/2023 15:46:18
171731A64	192.168.33.195	00:1E:E0:03:34:F9	13/07/2023 15:46:18
176131	192.168.33.194	00:1E:E0:05:26:1E	13/07/2023 15:46:18
106048	192.168.33.3	00:1E:E0:05:B3:03	13/07/2023 15:46:18

Figure 77: list of devices with the same configuration

Press the "Site" tab to display the following screen:

Figure 78: "Site" tab with project and site aligned

The most important things to observe are the following:

- the identifier of project and site are the same, because the 2 identifiers are calculated starting from the creation date of the same configuration file;
- the configuration is aligned as the last modification date of the configuration file of the project and system site are the same;
- the "Site name" field, after applying the configuration, was filled in with the name given in the *configurator*.

Now the system has been configured: it is possible to save the project by pressing the "Save" button.

In this way the project with ID 1689259875 has been associated to the newly configured system: any attempt to apply to the system a configuration coming from a project with a different ID is prevented. This is to avoid loading "wrong" local configuration files on the system. Any modifications must be made starting from the project just saved (or from any of its backups that have the same identifier) and then transferred to the system so that the situation is always aligned between the project and the system. The correct way to operate will be explained later in a dedicated paragraph ([How to use IPerCom Installer Tools to edit the configuration with system already installed and configured](#)).

From what is written above it can be deduced that once a system has been configured via a project, this (with any backups) becomes the only point of reference for any subsequent changes. In other words, each plant must be associated with one or more projects with the same "System ID".



*Once the system configuration is complete, for safety reasons it is necessary to lock it. The procedure to block the system is always carried out through IPerCom Installer Tools and it will be explained in detail in paragraph "[System block](#)".*

#### 6.9.9 Creating the configuration file with import from external file

In the third system configuration mode, the open project configuration file is imported from an external file instead of being created from scratch. In this way the steps to follow are the following (still assuming that the system has been installed but not configured):

- import the configuration from external file;
- connect to the system;
- set the proper system date and time;
- distribute the newly imported configuration to the system.

In detail, after creating a new project with system ID equal to zero, press the "Configuration" tab, the "From File" button allows importing a previously saved configuration file from PC:

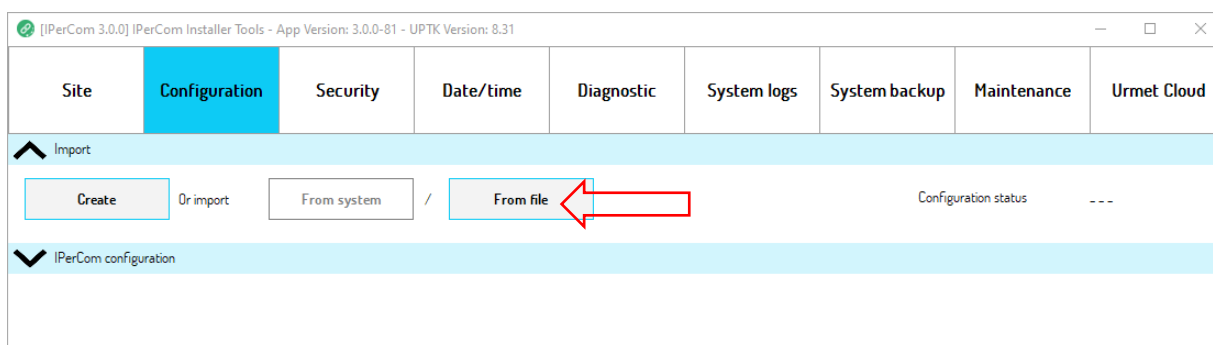


Figure 79: creating the local site configuration from an external file

The configuration files that can be imported have the ccf extension and, for example, can come from configurations created on *MAX*, *VOG<sup>7</sup>* or *Basic video door phone*, exported to SD card and then saved on PC (for further details see paragraph [“Exporting the configuration to an SD card”](#)).

After importing a configuration file, you are prompted to enter the installer password used to create the project.

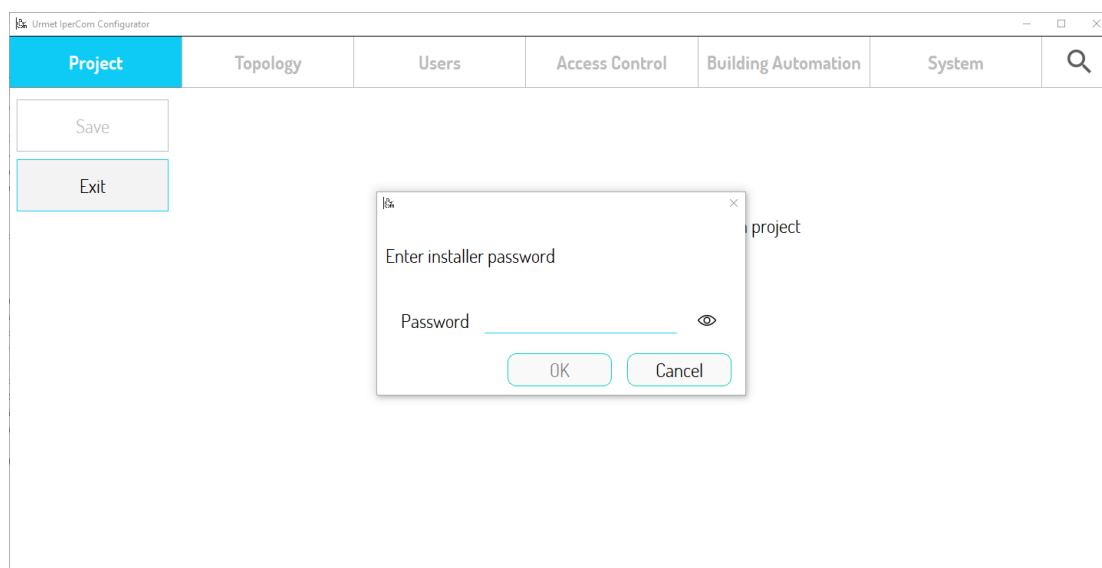


Figure 80: entering the installer password after importing the file

After entering the correct password, the *configurator* opens the relevant project:

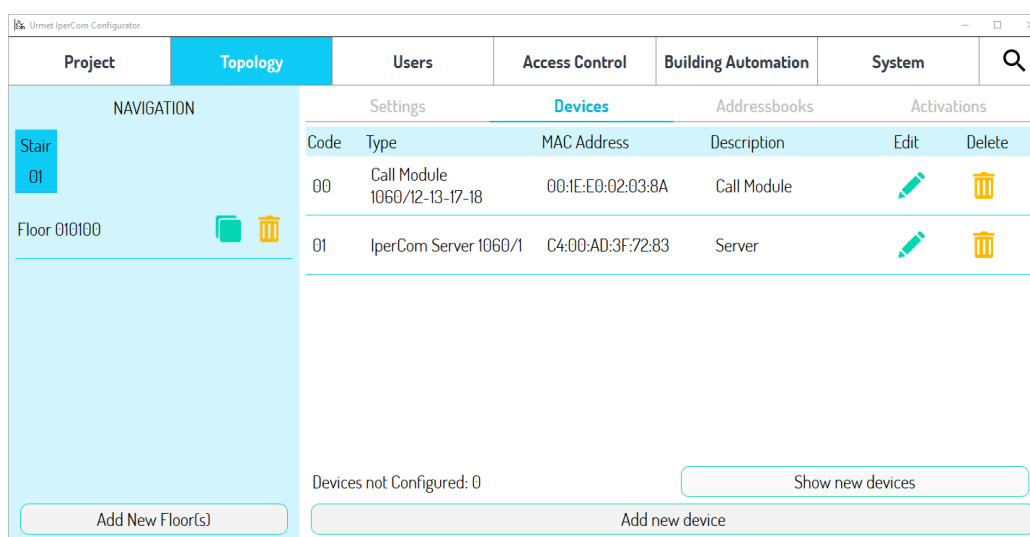


Figure 81: configuration of the imported file

After saving the configuration and exiting the *configurator* (see paragraph “[How to save the configuration](#)”), the way the configuration is transferred to the system is like the previous case.

**If you import a configuration file onto another PC and this configuration has already been applied on a system, it is absolutely forbidden to transfer it to another system. The import function can be used (for example) to pass a project from one installer to another, assuming that both installers work on the same system.**

## 6.10 How to use *IPerCom Installer Tools* to edit the configuration with system already installed and configured

When a system has been installed and configured, it may be necessary to modify its configuration for various reasons (that is change of topology, change of system parameters or addition of devices). The various steps to follow to modify the configuration of a system with *IPerCom Installer Tools* are described below:

- open the project connected to the previously configured system;
- make the required modifications;
- connect to the system;
- distribute the newly modified configuration to the system.

A variant of this procedure can be to connect to the system and then make the modifications: the advantage of this procedure is that, if new devices must be added, it is not necessary to know their MAC addresses, as these are automatically proposed by the *configurator*, which is not the case if you are not connected to the system. In this way it is also possible to check that the dates of the last modification of project and system are aligned and therefore be sure that you are starting from an already aligned situation.

In both cases, the essential point is that the project associated with the system with which the first configuration was made is available and to make sure that the system has not been modified by the MAX, VOG<sup>7</sup> or Basic video door phone which have the configurator on board.

In this situation, after opening the right project with the "Open" button from the "Site" tab, connecting to the system with the "Connect" button and making the required modifications with the "Edit" button (from the "Configuration" tab through the configurator), the following screen is displayed:

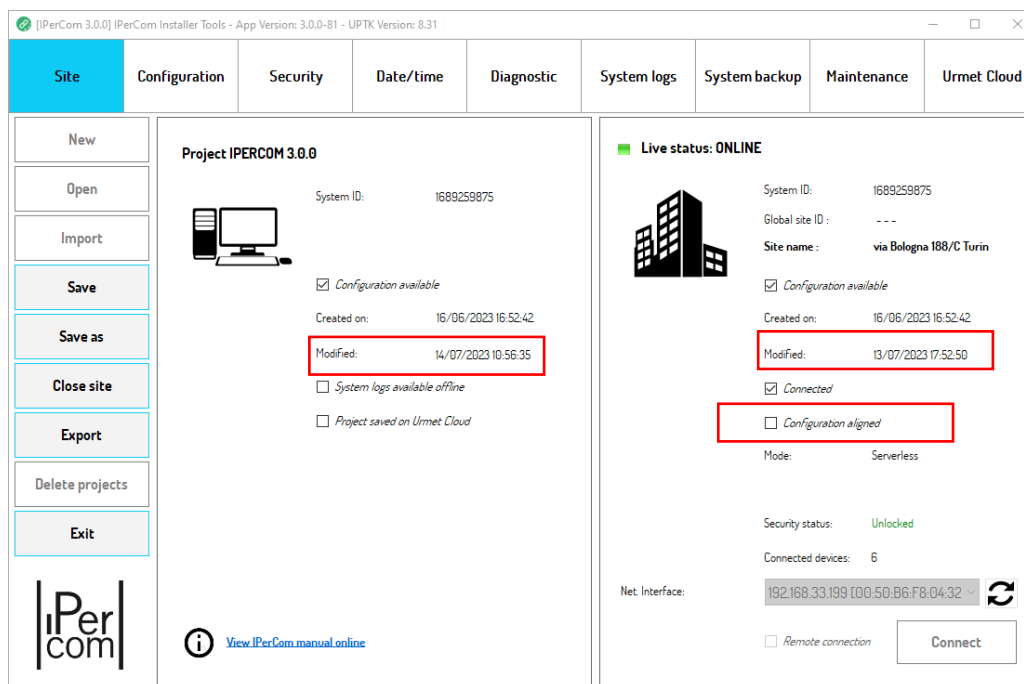


Figure 82: "Site" tab with project modified and connected to the system

As the local configuration has been modified with the "Modify" button, this is highlighted on the "Site" tab, as shown in the figure above: the modification date of the project is more recent than the modification date of the system site. This means that the configuration is not aligned (red boxes).

Local configuration modification requires the installer password, set through the configurator the first time the configuration has been created.

Connection to the system site may require the administrator password if the system is blocked.

The "System ID" fields are the same, since they are calculated starting from the creation date of the same configuration file (that of the project then transferred to the site);



The "Configuration" tab instead shows that the system devices have an older configuration than the project (as shown in the red box):

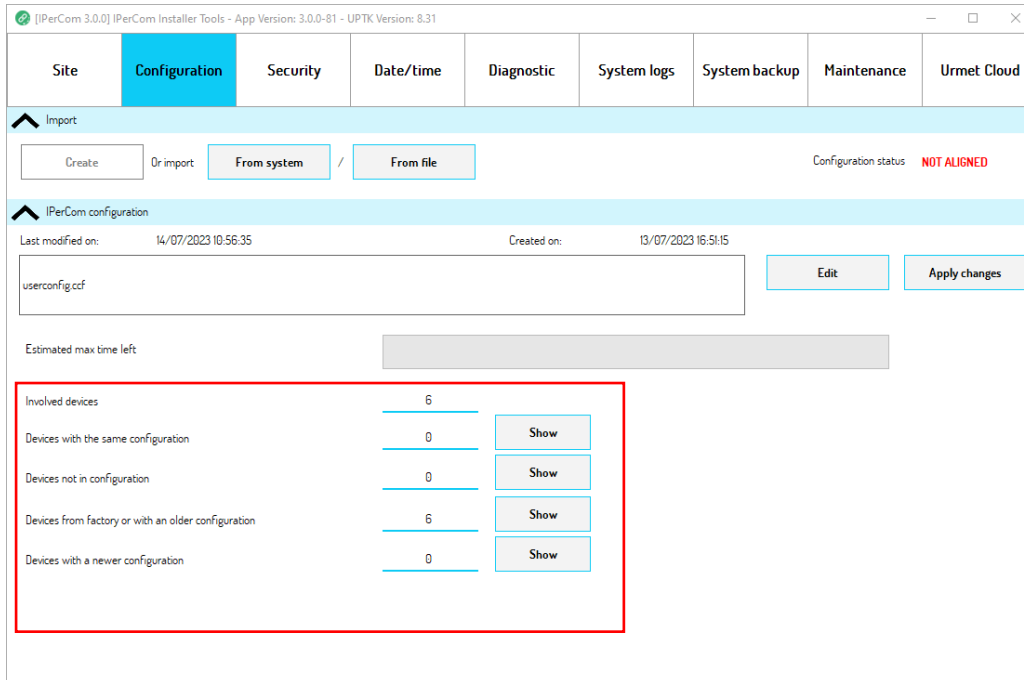


Figure 83: "Configuration" tab with local configuration not yet transferred to the system

The "Apply changes" button allows you to align the configuration: in fact (after applying the changes) the "Modified" field on the "Site" tab is the same both on the project and on the system site and therefore the configuration is aligned. In the "Configuration" tab, the "Devices from factory or with an older configuration" field is reset to zero, while the "Devices with the same configuration" field takes the same value as the system devices (with the same configuration associated to the project):



Figure 84: aligned configuration between project and system site

Involved devices	6	
Devices with the same configuration	6	Show
Devices not in configuration	0	Show
Devices from factory or with an older configuration	0	Show
Devices with a newer configuration	0	Show

Figure 85: system devices aligned to the local configuration

Now it is possible to save the project and then close it: the modification to the system has been correctly made through the same project that was used to configure the system for the first time.



*The configuration distribution procedure ends correctly when the number of devices with an old configuration or without configuration and the number of devices with a newer distribution are zero.*

The next paragraph describes an example of devices in the system with a newer configuration.

## 6.11 System modified locally by MAX, VOG<sup>7</sup> or Basic video door phone

In the example of use described above, it may happen that the configuration of the system site is more recent than that of the project: this may occur if changes have been made to the configuration file through the MAX, VOG<sup>7</sup> or Basic video door phone and the configuration associated to the project has never been changed (assuming you are starting from a situation where the project and system site were aligned). In this hypothesis, by opening *IPerCom Installer Tools*, after opening the project associated to the system and after connecting to the system, the following screen is displayed:

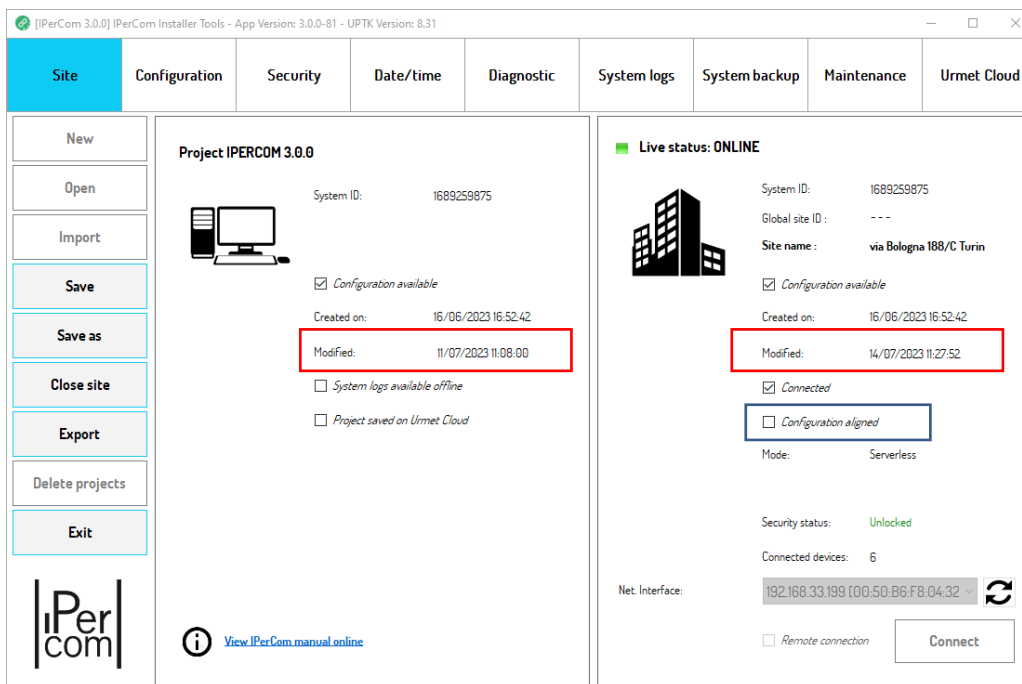


Figure 86: "Site" tab with system site modified

As the system configuration has been modified from the MAX, VOG<sup>7</sup> or Basic video door phone, this is highlighted on the "Site" tab, as shown in the figure above: the modification date of the site configuration is more recent than the modification date of the project configuration. This means that the configuration is not aligned (blue box).



The connection to the system site may require the administrator password if the system is locked.

The "Configuration" tab instead shows that the system devices have a newer configuration than the project. In fact, the "Devices with a newer configuration" field is equal to 6, that is all the system devices:

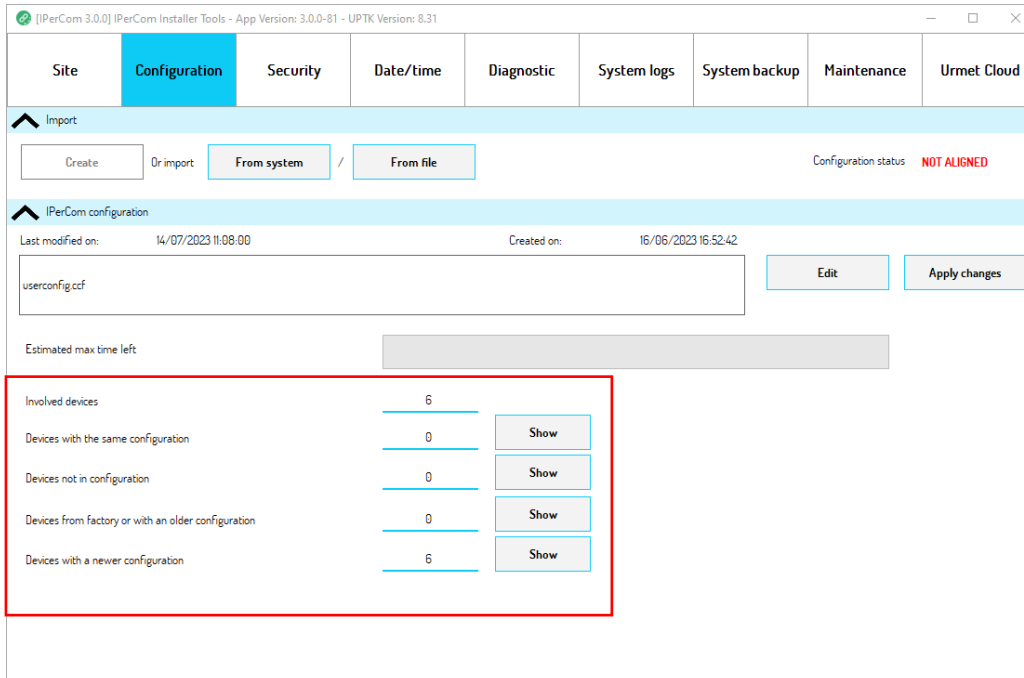


Figure 87: "Configuration" tab with system site with more recent configuration than the local site

The "Apply changes" button allows you to align (if you want) the configuration associated to the project to the configuration associated to the site, but losing all the modifications made on the system site. The warning message below is displayed:

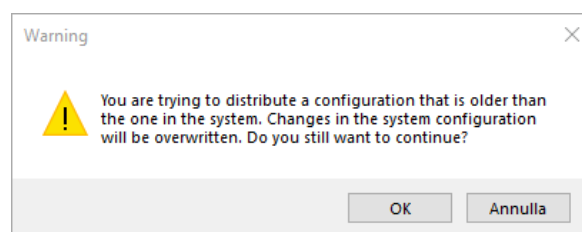


Figure 88: alignment of system site to local site with loss of modifications



The above message also appears when an attempt is made to restore an old configuration on a system using the backup function: in this case the configuration present on the system is more recent than that associated to the project.

Press the "OK" button at the end of the configuration distribution: the "Site" tab, the "Modified" field on the project and the system site have the same date and then the "Configuration aligned" field is selected:

Modified: 14/07/2023 12:16:01	Modified: 14/07/2023 12:16:01
<input type="checkbox"/> System logs available offline	<input checked="" type="checkbox"/> Connected
<input type="checkbox"/> Project saved on Urmet Cloud	<input checked="" type="checkbox"/> Configuration aligned

Figure 89: aligned configuration between project and system site



The "Modified" field reports the date and time the configuration was applied.

In the "Configuration" tab, the "Devices with a newer configuration" field is reset to zero, while the "Devices with the same configuration" field takes the same value as the system devices with the same configuration associated to the project:

Involved devices	6	
Devices with the same configuration	6	Show
Devices not in configuration	0	Show
Devices from factory or with an older configuration	0	Show
Devices with a newer configuration	0	Show

Figure 90: system devices aligned to the project

If, on the other hand, you do not want to lose the modifications made on the system site through the MAX, VOG<sup>7</sup> or Basic video door phone and you want to align the local configuration with the system configuration, simply press the "From system" button in the "Configuration" tab: in this way the system site configuration is transferred to that associated to the project. The following screen is displayed, where the only configuration available on the system must be selected:

Import configuration from system

Configuration

Please select configuration

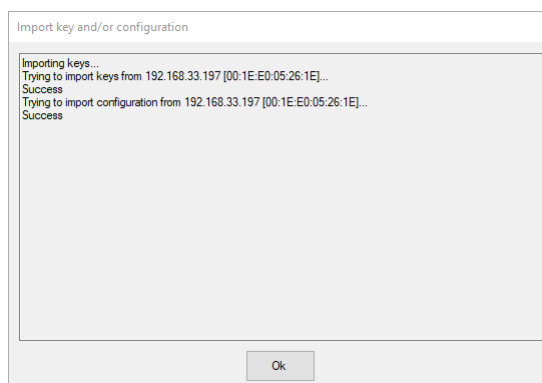
System ID	Configuration	Devices
1689259875	14/07/2023 11:27:52	6

Figure 91: window to select the configuration to be imported on the local site



*In systems with at least one Server 1060/1, when importing the configuration from the system site to the project, the only device recognised is one of the system Servers.*

Now enable the "Import" button, and press it to import the keys (installer and administrator password) as shown below:



*Figure 92: importing passwords*

After pressing the "OK" button, the configuration is aligned again, that is the project and the system site modification date is the same and the devices have the same configuration.

## 6.12 Importing configuration files with different IDs

After locally creating a project with a configuration file and transferring the configuration to the system, the situation is as follows:

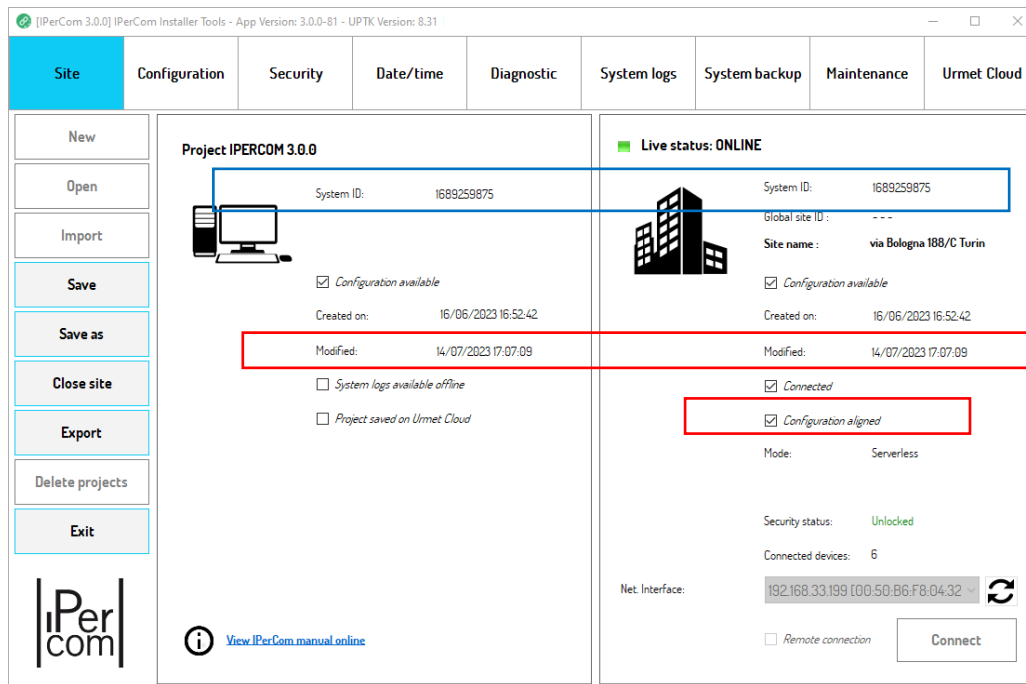


Figure 93: "Site" tab with project and system site aligned

The system is aligned, as shown in the red boxes, that is the modification date of the local configuration and that of the system are the same.

The "Modified" field is useful to understand if the configuration file is more recent on the project or on the system site and then to understand where the last modifications were made (whether on project or on system). The identifier of project and system site are also aligned (blue box), because the 2 identifiers are calculated starting from the creation date of the same configuration file.

This parameter is useful to avoid importing configuration files from other sites with different system identifiers on an already configured and functioning system, and thus creating malfunctions. If modifications need to be made to the system, they must be made from the project associated with the system and then transferred to the system, so that there is always an aligned situation between the project and the system site.

If project and system site have different identifiers and you try to apply the project configuration to the system site, the following occurs.

If you create a configuration file with an identifier other than 1689259875 (which is the right system identifier), i.e. with a creation date other than "16/06/2023 16:52:42", and if you are not yet connected to the system (which has the same identifier as the local site "1637772037"), the following situation occurs:

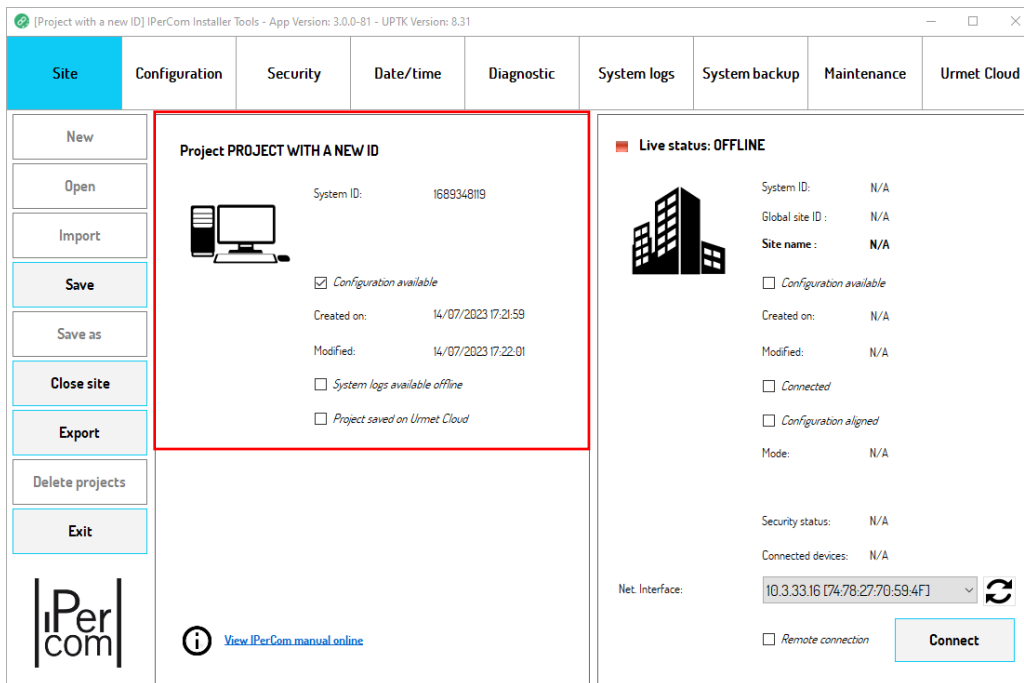


Figure 94: "Site" tab with project identifier different from that of the system site

As shown in the figure above, the project identifier is different from 1689259875. If you connect to a system already configured and working (with identifier 1689259875) and try to apply this configuration, you could inevitably lose the work already done. To avoid this, when the local identifier does not coincide with the system identifier (that is with system already configured), after pressing the "Connect" button, the following message is displayed:

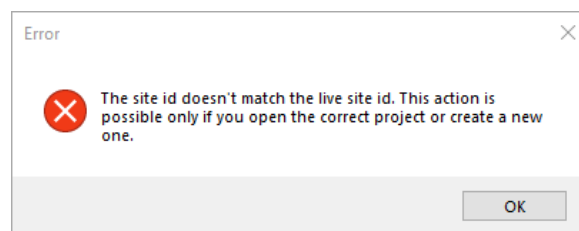


Figure 95: error message if project identifier and system site identifier do not match

Press the "OK" button to close the application and open it again on the "Site" tab with no project open.

The only way to connect to the system is to load the project connected to this system: the correct use of the application requires in fact to have a unique project for each system from which to connect to the system and make the modifications.





The above error also occurs if the project configuration is taken from an external configuration file saved on a PC and you try to connect to a different identification system.

If by mistake the project has been deleted and you want to restore it from the system site, you can create a new project with a zero identifier (that is without any configuration file):

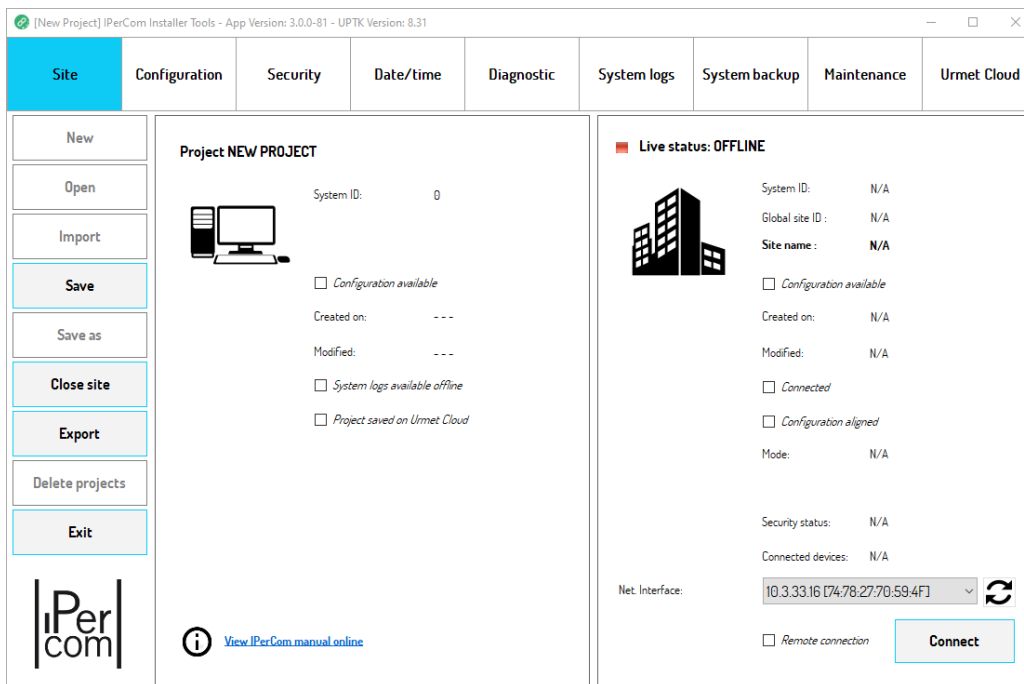


Figure 96: "Site" tab with project identifier equal to zero

Now, after choosing the right network interface, it is necessary to connect to the system.

The following screen is displayed:

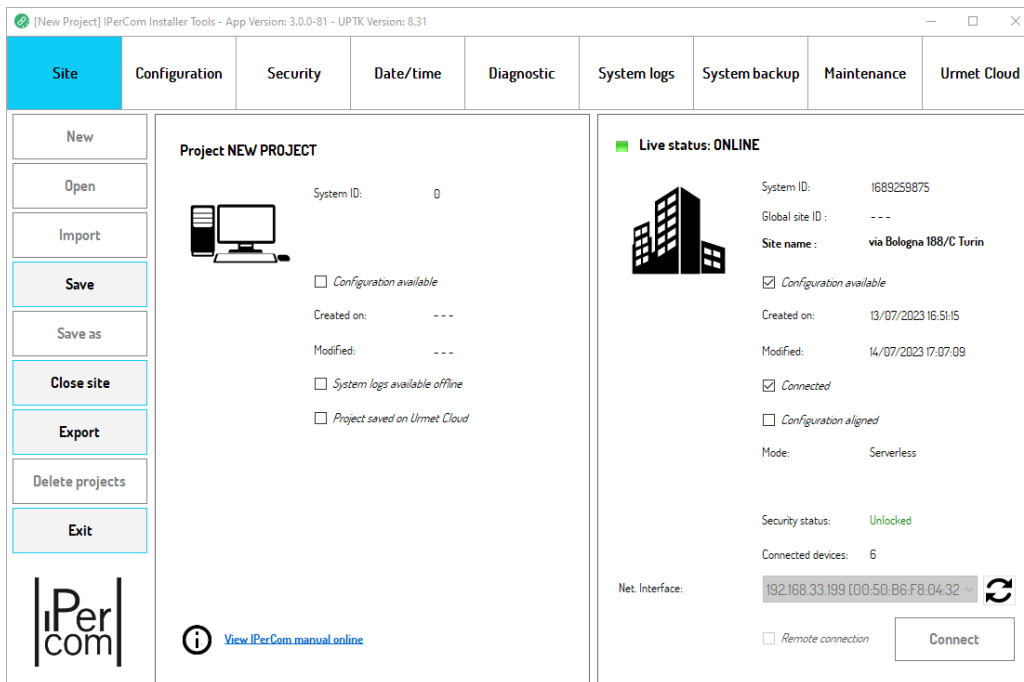


Figure 97: "Site" tab with connection to the system and project identifier equal to zero



Connection to the system site may require the administrator password if the system is blocked.

The system ID 1689259875 corresponds to that of the first configuration. Now move to the "Configuration" tab, the following screen is displayed:

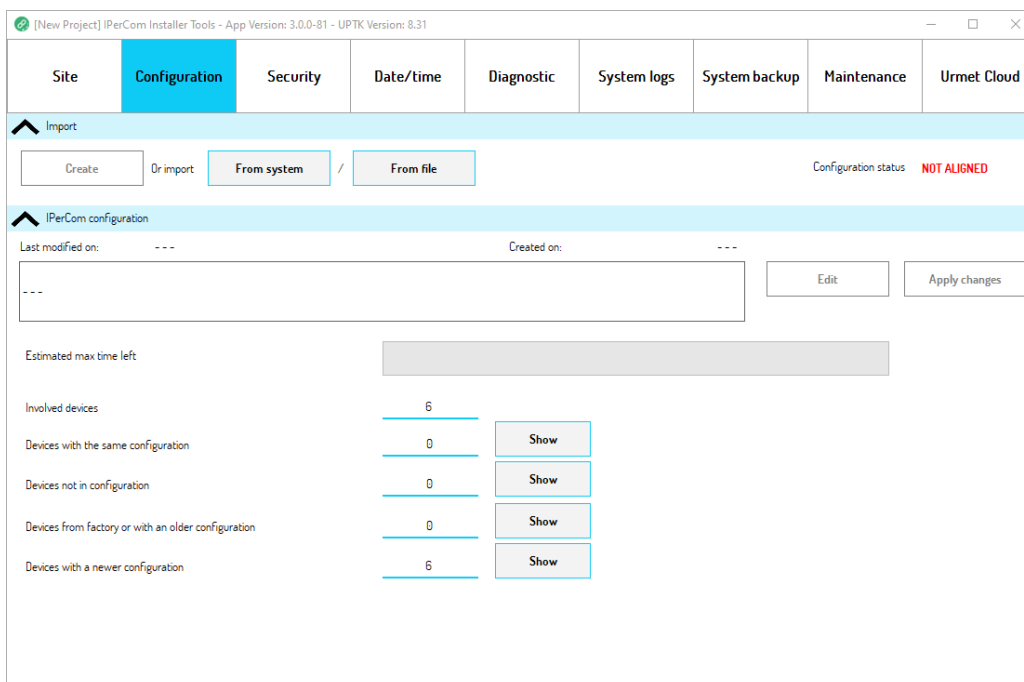


Figure 98: "Configuration" tab to import the configuration from the system

In this case the "Create" button is frozen because any local configuration created would have a different identifier from the one already present on the system site and could not be transferred.

The quickest way to restore a project configuration compatible with the system site configuration is to press the "From system" button. The following screen is displayed:

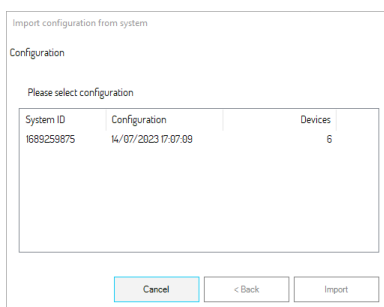


Figure 99: importing from system configuration

After selecting the only available configuration on the system, the "Import" button is enabled. Press the "Import" button to import the keys and the system configuration, as already described above.

Press the "OK" button, the "Site" tab restores the alignment:

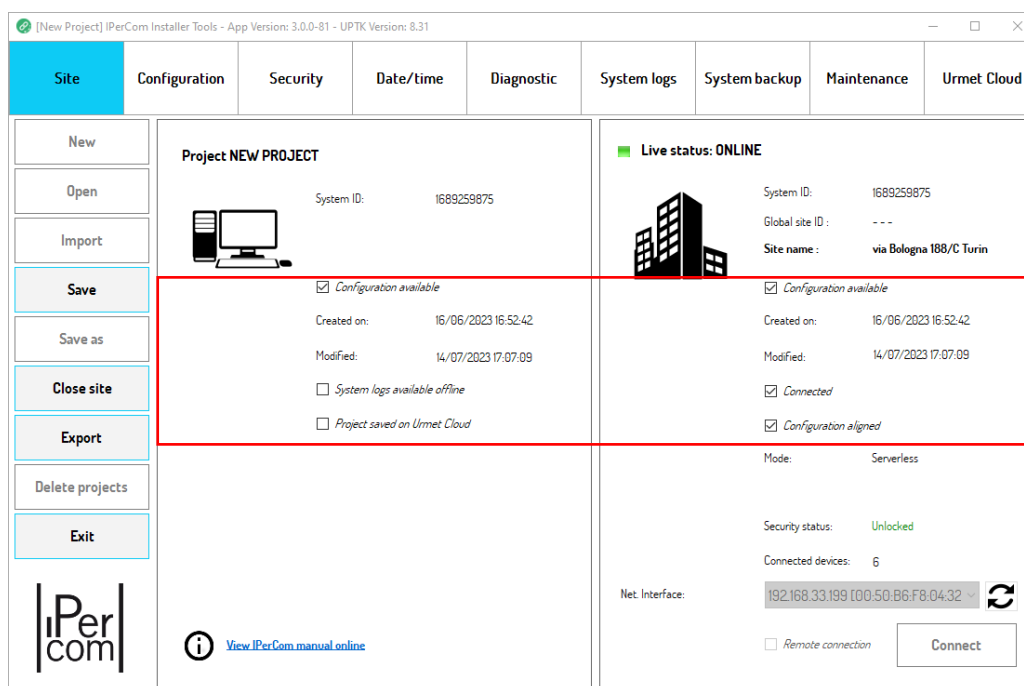



Figure 100: "Site" tab with project and system site aligned

The procedure of creating a new project without any configuration is mandatory if you want to change the configuration of a villa kit in iPerCloud mode with a 1060/21 entry panel. In this case, however, after having connected to the system and downloaded the configuration, to modify it it is necessary to set an installer password from the "Security" tab (see paragraph Security). With this password you can then access the configuration for any changes.

### 6.13 Systems with two configurations

Once the system configuration has been completed, it is good to lock the system (see section “[System block](#)”): in this way the installer can no longer have access to the system configuration except by means of the administrator password. Blocking the system is essential even in case of a wrong connection of a MAX, VOG<sup>7</sup> or Basic video door phone with a different configuration from the one present on the system. In fact (when the system is unlocked) if the configuration modification date of the connected device is more recent than that of the system configuration, the result is the loss of configuration for all the devices in the system. This is because in the presence of 2 different configurations, coming from unlocked systems, the more recent one prevails over the less recent one.

 In addition to the MAX, VOG<sup>7</sup> or Basic video door phones, the devices that can delete a system configuration are the Server 1060/1 and the Switchboard and the IPerCom Client applications.

If, on the other hand, the system is blocked, any device incorrectly connected to the system does not cause any loss of configuration: the system and the added device remain with their configuration. In this situation, after connecting to the system, *IPerCom Installer Tools* signals the presence of 2 different configurations, as shown in the figure:



Figure 101: message in case of devices/applications with different configurations

This situation is abnormal and must be fixed immediately by disconnecting the device added incorrectly.

Therefore, **before adding a new device on an already configured system (blocked and especially not blocked), it is good to make sure that it is not configured (i.e. with factory settings).**

## 6.14 System remote access

All the operations described above can also be carried out with the system in remote mode, that is without being physically connected to the system with your PC. This operating mode is possible if the following conditions are met on the system to which you need to connect remotely:

- at least one of the following devices is present: *Server 1060/1, Modular Calling Station with 1060/48, Entry Panel 1060/21, Entry Panel 1060/33, Entry Panel 1060/34, Video door phone 7" VOG<sup>7</sup> 1761/3x, Video door phone 5" VOG<sup>5+</sup> 1761/15-16-18-19, Video door phone 5" VOG<sup>5</sup> 1761/6, Video door phone MAX 1717/2x, 3x, 4x, Video door phone 7" Basic 1741/1-2-3, Door phone Miro 1160/3;*
- the system is connected to the Internet;
- the system has the remote access function enabled.



*The remote access function can be configured in the "Maintenance settings" section of the "System" tab of the configurator. For further details see the "[Maintenance Settings](#)" paragraph.*

Remote access is carried out via an already existing project with the same identifier as the (remote) plant site to which you want to connect.

This represents the most common use case: the installer, connected to the system with his PC, defines the configuration of the system itself; the relevant project remains available on *iPerCom Installer Tools* for any modifications, even remotely, by the installer himself.



**Authentication on Urmet Cloud is mandatory, so that the installer can remotely access a system.**

How to remotely access a system is now described in more detail.

**REMOTE ACCESS THROUGH ALREADY EXISTING PROJECT (WITH IDENTIFIER SAME AS THE REMOTE SYSTEM SITE)**

After starting *IPerCom Installer Tools* and opening the correct project with the "Open" button, the screen that appears is the following:

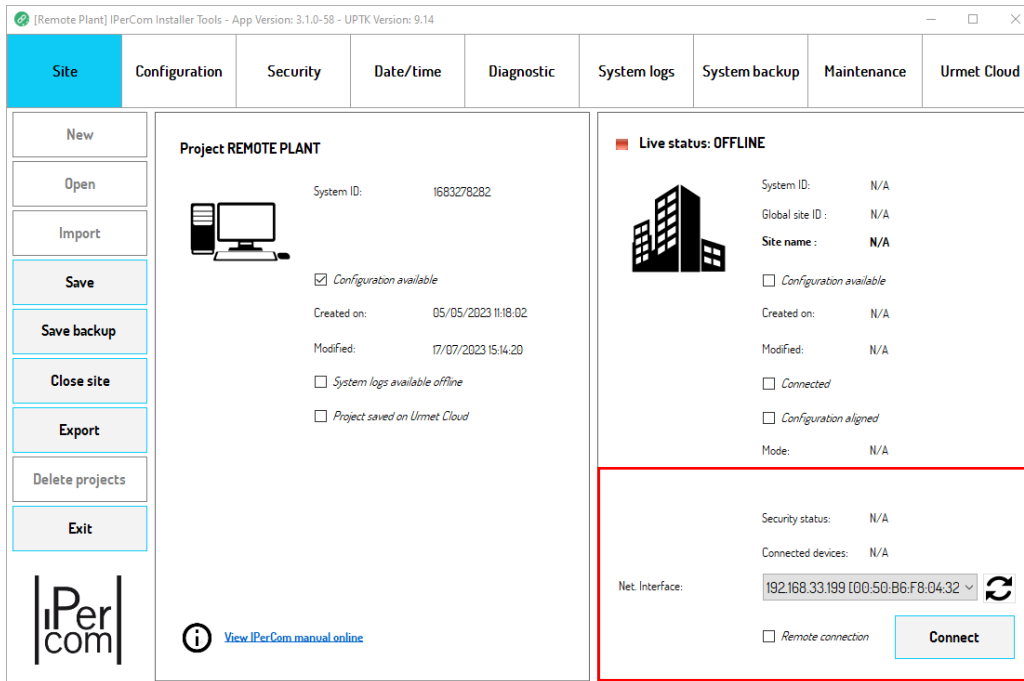


Figure 102: project with the same identifier as that of the plant site (remote)

At this point, in the red section of the above figure:

- select the network interface (IP address and MAC address) through which your PC connects to the remote system via the Internet;
- select the "Remote connection" item;
- press the "Connect" button.

The following window is displayed:

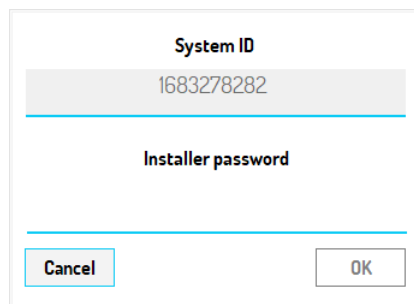


Figure 103: parameters for remote access with local identifier equal to that of the remote site

To complete remote access, only the installer password must be entered.



The "System id" field is already filled in and cannot be changed and is the same as the system id of the project previously opened.



If the installer password entered is incorrect, the following error message appears:

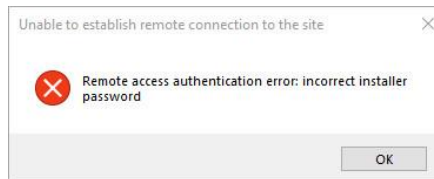


Figure 104: error message in case of incorrect installer password

After pressing the "OK" button (and after entering the administrator password if the system is locked), a window like the one below appears:

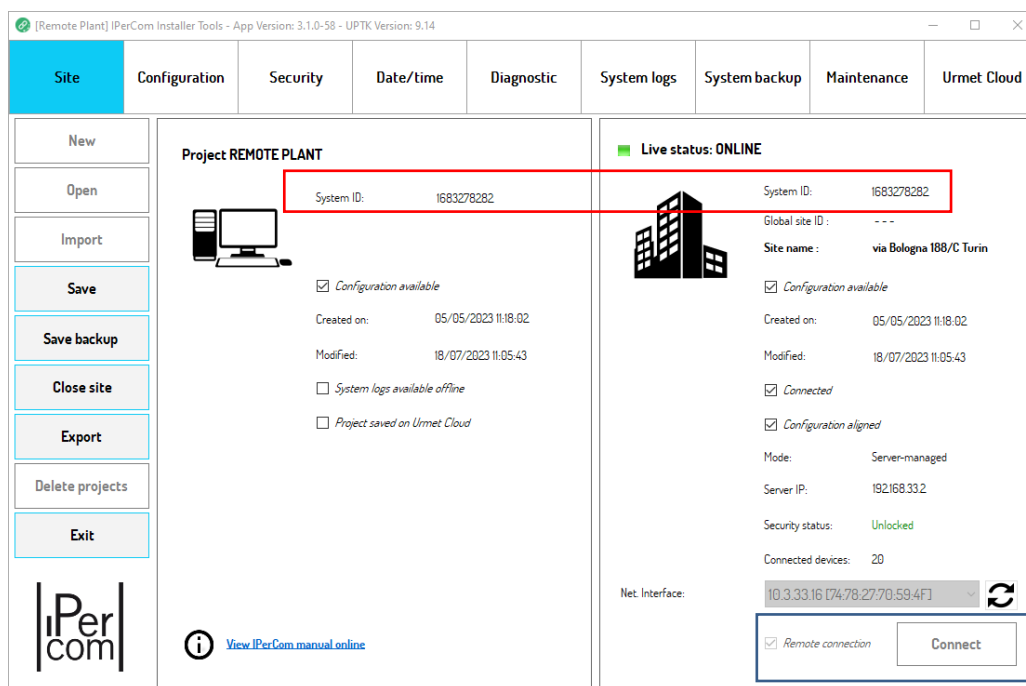


Figure 105: remote access done

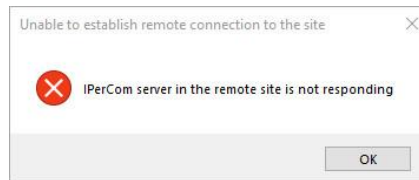
As you can see in the red box, the system identifier and that of the project are the same and the connection to the system is a remote connection (blue box).



The configuration may be aligned or misaligned: in the latter case it is advisable to align it with that of the remote system or the project, after which any changes can be made to the project and then remotely transferred to the system.



*If remote access has not been enabled, after entering the password and / or system identification, the following error message appears:*



*Figure 106: remote access not enabled by configurator*



*From version 3.1.0 of IPerCom it is no longer possible to connect remotely to a system with a project whose identifier is equal to zero.*



## 6.15 Other functions of IperCom Installer Tools

The other functions of *IperCom Installer Tools* concern the “Security”, “Date/Time”, “Diagnostic”, “System Log”, “System backup”, “Maintenance” and “Urmet Cloud” tabs.

The functions relating to these tabs are enabled based on the following events:

- opening a project using the “Open” button;
- connection to the site via the “Connect” button;
- alignment of the configuration between project and plant site;
- presence of one or more 1060/1 Server in the system.

The following table shows which of the above events must occur (symbol **V**) for the tab functions to be active (the symbol **---** indicates that the relevant condition is not mandatory):

Tab	Condition			
	Project opening	Site connection	Configuration alignment	System with server
Security	V	V	V	---
Date/Time	V	V	---	---
Diagnostic	V	V	V	---
System Log	V	V	V	V
System backup	V	V	---	V
Maintenance	V	V	---	---
Urmet Cloud	---	---	---	---

Table 5: Activation condition for IperCom Installer Tools tabs

The “Urmet Cloud” tab is the only one that is always active regardless of whether the above conditions are verified or not. The functions of this tab are mainly linked to the installer's access to the Urmet cloud and will be explained in detail in the next paragraph.

### 6.15.1 “Urmnet Cloud” tab

The “*Urmnet Cloud*” tab allows you to authenticate on the Urmnet cloud. Authentication on Urmnet Cloud allows you to:

- save your projects on a virtual storage space,
- transfer a configuration with IPerCloud apartments to a system,
- use the CallMe Manager application to configure call forwarding,
- log in remotely to another system,
- pre-activate the licenses,
- view the history of pre-activated license packages,
- activate IPerCloud test mode,
- manage site access permissions (for the building manager via the *CallMe Manager* application or for another installer)

The activation of the test mode and the management of access authorizations is also linked to the opening of a project, the connection to the system and appropriate settings made via the configurator.

The following paragraphs will explain in detail how to do the above.

#### 6.15.1.1 Urmnet Cloud access

If you are not logged into Urmnet Cloud when *IPerCom Installer Tools* is started, this can be done later from the “*Urmnet Cloud*” tab, which appears as shown below:

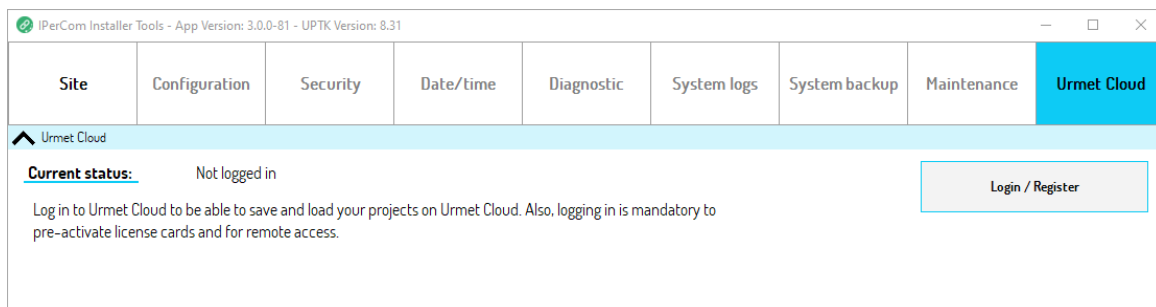


Figure 107: access to the Urmnet cloud not performed

In the **Urmnet Cloud** section the "Login/Register" button allows you to create an account for registering with Urmnet Cloud or to use one already created previously. If you have never accessed Urmnet Cloud, the screen that appears is the following:

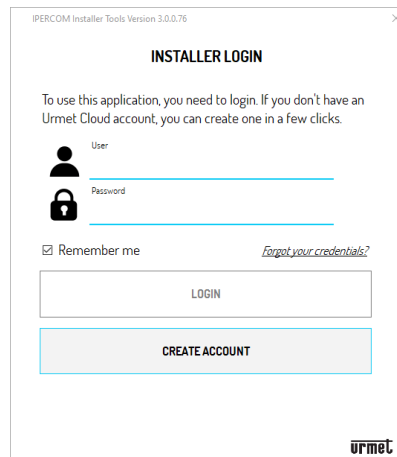


Figure 108: access to Urmnet Cloud via account creation or login

The "CREATE ACCOUNT" button allows you to create a new account (see [Urmnet Cloud authentication](#) paragraph).



*If you are not connected to Urmnet Cloud it is not possible to configure IPerCom systems in IPerCloud mode.*

If, however, Urmnet Cloud has already been accessed at least once and the "Remember me" field is selected, the above screen appears as shown below:

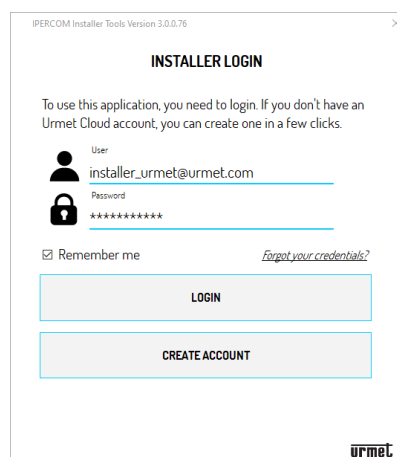


Figure 109: access to Urmnet Cloud at least once with an account already created

After logging in with the "LOGIN" button, the "Urmnet Cloud" tab presents an additional section, as described below.

### 6.15.1.2 Urmnet cloud access performed

The “Urmnet Cloud” tab appears as shown below:

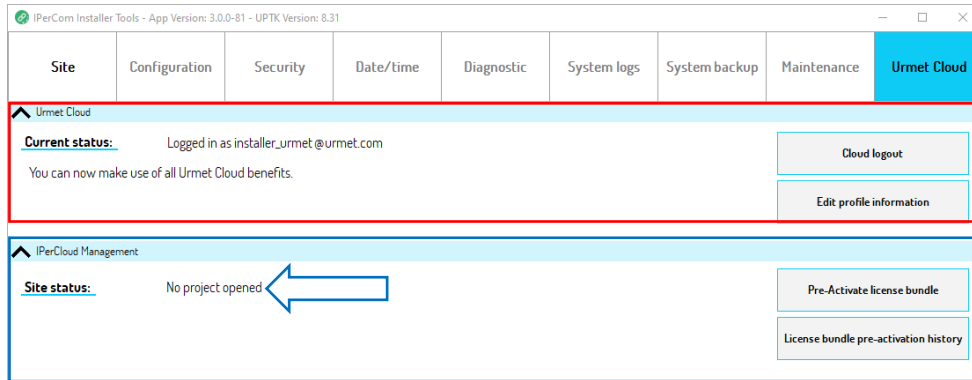


Figure 110: access to the Urmnet cloud completed

The **Urmnet Cloud** section (red box) shows the user with whom access was made and shows 2 buttons that allow you to:

- log out from Urmnet Cloud;
- modify the data of your user profile entered during registration (see [Urmnet Cloud authentication](#) paragraph).

The **iPerCloud Management** section (blue box) instead shows 2 buttons through which the installer can pre-activate the license bundles and view the history of the pre-activated license bundles (see paragraph [Pre-activation license bundle and pre-activation license bundle history](#)). The section in question also reports the information that no site has been loaded (blue arrow).

### 6.15.1.3 Urmnet Cloud access and opening of a project

After opening a project saved on your PC or on the cloud, the “Urmnet Cloud” tab appears as shown below:

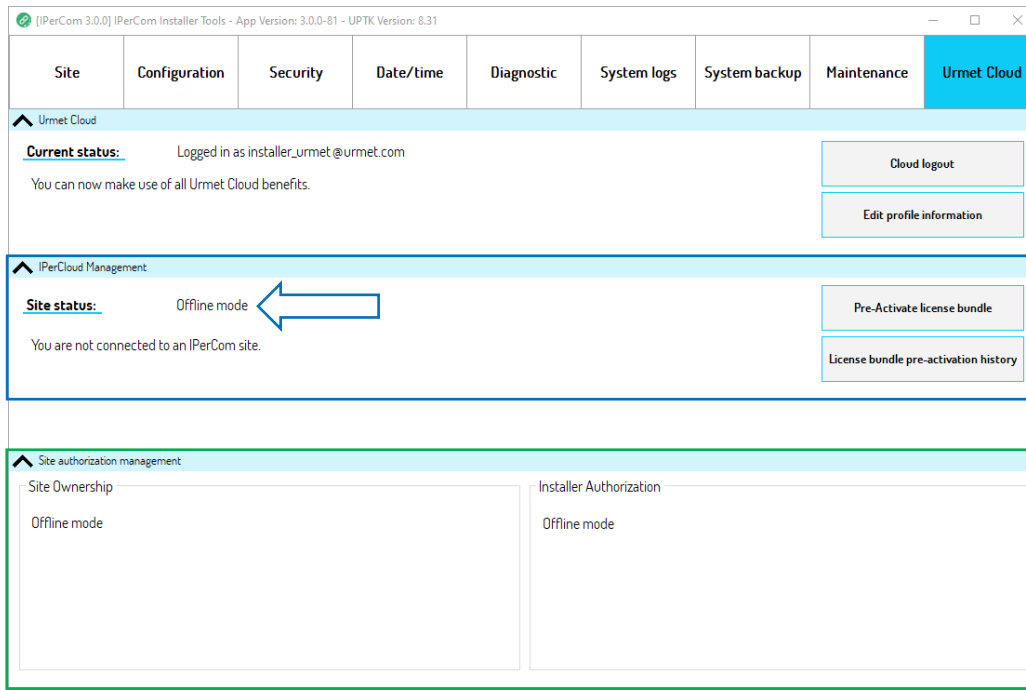


Figure 111: access to the Urmnet cloud performed with the opening of a project

The **Urmnet Cloud** section has not changed compared to before.

The **IPerCloud Management** section (blue box) shows the “Offline mode” indication: this means that you are not yet connected to any site.

The **Site Authorization Management** section (green box) shows two subsections: **Site Ownership** and **Installer Authorization**. Both show the “Offline mode” indication, meaning that you are not yet connected to any site. The usefulness of this new section will be explained in the next paragraph, after connecting to the site.

#### 6.15.1.4 Urmnet Cloud access, opening of a project and connection to a site

After connecting to the system (with the configuration aligned with that of the project), the "Urmnet Cloud" tab appears as shown below:

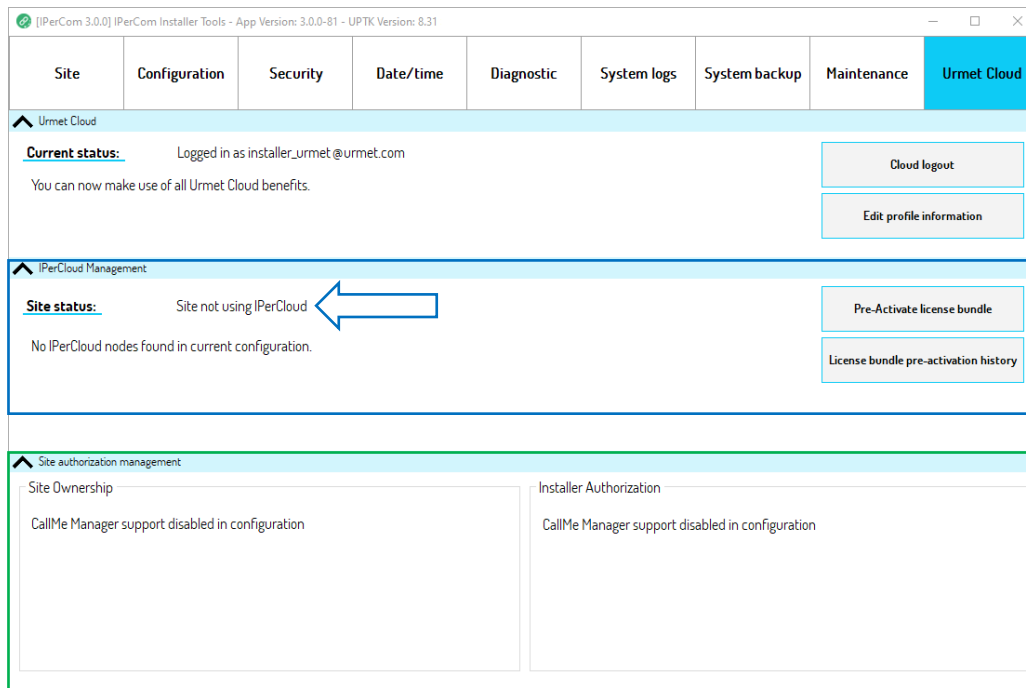


Figure 112: access to the Urmnet cloud performed with the opening of a project and connection to the site

The **Urmnet Cloud** section has not changed compared to before.

The **IPerCloud Management** section (blue box) shows the indication "The site does not use IPerCloud": this means that no IPerCloud apartment (or more generally node) has been detected.





*It is necessary that the configuration between the project and the plant site is aligned so that the presence or absence of one or more IPerCloud nodes is reported in the **IPerCloud Management** section. If this is not the case, the non-aligned configuration information is reported.*

The **Site Authorization Management** section (green box) shows in both subsections the indication *CallMe Manager* support disabled in configuration: this means that *CallMe Manager* support is not enabled in the configurator.

### 6.15.1.5 CallMe Manager support enabled with or without IPerCloud apartments

In IPerCom systems without IPerCloud apartments, the use of the *CallMe Manager* application is optional and is recommended for those medium/large home topologies where the figure of the building manager is required. In this case the application is used to generate the QR code, which the building manager will send via email to the end user: the latter, by scanning the QR code via the *CallMe* app, will be able to activate the call forwarding function on their smartphone/tablet. If, however, the IPerCom system is in IPerCloud mode, the use of the application is mandatory to associate the license with the apartment and therefore generate the QR code to activate the call forwarding function on the end user's smartphone/tablet.

 To enable or disable *CallMe Manager* support, see the [Call Forwarding Settings](#) paragraph relating to the configurator.

 To use the *CallMe Manager* application you must first authenticate to *Urmnet Cloud*. If this is not the case, *IPerCom Installer Tools* reports the anomaly with an error during configuration distribution.

If the IPerCom system is not in IPerCloud mode but the use of the *CallMe Manager* application is required, the "Urmnet Cloud" tab appears as shown below:

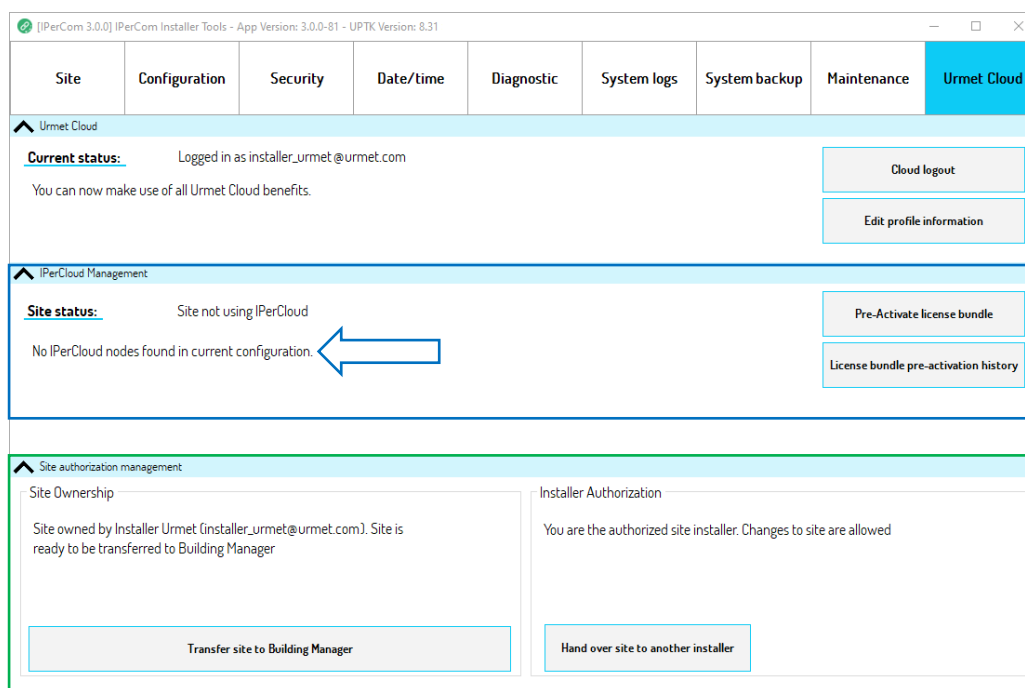


Figure 113: access to the Urmnet cloud carried out with *CallMe Manager* support enabled and no IPerCloud node

The **Urmnet Cloud** section does not show any changes.

The **IPerCloud Management** section (blue box) shows the indication "The site does not use IPerCloud": this means that no IPerCloud apartment has been detected.

The **Site authorization management** section concerns the possibility of:

- transfer the site from an installer to a condominium administrator for configuring the call forwarding function;
- transfer the site from one installer to another installer.

For further details on the 2 points above, see the [Site authorization management](#) paragraph.

If, however, the IPerCom system is in IPerCloud mode, the "Urmet Cloud" tab appears as shown below:

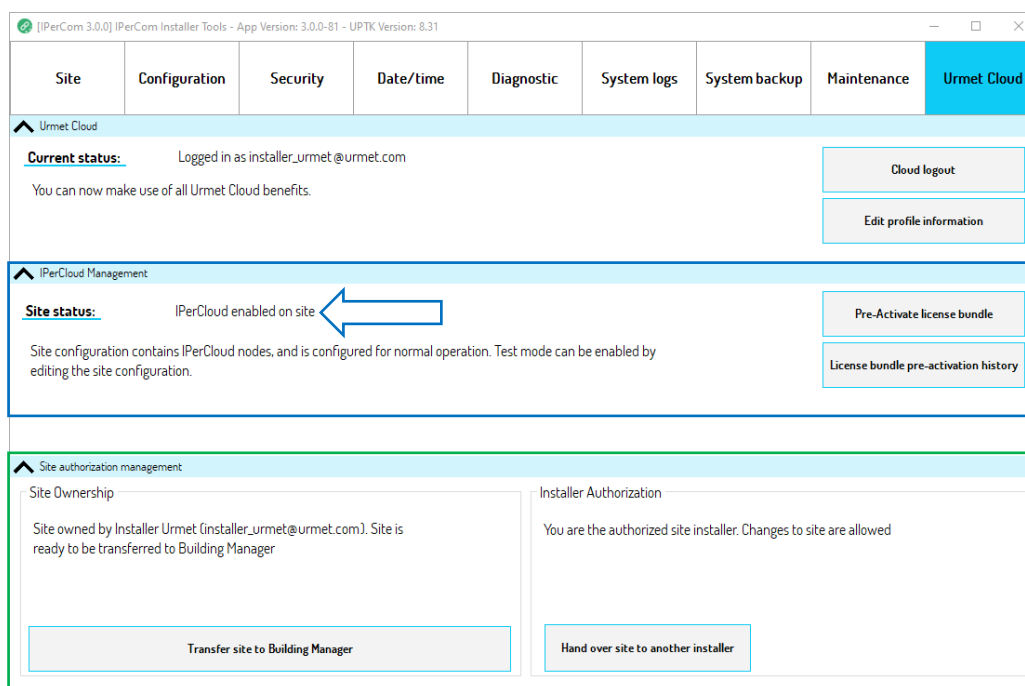


Figure 114: access to the Urmet cloud carried out with CallMe Manager support enabled and at least one IPerCloud node

The **Urmet Cloud** and **Site authorization management** sections have not changed compared to before.

The **IPerCloud Management** section (blue box) shows the indication "IPerCloud enabled on the site": this means that one or more IPerCloud apartments have been detected.

The **Site authorization management** section has not changed compared to before (system without IPerCloud apartments).

So, regardless of the presence of IPerCloud apartments, if *CallMe Manager* support is enabled, you can:

- transfer the site ownership from an installer to a building manager for configuring the call forwarding function,
- transfer the site ownership from one installer to another installer.

These two features will be described in the next paragraph [Site authorization management](#).





**From version 3.1.0 it is possible to transfer ownership of the site from an installer to a building manager or to another installer even if CallMe Manager support is disabled.**

### 6.15.1.6 Site authorization management

If CallMe Manager support has been enabled from the *configurator*, the **Site Authorization Management** allows to:

- transfer the site ownership from an installer to a building manager (for generating letters in pdf format for the call forwarding function),
- transfer the site ownership from one installer to another installer,

in the ways indicated below.

#### 6.15.1.6.1 Transfer of the ownership of the site from installer to a building manager

If the ownership of the site is transferred to the building manager, this means that the installer has completed the configuration part of the system via *IPerCom Installer Tools* and consequently the building manager can generate the letters in pdf format via the *CallMe Manager* application for call forwarding function. To start the ownership transfer procedure, the installer must press the “*Transfer site to Building Manager*” button in the section **Site authorization management** ---> **Site Ownership**:

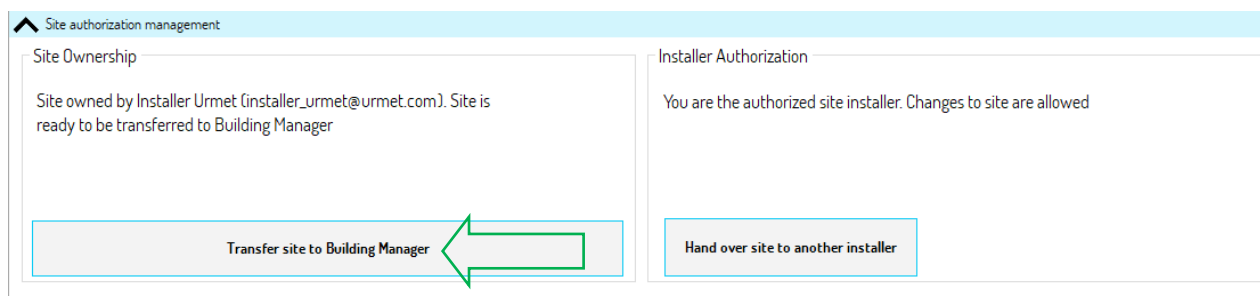


Figure 115: button to transfer site ownership to the building manager

Pressing this button, the following dialog box is shown:

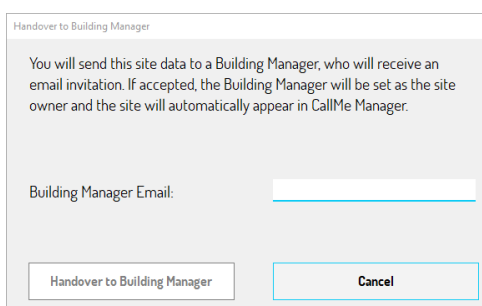


Figure 116: dialog box to transfer the site to the building manager

It is necessary to enter the e-mail address that the building manager previously communicated to the installer:

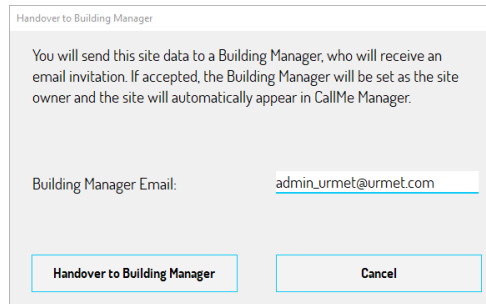


Figure 117: building manager email entered

Pressing the “*Handover to Building Manager*” button, an invitation e-mail is sent to the building manager and the correct outcome of the operation is confirmed by the following dialog box:

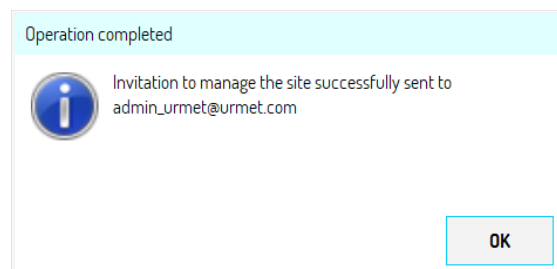


Figure 118: correct outcome of the invitation to the building manager

The content of the email sent to the administrator appears as follows:

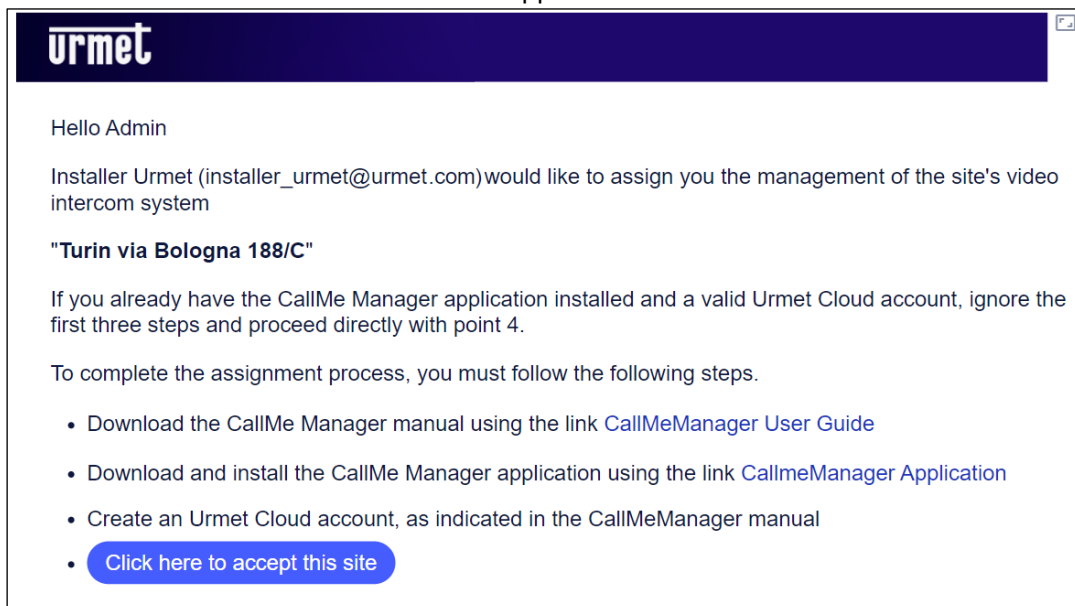

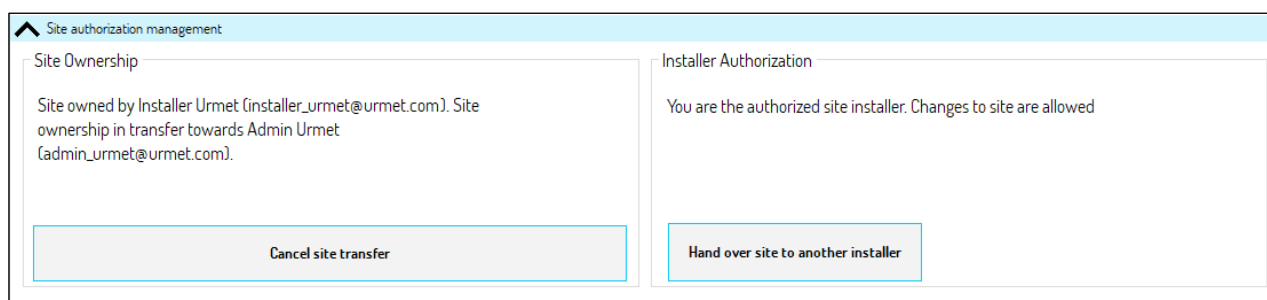


Figure 119: content of the email sent to the building manager

It is necessary that the e-mail address communicated by the building manager is associated with an Urmet Cloud account through registration on the *CallMe Manager* application. If this is not the case, from the content of the same e-mail it is possible to download the *CallMe Manager* application and the related manual, then install the application on your PC and create an Urmet Cloud account (using the e-mail address communicated to the installer).

 *If the e-mail address communicated by the building manager is already associated with an Urmet Cloud account, the name of the building manager entered when creating the account appears at the top of the email content (green arrow); otherwise, the email address will appear.*

After sending the invitation e-mail, the following screen appears in the Urmet Cloud tab of *IPerCom Installer Tools* relating to the section **Site Authorization Management** ---> **Site Properties**:



*Figure 120: invitation not yet accepted by building manager*

At this point there are 2 possibilities listed below.

## THE BUILDING MANAGER ACCEPTS THE INVITATION

In the invitation email the building manager presses the link highlighted in blue at the bottom of the content of the same email to confirm the site transfer operation:

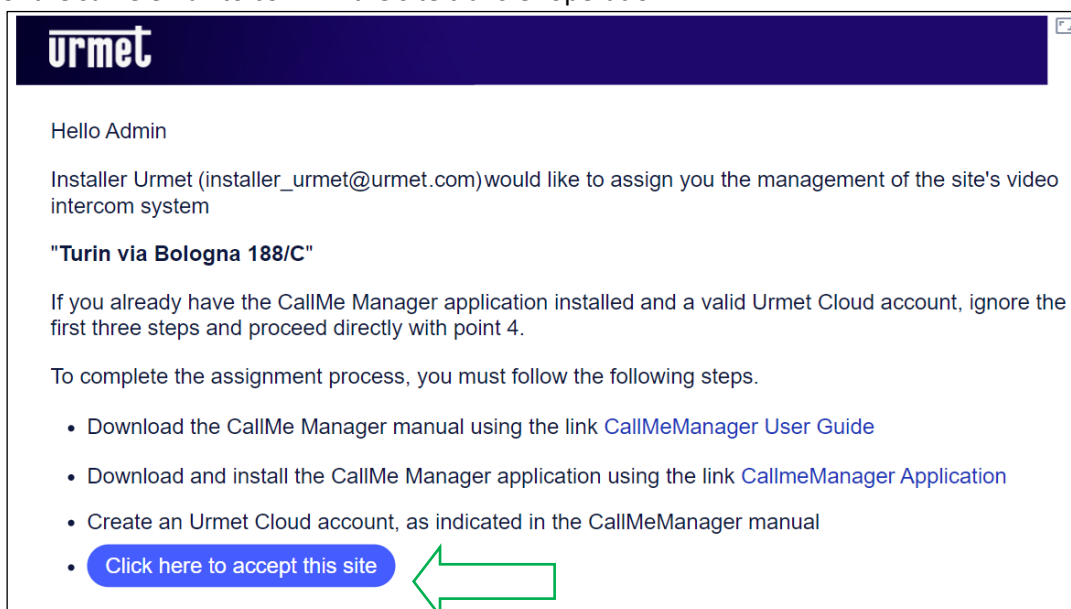


Figure 121: link to accept the transfer of ownership of the site

The installer receives a notification via email that the building manager has accepted the transfer of ownership of the site.

In *IPerCom Installer Tools* the transfer of site ownership is notified as follows (green box):

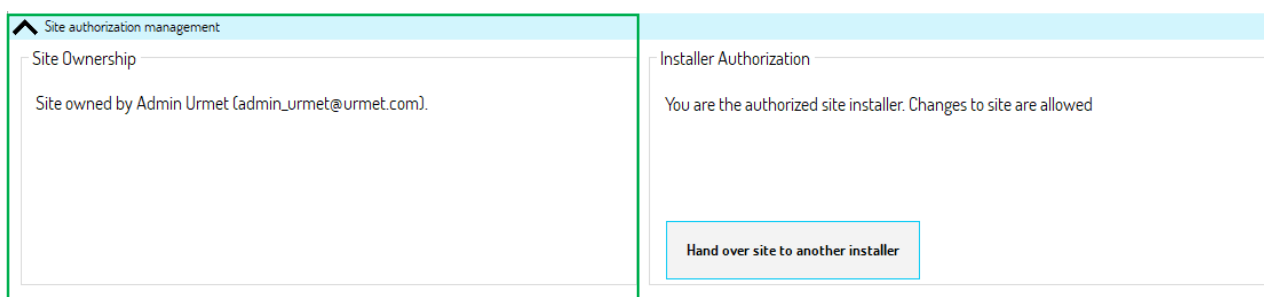





Figure 122: installer invitation accepted


Once the invitation has been accepted, the building manager, by accessing the *CallMe Manager* application, can view the acquired site and configure the call forwarding function (for further details see the paragraph [Configuring the call forwarding function in IPerCom systems in IPerCloud mode](#) or [Configuring call forwarding function with CallMe Manager application support](#)).


 *When an installer creates a site, he is also the building manager and therefore, by authenticating on the CallMe Manager application with the same credentials with which he logged in to IPerCom Installer Tools, he can view the same site. After the transfer of ownership to the building manager, viewing on the CallMe Manager application will no longer be possible and the installer can only make changes to the configuration and distribute them to the system via IPerCom Installer Tools.*


In the case of IPerCom systems in IPerCloud mode, it is recommended to transfer the site to the building manager after the installer has assigned the licenses to the apartments: in this way, the building manager's only task will be (as in the case of systems without IPerCloud apartments) to print the letters for the end users for configuring call forwarding and not worry about associating the licenses with the apartments.


 *If a building manager also wants to take care of associating the licenses with the apartments, the installer can transfer the site to him after completing the configuration, carrying out the test mode, and the pre-activating the licenses.*

 *After transferring ownership of the site to the building manager, the installer can still make changes to the system configuration and apply them to the system itself and the building manager is able to view these changes on the CallMe Manager application.*

 *Make sure that the configuration between the project and the plant site is aligned before transferring the site from installer to building manager. If this were not the case, the building manager would not see on the CallMe Manager application all changes made by the installer.*

 *During the transfer, it is necessary that any apartment stations are installed in the apartments and connected to the system. If this were not the case, the apartments, whose apartment stations are not connected to the system, will not appear in the topological structure transferred to the building manager in the CallMe Manager application.*

 *The 2Voice apartments do not appear in the topological structure displayed by the building manager in the CallMe Manager application.*

 *For further details on using the CallMe Manager app, see the paragraph [Configuring the call forwarding function in IPerCom systems in IPerCloud mode](#) or [Configuring call forwarding function with CallMe Manager application support](#).*

## THE INSTALLER CANCELS THE INVITATION

If the installer presses the “Cancel site transfer” button ([Figure 120](#)), the following window appears:

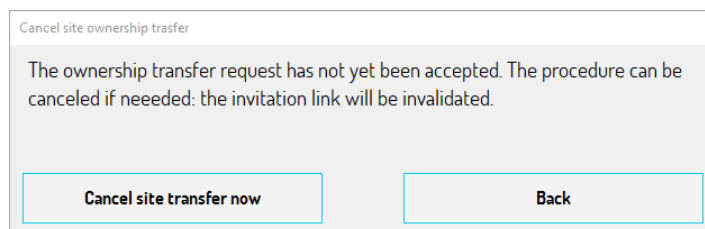


Figure 123: cancel of the transfer

The “Cancel site transfer now” button allows you to cancel the transfer request (only if the building manager has not already clicked on the site acceptance link). The correct outcome of the operation is confirmed by the following dialog box:

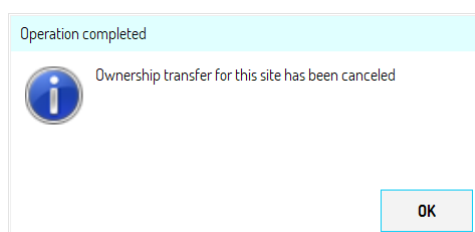


Figure 124: transfer cancelled

An email notifying the cancellation is sent to the building manager and on *IPerCom Installer Tools* the installer has the possibility to transfer the site again to another building manager.

### 6.15.1.6.2 Transfer of the site ownership to another installer

The installer who created the project and the related configuration is the only “authorized” installer capable of connecting to the system, making changes to the configuration, and applying them to the system: for safety reasons, any other installer who has not accessed to Urmet Cloud and is different from the authorized one cannot connect to the system. In this case, in fact, *IPerCom Installer Tools* reports the following messages:

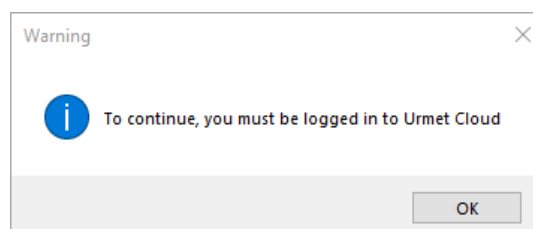


Figure 125: message in case of connection to a system without being connected to Urmet Cloud

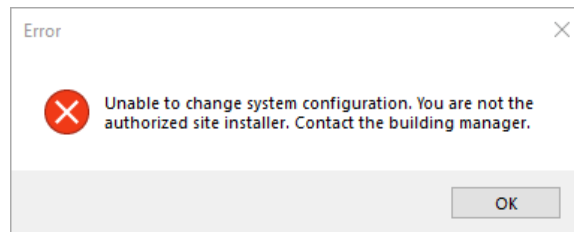


Figure 126: message in the event of connection to a system by an unauthorized installer

However, it could happen that another installer needs to make changes to the system configuration. To do this, the installer who created the site can transfer it to another installer via the *“Hand over site to another installer”* button in the **Site Authorization Management** section ---> **Installer Authorization**:

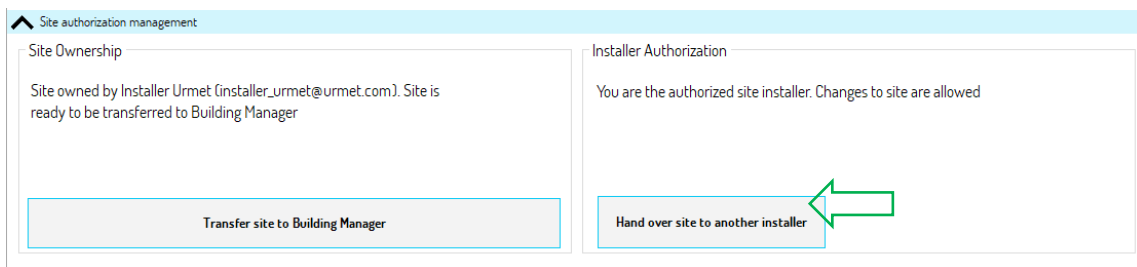


Figure 127: transfer to another installer

The transfer methods are the same as those seen for transferring the site from an installer to a building manager, that is an invitation is sent via e-mail from the old installer to the new installer, who must accept the invitation.

When the new installer accepts the invitation by pressing the relevant link, he will be the only one able to make changes to the system.

The *“Hand over site to another installer”* button has two operating modes depending on whether the site has already been transferred to a building manager or not.

### SITE NOT YET TRANSFERRED TO A BUILDING MANAGER

If the site has not yet been transferred to a building manager, the installer who created the project is also the site building manager: this means that the installer, by authenticating on the *CallMe Manager* application with the same credentials with which he logged in to *IPerCom Installer Tools*, is able to view the site. In this situation the “*Hand over site to another installer*” button displays the following dialog box:

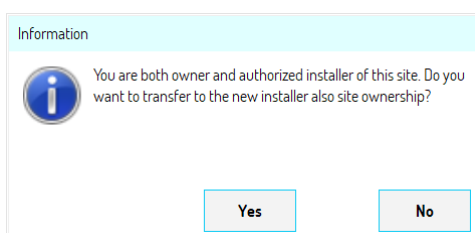


Figure 128: dialog box following transfer to another installer

In practice, it is possible to choose whether to transfer only the ownership of installer to the new person (“*No*” button) or also that of building manager (“*Yes*” button).

By pressing the “*Yes*” button, a window appears where you can enter the e-mail address through which to invite the new building manager/installer. Once the invitation has been accepted, the new installer will be not only the installer but also the building manager, while the old installer will be notified that he will no longer be able to make changes to the system.

The content of the e-mail will be of this type:

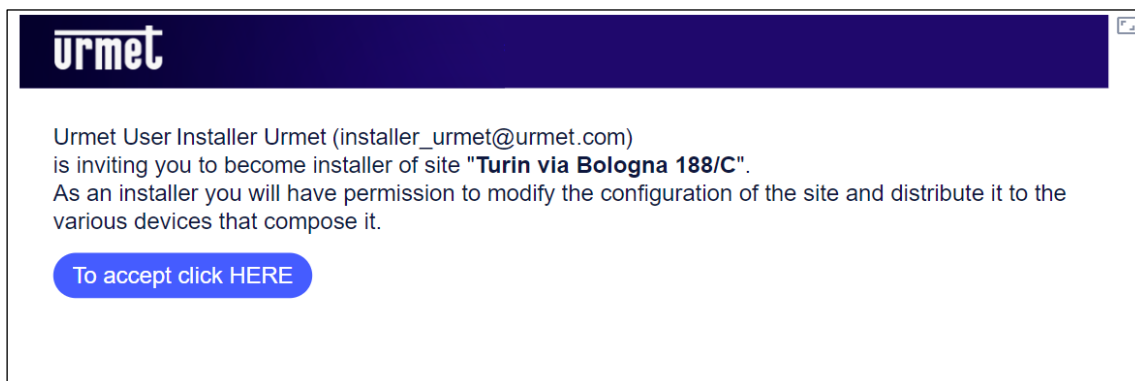


Figure 129: content of the email sent to the new installer

To accept the invitation, you need to press on the link highlighted in blue.



For example, if “*installer\_1\_urmet*” transfers the building manager and installer properties of the site to “*installer\_2\_urmet*” and “*installer\_2\_urmet*” accepts the invitation, when “*installer\_1\_urmet*” connects to the same system, the following appears in the “*Urmet Cloud*” tab (box in green):

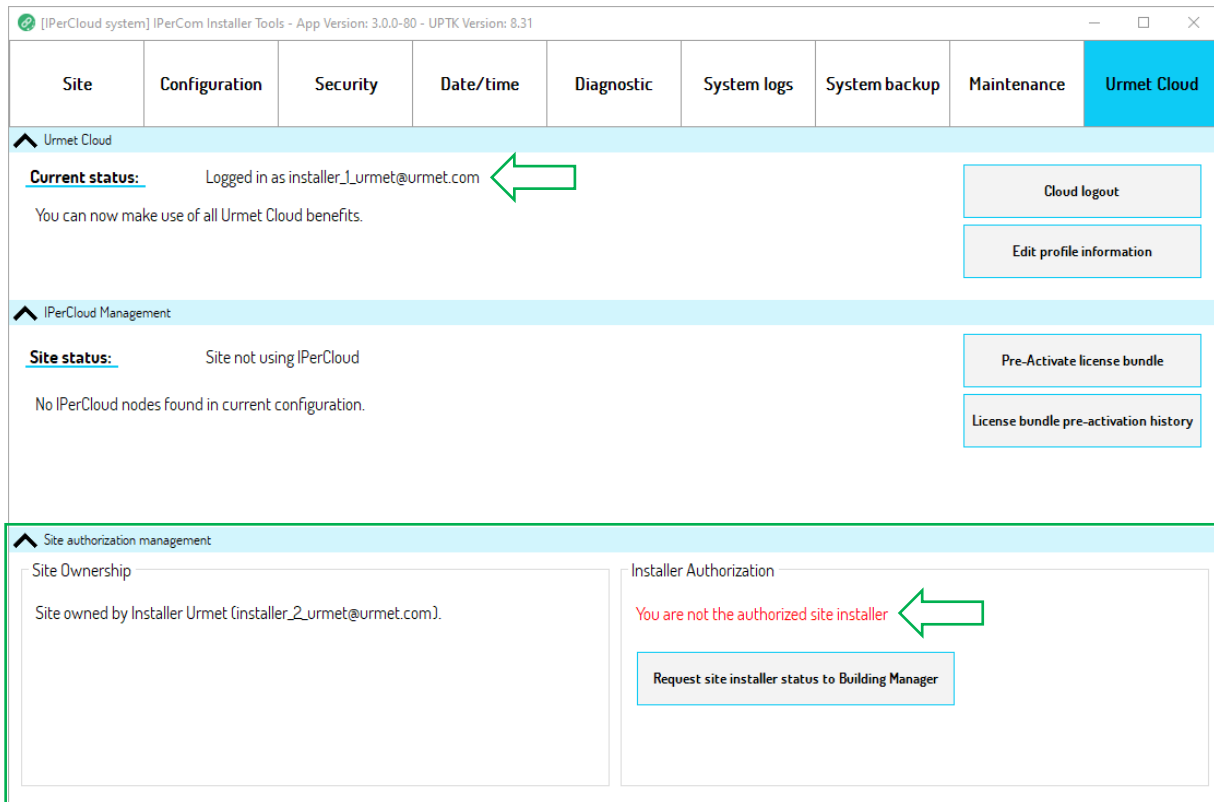


Figure 130: not authorized installer

As you can see, “*installer\_1\_urmet*” is no longer authorized to make changes to the plant site and must ask the new building manager/installer for authorization via the “*Request site installer status to Building Manager*” button. Furthermore, the site is owned by “*installer\_1\_urmet*”.

On the contrary, “*installer\_2\_urmet*” is the new building manager/installer of the system as shown below:

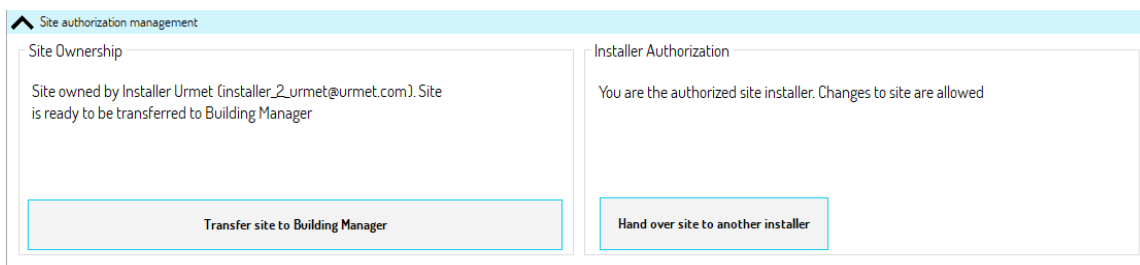


Figure 131: site transferred to another building manager/installer

This means that “*installer\_2\_urmet*” can make changes both through the *IPerCom Installer Tools* application (to modify the system configuration) and through the *CallMe Manager* application (to configure the call forwarding function).

However, if you press the “No” button in [Figure 128](#), the procedure remains identical to what is reported above with the only difference that the new installer will not have building manager functions. For example, if “*installer\_1\_urmet*” transfers only installer ownership of the site to “*installer\_2\_urmet*” and “*installer\_2\_urmet*” accepts the invitation, when “*installer\_1\_urmet*” connects to the same system, the following appears in the “*Urmet Cloud*” tab:

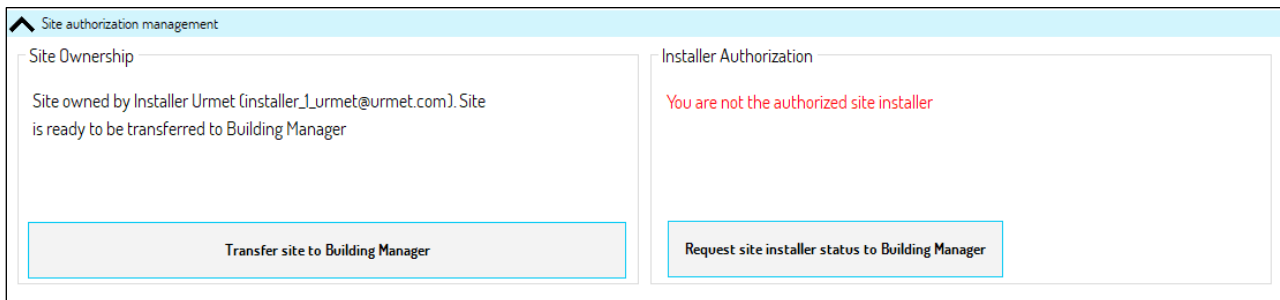


Figure 132: Urmet Cloud user as site building manager without installer ownership

As you can see, “*installer\_1\_urmet*” is no longer authorized to make changes to the plant site but remains the owner of the site. On the contrary, “*installer\_2\_urmet*” can make changes to the plant site but is not its building manager:

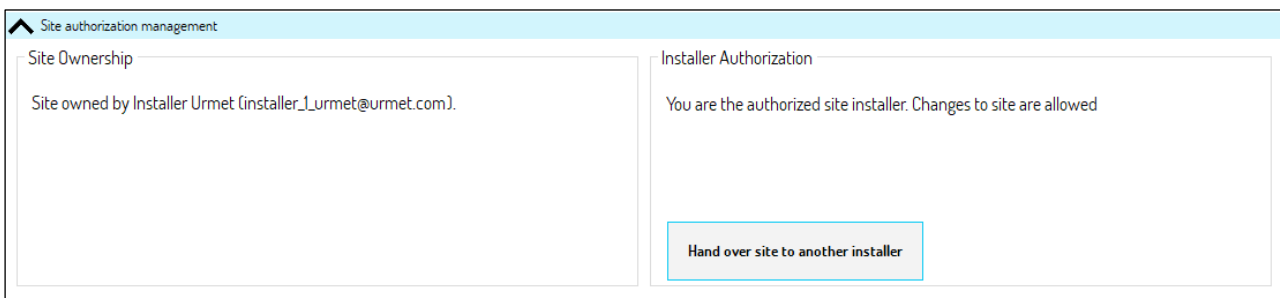


Figure 133: Urmet Cloud user as site installer without building manager ownership

This means that “*installer\_1\_urmet*” can make changes via the *CallMe Manager* application to configure the call forwarding function while “*installer\_2\_urmet*” can make changes via the *IPerCom Installer Tools* application to change the configuration.



Even for the change of installer it is possible to cancel the transfer procedure, in the same way as for the transfer to administrator.

### SITE ALREADY TRANSFERRED TO A BUILDING MANAGER

If the ownership of the site is transferred to the building manager, this means that the installer has completed the configuration part of the system using *IPerCom Installer Tools* and consequently the building manager can begin to configure the call forwarding function via the *CallMe Manager* application.

For example, if “*installer\_urmet*” transfers the site to the building manager “*admin\_urmet*” and “*admin\_urmet*” accepts the invitation, the following appears in the “*Urmet Cloud*” tab of *IPerCom Installer Tools* (the login to Urmet Cloud was done with the user “*installer\_urmet*”):

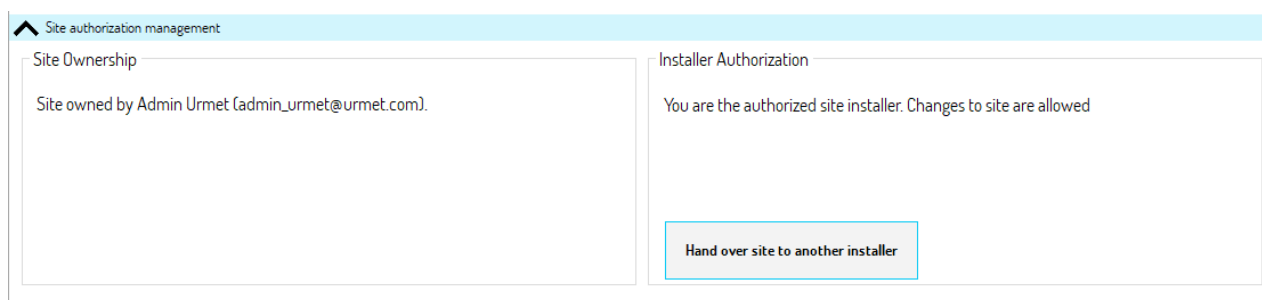


Figure 134: transfer site to the building manager

In this case pressing the button “*Hand over site to another installer*” the following window appears:

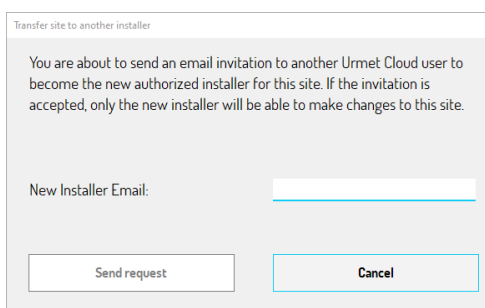





Figure 135: window to transfer the site to another installer

In this case, only the ownership of installer is transferred to the new subject and not that of building manager which remains with the subject “*admin\_urmet*”; on the contrary, the “*admin\_urmet*” subject will only have the ownership of building manager and not that of installer, therefore he will be able to make changes to the site only via the *CallMe Manager* application.

### 6.15.1.7 IPerCloud Test Mode

The IPerCloud test mode is useful to check that the call from any calling station arrives correctly at an IPerCloud test apartment (that is, the call arrives to *CallMe* app). In this way the installer avoids to purchase specifically a license bundle to carry out installation tests (thus also avoiding the procedure of pre-activating the license bundle, transferring the site to a building manager, activating the license bundle, assigning a license to an apartment, and printing the letter).

-  The IPerCloud test mode must be enabled from the "System" tab of the configurator (see [Call Forwarding Settings](#)).
-  Once enabled, it is necessary to have at least one apartment in IPerCloud mode in the configurator, for the **IPerCloud Management** section of the "Urmnet Cloud" tab to display the relevant test mode button.
-  It is possible to activate the IPerCloud test mode only if all the requirements for creating an IPerCom system in IPerCloud mode are met on the system. For all details see paragraph [System IPerCom in IPerCloud mode](#).

Therefore, if the test mode has been enabled in the *configurator* and if there is at least one IPerCloud apartment in configuration, the **IPerCloud management** section of the "Urmnet Cloud" tab appears as shown in the figure (red box):

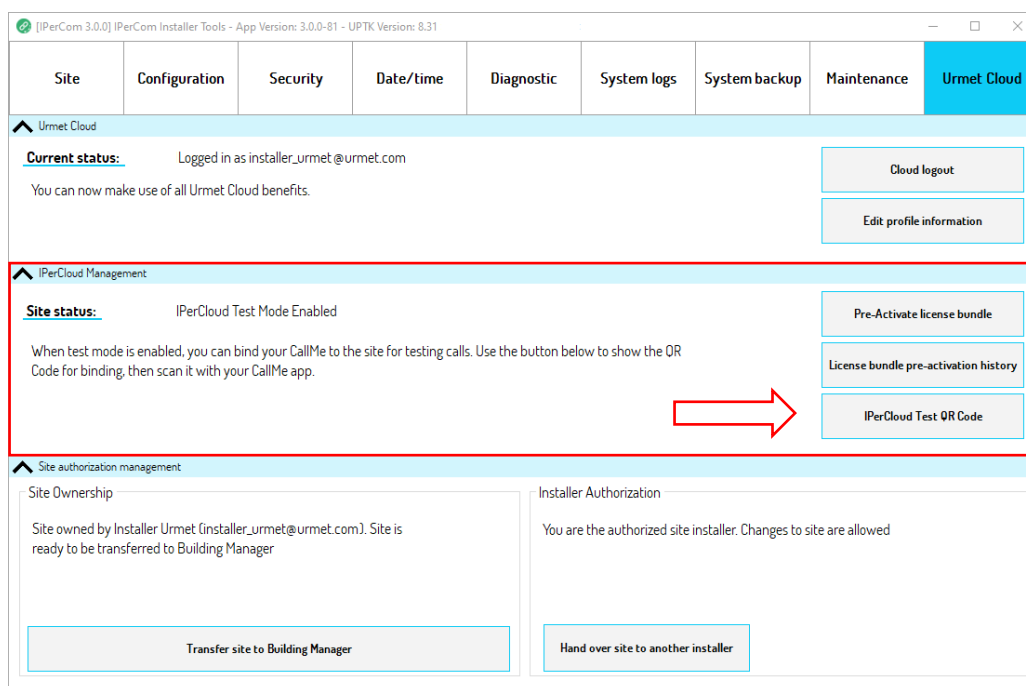


Figure 136: IPerCloud test mode enabled

To carry out the IPerCloud test mode, the installer must have downloaded, installed, and started the *CallMe* app on his smartphone/tablet.



The fundamental steps for carrying out the test mode with the CallMe app will be shown below. For all more detailed information relating to the use of the CallMe app see the related [booklet](#) on site [www.urmet.com](http://www.urmet.com).

To use the CallMe app, simply log in with the same account used on IPerCom Installer Tools. Once logged in, this screen appears:

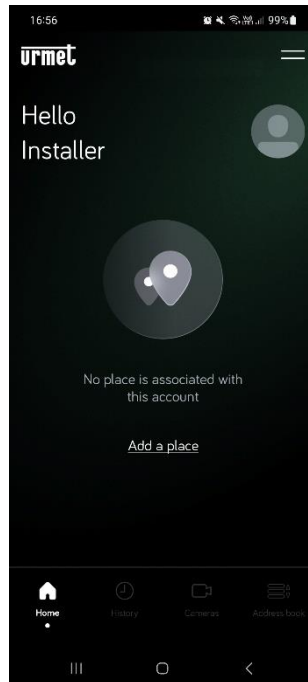


Figure 137: CallMe app home page

Pressing the “Add a place” button the following screen appears:

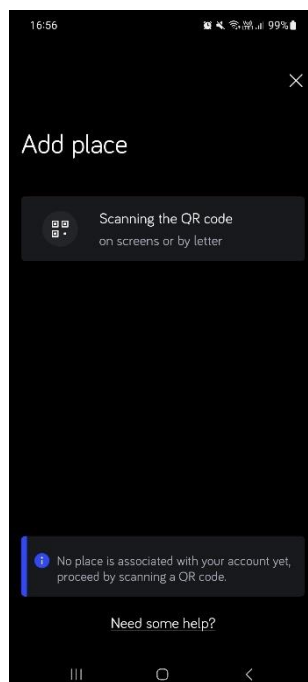


Figure 138: add of a place

Press the “*Scanning the QR code*” button to start the QR code reader application.

Then press the “*IPerCloud Test QR Code*” button displayed on *IPerCom Installer Tools*. The following screen appears:

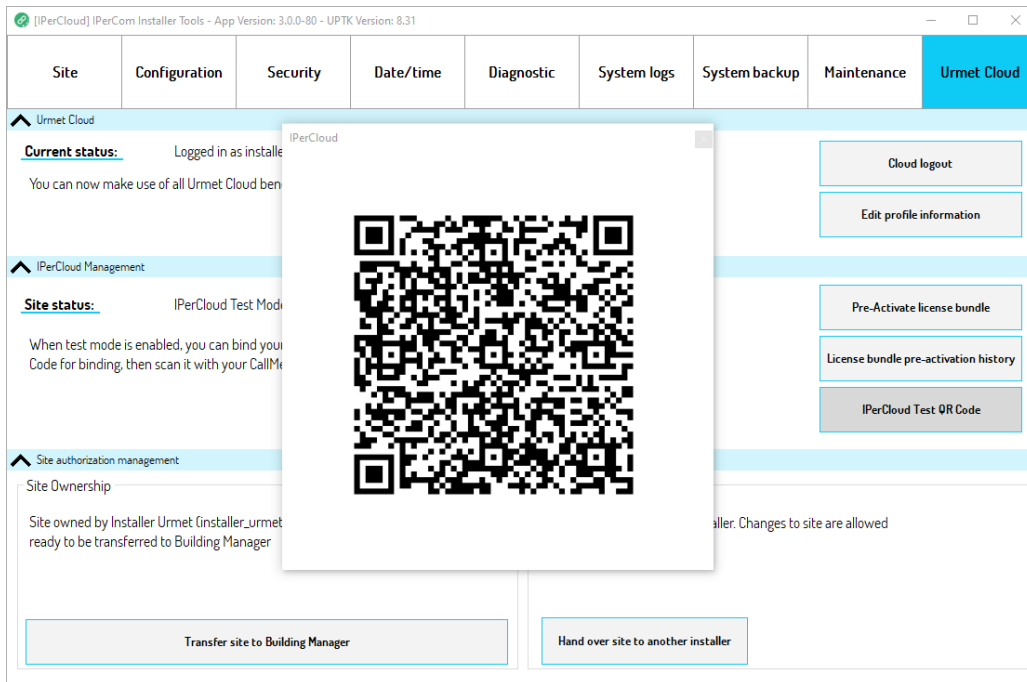


Figure 139: scan of QR code in test mode

Then with app *CallMe* scan the QR code displayed on the PC where the *IPerCom Installer Tools* application is installed. After scanning the QR code, the following screen will appear on your smartphone/tablet to indicate that the place has been added correctly:

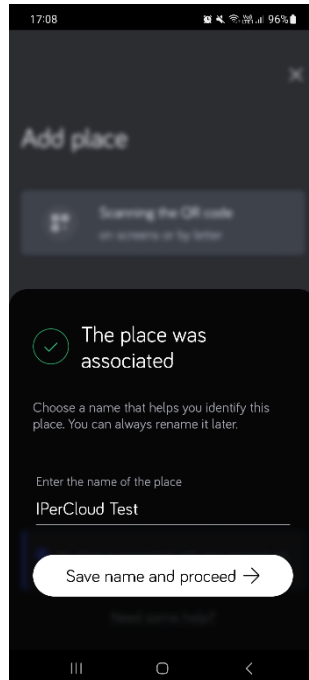


Figure 140: place added

The default name given to the place is "*IPerCloud Test*" but it is possible to rename it (even later): at this point the *CallMe* app has been associated with a (not real) *IPerCloud* test apartment. The installer can therefore make a call from any calling station to the *IPerCloud* test apartment: in fact, on all calling stations with display the relevant address books show only the name "*IPerCloud Test*" while calling stations with buttons call the "*IPerCloud Test*" apartment (from any button).



*Address books present on the calling stations with displays will appear again after disabling the test mode from the configurator.*

In test mode the installer can only do the following:

- call the test *IPerCloud* apartment from any calling station,
- check that the call arrives to the *CallMe* app;
- answer the call by checking the correct presence of audio and video;
- open the doors (main door and gate) only during conversation;
- auto-insertion on calling stations.

The test mode can therefore be considered passed if the points listed above work correctly.



*In test mode from the CallMe app it is not possible to open the doors (main door and gate) outside of a call and it is not possible to activate any user activation.*

## 6.15.2 Security

The “Security” tab allows you to:

- modify the installer password, (for example if the administrator decides to change installer or if the installer can no longer remember his/her password);
- block the system, that is enter an administrator password after the configuration step is finished.

As described in paragraph “[Security level of an IPerCom system](#)”, there are two access password levels:

- **installer level**, which provides a password that the installer chooses when creating the project and that is requested every time you want to access the system configuration;
- **administrator level**, which provides for a password that the administrator chooses to secure the system when the configuration step is finished.

Press the “Security” tab, the screen that is displayed is as follows (with system unlocked):

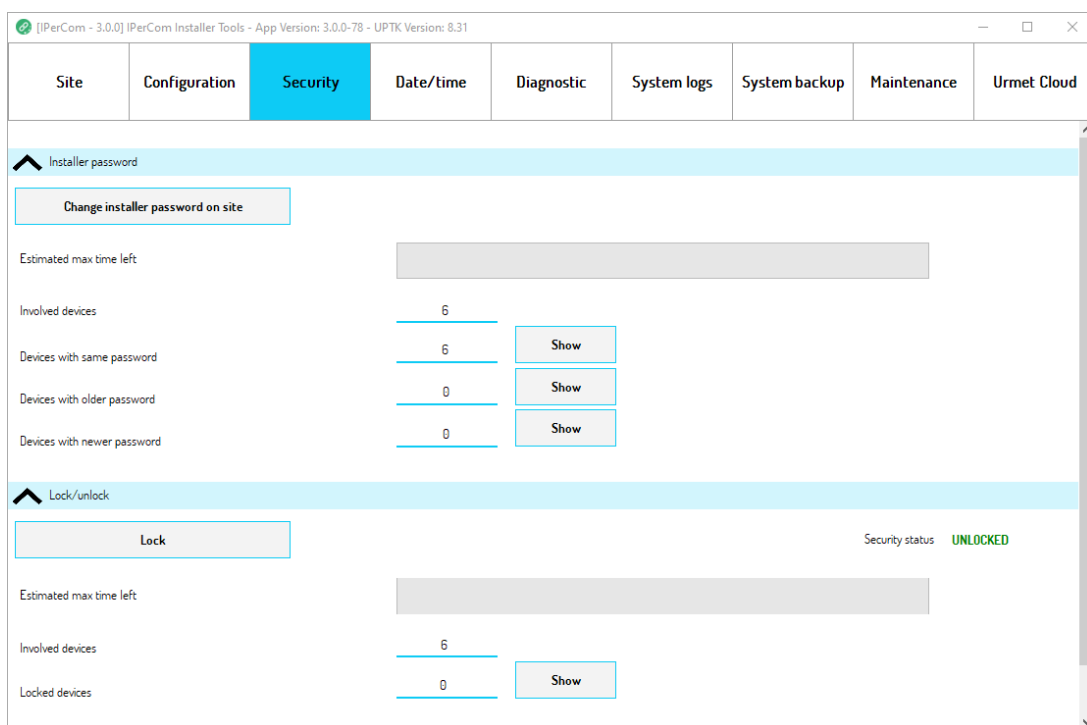





Figure 141: “Security” tab



-  The installer password change does not require to enter the old password.
-  For proper security management of a system, the installer password must not be known to the system administrator and similarly the administrator password must not be known to the installer.
-  After locking the system, you can perform the reverse operation, that is unlock it. This is necessary if the installer must access the configuration several times to make the necessary modifications.

The installer password change, administrator password entry (that is system block) and administrator password disabling (system unlock) are now described in more detail.

### 6.15.2.1 Modifying the installer password

To change the installer password, press the "Change installer password on site" button (red arrow):

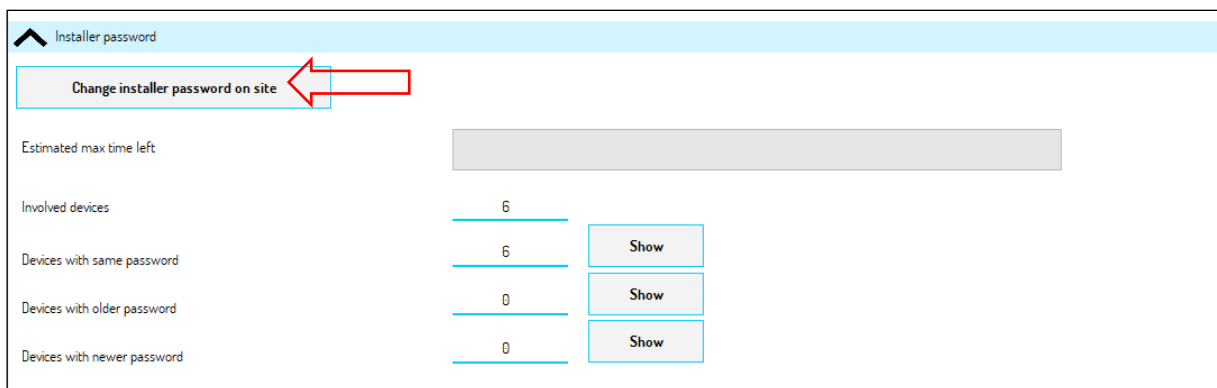


Figure 142: modifying the installer password

A screen is displayed where it is possible to enter the new password:

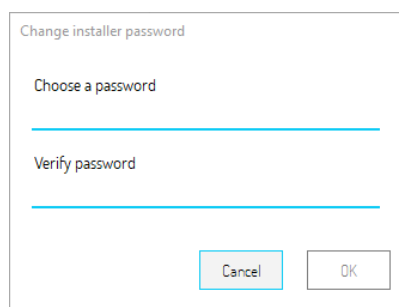


Figure 143: entering the new password

After entering the new password and pressing the "OK" button, it is possible to check in real time that the installer password change process is correctly performed. Once the procedure is complete, the following screen is displayed:

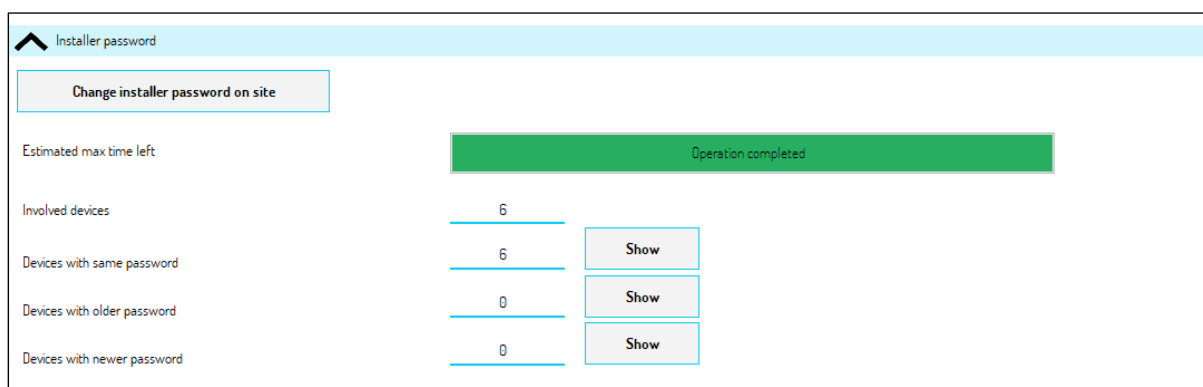


Figure 144: installer password modification successfully performed

The installer password update does not affect devices such as Lift Interface, Relay Actuator, Key Readers, RTSP Cameras, IPassan Controller and iPerTalk Server.

The installer password is requested every time it is necessary to modify the configuration file of an IPerCom system through the configurator (regardless of whether the system is unlocked or locked).

### 6.15.2.2 System block

If the IPerCom system is unlocked, it is necessary to press the "Lock" button (red arrow) to block it:

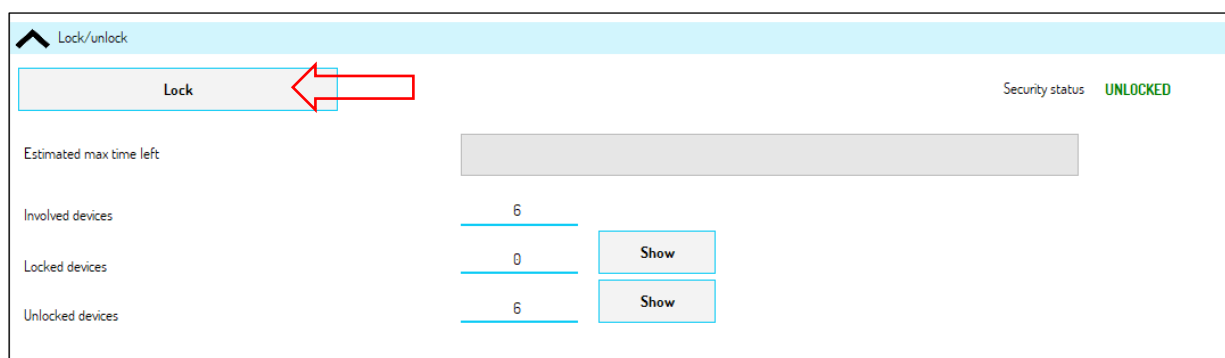
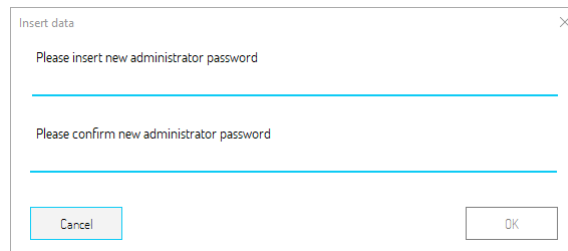


Figure 145: how to block the system

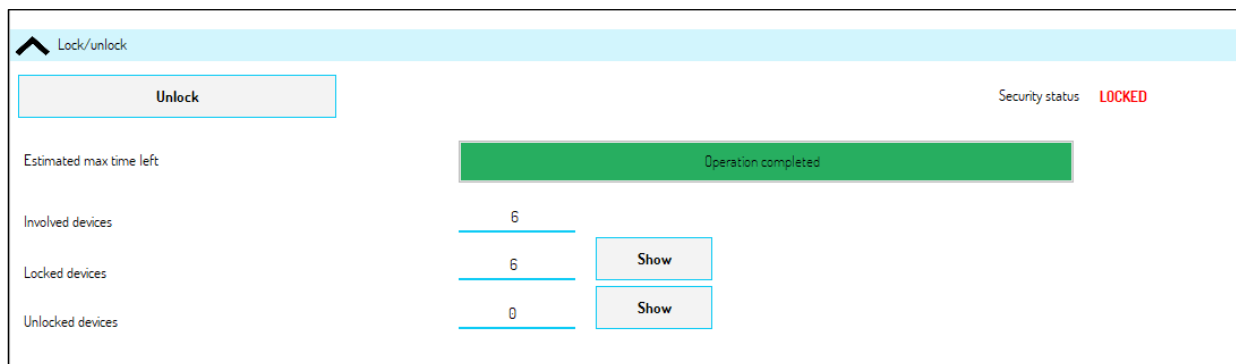
A screen is displayed where it is possible to enter the password:



The dialog box titled "Insert data" contains two text input fields. The first field is labeled "Please insert new administrator password" and the second is labeled "Please confirm new administrator password". At the bottom of the dialog, there are two buttons: "Cancel" on the left and "OK" on the right.

Figure 146: entering the administrator password

After entering the new administrator password and pressing the "OK" button, it is possible to check in real time that the administrator password entering process is correctly performed. Once the procedure is complete, the following screen is displayed:



The "Lock/unlock" screen features a light blue header with a home icon and the text "Lock/unlock". Below the header is a large "Unlock" button. In the top right corner, the "Security status" is displayed as "LOCKED" in red text. A green progress bar indicates "Operation completed". The screen also displays a table of device statistics:

Category	Count	Action
Involved devices	6	
Locked devices	6	Show
Unlocked devices	0	Show

Figure 147: system blocked

The "Security Status" item has been changed to "Locked".



*Locking a system at configuration distribution level does not apply to devices such as Lift Interface, Relay Actuator and Key Readers, RTSP Cameras, IPassan Controller and iPerTalk Server.*



*At IPerCom Installer Tools level, if a system is locked, when you connect to the system, the administrator password is requested.*

### 6.15.2.3 Unlocking the system

If the IPerCom system is blocked, it is necessary to press the “Unlock” button to unlock it:

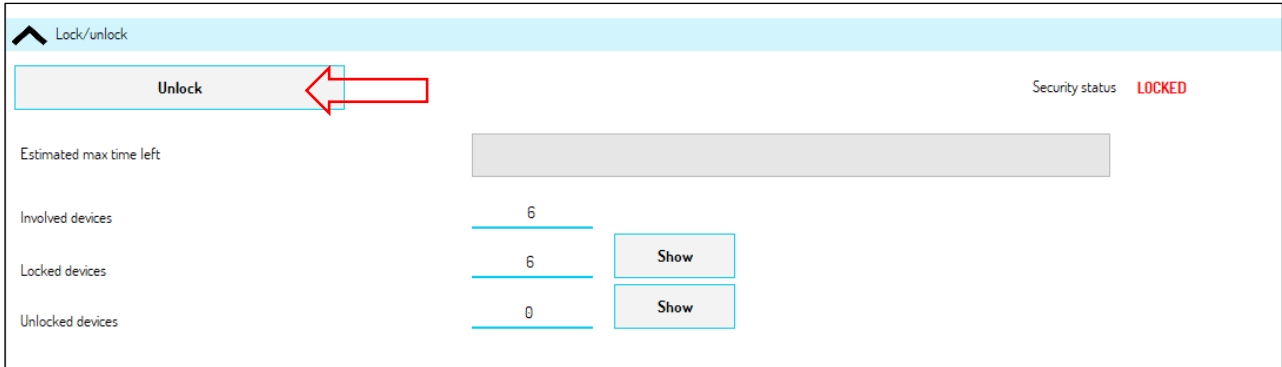


Figure 148: how to unlock the system

It is possible to check in real time that the system unlocking process is carried out correctly. Once the procedure is complete, the following screen is displayed:

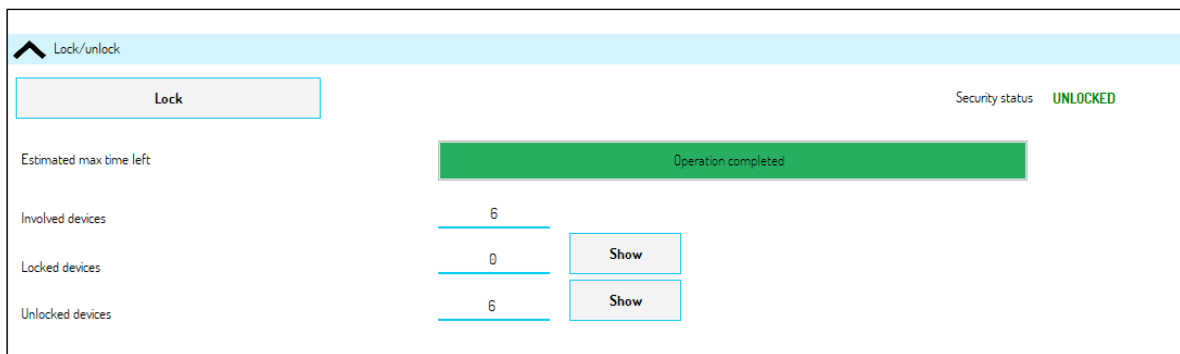


Figure 149: unlocked system

The “Security Status” item has been changed to “Unlocked”.



*Unlocking a system at configuration distribution level does not apply to devices such as Lift Interface, Relay Actuator and Key Readers, RTSP Cameras, IPassan Controller and iPerTALK Server.*

### 6.15.3 Date/Time

The "Date/Time" tab allows you to:

- set date and time of the PC on the IPerCom system;
- obtain the IPerCom system date and time.

#### 6.15.3.1 Configuring date and time from PC

If you want to apply the date and time from PC to the IPerCom system, press the "Set date and time" button (red arrow):

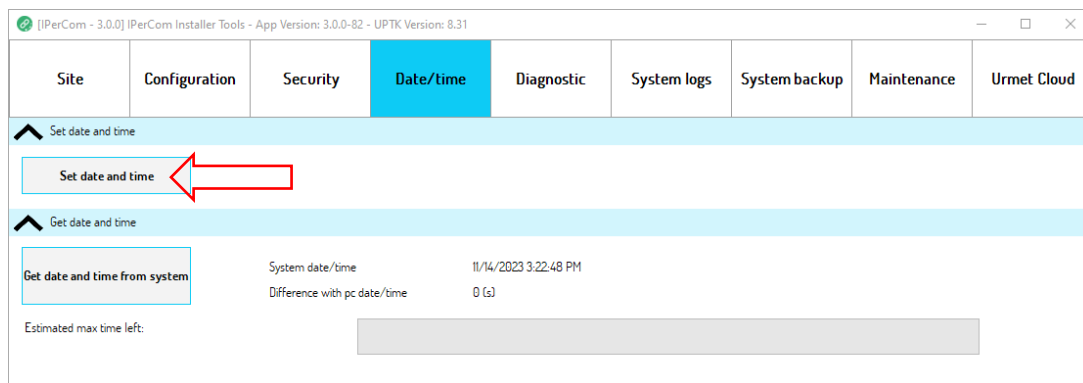


Figure 150: "Date/Time" tab - date/time setting of the PC on the system

You are prompted to confirm the operation as shown below:

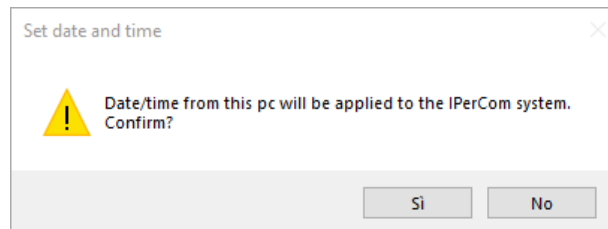


Figure 151: confirmation window for date/time alignment operation

After pressing the "Yes" button, the date and time are applied to the IPerCom system.

The correct date and time application is indicated by a confirmation message:

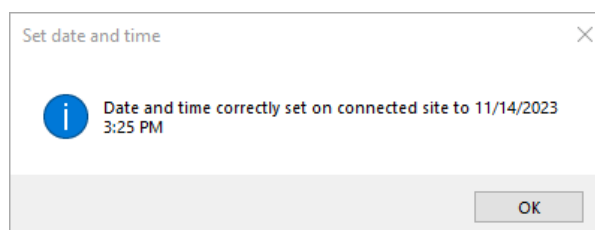




Figure 152: date/time alignment successfully performed

 For proper system operation, the date and time of the IPerCom system must be correctly configured. On a system installed but not configured, before applying the configuration associated to the project to the system, it is necessary to set the date and time with the "Set Date/Time" button, as explained in paragraph "[How to set date and time on the system](#)". If date and time are not set via IPerCom Installer Tools and the configuration associated to the project is still applied to the system, it is necessary to configure date and time of the system from the MAX, VOG<sup>7</sup> or Basic video door phones.

 If the configuration associated to the project is applied to the system but it is made with a date and time incorrectly set in the future (i.e. later than the current date), after setting the date and time correctly, any changes to the configuration associated to the project will never be applied to the system, because IPerCom devices do not accept a configuration with a modification date older than the one they already contain. For this reason, the correct date and time configuration is essential when commissioning a system. In "[APPENDIX H: Date and time incorrectly set in the future.](#)" it explains how to solve the problem.

### 6.15.3.2 Obtaining date and time from IPerCom system

To obtain the date and time updated from the IPerCom system, it is necessary to press the "Get date and time from system" button. The date and time displayed and their difference in seconds compared to those of the PC refer to the time when the connection is made on the system.

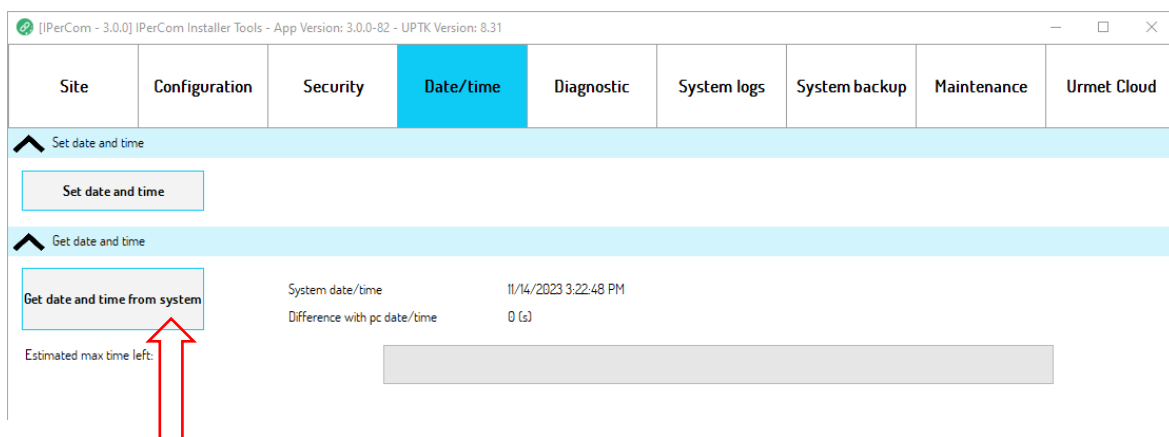


Figure 153: "Date/Time" tab - date/time request from system

Now it is possible to check the status of the procedure in progress in real time:

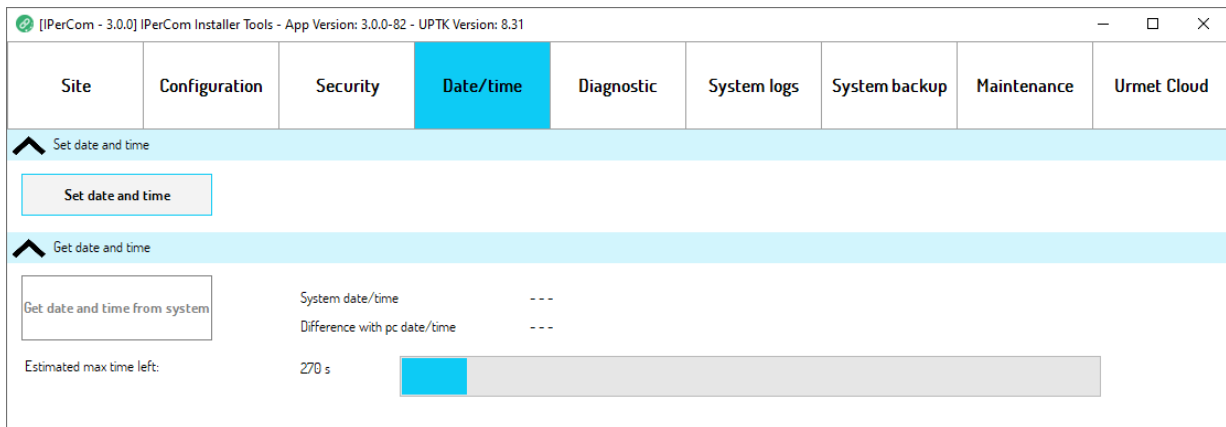


Figure 154: date/time request in progress

At the end of the procedure, a screen with the date and time detected and any difference with the date and time of the PC (in seconds) is displayed:

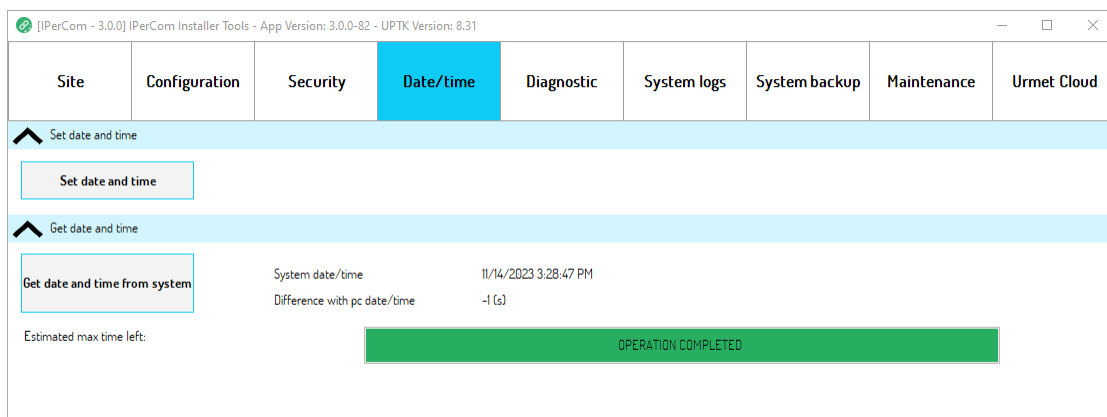



Figure 155: date/time request completed

 If the date and time difference between PC and system is greater than 60s, IPerCom Installer Tools signals the anomaly automatically with the following message:

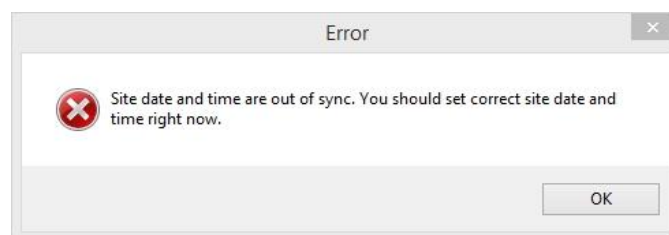


Figure 156: Error: incorrect date and time



If "Request Date/Time from the system" button is pressed on a system where date and time have not yet been configured, the procedure shows the following message:

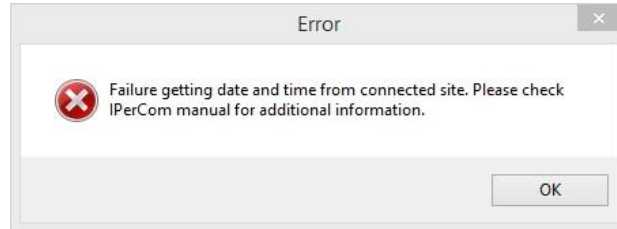


Figure 157: Error to obtain dates and times from the system



The system must have configured date and time to request them correctly. To set the date and time correctly, press the "Set Date/Time" button.



### 6.15.4 Diagnostics

The “Diagnostic” tab allows you to easily understand if all the devices in the system are working regularly or if there are problems of various types (connection, firmware alignment or other). The screen displayed is as follows:

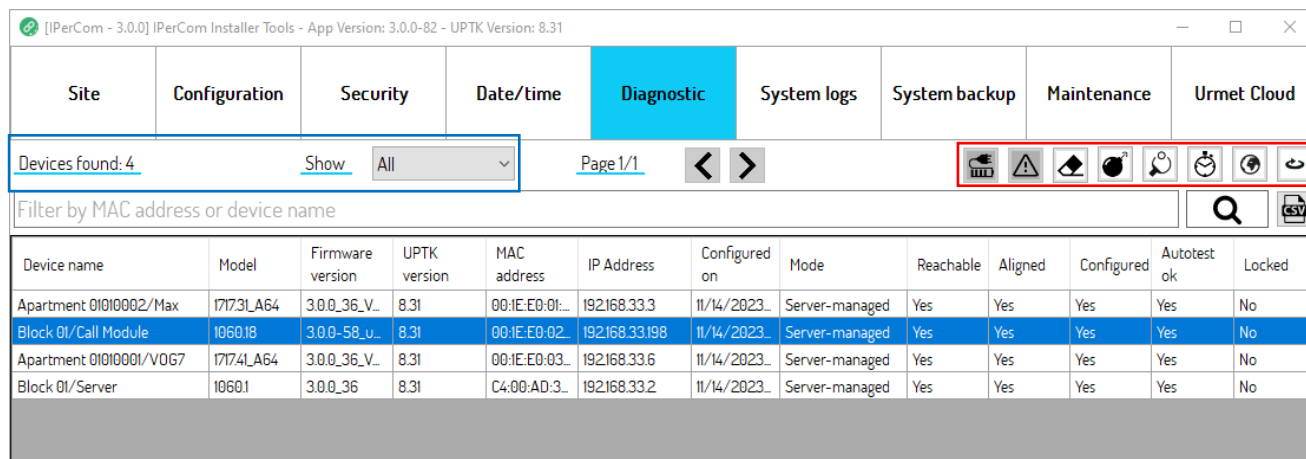


Figure 158: “Diagnostic” tab

The following information is detailed for each device:


Column Name	Meaning
<i>Device Name</i>	Name assigned to the device in the <i>configurator</i>
<i>Model</i>	Device product data sheet
<i>FW version</i>	Device firmware release
<i>UPTK version</i>	Device UPTK version (software development platform)
<i>MAC Address</i>	Device MAC address
<i>IP</i>	Device IP address
<i>Configured on</i>	Date of the last update of the device configuration file
<i>Mode</i>	If the device works in server mode or without server
<i>Reachable</i>	Whether the device is reachable or not
<i>Aligned</i>	Whether the device is aligned with the UPTK version of <i>IPerCom Installer Tools</i> or not
<i>Configured</i>	Whether the device is configured or not
<i>Autotest OK</i>	Whether the device is working or not. The function is only active for <i>Server 1060/1</i> and <i>Modular Entry Panel with 1060/48</i> . If there are any problems, the NO value is signalled and the  button is enabled to provide more information about the problem.
<i>Blocked</i>	Whether the device is on a blocked system or not

Table 6: Columns shown in tab Diagnostic and their meaning

The icons in the red box are active depending on the selected device. The operation of each icon is explained below.













Icon	Name/Meaning
	<b>Get UPS info:</b> It allows you to obtain information on the UPS (uninterruptible power supply) status, including the percentage of battery charge and autonomy time. The button is enabled only if the selected device is a <i>Server 1060/1</i> .
	<b>Error details:</b> It allows you to obtain information about possible errors regarding the selected device. The button is active only if the selected device ( <i>Server 1060/1</i> or <i>Modular Entry Panel with 1060/48</i> ) has errors ( <i>Autotest OK</i> field value to NO).
	<b>Erase configuration:</b> It allows you to delete the configuration on the selected device (through confirmation pop-up). The button is enabled on all devices except <i>IPassan Controllers</i> and <i>iPerTALK Servers</i> .
	<b>Factory reset:</b> it allows you to perform a factory reset of the device. The button is enabled on all the devices except <i>Lift Interface</i> , <i>Relay Actuator</i> , <i>Key Readers</i> , <i>IPassan Controllers</i> and <i>iPerTALK Servers</i> .
	<b>Ping device:</b> it allows you to check that the selected device is reachable from any PC connected to the IPerCom network. The button is enabled on all the devices except <i>Lift Interface</i> , <i>Relay Actuator</i> , <i>Key Readers</i> , <i>IPassan Controllers</i> and <i>iPerTALK Servers</i> .
	<b>Get date and time:</b> It allows you to get the date and time set on the device and for how long (in seconds) the device is reachable. The button is enabled on all devices except <i>Lift Interface</i> , <i>Relay Actuator</i> , <i>Key Readers</i> , <i>IPassan Controllers</i> and <i>iPerTALK Servers</i> .
	<b>Check device Internet connection:</b> it allows you to check whether the selected device is connected to the Internet. The button is enabled on all the devices except <i>Lift Interface</i> , <i>Relay Actuator</i> , <i>Key Readers</i> , <i>IPassan Controllers</i> and <i>iPerTALK Servers</i> .
	<b>Reboot device:</b> it allows you to restart the selected device. The button is enabled on all the devices except <i>Lift Interface</i> , <i>Relay Actuator</i> , <i>Key Readers</i> , <i>IPassan Controllers</i> and <i>iPerTALK Servers</i> .

Table 7: diagnostic icons and their meaning

The blue box, instead, contains:

- the number of devices connected to the system (whether they are in the configuration or not);
- a drop-down menu to filter the devices according to the "All" (default setting), "Operational" and "Not Operational" items. A device not operational is a device that is not reachable or not aligned or not configured or with autotest failed. A device operational is a device that is reachable, aligned, configured and with autotest not failed;
- a text box to filter in the table the devices whose name or MAC address contains the text typed (the table updates as soon as you enter a text);
- the  button to export the information in the diagnostic table to a csv file.

-  For a correct display of the csv file, it is necessary to open Excel, go to the "Data" tab, press the "From text" icon, select the exported file and press "Import". You must now select "65001" as the character encoding: Unicode (UTF-8)" and the character "comma" as text delimiter.
-  Devices Lift Interface, Relay Actuator, Key Reader, IPassan Controller and iPerTAlk Server do not recognise the operating mode "with server" or "without server" and similarly do not recognise whether a system is blocked or not. Therefore, for these devices the columns *Blocked* and *Mode* are marked with "---".
-  RTSP cameras are not shown in the "Diagnostics" tab because they are not IPerCom devices.

### 6.15.5 System Logs

The “*System Logs*” tab allows you to record in a log a set of events related to the operation of an iPerCom system. To display the complete log with all its functions, it is necessary that at least one *Server 1060/1* is present on the system.

If this condition is verified, after opening a project associated with a system, connecting to the system, and checking that the configuration is aligned, the “*System logs*” tab is displayed as shown below:

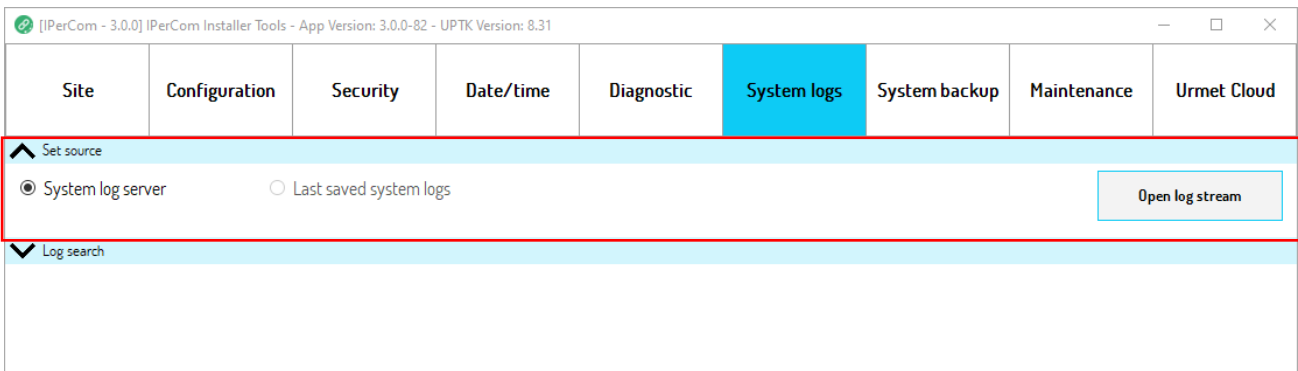


Figure 159: “*System Logs*” tab (if a *Server* is in the system)

The red box (**Set Source** section) highlights that the source of the System Logs is *Server 1060/1*, renamed as **System log server**.

If, in fact, there is no *Server 1060/1* in the system and therefore no event source, the “*System logs*” tab is shown as in the figure below:

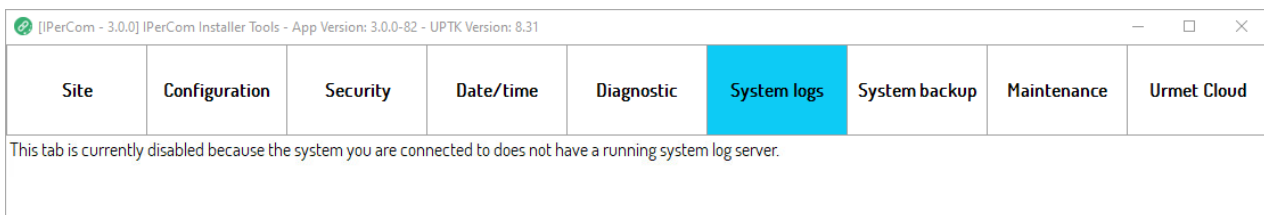


Figure 160: “*System Logs*” tab (if no *Server* is in the system)

If there are more than a *Server 1060/1* in the system, the System Logs display is obviously independent of the *Server* chosen by the system as source (of System Logs) and is done by pressing the “*Open System Logs*” button.

The screen displayed (after a set of processing) is as follows:

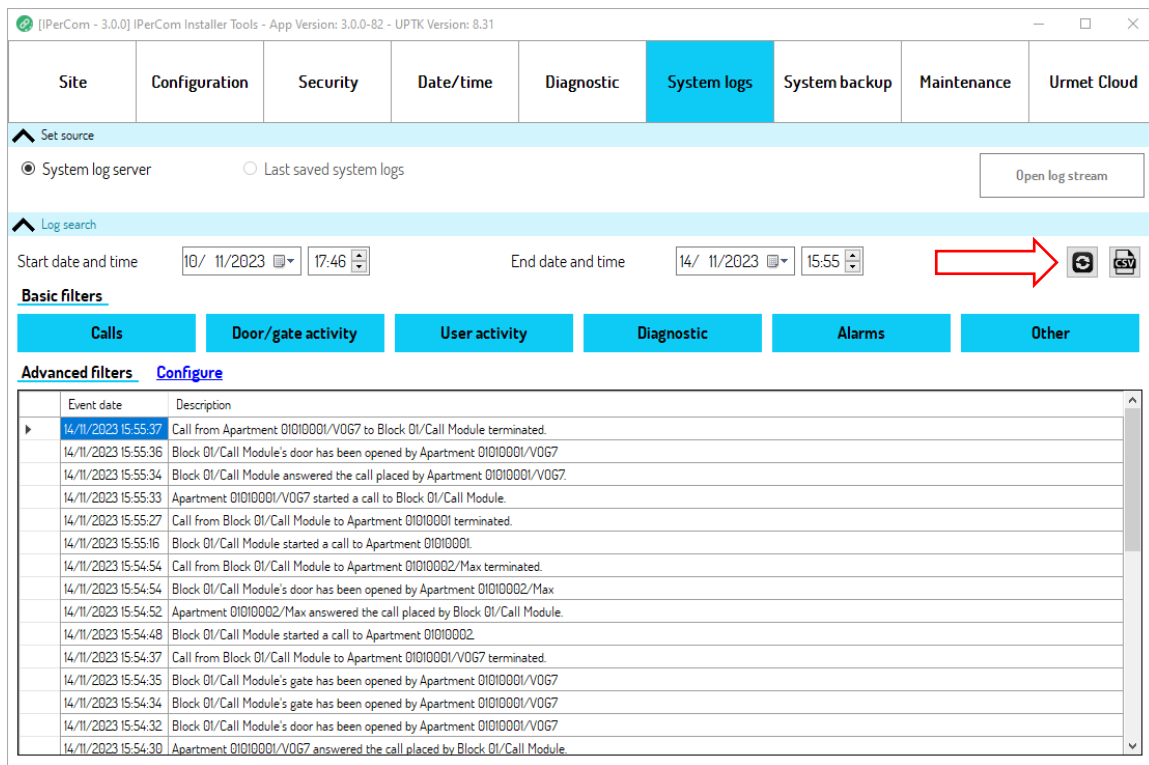


Figure 161: displaying the System Logs (static mode)

The figure above shows the **static** operation mode of the System Logs, i.e. a static representation of the events is displayed over a time interval of one week from the current date. Press the button (red arrow), to update the System Logs to the current time instant and download it again from the selected source.

Obviously, it is possible to vary the time interval to display events before one week from the current date.

The button (red box) allows you to export the information in the System Logs to a csv file.

For a correct display of the csv file it is necessary to open Excel, go to the **Data** tab, press the **From text** icon, select the exported file and press "Import". You must now select "65001" as the character encoding: Unicode (UTF-8)" and the character "comma" as text delimiter.

The maximum default number of recordable events is set to 10,000. When this number is reached, the oldest events are deleted. The number of recordable events can be changed for special needs up to a maximum of 100,000. This value can be changed from the iPerCom configurator (see the relevant paragraph "[System parameters](#)").

When the System Logs is displayed for the first time in static mode, in the "Site" tab the item "System logs available offline" is selected (red arrow):

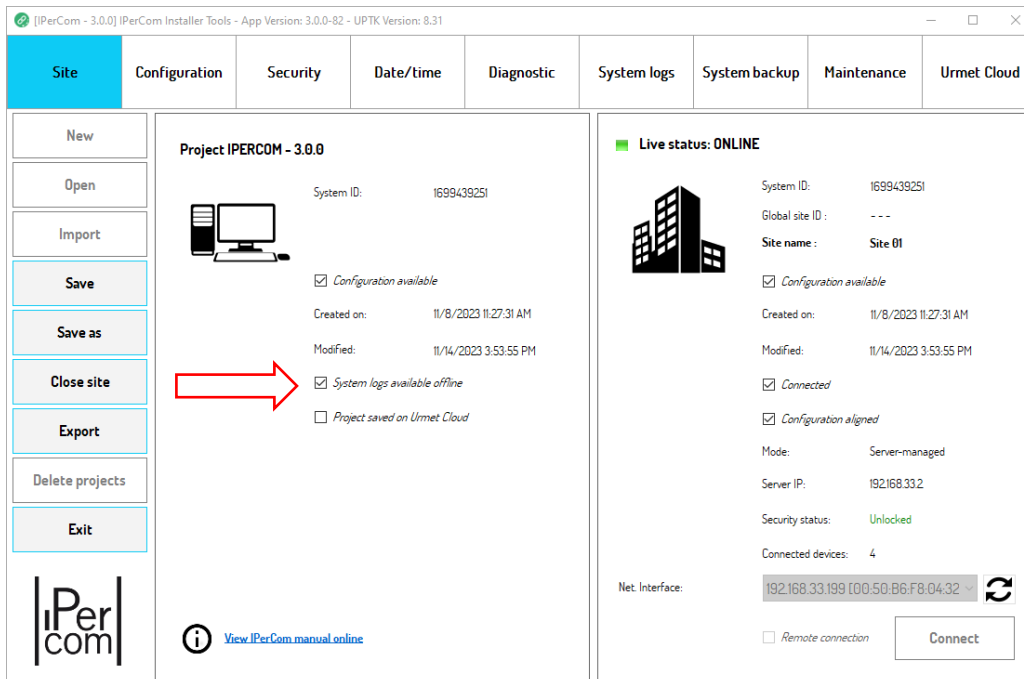


Figure 162: "Site" tab with System Logs saved locally

If this item is selected, the next time *iPerCom Installer Tools* is started it is possible to consult the system logs by simply opening the project, even if you are not connected to the system (and therefore even if the configurations of the project and site are not aligned). In this case the "System Logs" tab looks like this:

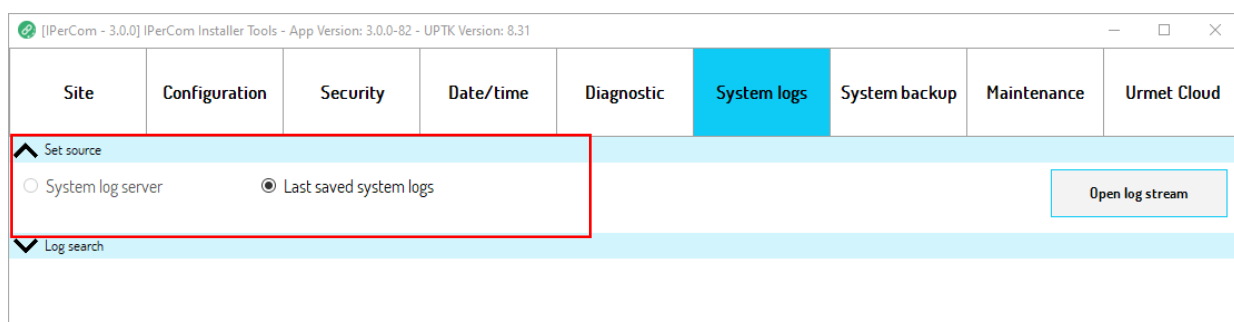


Figure 163: "System Logs" tab with System Logs saved locally

In this case, the source is not the *Server 1060/1*, but the backup of the System Logs automatically saved on your PC the first time it was displayed in static mode and updated every time the button was pressed. In this case the "Open System Logs" button shows the same screen as before, with the only difference that the System Logs cannot be updated in real time with the button, which in fact is frozen.

In this case it is possible also to export the System Logs to a csv file.

To display the System Logs saved locally (backup), the same System Logs must have been displayed at least once in online mode: the backup, in fact, is created as soon as the static System Logs operation mode is activated.

Every time the "Open System Logs" button is pressed (except the first time) in static mode, the local System Logs is downloaded again. To prevent the previous one from being automatically overwritten, the following message is shown:

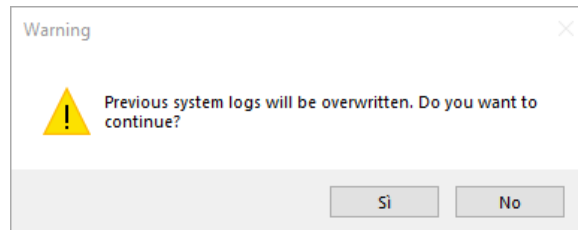


Figure 164: request to overwrite the local System Logs

If the "Yes" button is pressed, the previous local System Logs is overwritten and the static operation mode is enabled. If "No" is pressed, the static operation mode is not enabled.

If the System Logs has never been opened in static mode, if you try to enable it only with the project open, the following screen is displayed:

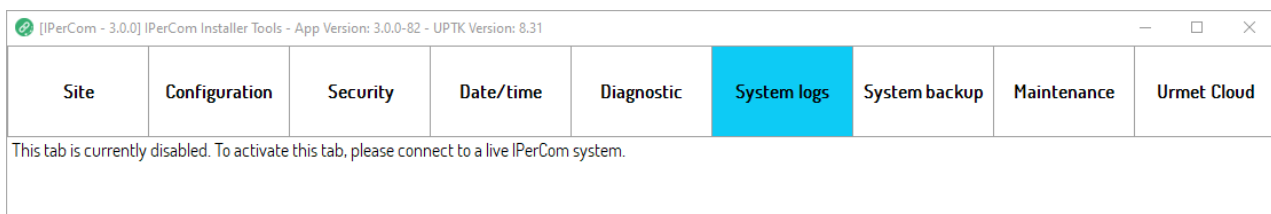



Figure 165: "System Logs" tab (without connection to the system) if the System Logs has never been opened in static mode

Below is explained in more detail which information is tracked in the System Logs and how to filter it.

### 6.15.5.1 How to filter System Logs: basic and advanced filters

The basic and advanced filters (**Search in System Logs** section in the red box) work in the same way regardless of whether the source of the System Logs is the server or a backup saved according to what was previously written. The only difference between the 2 ways to view the System Logs is the possibility to update it with the  button, when the source is a *Server 1060/1*. In both cases the screen displayed is as follows:

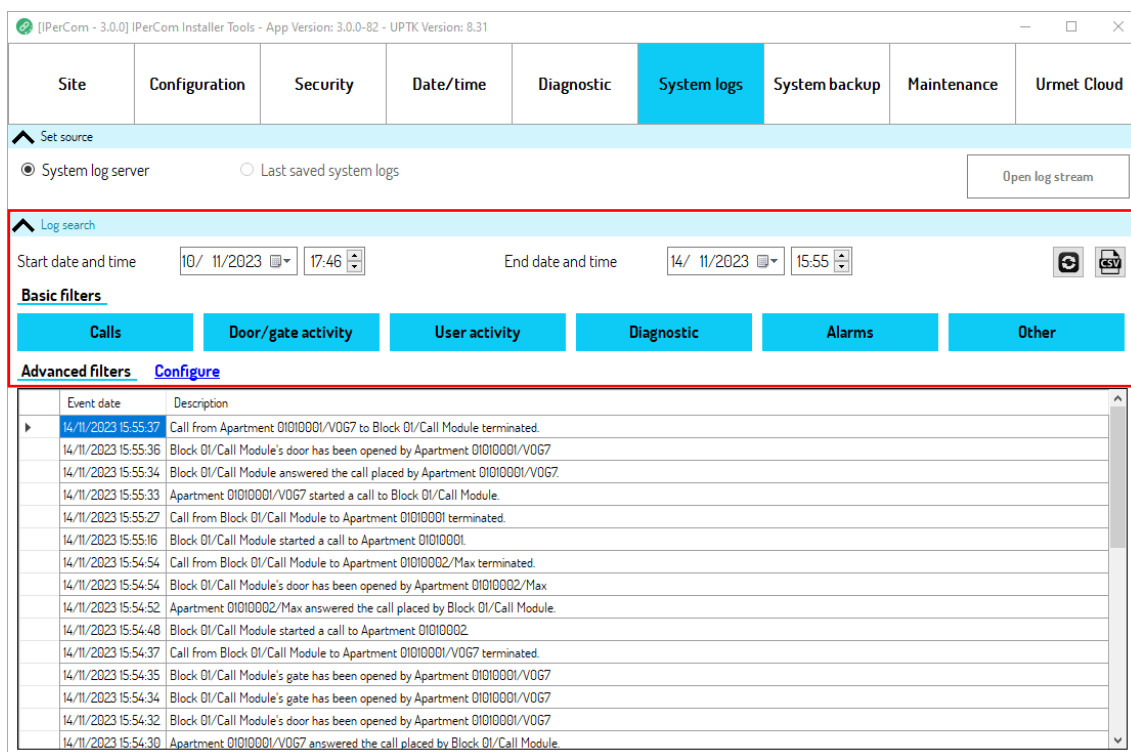


Figure 166: System Logs filters

### FILTERING THE SYSTEM LOGS BY TIME INTERVAL

The **Start Date and Time** and **End Date and Time** fields (in the red rectangle) allow you to display the System Logs within the selected time interval. The default time interval is one week.

### BASIC FILTERS

Each time the System Logs window is opened, all the buttons related to the event categories in the **Basic filters** section are blue, i.e. selected: this means that *IPerCom Installer Tools* displays all the events and no basic filter has been applied. To deselect an event and then automatically not display it, it is necessary to press one of the buttons: its colour switches from blue to white.

A more detailed explanation of the various categories of events is given below.



## CALLS

The "Calls" event category includes all types of calls between the various system devices (including auto-on): for each call the source device (from which the call starts), the destination device (to which the call arrives), the possible response and the end of the call are displayed in detail. The name of each device is preceded by the name of the topological node where the device has been placed. An example is given below:

Event Date	Description
17/06/2020 09:28:00	Call from Block 01/Call Module to Apartment 01010101/Monitor Max 1 terminated.
17/06/2020 09:27:58	Apartment 01010101/Monitor Max 1 answered the call placed by Block 01/Call Module.
17/06/2020 09:27:53	Block 01/Call Module started a call to Apartment 01010101.
17/06/2020 09:27:02	Call from Block 01/Call Module to Apartment 01010103/Doorphone Miro terminated.
17/06/2020 09:26:59	Apartment 01010103/Doorphone Miro answered the call placed by Block 01/Call Module.
17/06/2020 09:26:49	Block 01/Call Module started a call to Apartment 01010103.

Figure 167: System Logs filtered by call event

## ACCESS POINT ACTIVITIES

The "Access Point Activities" event category includes the opening of all access points (pedestrian and driveway access point) of the various apartment station, resident/non-resident devices (by means of door opener code or proximity key), entrance hall button, trade function and from *Switchboard* application. The name of each device to which the access point belongs is preceded by the name of the topological node where the device has been placed. An example is given below:

Event Date	Description
17/06/2020 09:29:23	Block 01/Call Module's door has been opened by Resident 3
17/06/2020 09:27:59	Block 01/Call Module's door has been opened by Apartment 01010101/Monitor Max 1
17/06/2020 09:26:56	Block 01/Call Module's door has been opened by Apartment 01010103/Doorphone Miro
17/06/2020 09:25:00	Block 01/Call Module's door has been opened by Apartment 01010102/Monitor Max 2
17/06/2020 09:24:36	Block 01/Call Module's gate has been opened by Apartment 01010101/Monitor Max 1
17/06/2020 09:24:34	Block 01/Call Module's door has been opened by Apartment 01010101/Monitor Max 1

Figure 168: System Logs filtered by access point activities

## USER ACTIVITIES

The "User Activities" event category includes, for residents and non-residents, the request to open an access point (with proximity key or door opener code) and its outcome, the assignment/removal/suspension/restoring of a key code, the assignment/suspension/restoring of a door opener code; for the last 2 events the MAC address of the device from which the assignment/removal/suspension/restoring of the key code or door opener code is made is also reported. The name of each device to which the access point belongs is preceded by the name of the topological node where the device has been placed. An example is given below:

Event Date	Description
17/06/2020 10:01:27	Configuration changed by MAC 00:50:B6:22:73:44: door code 6**0 has been added for user Resident 4
17/06/2020 09:59:45	Resident 2 requested door/gate opening on Block 01/Call Module using a door opening code. Request approved.
17/06/2020 09:29:21	Resident 3 requested door/gate opening on Block 01/Call Module using a door opening code. Request approved.
17/06/2020 09:25:48	Configuration changed by MAC 00:50:B6:22:73:44: door code 1**0 has been added for user Resident 3

Figure 169: System Logs filtered by user activities

## DIAGNOSTICS

The event category "*Diagnostic*" indicates for each device if it is no longer reachable and when it is reachable again. The name of each device is preceded by the name of the topological node where the device has been placed. An example is given below:

Event Date	Description
17/06/2020 10:06:25	Video Doorphone Apartment 01010101/Monitor Max 1 (MAC 00:1E:E0:01:01:F5) is reachable again
17/06/2020 10:04:06	Video Doorphone Apartment 01010101/Monitor Max 1 (MAC 00:1E:E0:01:01:F5) is not reachable
16/06/2020 15:20:44	Audio Doorphone Apartment 01010103/Miro Doorphone (MAC 00:1E:E0:01:D3:8C) is reachable again
16/06/2020 15:17:54	Audio Doorphone Apartment 01010103/Miro Doorphone (MAC 00:1E:E0:01:D3:8C) is not reachable

Figure 170: System Logs filtered by diagnostics

## ALARMS

The "*Alarms*" event category includes all the alarms generated by the IPerCom system: in detail, which device has generated a specific alarm, which *Switchboard* has taken charge of the alarm and which *Switchboard* has reset it. The name of each device is preceded by the name of the topological node where the device has been placed. An example is given below:

Event Date	Description
17/06/2020 10:26:02	Alarm Coercion, raised by Block 01/Call Module, has been reset by Site 01/Switchboard
17/06/2020 10:25:44	Alarm Coercion raised by Block 01/Call Module
17/06/2020 10:25:37	Alarm Coercion raised by Block 01/Call Module
17/06/2020 10:24:14	Alarm Panic, raised by Apartment 01010101/Monitor Max 1, has been reset by Site 01/Switchboard
17/06/2020 10:22:06	Alarm Panic raised by Apartment 01010101/Monitor Max 1

Figure 171: event history filtered by alarms

## OTHER

The "*Other*" event category includes other events that do not fall into the above categories: in detail, events related to the *Lift Interface*, access and disconnection operations from the *Switchboard* application, MAC address of the device from which a configuration change to the system or an installer password change has been made. An example is given below:

Event Date	Description
17/06/2020 10:26:08	Switchboard user 1 has logged out on Site 01/Switchboard
17/06/2020 10:01:27	Device with MAC address 00:50:B6:22:73:44 has changed system configuration. The new configuration timestamp is 1592380859 (17/06/2020 10:00:59).
17/06/2020 09:43:03	Site locked by device with MAC 00:50:B6:22:73:44
17/06/2020 09:29:32	Device with MAC address 00:50:B6:22:73:44 has changed system configuration. The new configuration timestamp is 1592378944 (17/06/2020 09:29:04).
17/06/2020 09:25:48	Device with MAC address 00:50:B6:22:73:44 has changed system configuration. The new configuration timestamp is 1592378720 (17/06/2020 09:25:20).

Figure 172: System Logs filtered by other events

Each event category can be further filtered in the Advanced Filters section, which can be enabled by pressing the "Configure" item, as shown in the figure:

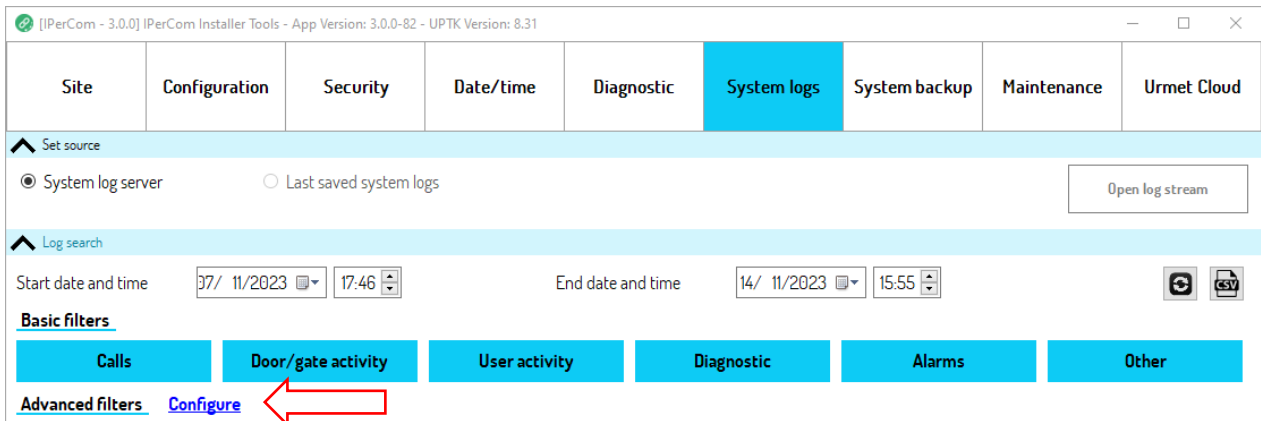


Figure 173: advanced System Logs filters

The next screen contains a drop-down menu with the various categories of events and, depending on the type of event selected, the relevant filter, as explained in more detail below.

#### 6.15.5.2 Filter on Calls event

If, in the **Category** drop-down menu, the event type "Calls" (default setting) is selected, the following is displayed:

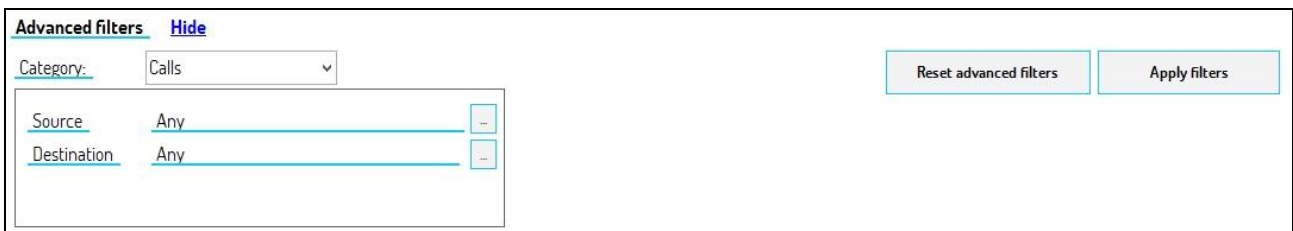


Figure 174: advanced filter for calls event

Calls can be filtered according to the calling device ("Source") and the called device ("Destination").

The source and destination are selected by pressing the button .

A screen opens where it is possible to navigate the topological structure of the system and generally choose a call station for the source, as shown below:

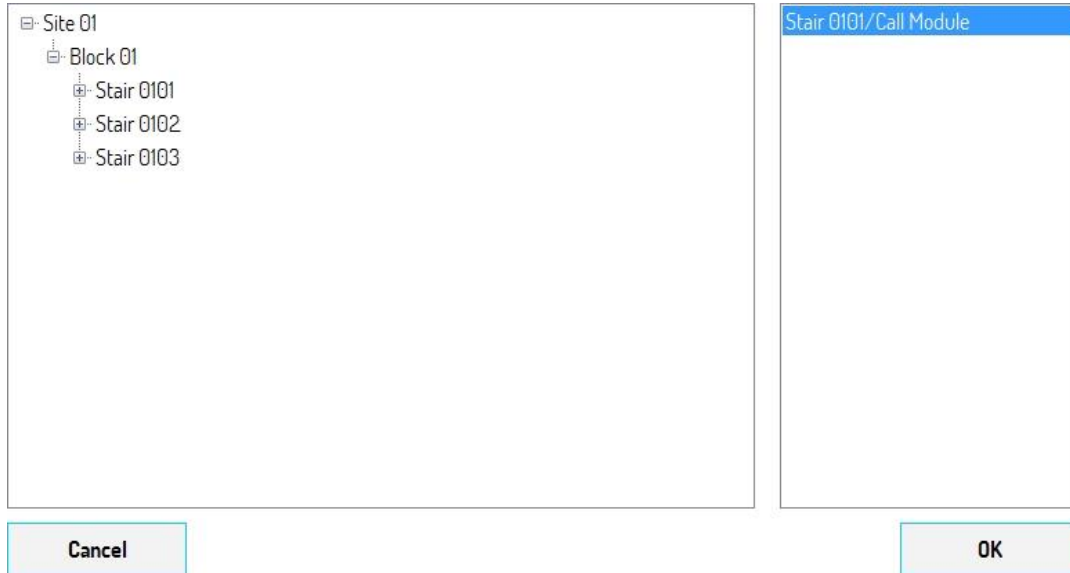


Figure 175: navigation of the system topological structure

The called device is selected in the same way.

After pressing the "OK" button and then the "Apply filters" button, only calls between the devices selected above will be displayed for the *Calls* event category.

After pressing the "Apply filters" button, only calls between the devices selected above will be displayed for the *Calls* event category.



One of the "Source" and "Destination" fields can be left to Any value.

#### FILTER ON ACCESS POINT ACTIVITY EVENT

If, in the **Category** drop-down menu, the event type "Access point activities" is selected, the following is displayed:

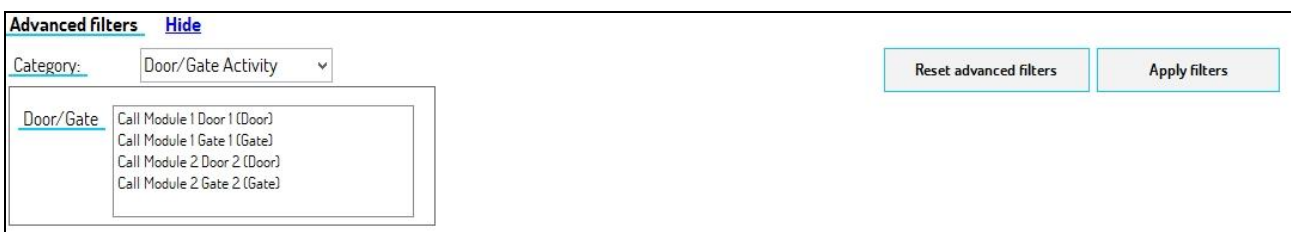


Figure 176: advanced filter for access point activity event

By selecting one or more of the access points listed and after pressing the "Apply filters" button for the *Access point activities* event category, only the events related to the opening of the selected access points are displayed.

### FILTER ON USER ACTIVITY EVENT

If, in the **Category** drop-down menu, the event type "User activities" is selected, the following is displayed:



Advanced filters <a href="#">Hide</a>	
Category:	User Activity
User	Resident 1 (Apartment 01010101) Resident 2 (Apartment 01010101) Resident 3 (Apartment 01010101) Resident 4 (Apartment 01010102)
<input type="button" value="Reset advanced filters"/> <input type="button" value="Apply filters"/>	

Figure 177: advanced filter for user activity event

Select one or more residents/non-residents among those listed and press the "Apply filters" button: for the *User activities* event category, the access point opening requests (with proximity key or door opener code) and relevant outcome of the selected residents/non-residents only will be displayed. Also for the selected residents/non-residents, the events of assignment, removal, suspension, restoring of a key code and assignment, suspension, restoring of a door opener code with MAC address of the device from which the operation in question is carried out are also displayed.

### FILTER ON DIAGNOSTIC EVENT

If, in the **Category** drop-down menu, the event type "Diagnostic" is selected, the following is displayed:



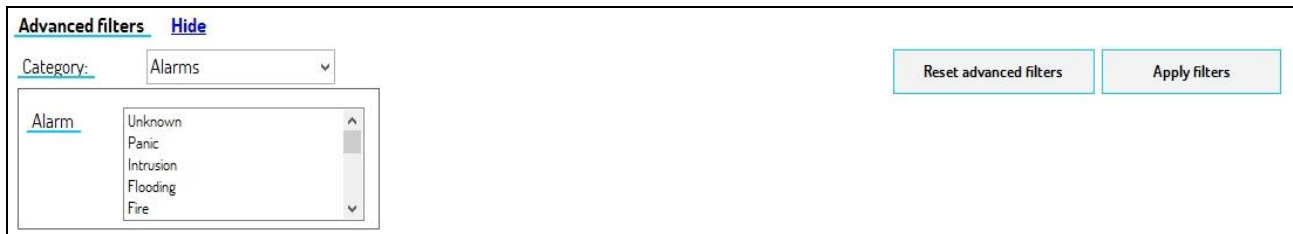
Advanced filters <a href="#">Hide</a>	
Category:	Diagnostic
MAC Address	00:1E:E0:02:03:8A 00:50:B6:22:73:44 00:10:F3:4A:D6:B8 00:1E:E0:01:01:F5 00:1E:E0:01:3F:45
<input type="button" value="Reset advanced filters"/> <input type="button" value="Apply filters"/>	

Figure 178: advanced filter for diagnostic event

Select the MAC address of one or more devices among those present in the system and press the "Apply filters" button of the event category "Diagnostic", only the diagnostic events of the selected devices are displayed.

## ALARM EVENT

If, in the **Category** drop-down menu, the event type "Alarms" is selected, the following is displayed:




The screenshot shows the 'Advanced filters' section with the 'Category' dropdown set to 'Alarms'. A sub-menu is open under 'Alarm', listing the following options: Unknown, Panic, Intrusion, Flooding, and Fire. To the right of the sub-menu are two buttons: 'Reset advanced filters' and 'Apply filters'.

Figure 179: advanced filter for alarm event

By selecting one or more types of alarms among those listed and after pressing the "Apply filters" button for the "Alarms" event category, only the events related to the selected alarms are displayed.

## OTHER

If, in the **Category** drop-down menu, the event type "Other" is selected, the following is displayed:



The screenshot shows the 'Advanced filters' section with the 'Category' dropdown set to 'Other'. A sub-menu is open under 'Event Type', listing the following options: SWITCHBOARD\_LOGIN, SWITCHBOARD\_LOGOUT, SWITCHBOARD\_MODE, CONFIG\_CHANGED, and LOG\_KEYS\_CHANGED. To the right of the sub-menu are two buttons: 'Reset advanced filters' and 'Apply filters'.

Figure 180: advanced filter for other events

By selecting one or more types of events among those listed and after pressing the "Apply filters" button for the event category *Others*, only the events selected are displayed.

## HOW TO CANCEL THE PREVIOUSLY SET FILTERS

To cancel the previously set filters in the **Advanced Filters** section, simply press the "Reset Advanced Filters" button. This button resets all the previously selected advanced filters.

## DISPLAYING THE EVENTS

For each event, the data that characterise it and help identify it are reported, i.e. date and time and a short description of the event.

### 6.15.6 System backup

The "System backup" tab allows you to periodically save the system configuration (backup) manually or automatically. The function is useful if:

- after making changes to the configuration, it is necessary to restore the situation before the changes;
- it is necessary to update the system to a different firmware version (having a backup of the system configuration is highly recommended in this case).

The configuration changes are saved in the backup both if made by the *configurator* of *IPerCom Installer Tools* and if made by the configurator integrated in the *MAX*, *VOG7* and *Basic* video door phones and if made by the access control configurator of the "Switchboard" application.

The function is only available if there is at least one *Server 1060/1* in the system.

In manual mode, the configuration is saved on your PC (connected to the IPerCom system). In automatic mode, the configuration is saved on a USB stick connected to one of the 3 available ports of the *Server 1060/1*.



To be able to save the system configuration on a USB stick, it must have a FAT32 file system.

The "System backup" tab looks like below:

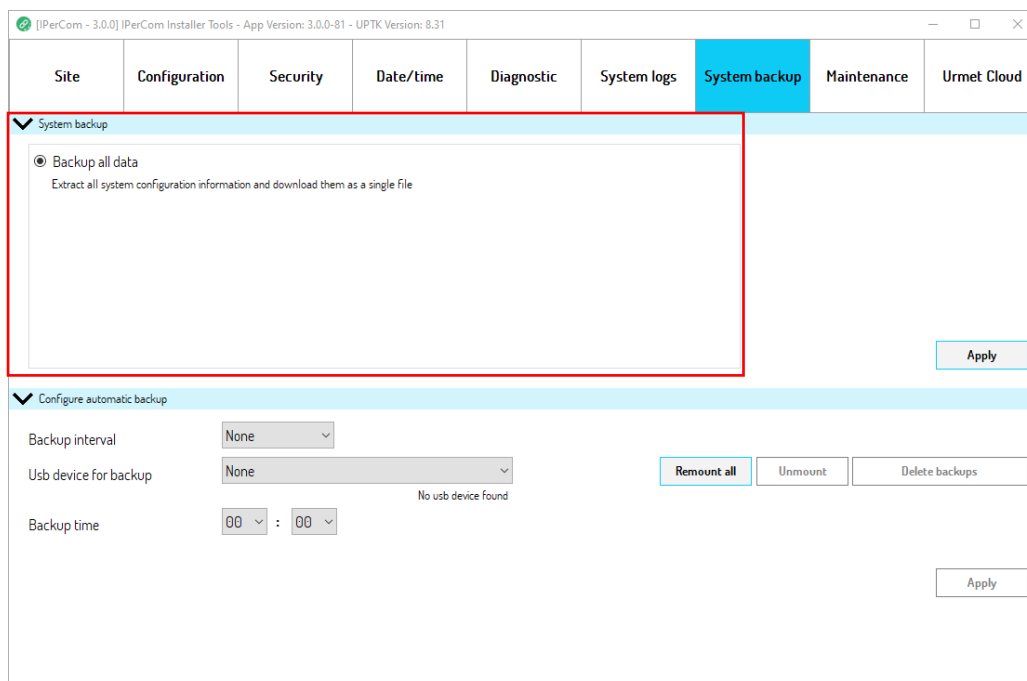


Figure 181: "System backup" tab

## MANUAL BACKUP

The "System backup" section (in red) allows you to manually save the system configuration on your PC ("Save all data" option by default).

Press the "Apply" button to open a window through which you can choose the path where to save the configuration on your PC. The backup file has an "sbz" extension and name with preset date and time. A pop-up window with the file name, path and size indicates that the operation was completed successfully.

The saved sbz file is to be imported in the same way as a project previously exported with the "Export" button. The imported local configuration must be applied to the system (for further details see paragraph "[System modified locally by MAX, VOG7 or Basic video door phone](#)").

## AUTOMATIC BACKUP

The section "Configure automatic backup" (in red) allows you to set up automatic system backups:

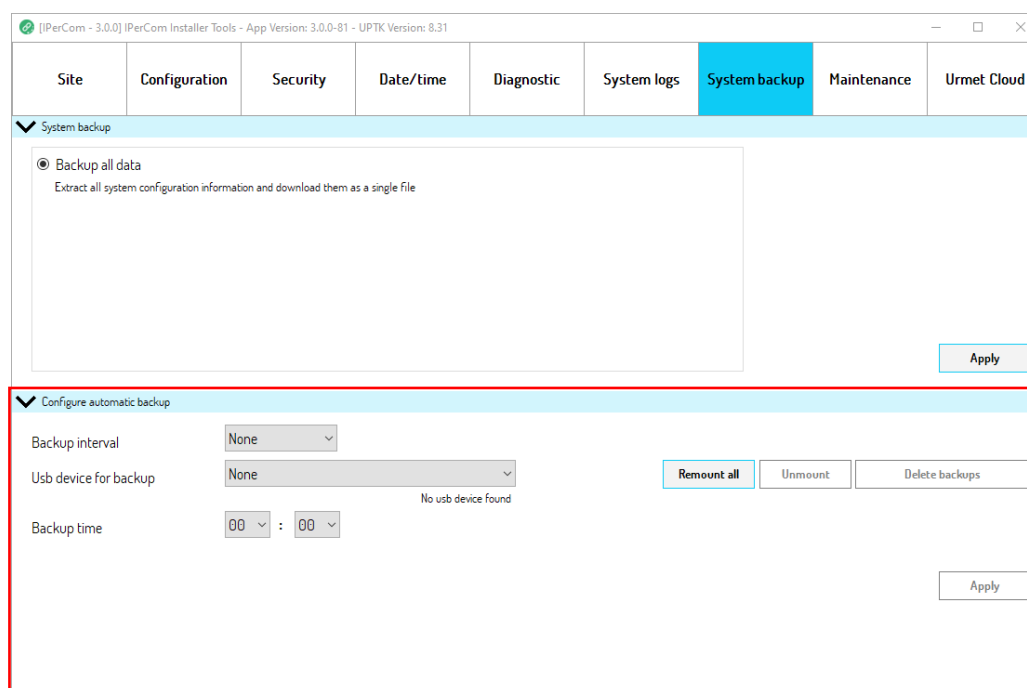


Figure 182: Automatic backup

To use this feature, you need to connect a USB stick to the *Server 1060/1* to one of the 3 available ports.

Then click on the "Connect all" button: the "USB device for backup" drop-down menu will display the USB stick connected to the *Server 1060/1* where the backup should be saved.

Via the "Backup interval" drop-down menu you can choose whether to set the backup daily ("Daily" item) or weekly ("Weekly" item) at the set time ("Backup time"). The "None" item (default) simply disables the previously made choices.



The "Apply" button allows you to save the set changes.

Whenever you need to remove the USB stick from the Server 1060/1, you must remove it using the "Eject" button.

Even in the case of automatic backup, the generated file has an "sbz" extension and name with preset date and time. All backup files are saved in a folder named "AUTO BACKUP IPERCOM".

The sbz files thus created can be imported in the same way as the manual backup.

You can delete previously saved backup files using the "Delete backups" button.



**If you back up a project whose configuration has already been applied on a site, it is absolutely forbidden to transfer the same configuration to another site. The backup function is to be used only to restore old configurations relating to the same site.**

### 6.15.7 Maintenance

The “Maintenance” tab is useful if it is necessary to:

- switch from a system with server to a system without server;
- import a new configuration to the system;
- restart all system devices (useful function if one or more devices (not in configuration and not aligned with the IPerCom version of the system) are connected to the system);
- enable or disable access to IPerCom system configuration from *MAX*, *VOG<sup>7</sup>* or *Basic* video door phones.

These operations are explained in more detail below.

#### SWITCHING FROM A SYSTEM WITH SERVER TO A SYSTEM WITHOUT SERVER

The transition from a system with *Server 1060/1* to one without *Server 1060/1* is possible only if:

- the number of devices is less than or equal to 1000,
- the number of apartments is less than or equal to 1000,
- the total number of users is less than or equal to 1000.

Otherwise, for the correct functioning of the system, the presence of at least one *1060/1 Server* is required.

In case of system with *1060/1 Server*, the “Maintenance” tab of *IPerCom Installer Tools* appears as shown below:

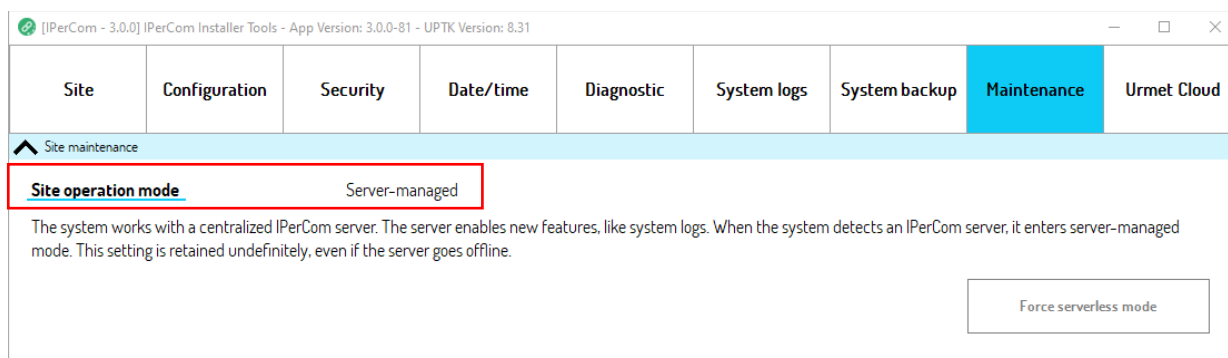


Figure 183: “Maintenance” tab - operation with server

As you can see, the system works in “server” mode.

If the number of devices, apartments, and users is less than or equal to 1000 and you want to switch to a system without *Server 1060/1*, the operations to do are as follows:

- disconnect the various servers from the system;
- start *IPerCom Installer Tools* (if already started, close and start the application again);
- open the project associated with the system;
- connect to the system;
- enter the “*Maintenance*” tab.

The screen displayed is as follows:

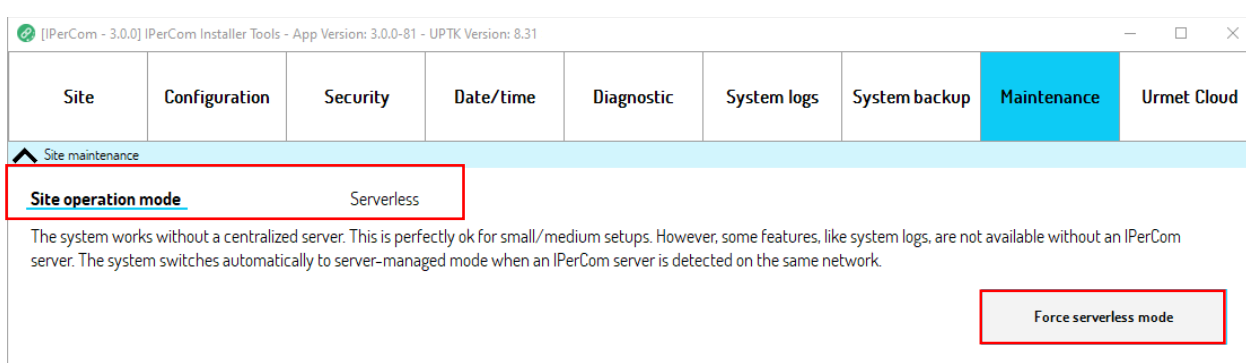


Figure 184: “Maintenance” tab - operation without server

As you can see, *IPerCom Installer Tools* detects that the system is without server, because the various servers have been disconnected from the system. However, to complete the operation correctly, it is necessary to press the “*Force Mode Without Server*” button (which was frozen in the previous screen). The following message is displayed:

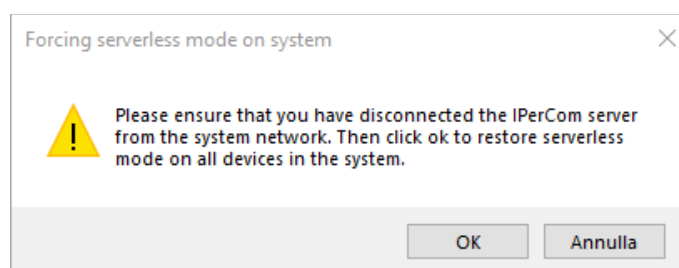


Figure 185: request to restore the mode without server

Press "OK", to restart the devices in the system so that they operate in "without server" mode. At the end of the operation (after entering the administrator password if the system is blocked), the following message is displayed:

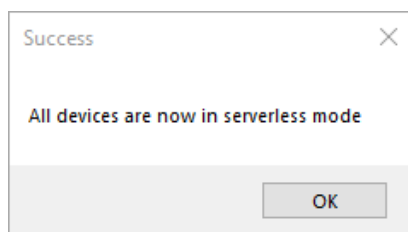


Figure 186: mode without server set correctly

Now the last step is to enter the *configurator*, delete the various servers from the configuration and distribute it again (see paragraph "[The configurator](#)").



*When switching from "with server" to "without server" mode, all devices restart, except those that do not support the UPTK software development platform, that is Key Reader, Relay Actuator, Lift Interface, iPerTalk server, IPassan Controller and RTSP Cameras.*



*When switching from "with server" to "without server" mode upon IPerCom Installer Tools start (after disconnecting the server), the number of connected devices in the "Configuration" tab is equal to those that do not support the UPTK software development platform. In addition, all data relating to the system configuration file are not assigned a value. To return to a correct displaying of the above, it is necessary to press the "Force Mode Without Server" button as described above.*

The switch from "with server" to "without server" is in any case automatic in medium-size systems (that is with several devices, apartments, and users less than or equal to 1000); the devices restart within 15 minutes; in case all the servers are not working properly. In this way, the system continues to operate and you have a malfunction of only about 15 minutes.

In systems with more than 1000 IP devices or apartments or users at least one 1060/1 Server is needed; it is important to keep in mind, however, that in case of malfunction of the only server, the devices do not restart automatically and therefore the system no longer works properly. Therefore, if there are more than 1000 devices and/or apartments and/or users, it is advisable to have more than one server in the system; in this way, if one server is no longer working, the presence of other servers guarantees the correct functioning of the system.

The same goes for an IPerCom system in IPerCloud mode where at least the presence of a 1060/1 Server is required: if the only 1060/1 Server present in the system no longer functions correctly, the entire system stops working.

In "[APPENDIX P3: Replacing a 1060/1 Server that is no longer working.](#)" the procedure for replacing a 1060/1 Server is shown in any case.

## ADDING A SERVER TO THE SYSTEM

To add a 1060/1 *Server* (not configured and with default settings) to a system in "without server" mode, it is necessary in a first step to connect only the 1060/1 *Server* to the PC (not to the IPerCom system) and perform the following operations in the order shown.

1. upgrade with *IPerUpgrade* the 1060/1 *Server* to the same IPerCom version present on the system;
2. through *IPerCom Installer Tools* open the project related to the system on which you want to add the 1060/1 *Server*;
3. add 1060/1 *Server* with its MAC address to the configuration and apply (in this case to 1060/1 *Server* only) the new configuration;
4. save the changes you have just made, close the site, disconnect 1060/1 *Server* from your PC, and turn it off.

At this point, you can connect the 1060/1 *Server* to the IPerCom system, turn it on and wait about 10 minutes for the devices to restart to switch to "with server" mode.

By connecting to the system through *IPerCom Installer Tools*, it is possible to verify that all the devices of the system have the same configuration and that the system itself is in "server" mode.

If 1060/1 *Server* is added when the *IPerCom Installer Tools* application is running, the following message appears:

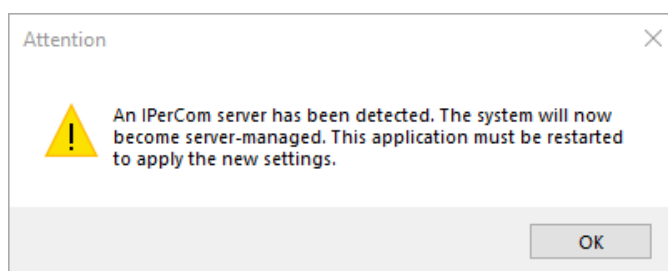


Figure 187: detecting one or more servers on the system

Pressing the "OK" button to restart the application.

## IMPORTING OR CREATING A NEW CONFIGURATION ON THE SYSTEM

To create or import a new configuration on an already configured system, it is necessary to delete the configuration already existing on the various devices. In fact, if the system has already been configured, it has its own identifier (**System ID** field): in this situation the attempt to import other configurations with different ID into the system is blocked to avoid the irreversible loss of the work already done.

If, however, it is necessary to change a configuration previously made, the only way to do this is to delete it from all the devices in the system and then reset these devices to factory settings.

To do this it is necessary to press the "*Erase configuration on all devices*" button:

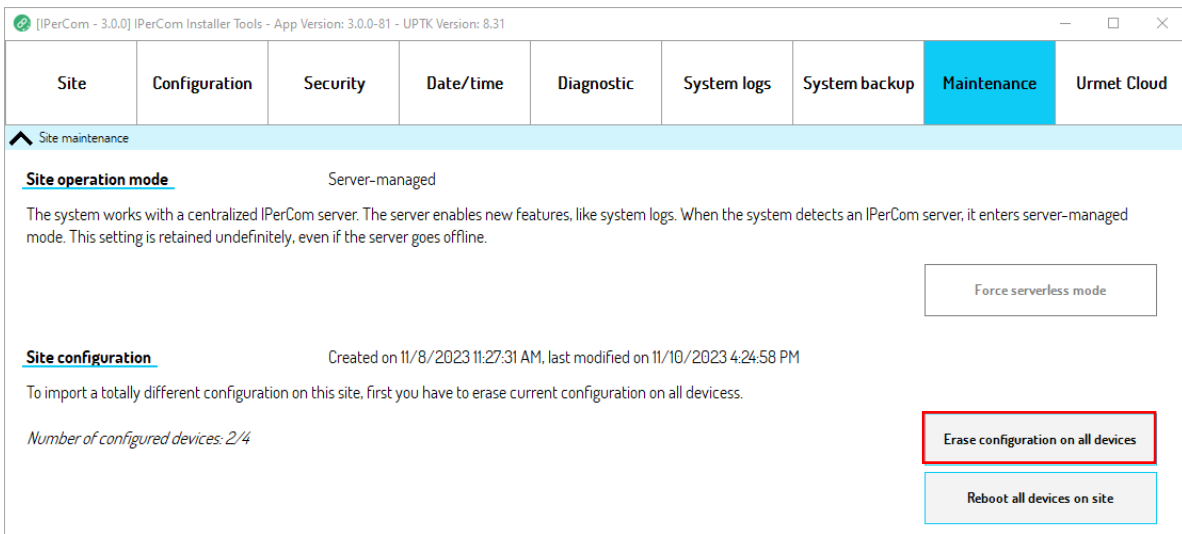


Figure 188: "Maintenance" tab - deleting the configuration

The following pop-up window is displayed:



Figure 189: request to delete the configuration from the system devices



*Deleting the configuration will reboot the devices. Those equipped with display start with the screen that contains, among other things, the information "Not configured".*

Press the "OK" button to delete the configuration from all the devices in the system to bring them back to factory settings and create automatically a backup file of the previous configuration.

At the end of the procedure, *IPCom Installer Tools* shows the following pop-up window:

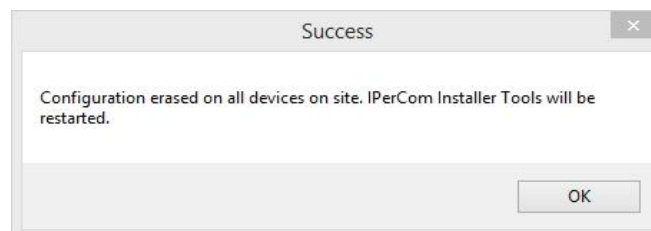



Figure 190: configuration deletion successfully performed

Press the "OK" button to restart the application.

Now it is possible to configure again the site creating a new project or opening another project and apply the configuration.

 *If the project associated to the system whose devices have been brought back to the factory configuration is opened again, IPerCom Installer Tools shows a dialogue box that warns installer that configuration associated to this project (saved through backup) will be imported in automatic way. Pressing the "OK" button, configurator opens with the old project: simply save it to associate the old configuration and transfer it to the system after connecting.*

## SYSTEM RESTART

The "Reboot all devices on site" button (red box) allows you to restart all devices in the system:

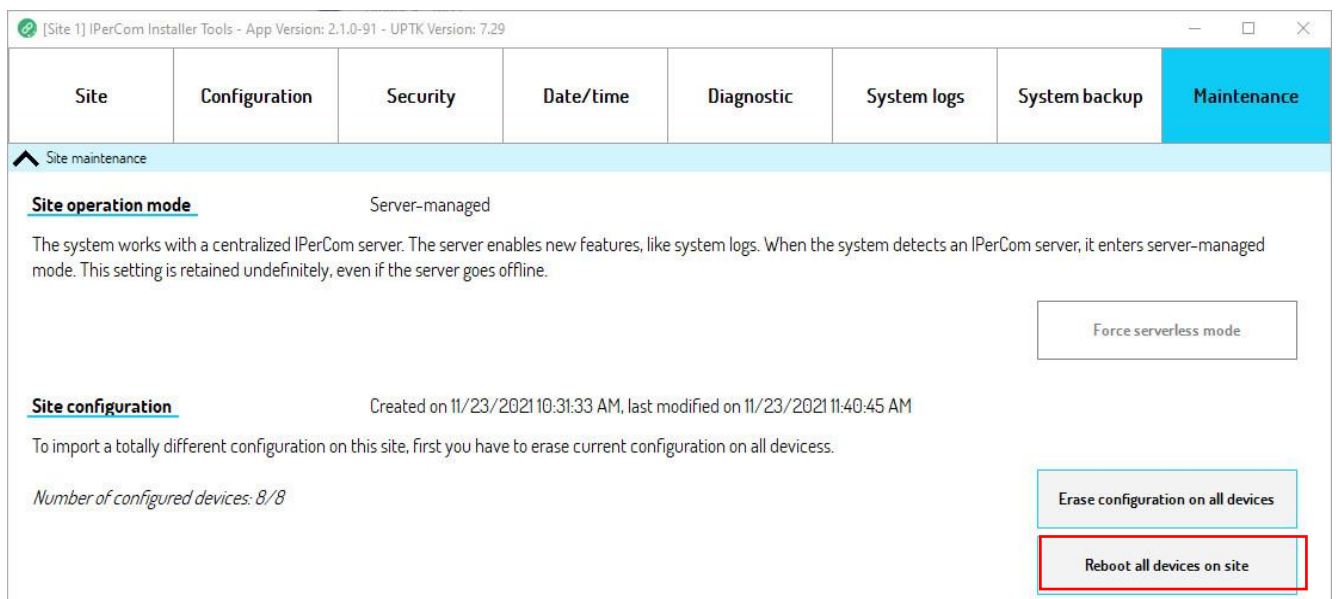


Figure 191: "Maintenance" tab - restarting the devices in the system

The function is useful if one or more devices are connected to a system and these devices are:

- not aligned with the IPerCom version already present on the system,
- present in the configuration.

As written in the paragraph [Device/application firmware upgrade](#), a warning message indicating the presence of misaligned devices appears on the video door phones, *Switchboard*, *iPerCom Client* and *iPerCom Installer Tools* applications. The message is like the one reported below:



Figure 192: Presence of devices with UPTK versions not aligned

The fastest way to bring the system back to normal operation involves:

- disconnect unaligned devices,
- press the “OK” button in the above window relating to *iPerCom Installer Tools*,
- go to the “Maintenance” tab,
- press the “Reboot all devices on site” button.

In this way all the devices in the system restart and thus avoid having to manually restart each individual video door phone, a very difficult operation in medium or large sized systems.



*The message shown in the figure disappears automatically once the not-aligned devices are disconnected but it may be necessary to wait up to 30 minutes for this to happen on all the video door phones.*



## ENABLING/DISABLING ACCESS TO IPerCOM CONFIGURATION FROM A MAX, VOG7 OR BASIC VIDEO DOOR PHONE THAT HAS NOT BEEN CONFIGURED YET

Access to the IperCom configuration by *MAX*, *VOG7* or *Basic* video door phones not yet configured and connected to the system is enabled (default value). To disable access to the IperCom simply press the "Prevent access" button in the relevant section "Access to IPerCom configuration from video door phones":

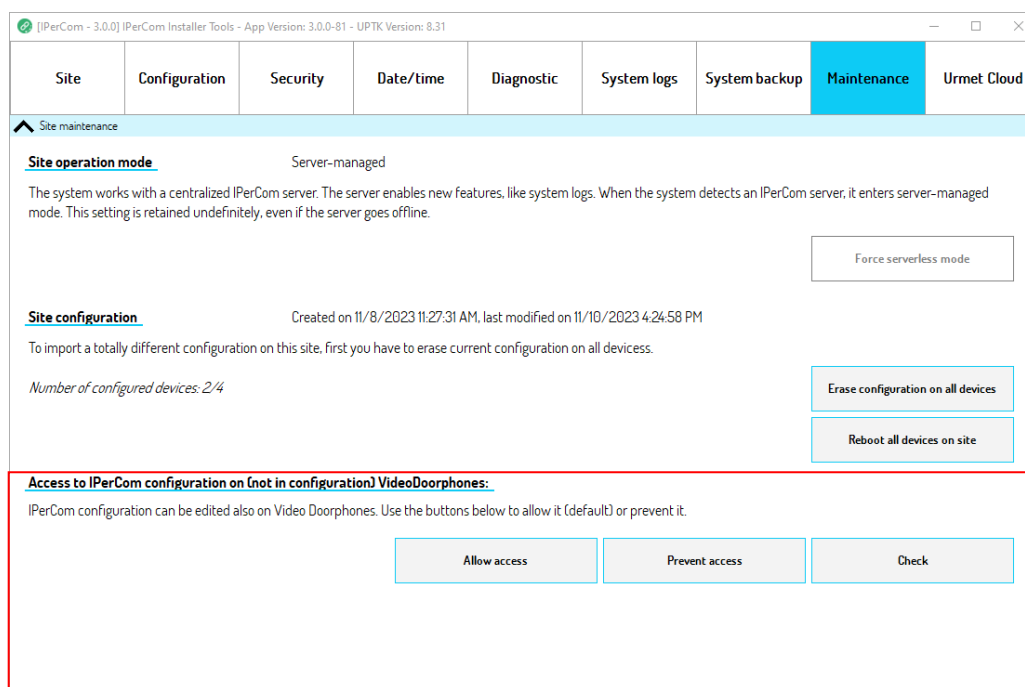


Figure 193: "Maintenance" tab - access to IPerCom configuration

The correct outcome of the operation is confirmed by the following pop-up window:

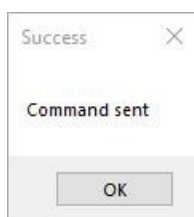


Figure 194: access to IPerCom configuration not possible

Similarly, if you want again to enable access, simply press the "Allow Access" button. Also in this case, the correct outcome of the operation is confirmed by a similar pop-up window.

The "Check" button lets you know if access to the configuration is enabled or not on all video door phones of the plant (configured and not configured).



For details on how to access IPerCom configuration from *MAX*, *VOG7* or *Basic* video door phones, please refer to the relevant manuals available at [www.urmet.com](http://www.urmet.com).

#### 6.15.8 Devices not aligned to the same IPerCom or software development platform (UPTK) version

The possible presence of a misalignment between the UPTK versions of the devices and/or software applications is reported by the *IPerCom Installer Tools* application, which compares it with its own local UPTK version. The report is made after opening a project and connecting to the relevant site. A misalignment between UPTK versions simply implies the presence in the system of devices/applications with different IPerCom versions.

The most common cases of misalignment can occur in the following 3 ways:

1. with the system and software application aligned, one or more devices that are not updated to the same IPerCom version of the system and are not present in the system configuration are connected to the system;
2. with the system and software application aligned, one or more devices that are not updated to the same IPerCom version of the system but are present in the system configuration are connected to the system;
3. *Switchboard* and/or *IPerCom Client* applications present in the system configuration have not been updated to the latest IPerCom version present on the system.

What happens in the three cases reported above is reported in detail.

## CASE 1

The misalignment is reported by *IPerCom Installer Tools* via the dialog box shown below:

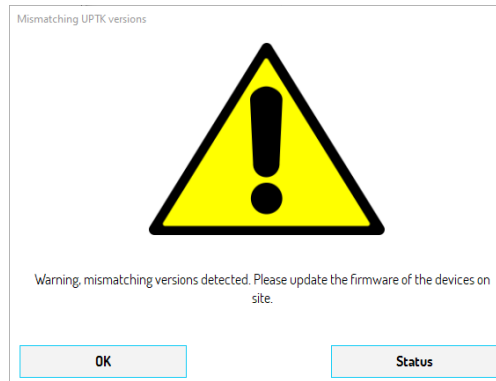


Figure 195: UPTK version misalignment reported on *IPerCom Installer Tools*

By pressing the "Status" button, the devices (or device) whose UPTK version (for example 8.22) is not aligned with that of *IPerCom Installer Tools* (for example 8.31) are displayed:

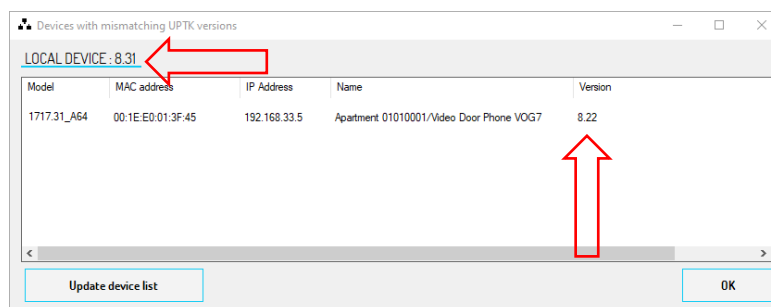


Figure 196: list of devices whose UPTK version is not aligned with the local version

By pressing the "OK" button in [Figure 195](#) the dialog box disappears and it is still possible to continue using *IPerCom Installer Tools* in all its functions.

## CASE 2

The misalignment is reported by *IPerCom Installer Tools* via the dialog box shown below:

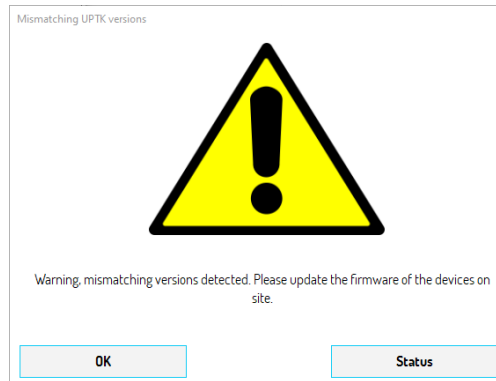


Figure 197: UPTK version misalignment reported on *IPerCom Installer Tools*

By pressing the "Status" button, the devices (or device) whose UPTK version is not aligned with that of *IPerCom Installer Tools* are displayed, in the same way as written in the previous case.

By pressing the "OK" button the dialog box disappears and you can continue to use *IPerCom Installer Tools* in all its functions.

### CASE 3

The misalignment is reported both by the software application and by *IPerCom Installer Tools* in the same ways described in the previous points. For example, if the *Switchboard* application has not been updated to the latest IPerCom version present on the system, after connecting to the system itself, the *IPerCom Installer Tools* application displays the following dialogue window:

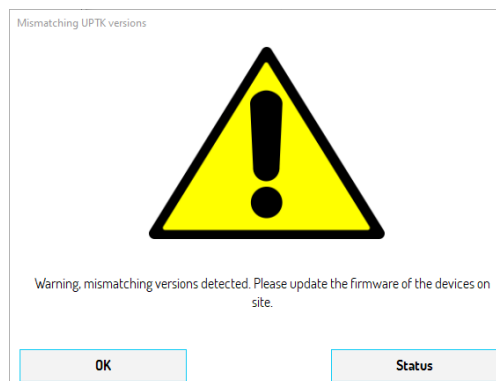


Figure 198: UPTK version misalignment reported on IPerCom Installer Tools

By pressing the “OK” button the dialog box disappears and you can continue to use *IPerCom Installer Tools* in all its functions.

By pressing the “Status” button, *Switchboard* application whose UPTK version is not aligned with that of the system is displayed:

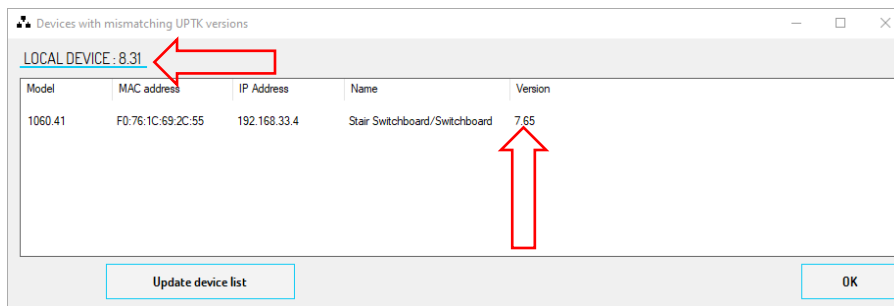


Figure 199: Switchboard application with UPTK not aligned

According to what is written above, it is therefore of fundamental importance:

- add new devices to a system only after having updated them to the correct IPerCom version using the *IPerUpgrade* application for Windows operating system, available with the relevant manual on the website [www.urmet.com](http://www.urmet.com);
- always update (also via the *IPerUpgrade* application) the *Switchboard* and *IPerCom Client* applications when a system has been updated to a more recent IPerCom version.



*The Switchboard and IPerCom Client applications can also be updated by downloading the relevant executable files from the website [www.urmet.com](http://www.urmet.com).*

If one or more 1060/1 Servers are present in the system and in configuration and at least one has the “Automatic update by Server” option enabled, it is also possible to connect devices to the system that are not aligned with the correct IPerCom version: these will be updated automatically by the *Server* itself. Similarly, if you start one of the out-of-date *Switchboard* and *IPerCom Client* applications, the *Server* will take care of updating them to the correct version.

After updating the non-aligned devices to the correct IPerCom version, the screen notifying the misalignment automatically disappears.

If the not-aligned devices are disconnected from the system, the message on *IPerCom Installer Tools* automatically disappears in the following cases:

- system without *Server* 1060/1 and not-aligned devices not present in the system configuration;
- system without *Server* 1060/1 and not-aligned devices present in the system configuration;
- system with *Server* 1060/1 and not-aligned devices present in the system configuration.

If there is a 1060/1 *Server* in the system and the not-aligned devices are not in configuration, every time *IPerCom Installer Tools* is started, the dialog box indicating the presence of not-aligned devices is shown, even if these have been disconnected from the system.

In this case after pressing the “*Status*” button, simply press the “*Update device list*” button, as shown below:

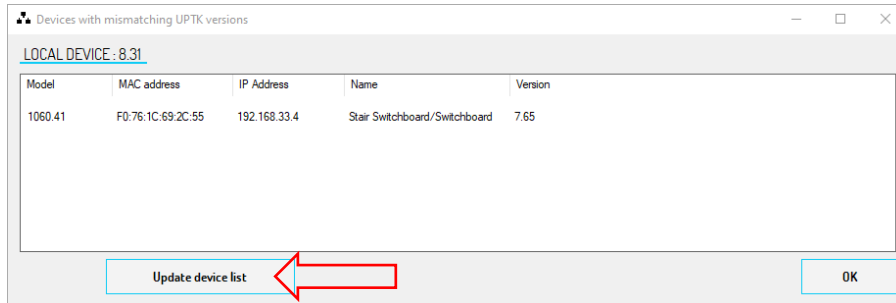


Figure 200: “*Update device list*” button

The following message is shown with the request to restart both *iPerCom Installer Tools* and the system:

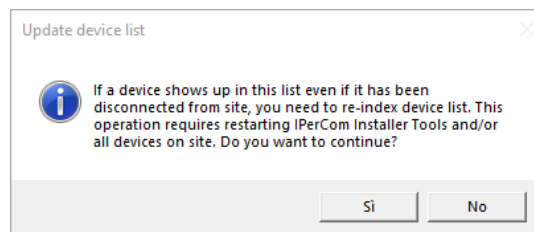


Figure 201: request to restart the system

By pressing “*Yes*”, all the system devices are restarted and at the end of the operation the following message is displayed:

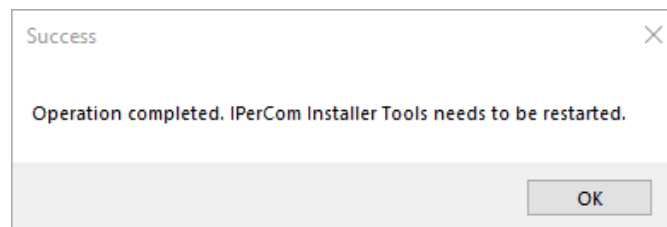


Figure 202: request to restart *iPerCom Installer Tools*

In this way, the next time *iPerCom Installer Tools* is started, it will not show any message indicating the presence of misaligned devices/software applications.

### 6.15.8.1 IPerCom Installer tools application not aligned to the same IPerCom or software development platform (UPTK) version

If a PC with a version of *IPerCom Installer Tools* whose version is not updated to that of the rest of the system is connected to a regularly functioning system, as soon as you connect to the system *IPerCom Installer Tools* signals the misalignment via the dialog box below:

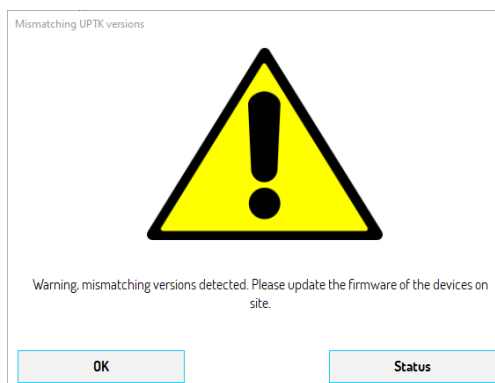


Figure 203: UPTK version misalignment reported on IPerCom Installer Tools

By pressing the "Status" button, the following window is displayed:

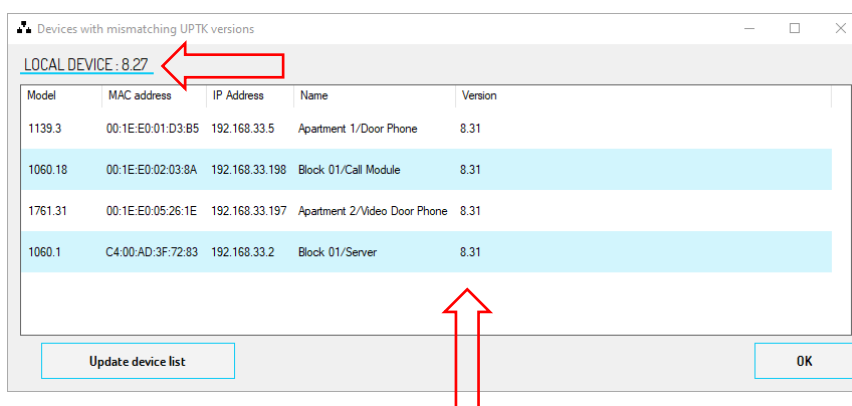



Figure 204: IPerCom Installer Tools not aligned with the system

You can see how the local version of UPTK (that of the *IPerCom Installer Tools* application) is not the same as that of the system: in this situation it is necessary to update *IPerCom Installer Tools* to the correct version. The various officially released versions of IPerCom Installer Tools are available for download on [www.urmet.com](http://www.urmet.com) website.



## 7 The configurator

The *configurator* allows defining the system topology, associating the various devices to the system nodes, creating directories, activation rules, access control rules, residents, and non-residents, setting the operating mode of the system.

 *The configurator is integrated in both IPerCom Installer Tools and the MAX, VOG<sup>7</sup> or Basic video door phones and the operating mode is similar.*

In both cases it is necessary to create the system configuration by defining (as described later) the system project. In the next paragraphs the use of the *configurator* within *IPerCom Installer Tools* is explained.

### 7.1 Creating or editing the configuration file from *IPerCom Installer Tools*

The creation (or modification) of the configuration is done through the “*Configuration*” tab, after opening a project.

The buttons to create a new configuration or modify an existing one are shown below and are active according to the description below:

- “*Create*”, to create a new configuration (if you are not connected to a system or you are connected to a system without configuration);
- “*From File*”, to import the configuration from an external .ccf file (with the constraints described in the previous paragraphs, connected or not connected to a system) and modify it;
- “*From system*”, to import the configuration from the system to which you are connected (with the constraints described in the previous paragraphs) and modify it;
- “*Edit*”, to edit an already existing configuration (connected or not connected to a system).

It is also possible to modify a configuration by opening directly a file with the ccf extension (that is, by double clicking with the mouse on the file in question). After doing this, you are asked to enter the installer password, with which the configuration file was saved and you can make changes. If the configuration file was created through the 3.0.0 *configurator* of *IPerCom Installer Tools* and has *CallMe Manager* support enabled, it is not possible to modify and save the configuration except through the same *configurator* started by *IPerCom Installer Tools*, as shown by following message:

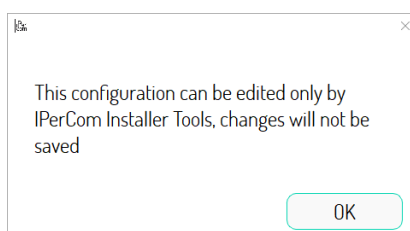


Figure 205: configuration not editable

The configuration creation (and thus the *configurator*) allows you to:

- define the system topology,
- add IPerCloud apartments (if present),
- add the devices on the topological nodes of the system,
- customize the system (assigning appropriate names to apartments, topological nodes, devices, etc.),
- define the address books,
- create the activation rules,
- create users (residents and non-residents),
- set the access control,
- configure system parameters and call forwarding.

All these points will be explained in detail in the following paragraphs.

### 7.1.1 Selecting the system topology (model) and the *configurator* structure

To create a new configuration, simply press the “Create” button in the “Configuration” tab. The following screen is displayed:

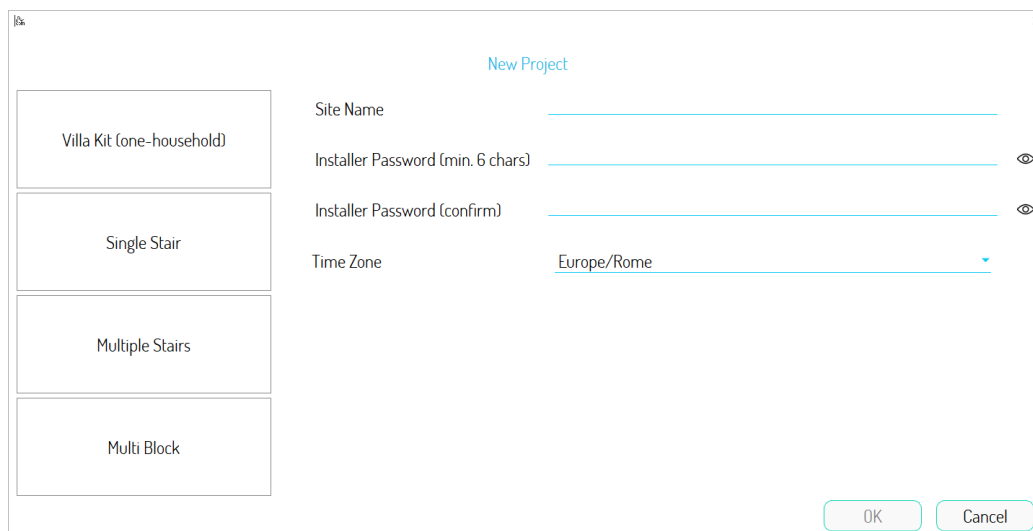





Figure 206: system topology

In this screen it is possible to define the main data to create a new project (from which you can start to create the system configuration). The data are the following ones:

- site name;
- installer password;
- system model (or topology);
- time zone.

 The name of the site is the one that will then appear in the IPerCom Installer Tools application in the "Site" tab in the relevant "Site Name" field, after aligning the project configuration with that of the system.

 To enter the name of the project and the installer password use the alphanumeric keyboard present in the configurator. Special characters (for example the "emoticons") may not be displayed correctly (also on Call Module or Switchboard or Modular entry panel with 1060/48). It is therefore advisable to check the correct display of the characters on the system devices and configurator at the end of the configuration.

 If, instead of creating a new configuration, you want to modify an existing one, the configurator is opened with the configuration present on the system, after entering the installer password.


As for the choice of the plant model, there are 4 options available, depending on your needs:

1. *Villa Kit (one-household)*
2. *Single Stair*
3. *Multiple Stairs*
4. *Multi Block*

The choice of a plant model rather than another determines the topological structure of the plant model itself and the behaviour of the network interfaces of the *MAX video door phones* in the system; if you are not sure of the choice, we recommend to select the most generic model, i.e. *Multi Block*.

As for the plant models *Multiple Stairs* and *Multi Block*, these are the only ones that allows placing both secondary and primary *Call Modules*.

The *Kit Villa (single-family)* model, on the other hand, is the only one that allows video door phones to access the Internet via the *ETH0* network interface, which is not normally used for this purpose. For the other system models, the video door phones access to the Internet via the *ETH1/WiFi* network interfaces (if present).

 The *ETH1/WiFi* interfaces (used by third-party apps on the video door phones to access the Internet) must never be connected to networks without Internet access as this compromises the device's call forwarding performance.

Once all the fields have been filled in and the desired model has been selected, by pressing “OK” a basic project will be created and the “Topology” tab will be displayed:

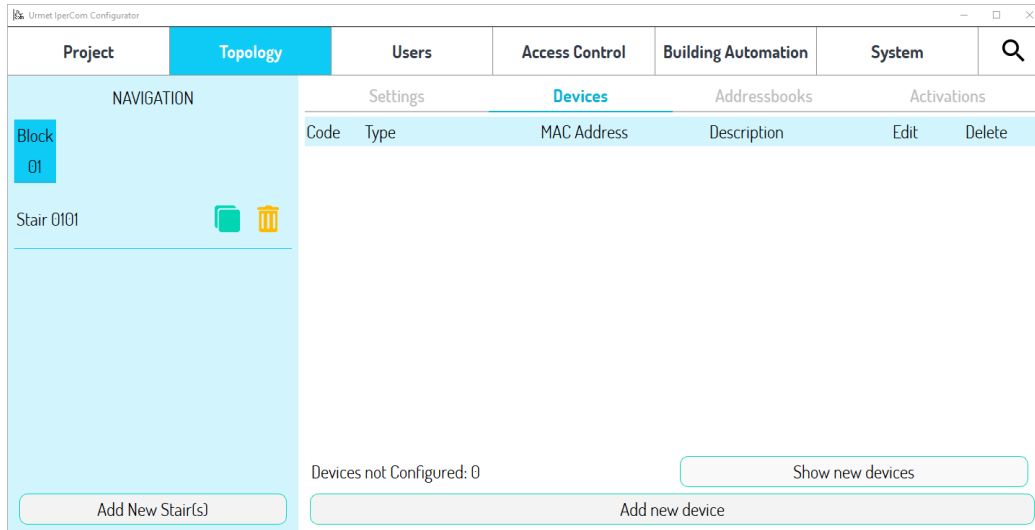


Figure 207: “Topology” tab of a “Multiple Stairs” configuration

The shown screen is related to the case in which the *Multiple Stairs* topology was chosen during the project creation phase.

To browse through the various topological nodes, it is necessary to use the navigation module, visible on the left in Figure:

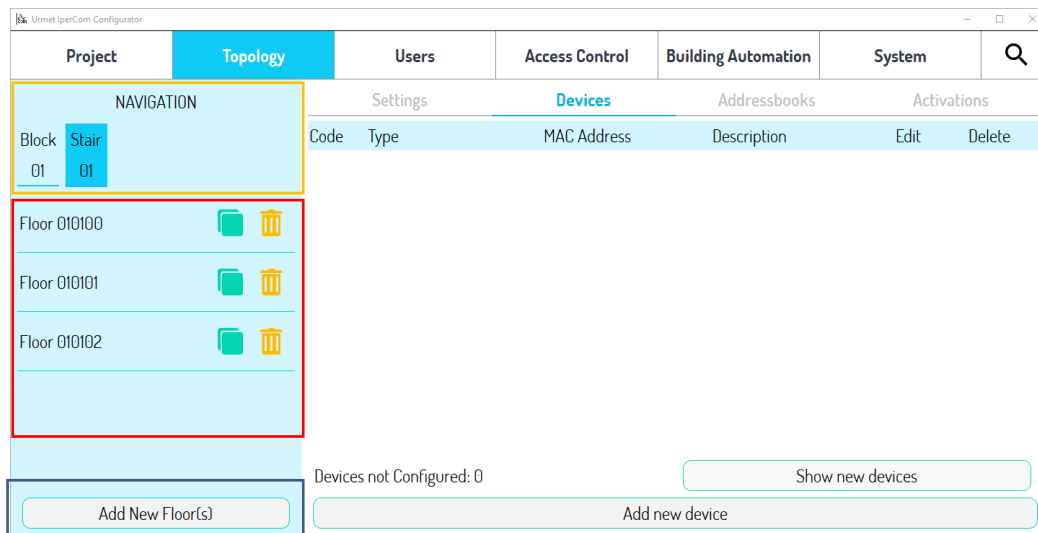




Figure 208: Example of navigation in topology for a “Multiple Stairs” project


it is possible to identify three zones:

- an upper part (in yellow), showing the current topological node;
- a central part (in red), with a list of all the topological nodes that derive directly from it;
- a lower button (in blue), to add new nodes to the topology.

Two buttons are available for the topological nodes:

-  clone, which allows you to create an identical copy of the topological node and of all the nodes that derive from it; this button is not available in case of apartments.
-  delete, which allows removing the topological node and all the nodes that derive from it.

When creating the topology, it must be considered that *IPerCom* supports a maximum number of 99 blocks, a maximum number of stairs per block of 30, and a maximum number of floors per stair of 1000. Therefore, a maximum of 1000 apartments can be added to each floor, for a **maximum of 1000 apartments in total in the entire system**.


 *It is also possible to define several underground floors among the floors, identified (within a site, block, and staircase) by the code U1, U2 and so on up to the code ZZ. For example, on the staircase 010101##### the first underground floor has topological code 010101U1##.*


The overall number of apartments on a system remains limited and is linked to the presence or absence of a 1060/1 Server on the system, as is the overall number of topological nodes, devices, and users.

The following table shows the number of apartments/devices/users (residents and non-residents) for which the presence of a Server 1060/1 is not required (green line) or is required (yellow line):

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

*Table 8: Presence of at least one 1060/1 Server in IPerCom systems*

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

 *The total number of residents and non-residents must be less than or equal to 1000 for the system to function correctly without any 1060/1 Server.*

If the presence of a 1060/1 Server is requested, the configurator signals its lack in the configuration via a message when saving the configuration itself (see paragraph [How to save the configuration](#)):

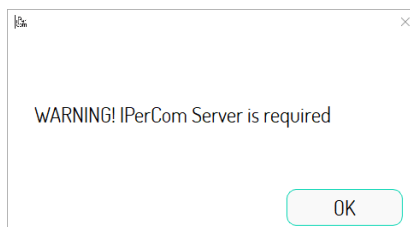


Figure 209: message on configurator in the absence of Server 1060/1

If the 1060/1 Server is added to the configuration but is not physically installed on the system, during the saving phase the *configurator* allows you to save the configuration but when you try to apply it via *IPerCom Installer Tools* the following message is shown:

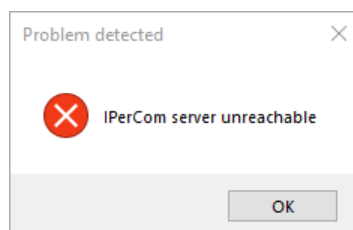


Figure 210: message on IPerCom Installer Tools in the presence of Server 1060/1 added on the configurator but not present on the system

In addition, the *MAX*, *VOG<sup>7</sup>*, *VOG<sup>5</sup>*, *VOG<sup>5+</sup>* video door phones, *Switchboard* and *IPerCom Client* applications show a screen like the one below:

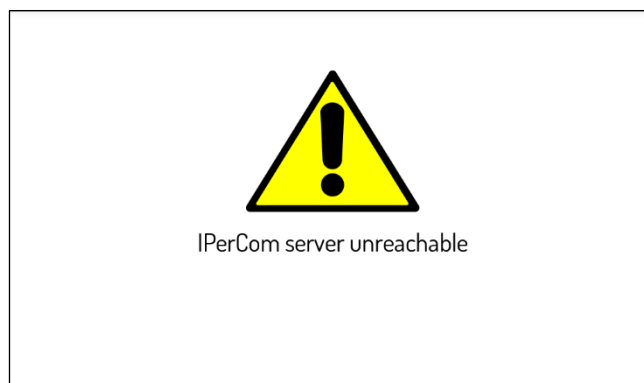


Figure 211: message on MAX, VOG<sup>7</sup>, VOG<sup>5</sup>, VOG<sup>5+</sup>, Switchboard and IPerCom Client in the presence of Server 1060/1 added on the configurator but not present on the system

Calling stations equipped with displays also show a screen indicating that the device is not configured.

The screens below refer to systems without Server 1060/1.

In the context module within “Topology” it is possible to access 4 configuration panels that allow you to make changes related to the current node:

- “Settings”, that allows accessing the node properties;
- “Devices”, that allows adding/modifying/removing devices;
- “Address books”, that allows creating the address books used by above all by apartment station;
- “Activations”, that allows activating *Relay Actuators* outputs.

The “Project” tab can be used to set all the basic information of the project.

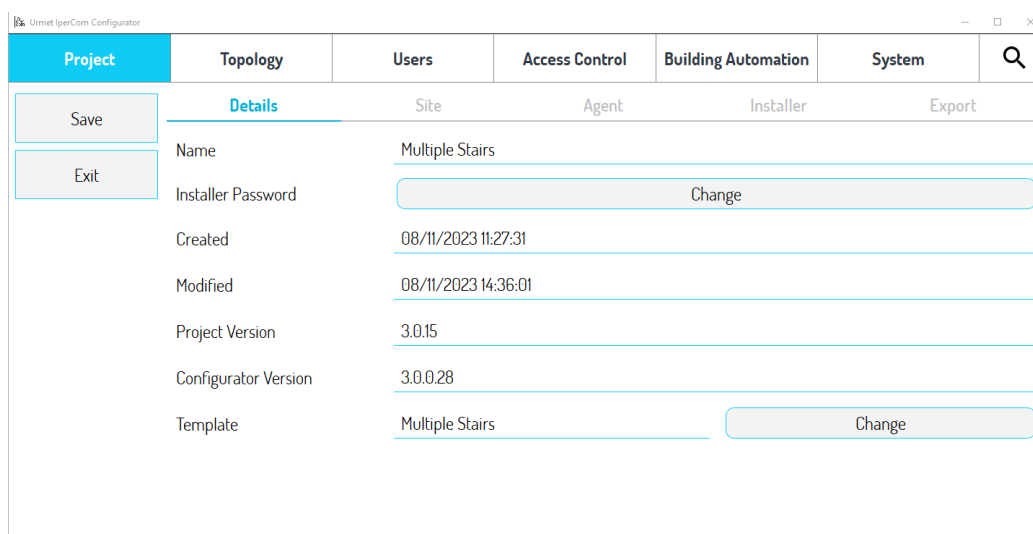


Figure 212: “Project” tab of a multiple stair configuration

It is possible to distinguish the following 5 tabs:

#### Details

The tab contains some general information about the project (name, creation and modification dates, project version and version of the *configurator* with which it was created) and allows you to change the installer password and the project template;

#### Website

The tab allows you to enter all the information regarding the system site address.

#### Agent

The tab allows you to enter all the information concerning the personal details of the agent who commissioned the system.

#### Installer

The tab allows you to enter all the information concerning the personal details of the system installer.

## Export

The tab allows you to:

- export a file in html format that contains a summary of the topology and the devices that make up the system;
- export a file in xml format useful for the integration of the IPerCom system with the IPassan access control system (for further details see "[APPENDIX O: IPassan integration with IPerCom](#)").

About the summary in html format of the system, it is possible to:

- choose whether to export information about nodes or devices in the system or both;
- choose from which node to export the above information.
- sort the devices by MAC address or topological address.

For each node, the name, the type (if site node, block or other), the topological code and whether it is a 2Voice node is shown; in case of 2Voice apartment, the configuration of the dip-switches is also shown (for further details see paragraph "[Adding a Gateway IPerCom-2Voice on a stair node](#)").

For each device, the MAC address, the device type, the name, and the topological node where it has been added is shown (for further details see paragraph "[Adding devices](#)").

The installer can use the "Change" button in "Project" field of the "Details" tabs to change the system model. Press the button to open a dialogue box in which you can select the desired new model.

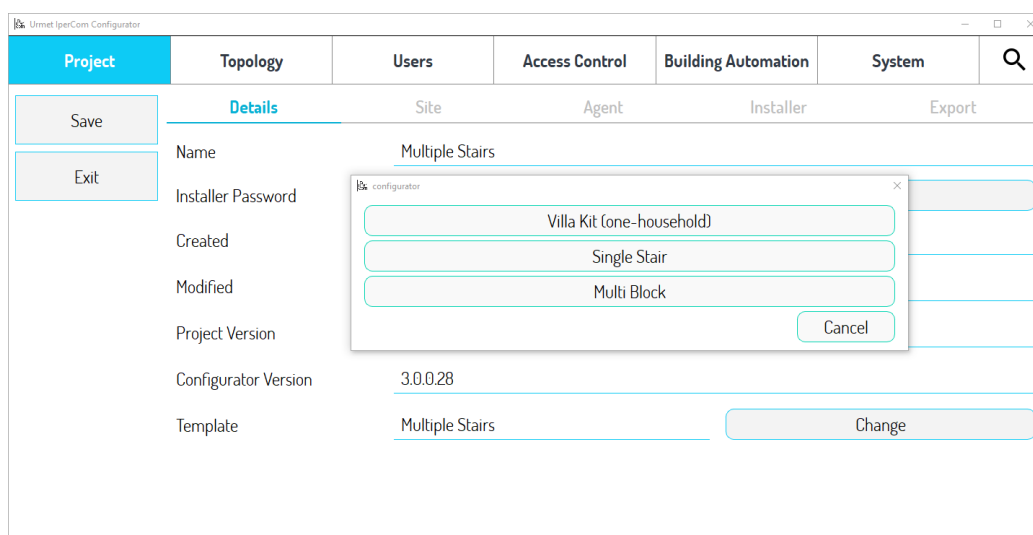


Figure 213: Changing the system model

If you go from a simpler model to a more complex one (e.g., from a "Villa Kit" model to a "Multiple Stairs" model), conversion is immediate and no further intervention by the user is required. If you go from a more complex system model to a simpler one (e.g., from a "Multi Block" model a "Single Stair" model), you may need to remove the topological nodes in excess and shift the devices.



Transition from one system model to another is usually required in the following cases:

- if the model was not chosen correctly during the creation phase of the project;
- if the system layout greatly evolved after the project was created.

For example, if you have a "Single Stair" project model and only later you discover that main and secondary Call Modules are needed (which requires a "Multiple Stairs" or "Multi Block" model), you will need to change the model in the configuration to meet the new specifications.

The various types of system are now described in more detail.

### 7.1.1.1 Villa Kit (one-household) systems

The **Villa Kit (one-household)** systems are those systems with one floor and only one apartment where up to 20 apartment station can be installed.

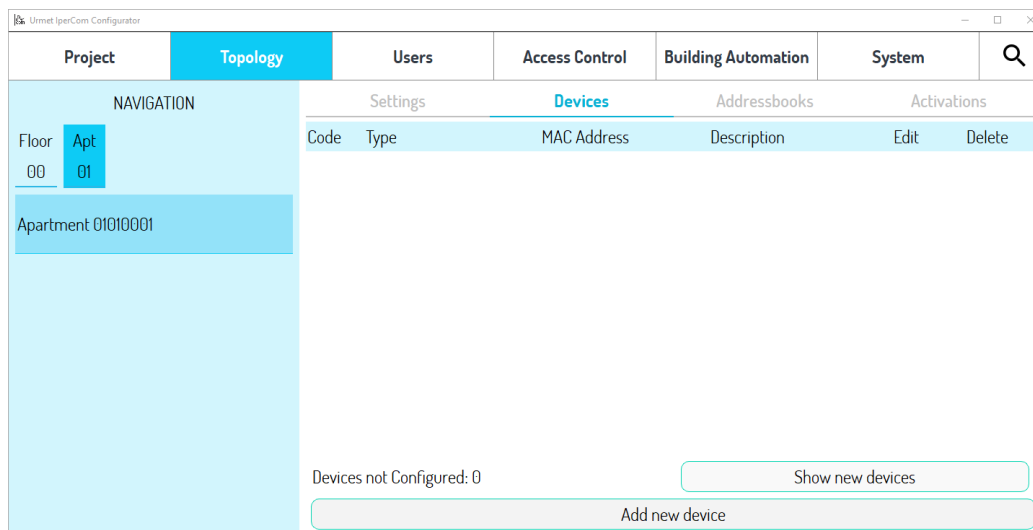


Figure 214: "Topology" tab for Villa Kit (one-household) system

The "Villa Kit (one-household)" systems are those systems with one floor and only one apartment where up to 20 devices can be installed between apartment stations.

### 7.1.1.2 Single Stair systems

The **single stair** systems are characterised by the fact that all the apartments are arranged on the floors belonging to a single stair. This mode is also suitable for two-family systems. On this system it is possible to have any number of apartments and floors on which *IPerCom* devices will be placed.

By selecting *Single Stair* as plant model, a stair with a floor and a single apartment is created automatically.

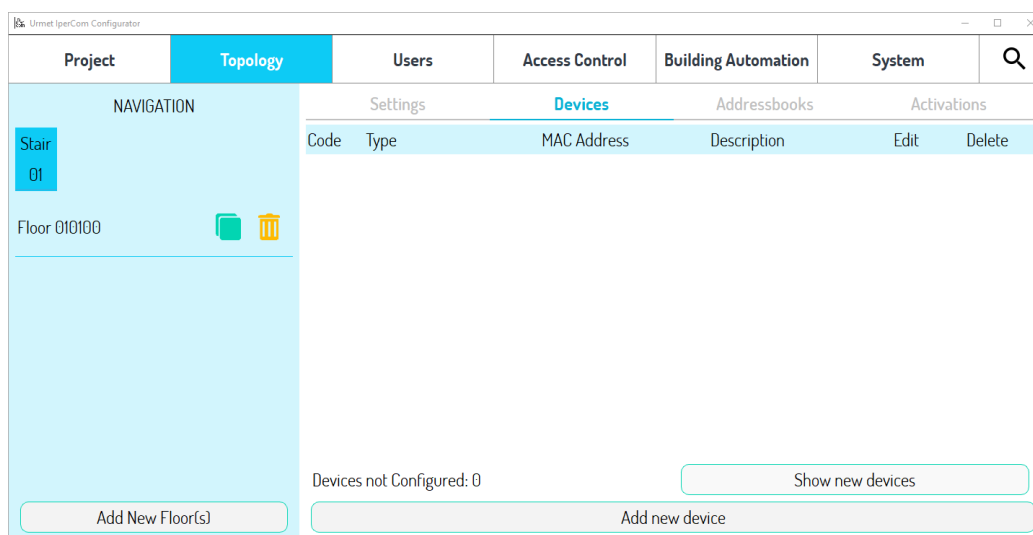


Figure 215: "Topology" tab for Single Stair system

It will then be possible to add the desired number of floors and the relevant apartments by clicking on the relevant button at the bottom of the navigation module.

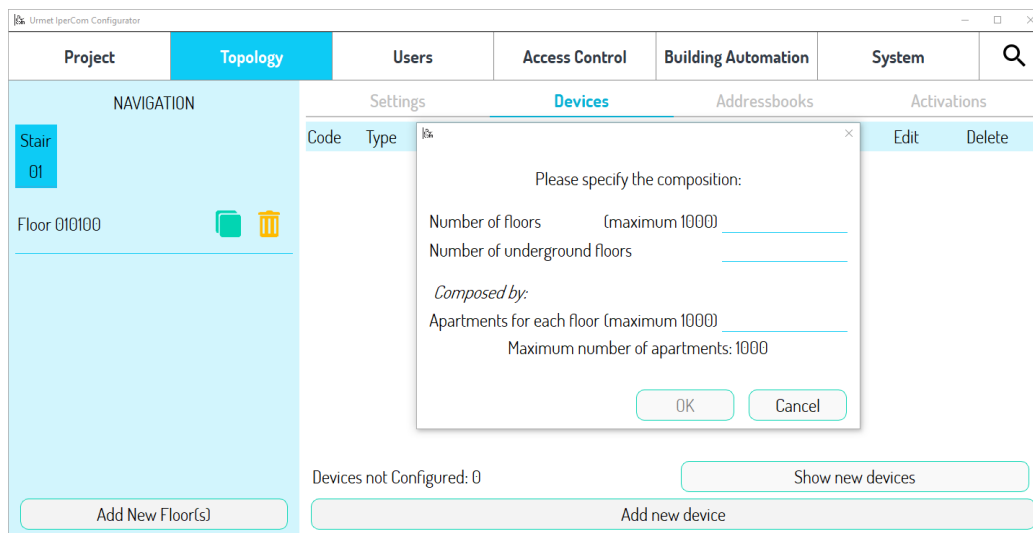


Figure 216: Adding of new floors to the topology

### 7.1.1.3 Multiple Stairs systems

If the system topology consists of several stairs within the same block, a **Multiple Stairs** configuration can be created.

In this case a block is automatically created with one stair, one floor and a single apartment.

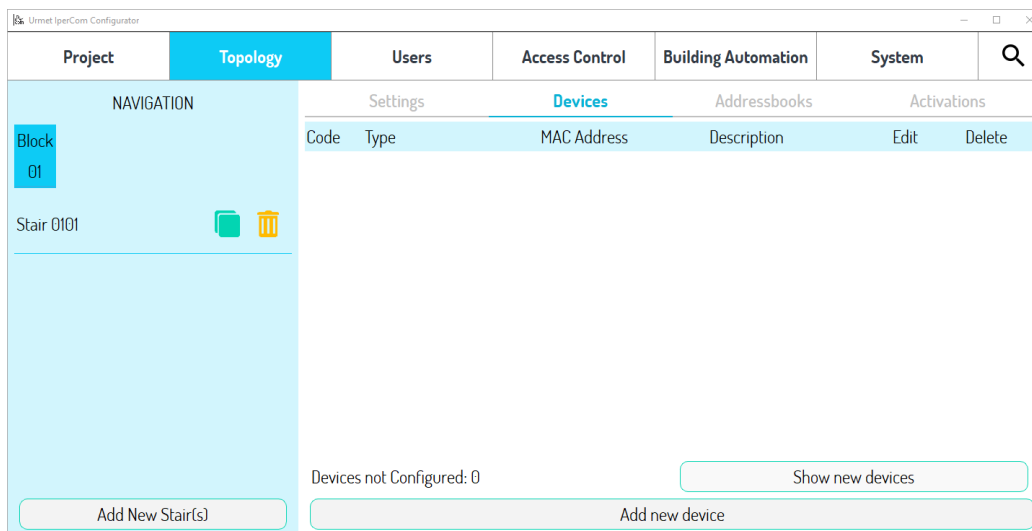


Figure 217: "Topology" tab for Multiple Stairs system

If you need to add or remove stairs/floors/apartments, you can do it in subsequent steps using the relevant button at the bottom of the navigation module.

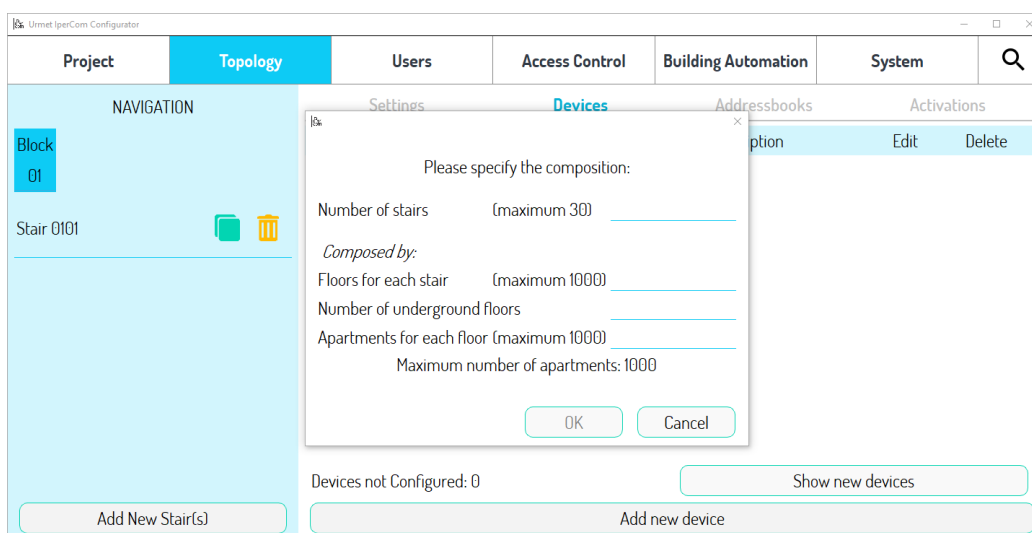


Figure 218: Adding of new stairs to the topology

### 7.1.1.4 Multi Block systems

The last type of plant model supported by the *configurator* is the **Multi Block** one, that allows creating a project with any number of blocks/stairs/floors/apartments.

The selection of *Multi Block* as plant model automatically leads to the creation of a site without blocks, as shown in the following figure:

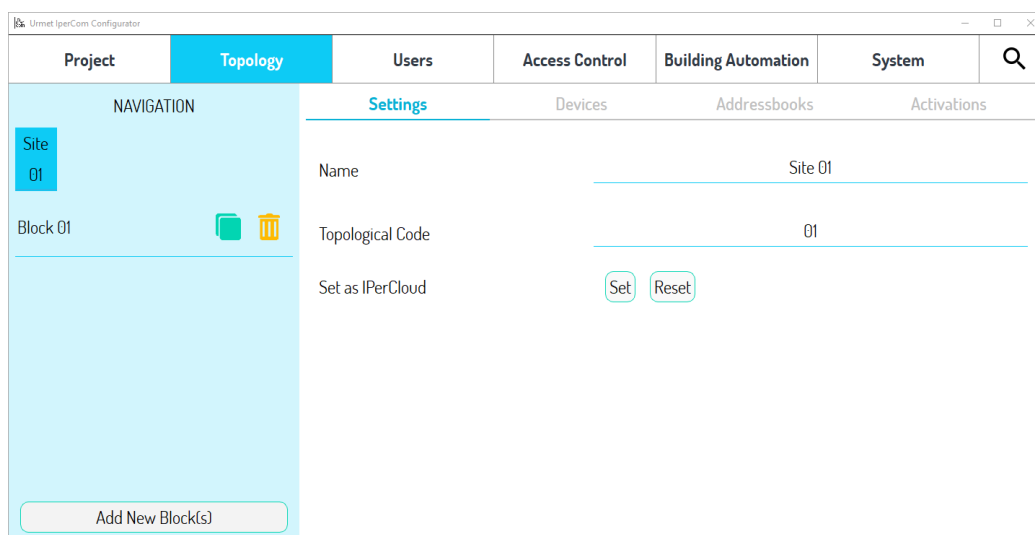


Figure 219: "Topology" tab for Multiple Block system

As in the previous cases it will be possible to add all the blocks with their stairs/floors/apartments with a single command.

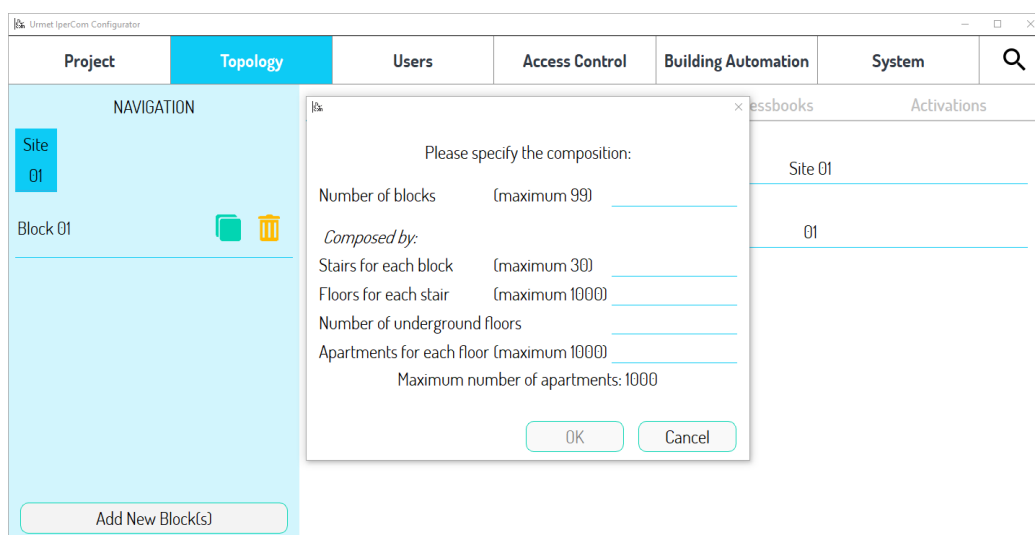


Figure 220: adding of new blocks to the topology

If the topological structure of the system is not homogeneous, it will be possible to add/remove blocks/floors/stairs/apartments later.

The configurations are created and edited using the *IPerCom Configurator* application, also known as the *configurator*.

The *configurator* consists of three main components, shown in the following figure:

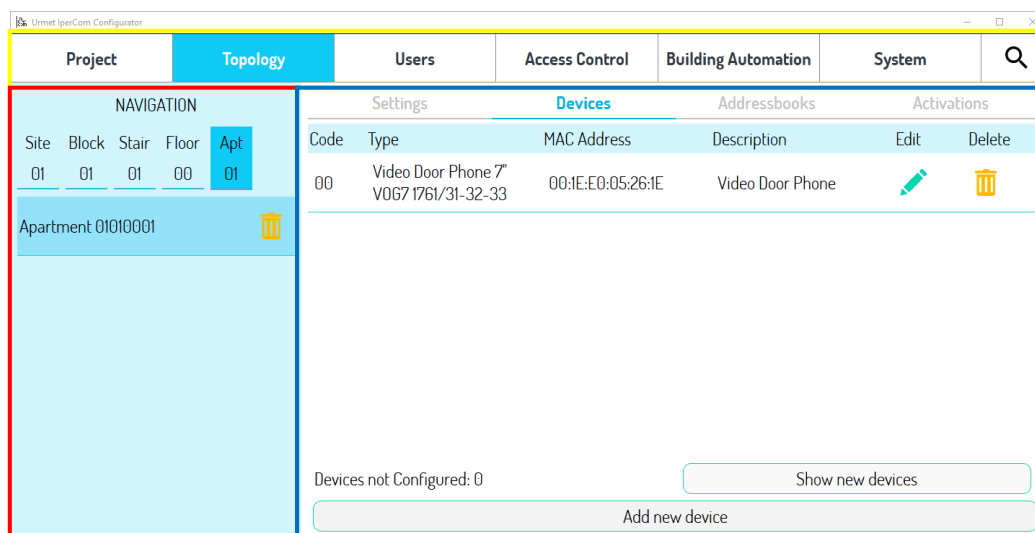


Figure 221: Main components of the configurator

It is possible to see:

- an *upper bar* (in yellow), which allows accessing to the main functions through the following items:
  - “*Project*”, to set the basic information about the project (name, installer password, etc.);
  - “*Topology*”, to change the system topology, add devices, create address books and set activations;
  - “*Users*”, to add residents and non-residents, as well as users enabled to access the *Switchboard* application, “*Access Control*”, to set the rules to access the system;
  - “*Building Automation*”, to define the activation rules of *Relay Actuator* of the system;
  - “*System*”, for the system global settings;
  - “*Search*”, to perform a fast search among the system elements.
- a *navigation module* (in red), to view and add/modify/remove system topological nodes: blocks, stairs, floors, and apartments;
- a *context module* (in blue), to set the configuration parameters.

### 7.1.2 Adding devices

Once the topology has been defined, it will be possible to add the devices in the system configuration.

There are 3 different ways to configure the devices, depending on whether you are connected to the system via PC.

In any case, regardless of the chosen installation mode and topology, it is necessary to associate each device to a topological node, bearing in mind that:

- calling stations (except *Private Call Module 1060/22*) and *Switchboards* cannot be associated to an apartment node;
- *Private Call Module* can be associated only to an apartment node;
- the *IPerCom-2Voice Gateway* and the *Lift Interface* can only be added to a stair node.

The apartment stations are not subject to any rules and therefore can be associated with any topological node, therefore also with nodes such as site, block, stair, or floor. This is useful if you want to provide a "*calling station*" in a "*Swimming pool*" room associated (for example) with a stair node: by positioning a video door phone on this node it is possible to call the *Switchboard* or be reached by calls from the *Switchboard* or from the apartments.

The "*IPerCom Clock Module*", where applicable, must be added in the configuration as every other device and can be positioned in any topological node of the system.

The device can be configured in 3 ways, as briefly described below.

The first method should be followed if you are not yet connected to the system, the others if you are connected to the system. In all cases, go to the "*Topology*" tab and then to the "*Devices*" tab.

**ADDING DEVICES TO THE CONFIGURATION THROUGH THE "ADD NEW DEVICE" BUTTON. NO CONNECTION TO THE SYSTEM.**

The "Topology" tab and the relative "Devices" tab appear as shown below:

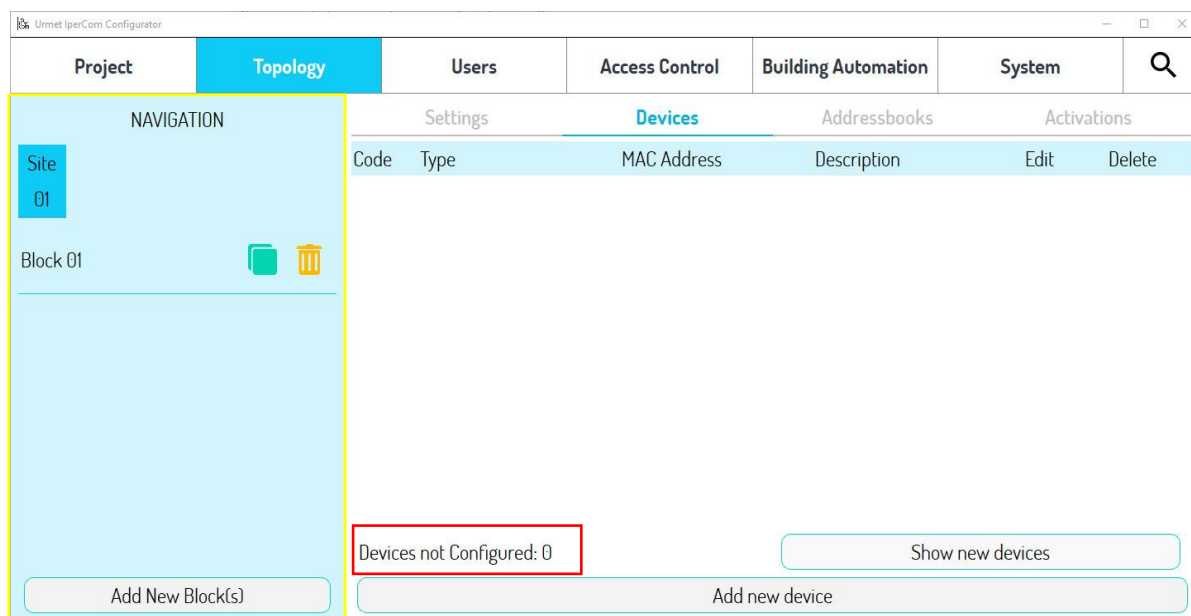


Figure 222: screen page through which to add devices without being connected to the system

Non-configured devices cannot be considered (red box) because you are not yet connected to the system and consequently the "Show new devices" button will display an empty list.

The configuration of the devices is always done by positioning on the node where they must be added through the navigation module (yellow box).

To add a new MAX video door phone to an apartment, the situation is shown below:

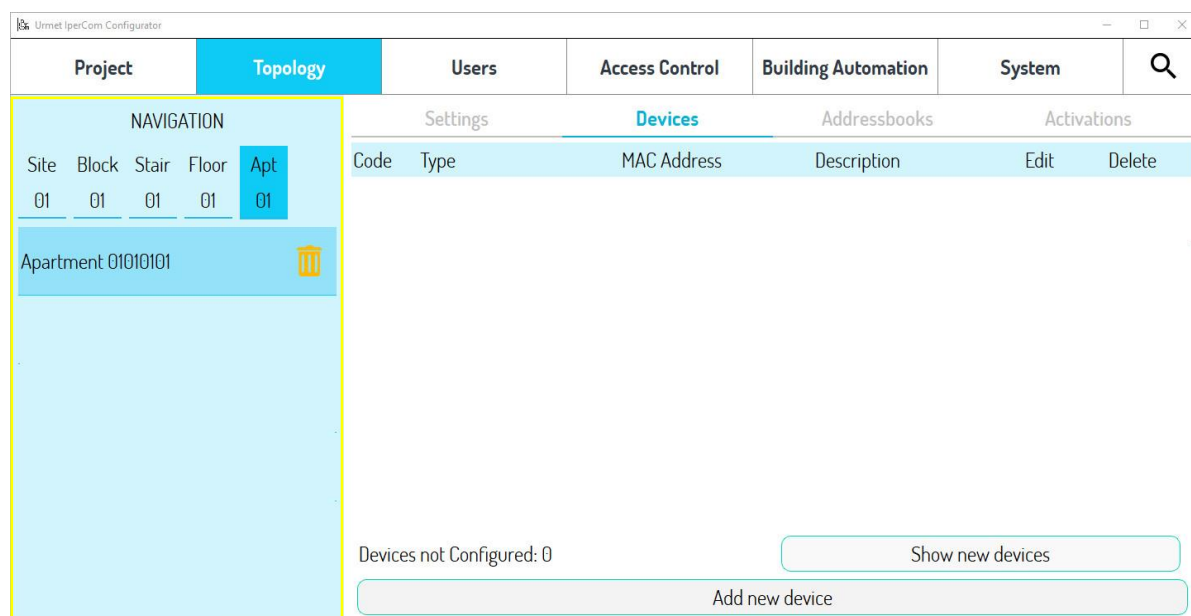


Figure 223: how to add a new device

Now simply press the "Add new device" button. A list of all devices that can be added to the apartment node is displayed:

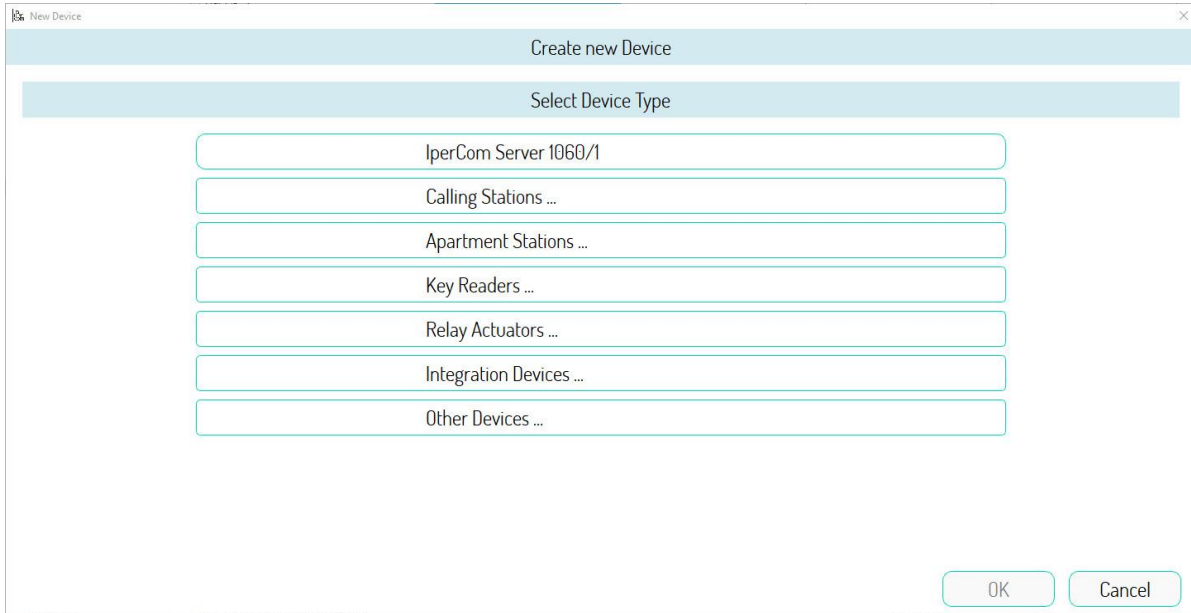


Figure 224: list of device categories that can be added on the apartment node

To add a MAX video door phone, simply press on "Apartment stations" item. The following screen opens:

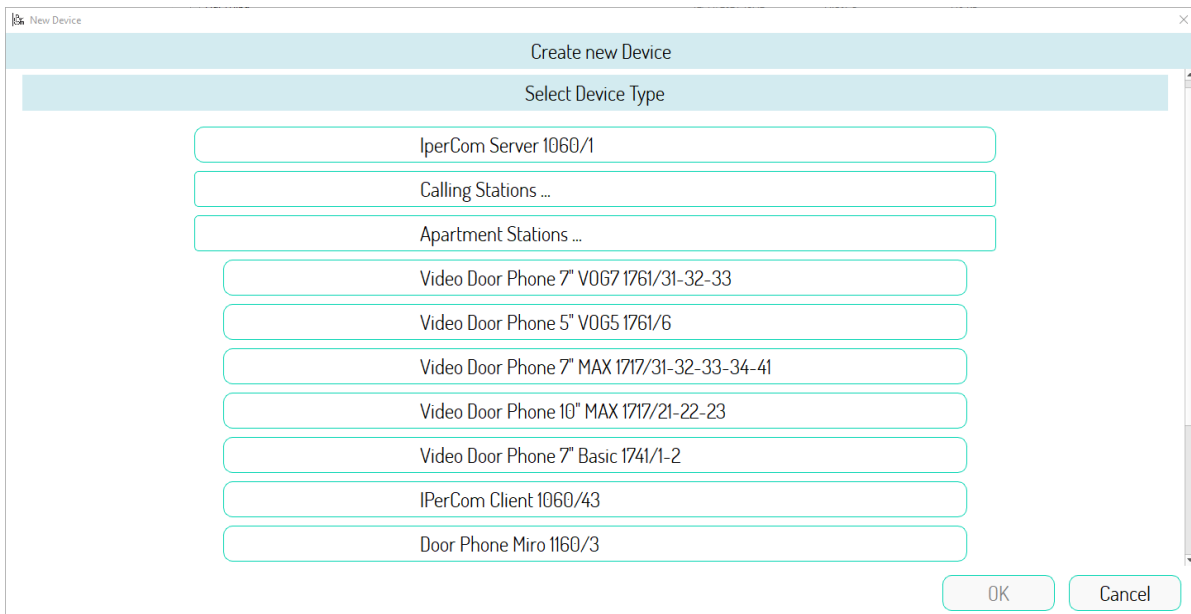


Figure 225: list of apartment stations



To add a MAX video door phone, simply press on “Video door phone 7” MAX 1717/31-32-33-34-41”. The following screen opens:

Figure 226: MAX video door phone configuration


Fill in the fields in the red box to configure-the device in question (in this case the MAC address and a name to associate with the video door phone). After this operation, press the “OK” button: the MAX video door phone is displayed on the topological node previously chosen:


Code	Type	MAC Address	Description	Edit	Delete
00	Video Door Phone 7" MAX 1717/31-32-33-34...	00:1E:E0:01:3F:45	Video Door Phone MAX - Apt 1		

Figure 227: Adding a MAX video door phone to an apartment

For the configuration of the other devices, it is therefore necessary to:

- position on the node where you want to add the device (through the navigation module);
- press the "Add Devices" button;
- choose the device to be added from the list of categories;
- configure the device;
- press the OK button in the relevant configuration screen.

 In "[APPENDIX A: Configuration parameters of IPerCom devices](#)" the configuration parameters of all the IperCom devices are shown and explained in detail.

 For each node selected in the "Settings" tab it is possible to customise the name of the node in question through the "Name" field.

#### ADDING DEVICES TO THE CONFIGURATION USING THE "SHOW NEW DEVICES" BUTTON WITH CONNECTION TO THE SYSTEM.

The "Topology" tab and the relative "Devices" tab appear as shown below:

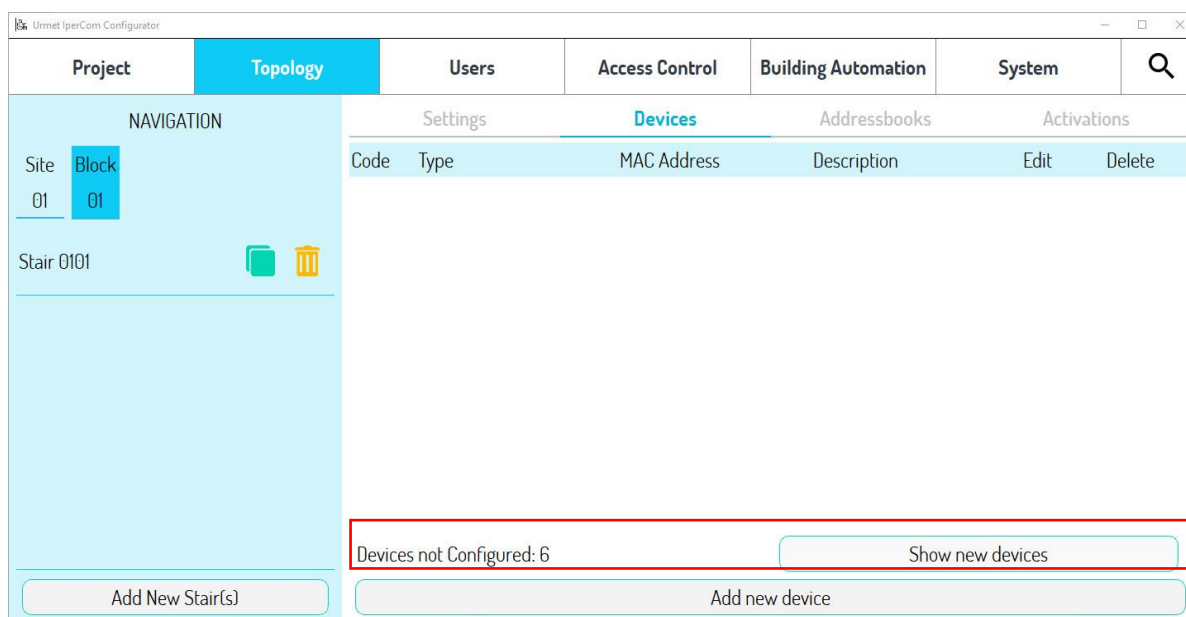


Figure 228: screen page through which to add the devices with connection to the system

Non-configured devices can be considered as you are connected to the system and consequently these will be displayed when pressing the "Show new devices" button (red box):

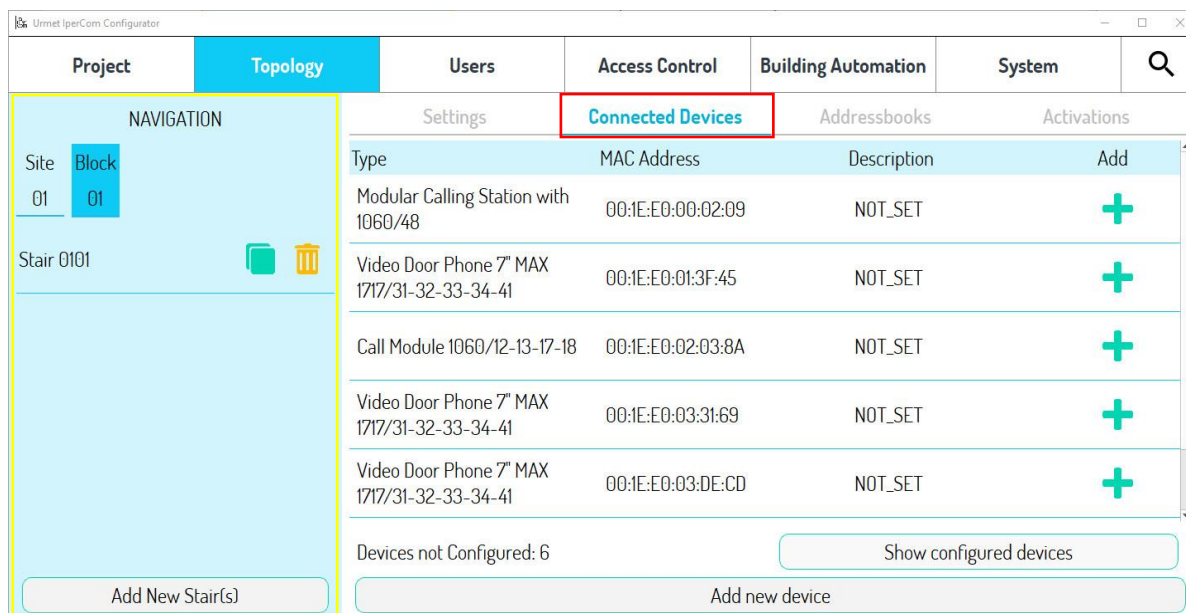


Figure 229: list of devices connected to the system and not yet configured

When displaying the list of devices to be configured, the "Devices" tab is renamed to "Connected Devices".

The advantage of this second way of proceeding is that all the devices to be configured are listed in a single screen page.

Configuration is done following the two steps below (like the first mode):

- select the node where to add the device through the navigation module (yellow box);
- press the button for the device you are adding.

For example, if you want to add a MAX video door phone in an apartment, after positioning on the topological node in question, simply press the button on the relevant video door phone.

The same configuration page appears as in the first mode, with the only difference that the MAC address field is already filled in:

Figure 230: MAX video door phone configuration with MAC address already filled in

Once the MAX video door phone has been configured, press the "OK" button to return to the list of devices to be configured:

Project					Topology	Users	Access Control	Building Automation	System	Q
NAVIGATION					Settings	Connected Devices	Addressbooks	Activations		
Site	Block	Stair	Floor	Apt	Type	MAC Address	Description	Add		
01	01	01	01	01	Modular Calling Station with 1060/48	00:1E:E0:00:02:09	NOT_SET	+		
Apartment 01010101					Call Module 1060/12-13-17-18	00:1E:E0:02:03:8A	NOT_SET	+		
Apartment 01010102					Video Door Phone 7" MAX 1717/31-32-33-34-41	00:1E:E0:03:31:69	NOT_SET	+		
Apartment 01010103					Video Door Phone 7" MAX 1717/31-32-33-34-41	00:1E:E0:03:DE:CD	NOT_SET	+		
Apartment 01010104					IperCom Server 1060/1	C4:00:AD:3F:72:83	NOT_SET	+		
Apartment 01010105					Devices not Configured: 5			Show configured devices		
Apartment 01010106					Add new device					

Figure 231: devices still to be configured

As you can see, the "Non-configured Devices" field shows 4 (compared to the initial 5 non-configured devices).

The "Show configured devices" button instead shows the devices configured on the topological node in question:

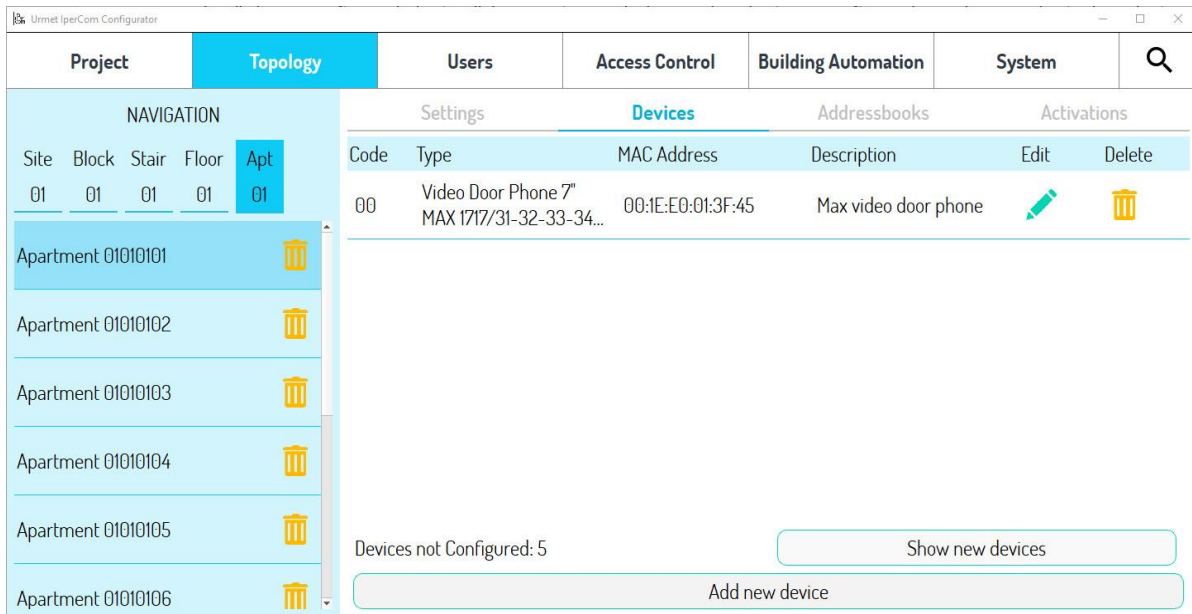


Figure 232: Adding a MAX video door phone to an apartment



If there are devices that cannot be configured on the topological node where you have positioned, they appear in light grey and the relevant button is disabled.

Once the configuration of all the devices has been completed, the "Non-configured Devices" field will show the value 0 and the relevant list accessible through the "Show new devices" button will be empty.

To view the devices configured on each topological node through the navigation module, select a topological node, then use the "Devices" tab to display a list of the devices configured in the topological node chosen.

**ADDING DEVICES TO THE CONFIGURATION USING THE "ADD NEW DEVICE" BUTTON WITH CONNECTION TO THE SYSTEM.**

This procedure is like the first one with the only difference that in the device configuration phase for entering the MAC address, it is useful to use the "... " button, as shown in the figure in the case of a MAXvideo door phone:


Figure 233: MAC address entry when connected to the system

By pressing the "... " button and then the "Scan" button, a list of all the MAX video door phones installed in the system with their MAC address but not yet added to the configuration is displayed:

Type	Model	MAC
Video Door Phone 7" MAX 1717/31-32-33-34-41	171731A64	00:1E:E0:01:3F:45
Video Door Phone 7" MAX 1717/31-32-33-34-41	171731A64	00:1E:E0:03:31:69

Figure 234: list of devices installed but not configured

Simply select the device to add, identifying it through its MAC address, and it is filled in automatically.

 *If you are connected to a system with one or more Servers 1060/1, they must be configured if you want to save the system configuration. Otherwise, it is impossible to save the configuration and the configurator shows the message below:*

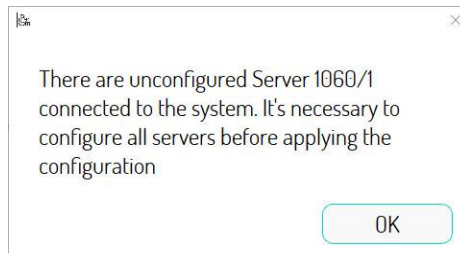


Figure 235: message when Servers 1060/1 are not configured

*This is to avoid starting a system with Servers 1060/1 connected but not configured: the concerned system will not operate properly.*

### 7.1.2.1 Adding a Gateway IPerCom-2Voice on a stair node

If a Gateway IPerCom-2Voice 1083/59 has been added on a stair node with one of the methods described above, the configurator has some differences compared to the addition of other devices. The addition of a Gateway IPerCom-2Voice 1083/59 on a stair node highlights the fact that on that stair node you want to install a riser column of 2Voice audio / video apartment stations. To distinguish the stairs with IPerCom audio / video apartment stations from the 2Voice stairs, these ones and all their underlying nodes are highlighted in yellow in the configurator's navigation module:

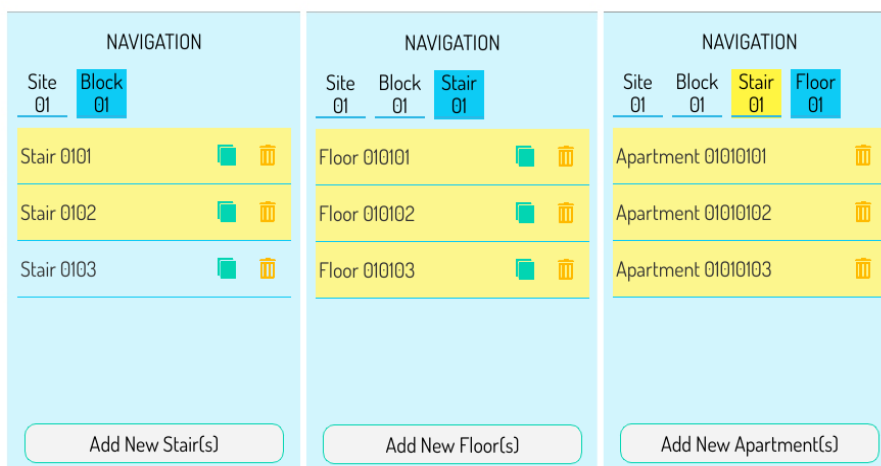


Figure 236: Stairs where a Gateway IPerCom-2Voice is placed with underlying floors and apartments

On the nodes below the stair node (floors and apartments), where a *Gateway IPerCom-2Voice 1083/59* has been placed, it is not possible to add any device; the "Add new device" button on these nodes shows the following screen:

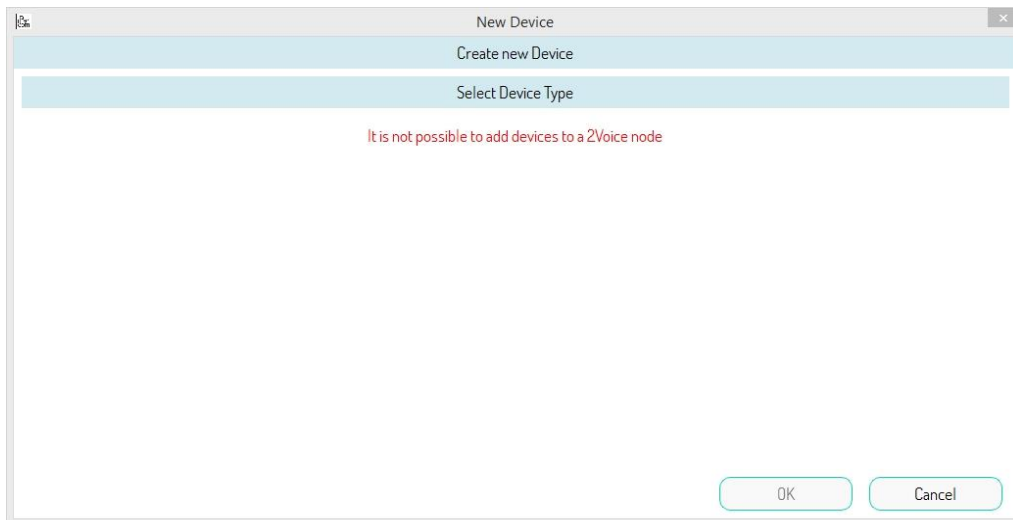


Figure 237: Adding devices on nodes below a stair with Gateway IPerCom-2Voice

On the stair node where the *Gateway IPerCom-2Voice* was added, it is possible to add new devices.

On the contrary, if a gateway is added on a stair node under which several IPerCom devices are placed, these will be deleted (excluding those placed on the stair node itself):

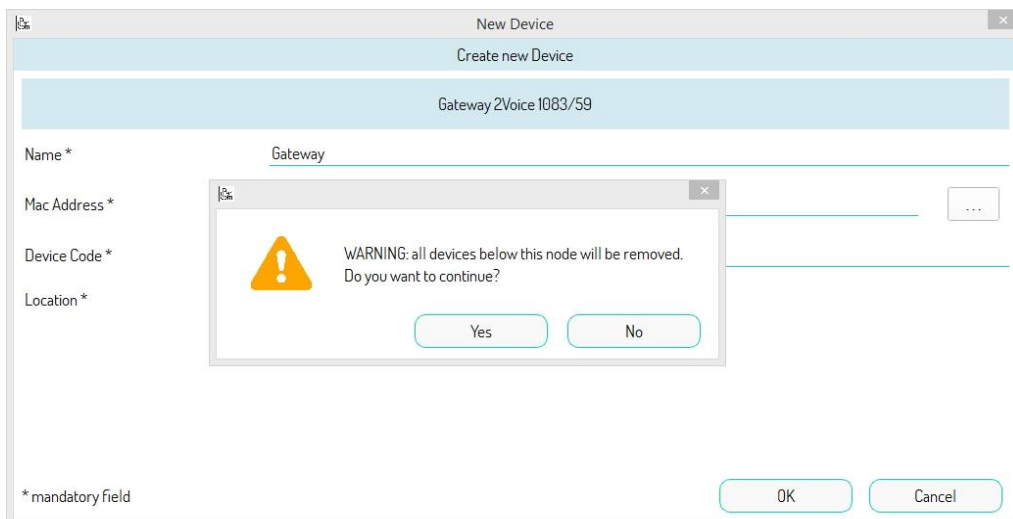


Figure 238: Remove devices if a gateway is added in stair



The 2Voice apartments that are thus created under the stair, where the gateway is located, have a different setting page than the IPerCom apartments: in addition to the “Name”, “Topological Code”, “Numerical Code” or “Logical Code” fields (if the system is set in numerical or logical mode), the “2Voice Code” field also appears:

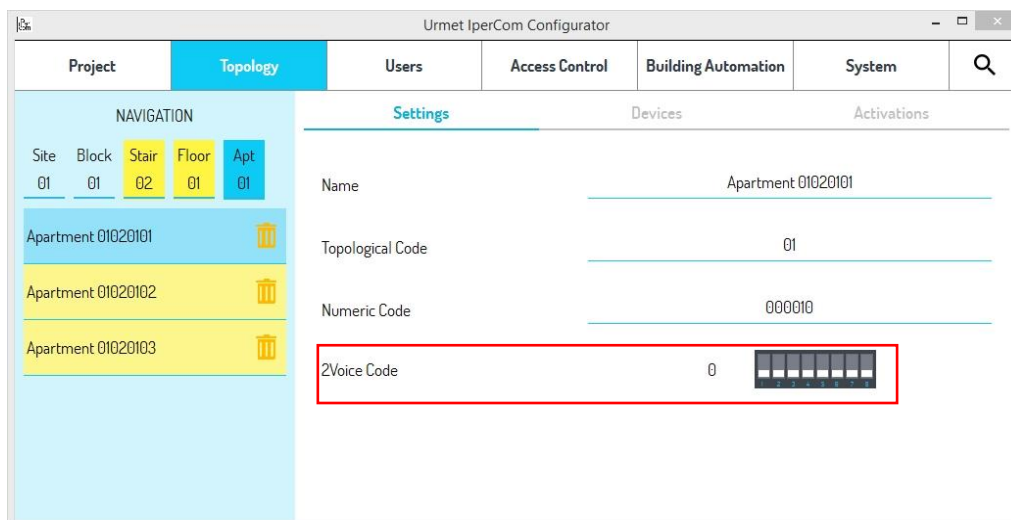


Figure 239: apartment 2Voice code setting

This field is used to set the physical code of the 2Voice user: the allowed values range from 0 to 126.

Pressing on the numerical value "0" opens the following window:

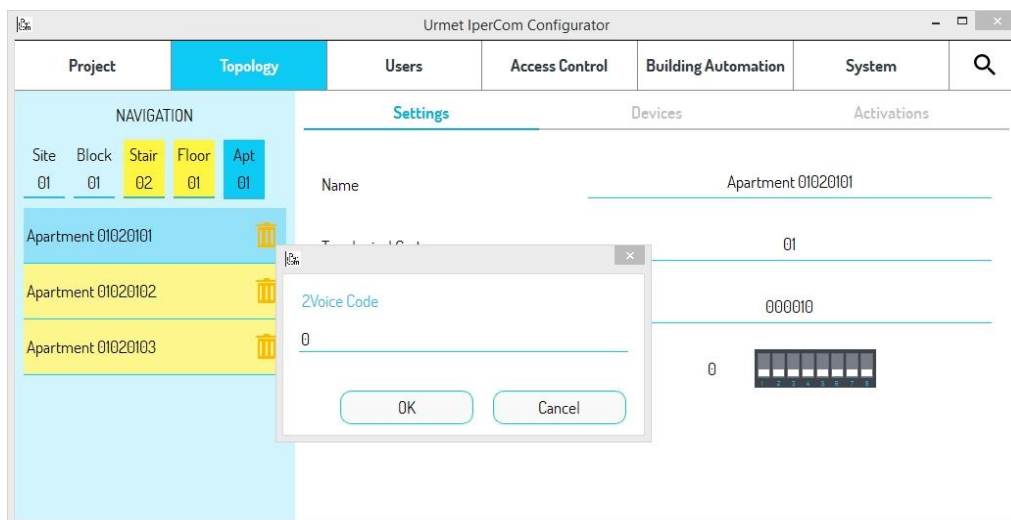


Figure 240: Window where enter apartment code

By entering an allowed value and pressing “OK”, the last 7 dip-switches in the image below are automatically positioned on the right position, to represent the previously entered number in binary format. Having entered 100, the figure shown below appears:

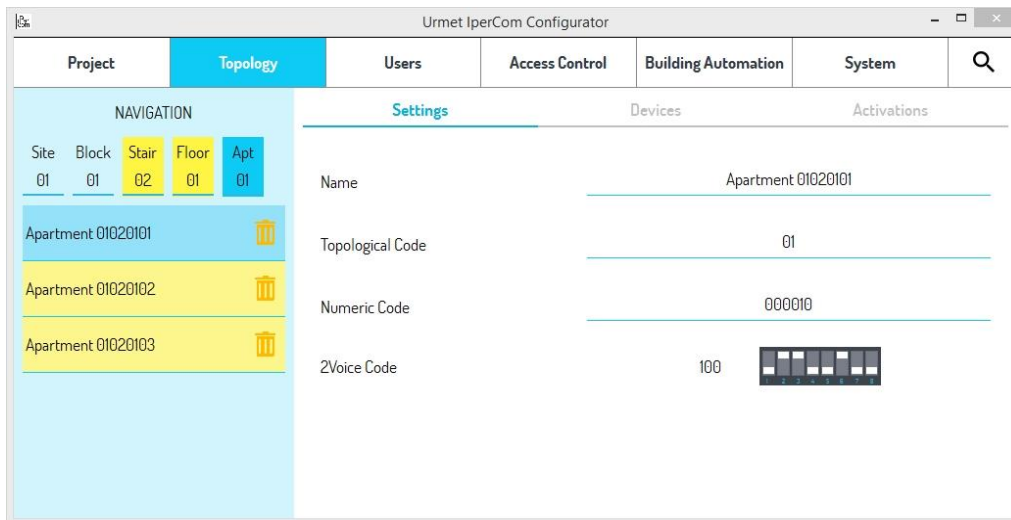



Figure 241: Binary code of the entered code

It is also possible to act directly on the dip-switches (pressing on the related image) to set the desired 2Voice code.

The setting of the dip-switches must be reported on apartment stations of the 2Voice riser column.

The first dip-switch (starting from the left) must not be modified as regards the setting of the physical code of the 2Voice users.

For details, follow the instructions in the 2Voice technical manual (available from the website [www.urmet.com](http://www.urmet.com)).

 *2Voice apartments cannot be set in IPerCloud mode.*

### 7.1.2.2 Adding a Lift Interface 1060/37 on a stair node

Add a *Lift Interface* 1060/37 to control the lift control panels to enable the ascent only to the defined floors according to the apartment called. The interfacing to the lift control units is typically made by changing the status of one or more inputs of these control panels through control relays.

The IPerCom system allows you to choose (via the "Mode" drop-down menu) among 3 modes of use for the lift interface:

- "Lift interface",
- "Lift interface-RS485",
- "Relay Actuator Mode".

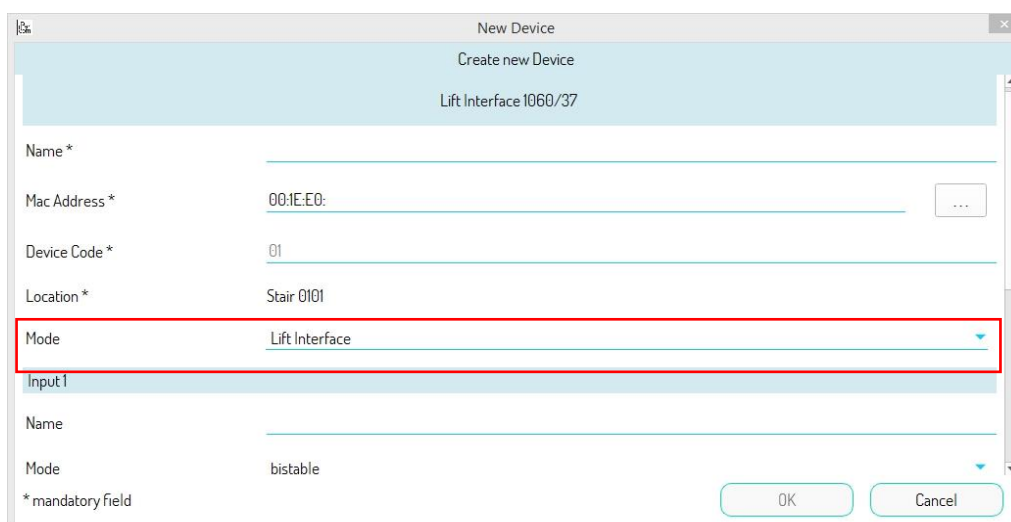


Figure 242: Lift Interface configuration - Selection of use mode

#### 7.1.2.2.1 Lift interface mode

The *Lift Interface* type allows you to associate relays to floors or apartments in the unit, it is possible to associate a relay to each floor (for example it is possible to associate a relay to each floor).

It is necessary to define the operating mode of the *Lift Interface*:

- "Floor",
- "Apartment".

The setting is made for each individual stair, as shown in the following figure. The first mode allows you to associate the interface commands according to the floor of the apartment: in this case several apartments on the same floor will share the same relay activation layout. The second mode allows you to associate a different configuration of commands for every single apartment in the unit: it is useful if there are several apartments on the same floor, each with its own dedicated lift.

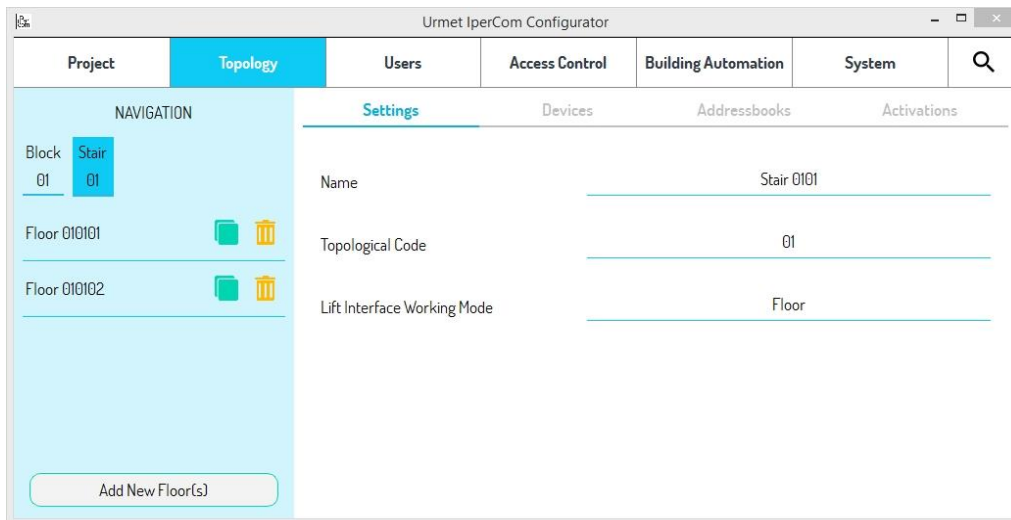


Figure 243: Lift Interface setting - Mode selection

#### 7.1.2.2.1.1 Creating the path

The lift interface is equipped with 24 relays that can be configured through the *IperCom Installer Tools configurator*, so that they close in response to an event occurring in the system. A typical case is to enable the visitor who accesses the residential complex to use a lift to access only the floor, or the apartment according to the operating mode, where the person with the selected name lives. For this to be possible, it is necessary to create a "path", i.e. an association between the access that allows accessing the structure (for example a main or secondary call station or a proximity reader module) and the destination to which the visitor will move, i.e. the floor/apartment.

To access the path configuration, it is necessary to enter the configuration page of the device, at the lift interface you want to configure. In the "paths" section the list of all paths already configured is shown. It is possible to edit or delete an existing path by pressing the "Edit" and "Delete" icons. It is possible to create a new path by pressing the "Add Path" button.

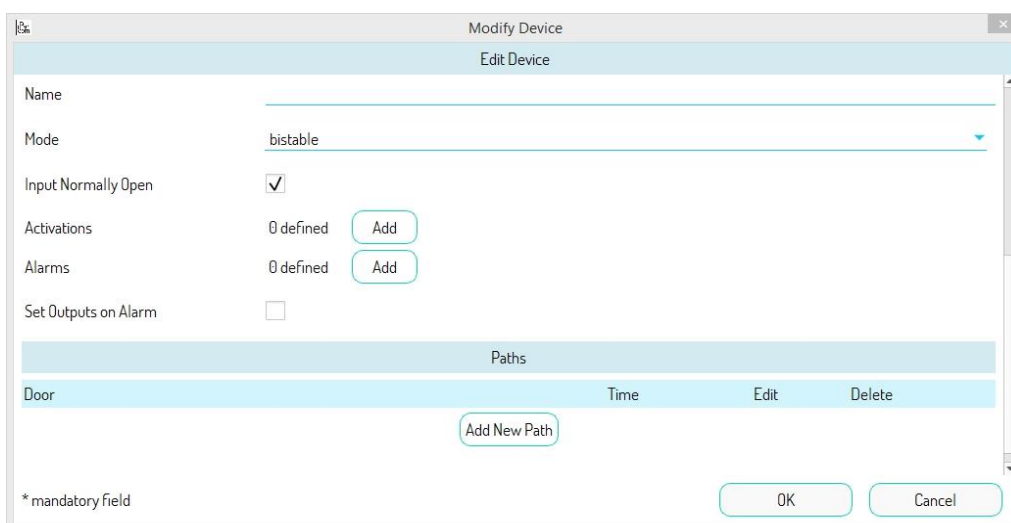


Figure 244: Lift interface configuration - Creating the access path

To create a path, it is necessary to select an access available in the system from the list. The types of devices that can be selected are:

- *Call Module 1060/12-13-17-18-23,*
- *Modular Calling Station with 1060/48,*
- *Entry panels 1060/21-33-34-71-74-75,*
- *Key readers 1060/45,*
- *Key readers 1060/86,*
- *Switchboard 1060/41.*


Then it is necessary to set the activation time of the relays associated with the path. The following options are possible:

- *"15 seconds",*
- *"5 minutes",*
- *"Unlimited",*
- *"Customized".*

In the last case it is necessary to specify the duration in seconds for which you want the relays to remain energised.

#### 7.1.2.2.1.2 Control Relay Assignment

The configuration of a lift interface is completed by assigning the control relays to the floors/apartments concerned. The way to make the assignment is the same whether it is used in "Floor" or "Apartment" mode, what changes is the section where the configuration is made: in the first case within the floor, in the second case within the apartment. Basically, it is necessary to match each floor/apartment you want to enable with the switching of one or more relays necessary to allow the lift to rise.

 *The possibility to activate even more than one relay for each floor/apartment is present to make complex selections, if required by the lift control panel (e.g. enabling via a multi-digit binary code).*

### 7.1.2.2.1.3 Assignment in *Floor* mode

Since the assignment operation is carried out through the settings of each *Floor* concerned, it is necessary to first select the desired floor, choose the lift interface to configure and finally enable the relays to be activated.

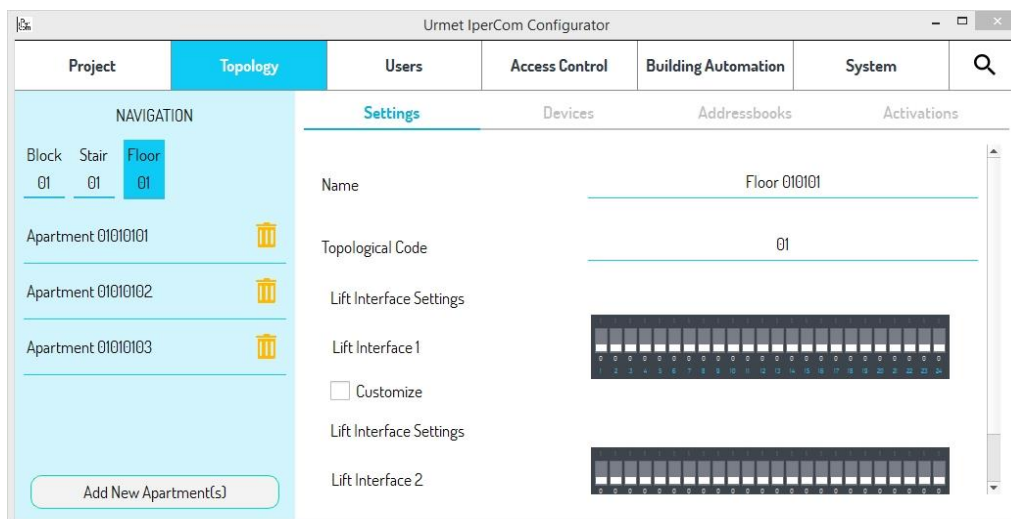


Figure 245: Lift Interface association - Floor selection

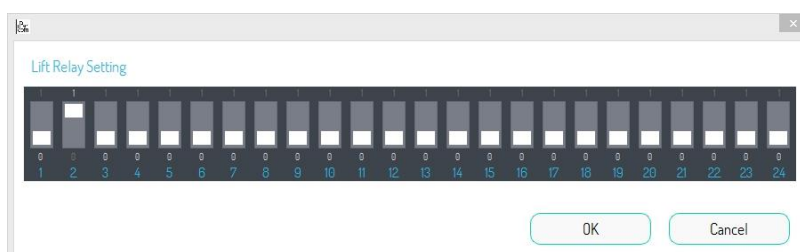



Figure 246: Lift Interface association - Enable control relay in floor mode

This operation must be repeated for each floor. The figures above show for example the activation of relay **1** in case you want to enable the lift on **Floor 01**.

 Each lift interface acts exclusively within the block/unit to which it is associated, so the floors to be selected will only be those relevant to its block and unit.

In a very active system, where several paths have been configured, each with its own activation time, the relay opening times may overlap, for example:

- **Path 1**
  - From the main entry panel to the lift.
  - 1st floor
  - Activation time: 5 minutes.
- **Path 2**
  - From the secondary entry panel to the lift.
  - 2nd floor
  - Activation time: 7 minutes.
- **Path 3**
  - From the proximity reader to the elevator.
  - 5th floor
  - Activation time: 10 minutes.

A visitor makes a call from the main entry panel to an apartment on the 1st floor (**Path 1**). When the apartment station of the apartment opens the door, a command is sent to the lift interface that enables the relevant relay(s) for 5 minutes. If within 5 minutes a call is made from the secondary entry panel to an apartment on the 2nd floor (**Path 2**) and in the meantime a door is opened through the proximity reader, for example in the garage, by a 5th floor resident (**Path 3**), the lift interface will ensure the activation time of the first call (**Path 1**) and at the same time, from the moment the lift interface has received the relay(s) activation command, the activation time of the second and third call (**Path2** and **Path 3**).

If there is a *Switchboard 1060/41* connected to a PC using the *SwitchBoard* application, it is necessary to create a path between the two devices. In the path settings the *Switchboard* does not have the **Activation time** parameter to configure as, for example, the call modules, because it is the switchboard operator who decides the activation time when enabling the output manually. For more details, see the [Switchboard user manual](#).

### 7.1.2.2.1.4 Assignment in Apartment mode

In this case the assignment operation is carried out through the settings of each apartment, it is necessary to first select the desired floor, choose the lift interface to configure and finally enable the relays to be activated.

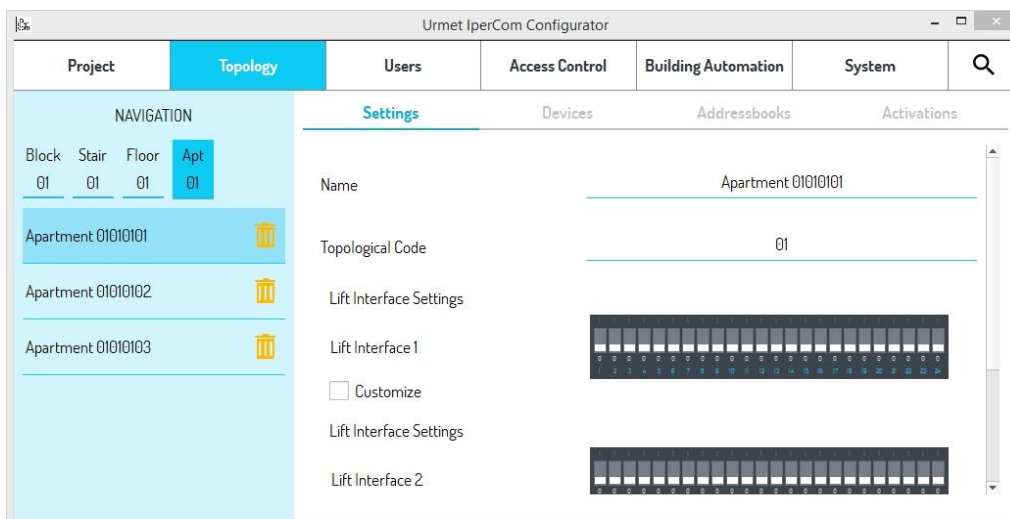


Figure 247: Lift Interface assignment - Apartment selection

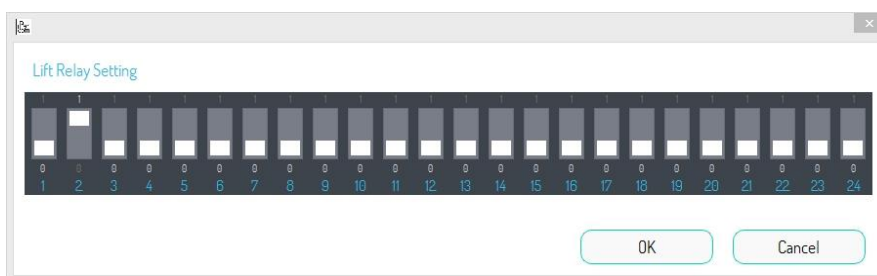


Figure 248: Lift Interface assignment - Enabling control relay in Apartment mode

As in the case described above, this operation must be repeated for each apartment. The figures above show for example the activation of relay **1** in case you want to enable the lift on **Apartment 1**.



*Each lift interface acts exclusively within the block/unit to which it is associated, so the apartments to be selected will only be those relevant to its block and unit.*



### 7.1.2.2.2 Access for non-residents

It is also possible to configure access paths for non-resident users. In the users section choose a "Not residents" user in case he/she is already present in the system, or press "Add" to create a new one (to add a *non-resident* user, see paragraph Not residents). After the selection, the following screen will open:

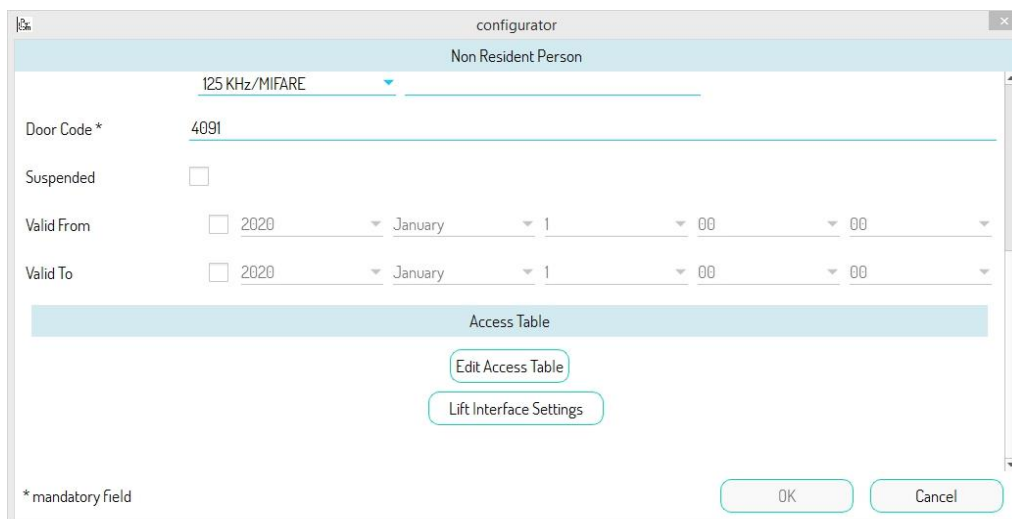


Figure 249: Lift Interface assignment - Setting of non-resident user paths

Press the "*Lift Interface Settings*" button to configure relay enabling.

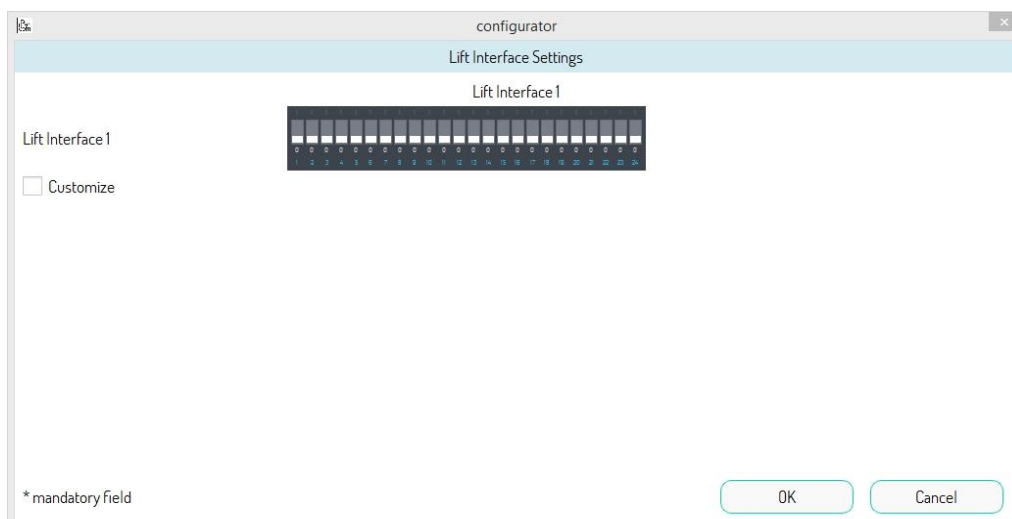


Figure 250: Lift Interface assignment - Enabling non-resident user relays (part 1)

In this screen it is possible to enable the relays that will be activated according to a certain event (e.g. by entering the door opener code) on all the paths created between the lift interface and the various devices.

Tick the "Customise" box to enable the relays to every single path created between the lift interface and the various devices.

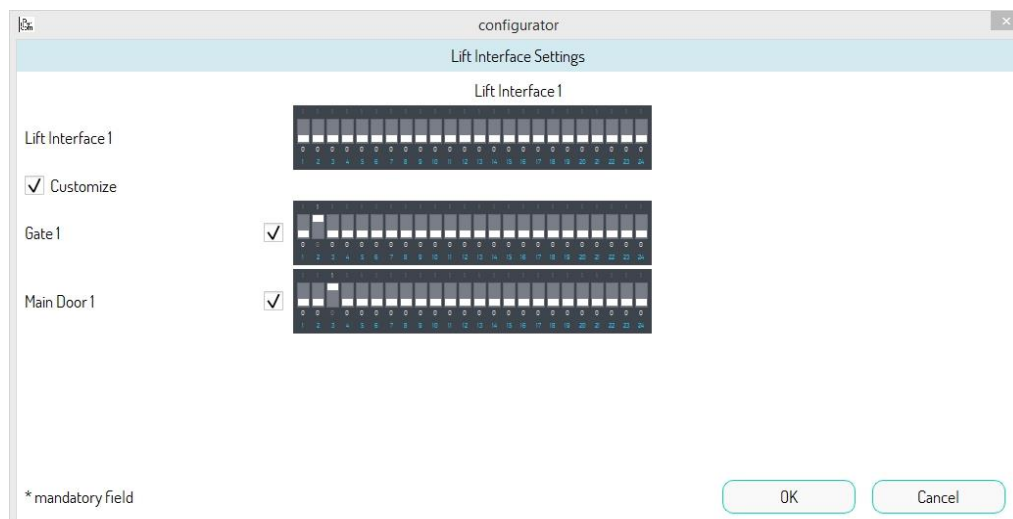


Figure 251: Lift Interface assignment - Enabling non-resident user relays (part 2)

#### 7.1.2.2.3 Lift interface-RS485 mode

The **Lift Interface-RS485** type allows interfacing the device with a possible third-party controller. In this case the lift interface will only communicate the event occurred in the system to the third-party controller that will perform the actions programmed according to the above event.

#### 7.1.2.2.4 Relay Actuator Mode

The "Relay Actuator Mode" type allows the lift interface to be used exactly like a *Relay Actuator 1060/84* but with 24 outputs. For relay operation and configuration, see paragraph "[APPENDIX A: Configuration parameters of IPerCom devices](#)".

### 7.1.3 System IPerCom in IPerCloud mode

The creation of the configuration of IPerCom systems in IPerCloud mode must be done exclusively starting from *IPerCom Installer Tools* (with authentication on Urmet Cloud and CallMe Manager support enabled) and not from the video door phones that integrate the *configurator* (*VOG<sup>7</sup>*, *MAX* or *Basic*).

Any changes must also always be made by *IPerCom Installer Tools* starting from the relevant project. This is necessary to always have the installer site aligned with the building manager site transferred via *IPerCom Installer Tools in CallMe*.

Given the above, to configure an IPerCom system in IPerCloud mode it is necessary:

- evaluate whether it is necessary to add a 1060/1 *Server* to the configuration;
- configure the relevant apartments in IPerCloud mode.

These aspects are explained in detail in the following paragraphs.

#### 7.1.3.1 Addition in configuration of a Server 1060/1 on an IPerCom system in IPerCloud mode

In IPerCom systems in IPerCloud mode the choice of the calling station model and the number of IPerCloud apartments may require the presence of a *Server 1060/1* for the system to function correctly.

Depending on the two variables reported above, the *Server 1060/1* is not required in the following 3 types of system configurations:

#### CONFIGURATION 1:

- calling stations of type *Modular Calling Station with 1060/48*;
- a maximum of 200 IPerCloud apartments.

To this system configuration it is possible to add one or more calling stations of the type *Entry Panel 1060/33-34* and/or *Entry Panel 1060/21*.

#### CONFIGURATION 2:

- calling stations of type *Entry Panel 1060/33-34*;
- a maximum of 32 IPerCloud apartments.

To this system configuration it is possible to add one or more calling stations of the type *Entry Panel 1060/21*.

**CONFIGURATION 3:**

- calling stations of type *Entry Panel 1060/21*;
- a maximum of 20 IPerCloud apartments.

If in the IPerCom system in IPerCloud mode it is instead required to have:

- at least one calling station other than *Modular Calling Station with 1060/48* or *Entry Panel 1060/33-34* or *Entry Panel 1060/21*,

or

- several IPerCloud apartments greater than 200,

or

- only *Entry Panels 1060/33-34* with several IPerCloud apartments greater than 32,

or

- only *Entry Panels 1060/21* with several IPerCloud apartments greater than 20,

then it is necessary to have at least one *1060/1 Server* in the system.



*In a system with IPerCloud apartments without any calling station and with at least one Switchboard 1060/41, it is necessary to have at least a Server 1060/1.*



*The request for a 1060/1 Server may still be mandatory if the number of apartments or devices or users (residents and not-residents) is greater than 1000.*

In relation to the case of IPerCom systems in IPerCloud mode, if the presence of a *1060/1 Server* is requested, the *configurator* signals any lack of it in the configuration via a message when saving the configuration itself (see paragraph [How to save the configuration](#)):

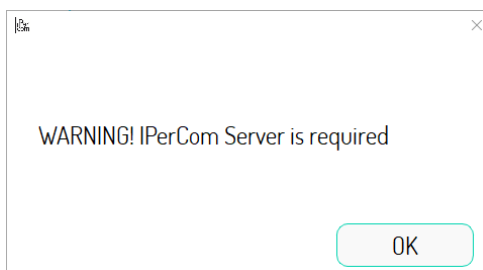


Figure 252: message on configurator in the absence of Server 1060/1

If the 1060/1 *Server* is added to the configuration but is not physically installed on the system, during the saving phase the *configurator* allows you to save the configuration but when you try to apply it via *IPerCom Installer Tools* the following message is shown (within 5 minutes):

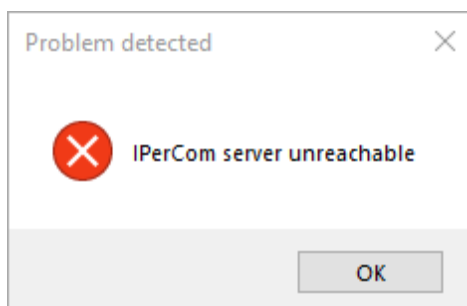


Figure 253: message on *IPerCom Installer Tools* in the presence of *Server 1060/1* added on the configurator but not present on the system

In addition, the *VOG<sup>7</sup>*, *VOG<sup>5+</sup>*, *VOG<sup>5</sup>*, *MAX* video door phones, *Switchboard* and *IPerCom Client* applications show a screen like the one below:

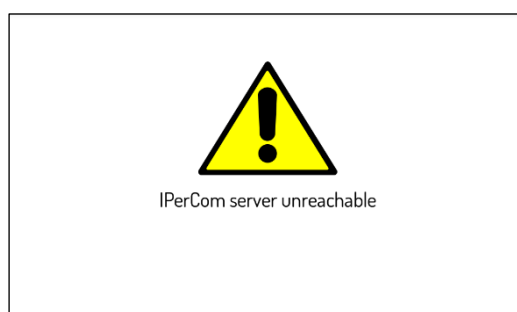


Figure 254: message on *MAX*, *VOG<sup>7</sup>*, *VOG<sup>5+</sup>*, *VOG<sup>5</sup>*, *Switchboard* and *IPerCom Client* in the presence of *Server 1060/1* added on the configurator but not present on the system

Calling stations equipped with displays show a screen indicating that the device is not configured.

It is therefore necessary to connect physically at least one 1060/1 *Server* to the system and add it as a device to the system configuration. If one or more *Server 1060/1* are connected to the plant but not configured, the following message is shown (with or without *IPerCloud* apartments):

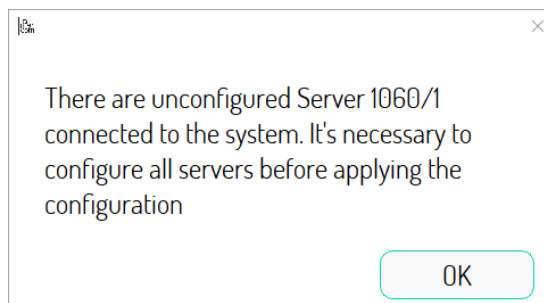


Figure 255: message in case of *Server* connected to the system but not configured

### 7.1.3.2 How to set up an apartment in IPerCloud mode

To set up an apartment in IPerCloud mode it is necessary to select the relevant node and the "Settings" tab, as shown below:

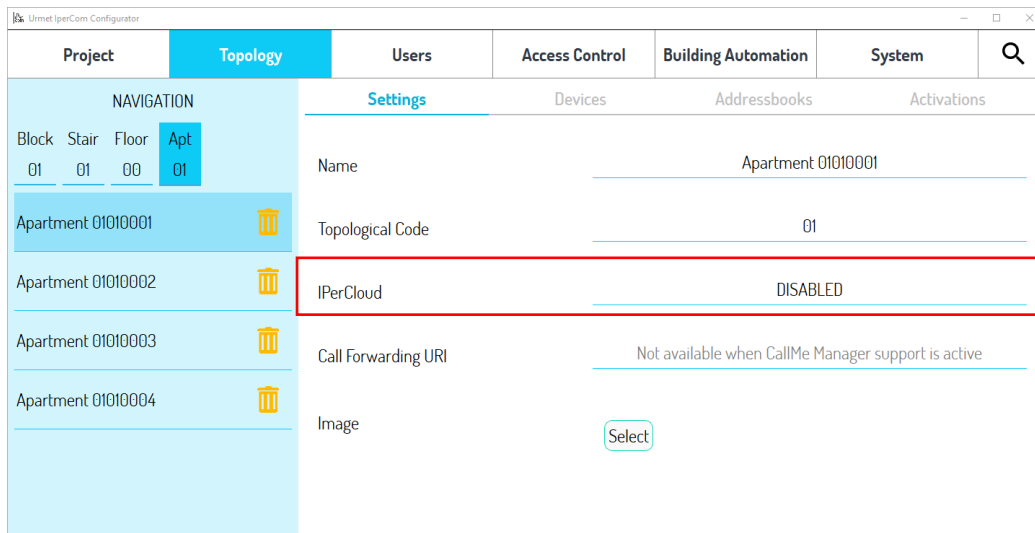


Figure 256: apartment in IPerCom mode

The section in red shows that the IPerCloud mode is disabled for the selected apartment. To enable it (and therefore create an IPerCloud apartment) simply press on the "DISABLED" item. A window opens through which you can enable IPerCloud mode:

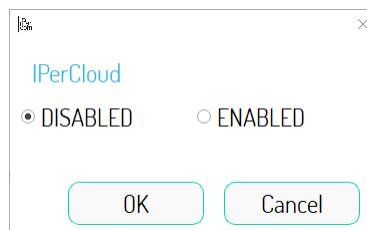


Figure 257: setting up an apartment in IPerCom or IPerCloud mode

By choosing the "ENABLED" item, the selected apartment becomes an IPerCloud apartment. This is highlighted by the relevant icon in the left navigation module (red arrow):

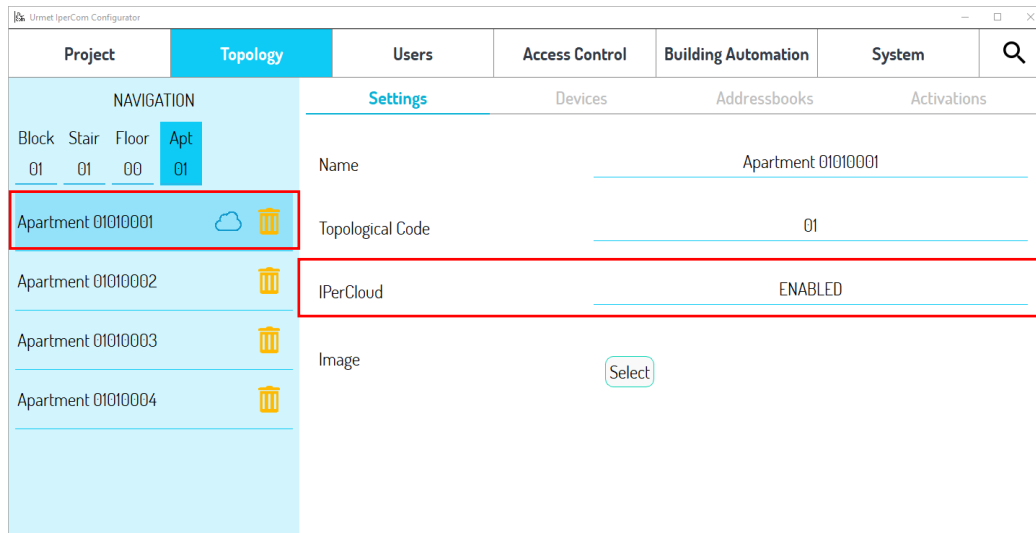


Figure 258: apartment in IPerCloud mode



The "Call forwarding URI" item is no longer visible as the use of the CallMe Manager application is required to configure the IPerCloud apartment and the parameter in question can only be set if this application does not It's requested.



In the presence of at least one IPerCloud apartment on the configurator, the CallMe Manager Support item is automatically enabled, if it was previously disabled.

Enabling the IPerCloud mode can be set not only by the apartment nodes, but also by the higher nodes (site, block, stair, floor) with the advantage that all the apartments of the relevant topological group acquire this mode. For example, to set the IPerCloud mode from a "block" node, simply press the relevant "Set" button, as shown in the figure:

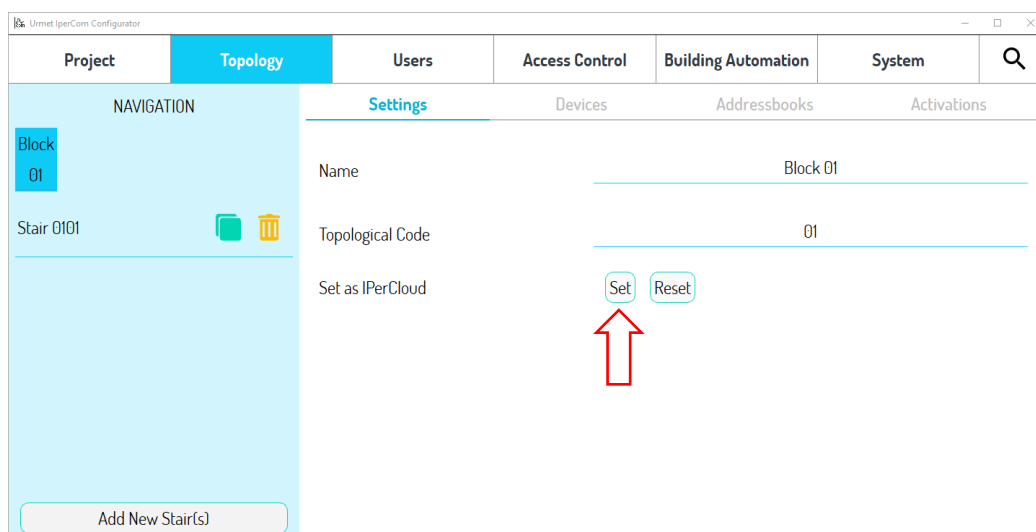


Figure 259: setting up an IPerCloud node

By pressing the "Yes" button in the next dialog box, the apartments present in the topological group of the "Block 01" node are automatically set as IPerCloud apartments, as shown below:

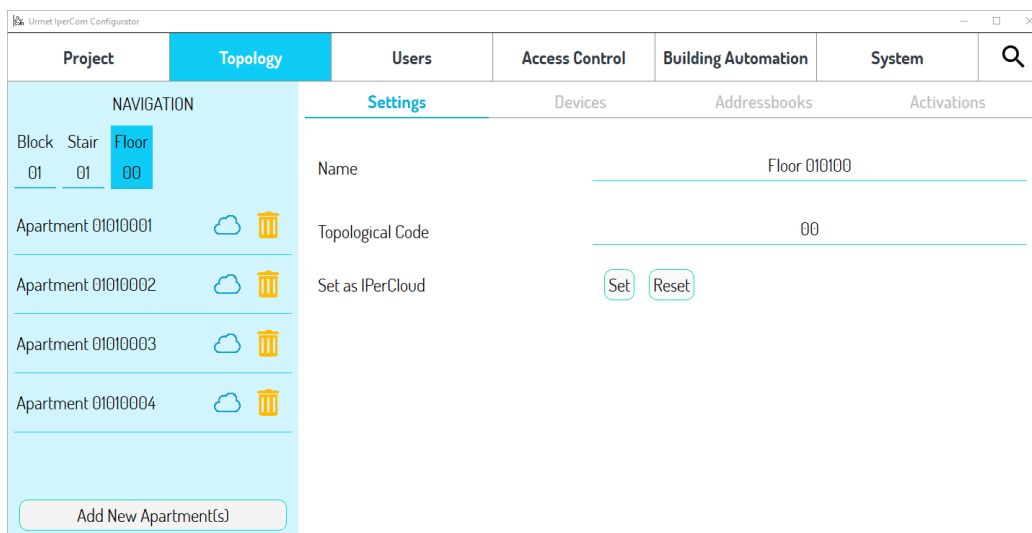


Figure 260: automatic acquisition of IPerCloud mode

By pressing the "Reset" button and then "Yes" in the subsequent dialog box, the IPerCloud apartments present in the topological group of the "Block 01" node become IPerCom.



*The 2Voice apartments under the stair node where the 2Voice Gateway has been positioned cannot be set in IPerCloud mode.*



*For the correct configuration of an IPerCom system in IPerCloud mode it is necessary to be authenticated on Urmet Cloud. Otherwise, it will not be possible to apply the configuration to the system.*

#### 7.1.3.2.1 Hybrid apartments

A hybrid apartment is an apartment in IPerCloud mode with one or more apartment stations. The hybrid apartment can be created starting from an IPerCloud apartment to which one or more apartment stations are added or starting from an apartment with one or more apartment stations to which the IPerCloud mode is then set.

With hybrid apartments, the call to a smartphone/tablet with the *CallMe* app comes by setting the apartment's video door phone to *Remote* mode (for further details see the video intercom user manual available on the website [www.urmet.com](http://www.urmet.com)). If the apartment video door phone no longer works, the call to the smartphone/tablet with the *CallMe* app continues to arrive via license or via call on the GSM or landline telephone network in the absence of Internet coverage.



#### 7.1.4 Contacts

In the "Topology" tab, through the "Address Books" item, it is very easy to create:

- **the contact list** for video door phones with address book (most common use),
- **the contact list** for IPerTalk extensions;
- **the contacts** associated with T1 and T2 buttons of the *Miro* door phone 1160/3 and T1, T2 and T3 buttons of the video door phone 1761/6 (most common use);
- **the list of additional cameras** on which auto-on can be enabled from the video door phones (special cases);
- **the contact list** in the address book of all types of call modules (*Call Module* 1060/12-13-17-18-23 or *Alpha Call Module*), i.e. contacts outside their visible residents (special cases).



*Video door phones with directory are MAX, VOG<sup>7</sup>, VOG<sup>5+</sup>, Basic video door phones as well as IPerCom Client 1060/43 video door phones.*



*By contact we mean not only an internal unit to be called but also a generic call station on which it is possible to self-activate from a video door entry unit, as explained below.*

Contacts are created in the address book according to the following requirements:

- to call apartment station from other apartment station (for example, if there is a dental practice or a swimming pool in the system, it will be possible to add the contact to the address book of all *video door phone* in the system);
- call *apartment station* from calling station;
- call *Switchboards* from video door phone and/or call modules, if the *Switchboards* are outside the topological path of the nodes where the video door phone and/or call modules are located;
- to call *Switchboards* from *Miro Door Phones 1160/3*;
- to implement the auto-on function on calling station, *RTSP cameras* that are outside the topological path of the node where a *MAX video door phone* is located.

The addition of contacts in the address book is linked to the concept of the node and its topological group.

If a contact is created on a topological node, it can be made available to:

- all the *apartment station* and/or calling station present on that node (creation of contact with **private** nature);
- all the apartment station and/or calling station present on the topological group of that node (with **public** nature).

Each contact created in address book will automatically be added also to the address book of the *switchboards*.

The following paragraphs will describe how to create contacts based on the above requirements. Reference will be made to the video door phone 1717/3x-4x (*MAX*) and the *Miro* door phone 1160/3.

What has been written for the video door phone 1717/3x-4x also applies to all other video door phones with address book.

To create contacts on the video door phone 1761/6, refer to what stated for the Miro door phone 1160/3, with the only difference that in addition to the T1 and T2 buttons there is also the T3 button.

As a common example we take a *Multi Block* project whose topology is shown in the figure:



Figure 261: Example of system topology for the creation of the address book

The system consists of two blocks with two stairs each, three floors per stair and three apartments per floor. We will assume there is a *Call Module* on the site, one in block "01", a *Switchboard* in block "02", a *MAX video door phone* in Stair "01" of block "01" and a *MAX video door phone* plus an *Miro door phone* in each apartment (not shown in the figure for the sake of simplicity).

#### 7.1.4.1 How to call MAX video door phones and Miro door phones from MAX video door phones, Miro door phones and/or call modules

In order to be able to call a MAX video door phone and/or an Miro door phone from other video door phone in the system, it is necessary to add a contact in the address book of the latter.

The recipient of the contact may be:

- a single device positioned in a topological node;
- a set of devices positioned in a topological node.

To understand the difference between the two cases, take as example the figure above, where every apartment has a *MAX video door phone* and a *Miro door phone*. We will suppose that one of these apartments, for example the one with topological code "0101010101", is a dental practice.

If you want to call only the *MAX* video door phone present in the dental practice from the apartment with topological code "0101010102", add a contact in its address book having that device as target. If, instead, you want to make both the *MAX* video door phone and the *Miro door phone* in the dental practice ring, the contact must be the set of devices in the dental practice, that is in the topological node in which they are placed.

You can create a contact in a topological node using the configurator on the "Address books" tab of the topological node itself.

If you want to add the dental practice as a contact in the address book of the *MAX video door phone* of apartment "0101010102", simply position the navigation unit on the concerned topological node and select the "Address books" tab, as shown in the following figure:

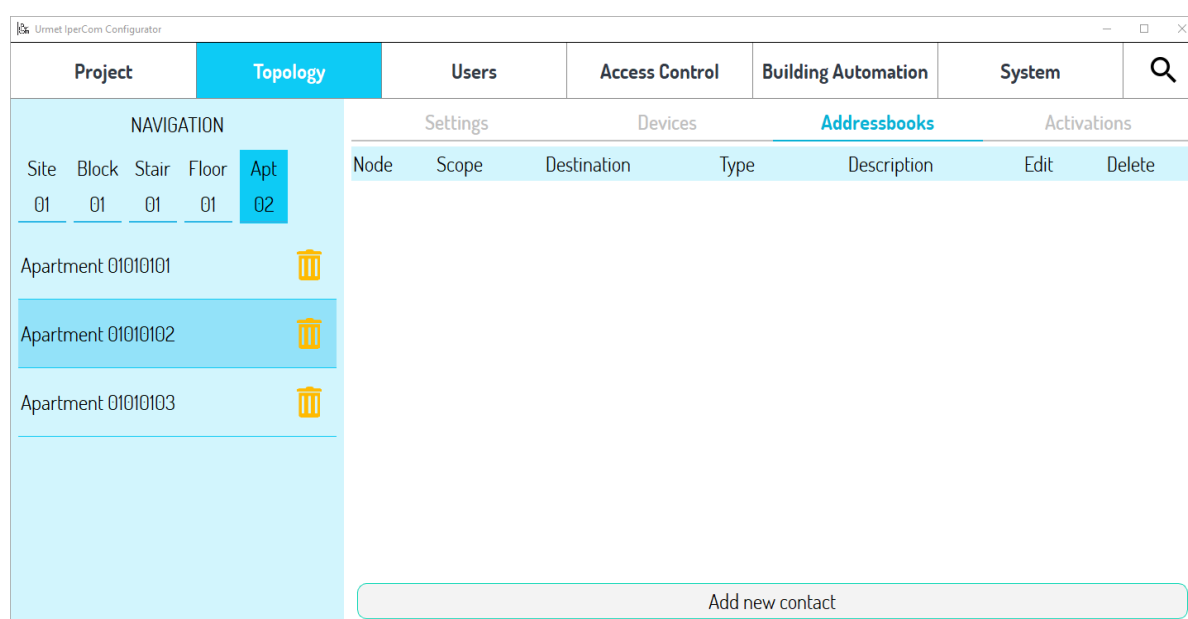


Figure 262: "Address Book" screen

To create the new contact, press the “Add new contact” button. The following page is displayed:

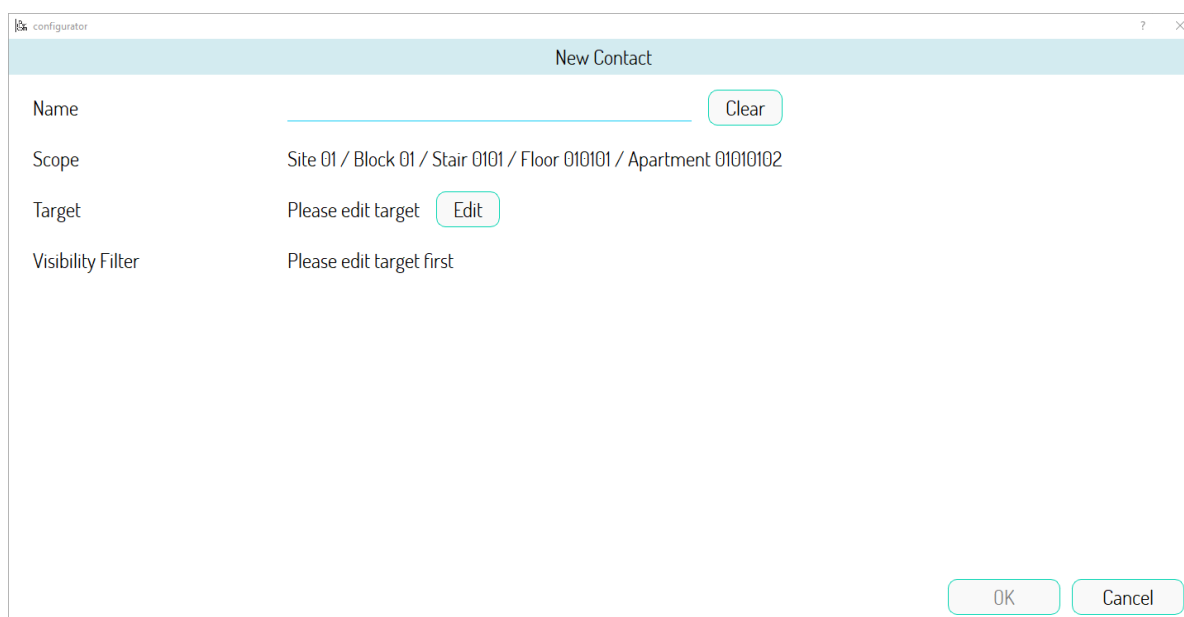





Figure 263: New contact creation screen

The following shows the meanings of the four fields:

<i>Name</i>	Name of contact
<i>Scope</i>	Scope of the contact. This shows the node in which you are creating the contact; if the topological node is different from the apartment, you can establish whether the contact should be public or private (it is public by default).
<i>Target</i>	Who should be contacted. It can be a device or a set of devices positioned on a topological node.
<i>Visibility Filter</i>	Selectable list of device types that should use contact. The list varies depending on the type of target and is displayed only after defining the target. The complete list includes the following items: <ul style="list-style-type: none"> <li>- “Video door phone with address book (VDP)”,</li> <li>- “Call Modules (CM)”,</li> <li>- “Door Phone by mean of button T1 (DP1)”,</li> <li>- “Door Phone by mean of button T2 (DP2)”,</li> <li>- “Door Phone by mean of button T3 (DP3)”,</li> <li>- “CallMe (CallMe)”,</li> <li>- “IPerTalk (IPerTalk)”.</li> </ul>

Table 9: Meaningful fields for creating a contact

-  The T1 and T2 buttons refer to both the Miro door phone 1160/3 and the video door phone 1761/6, while the T3 button refers only to the video door phone 1761/6. Below is an example on how to use these items.
-  The CallMe option, if selected, allows you to view the contact on the CallMe app as well. See the ["APPENDIX S: CallMe contacts"](#).
-  The "IPerTalk" item, if selected, allows you to add an IPerCom contact on an IPerTalk extension.

Assign a meaningful name to the contact, e.g. "Dental Practice", then next to "Target" press the "Edit" button. The following screen will appear, from which you can choose the target.

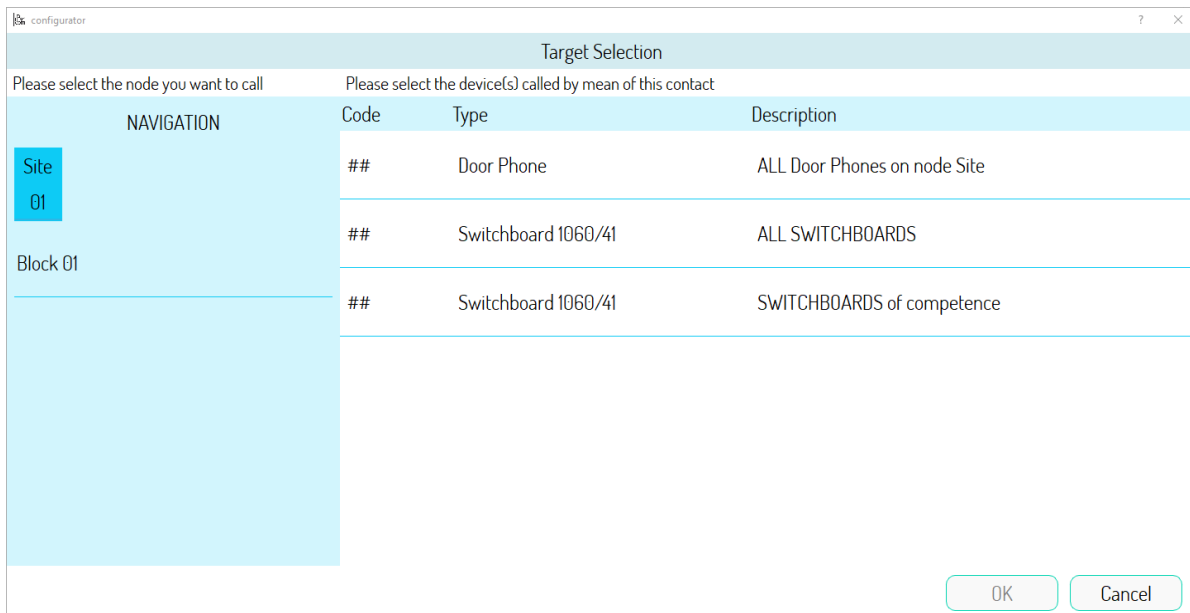


Figure 264: Target selection screen

Now, point to apartment "01010101" with the navigation unit on the left and add the target, selecting it from one of the items suggested on the right:

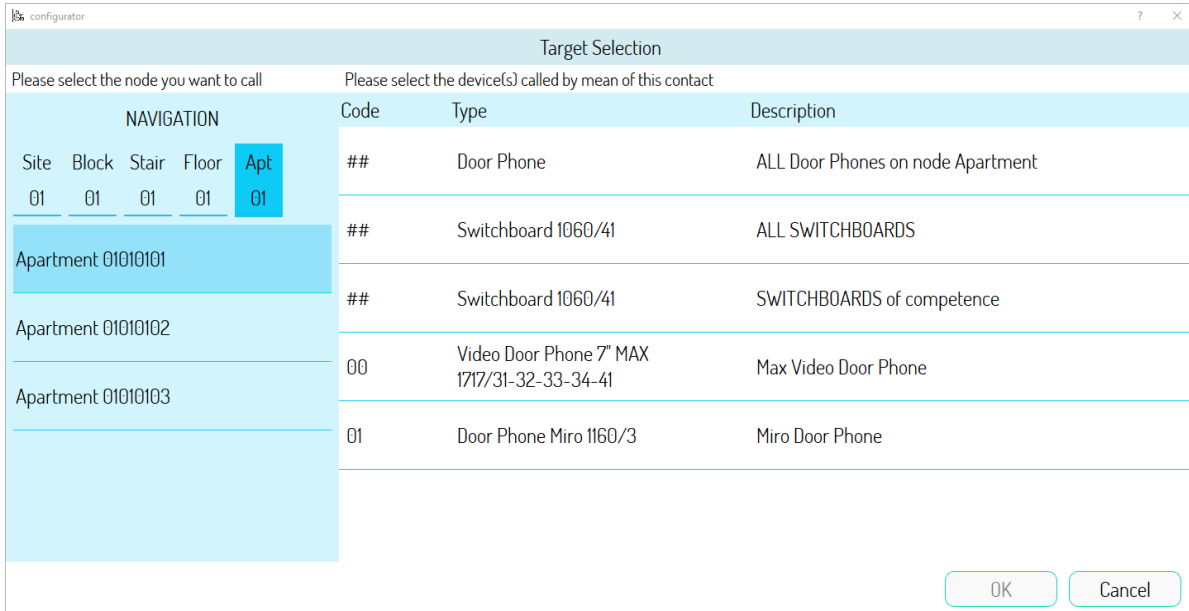


Figure 265: Target selection

As previously mentioned, you can select only one device of the dental practice as target (i.e. only the *MAX* video door phone or the only *Miro door phone*) or both devices referred to the concerned apartment. In the latter case, select "*All Door Phones Door Phones on node Apartment*".

For example, select "*ALL Door Phones on node Apartment*" and press the "OK" button to update the contact.

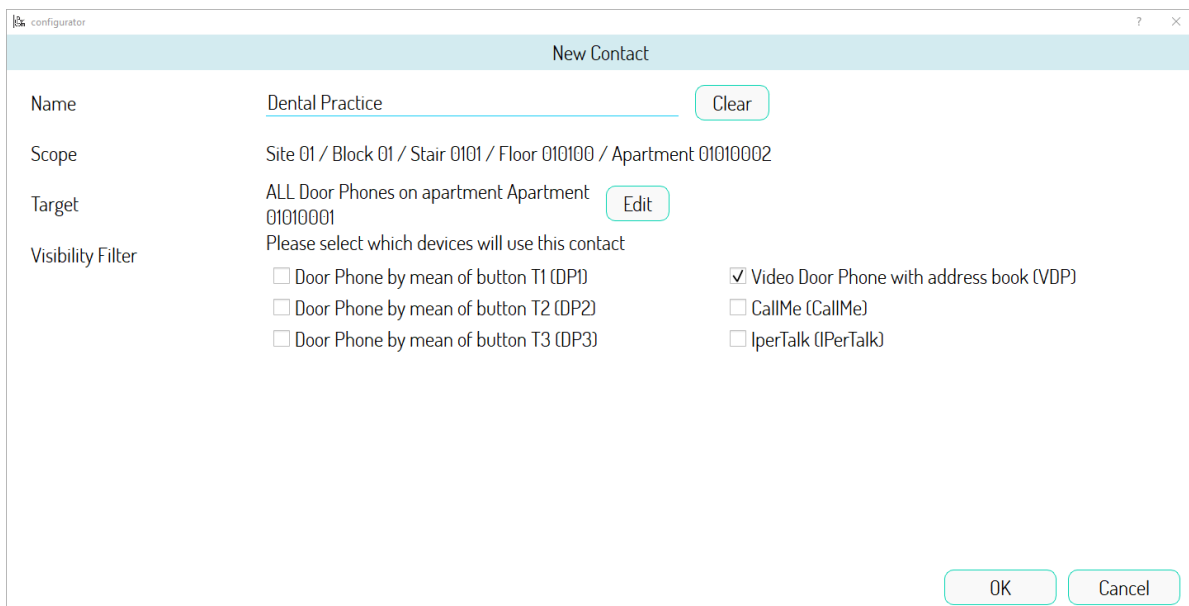


Figure 266: contact creation screen updated with recipient data

As shown in the figure, the “*Visibility Filter*” field is populated with the list of devices that could use the contact: the type of device already automatically selected is “*Video door phone with address book (VDP)*”. Since you want to make the contact visible in the address book of the *MAX* video door phone of the apartment “*0101010102*”, in this case simply press the “*OK*” button. The contact is thus created and the list on the relevant screen is updated:

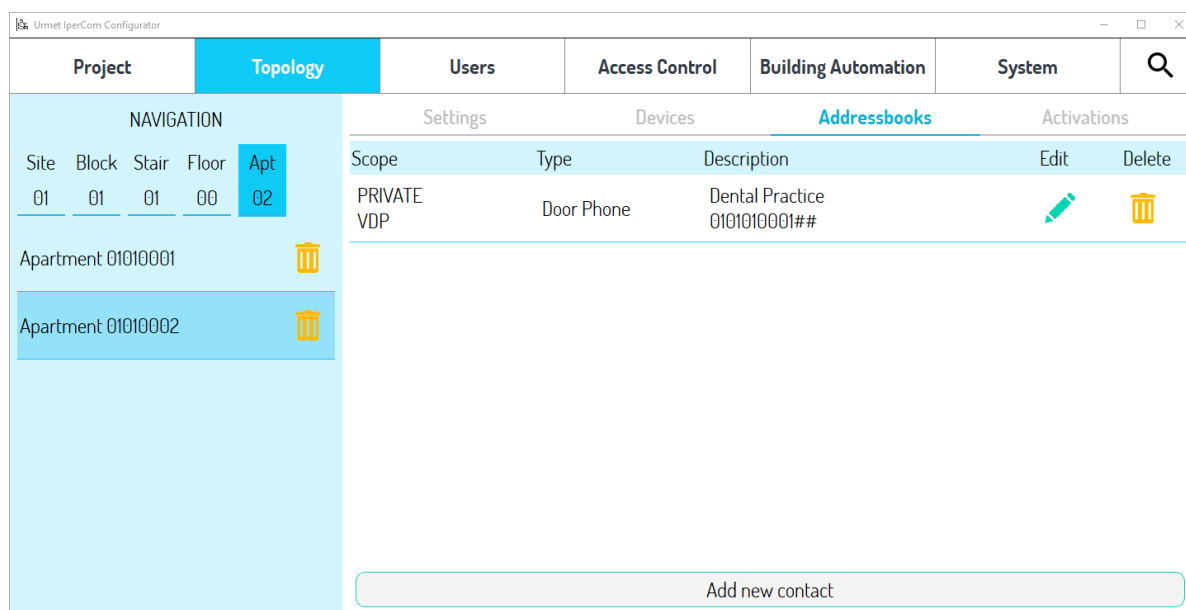


Figure 267: contact list with the new item created

In the “*Scope*” column, depending on what is selected, the “*VDP*” item indicates that the contact is available only for video door phone with address book, the “*DP1*”, “*DP2*” and “*DP3*” items indicate that the contact is available for the Miro door phone or 1761/6 video door phone, the “*CallMe*” item indicates that the contact is available on the CallMe application and finally the “*IperTalk*” item indicates that the contact is available on the extensions of the IperTalk system. These items appear consistently with the choices made in the “*Device Filter*” section (where they are also shown). It is also reported whether the contact is private or public.

The “*Type*” column shows the type of contact chosen, whether apartment station or calling station.

The “*Description*” column shows the name of the contact and its position in the system topology.

In this manner, the new contact *"Dental Practice"* will appear in the address book of the *MAX* video door phone of apartment *"01010102"* and can call it or start a chat with it.

In the list of contacts, the buttons in the *"Edit"* and *"Delete"* columns can be used to edit or delete data for each contact, respectively (via confirmation pop-up).

If you want to add the dental practice also to the address book of *MAX* video door phone in the apartment *"01010103"*, you need to create the contact directly on floor node *"01010101##"* as a public type contact, to display it in the address books of all the apartments of the floor. To do this, open the *"Address books"* screen at the floor node and proceed as described above to fill in the *"Name"*, *"Target"* and *"Visibility Filter"* fields.

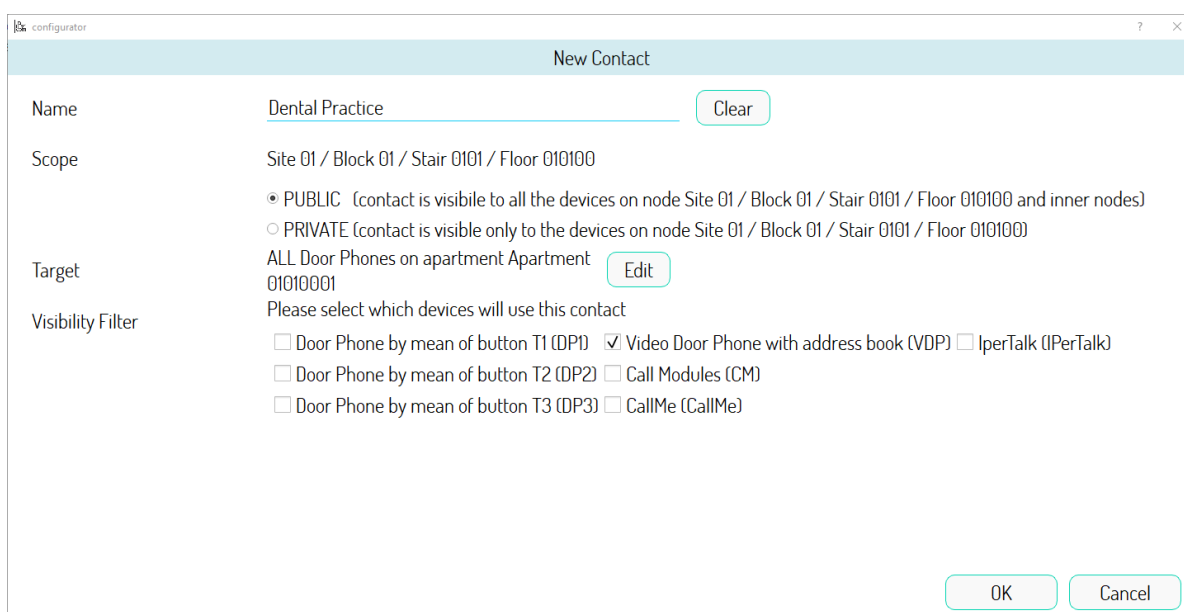


Figure 268: adding the desired contact on the plan

The *"Scope"* field, instead, confirms the *"PUBLIC"* selection so that the contact will appear in the address books of all *MAX video door phones* of the nodes which belong to the floor node, i.e. of all the apartments present on the floor topologic node *"01010101##"*.

If you want to add the *"Dental Practice"* contact also in address book of *MAX video door phone*, which is located on stair *"010101####"*, simply create a new contact in the *"Address books"* by pointing to the stair node rather than on the floor node. In this case, if the *"PRIVATE"* option is selected, in the *"Scope"* field, the contact will only be displayed by the *MAX video door phone* of the stair, while if you select the *"PUBLIC"* option, the contact will be also displayed on the address books of the *MAX video door phones* of the various floors of the stair.



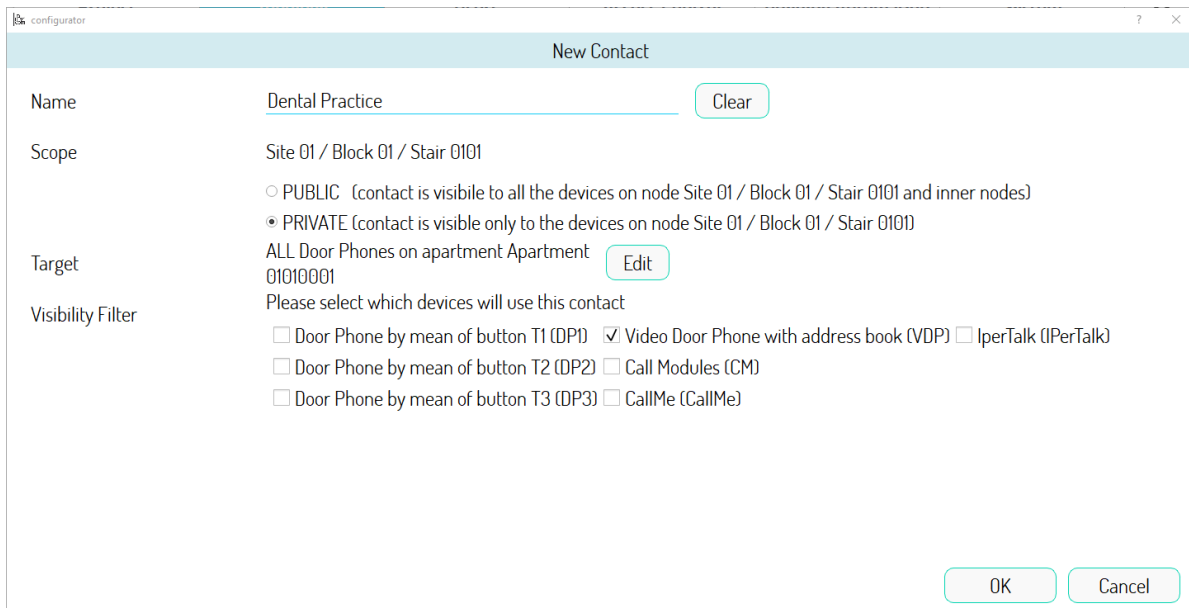


Figure 269: creation of the desired contact on the scale "010101 ####" (private scope)

Similar considerations apply to extend the "Dental Practice" contact to all MAX video door phones of the system. Simply create the public type contact on the site.

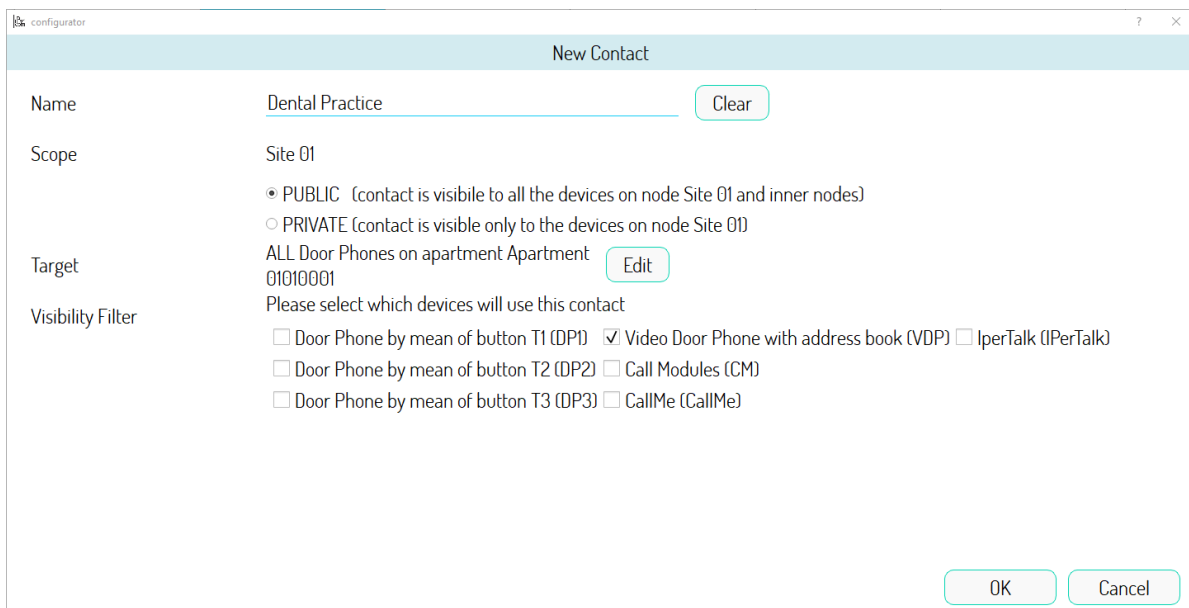


Figure 270: creation of the desired contact on the site node

Since in each apartment in the example there are a MAX video door phone and a Miro door phone, you can allow the Miro door phone of the whole site to call the "Dental Practice" contact.

To do this, select the "Door Phone by mean of button T1 (DP1)" option to call it using button T1 of the Miro door phone and/or the "Door phone by mean of button T2 (DP2)" option to call it using button T2.

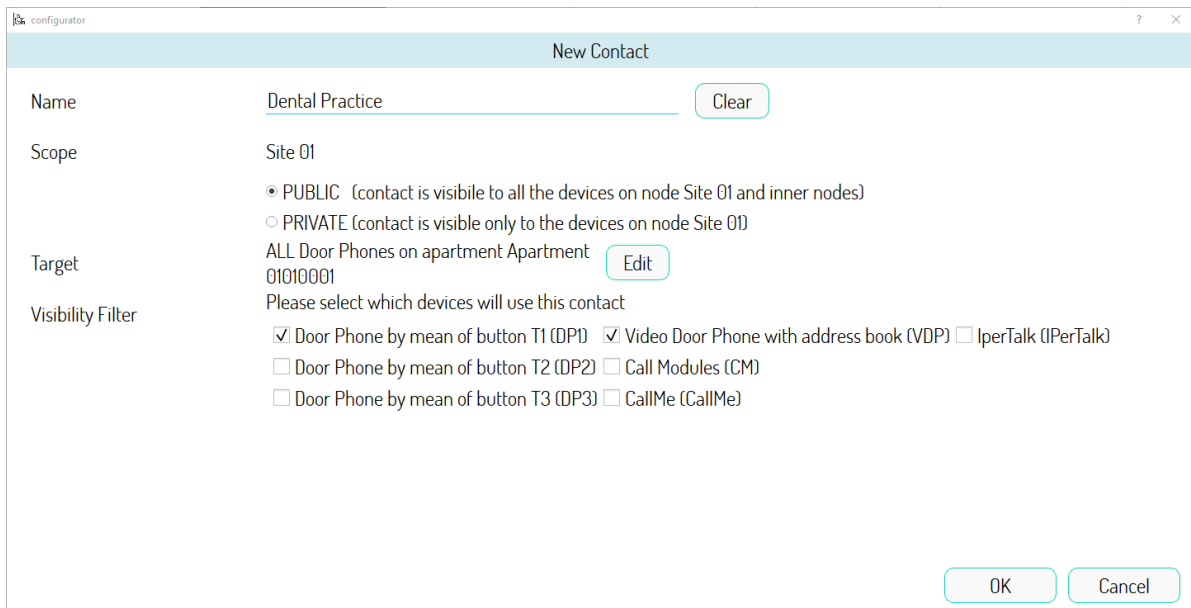


Figure 271: contact that can also be called via the T1 button of the Miro doorphone of the entire site

In the case shown in the figure, the created contact can be called by means of button T1 of each *Miro* door phone in the system.

To view the contacts that a *Miro* door phone can call, refer to the *Miro door phone* section in [APPENDIX A: Configuration parameters of IPerCom devices](#).



The association of contact - T1, T2 and T3 buttons for the video door phone 1761/6 takes place in the same way.

To make this contact also visible in the address books of *Call Modules* of the entire site, simply select the "Call Modules" option in the "Visibility Filter" field.

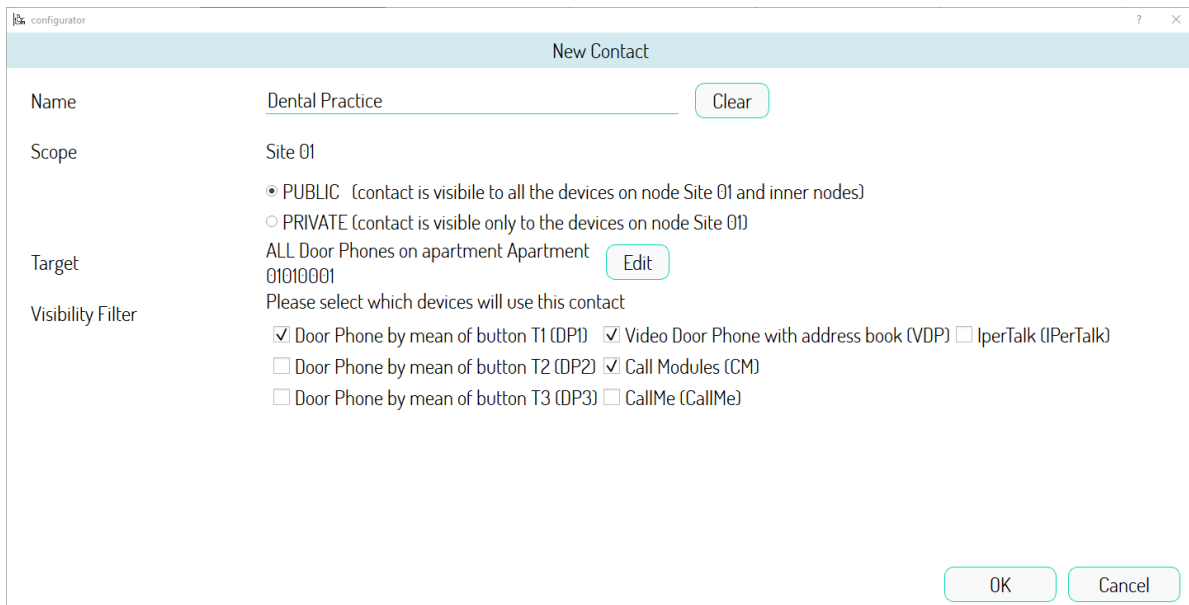





Figure 272: Adding a contact to the address books of *Call Modules* of the whole site

With this setting, the *Call Module* in the site and the one in block "0101#####" will both be able to call the Dental Practice using the "Dental Practice" contact added to their address book.

To allow calling the contact only from *Call Modules*, simply deselect the other options which are present in the "Visibility Filter" field.

-  If a generic apartment station on a node other than the apartment node (e.g. stair node) is chosen as recipient, the "ALL apartment stations on the Stair node" item indicates that the apartment stations on that node and not the apartment stations on the stair node and lower nodes are called.
-  MAX video door phone contacts in nodes other than the apartment: the addition of a contact in the address book is useful whenever a MAX video door phone is installed in a node other than the apartment. For instance, if we consider a "Swimming pool" room on the stair "010101#####" of the example in Figure 194 if you would like to contact the MAX video door phone present therein from the other apartments, simply create a contact in the public domain on the site related to that MAX video door phone.
-  This method can be used to create a contact in the address book of a *Call Module* which is outside the topological group of the node in which the *Call Module* itself is located. In this way, apartments whose residents (visible) do not automatically appear in the address book of the *Call Module* can be called for special needs.

### 7.1.4.1.1 How to call an IPerCloud apartment

If you want to call an IPerCloud apartment from a video door phone or a door phone, after selecting the IPerCloud apartment to define the recipient of the contact, the screen that appears is the following:

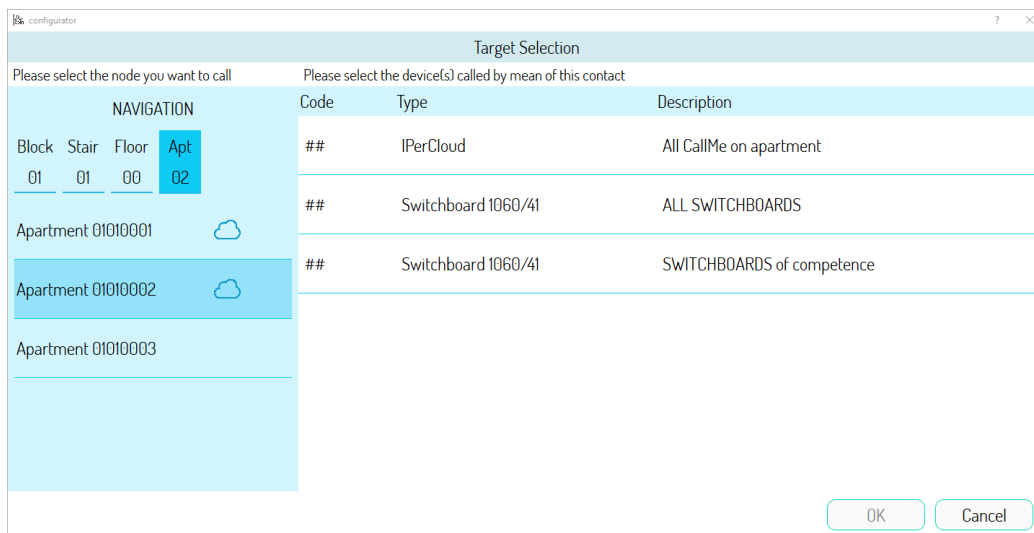


Figure 273: recipient selection screen in case of IPerCloud apartment

Selecting the item “All CallMe on apartment” and pressing the “OK” button, the following screen appears:

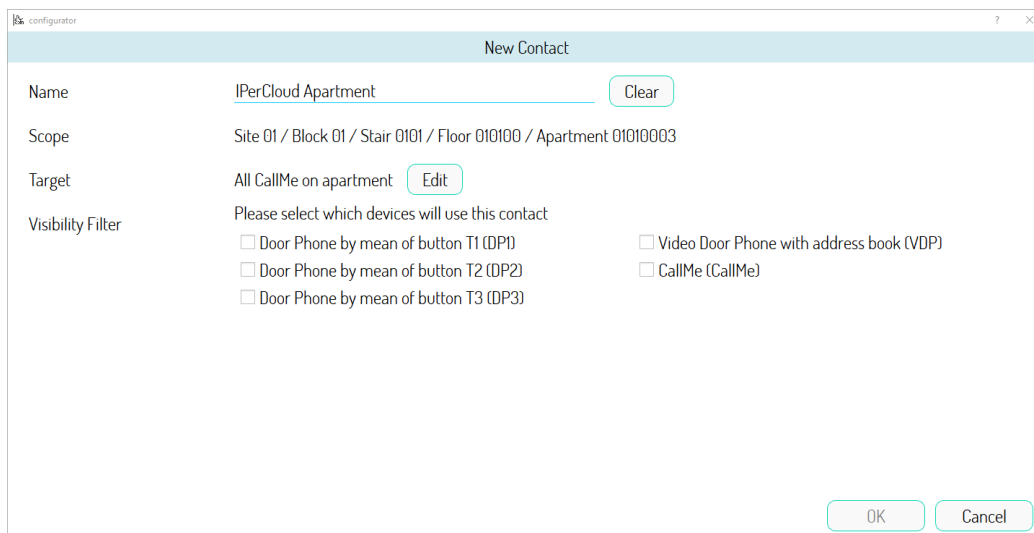


Figure 274: contact creation screen updated with recipient data

Selecting the “Video Door Phone with address book” item and pressing “OK”, the contact is created as shown below:

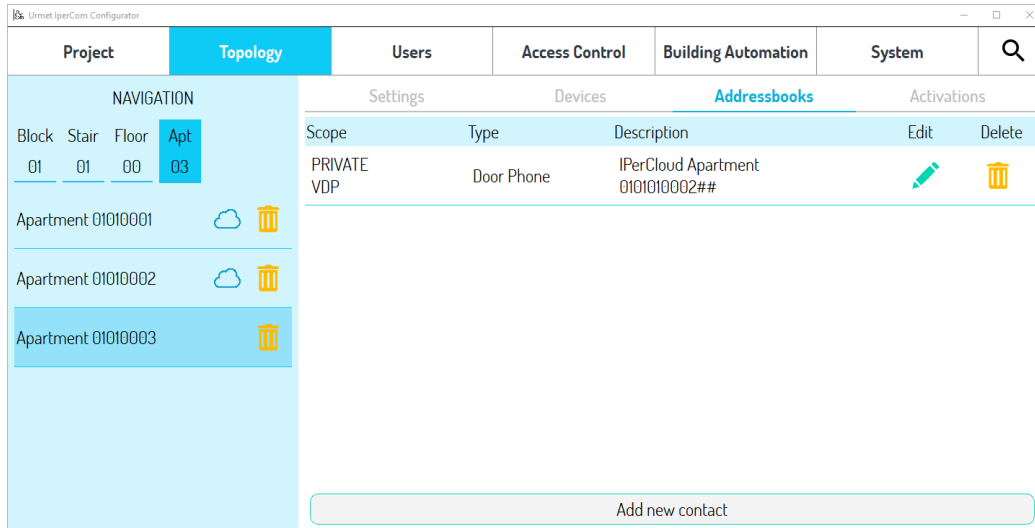


Figure 275: contact with destination IPerCloud apartment created

In this way the video door phone of the apartment "01010003" will see the contact relating to the IPerCloud apartment in the address book and by calling this contact it will receive the call on its own smartphone/tablet.

In the same way it is possible to call from an IPerCloud apartment another IPerCloud apartment or to a non-IPerCloud apartment with the only difference that in [Figure 275](#) you need to select the item “CallMe”.

7.1.4.2 How to call the Switchboards from MAX video door phones, Miro door phones and/or call modules

In the example in *Figure 180* there is a *Switchboard* on block "0102#####". Automatically, all *MAX video door phones* the topological path of which intercept the switchboard, will have a button in the video door phone application that can be used to call the respective *Switchboard*. The *MAX video door phones* are the ones included in the topological group of the block node "0102#####".

Otherwise, no *MAX video door phone* in topological group of block "0101#####" will have the button available (the *Switchboard* is not on their topological path), so the only way to be able to call the *Switchboard* is add a "Switchboard" contact in the address book using the "Contacts" tab.

For *Door Phones Miro* the topological path of which crosses the *Switchboard* and those which do not, there is no automatic association of calling buttons with the *Switchboard*. However, the "Switchboard" contact can be created and associated with buttons T1 and/or T2 of the generic *Miro door phone* so that it can be called.

Finally, also from the *Call Module* referred to block "0101#####", you cannot call the *Switchboard* using the dedicated button because the *Switchboard* is not on its topological path; therefore, also to be able to call the *Switchboard* from the *Call Module* you will need to create the contact in "Address Books".

We will supposed to add to the address book of all *MAX video door phones* of block "0101#####" the *Switchboard*, which is placed on block "0102#####". In this case, open the "Address books" screen at the topological node of block "0101#####" and create a new contact.

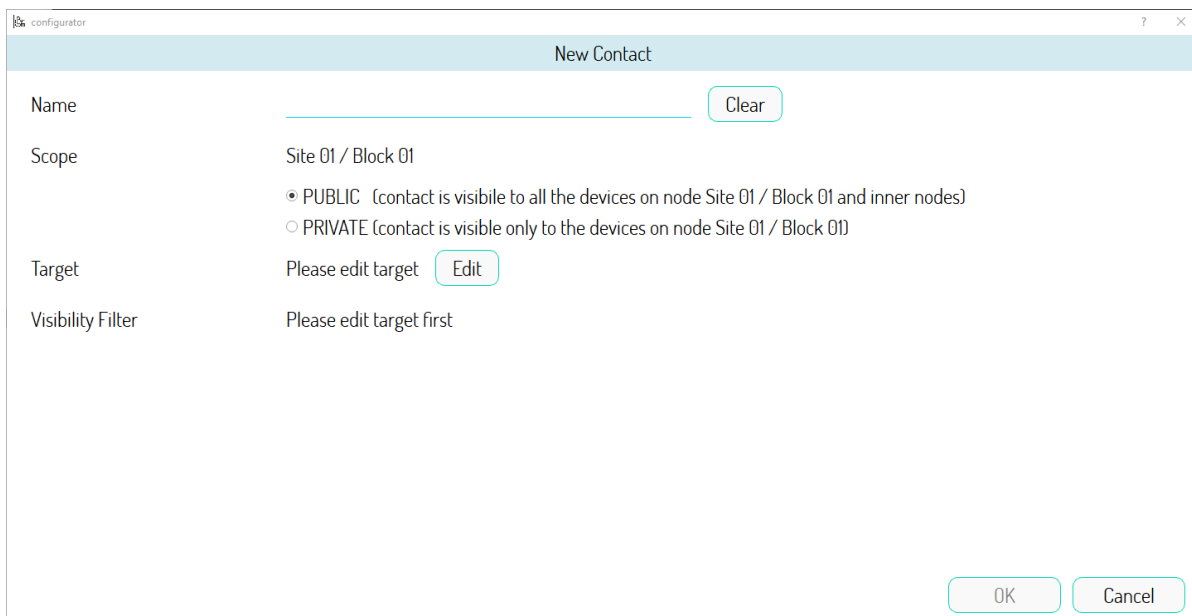


Figure 276: Creating a contact for the switchboard

After assigned meaningful name to the contact as "Switchboard", you should choose the target by pointing to the topological node in which the *Switchboard* is located.

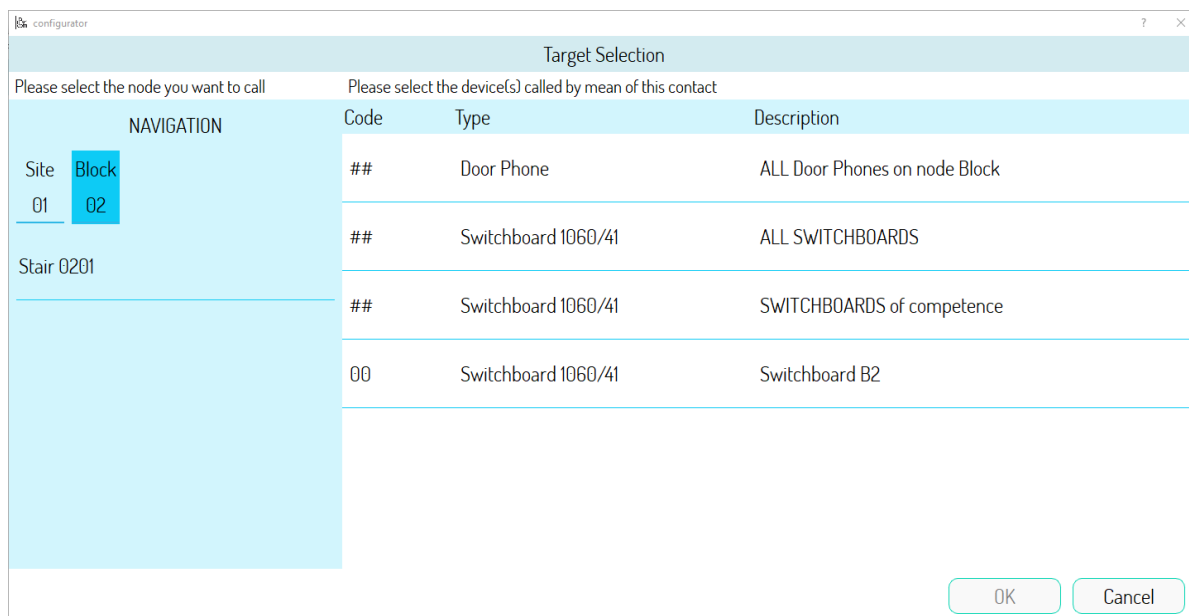


Figure 277: Selecting the target of the "Switchboard" contact

In the case of *Switchboards*, the following selections can be made (on each node):

- "*Switchboards of competence*", which can be used to select as target only the Switchboards which are placed on the topological path of monitor MAX, Door Phone and Call Module;
- "*ALL SWITCHBOARD*", i.e. all the *Switchboards* on the selected topological node, independently from competence.
- the single *Switchboard* which is located at that node topological.

Let us assume you choose single Switchboard called "Switchboard B2". The following screen will appear:

Figure 278: contact creation page updated with recipient data

Select the "MAX" option in the field " Video door phone with address book" field and confirm the "PUBLIC" selection in the "Scope" field, to make the contact appear in the address book of all MAX video door phones of the topological nodes which belong to block "0101#####".

Figure 279: setting the "Scope" and "Device Filter"



Press the "OK" button to finish creating the contact, as shown in the following figure:

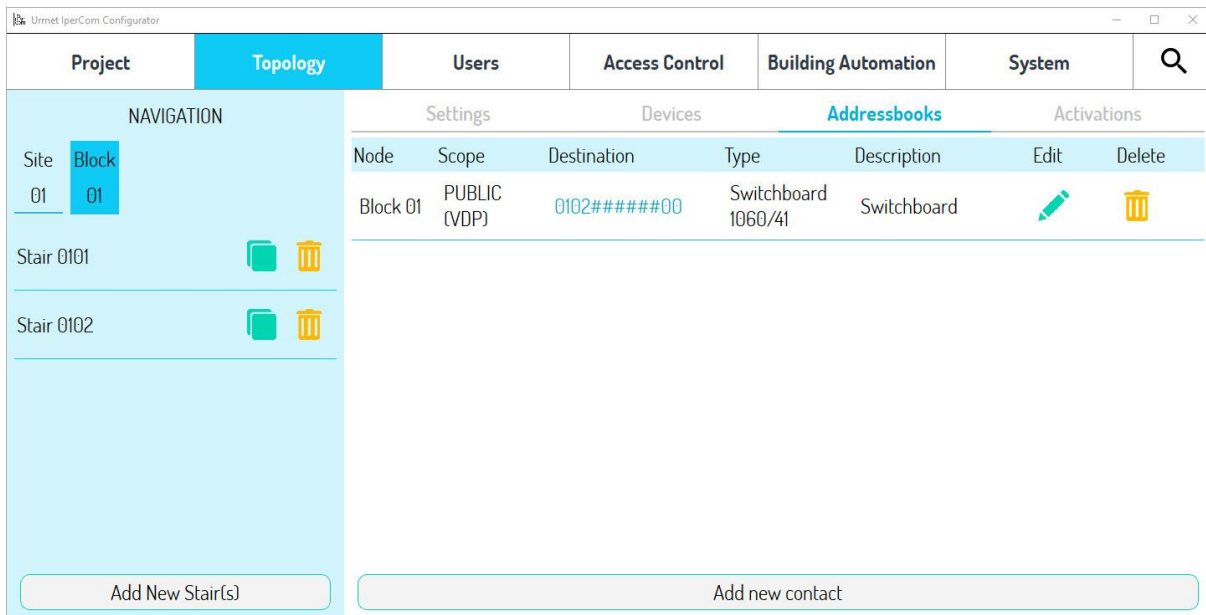


Figure 280: List of contacts with new created contact

In this way, the MAX video door phones of the topological nodes which belong to block "0101#####" will see the new "Switchboard" contact in their address book and will be able to call or chat with it.

To ensure that the *Miro door phone* in various apartments of block "0101#####" can call the *Switchboard*, simply select the "Apartment station by mean of button T1" option to call the "Switchboard" by pressing button T1 of the *Apartment station*. At the same way select "Apartment station by mean of button T2" option to call it by pressing button T2.

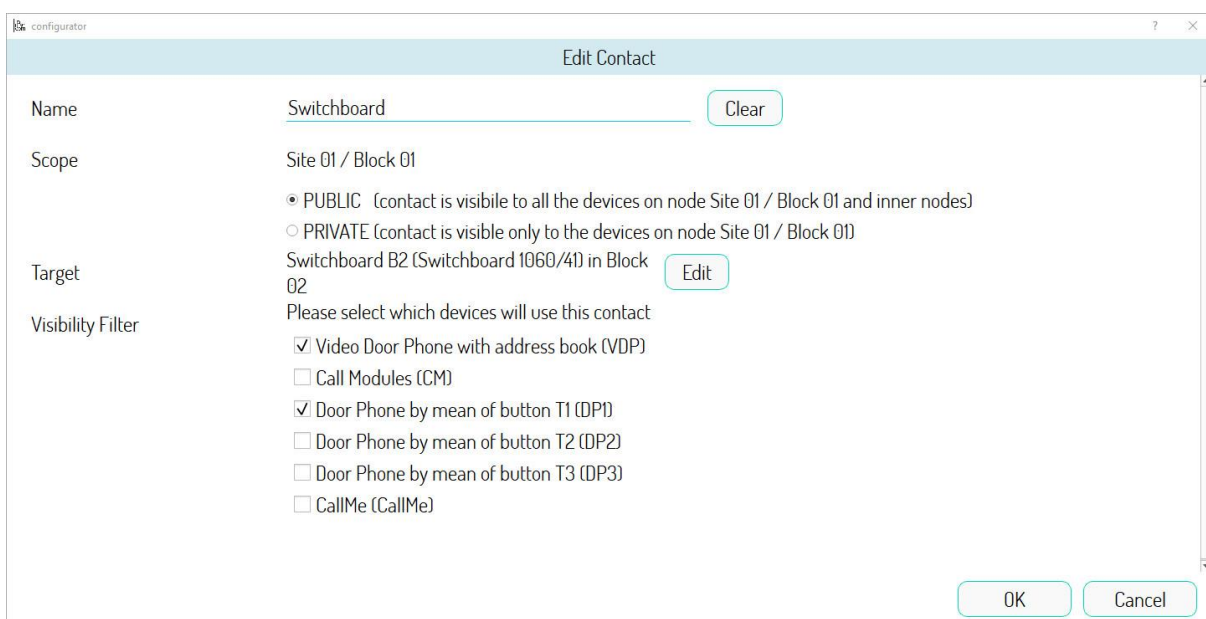


Figure 281: "Switchboard" contact which can also be called using button T1 on the Miro door phones in the block

In the case shown in the figure, the created contact can be called by means of button T1 of each *Miro door phone* in block "0101#####".

To make this contact also visible also in the address books of the *Call Modules* referred to block "0101#####", simply select the "Call Modules" option in the "Visibility Filter" field.

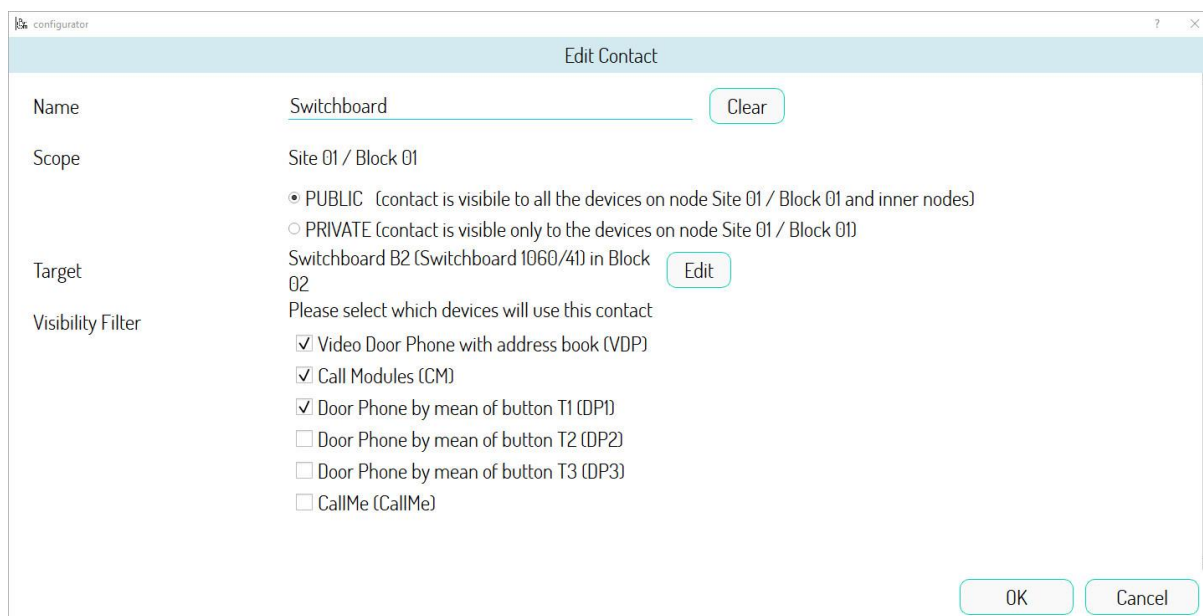


Figure 282: contact added to the address book of the Call Module in the block



*The video door phone 1761/6 has a button to automatically call all switchboards in its topological path. Therefore, unlike the Miro door phone, there is no need to create any association between the T1, T2 or T3 buttons and these switchboards. Instead, the association must be created for those switchboards that are not on its topological path, as seen above.*

7.1.4.3 *Auto-on function on Door Speaker Units, Call Modules and RTSP cameras from MAX video door phones outside their competence.*

The *MAX video door phones* can automatically make autoinsertion on *Entry Panels, Call Modules* and *RTSP cameras* only if these calling stations are on the topological path of the video door phones themselves and if the item “*Automatic assignment for CCTV cameras*” is enabled (see [Global Settings](#) paragraph).

If one of the devices listed above is not on the topological path of the *MAX video door phone* or it is but the item “*Automatic assignment for CCTV cameras*” is disabled, you can still enable auto-on by using the “*Address books*” screen.

Referring again to the example in *Figure 194*, all *MAX video door phones* under block “0101#####” can make autoinsertion on the *Call Module* in that block.

To use the auto-on function on this *Call Module* from a generic *MAX video door phone* on the other block, open the “*Address books*” screen at block “0102#####” and add a new contact.

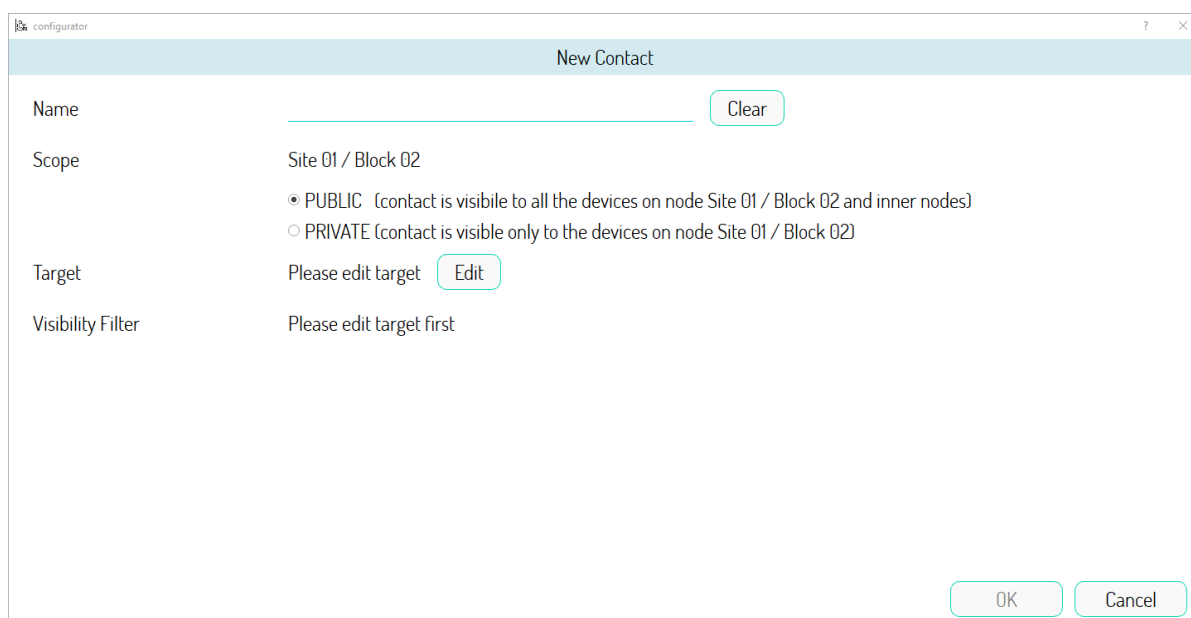


Figure 283: Creating a contact for a Call Module

Assign a meaningful name to the contact, e.g. "Call Module Block 01", because the target must be able to select the desired Call Module.

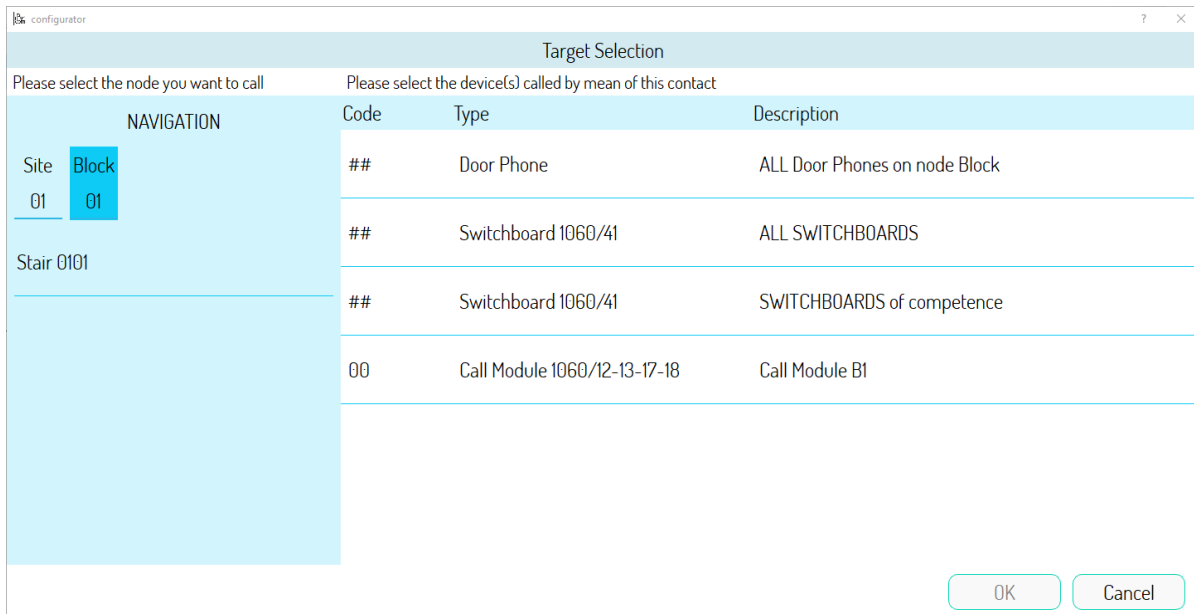


Figure 284: Selecting the target of the "Call Module Block 01" contact

Pressing the "OK" button will update the contact creation screen, as shown in the following figure:

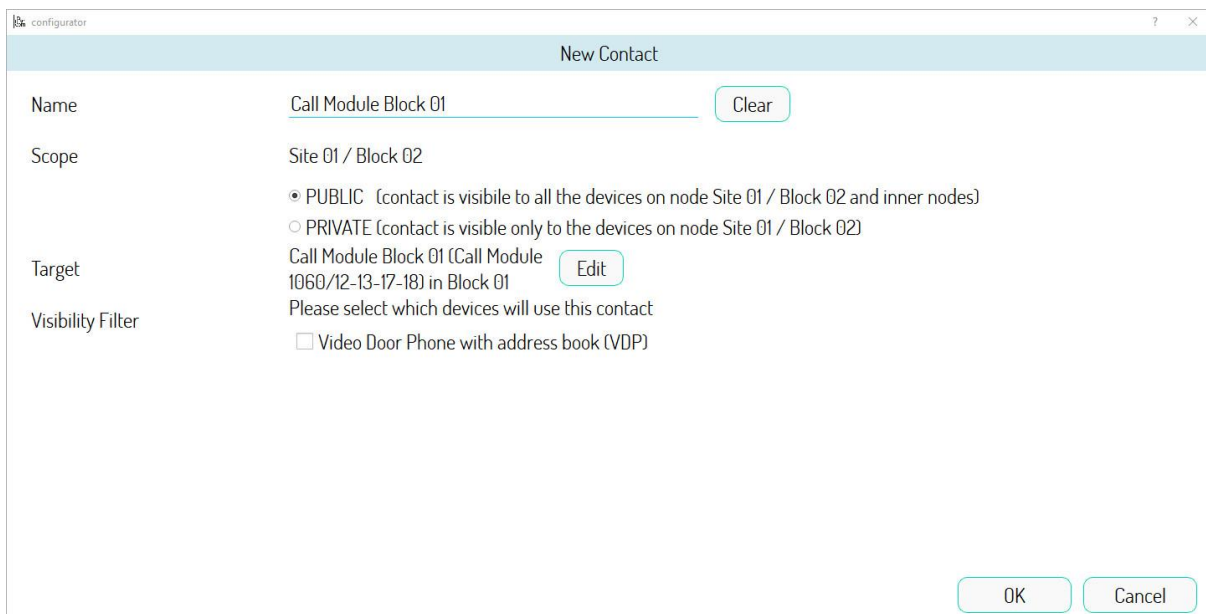


Figure 285: contact creation page updated with recipient data

Select the "Video door phone with address book" option in the field "Visibility Filter" field (the only option available in this case) and confirm the "PUBLIC" selection in the "Scope" field, to make the contact appear in the CAMERAS list of all MAX video door phones of the topological nodes which belong to block "0102#####".

Figure 286: "Scope" and "Device Filter" setting

Press the "OK" button to finish creating the contact, as shown in the following figure:

Settings		Devices		Addressbooks		Activations	
Node	Scope	Destination	Type	Description	Edit	Delete	
Block 02	PUBLIC (VDP)	0101#####01	Call Module 1060/12-13-1...	Call Module Block 01			

Figure 287: List of contacts with new created contact

In this way, the MAX video door phones of the topological nodes which belong to block "0101#####" will see the new "Call Module Block 01" contact in the "CAMERAS" list and be able to use the auto-on function of this device.



*In this mode of use of the “Contact” tab, the “Video door phone with address book” option also includes video door phone 1761/6*

If one or more gateways are present in an IPerCom system, the 2Voice apartment stations can carry out:

- intercom calls (to other apartment stations of the system);
- calls to switchboard;
- auto insertion on call stations.

with the following limitations:

1. 2Voice audio / video apartment stations can call the IPerCom apartment stations (*MAX video door phones or Audio Door Phones 1160/3*) or 2Voice audio / video apartment stations of another riser column only through the *Switchboard* application;
2. 2Voice audio / video apartment stations always use a dedicated button to call all the switchboards of the system that are not in stand-by and that are not in stand by and are on their topological path;
3. 2Voice audio / video apartment stations can make auto insertion on all the IPerCom *Call Modules* and *Entry Panels* that are on their topological path only on the secondary call stations placed on the gateway they belong to.



*The auto-on on RTSP cameras by 2Voice audio / video apartment stations is not supported.*



*2Voice audio / video apartment stations can directly call only other audio / video apartment stations of the same stair (where the gateway is placed) via properly programmed dedicated push buttons. For further details follow the instructions in the 2Voice technical manual.*

The limitations reported in the 3 points above are reflected in some differences on the construction of contacts with respect to what is written in the previous paragraphs.

Calls to apartment stations, switchboards and auto insertion are made by means of push buttons that can't be programmed through the IPerCom configurator and therefore the construction of the address book for audio / video 2Voice apartment stations must have of course limitations as explained below.

As an example, the following figure is shown:

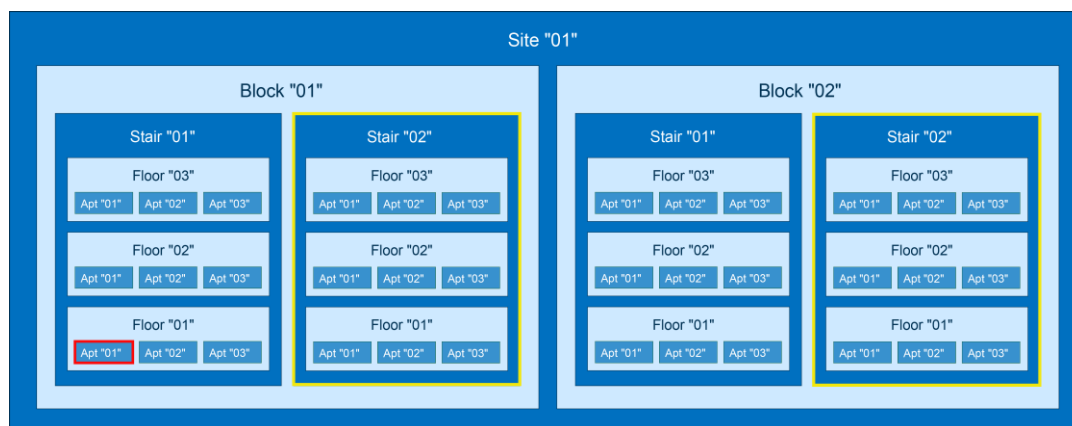


Figure 288: plant topology

where:

- stairs "010102#####" e "010202#####" are with Gateway IPerCom-2Voice 1083/59 (highlighted in yellow);
- stairs "010101#####" e "010201#####" are stairs with IPerCom apartment stations;
- "0101010101" topologic code apartment is a dental practice (in red).

If you want to add the dental surgery as a contact in the address book of a 2Voice audio/video apartment station, this is prevented by the configurator: in fact, by positioning on the nodes below the stair node with gateway, the *Contacts* tab is no longer available (up to 2Voice apartment nodes):

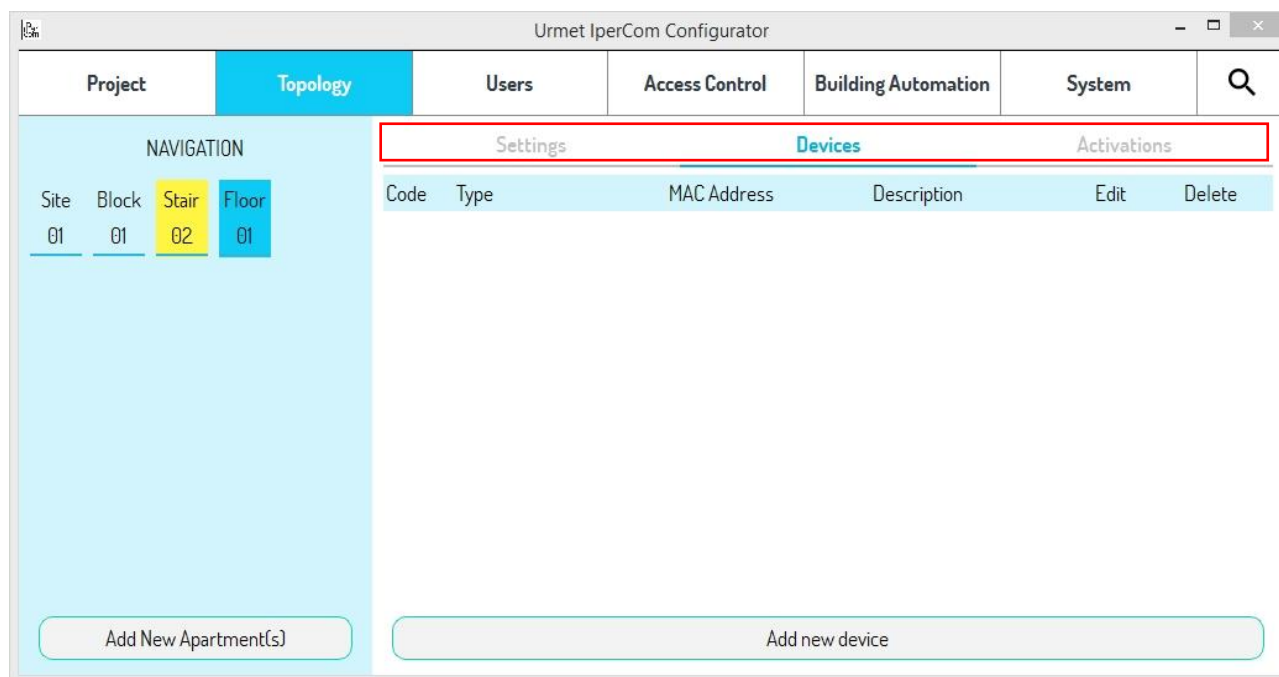


Figure 289: Tab "Address books" not present on nodes below the stair node with gateway

The *Contacts* tab instead remains available on each stair node with *2Voice Gateway*, as on these nodes it is possible to add other IPerCom devices (for example one or more *MAX video door phones* on which it may be necessary to create an address book).

On stair 1 of block 1, instead, the *Contacts* tab is normally present up to the apartment node:

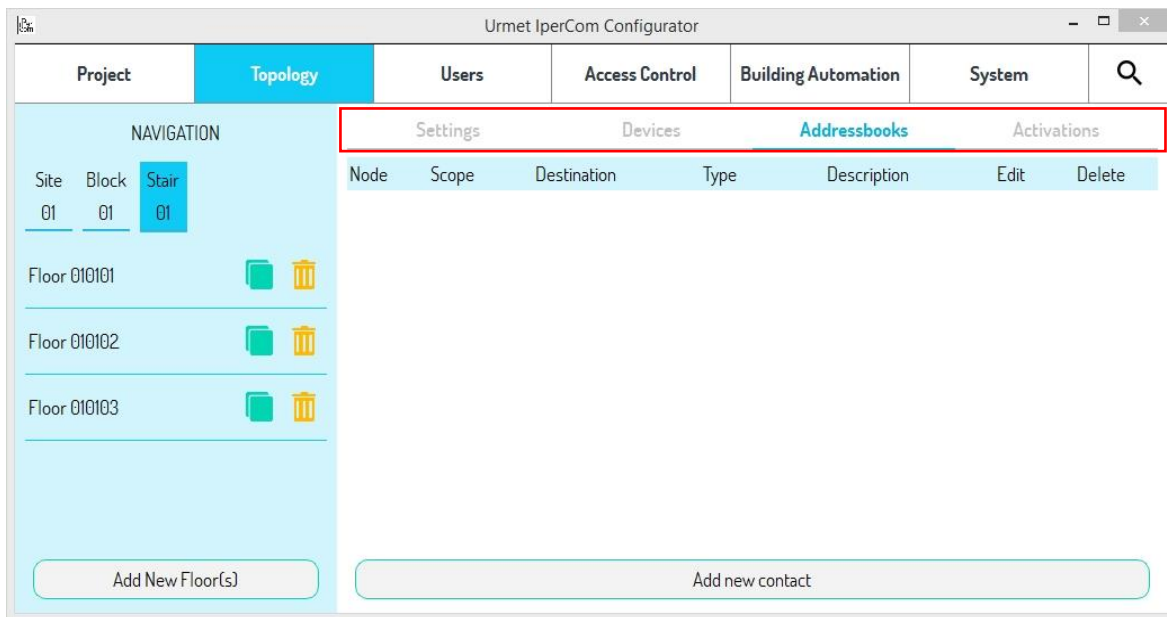


Figure 290: Tab "Address books" present on stair without gateway

Similarly, it is not possible to add a switchboard contact or a *Call Module* or *Entry Panel* to carry out the auto insertion on a *2Voice* audio / video apartment station.

If the dental practice contact (or other) is added on the site node with the "*Public*" option selected, this is not propagated on the stair nodes with gateways and its lower nodes.

In order that *2Voice* apartment stations can call the dental practice, they must call the switchboard, the switchboard call the dental practice and then make a call transfer.

In general, IPerCom and *2Voice* devices do not always behave in the same way about the most important services offered by the IPerCom system.

In Appendix B and Appendix C there are 2 tables that summarize these differences in performance, in detail in Appendix B differences in performance between an audio / video apartment station IPerCom and one *2Voice* are listed while in Appendix C differences in performance compared to Switchboard are listed.




### 7.1.5 Activations

The "activation rules" (more briefly "activations") allow defining the behaviour of the relay outputs in relation to events that can occur within the *IPerCom* system.

The devices that provide the control relays output are:

- *Relay Actuators* 1060/84: two fully independent relay outputs and two inputs,
- *Lift Interface* 1060/37: 24 relay outputs and one input,
- *Entry Panel* 1060/33-34-71-74-75-78: only the relay output that controls the gate,
- *Entry Panel* 1060/21: only the relay output that controls the gate,
- *Call Module* 1060/12-13-17-18-23: only the relay output that controls the gate,
- *Modular Calling Station with* 1060/48: only the relay output that controls the gate.

The devices *Relay Actuator* 1060/84 and *Lift Interface* 1060/37 connect directly to the IP network. For the other devices it is necessary to set the gate as the output of a relay actuator in the *configurator* (see paragraph [Gate contact used as output of a Relay Actuator](#)).

 *The relay output connected to the gate of a calling station can function alternatively as the output of a relay actuator or as an output that controls a gate.*

To program the outputs of the *Relay Actuator*, follow the instructions on the device configuration page ([APPENDIX A: Configuration parameters of IPerCom devices](#)).

For the programming mode of *Lift Interface* outputs in *Lift Interface* mode, follow the instructions in paragraph *Lift Interface*. In *Relay Actuator* mode, follow the *Relay Actuator* device configuration page (paragraph [APPENDIX A: Configuration parameters of IPerCom devices](#)).

The events that define the behaviour of the relay outputs can be divided into three groups listed below:

1. **Events on device:** outgoing call, auto-on, tamper alarm, coercion alarm, code activation; door opening, gate opening, user recognition (following proximity key passage or door opener code entry); these events can be set from the configuration page of the devices, i.e. *Call Module, Entry panel (1060/21-22-33-34-71-74-75), Modular Entry Panel with 1060/48, Key Reader*.
2. **Topological events:** door opening, gate opening, incoming call (only for apartment stations), user activation (on *MAX, VOG<sup>7</sup>, VOG<sup>5+</sup>, IPerCom Client* and *Basic* video door phones), user activation - Apartment station T1 (key 1 of *Miro* door phone 1160/3 and video door phone 1761/6), user activation - Apartment station T2 (key 2 of *Miro* door phone 1160/3 and video door phone 1761/6), lift up, lift down, panic alarm, activation from switchboard. Except the last event, all others can generally be set on a precise topological node of the system (i.e. at site, block, unit, floor, or apartment level) and are then propagated on all apartment station contained in the topological group of the node on which the activation will be created. If the activation has been set on an apartment, it will only apply to that individual apartment. Switchboard activations, on the other hand, concern only the **Switchboard** application and, more precisely, they are activation rules created on the topological path of the application itself.
3. **Automation events:** events related to the configuration of the inputs of *Relay Actuator 1060/84* (with firmware version 3.04 or higher).



*Door and gate opening events on call devices activate one or more relay outputs only during the call phase. The same events defined at topological level activate the relay outputs also outside the call, by simply pressing the door and gate opening keys of apartment stations.*

On the *configurator* the choice of the above events and the configuration of the corresponding relay outputs can be carried out as follows.

For the **events on device**, it is necessary to open the configuration page of the devices indicated in point 1:

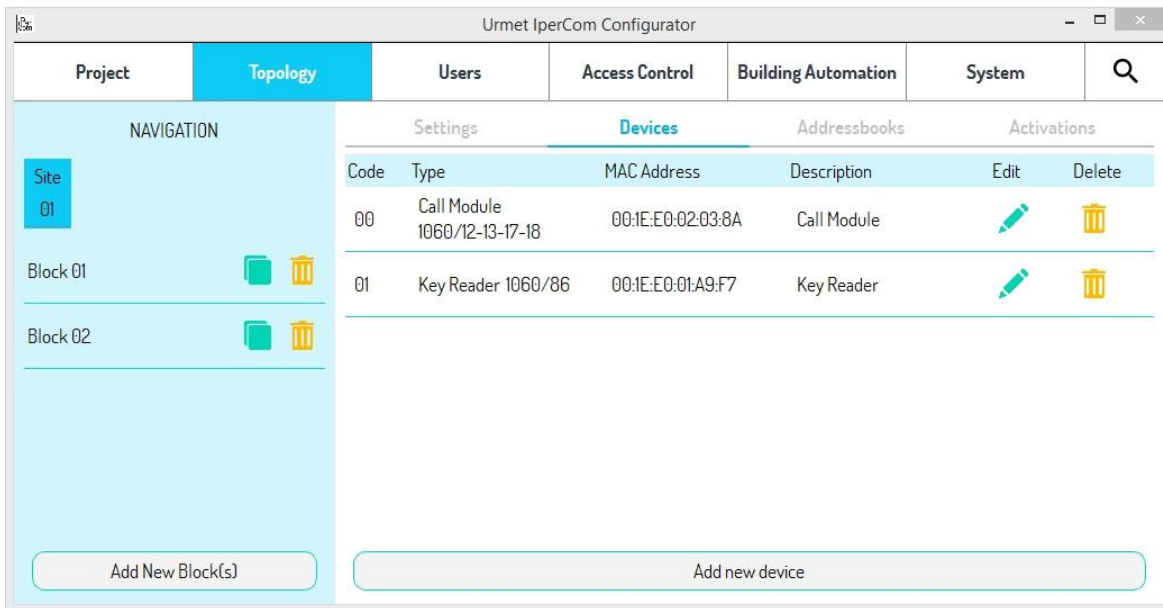


Figure 291: Devices present on site node

Simply press the "Edit" button of the Call Module. At the bottom of the screen there is the "Add" button in the "Activations" section, from which it is possible to create the activation rule as described below.

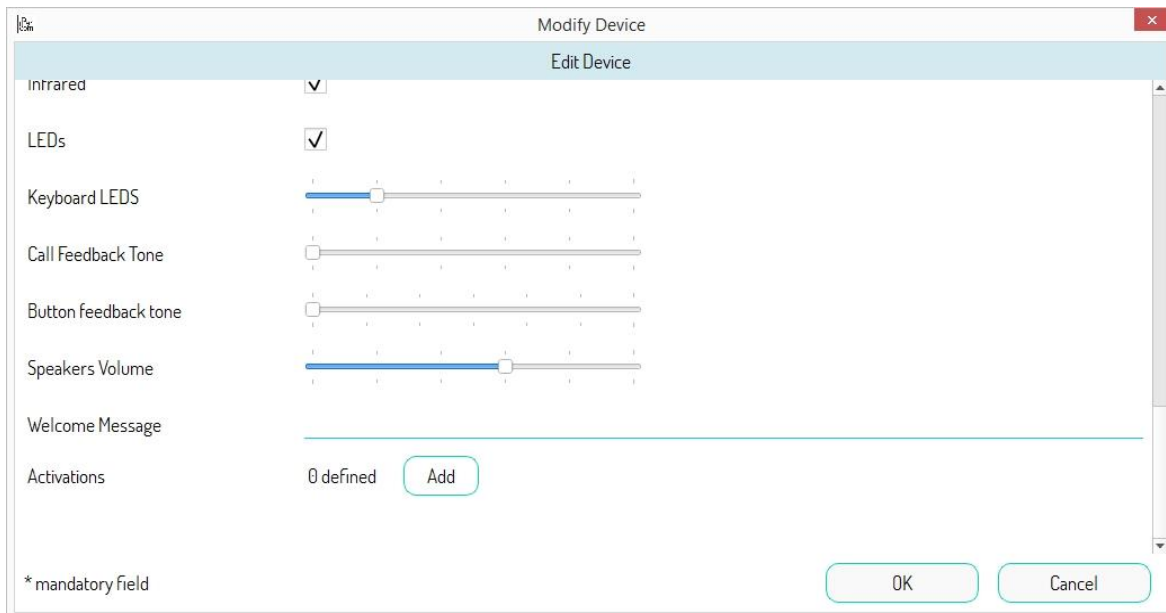


Figure 292: "Activations" button to connect device events to the outputs

For **topological events**, press the "Activations" tab on the "Topology" page and navigate the topological structure of the system to the node where you want to create the activation rule:

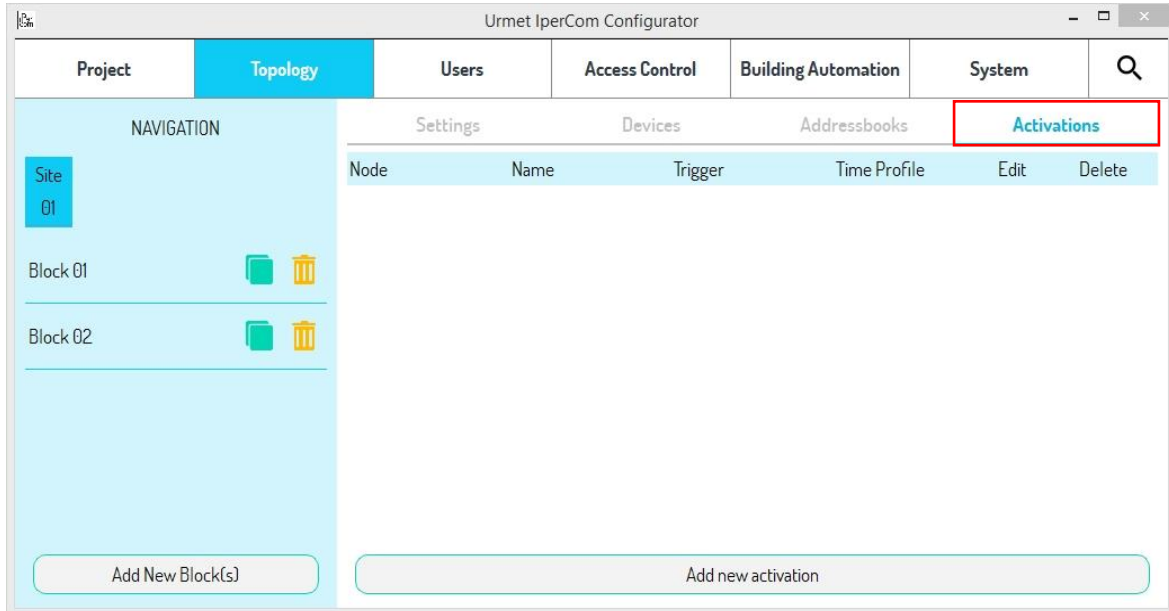


Figure 293: "Activations" tab to connect topological events to outputs

For **automation events**, press "Automation" on the main screen of the configurator:

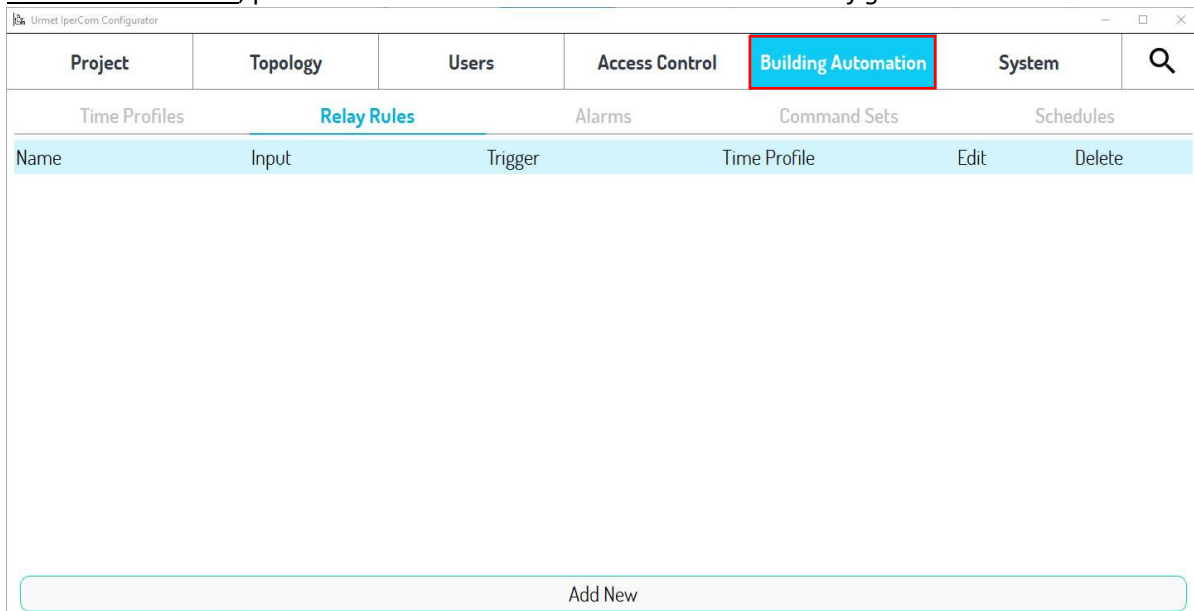


Figure 294: "Automation" tab for linking input events to outputs

The following summary table groups the possible events according to the source (device) or type of event itself:

<i>DEVICE/EVENT TYPE</i>	<i>EVENTS</i>
<i>Entry panel (1060/33-34-71-74-75-78)</i>	Outgoing call, auto-on, door opening, gate opening.
<i>Entry panel (1060/21)</i>	Outgoing call, auto-on, user recognition, door opening, gate opening,
<i>Private Call Module (1060/22)</i>	Outgoing call, auto-on.
<i>Call Module (1060/12-13-17-18-23)</i>	Outgoing call, auto-on, tamper alarm, coercion alarm, code activation, user recognition, door opening, gate opening.
<i>Modular Calling Station with 1060/48</i>	Outgoing call, auto-on, coercion alarm, code activation, user recognition, door opening, gate opening.
<i>Key Reader</i>	Tamper alarm, user recognition, door opening.
<i>Topological events</i>	Door opening, gate opening, incoming call, user activation - MAX, user activation - apartment station T1, user activation - apartment station T2, lift up, lift down, panic alarm.
<i>Automation events</i>	ON, OFF, short press, long press (on <i>Relay Actuator</i> inputs).

*Table 10: Sources and related events associated with relay outputs*

We will now explain how to build the activation rules in the cases listed above in detail.

7.1.5.1 Activation for events on Entry panel 1060/33-34-71-74-75-78

The "Add" button, at the bottom of the configuration page of *Entry Panel*, allows creating one or more activation rules, as shown below.

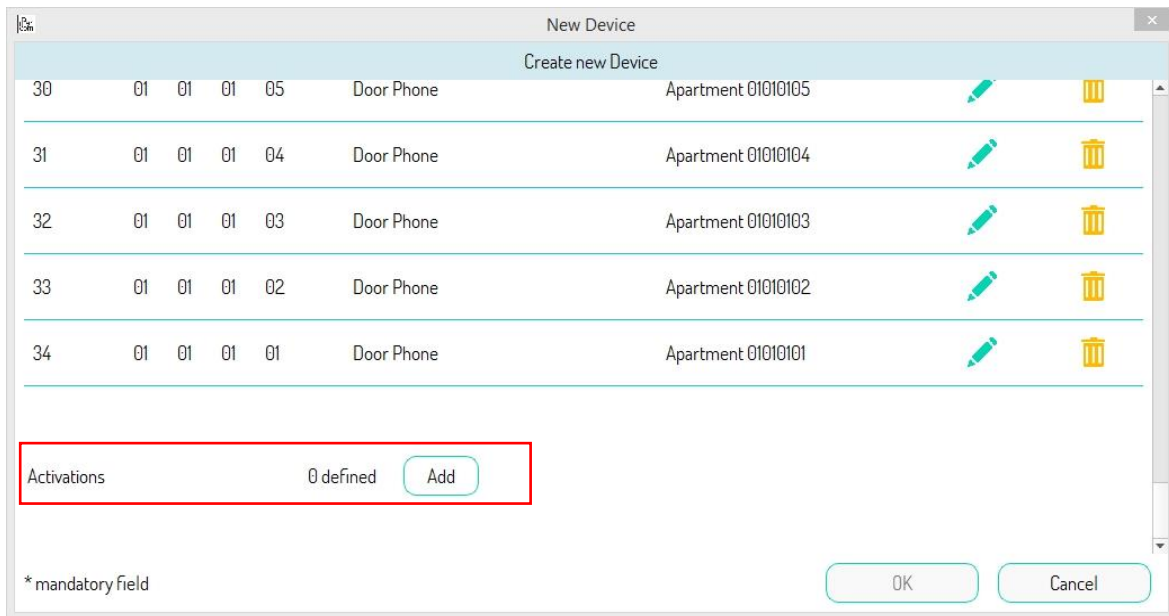


Figure 295: addition of an activation rule

Press this button to open a screen containing the list of activation rules already set, if any. If the device has just been added to the configuration or no rule has been set yet, this list will be empty, as shown in the figure:

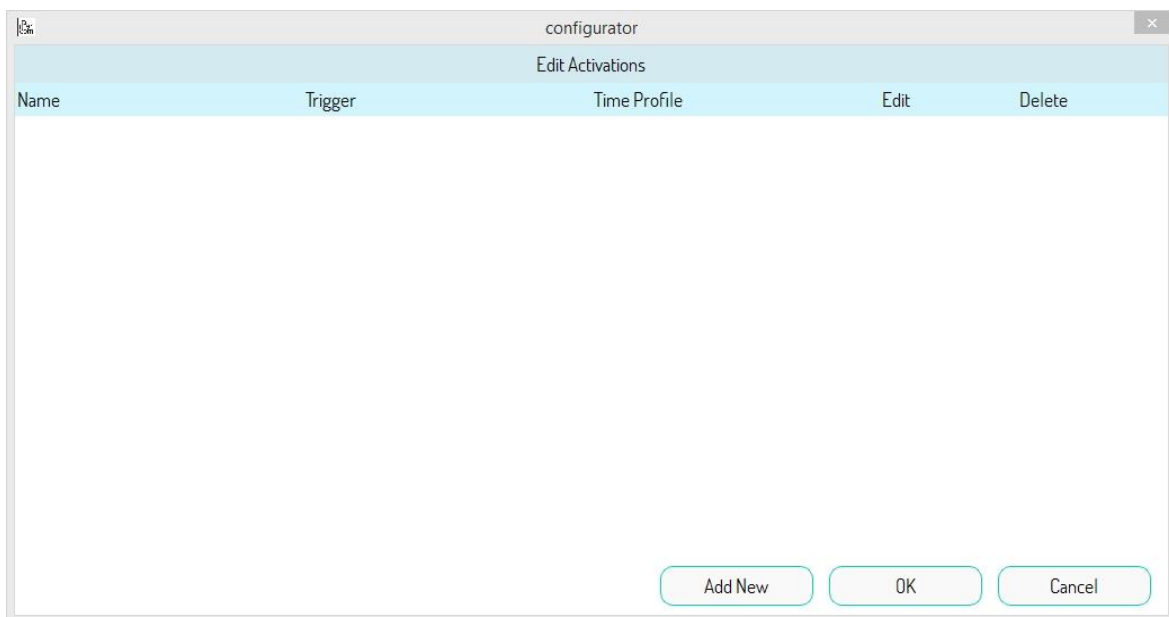


Figure 296: list of activations

To create a new activation, press the "Add New" button.

The following screen opens in which you can set all the parameters needed to build the activation rule:

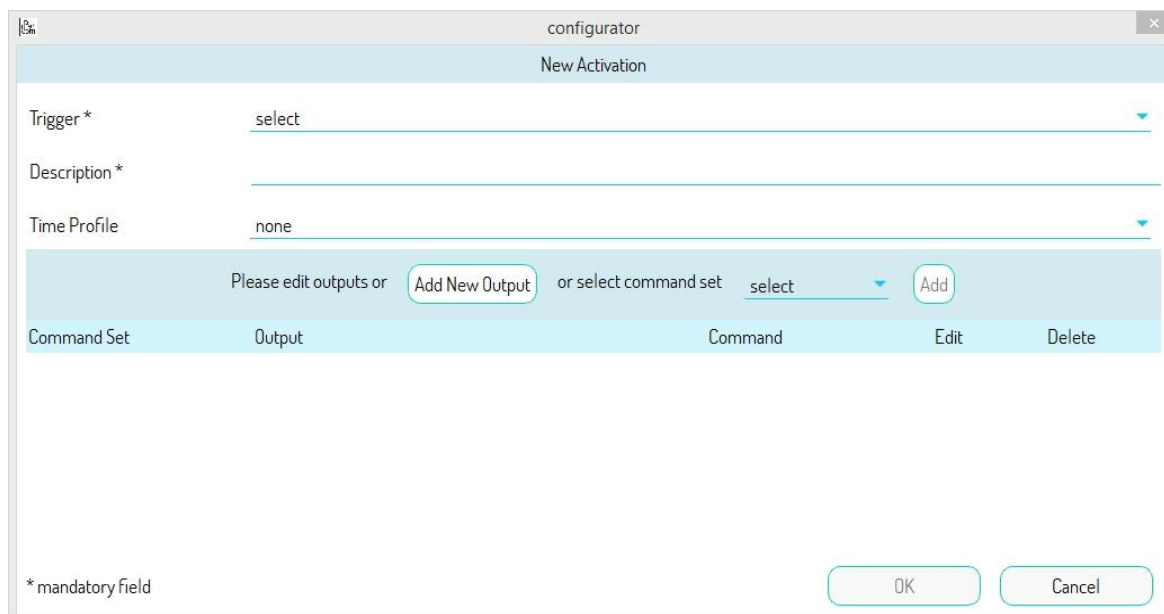


Figure 297: Screen for creating an activation with event on Entry Panel

The "Trigger" drop-down menu can be used to select the event to be associated with one or more outputs of the *Relay Actuators*. Possible events are:

- "Outgoing Call", i.e., call from the *Door Speaker Unit*.
- "Auto-on", i.e., connection from the *video door phone* to the camera of the *Entry Panel*.
- "Door opening", i.e., opening the pedestrian door of the *Entry panel*,
- "Gate opening", i.e., opening the gate/driveway of the *Entry panel*,

as shown on the respective screen:

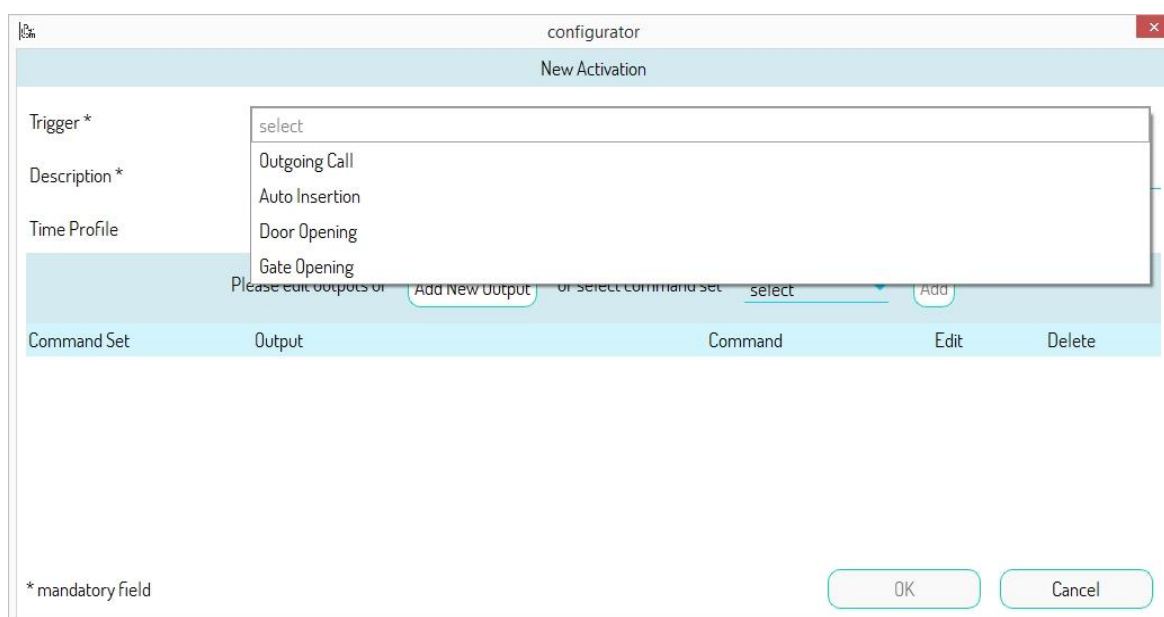


Figure 298: List of events on Entry Panel

The "*Description*" field can be used to give a meaningful name to the activation you are creating.

The "*Time Profile*" drop-down menu can be used to associate a previously created time profile with the activation rule. In this way, the rule will only be active within the selected time profile.

For example, having selected the auto-on event and given a meaningful name to the activation, the screen that appears is as follows:

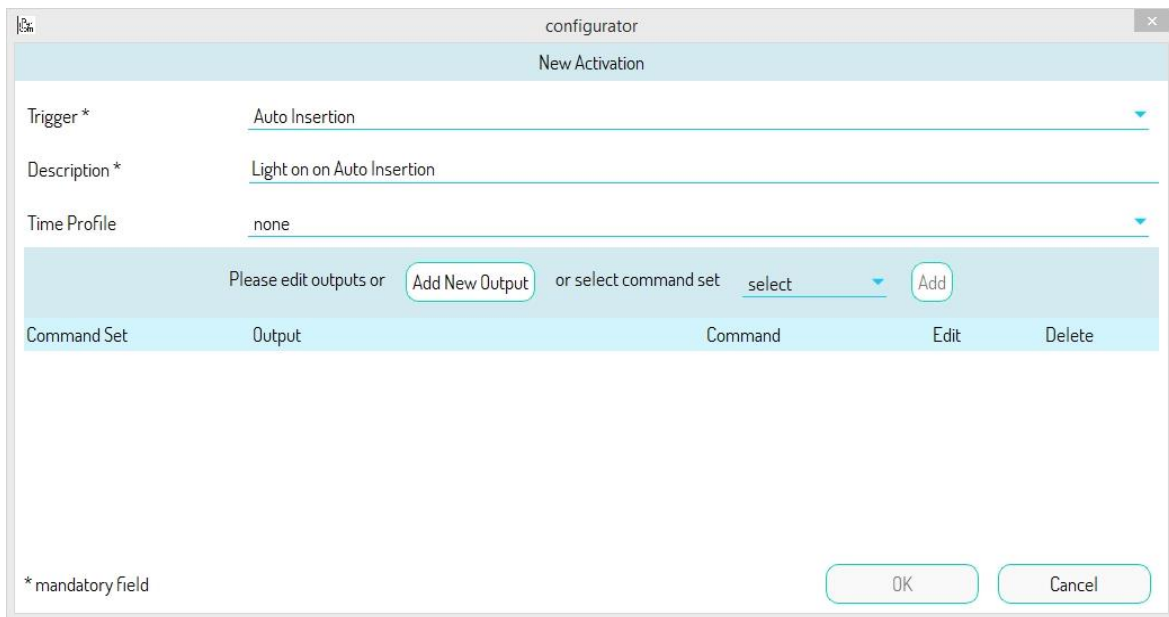


Figure 299: Partial activation creation

The "*Add a New Output*" button can be used to add one or more outputs to the activation. On the new screen that appears, go to the topological node of the *Relay Actuator*, select the desired device, then choose the output and set the respective command.

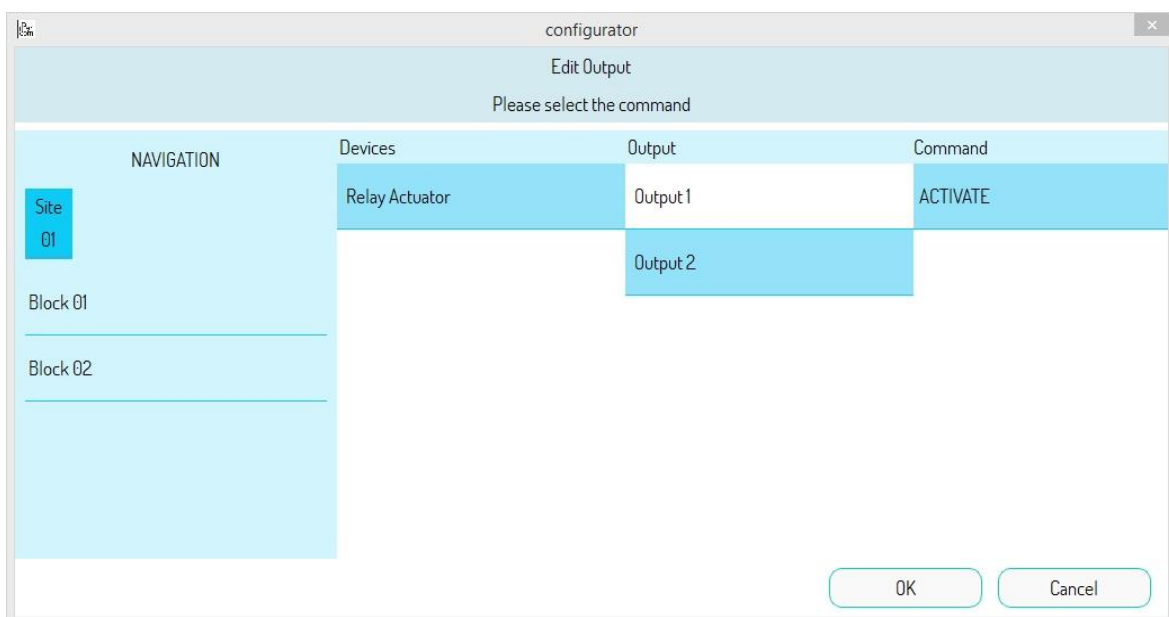


Figure 300: Selection of the desired device output

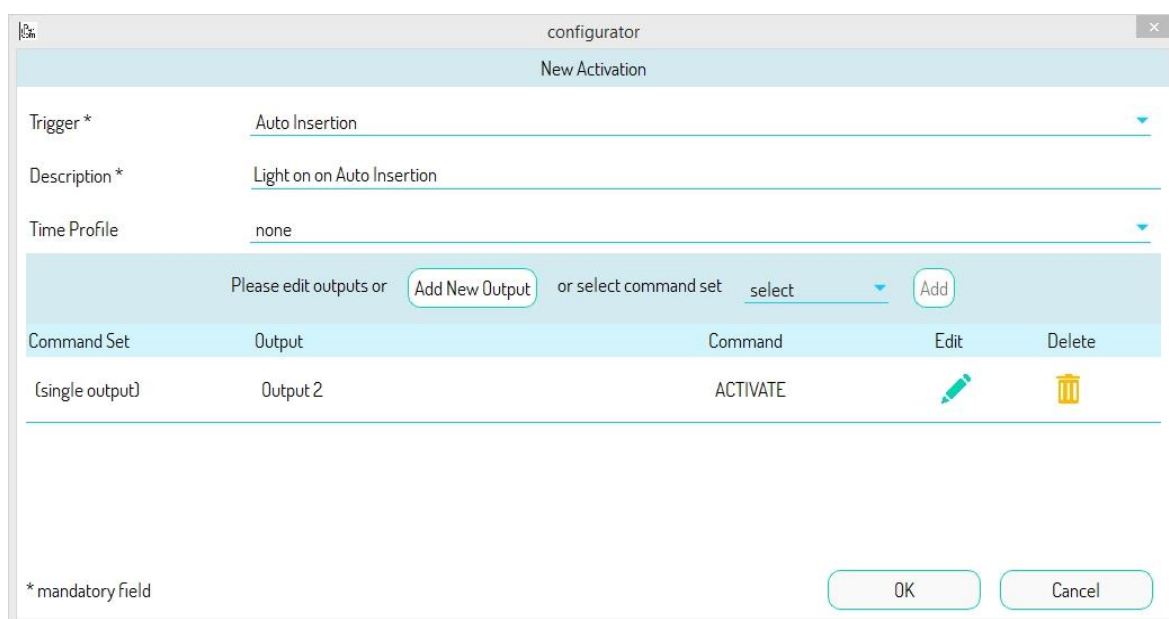


The available commands depend on how the output has been configured, i.e. monostable or bistable. In case of monostable output, only the "ACTIVATE" and "DISACTIVATE" commands are available. In the other case, the available commands are "ON", "OFF" and "SWITCH". For more details, see [APPENDIX A: Configuration parameters of IPerCom devices](#).



The "DISACTIVATE" command in monostable mode is present only on the Relay Actuator 1060/84 v. 4.05 starting from version 2.1.0 of IPerCom.

Press the "OK" button to add the set output as shown below:





Command Set	Output	Command	Edit	Delete
(single output)	Output 2	ACTIVATE		

Figure 301: List of outputs associated with the activation rule

Different outputs can be associated with the same event by pressing "Add New Output" and repeating the steps shown above. Since these are single outputs, the "Scenario" item will appear in brackets in the "Group Name" column. It is possible to add groups of previously commands created using the "Automation" function on the "Command Sets" tab (see dedicated paragraph [Creating a scenario](#)). In this case, the "Scenario" column shows the name given to the previously created group of commands.

Once configuration of the activation rule is finished, press the "OK" button to end the rule creation procedure.

The list of activation rules shown will contain the new created activation.

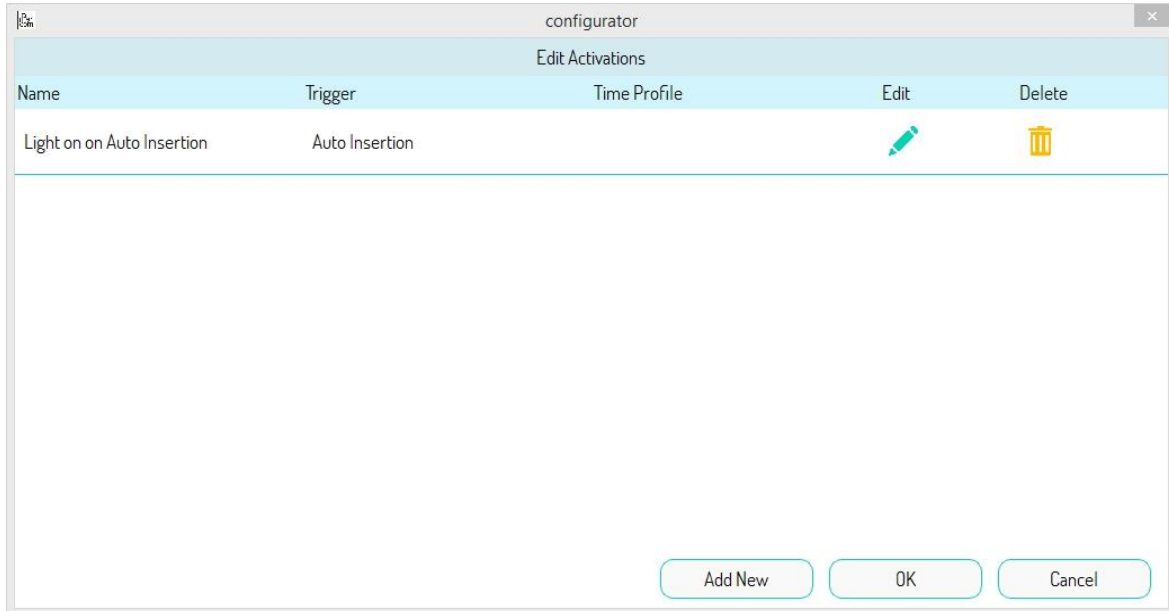


Figure 302: Activation table with the newly created element

The second output of the *Relay Actuator* is automatically activated in monostable mode every time an auto-on is performed in the entry panel.

In any case it is possible to modify or delete the newly created activation using the "Edit" or "Delete" buttons, or create new ones using the "Add" button.

Press the "OK" button, instead, for a summary of the number of rules created:



Figure 303: summary number of activations created

### 7.1.5.2 Activation for events on Entry panel 1060/21

The "Add" button, at the bottom of the configuration page of *Entry panel 1060/21*, allows you to create one or more activation rules, as shown below:

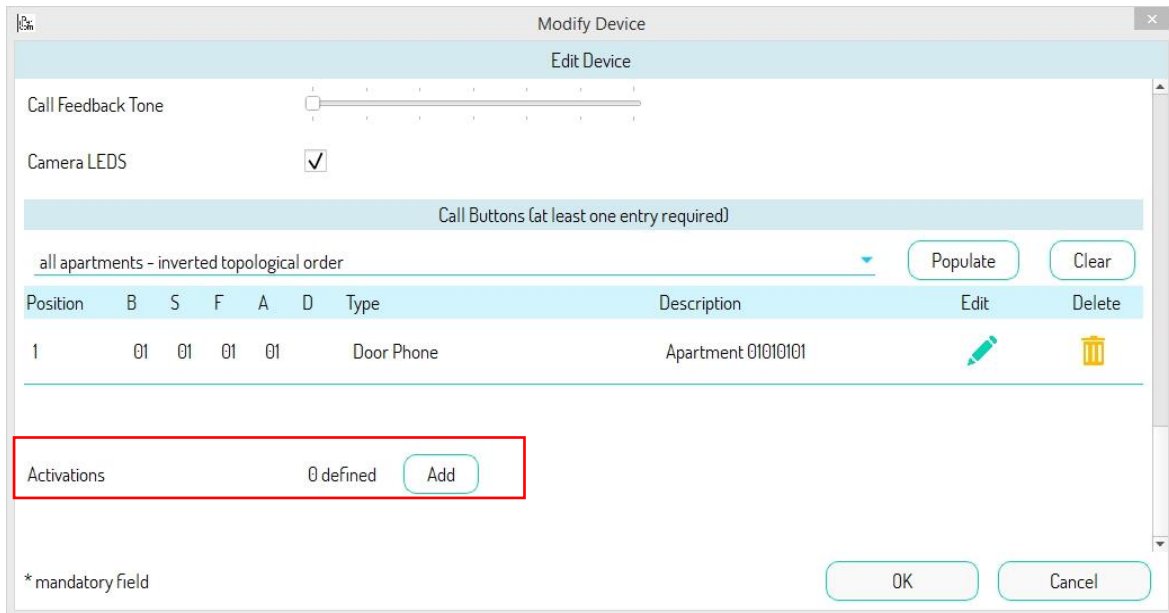


Figure 304: addition of an activation rule

Press this button to open a screen containing the list of activation rules already set, if any. If the device has just been added to the configuration or no rule has been set yet, this list will be empty, as shown in the figure:

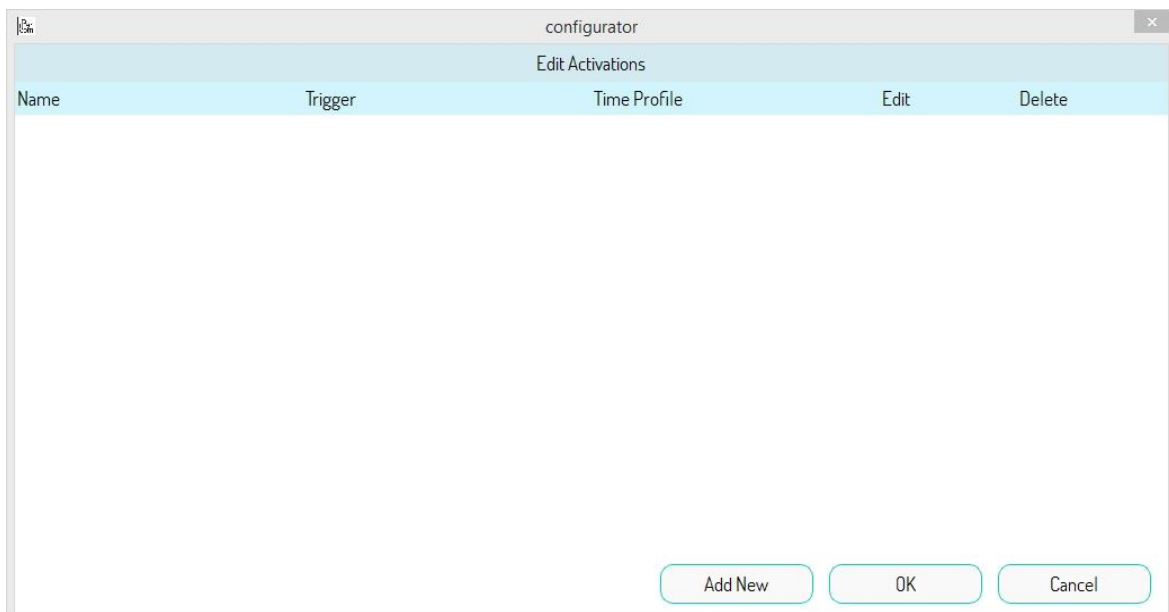
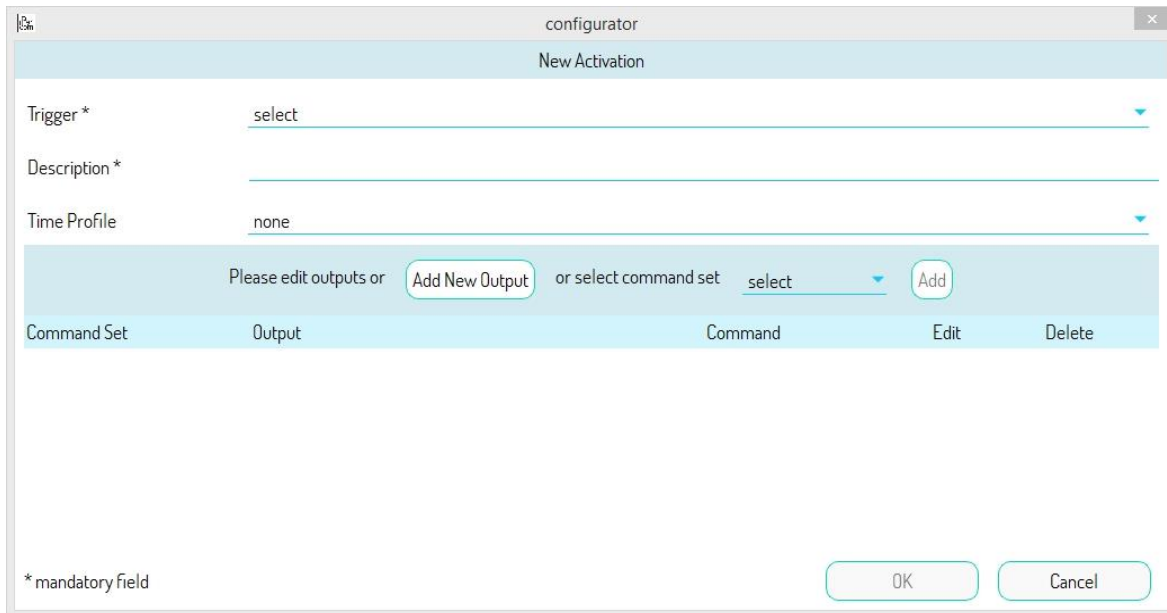


Figure 305: list of activations

To create a new activation, press the "Add" button.

The same screen as for the creation of activations with event on *Entry panel 1060/71-74-75-78* opens, where it is possible to set all the parameters necessary to create the activation rule:



The screenshot shows a window titled "configurator" with a sub-window "New Activation".

Fields and options:

- Trigger \*: select
- Description \*
- Time Profile: none
- Below the Time Profile field, there is a light blue bar containing: "Please edit outputs or **Add New Output** or select command set select **Add**".
- Below this bar is a table with columns: Command Set, Output, Command, Edit, Delete.
- At the bottom left, there is a note: "\* mandatory field".
- At the bottom right, there are "OK" and "Cancel" buttons.

Figure 306: screen for creating an event activation

The “*Event*” drop-down menu allows selecting the event to be associated to one or more *Relay Actuator* outputs. The possible events on *Entry panel 1060/21* are:

- “*Outgoing Call*”, i.e. call from the *Entry Panel*;
- “*Auto-on*”, i.e. connection from the *video door phone* to the camera of the *Entry Panel*;
- “*User Recognition*”, i.e. passing a proximity key or door opener code associated with a user (resident or non-resident);
- “*Door opening*”, i.e. opening the pedestrian door of the *Entry panel*,
- “*Gate opening*”, i.e. opening the gate/driveway of the *Entry panel*,

as shown in the relevant screen:

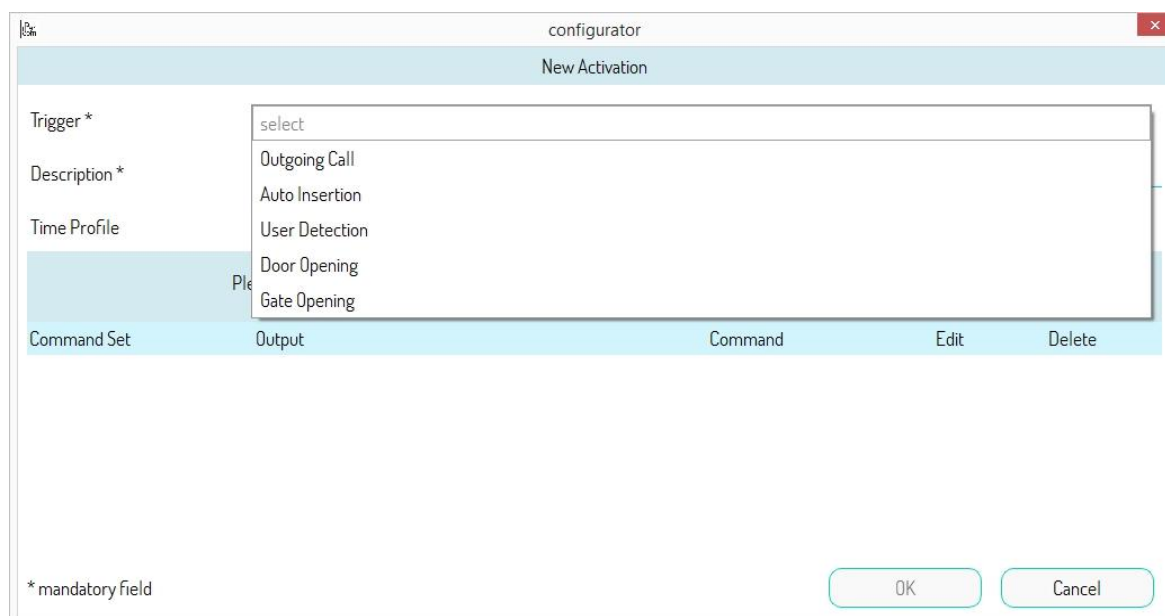


Figure 307: events list on Entry Panel 1060/21

The creation of the activation rule is carried out in the same way as seen for the *Entry panels*.

### 7.1.5.3 User recognition event

The user recognition event allows you to activate one or more *Relay Actuator* outputs after:

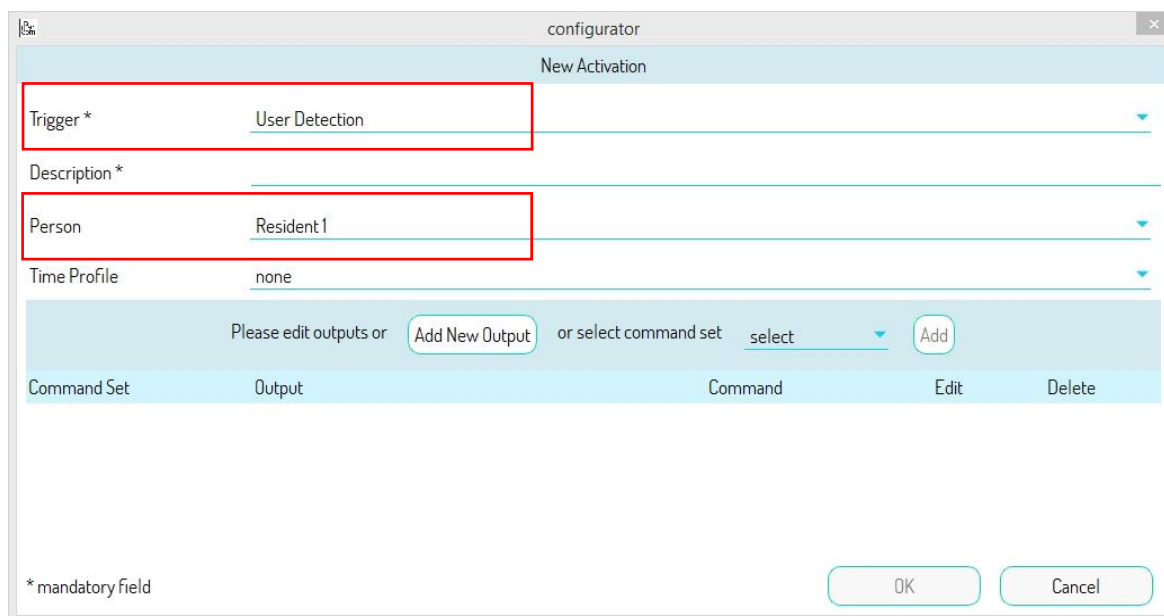
- passing a valid proximity key of a resident or non-resident;
- entering a valid door opener code of a resident or non-resident.

This function is available on the following devices:

- *Entry panel 1060/21* (passing a valid proximity key),
- *Call Module* (passing a valid proximity key or entering a valid door opener code),
- *Modular Entry Panel with 1060/48* (passing a valid proximity key or entering a valid door opener code),
- *Key Readers 1060/45* (passing a valid proximity key),
- *Key Readers 1060/86* (passing a valid proximity key).

In this way, for example, when a valid key is passed on a *Key Reader* at the entrance of a building basement, it is possible to automatically open a garage up-and-over door or switch on the basement lights.

Once the "User Recognition" event has been chosen, the "Person" drop-down menu is displayed in the activation rule construction screen, which allows you to select the resident or non-resident whose proximity key and/or door opener code activates one or more *Relay Actuator* outputs, as shown in the screen below:



The screenshot shows a window titled 'configurator' with a 'New Activation' tab. The 'Trigger' dropdown menu is set to 'User Detection' and is highlighted with a red box. Below it is a 'Description' field. The 'Person' dropdown menu is set to 'Resident 1' and is also highlighted with a red box. Below the 'Person' dropdown is a 'Time Profile' dropdown set to 'none'. A section below these fields contains the text 'Please edit outputs or' followed by an 'Add New Output' button, 'or select command set' followed by a 'select' dropdown and an 'Add' button. Below this is a table with columns 'Command Set', 'Command', 'Edit', and 'Delete'. The 'Command Set' dropdown is set to 'Output'. At the bottom of the window are 'OK' and 'Cancel' buttons. A note at the bottom left states '\* mandatory field'.

Figure 308: user choice if the selected event is User Recognition

The key and door opener codes are defined during the creation of the resident or non-resident (for further details see paragraph [User management](#)).

#### 7.1.5.4 Activation for events on Floor Entry panel 1060/22

The "Add" button, at the bottom of the configuration page of *Floor Entry panel 1060/22*, allows you to create one or more activation rules, as shown below:

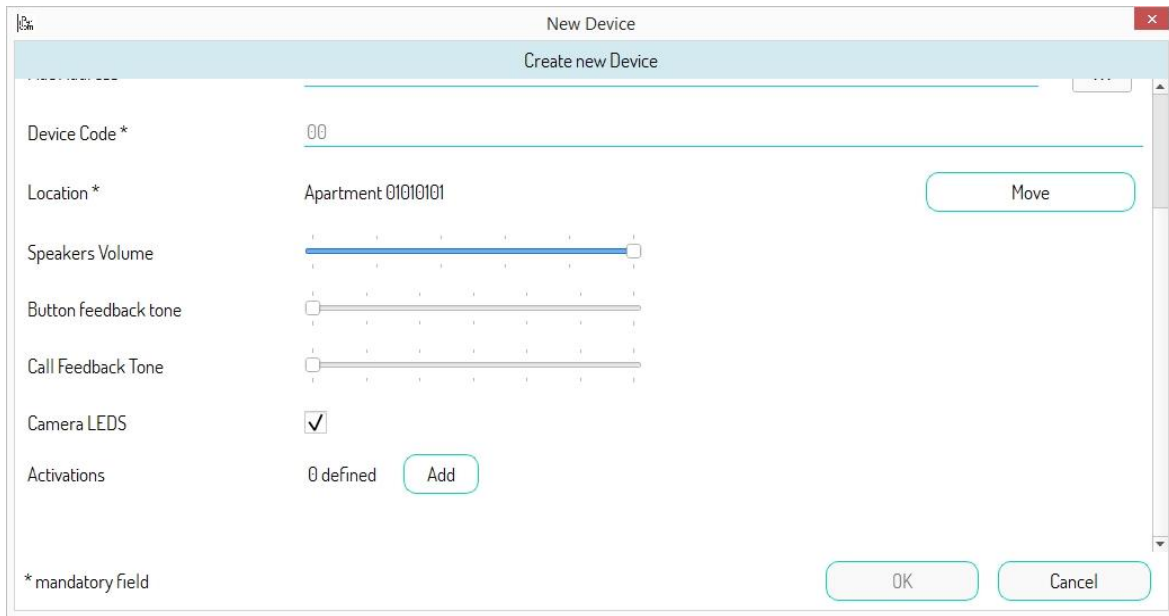


Figure 309: addition of an activation rule

Press this button to open a screen containing the list of activation rules already set, if any. If the device has just been added to the configuration or no rule has been set yet, this list will be empty, as shown in the figure:

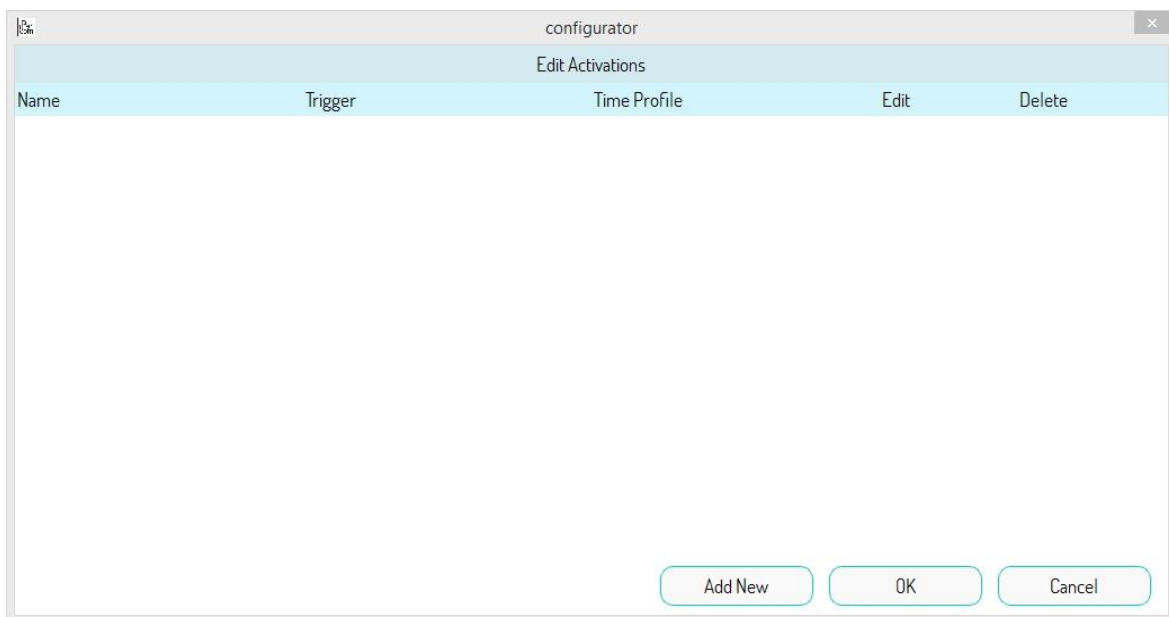


Figure 310: list of activations

To create a new activation, press the "Add New" button.

The same screen as for the creation of activations with event on *Entry panel 1060/33-34-71-74-75-78* opens, where it is possible to set all the parameters necessary to create the activation rule:

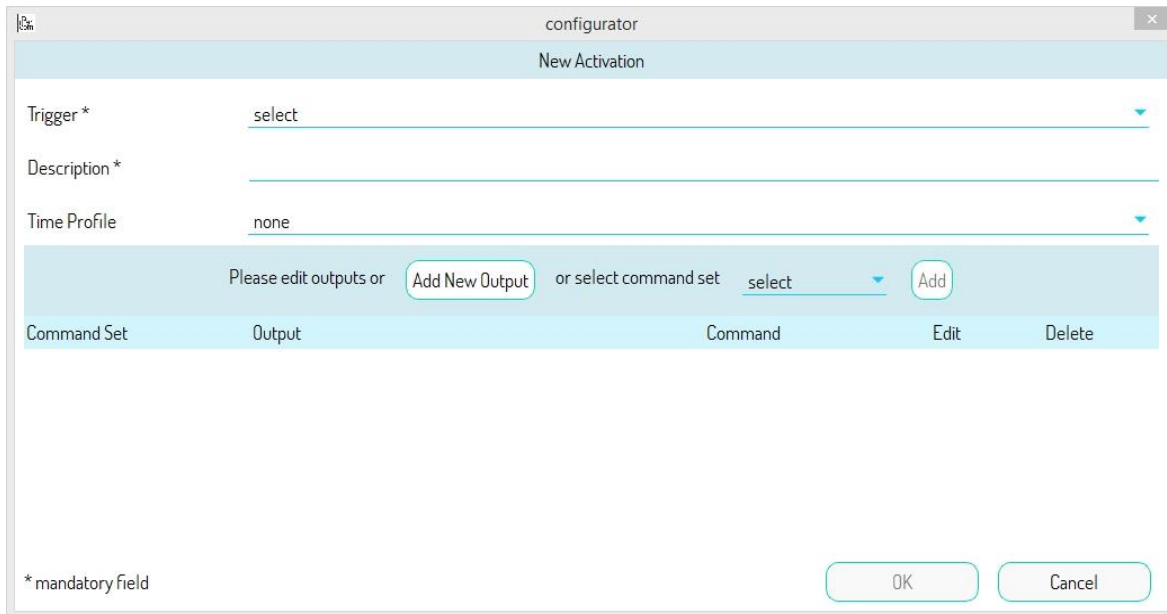


Figure 311: screen for creating an event activation

The “Event” drop-down menu allows selecting the event to be associated to one or more *Relay Actuator* outputs. The possible events are:

- “Outgoing Call”, i.e., call from the *Floor Entry Panel*;
- “Auto-on”, i.e., connection from the *video door phone* to the camera of the *Floor Entry Panel*;

as shown in the relevant screen:

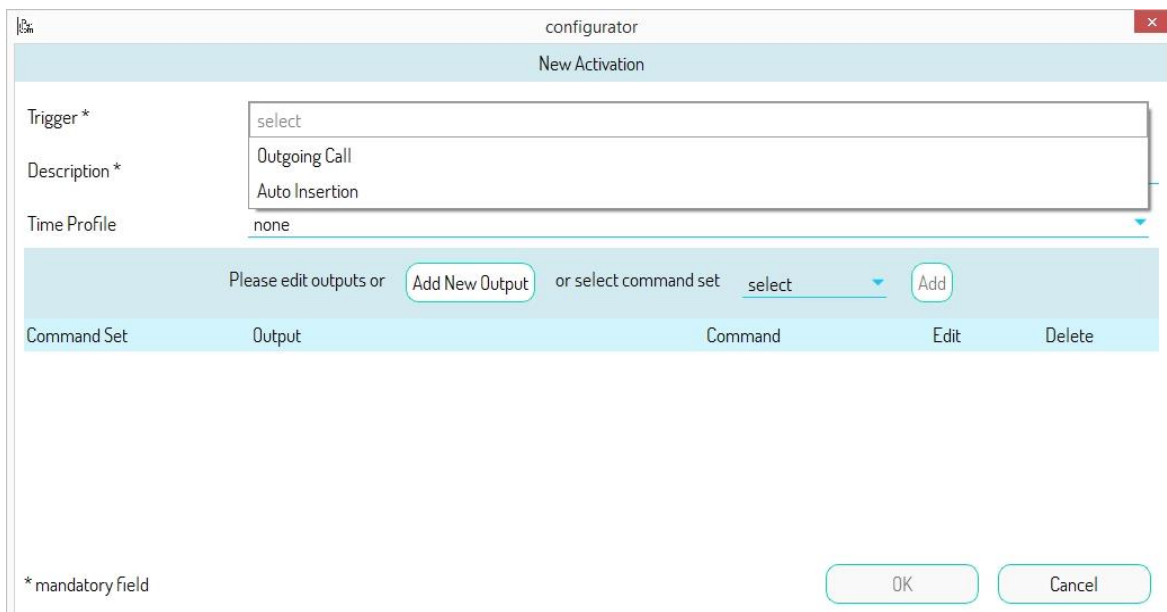


Figure 312: events list on Floor Entry Panel 1060/22

The creation of the activation rule is carried out in the same way as seen for the *Entry panels*.



### 7.1.5.5 Activation for events on Call Module

The "Add" button, at the bottom of the configuration page of *Call Module*, allows you to create one or more activation rules, as shown below.

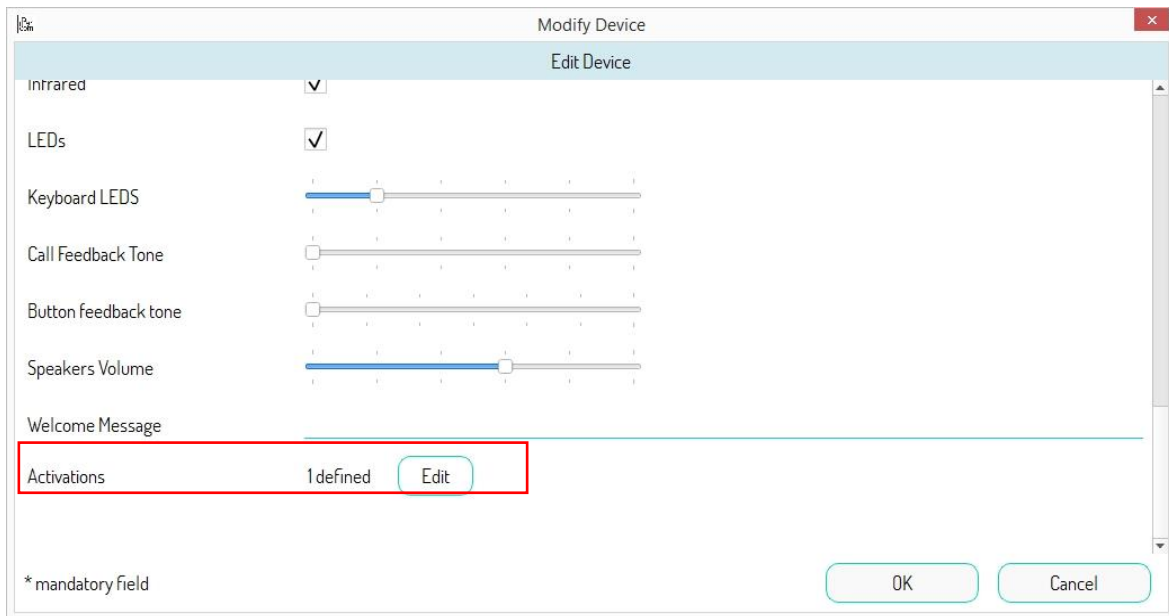


Figure 313: addition of an activation rule

Press this button to open a screen containing the list of activation rules already set, if any. If the device has just been added to the configuration or no rule has been set yet, this list will be empty, as shown in the figure:

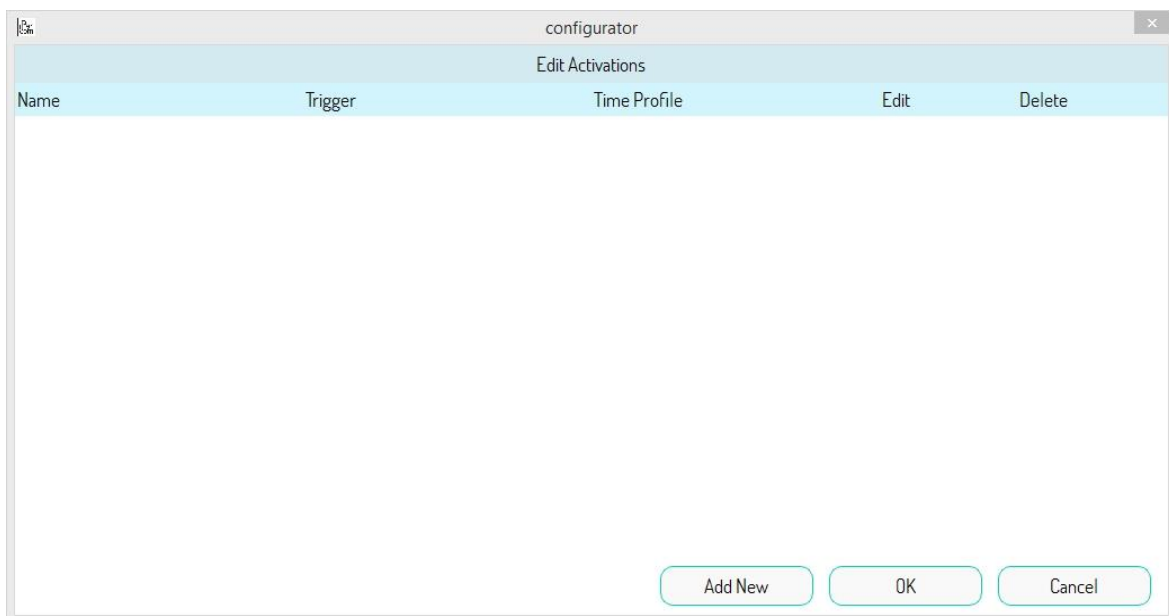


Figure 314: list of activations

To create a new activation, press the "Add" button.

The same screen as for the creation of activations with event on *Entry panel 1060/71-74-75-78* opens, where it is possible to set all the parameters necessary to create the activation rule:

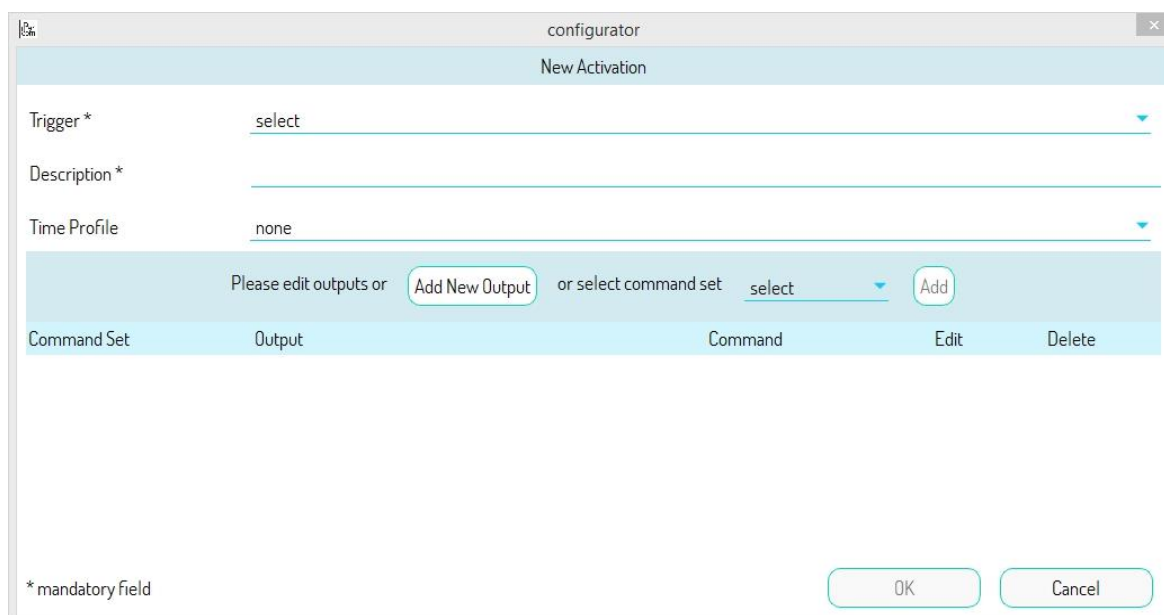


Figure 315: screen for creating an event activation

The “Event” drop-down menu allows selecting the event to be associated to one or more *Relay Actuator* outputs. The possible events on *Call Module* are:

- “Outgoing Call”, i.e., call from the *Call Module* to the *video door phone*, *Audio Door Phone* or *Switchboard*,
- “Auto-on”, i.e., connection from the *video door phone* on the camera of the *Call Module*,
- “Sabotage alarm”, which means attempted tampering with the *Call Modules*,
- “Duress Alarm”, i.e., an attempt to insert a forced key code on a *Call Module* (key code increased by 1),
- “Code activation”, i.e., entry on the *Call Module* of a numerical code between 4 and 8 digits (the entry is made by entering “0” and “X” in sequence), as shown on the respective screen:
- “User Recognition”, i.e., passing a proximity key or door opener code associated with a resident or non-resident;
- “Door opening”, activation of the relay associated with the pedestrian crossing;
- “Gate opening”, activation of the relay associated with the driveway.

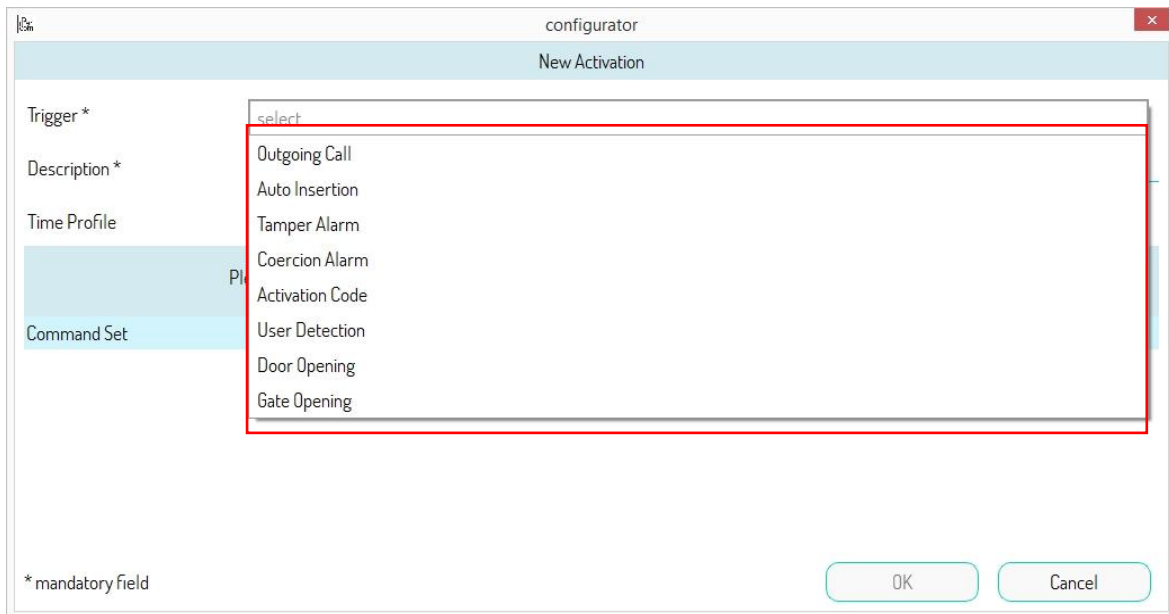


Figure 316: Event list on Call Module

The activation rule is created in the same way as for the *Entry Panels*.



*In the "Code activation" event, the code is entered in the "Code" field in the relevant screen.*

### 7.1.5.6 Activation for events on Entry Panel with 1060/48

The "Add" button, at the bottom of the configuration page of *Modular Entry Panel with 1060/48*, allows you to create one or more activation rules, as shown below:

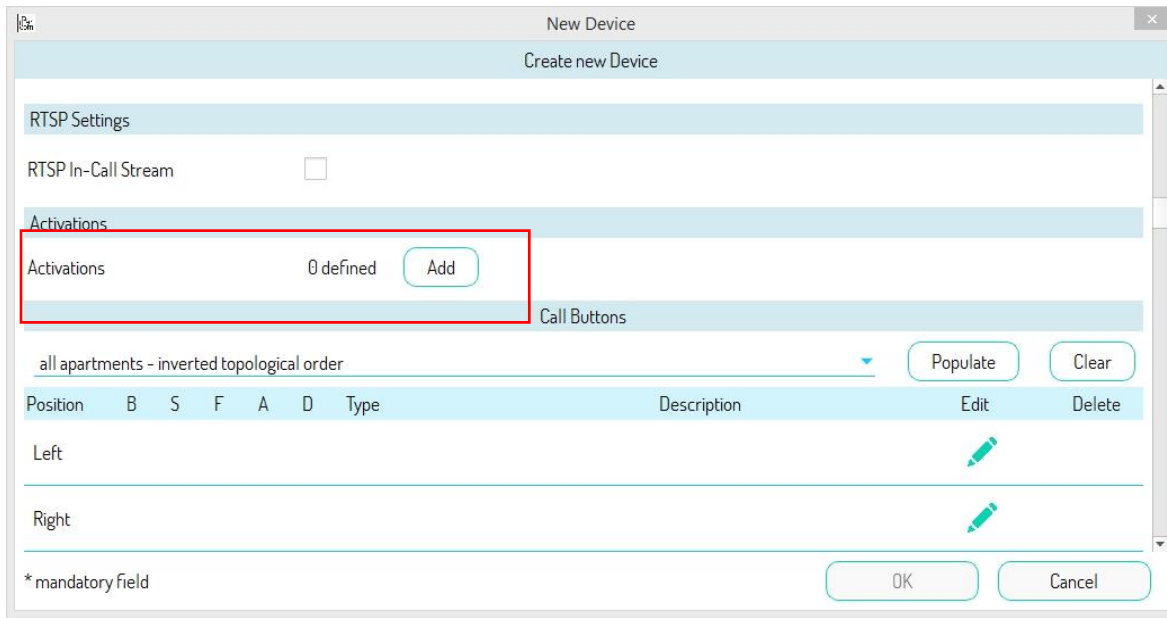


Figure 317: addition of an activation rule

The creation of the activation rule takes place as already described for the *Call Module* with the only difference that the tamper alarm is not present in the list of possible events.

### 7.1.5.7 Key Reader activations

The "Add" button, at the bottom of the configuration page of *Key Reader*, allows you to create one or more activation rules, as shown below:

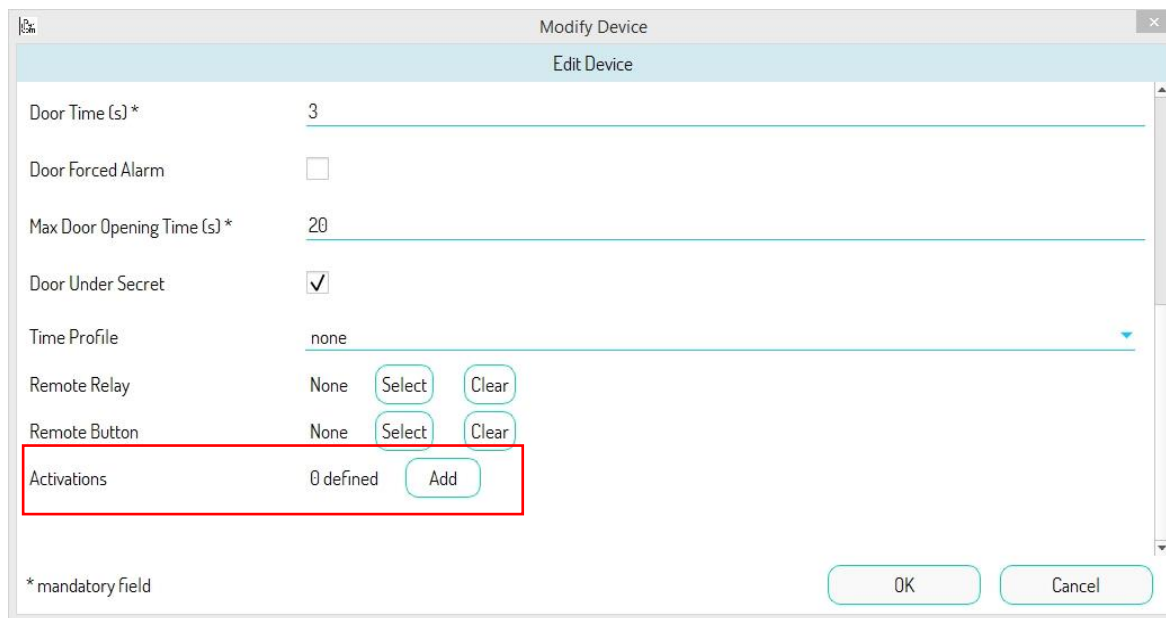


Figure 318: "Activations" button for Key Readers

Press this button to open a screen containing the list of activation rules already set, if any. If the device has just been added to the configuration or no rule has been set yet, this list will be empty, as shown in the figure:

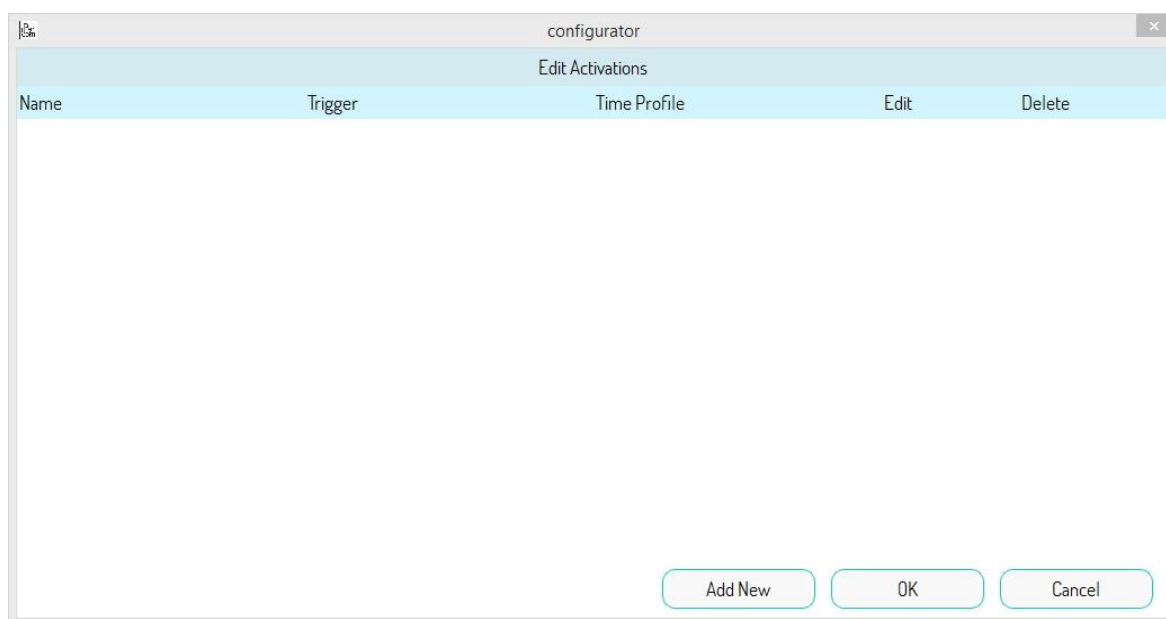


Figure 319: "Activations Tables"

To create a new activation, press the "Add New" button.

The same screen as for the creation of activations with event on *Entry panel 1060/71-74-75-78* opens, where it is possible to set all the parameters necessary to create the activation rule:

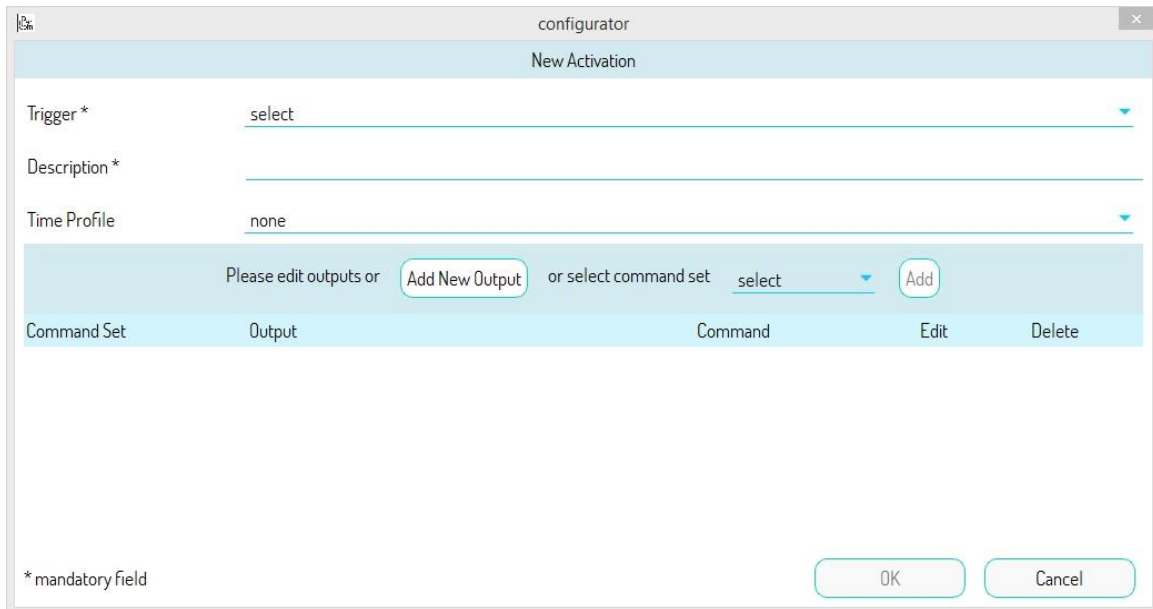


Figure 320: Screen for creating an activation with event on Key Reader

The “*Event*” drop-down menu allows selecting the event to be associated to one or more *Relay Actuator* outputs. The possible events on *Key Reader* are:

- “*Tamper Alarm*”, i.e. attempt of tampering with the *Call Modules*,
- “*User Recognition*”, i.e. passing a proximity key or door opener code associated with a resident or non-resident;
- “*Door Opening*”, i.e. actuation of the relay associated with the pedestrian passageway;

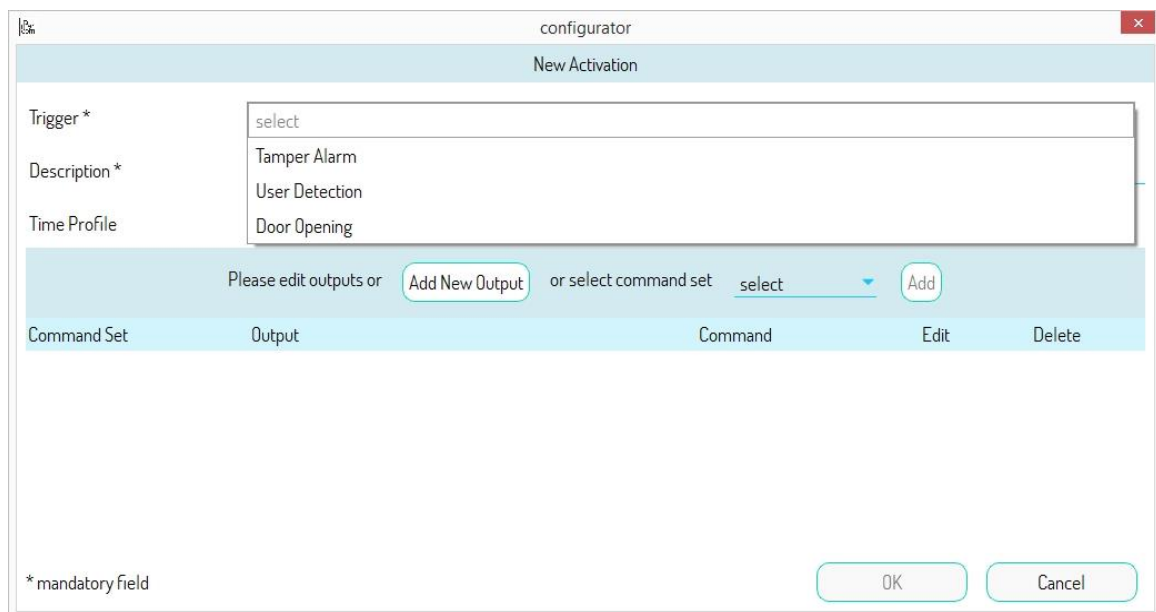


Figure 321: list of events on Key Reader

The creation of the activation rule is carried out in the same way as seen for the *Entry panels*.

### 7.1.5.8 Activations for topological events

To associate a topological event to one or more outputs of a *Relay Actuator*, *Lift Interface*, or gate of a calling station it is necessary to click on the “Topology” tab and then on the “Activations” tab.

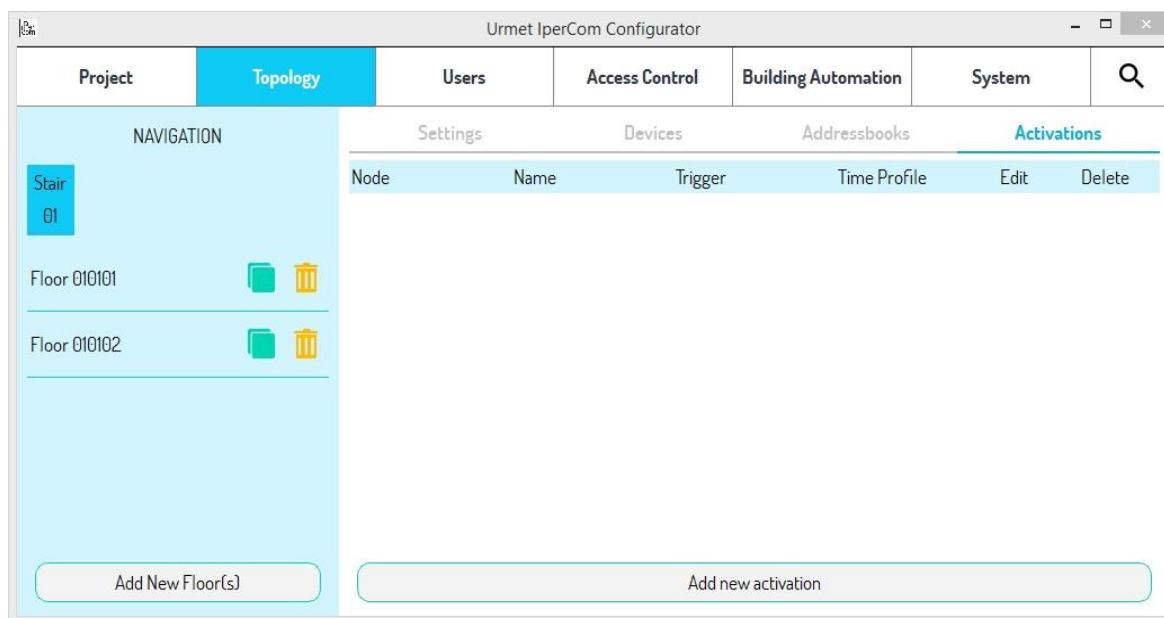


Figure 322: “Activations” screen

In the provided example, the created topology includes one stair with 2 floors and 1 apartment on each floor.

In this example, we will assume a *Relay Actuator* positioned on the stairs configured to have two monostable outputs (see [APPENDIX A: Configuration parameters of IPerCom devices](#))

The activation rule can be set at a specific topological point of the system, i.e. on site, block, staircase, floor or apartment level. This means that the activation will be propagated to all the apartments (generally on all nodes) contained in the topological group of the node on which the rule is created. If the activation has been set on an apartment, it will only apply to that single apartment.

In the case of the figure above, the activation rule will be set to “Stair 01” (since you have selected that topological node in the navigation module) and then it will be applied to both apartments.



*The propagation of the activation rule does not depend on the topological position of the Lift Interface or Relay Actuators or calling stations in the system but only on the topological group of the node where the rule is created.*

To create the activation rule, press the "Add New Activation" button on the "Activations" screen. The same view screen opens for creating of activations with event on *Entry Panel* that can be used to set all the parameters needed to build the activation rule.

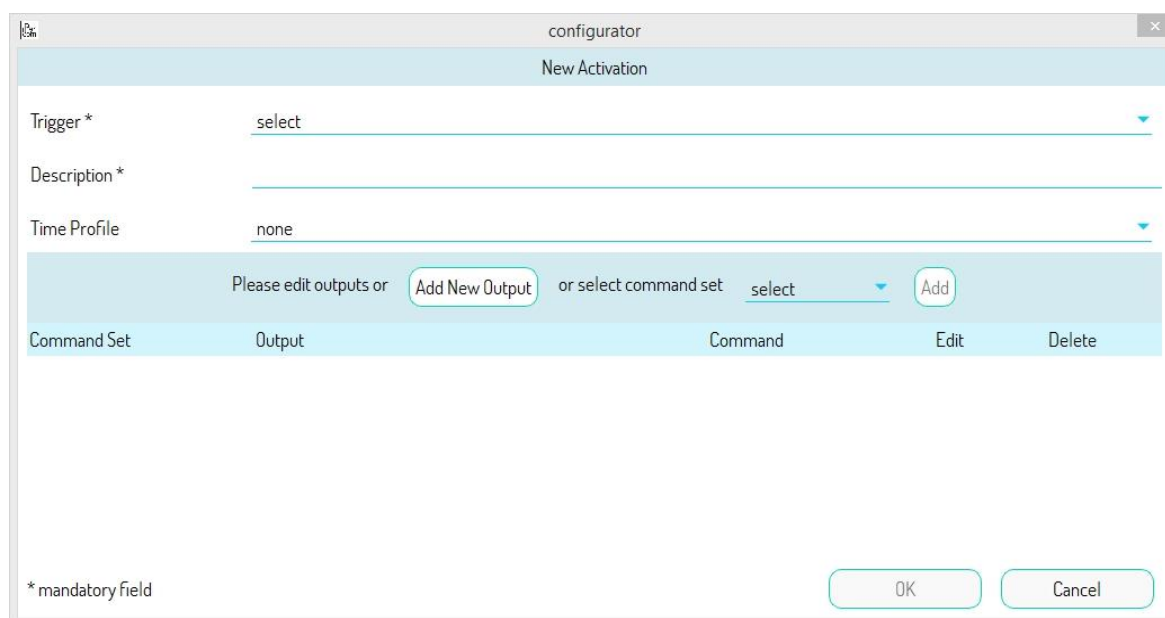


Figure 323: Screen for creating an activation with a topological event

The "Event" drop-down menu allows you to select the event to be associated to one or more *Relay Actuator* or *Lift interface outputs*.

The possible topological events for the *Relay Actuator* device are

- "Door Opening", i.e., an event caused by pressing the door opening button (generic or a specific door) on the apartment station;
- "Gate Opening", i.e., an event caused by pressing the gate opening button (generic or a specific gate) on the apartment station;
- "Incoming Call", i.e., incoming call event on the apartment station;
- "User Activation", i.e., event generated by the user via *MAX*, *VOG<sup>7</sup>*, *VOG<sup>5+</sup>*, *Basic* or *VOG<sup>5</sup>* video door phones or *Miro* door phone;
- "Lift Up" and "Lift Down" (lift function), events enabled only on stair, floor, and apartment nodes;
- "Panic alarm", i.e., an event triggered by pressing the panic button on the apartment station.
- "Switchboard Activation", i.e., activation rules that appear only on the *Switchboard* application.



*Switchboard activations are shown only on the Switchboard application and only if they are created on its topological path.*



The possible topological events for the *Lift Interface* device are:

- “*Lift Up and Lift Down*” (lift function), events enabled only for stair, floor, and apartment nodes;

as shown on the respective screens:

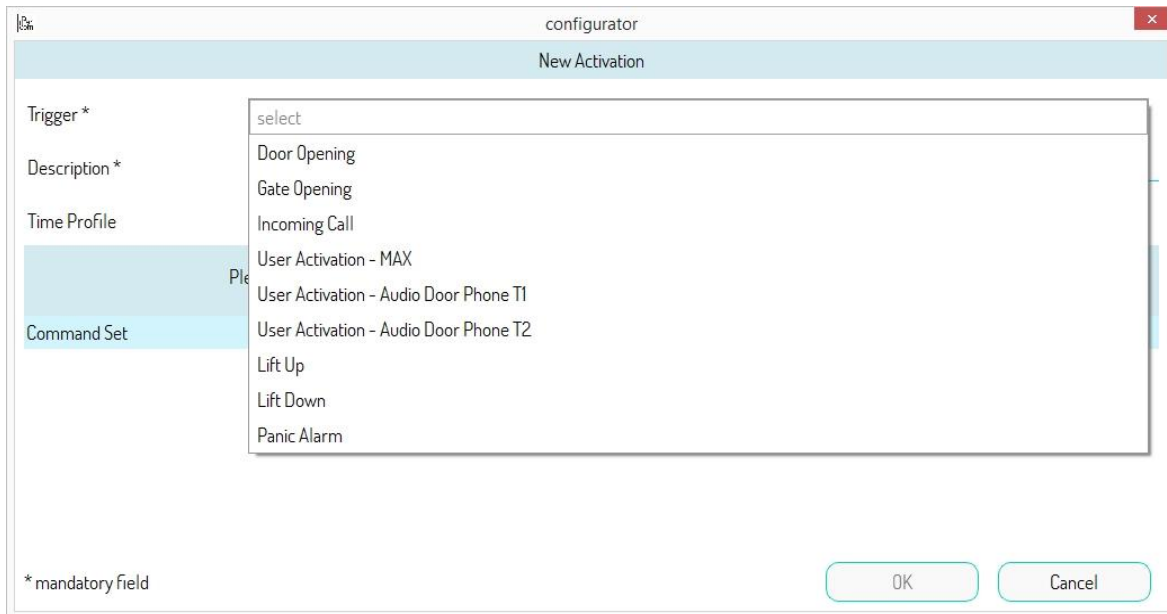


Figure 324: List of events for MAX video door phones

#### 7.1.5.8.1 Topological events for Relay Actuator

Having selected the incoming call event and given a meaningful name to the activation, the following screen will appear:

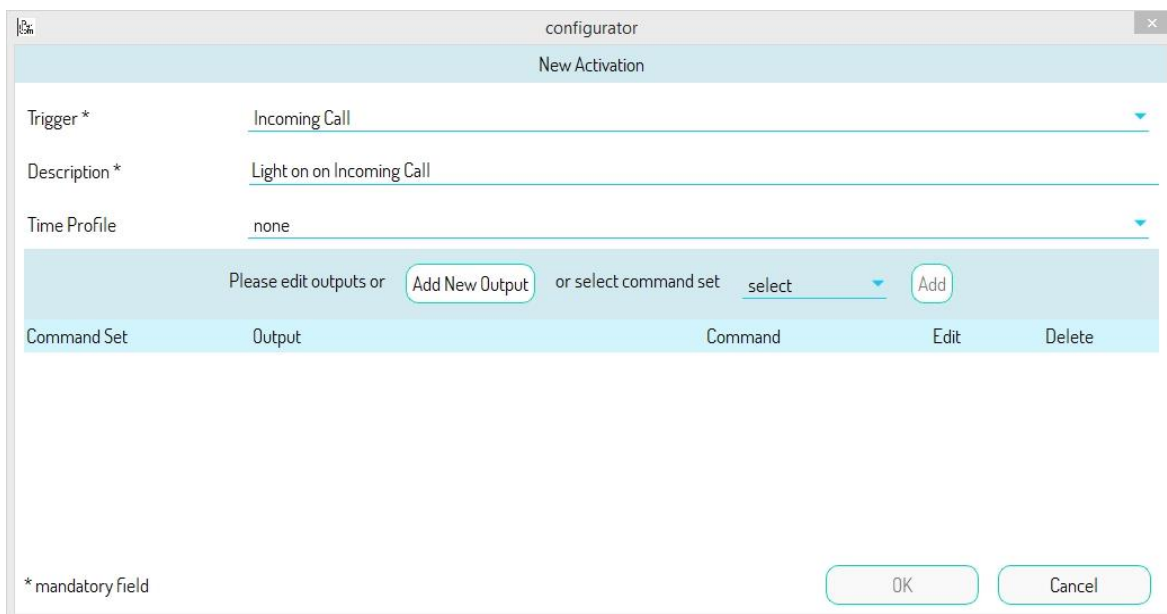


Figure 325: Description of the activation rule

To add outputs to the activation rule, proceed as described for creating activations for *Entry Panels*. For example, a screen of this type will appear:

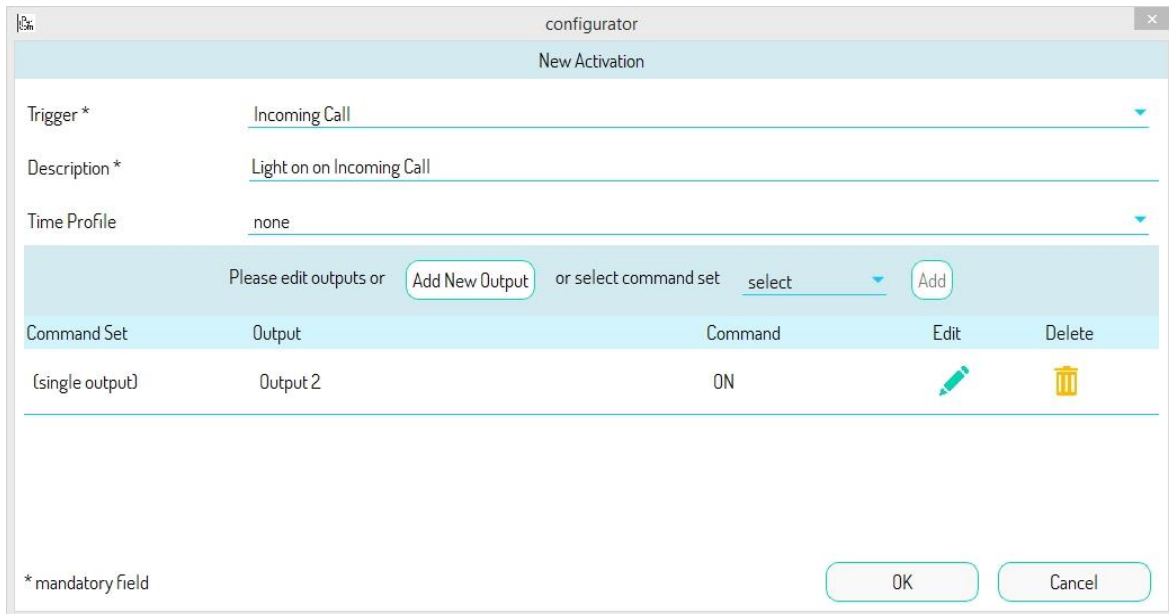


Figure 326: List of outputs associated with the activation rule

Once all the outputs have been added to the activation rule and a possible time profile has been selected, press the "OK" button to create the activation and add it to the activation list of the concerned topological node.

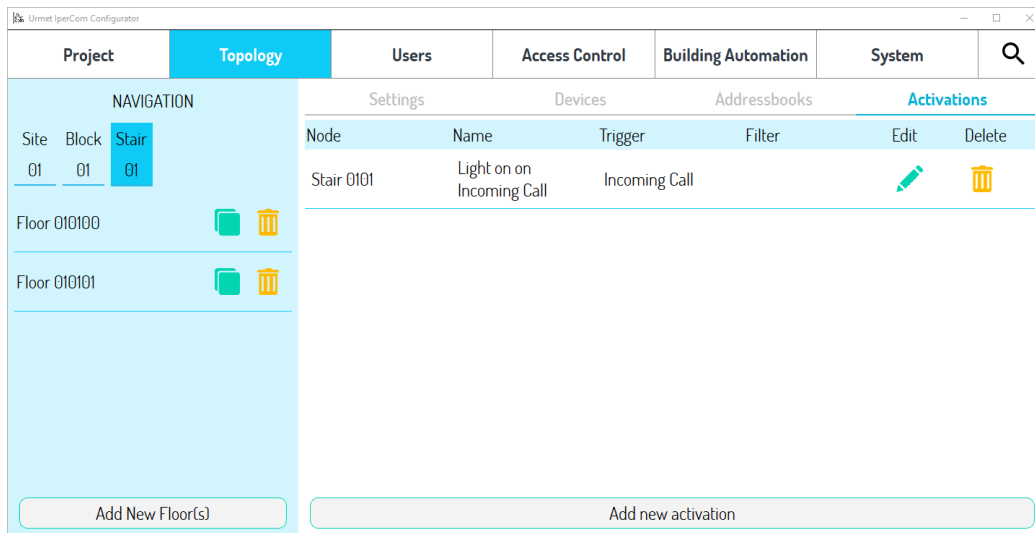


Figure 327: List of activation rules for the "Stair 01" topological node

If instead "User Activation" is chosen as the event, the following screen will appear:

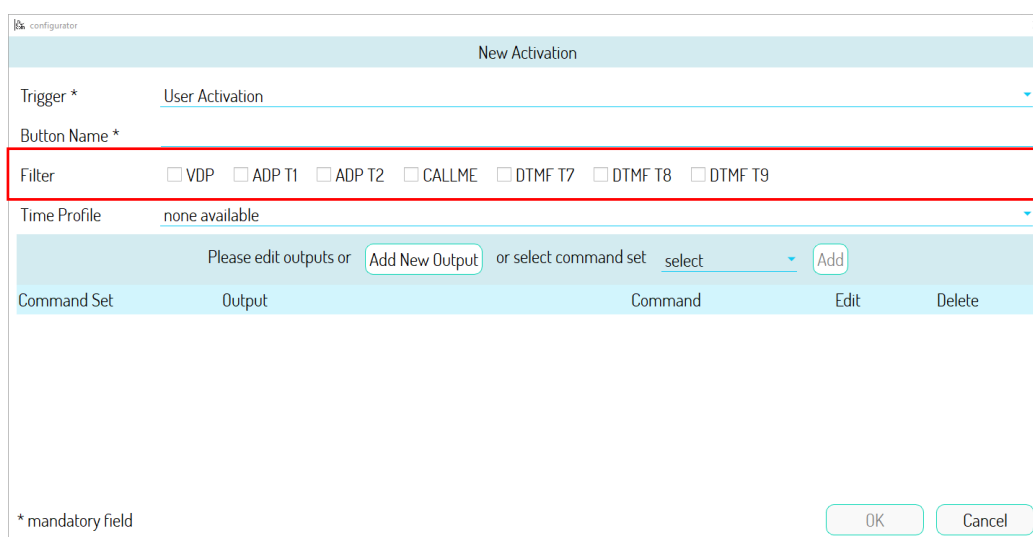


Figure 328: user activation

In the field "Button Name" it is advisable to enter a meaningful name of the activation (for example "Staircase lights").

The "Filter" field allows you to choose where to add the activation rule as shown below:

- if the "VDP" item is selected, the rule is added on video door phones with address book, that is MAX, VOG<sup>7</sup>, VOG<sup>5+</sup>, Basic and IPerCom Client application;
- if you select the "ADP T1" or "ADP T2" items, the rule is added on the VOG<sup>5</sup> video door phone and Miro door phone;
- if the "CallMe" item is selected the rule is added to the CallMe app;
- if the "DTMF T7" or "DTMF T8" or "DTMF T9" item is selected, the rule is added on the iPerTALK extensions.

For further details regarding the first 3 points above, see the paragraph [Addition of a user activation on video door phones / door phones / CallMe application](#).

As regards the last point, however, the choice of the items "DTMF T7" or "DTMF T8" or "DTMF T9" allows you to drive the output of a Relay Actuator or Lift Interface from an iPerTALK extension by pressing respectively button 7 or 8 or 9 only during conversation, that is in more detail in the following scenarios:

- an IPerCom calling station calls an IPerTALK extension and the latter answers the call;
- an iPerTALK extension carries out an auto on with two-way audio towards an IPerCom calling station.



In the case of IPerCloud apartments with call forwarding also on the GSM or landline telephone network, the selection of the "DTMF T7" or "DTMF T8" or "DTMF T9" items allows you to control the output of a Relay Actuator or a Lift Interface from a smartphone by pressing button 7 or button 8 or button 9 respectively only during a conversation with the calling station. If you answer from the CallMe application, this is obviously not possible.

Once the activation rule has been created (as seen in the previous paragraphs) the "Filter" column shows the previously selected items:

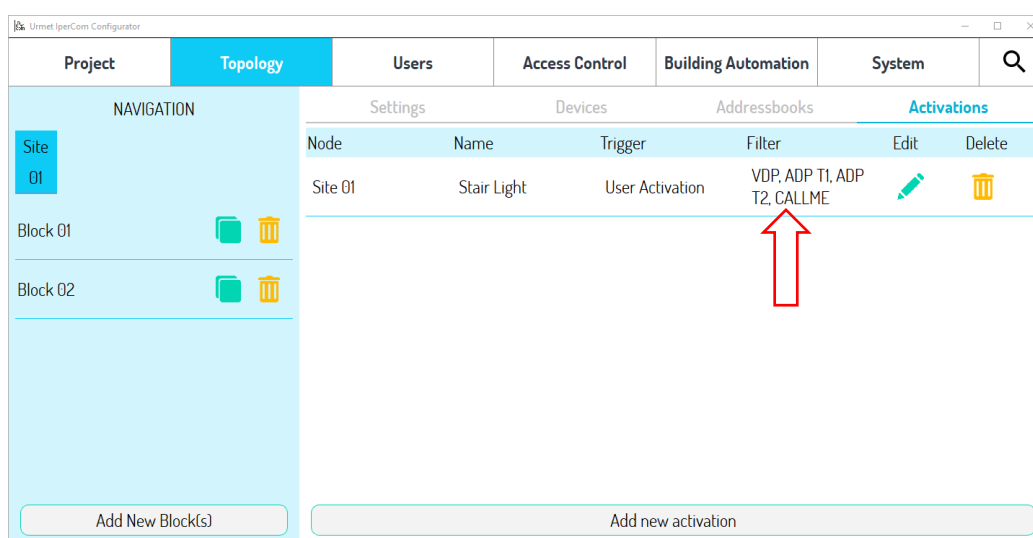


Figure 329: User activation created with all filters selected

If the activation rules have been created for the "Stair 01" node, these will be propagated to all the apartments included in the topological group of the " Stair 01" node.

By selecting an apartment in the navigation module, in correspondence of the "Activations" tab we will see the activation applied by the stair node, as shown in the following figure:

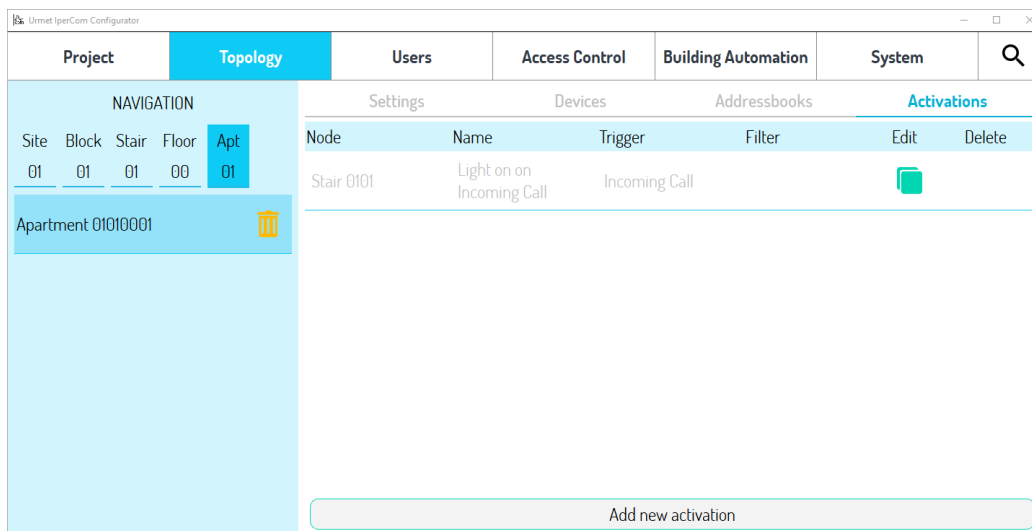



Figure 330: Activation "inherited" from the apartment

The activation is greyed out to show that it was created on the stair node, not on the apartment node. Therefore, it can only be modified by going to on the stair node and not to the current topological node.

If you want to replace the activation on the apartment with a custom one, just press the replacement  button and change the data.

Assuming you want to change the *Relay Actuator* output from "Output 2" to "Output 1" in the previous created activation, a screen like this will appear (the activation rule is no longer greyed out):

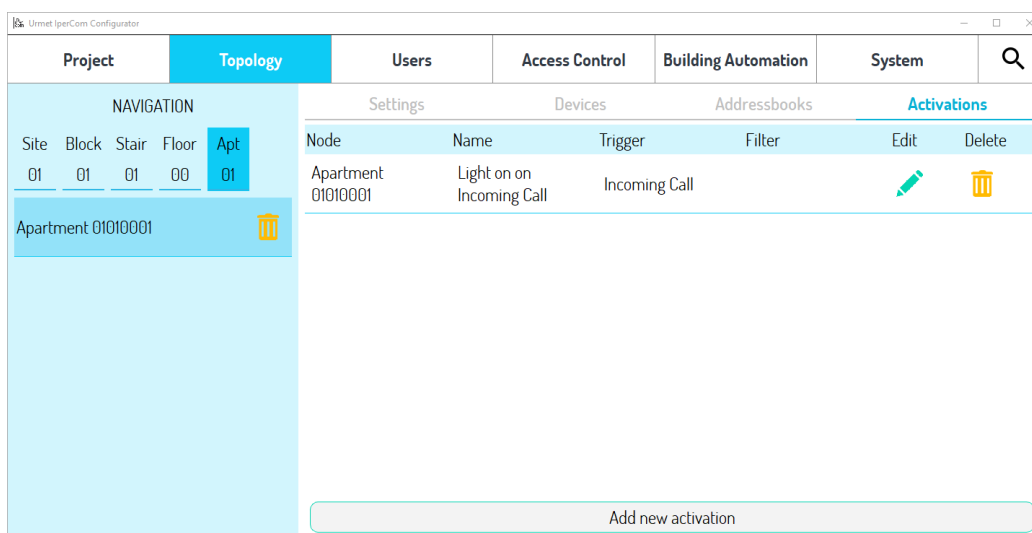


Figure 331: Replacement of the activation on the apartment with a personalised one

#### 7.1.5.8.1.1 Addition of a user activation on video door phones / door phones / CallMe application

When creating a user activation rule, it is possible to choose which type of apartment station/application to add via the "*Filter*" field. The possibilities are summarized below:

- addition of the activation rule on video door phones with address book, that is *MAX*, *VOG<sup>7</sup>*, *VOG<sup>5+</sup>*, *Basic*, and *IPerCom Client* application (corresponds to the "*VDP*" item in the "*Filter*" section);
- addition of the activation rule on the *VOG<sup>5</sup>* video door phones and *Miro* door phone (corresponds to the "*ADP T1*" or "*ADP T2*" entries in the "*Filter*" section);
- addition of the activation rule on the *CallMe* application (corresponds to the "*CallMe*" item in the "*Filter*" section).

Below is an explanation of what the user must do to make the activation work (for example to turn on the staircase lights) based on the choices made above.

### ADD USER ACTIVATION ON VIDEO DOOR PHONES WITH ADDRESS BOOK ("VDP" ITEM)

In the "Video door phone" screen of the MAX, VOG<sup>7</sup>, VOG<sup>5+</sup>, Basic video door phones and IPerCom Client application of these apartments, a new "ACTIVATION LIST" button will appear with a yellow light bulb icon:

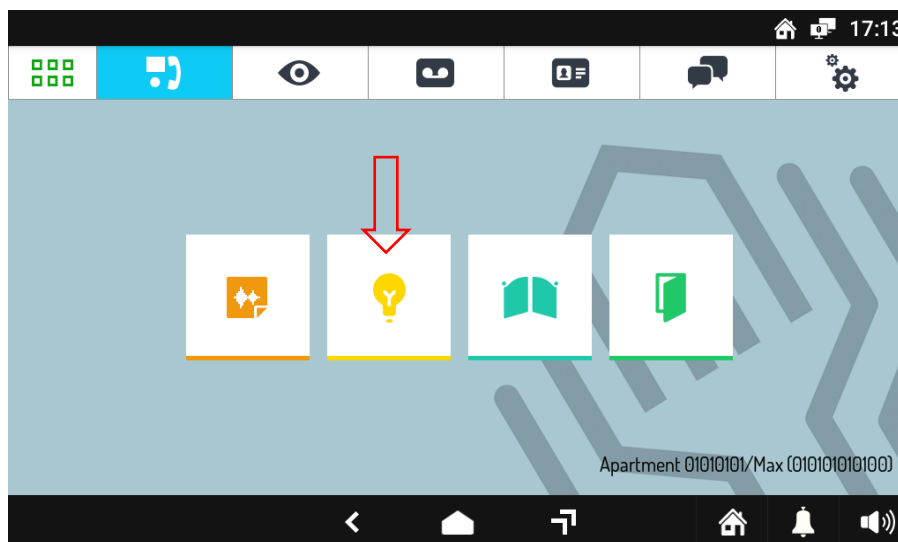


Figure 332: "ACTIVATION LIST" button

By pressing this button, the list of available activations will appear, which will, for example, show the "Stair Light" item assigned during configuration:

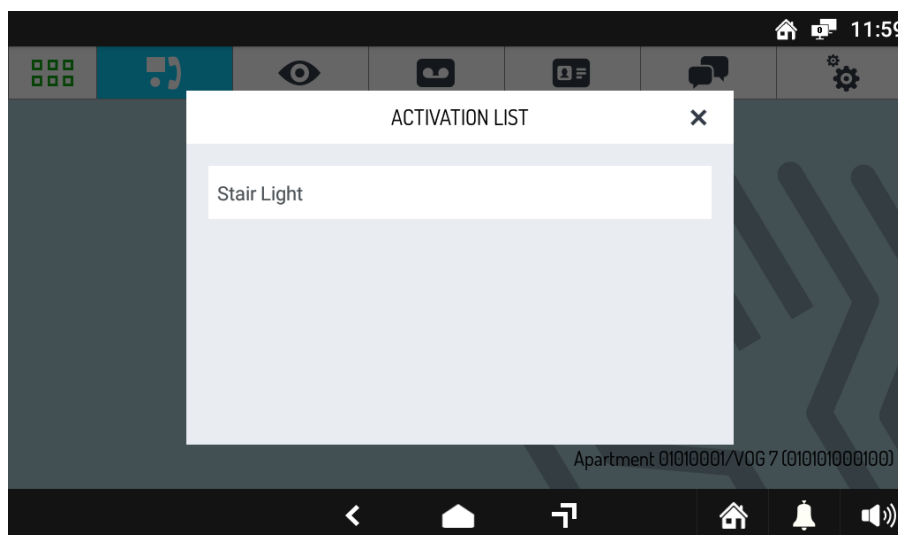


Figure 333: List of the user activation "Buttons"

By pressing on the "Staircase Light" item, the output of the *Relay Actuator* chosen during the configuration phase will be piloted, which will turn on the stair lights.

**ADD USER ACTIVATION ON VIDEO DOOR PHONE VOG<sup>5</sup> AND MIRO DOOR PHONE ("ADP T1" AND "ADP T2" ITEMS)**

Miro 1160/3 door phone and the VOG<sup>5</sup> 1761/6 video door phones have two buttons associated with the items "ADP T1" and "ADP T2". The buttons are shown in the following two figures:



Figure 334: T1 and T2 buttons of Miro door phone



Figure 335: T1 and T2 buttons of VOG5 1761/6

The button marked with a dot/gate corresponds to the "ADP T1" item while the other marked with two dots/light bulb corresponds to the "ADP T2" item. Therefore, depending on the button pressed, the output of the *Relay Actuator* chosen during the configuration phase will be driven, which will turn on the staircase lights.

*If the "Button T1 used for" option is set to the value "Gate Open" in the settings screen of the generic Miro door phone or 1761/6 video door phone, the activation rule described above will be inhibited (see [APPENDIX A: Configuration parameters of IPerCom devices](#)).*



### ADD USER ACTIVATION ON CALLME APP

The “*Staircase Lights*” button appears on the Home Page of the *CallMe* application (previously associated with the apartment):

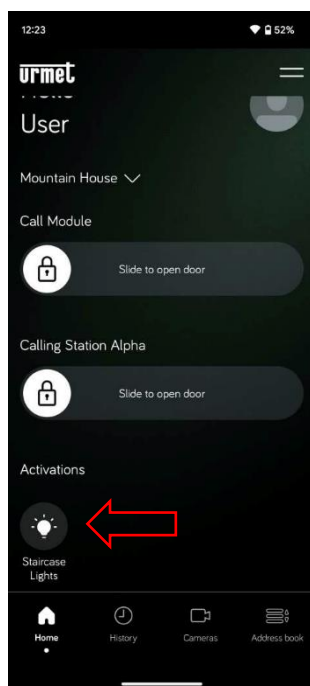


Figure 336: activation list

By pressing the "*Staircase Lights*" icon, the output of the *Relay Actuator* chosen during the configuration phase will be piloted, which will turn on the staircase lights.

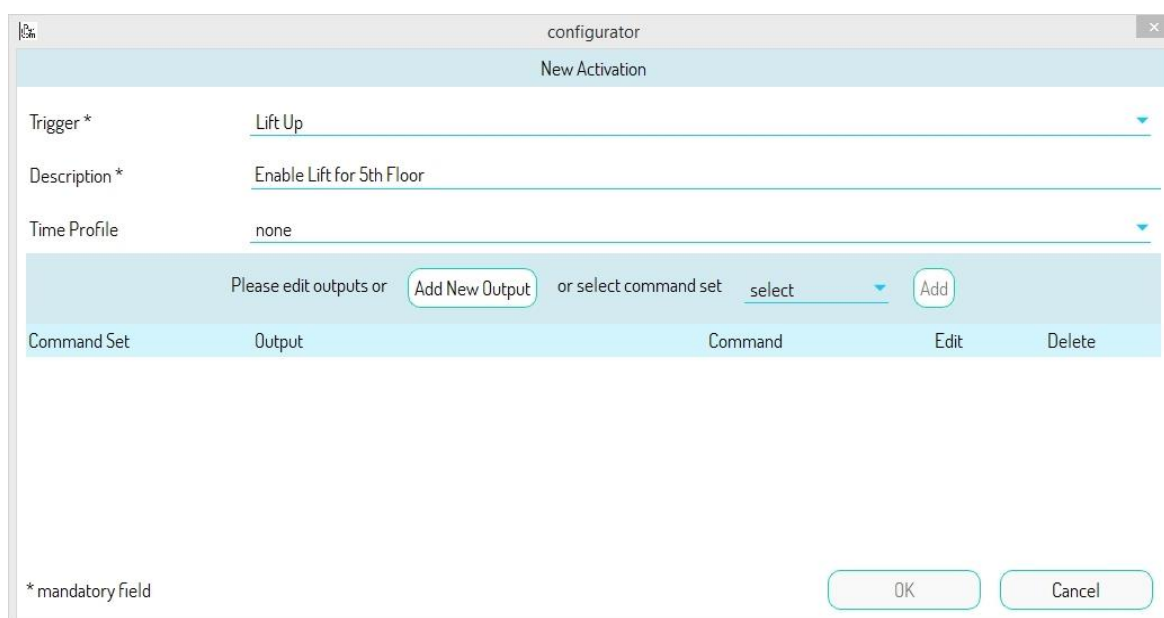
### 7.1.5.8.2 Topological events Lift Up and Lift Down

Regarding the selection of the “Lift Up” and “Lift Down” events, these options are only visible if you go in correspondence of stairs, floors, or apartments, as they are only associated with the use of the lifts.

In a system where there is a *Lift Interface* or a *Relay Actuator*, it is possible to create activation rules (maximum 2) that, for example, allow each resident to enable, through the *MAX*, *VOG<sup>7</sup>*, *VOG<sup>5+</sup>*, *VOG<sup>5</sup>* or *Basic* video door phone or *Miro* door phone or *IPerCom Client application*, the lift to reach either their own residence floor or the parking of the residential complex.

Position through the navigation module on a floor, on the “Activations” tab, press the *Add new activation* button.

In the “Event” field select “Lift Up”. It is recommended to enter a meaningful name in the “Description” field (e.g., “Lift enabling for floor 5”).



The screenshot shows a window titled "configurator" with a sub-header "New Activation". It contains the following fields and controls:

- Trigger \***: A dropdown menu with "Lift Up" selected.
- Description \***: A text input field containing "Enable Lift for 5th Floor".
- Time Profile**: A dropdown menu with "none" selected.
- A section with the text "Please edit outputs or" followed by an "Add New Output" button, "or select command set" followed by a "select" dropdown and an "Add" button.
- A table with the following structure:
 

Command Set	Command	Edit	Delete
Output			

At the bottom left, there is a note: "\* mandatory field". At the bottom right, there are "OK" and "Cancel" buttons.

Figure 337: screen for creating an activation with "Lift Up" event

Press the "Add New Output" button to configure the *Lift Interface* or *Relay Actuator* relays.

Position through the navigation module on the "Stair" where the device to be configured is located.

In the “Devices” area select the *Lift Interface* or *Relay Actuator*.

Select the *Lift Interface* in the "Control" area to display the relays to be configured. For more details on the configuration of Lift Interface relays see paragraph "[Control Relay Assignment](#)".

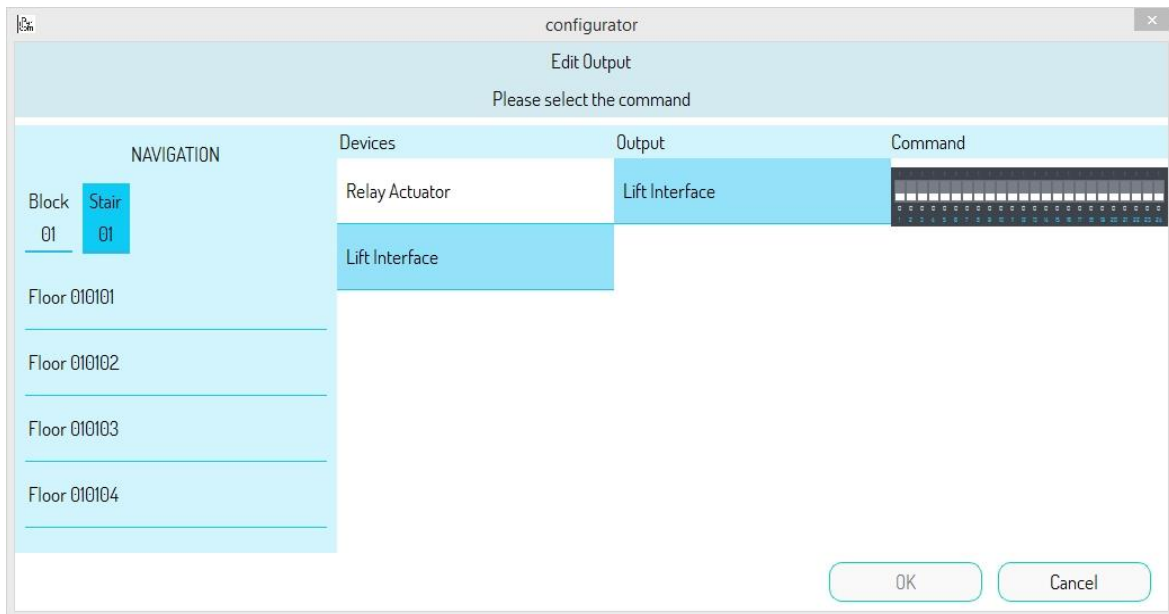


Figure 338: activation screen of Lift Interface relays

Select the relay(s) to be enabled and set the relay activation time in the "Duration" field.

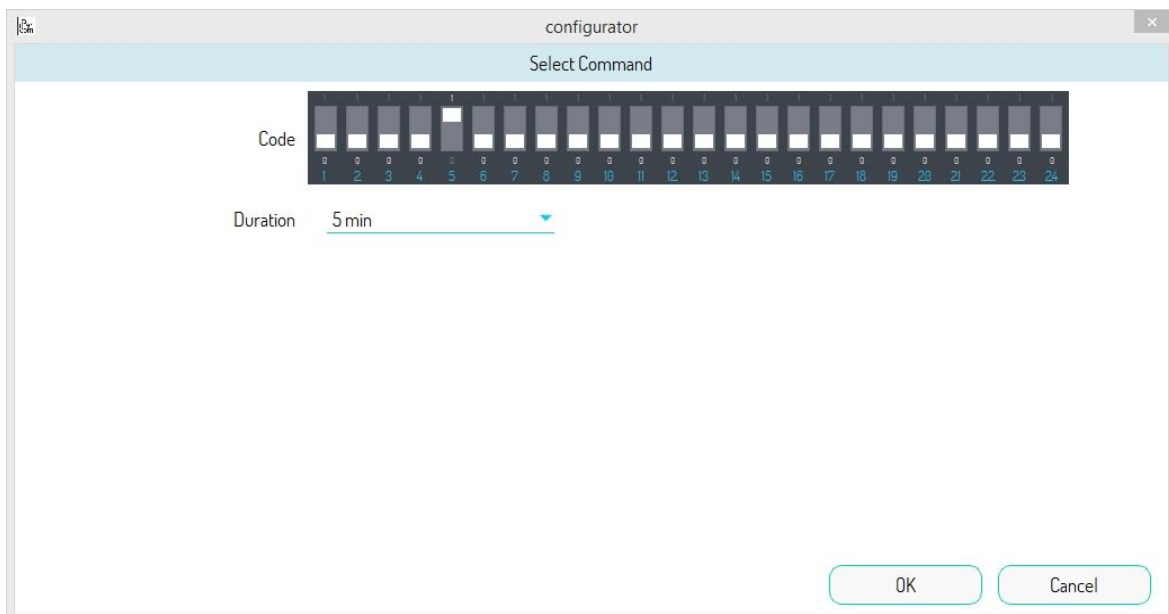


Figure 339: enabling the Lift Interface relays

Select the *Relay Actuator* in the "Output" area to display the outputs to be configured. The outputs must be set in monostable mode and the relay activation duration must be enabled in the device configuration page (see [APPENDIX A: Configuration parameters of IPerCom devices](#)).

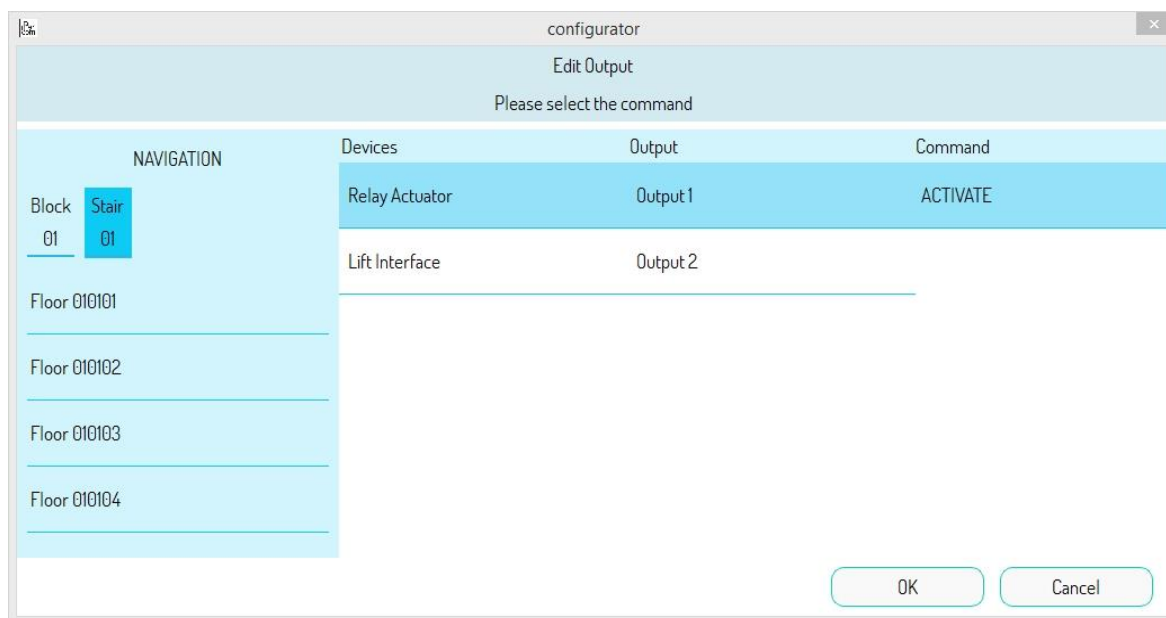


Figure 340: activation screen of the Relay Actuator

In the "Video Door Phone System" screen of the MAX, VOG<sup>7</sup> or Basic video door phones or IPerCom Client application belonging to the topological group of the "Stair 01" node, a new "LIFT" icon will appear (highlighted in red).

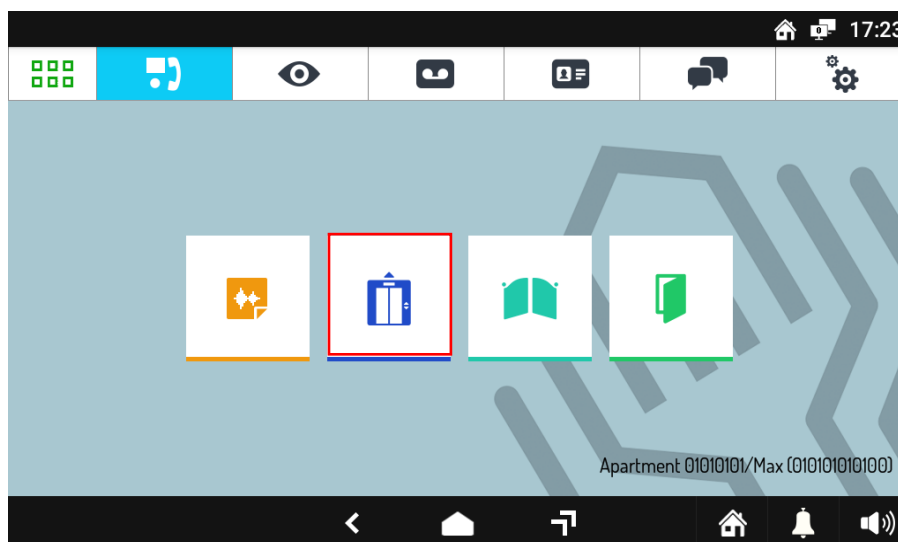


Figure 341: "LIFT" button

Press the *Lift Interface* or *Relay Actuator* icon to activate the configured relays by sending the "Up" or "Down" command to the lift, for the set time.

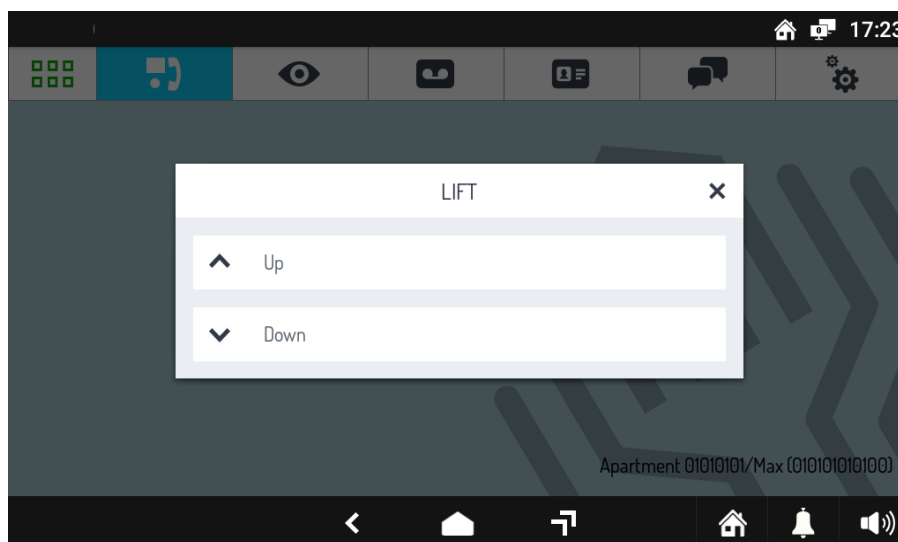




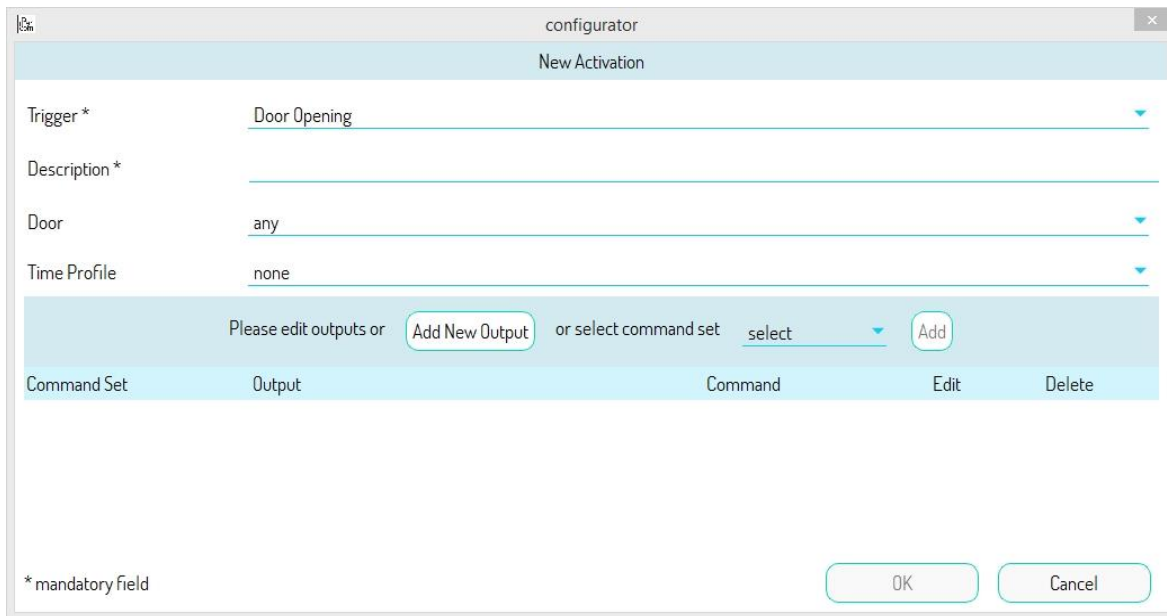
Figure 342: Lift "Up" and "Down" commands

 To obtain the same functions on the VOG5 video door phone and on the Miro door phone, the relative keys T1 and T2 must be set to the "Lift Down" and "Lift Up" events (see [APPENDIX A: Configuration parameters of IPerCom devices](#)).

 This feature is not available via the CallMe app on smartphones/tablets.

### 7.1.5.8.3 Events Open Door and Open Gate

The "Open Door" and "Open Gate" events can refer to any door or gate in the system. If you choose one of these two events, the "any" (default) events will appear, as shown in the image below:



configurator

New Activation

Trigger \* Door Opening

Description \*

Door any

Time Profile none

Please edit outputs or  or select command set select

Command Set	Output	Command	Edit	Delete

\* mandatory field

Figure 343: Open door/gate activation

In this case, about calling station access points, the activation of one or more relay outputs also takes place outside the call step itself, by simply pressing the door and gate opening keys of apartment stations

Alternatively, you can choose a precise entrance (door or gate) using a special drop-down menu.

In this second case the relay outputs are piloted only after the actual opening of the selected access point.

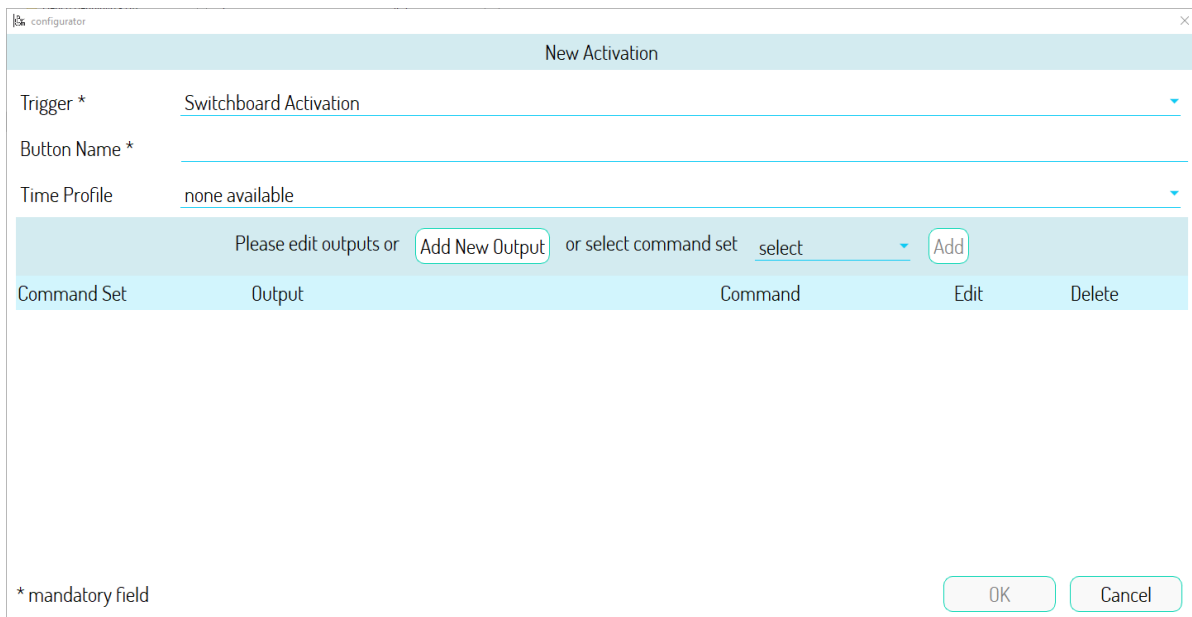


*If the door of a Key Reader is chosen for the Door Opening event, the selected outputs are controlled only if the Key Reader is on the topological path of the concerned apartment and not when an enabled key is passed.*

#### 7.1.5.8.4 Switchboard Activations

Switchboard activations are activation rules that appear only on the *Switchboard* application, if created on its topological path. For example, if placed on the unit node, the activations that will be shown on the **Switchboard** application are those created from the unit (where the **Switchboard** application is present), block or site node.

So once the correct topological node has been chosen, after pressing the "Add new activation" button, the "Event" drop-down menu will allow you to choose the "Switchboard Activation" item, as shown below:



The screenshot shows a 'New Activation' dialog box. The 'Trigger' dropdown is set to 'Switchboard Activation'. The 'Button Name' field is empty. The 'Time Profile' dropdown is set to 'none available'. Below the fields is a bar with the text 'Please edit outputs or Add New Output or select command set select Add'. Below this bar is a table with columns: Command Set, Output, Command, Edit, and Delete. At the bottom left is the text '\* mandatory field' and at the bottom right are 'OK' and 'Cancel' buttons.

Figure 344: creation of activation from the switchboard

Also in this case, give a meaningful name to the activation ("*Button Name*" field), select one or more outputs through the "*Add a New Output*" button and eventually a time profile, as seen in the previous paragraphs. When pressing the "OK" button, the activation is created and added to the list of activations of the topological node chosen before:

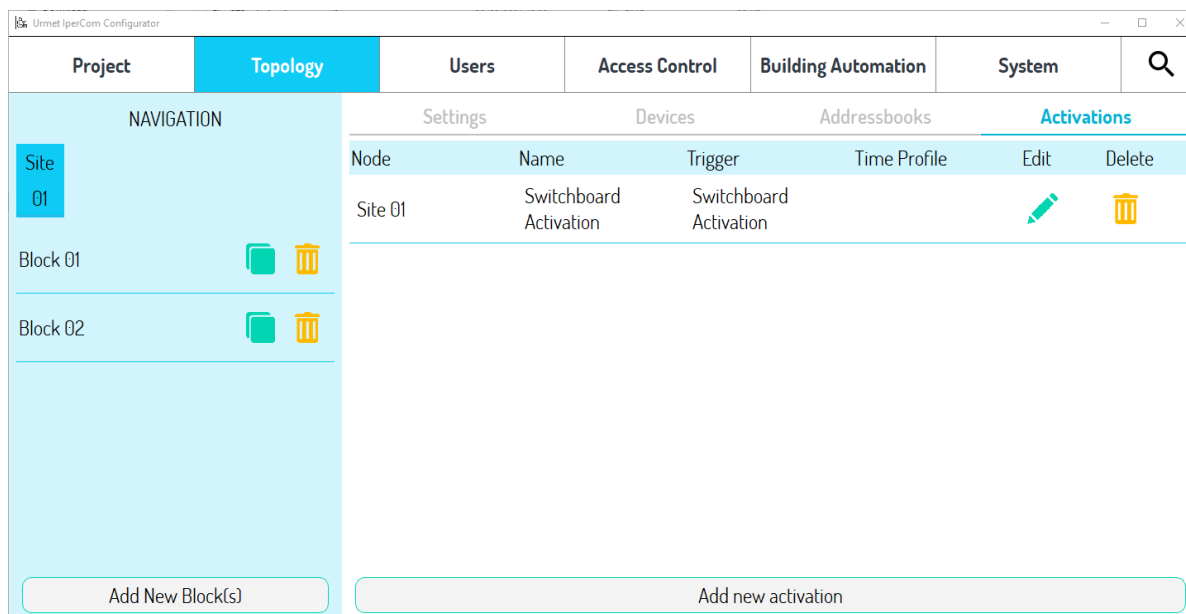


Figure 345: activation from switchboard created on the configurator

The newly created activation rule will appear on the *Switchboard* application as below:

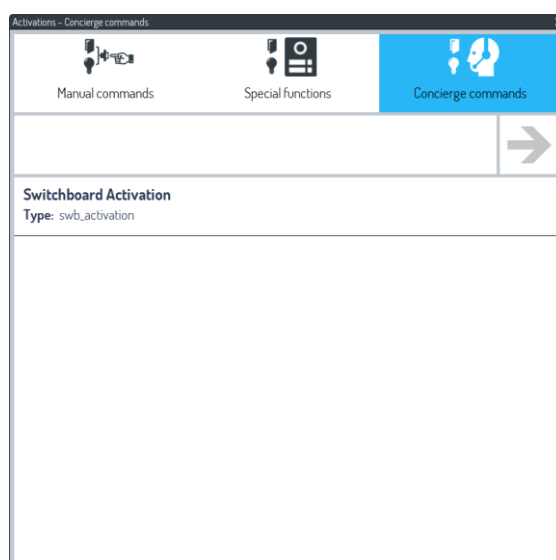


Figure 346: activation from switchboard on related application

For further details see the Switchboard application manual downloadable from [www.urmet.com](http://www.urmet.com)



### 7.1.5.8.5 Activations for topological events with 2Voice audio/video apartment stations

Activations for topological events also apply to topological stair nodes with *2Voice Gateway* with the following differences:

1. The *User Activations - MAX, Lift Down* and *Lift Up* events are not present on the nodes below a stair node with *2Voice Gateway*:

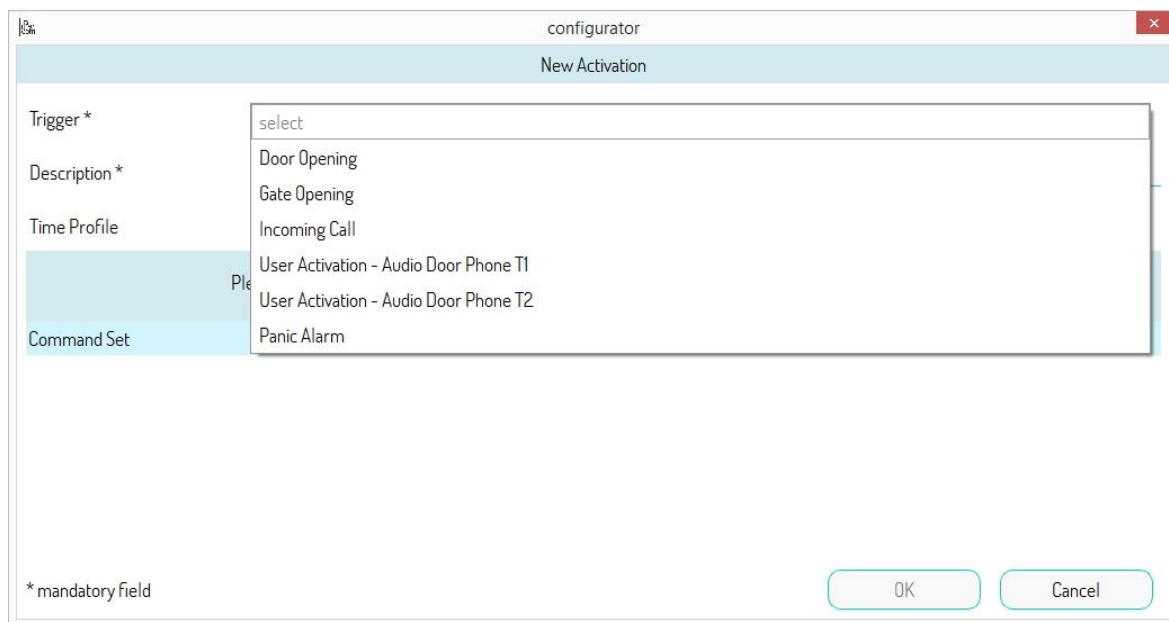


Figure 347: List of events for audio/video Door Phone 2Voice

The events in question are instead present on each stair node with *2Voice Gateway*, because on these nodes it is possible to add other IPerCom devices (e.g., one or more *MAX, VOG<sup>7</sup>* or *Basic video door phones* where it could be necessary to create activations related to these events):

2. *User Activation - Door Phone T1* and *User Activation - Door Phone T2* events do not refer to buttons T1 and T2 of the Door Phone 1160/3 or 1761/6 video door phone and correspond to the pressing of two specific buttons of the 2Voice audio/video Door Phone that activate *special function 7* (T1) and *special function 8* (T2) (under certain conditions) instead. Only these two special functions are correctly interpreted by the gateway and sent to the *Relay Actuator 1060/84*. Refer to the individual instruction manuals of 2Voice Door Phones for more details on the buttons which activate these special functions and under which conditions these buttons must be pressed.

The activation rule, if set on apartment level, will only apply to the individual apartment. This allows you to have different activation rules on individual apartments located on the same gateway.

If set on site or block level, the activation rule is inherited by the 2Voice apartments and by apartments with IPerCom Door Phones. It is always light grey (to highlight that it was not created in the apartment node):

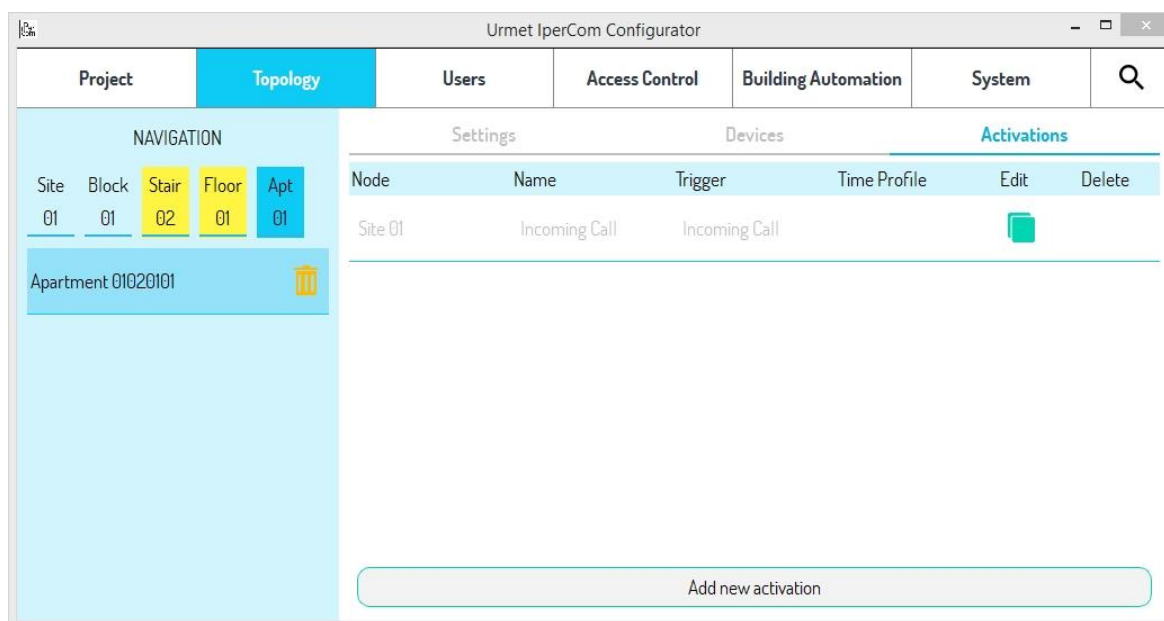







Figure 348: Activation "inherited" from 2Voice apartment

If you want to replace the activation on the 2Voice apartment with a custom one, just press the replacement button  and change the data.

If set on scale or floor level, the activation rule will be propagated only to 2Voice apartments of the topological group of the respective node. Again, in this case, the activation rule appears greyed out on the apartment and the button  can be used to modify the data.

 *The Incoming Call event regards both the calls arriving from the IPerCom call stations and those arriving from the 2Voice call stations.*

 *The association of the 2Voice apartment level events to one or more relay outputs can also be done using the special 2Voice 1083/80 decoding. For further details follow the instructions in the 2VOICE technical manual and in the instruction manual of the special decoder Ref. 1083/80.*

 *The "User Activation - Max" event, if activated on a site or block node, is not propagated on the 2Voice apartments.*

### 7.1.5.9 Automation events: input/output association

Each relay actuator is provided with two inputs (controlled by buttons or switches) to:

- control the respective outputs locally;
- control one or more outputs of different relay actuators by means of events (of the inputs).

In the first case, staircase light control is a typical example in which it may be useful to have a local output control. According to the previous paragraphs, the "Door Opening" topological event, which activates an output on the relay actuator, can be used to turn on the staircase lights, for example. Similarly, using a button located in the entrance hall and connected to the input of the same actuator, it is possible to switch the staircase lights on locally in the same way.

For the second case, instead, the outputs (**one or more of several relay actuators**) are controlled by events associated with the **single** input of a relay actuator, which can be configured in bistable mode (switch) or monostable mode (button). In the latter case it is also necessary to define the button pressure time. If it is assumed that in case of switch the pressure time is zero, the possible events are shown in the table below.

Mode	Event 1	Event 2
Bistable (t= 0)	ON	OFF
Monostable (t> 0)	Short press	Long press

Table 11: Automation rules to be implemented

The operating mode of the input can be set in the *Relay Actuator* input configuration page (see [APPENDIX A: Configuration parameters of IPerCom devices](#)).

Again, on the *Relay Actuator* configuration page you can deselect the "Output linked to input" option, which selected by default. In this way, the output is controlled only by the rules which will be defined on the *Automation* page and will be locally disconnected from the input.

The inputs can be set as normally closed or normally open (default choice) to meet different installation needs.

To program the inputs and outputs of the Relay Actuator, follow the instructions on the device configuration page (see [APPENDIX A: Configuration parameters of IPerCom devices](#)).

The correct approach to create automation rules (input/output association) is to firstly identify the combinations of commands to be imparted by the system (relay output activation), then to create a rule for each combination of commands with the respective event. The following example shows the procedure.

### 7.1.5.9.1 Input-output activation on two different relay actuators

In this example, we will assume there are two combinations of commands to be imparted on the system:

- switch on light 1 for a predefined time;
- switch on light 1 and light 2 for the predefined time.

Two automation rules are required.

Switching on a generic light for a predefined time means having a relay output programmed as monostable.

Let's assume that want to create the two rules using two different events (long and short press) of the same input of a "Relay Actuator A". The two outputs are on a "Relay Actuator B". The situation is shown in the following table:

Rule	Inputs (Relay Actuator A)	Event	Outputs (Relay Actuator B)	Outputs (Relay Actuator B)
Rule 1	Input 1	Short press	Output 1 - Active	-----
Rule 2	Input 1	Long press	Output 1 - Active	Output 2 - Active

Table 12: Automation rules to be implemented



*Input programming is only possible on Relay Actuators **with firmware version 3.04 or higher supported from IPerCom version 1.3 or higher.***

From the table above you can see how the same button with two different events can be used to execute two combinations of different commands, i.e. switch on one light (short press event) or switch on two lights (long press event).



*Before building the activation rules, it is advisable to give meaningful names to the inputs and outputs of the individual Relay Actuators and to set their times correctly, so that the inputs and outputs are easily identifiable during the rule building phase. Go to the device configuration page to do this (see [APPENDIX A: Configuration parameters of IPerCom devices](#)).*

Having followed the instructions in the note, the input/output association can be set on the *Automation* tab under "*Activation Rules*", as shown in the following figure:

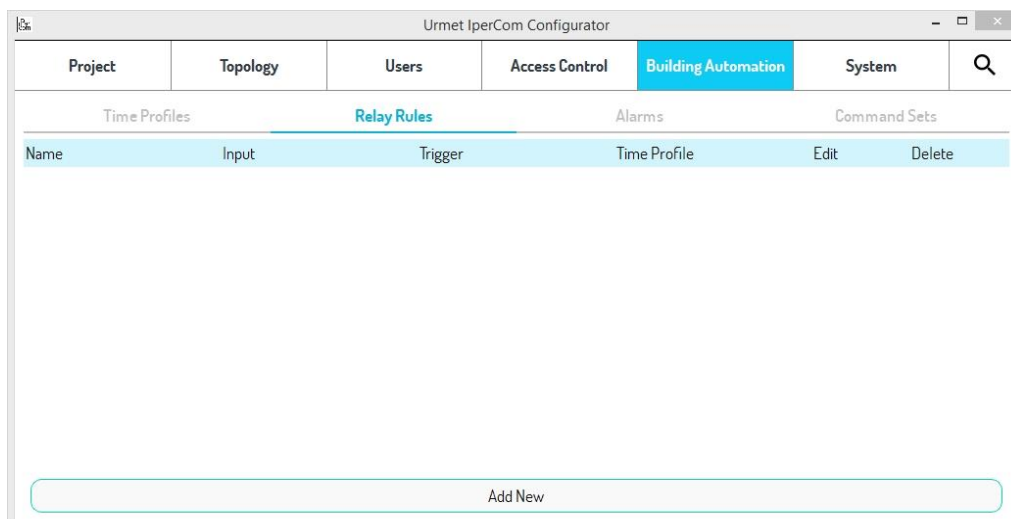


Figure 349: "Automation" page, "Activation Rules" tab

Press "Add New" to open the following page:

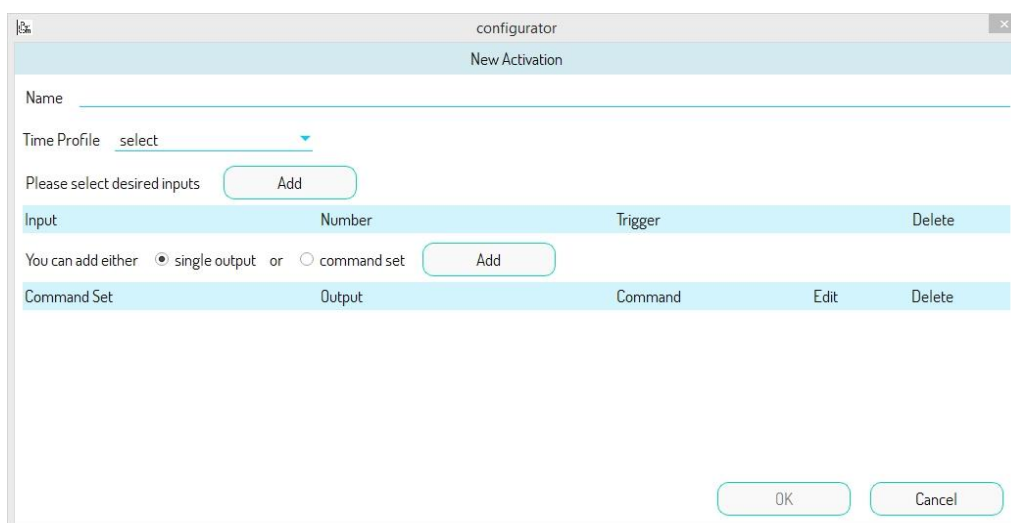


Figure 350: Creating a new activation

On this page, you can:

- give a meaningful name to the new activation in the "*Name*" field;
- associate a time profile (previously created) with the activation using the "*Time Profile*" drop-down menu (the association is not mandatory) to restrict its validity in time;
- select the relay actuator inputs and outputs by pressing the respective "*Add*" buttons.

The input selection "Add" button opens the following screen:

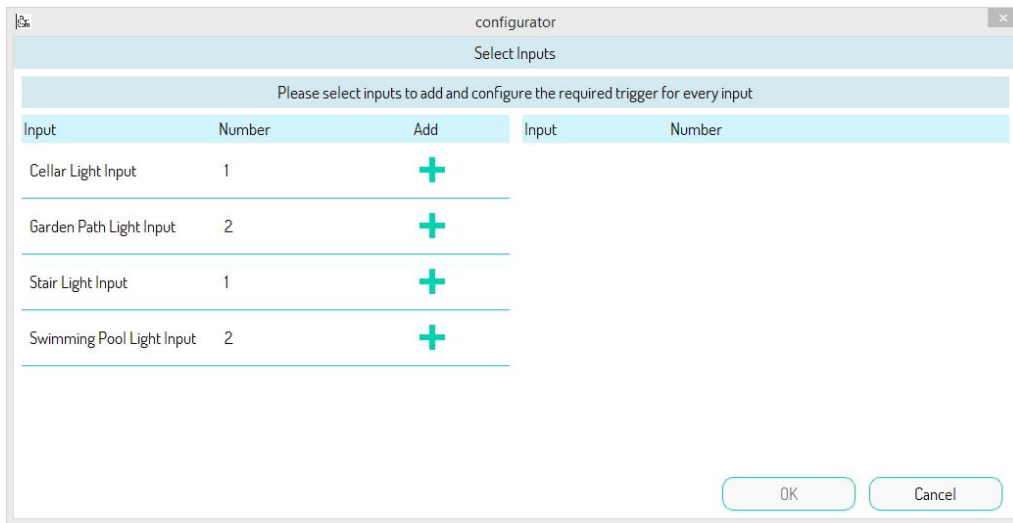



Figure 351: List of available inputs

If the default names of the inputs were still used for each *Relay Actuator* (i.e. *Input 1* and *Input 2*, instead of the previously assigned meaningful names), it would have been difficult to identify the input with which to associate the rule you want to build.

Assuming you want to build a rule on how to turn on the garden path lights and that you have set the desired time at the concerned input (greater than zero) in the configuration phase, pressing the respective button  will move the input to the right side of the screen:

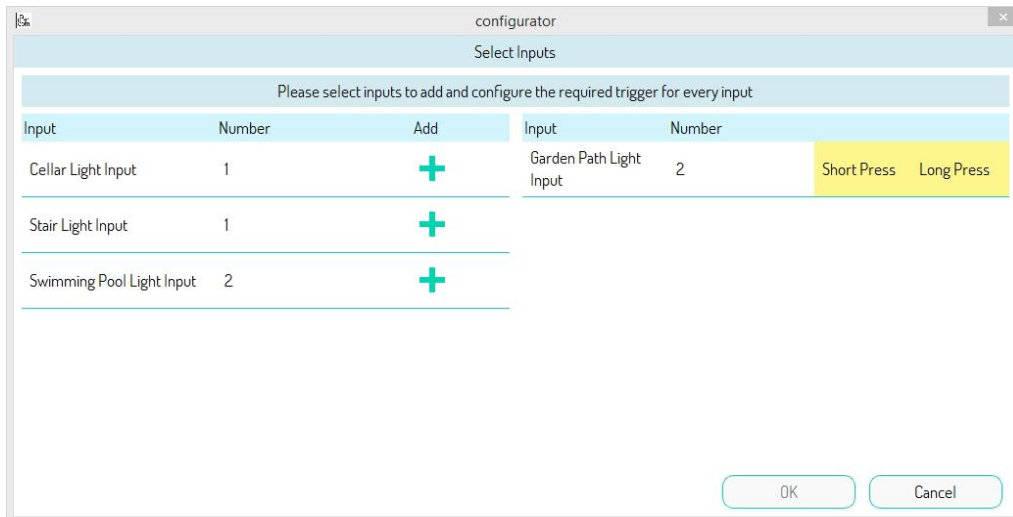


Figure 352: Events that can be selected with press time other than zero

For example, if you choose the "Short press" event, it will be highlighted with a different colour from the previous one:

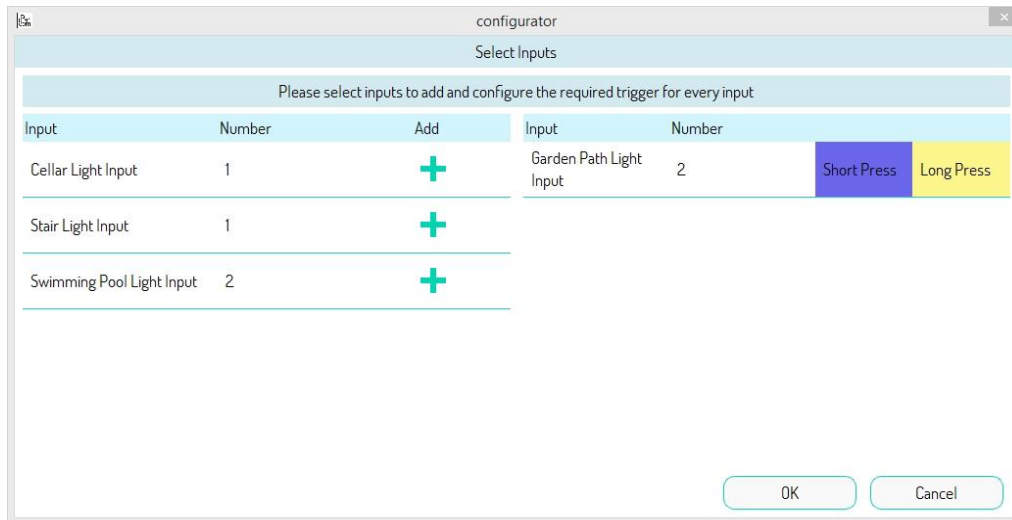


Figure 353: "Short Pressure" event selected



If the input in question were set as bistable, the events displayed would be "ON" and "OFF".



The input you are associating with the rule passes to the right of the screen, while those not yet associated remain on the left. In this way, you can associate the inputs of all the relay actuators of the system with the same rule on a single screen.

Press "OK" button to see a summary of the choices made for the input:

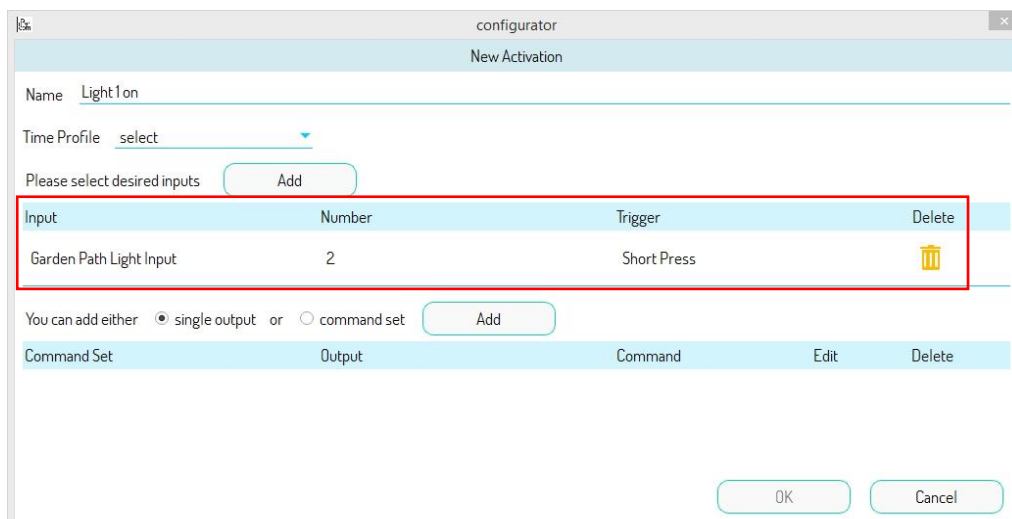


Figure 354: Selected input and event

The "Delete" button allows you to delete the rule on the newly created input (by means of a confirmation pop-up).

At this point, as shown in the table, you must choose the output to be controlled. If with the "Short press" event you want to control only one "Garden Path light 1" output of the second relay actuator, you must select the "single output" item:

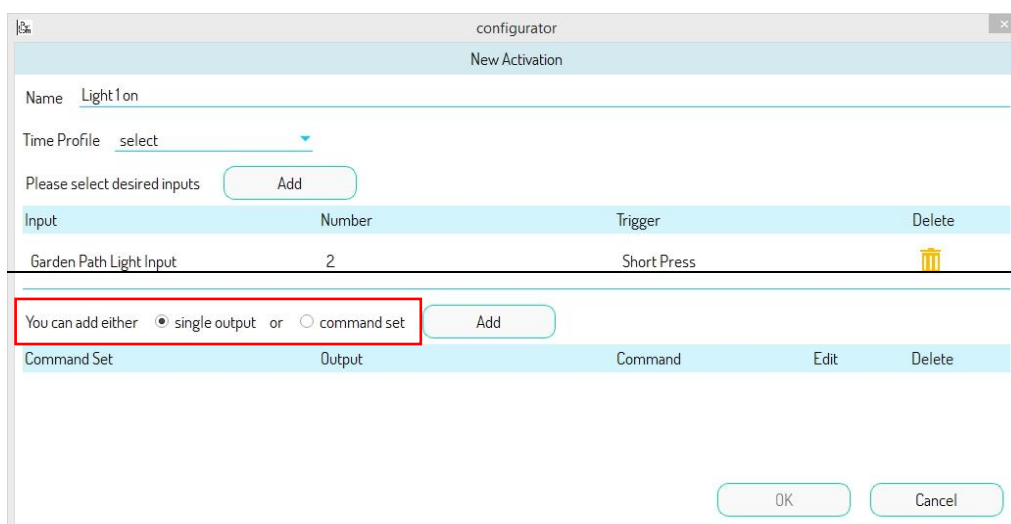


Figure 355: Selection of a single output

Press the "Add" button for the outputs. The following page will appear:

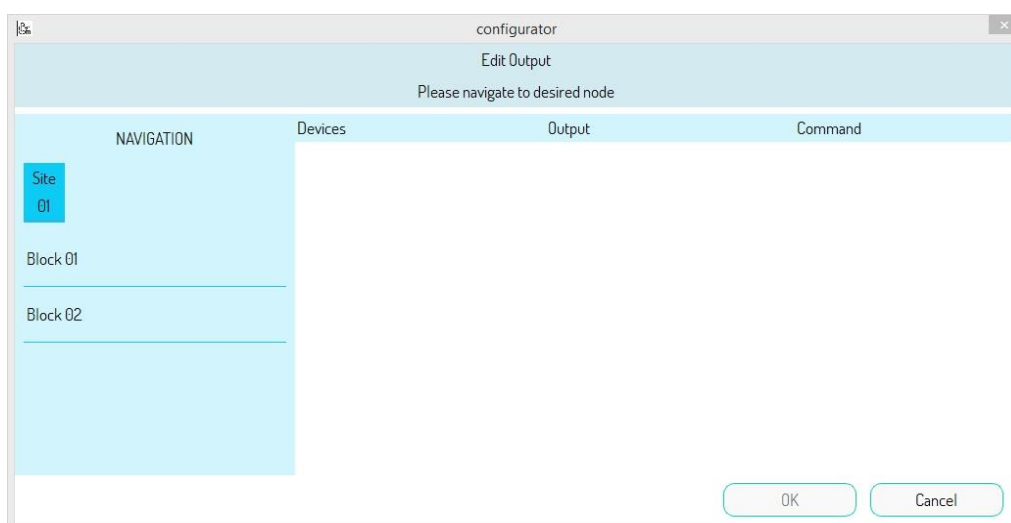


Figure 356: Topological structure for relay actuator search



Go to the topological node of the *Relay Actuator 2*, select the concerned device, then choose the output and set the respective command:

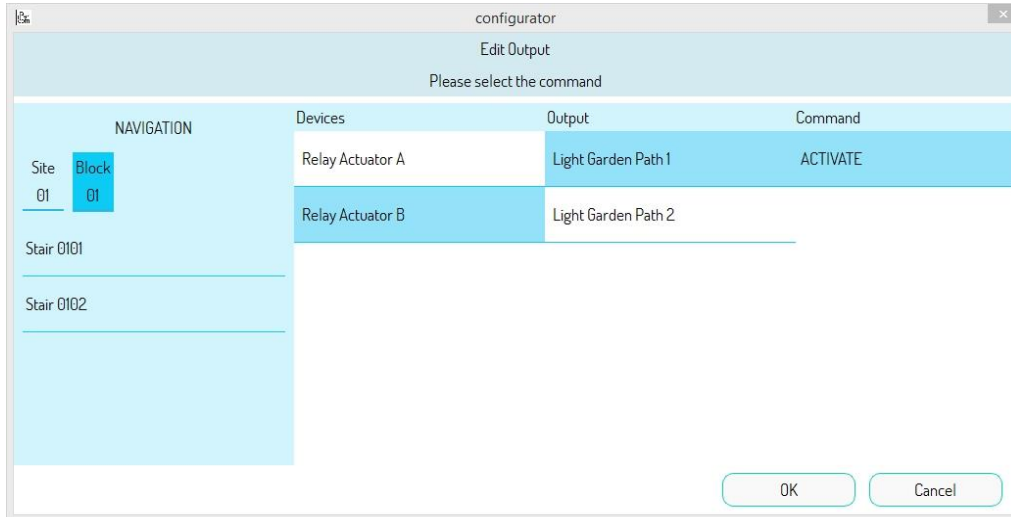


Figure 357: Topological structure navigation for relay actuator search, output selection and respective command

Press the "OK" button to open the following screen with a summary of the choice made regarding the output:

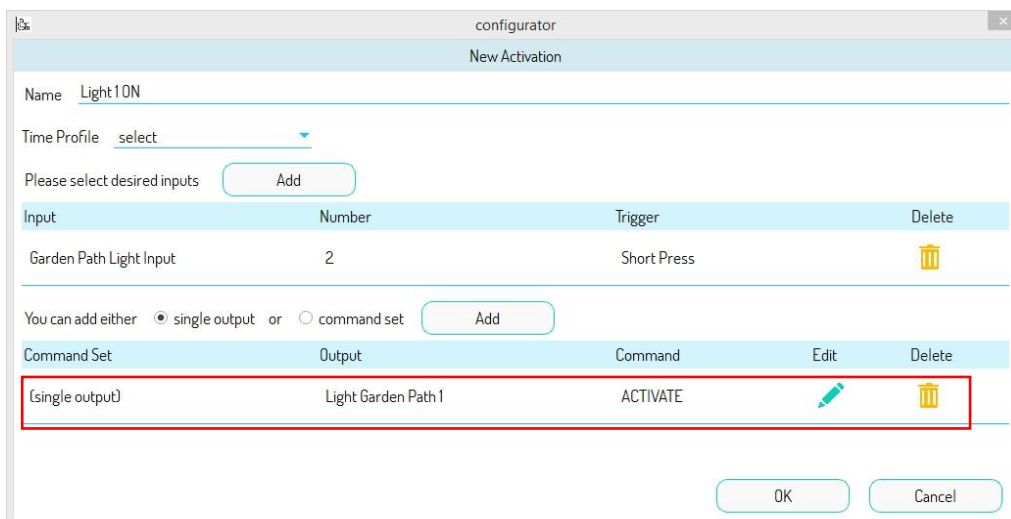


Figure 358: Selected output and respective command

The buttons in the "Edit" and "Delete" columns can be used to modify or delete the output and the respective command (via confirmation pop-up), respectively.

Press the OK button again to go back to the main screen where the name of the activation, the input and the relative event are shown:

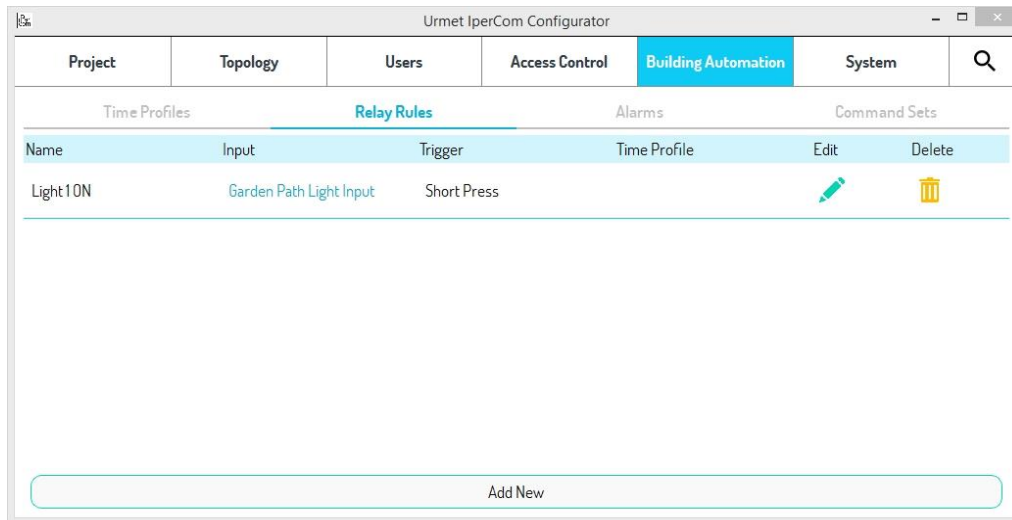


Figure 359: Activation created

The buttons in the "Edit" and "Delete" columns can be used to modify or delete the newly created rule (via confirmation pop-ups), respectively.



*It is advisable to give a meaningful name to the created rules so that they can be quickly identified, since no reference to the controlled output(s) appears in the summary. The reference can be retrieved in all cases by pressing the "Edit" button.*

A second rule must be constructed to implement the second command combination (Garden Path Light 1 and Garden Path Light 2).

Using the same input of the first *Relay Actuator*, the one named as "*Garden Path Light Switch Input*", it is possible to switch on both the first and the second light (outputs linked to the second *Relay Actuator*). So it is possible taking advantage of the second event linked to the programming of the input, that is the "*Long press*" event, as shown in the figure:

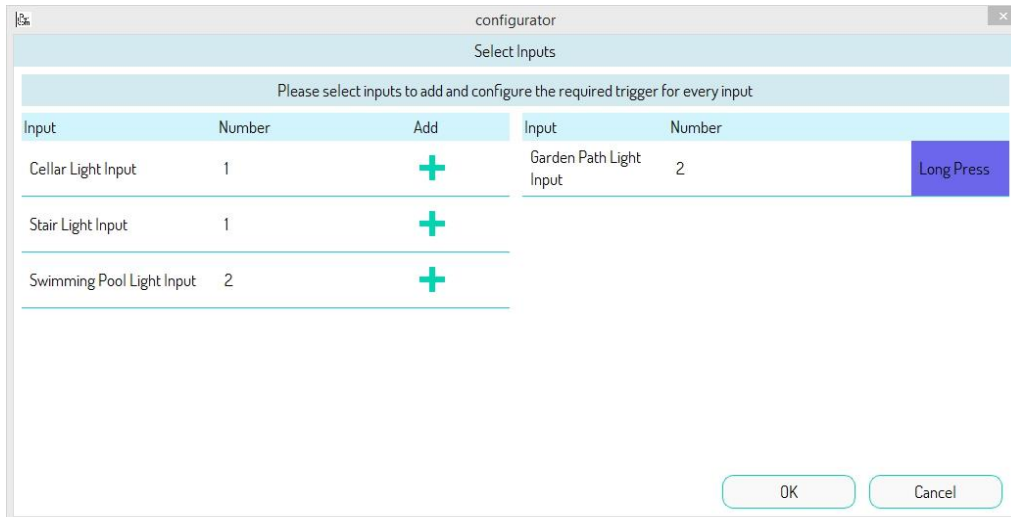


Figure 360: second selectable event in monostable mode

The procedure is like what we saw before with the only difference that in the selection of the outputs both outputs of the *Relay Actuator 2* in "*ACTIVATED*" mode are added, as shown in the figure:

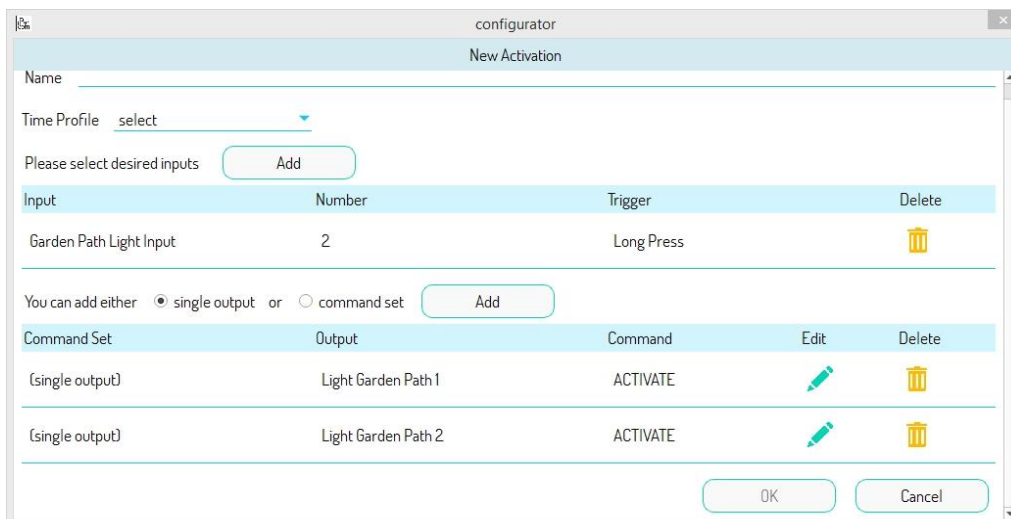
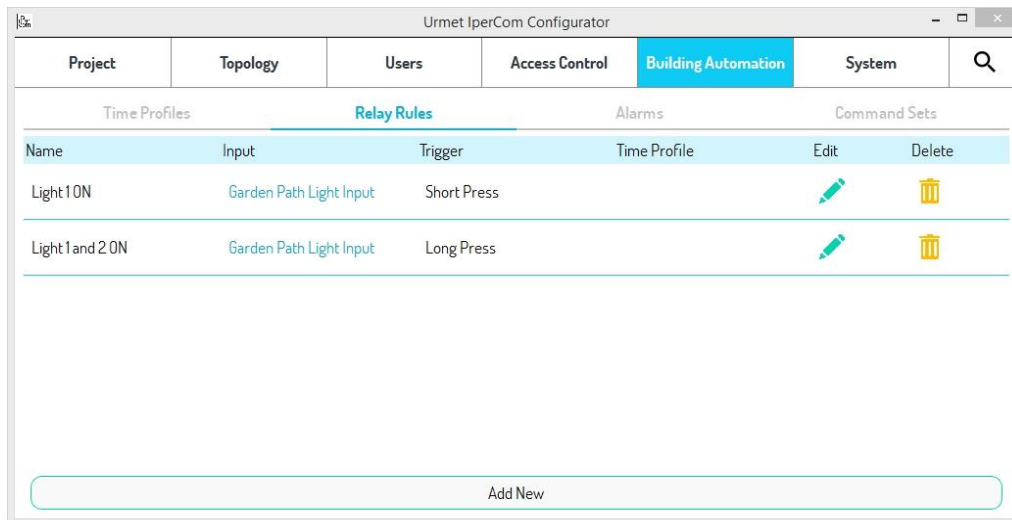


Figure 361: input associated with 2 outputs with long pressure command

After having given a meaningful name to the newly created rule and having pressed "OK", you have the situation shown in the figure, where the name of the activation, the input and the respective event will appear:







Urmel IperCom Configurator						
Project	Topology	Users	Access Control	Building Automation	System	Q
Time Profiles		Relay Rules		Alarms	Command Sets	
Name	Input	Trigger	Time Profile	Edit	Delete	
Light 10N	Garden Path Light Input	Short Press				
Light 1 and 2 ON	Garden Path Light Input	Long Press				
Add New						

Figure 362: Summary of created activations

The buttons in the "Edit" and "Delete" columns can be used to modify or delete the newly created rule (via confirmation pop-ups), respectively.



*Once an output has been added to the rule, it is no longer re-submitted by navigating the topological structure of the system to add more outputs.*

The example shown above is just one example of how to build an activation. For example, you could also use the two buttons on *Relay Actuator 1* to activate the two outputs of the second *Relay Actuator* with events other than short and long presses.

### 7.1.5.9.2 Creating a scenario

In this example, we will suppose that the combination of commands to be imparted on the system consists in switching on four lights and switching off two lights using three different events:

- Automation event (e.g., short press on input)
- Topological event (e.g., activation by user on *MAX video door phone*)
- Event on device (e.g., *Call Module auto-on*).

In this case, it is convenient to group the commands, i.e. to create a scenario.

A scenario lets you add a combination of commands through a single item to avoid the need to add multiple commands in three different points of the configurator one at a time.

If you then need to change the combination of commands (adding lights or changing output commands), simply do this on the scenario and not on the individual activations.

The following table summarises this regarding the automation event (three *Relay Actuators* are needed to have one input and six outputs):

Rule	Inputs ( <i>Relay Actuator A</i> )	Event	Outputs ( <i>Relay Actuator</i> )
Rule 1	Input 1	Short press	Light 1 - ON - <i>Relay Actuator A</i>
			Light 2 - ON - <i>Relay Actuator A</i>
			Light 3 - ON - <i>Relay Actuator B</i>
			Light 4 - ON - <i>Relay Actuator B</i>
			Light 5 - OFF - <i>Relay Actuator C</i>
			Light 6 - OFF - <i>Relay Actuator C</i>

Table 13: Command groups

To create the scenario, go to the "Automation" page, "Scenarios" tab:

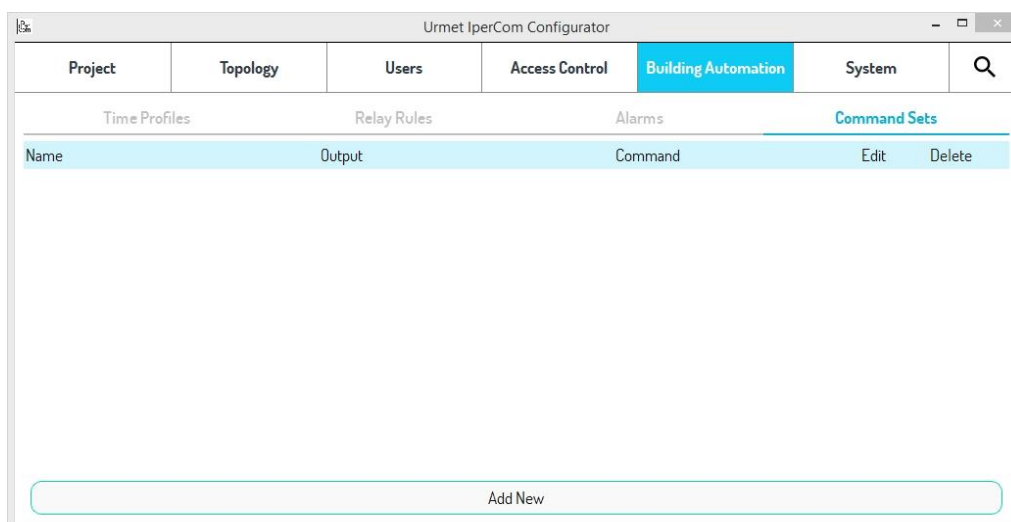


Figure 363: "Scenarios" tab for creating a group of outputs

To build the group of commands press the "Add New Output" button. The following page will appear:

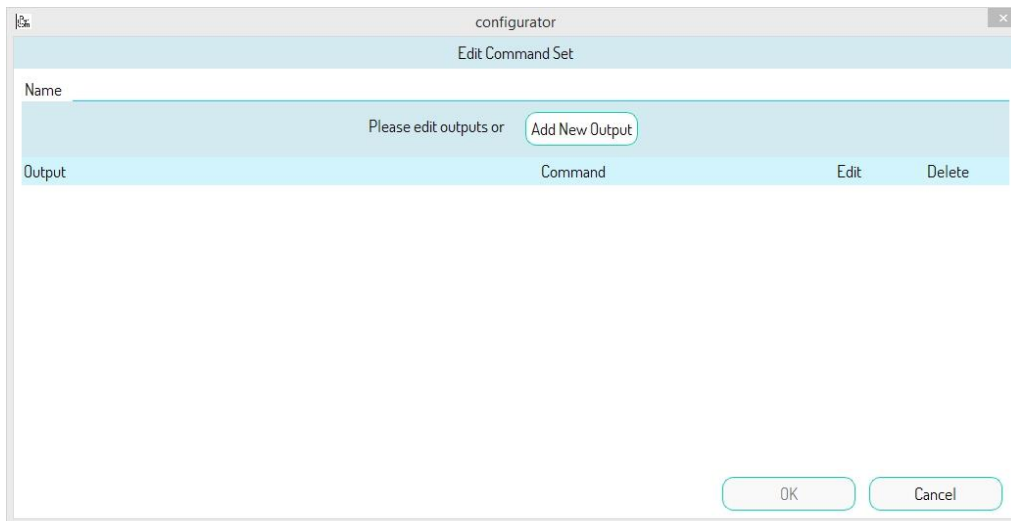


Figure 364: Creation of a group of commands

First, you need to give a meaningful name to the group of commands, then add the outputs you want them to be part of the group. To do this, press the "Add a New Output" button. A screen will open. Go to the topological node of the *Relay Actuator*, select the concerned device, then choose the output and set the respective command:

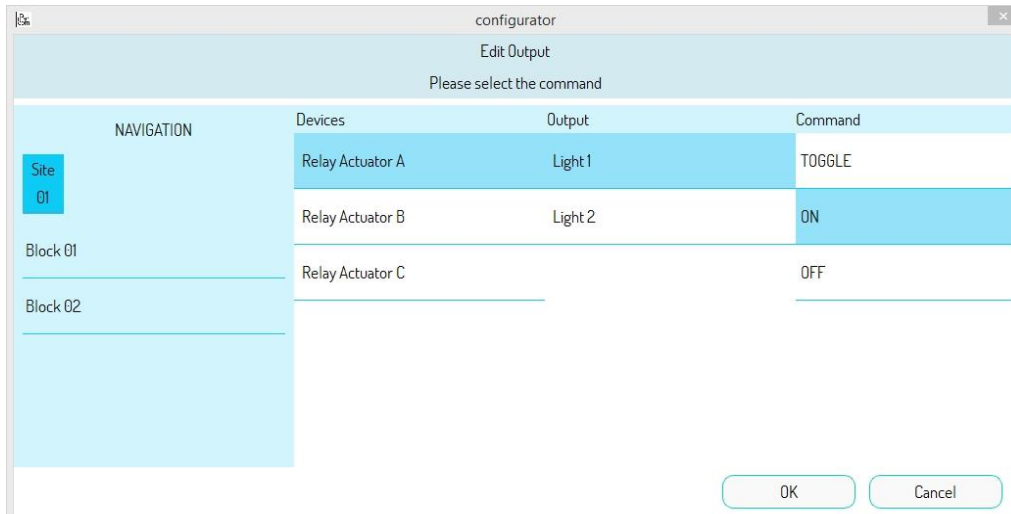


Figure 365: First output selection with scenario command

Press the "OK" button to add the first output to the group you are about to create:

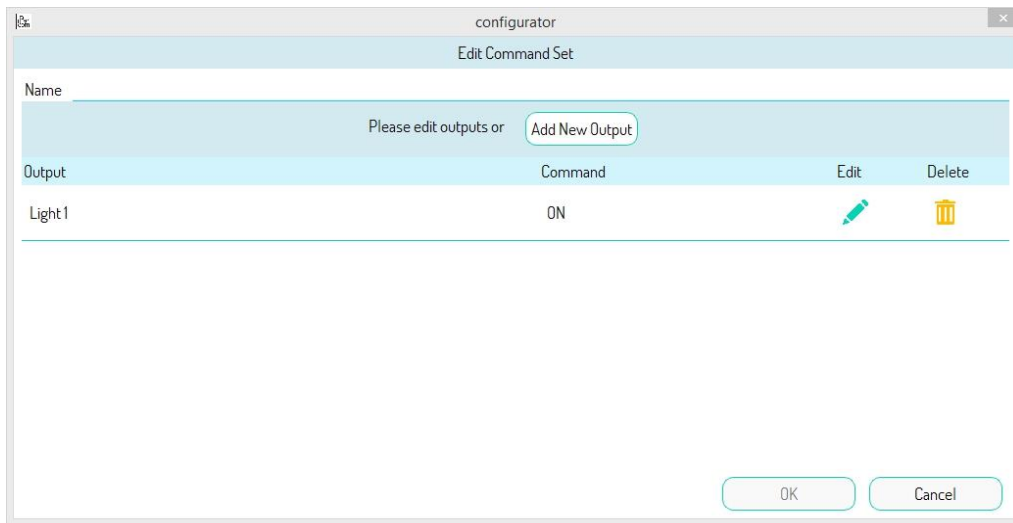


Figure 366: Adding the first output to the scenario

The buttons in the "Edit" and "Delete" columns can be used to modify or delete the output and the respective command (via confirmation pop-up), respectively.



Once an output has been added to the scenario, it is no longer re-submitted by navigating the topological structure of the system to add more outputs to the scenario.

After adding the other five outputs with their command and having given a meaningful name to the scenario, press "OK" to open the following screen:

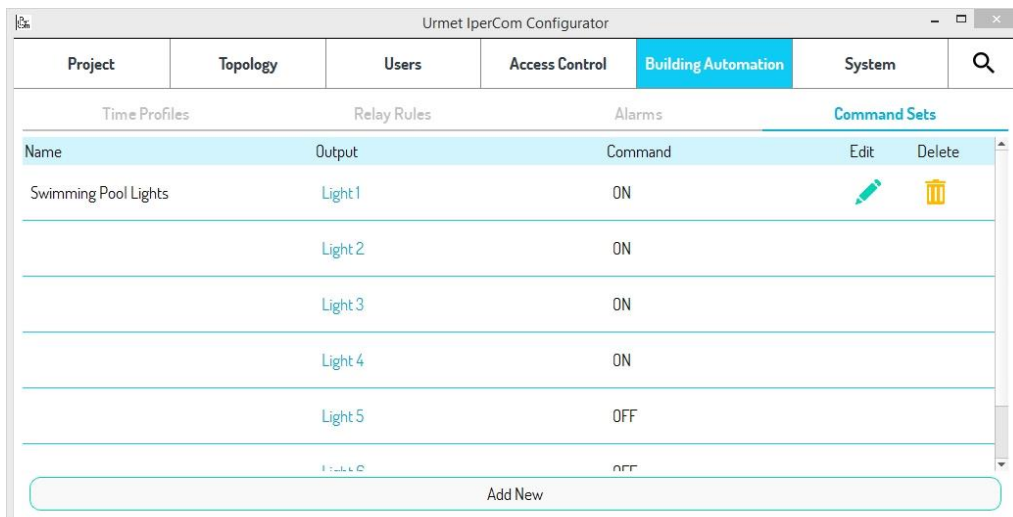


Figure 367: Scenario creation

The buttons in the "Edit" and "Delete" columns can be used to modify or delete the newly created scenario (via confirmation pop-ups), respectively.

At this point, if you want the input named as "Pool Lights On Input" to control the newly created group of outputs on a short press event (for example), go to the "Activation Rules" tab and follow the instructions in the previous paragraph with the only difference of selecting the "command set" when selecting the output:

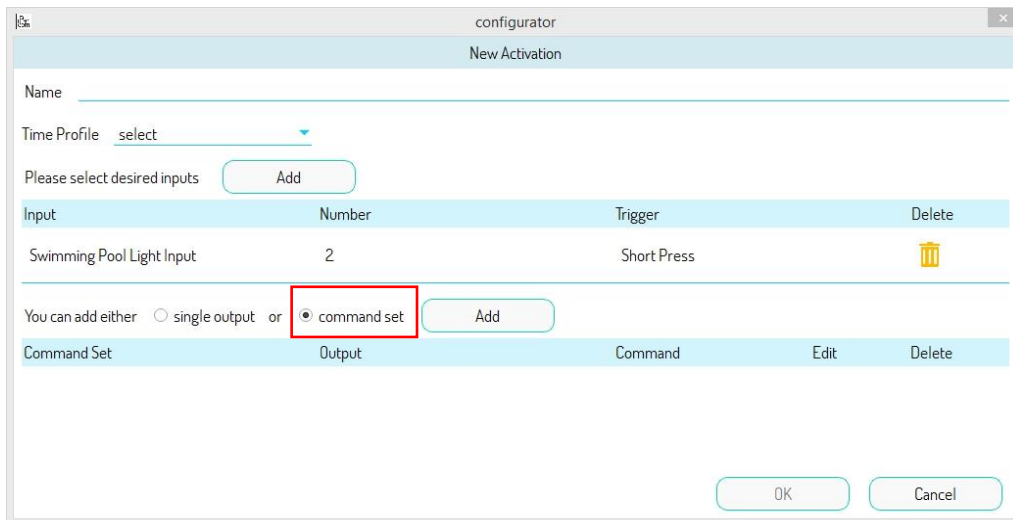


Figure 368: Adding a group of commands

Then, press the "Add" button to add the newly created group (by selecting it):

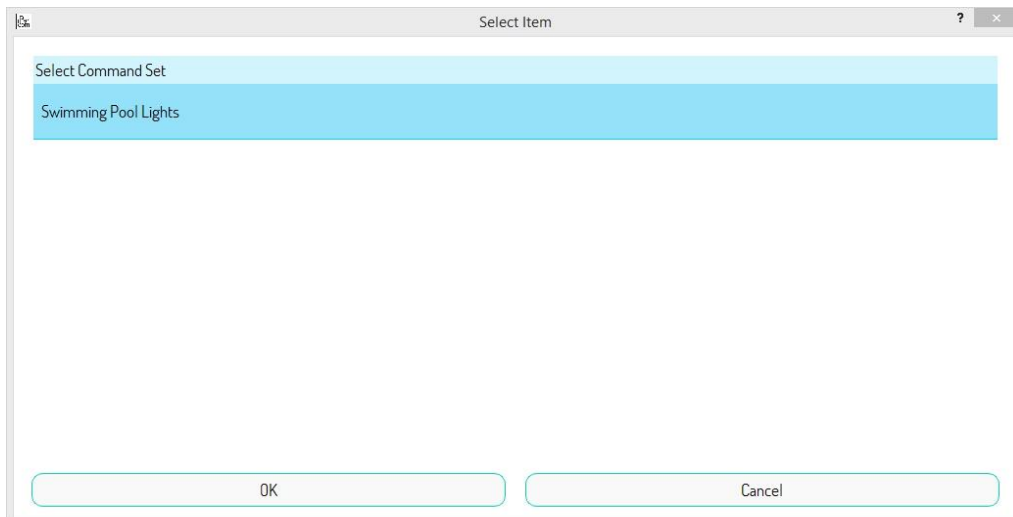


Figure 369: Selecting a group of commands



Then press "OK" to open this screen that summarises the choices made:



Figure 370: Selecting a group of commands

After giving a name to the activation, press the "OK" button to open the following screen:

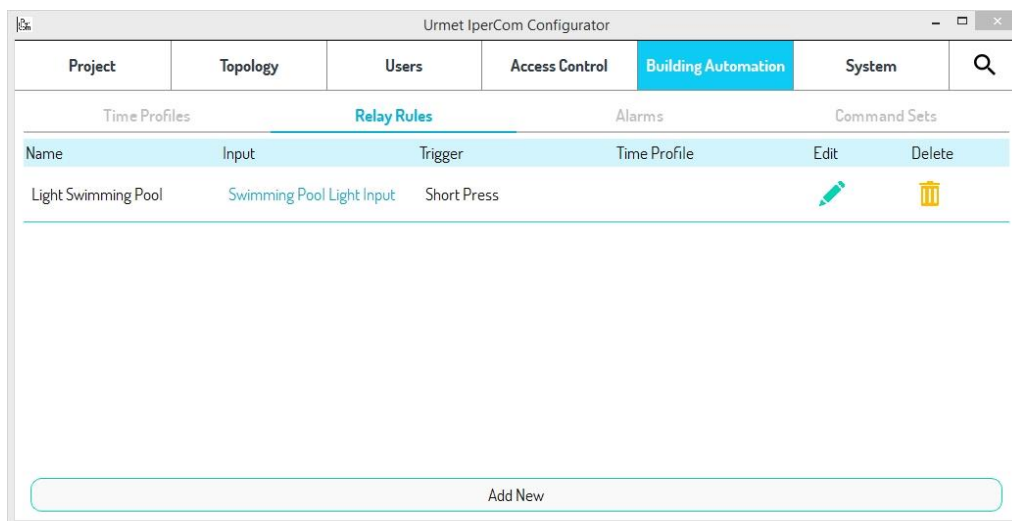


Figure 371: Activation with created group of commands



It is advisable to give a meaningful name to the created rule so that you can quickly identify that the concerned rule controls a group of outputs. The reference can be retrieved in all cases by pressing the "Edit" button.

The same scenario can be added when creating a topological activation rule or on a device, more precisely when adding outputs as shown in the following figure:

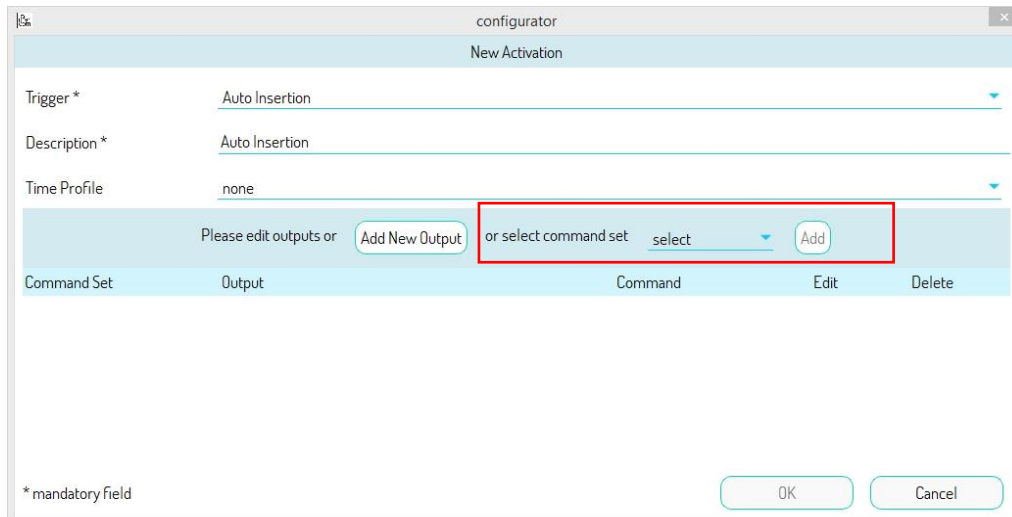


Figure 372: Activation with created group of commands

"Select" item can be used to choose the scenario, while the "Add" button allows you to add it to the rule you are creating.

### 7.1.5.9.3 Adding a time profile to the activation

Each activation created can be associated with a time profile, i.e. establish a time interval within which the activation is valid. The "Time Profiles" tab allows you to do this. The following page will appear:

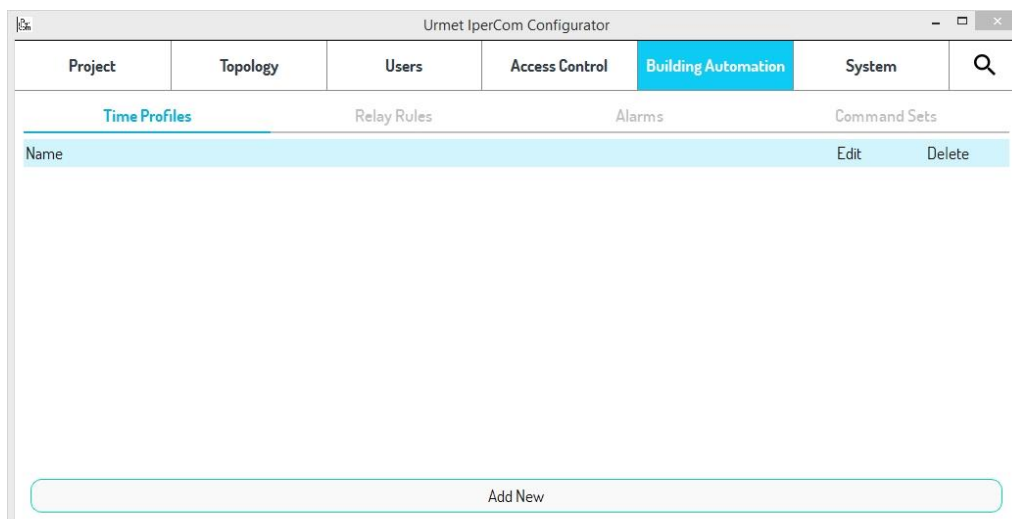


Figure 373: Page for creating a time profile

Press "Add New" to open the following page:

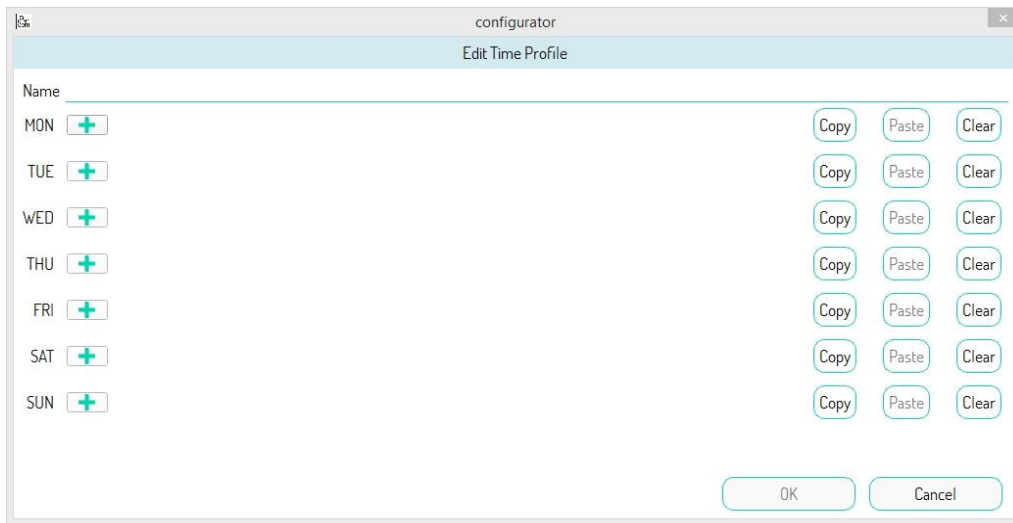



Figure 374: Adding a time profile

After having given a name to the time profile you want to create, the buttons  can be used to create a time interval for each day of the week within which the activation will be valid (through the following screen):

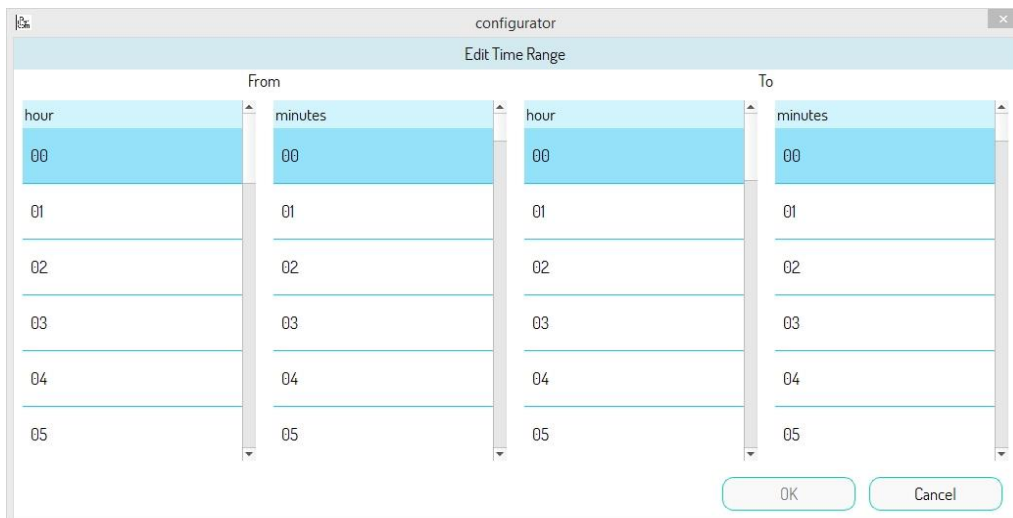


Figure 375: Creating a time profile

The scrolling menus in the figure above allow you to define the start and end of validity of the time profile for each day of the week. For example, if you want to activate a validity for Monday from 8:00 to 12:00, the result is as follows (after pressing the "OK" button):

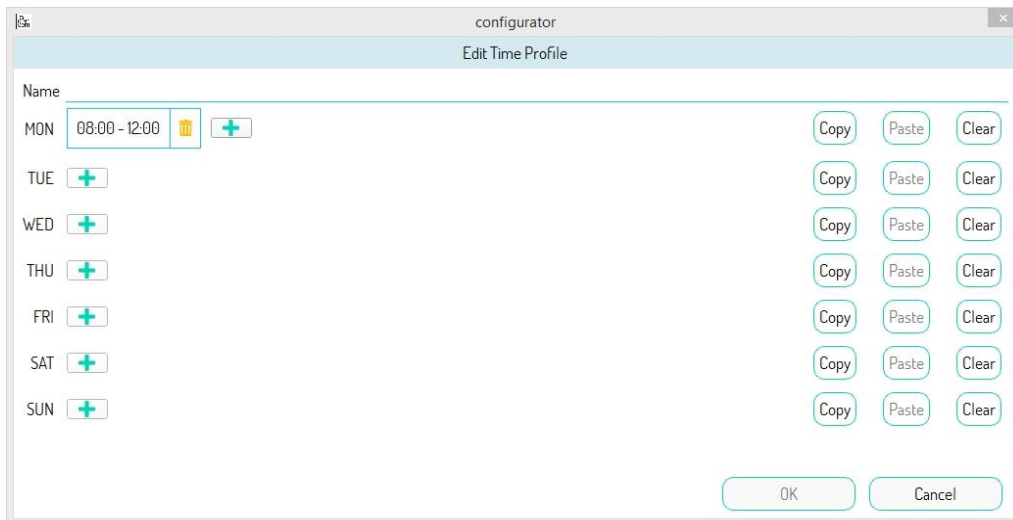


Figure 376: Time profile created for a day of the week

The "Copy" and "Paste" buttons allow you to quickly copy the time interval just created for all the other days of the week. You can press the "Copy" button on Monday which will enable the "Paste" buttons on the other days to do this. The following page will appear:

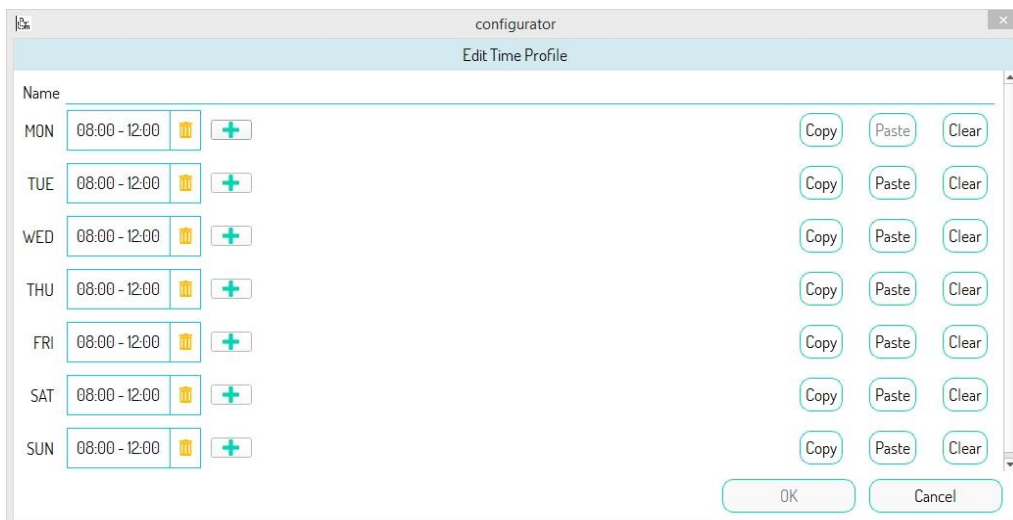


Figure 377: Time profile created for the entire week

The "Clean" button allows you to delete all previously created time intervals for one day of the week.

The  button allows you to delete a single time interval created.

Press the "OK" button to complete creating the time profile:

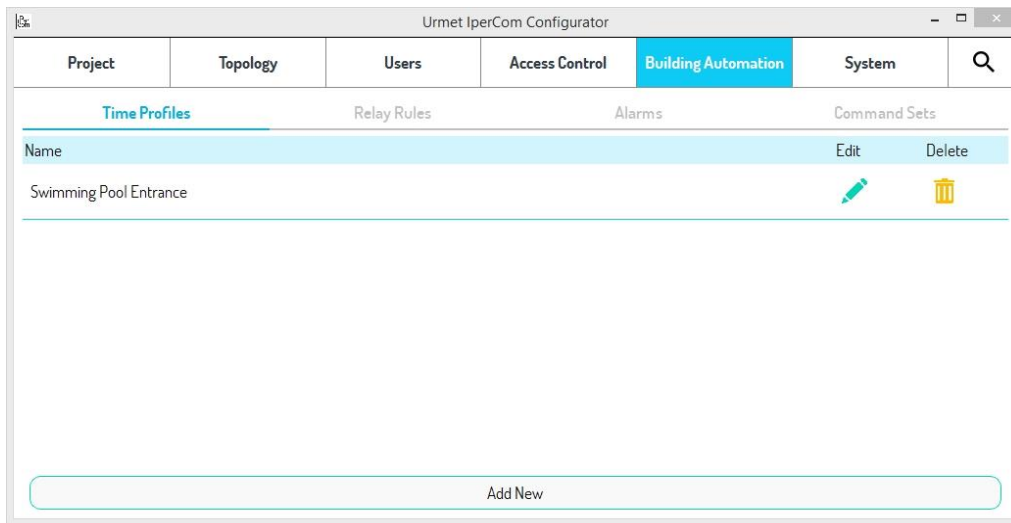


Figure 378: Saved time profile

The buttons in the "Edit" and "Delete" columns can be used to edit or delete data for each time profile, respectively (via confirmation pop-up).

At this point, in a previously created or new activation, the "Time Profile" drop-down menu allows you to add a time profile, as shown in the following image:

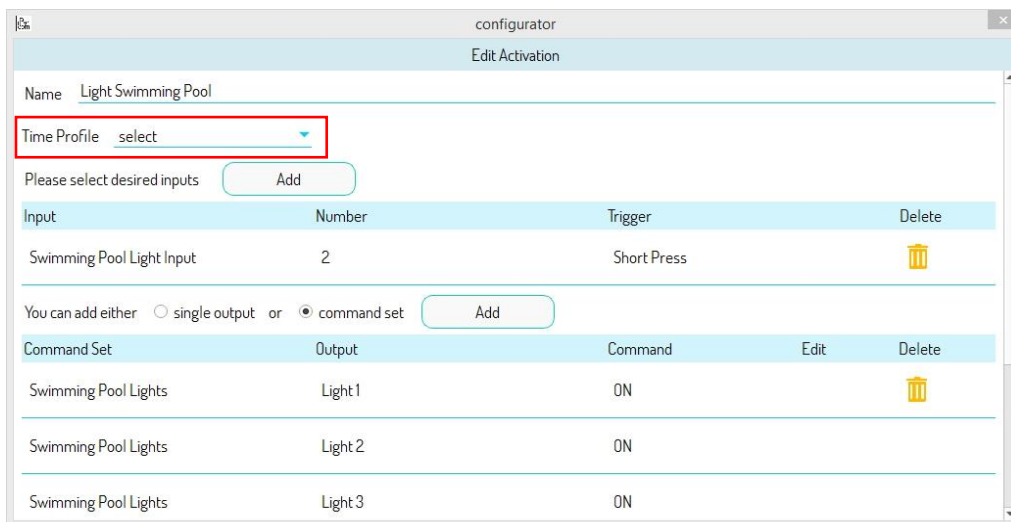


Figure 379: Time profile associated with activation

Press the OK button, to see the newly created activation with the associated time profile in the activation list:

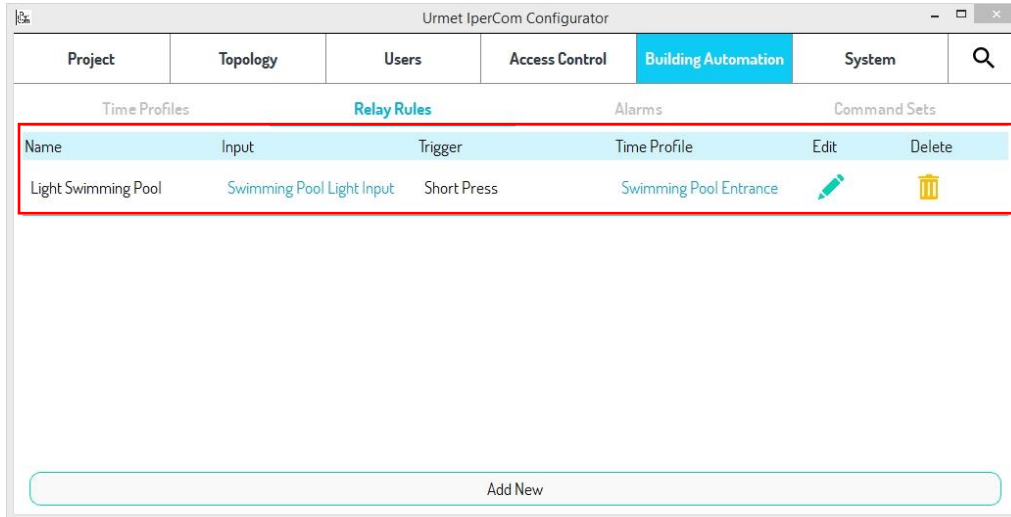


Figure 380: Time profile with activation

The buttons in the "Edit" and "Delete" columns can be used to edit or delete data for each activation, respectively (via confirmation pop-up).

#### 7.1.5.9.4 Sending alarms to the Switchboard via relay actuator inputs

It is possible to use the ON, OFF, long press and short press events to send one or more alarm signals to the *Switchboards* of the system through one or more sensors connected to the *Relay Actuator* inputs. The alarm signal is sent when the sensor generates the programmed event.

This can be used using the "Alarms" tab:

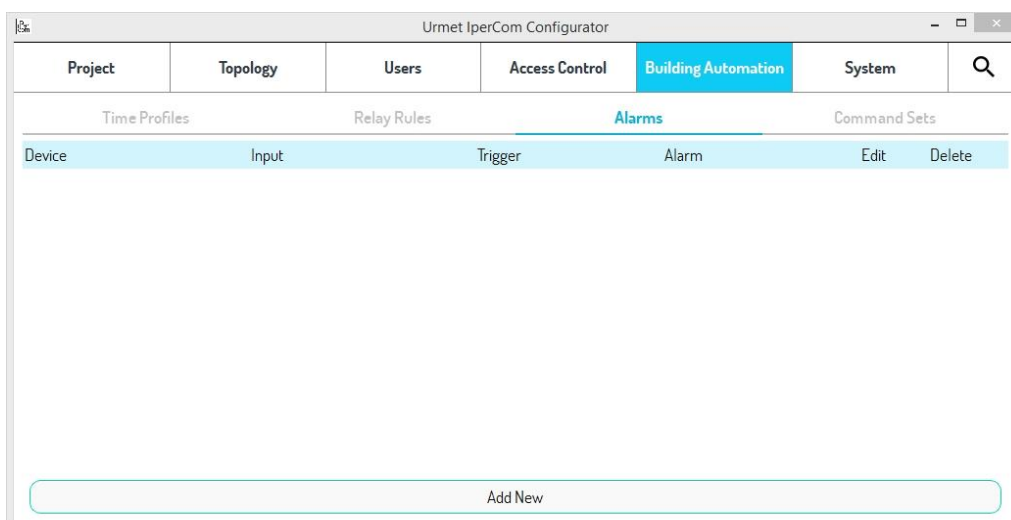


Figure 381: "Alarms" tab

Press the "Add New" button to open the following screen with all the available inputs of the various relay actuators (identified by their physical MAC address and a significant name):

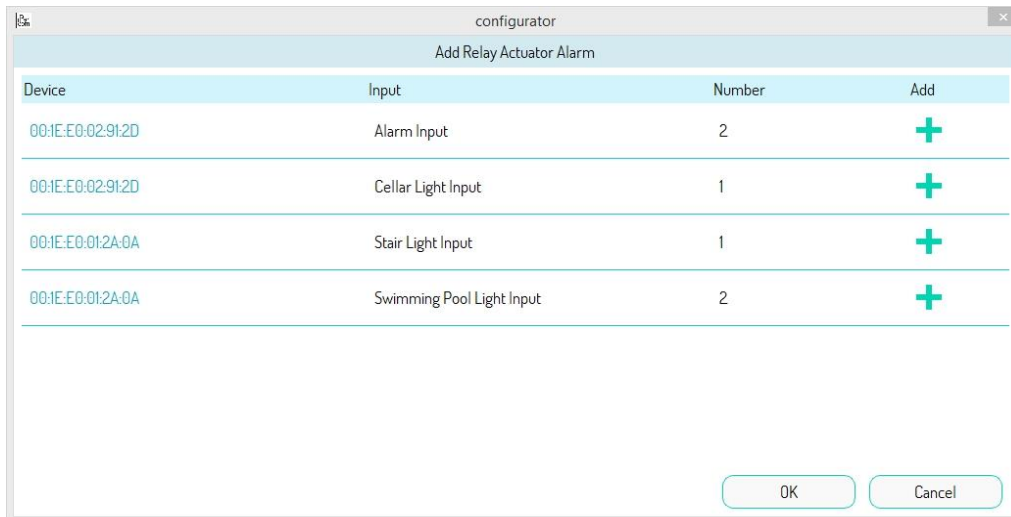


Figure 382: Inputs available for alarm generation

In this example, we will assume that the first input is reserved for alarm generation.

Press the button  to choose which event on this input generates the alarm. If the input has been configured in bistable mode ([APPENDIX A: Configuration parameters of IPerCom devices](#)), the possible events are the following:

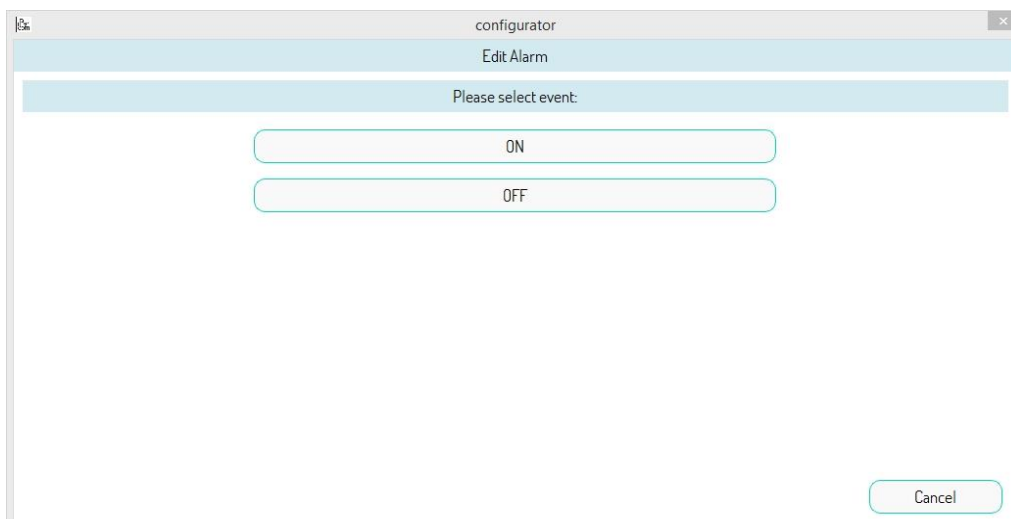


Figure 383: events available if the input is set to bistable mode

The *ON* and *OFF* events are used to generate instantaneous alarms. For example, if the input has been set to normally closed (paragraph [APPENDIX A: Configuration parameters of IPerCom devices](#)), a sensor connected to a port that is forced triggers an *ON* event and then generates an alarm.

If the input has been configured in monostable mode, the possible events are:

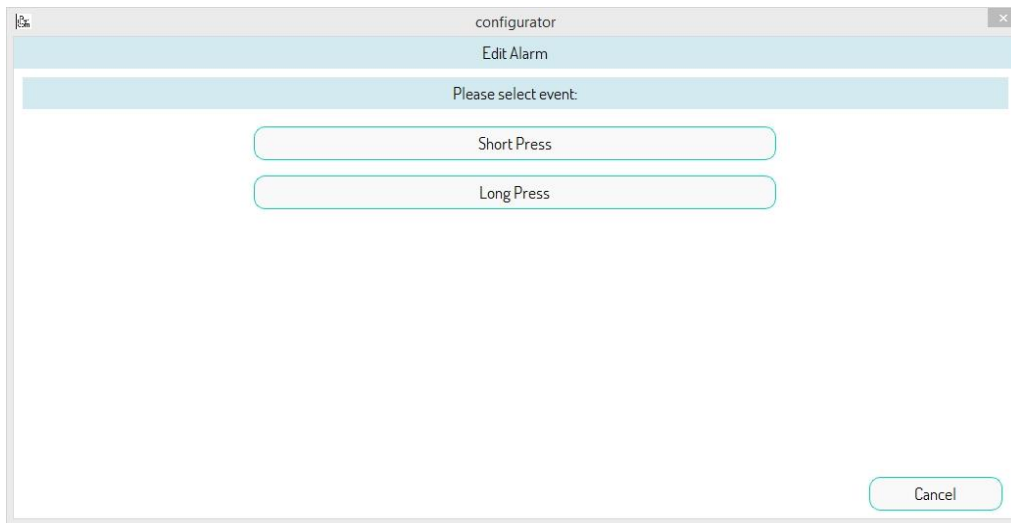


Figure 384: events available if the input is set to monostable mode

The *Short press* and *Long press* events are used to generate non-instantaneous alarms. For example, if the input has been set to normally closed, a sensor connected to a door that is left open for a time longer than the time set at the input triggers a *Long press* event and then generates an alarm.



*For each input it is possible to associate an alarm to only one of the 2 events (ON/OFF if the input has been set as bistable, Short Pressure and Long Pressure if it has been set as monostable). This means that if an alarm has been associated with the ON event of an input, no other alarm can be associated with the OFF event of the same input (and vice versa). The same applies to the other 2 events of Short Pressure and Long Pressure of another input.*

If the input has been configured in bistable mode and the "ON" event is selected, the following screen is displayed:

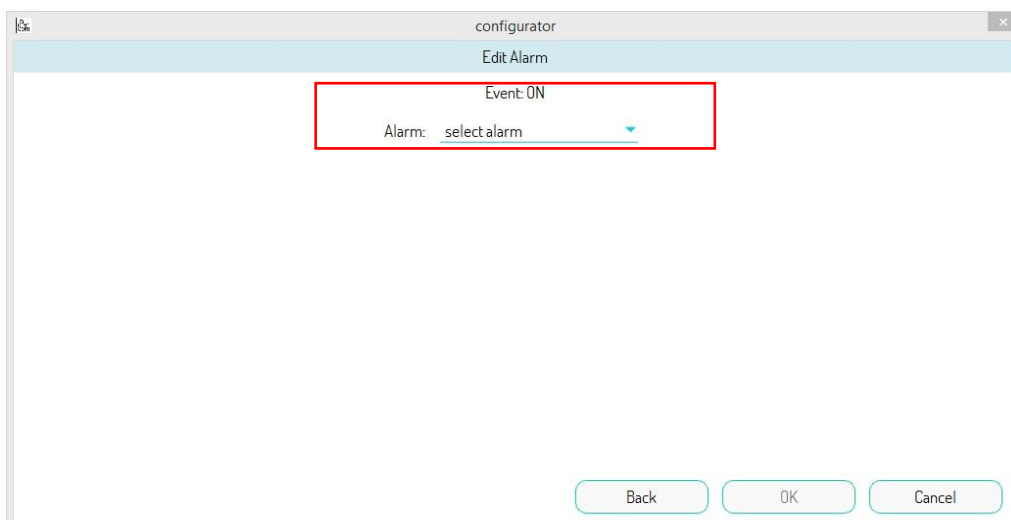


Figure 385: Choosing the alarm type



It is possible to select the alarm type to be sent to the Switchboard from the drop-down menu with the red box. The available alarms are listed below:

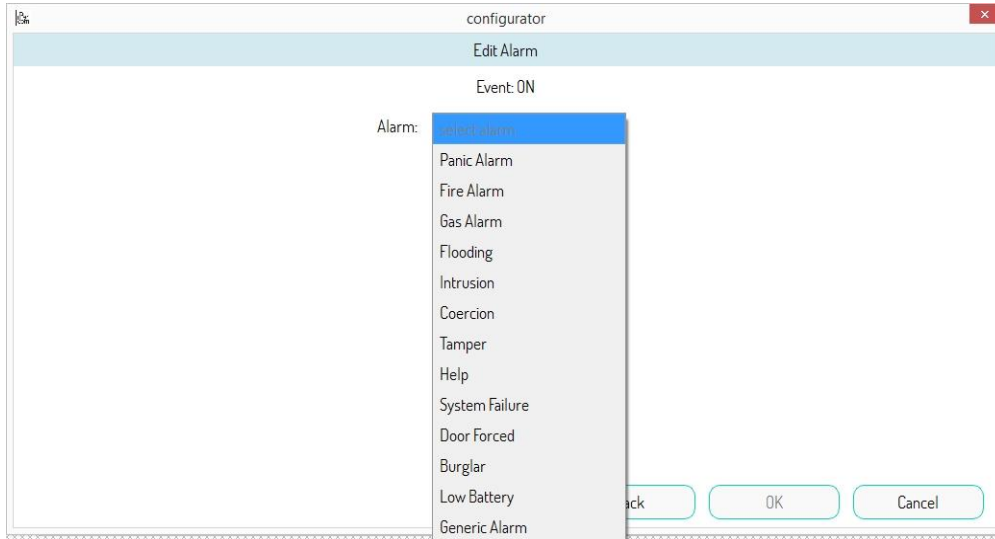


Figure 386: Available alarms

For example, if you select the "Door Forced" alarm, press the "OK" button to see the list of inputs on the screen. Then press "OK" again to see what you have just created:

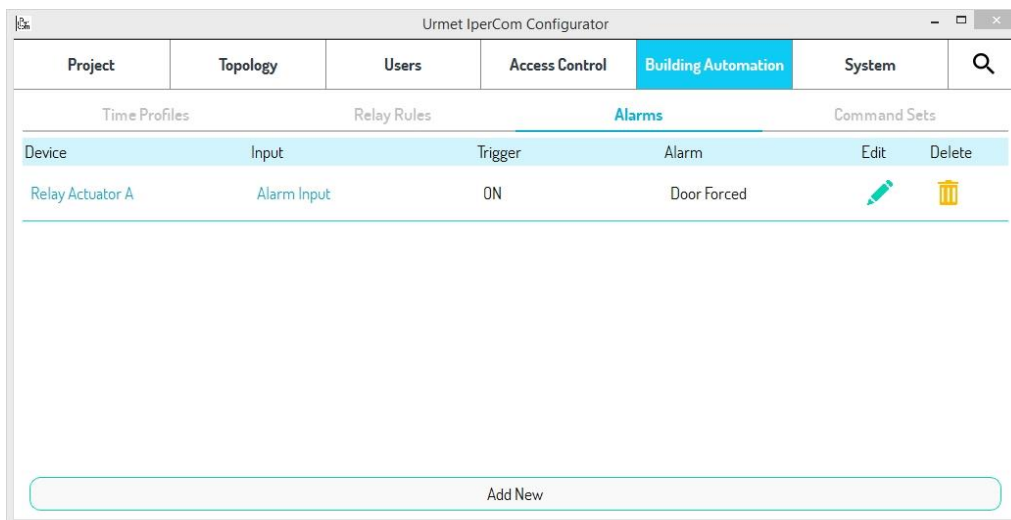


Figure 387: Alarm associated with the input

The buttons in the "Edit" and "Delete" columns can be used to edit or delete data for each alarm, respectively (via confirmation pop-up).



*A single input can generate an alarm and simultaneously activate one or more relay outputs.*

### 7.1.5.9.5 Creation of relay actuator activations and alarms

The activation and alarm generation rules seen in the previous paragraphs can also be created on the configuration page of the relay actuator in the section dedicated to inputs.

Note that the input programming method described in the previous paragraphs is only possible on relay actuators **with firmware version 3.04 or higher. If the firmware version is 2.07, the inputs are not programmable and therefore the following is not valid.**

The section relating to the inputs (both input 1 and input 2) of a *Relay Actuator* is as shown below (if no name has been given to the inputs yet):

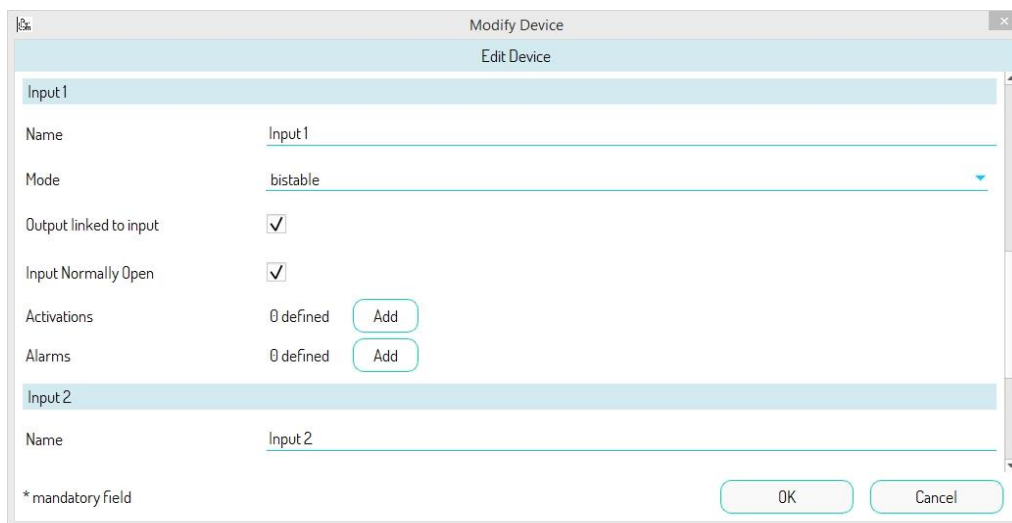


Figure 388: Input configuration of a relay actuator ver.3.04

The "Activations" and "Alarms" buttons can be used to create that described in the previous paragraphs but only for the concerned input. Press the "Activations" button to open the following page:

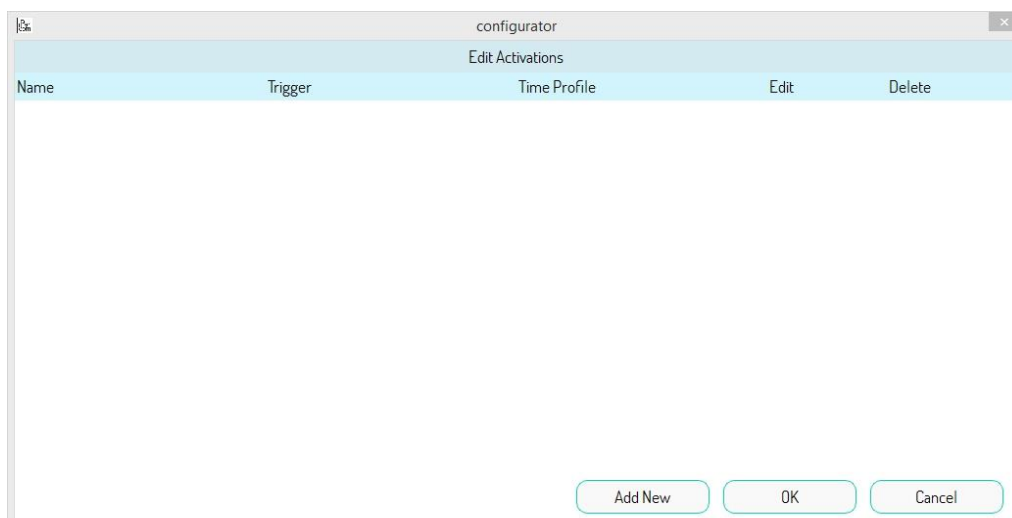


Figure 389: Adding relay actuator input activations

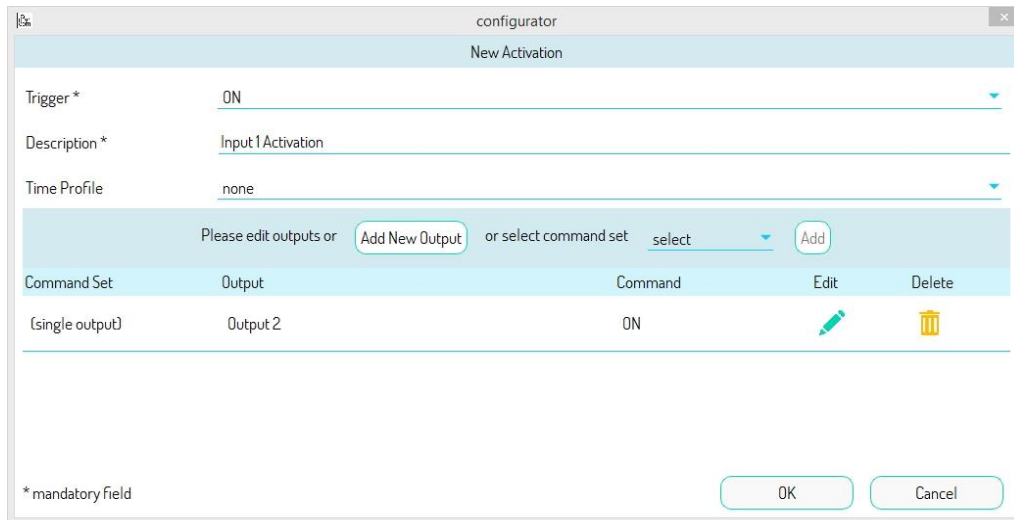
Press the "Add" button to open the following page:

Figure 390: Screen to create activation on a single input

The "Trigger" drop-down menu allows you to select the event to be associated with the input, in this case "ON" or "OFF":

Figure 391: Possible events on the input

After having selected an event (e.g. "ON") and given a meaningful name to the activation, associated it with a time profile if required and added one or more outputs, the following screen will appear:



configurator



New Activation

Trigger \* ON

Description \* Input 1 Activation

Time Profile none

Please edit outputs or [Add New Output](#) or select command set [select](#) [Add](#)

Command Set	Output	Command	Edit	Delete
(single output)	Output 2	ON		

\* mandatory field

[OK](#) [Cancel](#)

Figure 392: Event output settings

The result is what we saw in the previous paragraphs, as well as for the creation of alarms.

### 7.1.5.9.6 Schedules

Through the “Schedules” tab you can program on a weekly basis the behaviour of the outputs of the *Relay Actuators* (activation rules). A schedule may consist of one or more activation rules. Press the *Schedules* tab, to display the following page:

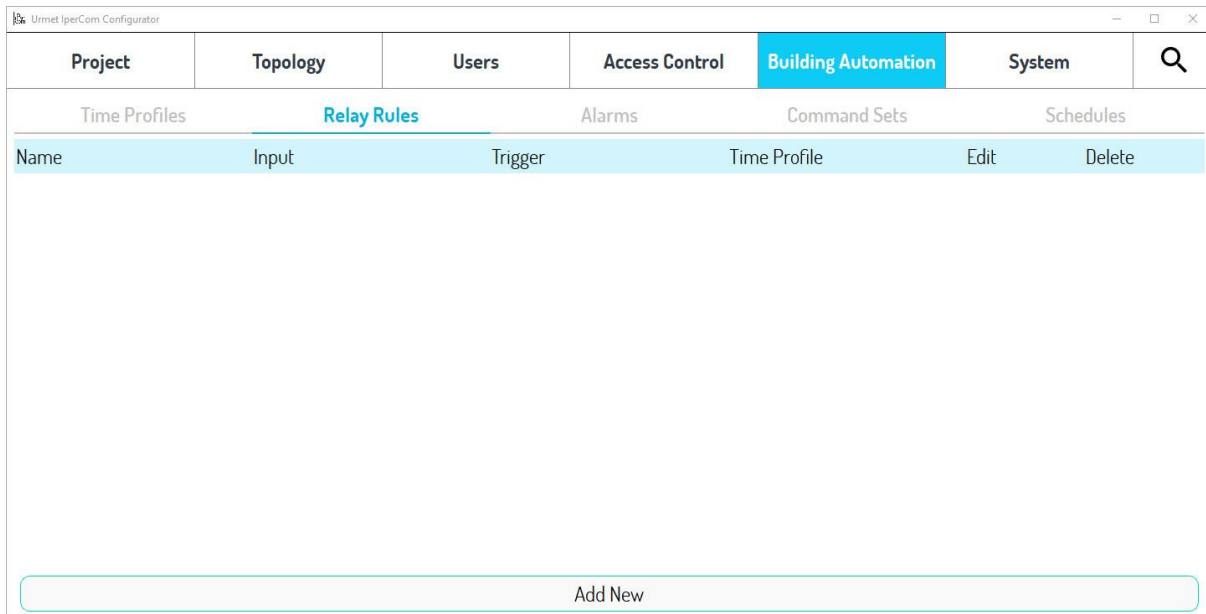



Figure 393: "Schedules" tab

By pressing the “Add” button the following page is displayed:



Figure 394: adding a schedule


The “Name” field allows you to assign a meaningful name to the schedule.

The buttons  allow you to add one or more activations for each day of the week and at a preset time.

Activations are created by choosing:

- one or more outputs of the *Relay Actuators*, setting the relative command;
- one or more groups of commands (scenarios) previously created.

The activations thus created are repeated on a weekly basis.

For example, if you press the button  on Monday, the following screen page will appear:

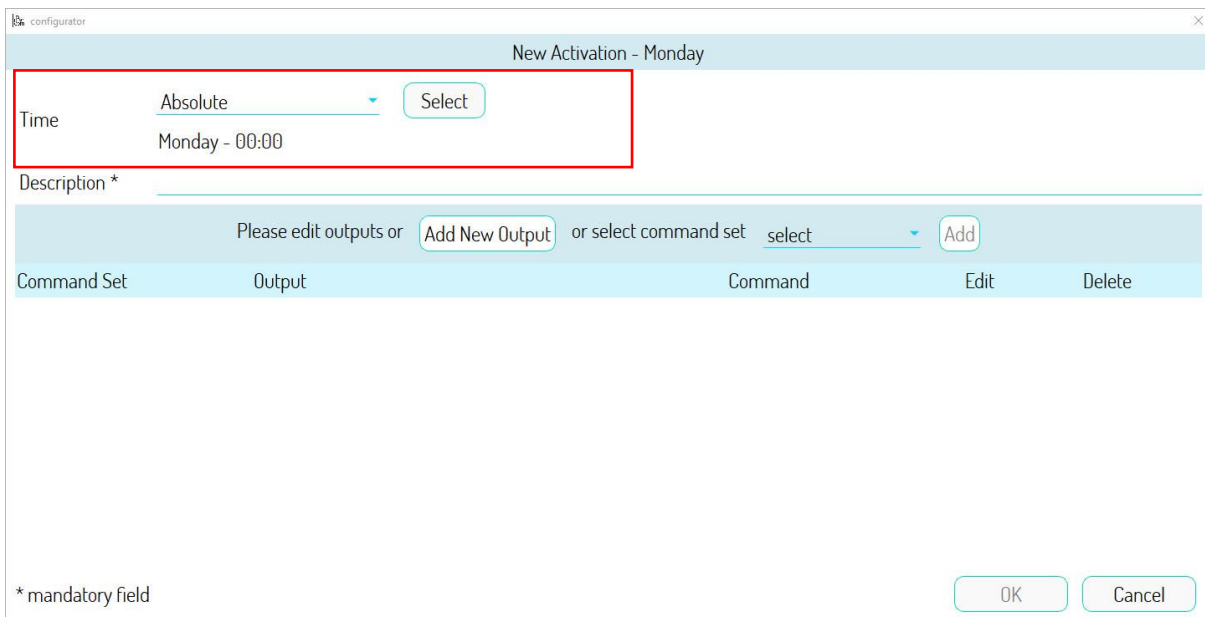


Figure 395: creating a schedule

In the "Time" section (red box) a drop-down menu allows you to choose the time at which to trigger the commands and/or scenarios according to the items below:

- "*Absolute*", to choose a time consistent with the time set on the system;
- "*Sunrise*", to choose a time that coincides with the sunrise of your geographical location;
- "*Sunrise + offset*", to choose a time that coincides with the sunrise of your geographical location to which a time delta is added;
- "*Sunrise - offset*", to choose a time that coincides with the sunrise of your geographical location from which a time delta is subtracted;
- "*Sunset*", to choose a time that coincides with the sunset of your geographical location;
- "*Sunset + offset*", to choose a time that coincides with the sunset of your geographical location to which a time delta is added;
- "*Sunset - offset*", to choose a time that coincides with the sunset of your geographical location from which a time delta is subtracted.



To set the time to sunrise and sunset (corresponding to your geographical location), see the paragraph [Sunrise/Sunset Settings](#) of the chapter on system parameters.

Press the "Select" button to open a screen page where you can choose the absolute time or the offset (in hours and minutes) to associate with the sunrise or sunset:

Figure 396: choice of absolute time or offset to associate with sunrise or sunset

Below are 3 examples of how the "Time" section appears, if you choose in order an absolute time (7:00 am), a time referred to sunrise in Milan and a time referred to sunrise in Milan with one hour offset:

Figure 397: absolute time

Figure 398: sunrise set to Milan

Figure 399: sunrise set to Milan with one hour offset

The "Description" field allows you to give a meaningful name to the time activation you are creating.

The "Add a New Output" button allows you to add one or more outputs with the relative command to the activation you are creating.

Press this button and position on the topological node of the *Relay Actuator*, select the desired device (if there are more than one *Relay Actuators*), then choose the output and set the relative command:

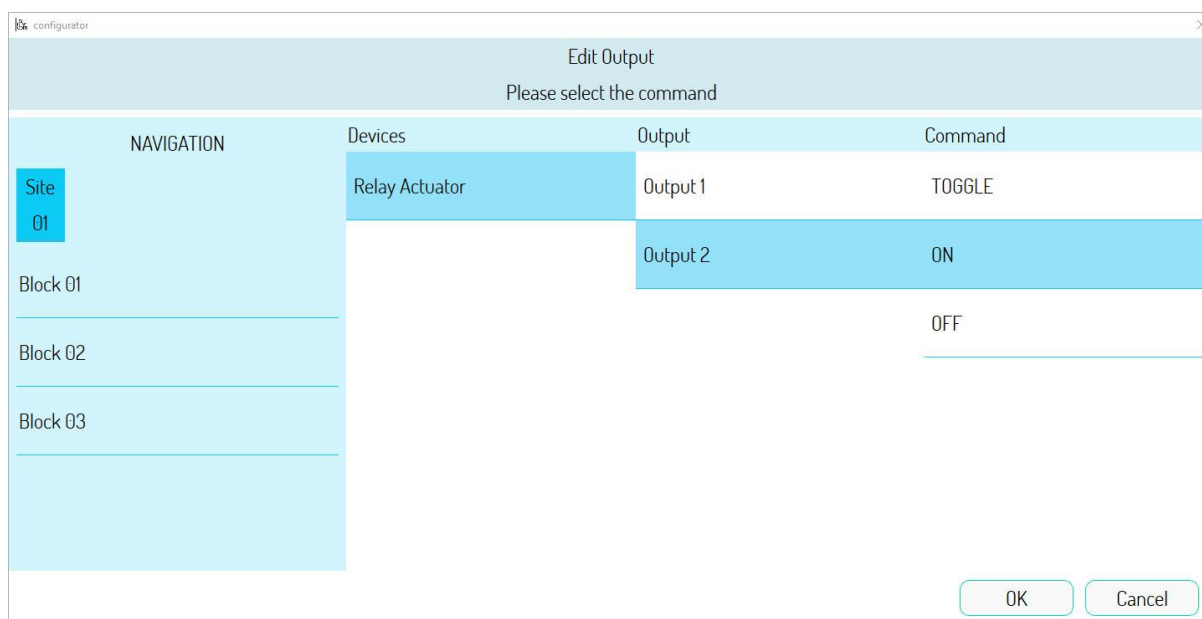



Figure 400: selection of a Relay Actuator output

The commands available depend on how the output has been configured (whether monostable or bistable). In case of monostable output commands "ACTIVATE" and "DEACTIVATE" are present, in the other case the available commands are "ON", "OFF" and "TOGGLE". For further details, see paragraph [APPENDIX A: Configuration parameters of IPerCom devices](#).

 The "DISACTIVATE" command in monostable mode is present only on the Relay Actuator 1060/84 v. 4.05 starting from version 2.1.0 of IPerCom.



Press the "OK" button to add the output selected with the relative command, as shown in the following (by way of example) figure:

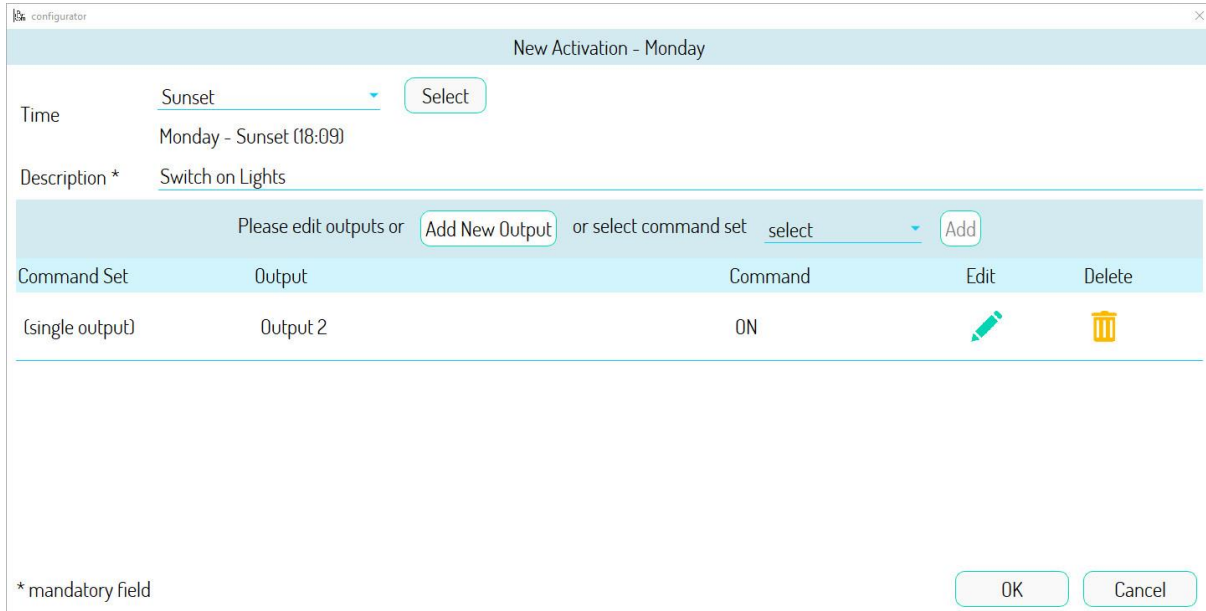


Figure 401: list of outputs associated with the schedule

It is possible to associate different outputs to the same activation by pressing "Add a new output" and repeating the above steps. As they are single outputs, the "Scenario" column shows the "single output" in brackets. It is also possible to add groups of commands previously created through the "Automation" and "Scenarios" tabs (see dedicated paragraph). In this case the "Scenario" column shows the name given to the previously created group of commands.

When Monday activations are configured, press the "OK" button to display the following screen page:

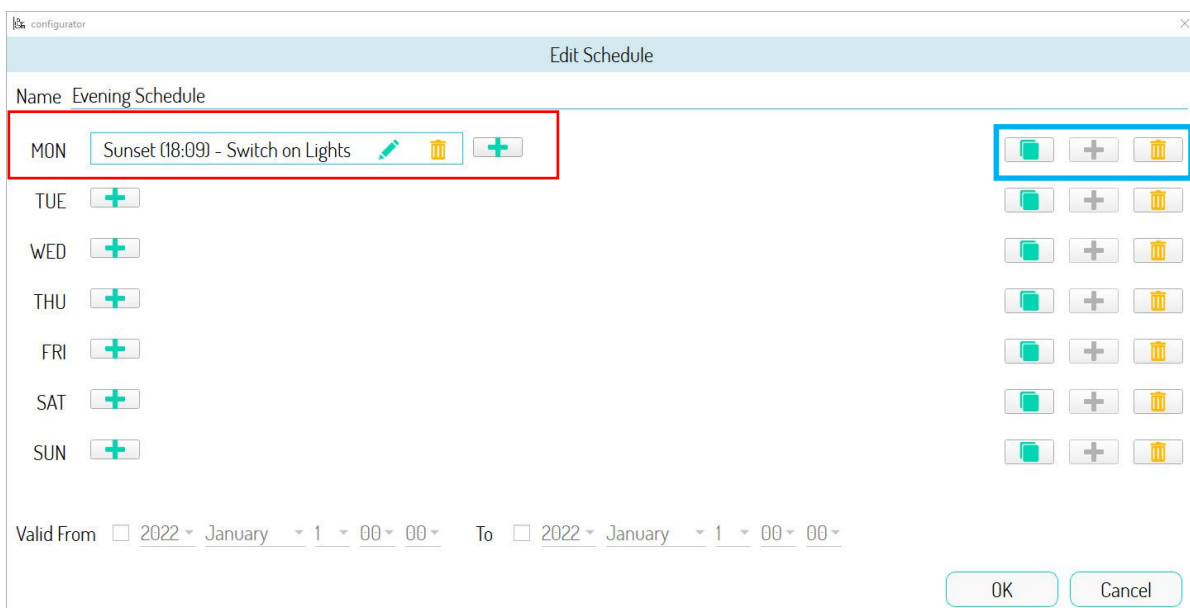







Figure 402: Monday schedule completed

The buttons in the red box allow you to:

- modify the activation just created (button );
- delete the activation just created (button );
- add another activation for the same day ().

The  ("Copy") and  ("Paste") buttons in the blue box allow you to copy the activations you have just created to the other days of the week: in fact, if you press the "Copy" button on Monday, the "Paste" buttons of the other days will be enabled, allowing you to do the above. The screen displayed is as follows:

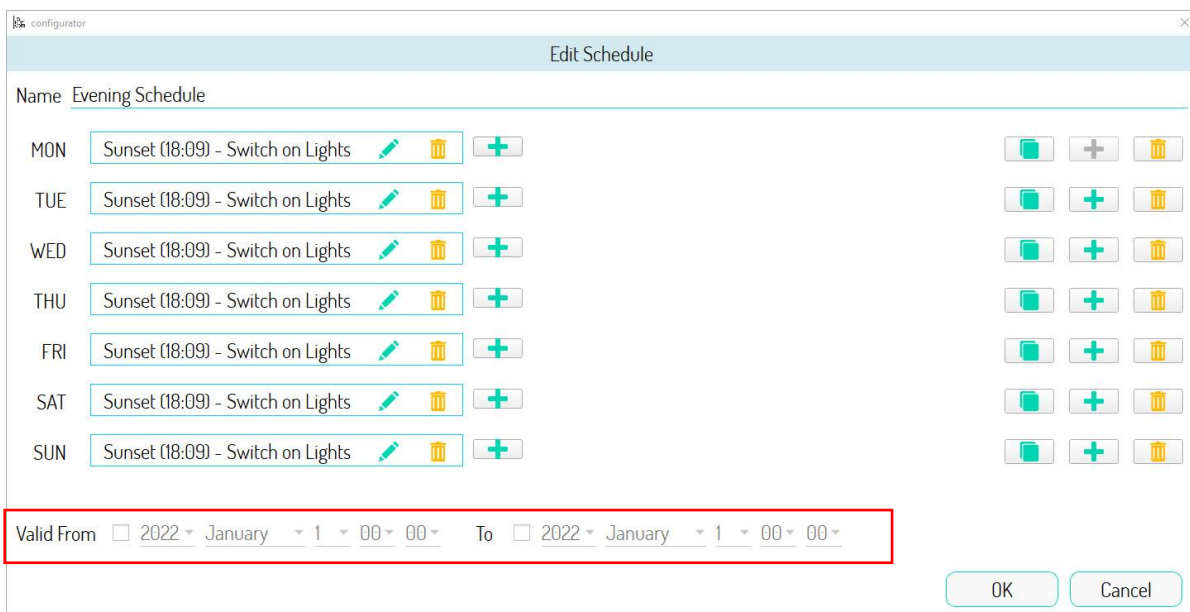



Figure 403: scheduling for the entire week

Finally, the button  (in the blue box) allows you to delete all the activations created in a single day.

You can also assign (in the red box) a time validity to the schedule you just created, by selecting the "Valid From" and "To" fields and choosing a year, day, month, and time for both.

By pressing the "OK" button, the schedule is saved and added to the schedule list:

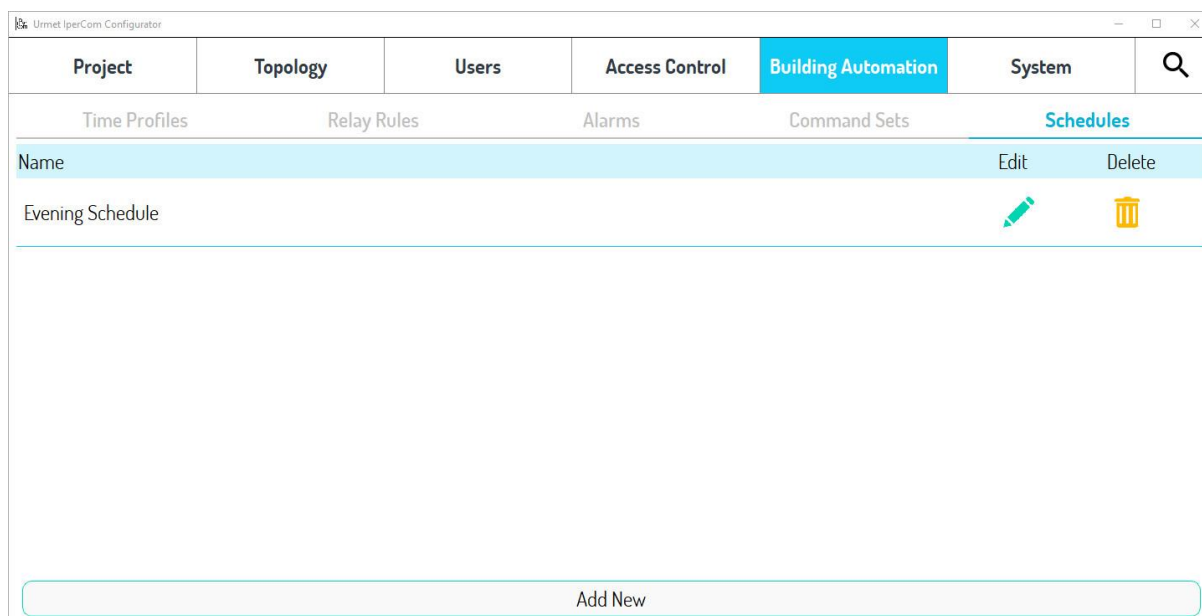


Figure 404: saved schedule

The buttons "Edit" and "Delete" allow you to modify the data or delete each schedule created, respectively (through confirmation pop-up).

### 7.1.6 Gate contact used as output of a Relay Actuator

For activation rules it is possible to use the gate contact of any calling station as a relay output (in addition to the relay outputs of 1060/84 *Relay Actuator* and the 1060/37 *Lift Interface* devices). The calling stations that allow the gate contact to be used as the output of a relay actuator are:

- *Entry Panel 1060/71-74-75-78;*
- *Entry Panel 1060/21-33-34;*
- *Call Module 1060/12-13-17-18-23;*
- *Modular Calling Station with 1060/48.*

To use the gate contact of a calling station as relay output of an actuator, from the *configurator* it is necessary to press the *Edit* button of the *Call Module 1060/12-13-17-18-23* (for example):

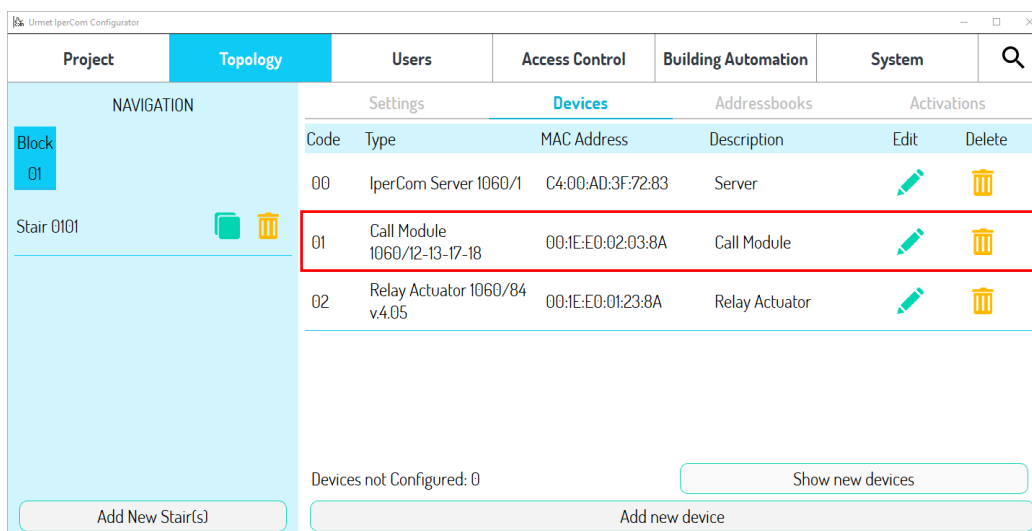


Figure 405: gate contact to be set as the output of a relay actuator

The page relating to the configuration parameters of the *Call Module* opens. In the section relating to the **Gate**, the "Enabled" field must be set to the value "Relay actuator", as shown below:

The screenshot shows a window titled "Edit Device" with a "Gate" section highlighted by a red box. The "Enabled" dropdown menu is set to "Relay Actuator". The "Name" field contains "Gate as Relay Actuator" and the "Gate Time (s) \*" field contains "3". Below the "Gate" section is a "Settings" section with the following options:

- Concierge button:
- Infrared:
- LEDs:
- Keyboard LEDs:  (with a slider)
- Call Feedback Tone:  (with a slider)
- Button feedback tone:  (with a slider)

At the bottom right of the window are "OK" and "Cancel" buttons. A note at the bottom left states "\* mandatory field".

Figure 406: gate contact used as output of a relay actuator

The following fields are shown in automatic way:

- "Name", that allows to give an appropriate name to the output;
- "Gate Time (s)", (from 1s to 90s) which allows to configure the relay output in monostable mode only;

At this point, if you want to create an activation rule linked to a topological event (for example a panic alarm from an apartment station), the following screen appears:

The screenshot shows a window titled "New Activation" with the following fields:

- Trigger \*: Panic Alarm
- Description \*: Activation for Panic Alarm
- Time Profile: none available

Below these fields is a section with the text "Please edit outputs or" followed by an "Add New Output" button, "or select command set" followed by a "select" dropdown menu, and an "Add" button. Below this is a table with the following columns: Command Set, Output, Command, Edit, and Delete.

At the bottom right of the window are "OK" and "Cancel" buttons. A note at the bottom left states "\* mandatory field".

Figure 407: panic alarm topological event

Pressing the "Add a New Output" button, both the outputs of any *Relay Actuators* and the relay output of the gate of the *Call Module* are displayed:

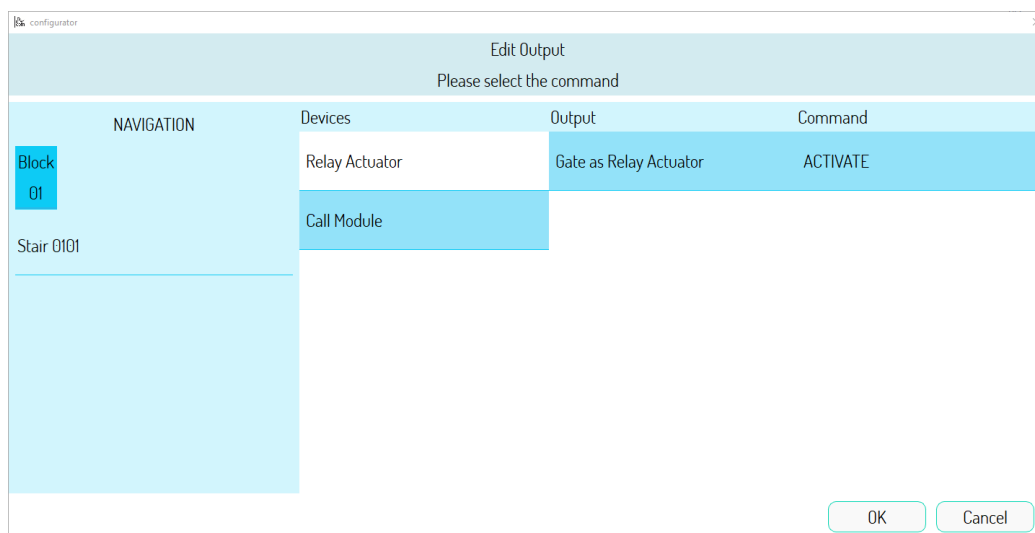


Figure 408: gate contact used in the activation rule

By pressing the "OK" button, the activation is correctly created.

### 7.1.7 Remote relay functions, remote entrance hall button and remote sensor

The remote relay function, available on devices such as *Call Module 1060/12-13-17-18-23*, *Entry panel 1060/33-34-71-74-75-78*, *Entry panel 1060/21*, *Modular Entry Panel with 1060/48*, *Key Reader 1060/45* and *Key Reader 1060/86*, allows you to remotely control the outputs that operate the pedestrian door and the driveway (if any) on those of a **Relay Actuator 1060/84 with firmware version 4.05 or higher**. This increases the security level of the access control: if, for example, the *call module* and the relevant output that drives the pedestrian door are tampered with to open the access point in question, this would not lead to the desired result, since the output that controls the access point opening is located in a completely different area, i.e. beyond the door that has to be opened. In addition to the pedestrian door, it is also possible to remotely control the entrance hall button by using one of the inputs of the *Relay Actuator 1060/84* (with firmware version 4.05 or higher), to further increase the security level at the access point in question.

In addition to the pedestrian door (and driveway if present) you can also remotely control:

- the pedestrian door entrance hall button;
- the door sensor (left open) of the pedestrian passage.

In both above cases, however, the inputs of the *Relay Actuator 1060/84* are used **(always with firmware version 4.05 or higher)**.

To implement these 3 features, in addition to firmware version 4.05, the *Relay Actuator* must also meet the conditions below:

- remote control of pedestrian door or driveway: have at least one output set in monostable mode, not connected to the input and not used in any other activation rule;
- remote control of entrance hall button: have at least one input set in monostable mode and not used in any other activation rule;
- remote control of door open sensor: have at least one input set in bistable mode, normally closed and not used in any other activation rule.



*To set an output to monostable or bistable mode and to have an input not connected to the output, it is necessary to go to the Relay Actuator configuration page (APPENDIX A: Configuration parameters of IPerCom devices).*

If you want to implement this service on the pedestrian door of a *Call Module* (for example), it is necessary to go to the configuration page of the device in question, i.e. open the *configurator* on the "Topology" tab, then on the "Devices" tab. A screen with the list of devices present on the system on the selected node is displayed:

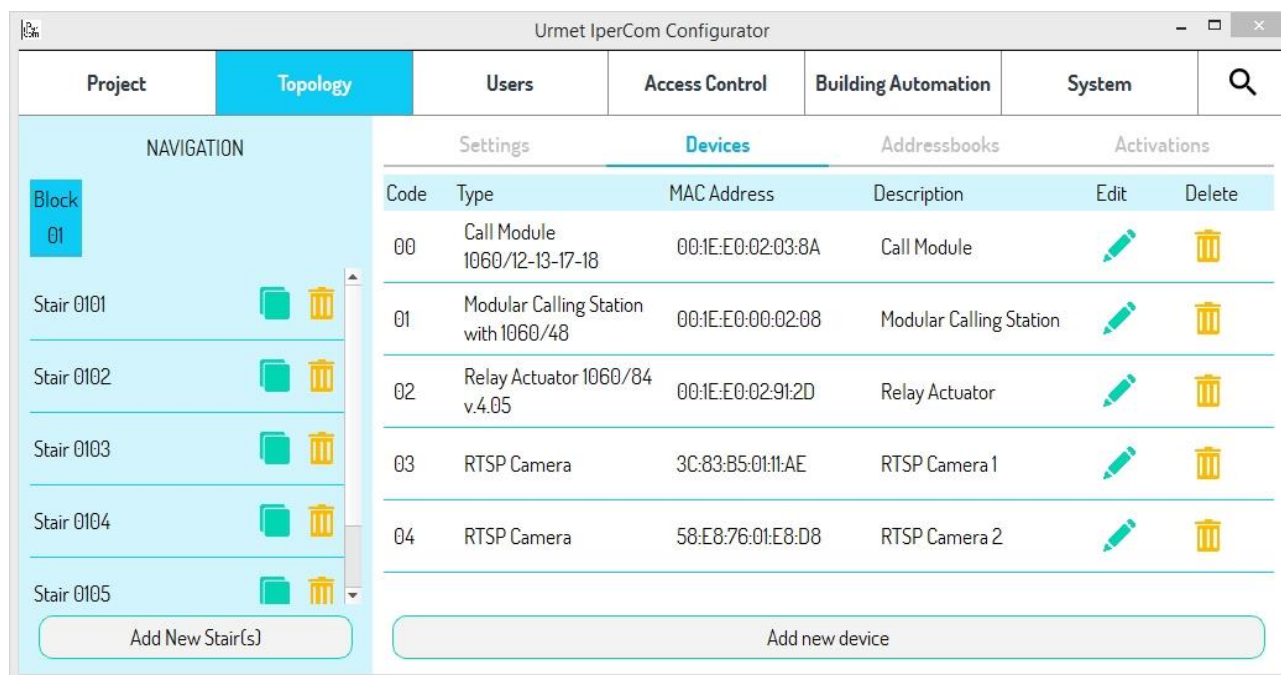


Figure 409: Devices present on the site node

By pressing the modification button on the *Call Module*, the remote relay function setting part is displayed in the pedestrian door section, as shown below:

Remote Relay	None	Select	Clear
Remote Sensor	None	Select	Clear

Figure 410: Remote Relay and Remote Sensor sections for the pedestrian door



About the “Remote Relay” item, the “Select” button allows you to navigate the topological structure of the system, position on the topological node of the *Relay Actuator 1060/84 v. 4.05* that you want to use to remotely control the pedestrian passage, select one of the 2 outputs, then press “OK” as shown in the figure below to confirm:

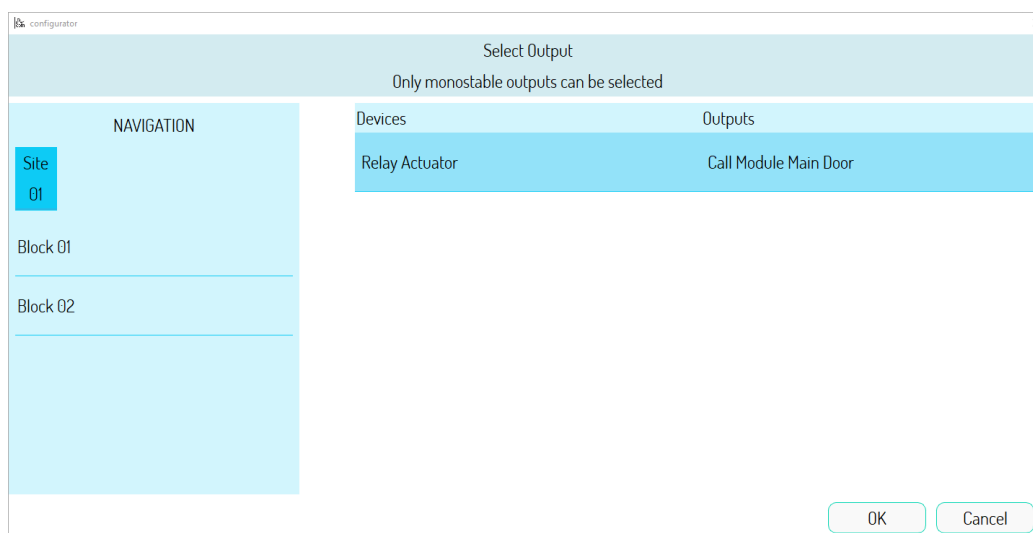


Figure 411: Output selection Relay actuator for pedestrian door remote control

After pressing the “OK” button, the remote relay function section is displayed as below:

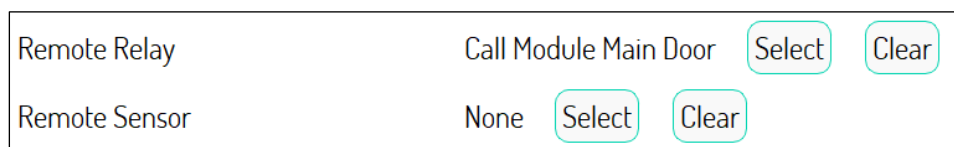


Figure 412: remote pedestrian door






The “Clear” button allows you to delete what you have done.



*It is recommended to give a meaningful name to the outputs of a Relay Actuator so that they are immediately identifiable. The default names that the configurator assigns are in fact composed of the last 6 hexadecimal digits of the MAC address followed by the name **Output 1** or **Output 2** (for example **01:14:03 - Output 1**). If there are several Relay Actuators it is difficult to identify which output must implement the remote relay function. The same applies to the name assigned to the Relay Actuator device.*

In the same way, it is possible to remotely control the pedestrian door entrance hall button or the open-door sensor with the only difference that, instead of selecting the output of a *Relay Actuator*, it is necessary to select an input. The remote entrance hall button will activate (for a pre-set time) the same output used to remotely control the pedestrian passage.

The “*Remote Button*” item for hall button is always found on the configuration page of the *Call Module* in the section relating to the hall button.

-  *If the pedestrian door is remote-controlled, the relevant entrance hall button, if not remote-controlled, does not activate the output of the Relay Actuator connected to the pedestrian door.*
-  *The choice of the outputs or inputs through which you can remotely control the pedestrian door or driveway or the entrance hall button can also be made on the Lift Interface device when this is used in Relay Actuator mode.*
-  *The relay output used to remotely control the pedestrian door of any call station cannot be used for other activation rules.*
-  *The remote setting of an entrance hall button must always be associated with the remote setting of the relevant pedestrian passage.*
-  *The remote setting of a driveway is done in the same way as for a pedestrian passage, the only difference is that for the driveway there is no entrance hall button and the relevant door open sensor.*

### 7.1.8 User management

In the four possible plant models (*Villa Kit*, *Single Stair*, *Multiple Stairs*, *Multi Block*) the management of the users is implemented in the relevant "Users" tab, as shown in the following figure:

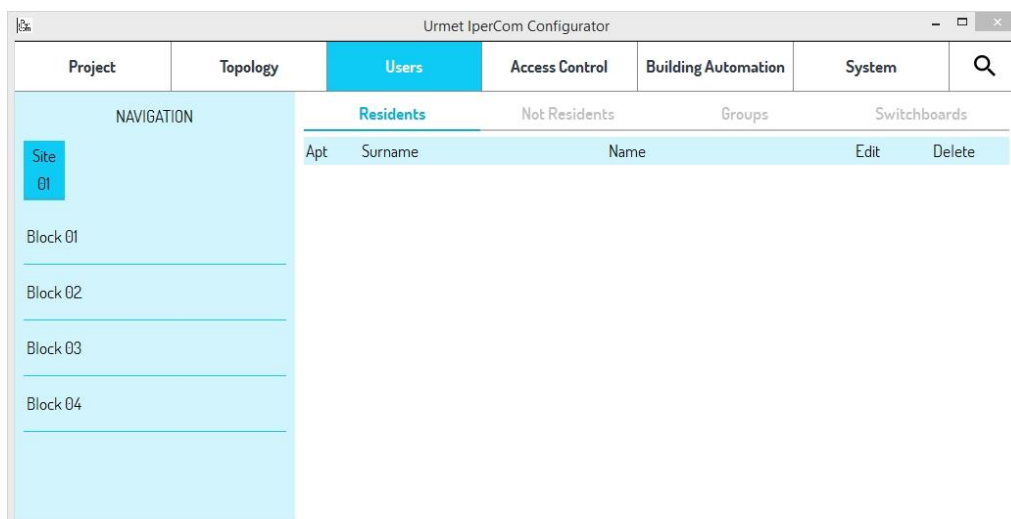


Figure 413: "Users" tab

The screen shows 4 different types of users, described in the dedicated paragraphs: "[Residents](#)", "[Not residents](#)", "[Groups](#)", "[Switchboards](#)".

#### 7.1.8.1 Residents

Residents are associated with the apartments, so to be able to add residents it is necessary to access the navigation window on one of the created apartments.

Let us suppose you want to create a *Multi Block* project, as shown in the following figure:

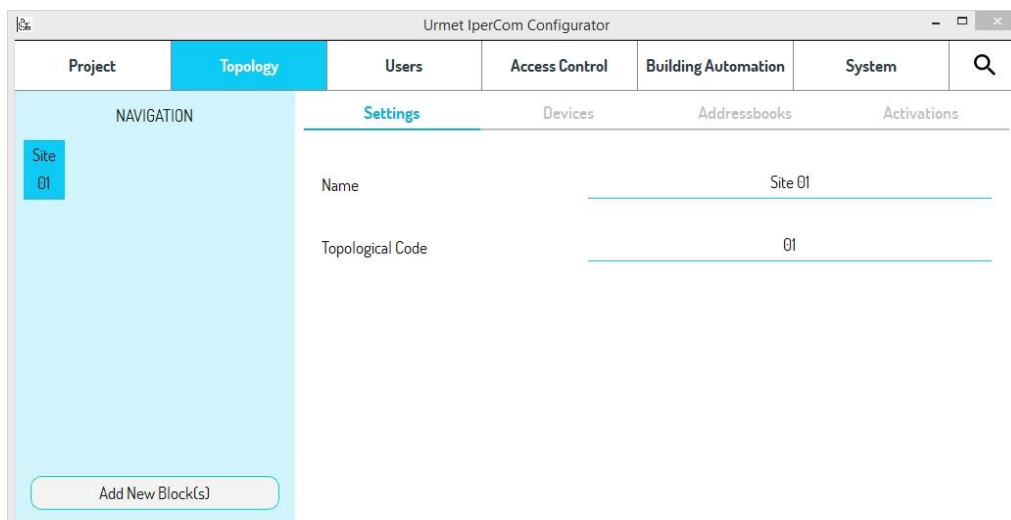


Figure 414: multi block configuration

In the configuration, no topological node has yet been entered, so the "Users" tab will not allow the addition of residents, since it is only allowed in the apartments.

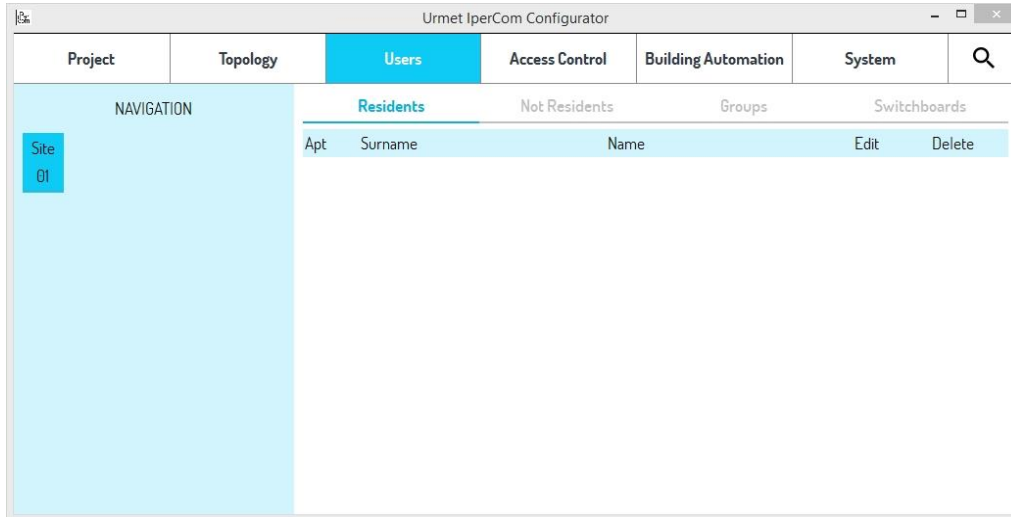


Figure 415: "Residents" screen in a topological node different from the apartment

If you want to add a block, with a stair, a floor and 3 apartments to the topology: go through the navigation module to one of the apartments, you will see the "Add" button in the "Residents" tab, as shown in the following figure:

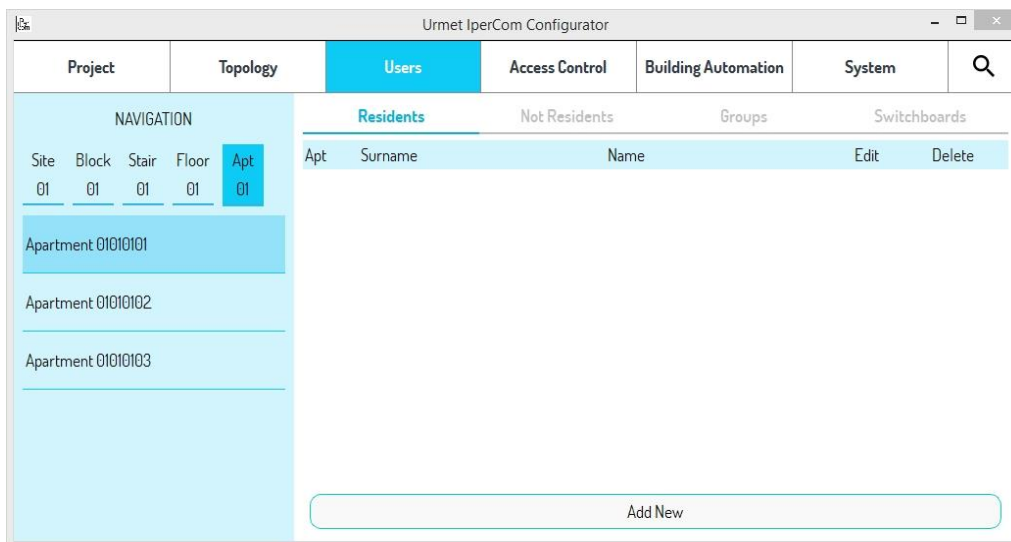


Figure 416: "Residents" screen for an apartment

The "Add New" button allows adding the residents to be associated with the apartment selected in the navigation module, in this case "Apartment 01010101".

Press the button to access the following screen, with the fields to be filled in for the creation of the new user.

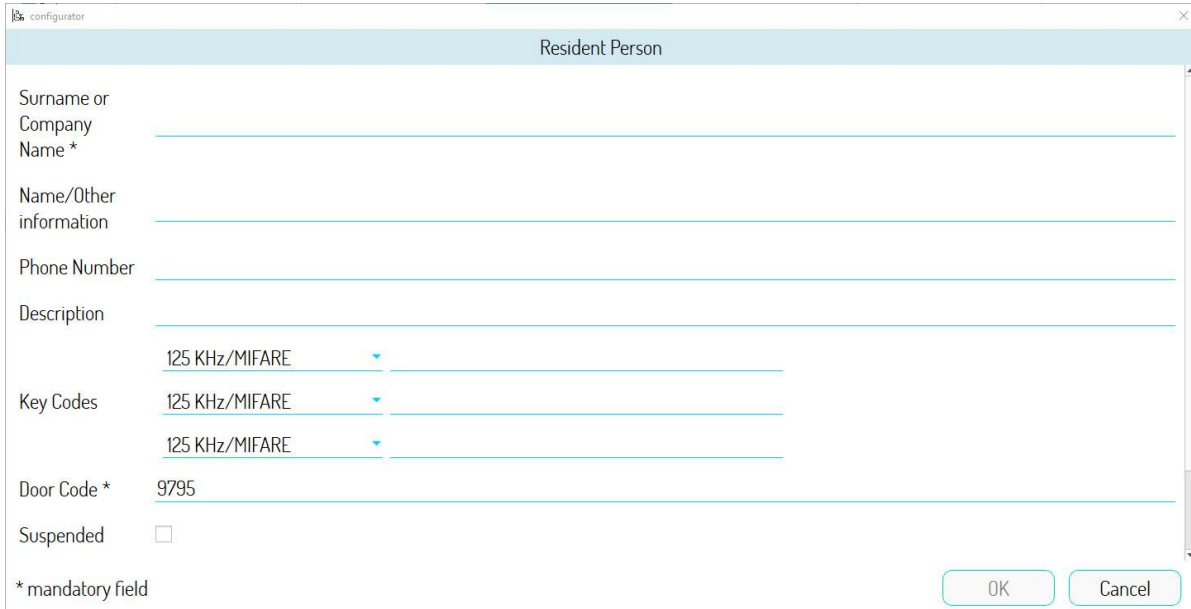


Figure 417: Creating a new resident – first part

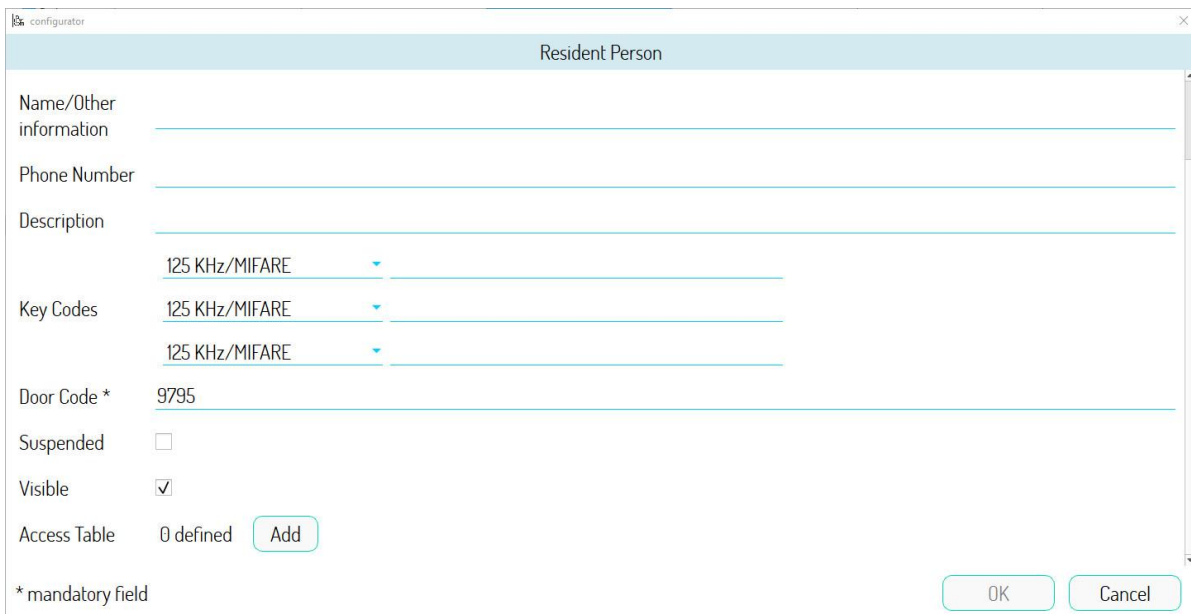





Figure 418: Creating a new resident – second part

The following table helps you to understand the meaning of the fields

<i>Surname or Company Name</i>	Surname of the resident or company name. Maximum length: 32 characters.
<i>Name/Other information</i>	Resident name or other information. Maximum length: 32 characters.
<i>Telephone number</i>	Telephone number associated to the resident. Maximum length: 16 numeric characters.
<i>Description</i>	Short description of the resident.
<i>Key codes</i>	Proximity key codes associated with the user (up to three key codes per user). The code must be unique in the plant. It is possible to choose between 4 different types of key according to the device set to read the key.
<i>Door Code</i>	Door opener numerical code associated to the user; the <i>configurator</i> automatically generates a 4-digit code, which can be modified. The code must be univocal in the system.
<i>Suspended</i>	If selected, access to all access points (on the topological path of the relevant apartments and not) is not allowed with either the key code or the door code.
<i>Visible</i>	If selected, the name will be shown in the Call Module. Otherwise, the name will not be shown in the address book.

Table 14: resident fields

-  *The number of digits of the Door Code can be changed from a minimum of 4 digits to a maximum of 8. For further details, see paragraph [System parameters](#).*
-  *The door opener code, besides being unique in the system, cannot be the same as other codes already generated and increased by one unit. In fact, these codes are reserved for the coercion alarm generation (in addition to the entrance hall opening). For further details see the installation and user manual of the Switchboard downloadable from [www.urmet.com](http://www.urmet.com)*
-  *Door opener codes and related coercion alarm codes can be entered on call stations equipped with numeric keypad, i.e. Call Module 1060/12-13-17-18-23 and Modular Entry Panel with 1060/48.*

As for the key code, this is shown on one of the 2 sides of the proximity key. The code must be entered in the relevant field of the *configurator*.

The types of keys available are:

- 125KHz,
- Mifare,
- Mifare Plus
- dual technology (125KHz and Mifare).

**APPENDIX E: Type of proximity keys that can be read by IPerCom devices with access control function**

contains a table with a list of devices that integrate a key reader and the different types of proximity keys that can be read by these devices.

To speed up the insertion of the key code in the *configurator* page, an automatic reading device (Universal Encoder) of the code is available for keys with Mifare, Mifare Plus technology and dual technology.

Simply connect the *Universal Encoder* device to a USB port on your computer (using the supplied cable): in this way the device is powered and the LED on the front panel switch from green (about 1s) to steady red. Now, after opening any text editor on your PC (Notepad for example), simply bring the key close to the white recess on the front of the device: the key code is immediately displayed on the text editor and can then be copied and pasted in the relevant field of the resident or non-resident page you are adding to the configuration.



*Residents may also be associated with 2Voice apartments as described above. These residents will appear in the address books of the IPerCom Call Modules and will have access to the respective gates within their competence and not via Proximity Keys or Door Codes which may have a time limit or not.*

After adding for example 2 users for the “Apartment 01010101”, if you go to that topological node you will see the updated list of residents in the context menu.

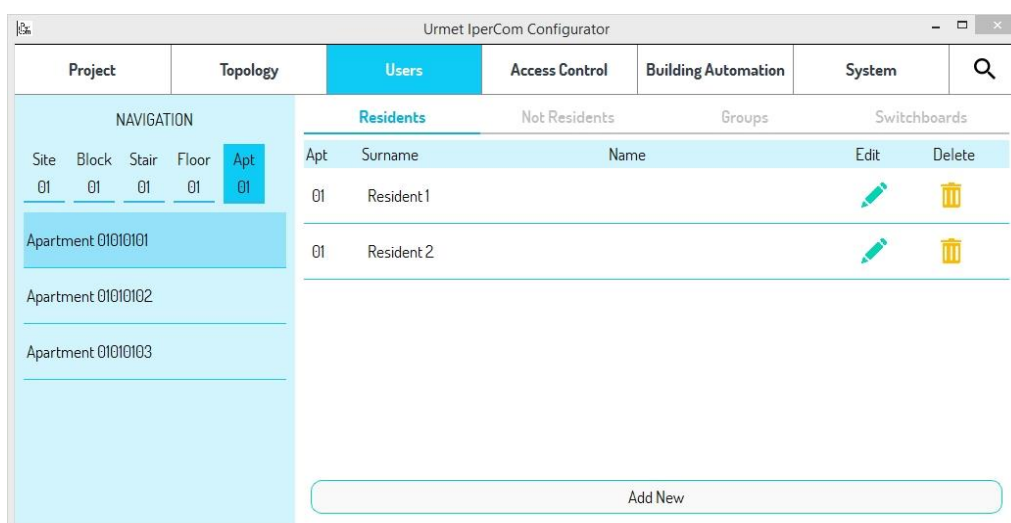


Figure 419: List of residents for the selected apartment

The buttons in the columns "Edit" and "Delete" allow you to modify the data or delete each user created, respectively (through confirmation pop-up).

The creation of the residents allows:

- having a contact address book that can be viewed on the *Call Modules* and *Modular entry panel with 1060/48*;
- giving residents access (through *Proximity Keys* or *Door Codes*) to the accesses on the topological path of their apartments without any time limit;
- giving residents access (through *Proximity Keys* or *Door Codes*) to the accesses not present on the topological path of their apartments with any time limit (refer to the [Access control](#) paragraph).



*For 2Voice apartment residents, the Proximity Keys and/or Door Codes allow access only to the IPerCom system call module doors. Program the key and/or door opener codes as shown in the user manuals of the respective 2Voice system products to access the doors of any call module in the 2Voice system, if required.*

### 7.1.8.2 Not residents

The IPerCom system can manage the controlled access to the residential structure also for external personnel (maintenance technicians, suppliers, etc.).

The "not resident" is not associated with any apartment of the system: in fact, by going to the tab "Not Resident" in the tab "Users", the navigation module will not show the topology of the system.

The addition of a non-resident is therefore always allowed regardless of the topology of the system.

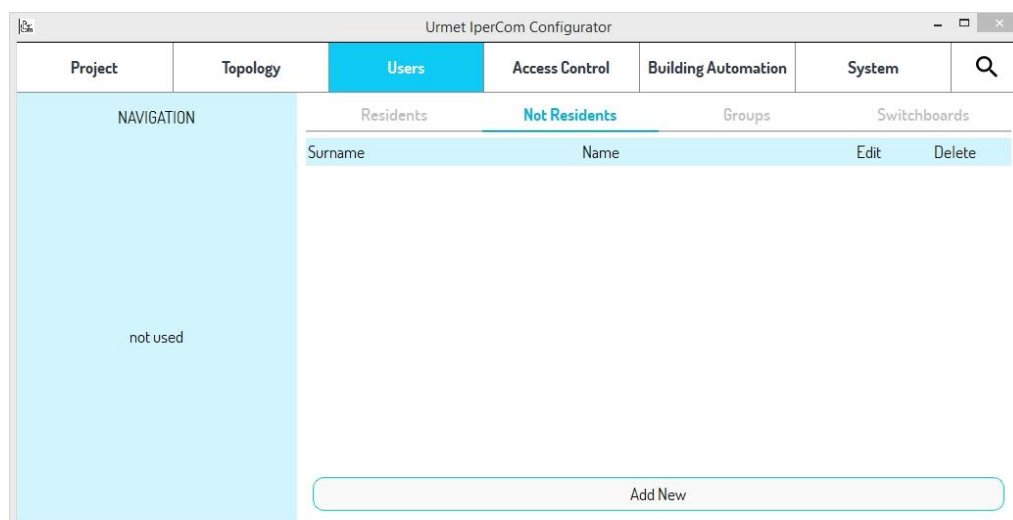


Figure 420: "Not Resident" screen



By pressing the “Add New” button, a screen like the following one will open:

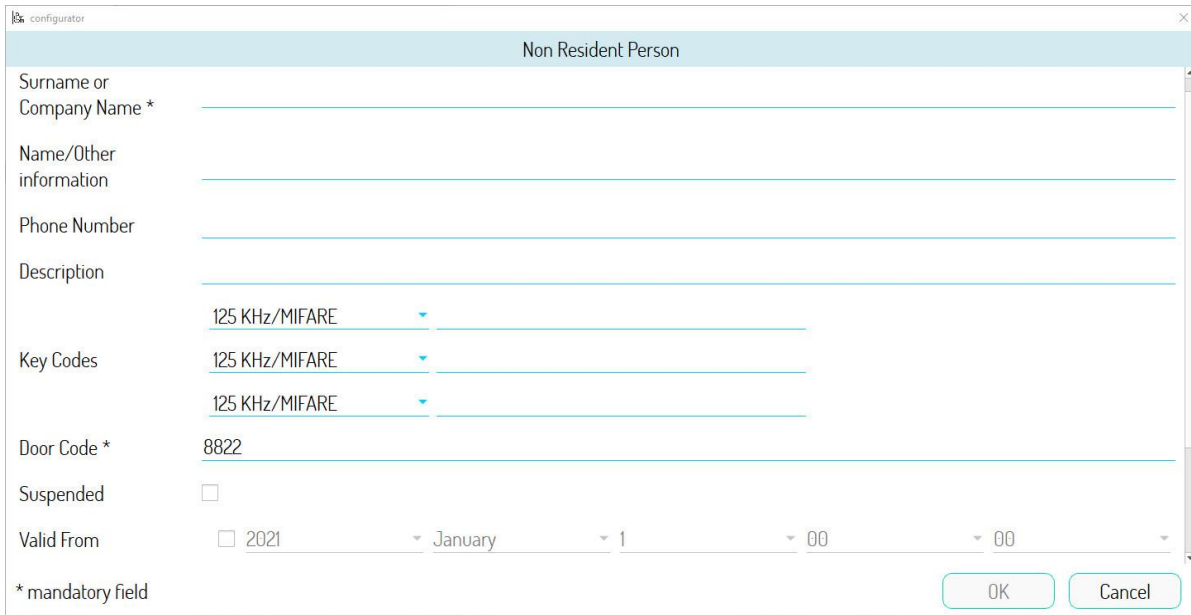


Figure 421: creation of a non-resident - part one

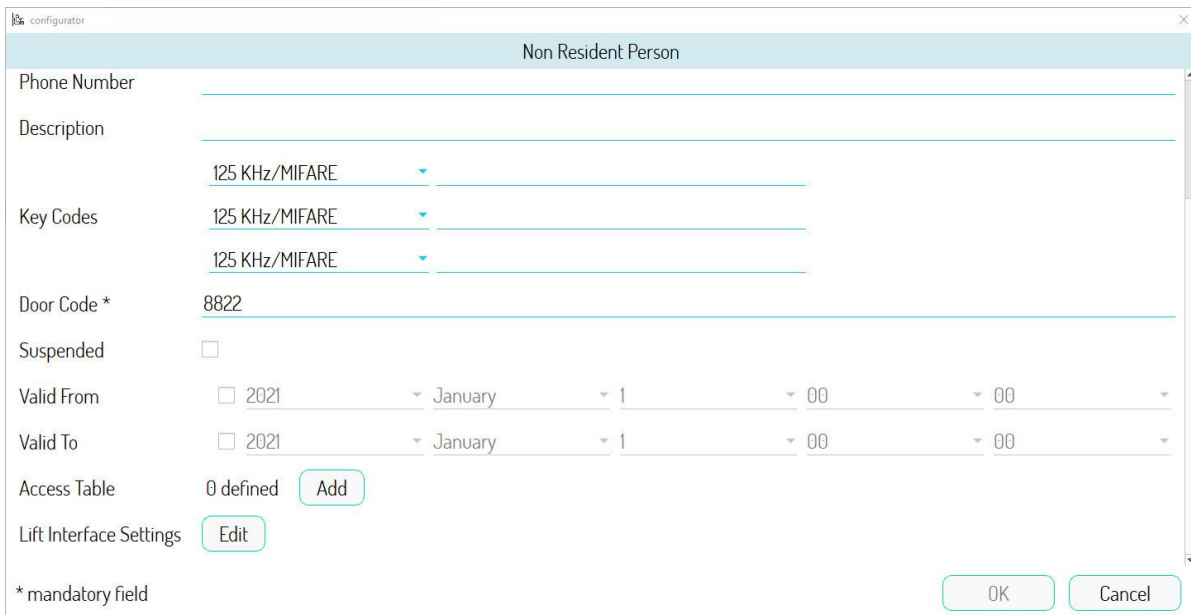





Figure 422: creation of a non-resident - part two

The following table helps you to understand the meaning of the fields:

<i>Surname or Company Name</i>	Surname of the resident or company name. Maximum length: 32 characters.
<i>Name/Other information</i>	Resident name or other information. Maximum length: 32 characters.
<i>Telephone number</i>	Telephone number associated to the not resident. Maximum length: 16 numeric characters.
<i>Description</i>	Short description of the not resident.
<i>Key codes</i>	Proximity key codes associated with the non-resident (up to three key codes per user). The code must be unique in the plant. It is possible to choose between 4 different types of key according to the device set to read the key
<i>Door Code</i>	Door opener numeric code associated to the non-resident. The <i>configurator</i> automatically generates a 4-digit code, which can be modified. The code must be univocal in the system. The code must be univocal in the system..
<i>Suspended</i>	If selected, access to all access points is not allowed with either the key code or the door code.

Table 15: Not Resident fields

-  The number of digits of the Door Code can be changed from a minimum of 4 digits to a maximum of 8. For further details, see paragraph [System parameters](#).
-  The door opener code, besides being unique in the system, cannot be the same as other codes already generated and increased by one unit. In fact these codes are reserved for the coercion alarm generation (in addition to the entrance hall opening). For further details see the installation and user manual of the Switchboard downloadable from [www.urmet.com](http://www.urmet.com)
-  Door opener codes and related coercion alarm codes can be entered on call stations equipped with numeric keypad, i.e. Call Module 1060/12-13-17-18-23 and Modular Entry Panel with 1060/48.

For security reasons, it may be necessary to make access to the doors available to non-residents in a specific time interval: to do this, at the bottom of the screen it is possible to set a time interval for the validity of the Key Codes and of the Door Codes, as highlighted below.



Valid From  2021 - January - 1 - 00 - 00

Valid To  2021 - January - 1 - 00 - 00

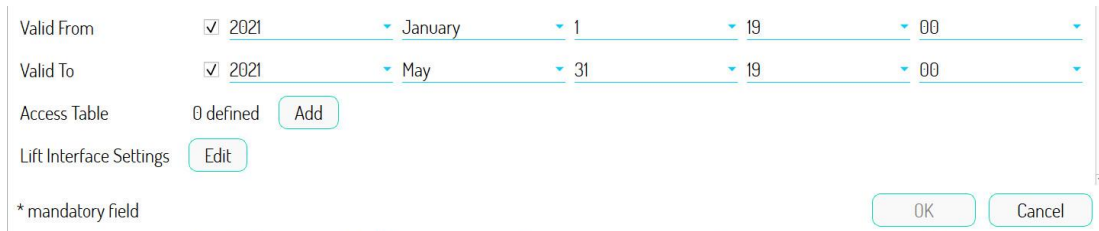
Access Table 0 defined

Lift Interface Settings

\* mandatory field

Figure 423: period of validity of the Key Codes and of the Door Codes

Generally, the validity period is not set, so access is always granted to the non-resident; to set a validity period, select the “Valid From” and “Valid To” items in the red rectangle (using the relevant tick boxes) and then set a validity start date and end date. An example is provided in the following figure.

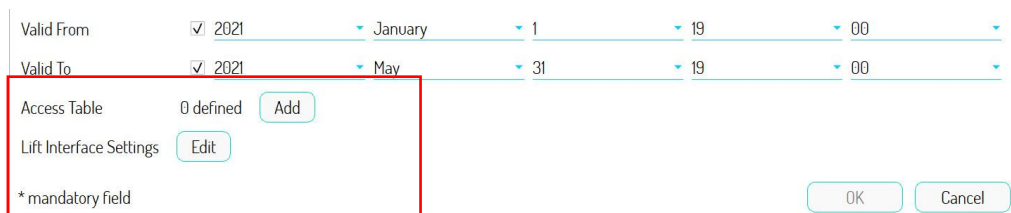


The screenshot shows a configuration window with the following fields and controls:

- Valid From:** A row with a checked tick box, the year '2021', a dropdown menu set to 'January', a dropdown menu set to '1', a dropdown menu set to '19', and a dropdown menu set to '00'.
- Valid To:** A row with a checked tick box, the year '2021', a dropdown menu set to 'May', a dropdown menu set to '31', a dropdown menu set to '19', and a dropdown menu set to '00'.
- Access Table:** A label '0 defined' followed by an 'Add' button.
- Lift Interface Settings:** An 'Edit' button.
- \* mandatory field:** A label at the bottom left.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Figure 424: selection of date and time of the period of validity

An important difference is noted on the operation of the *Door Codes* and *Key Codes*. While for residents, the *Door Codes* and the *Key Codes* automatically open the doors associated with the *Call Modules* and *Key Readers* which are on the topological path of the apartment, for non-residents the doors, which the respective *Proximity Keys* and *Door Codes* can open as specified in an external table. This external table can be accessed by pressing the “Add” button in the figure above.



This screenshot is identical to Figure 424, but with a red rectangular box highlighting the 'Access Table' and 'Lift Interface Settings' sections, including the 'Add' and 'Edit' buttons respectively.

Figure 425: association of gates to non-residents

A screen page opens displaying the various access profiles loaded into the system to be associated with non-residents, or a list of doors that can be opened, if necessary, during a certain time frame:

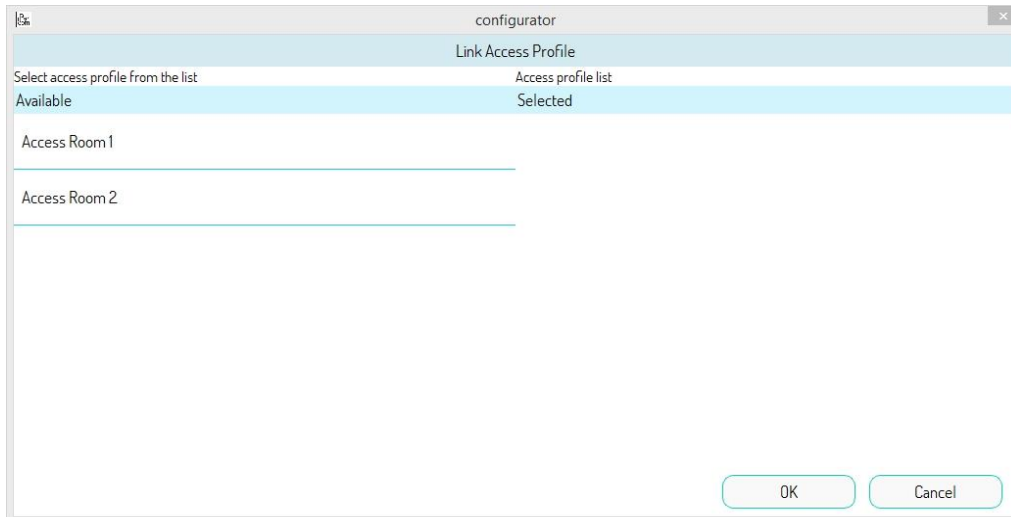


Figure 426: selection of access profiles for non-residents



Access profiles can be created in the "Access Control" tab (see section [Access control](#)).

To associate an access profile to a non-resident, press the relevant name: the access profile will move from the list of available profiles to that of the selected profiles. To delete the association, press the same item in the list of selected profiles.

In conclusion, the creation of non-residents allows giving access (through *Proximity Keys* or *Door Codes*) to external personnel only at the relevant access points with or without time limit. Once you have entered for example 2 non-residents, the list of non-residents in the configuration will appear as shown in the figure:

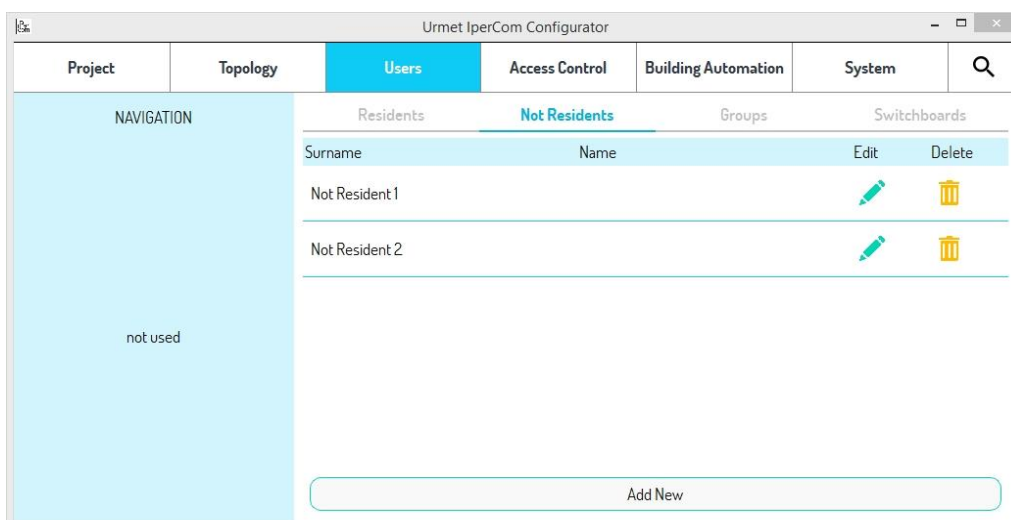


Figure 427: List of non-residents

The buttons in the columns "Edit" and "Delete" allow you to modify the data or delete each user created, respectively (through confirmation pop-up).

The "Lift Interface Settings" button in the red box of *Figure 296* allows setting the activations of the lift interface (if present in the system) according to the defined paths (see paragraph

[Adding a Lift Interface 1060/37 on a stair](#) node).

### 7.1.8.3 Groups

The "Groups" screen allows you to quickly create groups of residents and/or non-residents who have special access needs to certain doors, possibly at specific times.

For example, there could be a "Swimming pool" group to which all those with access to the pool must be added. The group, in turn, should be associated with a "Swimming pool access profile" that allows access to the doors of the pool in the time intervals in which the courses are held. In this way, every time a user enrolls in the course, it is sufficient to add him/her to the corresponding group.

To create the "Swimming pool" group, click on the "Users" tab, then on the "Groups" tab.

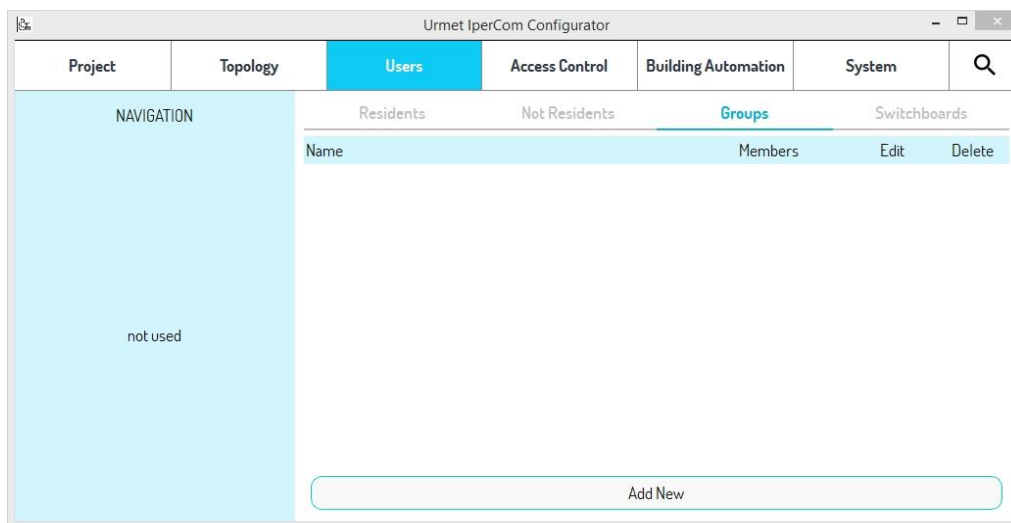


Figure 428: "Groups" screen

Pressing the "Add" button, the following screen appears:

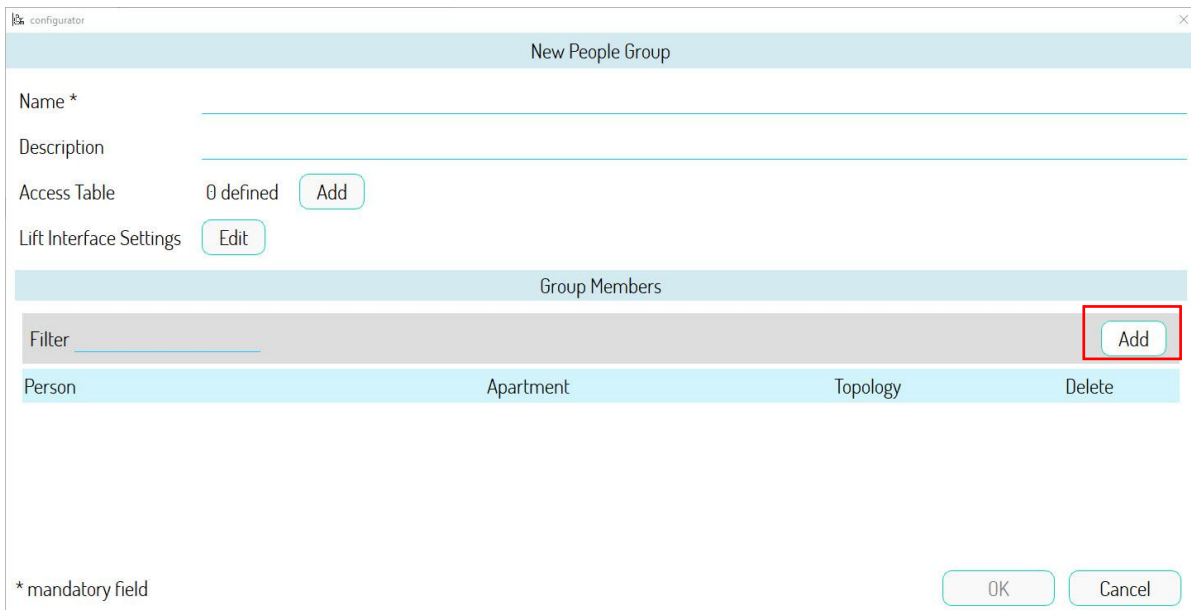


Figure 429: adding a group

The "Name" and "Description" fields allow you to give a meaningful name and description to the group you are creating.

The "Add" button in the "Access Table" section allows you to associate a previously created access profile to the group (see chapter [Access control](#)).

In the "Lift Interface Setting" section, it is possible to set the *Lift Interface* activations (if present in the system) according to the established paths.

To add (for example) residents just press on the "Add" button (red box). The following screen is displayed:

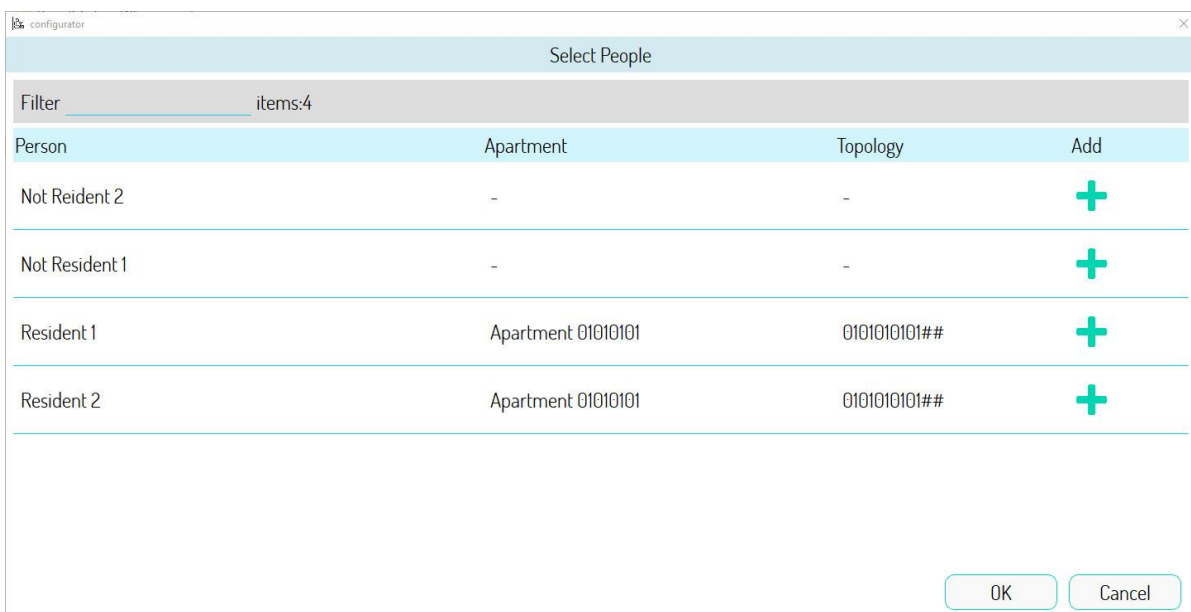



Figure 430: adding users to a group

To add residents, simply press the corresponding button : they disappear from the list above.

The "Filter" field allows you to search for people by name, apartment, and topology according to the string entered in this field.

By pressing the "OK" button, this screen appears:

**New People Group**

Name \*

Description

Access Table 0 defined

Lift Interface Settings

**Group Members**

Filter  items:2

Person	Apartment	Topology	Delete
Resident 1	Apartment 01010101	0101010101###	
Resident 2	Apartment 01010101	0101010101###	

\* mandatory field

Figure 431: New group

Then simply give the group a meaningful name and description and confirm with the "OK" button: the group will be added to the list of user groups.

**Urmet IperCom Configurator**

Project | Topology | **Users** | Access Control | Building Automation | System |

NAVIGATION | Residents | Not Residents | **Groups** | Switchboards

Name	Members	Edit	Delete
Swimming Pool Group	2		

not used

Figure 432: List of groups

The buttons in the columns "Edit" and "Delete" allow you to modify the data or delete each user created, respectively (through confirmation pop-up).

### 7.1.8.4 Switchboards

Through the "Switchboards" tab of the "Users" tab it is possible to manage the users of the switchboards in the system.

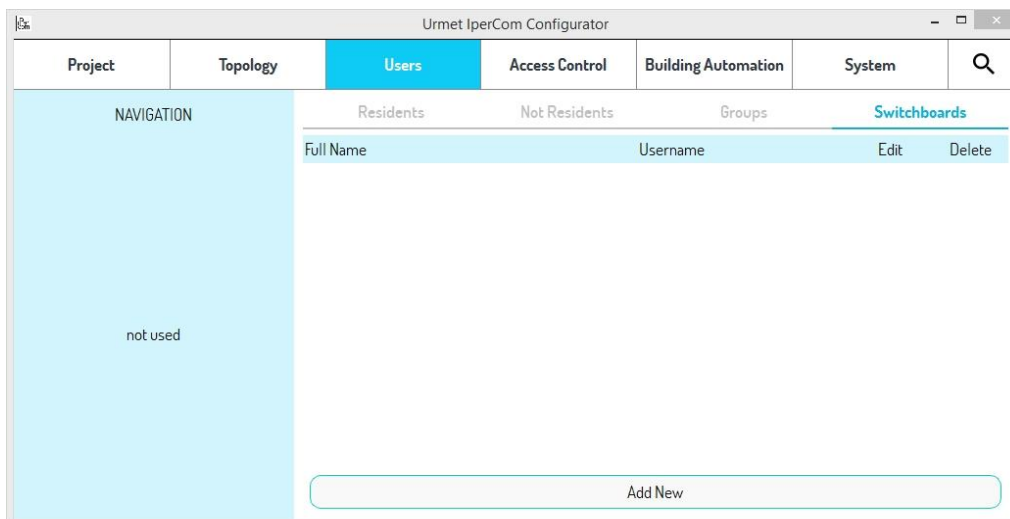


Figure 433: "Switchboard" screen

The "Add" button allows adding new users of the switchboards. Press it to open the following screen:

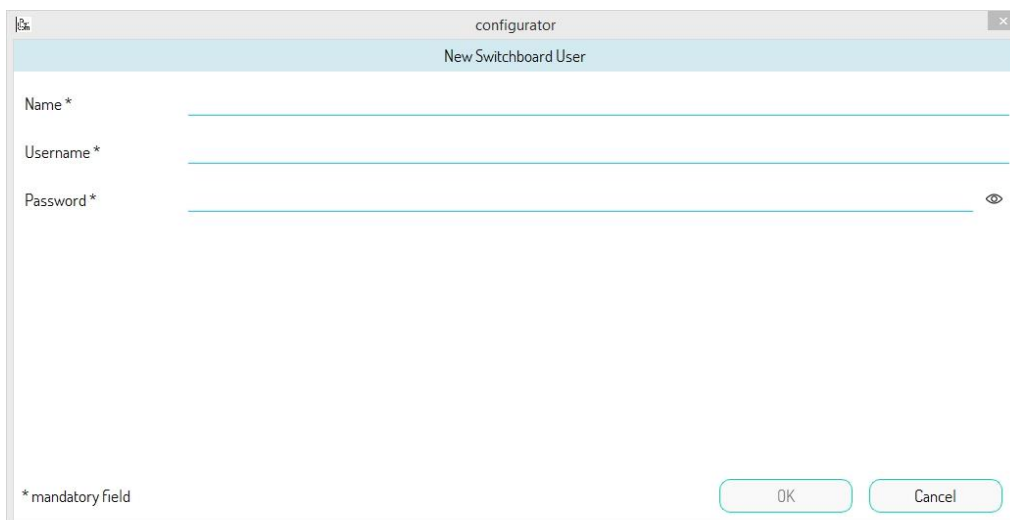


Figure 434: Creation of a new user



Once all fields have been edited appropriately and the "OK" button has been pressed, another user is added to the user list.

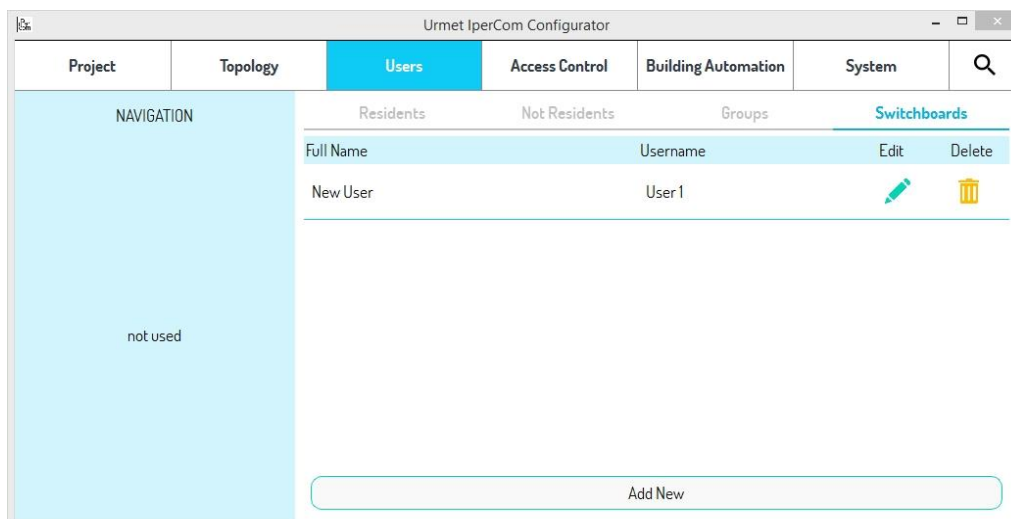


Figure 435: List of the switchboard users

The buttons in the columns "Edit" and "Delete" allow you to modify the data or delete each user created, respectively (through confirmation pop-up).

The "User Name" and "Password" fields associated to each switchboard user correspond respectively to the "User" and the "Password" fields used for the access through the *Switchboard* application software installed on a PC connected to the system.

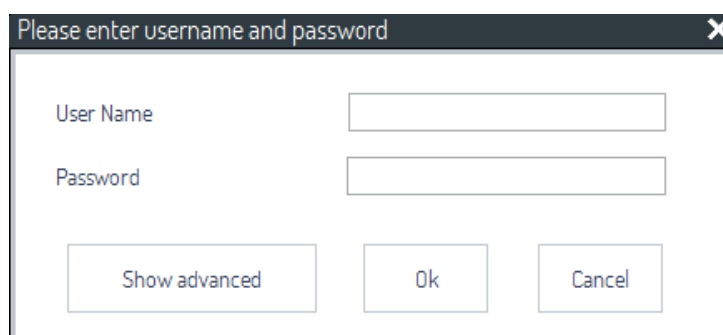


Figure 436: Switchboard 'application access screen

For the operation of the "Switchboard" programme, refer to the relevant manual.

### 7.1.9 Access control

The *iPerCom* system integrates an **access control service**, which allows the opening of gates (doors, gates, barriers, etc.) by recognising *proximity keys* or entering *door codes*. *Call Modules*, *Entry Panels 1060/21* and *Key Readers* can be used to open the access. *Call Modules with 1060/48* and *Entry Panels 1060/21* integrate a *Proximity Key reader*.

The opening of a door is subject to the recognition of a *Proximity Key* or an access code by a *Call Module*, an *Entry Panel 1060/21* or a *Key Reader*.

For a *Proximity Key* or access code to be valid and thus able to open a certain access point:

- they must be associated with a user (resident or non-resident);
- they must be associated with the access points to be opened.

This is partially already done automatically by the system through the concept of topology and competence.

Let us supposed to have a building with a block and two stairs like the one shown below:

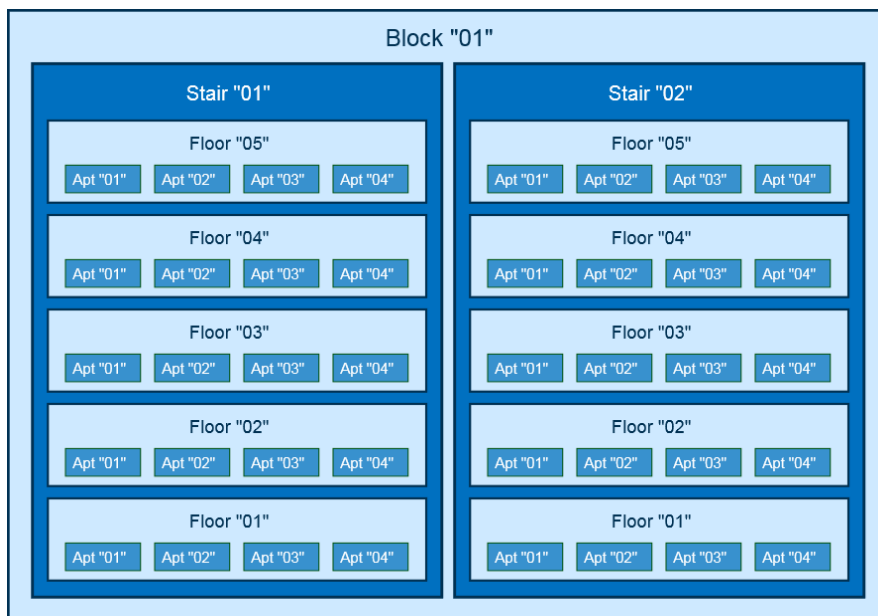
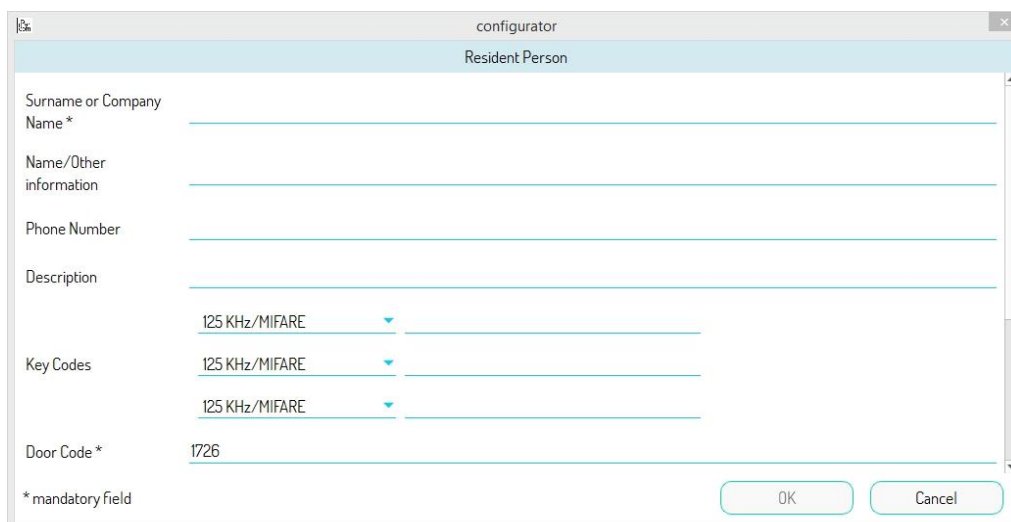


Figure 437: System consisting of a block with two stairs

There is a main *Call Module* on the topological node of Block "01", while there is a *Key Reader* on the topological node of Stair "02".

All residents of Stair "02" are automatically enabled to open the accesses associated with the main *Call Module* and the *Key Reader* with a key code and a door code (both the *Call Module* and the *Key Reader* are on the topological path of these residents).



The screenshot shows a software window titled "configurator" with a sub-header "Resident Person". The form includes the following fields and values:

- Surname or Company Name \* (empty)
- Name /Other information (empty)
- Phone Number (empty)
- Description (empty)
- Key Codes: Three dropdown menus, each showing "125 KHz/MIFARE".
- Door Code \*: 1726

At the bottom left, there is a note: "\* mandatory field". At the bottom right, there are "OK" and "Cancel" buttons.

Figure 438: User setting screen

If you want to give the residents of Stair "02" access to other accesses that are not on their topological path (e.g. a *Key Reader* on the topological node of Stairs "01"), you must use the access control service.

### 7.1.9.1 Access profiles

The "Access Profiles" screen is the same as the one that appears when you open the "Access Control" tab.

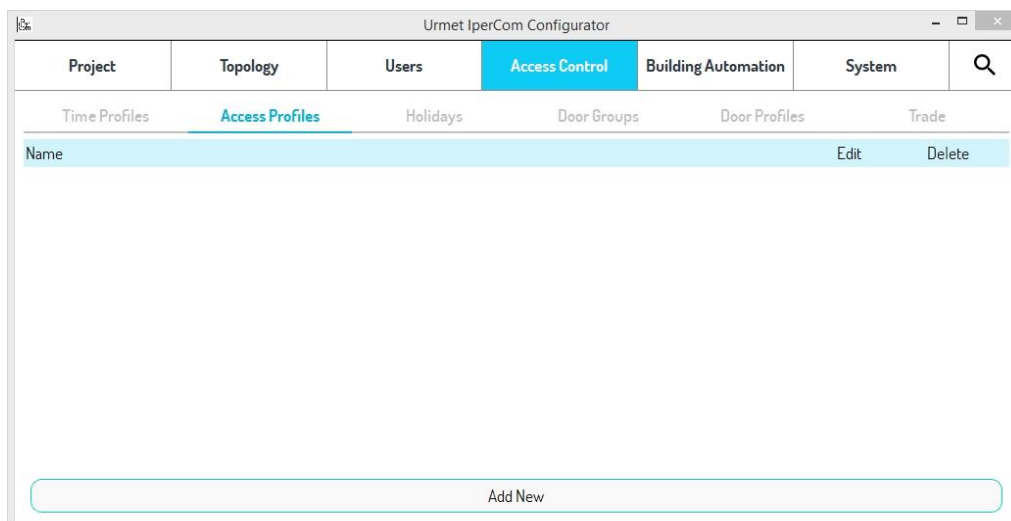


Figure 439: "Access profiles" screen

Access profiles allow to group a set of accesses that a group of users' needs to open in a single rule even if these accesses are not on the topological path of the apartments of these users. For example, if two *Key Readers* satisfy the two points above, press the "Add" button that opens the following screen to create an access profile with these two accesses:

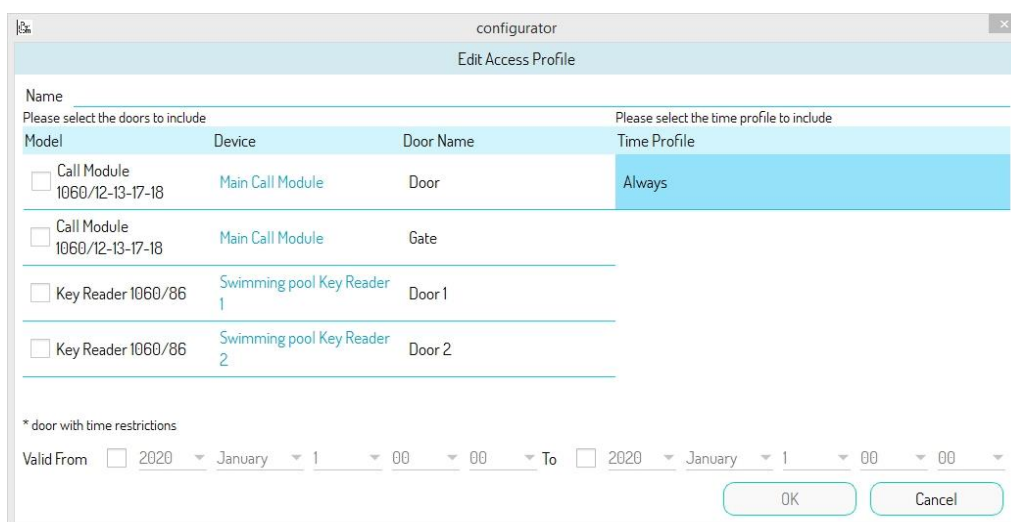


Figure 440: Creation of a new access profile

It is necessary to give a name to the access profile that is being created in the "Name" field at the top left, and then select the access points that are part of it by simply pressing on the relevant record (the relevant tick box is selected automatically). It is also possible to assign a time validity to the access profile, i.e. a time interval (year, month, day, hours and minutes) in which access to the access points is valid. Instead, in the "Time Profile" column, an access time limit is defined during the validity period; by default, "Always" is selected, but custom settings can be created (for example, only for weekdays or holidays), as shown in paragraph "[Time Profiles](#)".

For example, if the two access points associated with the *Key Readers* give access to a swimming pool in the summer, it is possible to set the name and time validity as shown in the following figure:

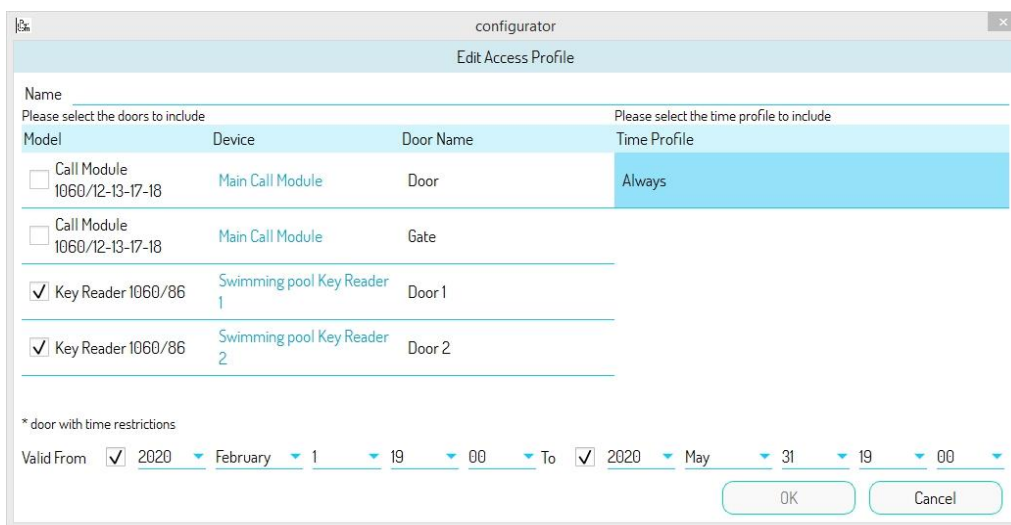


Figure 441: Setting the access profile

By pressing the "OK" button, the profile is saved and added to the access profile list.

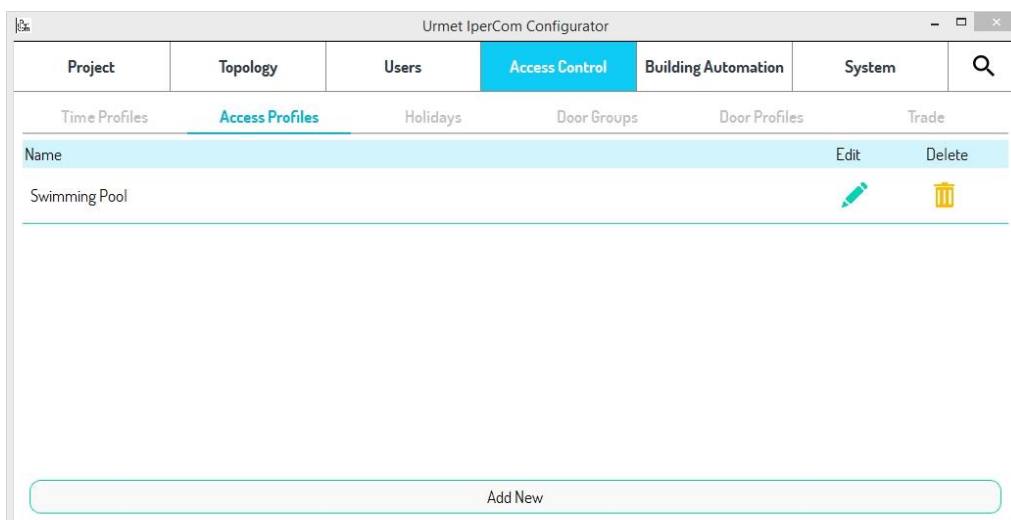


Figure 442: List of the created access profiles

In the “Access profiles” screen page, the buttons in the columns “Edit” and “Delete” allow you to modify the data or delete each access profile created, respectively (through confirmation pop-up).

Each resident/non-resident can be assigned an access profile during the user creation/editing phase:

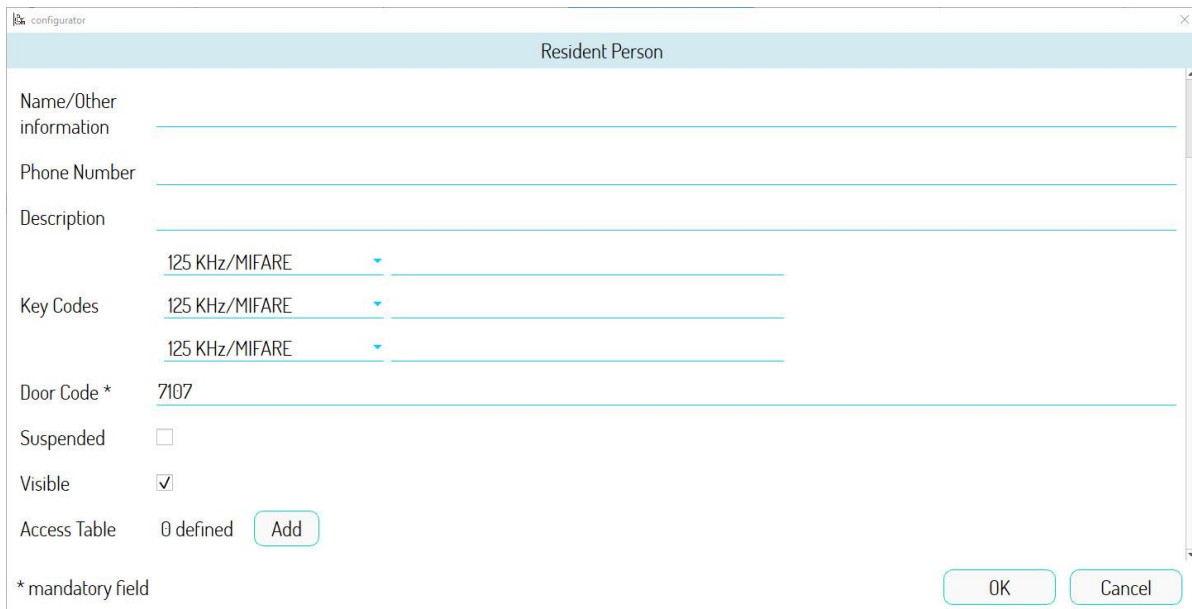


Figure 443: Resident editing screen di un residente

By pressing the “Add” button in the “Access Table” section, the following screen page will open.

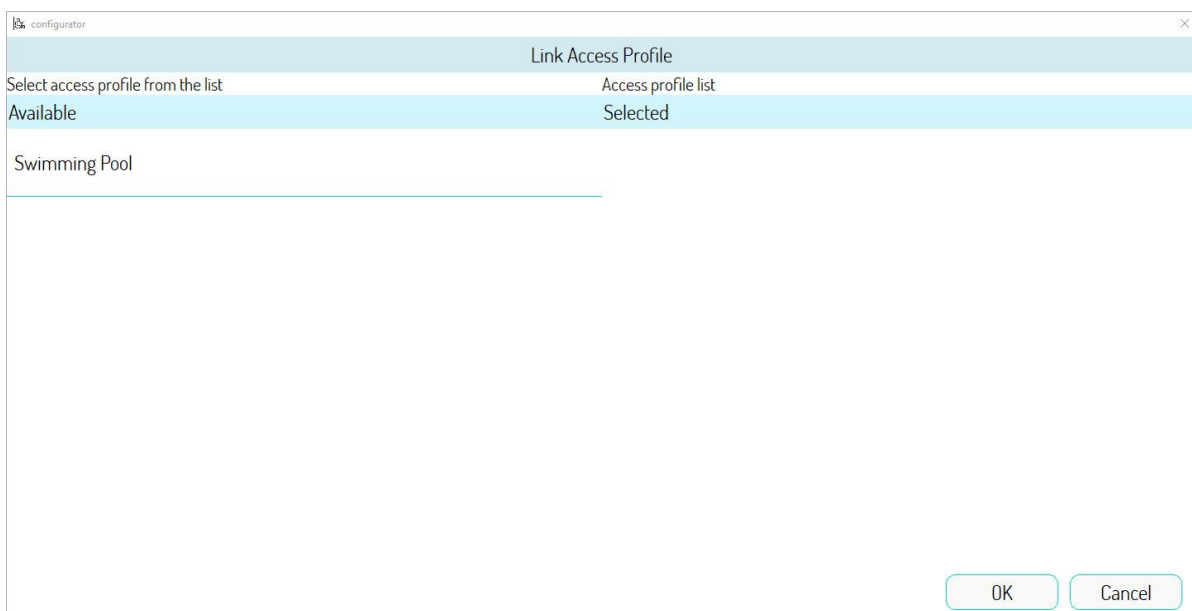


Figure 444: List of access profiles

The access profiles available are listed on the left, while those already selected for the concerned user are listed on the right.

By selecting an item on the left, it will be moved automatically to the right list.  
 Assuming you want to select the previously created access profile, you get the following:

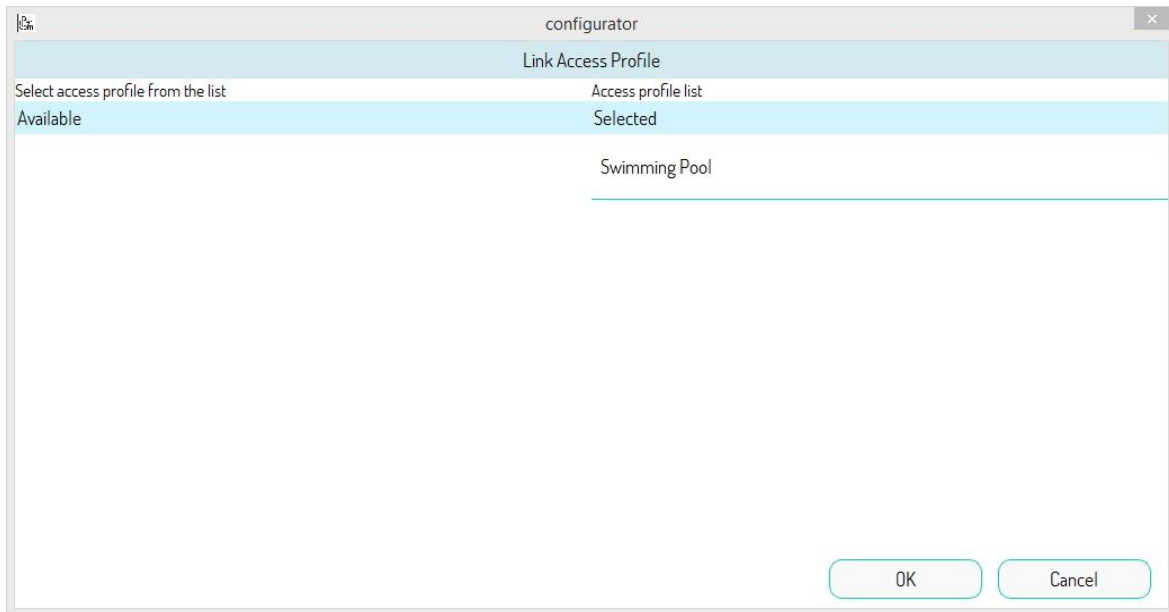


Figure 445: Selection of an access profile

Press the "OK" button to automatically associate the access profile with the created user:

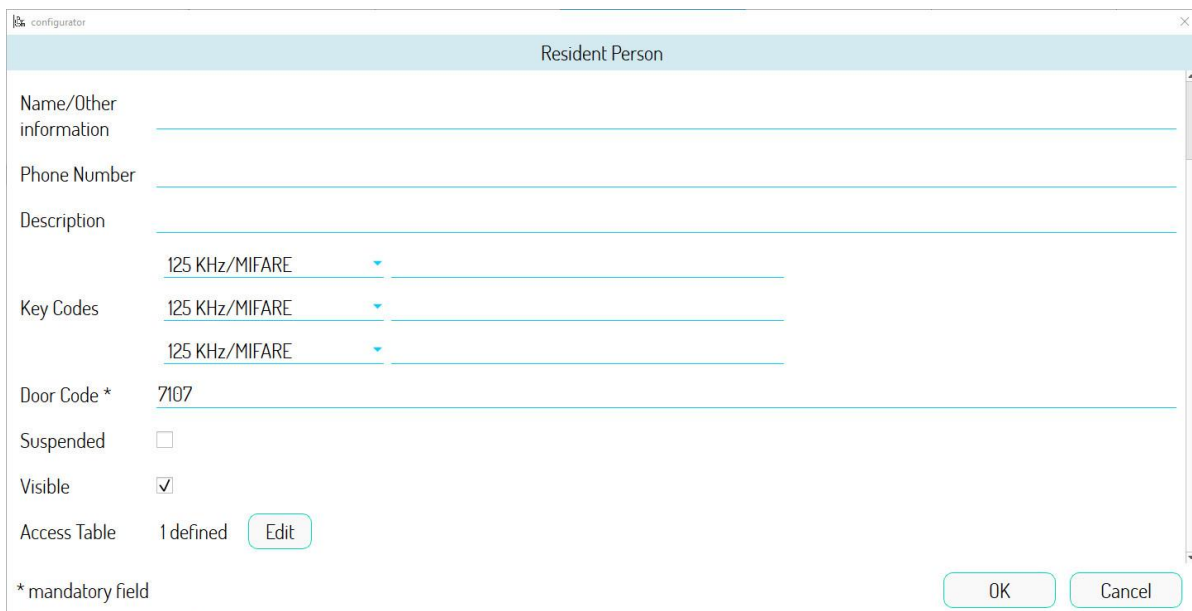


Figure 446: association of access profile to resident



**An access profile must be associated with a resident or non-resident or user group to be effective. If this association is not made, the access profiles are not applied.**

### 7.1.9.2 Time Profiles

A **time profile** is a set of time intervals for the validity of accesses.

To manage time profiles, go to the "Access Control" tab, then click on the "Time Profiles" tab.

The following screen will open:

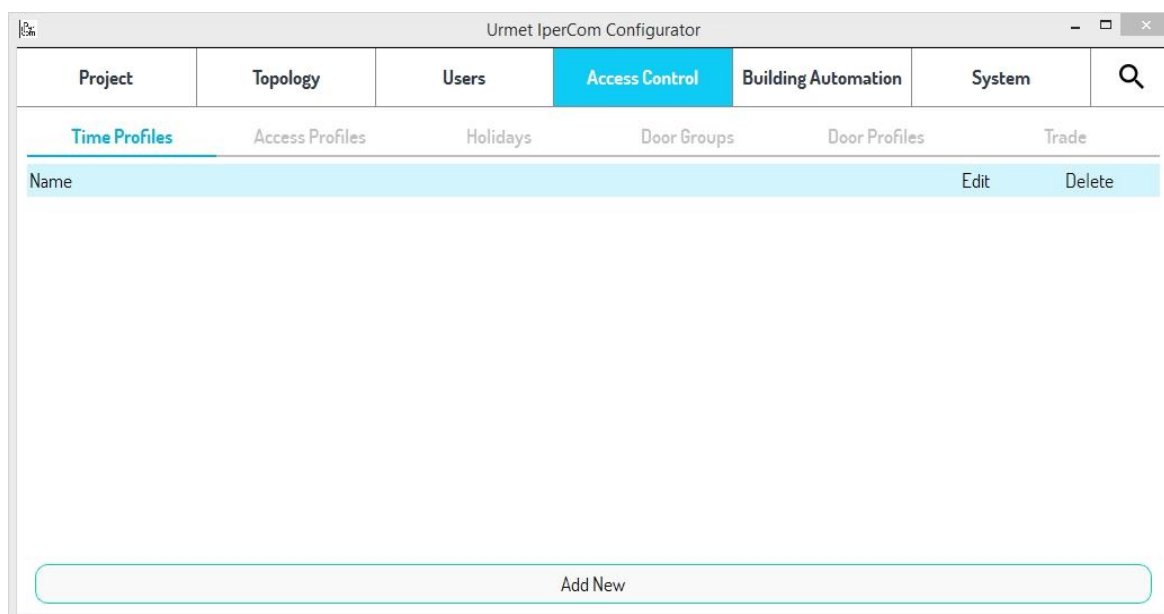


Figure 447: "Time profiles" screen

By pressing the "Add New" button it is possible to create a time profile associated with the days of the week.

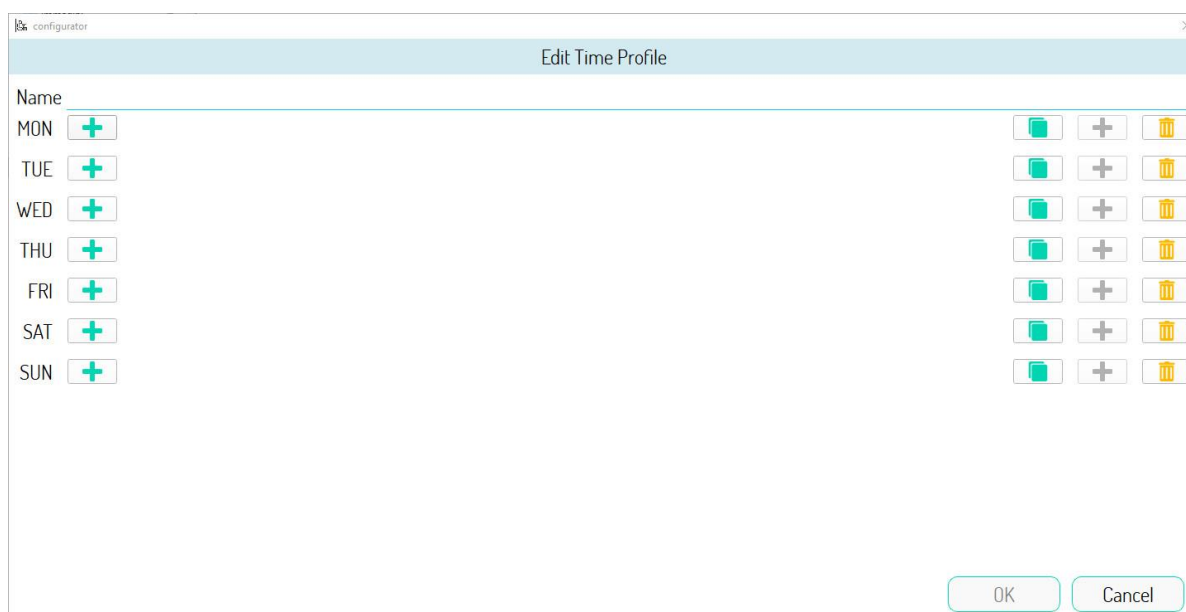


Figure 448: "Time profile" creation screen



Up to three access time intervals can be created for each day.

To create a new time interval, press button  to open the following screen:

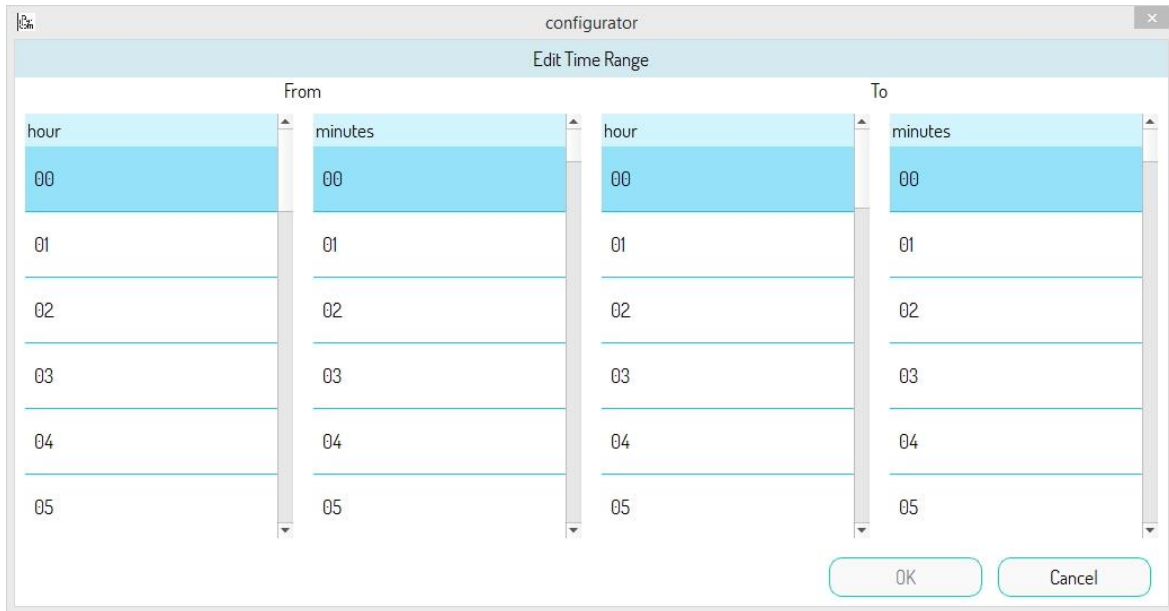


Figure 449: Creation of a time interval

After setting the time interval and pressing the "OK" button, the interval will be added to the selected day, as shown in the following figure:

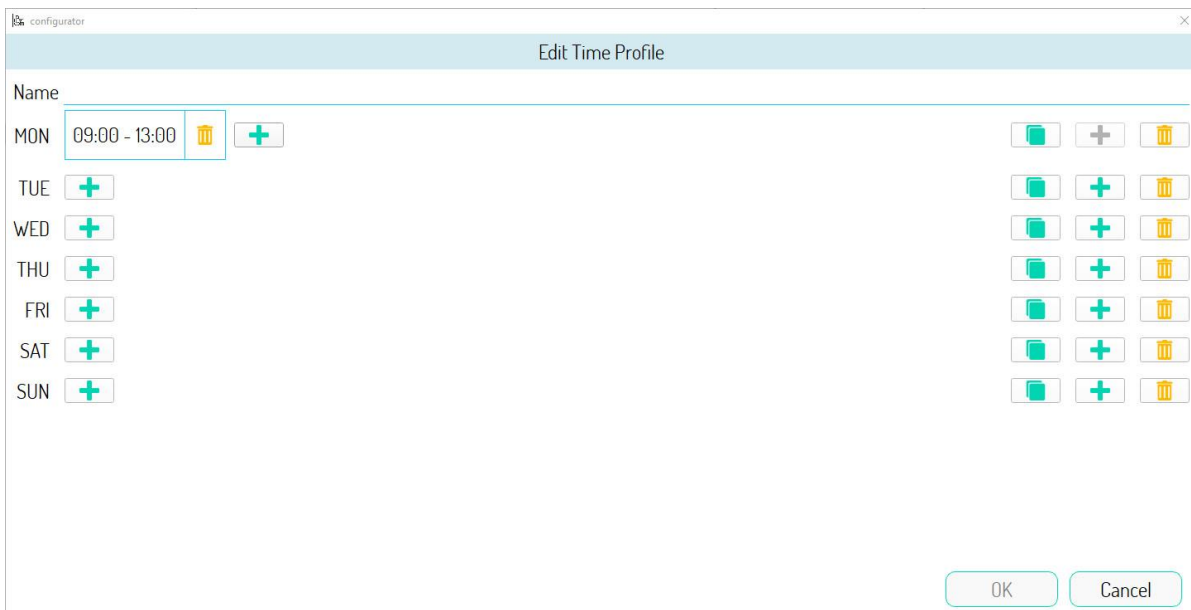






Figure 450: time interval added to the selected day

The buttons “” and “” allow you to quickly copy the time interval you have just created for all the other days of the week: in fact, if you press the button “” on Monday, you enable the buttons “” of the other days, which allow you to do what just described.

For example, copying the time interval set for Monday (“MON”) and pasting it in the line corresponding to Thursday (“THU”), the result will be as follows.

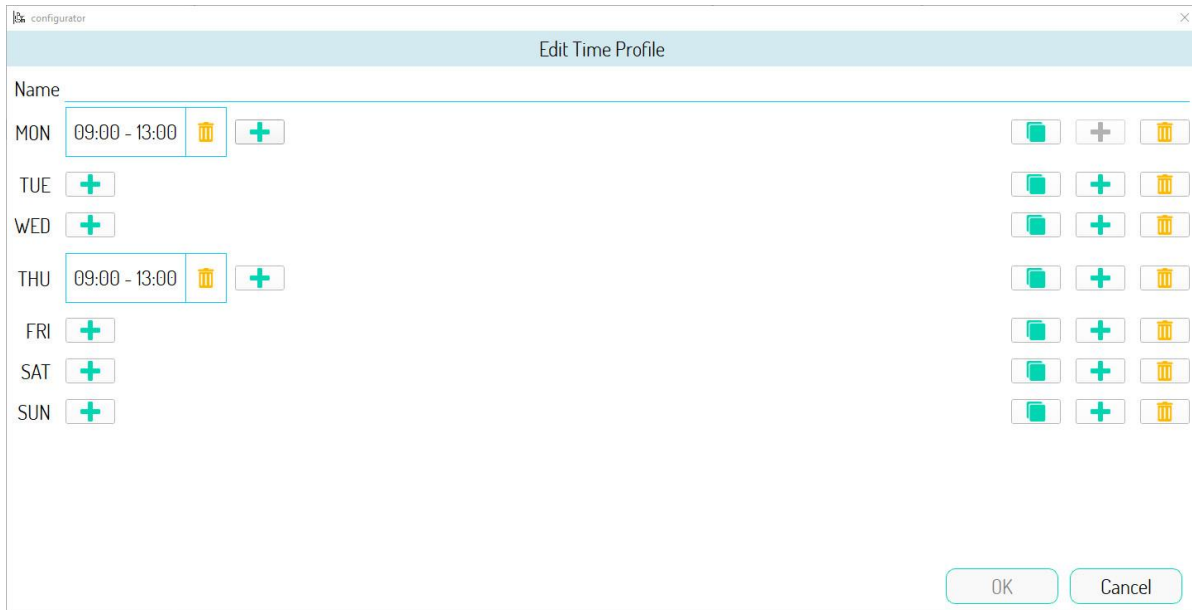




Figure 451: copying and pasting the time intervals of a day

The  button (at the right) allows deleting all previously created time intervals for one day of the week.

The  button (at the left) allows you to delete a single time interval created.

After naming the time profile and pressing the "OK" button, the new time profile will be added to the time profile list.

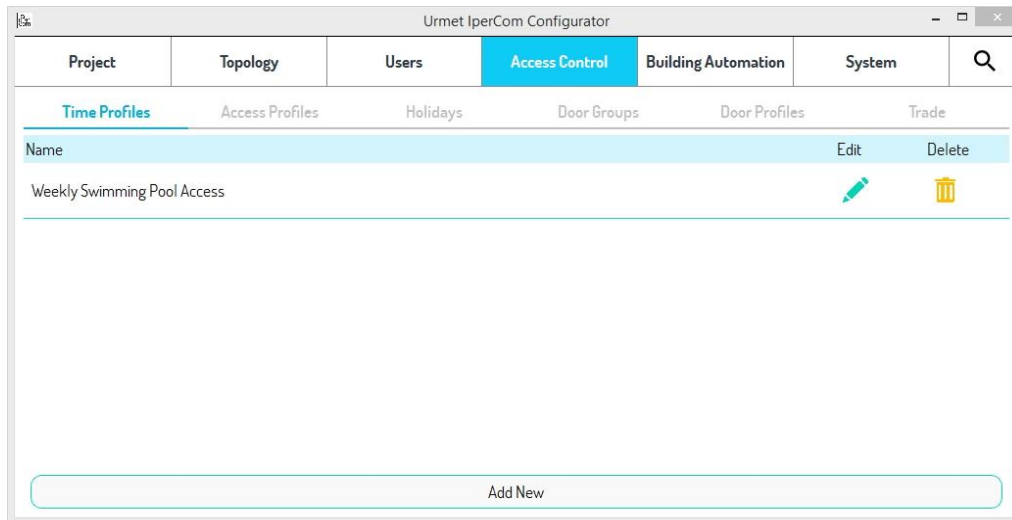


Figure 452: List of the created time profiles

The buttons in the columns "Edit" and "Delete" allow you to modify the data or delete each time profile created, respectively (through confirmation pop-up).

If you want to associate the time profile "Weekly Swimming Pool Access" to the previously saved access profile, simply reopen the latter in edit mode and select the created time profile, as shown in the following figure:

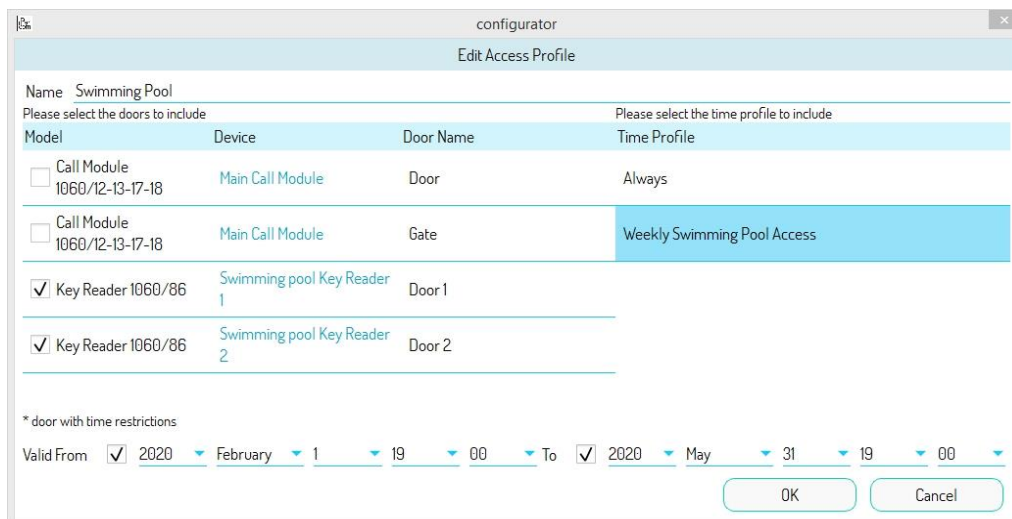


Figure 453: Selection of the new time profile in the saved access profile

A time profile may also be associated with a single access as well as an access profile if the concerned access has time restrictions. To do this, you need to go to the "Topology" page, then to the "Devices" tab. Press the "Edit" button of the device, the access of which must be associated with a time profile and search for the "Time Profile" item of the concerned access.

For example, if you want to associate a time profile to a *Key Reader* access point, you will see the following screen, where no time profile is set.

The screenshot shows a 'Create new Device' dialog box with the following fields and values:

- Door Profile: custom
- Door Name: (empty)
- Door Time (s) \*: 3
- Door Forced Alarm:
- Max Door Opening Time (s) \*: 20
- Door Under Secret:
- Time Profile: none available (highlighted with a red box)
- Remote Relay: None (with Select and Clear buttons)
- Remote Button: None (with Select and Clear buttons)
- Remote Sensor: None (with Select and Clear buttons)
- Activations: 0 defined (with Add button)

\* mandatory field

Figure 454: Time profile not set

To associate a previously created one, click on the respective drop-down menu to open a screen with all the created time profiles. After selecting one and pressing the "OK" button, the following screen will appear:

The screenshot shows the same 'Create new Device' dialog box as Figure 454, but with the 'Time Profile' field now set to 'Weekly access swimming pool' (highlighted with a red box).

Figure 455: Set time profile

If a time profile is associated with a generic access, it appears with an asterisk when creating an access profile:

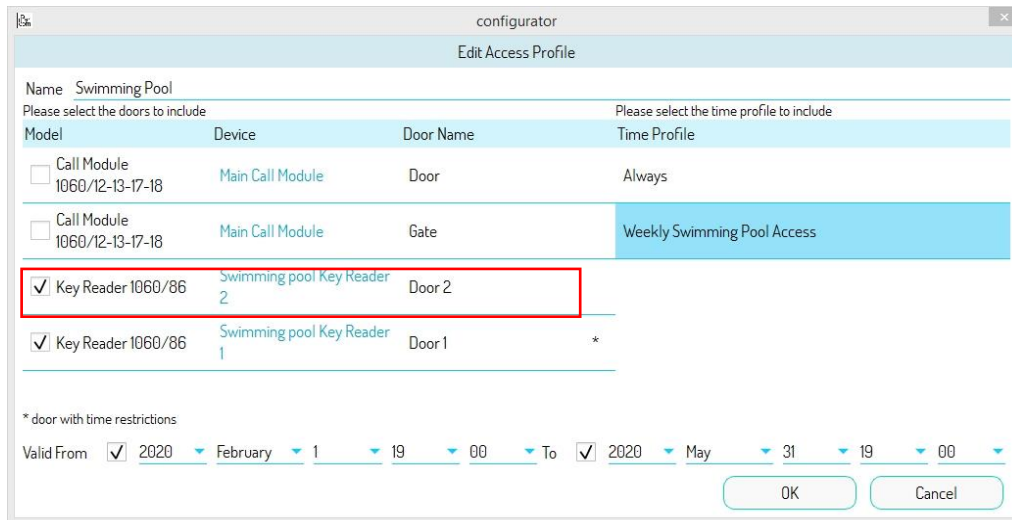


Figure 456: Door with associated time profile

### 7.1.9.3 Holidays

**Holidays** allow you to define one or more particular dates of the year (e.g. Christmas) on which to alter a previously created time profile. In other words, they allow you to create exceptions in a weekly schedule.

To create a holiday, go to the "Access Control" page and then press the "Holiday" tab. The following page will appear:

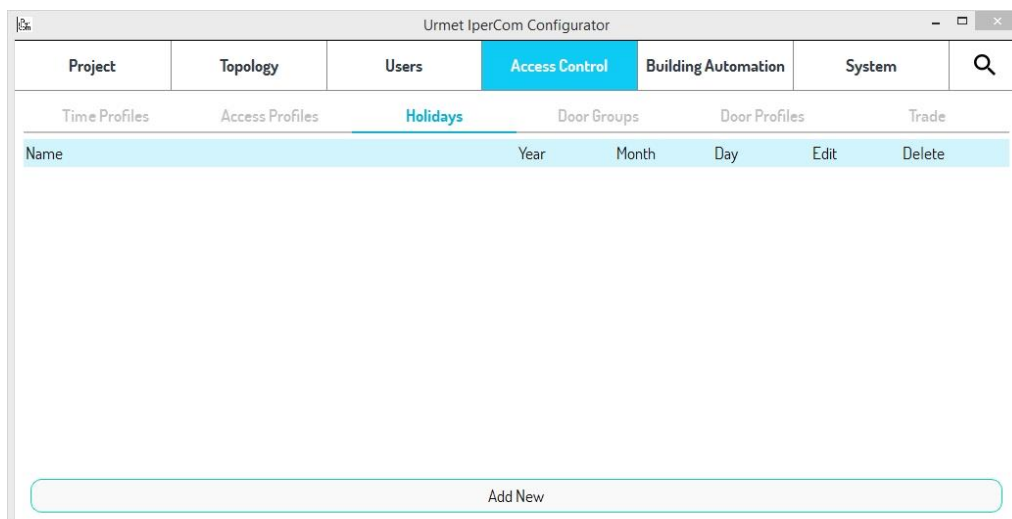


Figure 457: "Holidays" screen

Pressing the "Add New" button you can create a holiday by defining the following fields:

- "Name": significant name to give to the festivity;
- "Year": field not mandatory. If not set, the exception (i.e. the holiday) that is being created is valid for each year;
- "Month": mandatory field;
- "Day": mandatory field.

If, for example, you want to set a public holiday on the 25th December of each year, the choices to make are as follows:

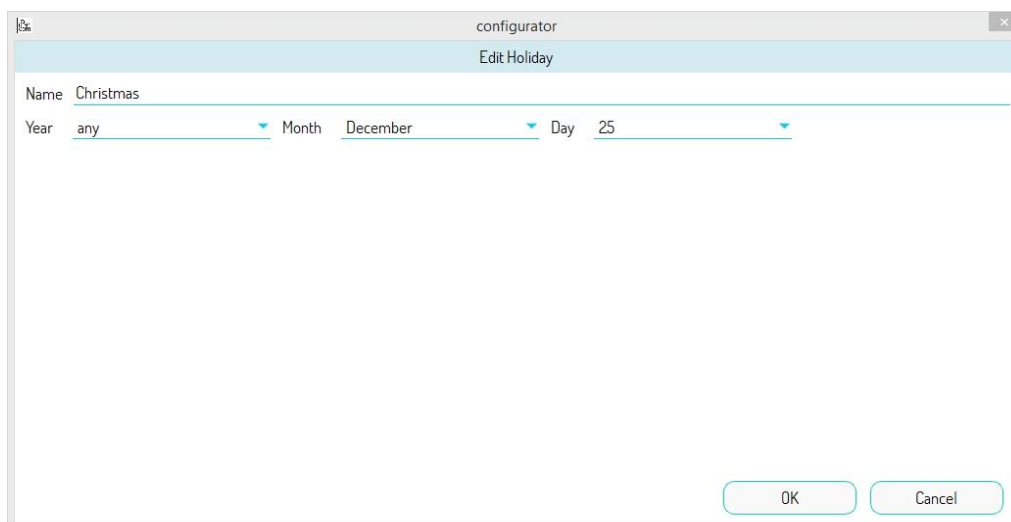


Figure 458: Set holiday

Press "OK" to see a summary of the choices made:

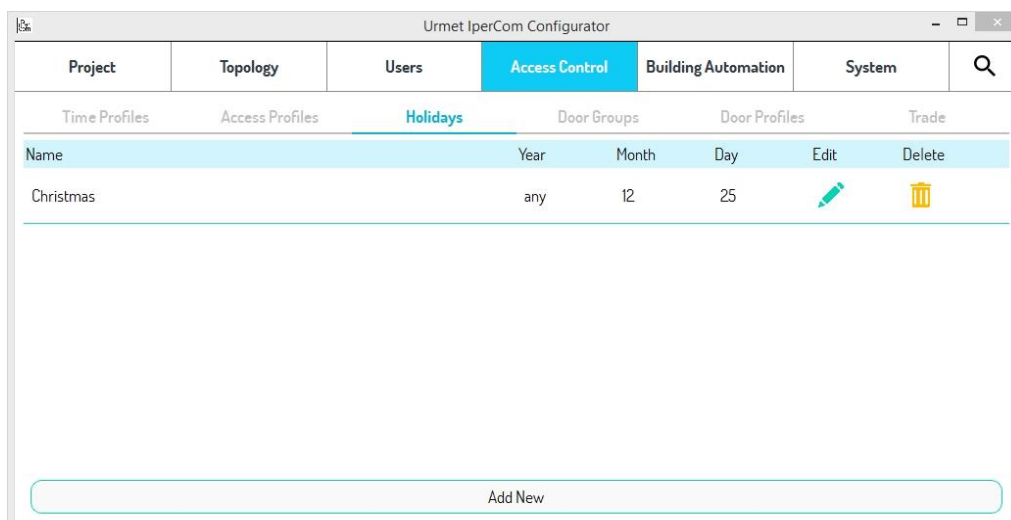


Figure 459: Created holiday

At this point, the following screen will appear when opening a previously created time profile, for example, where you can set a new time profile for the 25th of December of each year, as seen in the previous paragraph:

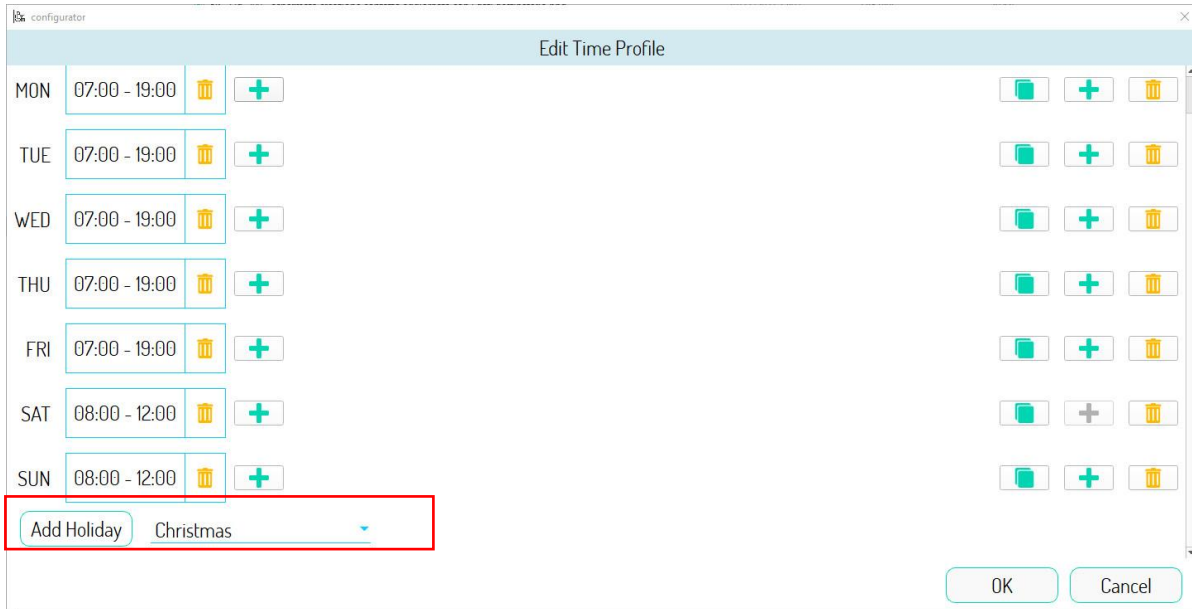


Figure 460: time profile with the possibility of adding a holiday

Press "Add Holiday" to open the following page:

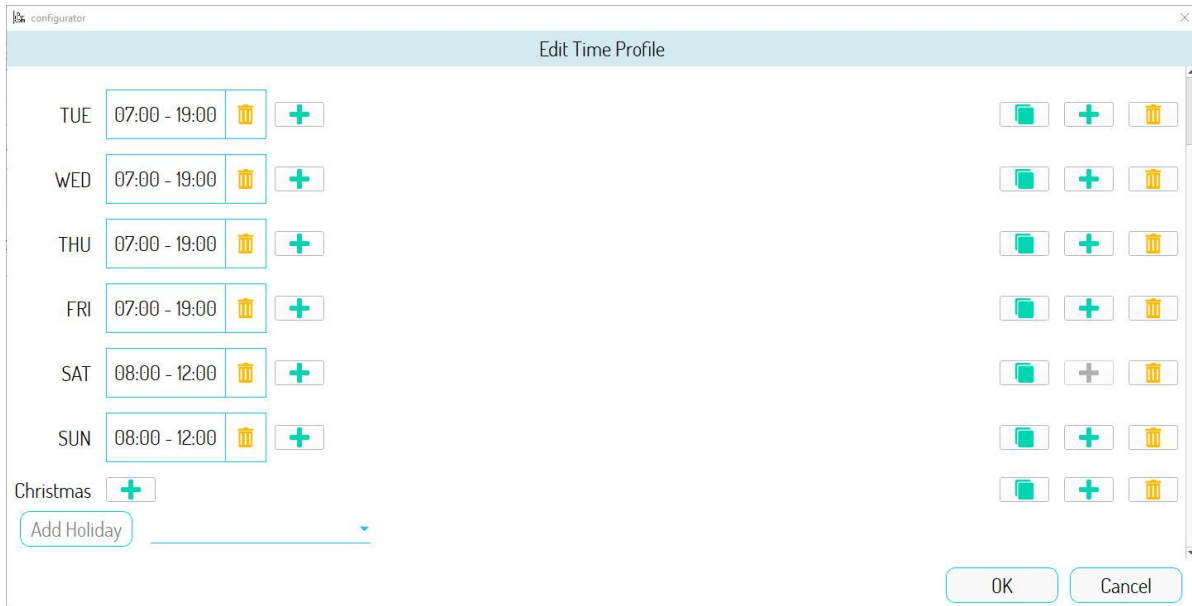



Figure 461: holiday added without setting any time

By pressing button  it is possible to create up to three time intervals within the holiday period.

Assuming you want to create a single interval from 8 to 10, the following page will appear:

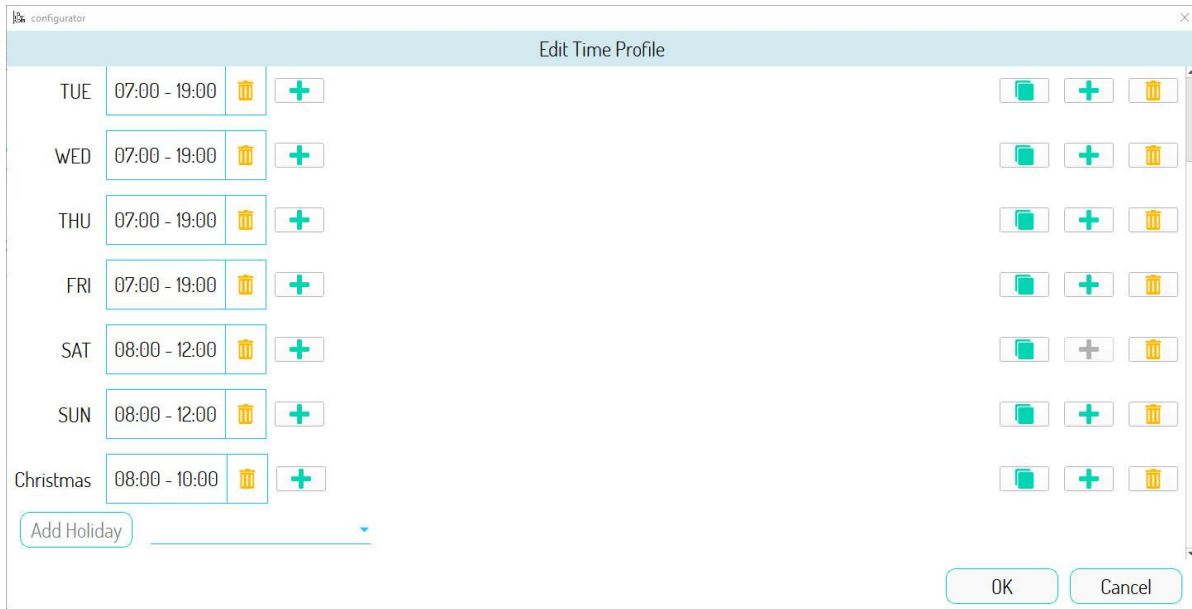


Figure 462: Additional holidays with timetables

The "OK" button confirms the changes made. In this way, the time profile followed on the day of the week coinciding with December 25th will be the one set in the newly created holiday, i.e. from 08:00 to 10:00.



*If the holiday is added without any time slot, entry will not be allowed for the entire day of the week coinciding with the holiday.*



### 7.1.9.4 Door groups

The **door group** is a set of doors that must obey the same rules, have the same temporal validity and the same temporal profile. The **Doors Group** function is useful if a group of people needs to access a group of doors in the same way.

To create a group of doors, go to the "Door Groups" screen in the "Access Control" tab. Once a group of doors has been created, it will be shown in the list of doors on the "Access Profiles" screen.

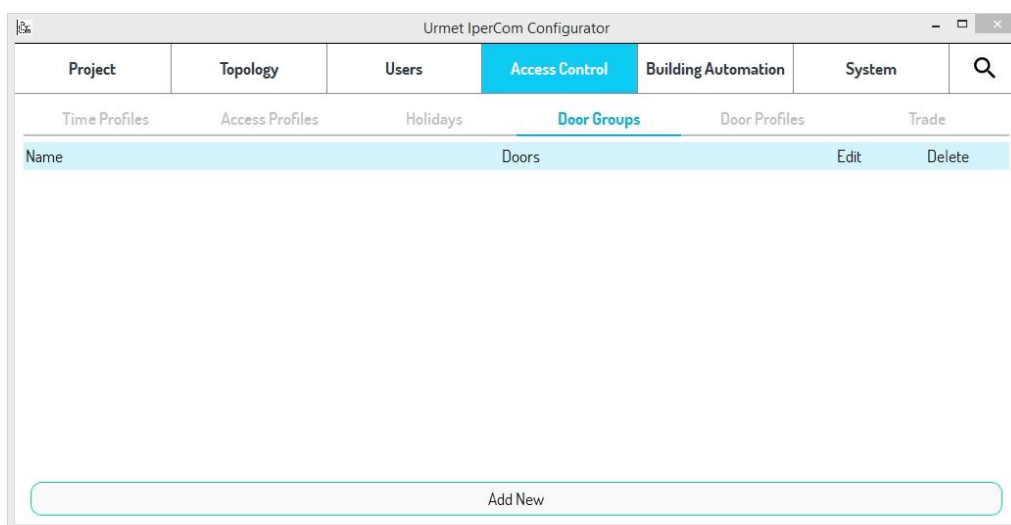


Figure 463: "Door Groups" screen

By pressing the "Add New" button a creation screen opens with a list of all available doors.

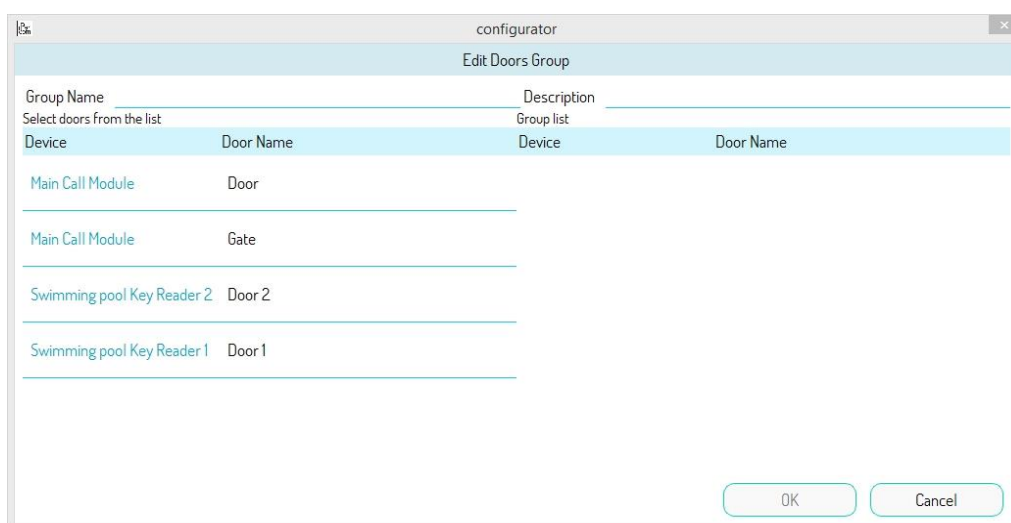


Figure 464: Screen of the door group creation

To create a group of doors, it is necessary to assign a name and select the desired doors: these are moved to a list on the right to form the desired list of doors.

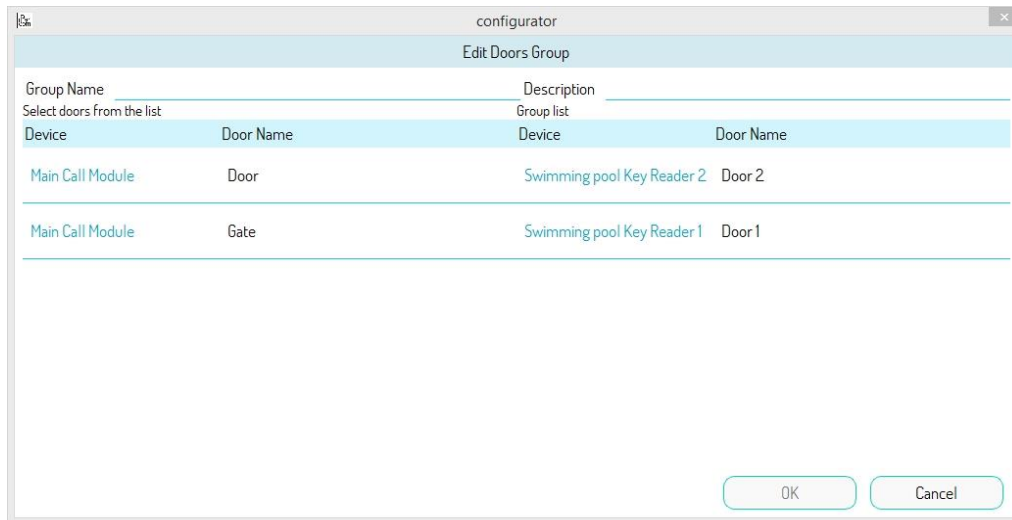


Figure 465: Selection of desired doors

To delete a door from the list, simply select it: it will be moved back to the list on the left.

Press the "OK" button to confirm the creation of the group of doors, which will appear in the "Door Groups" list.

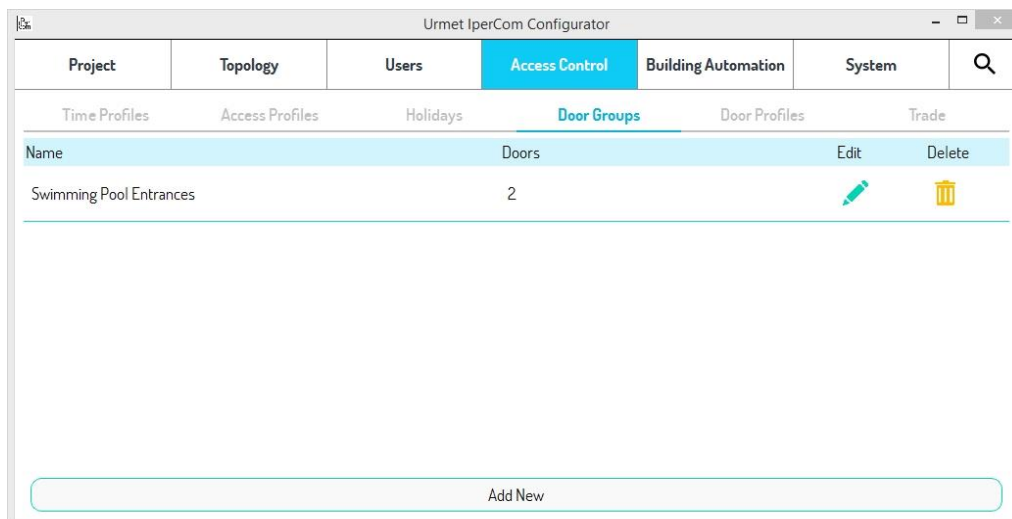


Figure 466: List of the created door groups

The buttons in the columns "Edit" and "Delete" allow you to modify the data or delete each door group created, respectively (through confirmation pop-up).

If you want to use the "Swimming pool doors" door group in the previously saved access profile, simply open it again and select as door group the group "Swimming pool doors" instead of the previously selected *Key Readers*.

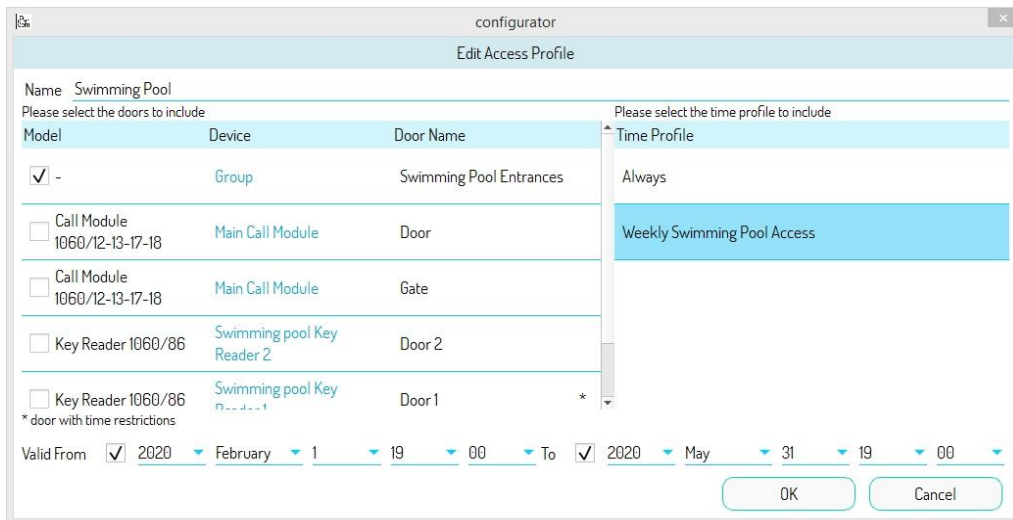


Figure 467: Selection of the new door group in the saved access profile

### 7.1.9.5 Door profiles

A **Door Profile** is a set of parameters that define the behaviour of a generic door. This functionality is useful if there are several doors in the system which must comply with the same rules. Instead of applying the set of rules several times to different doors, it is sufficient to create the set of rules once and then apply it to the individual doors.

To create an access profile, go to the "Access Control" page and then press the "Door Profiles" tab. The following page will appear:

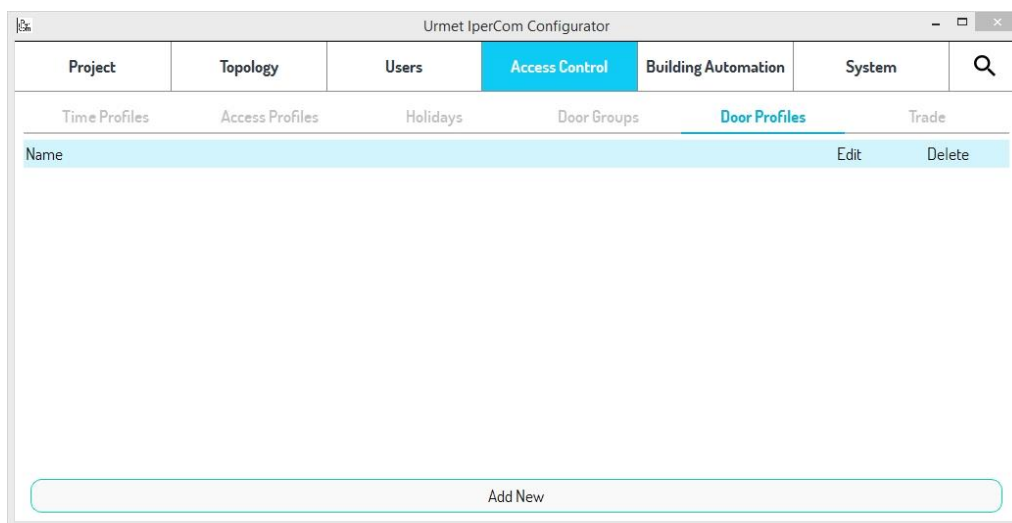


Figure 468: "Access Profiles" screen

Press "Add New" to open the following page:



Figure 469: Generic access parameters

For the meaning of the various parameters, see "[APPENDIX A: Configuration parameters of IPerCom devices](#)". An example of configuration is shown below:

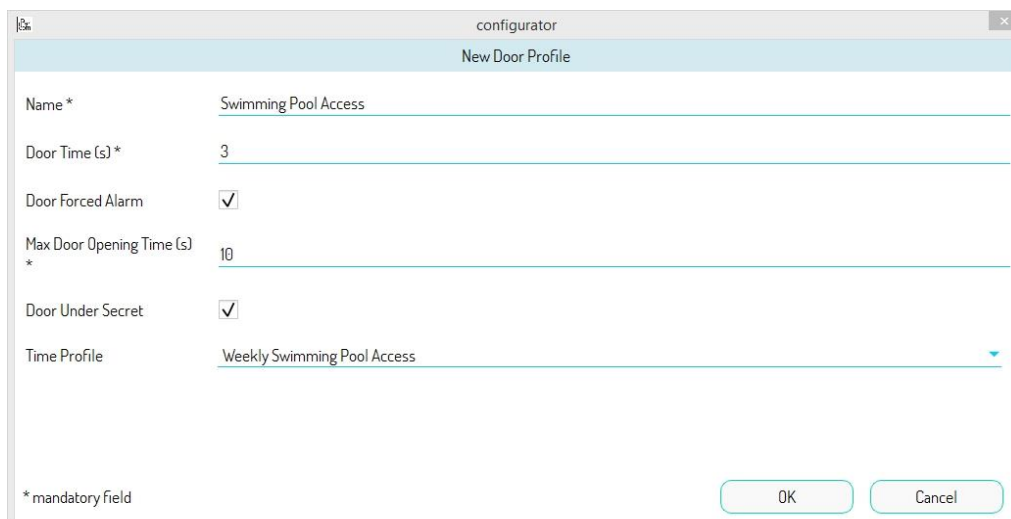


Figure 470: Setting parameters for an access

Press "OK" to create the access profile:

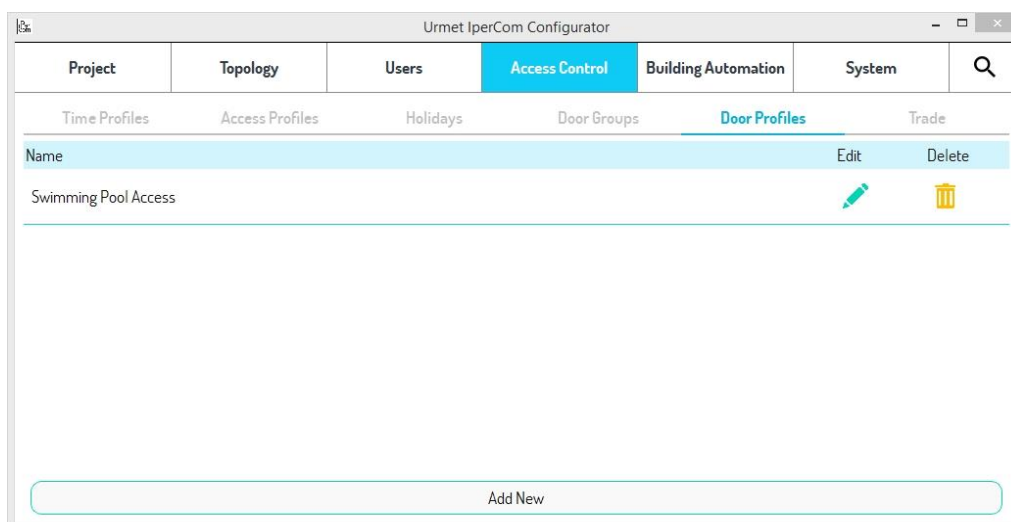


Figure 471: Creating an access profile

Once the access profile has been created, it can be applied to several doors. For example, if there are two *Key Readers* in the system that must give access to a swimming pool during the summer with the opening profile filled in above, you must load the newly created *Key Reader* in the "Door Profile" item.

To do this you need to go to the "Topology" page, then to the "Devices" tab:

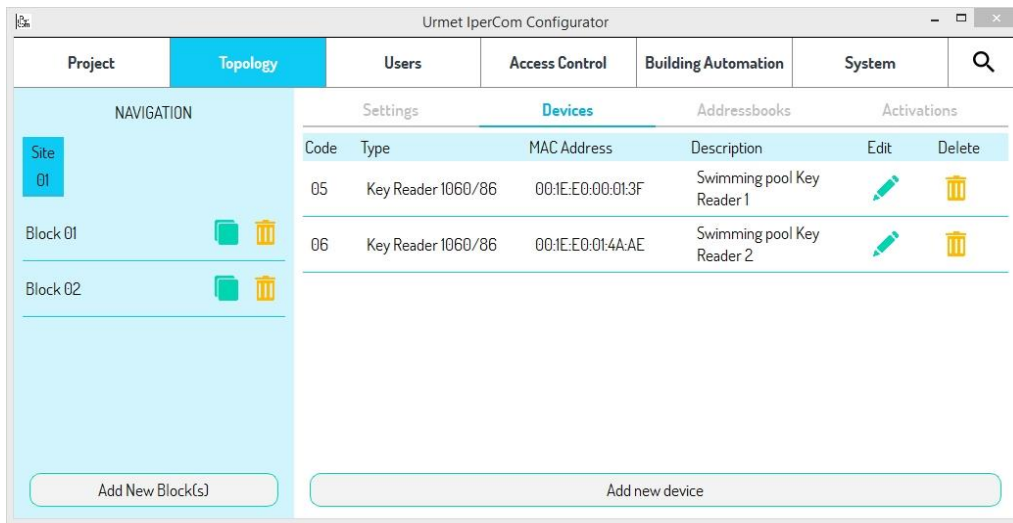


Figure 472: Devices on which to load the access profile

Press the "Edit" button of the first Key Reader to open the following screen where "Custom" appears next to the concerned access (i.e. no profile is loaded and each field can be filled in individually):

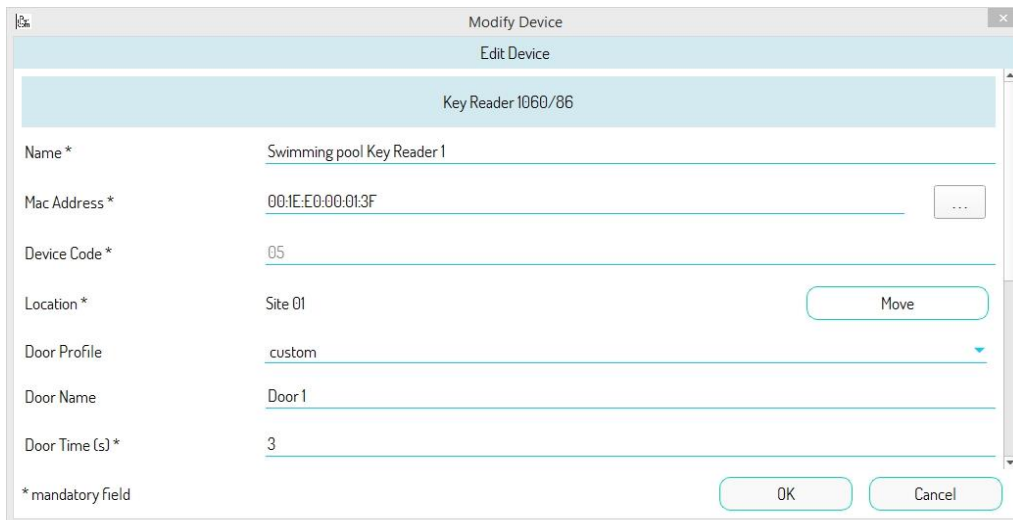


Figure 473: Key reader without door profile

Click on "custom" to choose the previously created access:

The screenshot shows a 'Modify Device' window for a 'Key Reader 1060/86'. The 'Door Profile' dropdown is open, with 'custom' selected. The 'Swimming Pool Access' option is also visible. Other fields include Name (\*), Mac Address (\*), Device Code (\*), Location (\*), Door Name, and Door Time (s) (\*). Buttons for 'Move', 'OK', and 'Cancel' are present.

Figure 474: Selecting a door profile

Press the "OK" button to load the door profile on the concerned door:

The screenshot shows the 'Modify Device' window with the 'Door Under Secret' checkbox checked. The 'Time Profile' dropdown is set to 'Weekly Swimming Pool Access'. The 'Remote Relay', 'Remote Button', and 'Activations' fields are greyed out, indicating they are loaded from the profile. Buttons for 'Select', 'Clear', and 'Add' are visible for the greyed-out fields. 'OK' and 'Cancel' buttons are at the bottom.

Figure 475: Loading the access profile

The loaded parameters are greyed out to highlight the fact that they come from a previously created access profile.



*The access profiles can be loaded on the doors of the Call Modules, Entry Panel, Key Reader devices. If some parameters are not present on the doors, these parameters are not loaded.*

### 7.1.9.6 Trade

The **trade** function allows opening the pedestrian door and/or the driveway (if enabled) directly from the *Call Modules* and *Modular Entry Panel with 1060/48* keypad during a time set during the creation of the *trade* itself.

The application can be useful if external personnel needs to access the residential complex in pre-set time intervals.

The *Trade* function is set on the "Access Control" page via the "Trade" tab.

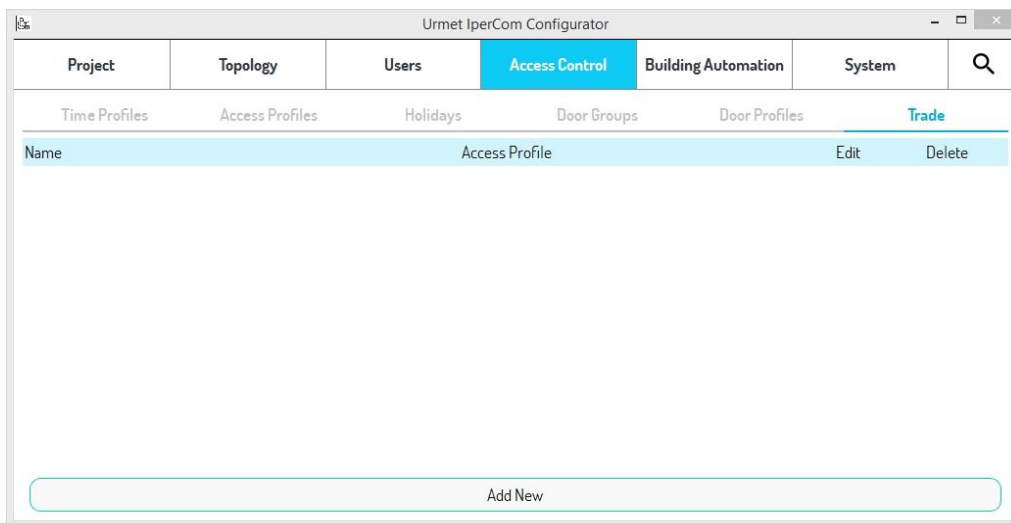


Figure 476: "Trade" screen

Trade is an access profile that groups together the accesses (pedestrian door and/or gate) of one or more *Call Modules* or *Modular Entry Panel with 1060/48*. This access profile can be associated with a profile and/or a time validity. For special needs, it is also possible to associate a time profile with the accesses. Once this access profile has been created, press the "Add" button to open a screen with all the created access profiles.

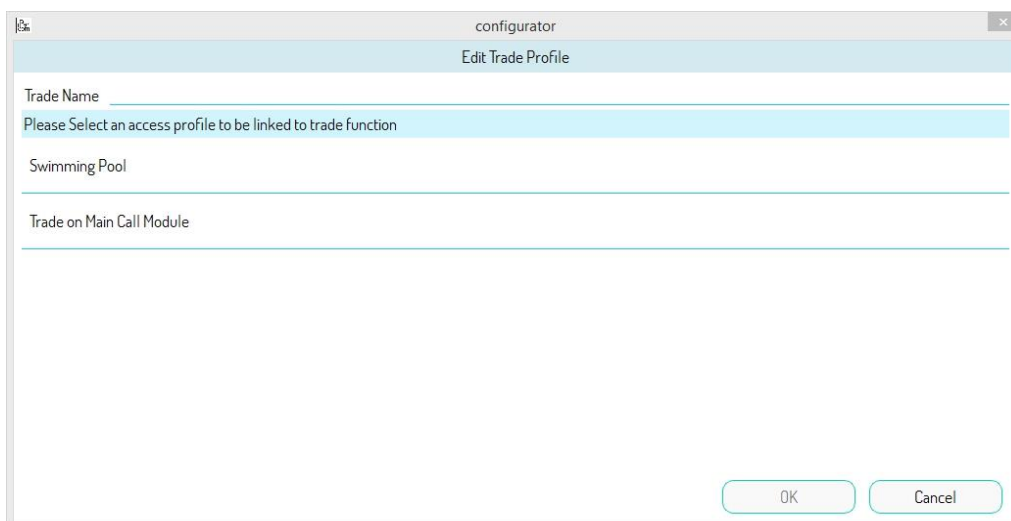


Figure 477: Trade creation screen



In the screen above you need to select the access profile created as a trade. After assigning a name to the *trade*, pressing the “OK” button the trade is created and added to the list of available trades.

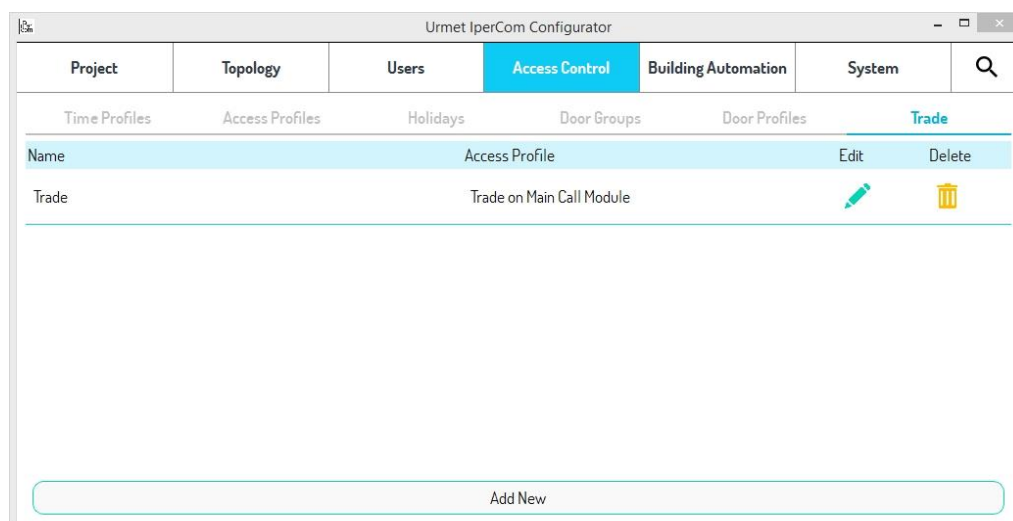


Figure 478: List of created trades

The buttons in the columns "Edit" and "Delete" allow you to modify the data or delete each *trade* created, respectively (through confirmation pop-up).



*The "Trade" function cannot be applied to calling stations 1060/21-71-74-75-78.*



*In systems with lift interface Ref. 1060/37, the door opening through the trade function does not allow the lift to reach the floors or apartments of the residential complex.*

For correct application of the “Trade” function, see the user manual of *Elekta and Elekta Steel Call Modules 1060/12-13-17-18* and *Alpha Display Module 1168/1 for Modular Entry Panel with 1060/48*.

### 7.1.10 System parameters

The "System" tab allows setting several parameters related to the system operation and its performance. For simplicity, the parameters have been divided into the following sections:

- "Global Settings",
- "Door/Gate Settings",
- "Call Forwarding Settings",
- "Call Divert settings"
- "Network Settings",
- "Custom Network Settings",
- "Maintenance Settings".
- "Sunrise/Sunset Settings",

For each parameter it is possible to select the relevant values through intuitive drop-down menus.

Once the value of one or more parameters has been set, the "Apply" button at the bottom of the screen allows you to apply the selected settings.

The screen displayed by pressing the "System" tab is as follows:

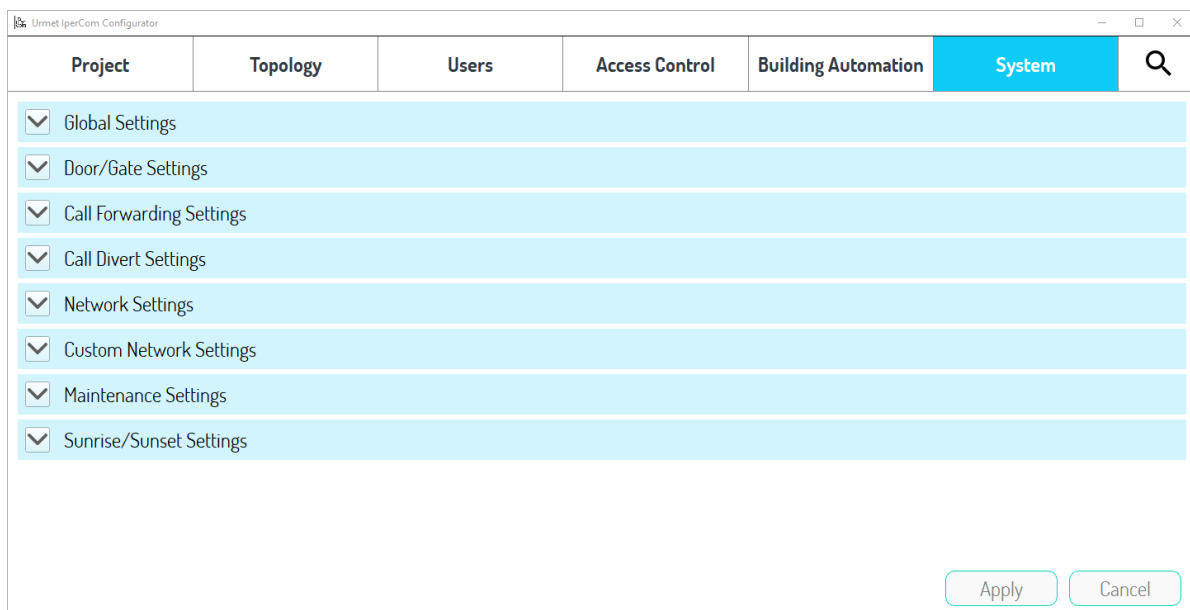


Figure 479: "System" tab

The meaning of the parameters of the various sections listed above is described below.

### 7.1.10.1 Global Settings

The parameters are shown in the following figures:

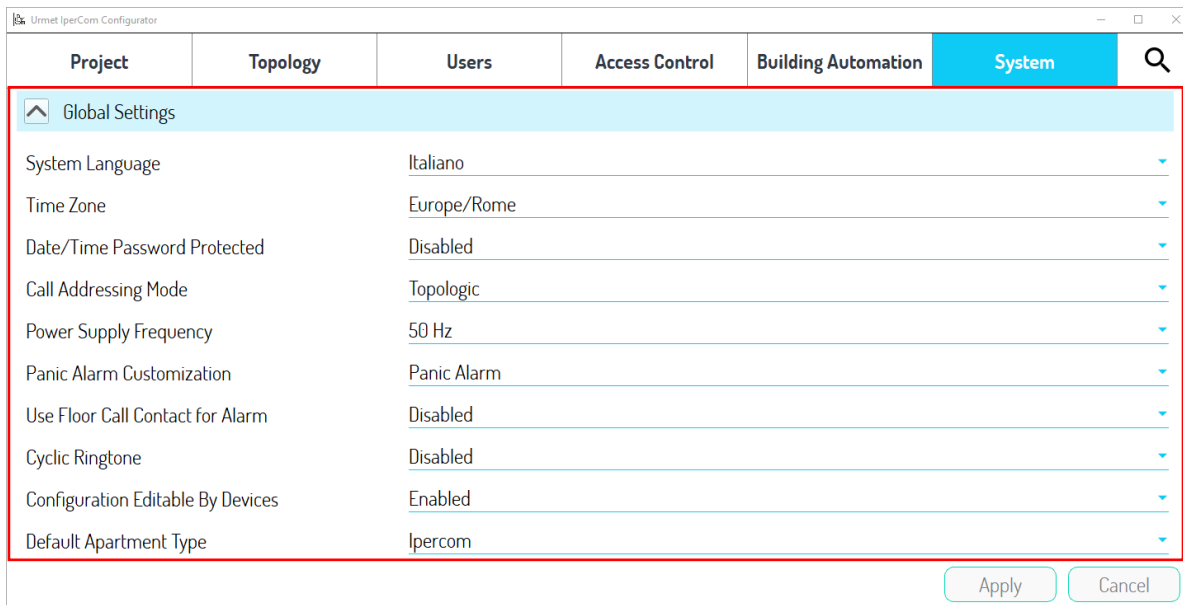


Figure 480: "System" tab - "Global Settings" (first part)

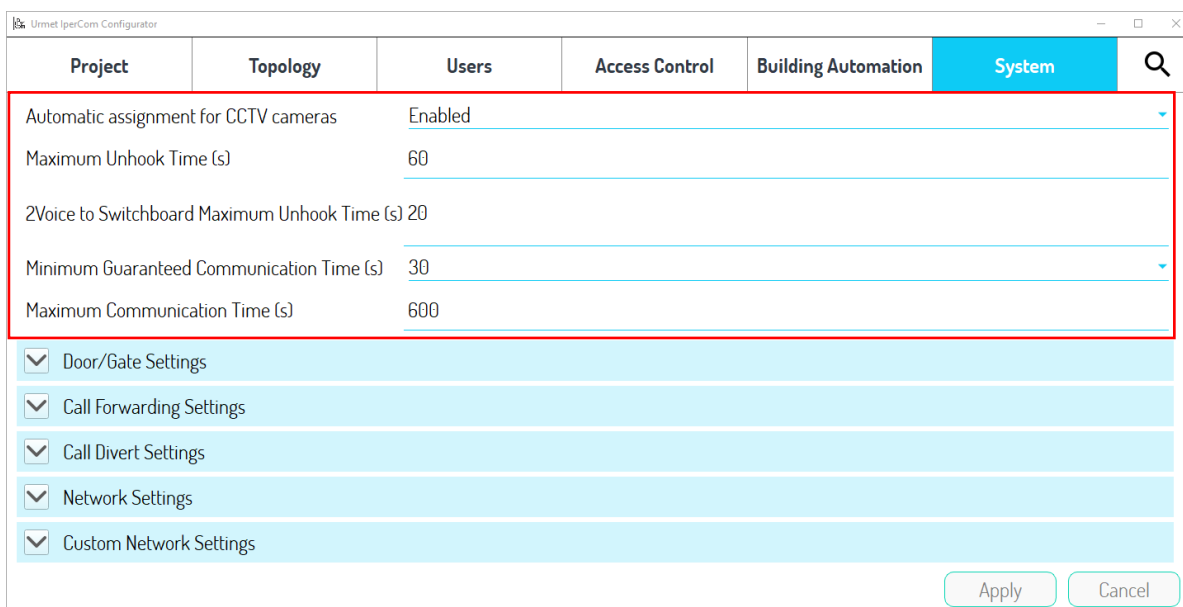


Figure 481: "System" tab - "Global Settings" (second part)

The meaning of the single items is shown in the following table:

<i>System Language</i>	Language used by <i>IPerCom</i> devices with display or <i>IPerCom</i> applications with graphical interface ( <i>Switchboard</i> and <i>IPerCom Client</i> ).
<i>Time Zone</i>	Time zone selected for time management. Default value: "Europe/Rome".
<i>Date/Time Protection with Password</i>	If enabled, date and time can be modified from <i>MAX</i> , <i>VOG</i> <sup>7</sup> or <i>Basic</i> video door phones only with password and password entry field is shown just below the item "Date/Time Protection with Password". Default value: disabled.
<i>Call Addressing Mode</i>	Mode used to call an apartment from calling stations with alphanumeric keypad. Allowed values: "Topologic", "Numeric", "Logic", "Block Mode". For further details see the paragraph <a href="#">Call addressing mode</a> .
<i>Numeric Codes Assignment</i>	The field is visible only if "Numeric", "Logic" or "Block mode" is chosen as the type of addressing: in this case it is possible to assign the codes to the apartments in automatic or manual mode.
<i>Power supply frequency</i>	Frequency of the electric power supply. Default value: 50Hz.
<i>Panic Alarm Customization</i>	This function allows customizing the type of alarm sent to the <i>Switchboard</i> by apartment stations (only if the alarm is generated by the relative external terminals).
<i>Use Floor Call Contact for Alarm</i>	If enabled, the floor call button of all the apartment stations in the system allows you to send to the <i>Switchboard</i> a type of alarm among those listed. Default value: disabled.
<i>Cyclic Ringtone</i>	If enabled, the chime assigned to an apartment station is repeated cyclically during the entire call phase. Default value: disabled.
<i>Configuration Editable by Devices</i>	The value is disabled and cannot be modified if at least one 1060/1 <i>Server</i> is present in the system. If there is no 1060/1 <i>Server</i> in the system, the configuration can be modified from the <i>MAX</i> , <i>VOG</i> <sup>7</sup> and <i>Basic</i> video door phones only if the system model chosen during the configuration phase is the "Villa Kit (one-household)". If the <i>CallMe Manager Support</i> parameter is enabled, it is not possible to access the configuration from the video door phones listed above (the item in question is not present).

<p><i>Default Apartment Type</i></p>	<p>If the <i>IPerCom</i> value is set, all the apartments added in the configuration are of the <i>IPerCom</i> type, that is with at least one apartment station; if the <i>IPerCloud</i> value is set, all the apartments added in the configuration are of the <i>IPerCloud</i> type, that is they can have no apartment station. The <i>IPerCom/IPerCloud</i> choice does not preclude the possibility of subsequently changing the value from the <i>configurator</i> on each individual apartment. Default value: <i>IPerCom</i>. <u>The field can be modified only if <i>configurator</i> is started from <i>IPerCom Installer Tools</i>. On the contrary, the field cannot be modified if:</u>  <u>-) <i>configurator</i> is started by the video door phones that integrate it;</u>  <u>-) <i>configurator</i> is started by opening a configuration file with <i>ccf</i> extension.</u></p>
<p><i>Automatic Assignment for CCTV Cameras</i></p>	<p>If enabled, the camera address book of video door phones automatically presents all the calling stations and RTSP cameras located on the topological path of the respective apartment nodes. If disabled, the camera address book must be created via the <i>Contacts</i> tab of the configurator. Default value: enabled.</p>
<p><i>Maximum Unlook Time (s)</i></p>	<p>Answer waiting time after which the call is missed. Min: 30s, Max: 120s. Default value: 60s.</p>
<p><i>2Voice to Switchboard Maximum Unhook Time (s)</i></p>	<p>Answer waiting time from 2Voice apartment station to <i>Switchboard</i> after which the call is missed and stored in the missed calls of the <i>Switchboard</i>. Min: 10s, Max: 30s. Default value: 20s</p>
<p><i>Maximum Guaranteed Communication Time (s)</i></p>	<p>Guaranteed communication time. Min 1s, Max: 90s (in steps of 10s). With at least one <i>IPercom 2Voice Gateway</i> in the system, the maximum value decreases to 70s. Default value: 30s.</p>
<p><i>Maximum Communication Time (s)</i></p>	<p>Maximum conversation duration time (in the absence of interruptions) between calling station and apartment station and between 2 apartment stations. The set value also applies for auto-on. Min: 30s, Max: 600s. Default value: 600s.</p>

Table 16: meaning of the parameters in the "Global Settings" section



*If the cyclic ringtone is enabled, it is recommended not to use voice commands on video door phones but gesture commands to enable the main video door phone functions.*



*All alarms generated by external terminals (except the panic alarm) can only be reset from the Switchboard: for this type of alarm, therefore, it is necessary that at least one Switchboard application is present on the system. The panic type alarm can be reset from the switchboard or from the same video intercom that generated it.*



Regarding the item “Automatic Assignment for CCTV Cameras”, the CallMe app linked to the apartment behaves as shown below.

*Item “Automatic Assignment for CCTV Cameras” enabled*

*The list of cameras in the CallMe app on which making auto on is the same as the apartment video door phone or video door phones, excluding any RTSP cameras. In detail, all the calling stations placed on the topological path of the apartment node are shown and any calling stations added manually via the “Contacts” tab.*

*Item “Automatic Assignment for CCTV Cameras” disabled*

*The list of cameras in the CallMe app on which making auto on is the same as the apartment video door phone or video door phones, excluding any RTSP cameras. In detail, all the calling stations added manually via the “Contacts” tab are shown. If no calling station is manually added, the list will be empty.*

### 7.1.10.2 Door/Gate Settings

The parameters are shown in the red rectangle in the following figure:

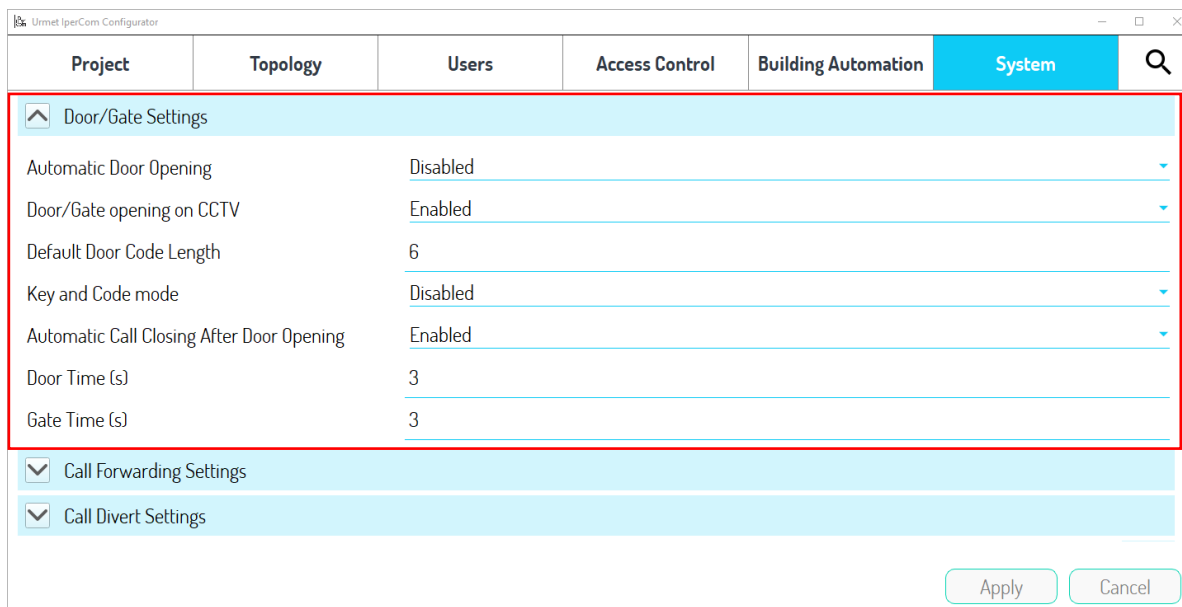




Figure 482: "System" tab – "Door/Gate Settings"


The meaning of the single items is shown in the following table:


<i>Automatic Door Opening</i>	If enabled, it allows the automatic opening of the doors during the call phase. Default value: disabled. The function must also be locally enabled on apartment station. Default value: not enabled.
<i>Door/Gate opening on CCTV</i>	If disabled, it allows door/gate opening only and exclusively during the call step. Default value: enabled (it is possible to open door/gate also in auto-on).
<i>Default Door Code Length</i>	Numeric door opener code length for residents and non-residents. Default value: 6 (min 4, max 8).
<i>Key and Code mode</i>	If enabled, the access to the doors of the <i>Call Module</i> and <i>Modular Calling Station with 1060/48</i> occurs using both the <i>Proximity Key</i> and the <i>Door Code</i> associated to the user. Default value: disabled.
<i>Automatic Call Closing After Door Opening</i>	If enabled, if the door is opened during the unhook time or during the conversation, the call is automatically closed 10s after sending the door opening command. Similarly, if the door is opened during auto on (with mono or bidirectional audio), the same auto on is automatically closed 10s after sending the door opening command. Default value: enabled.
<i>Door Time (s)</i>	Door opening time. Default value: 3s.
<i>Gate Time (s)</i>	Gate opening time. Default value: 3s.

Table 17: meaning of the parameters in the "Door/Gate Settings" section

 *If the door is opened during the unhook time and the call is also answered within 10s, the call itself is no longer closed automatically.*

 *With automatic call closing after door opening function enabled, if the door is opened during the unhook time, any call divert enabled on the called apartment is ignored.*

 *If during an auto-on on a calling station the pedestrian door is opened and within 10s you make a cyclic sequence to other calling stations (or RTSP Cameras), the auto-on remains active even 10s after the previous door opening.*

 *Regarding the item “Door/Gate opening on auto-on”, the CallMe app linked to the apartment behaves as shown below.*

*Item “Door/gate opening on auto on” enabled*

*It is possible to open the door and the gate both from the Home Page of the CallMe app and during an auto-on from the CallMe app itself.*

*Item “Door/gate opening on auto on” disabled*

*It is not possible to open the door and the gate either from the Home Page of the CallMe app or during an auto-on from the CallMe app itself.*



### 7.1.10.3 Call Forwarding Settings

The parameters are shown in the following figure:

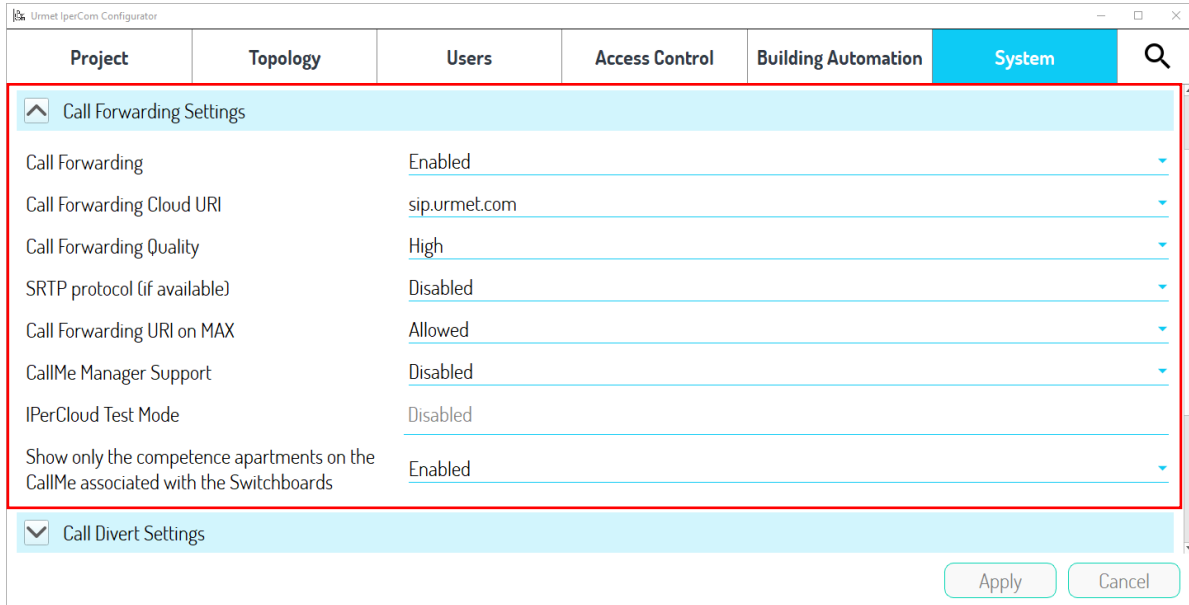


Figure 483: "System" tab – "Call Forwarding Settings"

The meaning of the single items is shown in the following table:

<i>Call forwarding</i>	If enabled, it allows call forwarding on smartphone/tablet. Default value: enabled.
<i>Call forwarding Cloud URI</i>	SIP server where to register the user for call forwarding on smartphone/tablet. Default value: sip.urmet.com
<i>Call Forwarding Quality</i>	Video quality of the call forwarded to a smartphone/tablet. Allowed values: “High”, “Medium”, “Low”. Default value: “High”.
<i>SRTP protocol (if available)</i>	If enabled, it allows to enable the SRTP protocol on all calling stations (except the 1060/12-13-17-18-23 <i>Call Module</i> ), all apartment stations and apps <i>Switchboards</i> and <i>IPerCom Client</i> : in this way calls to the <i>CallMe</i> application and from the <i>CallMe</i> application are encrypted. Default value: disabled.
<i>Call Forwarding URI on Max</i>	If enabled, it allows modifying the username registered on the SIP server for call forwarding on smartphone/tablet from the <i>MAX</i> , <i>VOG<sup>7</sup></i> or <i>Basic</i> video door phones. If not enabled, the user’s name is the one defined by the <i>configurator</i> in the apartment settings. The following parameter is visible in the settings only if the parameter “ <i>CallMe Manager support</i> ” is disabled.
<i>CallMe Manager Support</i>	If enabled, it allows you to activate the call forwarding function through the support of the <i>CallMe Manager</i> app. Furthermore, if enabled, it is not possible to access the configuration and modify it from the <i>MAX</i> , <i>VOG<sup>7</sup></i> or <i>Basic</i> video door phones connected to the system (and configured). Default value: disabled (the value automatically switches to enabled if one or more apartments are set in IPerCloud mode during the configuration). <u>The field can be modified only if the configurator is started from IPerCom Installer Tools. On the contrary, if it is started by the video door phones that integrate it, the field cannot be modified.</u>
<i>IPerCloud test Mode</i>	If enabled, this mode allows you to check the correct functioning of the IPerCloud system through a test apartment (IPerCloud). To correctly execute the test mode, see the <a href="#">IPerCloud Test Mode</a> paragraph. Default value: disabled. <u>The field can be modified only if the configurator is started from IPerCom Installer Tools and if CallMe Manager support is enabled. On the contrary, if it is started by the video door phones that integrate it, the field cannot be modified.</u>
<i>Show only the competence apartments on the CallMe associated with Switchboards</i>	If the item is enabled, only the <u>competence apartments</u> will be visible on the <i>CallMe</i> app linked to the <i>Switchboard</i> application, that is the apartments that are placed in the topological group of the <i>Switchboard</i> application. However, if the item is disabled, all the apartments in the system will be visible. Default value: enabled.

Table 18: meaning of the parameters in the “Call Forwarding Settings” section



*If CallMe Manager support is disabled and IPerCloud apartments are present in the configuration, these are automatically set to IPerCom mode.*

### 7.1.10.4 Call divert settings

The parameters are shown in the following figure:

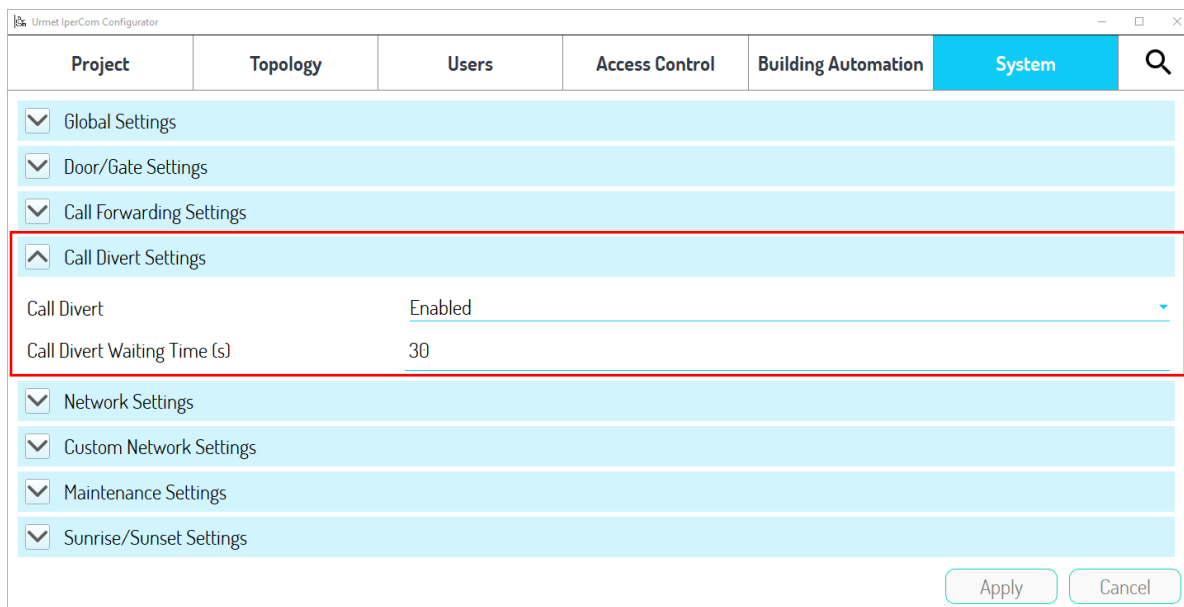






Figure 484: "System" tab – "Call Divert Settings"

The parameter meaning is as follows:

<i>Call Divert</i>	If enabled, it allows diverting the direct call to an apartment station (including <i>IPerCom Client</i> application) towards relevant switchboards or towards the contacts in the address book. Default value: enabled.
<i>Call Diversion Waiting Time (s)</i>	Waiting time after which the call is diverted to another apartment station. Immediate diversion is also possible. Default value: 30s.

Table 19: meaning of the parameters in the "Call Divert Settings" section

-  In addition to the configurator, the call divert function must also be enabled on the video door phone apartment stations and *IPerCom Client* application. For further details, see the user's manuals available at [www.urmet.com](http://www.urmet.com).
-  The call divert function cannot be set on the Miro door phone 1160/3 or video door phone 1761/6.
-  The call diversion function can only be set on the master video door phone (or *IPerCom Client* application) in the apartment.
-  From the *CallMe* app it is not possible to call an apartment station on which the call forwarding function has been set up.

### 7.1.10.5 Network settings

The parameters are shown in the following figure:

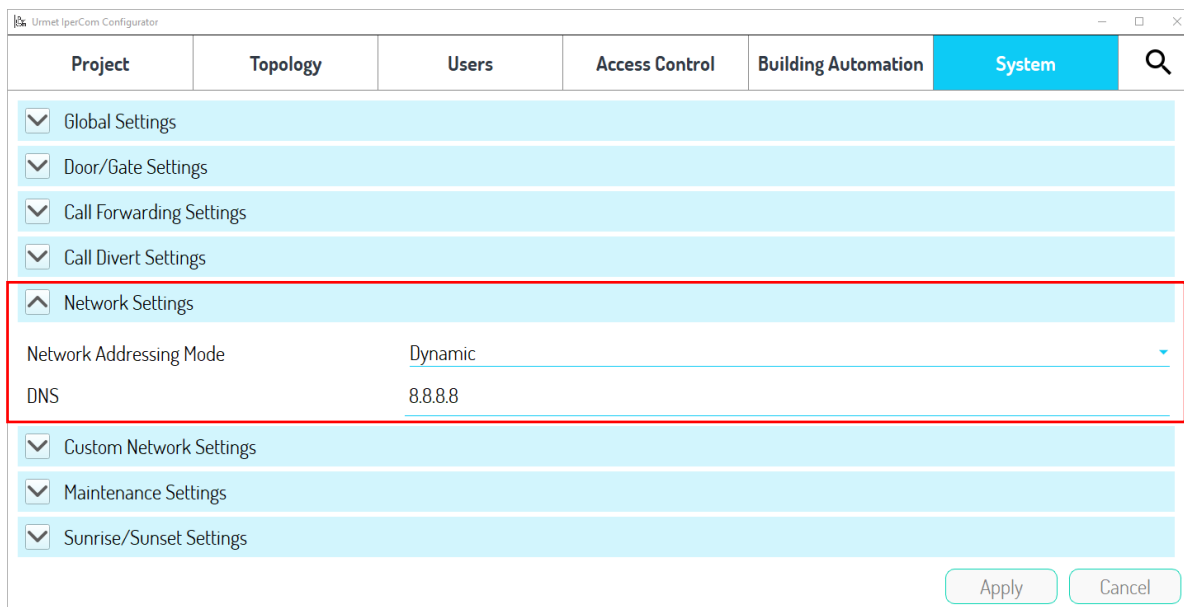


Figure 485: "System" tab – "Network Settings"

The parameter meaning is as follows:


#### NETWORK SETTINGS


<i>Network Addressing Mode</i>	The "Dynamic" item means that the devices automatically acquire an IP address consistent with the network in which they are installed (networks with DHCP server); the "Static" item allows you to set the IP address range according to your needs and depending on the network in which the system is installed (networks without DHCP server).
<i>DNS</i>	IP addresses of the DNS server (default value: 8.8.8.8)


Table 20: meaning of the parameters in the "Network Settings" section




After a change in network addressing mode (from dynamic to static or vice versa), it is recommended (after the configuration distribution) to **restart all switches in the system**. If this is carried out through a main switch, make sure that the Server 1060/1 is connected to a UPS (uninterruptible power supply) device to avoid irreparable damage caused by a sudden power failure. In the absence of UPS, it is necessary to turn off the Server 1060/1 through the dedicated button and then turn it on again after restoring power supply to the system. Restarting the switches (in the same way as described above when there is a main switch) is recommended if a router with DHCP service is added to the system or removed from the system.

 After a change in network settings, any devices in the system with a static IP address (e.g. RTSP cameras) must be made compatible with the new address assigned to the system.

 If a system contains MAX 1717/3x, MAX 1717/2x and/or VOG7 1761/3x video door phones to also be connected to domestic networks via the second LAN connector, it is recommended to configure the network for the IPerCom system with addresses of the type “10.x.y.z” and not the “192.168.x.y” type usually used in common home networks. In general, pay particular attention not to have devices with multiple network interfaces with subnets that can overlap.

 If a static network setting is selected, it is also necessary to set the “IP Range Minimum”, “IP Range Maximum”, “Network mask”, “Default Gateway” and “DNS” parameters. These parameters are the same as those presented in the “Custom Network Settings” section and their meaning is explained in the following paragraph. In general, refer to a network administrator for the correct configuration of the network itself.

 If it is necessary to configure a system with Server 1060/1 where CallMe Manager support and static IP addressing is required, follow the steps below:

- configure the PC with IPerCom Installer Tools in link local addressing;
- create the configuration only with Server 1060/1;
- set the static addressing mode on the system;
- connect the Server 1060/1 to the system;
- configure the PC with IPerCom Installer Tools with addressing compatible with the chosen static addressing;
- verify that Server 1060/1 has a consistent address;
- configure the rest of the system.

### 7.1.10.6 CUSTOM NETWORK SETTINGS

The parameters are shown in the following figure:

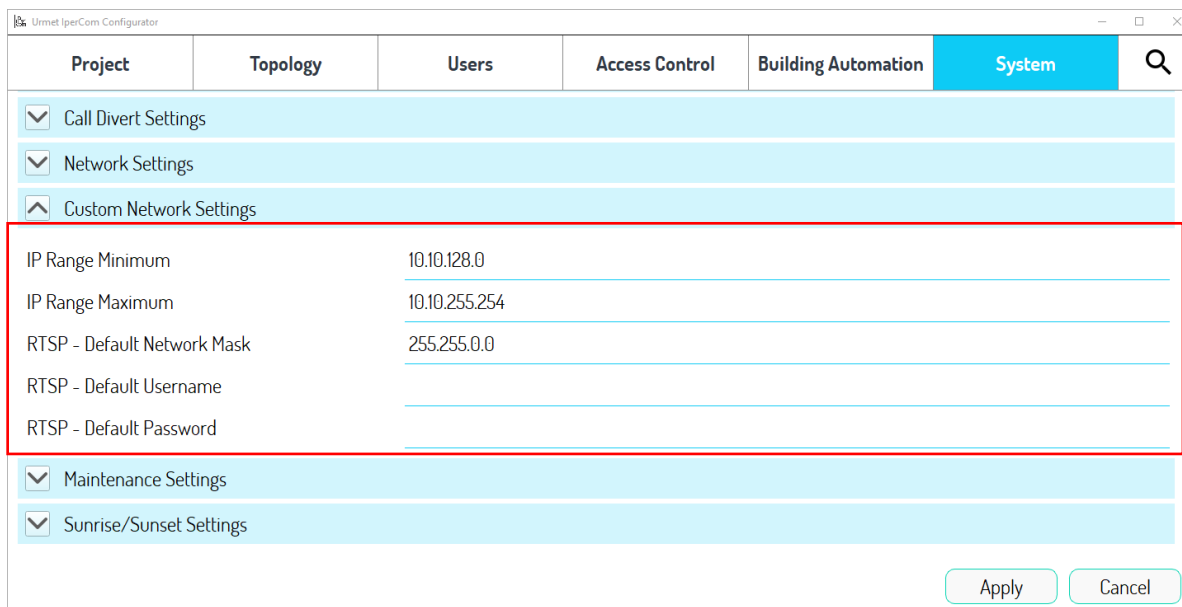


Figure 486: "System" tab - "Custom Network Settings"

The parameter meaning is as follows:

<i>IP Range Minimum</i>	Lower limit of the IP address range for the custom subnet you are creating
<i>IP Range Maximum</i>	Upper limit of the IP address range for the custom subnet you are creating
<i>RTSP - Network Mask</i>	Custom subnet mask you are creating
<i>RTSP - Default Username</i>	Username to view the RTSP streaming video from calling stations (if enabled)
<i>RTSP - Default Password</i>	Password to view the RTSP streaming video from calling stations (if enabled)

Table 21: meaning of the parameters in the "Custom Network Settings" section

For more details on how to use custom network settings, see [APPENDIX F1: How to use customized network settings in IperCom system](#).



*If a static network setting is chosen for the IPerCom system, the IP address assigned to any IPerCom device can be customized by choosing a value from those defined in the "Customized Network Settings" section (for further details see [APPENDIX F2: Custom network settings and editable static IP addresses for IPerCom devices](#)).*



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.



It is possible to leave the "RTSP - Default Username" and "RTSP - Default Password" fields blank: in this case the "Username" and "Password" fields must be filled in individually for each call station with the RTSP streaming function enabled.



The "Username" and "Password" fields of the RTSP Cameras are not automatically populated with the values set in the "RTSP - Default Username" and "RTSP - Default Password" fields.

### 7.1.10.7 Maintenance Settings

The parameters are shown in the following figure:

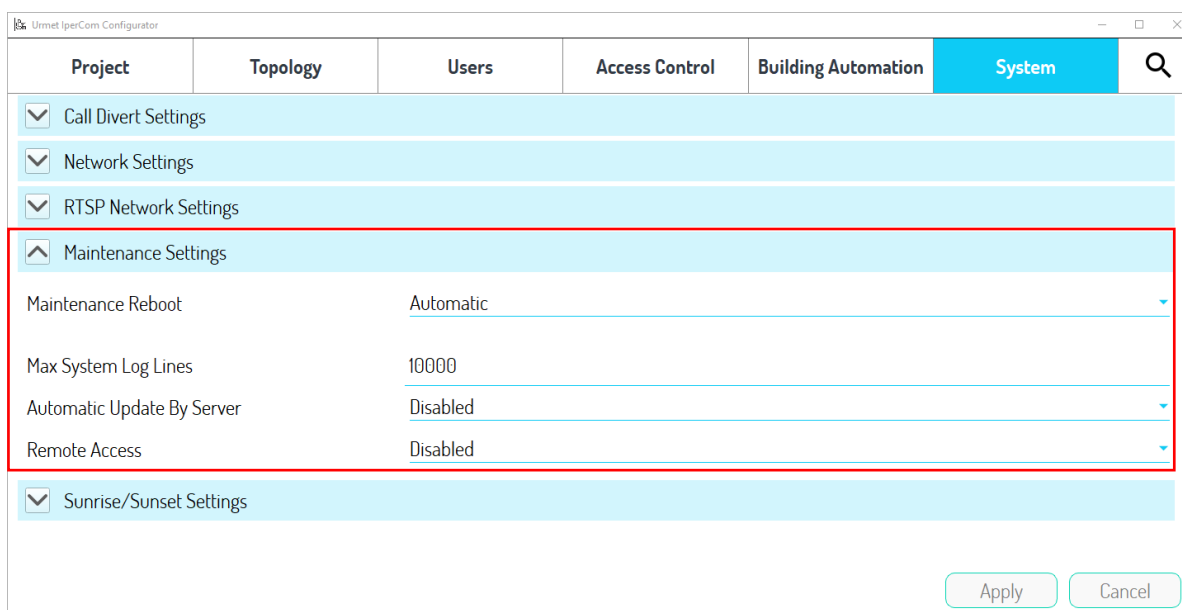


Figure 487: "System" tab - "Maintenance Settings"

The parameter meaning is as follows:

<i>Maintenance Reboot</i>	"Automatic" means that all devices in the system restart at 4:00 am. "Manual" allows you to change the time (at half-hourly intervals) and set weekly reboot days for the displayed devices.
<i>Max System Log Lines</i>	Number of events that can be displayed in the "System logs" of IPerCom Installer Tools. Default value: 10000. Maximum value: 100,000
<i>Automatic Update by Server</i>	If enabled, it allows the firmware upgrade of the devices through the Server 1060/1. Default value: disabled.



<i>Remote Access</i>	If enabled, it is possible through <i>IPerCom Installer Tools</i> to connect to a remote system. Default value: disabled.
----------------------	---

*Table 22: meaning of the parameters in the "Maintenance Settings" section*



*For manually scheduled restarts, it is necessary to respect the constraint of at least 2 restarts every 4 days.*



*Devices such as Relay Actuator, Key Reader and Lift Interface cannot be restarted either automatically or manually.*

### 7.1.10.8 Sunrise/Sunset Settings

The parameters are shown in the following figure:

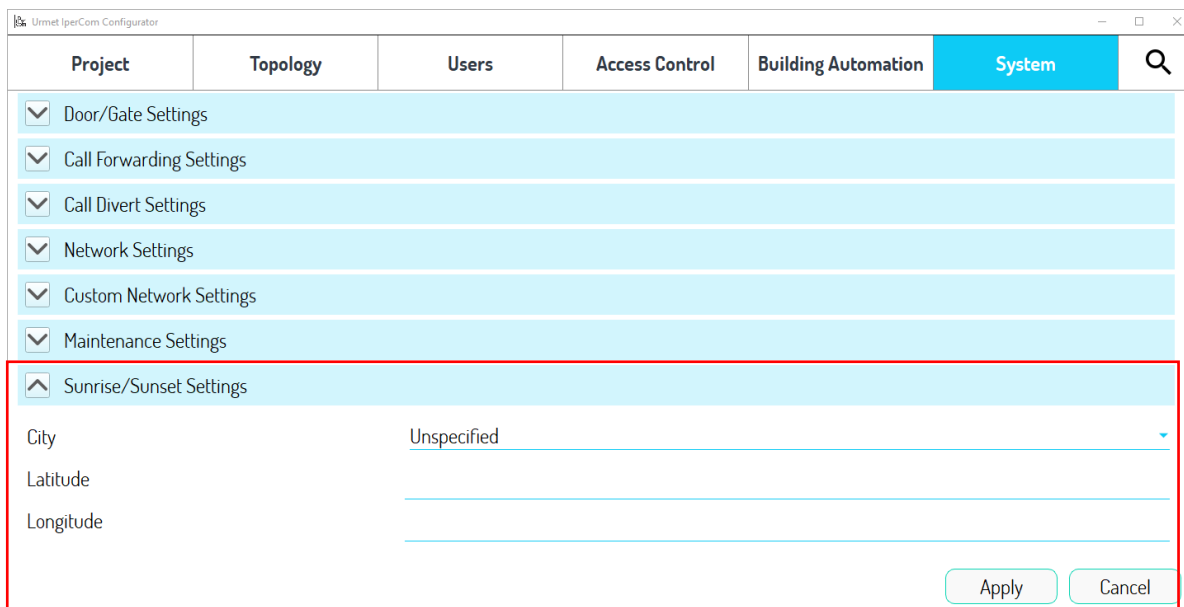


Figure 488: "System" tab - "Sunrise/Sunset Settings"

The parameter meaning is as follows:

<i>City</i>	The value chosen in this drop-down menu allows you to set automatically the " <i>Latitude</i> " and " <i>Longitude</i> " values used to calculate the sunrise and sunset time to program the activation of the outputs of one or more <i>Relay Actuators</i> or one or more scenarios on a weekly basis.
<i>Latitude</i>	Value calculated automatically according to the city chosen in the previous menu. The value can also be set manually if no value is set in the previous menu.
<i>Longitude</i>	Value calculated automatically according to the city chosen in the previous menu. The value can also be set manually if no value is set in the previous menu.

Table 23: meaning of the parameters in the "Sunrise/Sunset Settings" section

### 7.1.11 Call addressing mode

The call addressing mode in the “*Global Settings*” section of the system parameters affects how an apartment can be called by the alphanumeric keypad of the calling stations with display (*Call Module 1060/12-13-17-18-23* and *Modular calling station with 1060/48*) and *Switchboard*.

The call addressing mode to an apartment with the remaining calling stations with call buttons is not affected by the type of addressing mode chosen, that is:

- the call buttons of the *Entry Panel 1060/71-74-75-78*, *Entry Panel 1060/21*, *Entry Panel 1060/33* always call the same apartment set by the *configurator*;
- the call buttons of the *Modular calling station with 1060/48* made up by the *1060/48 IP audio video Entry Panel* and *1168/4* and *1168/8* expander modules always call the same apartment set by the *configurator*;
- the *Entry Panel 1060/34* will always show the same address book, that is the residents of its topological group.



*The Modular calling station with 1060/48 can be used to create calling stations with only call buttons or call modules in combination with the display module and numeric keypad (minimum configuration).*

There are four types of addressing:

- *topologic*,
- *numeric*,
- *logic*,
- *block mode*.

## TOPOLOGIC ADDRESSING TYPE

In topologic addressing type to call an apartment from *Call Module* or *Modular Calling Station with 1060/48* or *Switchboard*, the topologic code of the apartment in question must be entered by the keypad (starting from the block node).

The topologic code of an apartment is a fixed parameter defined by the *configurator* during the creation of the system topology and is visible on the red box reported in the picture below:

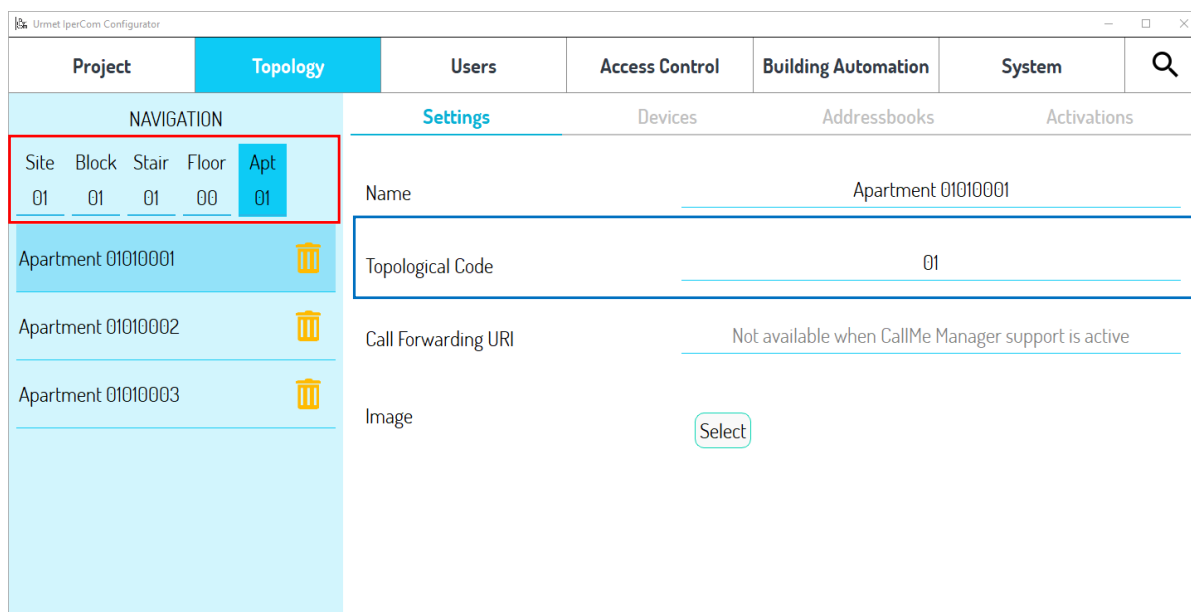




Figure 489: "Settings" screen for topologic addressing

In the "Settings" tab of the "Topology" tab, the "Topological Code" field (blue box) shows only the part of the topologic code relating to the topologic node in which you are positioned in the navigation module. The "Name" field (if not modified) shows the topological code of the node where you are positioned (starting from the block node).

 To call an apartment via the keypad of a *Call Module* or a *Modular Calling Station with 1060/48* or a *Switchboard*, it is recommended to use the logic or numeric or numeric block addressing type, described below.

 The "Select" button in the "Image" section allows you to upload an image on the display of the *Call Module 1060/12-13-17-18-23* which is intended to provide the guest with a "visual" aid in reaching the called apartment. The selected image appears as soon as the call is forwarded and disappears when the call is ended. Supported file formats include the most common ones like jpg, bmp and png. We recommend uploading images with an aspect ratio of 200x58 pixels: this way the image will not be cropped. Once an image is uploaded, you can delete it using the "Delete" button.

## NUMERIC ADDRESSING TYPE

In numeric addressing to call an apartment from *Call Module* or *Modular Calling Station with 1060/48* or a *Switchboard*, a numeric code must be entered by the keypad. You can set this code in automatic or manual mode (see paragraph [Global Settings](#) for further details). In the first case, for each apartment the "Settings" tab of the "Topology" tab appears as shown below:

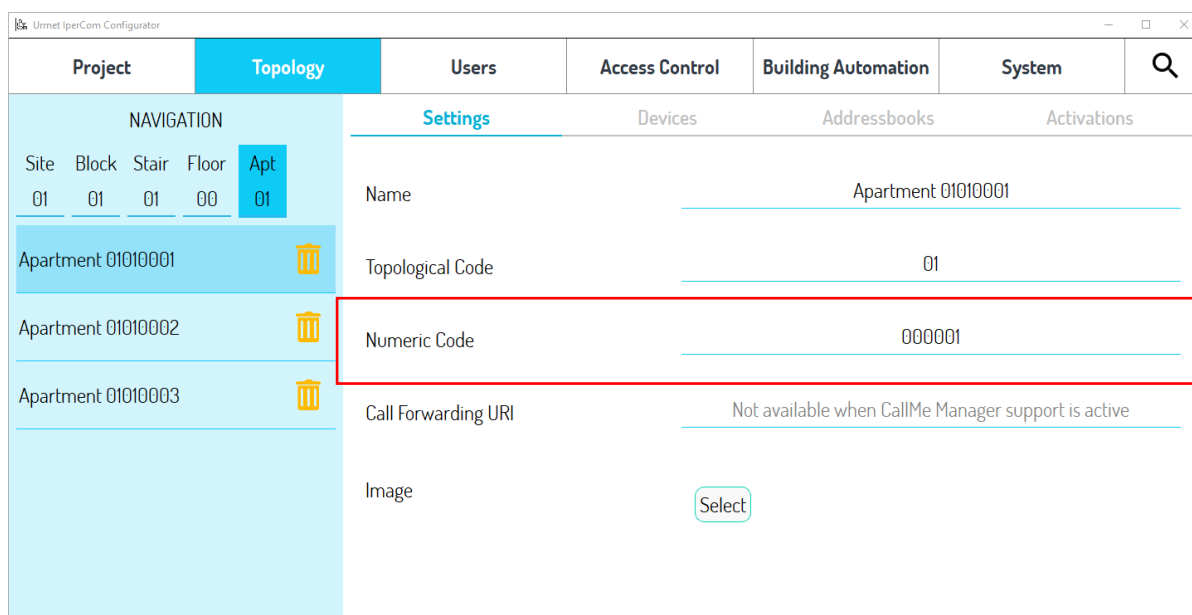


Figure 490: "Settings" screen for numeric addressing

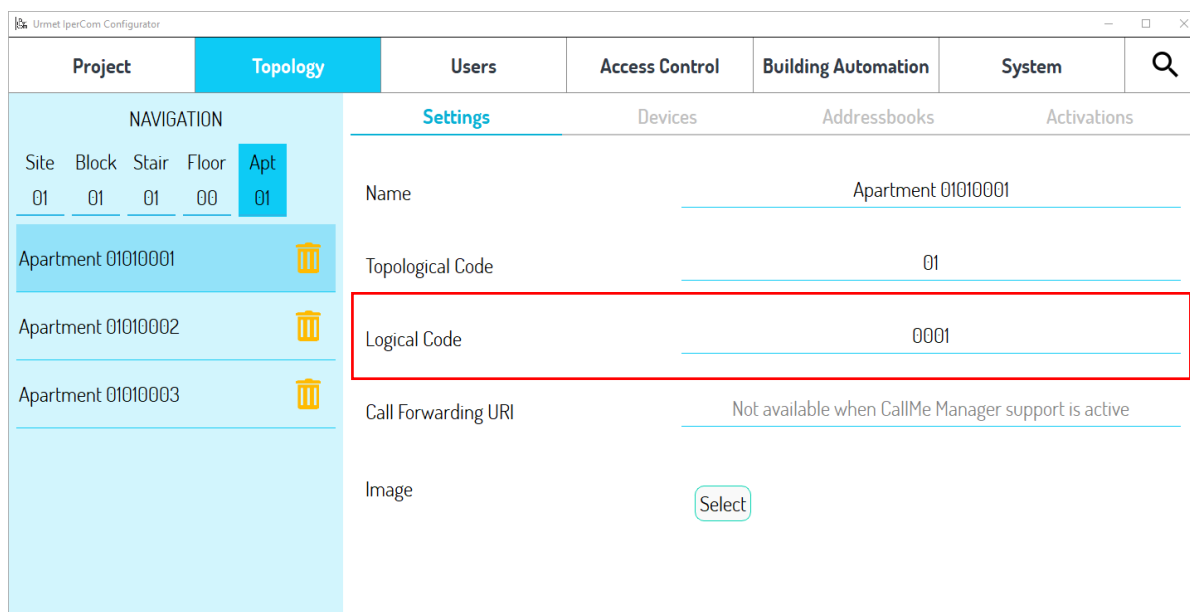
As you can see, the "Numeric Code" field is automatically filled in by the *configurator*. If, on the other hand, you choose the manual mode, the numeric code must be filled in by the installer.

Numeric codes with a maximum of 6 digits can be entered from the *configurator*.

When typing the code from the alphanumeric keyboard, the on the left zeros can be omitted.

## LOGIC ADDRESSING TYPE

In logic addressing to call an apartment from *Call Module* or *Modular Calling Station with 1060/48* or a *Switchboard*, an alphanumeric code must be entered by the keypad. You can set this code in automatic or manual mode (see [Global Settings](#) paragraph for further details). In the first case, for each apartment the "Settings" tab of the "Topology" tab appears as shown below:







Project	Topology	Users	Access Control	Building Automation	System
NAVIGATION					
Site	Block	Stair	Floor	Apt	
01	01	01	00	01	
Apartment 01010001 					
Apartment 01010002 					
Apartment 01010003 					
Settings   Devices   Addressbooks   Activations					
Name		Apartment 01010001			
Topological Code		01			
Logical Code		0001			
Call Forwarding URI		Not available when CallMe Manager support is active			
Image		<input type="button" value="Select"/>			

Figure 491: "Settings" screen in case of logic addressing

As you can see, the "Logical Code" field is automatically filled in by the *configurator*. If, on the other hand, you choose the manual mode, the numeric code must be filled in by the installer.

From the configurator it is possible to enter logic codes with a maximum of 8 alphanumeric characters.

When typing the code from the alphanumeric keyboard, the on the left zeros cannot be omitted.


 To enter alphanumeric codes, the *Modular Calling Station with 1060/48* must be equipped with an alphabetic keyboard 1168/49.

## BLOCK MODE ADDRESSING TYPE

In block mode addressing to call an apartment from the *Call Module* or *Modular Calling Station with 1060/48* it is necessary to distinguish whether these are positioned on the “*Site*” node or not.

### CALL MODULE OR MODULAR CALLING STATION WITH 1060/48 ON SITE NODE

To call an apartment by the keypad you need:

- from *Call Module* (by means of arrow buttons) first select the block in which the apartment in question is placed, then enter the numeric code associated with the apartment;
- from *Modular Calling Station with 1060/48*, press the button corresponding to the icon , then select block in which the apartment in question is placed, then enter the numeric code associated with the apartment.

### CALL MODULE OR MODULAR CALLING STATION WITH 1060/48 ON NODE BLOCK/STAIR/FLOOR

To call an apartment by the keypad you need:

- from *Call Module* enter the numeric code associated with the apartment;
- from *Modular Calling Station with 1060/48* enter the numeric code associated with the apartment.

Again, in this type of addressing, the numeric code (which appears in the “*Settings*” tab of the “*Topology*” tab) can be set automatically or manually, as already seen previously.

When typing the code from the alphanumeric keyboard, the on the left zeros can be omitted.

If the numeric codes of the apartments are set manually, a numeric code must also be set for the blocks present in the topological structure of the system, as shown below:

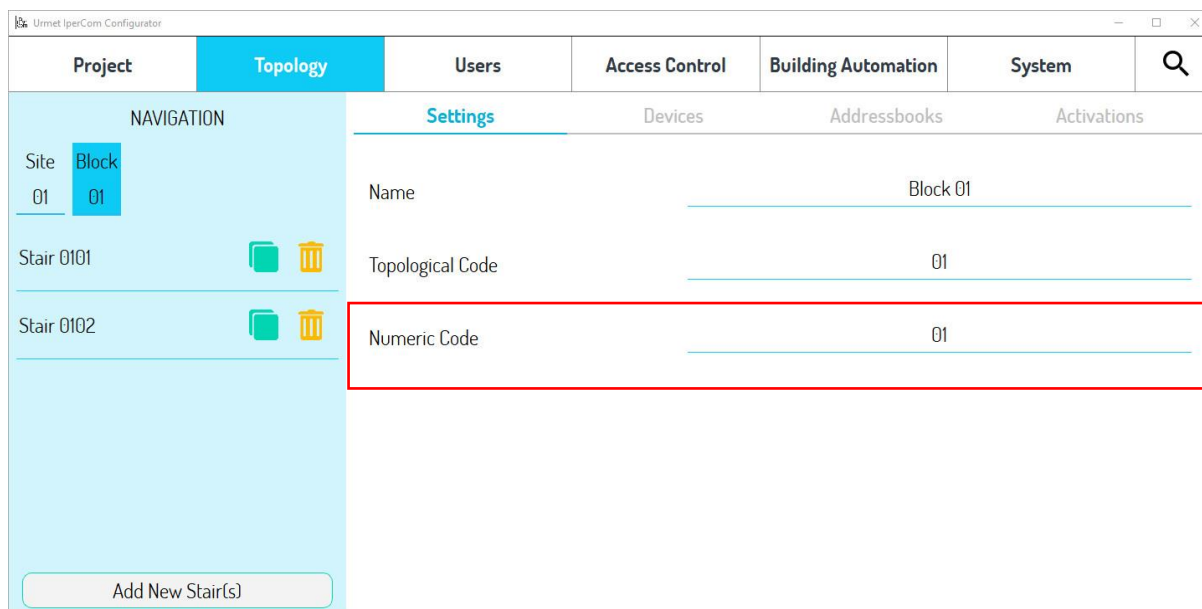





Figure 492: block "Settings" screen in case of block mode

-  **If some blocks do not have a valid numeric code, it is impossible to save the configuration.**
  
-  **In block mode addressing type, the Switchboard can call the apartments only using the address book.**
  
-  *If the Call Module 1060/12-13-17-18-23 or the Modular Calling Station with 1060/48 are positioned on the block/stair/floor node, it is possible to also make the directory (of their topological group) appear by selecting the "Show Address Book" item from the relevant configuration page (see [APPENDIX A: Configuration parameters of IPerCom devices](#) for further details). In this case it is possible to call the apartment both via numeric code and via the resident's name.*



### 7.1.12 Setting of call forwarding function in IPerCom system not in IPerCloud mode

The **call forwarding** function allows receiving a call from

- *Entry panel 1060/71-74-75-78,*
- *Entry panel 1060/21-33-34,*
- *Call module 1060/12-13-17-18-23,*
- *Modular Entry Panel with 1060/48,*
- *Private Call Module 1060/22,*
- *Switchboard,*

on one or more smartphones/tablets as well as in the apartment.

The function is also available if:

- the call from a calling station is directed to a specific apartment station;
- the call arrives from an apartment station of an apartment to another apartment or to a single apartment station of this one.

The call forwarding function can be configured in 2 ways:

- through the support of the *CallMe Manager* app (Urmet Cloud authentication via *IPerCom Installer Tools* is mandatory);
- without the support of the *CallMe Manager* app.

To configure the call forwarding function with the *CallMe Manager* app, it is necessary to enable the relevant item via the *IPerCom Installer Tools* configurator, the default value of which is disabled (see the [Call Forwarding Settings](#) paragraph).

*CallMe Manager* app support is useful by useful for medium-large system/house topologies where the figure of the building manager is generally required, that is “*Single Stair*”, “*Multiple Stairs*” and “*Multi Block*”. The *IPerCom Installer Tools* allows choosing one of the 3 system topologies listed above and allows enabling the *CallMe Manager* app support if a building manager is present. In the latter case, follow what is stated in the section [Configuring call forwarding function with CallMe Manager application support](#).



*In apartments with Audio Apartment stations 1160/3 only, the call forwarding function can only be enabled via CallMe Manager support.*



*If an IPerCom system with the call forwarding function already configured is updated to version 2.1.0 or higher, in order to take advantage of the new features of the function it is necessary:*

- *scan the QR code on the letter sent by the administrator if CallMe Manager **is used**;*
- *scan the QR Code in the video door phone setting menu if CallMe Manager **is not used** (for further information please refer to the function configuration paragraph).*

*For further information, refer to the 2 paragraphs below.*

### 7.1.12.1 *Configuring call forwarding function [with CallMe Manager application support](#)*

Below are the various actions to perform to correctly configure the function.

#### 1. INSTALLER

- Connect a router to the IPerCom system network that can provide Internet access;
- Installation of the *IPerCom Installer Tools* PC application;
- Creation of an Urmet Cloud account to authenticate on *IPerCom Installer Tools*;
- Using the *IPerCom Installer Tools* application, create a system configuration and verify that the parameters of the call forwarding function are correct;
- Transfer of the site to the building manager.

#### 2. BUILDING MANAGER

- Installation of the *CallMe Manager* application on PC;
- Creation of an Urmet Cloud account to authenticate on *CallMe Manager*;
- Site acquisition via the *CallMe Manager* app;
- Generation of letters (pdf format) with QR-code;
- Sending letters via email or post to users.

#### 3. END-USER

- Installation of the *CallMe* application, distributed for Android and iOS operating systems and downloadable from the relevant stores;
- Creation of an Urmet Cloud account to authenticate on *CallMe*;
- Scan the QR code sent by the building manager to associate the account with the apartment;
- Possible sharing of access to the system with other users;
- Activate the call forwarding function, check its correct activation, check that the apartment's master video door phone shows the “Remote” mode icon (for further details see the video door phone user manual available on the website [www.urmet.com](http://www.urmet.com)).



*For the 1160/3 door phone the “Remote” mode is already set by default and is not displayed to the user either via icon or LED.*

## Configuration of the system and parameters of the call forwarding function (installer)

Using the *IPerCom Installer Tools* application, the installer creates the project and the related configuration, that is defines the system topology, adds the devices on the topological nodes, assigns appropriate names to the devices, apartments, and topological nodes, creates the address books, the users, and activations, configure the parameters of the call forwarding function in the "System" section of the configurator (as shown below):

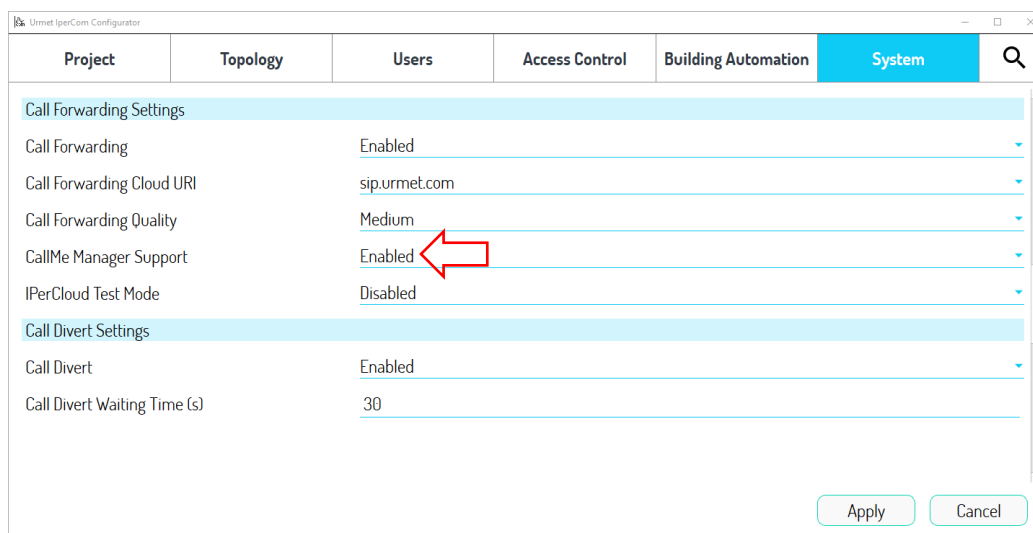


Figure 493: call forwarding parameters in tab "System"

Under the "Call Forwarding" item, check that the value is set to "Enabled", as shown in the figure above.

In correspondence with the "Call Forwarding Cloud URI" item, it is necessary to set the server on which the user is registered via the *CallMe* app: the default server is "sip.urmet.com", while the server "cn.sip.urmet.com" is to be used only for the Chinese market.

The "Call forwarding quality" item must be set based on the available bandwidth: if you encounter problems in the call, such as jerky video and/or incomprehensible audio, it is best to lower the quality of call forwarding call.

The "CallMe Manager Support" item must be enabled to configure the call forwarding function with the *CallMe Manager* app. The "IPerCloud Test Mode" item must be disabled.

After carrying out the configuration, it is necessary to apply it to the system. To do this, you must first save the configuration and exit the *configurator*. Then select the “*Configuration*” tab and press the “*Apply changes*” button to transfer the configuration to the system:

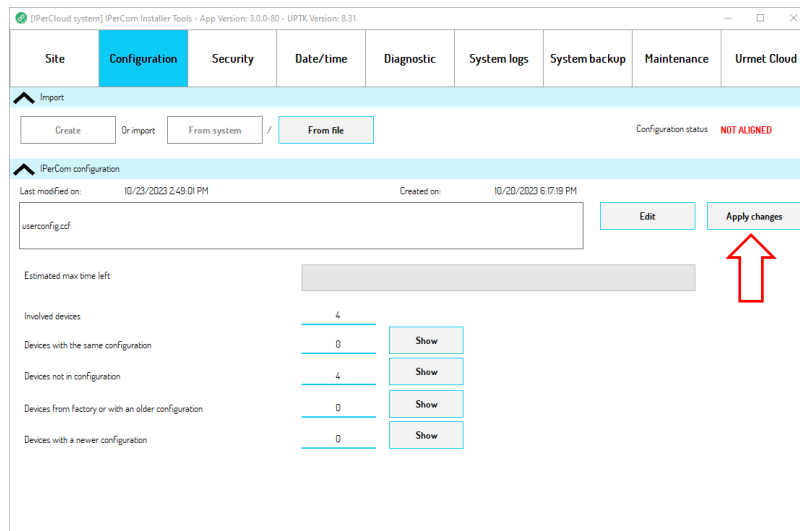


Figure 494: Configuration transfer

After this, it is necessary to go to the “*Urmet Cloud*” tab in the **Site authorization management** section:

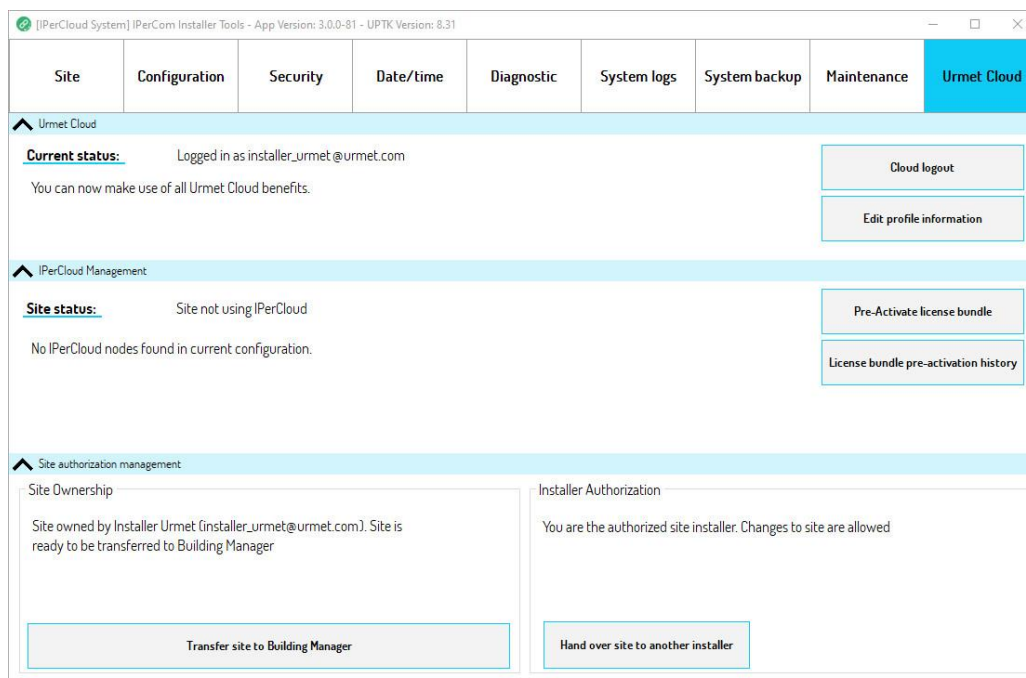


Figure 495: site transfer from installer to building manager

It is necessary to press the "Transfer site to Building Manager" button to transfer ownership of the site to the building manager, who with the *CallMe Manager* application will be able to configure the call forwarding service by printing the relevant letters. The following dialog box is shown in which it is necessary to enter the email with which the building manager registered with Urmet Cloud:

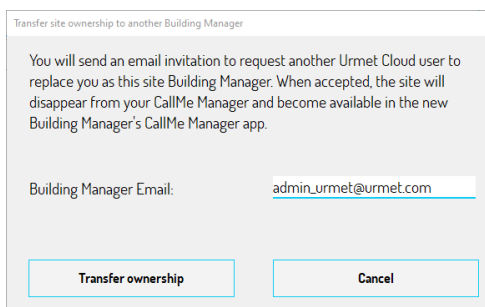


Figure 496: transfer of the site to building manager

By pressing the "Transfer ownership" button, an email is sent to the building manager and the correct outcome of the operation is confirmed by the following dialog box:

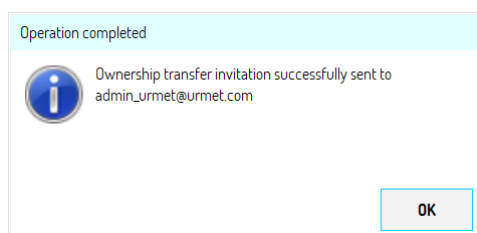


Figure 497: correct outcome of the invitation to the building manager



*At the time of transfer, it is necessary that any internal stations are installed in the various apartments and connected to the system. If this were not the case, the apartments, whose internal stations are not connected to the system, will not appear in the topological structure transferred to the building manager in the CallMe Manager application.*

## Import of the topological structure of the system and printing of letters (Building Manager)

Below are illustrated the fundamental steps that the building manager must follow to allow residents to use the call forwarding function. For all information on managing users, refer to the user manual of the *CallMe Manager* application.

The building manager must download the *CallMe Manager* application and the related user manual from the website [www.urmet.com](http://www.urmet.com).

The *CallMe Manager* application allows to:

- generate the pdf files to send to users to allow the association of accounts with apartments for use of the call forwarding function;
- manage the accounts of users who use the call forwarding function.

Before using the *CallMe Manager* application, the building manager must open the email that he received following the transfer of the site from the installer and press on the relevant link to make the transfer effective. The positive outcome of the operation is confirmed by the message "*Site acquired successfully*".

At this point it is possible to start the *CallMe Manager* application, authenticate with the Urmet Cloud account previously created by the building manager and press the "*Login*" button:

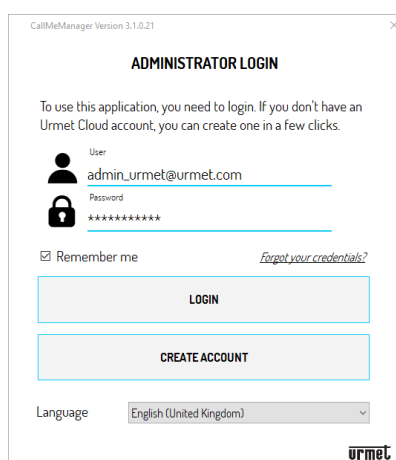


Figure 498: CallMe Manager login window

The *CallMe Manager* application shows the following dialog box relating to the presence of a new site ("*System with CallMe Manager*") transferred to the building manager account:

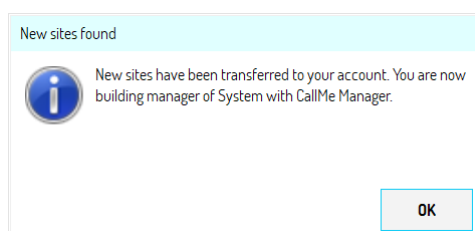


Figure 499: new site transferred to building manager

By pressing the "OK" button, the homepage of the *CallMe Manager* application appears with the new site loaded:

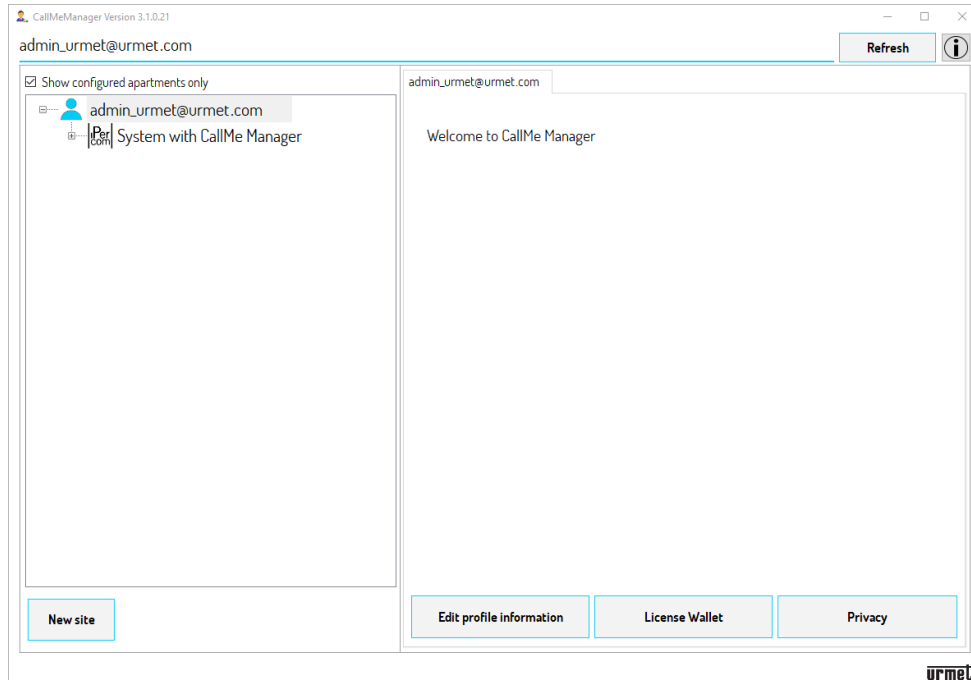


Figure 500: CallMe Manager app homepage

By expanding the topological structure, it is possible to view all the topological nodes present in the system, that is blocks, stairs, floors, and apartments:

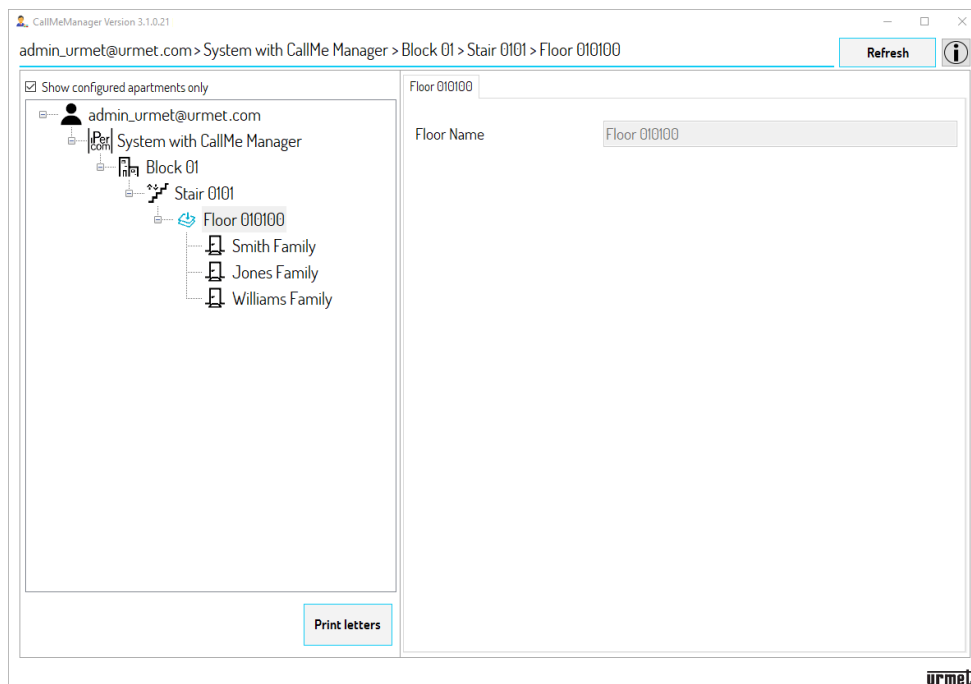


Figure 501: topological structure of the system



Once the topology has been imported, it is necessary to generate the letters (pdf file) which must be sent via email or post to the users, to allow the association of the accounts with the apartments (via the *CallMe* app) and the use of the function call forwarding: to do this, press the “*Print letters*” button.

Depending on the selected node, the letters of the users (and/or switchboard operator, if present) who are in the topological group of the node in question (including the node itself) are generated.

For example, if in the topological structure there is a block with 2 stairs (“*Stair 1*” and “*Stair 2*”) in which there are 10 floors in each stair and 10 apartments in each floor, positioning on the “*Stair 1*” node, only the letters for the users/apartments present in the “*Stair 1*” node are generated, that is 100 letters.

Relative to the previous figure, a pdf file with 3 letters is generated:

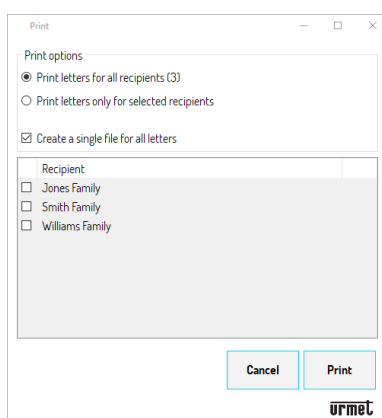


Figure 502: Print of pdf letters

The “*Print letters for all recipients*” item allows you to generate pdf files for all recipients present within the selected node.

The “*Print letters only for selected recipients*” item allows you to generate pdf files only for selected recipients (to select a recipient, tick the box next to the recipient's name).

By checking the “*Create a single file for all letters*” box, a single pdf file containing all the letters from all recipients is generated (useful option for printing). If the box is not checked, a pdf file is generated for each individual recipient (useful option if you want to send pdf files for each recipient via email).

Press the “*Print*” button to generate letters in pdf format to send to users.

### [Activating and enabling the call forwarding feature \(end-user\)](#)

Below the basic steps that the end-user must perform with the *CallMe* app, after receiving the letter from the building manager, to activate the call forwarding function are reported. For all information on configuring the app, refer to the [relevant booklet](#) on the website [www.urmet.com](http://www.urmet.com).

Download the app from the Apple Store (iOS) or the Play Store (Android) and install it on your smartphone/tablet. The login page appears:

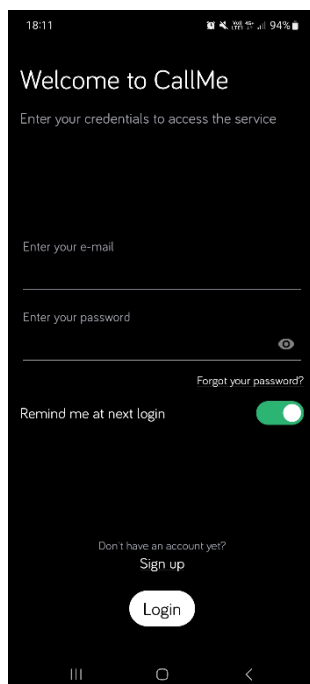


Figure 503: app login page or to create an account

Once logged in with a newly created or existing account, the application homepage is displayed:

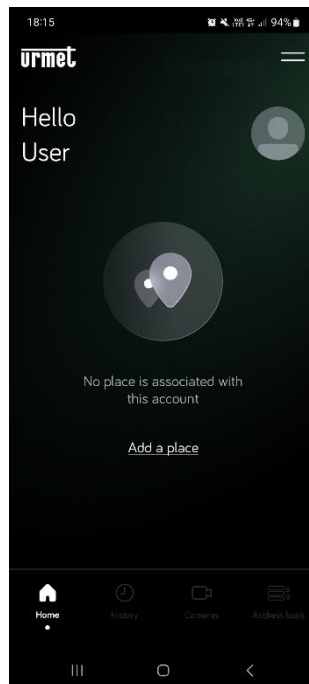


Figure 504: application homepage

Pressing the “Add a place” button the following screen appears:

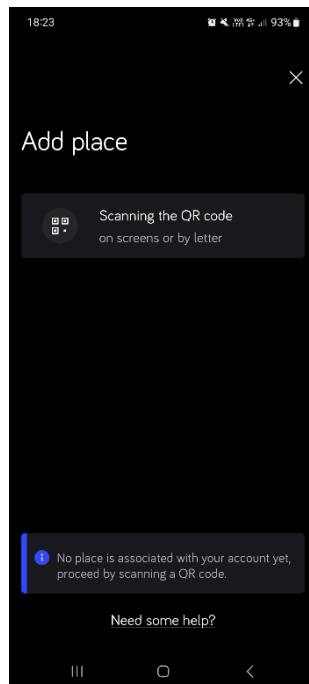


Figure 505: add of a place

Press the "Scanning the QR code" button to start the QR Code Reader application, then scan the QR code displayed in the letter sent by the building manager relating, for example, to the first apartment. The app shows the following screen:

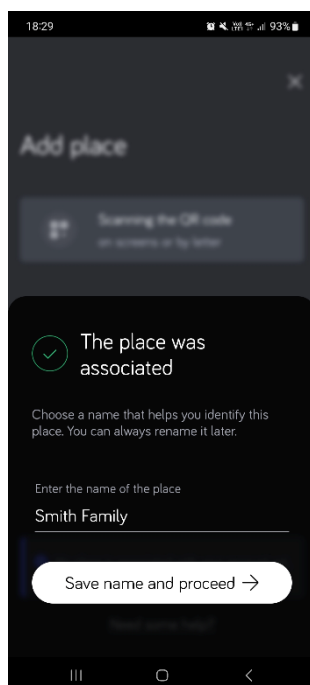


Figure 506: association of a place/apartment with the CallMe account

If you want, you can change the name "Smith Family". By pressing the "Save name and proceed" button, the CallMe application home page appears as shown below:

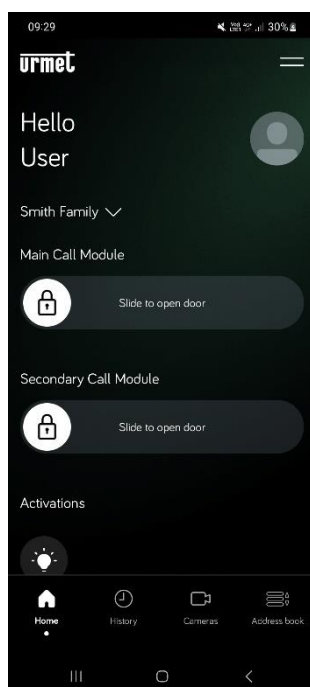




Figure 507: account associated with the apartment

At this point on the video door phone, it is necessary to:

- press the “*Activate and Verify*” button to activate the call forwarding function and verify its correct activation;
- check that the apartment's master video door phone automatically shows (if the function is activated for the first time) the *Remote* mode icon;

Depending on the video door phone model, the various steps to carry out the above are shown.

**VIDEO DOOR PHONE 7" VOG<sup>7</sup> 1761/31-32-33, 7" MAX 1717/31-32-33-34-41, 10" MAX 1717/21-22-23, 7" BASIC 1741/1-2-3**

- Switch on the master video door phone display by pressing anywhere on the screen or by pressing the Home button.
- If you are not already viewing the *Video Door Phone* page, press the icon  to access the "Top Page" and then the icon :

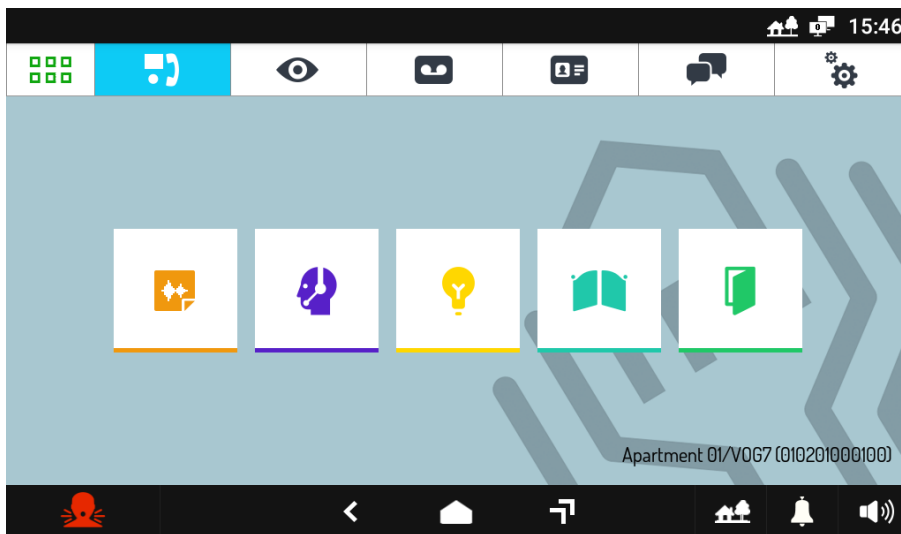



Figure 508: video door phone application

- Press the icon  at the top right to access the video door phone configuration page:

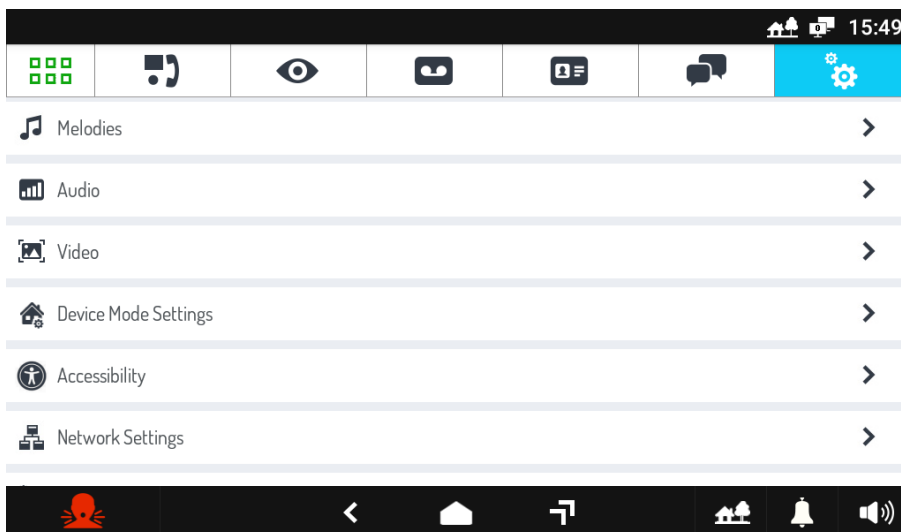


Figure 509: video door phone application settings

- Press on the “*Device Mode Settings*” item:

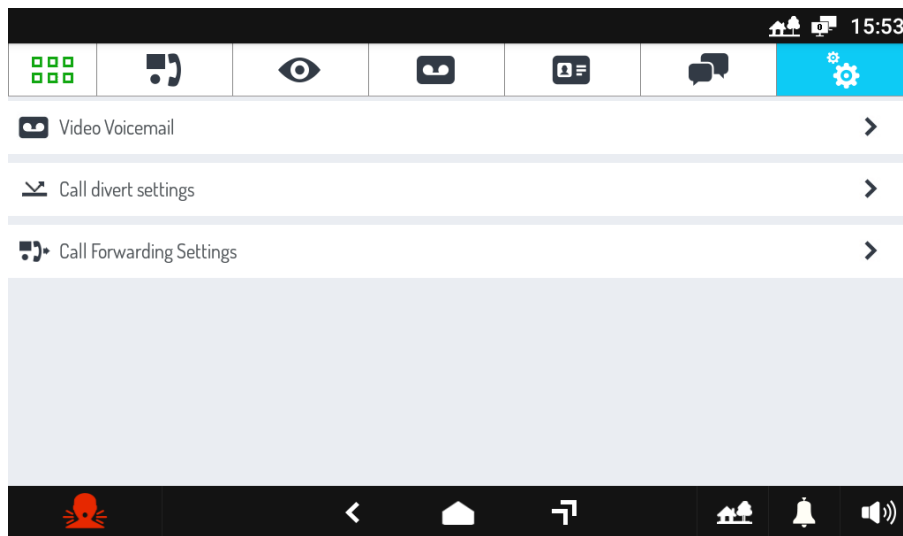


Figure 510: device mode settings

- Press on the item “*Call Forwarding Settings*” and then on the item “*Activate/Verify Call Forwarding service*”:

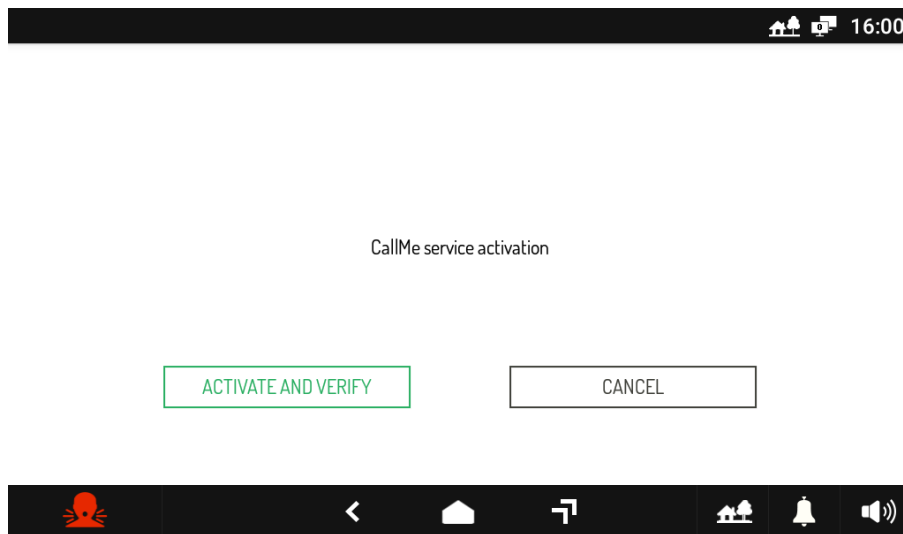


Figure 511: activation and verification of the call forwarding function

- Press the “ACTIVATE AND VERIFY” button and check that the following screen is shown for correct activation of the service:

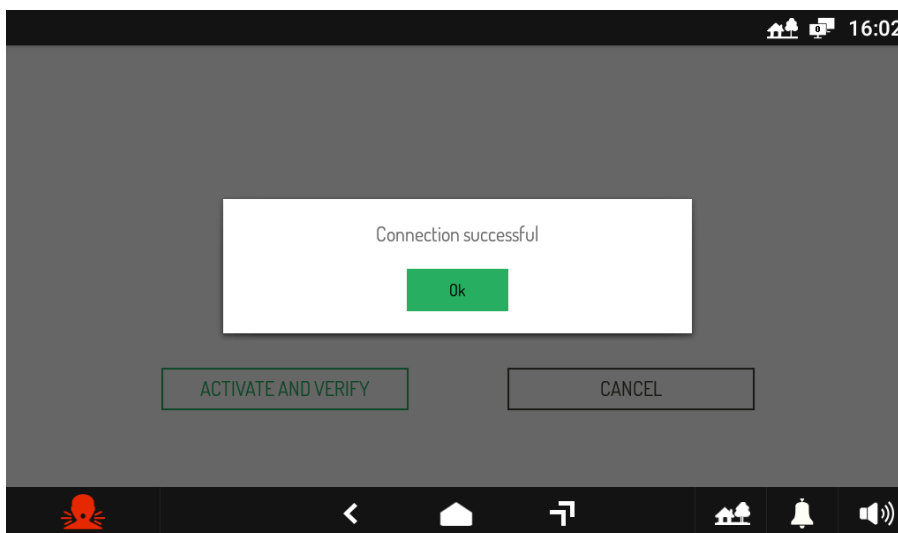


Figure 512: correct activation of the call forwarding function

As a last step it is necessary to check that the icon  appears at the bottom and top right of the master video door phone display as shown below:

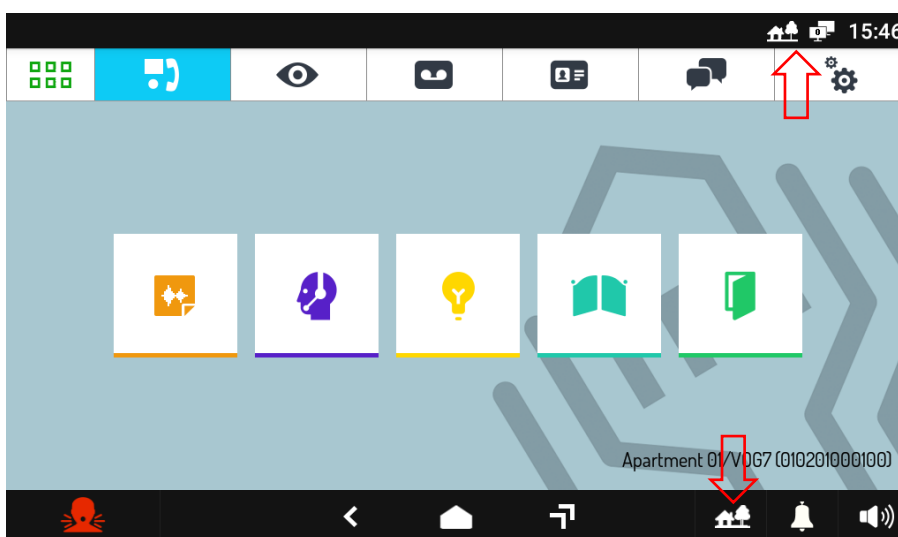







Figure 513: operating icon in “Remote” mode

 On any slave video door phones, the “Remote” mode operating icon is only shown at the top right.

 If operation in “Remote” mode has already been activated and deactivated previously on the video door phone, the relevant icon must be activated manually: it is necessary to press the icon  (bottom right) only on the master video door phone and then select the icon .



## VIDEO DOOR PHONE VOG<sup>5+</sup> 1761/15-16-18-19

- Press the button  twice to access the homepage, the following screen appears on the video door phone display:

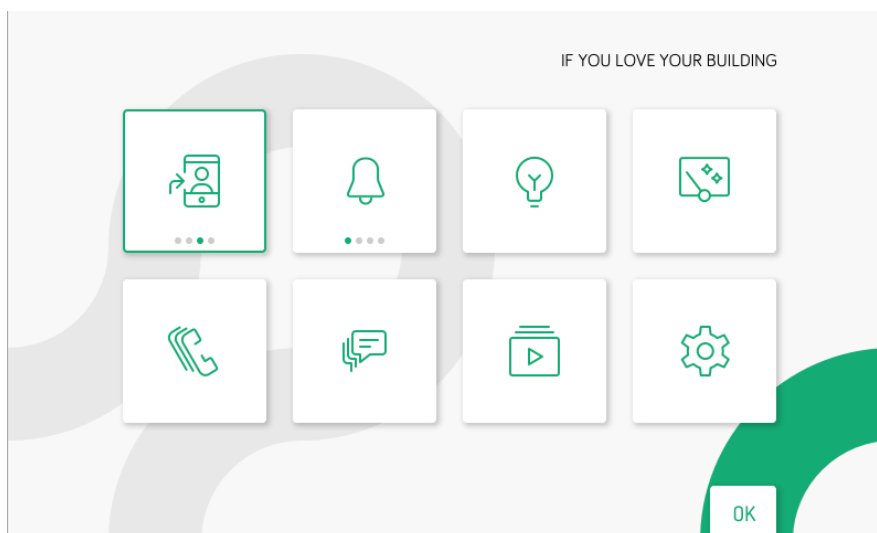








Figure 514: homepage

- Press the , , , and  buttons to select the following icon , then press the button  to access the video door phone configuration menu:

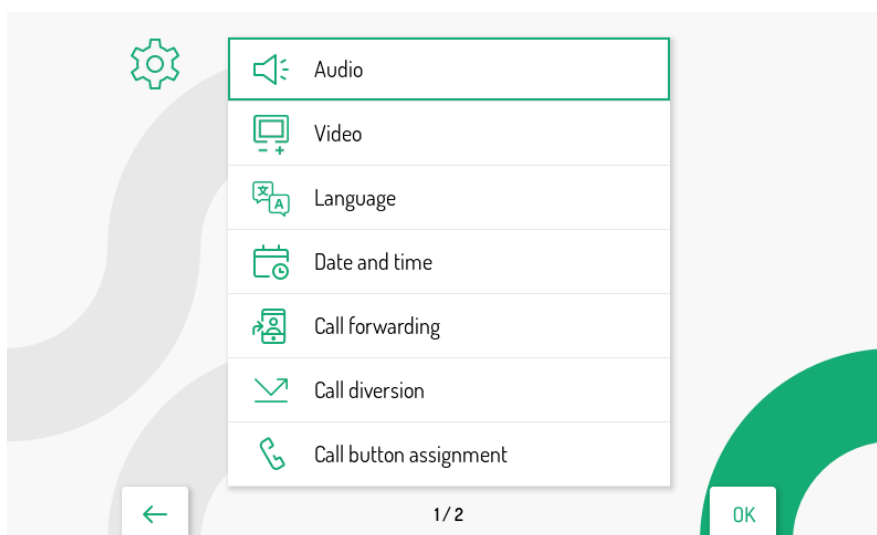




Figure 515: setting menu

- Press the  button and select the “Call forwarding” item, press the button  to confirm the selection.
- The following screen appears on the display:

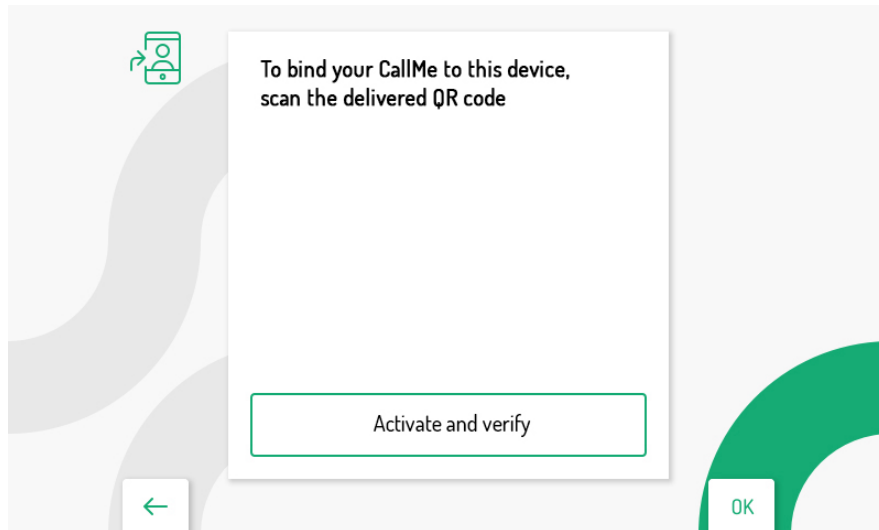



Figure 516: activation and verification button

- Press the “Activate and verify” item using the button  and check that the following screen is shown for correct activation of the service:

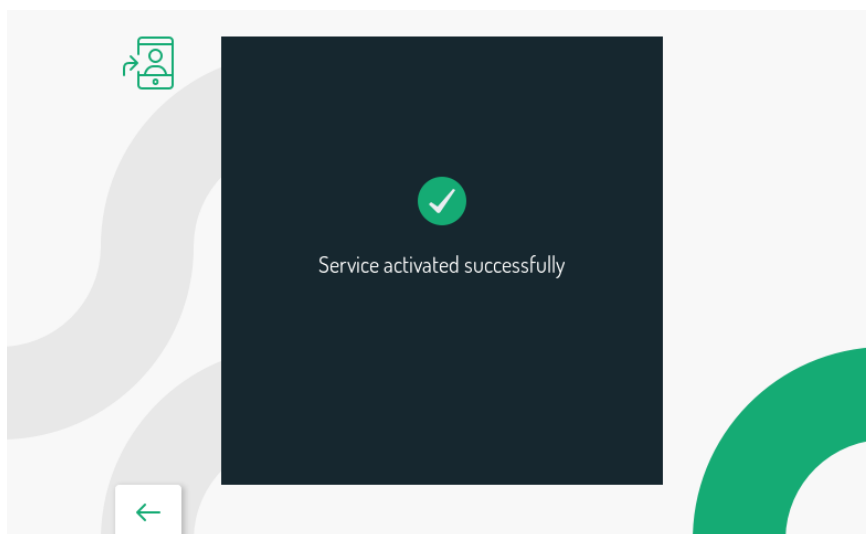



Figure 517: correct activation of the call forwarding function

As a last step it is necessary to check that the icon  as shown below appears on the homepage of the master video door phone:

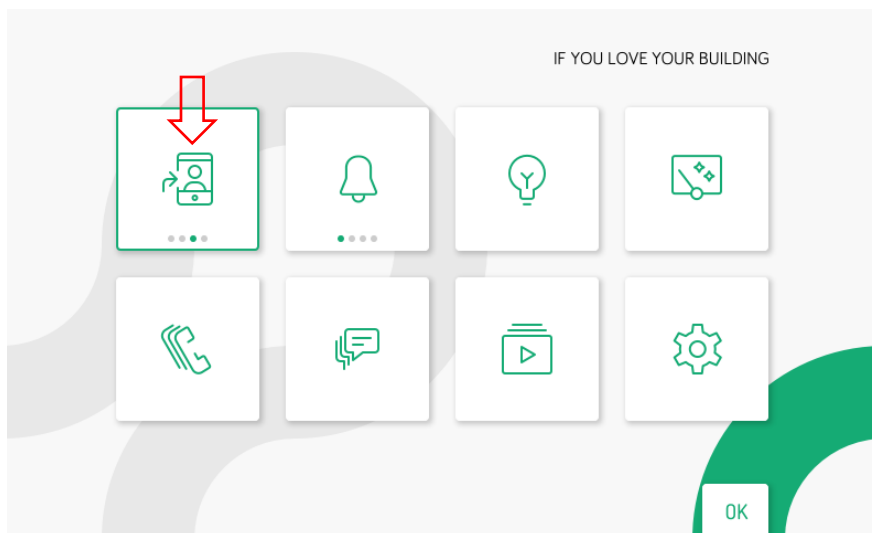









Figure 518: operating icon in “Remote” mode

 On any slave video door phones, it is possible to view the “Remote” mode operating icon at the top right by pressing the button  once with the screen off.

 If operation in “Remote” mode has already been activated and deactivated previously on the video door phone, the relevant icon must be activated manually: it is necessary (only on the master video door phone) to select the icon  and with button  select the icon .

**VIDEO DOOR PHONE VOG<sup>5</sup> 1761/6**

- Access the configuration menu by pressing and holding down the button  for at least 5 seconds with the display off:

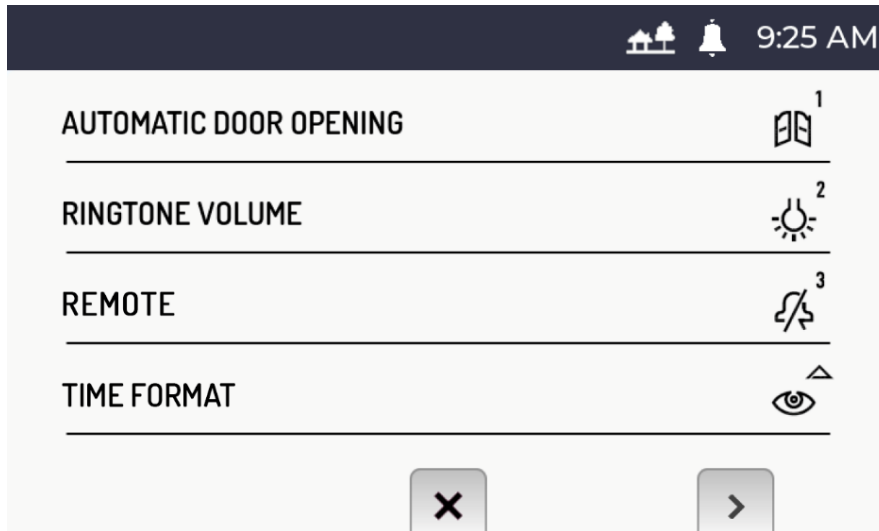



Figure 519: configuration menu (first window)

- Press the button  to display the second window of parameter configuration:

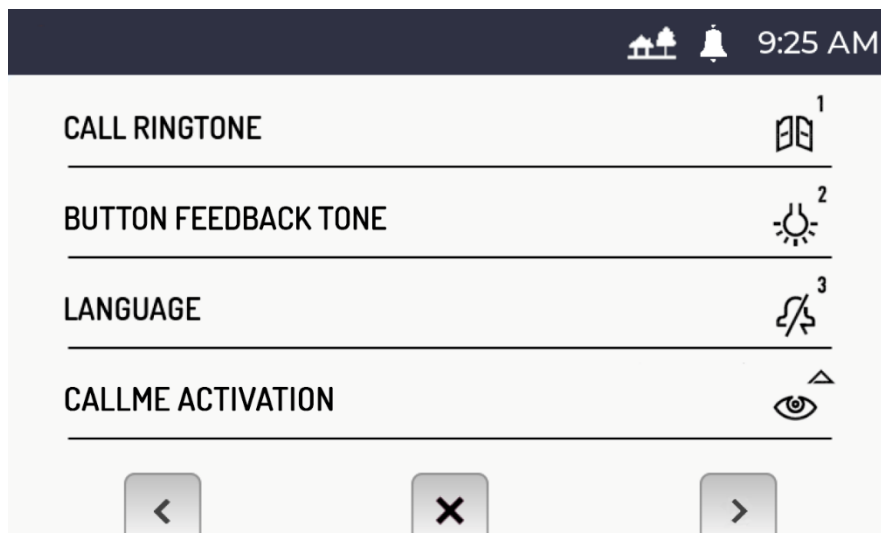



Figure 520: configuration menu (second window)

- Press the button  in the second screen of the configuration menu, the display will show the following window:

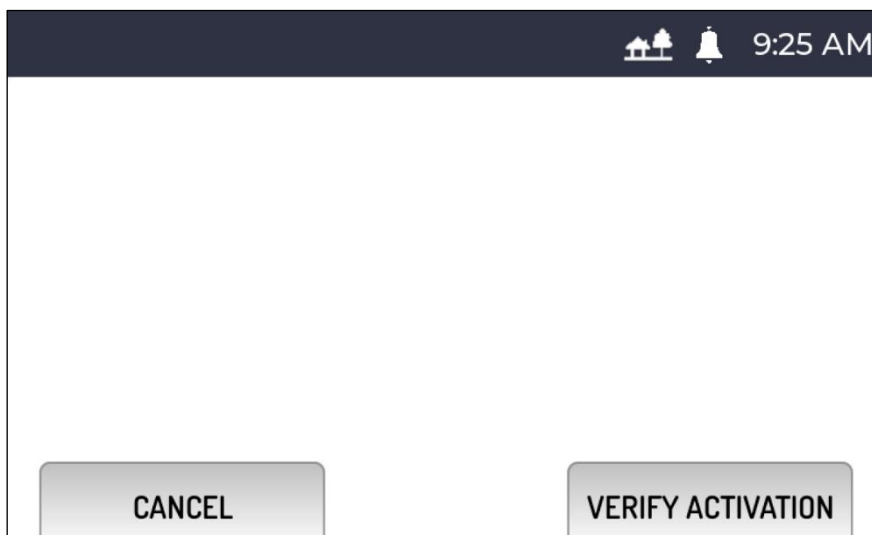



Figure 521: verify the correct activation of the call forwarding function

- Press the “VERIFY ACTIVATION” item using the button  and check that the following screen is shown for correct activation of the service:

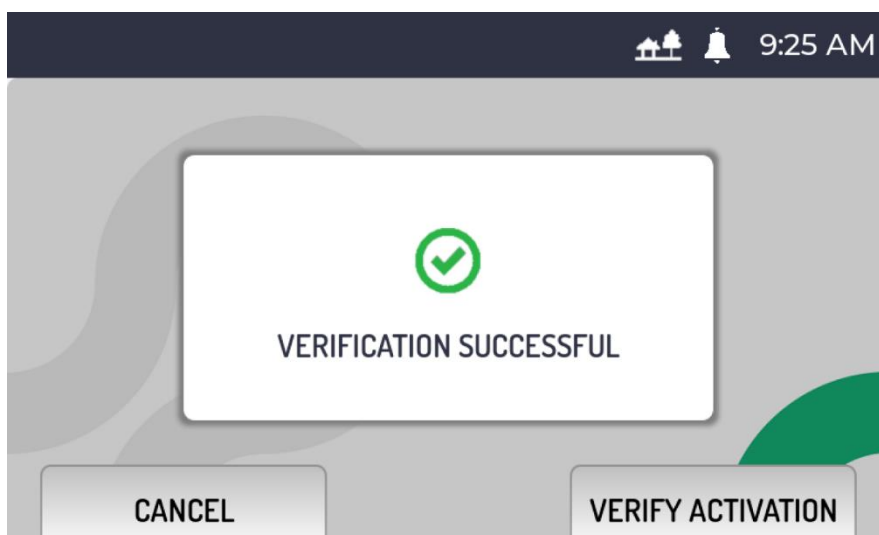





Figure 522: correct activation of the call forwarding function

As a final step, press the button  and then the button  and check that the icon  appears on the homepage of the master video door phone at the top right, as shown below:

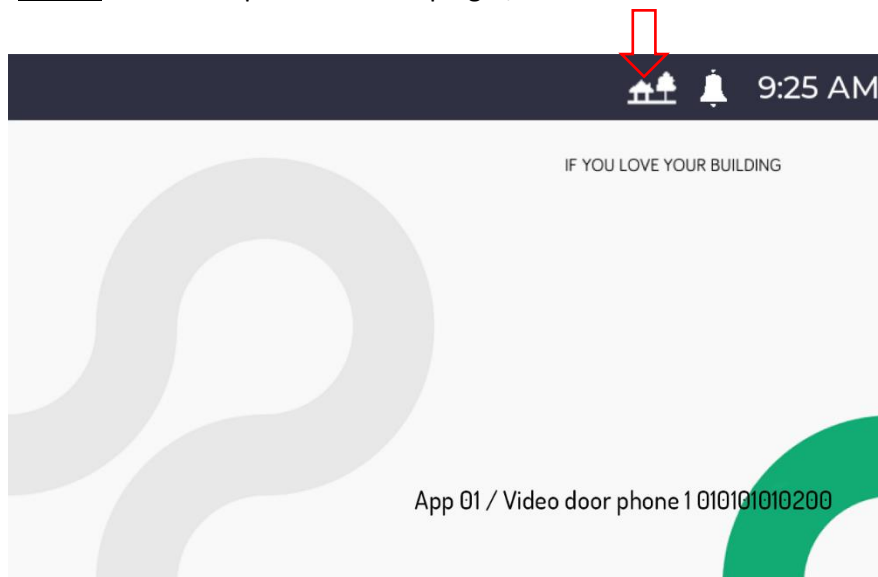






Figure 523: operating icon in "Remote" mode


 On any slave video door phones, it is possible to display the operating icon in "Remote" mode in the same way as seen for the master video door phone.



 If operation in "Remote" mode has already been activated and deactivated previously on the video door phone, the relevant icon must be activated manually: it is necessary (only on the master video door phone) with the screen off, press and hold down the icon  for at least 5s and use the button  to set the "Remote" mode.

At this point the configuration of the call forwarding service is finished and the *CallMe* app is ready for use.

The main features of the *CallMe* app are listed below:

- call forwarding to the apartment on smartphone/tablet (video door phone must be set in "remote" mode);
- auto-insertion on calling stations;
- intercom call to apartment stations;
- sending activation commands;
- door and gate opening even outside of the call.

 Auto-insertion on RTSP cameras is not supported by *CallMe* app.

-  *The QR code on PDF document sent by the building manager can only be used once. It cannot be used again after it has been scanned. The entire service activation procedure must be performed after scanning. If procedure is interrupted, the administrator will have to generate a new document with a new QR code to allow service activation.*
  
-  *Once the call forwarding function has been configured for the various apartments and **Switchboard** applications, it is of fundamental importance not to redo a new system configuration from scratch (even if the topology is the same): if so, the procedure described above to associate the smartphone/tablet to apartments/**Switchboard** applications is to be repeated.*

### 7.1.12.2 *Configuring call forwarding function without CallMe Manager application support*

The configuration of the call forwarding function without the support of the *CallMe Manager* app is foreseen for all those types of systems in which there is no building manager.

Below are the various actions to perform to correctly configure the function.

#### 1. INSTALLER

- Connect a router to the IPerCom system network that can provide Internet access;
- Installation of the *IPerCom Installer Tools* PC application;
- Using the *IPerCom Installer Tools* application, create a system configuration and verify that the parameters of the call forwarding function are correct.



*Creating an Urmet Cloud account to authenticate on IPerCom Installer Tools is not mandatory.*

#### 2. END-USER

- Installation of the *CallMe* application, distributed for Android and iOS operating systems and downloadable from the relevant stores;
- Creation of an Urmet Cloud account to authenticate on *CallMe*;
- Scan the QR-code present on the video door phones to associate the account with the apartment;
- Possible sharing of access to the system with other users;
- Activate the call forwarding function, check its correct activation, check that the apartment's master video door phone shows the “*Remote*” mode icon (for further details see the video door phone user manual available on the website [www.urmet.com](http://www.urmet.com)).



*For the 1160/3 door phone the “Remote” mode is already set by default and is not displayed to the user either via icon or LED.*



## Configuration of the system and parameters of the call forwarding function (installer)

Using the *IPerCom Installer Tools* application, the installer creates the project and the related configuration, that is defines the system topology, adds the devices on the topological nodes, assigns appropriate names to the devices, apartments, and topological nodes, creates the address books, the users, and activations, configure the parameters of the call forwarding function in the "System" section of the configurator (as shown below):

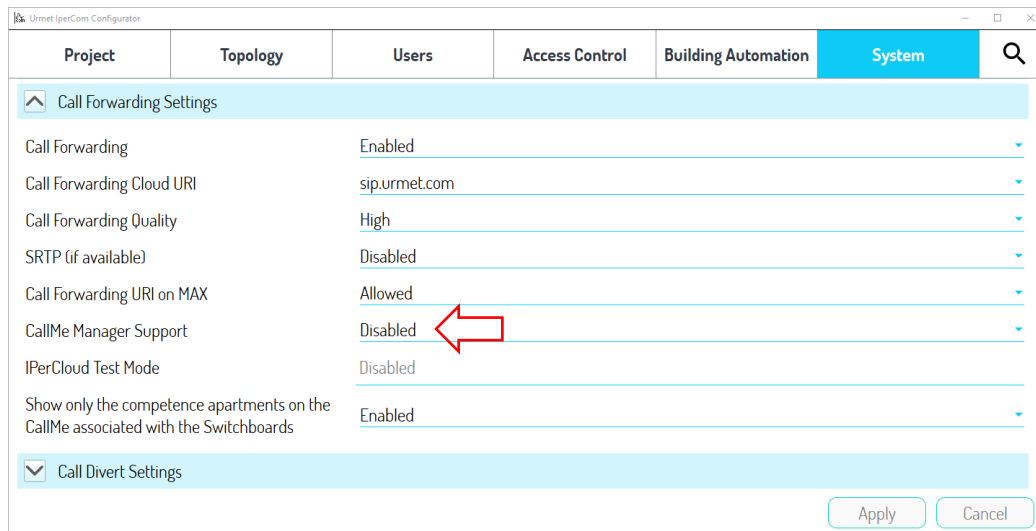


Figure 524: call forwarding parameters in tab "System"

In correspondence with the "Call Forwarding" item, check that the value is set to "Enabled", as shown in the figure above.

In correspondence with the "Call Forwarding Cloud URI" item, it is necessary to set the server on which the user is registered via the *CallMe* app: the default server is "sip.urmet.com", while the server "cn.sip.urmet.com" is to be used only for the Chinese market.

The "Call forwarding quality" item must be set based on the available bandwidth: if you encounter problems in the call, such as jerky video and/or incomprehensible audio, it is best to lower the quality of call forwarding call.

The "CallMe Manager Support" item must be disabled.

After carrying out the configuration, it is necessary to apply it to the system. To do this, you must first save the configuration and exit the *configurator*. Then select the “*Configuration*” tab and press the “*Apply changes*” button to transfer the configuration to the system:

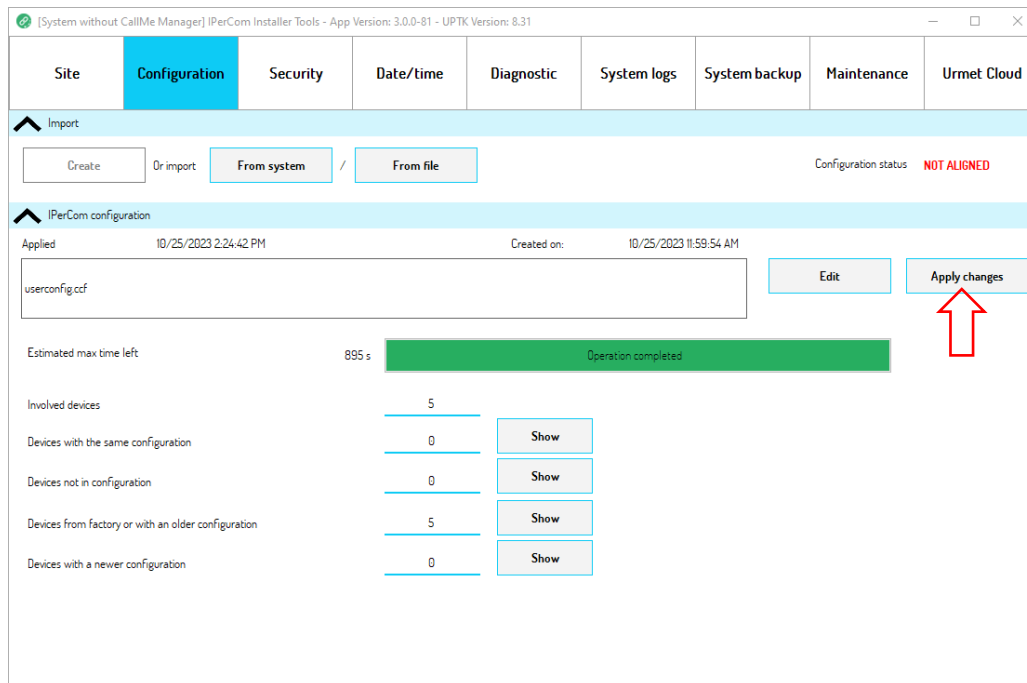


Figure 525: configuration transfer

### [Activating and enabling the call forwarding feature \(end-user\)](#)

Below the basic steps that the end-user must perform with the *CallMe* app to activate the call forwarding function are reported. For all information on configuring the app, refer to the [relevant booklet](#) on the website [www.urmet.com](http://www.urmet.com).

Download the app from the Apple Store (iOS) or the Play Store (Android) and install it on your smartphone/tablet. The login page appears:

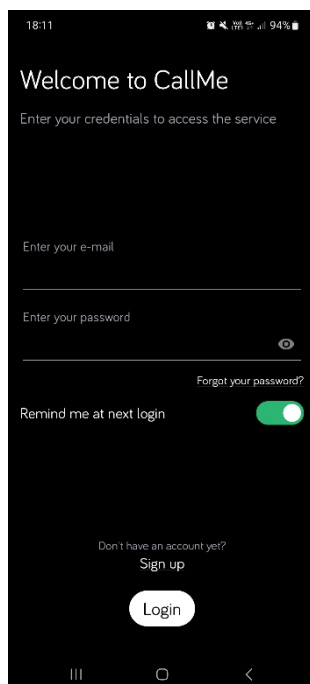


Figure 526: app login page or to create an account

Once logged in with a newly created or existing account, the application homepage is displayed:

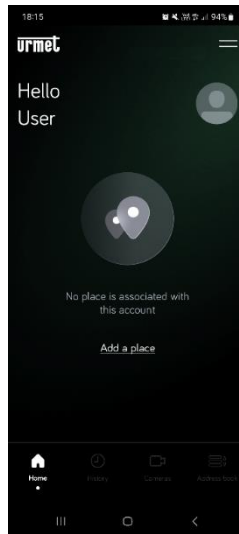


Figure 527: Create an account or log in

Pressing the “Add a place” button the following screen appears:

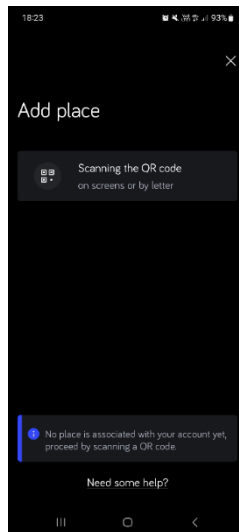




Figure 528: add of a place

Press the "Scanning the QR code" button to start the QR Code Reader application, then scan the QR code displayed on the apartment video door phone. Depending on the video door phone model, the various steps to view the QR code to scan are shown.

**VIDEO DOOR PHONE 7" VOG<sup>7</sup> 1761/31-32-33, 7" MAX 1717/31-32-33-34-41, 10" MAX 1717/21-22-23, 7" BASIC 1741/1**

- Switch on the master video door phone display by pressing anywhere on the screen or by pressing the Home button.
- If you are not already viewing the *Video Door Phone* page, press the icon  to access the "Top Page" and then the icon :

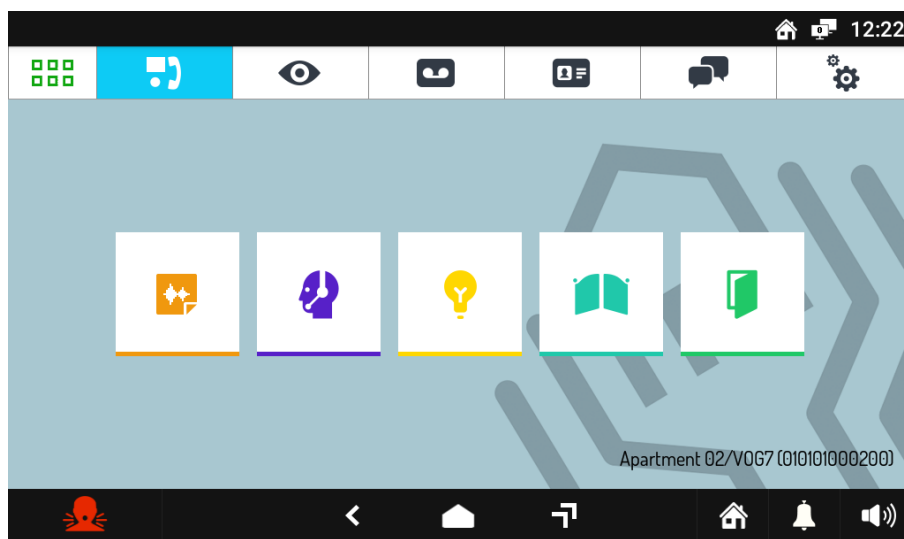



Figure 529: video door phone application

- Press the icon  at the top right to access the video door phone configuration page:

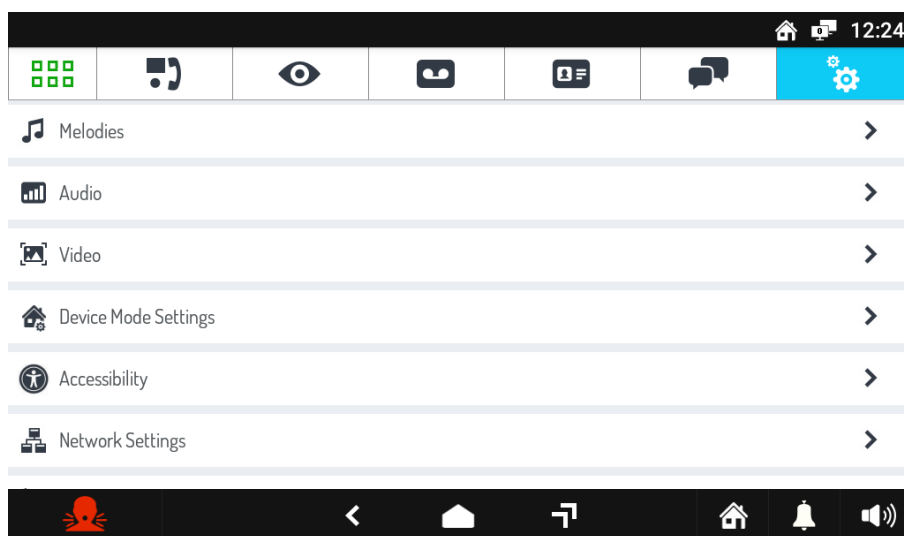


Figure 530: video door phone application settings

- Press on “Device Mode Settings” item:

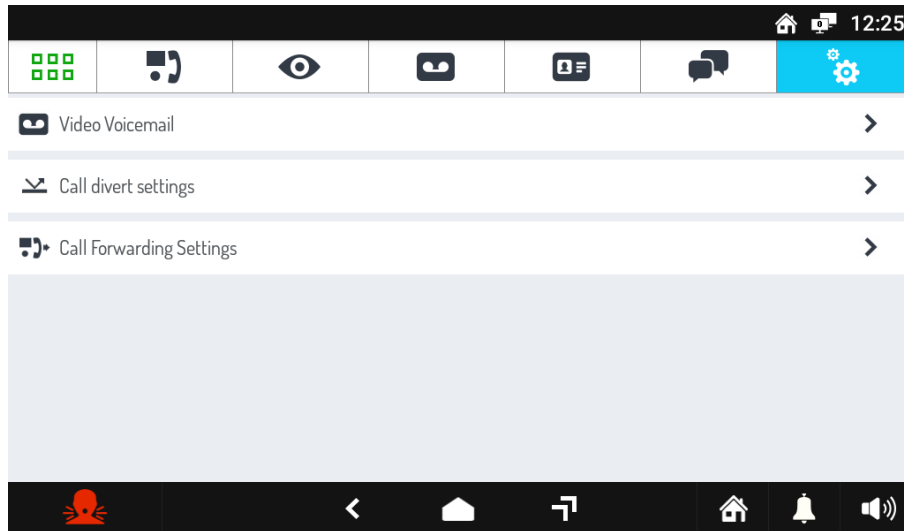


Figure 531: device mode settings

- Press on the item “Call Forwarding Settings” and then on the item “Activate/Verify Call Forwarding service”:

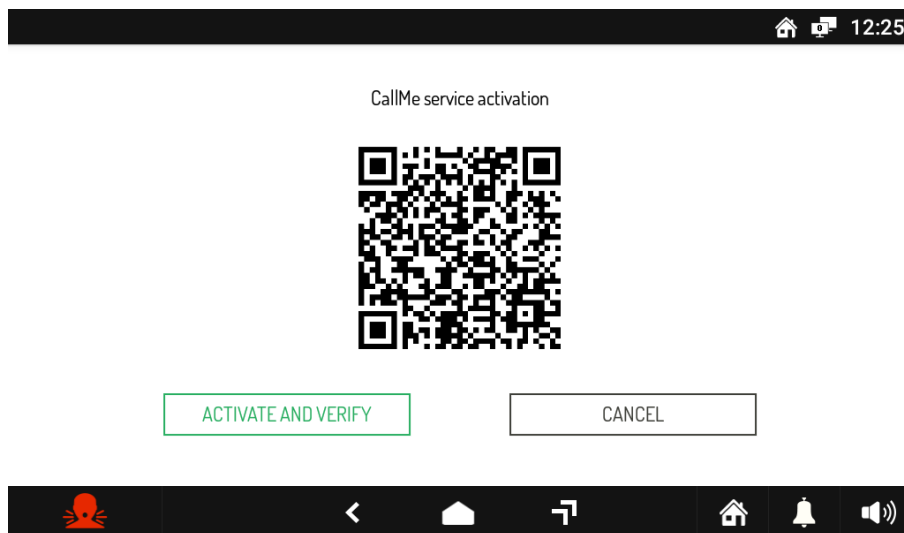



Figure 532: QR code for call forwarding function activation

## VIDEO DOOR PHONE VOG<sup>5+</sup> 1761/15-16-18-19

- Press the button  twice to access the homepage, the following screen appears on the video door phone display:

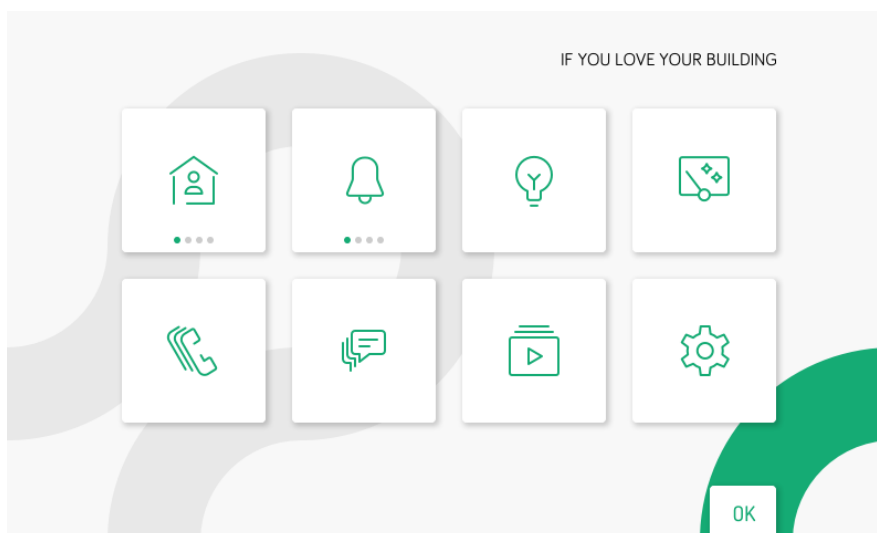








Figure 533: homepage

- Press the , , , and  buttons to select the following icon , then press the button  to access the video door phone configuration menu:

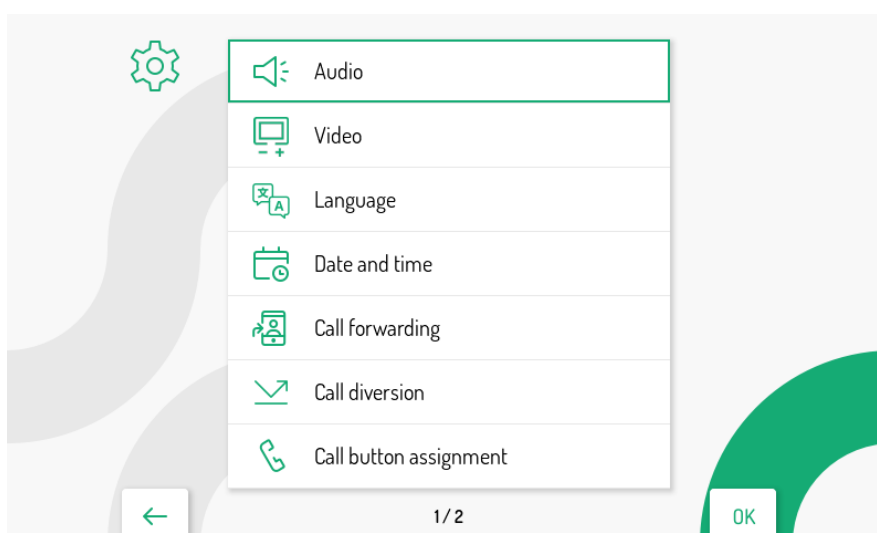




Figure 534: configuration menu

- Press the  button and select the “Call forwarding” item, press the button  to confirm the selection.
- The following screen appears on the display:

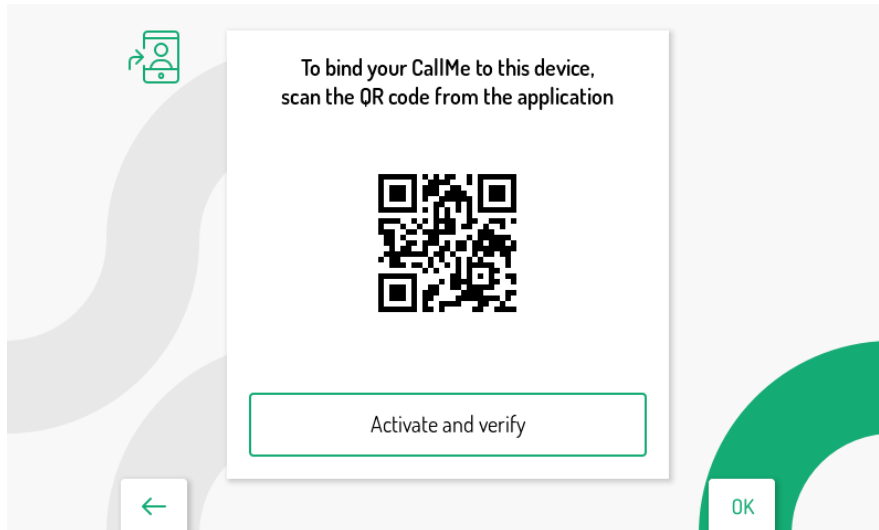



Figure 535: QR-code to associate the account with the apartment



**VIDEO DOOR PHONE VOG<sup>5</sup> 1761/6**

- Access the configuration menu by pressing and holding down the button  for at least 5 seconds with the display off:

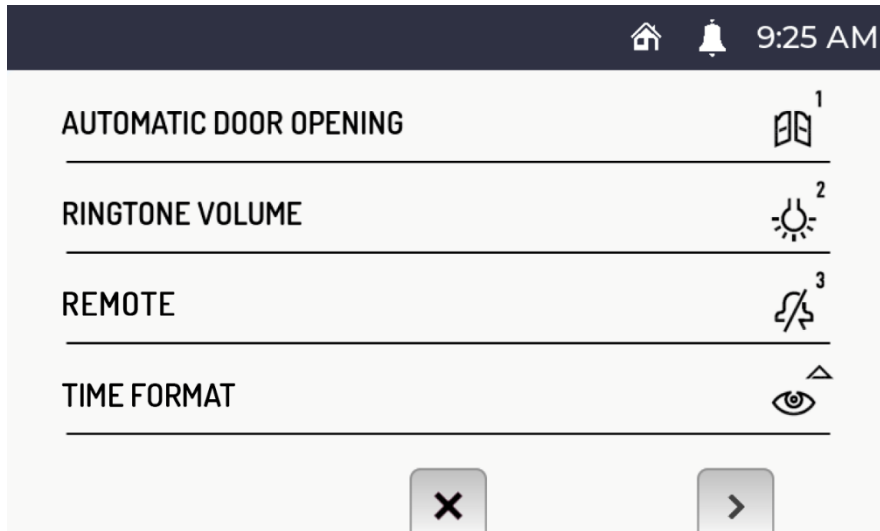



Figure 536: configuration menu (first window)

- Press the button  to display the second window of parameter configuration:

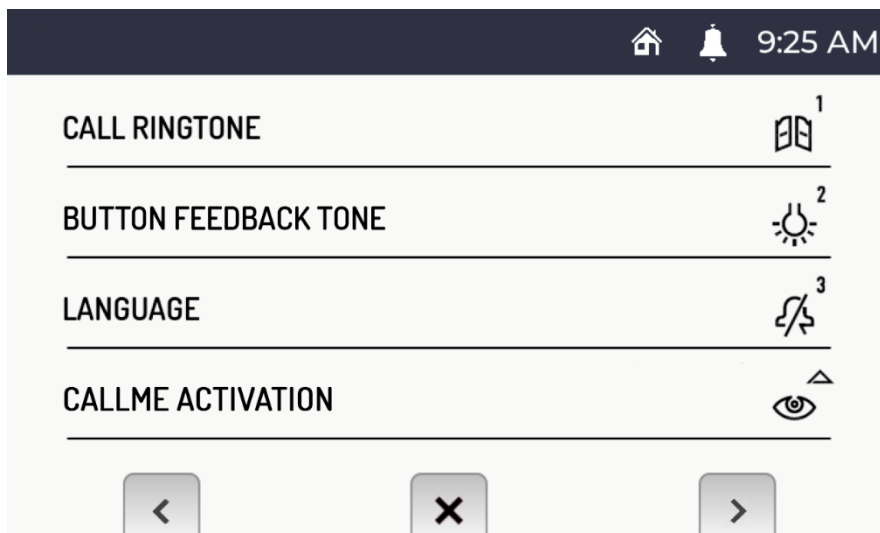


Figure 537: configuration menu (second window)


- Press the button  in the second screen of the configuration menu, the display will show the following window:



Figure 538: QR-code to associate the account with the apartment

After scanning the QR-code (in one of the three cases above), the app shows the following screen:

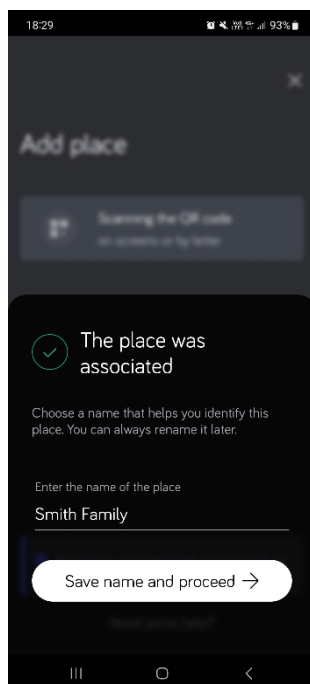


Figure 539: association of a place/apartment with the CallMe account

If you want, you can change the name “Smith Family”. By pressing the “Save name and proceed” button, the *CallMe* application home page appears as shown below:

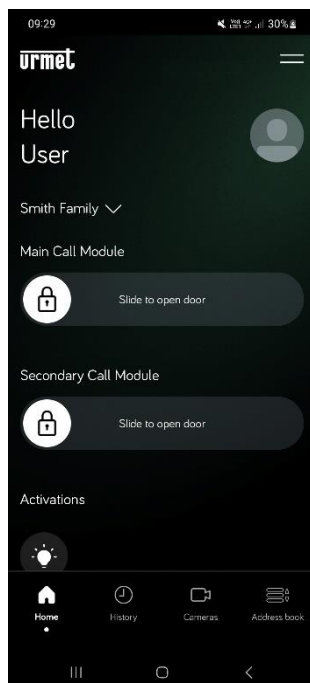


Figure 540: the account has been associated with the apartment

At this point on the video door phone, it is necessary to:

- press the “Activate and Verify” button to activate the call forwarding function and verify its correct activation;
- check that the apartment's master video door phone automatically shows (if the function is activated for the first time) the *Remote* mode icon.

The "Activate and Verify" button is located on the same screen where there is the QR-code associating the CallMe account with the apartment. Once pressed, the correct outcome of the operation is indicated by the following dialogue box depending on the different models of video door phone:

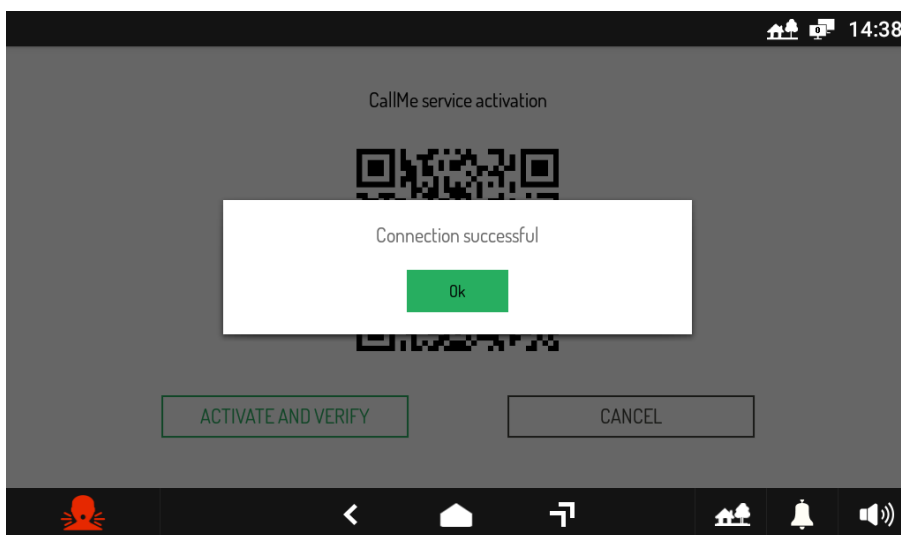


Figure 541: correct activation of the call forwarding function on video door phones 1717/xx - 1761/3x - 1741/x

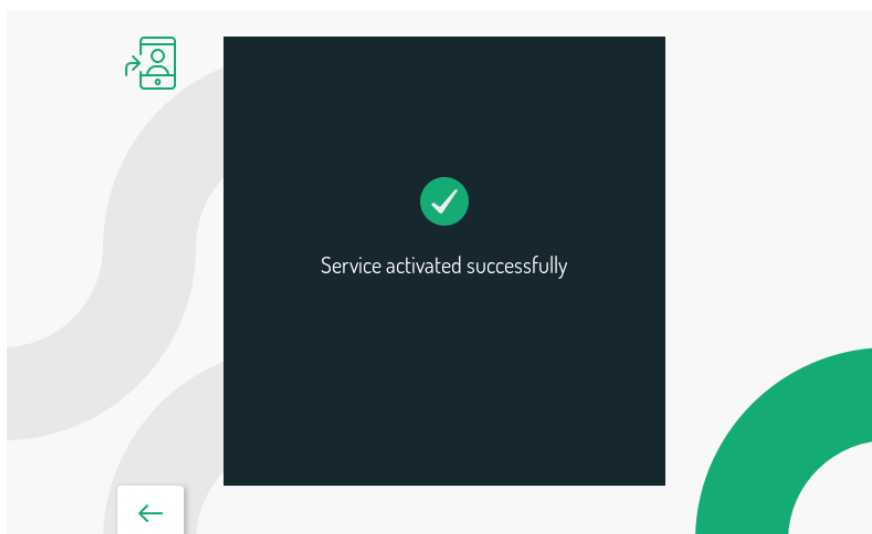


Figure 542: correct activation of the call forwarding function on video door phones 1761/1x

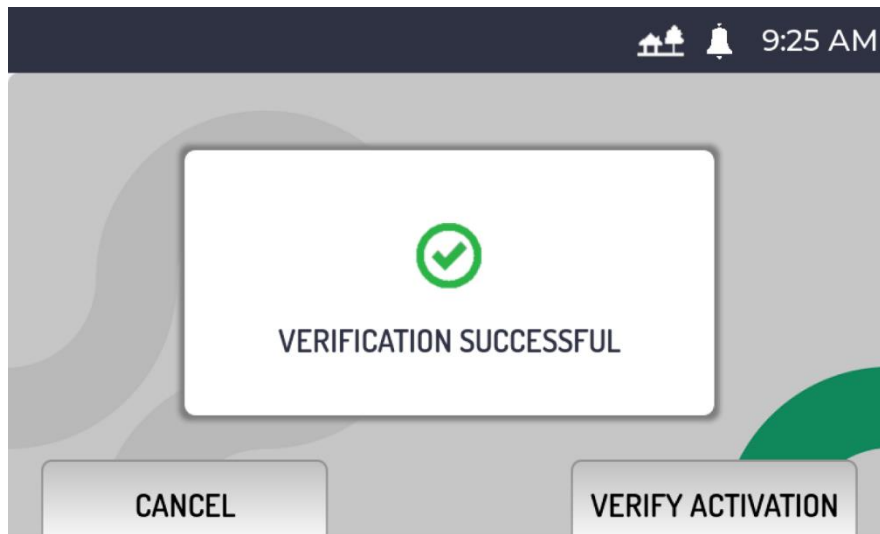


Figure 543: correct activation of the call forwarding function on video door phones 1761/6

As a final step, it is necessary to check that the “Remote” mode operating icon appears on the master video door phone as shown below depending on the different types of video door phone models:

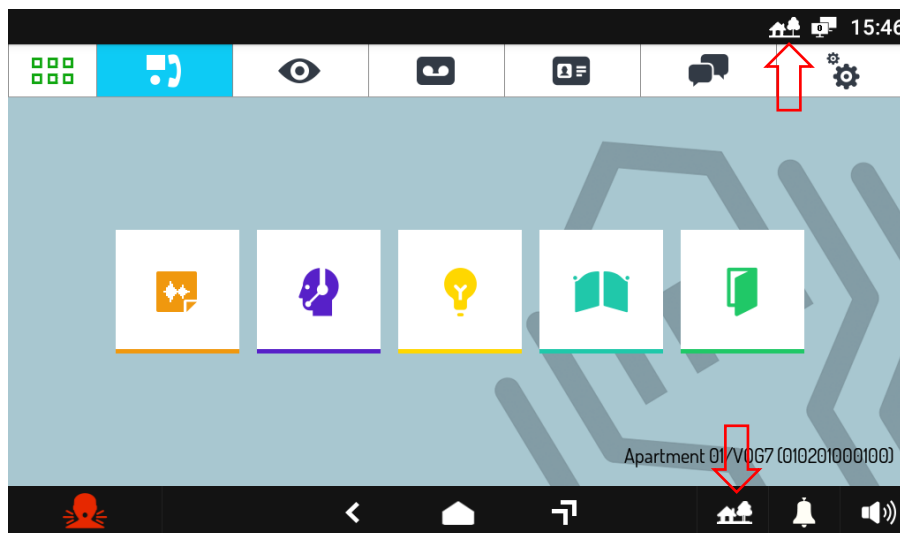


Figure 544: “Remote” mode operation icon on video video door phones 1717/xx - 1761/3x - 1741/x

On any slave video door phones, the “Remote” mode operating icon is only shown at the top right.

If operation in “Remote” mode has already been activated and deactivated previously on the video door phone, the relevant icon must be activated manually: it is necessary to press the icon (bottom right) only on the master video door phone and then select the icon .

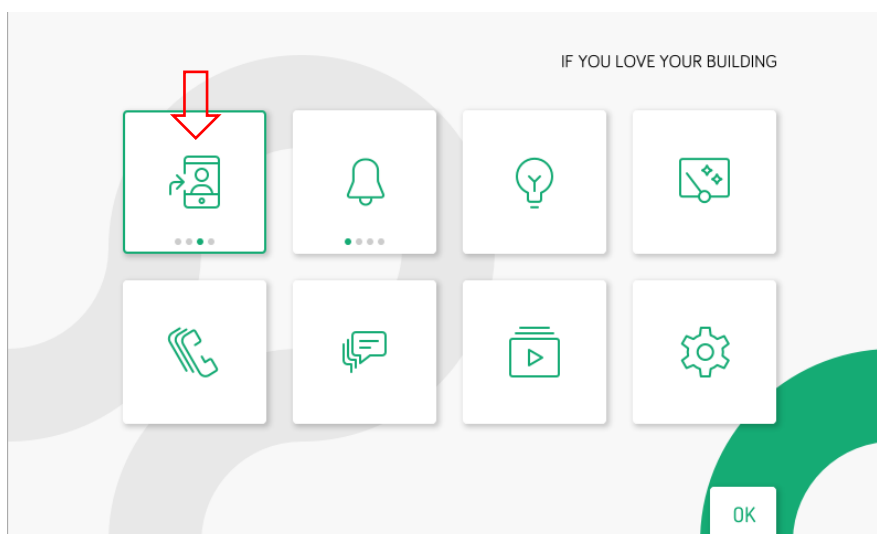








Figure 545: "Remote" mode operation icon on video video door phones 1761/15-16-17-18

 On any slave video door phones, it is possible to view the "Remote" mode operating icon at the top right by pressing the button  once with the screen off.

 If operation in "Remote" mode has already been activated and deactivated previously on the video door phone, the relevant icon must be activated manually: it is necessary (only on the master video door phone) to select the icon  and with button  select the icon .

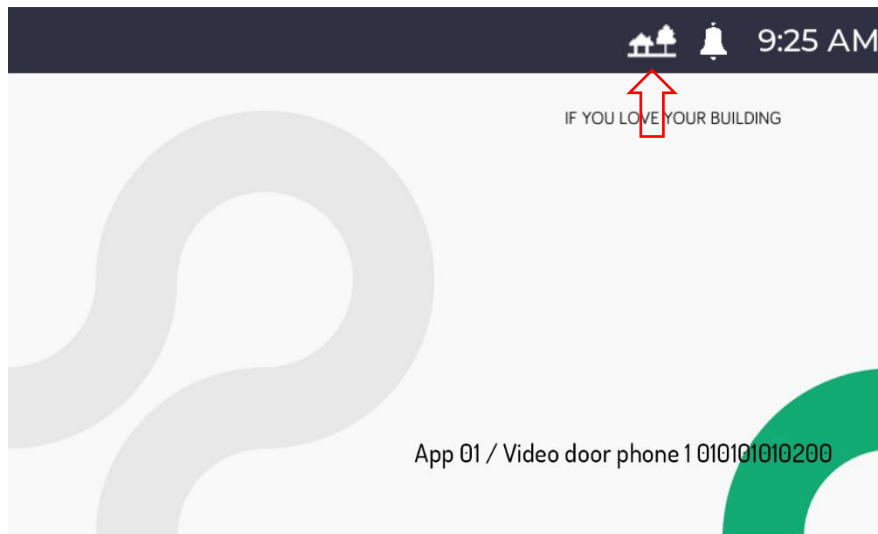







Figure 546: "Remote" mode operation icon on video video door phones 1761/6

 On any slave video door phones, it is possible to display the operating icon in "Remote" mode in the same way as seen for the master video door phone.


 If operation in "Remote" mode has already been activated and deactivated previously on the video door phone, the relevant icon must be activated manually: it is necessary (only on the master video door phone) with the screen off, press and hold down the icon  for at least 5s and use the button  to set the "Remote" mode.

The main features of the CallMe app are listed below:

- call forwarding to the apartment on smartphone/tablet (video door phone must be set in "remote" mode);
- auto-insertion on calling stations;
- intercom call to apartment stations;
- sending activation commands;
- door and gate opening even outside of the call.

 Auto-on on RTSP cameras is not supported by CallMe app.

For a detailed description of all the features of the CallMe application, please refer to the [relevant booklet](#) which can be consulted on the website [www.urmet.com](http://www.urmet.com).

 Once the call forwarding function has been configured for the various apartments and Switchboard applications, it is of fundamental importance not to redo a new system configuration from scratch (even if the topology is the same): if so, the procedure described above to associate the smartphone/tablet to apartments/Switchboard applications is to be repeated.



### 7.1.13 Configuring the call forwarding function in IPerCom systems in IPerCloud mode

The configuration of the call forwarding function in IPerCom system in IPerCloud mode requires the mandatory use of the following applications to be used in the following order:

- *IPerCom Installer Tools* (Windows application) for the installer (registration on Urmet Cloud is required),
- *CallMe Manager* (Windows application) for the installer and building manager (registration on Urmet Cloud is required),
- *CallMe* (Android or iOS smartphone/tablet application) for the end-user (registration on Urmet Cloud is required).

To configure the call forwarding function with the *CallMe Manager* app, it is necessary to enable the relevant item via the *IPerCom Installer Tools configurator*, the default value of which is disabled (see paragraph [Call Forwarding Settings](#)).

Below are the various actions to perform to correctly configure the function.

#### 1. INSTALLER

- Connect a router to the IPerCom system network that can provide Internet access;
- Install the *IPerCom Installer Tools* PC application;
- Create an Urmet Cloud account via *IPerCom Installer Tools* and authenticate on *IPerCom Installer Tools* with this account;
- Using the *IPerCom Installer Tools* application, create a system configuration with IPerCloud apartments and verify that the parameters of the call forwarding function are correct;
- Enable the *test mode* (from the *configurator*) and then verify that the call to a test IPerCloud apartment from any calling station arrives to the *CallMe* application without pre-activating (and therefore wasting) any license;
- Disable test mode (from the *configurator*);
- Pre-activate license bundle;
- Install the *CallMe Manager* application and authenticate with the same Urmet Cloud account created before;
- Using the *CallMe Manager* application, activate the license bundle, assign them to the IPerCloud apartments and transfer the site to the building manager via invitation sent via e-mail.

## 2. BUILDING MANAGER

- Install the *CallMe Manager* application on the PC;
- Create an Urmet Cloud account via *CallMe Manager* and authenticate on *CallMe Manager* with this account;
- Acquire the site created by the installer via the *CallMe Manager* app;
- Generate letters (pdf format) with the QR-code;
- Send letters via email or post to users.

## 3. END-USER

- Install the *CallMe* application, distributed for Android and iOS operating systems and downloadable from the relevant stores;
- Create an Urmet Cloud account via *CallMe* and authenticate on *CallMe* with this account;
- Scan the QR code sent by the building manager to associate the account with the apartment.

## What the installer must do

Using the *IPerCom Installer Tools* application, the installer creates the configuration associated with the project, that is defines the system topology, adds the devices on the topological nodes, assigns appropriate names to the devices, **IPerCloud apartments** and topological nodes, creates the address books, the residents, not residents, and activations, configure the parameters of the call forwarding function in the "System" section of the *configurator* (as shown below):

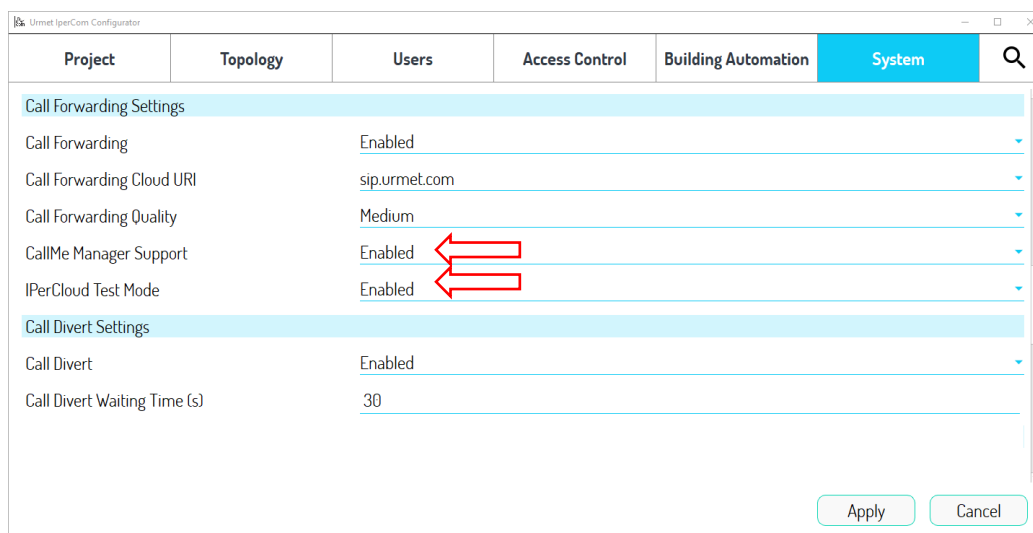


Figure 547: call forwarding parameters in tab "System"

For the "Call Forwarding" item, check that the value is set to "Enabled", as shown in the figure above.

For the "Call forwarding Cloud URI" item, it is necessary to set the server on which, via the *CallMe* app, the user is registered: the default server is "sip.urmet.com", while the "cn.sip.urmet.com" server is to be used only for the Chinese market.

The "Call forwarding quality" item must be set according to the available bandwidth: if you encounter problems in the call, such as jerky video and/or incomprehensible audio, it is best to lower the quality of call forwarding.

The "CallMe Manager Support" item must be enabled to configure the call forwarding function with the *CallMe Manager* app (if not enabled, the item is enabled automatically as soon as an IPerCloud apartment is added).

The "IPerCloud Test Mode" item must be enabled to be able to run the test mode of a generic IPerCloud apartment without using the licenses.

After carrying out the configuration, it is necessary to apply it to the system. To do this, you must first save the configuration and exit the *configurator*. Then select the “*Configuration*” tab and press the “*Apply changes*” button to transfer the configuration to the system:

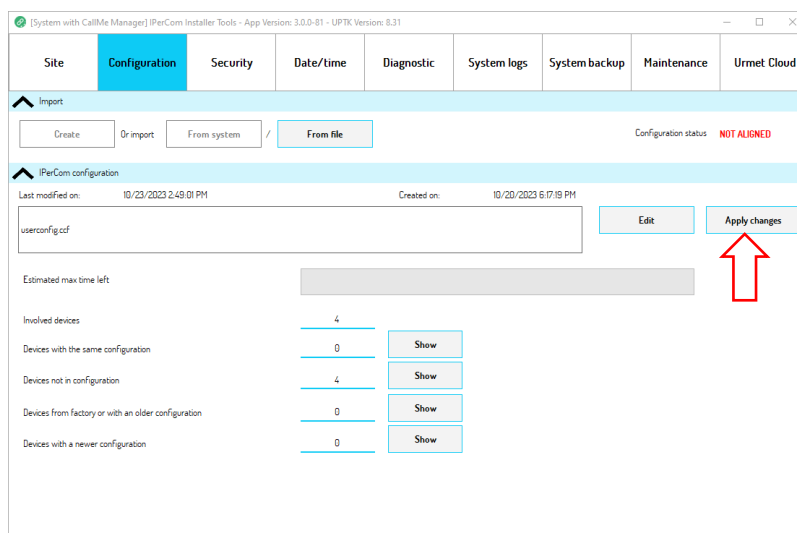


Figure 548: configuration transfer

After applying the configuration to the system, the installer must carry out the test mode: this mode is useful for verifying that the call from any calling station to a test IPerCloud apartment arrives correctly at the CallMe application.

Therefore, to carry out the test mode, the installer must have downloaded, installed, and started the CallMe app on his smartphone/tablet and then log in with the same account used on *iPerCom Installer Tools*.

Once logged in, this screen appears:

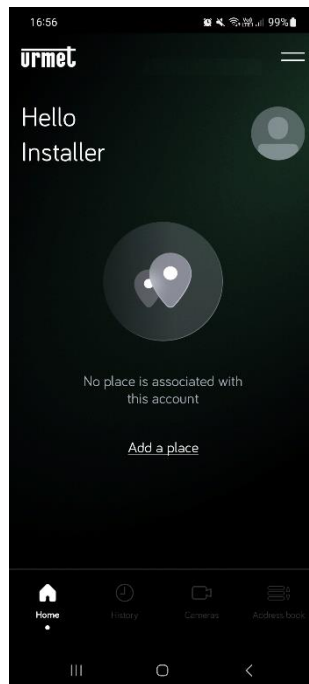


Figure 549: log in to app CallMe

Pressing button “Add a place”, the following window appears:

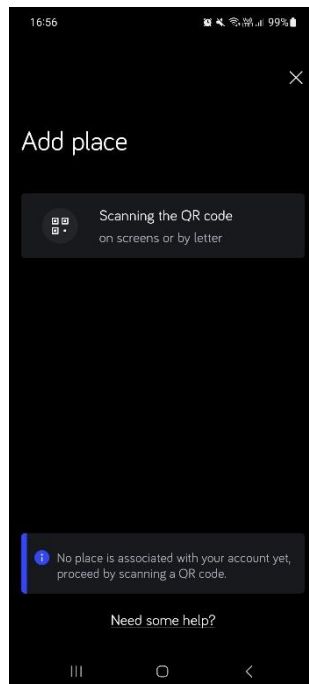


Figure 550: add a place

Press button “*Scanning the QR code*” to run app QR code reader.

Then press the “*IPerCloud Test QR Code*” button displayed on *IPerCom Installer Tools*. The following window appears:

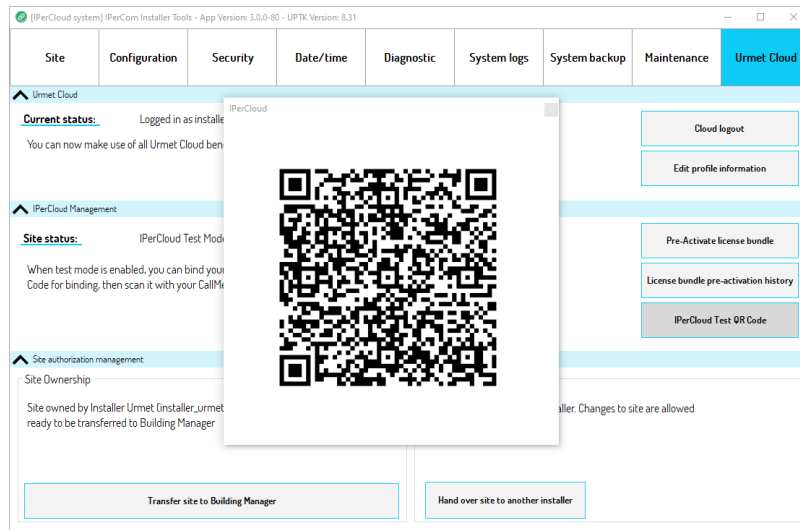


Figure 551: scan the test mode QR Code

Then scan the QR code displayed on the PC where the *IPerCom Installer Tools* application is installed.

After scanning the QR code, the following screen appears on smartphone/tablet of the installer to indicate that the place has been added correctly:

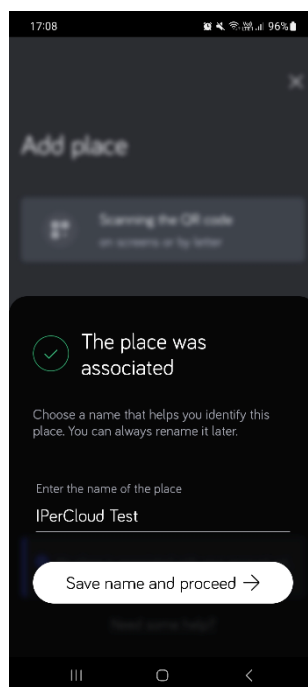


Figure 552: place added

The default name given to the place is “*IPerCloud Test*” but it is possible to rename it (even later): at this point the *CallMe* app has been associated with a (not real) IPerCloud test apartment. The installer can therefore make a call from any calling station to the IPerCloud test apartment: in fact, on all calling stations with displays the relevant address book displays only the name “*IPerCloud Test*” while calling stations with button call (from any button) the “*IPerCloud Test*” apartment.



*Any address book present on the calling stations with displays reappear after disabling the test mode from the configurator.*

In test mode the installer can only do the following:

- call the test IPerCloud apartment from any calling station,
- check that the call reaches the *CallMe* app,
- answer the call by checking the correct presence of audio and video,
- open the doors (main door and gate) only during conversation,
- auto-insertion on calling stations.

The test mode can therefore be considered passed if the points listed above work correctly.



*In test mode from the CallMe app it is not possible to open the doors (main door and gate) outside of a call and it is not possible to activate any activation.*

Once the test mode is finished, you need to disable it from the *configurator* and apply the configuration.

After that, go to tab “Urmet Cloud” in the section **IPerCloud Management**:

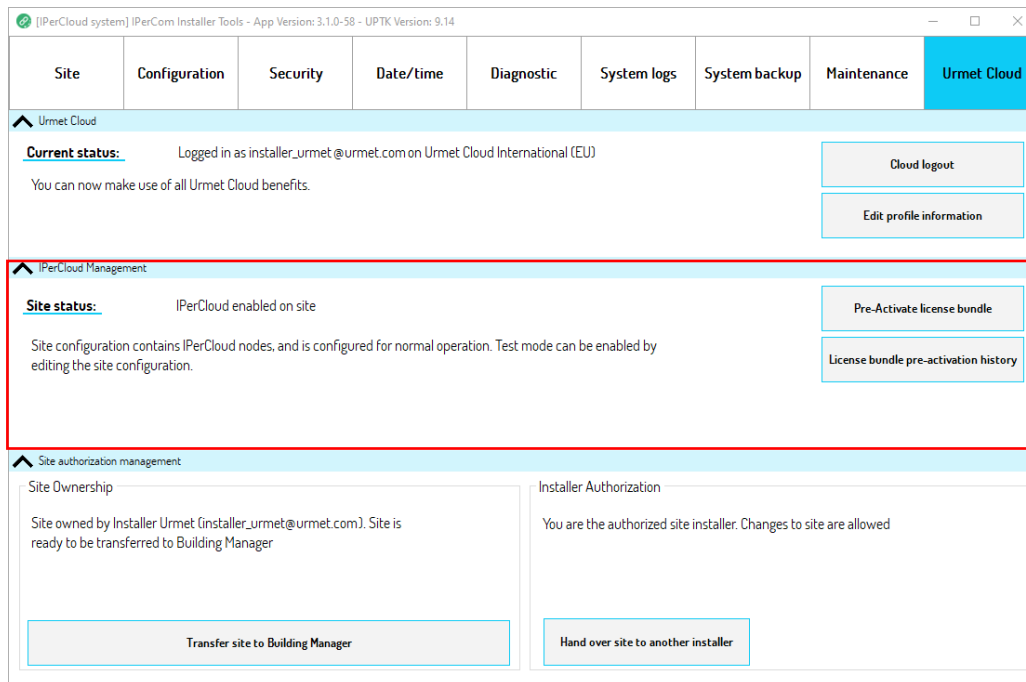


Figure 553: IPerCloud management

In this section the installer pre-activates a license bundle for the system by pressing the "Pre-Activate license bundle" button. The following window opens:

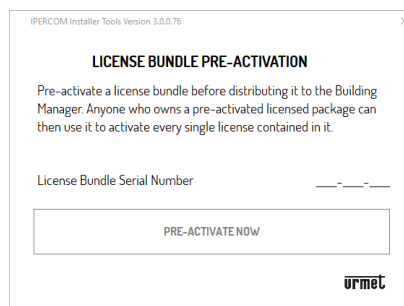


Figure 554: license bundle pre-activation

In the "License Bundle Serial Number" field it is necessary to enter the serial number of the license bundle for pre-activation by the installer. The number is shown on the license card with the abbreviation “S/N”.



After entering the serial number, pressing the "PRE-ACTIVATE NOW" button, and accepting the license agreement relating to the IPerCloud software (End User License Agreement), the positive outcome of the pre-activation is confirmed by the following message:

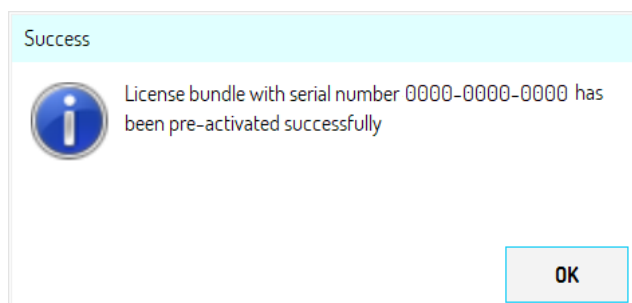


Figure 555: bundle license pre-activation with serial number

Once the pre-activation of the licenses has been completed, the installer must install the *CallMe Manager* application: the application and the related user manual are available on the website [www.urmet.com](http://www.urmet.com) at the download section.

You can then start the application and authenticate with the Urmet Cloud account already used for *IPerCom Installer Tools*:

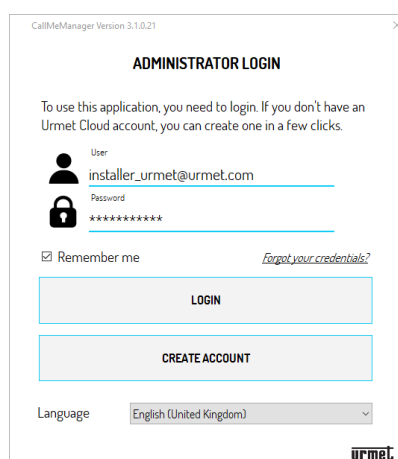


Figure 556: authentication on CallMe Manager by installer

By pressing the "Login" button, the *CallMe Manager* application starts and shows the following dialog box relating to the presence of a new site ("IPerCloud System") transferred to the installer account (which in this case is also the site building manager):

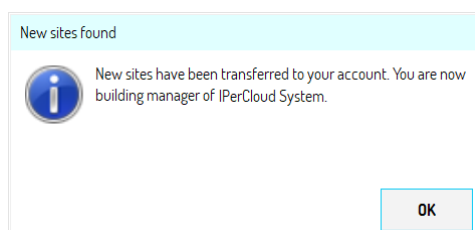


Figure 557: new site transferred to building manager/installer

By pressing the "OK" button, the home page of the *CallMe Manager* application appears with the new site loaded:

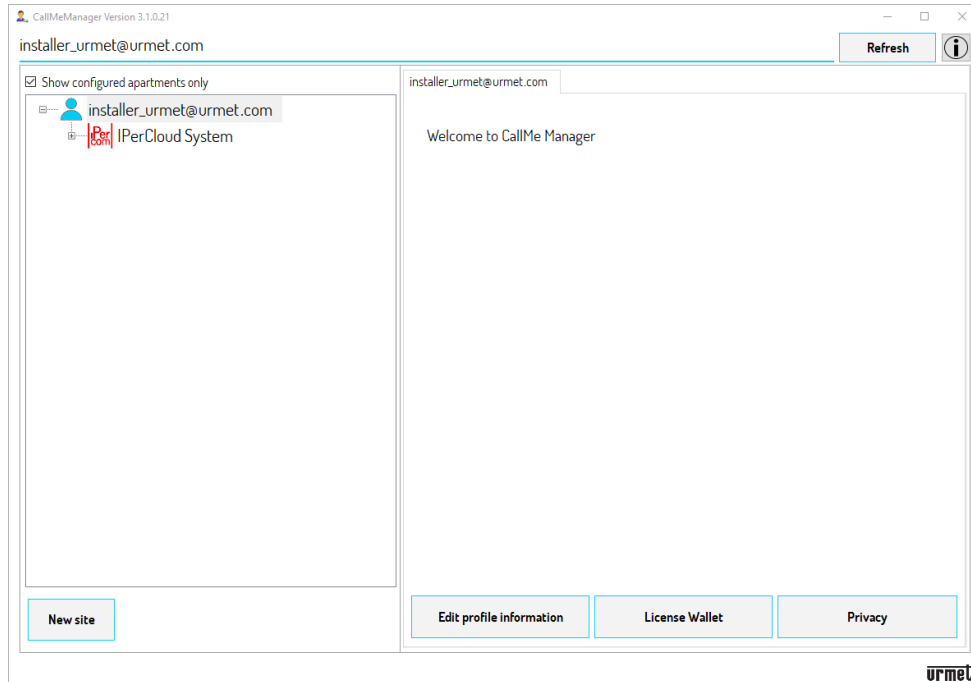


Figure 558: *CallMe Manager* home page (installer login)

By expanding the topological structure, it is possible to view all the topological nodes present in the system, that is blocks, stairs, floors, and apartments:

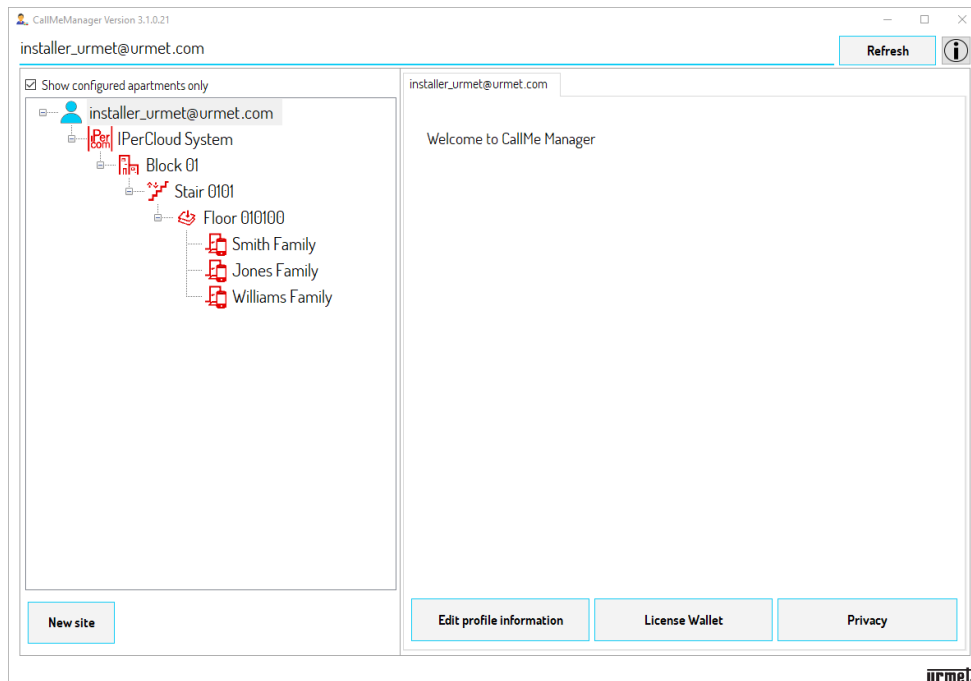




Figure 559: plant topological structure

 The topological node icons are displayed in red to indicate that the topological structure contains Ipercloud apartments to which a license has not yet been associated. More precisely, the icons of the nodes located on the topological path of the IPerCloud apartments are colored red.

 Hybrid apartments (i.e. IPerCloud apartments with one apartment station) are displayed in black.

At this point it is necessary to activate the licenses pre-activated previously by IPerCom Installer Tools. It is necessary to select the node where the installer's email appears and press the "License Wallet" button:

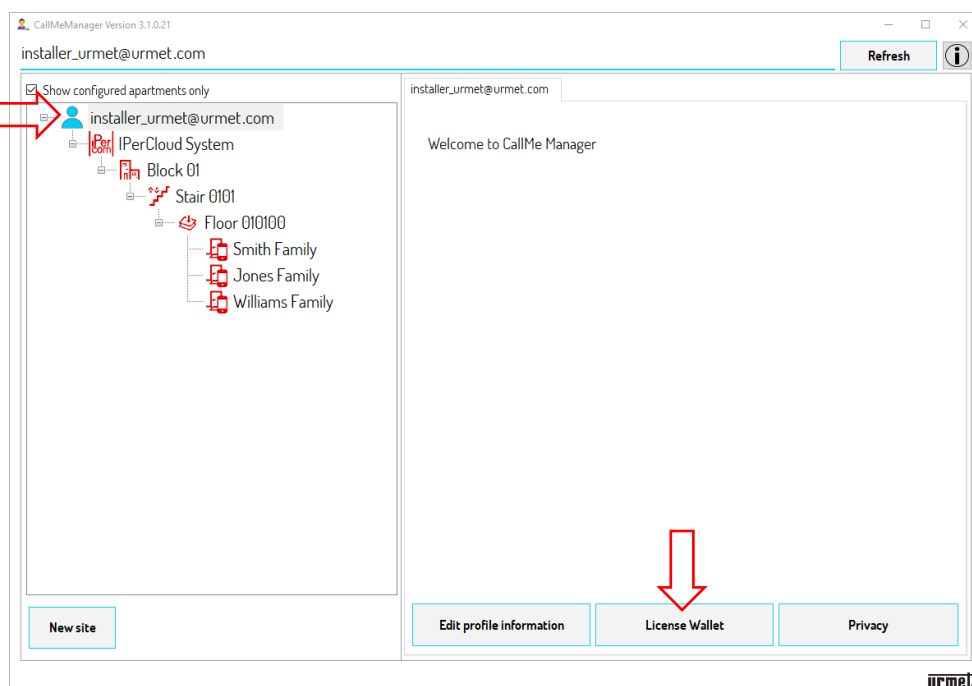


Figure 560: license wallet button

The following window is shown:

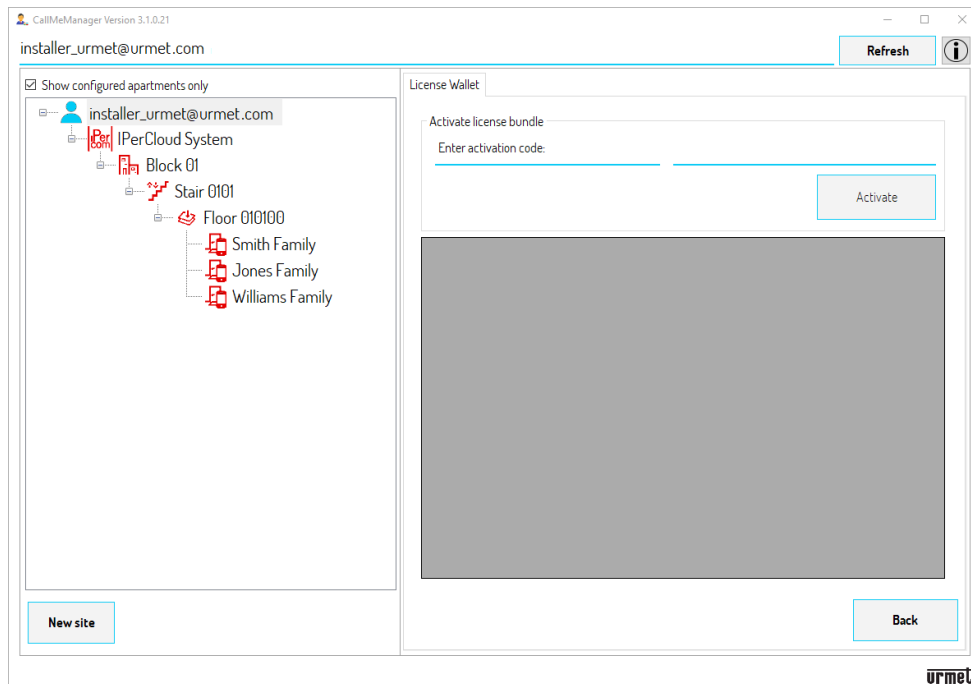


Figure 561: license wallet window

To activate one or more license bundles, it is necessary to know the activation code (A/C) shown on the license card as shown below:

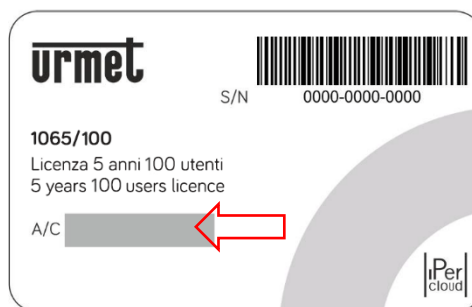


Figure 562: license bundle activation code



To view the activation code, you need to scratch the silver band next to the red arrow with a coin.

At this point, simply enter the activation code in the relevant field and press the "Activate" button:

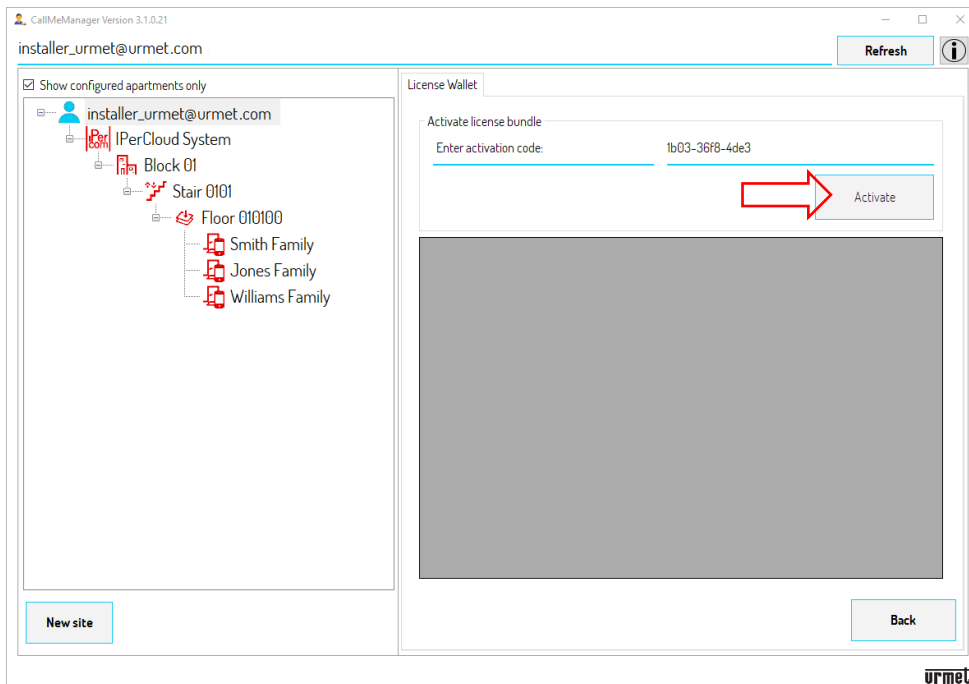


Figure 563: license bundle activation request

The correct outcome of the procedure is confirmed by the following dialog box:

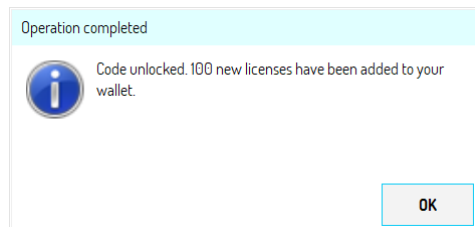


Figure 564: license bundle activated successfully

By pressing the “OK” button, the license is added to the installer's wallet:

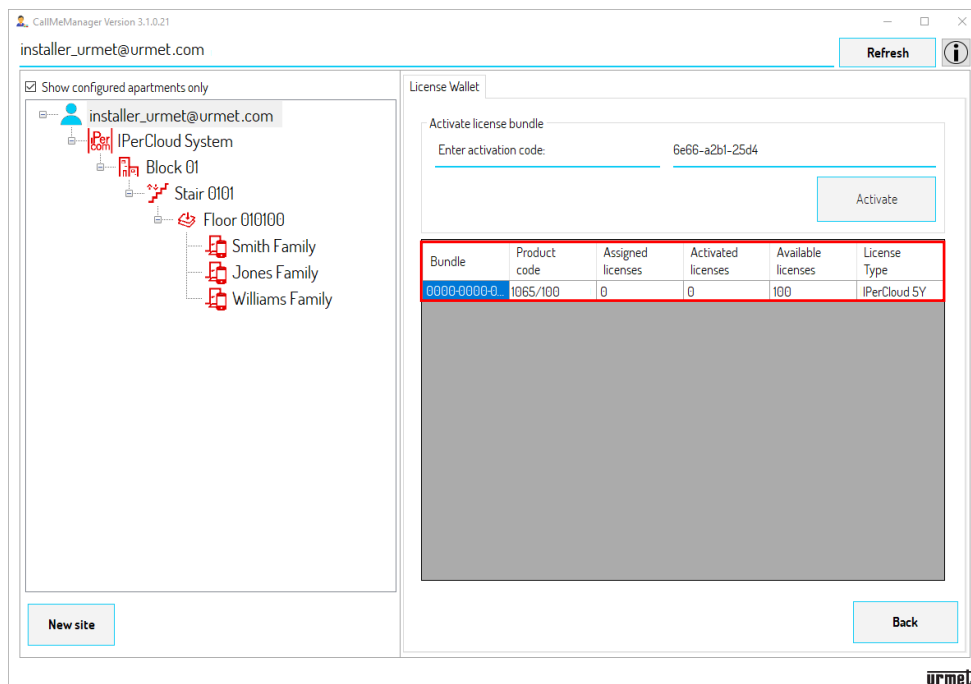


Figure 565: license added to installer wallet

All the information relating to the newly activated license bundle is displayed in the red box, that is:

- **Bundle:** identifies the serial number of the Ipercloud license bundle (entered during the pre-activation phase);
- **Product code:** identifies the product code of the license bundle;
- **Assigned licenses:** identifies the number of licenses assigned to the apartments;
- **Activated licenses:** identifies the number of licenses activated by users via *CallMe*;
- **Available licenses:** identifies the number of available licenses that can still be assigned to apartments;
- **License type:** identifies the duration of the license, 5Y (5 years) or LT (15 years).

After activating a license bundle, it is necessary to associate the single licenses with the apartments. To do this, simply select the topological node where the IPerCloud apartments are present (in this case "Floor 010100") and press the "Licenses" button:

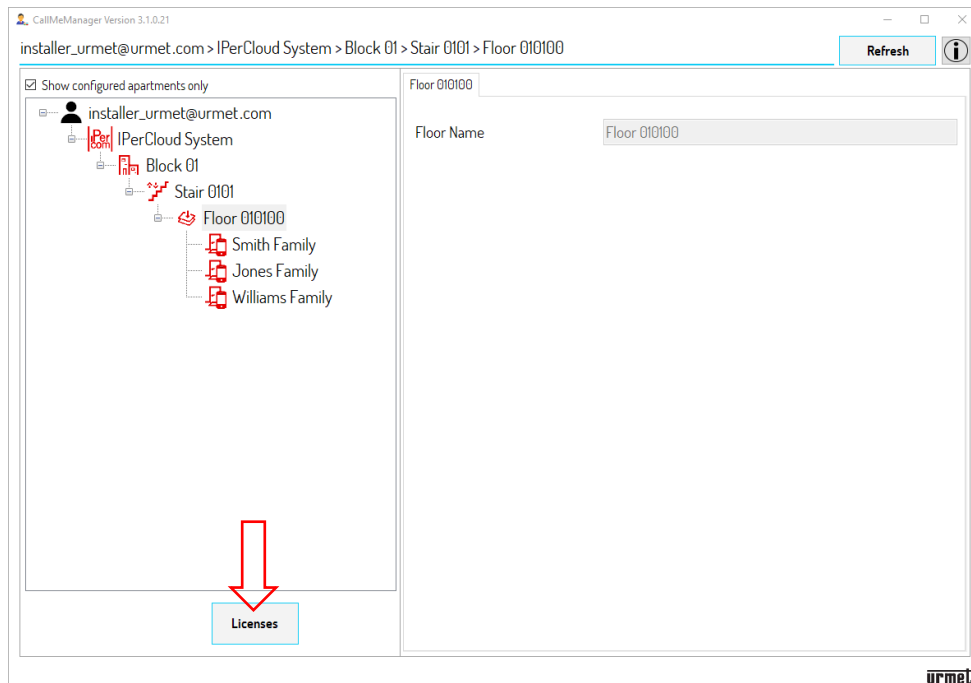


Figure 566: license association

The following window is shown:

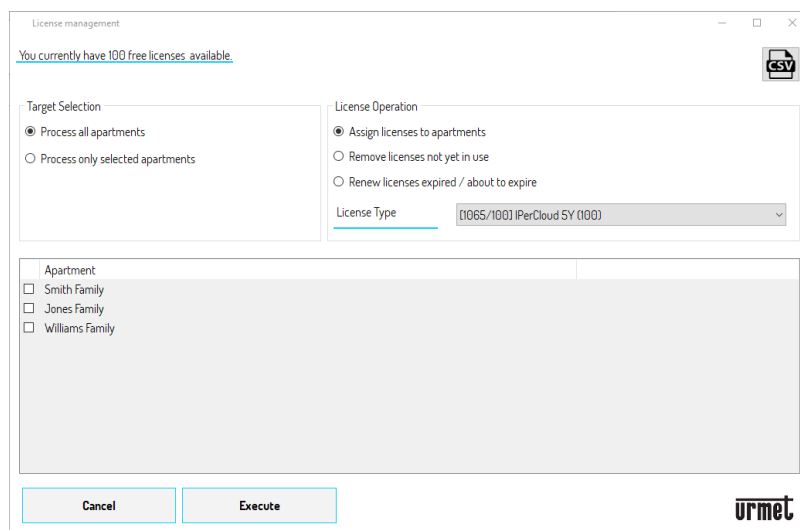


Figure 567: list of apartments to which to assign a license

In the **Target Selection** section, you can choose whether:

- assign licenses to all the apartments present on the topological node "Floor 010100" (item "Process all apartments"),
- assign licenses to only the selected apartments (item "Process only selected apartments").

In the **License Operation** section, select the item "Assign licenses to apartments".

In the **License Type** section, select the activated license bundle.

Then press the "Execute" button to associate the licenses with the 3 apartments.

The correct outcome of the procedure is confirmed by the following dialog box:

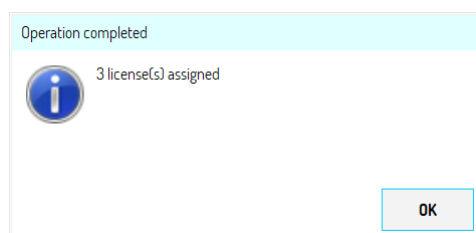


Figure 568: licenses correctly assigned to apartments



*The assignment of licenses can be carried out by positioning on any topological node. For example, if there are several floors with IPerCloud apartments, you can position yourself on the relevant upper stair node and assign licenses from this node. Similarly, if there are IPerCloud apartments on different stairs, it is sufficient to assign the licenses by positioning on the relevant upper block node.*



By pressing the “OK” button, the following screen appears:

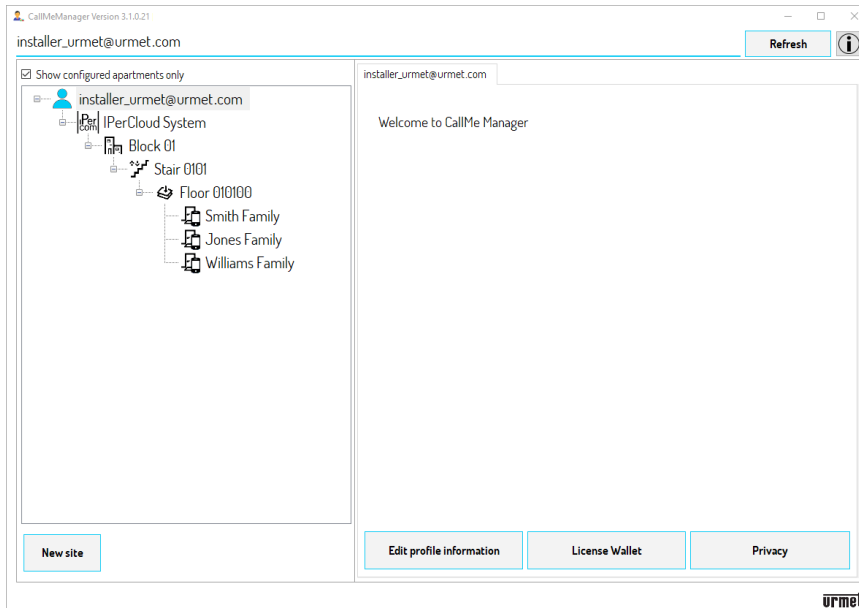


Figure 569: topological structure after assigning licenses to the apartments

After assigning licenses to apartments, the topological node icons are displayed in black to indicate that licenses have been assigned to Ipercloud apartments. By selecting a single apartment, you can view the single license in use:

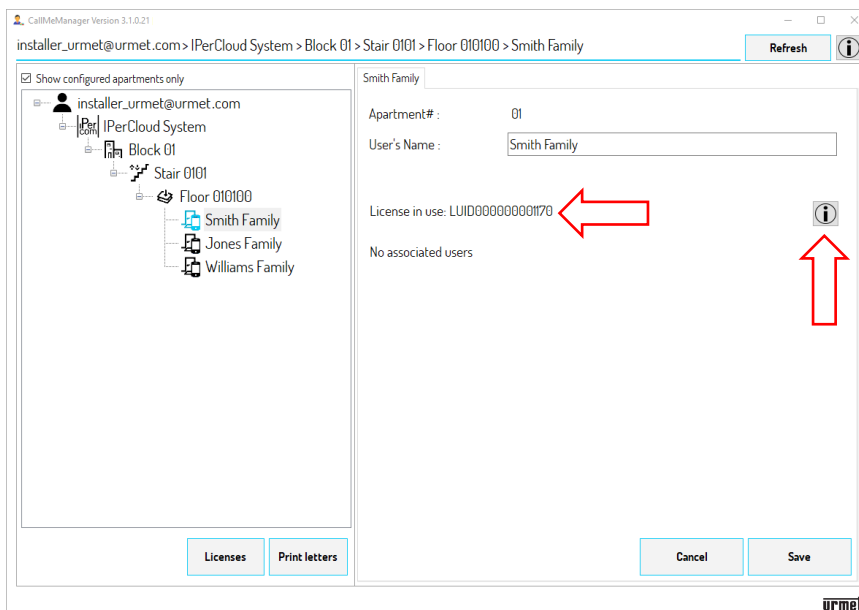


Figure 570: single license associated with an apartment

The "Info" button allows you to view all the information on the license in use by the apartment:

License Information LUID000000001170			
<u>License Type:</u>	IPerCloud SY	<u>Origin:</u>	CARD
<u>Assignment date:</u>	2023-10-24 15:16		
<u>Activation date:</u>	---		
<u>License expiry date:</u>	---	<u>Status:</u>	<b>Assigned</b>

Figure 571: information about the assigned license



The "Activation date" and "License expiry date" fields will be filled in as soon as the end user associates the account (created to authenticate on the CallMe app) with the apartment via the letter with QR code sent by the building manager.

At this point the installer's last task is to transfer the site to the building manager for printing the letters. To do this it is necessary to select the node that shows the name of the site (in this case "IPerCloud System"); on the right side of the CallMe Manager application a series of information relating to the building manager and installer of the current site is then displayed:

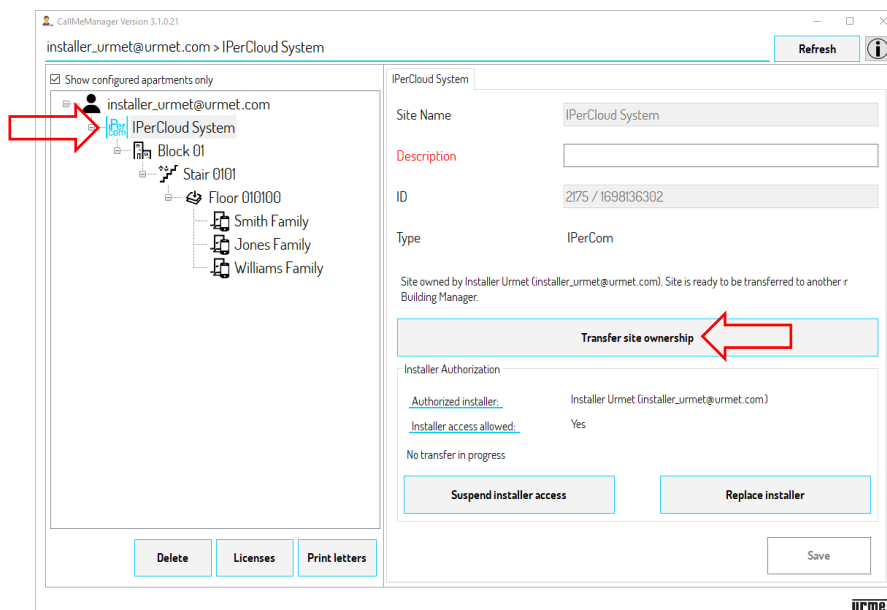


Figure 572: site transfer from installer to building manager

The "Transfer site ownership" button allows you to transfer the site to the building manager, who with the *CallMe Manager* application will be able to print the letters to send to the residents in the apartments. By pressing this button, the following dialog box is displayed in which it is necessary to enter the email with which the building manager has already registered with Urmet Cloud:

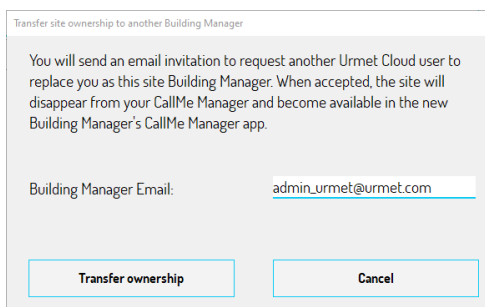


Figure 573: transfer of the site to building manager

By pressing the "Transfer ownership" button, an email is sent to the building manager and the correct outcome of the operation is confirmed by the following dialog box:

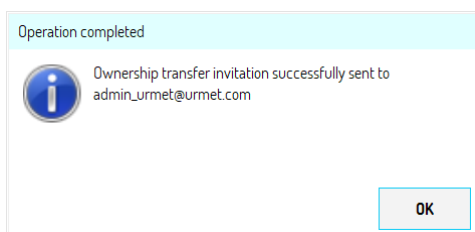


Figure 574: correct outcome of the invitation to the building manager

## What the building manager must do

Below are illustrated the fundamental steps that the building manager must follow to allow residents in IPerCloud apartments to use the call forwarding function. For all information on managing users, refer to the user manual of the *CallMe Manager* application.

The building manager must download the *CallMe Manager* application and the related user manual from the website [www.urmet.com](http://www.urmet.com).

The *CallMe Manager* application allows you to:

- generate the pdf files to send to users to allow the association of accounts with apartments for use of the call forwarding function;
- manage the accounts of users who use the call forwarding feature.

Before using the *CallMe Manager* application, the building manager must open the email that he received following the transfer of the site from the installer and press on the relevant link to make the transfer effective. The positive outcome of the operation is confirmed by the message "*Site acquired successfully*".

At this point it is possible to start the *CallMe Manager* application, authenticate with the Urmet Cloud account previously created by the building manager and press the "*Login*" button:

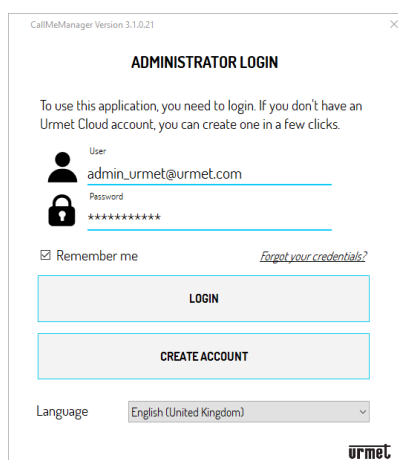


Figure 575: *CallMe Manager* login window

The *CallMe Manager* application displays the following dialog box relating to the presence of a new site ("*IPerCloud System*") transferred to the building manager account:

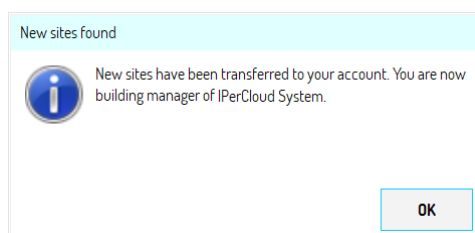


Figure 576: new site transferred to the building manager

By pressing the "OK" button, the homepage of the *CallMe Manager* application appears with the new site loaded:

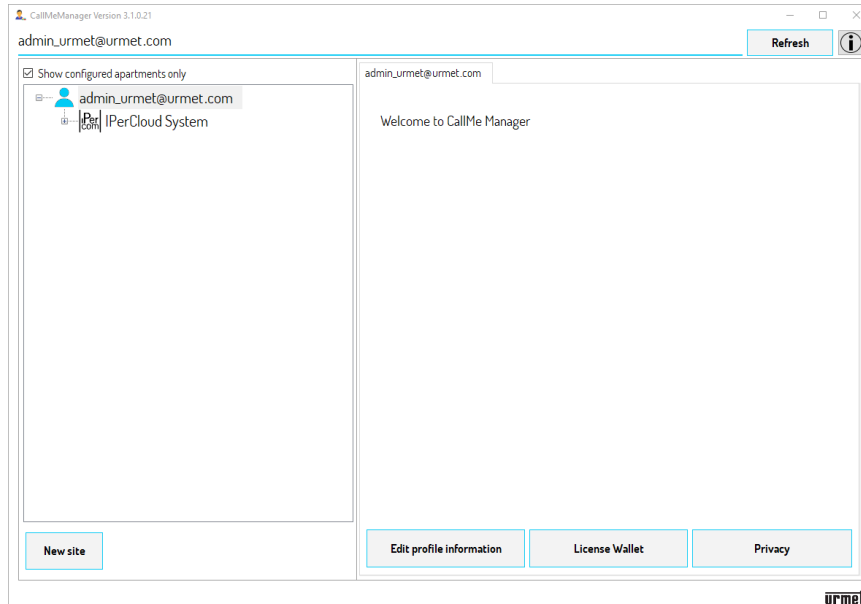


Figure 577: CallMe Manager app homepage

By expanding the topological structure, it is possible to view all the topological nodes present in the system, that is blocks, stairs, floors, and apartments:

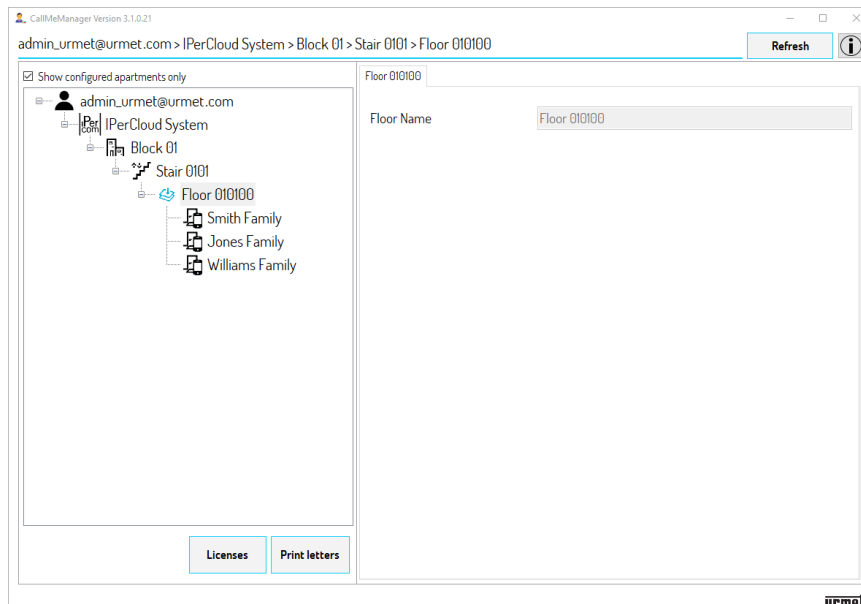


Figure 578: topological structure of the system

Once the topology has been imported, it is necessary to generate the letters (pdf file) which must be sent via email or post to the users, to allow the association of the accounts with the apartments (via the *CallMe* app) and the use of the function call forwarding: to do this, press the “*Print letters*” button.

Depending on the selected node, the letters of the users (and/or switchboard operator, if present) who are in the topological group of the node in question (including the node itself) are generated.

For example, if in the topological structure there is a block with 2 stairs (“*Stair 1*” and “*Stair 2*”) in which there are 10 floors in each stair and 10 apartments in each floor, positioning on the “*Stair 1*” node, only the letters for the users/apartments present in the “*Stair 1*” node are generated, that is 100 letters.

Relative to the previous figure, a pdf file with 3 letters is generated:

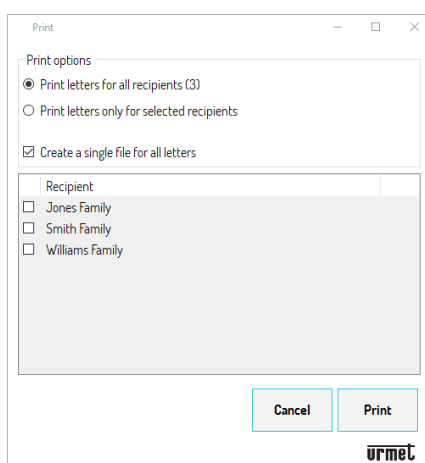



Figure 579: print of pdf letters

The “*Print letters for all recipients*” item allows you to generate pdf files for all recipients present within the selected node.

The “*Print letters only for selected recipients*” item allows you to generate pdf files only for selected recipients (to select a recipient, tick the box next to the recipient's name).

By checking the “*Create a single file for all letters*” box, a single pdf file containing all the letters from all recipients is generated (useful option for printing). If the box is not checked, a pdf file is generated for each individual recipient (useful option if you want to send pdf files for each recipient via email).

Press the “*Print*” button to generate letters in pdf format to send to users.

 *Printing the letters in pdf format is an activity that the installer could also do via the CallMe Manager application, after assigning the licenses. Once printed, the installer can send them via email to the building manager, who forwards them to the various residents.*

## What the building manager can still do (optional)

If in the topological structure shown on the left side of the *CallMe Manager* application, the building manager selects the node that shows the name of the system (red arrow), the following screen appears:

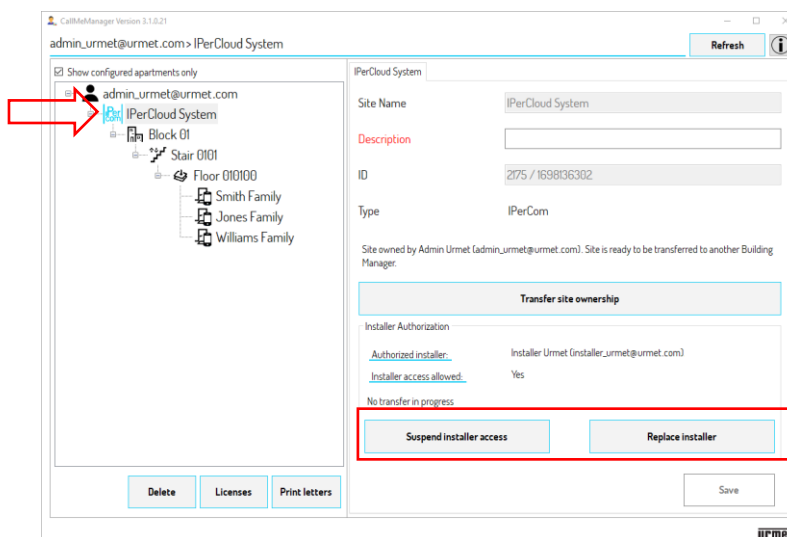


Figure 580: new features for building manager

The red box shows two new features for the building manager which are explained below.

### 1. SUSPEND/RESTORE INSTALLER

This feature is useful if the building manager wants to prevent the installer from making changes to the system after having correctly configured it; once suspended, you can still re-enable it if it is necessary to make changes to the system again.

The installer can be suspended by pressing the "*Suspend installer access*" button. The correct outcome of the operation is confirmed by the following dialog box:

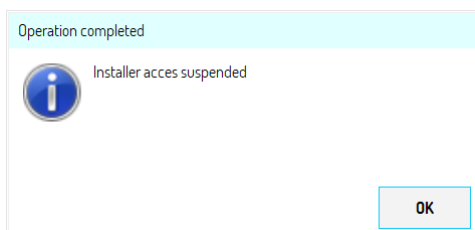


Figure 581: temporary suspension of installer

In this way the installer can make changes to the configuration via *IPerCom Installer Tools* but cannot apply them to the system. If the installer authenticates on Urmet Cloud via *IPerCom Installer Tools*, the "*Urmet Cloud*" tab shows the information that he has been suspended from making changes to the system, as shown below:

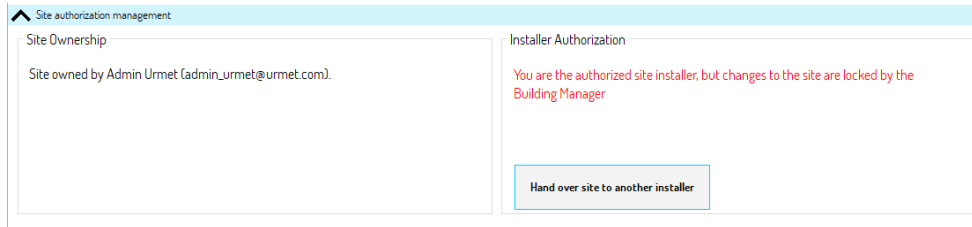


Figure 582: temporary installer suspension displayed in IPerCom Installer Tools

Once suspended, the building manager can re-enable the same installer via the "*Restore installer access*" button: a specific dialog box notifies the building manager regarding the correct outcome of the operation.

## 2. REPLACE INSTALLER

The "*Replace installer*" button allows the building manager to replace the installer of the system via an invitation sent via email. The procedure is the same as for transferring a site from installer to building manager: the building manager sends an invitation to the new installer via email, the installer accepts the invitation by pressing on a specific link contained in the same email, the building manager receives an email notification that the installer has accepted the invitation. If the old installer authenticates on Urmet Cloud via *IPerCom Installer Tools*, the "*Urmet Cloud*" tab shows the information that he is no longer authorized to make changes to the system, as shown below:

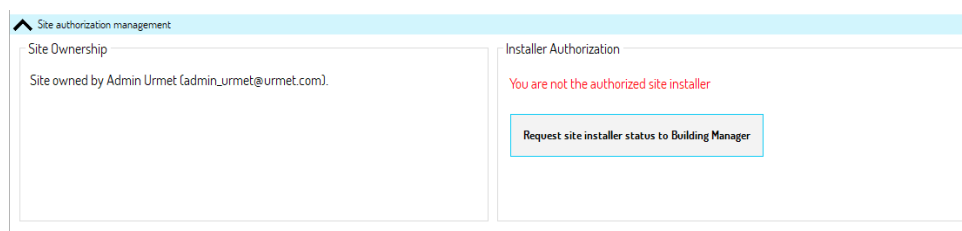


Figure 583: installer replacement displayed in IPerCom Installer Tools



### What the end-user must do

Below the basic steps that the end-user must perform with the *CallMe* app, after receiving the letter from the building manager, to activate the call forwarding function are reported. For all information on configuring the app, refer to the [relevant booklet](#) on the website [www.urmet.com](http://www.urmet.com).

Download the app from the Apple Store (iOS) or the Play Store (Android) and install it on your smartphone/tablet. The login page appears:

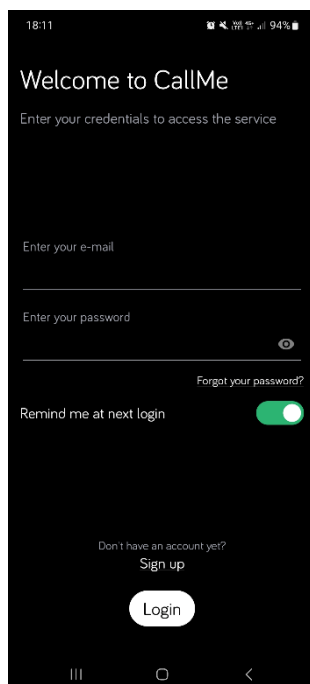


Figure 584: app login page or to create an account

Once logged in with a newly created or existing account, the application homepage is displayed:

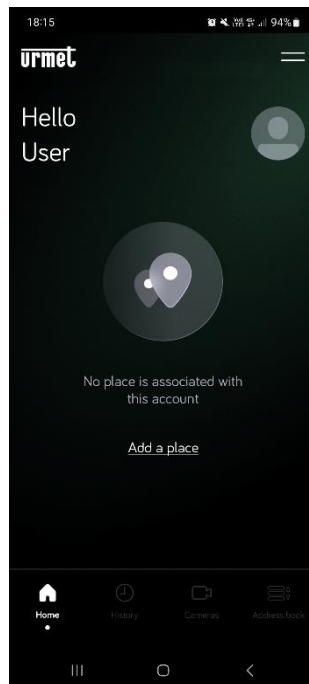


Figure 585: application homepage

Pressing the “Add a place” button the following screen appears:

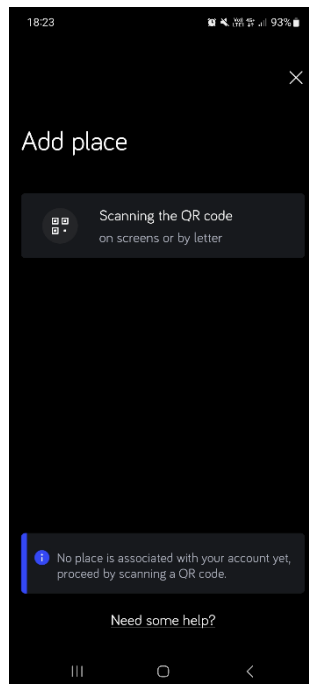


Figure 586: add of a place

Press the "Scanning the QR code" button to start the QR Code Reader application, then scan the QR code displayed in the letter sent by the building manager relating, for example, to the first apartment. The app shows the following screen:

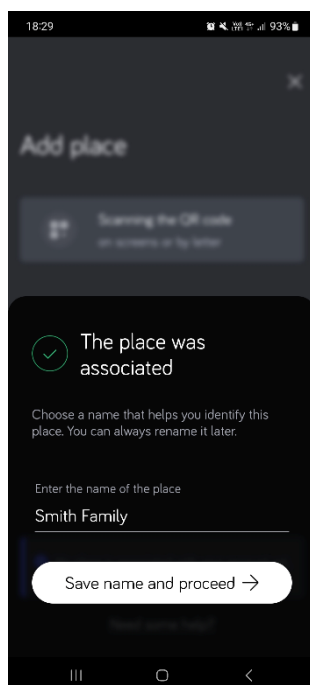


Figure 587: association of a place/apartment with the CallMe account

It is possible to change the name "Smith Family". By pressing the "Save name and proceed" button, the call forwarding function on the smartphone relating to the "Smith Family" apartment is activated:

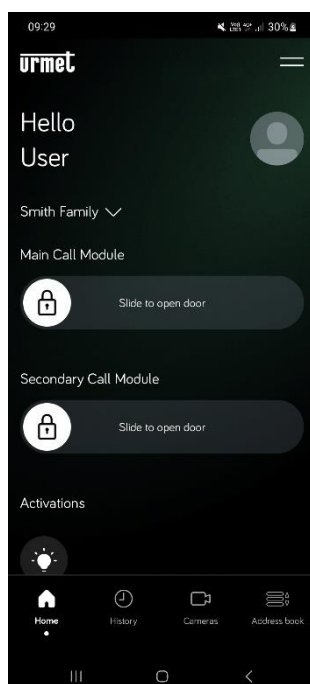


Figure 588: account associated with the apartment

The main features of the *CallMe* app are listed below:

- call forwarding to the apartment on smartphone/tablet;
- auto-insertion on calling stations;
- intercom call to apartment stations;
- sending activation commands;
- door and gate opening even outside of the call.



*Auto-insertion on RTSP cameras is not supported by CallMe app.*

For a detailed description of all the features of the *CallMe* application, please refer to the relevant [booklet](#) which can be consulted on the website [www.urmet.com](http://www.urmet.com).




*The QR Code present on the document sent by the administrator is disposable, once scanned it will no longer be usable. It is necessary to carry out the entire service activation procedure after the scan. If the procedure is interrupted, the administrator will have to generate a new document with a new QR code to allow the activation of the service*



*Once the call forwarding function has been configured for the various apartments and Switchboard applications, it is of fundamental importance not to redo a new system configuration from scratch (even if the topology is the same): if this were the case, the procedure seen above to associate the smartphone/tablet to apartments/Switchboard applications is to be repeated.*

### 7.1.14 Search function

The function allows a quick search of the items in the system.

Press  on the main screen of the configurator to open the following screen (relating to a generic system):

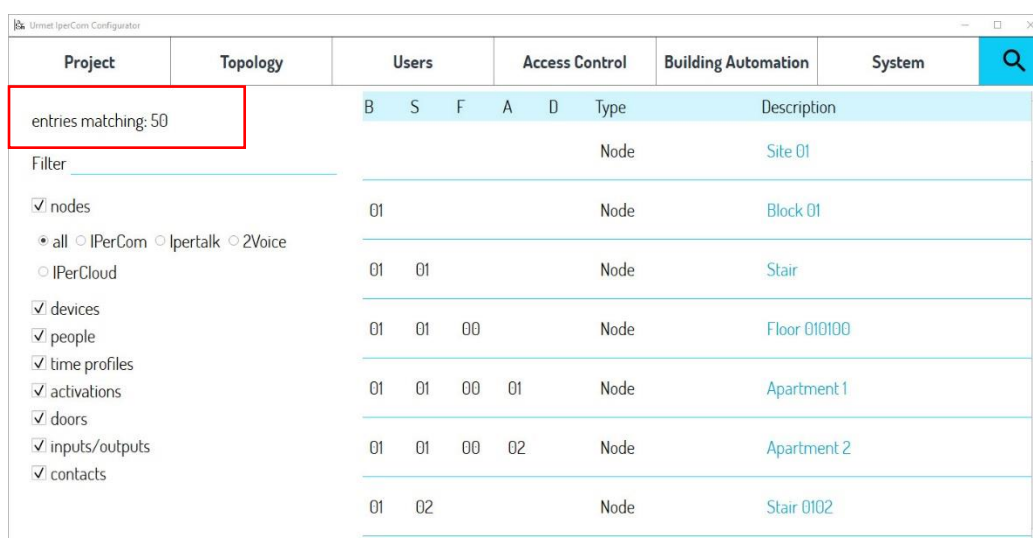


Figure 589: Search Function Screen

You can search for the following items or only one of them:

- nodes,
- devices,
- people,
- time profiles,
- activations,
- doors,
- inputs/outputs,
- contacts.

The “Nodes” field allows you to view all the topological nodes of the system and possibly filter them according to the type of node (either iPerCom nodes or iPerTalk nodes or 2Voice nodes or iPerCloud nodes).

The *Filter* field (top left of the screen above) allows you to further refine the search for the items displayed. For example, it is possible to filter by the *Name* field, a field that is filled in when creating all the elements created above (only for residents/non-residents this field corresponds to the *Surname* field). This field is displayed in the *Description* column of the screen above.

Furthermore, only for the devices, it is possible to further filter by MAC address or part of it or by device code (that is 1060/12 for the *Call Module*).

The “*Entries Matching*” field shows the number of elements found depending on the selected entries (red box).

For example, the search for IPerCloud nodes shows the IPerCloud nodes of the system with the corresponding topological code (block, staircase, floor, and apartment):

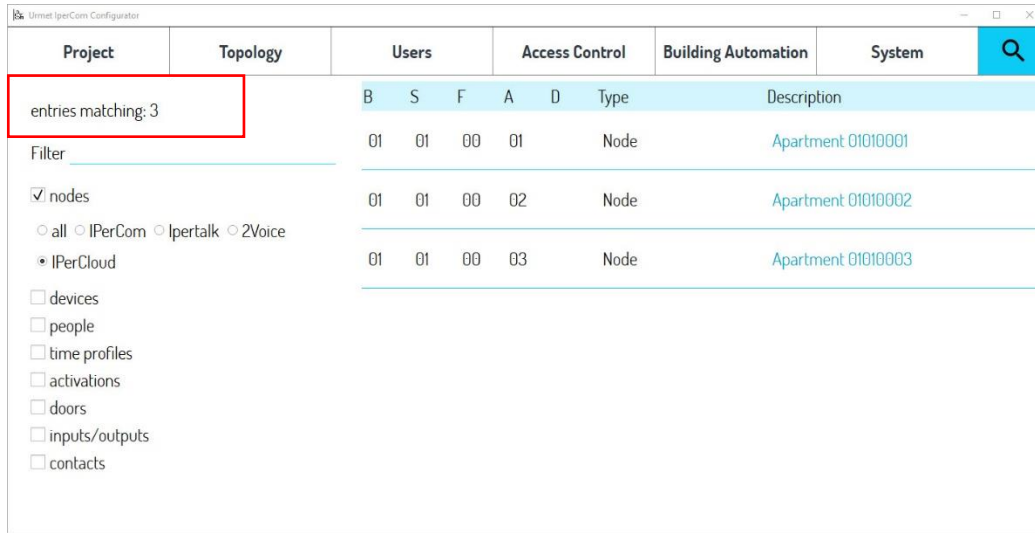


Figure 590: search for nodes

The number of entries matching the search (red box) has obviously decreased compared to the initial search where all the entries were selected.

The links in the “*Description*” column take you to the “*Settings*” page of the corresponding topological node. For example, the link “*Site 01*” takes you to the following page:

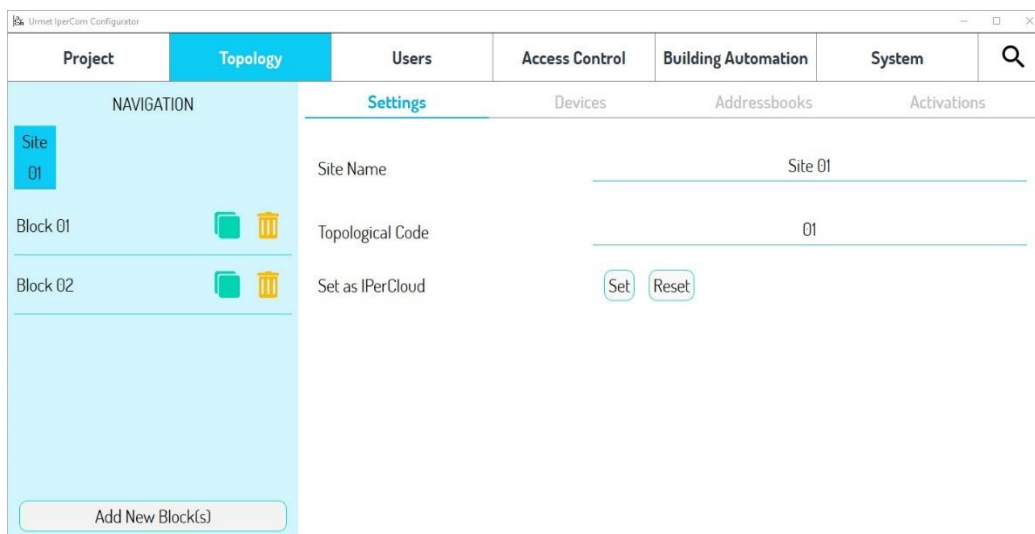
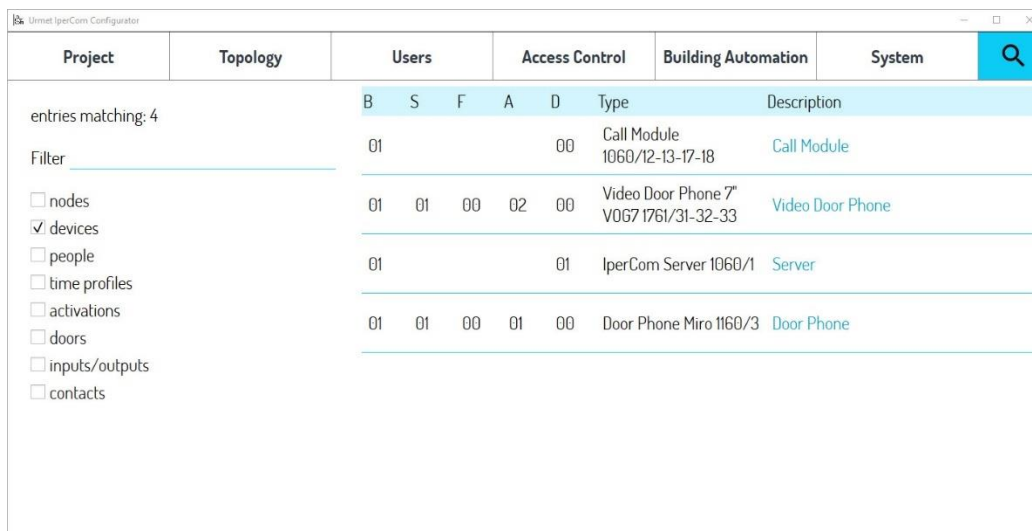


Figure 591: Setting a site node

The device search shows the various devices present in the system with the corresponding topological code (block, stair, floor, and apartment), device code (column "D") and device type:



Project	Topology	Users					Access Control	Building Automation	System	
entries matching: 4		B	S	F	A	D	Type	Description		
	Filter	01				00	Call Module 1060/12-13-17-18	<a href="#">Call Module</a>		
<input type="checkbox"/> nodes		01	01	00	02	00	Video Door Phone 7" VOG7 1761/31-32-33	<a href="#">Video Door Phone</a>		
<input checked="" type="checkbox"/> devices		01				01	IperCom Server 1060/1	<a href="#">Server</a>		
<input type="checkbox"/> people		01	01	00	01	00	Door Phone Miro 1160/3	<a href="#">Door Phone</a>		
<input type="checkbox"/> time profiles										
<input type="checkbox"/> activations										
<input type="checkbox"/> doors										
<input type="checkbox"/> inputs/outputs										
<input type="checkbox"/> contacts										

Figure 592: search for device

If the device is located on the site node, the table above only shows the device code and not its topological path.

The links in the "Description" column take you to the configuration page of the individual device.

The search by persons, time profiles, activations, doors, inputs/outputs (of *Relay Actuators*) and contacts works in the same way as described above. The corresponding links take you to the person, time profile, activation, doors, inputs/outputs (of *Relay Actuators*) and contacts editing page.

### 7.1.15 How to save the configuration

After creating the configuration, it is possible to save it through the "Project" tab of the *configurator*. The screen displayed is as follows:

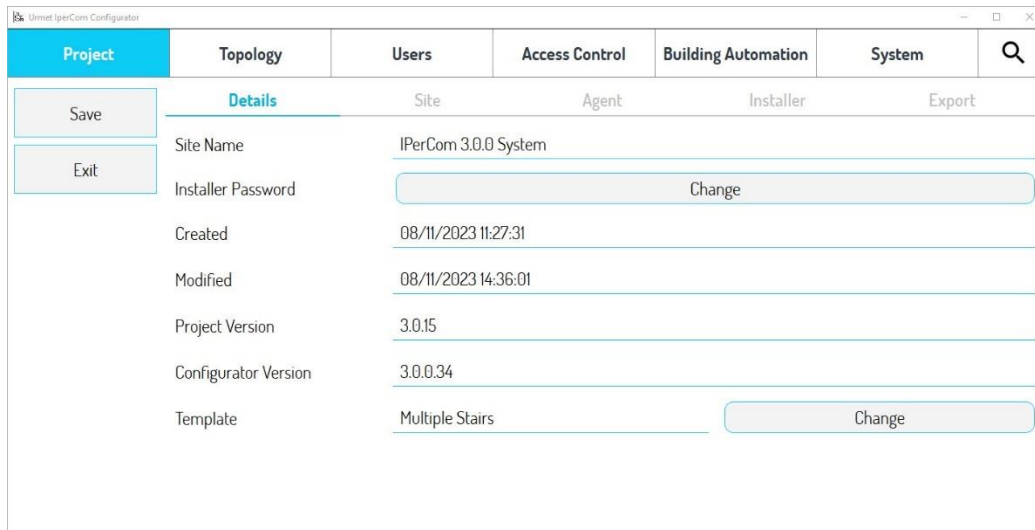


Figure 593: project sheet

Press the "Save" button to save the configuration.

The "Exit" button allows you to exit the *configurator* and return to the "Configuration" tab of *IPerCom Installer Tools*. To transfer the configuration to the system, please refer to paragraph [How to use IPerCom Installer Tools for the configuration of a system](#) where the most common use cases of the system configuration are described.



## 8 Commissioning a system through *MAX*, *VOG<sup>7</sup>* or *Basic* video door phones: the *configuration menu*

*MAX*, *VOG<sup>7</sup>* or *Basic* video door phones *configuration menu* allows commissioning an *IPerCom* system.

**From version 3.1.0 this is only possible if the two conditions below are met:**

- **there is no 1060/1 Server in the system;**
- **the system you want to configure is of the “Villa kit (one-household)” type.**

**If there is at least one 1060/1 Server in the system or the system topology is of the “Single Stair”, “Multiple Stairs” or “Multiple Blocks” type, it is necessary to use the *IPerCom Installer Tools* application to configure a system.**

As already said for *IPerCom Installer Tools*, the commissioning of a system concerns the following points:

- setting of date and time;
- setting the system parameters and topology (only for “*Villa kit (one-household)*”) by creating the so-called **system project** or simply **configuration**;
- distribution of the configuration to the devices;
- securing the system.

There are two ways to access the *configuration menu*:

1. via the start screen with QR code on devices not yet configured;
2. from the Top Page screen in case of closed start screen with QR code or for devices already configured.

## 8.1 Mode 1: Access to the configuration menu from the start screen page of non-configured MAX, VOG<sup>7</sup> or Basic video door phones

Non-configured MAX 1717/2x, MAX 1717/3x and VOG<sup>7</sup> video door phones upon starting show a screen like the one below:

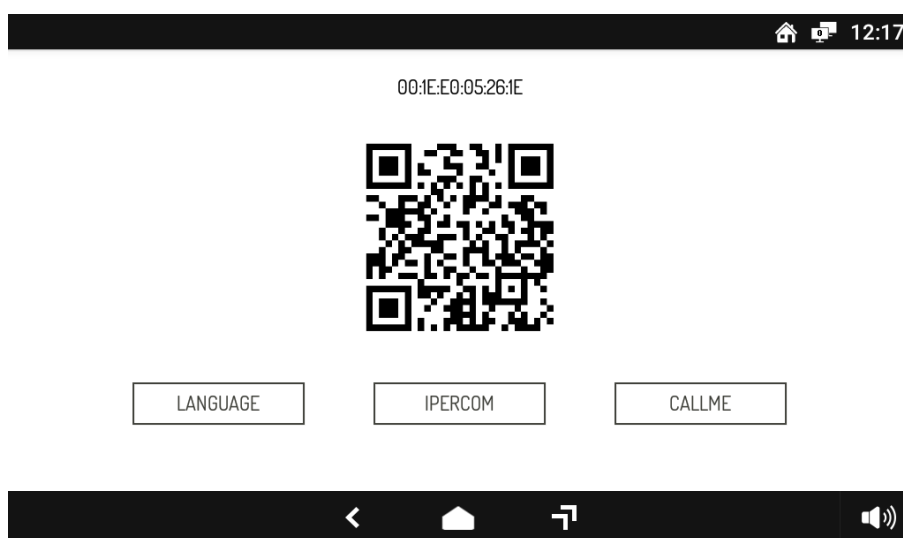


Figure 594: start screen of an unconfigured VOG<sup>7</sup> and MAX 1717/3x video door phone

In addition to the “IPerCom” button for configuring the video door phone in an IPerCom system, there is also the “CallMe” button to configure the video door phone in “CallMe” mode (for further details see [APPENDIX X: CallMe operating mode for VOG7, MAX 1717/3x and 1717/2x video door phones](#)).

The “*LANGUAGE*” button allows you to change the video door phone language, choosing one from those shown in the relevant list:

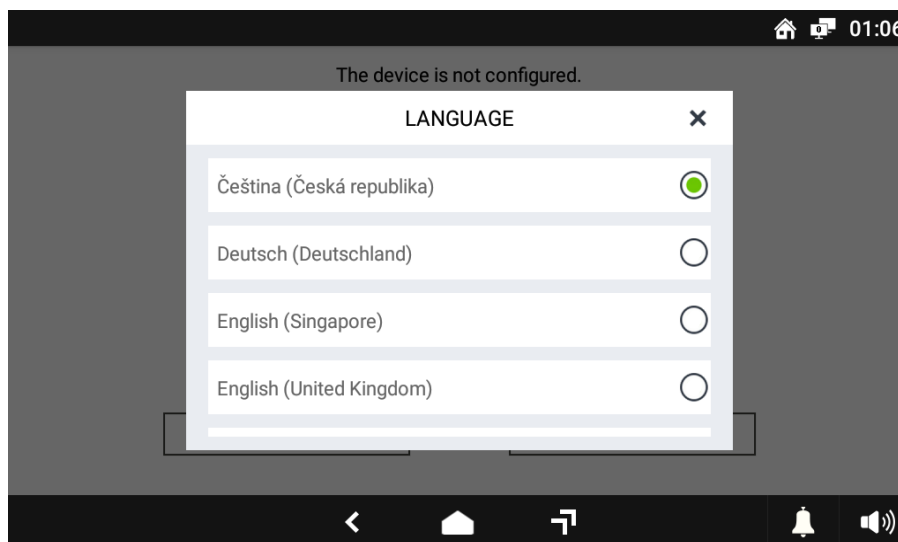


Figure 595: selection of the device language

The language thus chosen is immediately applied to the video door phone.

The “*IPerCom*” button allows (after confirmation in the relevant dialog box) to set the video door phone in IPerCom mode, that is in normal use of the video door phone in an IPerCom system, as shown below:

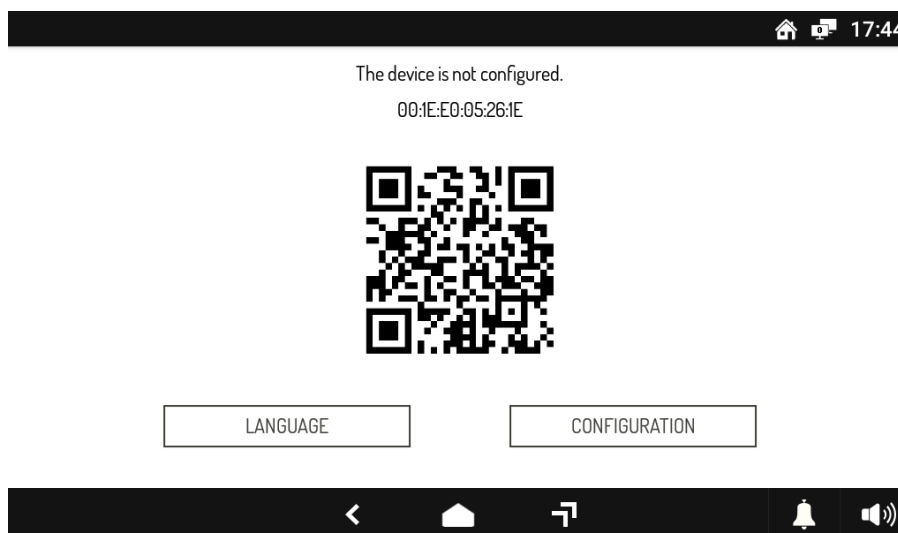


Figure 596: video door phone in IPerCom mode

MAX 1717/4x and Basic video door phones that are not configured at startup show a screen like the one below:

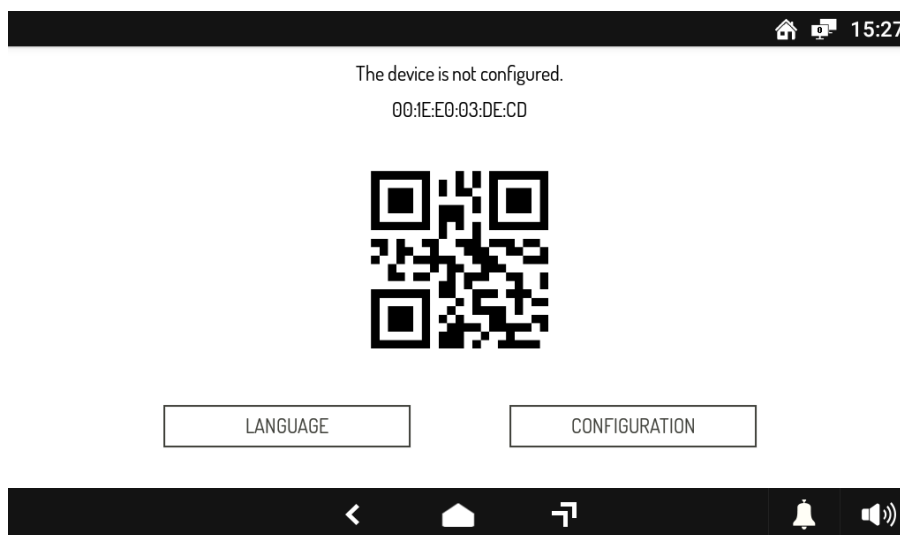


Figure 597: start screen of an unconfigured Basic and MAX 1717/4x video door phone

For these video door phones there is no “CallMe” button and they start directly in IPerCom mode.

In both cases, from this screen it is possible to access the configuration menu via the “CONFIGURATION” button.

You will be asked to change the date and time of the system, as shown below:

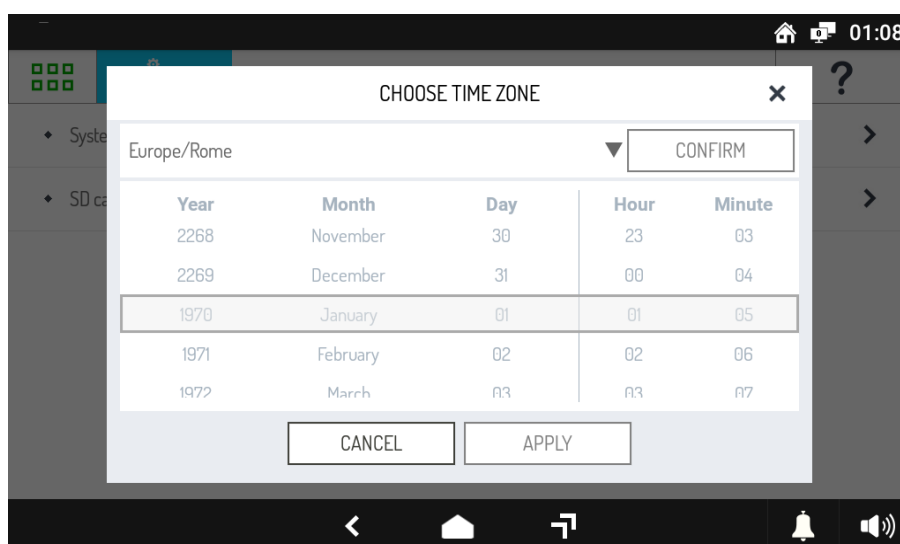


Figure 598: How to set date and time

### 8.1.1 Date and time setting

The first step of the system commissioning is to set the correct date and time.

Date and time are used to identify configuration files and determine which one is the most up-to-date during the automatic distribution between devices; therefore, as already mentioned, it is essential to set them correctly before proceeding with the following steps.

Manual setting instead is usually suggested:

- as soon as you access the *configuration menu* of a non-configured *MAX*, *VOG<sup>7</sup>* or *Basic* video door phone;
- after starting up a *MAX*, *VOG<sup>7</sup>* or *Basic* video door phone if the system has been switched off for more than 36 hours without an *IPerCom Clock Module* or without *Server 1060/1* (this requires resetting the date and time outside the *configuration menu*).

In all cases, the data and time request window are shown in the following figure:

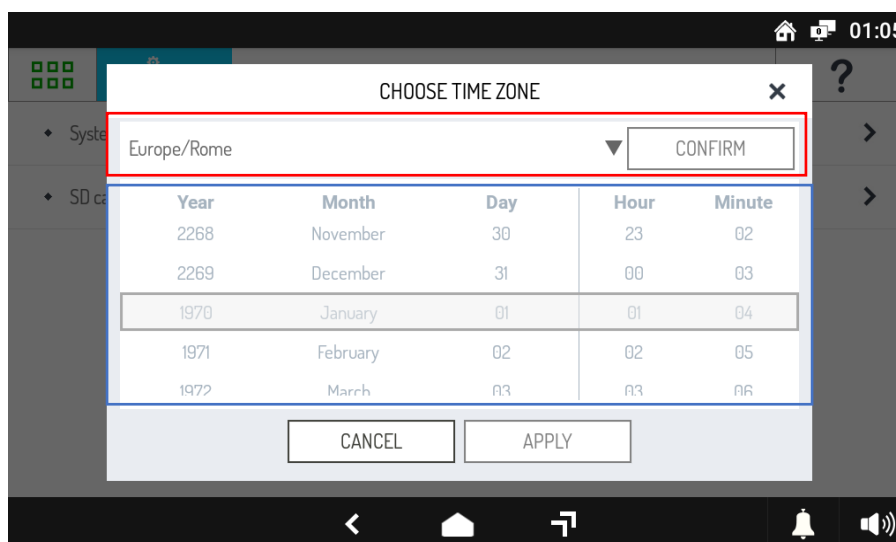


Figure 599: Date and time setting

Two sections can be seen:

- time zone (highlighted with a red border), in which you can select the desired time zone;
- date and time (highlighted with blue border), in which you can set the current date and time.

First set the time zone. Select the desired item from the convenient drop-down menu in the section highlighted with red edge, as shown in figure:

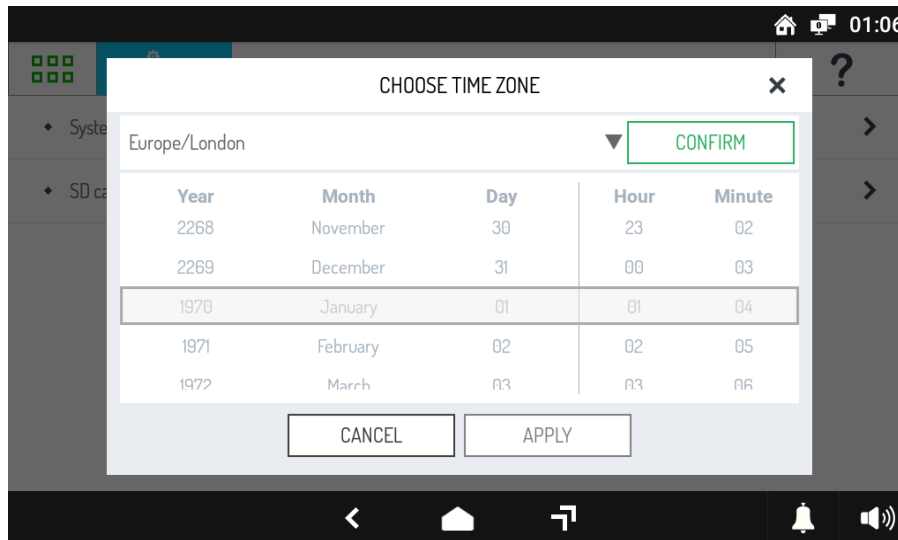


Figure 600: Choose of time zone

Press the "CONFIRM" button to confirm the selection of the time zone and enable the section highlighted with the blue border to set the date and time is enabled.

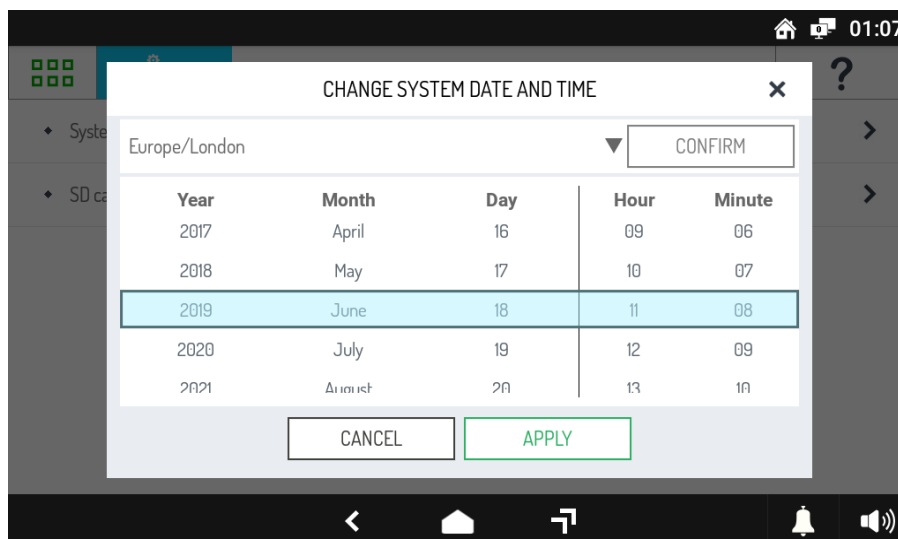


Figure 601: Choose of date and time

After selecting year, month, day, hour, and minutes, pressing the "APPLY" button, the system acquires correct date and time.

In fact, once the changes have been applied, date and time settings will be applied automatically also to all other devices of the system.

The time zone setting will be applied only to the current device. The time zone of the whole system is selected during configuration, as shown in paragraph [System parameters](#).

Therefore, in addition to setting the time zone using the *MAX*, *VOG<sup>7</sup>* or *Basic* video door phone as shown, it is also recommended to confirm your selection of the time zone using the configurator, so that the entire system is set to the desired date and time.

As shown above, the screen for editing date and time automatically opens when the configuration menu is accessed. To open it again after setting the date and time, go to "System configuration" in the configuration menu and then click on "Change system date and time".

If the generic *MAX*, *VOG<sup>7</sup>* or *Basic* video door phone has been configured, i.e. is set to the time zone in common to the whole system, it is not possible to change the time zone using the window shown in Figure (the respective section will be disabled). In this case, to make a change, you will need to change the system configuration as shown in paragraph [System parameters](#).

### 8.1.2 Configuration menu

After setting date and time the *configuration menu* will appear as shown in the following figure:

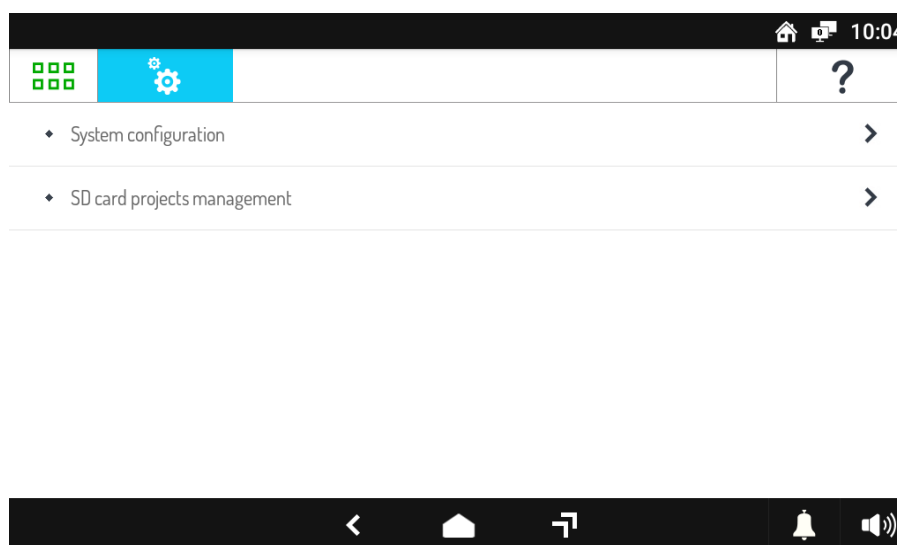


Figure 602: The configuration menu

The *configuration menu* is divided into two sub-menus: "System configuration" and "SD card projects management".

The sub-menu “*System configuration*” is structured as follows:

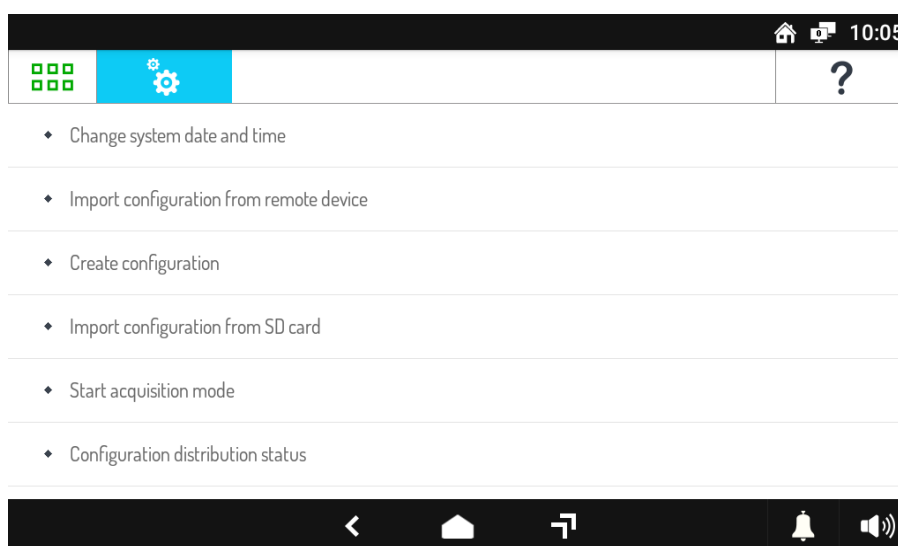


Figure 603: “*System configuration*” sub-menu (part 1)

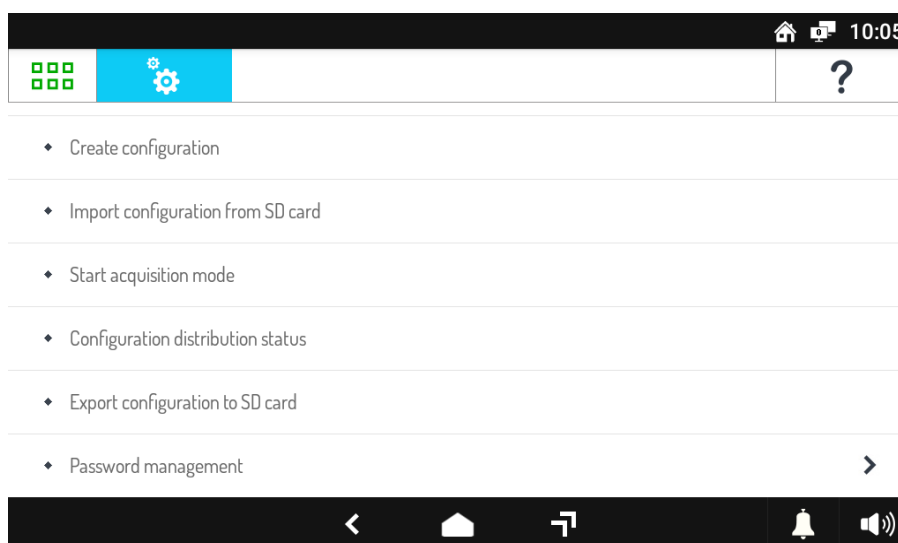


Figure 604: “*System configuration*” sub-menu (part 2)

This menu allows you to:

1. change the system date and time;
2. import the configuration from another already configured device in the network;
3. create a new system configuration or change the current one: in the latter case, the *configurator* will open;
4. import the configuration from SD card;
5. start the “*acquisition mode*”;
6. check the status of the configuration distribution to the *IPerCom* devices on the IP network;
7. export the system configuration to SD card;
8. manage the administrator and installer passwords.



The “SD card projects management” sub-menu is as follows:

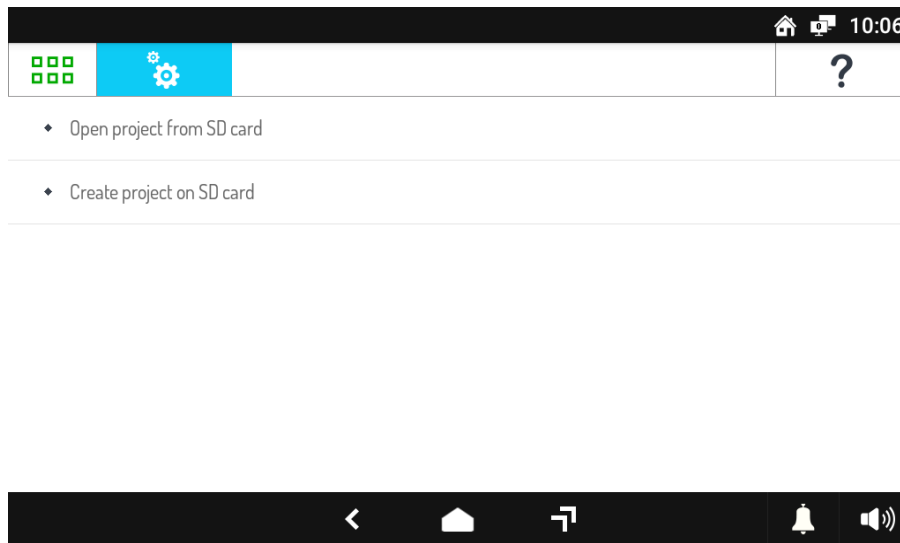


Figure 605: “SD card projects management” sub-menu

This sub-menu allows you to:

1. modify *IPerCom* configuration projects on SD card
2. create a project to be saved directly on SD card.

These operations allow you to use the *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* as a configuration editor regardless of which system is installed.

## 8.2 Access to the configurator from the MAX, VOG<sup>7</sup> or Basic video door phone

Access to the *configurator* from MAX, VOG<sup>7</sup> or Basic video door phone is carried out with the "Create configuration" item if the system is not configured or with the "Change current configuration" item if the system has already been configured. Both items are under the *configuration menu* (see paragraph [Configuration menu](#)).



Access to the configurator from the MAX, VOG<sup>7</sup> or Basic video door phone is prevented if the video door phone is present in the configuration of an IPerCom version 3.0.0 system with CallMe Manager support enabled.

If you choose to create a new configuration the following screen will be displayed:

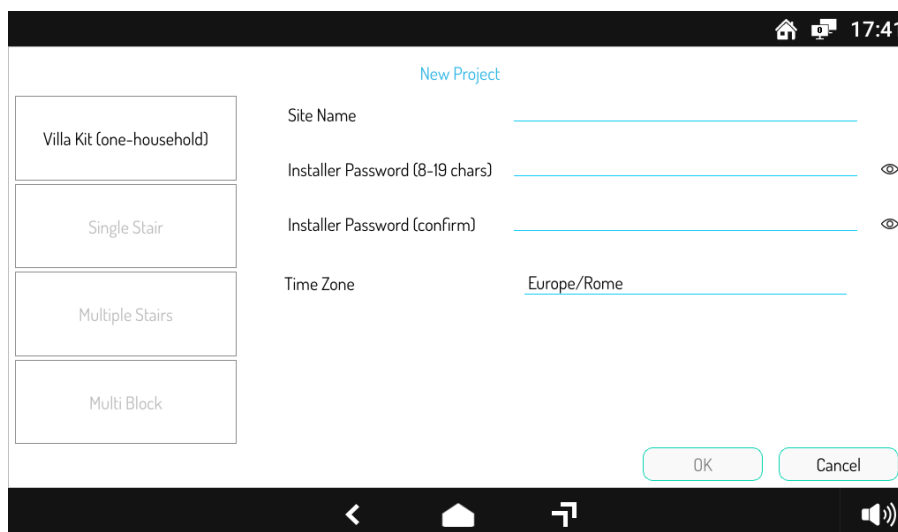


Figure 606: creating a new project through configurator

In this screen it is possible to enter the project name, the installer password and select the only "Villa Kit (one-household)" model.

If the system has already been configured and the *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* is part of it, by changing the current configuration the *configurator* will open with the configuration on the system (after entering the installer password):

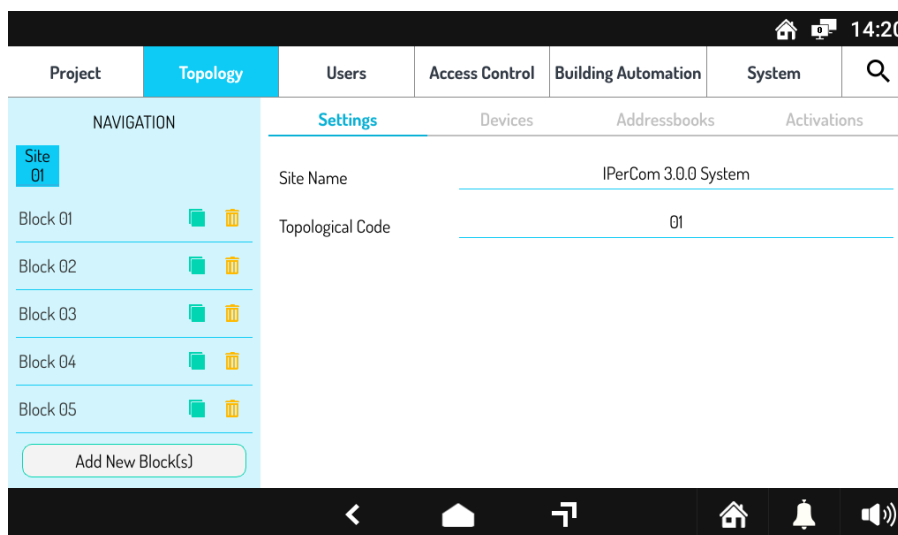


Figure 607: Opening a Multi Block configuration using the configurator

As mentioned in the paragraph "[Configuration menu](#)" the *configurator* can also be opened as a configuration editor, so not only to create or modify the current configuration of the system.

In this case you can launch the programme by opening a project from SD Card or by creating a project on SD Card.

In the first case a window will appear with a list of configuration files previously saved on SD Card.

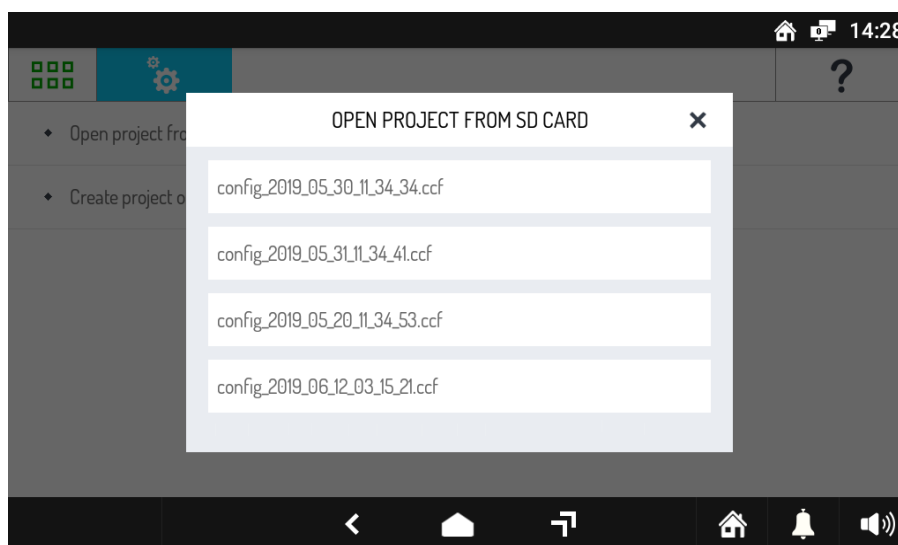


Figure 608: Opening a configuration from SD card

By selecting the desired file name, the *configurator* will open and show the contents of the chosen configuration.



If you open a file with *ccf* extension created through the *IPerCom Installer Tools* version 3.0.0 configurator and with *CallMe Manager* support enabled, it is not possible to make any changes to the configuration except through the same configurator started by *IPerCom Installer Tools*, as shown in the following message:

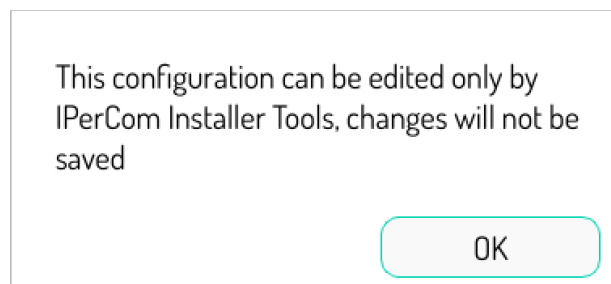


Figure 609: configuration not editable

If you want to create a new configuration on SD Card, the *configurator* will be opened on the screen for the creation of a new project, as shown in [Figure 605](#).

If the *configurator* is opened, by changing the current configuration, the “*Project*” screen will appear as follows:

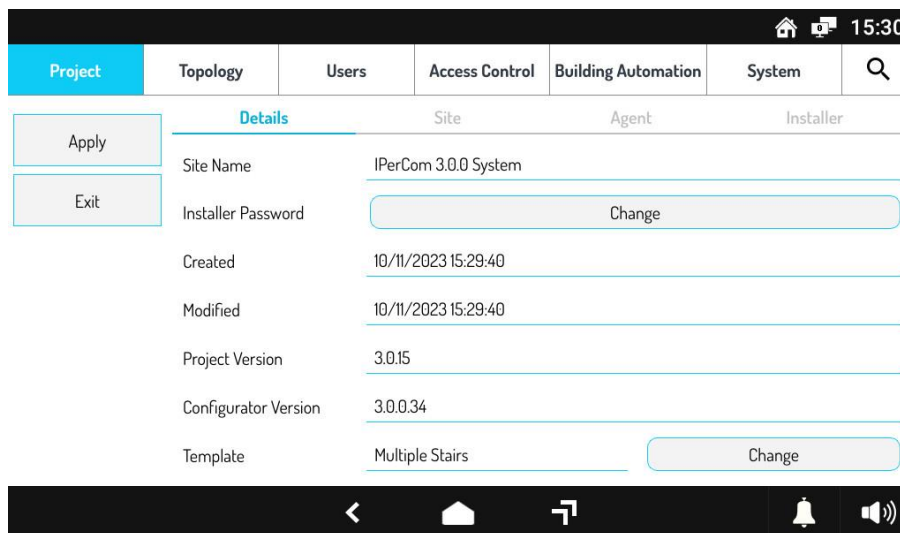


Figure 610: “Project” screen of the configurator when changing the current configuration

Two buttons are shown on the left: “*Apply*”, that allows saving and applying the modified configuration to the entire system, and “*Exit*”, that allows exiting the *configurator* yet losing the last applied changes.

If instead the *configurator* is open as configuration editor (that is from the "SD card projects management " submenu), the "Project" tab appears as follow:

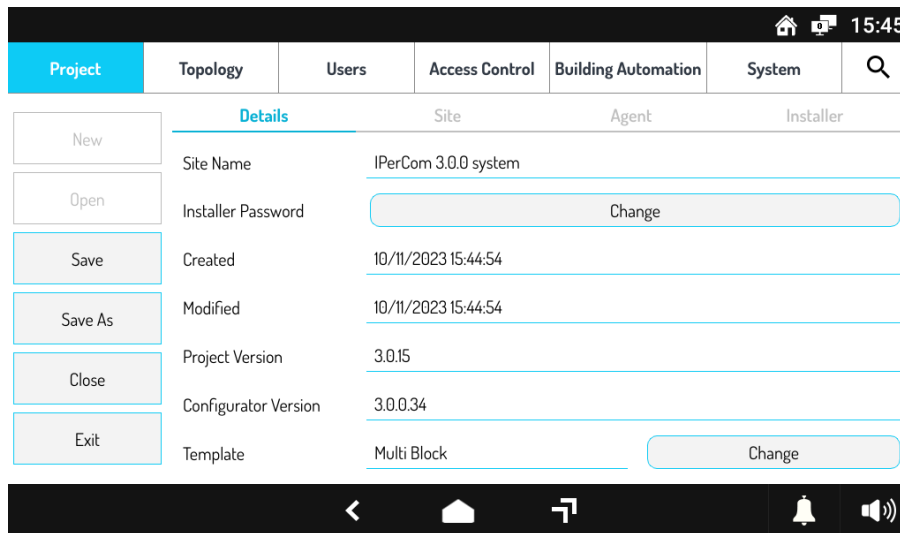


Figure 611: "Project" screen of the configurator in editor mode

In case a configuration has been suspended while using a *MAX*, *VOG<sup>7</sup>* or *Basic video door phone*, as soon as you launch the application again you will be asked whether to recover the last interrupted configuration project.

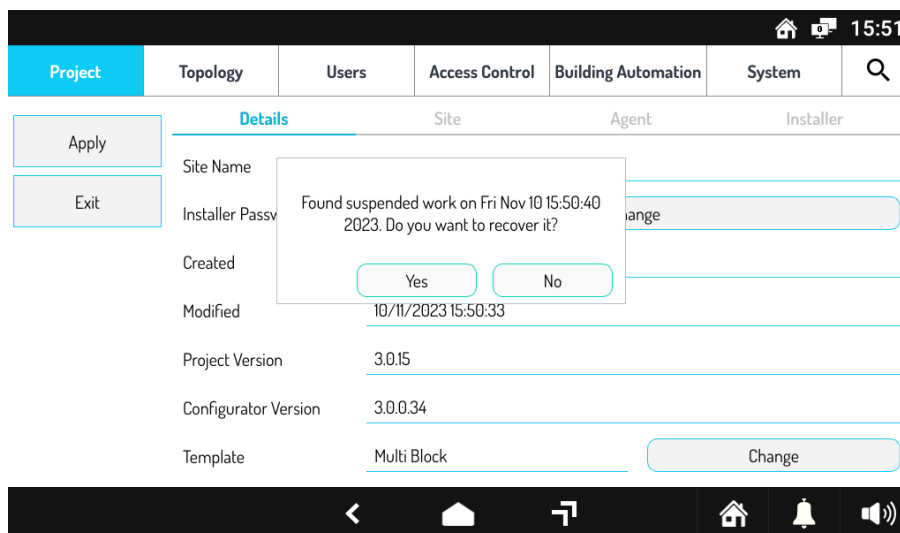


Figure 612: Recovering an unsaved configuration on MAX video door phone

### 8.2.1 The *configurator* on Android tablets

The configuration of an IPerCom system can also be made through Android tablet (minimum version required 5.0) with the *IPerCom Configurator app* downloadable from Play Store. For each officially released version of IPerCom the app, through a "*launcher*", allows you to:

- install the relevant *configurator*,
- create configuration files;
- open configuration files, possibly convert them to higher IPerCom versions and then modify them.

In the apps before version 2.0 it was possible to create and open configuration files only for the IPerCom version for which the app was released.

The new functions above are briefly described below.

After installing the *IPerCom Configurator app* on your tablet for the first time, the first time you launch it the following screen is displayed:

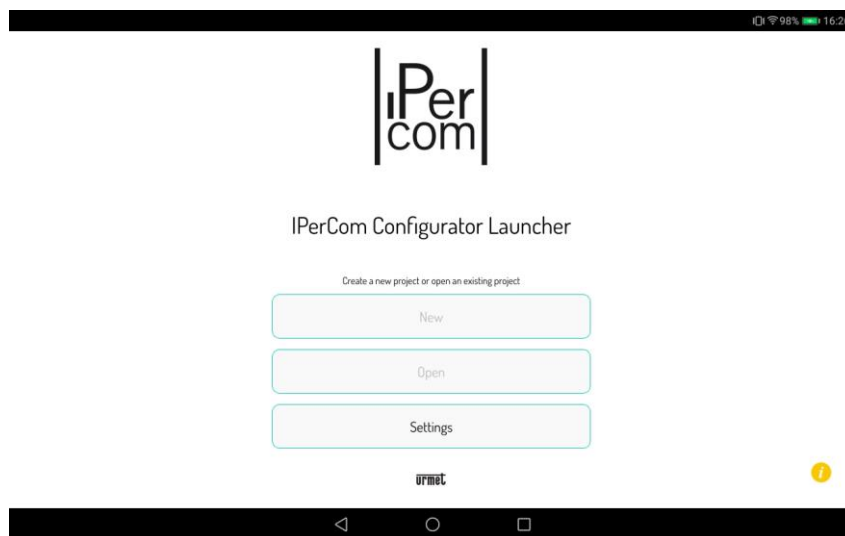


Figure 613: app startup screen

The "*New*" and "*Open*" buttons are disabled as there is no *configurator* version installed yet.

Press the "Settings" button to install the *configurator* versions related to the IPerCom version you want to work with. The screen displayed, in fact, is as follows:

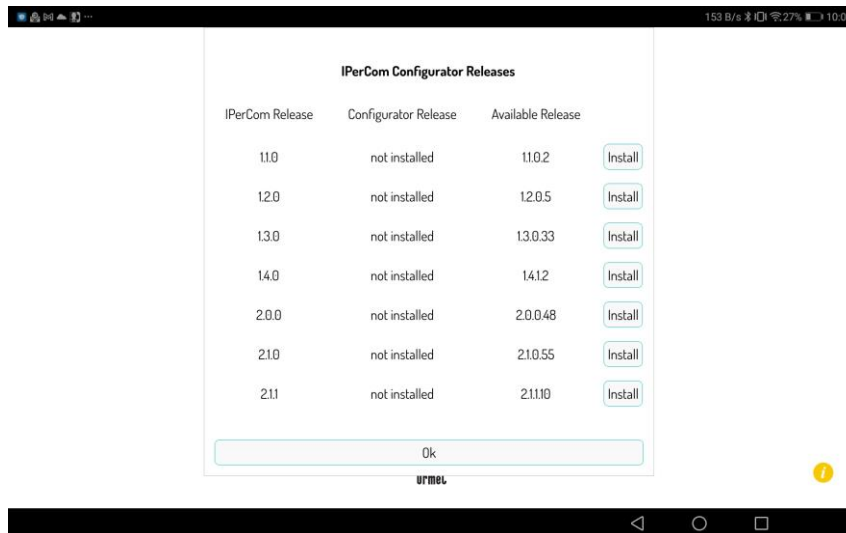


Figure 614: list of the various configurators that can be installed

For example, if you want to install the *configurator* version related to IPerCom versions 1.4 and 2.0, simply press the relevant "Install" buttons and make sure that the tablet has an Internet connection: after the download step, you will be prompted to enable the installation from the "launcher". Then the installation starts and the following screen is displayed when finished:

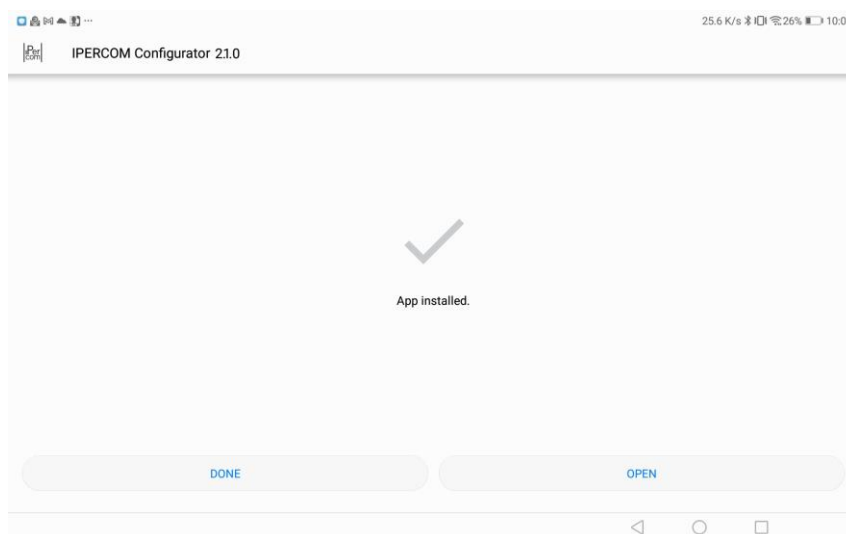


Figure 615: configurator 2.1.0 installed correctly

To finish the installation correctly, it is necessary to press the "END" button, which brings back to the initial screen of the *iPerCom Configurator* app. The "Open" button does not allow you to launch the newly installed *configurator* version as this can be done only from the *iPerCom Configurator* app (by opening a configuration file or creating a new one).

After the installation, the "Settings" button shows the installed *configurator* versions for the released iPerCom versions, as shown below in the red box:

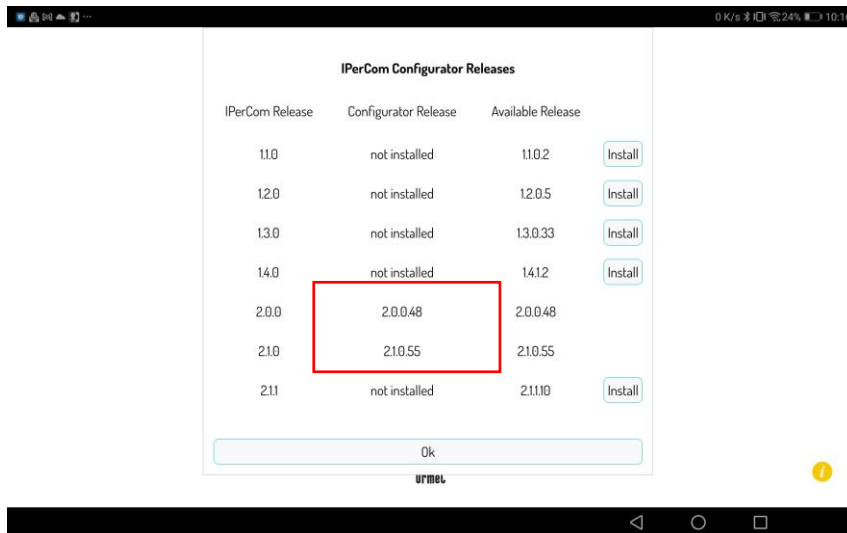


Figure 616: list of configurators installed and not installed

By pressing the "OK" button, the "New" and "Open" buttons are active:

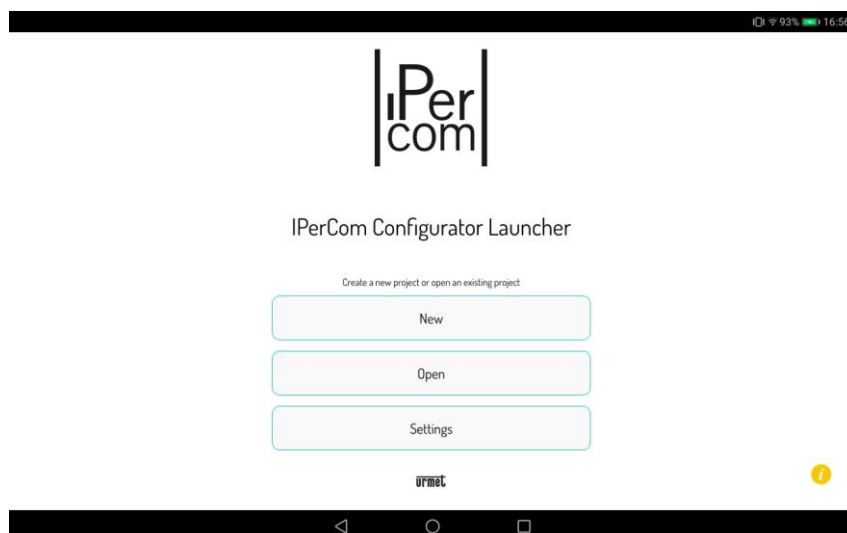


Figure 617: "New" and "Open" buttons active



The "New" button allows you to select the IPerCom version for which you want to create the new configuration (depending on the previously installed *configurator* versions). Then, in relation to the above, by pressing the "New" button, the following screen is displayed:

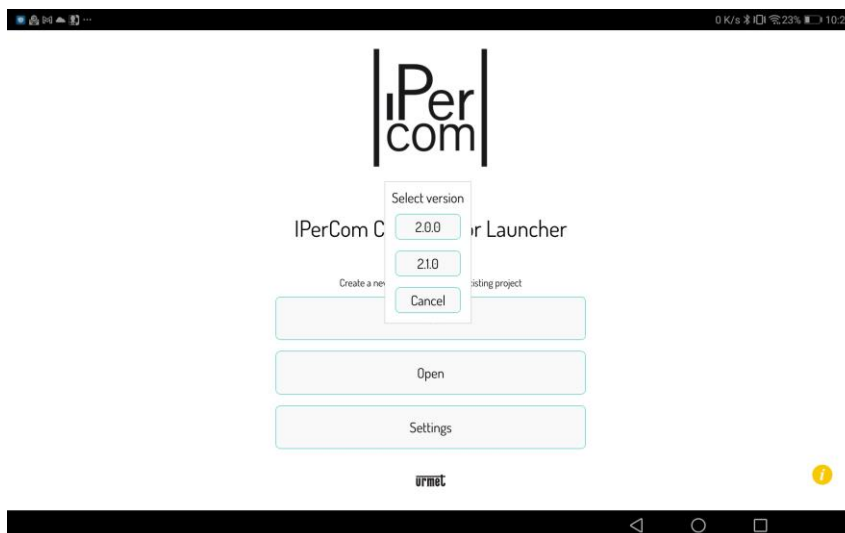


Figure 618: choice of the configurator version to start

After selecting one of the proposed versions, the previously installed *configurator* for the selected IPerCom version is launched.

For example, by pressing the button 2.1.0 this screen is displayed (like the one shown for the *MAX video door phone*):

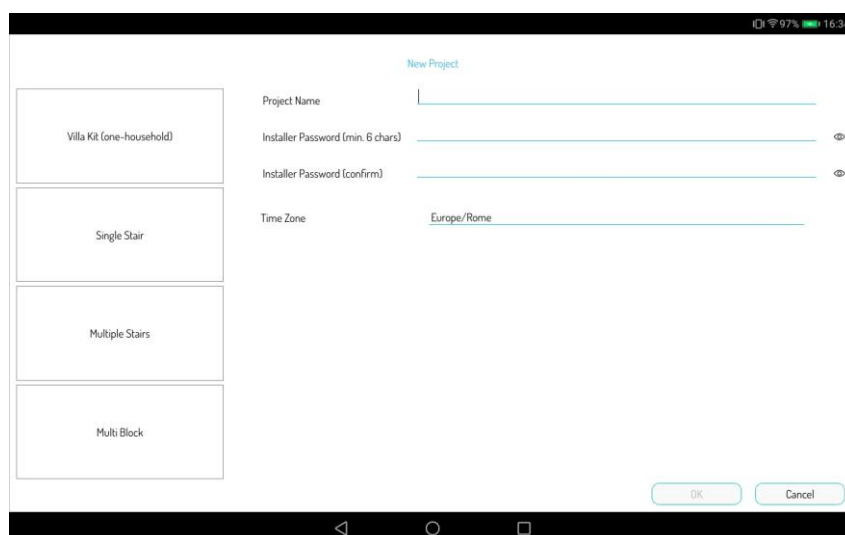


Figure 619: start configurator version 2.1.0

After entering all the data correctly, it is possible to press the "OK" button to start creating the new configuration as described in paragraph [The configurator](#).

Once the configuration is finished, the *Project* tab of the *configurator* allows you to:

- save the project (*Save* and *Save As* buttons);
- close the project (*Close* button) to create a new one (*New* button) or quit the *configurator* (*Quit* button) to return to the launcher;
- directly quit the *configurator* (*Quit* button) to return to the launcher.

The *Project* tab screen with all the options just described is shown below:

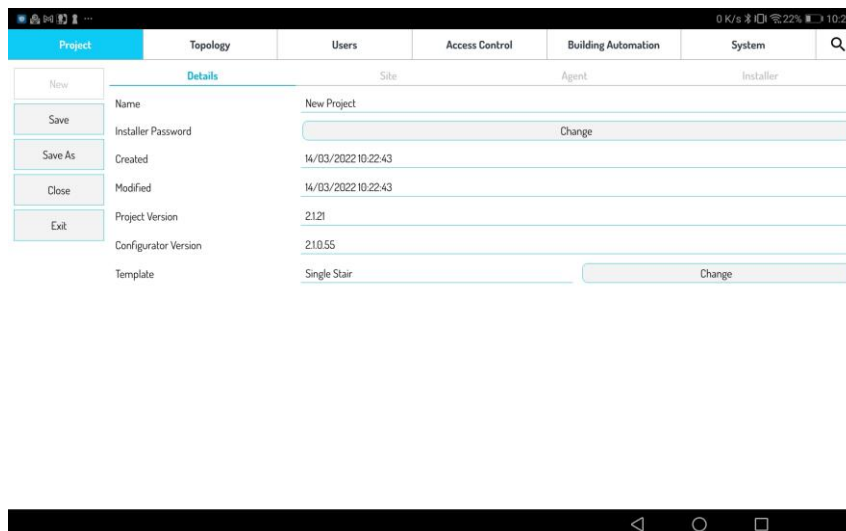


Figure 620: "Project" tab of the configurator

The "Open" button allows you to open, convert and edit previously created configuration files. Once identified and selected the file to open (with ccf extension) through the file manager of the tablet, the following screen opens:

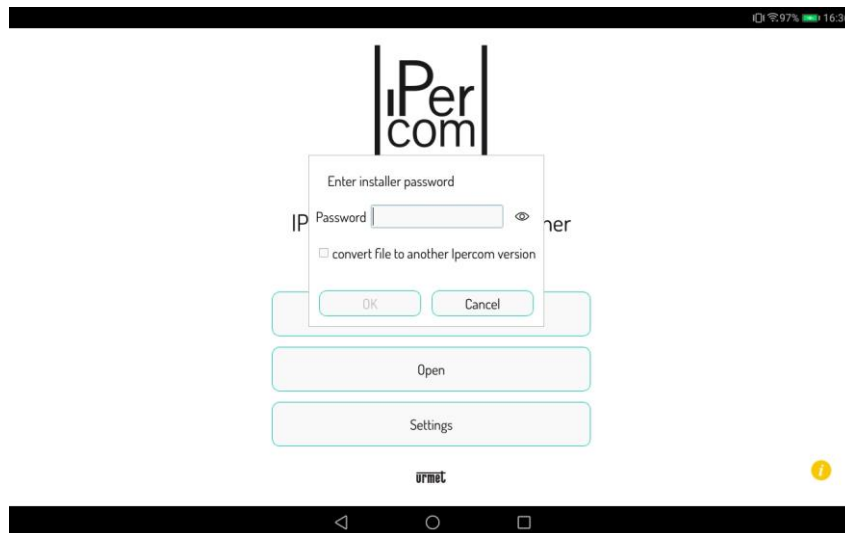


Figure 621: open a configuration file already saved

To open the configuration file without converting it to a later version of IPerCom, it is necessary to enter the installer password for the project and press the "OK" button. The *configurator* opens with the contents of the previously created configuration:

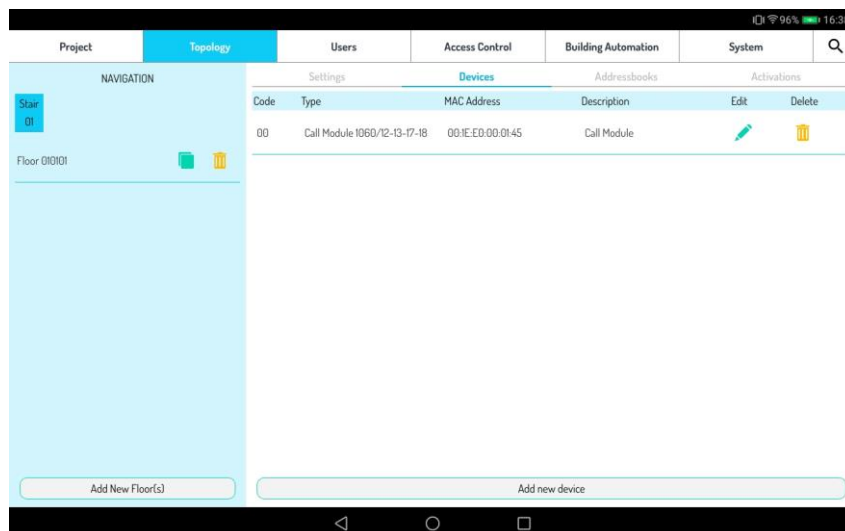


Figure 622: content of the configuration already created

If you also want to convert the file to a later IPerCom version (whose *configurator* version has been installed through the "Settings" button), it is also necessary to select the "Convert the file to another IPerCom version".

Then by pressing the "OK" button, the following screen opens:

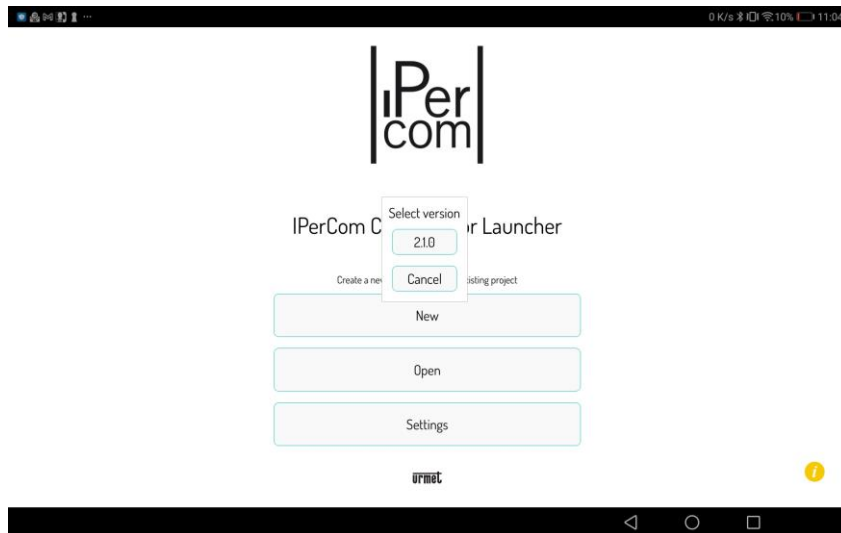


Figure 623: conversion of the configuration file to a higher version

Only the IPerCom versions higher than the one related to the file you are opening and whose *configurator* version has been installed as described above are automatically shown. Once the version has been selected, to make sure that the conversion has been successful, simply check the *Configurator Version* field in the *Project* tab:

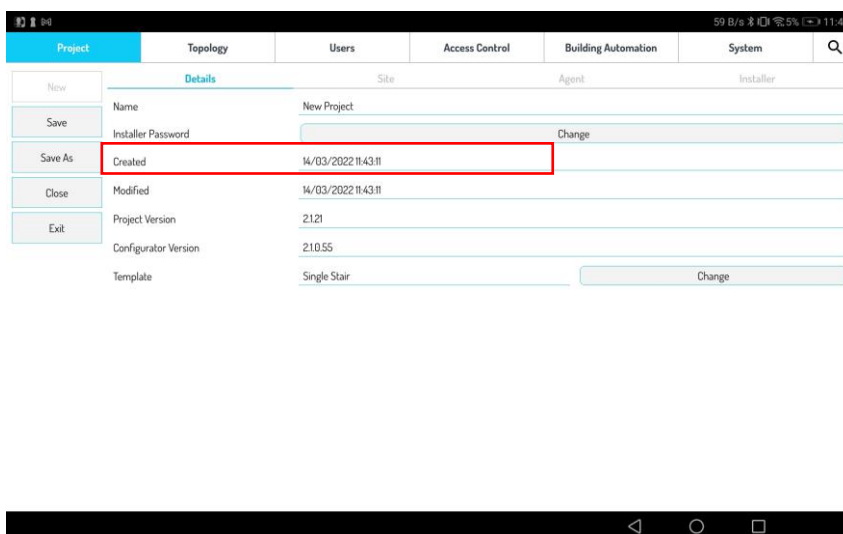


Figure 624: conversion successful


When the modifications have been completed, in the *Project* tab it is always possible to:

- save the project (*Save* and *Save As* buttons);
- close the project (*Close* button) to open another one;
- directly quit the *configurator* (*Quit* button) to return to the “*launcher*”.



*It is not possible to open configuration files related to IPerCom versions whose configurator has not been installed through the "Settings" button.*



*The  button opens a window showing the installed version of the app, the privacy policy, the terms of use of the app and the link to the Urmec website.*



*You may need to update already installed configurator versions if they are updated online. This can be checked by pressing the "Settings" button, which shows the "Update" button active on the configurator versions to be updated. It is highly recommended to always update the various configurator versions to the latest version.*

### 8.3 System first configuration

This section describes the steps to be followed when configuring an *IPerCom* system for the first time referring both to the *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* and to the *IPerCom Configurator* app.

When doing this, all devices must have the factory settings; otherwise, it is necessary to reset to the factory settings (see chapter [Restoring the factory settings](#)).

After setting the date and time, the next step is to create the configuration, which includes the following points:

1. definition of the system topology,
2. addition of the devices to the configuration,
3. creation of the directories,
4. creation of activations,
5. creation of residents and non-residents,
6. setting of the access control,
7. configuration of the system parameters and call forwarding.

Once the configuration is finished, it is necessary to distribute it to the various devices of the system, export it to SD card and as last step to secure the system.



*We recommend to pay particular attention to the system date and time setting phase, which must be carried out before any other step.*



*We recommend to distribute the configuration to the system only after waiting at least 10 minutes from the connection of the last device.*



*The IPerCom Configurator app can create the configuration but not to distribute it to the other devices in the system or secure the system.*

### 8.3.1 Creation of a new configuration: definition of the system topology

To create the first configuration on a *MAX*, *VOG7* or *Basic video door phone* it is necessary to access the *configuration menu*, then to “*System configuration*” and choose “*Create configuration*”, as shown in the figure:

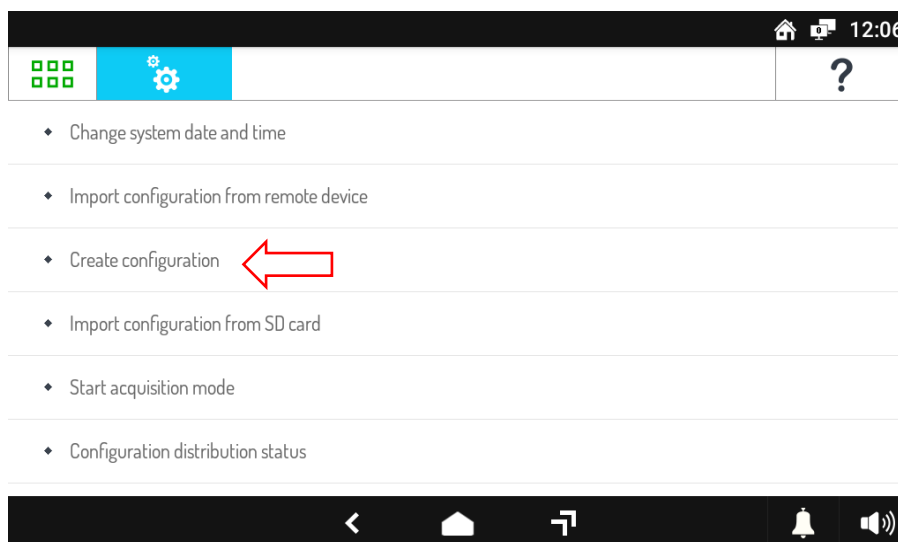


Figure 625: Creation of the first system project on MAX video door phone

Confirming the request will open the screen for creating a new *project*.

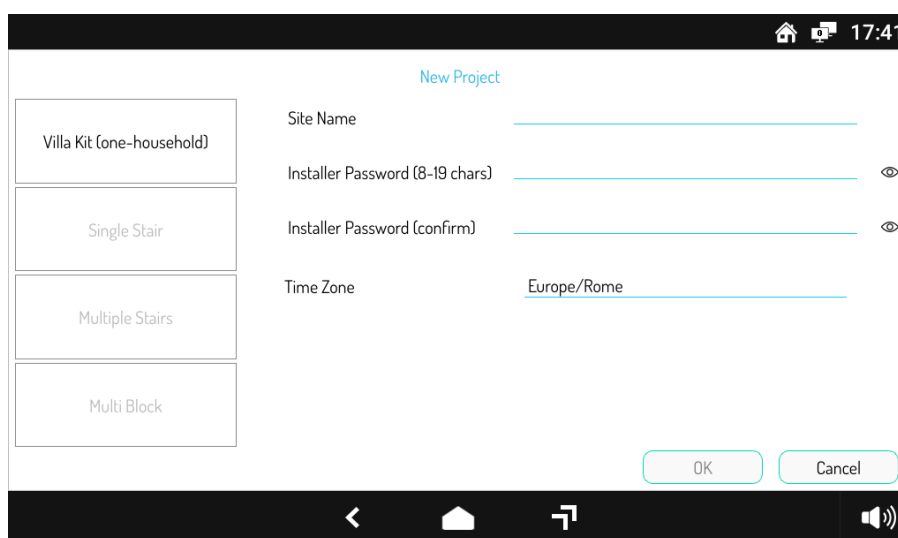


Figure 626: new project

You get to the same screen if you want to use an Android tablet and then the *IPerCom Configurator app* to *create a new project*. Once the app starts, it is necessary to press the *New* button and then select the IPerCom version for which you want to create the new configuration. The screen displayed is as follows:

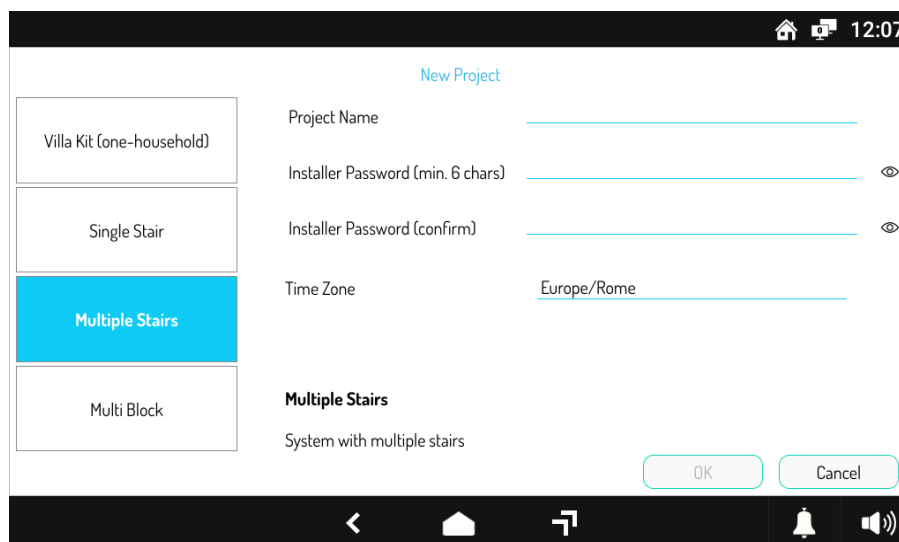


Figure 627: Selecting the plant model when creating a project

As you can see, the screen to define the system topology (both for the *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* and the *IPerCom Configurator app*) is like what described in paragraph [The configurator](#), as well as the other possible steps for the configuration of a system, i.e.:

1. definition of the topological structure,
2. addition of the devices to the configuration,
3. creation of the directories,
4. creation of activations,
5. creation of residents and non-residents,
6. setting of the access control,
7. configuration of the system parameters and call forwarding.



To add the various devices of the system from *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* in the configuration, it is advisable to follow one of the 4 methods described in the following paragraph, being understood that also from *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* the same rules described for *IPerCom Installer Tools* are valid, i.e.:

- each device is associated with a topological node through the *Add Device* button;
- the *Call Module*, the *Entry panel 1060/21-33-34-71-74-75*, the *Modular Entry Panel* with 1060/48 and the *Switchboard* cannot be added to an apartment node;
- the *IPerCom-2Voice Gateway* and the *Lift Interface* can only be added to the stair node;
- the *Floor Entry panel* can be added only to the apartment node;
- to access the list of devices, present in each topological node, you need to select the “*Topology*” tab: by using the navigation module you must select the desired position, then go to the context module of the “*Devices*” tab, where you will find a table showing all the devices installed in the selected node.

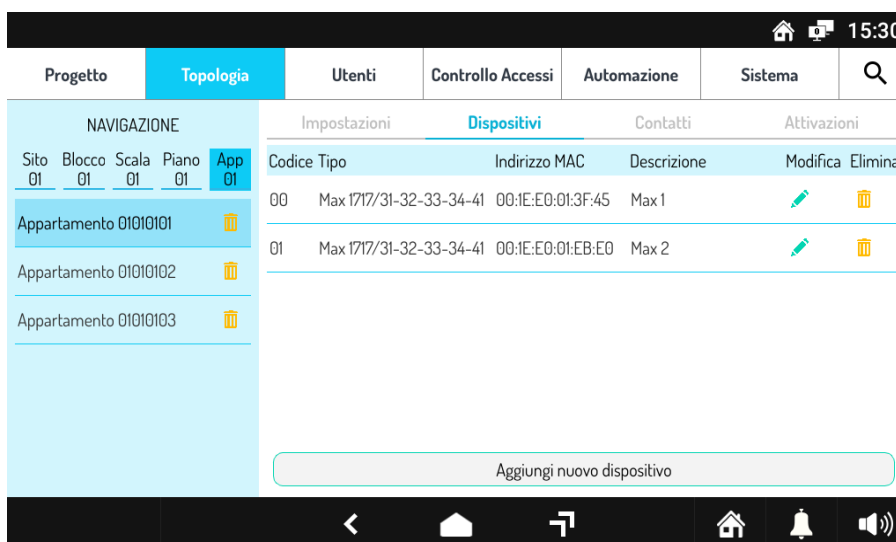


Figure 628: list of devices attested in a topological node

### 8.3.2 Adding devices to the system using the *MAX video door phone* and/or the Android tablet app

To add all the devices of the system to the configuration, it is advisable to follow one of the 4 procedures below. In this way, you can speed up the configuration operations by exploiting some features of the *MAX*, *VOG<sup>7</sup>* or *Basic* video door phones and the Android tablet app.

The examples below refer to the *MAX 1717/3x-4x* video door phone, but what is stated is valid for all other *MAX 1717/2x*, *VOG<sup>7</sup>* or *Basic* video door phones.

#### 8.3.2.1 Mode 1: installer uses only *MAX video door phones* for the system configuration

**Application case:** The devices are already installed on the system, but not yet configured

**Pros:** Only *MAX video door phones* are required; there is no need of an Android PC or tablet; you do not need to know the physical MAC addresses of your *MAX video door phones*

**Cons:** Requires to enter the installer password and open the *configurator* from one device at a time; requires knowledge of the MAC addresses of all other devices in the system.

In this case, it is assumed that the system is already installed. The installer uses one of the *MAX video door phones* and starts creating the configuration project as explained below.

#### 1. Adding the first *MAX video door phone* to the configuration

For example, if you create a *Single Stair* configuration on a system *MAX video door phone*, the first step is to add such device to the relevant topological node. Then it is necessary to go to the "*Devices*" tab and click on the "*Add new device*" button.

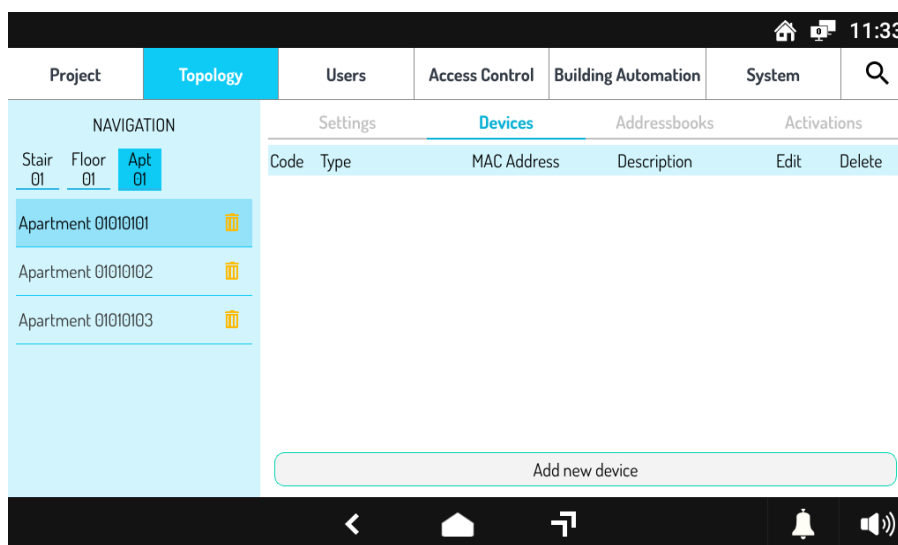


Figure 629: Adding a new device

The following selection screen will be displayed, allowing to choose the type of device to add.

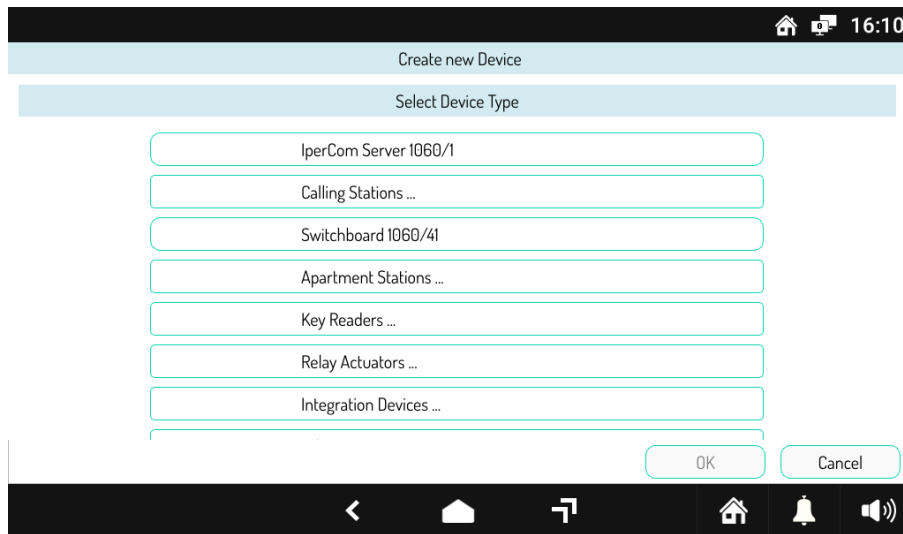


Figure 630: Selecting the type of device to add

To add a MAX video door phone, select "Video door phone 7" MAX 1717/31-32-33-34-41". The following screen page will then open:

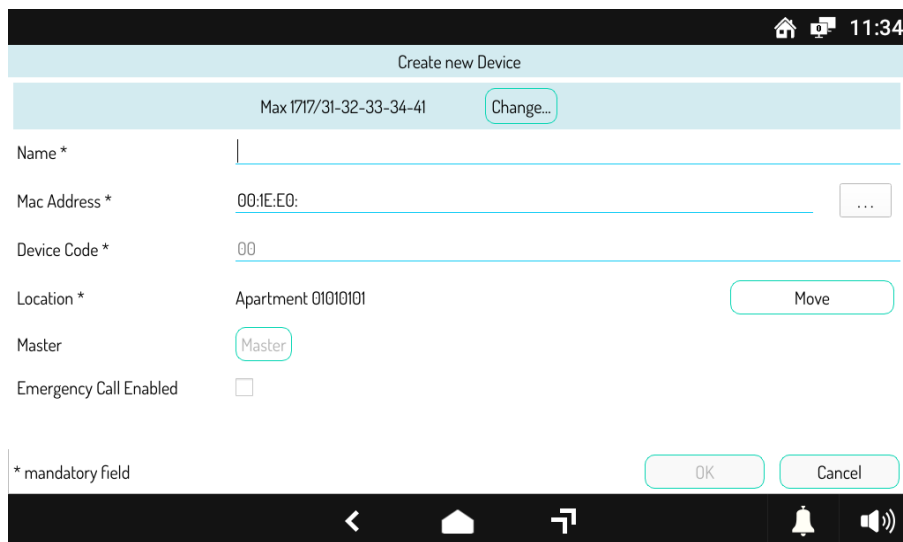


Figure 631: Entering device parameters

The "Name", "MAC Address", "Device Code", and "Location" fields are present on the setting page of all devices.

In this case, simply fill in the fields "Name" and "MAC Address" to add the device: the field "Name" is arbitrary and chosen by the installer, the field "MAC Address" instead is well defined and associated with the device in use. To enter the latter parameter, in this case you do not need to know the single digits, as there is a quick selection button "..." available that allows to set it up immediately.

If you press in fact this button, a dialog box will appear:

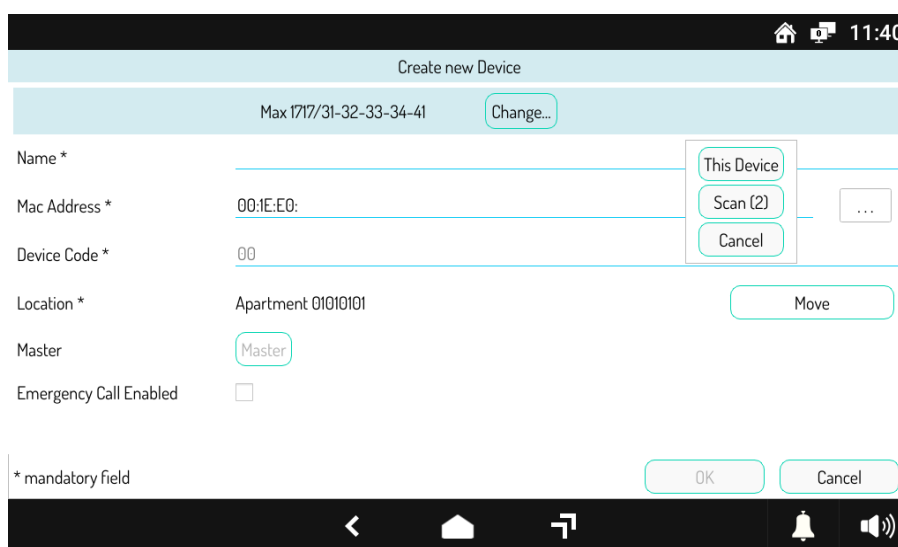


Figure 632: Selecting the MAC Address of the current device

Pressing the "This Device" button to automatically set the MAC address of the MAX video door phone. Press "Scan (.../...)" to display a list of devices (with respective MAC address) which are present on the system but which have not yet been added to the configuration, as shown in the next step.

Press the first button to add the MAC address of the current device:

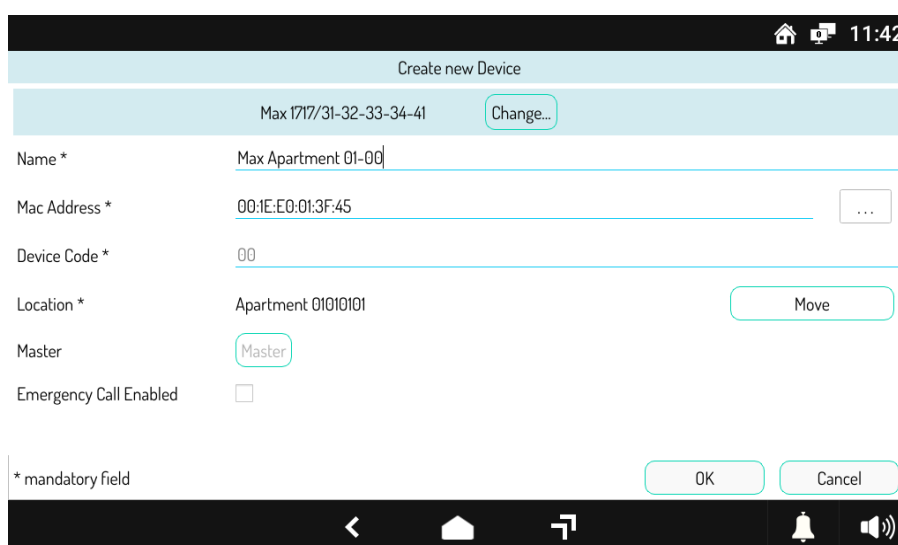


Figure 633: Automatic setting of the current device MAC Address

By pressing "OK", the device is added to the device list of the configuration.

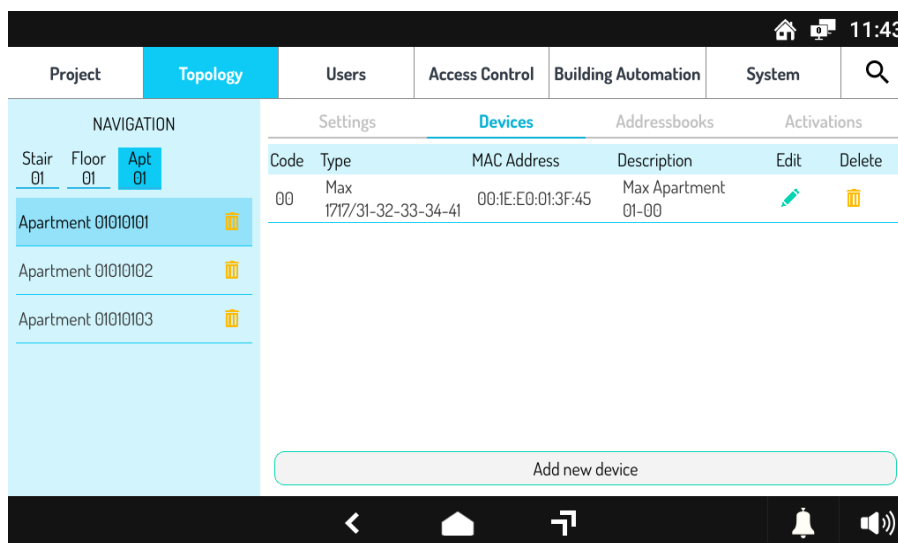


Figure 634: List of devices for the selected apartment

## 2. Adding other device types to the configuration

When the first *MAX video door phone* has been added, a similar procedure is to be followed to add all other devices installed in the system.

For example, if you want to add a *Call Module* to the configuration in the specific topological node where it is installed, by following the procedure previously indicated for the *MAX video door phone* you will see a screen like the following one:

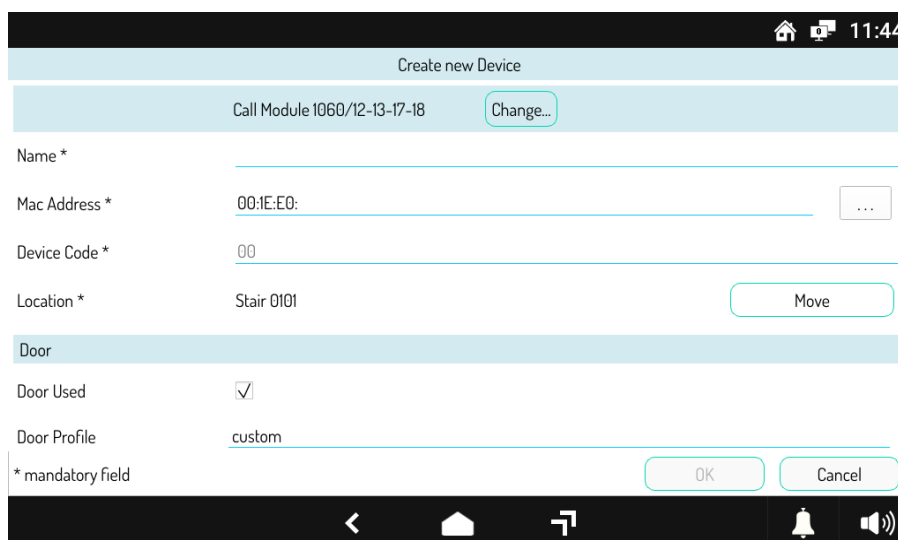
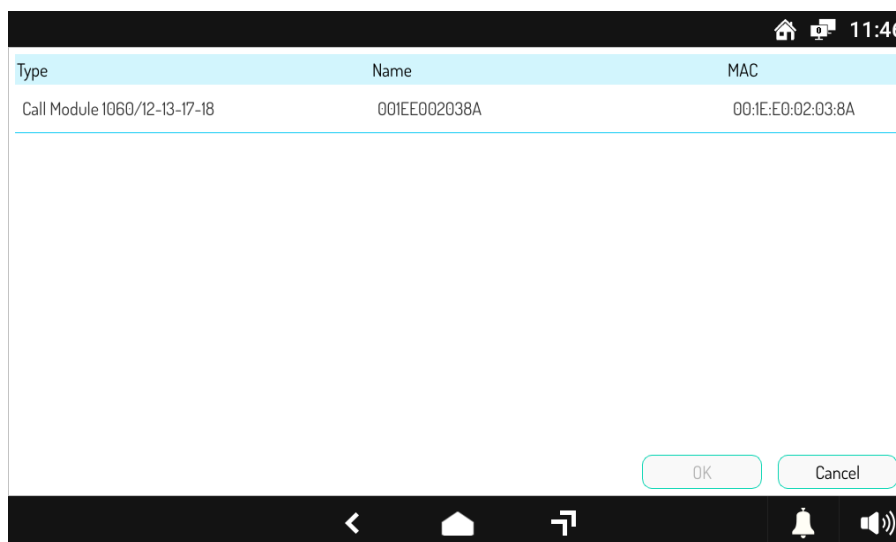


Figure 635: Adding a Call Module to a block

This time you need to know the MAC address of the device to be added to fill in the relevant field; there are therefore two possible modes to fill it in:

- manually entering the MAC address digits, or
- pressing the "... " button, then the "Scan" button, in order to obtain a list with the devices installed in the system (but not yet added to the configuration), and then select the devices from this list, as shown in the following figure:



Type	Name	MAC
Call Module 1060/12-13-17-18	001EE002038A	00:1E:EO:02:03:8A

Figure 636: List of "Call Modules" detected in the system

### 3. Exit from the current configuration and distribution of the configuration

Once all the needed devices have been added to the configuration, go to the "Project" tab and press the "Apply" button to distribute the configuration (refer to paragraph [Configuration distribution](#))

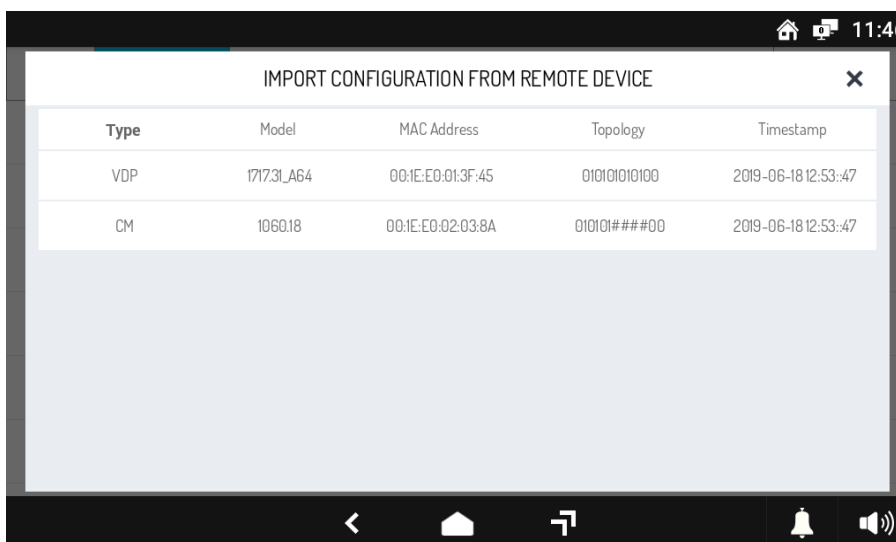
At the end of the configuration distribution the *MAX video door phone* and the other monitors installed in the system are correctly updated to the current configuration.

### 4. Adding the remaining *MAX video door phones* to the configuration

The only monitors not yet configured are any other *MAX video door phones* present in the system.

To apply the configuration to them as well, you will need to go from *MAX video door phone* to *MAX video door phone* and follow the instructions below.

So, to proceed with a second *MAX video door phone*, you will need to access the *configuration menu*, then go to *"System configuration"* and *"Import configuration from remote device"*: a screen like the following one will appear.



Type	Model	MAC Address	Topology	Timestamp
VDP	17173L_A64	00:1E:E0:01:3F:45	0101010100	2019-06-18 12:53:47
CM	106018	00:1E:E0:02:03:8A	010101###00	2019-06-18 12:53:47

Figure 637: Importing the configuration from a remote device

A list of devices from which to import the configuration is displayed: by pressing on the configured *MAX video door phone* and confirming the request, the configuration will be imported into the system.

Once *IPerCom Configurator* is opened on the new device and the installer password is entered, it is possible to see all the parameters of the previously set up configuration and add the current *MAX video door phone* to the same configuration: the steps are the same as described previously for the first *MAX video door phone*.

Also in this case, once the addition is complete, you need to apply the configuration and distribute it, so that the first *MAX video door phone* receives the updated version.

To import the configuration into all other *MAX video door phones*, you follow the same procedure.



**Case of an already blocked system:** if the system has already been blocked (see paragraph [Securing the system](#)), importing the configuration from an already configured device will require entering the administrator password.



**Case of system configured with IP static:** The configuration imported from remote device cannot be used if the system is configured for operation with static IP or if manual setting of the network was chosen in system parameters (see paragraph [System parameters](#)).

8.3.2.2 *Mode 1.1: The installer creates the configuration in the laboratory on the MAX video door phone/PC/Android tablet and adds the devices to the configuration via the MAX video door phone*

**Application case:** The devices are already installed on the plant, but not yet configured. There is a basic configuration on SD Card in which the topology has been defined but the devices have not been added yet

**Pro:** It is not necessary to know the physical MAC addresses of the *MAX video door phones* and the topology can be easily created in the laboratory.

**Cons:** The disadvantages are the same as in MODE 1

This is a variant of MODE 1.

1. Configuration creation (topology only) in the laboratory and export to SD card

Instead of creating the configuration on-site on the first *MAX video door phone* of the installed system, the installer creates it in the laboratory on the *MAX video door phone/PC/Android tablet*, by setting only the system topology, and then exports it to an SD card.

2. Configuration import from SD card and subsequent distribution

Once in the field, with the system installed, the installer goes to the first *MAX video door phone* and imports the configuration from the SD card.

To import the SD card, it is necessary to access the *configuration menu*, then press "*System configuration*" and "*Import configuration from SD card*". A list of projects saved on SD card will be shown from which to select the desired one.

For further information on how to distribute the configuration, refer to paragraph [Configuration distribution](#).

3. Following are all the steps indicated in MODE 1

We summarise the steps that need to be taken: add the current *MAX video door phone* to the configuration, then add all devices other than the *MAX video door phones*, and then distribute the configuration. Finally, for all the other *MAX video door phones* in the system, proceed as described above, i.e. import the configuration, add the current *MAX video door phone* to the configuration and distribute the configuration.



### 8.3.2.3 *Mode 2: The installer creates the configuration in the laboratory on the MAX video door phone/PC/Android tablet but adds the devices via Android tablet*

**Application case:** The devices are already installed on the plant, but not yet configured. There is a basic configuration on SD Card in which the topology has been defined but the devices have not been added yet. You have an Android tablet with the *IPerCom Configurator* app installed on it.

**Pros:** It is possible to create the topology in the laboratory through *MAX video door phone/Android tablet* and add devices (of any type) in the field by simply scanning the QR Code.

**Cons:** An Android tablet is required

The following mode takes advantage of the *IPerCom devices* feature to show a QR Code that contains its MAC address: in the case of *MAX video door phones* the QR Code is displayed when not configured, whereas in other devices it is shown frontally on a label.

1. Configuration creation (topology only) in the laboratory and saving on Android tablet

The installer creates the configuration in the laboratory on the *MAX video door phone/PC/Android tablet* by setting only the system topology. If you have used a *MAX video door phone* or a PC, the configuration must then be copied to an Android tablet (e.g. by saving it on an SD card).

2. Adding devices to the configuration by scanning the QR Code

The installer goes to the area where the system is already installed and brings with him/her an Android tablet containing the configuration.

Once the project saved on the tablet has been opened, the installer moves to each device of the system and adds it to the configuration as described below.

First, in the Topology tab it is necessary to go to the topological node of the device to be added, then in the context module you must select the "*Devices*" tab and press on "*Add new device*".

At this point, as already described, you select the type of device to add and fill in the fields shown on the screen, as usual: the only difference is the possibility, for Android tablets, to enter the MAC address by scanning the *QR Code* of the device, by pressing the "*QR Code*" button.

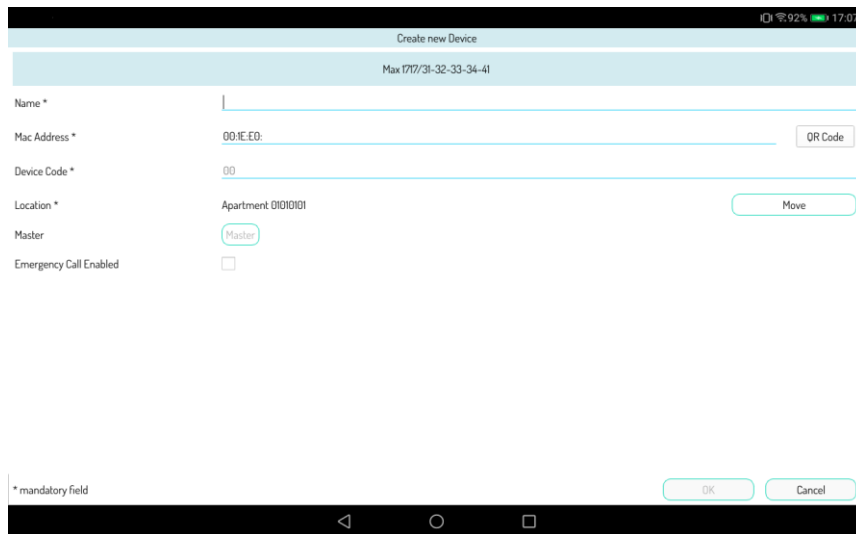


Figure 638: Adding a new device on Android tablet

By pressing this button, the "Barcode Scanner" app will start (if it is not in the system, the system will automatically prompt to install it through Google Play Store). When you open the app you have to position the camera in front of the QR Code of the device and wait for the scan and the automatic filling in of MAC address:

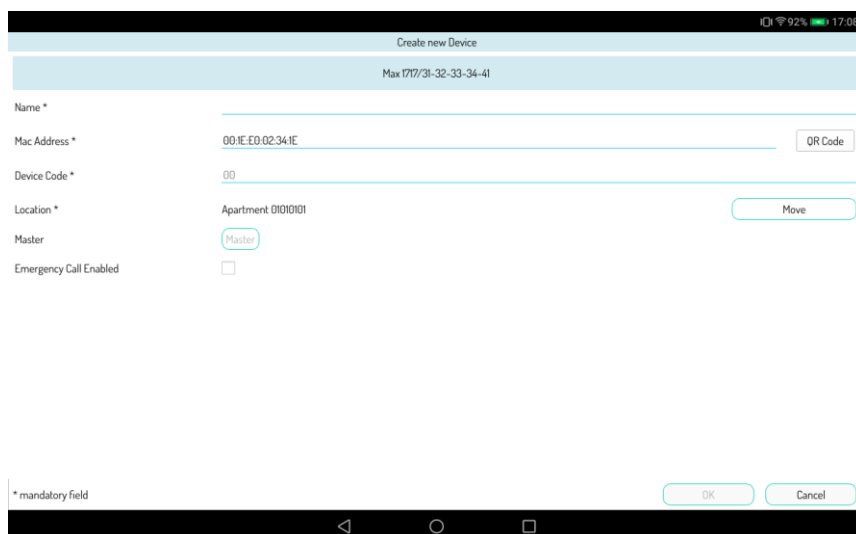


Figure 639: Automatic entering of the MAC address from the scanned QR Code

The device addition will be completed as usual after pressing "OK".

A similar procedure is to be followed to add all other devices installed in the system.

Once the devices are added to the configuration or in any case before distributing the configuration on the system, you will need to save the configuration on the SD card.



**Configuration file extension:** when saving the configuration you must assign a name to the file created; the default name of the file is "ipercom.ccf", but it can be changed by the user only by paying attention to always add the extension ".ccf" at the end of the name (otherwise the configuration cannot be imported from the MAX monitor).



**Removing the SD card after saving):** After you have saved the configuration via Android Tablet, to prevent the configuration file from being corrupted, it is advisable to remove the SD card before removing it from the device.

#### 8.3.2.4 Mode 3: The installer creates the configuration in the laboratory on the MAX video door phone/PC/Android tablet and adds at the same time the devices that are not yet installed

**Application case:** The devices are still in stock (therefore neither installed in the system nor configured): the configuration is created entirely in the laboratory taking note of the position of the devices and their MAC address.

**Pros:** It is possible to create the topology in the laboratory on a PC and add devices (of any type) by manually entering their MAC address or by scanning the QR Code.

**Cons:** Care must be taken when noting the devices arrangement in the system.

In this case, the installer has the devices not yet installed in the system and prepares the configuration offline in the laboratory via *MAX video door phone/PC/Android tablet*.

1. Configuration creation (topology only) in the laboratory and export to SD card

The installer creates the configuration in the laboratory on the *MAX video door phone/PC/Android tablet* by initially setting only the system topology.

2. Addition of the devices to the configuration directly in the laboratory, before their installation on the system

When the devices are available, it is possible to add them to the configuration as usual, by manually entering the MAC address indicated on the package or, if using an Android tablet, by scanning the QR Code, as described before.

The only thing we suggest to pay attention to, is to write down the position in which each device is to be installed.

### 8.3.2.5 Mode 3.1: The installer creates the configuration in the laboratory on the MAX video door phone/PC/Android tablet and adds at the same time the previously installed devices

**Application case:** The devices have already been installed, taking note of the topological position (block/stair/floor/apartment) and of the relevant MAC.  
The configuration is created entirely in the laboratory by relying on the notes taken during the installation (correspondence between device type, MAC address and topological position).

**Pros:** It is possible to create the topology in the laboratory on a PC and add devices (of any type) by manually entering their MAC address.

**Cons:** There is a risk of making mistakes when:

- writing down the location of each device (and the relevant MAC), and;
- when copying the MAC address.

In this case the installer needs a list containing the following information for each installed device:

- the type of device (product model number, e.g. 1060/18);
- the MAC address of the device (e.g. 00:1E:E0:00:01:02), reported manually or by applying the label provided with QR code available on each *iPerCom* device;
- the topological location (e.g. Block 01, Stair 02, Floor 04, Apartment 04).

Then, based on this data, the installer prepares the configuration offline in the laboratory via *MAX video door phone/PC/Android tablet*.

The *APPENDIX D* contains a possible model for this purpose.

1. Configuration creation (topology only) in the laboratory and export to SD card

The installer creates the configuration in the laboratory on the *MAX video door phone/PC/Android tablet* by initially setting only the system topology.

2. Addition of devices to the configuration directly in the laboratory, based on the written down information

With the above information available, it is possible to add each device to the configuration by manually entering the reported MAC address or, if using an Android tablet, by scanning the QR Code, provided that the device label has been directly applied to the notes.

### 8.3.2.6 Mode 4: One MAX video door phone with configurator in "Acquisition" mode

**Application case:** The devices are already installed on the system. The configuration has already been created/imported on a *MAX video door phone* and the same *MAX video door phone* and all other devices have been added.

**Pros:** All *MAX video door phones* can be added to the configuration via an automatic procedure that can be followed at the same time by several people (the presence of more people speeds up the configuration creation).

**Cons:** It is necessary to keep one *MAX video door phone with configurator* in "Acquisition" mode.

In this case, it is assumed that the system has already been installed and that the installer creates a configuration as explained before, by adding only one *MAX video door phone* and other devices other than *MAX video door phones*.

The other *MAX video door phones* will be added automatically upon request by the current *MAX video door phone*.

1. Creation of the configuration and addition, to that configuration, of a selected *MAX video door phone* and of other devices (except *MAX video door phones*) according to one of the modes described above, and configuration distribution from the same *MAX video door phone*.
2. Start of the acquisition mode on the field from the selected *MAX video door phone*.

From the selected *MAX video door phone* go to the *configuration menu*, then to "System configuration" and to "Start acquisition mode", as shown in the following figure:

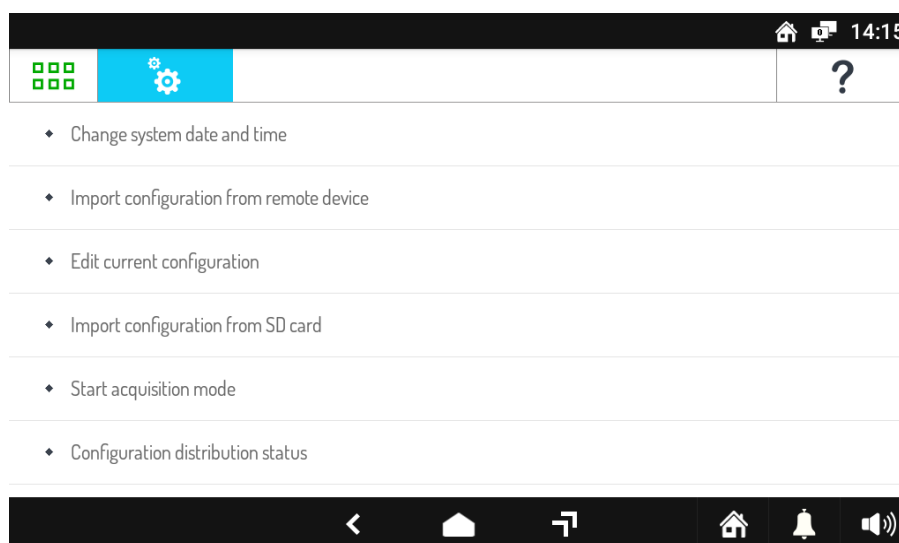


Figure 640: "Start acquisition mode" in the configuration menu

The following window will open:

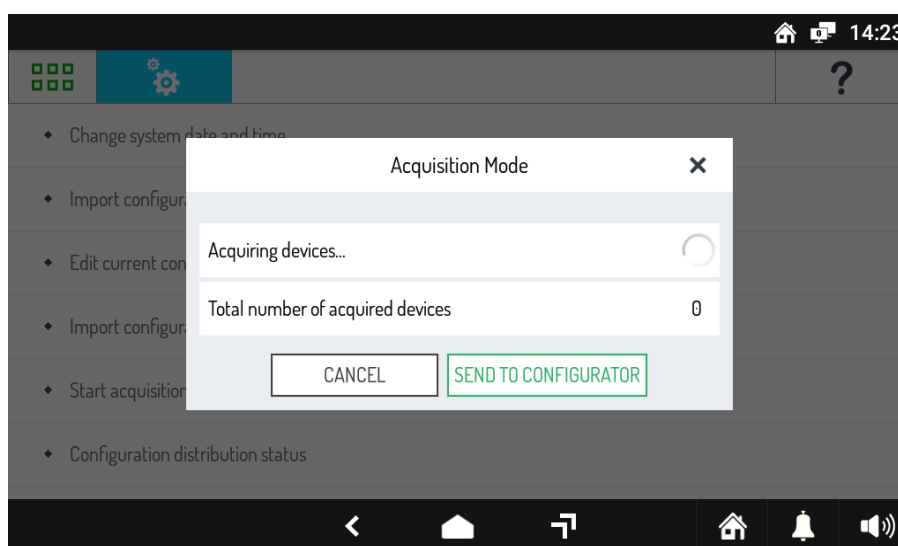


Figure 641: Acquisition mode

The selected *MAX video door phone* then sets to the "Acquisition" mode where it waits for all non-configured *MAX video door phones* to communicate their position in the system.

In fact, as soon as this mode is started, all the other *MAX video door phones* of the system not yet configured will display the following window:

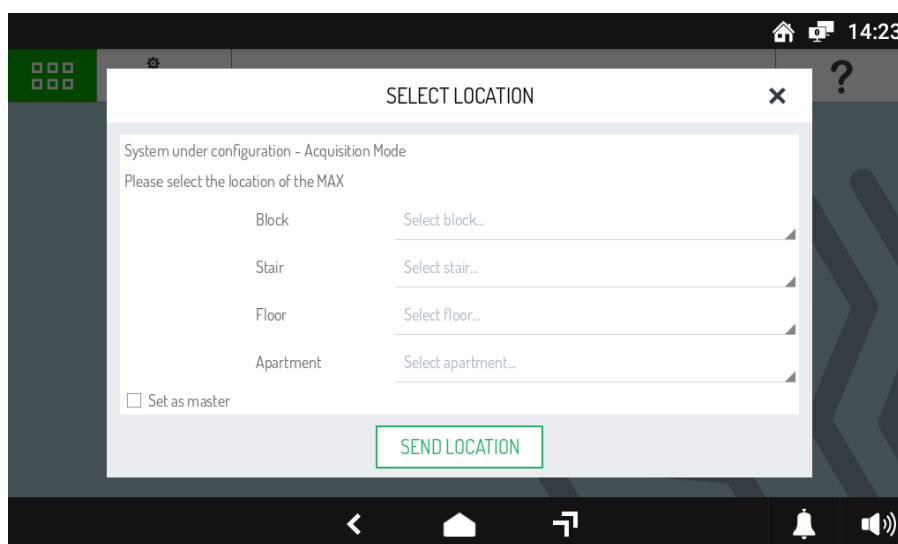


Figure 642: Entering the topology node in non-configured *MAX video door phones* during acquisition mode

No selections can be made in the Villa Kit type projects in the window shown in figure. The position of the *MAX video door phone* cannot be different from the apartment (the only one present in the system model).

3. Sending the position from all other *MAX video door phones* to the selected *MAX video door phone*

For all *MAX video door phones* of the system, except the selected one, it will be necessary to fill in the fields shown in the previous figure and press "SEND LOCATION" to send these data to the *MAX video door phone* that is in acquisition mode.

This operation can be performed contemporaneously by several people to speed it up.

Once the positions from all *MAX video door phones* have been sent, it is necessary to go back to the selected *MAX video door phone* and, after checking that the actual number of *MAX video door phones* to be configured is indicated in the "Number of devices acquired" field, press "SEND TO CONFIGURATOR".

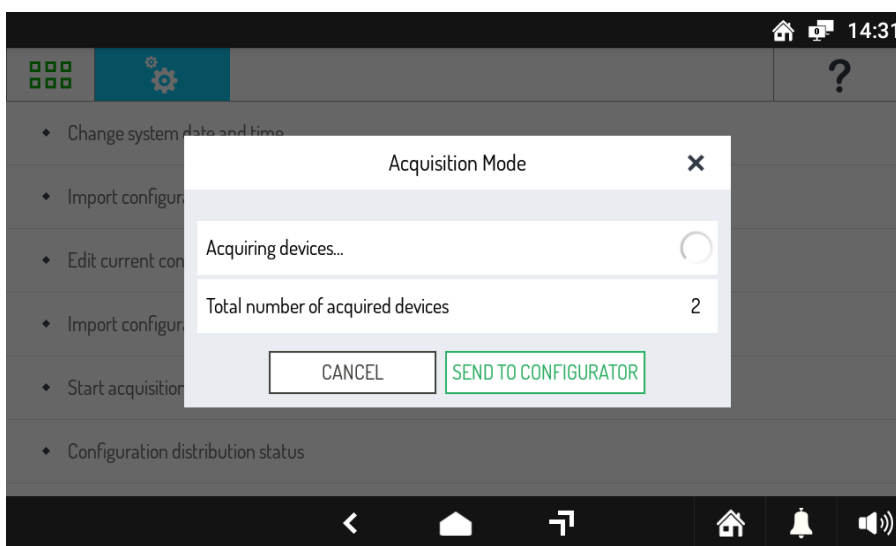




Figure 643: Updating acquisitions from non-configured *MAX video door phones*

*IPerCom Configurator* will then be opened (after entering the installer password), showing the automatically updated configuration, with all the *MAX video door phones* of the system added in the relevant topological nodes.

 **Case of manual network settings):** Mode 4 for adding devices only works if the "System" tab is as "Automatic" network setting. Therefore, this mode cannot be used in the case of manual network configuration (device static IP address).

 **Sending the default position):** if you leave all the fields unchanged in the window in Figure 426 and press the "SEND POSITION" button, a default position is sent for the *MAX* monitor: this position, in case of *Kit Villa* type projects, is that of the apartment; for all other types of project, the default position is instead the topological node at the highest system level.

## 8.4 Configuration distribution

The configuration is always distributed via *MAX*, *VOG<sup>7</sup>* or *Basic video door phone*, and can be done in two ways:

- directly from the *configurator* (if you are changing the configuration from a *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* connected to the system);
- from the *configuration menu* by importing from SD card (if you have a configuration saved on SD card).

If you have just finished modifying the configuration on the *MAX*, *VOG<sup>7</sup>* or *Basic video door phone configurator*, to apply it to the system, select the "Project" tab and press the "Apply" button.

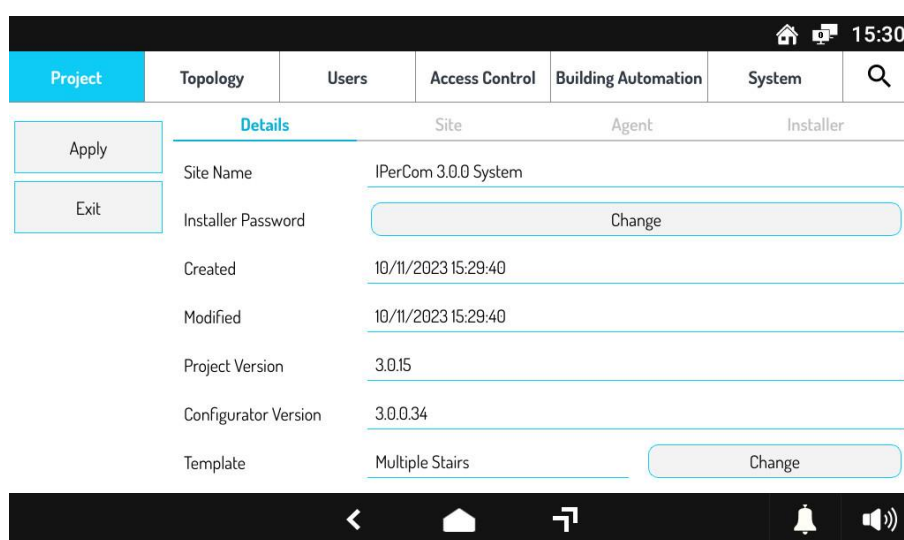


Figure 644: Configuration distribution from the configurator

You will be asked if you really want to apply the configuration to the system: confirm to start the configuration distribution to all the devices of the system.

If, on the other hand, the configuration has been previously saved to a file and you want to distribute it directly to the system without going through the *configurator*, you must import the configuration from the SD card.



To import a configuration from SD card, access the *configuration menu*, then select the option "Import configuration from SD card": the window shown in the figure will open.

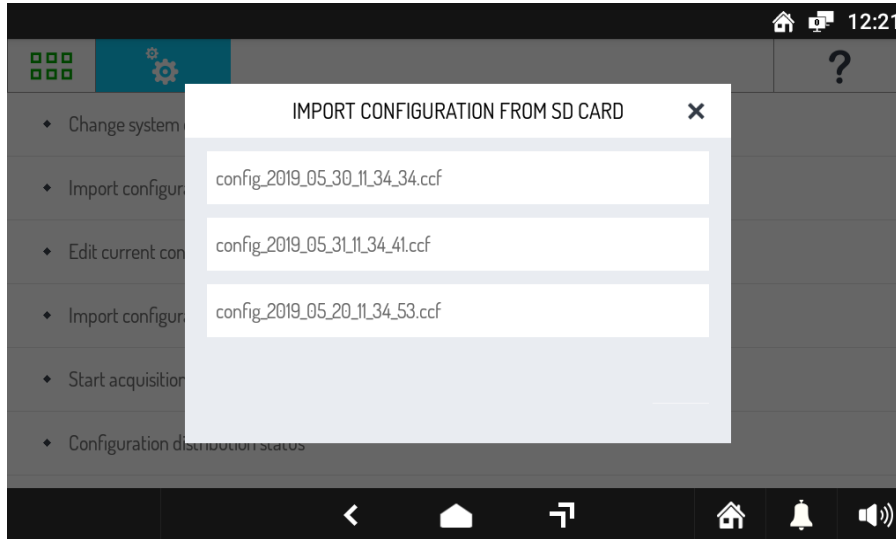


Figure 645: Configuration distribution by importing from SD card

The window shows all the configuration files saved on the SD card: once the desired file has been selected and the configuration distribution request has been confirmed, it will be applied to all the system devices.

Regardless of how the distribution of the configuration is started, the following window will be displayed as soon as it starts, showing the distribution status on the system.

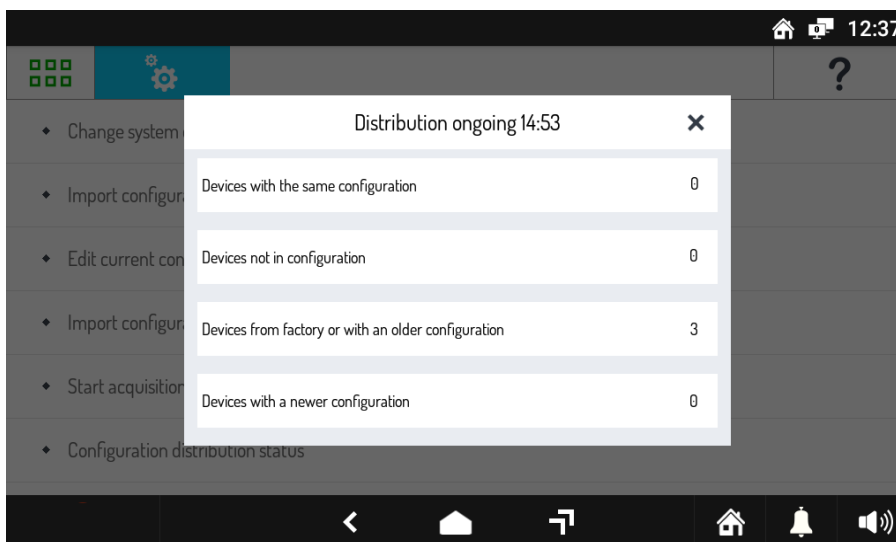


Figure 646: Status of configuration distribution

This window shows in sequence:

- the “*Devices with the same configuration*”, i.e. devices that at that moment have the same configuration present on the current device;
- the “*Devices not in configuration*”, i.e. devices that have not been included in the configuration present on the current device;
- the “*Devices from factory or with an older configuration*”, i.e. devices which are part of a configuration older than that on the current device, or which have no configuration at all;
- the “*Devices with a newer configuration*”, i.e. devices that have a configuration that is more recent than the one on the current device.

The configuration will be considered **complete** when all the devices which have been added to the configuration have received this configuration. In this case, the last two items of the configuration distribution state (“*Devices from factory or with an older configuration*” and “*Devices with a newer configuration*”) will be set to 0, as shown in the following figure.

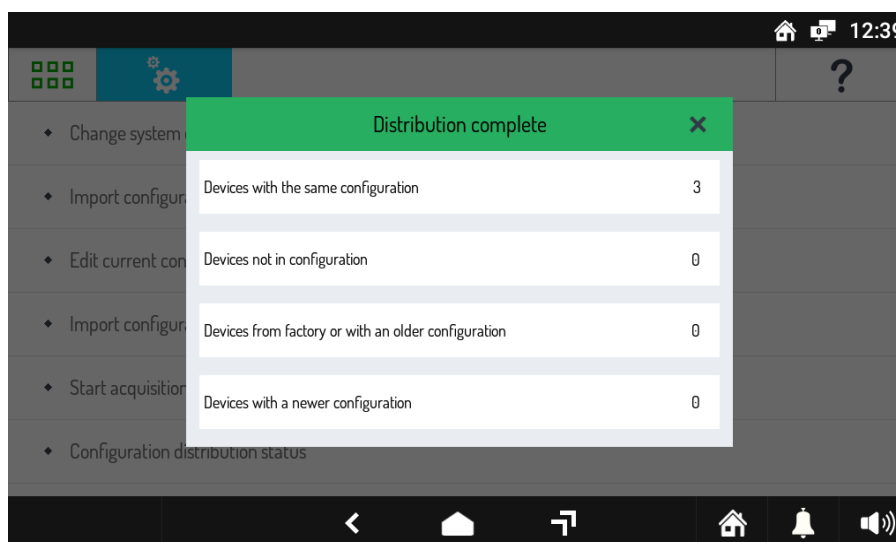





Figure 647: Indication of completed distribution

-  **Automatic device reboot:** According to the settings made (e.g. changes to network setting parameters), some devices may automatically reboot during configuration distribution.
-  **Changes to network settings:** If network settings changed, it is recommended to reboot the switch after having distributed the configuration.
-  **Devices not yet added to the configuration:** As mentioned, the configuration distribution will be deemed complete if all devices have received it correctly. Any non-configured devices which have not yet been added to the configuration will be indicated under “*Devices not in configuration*” in the distribution status window.

## 8.5 Exporting the configuration to an SD card

It is recommended to make always a copy of the configuration on a file by means of export to SD card.

To this purpose, in the *configuration menu*, in the sub-menu "*System configuration*" there is the function "*Export configuration to SD card*", which allows saving the current configuration to the SD card.

Once the SD card has been inserted and the above item has been selected, the following window will open:

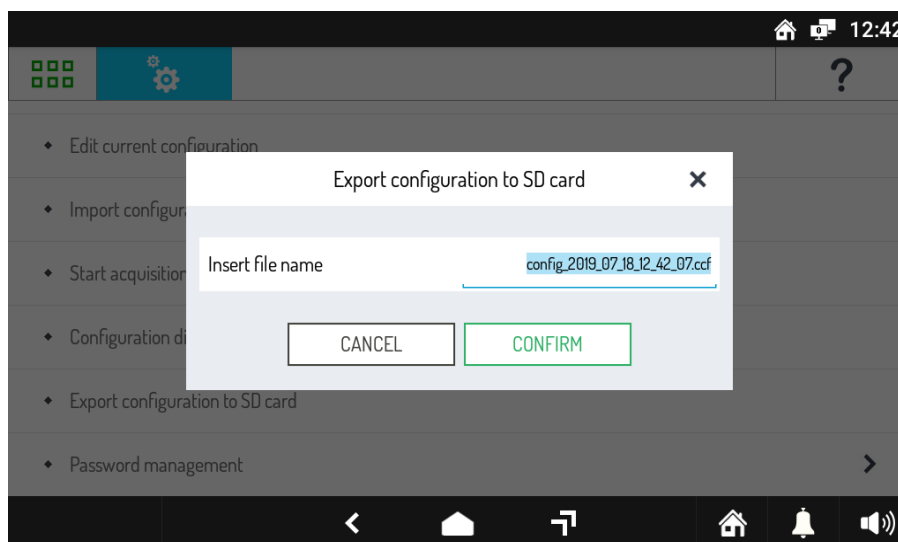


Figure 648: Exporting the configuration to SD card

Assign a name to the file to export, then press "*CONFIRM*" to export to the SD card.

## 8.6 Securing the system

Once the system configuration has been completed and distributed to all the devices, i.e. while the system is running, it is possible to secure the system by setting an administrator password in addition to the installer password. In practice this means that the installer can only make changes to the configuration and the system by requesting the administrator password. On the other hand the administrator cannot change the configuration to the system as he/she does not know the installer password. Therefore, the system has a double security level.

The administrator password can be entered from the *configuration menu* by selecting "System configuration", then "Password management" and then "Lock System" items.

The following screen will be displayed:

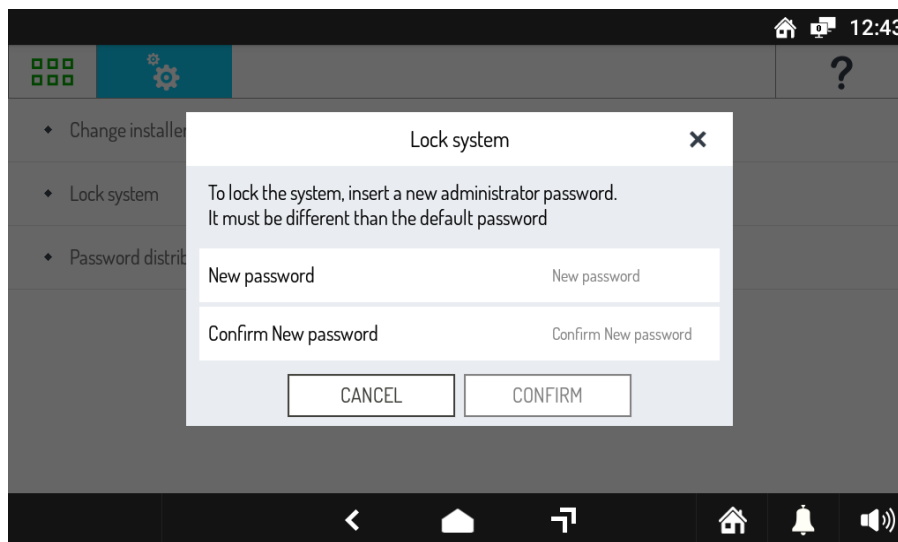


Figure 649: Administrator password setting

Once the password is entered, you will have to wait for the distribution of the administrator password to all the devices of the system: you can monitor the distribution status in the dialog box shown below.

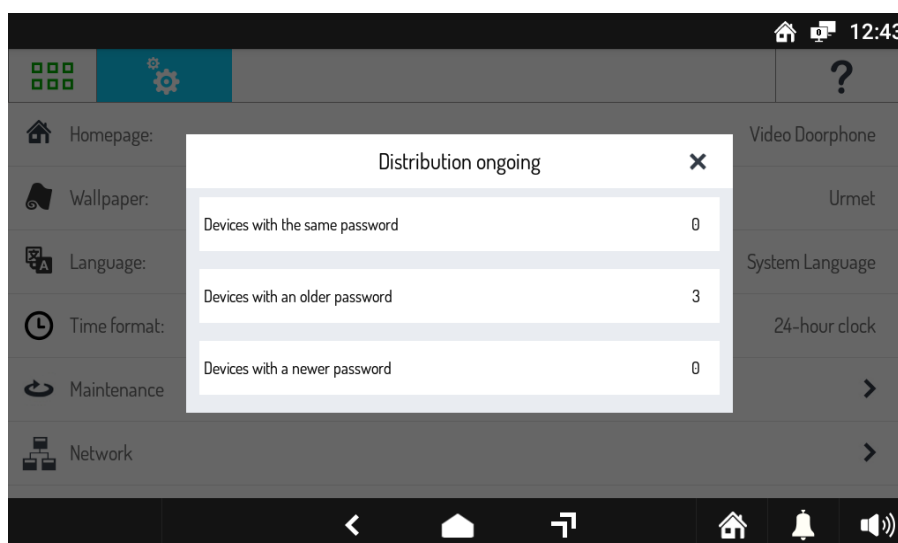


Figure 650: Password distribution status

As soon as the value of the last two fields is zero, the password distribution will be completed.

Once you have changed the password in the system, to access the *configurator* you will need to enter the administrator password and no longer the Urmet password.

## 8.7 Changing the system configuration

Once the first configuration of a system has been created, all the devices that make it up work as set in the configuration and any changes are made after entering the administrator password.

In fact, if all the steps of the first configuration have been carried out correctly, the system must have been properly blocked at the end of the procedure.

In these conditions, if you want to access the *configuration menu* of a *MAX*, *VOG<sup>7</sup>* or *Basic* video door phone belonging to the system, you would have to enter the administrator password instead of the Urmet one, as shown in the following figure:

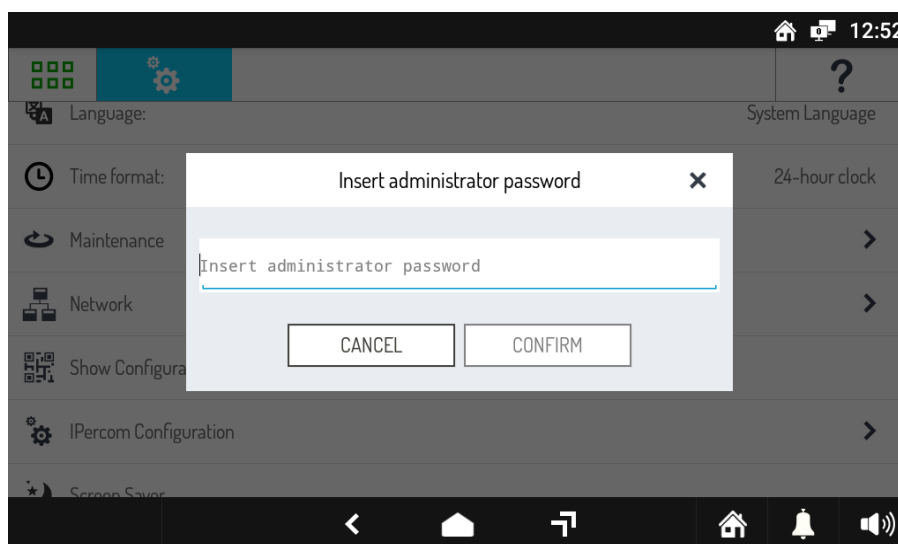


Figure 651: Access to the configuration menu of a blocked system

If you want to make significant changes to the system (for example, add a new block with several new devices), it is recommended to perform these operations with unlocked system (to unlock a system refer to paragraph [Unlocking a system](#)).

### 8.7.1 Unlocking a system

To unlock a previously blocked system, open the *configuration menu* from a *MAX*, *VOG<sup>7</sup>* or *Basic* video door phone belonging to the system, then select "System configuration" and then "Password management": the following screen will open.

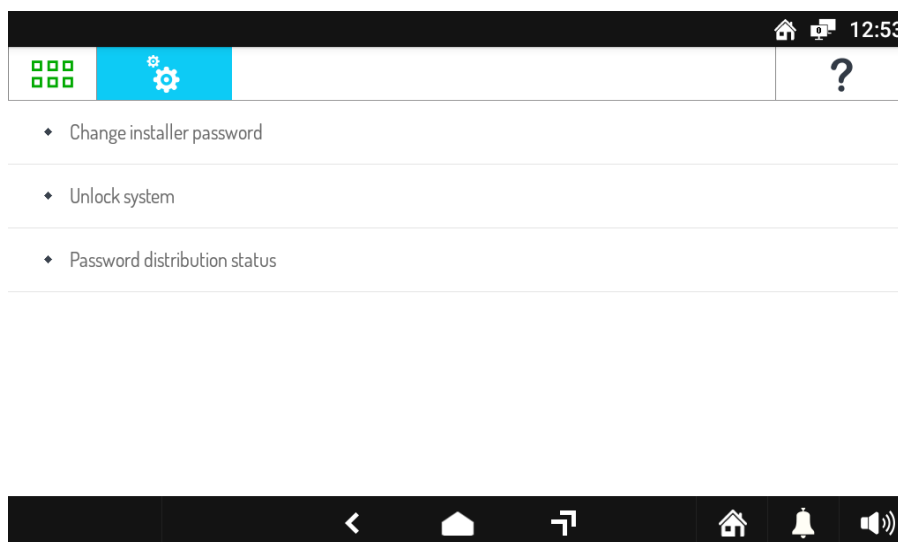


Figure 652: "Password management" screen in case of blocked system

By selecting "*Unlock system*" and confirming the request, the administrator password is no longer required; the distribution status of the new password will be visible in the status window shown in the figure below:

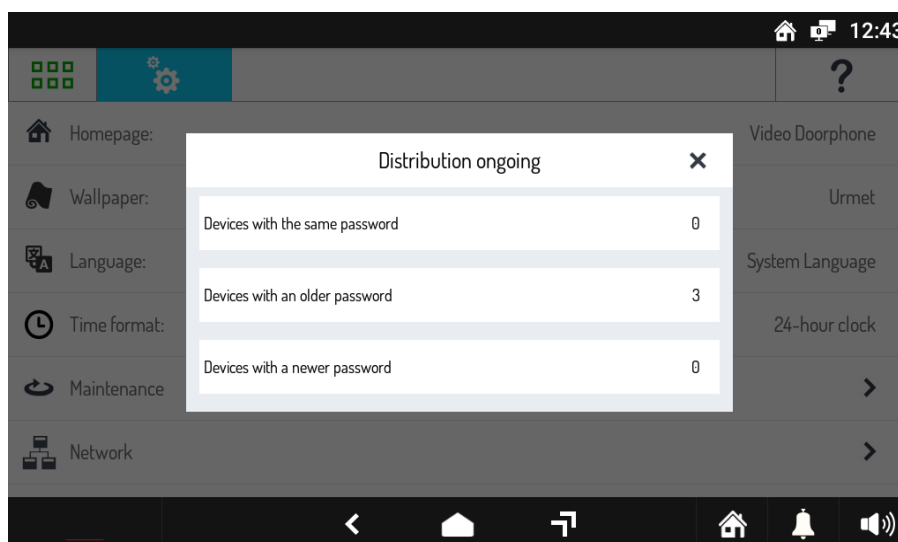


Figure 653: Password distribution status

## 8.7.2 How to change the configuration

The configuration of a system can be changed in different ways:

1. by updating the users from the *Switchboard* application installed on the system;
2. by opening the configurator from the *configuration menu* of a *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* installed in the system;
3. by exporting the system configuration to the SD card, by modifying the file in the office from the *configurator* for *MAX*, *VOG<sup>7</sup>* or *Basic video door phone*/PC/Android tablet and by importing it to the system.

While the first mode is performed by the *Switchboard* operator, the other two are used by the system installer.

To change the current configuration of a system, access the *configuration menu* of a properly configured *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* belonging to the system, then select "*System configuration*" and "*Edit current configuration*": once the installer password has been entered, the *configurator* will open in the "*Topology*" tab, as shown in the following figure:

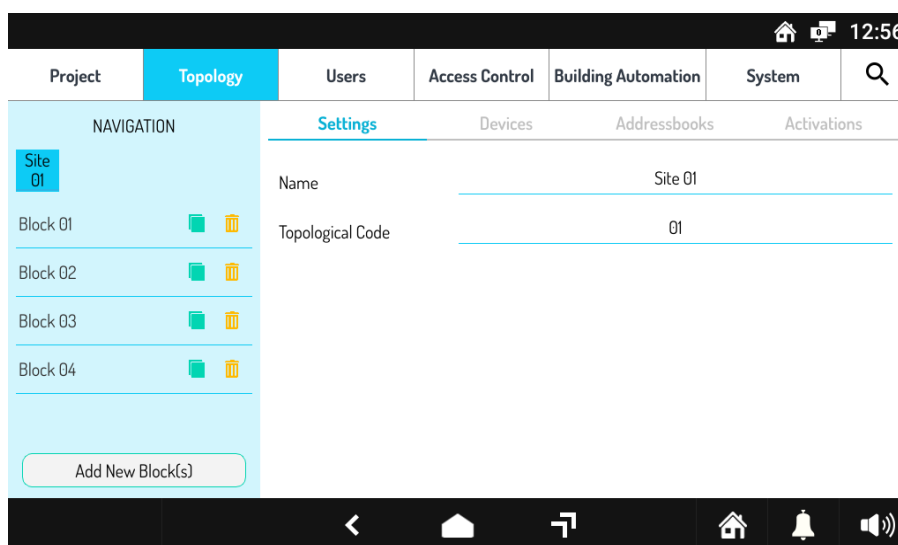


Figure 654: How to change the current configuration

Once the necessary changes have been made, to distribute the configuration to the system, select the "*Project*" tab and press the "*Apply*" button.

The modification of the current configuration from a *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* and that made via the *Switchboard* affect the current configuration of the system. If on the other hand you decide to use the last mode, i.e. changing the configuration in the office via *MAX*, *VOG<sup>7</sup>* or *Basic video door phone*/PC/Android tablet, you must consider that the change is not applied to the current configuration of the system, but on the latest version exported to SD card.

Exporting to SD card creates a file with CCF extension, which can be opened by clicking on "Open" in the "Project" tab of the configurator.

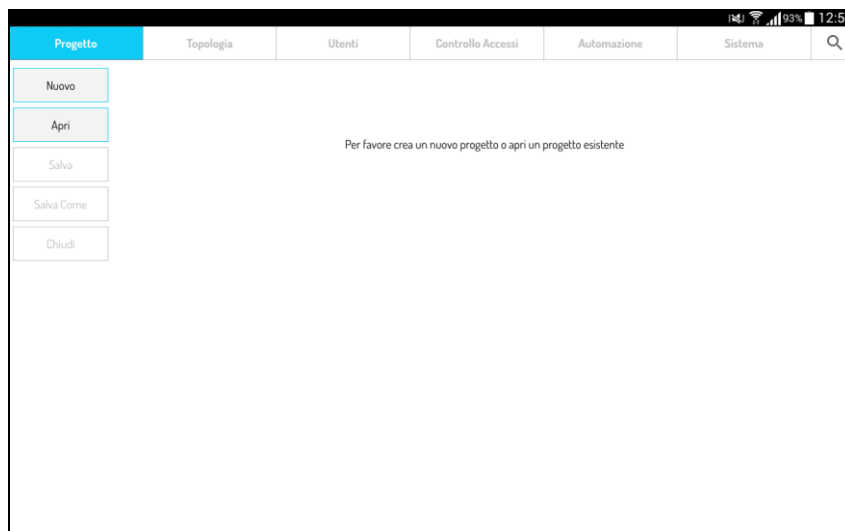


Figure 655: Opening a project from the configurator for MS Windows

Once the configuration changes have been made, in the "Project" tab, press the "Save" button to overwrite the project file on the SD card.

The last step at this point consists in importing the modified configuration on a MAX, VOG<sup>7</sup> or Basic video door phone of the system; then select the configuration menu, and in the "System configuration" sub-menu choose the option "Import configuration from SD card": the following screen will open:

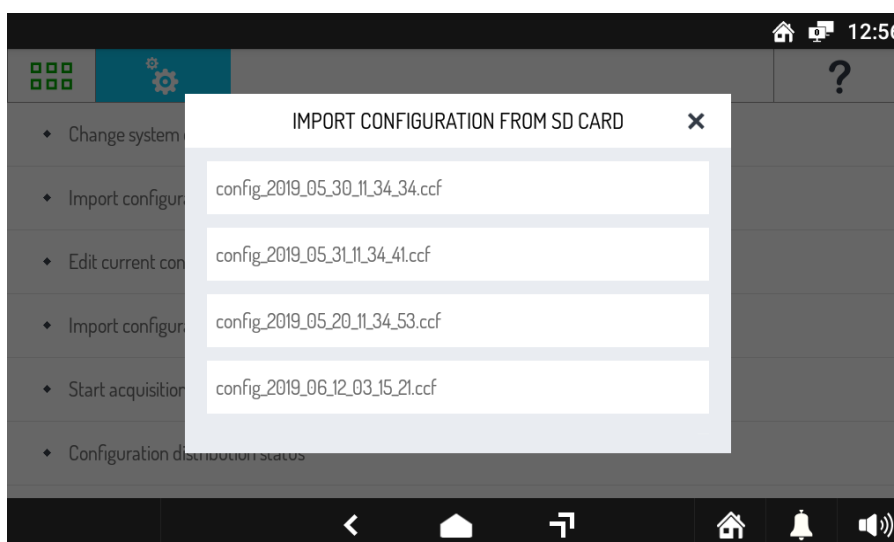



Figure 656: Importing the configuration from SD Card

Once the installer password is entered, the imported configuration will be distributed throughout the system.



 **Modification of the configuration off-site):** After having exported the current system configuration to change it off-site, the system may change its present configuration (via Switchboard or MAX, VOG<sup>7</sup> or Basic video door phone). In this case, loss of data may occur if you import the configuration modified off-site to the system. To avoid this problem, avoid modifying the configuration present on the system after exporting it or alternatively take note of all configuration changes which occurred on the system on the version modified off-site.

### 8.7.3 Changing the administrator password

The administrator-level security of the IPerCom system has only two statuses: blocked and unlocked.

To change the administrator password of a blocked system, it will therefore be necessary to unlock it and as soon as this operation is completed, lock the system again with the new administrator password.

During these steps it is necessary to pay attention to the correct distribution of passwords throughout the system, in order to be sure that the unlocking and the blocking operations are successful. To this purpose there is a user-friendly status window of the password distribution on the system, shown in the following figure:

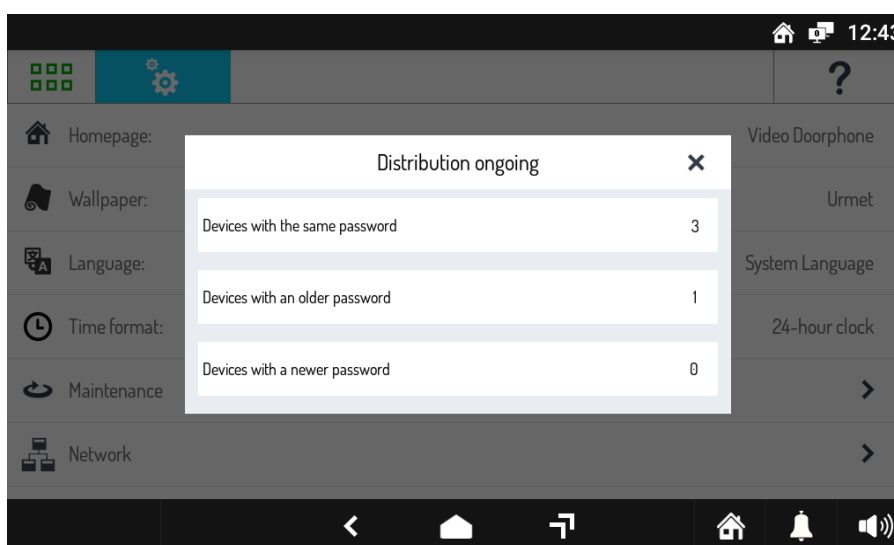


Figure 657: Password distribution status

Once the lock/unlock operation has been completed, before carrying out the opposite operation, check that the distribution of passwords is complete, i.e. that the value of the last two fields is equal to zero.

### 8.7.4 Changing the installer password

Changing the installer password is necessary if the administrator decides to change the installer or if the installer has forgotten the password. In both cases the password change does not require that you know the previous one. To change the installer password, open the *configuration menu* from a *MAX*, *VOG<sup>7</sup>* or *Basic video door phone* belonging to the system, then select "*System configuration*" and then "*Password management*". The screen displayed is as follows:

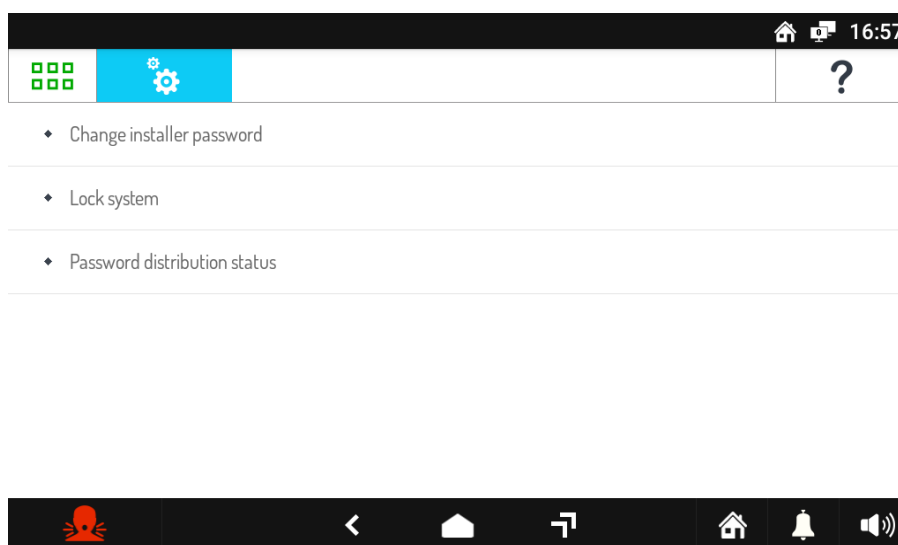


Figure 658: password management screen

Press "*Change installer password*" item, the following screen is displayed:

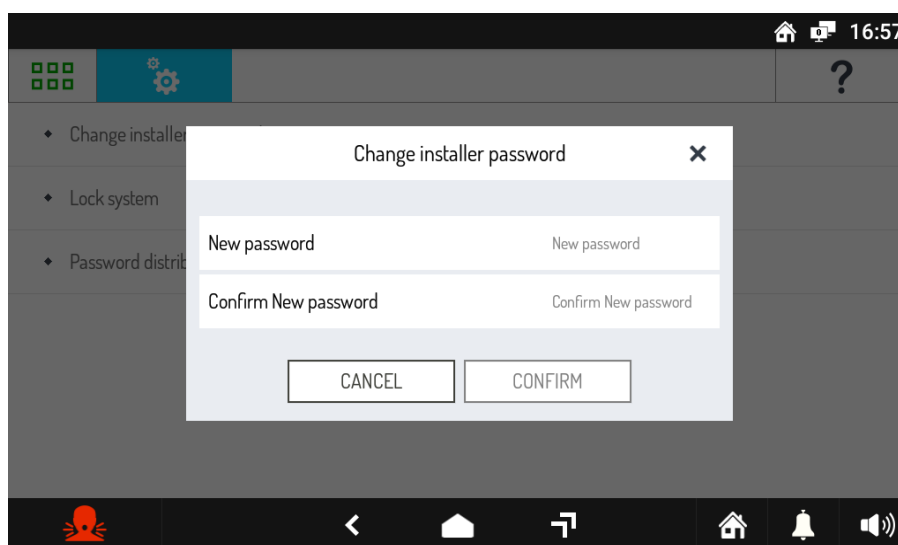


Figure 659: installer password change screen

Now simply enter and confirm the new password. Press the "CONFIRM" button and wait for the distribution of the new installer password to all the devices in the system. It is possible to monitor the status of this distribution in the dialogue box shown below:

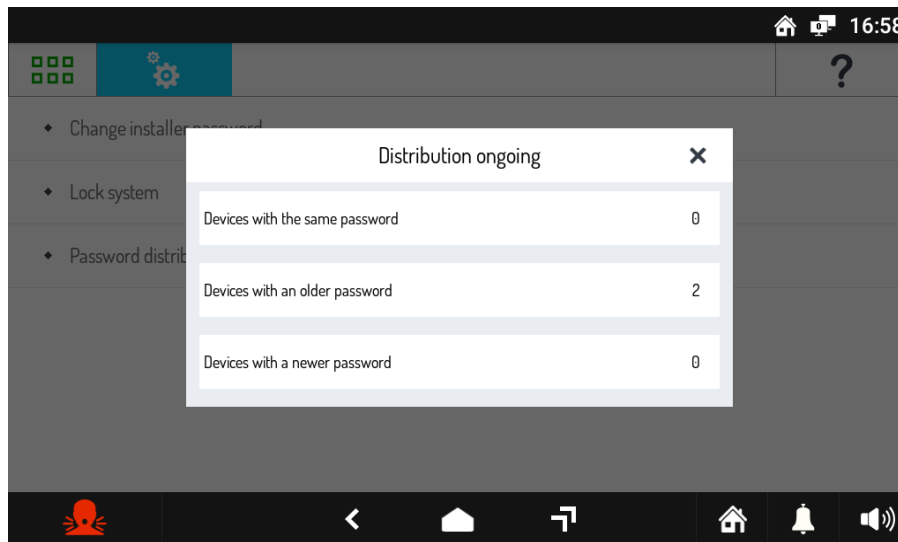


Figure 660: new installer password distribution

As soon as the value of the last 2 fields is zero, the password distribution will be completed.

### 8.7.5 Devices not aligned to the same IPerCom version or UPTK software development platform

The possible presence of a misalignment between the UPTK versions of the devices and/or software applications is also signalled by the *video door phones*, which compare them with their own local UPTK version. A misalignment between UPTK versions simply implies the presence on the system of devices/applications with different IPerCom versions.

The most common cases of misalignment can occur in the following 3 ways:

1. with the system and software applications aligned, one or more devices that are not updated to the same IPerCom version of the system and are not present in the system configuration are connected to the system;
2. with the system and software applications aligned, one or more devices that are not updated to the same IPerCom version of the system but are present in the system configuration are connected to the system;
3. *Switchboard* and/or *IPerCom Client* applications present in the system configuration have not been updated to the latest IPerCom version present on the system.

What happens in the three cases reported above is reported in detail.

### CASE 1

The misalignment **is not reported** by the configured video door phones already present on the system: this is to avoid compromising the functioning of the system itself. If the device connected and not updated to the same IPerCom version of the system is a video intercom, this signals the misalignment with the rest of the system, as shown below:

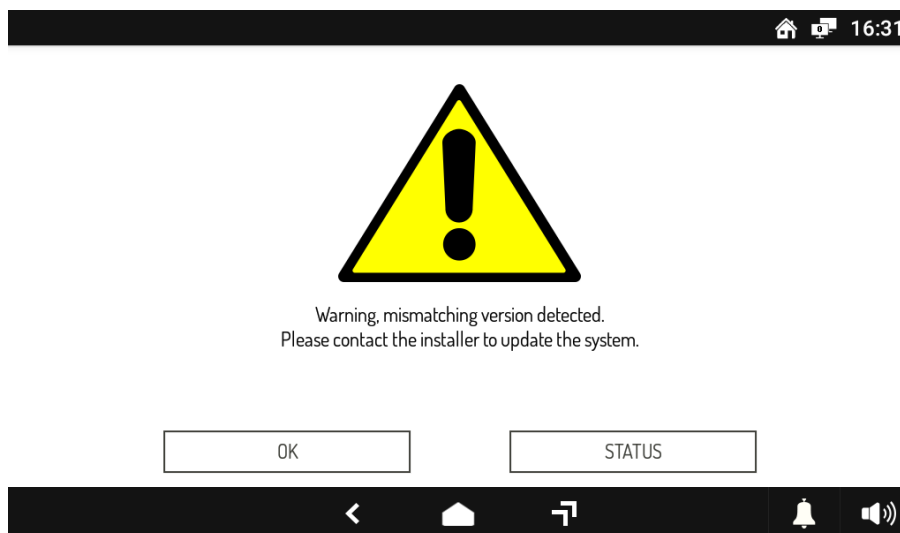


Figure 661: misalignment signalling on video door phone not present in the system configuration

Press the “Status” button to display the list of devices and/or software applications whose software development (UPTK) version (8.26) is not aligned with that of the local device (8.22) (in this case MAX, VOG<sup>7</sup> or Basic video door phone):

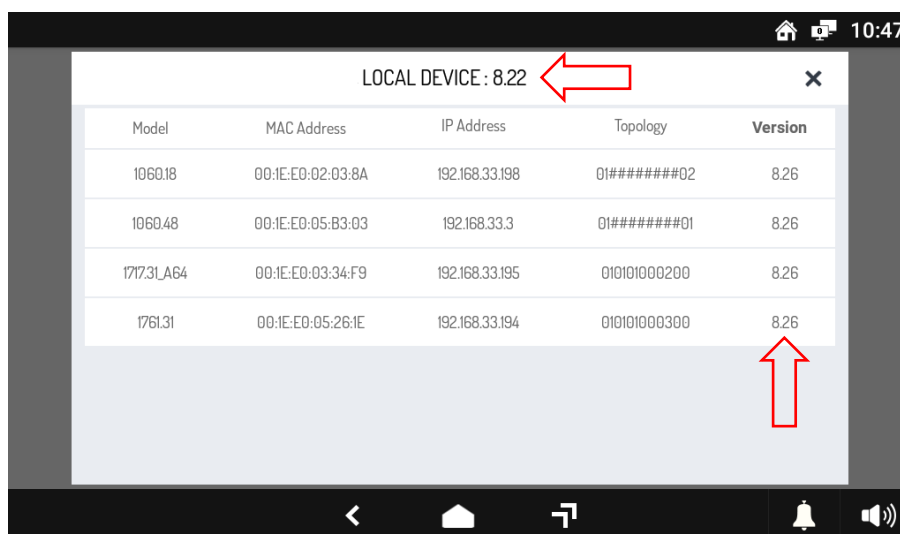


Figure 662: list of devices not aligned with the video door phone added to the system

The above list can list a maximum of 10 devices.

## CASE 2

The misalignment **is signalled** by the configured video door phones already present on the system in the same way as seen in the previous point. For example, if only one device is added that is not aligned and present in the system configuration, the video intercoms already present in the system report the following signal:

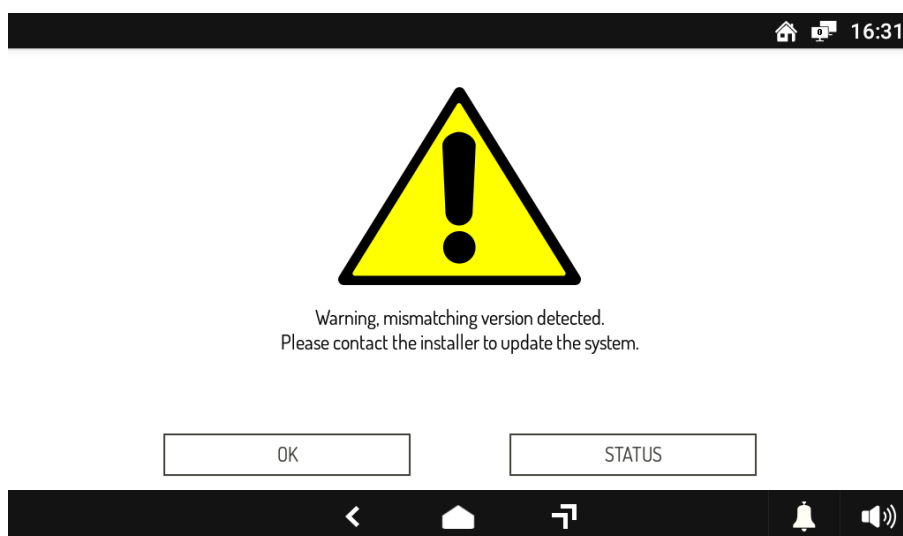


Figure 663: misalignment reporting on video door phone already present on the system

By pressing the "STATUS" button, only the newly added device is displayed (in the example a video door phone):

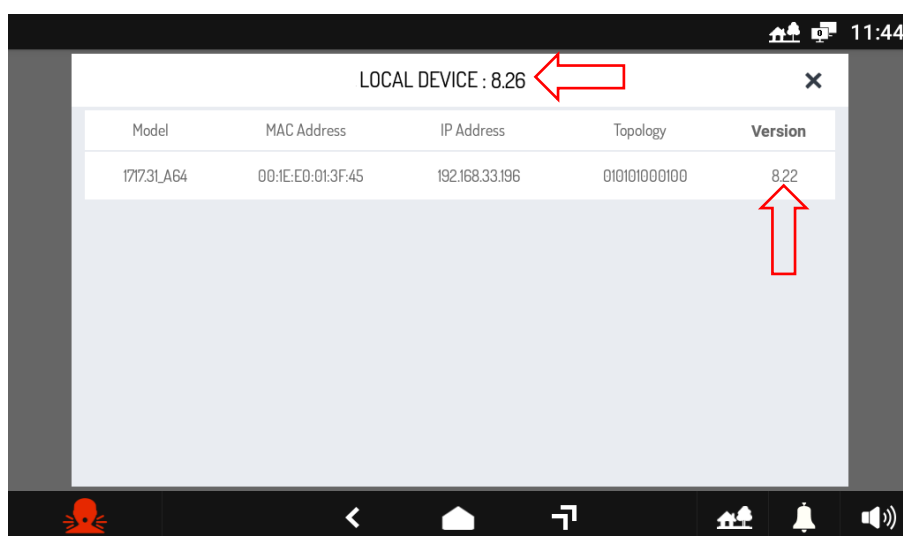


Figure 664: misalignment reporting on video door phone already present on the system

The IPerCom version of the device just connected (8.22) is not aligned with that of the system (8.26). Also in this case, if the connected device that is not updated to the same IPerCom version of the system is a video door phone, this signals its misalignment with respect to the rest of the system, as shown in [Figure 662](#).

**CASE 3**

The misalignment is reported both by the software application and by the video door phones configured in the same ways described in the previous points. For example, if the *Switchboard* application has not been updated to the latest IPerCom version present on the system, after connecting to the system itself, the configured video door phones already present on the system report the following signal:



Figure 665: misalignment reporting on video intercom for Switchboard application not aligned with the UPTK version of the system

By pressing the "STATUS" button, only the *Switchboard* application whose UPTK version is not aligned with that of the system is displayed:

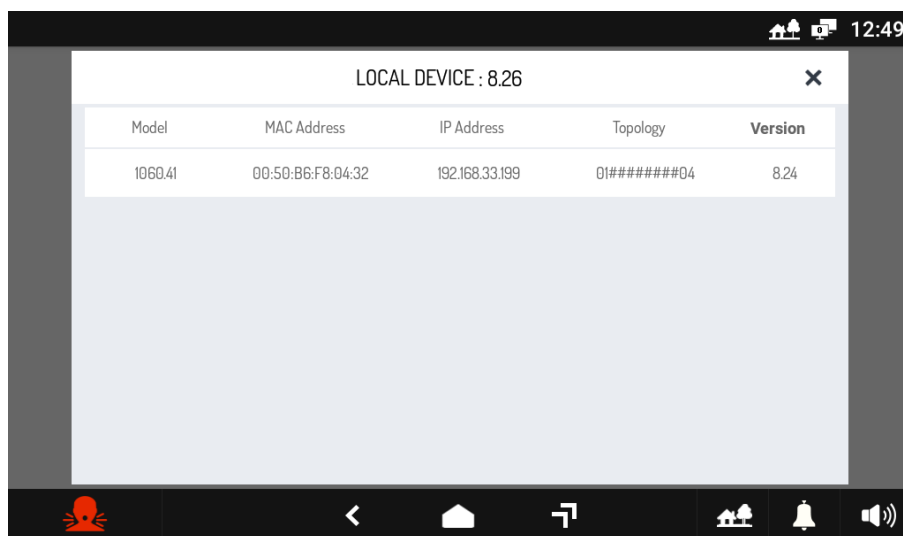


Figure 666: Switchboard application with misaligned UPTK



Similarly, the *Switchboard* application displays a similar window with the list of system devices that are not aligned with your version of UPTK (for further details see the *Switchboard* installation and use manual which can be downloaded from the website [www.urmet.com](http://www.urmet.com)).



*In all three cases reported above, the VOG<sup>5</sup> 1761/6 and VOG<sup>5+</sup> 1761/15-16-18-19 video door phones do not have the “OK” and “STATUS” buttons in the screen that notifies the presence of devices with misaligned UPTK.*

According to what is written above, it is therefore of fundamental importance:

- add new devices to a system only after having updated them to the correct IPerCom version using the *IPerUpgrade* application for Windows operating system, available with the relevant manual on the website [www.urmet.com](http://www.urmet.com);
- always update (also via the *IPerUpgrade* application) the *Switchboard* and *IPerCom Client* applications when a system has been updated to a more recent IPerCom version.



*The *Switchboard* and *IPerCom Client* applications can also be updated by downloading the relevant executable files from the website [www.urmet.com](http://www.urmet.com).*

If one or more 1060/1 Servers are present in the system and in configuration and at least one has the “Automatic update by Server” option enabled, it is also possible to connect devices to the system that are not aligned with the correct IPerCom version: these will be updated automatically by the *Server* itself. Similarly, if you start one of the out-of-date *Switchboard* and *IPerCom Client* applications, the *Server* will take care of updating them to the correct version.

After updating the non-aligned devices to the correct IPerCom version, the screen notifying the misalignment automatically disappears.

However, if the not-aligned devices are disconnected from the system, the message on the video door phones automatically disappears within 30 minutes. This operation can be speeded up using the Restart the system button of IPerCom Installer Tools (see the [Maintenance](#) paragraph).



*The **Updating Device List** function is present only on the *IPerCom Installer Tools* application but not on the video door phones nor on the *Switchboard* application, which only allow displaying the list of devices not aligned with the local UPTK version.*



*The “OK” button makes the message disappear, but it reappears every time you enter the system configuration from the video door phone (see paragraph [Commissioning a system through MAX, VOG7 or Basic video door phones: the configuration menu](#)).*

## 9 Integration with the iPerTALK system

IPerCom allows the integration of the iPerTALK system PBXs Ref. 1375/10-11-12-13 and Ref. 1375/10A-11A-12A-13A. This integration is useful for the following video door phone features:

- Audio or audio-video calls from Ipercom calling stations to iPerTALK extensions;
- Audio or audio-video calls from Ipercom apartment stations to iPerTALK extensions;
- Audio or audio-video calls from iPerTALK extensions to Ipercom *Switchboard* and vice versa;
- Door and gate opening from iPerTALK extensions;
- Auto-on function from iPerTALK extensions to Ipercom calling stations;
- Auto-on function from Ipercom apartment stations to iPerTALK calling stations;
- Auto-on function from Ipercom apartment stations to iPerTALK RTSP cameras;
- Audio or audio-video calls from iPerTALK extensions to IPerCom apartments or single IPerCom apartment stations (any *CallMe* application associated with the apartment also rings);
- Sending activation commands from iPerTALK extensions to IPerCom *Relay Actuators* (only during conversation).

**Integration with the IPerCom 3.1.0 system is only supported by iPerTALK version 2.2.10 or higher.**

Two integration modes are possible:

- **with iPerTALK switch Ref. 1375/701** in presence of an internal network in the iPerTALK system and you want to separate the network where iPerTALK is installed from the IPerCom network;
- **without iPerTALK switch Ref. 1375/701** when using iPerTALK as gateway to Volp phones on the Ipercom network.

The 2 integration modes are described below.

## 9.1 Configuration and installation sequence for integration of the iPerTALK system into the IPerCom system with the switch Ref. 1375/701

The following configuration steps must be followed for proper operation.

### 9.1.1 iPerTALK system configuration

Configure the iPerTALK system consisting of PBX, router, switches, and phones.

1. Connect the PBX, router, switches, phones, and PC that you will use for configuration to the iPerTALK Ref. 1375/701 switch, as shown in the connection diagram below.

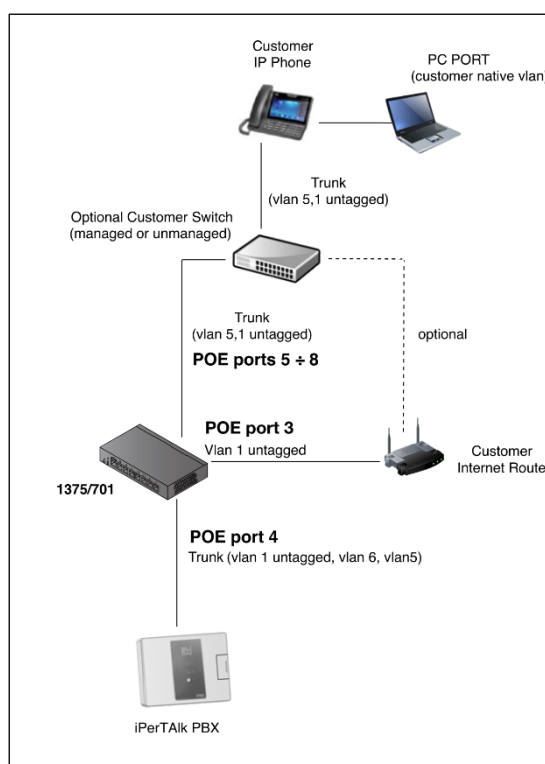


Figure 667: iPerTALK connection diagram with iPerTALK switch Ref. 1375/701

2. Wait until the PBX has booted up and the PC has received the IP from the router in the iPerTALK system.
3. On your PC open the web browser and type in the assigned IP address to PBX.
4. Proceed with phone acquisition and numbering assignment.
5. In the advanced system configurations add an IPerCom type line.
6. Create an inbound routing rule and add the IPerCom line as the destination trunk.
7. Enable the IPerCom network in the system network parameters.



Information relating to the specific configuration of the iPerTALK system integrated with the IPerCom system can be found in the [iPerTALK installation and configuration booklet](#).

### 9.1.2 IPerCom system configuration

1. Switch off the IPerCom system and the IPerTalk system.
2. Connect the iPerTalk switch Ref. 1375/701, the PBX, router, switches, and phones to the IPerCom network.



**Warning!** For a correct integration of the iPerTalk system with the IPerCom system, **exclusively** follow the instructions in the following connection diagram.

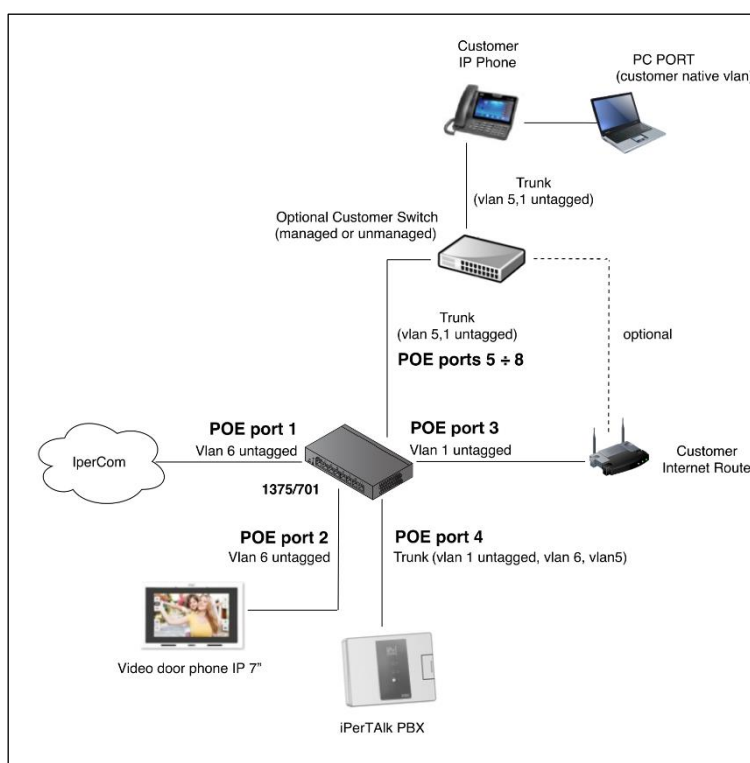


Figure 668: IPerCom connection diagram iPerTalk with iPerTalk switch Ref. 1375/701



**Warning!** In an apartment/floor with a Server iPerTalk V1 integrated with the IPerCom system, it is recommended to have an IPerCom apartment station so that all features of the system can be used.

3. Power the system up.
4. Create an IPerCom configuration, as described previously in this manual.
5. In the *configurator* select the "System" tab, then section "Network Settings", then choose as network addressing mode the item "Static", then set (for example) the following parameters:
  - a. "IP Range Minimum": 10.10.127.2
  - b. "IP Range Maximum": 10.10.127.254
  - c. "Network mask": 255.255.255.0
  - d. "Default Gateway": 10.10.127.1
  - e. "DNS": 8.8.8.8

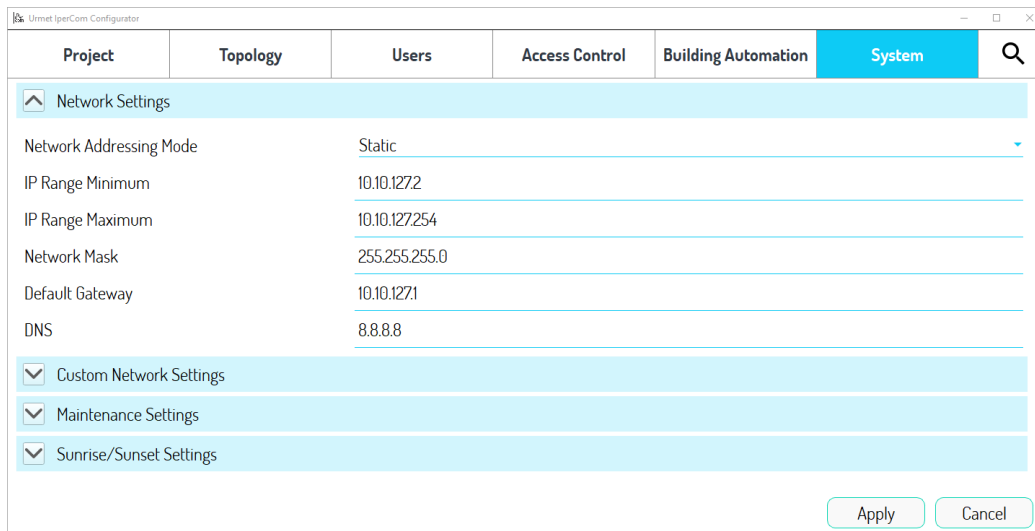


Figure 669: example of iPerCom network setup

6. In the “Topology” tab create the topological structure of the system and identify a topological node for Server *iPerTalk V1* (for example “Block 01” --> “Stair 01” --> “Floor 01”).
7. In the selected node add the Server *iPerTalk V1*.

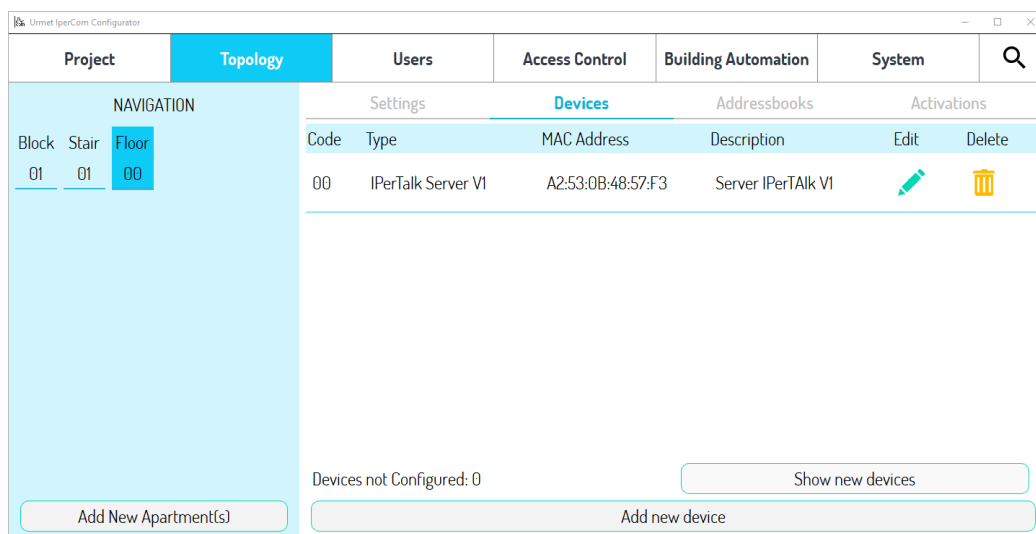


Figure 670: add of the iPerTalk Server V1

8. Navigating in the apartments of “Floor 00” (in this case where the Server *iPerTalk V1* has been added), on the “Settings” tab enable “iPerTalk” item and enter the number to call (item “iPerTalk ID”) (for example 90101, 90102, 90103, ...). Enabling the “iPerTalk” item, the apartment is considered as an extension in the iPerTalk system. Depending on how the system is structured, it may be necessary to configure several apartments equal to the number of extensions to be called from the iPerCom system. All apartments configured as iPerTalk extensions will be displayed in the iPerCom device directory.

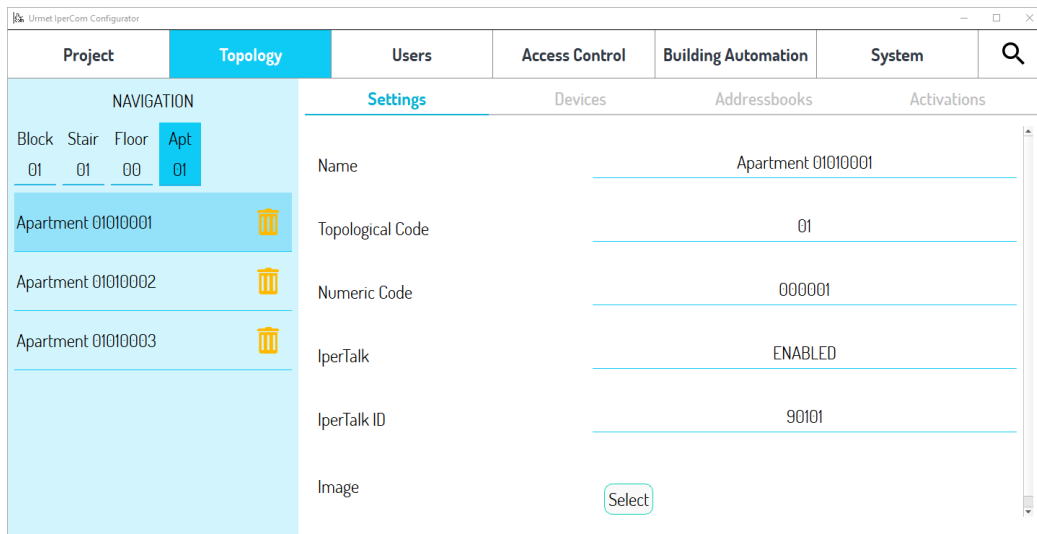


Figure 671: iPerTAlk ID configuration

9. Proceed with the configuration of the IPerCom calling stations and other IPerCom devices.

## 9.2 Configuration and installation sequence for integration of the iPerTALK system into the IPerCom system without the switch Ref. 1375/701

The following configuration steps must be followed for proper operation.

### 9.2.1 IPerCom system configuration

Configure the IPerCom system **without connecting the iPerTALK Server V1**.

1. Create an IPerCom configuration, as described previously in this manual.
2. In the *configurator* select the "System" tab, then section "Network Settings", then choose as network addressing mode the item "Static", then set (for example) the following parameters:
  - a. "IP Range Minimum": 10.10.127.2,
  - b. "IP Range Maximum": 10.10.127.254,
  - c. "Network mask": 255.255.255.0,
  - d. "Default Gateway": 10.10.127.1,
  - e. "DNS": 8.8.8.8
3. In the "Topology" tab create the topological structure of the system and identify a topological node for the *Server iPerTALK V1* (for example "Block 01" --> "Stair 01" --> "Floor 00").
4. In the selected node, add a *Server iPerTALK V1* by correctly setting the MAC address of the device (manually).

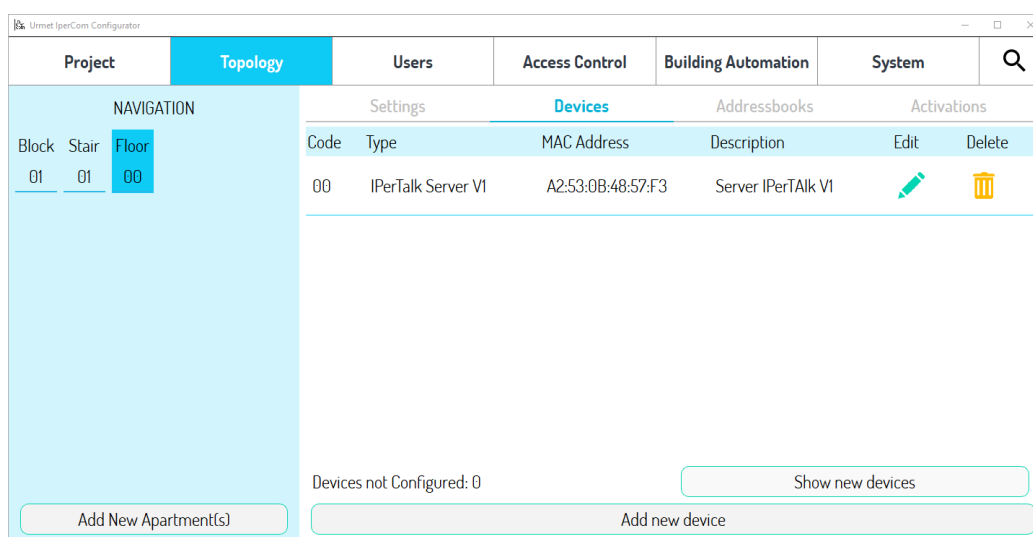


Figure 672: add of an iPerTALK Server

5. Navigating in the apartments of "Floor 00" (in this case where the *Server iPerTALK V1* has been added), on the "Settings" tab, enable "iPerTalk" item and enter the number to call (item "iPerTalk ID") (for example 90101, 90102, 90103, ...). Enabling the "iPerTALK" item, the apartment is considered as an extension in the iPerTALK system. Depending on how the system is structured, it may be necessary to configure several apartments equal to the number of extensions to be called from the IPerCom system. All apartments configured as iPerTALK extensions will be displayed in the Ipercom device directory.

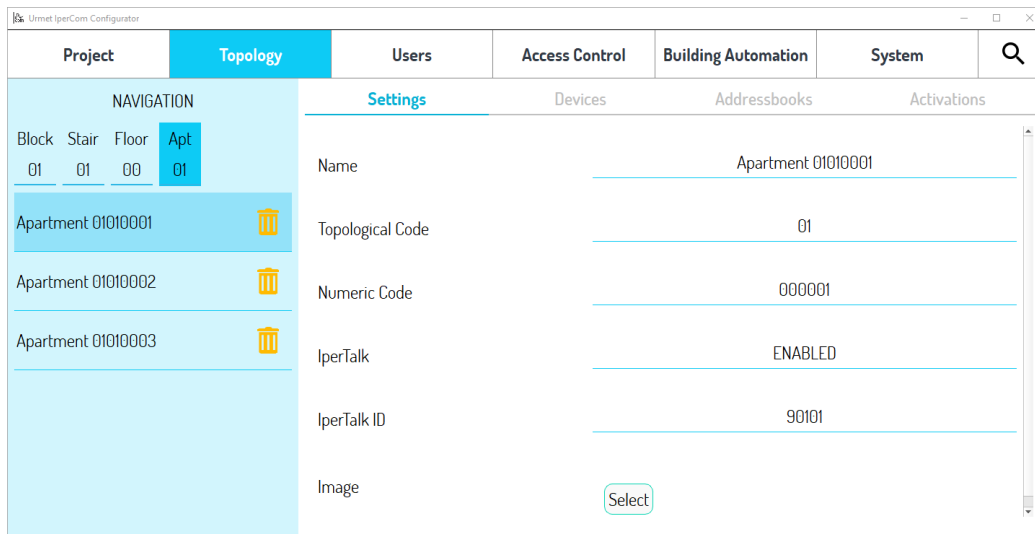


Figure 673: iPerTALK ID configuration

6. Proceed with the configuration of the IPerCom calling stations and other IPerCom devices.



## 9.2.2 iPerTALK system configuration

1. Switch off the IPerCom system.
2. Connect the PBX and phones to the switch in the IPercom system.

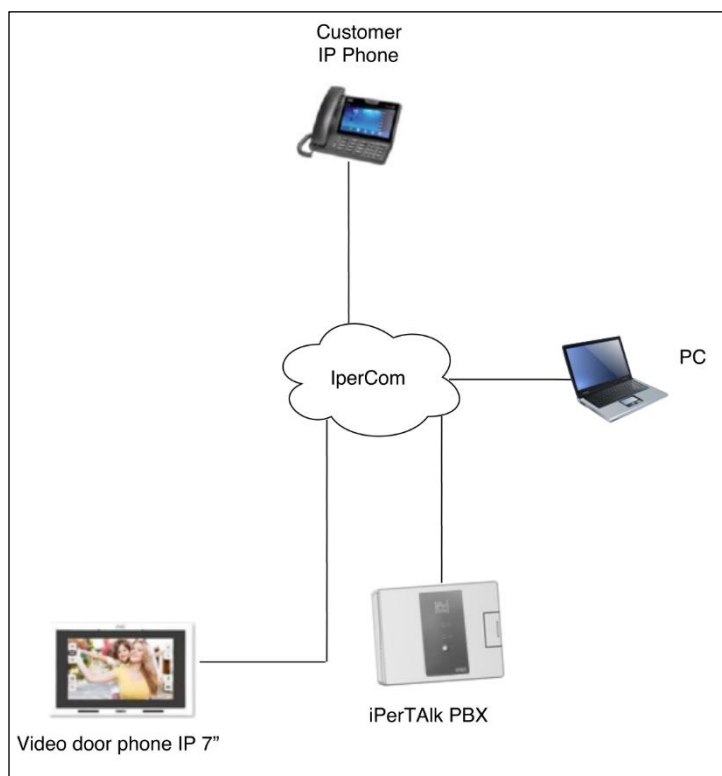


Figure 674: IPerCom connection diagram - iPerTALK without iPerTALK switch Ref. 1375/701

3. Power the system up.
4. Configure the iPerTALK system as follows.
5. Wait until the PBX has started and that the PC has received the IP if a DHCP server is present in the IPerCom system; otherwise, iPerTALK assigns IP address **192.168.56.245** to itself to allow it to be reached from the network.
6. On your PC open the web browser and type in the IP address of *Server iPerTALK V1*.
7. Acquire the phones and assign the numbering (as per IPerCom configuration, for example 90101, 90102, 90103, ...).
8. In the advanced system configurations add an IPerCom type line.
9. Create an inbound routing rule and add the IPerCom line as the destination trunk.
10. Disable the IPerCom network in the system network parameters.
11. Set in "static" mode the WAN configuration of iPerTALK with the IP address suggested by IPerCom.



Information on the specific configurations of the iPerTALK system integrated with the IPerCom system are reported in the iPerTALK [Installation and configuration booklet](#).

### 9.3 Auto-on function on iPerTALK RTSP cameras from IPerCom video door phones

The integration of the IPerCom system with the iPerTALK system allows you to do the auto-on function on iPerTALK RTSP cameras from IPerCom video door phones.

After having correctly configured the IPerCom and iPerTALK systems (as described in the previous paragraphs), the steps below must be followed via the IPerCom *configurator* so that IPerCom video door phones can also perform the auto-on function on RTSP cameras of iPerTALK system.

- 1.A In one of the apartments on “Floor 00” (where, for example, the *iPerTALK Server* is placed), create an iPerTALK apartment, enabling the relevant setting, and enter the internal extension number of the RTSP camera to be called using the “*iPerTALK ID*” parameter:

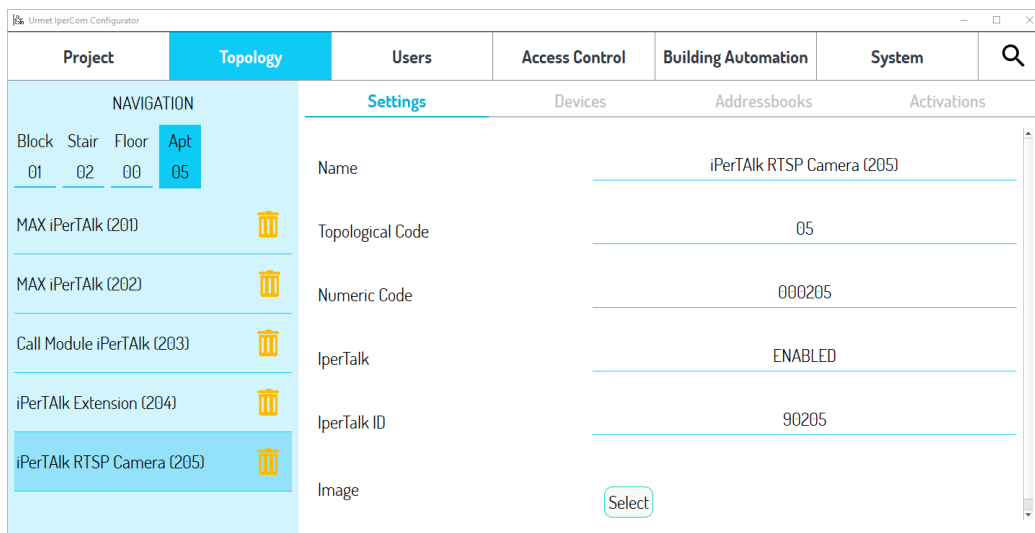


Figure 675: iPerTALK apartment with ID corresponding to an RTSP camera

- 2.A Press the “*Contact*” tab on the *configurator* and, in the *MAX*, *VOG<sup>7</sup>*, *VOG<sup>5+</sup>*, *Basic e IPerCom Client* video door phone directory, add a contact that has the iPerTALK apartment created in the previous step as recipient and in the “*Visibility Filter*” section select “*Video door phone with address book (VDP)*” item (for all the details on the contact creation procedure refer to chapter [Contacts](#)):

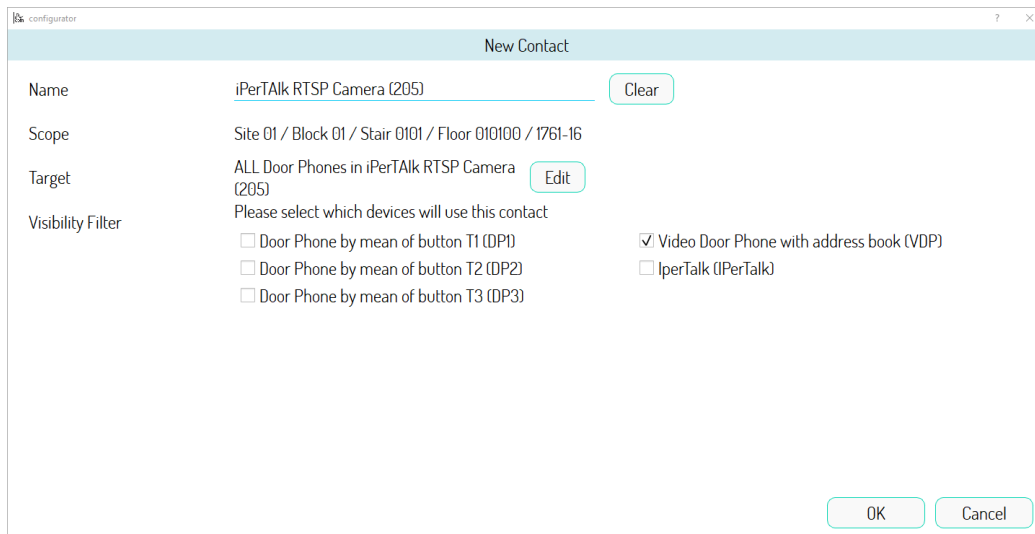


Figure 676: creation of a contact calling the iPerTALK apartment with RTSP camera in the apartment with video door phone 1761/16

2.B Press the “Contact” tab on the *configurator* and, in the VOG<sup>5</sup> video door phone directory, add a contact that has the iPerTALK apartment created in the previous step as recipient, and in the “Visibility Filter” section select the button with which to call the apartment, choosing among T1, T2 or T3 (for all the details on the contact creation procedure, refer to chap. [Contacts](#)):

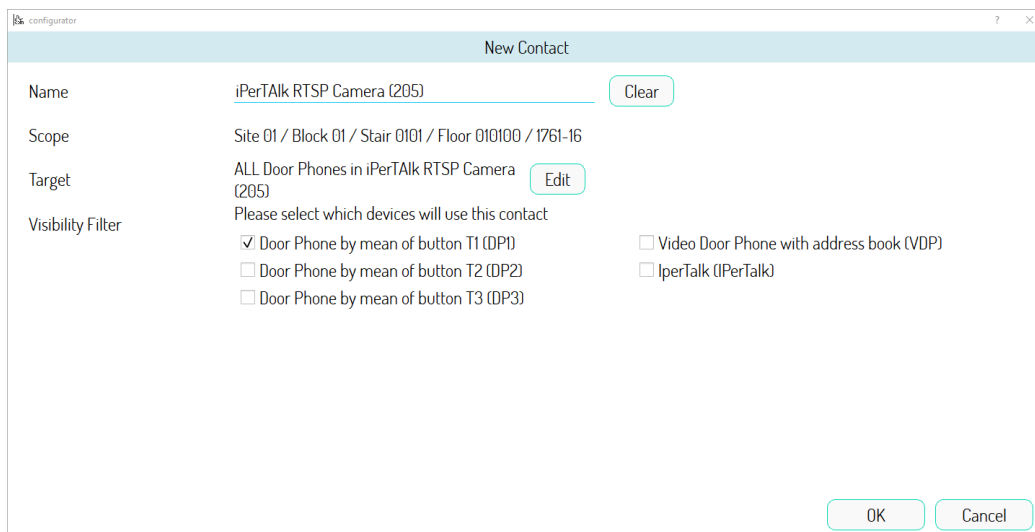


Figure 677: creation of a contact calling the iPerTALK apartment with RTSP camera in the apartment with video door phone 1761/6



The contact with the iPerTALK apartment as recipient can also be a public contact created on the site, block, stair, or floor node. If the MAX, VOG<sup>7</sup>, VOG<sup>5+</sup>, VOG<sup>5</sup>, Basic and IPerCom Client video door phones are part of the respective topology group, both the “Video door phone with address book (VDP)” option and one of the T1, T2 or T3 buttons (or more than one) must be selected.

3. Distribute the configuration on the Ipercom system.

In this way the *MAX*, *VOG<sup>7</sup>*, *VOG<sup>5+</sup>*, *Basic e IPerCom Client* video door phone directories will show the contact (with the same name given during the creation phase) that will enable the auto-on function on the RTSP camera. On the other hand, for the *VOG<sup>5</sup>* video door phone, the T1, T2 or T3 keys will enable the same feature. In both cases the contact must be called as if making an intercom call.

## 10 Restoring the factory settings

If devices are removed from the system or you want to restore the factory settings, it is necessary to make a restore to the factory settings, or easier factory reset.

## 10.1 Factory reset of MAX, VOG<sup>7</sup>, Basic video door phone and IPerCom Client app

To perform the *factory reset* it is first necessary to access the settings menu.

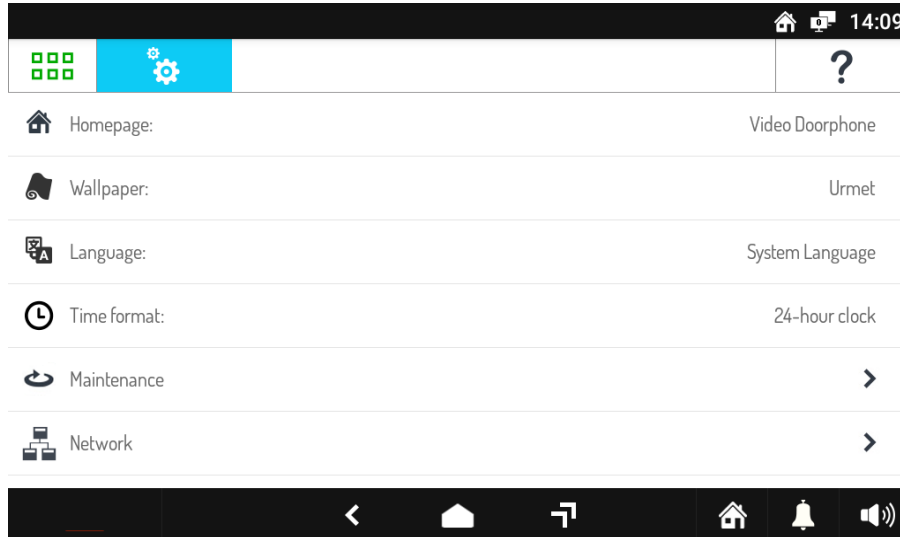


Figure 678: Settings menu

Select the "Maintenance" option, then "Factory Reset". After entering the administrator password (or Urmet password if the system is not locked), the MAX video door phone will start the *factory reset* process and restart.

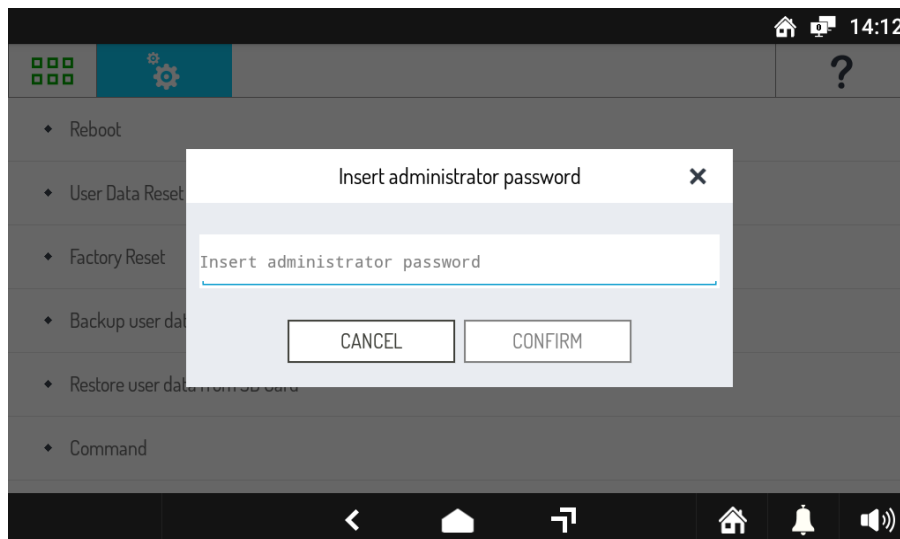





Figure 679: Restoring the factory settings

-  After a factory reset, if the device is connected to a router with a DHCP server and is not configured, the time zone may be different from that expected.
-  The reset to factory settings can be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab)..

## 10.2 Factory reset of video door phone VOG<sup>5+</sup>

To perform a *factory reset* of the VOG<sup>5+</sup> video door phone, access the Homepage by pressing the key twice. The display shows the following screen:

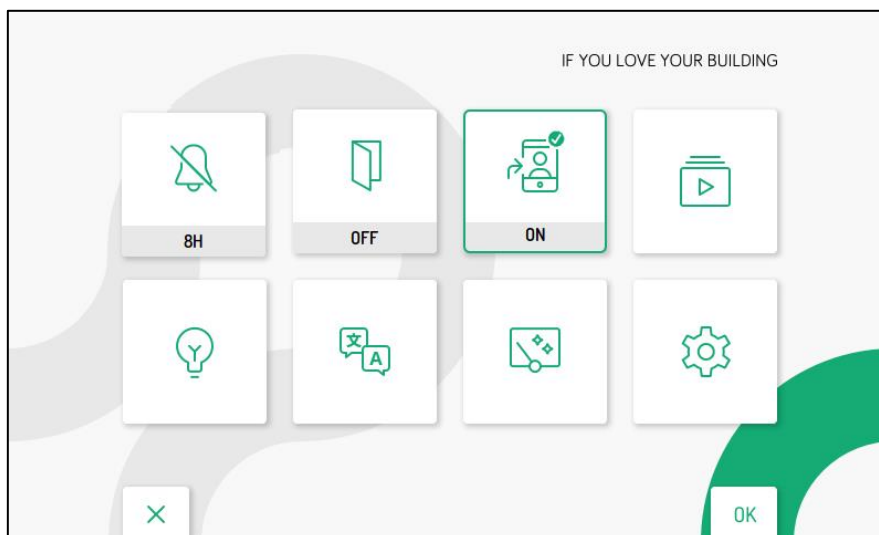


Figure 680: Homepage

Use keys , , , and to select the button and press the key (OK). The following screen is displayed:

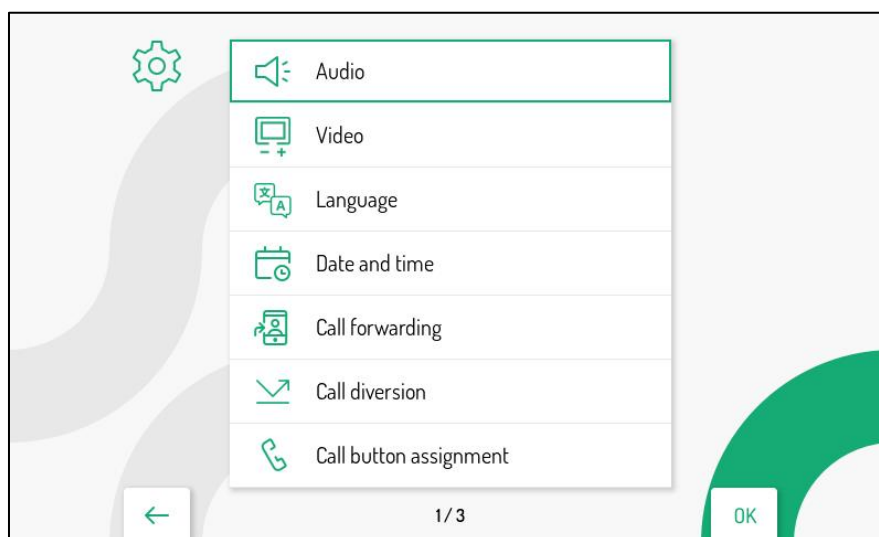


Figure 681: Configuration menu

Use the keys and to select “Reset factory settings”, then press the key (OK). The following screen is displayed:

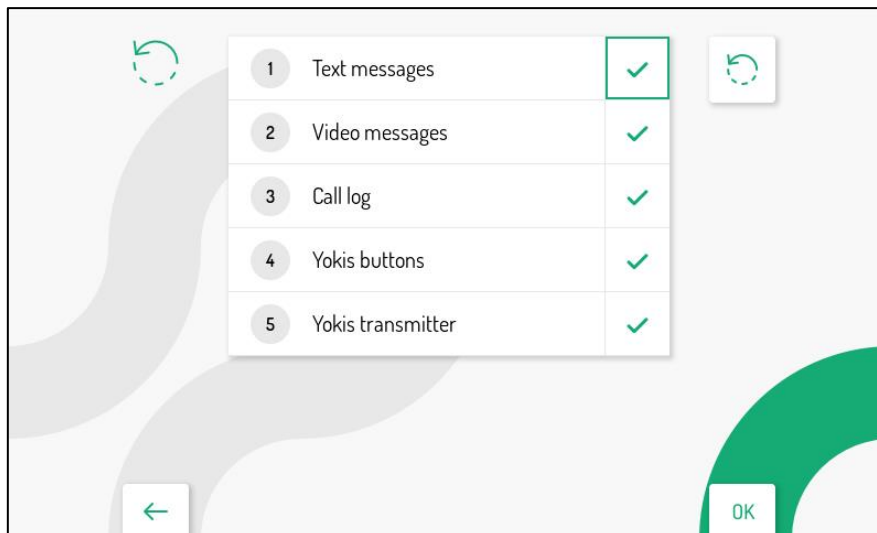


Figure 682: Restoring the factory reset

Press the keys and to select which video door phone parameters you want to reset to factory values. When the selection has been made, press the key (OK) to enable or disable the parameter for reset to factory values. Enabling is confirmed by the presence of the icon  (all video door phone parameters are initially enabled for resetting to factory settings).

Press the key to select the icon , then press the key (OK) to start reset to factory data. The display shows the following screen page:

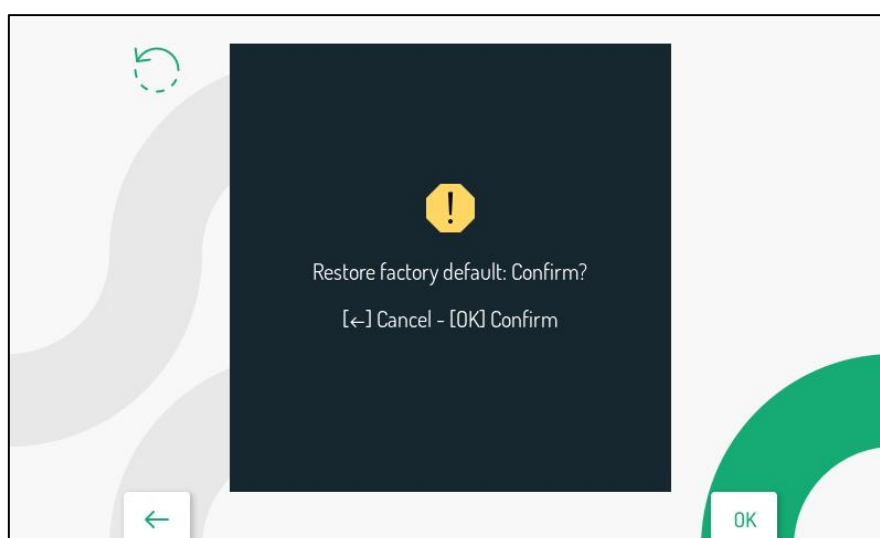


Figure 683: Confirm factory reset

Press the key (OK) to confirm reset to factory values.



### 10.3 Factory reset of video door phone VOG<sup>5</sup>

To perform a *factory reset* of the VOG<sup>5</sup> video door phone, access the configuration menu:

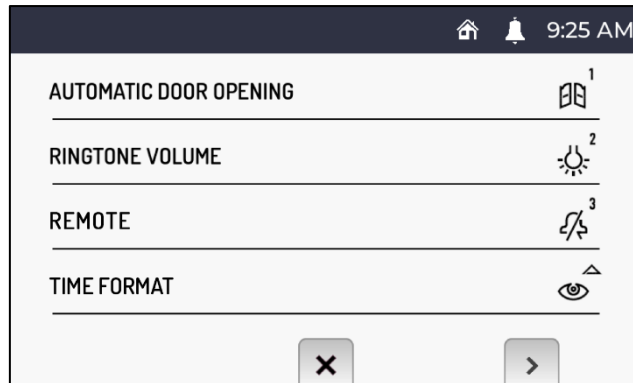


Figure 684: configuration menu - part 1

Press the key  to move to the screen page 2 of the configuration menu:

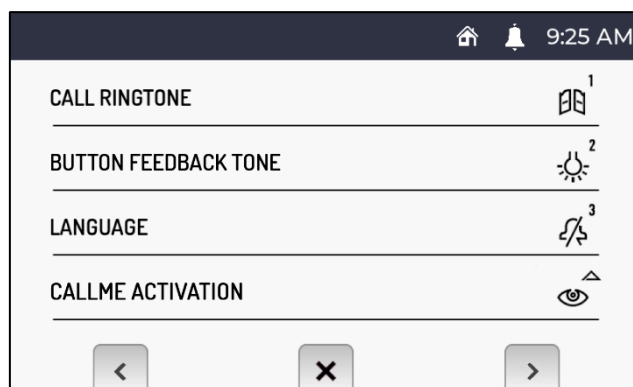



Figure 685: configuration menu - part 2

Press the key  again to move to screen page 3 of the configuration menu:

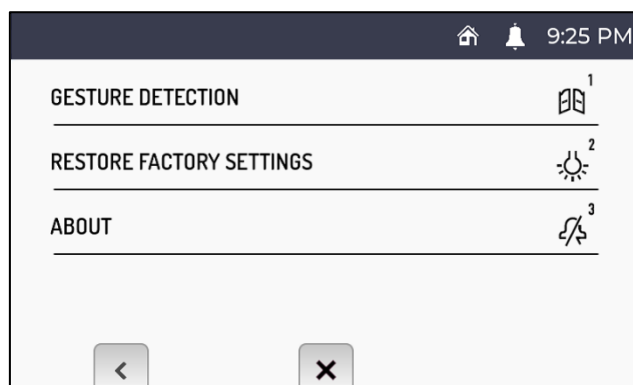


Figure 686: configuration menu - part 3

Press the key 2 in the screen page 3 of the configuration menu. The display shows the following screen:

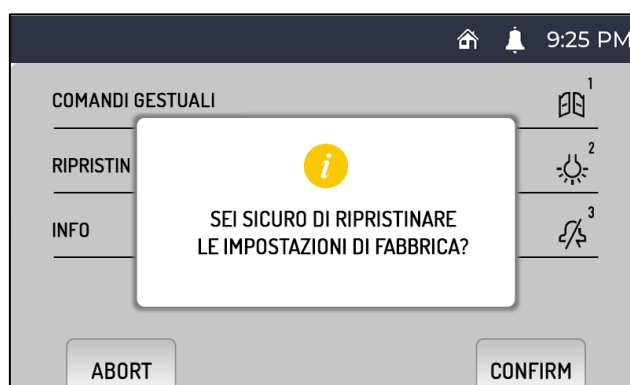




Figure 687: Confirm factory reset

Press the key  to confirm the reset to factory settings of the device.

 The reset to factory settings can be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab).

## 10.4 Factory reset of Door Phones Miro





To restore default parameters of a Miro door phone after entering programming mode, hold button T1 pressed for longer than 5 seconds, hold buttons  and  pressed for longer than 5 seconds. The device will generate 2 long beeps and reboot.



Figure 688: Miro door phone

 The reset to factory settings can be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab).

## 10.5 Factory reset of Call Modules 1060/12-13-17-18-23

The *factory reset* of the *Call Modules* can be carried out in two different steps:

1. during device startup
2. when the device is started and configured



Figure 689: Call Module

In the first case, during the start-up phase, the following screen is shown for five seconds:

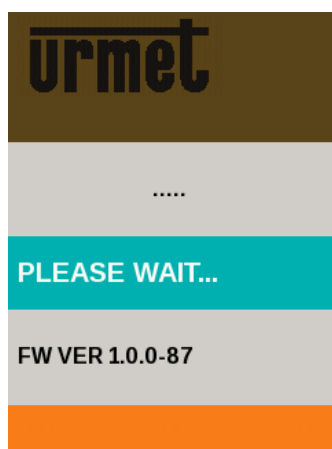


Figure 690: Call Module start screen

If during this time the buttons "X" and "0" are pressed several times in succession, the device will restart and perform a *factory reset*.

In the second case it is assumed to have a configured *Call Module* already started, as shown in the figure:



Figure 691: Main screen of a configured Call Module

In this case, press the "0" button twice in rapid succession. A screen will be shown where you can enter the administrator password (if the system is blocked, otherwise you need to enter the Urmnet password).



Figure 692: Entering the Urmnet or administrator password

Once the password has been entered and the "OK" button pressed, a screen opens where to select "CALL MODULE": press "OK" again to access the following *Call Module* maintenance menu.



Figure 693: Call Module maintenance menu

By selecting "RESET ALL SETTINGS" and pressing the "OK" button, you will be asked to confirm the action.

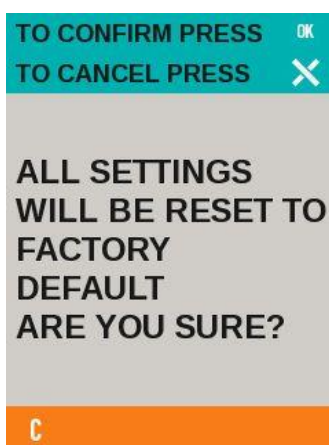




Figure 694: Factory reset confirmation screen

Press the "OK" button for the last time to start the factory reset procedure: the device will restart to complete the operation.

 The reset to factory settings can be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab).

## 10.6 Factory reset of the Modular Entry Panel with 1060/48

The *factory reset* of the *Modular Entry Panel with 1060/48* can be done via the *Outdoor Audio and Video IP Station 1060/48* or via the *Display Module 1168/1* (below):



Figure 695: Audio Video IP outdoor station (on the left) and Display Module (on the right)

### 10.6.1 Factory reset via the Outdoor Audio and Video IP Station 1060/48

There are 3 ways to perform a *factory reset* and they are listed below.

#### *Mode 1: factory reset with reset button (Modular Entry Panel with 1060/48 ON)*

Press the "RESET" button placed on the back of the *Outdoor Audio and Video IP Station 1060/48* 5 times within 10 seconds (indicated in the figure with the red arrow). Each time the button is pressed feedback tone is sent: the button must be pressed again immediately after the feedback tone. If the procedure has been carried out correctly, the orange LEDs on the front panel will flash quickly for 6 times. After about 1 minute, the white LEDs illuminating name tags and buttons start flashing: this means that the *factory reset* operation has been carried out correctly.

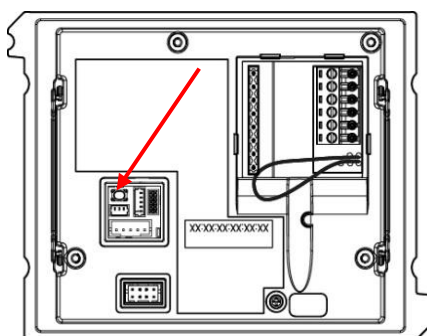


Figure 696: rear view of Outdoor Audio and Video IP Station 1060/48

*Mode 2: factory reset with call button (Modular Entry Panel with 1060/48 OFF)*

Press the call button on the right (indicated in the figure with the red circle) of the *Outdoor Audio and Video IP Station 1060/48*, turn on the device by continuing to hold down the relevant button until the orange LEDs begin to flash 6 times. You can now release the call button. After about 1 minute, the white LEDs illuminating name tags and buttons start flashing: this means that the *factory reset* operation has been carried out correctly.



Figure 697: front view of *Outdoor Audio and Video IP Station 1060/48*

*Mode 3: factory reset with call button and entrance hall button (Modular Entry Panel with 1060/48 ON)*

Press the call button on the right of the *Outdoor Audio and Video IP Station 1060/48* (the same as in the previous mode) and at the same time the entrance hall button (for about 20s) until the orange LEDs start flashing 6 times. You can now release the call button and the entrance hall button. After about 1 minute, the white LEDs illuminating name tags and buttons start flashing: this means that the *factory reset* operation has been carried out correctly.



## 10.6.2 Factory reset via the Display Module 1168/1

There are 2 ways to perform a *factory reset* and they are listed below.

### *Mode 1: press the X-9 buttons (Modular Entry Panel with 1060/48 ON)*

Quickly press the X-9 buttons in sequence using the *Numeric Keypad Module 1168/46*. The *Display Module 1168/1* shows a screen page where it is necessary to enter the Urmet or system administrator password (depending on whether the system is unlocked or locked). Once the correct password has been entered, confirm by pressing the soft-touch button at the green check mark. At this point, press the soft-touch button in correspondence of the *trash* icon and confirm always with the green check mark: the orange LEDs of the *Outdoor Audio and Video IP Station 1060/48* start flashing 6 times. The *Display Module 1168/1* will show the *Factory Reset* indication at the beginning of the procedure and after about 1 minute the *Not Configured* indication (at the end of the procedure). At the end of the procedure, the white LEDs illuminating the name tags and buttons of *Outdoor Audio and Video IP Station 1060/48* start flashing.

### *Mode 2: press the soft-touch buttons (Modular Entry Panel with 1060/48 OFF)*

Switch on the *Modular Entry Panel with 1060/48* and wait for the *Display Module 1168/1* to show the following screen page:

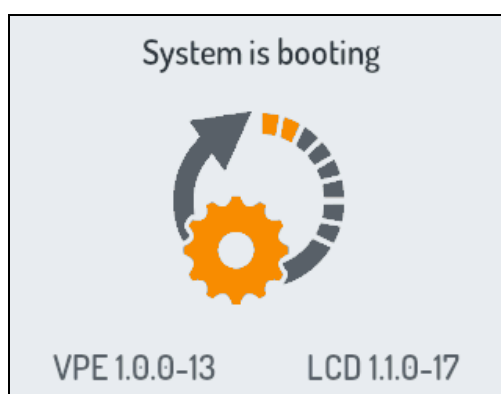




Figure 698: reset screen

Within 5 seconds, press the soft-touch buttons in the following sequence: 2-4-1-3 (button numbering starts from the leftmost button). The orange LEDs of the *Outdoor Audio and Video IP Station 1060/48* start flashing 6 times. The *Display Module 1168/1* will show the *Factory Reset* indication at the beginning of the procedure and after about 1 minute the *Not Configured* indication (at the end of the procedure). At the end of the procedure, the white LEDs illuminating the name tags and buttons of *Outdoor Audio and Video IP Station 1060/48* start flashing.

 Besides the 5 modes described above, the reset to factory settings can always be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab).



## 10.7 Factory reset of the Entry panels 1060/71-/74-75-78

To perform a *factory reset* of a *Door Speaker Unit*, press the entrance hall button and at the same time the second button of the keypad (the lowest button) for 20 seconds.



Figure 699: Entry panels

After 20 seconds, the device emits a beep before restarting; then release both buttons: the device will start the *factory reset* procedure and reboot.



 The reset to factory settings can be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab).

## 10.8 Factory reset of IPerCom 2Voice Gateway



Figure 700: IperCom 2Voice Gateway 1083/59

To perform a *factory reset* on a gateway, press the Reset button five times in a row (less than 1s in between). The device will be reset to default parameters; all configurations will be lost. Hold same button pressed for more than 10 seconds to make an hardware reboot the device. For more details, refer to the device installation manual at [www.urmet.com](http://www.urmet.com)

 The reset to factory settings can be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab).

## 10.9 Factory reset of the lift interface 1060/37



Figure 701: Lift interface 1060/37

To perform the *factory reset* of the lift interface, press the Reset button for 5 times in a row (with intervals of less than 1s). The device resets to factory parameters and loses all the configurations made. The same button briefly pressed 1 time reboots the device hardware. For more details, refer to the installation manual of the device available at [www.urmet.com](http://www.urmet.com).

## 10.10 Factory reset of the Entry panel 1060/33-34





Figure 702: Entry panel 1060/33 (on the left) and 1060/34 (on the right)

To perform the *factory reset* of the *Entry panel* Ref. 1060/33-34 carry out the following operations in sequence:

- switch the device off;
- for the *Entry panel* 1060/33: press and hold the first call key (the top key) and the hall key;
- for the *Entry panel* 1060/34: press and hold the “up arrow” key and the hall key;
- switch the device on;
- do not release the keys until the device performs the following steps in sequence:
  - 8 flashes in sequence of the key LEDs,
  - camera LEDs turning on and off,
  - flashes in sequence of the key LEDs,
  - camera LEDs turning on and off.

Now, you can release the 2 keys and the factory reset function is implemented and the device reboots.

 The reset to factory settings can be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab).

## 10.11 Factory reset of Entry Panel 1060/21



Figure 703: Entry Panel 1060/21



To perform a *factory reset* on an *Entry Panel* Ref. 1060/21, the following operations must be carried out in sequence:

- Switch the device off.
- Press and hold the call key and the hall key.
- Turn on the device.
- Do not release the two buttons for at least 25 seconds.

During this -time, the following events can be observed in sequence on the device:

- The camera LEDs will switch on and off.
- The LED tags will flash 8 times.
- The camera LEDs will switch on and off again.

The two buttons can now be released. After two seconds, factory reset is performed and the device restarts.

 *The reset to factory settings can be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab).*

## 10.12 Factory reset of Floor Entry Panel 1060/22



Figure 704: Floor Entry Panel 1060/22



To perform a *factory reset* on a *Floor Entry Panel* Ref. 1060/22, the following operations must be carried out in sequence:

- Switch the device off.
- Hold the call button pressed.
- Turn on the device.
- Do not release the buttons for at least 25 seconds.

During this time, the following events can be observed in sequence on the device:

- The camera LEDs will switch on and off.
- The LED tags will flash 8 times.
- The camera LEDs will switch on and off again.

The buttons can now be released. After two seconds, factory reset is performed and the device restarts.

 *The reset to factory settings can be carried out also via the Ipercom Installer Tools application (button  of the Diagnostic tab).*

## APPENDIX A: Configuration parameters of IPerCom devices

### Server 1060/1

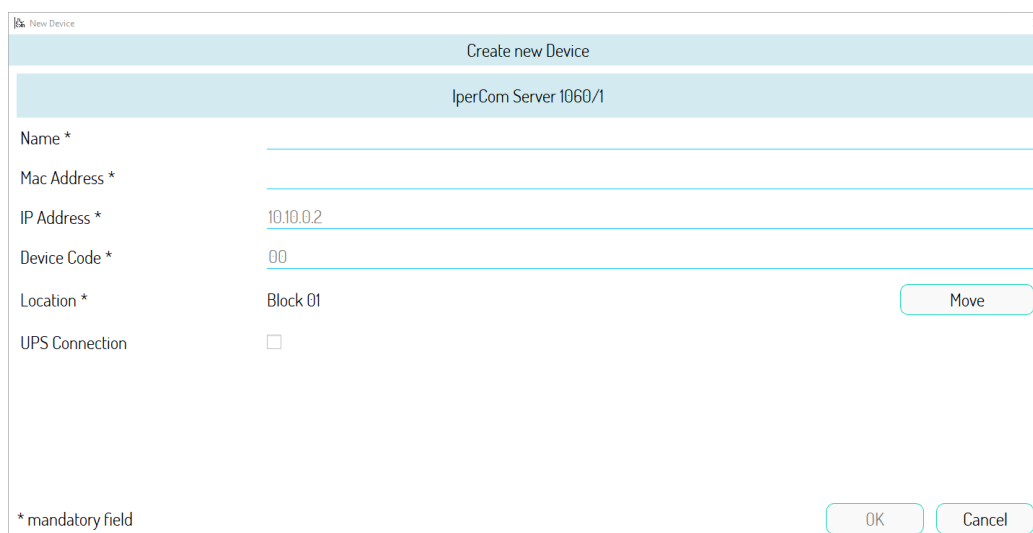


Figure 705: Server 1060/1 settings

The following table shows the meaning of the fields for Server 1060/1.

<b>Name</b>	Name to assign to the Server.
<b>MAC Address</b>	MAC address associated with the Server.
<b>IP Address</b>	IP address associated with the Server. Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<b>Device Code</b>	Value not editable.
<b>Location</b>	Position in the system topology: it is possible to move the device to another topological node by pressing the "Move" button.
<b>UPS connection (uninterruptible power supply)</b>	If selected, the server through the <i>Maintenance</i> tab of <i>IPerCom Installer Tools</i> can give several information about the UPS parameters, including the battery charge level. Default value: not selected. The connection between UPS and Server is made via the USB port of the server.

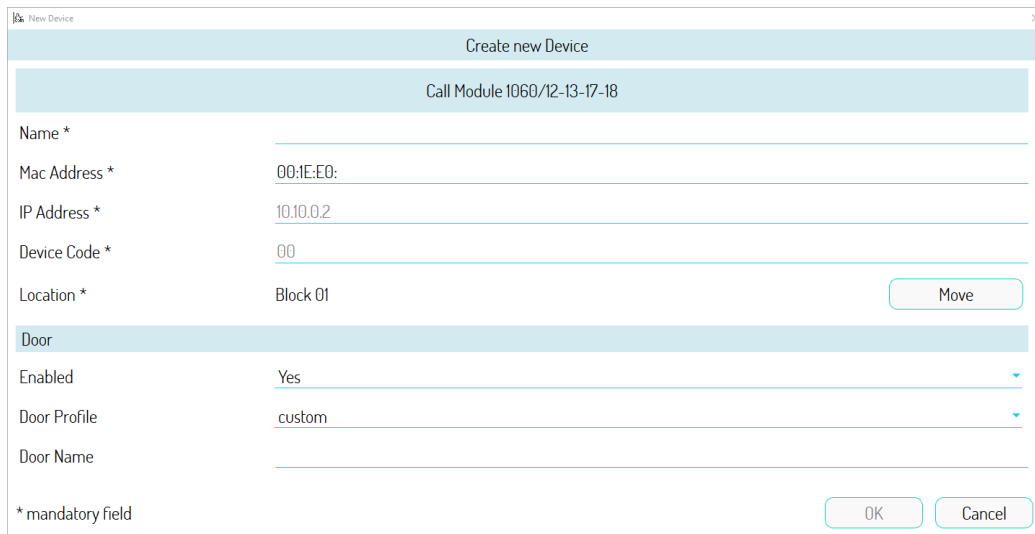
Table 24: general settings



It is highly recommended to connect a UPS (Uninterruptible Power Supply) to the IPerCom Server from the first power up to avoid irreparable damage caused by possible voltage drops or sudden power failures. The UPS models currently supported are the BK350EI/BK500EI/BK650EI. The information is managed through one of the 3 USB ports of the Server itself.



## Call Module 1060/12-13-17-18



**Create new Device**

Call Module 1060/12-13-17-18

Name \* \_\_\_\_\_

Mac Address \* 00:1E:E0: \_\_\_\_\_

IP Address \* 10.10.0.2 \_\_\_\_\_

Device Code \* 00 \_\_\_\_\_

Location \* Block 01 Move

**Door**

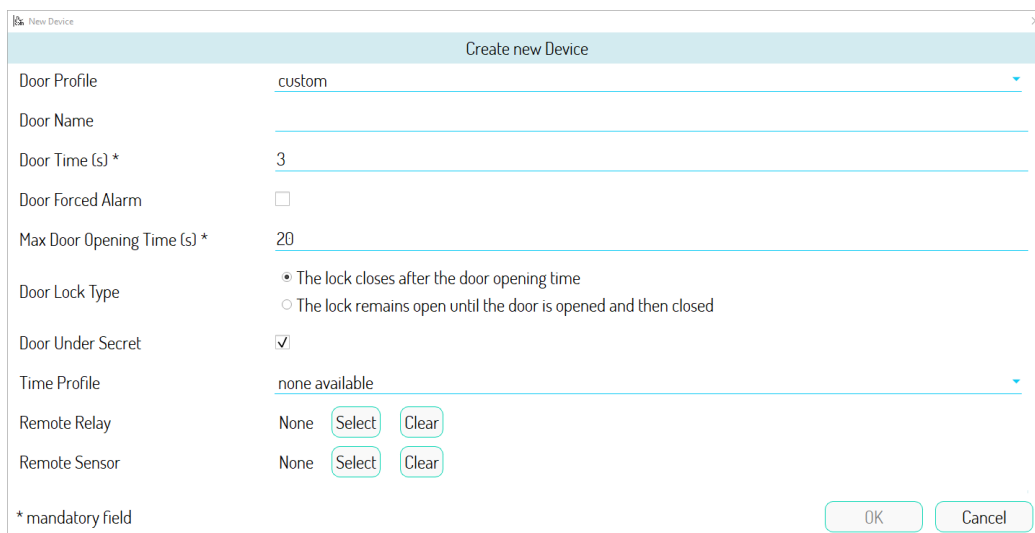
Enabled Yes ▼

Door Profile custom ▼

Door Name \_\_\_\_\_

\* mandatory field OK Cancel

Figure 706: Call Module 1060/12-13-17-18 settings (part 1)



**Create new Device**

Door Profile custom ▼

Door Name \_\_\_\_\_

Door Time (s) \* 3 \_\_\_\_\_

Door Forced Alarm

Max Door Opening Time (s) \* 20 \_\_\_\_\_

Door Lock Type

- The lock closes after the door opening time
- The lock remains open until the door is opened and then closed

Door Under Secret

Time Profile none available ▼

Remote Relay None Select Clear

Remote Sensor None Select Clear

\* mandatory field OK Cancel

Figure 707: Call Module 1060/12-13-17-18 settings (part 2)

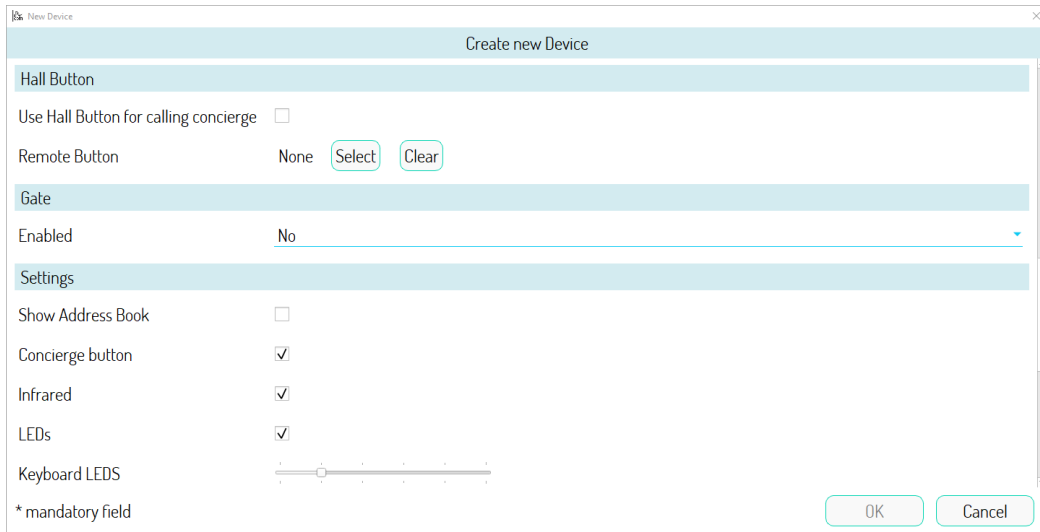


Figure 708: Call Module 1060/12-13-17-18 settings (part 3)

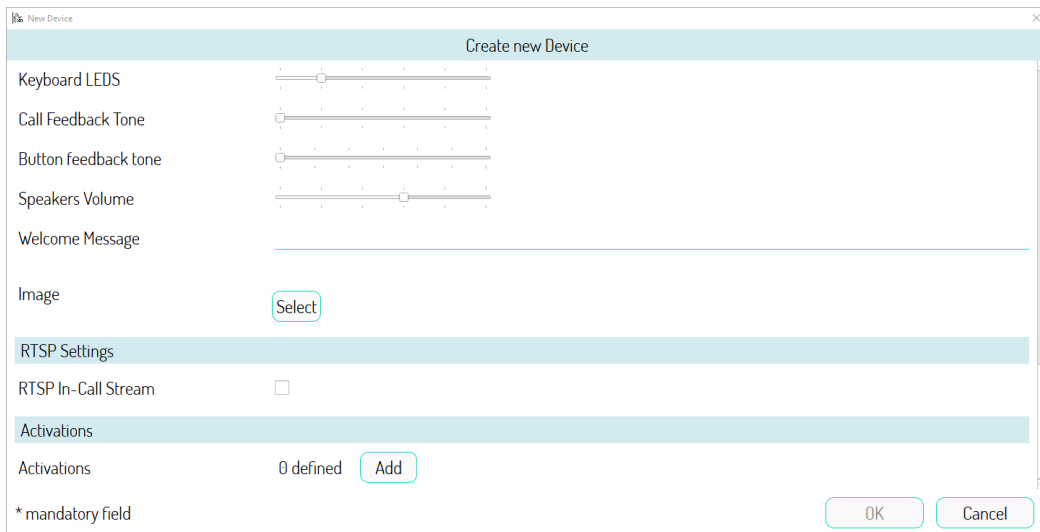


Figure 709: Call Module 1060/12-13-17-18 settings (part 4)

The following table shows the meaning of the fields for *Call Module* 1060/12-13-17-18.

<b>General Settings</b>	
<i>Name</i>	Name to assign to <i>Call Module</i> .
<i>MAC Address</i>	MAC address associated to the <i>Call Module</i> .
<i>IP Address</i>	IP address associated to the <i>Call Module</i> . Field visible only if manual network configuration is set in system parameters. Value cannot be changed.
<i>Device code</i>	Value that cannot be changed.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node by pressing the “ <i>Move</i> ” button.

*Table 25: general settings*

<b>Main Door settings</b>	
<i>Enabled</i>	The item <i>Yes</i> enables the main door: in this case the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the main door. Default value: <i>Yes</i> .
<i>Door Profile (#)</i>	This allows you to associate a previously created door profile with the concerned main door. In this case, the door parameters are automatically compiled (besides the name). Default setting: <i>Custom</i> (parameters must be compiled manually).
<i>Door Name (#)</i>	Name to assign to the main door.
<i>Door Time (s) (#)</i>	Pulse duration on the control relay. Default value: 3s.
<i>Door Forced Alarm (#)</i>	If selected, if the door is forced, the current event sends an alarm to the <i>Switchboard</i> .
<i>Max Door Opening Time (s) (#)</i>	If selected, if the accessed is forced, the concerned event sends an alarm to the <i>Switchboard</i> .
<i>Door Lock Type (#)</i>	It allows you to choose the type of lock installed on the main door (see note reported below).
<i>Door Under Secret (#)</i>	If selected, by pressing the door opener button (from an indoor station) it is possible to activate the electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the door can also be opened outside call mode from the apartments the topological path of which intercepts the <i>Call Module</i> . Default setting: selected.
<i>Time Profile (#)</i>	This allows you to associate a temporal profile to the main door. Access will be valid only within the selected time profile (except for residents of apartments whose topological path intercepts the <i>Call Module</i> ). Default setting: <i>none</i> .
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the main door of the <i>Call module</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .
<i>Remote Sensor (#)</i>	It allows you to remotely control the sensor that signals that main door has been left open. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 26: main door settings

Hall Button Settings	
<i>Use Hall Button for calling concierge</i>	If selected, it allows you to use the hall button to call the competence switchboard or switchboards of the system.
<i>Remote Button (#)</i>	It allows you to remotely control the entrance hall button that opens the main door of the <i>Call Module</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 27: hall button settings

Gate settings	
<i>Used</i>	<p>The item <i>Yes</i> enables the gate: in this case the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the gate.</p> <p>The <i>Relay Actuator</i> item allows you to use the gate relay output as the output (only in monostable mode) of a <i>Relay Actuator</i>: in this case the item marked with the symbol (\$) appears. For further details see the section <a href="#">Gate contact used as output of a Relay Actuator</a>.</p> <p>Default value: <i>No</i>.</p>
<i>Gate Profile (#)</i>	This allows you to associate a previously created access profile to the concerned gate. In this case, the gate parameters are automatically compiled (besides the name). Default setting: <i>Custom</i> (parameters must be compiled manually).
<i>Gate Name (#)</i>	Name to assign to the gate.
<i>Gate Time (s) (#) (\$)</i>	Pulse duration on the control relay. Default value: 3s. Allowed values: from 1s to 90s.
<i>Gate Under Secret (#)</i>	If selected, by pressing the gate button (from an indoor station) it is possible to activate electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the gate can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.
<i>Time Profile (#)</i>	This allows you to associate a temporal profile to the gate access. Access will be valid only within the selected time profile (except for residents of apartments whose topological path intercepts the <i>Call Module</i> ). Default setting: <i>none</i> .
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the gate of the <i>Call Module</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button</a> .


Table 28: gate settings

<b>End-user settings</b>	
<i>Show Address Book</i>	The item appears only if the call addressing mode is “ <i>Block Mode</i> ” and if the device is placed on a node other than the “ <i>Site</i> ” node. In this case, if the item is selected, the address book is shown on the call module; if the item is not selected, the address book does not appear. In the first case it will be possible to call the apartments via address book and numeric code, in the second case only via numeric code. Default value: unchecked.
<i>Switchboard Button</i>	Enable button to call to the respective <i>Switchboard</i> .
<i>Infrared</i>	Enabling of user presence competence through integrated infrared sensor.
<i>LEDs</i>	Enabling of the camera LED.
<i>Keyboard LEDs</i>	Enabling the keypad backlighting.
<i>Call Feedback Tone</i>	Call feedback setting.
<i>Button Feedback Tone</i>	Setting of audio feedback on buttons.
<i>Speakers Volume</i>	Loudspeaker volume setting
<i>Welcome Message</i>	This allows you to set a welcome message on the <i>Call Module</i> display. Some special characters (e.g. "emojicons") may not be displayed correctly, so we recommend that you check that the message is displayed correctly. Maximum length of the message: 64 characters.

Table 29: end-user settings

<b>RTSP In-Call stream settings</b>	
<i>RTSP In-Call stream</i>	If selected, the <i>Switchboard</i> application can display the RTSP video stream of the calling station during the call to an apartment station or during the auto-on from an apartment station. Fields marked with the hash mark (#) must be filled correctly.
<i>IP Address (#)</i>	IP address of calling station camera.
<i>Network mask (#)</i>	Subnet mask of RTSP cameras (including calling station camera).
<i>Port</i>	RTSP video stream port. Value not editable.
<i>Stream</i>	Name of the RTSP video stream. Value not editable.
<i>User Name (#)</i>	Username to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>Password (#)</i>	Password to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>Streaming URI</i>	Full URI of the RTSP video stream. Value not editable. It is built automatically by filling in the fields above respecting the following syntax: rtsp://[<username>:<password>@] <IP address>:<port>/<stream>


Table 30: RTSP streaming setting


 There are two types of electric locks on the market: with automatic rearm or without automatic rearm.

Installing a type of lock with automatic rearm and sending a door opening command, the door remains open only for the time established in the configurator ("Door Time (s)" parameter). After that time the lock rearms and the door is closed. In this case the option "The lock closes after the door opening time" must be chosen. In this context mounting a sensor on the door, a door left open alarm will be sent to the video door phones and switchboards only if the door remains opened (sensor) beyond the time set on configurator ("Max door opening time (s)" parameter).

On the other hand, installing a type of lock without automatic rearm and sending a door opening command, the door remains open until the door is opened and closed again. In this case the option "The lock remains open until the door is opened and closed" must be chosen. In this situation, by installing a sensor on the door, a door open alarm will be sent to the video door phones and switchboard if, after the door open command has been given, the door is not opened and closed within the time set on the configurator ("Max door opening time (s)" parameter).


The above also applies to the other calling stations that have this option.


 In the RTSP streaming settings to set the IP address it is recommended to follow what is reported in [APPENDIX F1: How to use customized network settings in IperCom system](#).

 It is possible to configure any Urmet NVR device to record calls made via Call Module 1060/12-13-17-18 and related auto-on activated by video door phone. In [APPENDIX M1: Streaming video from IperCom calling stations to NVR Urmet](#) the configuration procedure of the 1098/328P Urmet NVR device is shown. For the configurations of the other Urmet NVR devices contact the Urmet Service Centre.

The "Add" button in the "Activations" section has already been described in paragraph [Activations](#).

The "Select" button in the "Images" section allows loading a welcome image on the calling station display. Supported file formats include the most common ones like jpg, bmp and png. We recommend uploading images with an aspect ratio of 200x58 pixels: this way the image will not be cropped. Once an image is uploaded, you can delete it using the "Delete" button.

 The welcome image disappears if an apartment is called for which (in the configurator) a help image on how to reach it has been uploaded (see section [Call addressing mode](#)). This image is only replaced by the welcome image during the call phase (forwarding and answering). At the end of the call, the welcome image is displayed again.

 The address book of the Call Module is automatically created by importing the residents (set as visible) of all apartments in the topology group of the Call Module itself.

## Call Module 1060/23

The screenshot shows a 'Create new Device' dialog box with the following fields and values:

- Name \***: Call Module 1060/23
- Mac Address \***: 00:1E:E0:
- IP Address \***: 10.10.0.2
- Device Code \***: 00
- Location \***: Block 01 (with a 'Move' button)
- Door** section:
  - Enabled**: Yes
  - Door Profile**: custom
  - Door Name**: (empty)

\* mandatory field

Buttons: OK, Cancel

Figure 710: Call Module 1060/23 settings (part 1)

The screenshot shows the continuation of the 'Create new Device' dialog box with the following fields and values:

- Door Profile**: custom
- Door Name**: (empty)
- Door Time (s) \***: 3
- Door Forced Alarm**:
- Max Door Opening Time (s) \***: 20
- Door Lock Type**:
  - The lock closes after the door opening time
  - The lock remains open until the door is opened and then closed
- Door Under Secret**:
- Time Profile**: none available
- Remote Relay**: None (with 'Select' and 'Clear' buttons)
- Remote Sensor**: None (with 'Select' and 'Clear' buttons)

\* mandatory field

Buttons: OK, Cancel

Figure 711: Call Module 1060/23 settings (part 2)



**Create new Device**

**Hall Button**

Use Hall Button for calling concierge

Remote Button      None    **Select**    **Clear**

**Gate**

Enabled              No

**Settings**

Show Address Book     

Concierge button       

Infrared               

LEDs                    

Keyboard LEDS        

\* mandatory field

**OK**    **Cancel**

Figure 712: Call Module 1060/23 settings (part 3)

**Create new Device**

Keyboard LEDS        

Call Feedback Tone   

Button feedback tone  

Speakers Volume      

Welcome Message      \_\_\_\_\_

Image                    **Select**

**RTSP Settings**

RTSP In-Call Stream   

**Activations**

Activations            0 defined    **Add**

\* mandatory field

**OK**    **Cancel**

Figure 713: Call Module 1060/23 settings (part 4)

The following table shows the meaning of the fields for *Call Module 1060/23*.

<b>General settings</b>	
<i>Name</i>	Name to assign to <i>Call Module</i> .
<i>MAC Address</i>	MAC address associated with the <i>Call Module</i> .
<i>IP Address</i>	IP address associated with the <i>Call Module</i> . Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<i>Device Code</i>	Value not editable.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node by pressing the “ <i>Move</i> ” button.

*Table 31: general settings*

<b>Main door settings</b>	
<i>Used</i>	In this case, the item <i>Yes</i> enables the main door: the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the main door. Default value: <i>Yes</i> .
<i>Door Profile (#)</i>	It allows you to associate a previously created access profile to the main door in question. In this case the door parameters are automatically filled in (except the name). Default value: <i>customised</i> (the parameters must be filled in manually).
<i>Main Door Name (#)</i>	Name to assign to the main door.
<i>Door opening time (s) (#)</i>	Pulse duration on the control relay. Default value: 3 s.
<i>Door forced alarm (#)</i>	If selected, if the door is forced, the current event sends an alarm to the <i>Switchboard</i> .
<i>Max Door Opening Time (s) (#)</i>	Maximum door opening time beyond which a warning of opened door is sent to the <i>Switchboard</i> .
<i>Lock type (#)</i>	It allows you to choose the type of lock installed on the main door (see note at the end of the configuration section of the <a href="#">Call Module 1060/12-13-17-18</a> )
<i>Door under secret (#)</i>	If selected, by pressing the door opener button (from an indoor station) it is possible to activate the electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the door can also be opened outside the call phase only from all the apartments where the topological path detects the calling station. Default value: selected.
<i>Time profile (#)</i>	It allows you to associate a time profile to the main door. Access will be valid only within the selected time profile (except for the residents of the apartments whose topological path detects the calling station). Default value: <i>none</i> .
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the main door of the calling station. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .
<i>Remote Sensor (#)</i>	It allows you to remotely control the sensor that signals that main door has been left open. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 32: main door settings

Hall Button Settings	
<i>Use Hall Button for calling concierge</i>	If selected, it allows you to use the hall button to call the competence switchboard or switchboards of the system.
<i>Remote Button (#)</i>	It allows you to remotely control the entrance hall button that opens the main door of the <i>Call Module</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 33: hall button settings

Gate settings	
<i>Used</i>	<p>The item <i>Yes</i> enables the gate: in this case the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the gate. The <i>Relay Actuator</i> item allows you to use the gate relay output as the output (only in monostable mode) of a <i>Relay Actuator</i>: in this case the item marked with the symbol (\$) appears. For further details see the section <a href="#">Gate contact used as output of a Relay Actuator</a>. Default value: <i>No</i>.</p>
<i>Gate Profile (#)</i>	It allows you to associate a previously created access profile to the gate in question. In this case the gate parameters are automatically filled in (except the name). Default value: <i>customised</i> (the parameters must be filled in manually).
<i>Gate name (#)</i>	Name to assign to the gate.
<i>Gate Opening Time (s) (#) (\$)</i>	Pulse duration on the control relay. Default value: 3s. Allowed values: from 1s to 90s.
<i>Gate under secret (#)</i>	If selected, by pressing the gate button (from an indoor station) it is possible to activate electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the gate can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.
<i>Time profile (#)</i>	It allows you to associate a time profile to the gate. Access will be valid only within the selected time profile (except for the residents of the apartments whose topological path detects the calling station). Default value: <i>none</i> .
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the gate opener of the calling station. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button</a> .



Table 34: gate settings

<b>End user settings</b>	
<i>Show Address Book</i>	The item appears only if the call addressing mode is “ <i>Block Mode</i> ” and if the device is placed on a node other than the “ <i>Site</i> ” node. In this case, if the item is selected, the address book is shown on the call module; if the item is not selected, the address book does not appear. In the first case it will be possible to call the apartments via address book and numeric code, in the second case only via numeric code. Default value: unchecked.
<i>Switchboard Button</i>	Enabling of the button for the call to the relevant <i>Switchboard</i> .
<i>Infrared</i>	Enabling of user presence detection through integrated infrared sensor.
<i>LEDs</i>	Enabling of the camera LED.
<i>Keyboard LEDs</i>	Enabling the button backlighting.
<i>Call Feedback Tone</i>	Call feedback setting.
<i>Button Feedback Tone</i>	Setting of audio feedback on buttons.
<i>Loudspeaker Volume</i>	Loudspeaker volume setting
<i>Welcome Message</i>	It allows to set a welcome message on the calling station display. Some special characters (e.g. "emoticons") may not be displayed correctly: it is therefore advisable to check that the message is displayed correctly. Maximum message length: 64 characters.

Table 35: end user settings



<b>RTSP In-Call stream settings</b>	
<i>RTSP In-Call stream</i>	If selected, the <i>Switchboard</i> application can display the RTSP video stream of the calling station during the call to an apartment station or during the auto-on from an apartment station. Fields marked with the hash mark (#) must be filled correctly.
<i>IP Address (#)</i>	IP address of calling station camera.
<i>Network mask (#)</i>	Subnet mask of RTSP cameras (including calling station camera).
<i>Port</i>	RTSP video stream port. Value not editable.
<i>Stream</i>	Name of the RTSP video stream. Value not editable.
<i>User Name (#)</i>	Username to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>Password (#)</i>	Password to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>URI for Streaming</i>	Full URI of the RTSP video stream. Value not editable. It is built automatically by filling in the fields above respecting the following syntax: <code>rtsp://[&lt;username&gt;:&lt;password&gt;@] &lt;IP address&gt;:&lt;port&gt;/&lt;stream&gt;</code>

Table 36: RTSP streaming settings

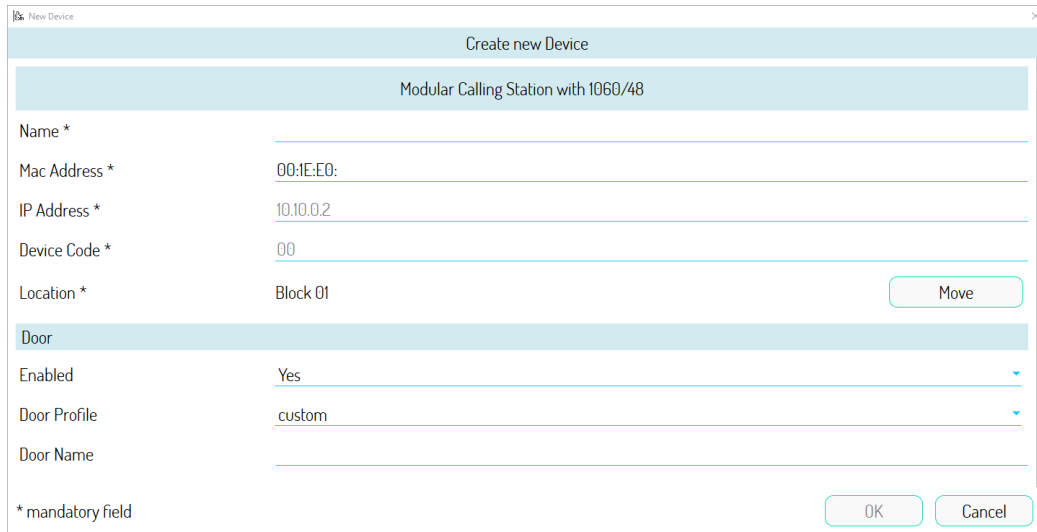
-  In the RTSP streaming settings to set the IP address it is recommended to follow what is reported in [APPENDIX F1: How to use customized network settings in IperCom system](#).
-  It is possible to configure any Urmet NVR device to record calls made via Call Module 1060/23 and related auto-on activated by video door phone. In [APPENDIX M1: Streaming video from IperCom calling stations to NVR Urmet](#) the configuration procedure of the **1098/328P** Urmet NVR device is shown. For the configurations of the other Urmet NVR devices contact the Urmet Service Centre.

The "Add" button in the "Activations" section has already been described in paragraph [Activations](#).

The "Select" button in the "Images" section allows loading a welcome image on the calling station display. Supported file formats include also the most common ones like jpg, bmp and png. We recommend uploading images with an aspect ratio of 200x58 pixels: this way the image will not be cropped. Once an image is uploaded, you can delete it using the "Delete" button.

-  The welcome image disappears if an apartment is called for which (in the configurator) a help image on how to reach it has been uploaded (see section [Call addressing mode](#)). This image is only replaced by the welcome image during the call phase (forwarding and answering). At the end of the call, the welcome image is displayed again.
-  The address book of the Call Module is automatically created by importing the residents (set as visible) of all apartments in the topology group of the Call Module itself.

## Modular Calling Station with 1060/48



**Create new Device**

Modular Calling Station with 1060/48

Name \*

Mac Address \* 00:1E:E0:

IP Address \* 10.10.0.2

Device Code \* 00

Location \* Block 01 Move

**Door**

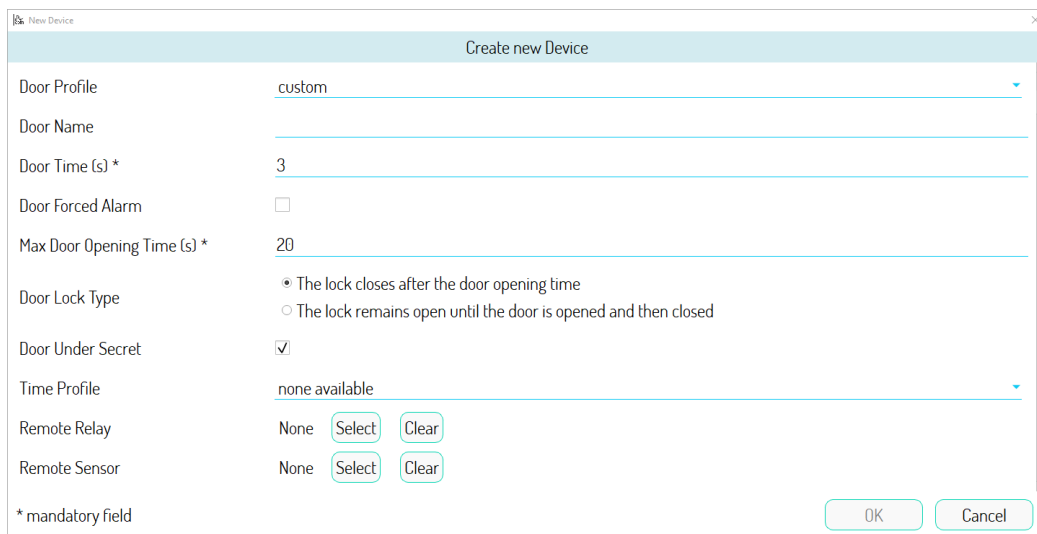
Enabled Yes

Door Profile custom

Door Name

\* mandatory field OK Cancel

Figure 714: Modular Calling Station with 1060/48 settings (part 1)



**Create new Device**

Door Profile custom

Door Name

Door Time (s) \* 3

Door Forced Alarm

Max Door Opening Time (s) \* 20

Door Lock Type

- The lock closes after the door opening time
- The lock remains open until the door is opened and then closed

Door Under Secret

Time Profile none available

Remote Relay None Select Clear

Remote Sensor None Select Clear

\* mandatory field OK Cancel

Figure 715: Modular Calling Station with 1060/48 settings (part 2)

**Create new Device**

**Hall Button**

Use Hall Button for calling concierge

Remote Button    None       

**Gate**

Enabled    No

**Settings**

Embedded Call Buttons     Call buttons disabled  
 Right call button enabled  
 Right and Left call buttons enabled

Camera LEDES   

Welcome Message

\* mandatory field       

Figure 716: Modular Calling Station with 1060/48 settings (part 3)

**Create new Device**

Camera LEDES   

Welcome Message

Call Feedback     Vocal Messages  
 Feedback Tones  
 None

Light Sensor   

Screen Saver Mode    Continuous run

Module Settings     Numeric Keyboard  
 Alphabetic Keyboard  
 ILA  
 LCD  
 Key Reader

\* mandatory field       

Figure 717: Modular Calling Station with 1060/48 settings (part 4)

**Create new Device**

Available	Used
Activations by code	Call from addressbook
	Call by manual code
	Door opening
	Call to competence switchboards

LCD menu items

\* mandatory field       

Figure 718: Modular Calling Station with 1060/48 settings (part 5)



New Device ×

Create new Device

---

RTSP Settings

RTSP In-Call Stream

---

Activations

Activations 0 defined Add

---

Call Buttons

all apartments - inverted topological order Populate Clear

Position	B	S	F	A	D	Type	Description	Edit	Delete
Left									
Right									

\* mandatory field OK Cancel

Figure 719: Modular Calling Station with 1060/48 settings (part 6)

New Device ×

Create new Device

---

Call Buttons

all apartments - inverted topological order Populate Clear

Position	B	S	F	A	D	Type	Description	Edit	Delete
Left									
Right									
1									
2									
3									

\* mandatory field OK Cancel

Figure 720: Modular Calling Station with 1060/48 settings (part 7)

The following table shows the meaning of the fields for *Modular entry panel with 1060/48*.

<b>General settings</b>	
<i>Name</i>	Name to assign to the calling station.
<i>MAC Address</i>	MAC address associated with the calling station.
<i>IP Address</i>	IP address associated with the calling station. Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<i>Device Code</i>	Value not editable.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node by pressing the "Move" button.

*Table 37: general settings*

<b>Main door settings</b>	
<i>Used</i>	The item <i>Yes</i> enables the main door: in this case the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the main door. Default value: <i>Yes</i> .
<i>Door Profile (#)</i>	It allows you to associate a previously created access profile to the main door in question. In this case the door parameters are automatically filled in (except the name). Default value: <i>customised</i> (the parameters must be filled in manually).
<i>Main Door Name (#)</i>	Name to given to the main door.
<i>Door Opening Time (s) (#)</i>	Pulse duration on the control relay. Default value: 3 s.
<i>Door Forced Alarm (#)</i>	If selected, if the door is forced, the current event sends an alarm to the <i>Switchboard</i> .
<i>Max Door Opening Time (s) (#)</i>	Maximum door opening time beyond which a warning of opened door is sent to the <i>Switchboard</i> . Default value: 60s.
<i>Lock type (#)</i>	It allows you to choose the type of lock installed on the main door (see note at the end of the configuration section of the <a href="#">Call Module 1060/12-13-17-18</a> ).
<i>Door Under Secret (#)</i>	If selected, by pressing the door opener button (from an indoor station) it is possible to activate the electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the door can also be opened outside the call phase from all the apartments where the topological path detects the <i>External unit</i> . Default value: selected.
<i>Time Profile (#)</i>	It allows you to associate a time profile to the main door. Access will be valid only within the selected time profile (except for the residents of the apartments whose topological path detects the <i>Call Module</i> ). Default value: <i>none</i> .
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the main door of the external unit. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .
<i>Remote Sensor (#)</i>	It allows you to remotely control the sensor that signals that main door has been left open. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 38: main door settings

Hall Button Settings	
<i>Use Hall Button for calling concierge</i>	If selected, it allows you to use the hall button to call the competence switchboard or switchboards of the system.
<i>Remote Button (#)</i>	It allows you to remotely control the entrance hall button that opens the main door of the <i>Call Module</i> . For further details, see paragraph <a href="#"><u>Remote relay functions, remote entrance hall button and remote sensor.</u></a>

Table 39: hall button settings

<b>Gate settings</b>	
<i>Used</i>	<p>The item <i>Yes</i> enables the gate: the following options are shown, marked with a hash mark (#).</p> <p>The item <i>No</i> disables the gate.</p> <p>The item “<i>By door opening</i>” allows you to use the relay contact of the driveway to open the main door.</p> <p>The <i>Relay Actuator</i> item allows you to use the gate relay output as the output (only in monostable mode) of a <i>Relay Actuator</i>: in this case the item marked with the symbol (§) appears. For further details see the section <a href="#">Gate contact used as output of a Relay Actuator</a>.</p> <p>Default value: <i>No</i>.</p>
<i>Gate Profile (#)</i>	<p>It allows you to associate a previously created access profile to the gate in question. In this case the door parameters of gate are automatically filled in (except the name). Default value: <i>customised</i> (the parameters must be filled in manually).</p>
<i>Gate Name (#)</i>	<p>Name to assign to the gate.</p>
<i>Gate Opening Time (s) (#) (§)</i>	<p>Pulse duration on the control relay. Default value: 3s. Allowed values: from 1s to 90s.</p>
<i>Gate Under Secret (#)</i>	<p>If selected, by pressing the gate button (from an indoor station) it is possible to activate electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the gate can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.</p>
<i>Time profile (#)</i>	<p>It allows you to associate a time profile to the gate. Access will be valid only within the selected time profile (except for the residents of the apartments whose topological path detects the <i>Call Module</i>). Default value: <i>none</i>.</p>
<i>Remote Relay (#)</i>	<p>It allows you to remotely control the relay that operates the gate opener of the External unit. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button</a>. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button</a>.</p>

Table 40: gate settings

<b>End user settings</b>	
<i>Integrated call buttons</i>	The 2 calling station buttons can be enabled or disabled as shown below: -) both disabled, -) only right call button enabled, -) both enabled.
<i>Camera LEDs</i>	Enabling of the camera LEDs. Default value: <i>selected</i> .
<i>Welcome Message</i>	It allows you to enter a text message that will be displayed on the display module 1168/1 in case of configuration as Alpha call module.
<i>Call Feedback</i>	This allows you to set call feedback via vocal message/sound feedback or to set no call feedback mode (default).
<i>Voice synthesis module</i>	It allows you to set up call feedback via voice message or audible feedback. Default value: <i>selected</i> .
<i>Twilight sensor</i>	It allows you to enable or disable the twilight sensor present on the module. Default value: <i>not selected</i> .
<i>Screen Saver operating mode</i>	It allows you to enable and configure a screen saver on the <i>Display Module</i> 1168/1 when in stand-by mode. Use modes are: -) OFF (screen saver disabled), -) alternating between home page and screen saver, -) continuous operation.
<i>Module configuration</i>	It allows you to select and enable the various modules that make up the calling station: -) <i>Numeric Keypad Module</i> 1168/46, -) <i>Alphabetic Keypad Module</i> 1168/49, -) <i>ILA Voice Synthesis Module</i> 1168/48, -) <i>Display Module</i> 1168/1, -) <i>Proximity key reader</i> 1168/45.
<i>LCD menu items</i>	It allows you to select which items will be displayed on the <i>Display Module</i> 1168/1: -) call from address book, -) call through manual code, -) door/gate opening, -) activation through code, -) call to the switchboards concerned, -) empty line.

Table 41: end user settings

<b>RTSP In-Call stream settings</b>	
<i>RTSP In-Call stream</i>	If selected, the <i>Switchboard</i> application can display the RTSP video stream of the calling station during the call to an apartment station or during the auto-on from an apartment station. Fields marked with the hash mark (#) must be filled correctly.
<i>IP Address (#)</i>	IP address of calling station camera.
<i>Network mask (#)</i>	Subnet mask of RTSP cameras (including calling station camera).
<i>Port</i>	RTSP video stream port. Value not editable.
<i>Stream</i>	Name of the RTSP video stream. Value not editable.
<i>User Name (#)</i>	User name to access the calling station RTSP video stream from the <i>Switchboard</i>
<i>Password (#)</i>	Password to access the calling station RTSP video stream from the <i>Switchboard</i> ,
<i>Uri per Io Streaming</i>	Full URI of the RTSP video stream. Value not editable. It is built automatically by filling in the fields above respecting the following syntax: <code>rtsp://[&lt;username&gt;:&lt;password&gt;@] &lt;IP address&gt;:&lt;port&gt;/&lt;stream&gt;</code>

Table 42: RTSP streaming settings



In the RTSP streaming settings to set the IP address it is recommended to follow what is reported in [APPENDIX F1: How to use customized network settings in IperCom system.](#)



It is possible to configure any Urmet NVR device to record calls made via Modular Calling Station with 1060/48 and related auto-on activated by video door phone. In [APPENDIX M1: Streaming video from IPerCom calling stations to NVR Urmet](#) the configuration procedure of the **1098/328P** Urmet NVR device is shown. For the configurations of the other Urmet NVR devices contact the Urmet Service Centre.

The "*Call Buttons*" section allows associating the apartment stations (or the *Switchboards*) to be called to the keys of the *Outdoor Station* by pressing on the icon "*Edit*". The relevant window will open allowing you to:

- set recipient's name and surname (field "*Name*"), which will appear on the outdoor station name tag at the corresponding call key;
- navigate the topological structure of the system and for each topological node choose whether the key should call one or all indoor stations of the topological node or any *Switchboards* ("*Modification*" button).

The "*Delete*" icon allows you to delete the assignment made before.

In the case of installation as modular entry panel it is possible to assign all keys from 1 to 90: in fact, the device has 2 keys (named "*Left*" and "*Right*"), which can be expanded to 88 (for a total of 90) by means of key add-on modules. In case of installation as call module, it is possible to assign only the "*Left*" and "*Right*" keys (for further details see [APPENDIX I: Modular entry panel with 1060/48 Alpha](#)).

The "*Delete*" button allows you to delete the association made for each single button.

The "*Populate*" button allows you to automatically assign all the indoor stations of the apartments of the system to each call key of the *Outdoor Station*. The assignment can take place in 4 ways (as per the relevant drop-down menu:

- all apartments in topological order,
- all apartments in reverse topological order,
- all apartments in alphabetical order,
- all apartments in reverse alphabetical order.

The automatic assignment only concerns apartments in the topological group of the *Outdoor Station*.

In this case, the "*Name*" field, automatically filled in with the name given to the apartment, can be edited using the "*Modification*" button.

The "*Clean*" button allows you to delete the assignment previously made.

The "*Add*" button in the "*Activations*" section has already been described in paragraph [Activations](#).



*The address book of the Call Module is automatically created by importing the residents (set as visible) of all apartments in the topology group of the Call Module itself.*



## Entry Panel 1060/71-74-75-/78

**Create new Device**

Entry Panel 1060/71-74-75-78

Name \*

Mac Address \* 00:1E:E0:

IP Address \* 10.10.0.2

Device Code \* 00

Location \* Block 01 Move

**Door**

Enabled Yes

Door Profile custom

Door Name

\* mandatory field OK Cancel

Figure 721: Entry Panel 1060/71-74-75-78 settings (part 1)

**Create new Device**

Door Time (s) \* 3

Door Forced Alarm

Max Door Opening Time (s) \* 20

Door Lock Type   
 The lock closes after the door opening time   
 The lock remains open until the door is opened and then closed

Door Under Secret

Remote Relay None Select Clear

Remote Sensor None Select Clear

**Hall Button**

Remote Button None Select Clear

\* mandatory field OK Cancel

Figure 722: Entry Panel 1060/71-74-75-78 settings (part 2)

**Create new Device**

**Gate**

Enabled No

---

**Settings**

Button feedback tone [Slider]

Call Feedback Tone [Slider]

Speakers Volume [Slider]

Camera LEDs

Model 1060/71

---

**Activations**

Activations 0 defined Add

\* mandatory field

OK Cancel

Figure 723: Entry Panel 1060/71-74-75-78 settings (part 3)

**Create new Device**

**RTSP Settings**

RTSP In-Call Stream

---

**Call Buttons (at least one entry required)**

all apartments - inverted topological order Populate Clear

Position	B	S	F	A	D	Type	Description	Edit	Delete
1									
2									
3									
4									

\* mandatory field

OK Cancel

Figure 724: Entry Panel 1060/71-74-75-78 settings (part 4)

**Create new Device**

29	
30	
31	
32	
33	
34	

\* mandatory field

OK Cancel

Figure 725: Entry Panel 1060/71-74-75-78 settings (part 5)

The following table shows the meaning of the fields for *Entry Panel 1060/71-74-75-/78*.

<b>General settings</b>	
<i>Name</i>	Name to assign to the <i>Entry Panel</i> .
<i>MAC Address</i>	MAC address associated with the <i>Entry Panel</i> .
<i>IP Address</i>	IP address associated with the <i>Entry Panel</i> . Field visible only if manual network configuration is set in system parameters. Value cannot be changed.
<i>Device Code</i>	Value cannot be changed.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node by pressing the "Move" button.

*Table 43: general settings*

<b>Main door settings</b>	
<i>Used</i>	In this case, the item <i>Yes</i> enables the main door: the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the main door. Default value: <i>Yes</i> .
<i>Door Profile (#)</i>	This allows you to associate a previously created door profile with the concerned main door. In this case, the door parameters are automatically compiled (besides the name). Default setting: <i>Custom</i> (parameters must be compiled manually).
<i>Door Name (#)</i>	Name to assign to the main door.
<i>Door Time (s) (#)</i>	Pulse duration on the control relay of the main door. Default value: 3s.
<i>Door Forced Alarm (#)</i>	If selected, if the accessed is forced, the concerned event sends an alarm to the <i>Switchboard</i> .
<i>Max Door Opening Time (s) (#)</i>	The maximum opening time of the door after which an opened door notification is sent to the <i>Switchboard</i> .
<i>Lock type (#)</i>	It allows you to choose the type of lock installed on the main door. See note at the end of the configuration paragraph of the <a href="#">Call Module 1060/12-13-17-18</a> .
<i>Door Under Secret (#)</i>	If selected, by pressing the door opener button (from an indoor station) it is possible to activate the electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the vehicle gate can also be opened outside call mode from the apartments the topological path of which intercepts the <i>Entry Panel</i> . Default value: selected.
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the main door of the <i>Entry panel</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button</a> .
<i>Remote Sensor (#)</i>	It allows you to remotely control the sensor that signals that main door has been left open. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 44: main door settings

Hall Button Settings	
<i>Remote Button (#)</i>	It allows you to remotely control the entrance hall button that opens the main door of the <i>Call Module</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 45: hall button settings

<b>Gate settings</b>	
<i>Used</i>	<p>In this case, the item <i>Yes</i> enables the gate: the following options are shown, marked with a hash mark (#).            The item <i>No</i> disables the gate.            The item “<i>By door opening</i>” allows you to use the relay contact of the gate to open the main door.            The <i>Relay Actuator</i> item allows you to use the gate relay output as the output (only in monostable mode) of a <i>Relay Actuator</i>: in this case the item marked with the symbol (§) appears. For further details see the section <a href="#">Gate contact used as output of a Relay Actuator</a>.            Default value: <i>No</i>.</p>
<i>Gate Profile (#)</i>	This allows you to associate a previously created door profile to the concerned vehicle gate. In this case, the door parameters of the gate are automatically compiled (besides the name). Default setting: <i>Custom</i> (parameters must be compiled manually).
<i>Gate Name (#)</i>	Name to assign to the door.
<i>Gate Opening Time (s) (#) (§)</i>	Pulse duration on the control relay. Default value: 3s. Allowed values: from 1s to 90s.
<i>Gate Under Secret (#)</i>	If selected, by pressing the gate button (from an indoor station) it is possible to activate electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the gate can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the gate of the Entry panel. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button</a> .

Table 46: gate settings

<b>End user settings</b>	
<i>Loudspeakers Volume</i>	Loudspeaker volume setting.
<i>Button feedback tone</i>	Audio feedback volume at button pressure.
<i>Call feedback tone</i>	Feedback volume of forwarded call.
<i>Camera LEDs</i>	Enabling of the camera LEDs.
<i>Model 1060/71</i>	This box must be ticked if you use a calling station with one button.

Table 47: end user settings

<b>RTSP In-Call stream settings</b>	
<i>RTSP In-Call stream</i>	If selected, the <i>Switchboard</i> application can display the RTSP video stream of the calling station during the call to an apartment station or during the auto-on from an apartment station. Fields marked with the hash mark (#) must be filled correctly.
<i>IP Address (#)</i>	IP address of calling station camera
<i>Network mask (#)</i>	Subnet mask of RTSP cameras (including calling station camera).
<i>Port</i>	RTSP video stream port. Value not editable.
<i>Stream</i>	Name of the RTSP video stream. Value not editable
<i>User Name (#)</i>	Username to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>Password (#)</i>	Password to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>URI for Streaming</i>	Full URI of the RTSP video stream. Value not editable. It is built automatically by filling in the fields above respecting the following syntax: <code>rtsp://[&lt;username&gt;:&lt;password&gt;@] &lt;IP address&gt;:&lt;port&gt;/&lt;stream&gt;</code>

Table 48: RTSP streaming settings



In the RTSP streaming settings to set the IP address it is recommended to follow what is reported in [APPENDIX F1: How to use customized network settings in IperCom system.](#)



It is possible to configure any Urmet NVR device to record calls made via Entry Panel 1060/71-74-75-78 and related auto-on activated by video door phone. In [APPENDIX M1: Streaming video from IperCom calling stations to NVR Urmet](#) the configuration procedure of the **1098/328P** Urmet NVR device is shown. For the configurations of the other Urmet NVR devices contact the Urmet Service Centre.

The "*Call Buttons*" section allows associating the indoor stations (or the *Switchboards*) to be called to the keys of the *Outdoor Station* by pressing on the icon "*Edit*". The relevant window will open allowing you to:

- set recipient's name and surname (fields "*Line 1*" and "*Line 2*"), which will appear on the outdoor station name tag at the corresponding call key;
- navigate the topological structure of the system and for each topological node choose whether the key should call one or all indoor stations of the topological node or any *Switchboards* ("*Modification*" button).

The "*Delete*" icon allows you to delete the assignment made before.

In the case of *Entry Panel 1060/74-75-78*, it is possible to associate all buttons from 1 to 34; in fact, the device has 2 buttons as standard, which can be expanded to 32 (for a total of 34) by means of key add-on modules.

In the case of *Entry Panel 1060/71*, (if the relevant option is ticked) key 1 in the list will be disabled: in fact, the device has only one key in the basic version (the second in the list), but it is possible to increase the number of keys by means of the key add-on modules of the *Outdoor Station 1060/74-75* (for a total of 33 keys).

The "*Populate*" button allows you to automatically assign all the indoor stations of the apartments of the system to each key of the *Outdoor Station*. The assignment can take place in 4 ways (as per the relevant drop-down menu):

- in topological order,
- in reverse topological order,
- in alphabetical order,
- in reverse alphabetical order.

The automatic assignment only concerns apartments in the topological group of the *Outdoor Station*. In this case, the "*Name*" field, automatically filled in with the name given to the apartment, can be edited using the "*Modification*" button.

The "*Clean*" button allows you to delete the assignment previously made.

The "*Add*" button in the "*Activations*" section has already been described in paragraph [Activations](#).

## Entry panel 1060/33

**Create new Device**

Entry Panel 1060/33

Name \* \_\_\_\_\_

Mac Address \* 00:1E:E0: \_\_\_\_\_

IP Address \* 10.10.0.2 \_\_\_\_\_

Device Code \* 00 \_\_\_\_\_

Location \* Block 01 Move

**Door**

Enabled Yes ▼

Door Profile custom ▼

Door Name \_\_\_\_\_

\* mandatory field OK Cancel

Figure 726: Entry Panel 1060/33 settings (part 1)

**Create new Device**

Door Time (s) \* 3 \_\_\_\_\_

Door Forced Alarm

Max Door Opening Time (s) \* 20 \_\_\_\_\_

Door Lock Type

- The lock closes after the door opening time
- The lock remains open until the door is opened and then closed

Door Under Secret

Remote Relay None Select Clear

Remote Sensor None Select Clear

**Hall Button**

Remote Button None Select Clear

\* mandatory field OK Cancel

Figure 727: Entry Panel 1060/33 settings (part 2)



New Device x

Create new Device

---

**Gate**

Enabled No

---

**Settings**

Call Feedback 
 Vocal Messages  
 Feedback Tones  
 None

Speakers Volume

Camera LEDES

---

**Activations**

Activations 0 defined Add

\* mandatory field

OK Cancel

Figure 728: Entry Panel 1060/33 settings (part 3)

New Device x

Create new Device

---

**RTSP Settings**

RTSP In-Call Stream

---

Call Buttons (at least one entry required)

all apartments - inverted topological order 
Populate Clear

Position	B	S	F	A	D	Type	Row 1	Row 2	Edit	Delete
1										
2										
3										
4										

\* mandatory field

OK Cancel

Figure 729: Entry Panel 1060/33 settings (part 4)

The following table shows the meaning of the fields for *Entry panel 1060/33*.

<b>General settings</b>	
<i>Name</i>	Name to assign to the <i>Entry Panel</i> .
<i>MAC Address</i>	MAC address associated with the <i>Entry Panel</i> .
<i>IP Address</i>	IP address associated with the <i>Entry Panel</i> . Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<i>Device Code</i>	Value not editable.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node by pressing the "Move" button.

*Table 49: General settings*

<b>Main door settings</b>	
<i>Used</i>	In this case, the item <i>Yes</i> enables the main door: the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the main door. Default value: <i>Yes</i> .
<i>Door Profile (#)</i>	It allows you to associate a previously created access profile to the main door in question. In this case the door parameters are automatically filled in (except the name). Default value: <i>customised</i> (the parameters must be filled in manually).
<i>Main Door Name (#)</i>	Name to assign to the main door.
<i>Door Opening Time (s) (#)</i>	Pulse duration on the control relay. Default value: 3 s.
<i>Door Forced Alarm (#)</i>	If selected, if the door is forced, the current event sends an alarm to the <i>Switchboard</i> .
<i>Max Door Opening Time (s) (#)</i>	Maximum door opening time beyond which a warning of opened door is sent to the <i>Switchboard</i> .
<i>Lock type (#)</i>	It allows you to choose the type of lock installed on the main door (see note at the end of the configuration section of the <a href="#">Call Module 1060/12-13-17-18</a> ).
<i>Door Under Secret (#)</i>	If selected, by pressing the door opener button (from an indoor station) it is possible to activate the electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the door can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the main door of the outdoor station. For further details, see paragraph " <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> ".
<i>Remote Sensor (#)</i>	It allows you to remotely control the sensor that signals that main door has been left open. For further details, see paragraph " <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> ".

Table 50: Main door settings

Hall Button Settings	
<i>Remote Button (#)</i>	It allows you to remotely control the entrance hall button that opens the main door of the <i>Call Module</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 51: Hall button settings

<b>Gate settings</b>	
<i>Used</i>	In this case, the item <i>Yes</i> enables the gate: the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the gate. The item “ <i>By door opening</i> ” allows you to use the relay contact of the gate to open the main door. The <i>Relay Actuator</i> item allows you to use the gate relay output as the output (only in monostable mode) of a <i>Relay Actuator</i> : in this case the item marked with the symbol (\$) appears. For further details see the section <a href="#">Gate contact used as output of a Relay Actuator</a> . Default value: <i>No</i> .
<i>Gate Profile (#)</i>	It allows you to associate a previously created access profile to the gate in question. In this case the gate parameters are automatically filled in (except the name). Default value: <i>customized</i> (the parameters must be filled in manually).
<i>Gate Name (#)</i>	Name to assign to the gate.
<i>Gate Opening Time (s) (#) (\$)</i>	Pulse duration on the control relay. Default value: 3s. Allowed values: from 1s to 90s.
<i>Gate Under Secret (#)</i>	If selected, by pressing the gate button (from an indoor station) it is possible to activate electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the gate can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the gate opener of the outdoor station. For further details, see paragraph “ <a href="#">Remote relay functions, remote entrance hall button</a> ”.

Table 52: Gate settings

<b>End user settings</b>	
<i>Call Feedback</i>	This allows you to set call feedback via vocal message/sound feedback or to set no call feedback mode (default).
<i>Loudspeaker Volume</i>	Loudspeaker volume setting
<i>Camera LEDs</i>	Enabling of the camera LEDs. Default value: <i>selected</i> .

Table 53: End user settings

<b>RTSP In-Call stream settings</b>	
<i>RTSP In-Call stream</i>	If selected, the <i>Switchboard</i> application can display the RTSP video stream of the calling station during the call to an apartment station or during the auto-on from an apartment station. Fields marked with the hash mark (#) must be filled correctly.
<i>IP Address (#)</i>	IP address of calling station camera
<i>Network mask (#)</i>	Subnet mask of RTSP cameras (including calling station camera).
<i>Port</i>	RTSP video stream port. Value not editable.
<i>Stream</i>	Name of the RTSP video stream. Value not editable
<i>User Name (#)</i>	Username to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>Password (#)</i>	Password to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>URI for Streaming</i>	Full URI of the RTSP video stream. Value not editable. It is built automatically by filling in the fields above respecting the following syntax: <code>rtsp://[&lt;username&gt;:&lt;password&gt;@] &lt;IP address&gt;:&lt;port&gt;/&lt;stream&gt;</code>

Table 54: RTSP streaming settings



In the RTSP streaming settings to set the IP address it is recommended to follow what is reported in [APPENDIX F1: How to use customized network settings in IperCom system](#).



It is possible to configure any Urmet NVR device to record calls made via Entry Panel 1060/33 and related auto-on activated by video door phone. In [APPENDIX M1: Streaming video from IPerCom calling stations to NVR Urmet](#) the configuration procedure of the **1098/328P** Urmet NVR device is shown. For the configurations of the other Urmet NVR devices contact the Urmet Service Centre.

The "Add" button in the "Activations" section has already been described in paragraph [Activations](#).

The "Call Keys" section allows associating the indoor stations (or the *Switchboards*) to be called to the 4 keys of the *Outdoor Station* by pressing on the icon "Modification". The relevant window will open allowing you to:

- set recipient's name and surname (fields "Name" and "Name2"), which will appear on the display of the *Outdoor Station* at the corresponding call key;
- navigate the topological structure of the system and for each topological node choose whether the key should call one or all indoor stations of the topological node or any *Switchboards* ("Modification" button).

The "Delete" icon allows you to delete the assignment made before.

The "Populate" button allows you to automatically assign all the indoor stations of the apartments of the system to each call key of the *Outdoor Station*. The assignment can take place in 4 ways (as per the relevant drop-down menu):

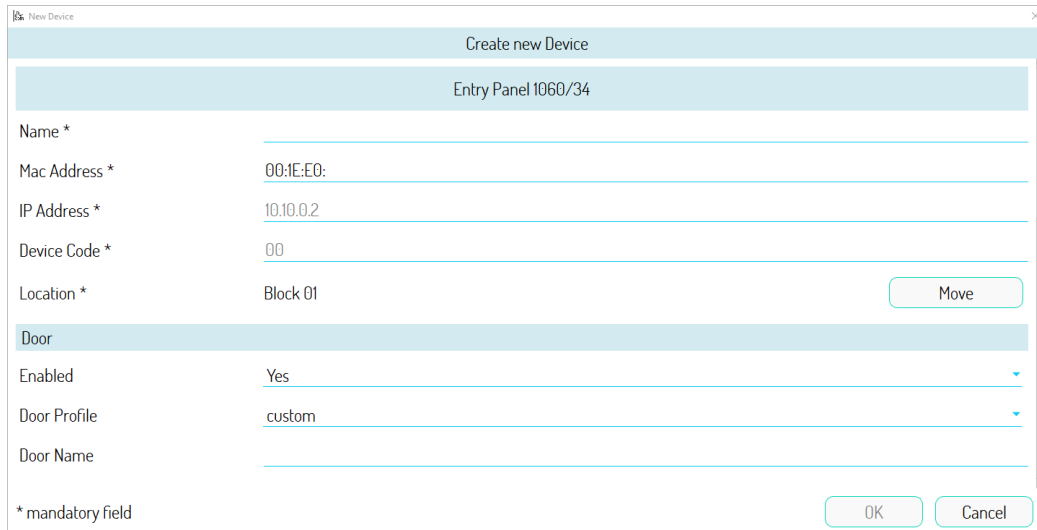
- in topological order,
- in reverse topological order,
- in alphabetical order,
- in reverse alphabetical order.

The automatic assignment only concerns apartments in the topological group of the *Outdoor Station*.

In this case, the "Name" field, automatically filled in with the name given to the apartment, can be edited using the "Modification" button.

The "Clean" button allows you to delete the assignment previously made.

## Entry panel 1060/34



**Create new Device**

Entry Panel 1060/34

Name \*

Mac Address \* 00:1E:E0:

IP Address \* 10.10.0.2

Device Code \* 00

Location \* Block 01 Move

**Door**

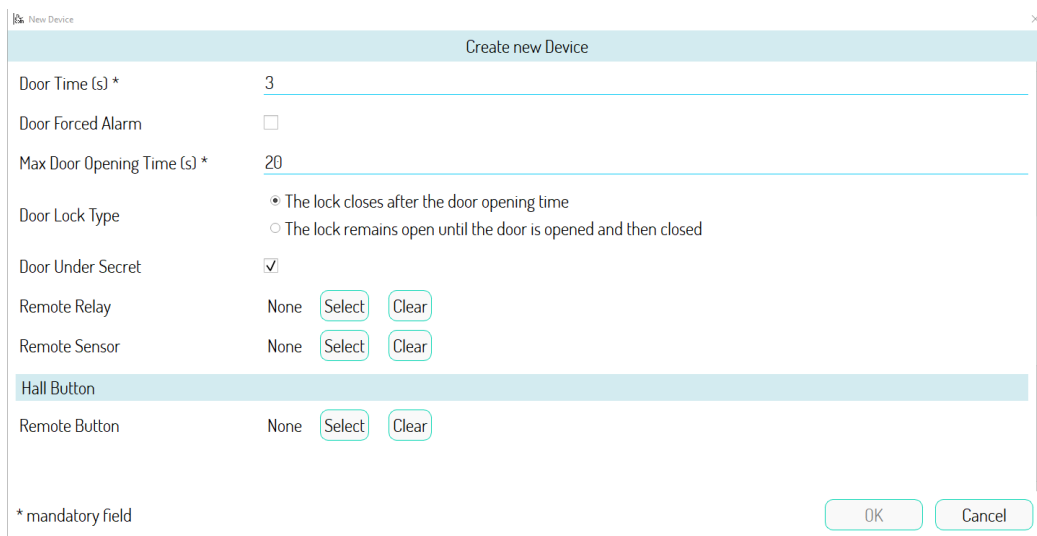
Enabled Yes

Door Profile custom

Door Name

\* mandatory field OK Cancel

Figure 730: Entry Panel 1060/34 settings (part 1)



**Create new Device**

Door Time (s) \* 3

Door Forced Alarm

Max Door Opening Time (s) \* 20

Door Lock Type

- The lock closes after the door opening time
- The lock remains open until the door is opened and then closed

Door Under Secret

Remote Relay None Select Clear

Remote Sensor None Select Clear

**Hall Button**

Remote Button None Select Clear

\* mandatory field OK Cancel

Figure 731: entry panel 1060/34 settings (part 2)

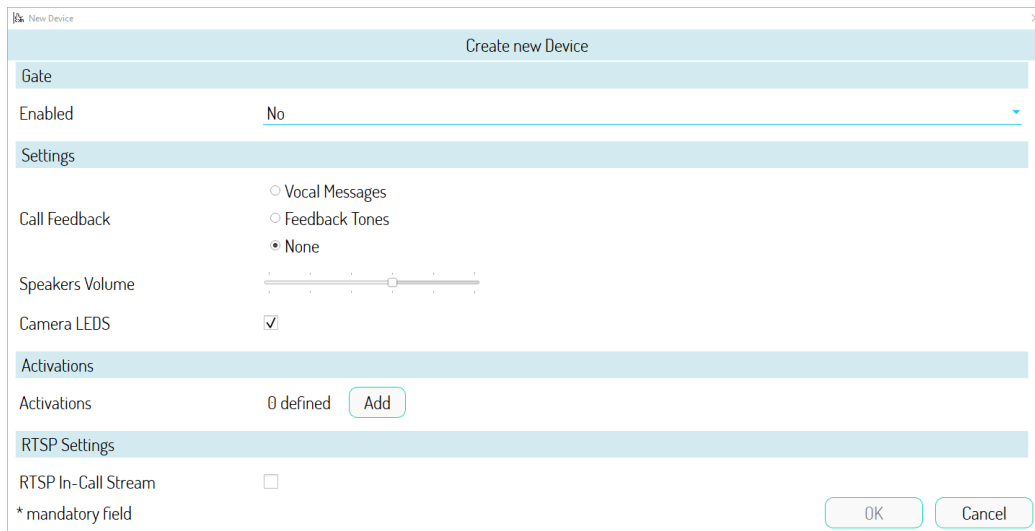


Figure 732: Entry Panel 1060/34 settings (part 3)

The following table shows the meaning of the fields for *Entry Panel 1060/34*.

<b>General settings</b>	
<i>Name</i>	Name to assign to the <i>Entry Panel</i> .
<i>MAC Address</i>	MAC address associated with the <i>Entry Panel</i> .
<i>IP Address</i>	IP address associated with the <i>Entry Panel</i> . Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<i>Device Code</i>	Value not editable.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node by pressing the "Move" button.

Table 55: General settings



<b>Main door settings</b>	
<i>Used</i>	In this case, the item <i>Yes</i> enables the main door: the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the main door. Default value: <i>Yes</i> .
<i>Door Profile (#)</i>	It allows you to associate a previously created access profile to the main door in question. In this case the door parameters are automatically filled in (except the name). Default value: <i>customized</i> (the parameters must be filled in manually).
<i>Main Door Name (#)</i>	Name to assign to the main door.
<i>Door Opening Time (s) (#)</i>	Pulse duration on the control relay. Default value: 3 s.
<i>Door Forced Alarm (#)</i>	If selected, if the door is forced, the current event sends an alarm to the <i>Switchboard</i> .
<i>Max Door Opening Time (s) (#)</i>	Maximum door opening time beyond which a warning of opened door is sent to the <i>Switchboard</i> .
<i>Lock type (#)</i>	It allows you to choose the type of lock installed on the main door (see note at the end of the configuration section of the <a href="#">Call Module 1060/12-13-17-18</a> ).
<i>Door Under Secret (#)</i>	If selected, by pressing the door opener button (from an indoor station), it is possible to activate the electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the door can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the main door of the outdoor station. For further details, see paragraph " <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> ".
<i>Remote Entrance Hall Button (#)</i>	It allows you to remotely control the entrance hall button that opens the main door of the outdoor station. For further details, see paragraph " <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> ".
<i>Remote Sensor (#)</i>	It allows you to remotely control the sensor that signals that main door has been left open. For further details, see paragraph " <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> ".

Table 56: Main door settings

Hall Button Settings	
<i>Remote Button (#)</i>	It allows you to remotely control the entrance hall button that opens the main door of the <i>Call Module</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 57: Hall button settings

Gate settings	
<i>Used</i>	In this case, the item <i>Yes</i> enables the gate: the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the gate. The item “ <i>By door opening</i> ” allows you to use the relay contact of the gate to open the main door. The <i>Relay Actuator</i> item allows you to use the gate relay output as the output (only in monostable mode) of a <i>Relay Actuator</i> : in this case the item marked with the symbol (\$) appears. For further details see the section <a href="#">Gate contact used as output of a Relay Actuator</a> . Default value: <i>No</i> .
<i>Gate Profile (#)</i>	It allows you to associate a previously created access profile to the gate in question. In this case the gate parameters are automatically filled in (except the name). Default value: <i>customised</i> (the parameters must be filled in manually).
<i>Gate Name (#)</i>	Name to assign to the gate.
<i>Gate Opening Time (s) (#) (\$)</i>	Pulse duration on the control relay. Default value: 3s. Allowed values: from 1s to 90s.
<i>Gate Under Secret (#)</i>	If selected, by pressing the gate button (from an indoor station) it is possible to activate electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the gate can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.

Table 58: Gate settings

<b>End user settings</b>	
<i>Call Feedback</i>	This allows you to set call feedback via vocal message/sound feedback or to set no call feedback mode (default).
<i>Loudspeaker Volume</i>	Loudspeaker volume setting.
<i>Camera LEDs</i>	Enabling of the camera LEDs. Default value: <i>selected</i> .

Table 59: End user settings

<b>RTSP In-Call stream settings</b>	
<i>RTSP In-Call stream</i>	If selected, the <i>Switchboard</i> application can display the RTSP video stream of the calling station during the call to an apartment station or during the auto-on from an apartment station. Fields marked with the hash mark (#) must be filled correctly.
<i>IP Address (#)</i>	IP address of calling station camera
<i>Network mask (#)</i>	Subnet mask of RTSP cameras (including calling station camera).
<i>Port</i>	RTSP video stream port. Value not editable.
<i>Stream</i>	Name of the RTSP video stream. Value not editable
<i>User Name (#)</i>	Username to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>Password (#)</i>	Password to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>URI for Streaming</i>	Full URI of the RTSP video stream. Value not editable. It is built automatically by filling in the fields above respecting the following syntax: <code>rtsp://[&lt;username&gt;:&lt;password&gt;@] &lt;IP address&gt;:&lt;port&gt;/&lt;stream&gt;</code>

Table 60: RTSP streaming settings



In the RTSP streaming settings to set the IP address it is recommended to follow what is reported in [APPENDIX F1: How to use customized network settings in IperCom system](#).



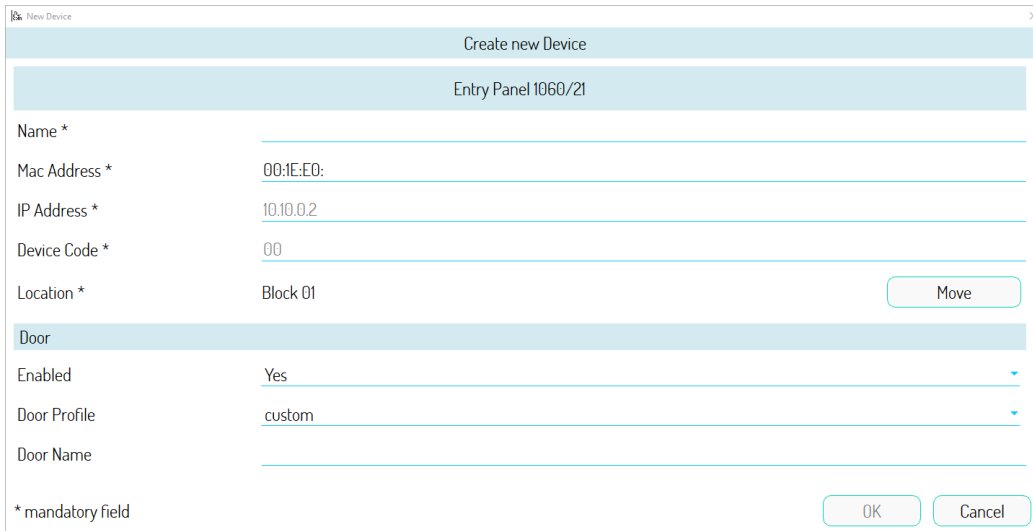
It is possible to configure any Urmet NVR device to record calls made via Entry Panel 1060/34 and related auto-on activated by video door phone. In [APPENDIX M1: Streaming video from IperCom calling stations to NVR Urmet](#) the configuration procedure of the **1098/328P** Urmet NVR device is shown. For the configurations of the other Urmet NVR devices contact the Urmet Service Centre.

The "Add" button in the "Activations" section has already been described in the paragraph "[Activations](#)".



*The address book of the Entry Panel is automatically created by importing the residents (set as visible) of all the apartments of the topological group of the Entry Panel itself.*

## Entry Panel 1060/21



**Create new Device**

Entry Panel 1060/21

Name \*

Mac Address \* 00:1E:E0:

IP Address \* 10.10.0.2

Device Code \* 00

Location \* Block 01 Move

**Door**

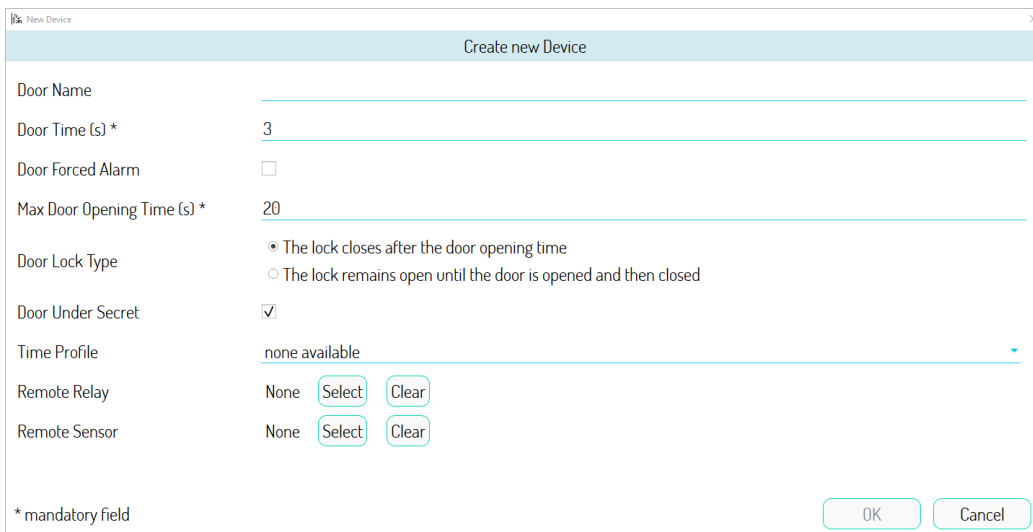
Enabled Yes

Door Profile custom

Door Name

\* mandatory field OK Cancel

Figure 733: Entry Panel 1060/21 settings (part 1)



**Create new Device**

Door Name

Door Time (s) \* 3

Door Forced Alarm

Max Door Opening Time (s) \* 20

Door Lock Type

- The lock closes after the door opening time
- The lock remains open until the door is opened and then closed

Door Under Secret

Time Profile none available

Remote Relay None Select Clear

Remote Sensor None Select Clear

\* mandatory field OK Cancel

Figure 734: Entry Panel 1060/21 settings (part 2)

Figure 735: entry panel 1060/21 settings (part 3)

Figure 736: Entry Panel 1060/21 settings (part 3)

The following table shows the meaning of the fields for the *Entry Panel 1060/21*.

<b>General settings</b>	
<i>Name</i>	Name to assign to the <i>Entry Panel</i> .
<i>MAC address</i>	MAC address associated with the <i>Entry Panel</i> .
<i>IP address</i>	IP address associated with the <i>Entry Panel</i> . Field visible only if manual network configuration is set in system parameters. Read-only value.
<i>Device code</i>	Read-only value.
<i>Position</i>	Position in system topology. The device can be moved to another topological node by pressing the "Move" button.

Table 61: General settings

<b>Main door settings</b>	
<i>Used</i>	The item “Yes” enables the main door: in this case the following options are shown, marked with a hash mark (#). The item “No” disables the main door. Default value: “Yes”.
<i>Door Profile (#)</i>	This allows you to associate a previously created door profile with the concerned main door. In this case, the door parameters are automatically compiled (besides the name). Default setting: <i>Custom</i> (parameters must be compiled manually).
<i>Access Name (#)</i>	Name to assign to the main door.
<i>Gate Opening Time (s) (#) (§)</i>	Pulse duration on the control relay. Default value: 3s. Allowed values: from 1s to 90s.
<i>Forced Door Alarm (#)</i>	If selected, if the access is forced, the concerned event sends an alarm to the <i>Switchboard</i> .
<i>Max Door Opening Time (s) (#)</i>	The maximum opening time of the door after which an open-door notification is sent to the <i>Switchboard</i> .
<i>Lock type (#)</i>	It allows you to choose the type of lock installed on the main door (see note at the end of the configuration section of the <a href="#">Call Module 1060/12-13-17-18</a> ).
<i>Door Under Secret (#)</i>	If selected, by pressing the door opener button (from an indoor station) it is possible to activate the electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the door can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.
<i>Time Profile (#)</i>	Allows you to associate a time profile with the main door. Access will only be valid within the selected time profile. Default setting: <i>none</i> .
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the main door of the <i>Entry panel</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button</a> .
<i>Remote Sensor</i>	It allows you to remotely control the sensor that signals that main door has been left open. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 62: Main door settings

Hall Button Settings	
<i>Remote Button (#)</i>	It allows you to remotely control the entrance hall button that opens the main door of the <i>Entry Panel</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 63: Hall button settings

<b>Gate settings</b>	
<i>Used</i>	In this case, the item <i>Yes</i> enables the gate: the following options are shown, marked with a hash mark (#). The item <i>No</i> disables the gate. The item “ <i>By door opening</i> ” allows you to use the relay contact of the gate to open the main door. The <i>Relay Actuator</i> item allows you to use the gate relay output as the output (only in monostable mode) of a <i>Relay Actuator</i> : in this case the item marked with the symbol (\$) appears. For further details see the section <a href="#">Gate contact used as output of a Relay Actuator</a> . Default value: <i>No</i> .
<i>Gate Profile (#)</i>	This allows you to associate a previously created door profile to the concerned gate. In this case, the gate parameters are automatically compiled (besides the name). Default setting: <i>Custom</i> (parameters must be compiled manually).
<i>Gate Name (#)</i>	Name to assign to the gate.
<i>Gate Opening Time (s) (#)</i>	Control relay pulse time. Default setting: 3s.
<i>Gate Under Secret (#)</i>	If selected, by pressing the gate button (from an indoor station) it is possible to activate electric lock of the outdoor station only when the caller is in conversation or is waiting for a response. If not selected, the gate can also be opened outside the call phase from all the apartments where the topological path detects the outdoor station. Default value: selected.
<i>Remote Relay (#)</i>	It allows you to remotely control the relay that operates the gate of the <i>Entry panel</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button</a> .

Table 64: Gate settings

<b>End user settings</b>	
<i>Speakers Volume</i>	Loudspeaker volume setting.
<i>Keyboard feedback tone</i>	Sound feedback volume when buttons are pressed.
<i>Call feedback tone</i>	Call feedback volume.
<i>Camera LED</i>	To enable the lighting LED of the camera.

Table 65: End user settings



<b>RTSP In-Call stream settings</b>	
<i>RTSP In-Call stream</i>	If selected, the <i>Switchboard</i> application can display the RTSP video stream of the calling station during the call to an apartment station or during the auto-on from an apartment station. Fields marked with the hash mark (#) must be filled correctly.
<i>IP Address (#)</i>	IP address of calling station camera
<i>Network mask (#)</i>	Subnet mask of RTSP cameras (including calling station camera).
<i>Port</i>	RTSP video stream port. Value not editable.
<i>Stream</i>	Name of the RTSP video stream. Value not editable
<i>User Name (#)</i>	Username to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>Password (#)</i>	Password to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>URI for Streaming</i>	Full URI of the RTSP video stream. Value not editable. It is built automatically by filling in the fields above respecting the following syntax: <code>rtsp://[&lt;username&gt;:&lt;password&gt;@] &lt;IP address&gt;:&lt;port&gt;/&lt;stream&gt;</code>

Table 66: RTSP streaming settings



In the RTSP streaming settings to set the IP address it is recommended to follow what is reported in [APPENDIX F1: How to use customized network settings in IperCom system](#).



It is possible to configure any Urmet NVR device to record calls made via Entry Panel 1060/21 and related auto-on activated by video door phone. In [APPENDIX M1: Streaming video from IperCom calling stations to NVR Urmet](#) the configuration procedure of the **1098/328P** Urmet NVR device is shown. For the configurations of the other Urmet NVR devices contact the Urmet Service Centre.

The "Call Keys" section allows associating the apartment stations or the *Switchboards* to be called to the only key of the *Entry panel* by browsing the topological structure of the system through the "Edit" button.

The assignment takes place in the same way as stated (for example) for *Entry panel* 1060/33.

The "Add" button in the "Activations" section has already been described in paragraph [Activations](#).

**If the 1060/21 calling station is part of a villa kit system in IPerCloud mode (that is, it is configured directly by scanning a QR-code with the CallMe app), some configuration parameters are different from the screens shown above. In detail, the gate is enabled with a relay opening duration set to 3s while the "Name" field is "MIKRA".**

## Private Call Module 1060/22

**Create new Device**

Private Call Module 1060/22

Name \*

Mac Address \*

IP Address \*

Device Code \*

Location \*

Speakers Volume

Button feedback tone

Call Feedback Tone

Camera LEDES

\* mandatory field

Figure 737: Private Call Module 1060/22 settings (part 1)

**Create new Device**

Device Code \*

Location \*

Speakers Volume

Button feedback tone

Call Feedback Tone

Camera LEDES

**Activations**

Activations 0 defined

**RTSP Settings**

RTSP In-Call Stream

\* mandatory field

Figure 738: Private Call Module 1060/22 settings (part 2)



The following table shows the meaning of the fields for the *Private Call Module 1060/22*.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the <i>Entry Panel</i> .
<i>MAC address</i>	MAC address associated with the <i>Entry Panel</i> .
<i>IP address</i>	IP address associated with the <i>Entry Panel</i> . Field visible only if manual network configuration is set in system parameters. Read-only value.
<i>Device code</i>	Read-only value.
<i>Position</i>	Position in system topology. The device can be moved to another topological node (only apartments) by pressing the "Move" button.
<i>Speakers Volume</i>	Speaker sound level.
<i>Keyboard feedback tone</i>	Sound feedback volume when buttons are pressed.
<i>Call feedback tone</i>	Call feedback volume.
<i>Camera LED</i>	To enable the lighting LED of the camera.

Table 67: General settings

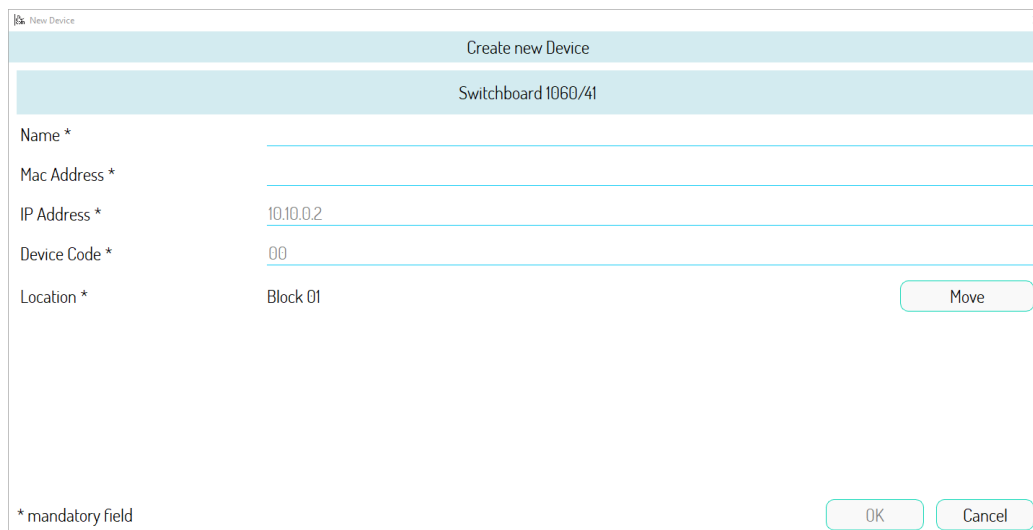
<b>RTSP In-Call stream settings</b>	
<i>RTSP In-Call stream</i>	If selected, the <i>Switchboard</i> application can display the RTSP video stream of the calling station during the call to an apartment station or during the auto-on from an apartment station. Fields marked with the hash mark (#) must be filled correctly.
<i>IP Address (#)</i>	IP address of calling station camera
<i>Network mask (#)</i>	Subnet mask of RTSP cameras (including calling station camera).
<i>Port</i>	RTSP video stream port. Value not editable.
<i>Stream</i>	Name of the RTSP video stream. Value not editable
<i>User Name (#)</i>	Username to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>Password (#)</i>	Password to access the calling station RTSP video stream from the <i>Switchboard</i> application.
<i>URI for Streaming</i>	Full URI of the RTSP video stream. Value not editable. It is built automatically by filling in the fields above respecting the following syntax: <code>rtsp://[&lt;username&gt;:&lt;password&gt;@] &lt;IP address&gt;:&lt;port&gt;/&lt;stream&gt;</code>

Table 68: RTSP streaming settings

-  In the RTSP streaming settings to set the IP address it is recommended to follow what is reported in [APPENDIX F1: How to use customized network settings in IperCom system.](#)
-  It is possible to configure any Urmet NVR device to record calls made via Entry Panel 1060/22 and related auto-on activated by video door phone. In [APPENDIX M1: Streaming video from IPerCom calling stations to NVR Urmet](#) the configuration procedure of the **1098/328P** Urmet NVR device is shown. For the configurations of the other Urmet NVR devices contact the Urmet Service Centre.

The "Add" button in the "Activations" section has already been described in paragraph [Activations](#).

## Switchboard 1060/41



The screenshot shows a 'New Device' dialog box titled 'Create new Device'. The device name is 'Switchboard 1060/41'. The fields are as follows:

Field	Value
Name *	
Mac Address *	
IP Address *	10.10.0.2
Device Code *	00
Location *	Block 01

Buttons: Move, OK, Cancel

\* mandatory field

Figure 739: Switchboard settings

The following table shows the meaning of the fields for *Switchboard 1060/41*.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the <i>Switchboard</i> .
<i>MAC Address</i>	MAC address associated with the PC on which the <i>Switchboard</i> programme is installed.
<i>IP Address</i>	IP address associated to the PC on which the <i>Switchboard</i> programme is installed. Field visible only if manual network configuration is set in system parameters. Value that cannot be changed.
<i>Device Code</i>	Value that cannot be changed.
<i>Location</i>	Position in the system topology: it is possible to move the <i>Switchboard</i> to another topological node by pressing the "Move" button.

Table 69: General settings

If there are two or more *Switchboard* applications on the same node, the following screen page will appear:

Up	Down	Location	Device
^	v	Block 01	This Device
^	v	Block 01	Switchboard North Site

Figure 740: Switchboard settings for CallMe priority feature

The buttons and in the "CallMe Priority" section allow you to move the *Switchboard* applications located on the relevant node up or down (in this case block 01).

This function is useful in the case of a call to "competence *Switchboards*" or to "all *switchboards*", if each *Switchboard* has the call forwarding function enabled (for further details see the paragraph [APPENDIX R: Call to several \*Switchboard\* applications each connected to a \*CallMe\* app](#)).

## Video door phone 7" VOG<sup>7</sup> 1761/31-32-33

Figure 741: Video door phone 7" VOG<sup>7</sup> 1761/31-32-33 settings

The following table shows the meaning of the various fields.

<b>General Settings</b>	
<b>Name</b>	Name to assign to the video door phone.
<b>MAC Address</b>	MAC address associated with the video door phone.
<b>IP Address</b>	IP address associated with the video door phone. Field visible only if a manual network configuration has been set. Value not editable.
<b>Device Code</b>	Value not editable.
<b>Location</b>	Position in the system topology: it is possible to move the video door phone to another topological node by pressing the "Move" button.
<b>Master</b>	The first video door phone in the apartment is automatically configured as the master one (it is possible to have only one master video door phone in the apartment). The other video door phones are set as slave units (you can configure them as master units by pressing the "Set as Master" button: the other video door phones are automatically set as slave units). A master video door phone has more functions than a slave video door phone (e.g. call forwarding can be enabled).
<b>Emergency Call from Switchboard Enabled</b>	If selected, in case of an alarm, it is possible to make an emergency call from the <i>Switchboard</i> in the concerned apartment.

Table 70: General settings



*If a video door phone 1761/6 is added to an apartment with video door phone 1761/3x, the 1761/6 video door phone cannot be configured as master.*

## Video door phone 5" VOG<sup>5+</sup> 1761/15-16-17-18

The screenshot shows a 'Create new Device' dialog box with the following fields and values:

- Name \***: Video Door Phone 5" VOG<sup>5+</sup> 1761/16
- Mac Address \***: 00:1E:E0:
- IP Address \***: 10.10.0.2
- Device Code \***: 00
- Location \***: Apartment 01010001 (with a 'Move' button)
- Master**: Master (selected)
- Emergency Call from Switchboard Enabled**:

At the bottom, there is a note: '\* mandatory field' and two buttons: 'OK' and 'Cancel'.

Figure 742: Video door phone 5" VOG<sup>5+</sup> 1761/15-16-17-18 settings

The following table shows the meaning of the various fields.

<b>General settings</b>	
<b>Name</b>	Name to assign to the video door phone.
<b>MAC Address</b>	MAC address associated with the video door phone.
<b>IP Address</b>	IP address associated with the video door phone. Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<b>Device Code</b>	Value not editable.
<b>Location</b>	Position in the system topology: it is possible to move the video door phone to another topological node by pressing the "Move" button.
<b>Master</b>	The first video door phone in the apartment is automatically configured as the master one (it is possible to have only one master video door phone in the apartment). The other video door phones are configured as slave units (you can configure them as master units by pressing the "Set as Master" button: the other video door phones are automatically set as slave units). A master video door phone has more functions than a slave video door phone (e.g. call forwarding can be enabled).
<b>Emergency Call from Switchboard Enabled</b>	If selected, in case of an alarm, it is possible to make an emergency call from the <i>Switchboard</i> in the concerned apartment.

Table 71: General settings



If the video door phone 1761/6 is added to an apartment with video door phone VOG<sup>5+</sup> 1761/15-16-18-19, the 1761/6 cannot be configured as master.



## Video door phone 5" VOG<sup>5</sup> 1761/6

**Create new Device**

Video Door Phone 5" VOG<sup>5</sup> 1761/6

Name \* \_\_\_\_\_

Mac Address \* 00:1E:EO: \_\_\_\_\_

IP Address \* 10.10.0.2 \_\_\_\_\_

Device Code \* 00 \_\_\_\_\_

Location \* Apartment 01010001 Move

Button T1 used for Gate Open

Button T2 used for User Activation

Master Master

Emergency Call from Switchboard Enabled

\* mandatory field OK Cancel

Figure 743: Video door phone 5" VOG<sup>5</sup> 1761/6 settings (part 1)

**Create new Device**

Call Buttons

Position	B	S	F	A	D	Type	Description
1							
2							
3							

User Activations

Position	Name	Output	Command
1		Gate Open	
2	-	-	-

\* mandatory field OK Cancel

Figure 744: Video door phone 5" VOG<sup>5</sup> 1761/6 settings (part 2)

The following table shows the meaning of the various fields.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the video door phone.
<i>MAC Address</i>	MAC address associated with the video door phone
<i>IP Address</i>	IP address associated with the video door phone. Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<i>Device Code</i>	Value not editable.
<i>Location</i>	Position in the system topology: it is possible to move the video door phone to another topological node by pressing the "Move" button.
<i>Master</i>	The first video door phone in the apartment is automatically configured as the master one (it is possible to have only one master video door phone in the apartment). The other video door phones are configured as slave units (you can configure them as master units by pressing the "Set as Master" button: the other video door phones are automatically set as slave units). A master video door phone has more functions than a slave video door phone (e.g., call forwarding can be enabled).
<i>Button T1 used for</i>	Default value: "Gate Open". Alternatively, button T1 can be associated to the topological events: "User Activation", "Lift up" and "Lift down" (the last 2 if not already associated with the T2 button).
<i>Button T2 used for</i>	Default value: "User Activation". Alternatively, button T2 can be associated to the topological events: "Lift up" and "Lift down" (the last 2 if not already associated with the T1 button).
<i>Emergency Call from Switchboard Enabled</i>	If selected, in case of an alarm, it is possible to make an emergency call from the <i>Switchboard</i> in the concerned apartment.

Table 72: General settings



*If there are other video door phones in the same apartment, the video door phone 1761/6 cannot be configured as master (other video door phones are video door phones other than the 1761/6). On the contrary, the 1761/6 is a master video door phone in the presence of Miro door phones or in the presence of other video door phones 1761/6.*

The "Call buttons" section shows the list of contacts associated to buttons T1, T2 and T3 of the video door phone (see paragraph [Contacts](#)).

The "User Activations" section shows the activation rules associated to T1 and T2 buttons of the video door phone (see paragraph [Activations](#)).

## Video door phone 7" MAX 1717/31-32-33-34-41

The screenshot shows a 'Create new Device' dialog box with the following fields and values:

- Name \*
- Mac Address \*: 00:1E:E0:
- IP Address \*: 10.10.0.2
- Device Code \*: 00
- Location \*: Apartment 01010001 (with a 'Move' button)
- Master: Master (selected)
- Emergency Call from Switchboard Enabled:

At the bottom, there are 'OK' and 'Cancel' buttons, and a note: '\* mandatory field'.

Figure 745: Video door phone 7" MAX 1717/31-32-33-34-41 settings

The following table shows the meaning of the various fields.

<b>General Settings</b>	
<b>Name</b>	Name to assign to the video door phone.
<b>MAC Address</b>	MAC address associated with the video door phone.
<b>IP Address</b>	IP address associated with the video door phone. Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<b>Device Code</b>	Value not editable.
<b>Location</b>	Position in the system topology: it is possible to move the video door phone to another topological node by pressing the "Move" button.
<b>Master</b>	The first video door phone in the apartment is automatically configured as the master one (it is possible to have only one master video door phone in the apartment). The other video door phones are configured as slave units (you can configure them as master units by pressing the "Set as Master" button: the other video door phones are automatically set as slave units). A master video door phone has more functions than a slave video door phone (e.g., call forwarding can be enabled).
<b>Emergency Call from Switchboard Enabled</b>	If selected, in case of an alarm, it is possible to make an emergency call from the <i>Switchboard</i> in the concerned apartment.

Table 73: General settings



*If the video door phone 1761/6 is added to an apartment with video door phone 1717/3x-4x, the 1761/6 cannot be configured as master.*

## Video door phone 10" MAX 1717/21-22-23

Figure 746: Video door phone 10" MAX 1717/21-22-23 settings

The following table shows the meaning of the various fields.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the video door phone.
<i>MAC Address</i>	MAC address associated with the video door phone.
<i>IP Address</i>	IP address associated with the video door phone. Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<i>Device Code</i>	Value not editable.
<i>Location</i>	Position in the system topology: it is possible to move the video door phone to another topological node by pressing the "Move" button.
<i>Master</i>	The first video door phone in the apartment is automatically configured as the master one (it is possible to have only one master video door phone in the apartment). The other video door phones are configured as slave units (you can configure them as master units by pressing the "Set as Master" button: the other video door phones are automatically set as slave units). A master video door phone has more functions than a slave video door phone (e.g. call forwarding can be enabled).
<i>Emergency Call from Switchboard Enabled</i>	If selected, in case of an alarm, it is possible to make an emergency call from the <i>Switchboard</i> in the concerned apartment.

Table 74: General settings



If a video door phone 1761/6 is added to an apartment with video door phone 1717/2x, the 1761/6 cannot be configured as master.

## Video door phone 7" Basic 1741/1-2-3

Figure 747: Video door phone 7" Basic 1741/1-2-3 settings

The following table shows the meaning of the various fields.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the video door phone.
<i>MAC Address</i>	MAC address associated with the video door phone.
<i>IP Address</i>	IP address associated with the video door phone. Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<i>Device Code</i>	Value not editable.
<i>Location</i>	Position in the system topology: it is possible to move the video door phone to another topological node by pressing the "Move" button.
<i>Master</i>	The first video door phone in the apartment is automatically configured as the master one (it is possible to have only one master video door phone in the apartment). The other video door phones are configured as slave units (you can configure them as master units by pressing the "Set as Master" button: the other video door phones are automatically set as slave units). A master video door phone has more functions than a slave video door phone (e.g. call forwarding can be enabled).
<i>Emergency Call from Switchboard Enabled</i>	If selected, in case of an alarm, it is possible to make an emergency call from the <i>Switchboard</i> in the concerned apartment.

Table 75: General settings



If video door phone 1761/6 is added to an apartment with 1741/1-2-3 video door phones, 1761/6 cannot be configured as a master.

## IPerCom Client 1060/43

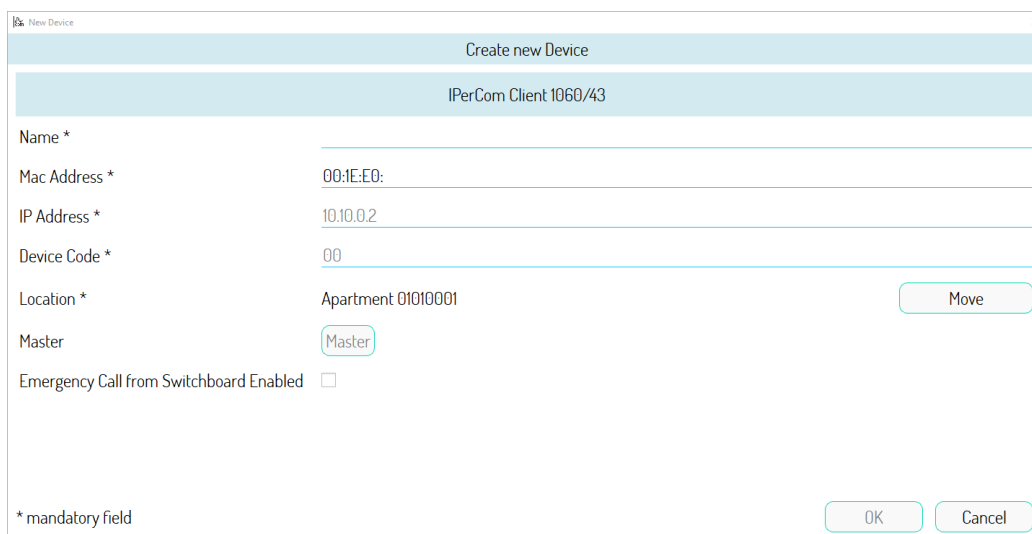


Figure 748: IPerCom Client 1060/43 settings

The following table shows the meaning of the various fields.

<b>General Settings</b>	
<b>Name</b>	Name to assign to the video door phone.
<b>MAC Address</b>	MAC address associated with the video door phone.
<b>IP Address</b>	IP address associated with the video door phone. Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<b>Device Code</b>	Value not editable.
<b>Location</b>	Position in the system topology: it is possible to move the video door phone to another topological node by pressing the "Move" button.
<b>Master</b>	The first video door phone in the apartment is automatically configured as the master one (it is possible to have only one master video door phone in the apartment). The other video door phones are configured as slave units (you can configure them as master units by pressing the "Set as Master" button: the other video door phones are automatically set as slave units). A master video door phone has more functions than a slave video door phone (e.g. call forwarding can be enabled).
<b>Emergency Call from Switchboard Enabled</b>	If selected, in case of an alarm, it is possible to make an emergency call from the <i>Switchboard</i> in the concerned apartment.

Table 76: General settings



*If at least one other apartment station (other than IPerCom Client) is added in an apartment with IPerCom Client, the IPerCom Client video door phone cannot be set as master. However, if there are only IPerCom Client video door phones in the apartment, one of these will necessarily be set as master.*

## Miro door phone 1160/3

**Create new Device**

Door Phone Miro 1160/3

Name \* \_\_\_\_\_

Mac Address \* 00:1E:EO: \_\_\_\_\_

IP Address \* 10.10.0.2 \_\_\_\_\_

Device Code \* 00 \_\_\_\_\_

Location \* Apartment 01010001 Move

Master Master

Button T1 used for Gate Open

Button T2 used for User Activation

Emergency Call from Switchboard Enabled

\* mandatory field OK Cancel

Figure 749: Miro door phone 1160/3 settings (part 1)

**Create new Device**

Emergency Call from Switchboard Enabled

**Call Buttons**

Position	B	S	F	A	D	Type	Description
1							
2							

**User Activations**

Position	Name	Output	Command
1		Gate Open	
2	-	-	-

\* mandatory field OK Cancel

Figure 750: Miro door phone 1160/3 settings (part 2)

The following table shows the meaning of the various fields.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the door phone.
<i>MAC address</i>	MAC address associated with the <i>Door Phone</i> .
<i>IP address</i>	IP address associated with the <i>Door Phone</i> . Field visible only if manual network configuration is set in system parameters. Read-only value.
<i>Device code</i>	Read-only value.
<i>Position</i>	Position in system topology. The device can be moved to another topological node by pressing the "Move" button.
<i>Master</i>	If selected, the <i>Door Phone</i> is added as the first device in the apartment (there can be only one Master device in an apartment). Other <i>Door Phones</i> monitors are added as slaves (you can add them as masters by pressing the "Set As Master" button: the other devices are set as slaves). If at least one <i>video door phone</i> will be present in the apartment, the Master will be chosen from <i>video door phones</i> and all <i>Door Phones</i> present will be automatically set as Slaves.
<i>Button T1 used for</i>	Default value: "Gate Open". Alternatively, button T1 can be associated to the topological events: "User Activation", "Lift up" and "Lift down" (the last 2 if not already associated with the T2 button).
<i>Button T2 used for</i>	Default value: "User Activation". Alternatively, button T2 can be associated to the topological events: "Lift up" and "Lift down" (the last 2 if not already associated with the T1 button).
<i>Emergency Call from Switchboard Enabled</i>	If selected, in the event of an alarm, it is possible to make an emergency call to the <i>Switchboard</i> in the concerned apartment.

Table 77: General settings

Buttons T1 and T2 of the Audio Door Phone are the buttons shown in the following figure:



Figure 751: T1 and T2 buttons of Door Phone 1160/3

The "Call Buttons" section shows the contacts list of the "Address Books" associated with buttons T1 and T2 of the *Miro door phone* (see paragraph [Contacts](#)).

The "User Activations" section shows instead the activation rules associated with buttons T1 and T2 of the *Miro door phone* (see paragraph [Activations](#)).



## Key Reader 1060/45 or 1060/86

**Create new Device**

Key Reader 1060/45-86

Name \*

Mac Address \* 00:1E:E0: ...

Device Code \* 05

Location \* Site 01 Move

Door Profile custom

Door Name

Door Time (s) \* 3

Door Forced Alarm

Max Door Opening Time (s) \* 20

\* mandatory field

OK Cancel

Figure 752: Key Reader settings (part 1)

**Create new Device**

Door Time (s) \* 3

Door Forced Alarm

Max Door Opening Time (s) \* 20

Door Under Secret

Time Profile none available

Remote Relay None Select Clear

Remote Sensor None Select Clear

**Hall Button**

Remote Button None Select Clear

**Activations**

Activations 0 defined Add

\* mandatory field

OK Cancel

Figure 753: Key Reader settings (part 2)

The following table shows the meaning of the fields for *Key Reader* 1060/45 e 1060/86.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the <i>Key Reader</i> .
<i>MAC Address</i>	MAC address associated with the <i>Key Reader</i> .
<i>IP Address</i>	IP address associated with the <i>Key Reader</i> . Field visible only if manual network configuration is set in system parameters. Value that cannot be changed.
<i>Device Code</i>	Value that cannot be changed.
<i>Location</i>	Position in the system topology: it is possible to move the device to another node of the system by pressing the "Move" button.
<i>Door Profile</i>	This allows you to associate a previously created door profile with the concerned door. In this case, the door parameters are automatically compiled (besides the name). Default setting: <i>Customised</i> (parameters must be compiled manually).
<b>Door settings</b>	
<i>Door Name</i>	Name to assign to the door.
<i>Door Time (s)</i>	Pulse duration on the control relay. Default value: 3 s.
<i>Forced Alarm Time (*)</i>	If selected, if the accessed is forced, the concerned event sends an alarm to the <i>Switchboard</i> .
<i>Max Door Opening Time (s)</i>	The maximum opening time of the door after which a notification is sent to the <i>Switchboard</i> .
<i>Door Under Secret</i>	If not selected, pressing the door lock release button on an <i>apartment station</i> , whose topological path intercepts the <i>Key Reader</i> , activates its electric lock, even not during a call. If selected, the door can only be opened by swiping a suitably registered key. Default setting: selected.
<i>Time Profile</i>	This allows you to associate a time profile with the door. Access will only be valid within the selected time profile (except for residents of apartments, whose topological path intercepts the key reader). Default setting: <i>none</i> .
<i>Remote Relay</i>	It allows you to remotely control the relay that allows the <i>Key Reader</i> port opening. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button</a> .
<i>Remote Sensor</i>	It allows you to remotely control the sensor that signals that main door has been left open. For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 78: General settings and door settings

<b>Hall Button Settings</b>	
<i>Remote Button (#)</i>	It allows you to remotely control the entrance hall button that opens the door of the <i>Key Reader</i> . For further details, see paragraph <a href="#">Remote relay functions, remote entrance hall button and remote sensor</a> .

Table 79: Hall button settings

The “Add” button in the “Activations” section has already been described in paragraph [Activations](#).



*For the Key Reader 1060/86 with firmware version 1.40 it is recommended to remotely control the door open sensor through the input of a Relay Actuator with firmware version 4.05 (remote sensor function). The firmware version of the Key Reader 1060/86 can be viewed through the Diagnostics button in IPerCom Installer Tools.*

Relay actuator 1060/84 v. 2.07 / 3.04 / v. 4.05

**Create new Device**

Relay Actuator 1060/84 v4.05

Name \_\_\_\_\_

Mac Address \* 00:1E:E0: \_\_\_\_\_

IP Address \* 10.10.0.2 \_\_\_\_\_

Device Code \* 00 \_\_\_\_\_

Location \* Block 01 Move

**Output 1**

Name \_\_\_\_\_

Mode bistable

**Output 2**

\* mandatory field OK Cancel

Figure 754: Relay actuator 1060/84 (part 1)

**Create new Device**

**Output 2**

Name \_\_\_\_\_

Mode bistable

**Input 1**

Name \_\_\_\_\_

Mode bistable

Output linked to input

Input Normally Open

Activations 0 defined Add

Alarms 0 defined Add

**Input 2**

\* mandatory field OK Cancel

Figure 755: Relay actuator 1060/84 (part 2)

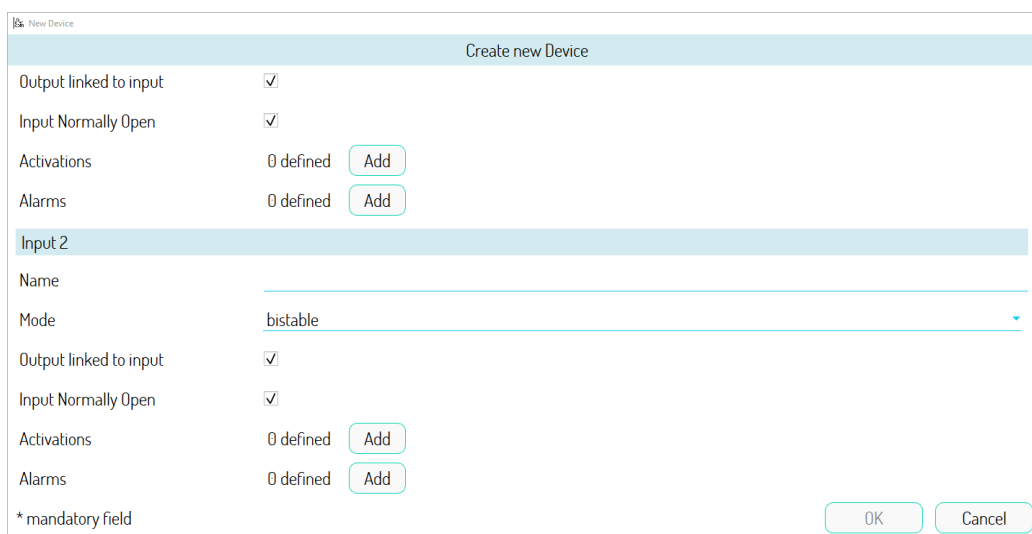


Figure 756: Relay actuator 1060/84 (part 3)

The following table shows the meaning of the fields for the *Relay Actuator 1060/84* and the version for which the field is present.

<b>GENERAL SETTINGS</b>	<b>v. 3.04/v. 2.07/v. 4.05</b>
<i>Name</i>	Name to assign to the <i>Relay Actuator</i> . If no name is assigned, the field is forced with the MAC address.
<i>MAC Address</i>	MAC address associated to the <i>Relay Actuator</i> .
<i>IP Address</i>	IP address associated to the <i>Relay Actuator</i> . Field visible only if manual network configuration is set in system parameters. Value that cannot be changed.
<i>Device Code</i>	Value that cannot be changed.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node by pressing the “Move” button.

Table 80: General settings

<b>Output 1 and 2</b>	<b>v. 3.04/v. 2.07/v. 4.05</b>
<i>Name</i>	Name to assign to the output. If no name is assigned, the field is forced by the last 3 pairs of alphanumeric characters of the MAC address followed by " - Output 1 (2)".
<i>Mode</i>	Output relay operating mode: monostable or bistable. If you choose the monostable mode, you must enter the time during which the relay operates in this mode. Default value: bistable.

Table 81: Output configuration

<b>Input 1 and 2</b>	<b>Only v. 3.04/v. 4.05</b>
<i>Name</i>	Name to assign to the input
<i>Mode</i>	Input operating mode. In bistable mode, the input is set as a switch (on and off events). In monostable mode, the input is set as a button (short and long pressure events): in this case the pressure time must be entered.
<i>Output connected to input</i>	If selected, it automatically associates the input with the corresponding output. If not selected, the input can control several outputs (also of other <i>Relay Actuators</i> ) through the events described above.
<i>Normally Open Input</i>	If selected, the input is normally open, otherwise it is normally closed.

Table 82: Input configuration

The "Activations" and "Alarms" buttons allow you to create an activation rule and an alarm for a specific *Relay Actuator* input.



The *Relay Actuator 1060/84 v. 4.05* is the only one to support the "DISABLE" command in monostable mode (from version 2.1.0 of *IPerCom*).

A table of the electrical meanings of the on, off, short press and long press events is shown depending on the input status (normally closed or normally open):

<b>Events</b>	<b>Normally Open Input</b>	<b>Normally Closed Input</b>
On	Closed	Open
Off	Open	Closed
Short press	Closed for $T < T_0$	Open for $T < T_0$
Long press	Closed for $T \geq T_0$	Open for $T \geq T_0$

Table 83: Meaning of on, off, short press and long press according to input status

## IPerTALK Server / IPerTALK Server V1

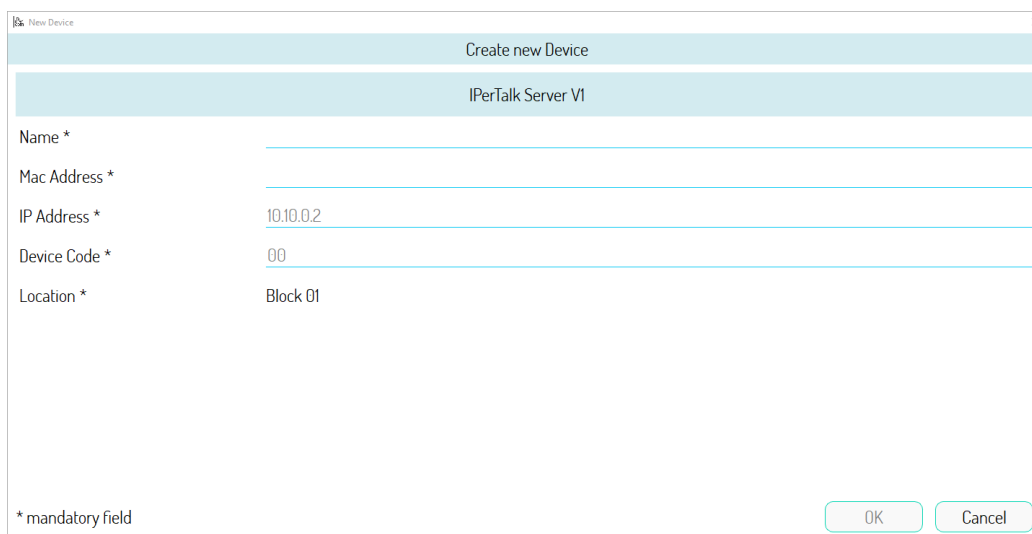


Figure 757: IPerTALK Server / IPerTALK Server V1 settings

The following table shows the meaning of the fields for the *IPerTALK Server / IPerTALK Server V1*.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the <i>IPerTALK Server / IPerTALK Server V1</i> .
<i>MAC address</i>	MAC address associated with the <i>IPerTALK Server / IPerTALK Server V1</i> .
<i>IP Adress</i>	IP address associated with the <i>IPerTALK Server / IPerTALK Server V1</i> . This field is visible only if a manual network configuration has been set in the system parameters. Not editable value.
<i>Device code</i>	Not editable value.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node pressing the "Move" button.

Table 84: General settings for IPerTALK Server / IPerTALK Server V1



The *IPerTALK Server V1* item appears only if the network addressing chosen for the IPerCom system is static and refers to the integration of the IPerCom 3.1.0 system with the IPerTALK 2.2.10 system or higher (which mandatorily requires static addressing for the IPerCom system). On the contrary, the *IPerTALK Server* item appears with both dynamic and static network addressing and refers to the first integration of the IPerCom 2.2.0 system with the IPerTALK 2.1.4 system or higher (up to and including version 2.2.3), which allowed below:

- audio or audio-video calls from Ipercom calling stations to iPerTALK extensions;
- auto-on function from iPerTALK extensions to Ipercom calling stations;
- audio or audio-video calls from iPerTALK extensions to Ipercom Switchboard and vice versa.

## IPassan controller

Figure 758: IPassan controller settings

The following table shows the meaning of the fields for the *IPassan Controller*.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the <i>IPassan Controller</i> .
<i>MAC Address</i>	MAC address associated with the <i>IPassan Controller</i> . Value not editable. The MAC address is automatically taken from the serial number.
<i>Device Code</i>	Value not editable.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node by pressing the "Move" button.
<i>IP Address</i>	IP address associated with the <i>IPassan Controller</i> . It is necessary to enter a static IP address and outside the network range of IPerCom devices and any RTSP cameras.
<i>Serial number</i>	Serial number of the <i>IPassan Controller</i> .
<i>Lift Control</i>	If selected, it allows you to control the lifts through the <i>IPassan Controller</i> . Default value: not selected.

Table 85: General settings



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.



## IPerCom-2Voice Gateway 1083/59

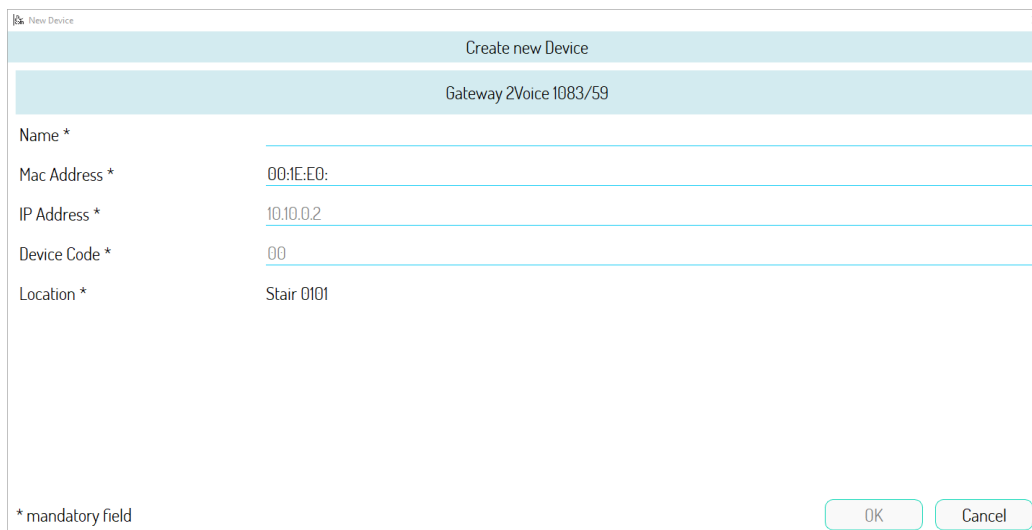





Figure 759: IPerCom-2Voice Gateway 1083/59 settings

Figure 759: IPerCom-2Voice Gateway 1083/59 settings

The following table shows the meaning of the fields for the *IPerCom-2Voice Gateway 1083/59*.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the <i>IPerCom-2Voice Gateway</i> .
<i>MAC address</i>	MAC address associated with the <i>IPerCom-2Voice Gateway</i> .
<i>IP address</i>	IP address of the <i>IPerCom-2Voice Gateway</i> . Field visible only if manual network configuration is set in system parameters. Read-only value.
<i>Device code</i>	Read-only value.
<i>Position</i>	Position in system topology. It is not possible to move the <i>IPerCom-2Voice Gateway</i> to other topological nodes.

Table 86: General settings

-  *The guaranteed conversation time set on the IPerCom system and on the 2Voice secondary stations connected to the Gateway must be the same for the system to work correctly.*
-  *Follow the instructions in the related manuals of devices to set the guaranteed conversation time at the 2Voice secondary call modules.*
-  *It is necessary to upgrade the IPerCom system to version 1.3.0 or higher for proper operation of the IPerCom 2Voice Gateway.*

## IperCom Clock Module 1060/85

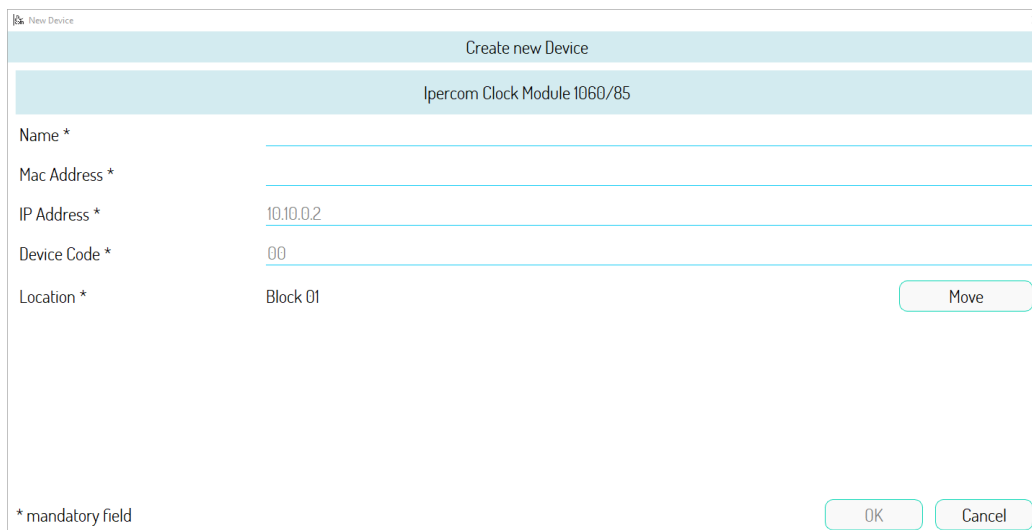


Figure 760: IperCom Clock Module 1060/85 settings

The following table shows the meaning of the fields for "IperCom Clock Module 1060/85".

<b>General Settings</b>	
<i>Name</i>	Name to assign to the <i>IperCom Clock Module</i> .
<i>MAC Address</i>	MAC address associated with the <i>IperCom Clock Module</i> .
<i>IP Address</i>	IP address associated to the PC on which the <i>IperCom Clock Module</i> programme is installed. Field visible only if manual network configuration is set in system parameters. Value that cannot be changed.
<i>Device Code</i>	Value that cannot be changed.
<i>Location</i>	Position in the system topology: it is possible to move the <i>IperCom Clock Module</i> to another topological node by pressing the "Move" button.

Table 87: General settings



It is necessary to upgrade the IPerCom system to version 1.2.0 or higher for proper operation of the module in question.

## Lift interface 1060/37

**Create new Device**

Lift Interface 1060/37

Name \*

Mac Address \* 00:1E:E0:

IP Address \* 10.10.0.2

Device Code \* 00

Location \* Stair 0101

Mode Lift Interface

**Input for activation or alarm**

Name

Mode bistable

\* mandatory field

OK Cancel

Figure 761: Lift interface 1060/37 settings (part 1)

**Create new Device**

Mode Lift Interface

**Input for activation or alarm**

Name

Mode bistable

Input Normally Open

Activations 0 defined Add

Alarms 0 defined Add

Set Outputs on Alarm

**Paths**

Door	Time	Edit	Delete
Add New Path			

\* mandatory field

OK Cancel

Figure 762: Lift interface 1060/37 settings (part 2)

The following table shows the meaning of the fields for *Lift Interface* 1060/37.

<b>General settings</b>	
<i>Name</i>	Name to assign to the <i>Lift Interface</i> .
<i>MAC Address</i>	MAC address associated with the <i>Lift Interface</i> .
<i>IP Address</i>	IP address of the <i>Lift Interface</i> . Field visible only if a manual network configuration has been set in the system parameters. Value not editable.
<i>Device Code</i>	Value not editable.
<i>Location</i>	Position in the system topology: it is possible to move the <i>Lift Interface</i> to another topological node.
<i>Mode</i>	It allows you to define the operating mode of the <i>Lift Interface</i> . Modes are: " <i>Lift Interface - RS485</i> ", " <i>Lift Interface</i> ", " <i>Relay Actuator Mode</i> ". Default mode: " <i>Lift Interface</i> "

Table 88: General settings

<b>Input 1</b>	
<i>Name</i>	Name to assign to the input.
<i>Mode</i>	Input operating mode. In bistable mode, the input is set as a switch (on and off events). In monostable mode, the input is set as a button (short and long pressure events): in this case the pressure time must be entered.
<i>Normally open input</i>	If selected, the input is normally open, otherwise it is normally closed.
<i>Set Outputs in case of Alarm</i>	If selected, it allows you to set which relays will be activated when an alarm is triggered.

Table 89: General settings

The "Add" buttons in the "Activations" and "Alarms" section have already been described in the paragraphs [Activations](#) and [Sending alarms to the Switchboard via relay actuator inputs](#).

The function of the "Add path" button has already been described in paragraph [Creating the path](#).

## RTSP Camera

New Device

Create new Device

RTSP Camera

Name \*

Mac Address \*

Device Code \* 00

Location \* Block 01 Move

Streaming URI rtsp://10.10.128.0:/

IP Address \* 10.10.128.0

Port \*

Stream \*

Username

\* mandatory field

OK Cancel

Figure 763: RTSP Camera settings (part 1)

New Device

Create new Device

Name \*

Mac Address \*

Device Code \* 00

Location \* Block 01 Move

Streaming URI rtsp://10.10.128.0:/

IP Address \* 10.10.128.0

Port \*

Stream \*

Username

Password

\* mandatory field

OK Cancel

Figure 764: RTSP Camera settings (part 2)

The following table shows the meaning of the fields for *RTSP Camera*.

<b>General Settings</b>	
<i>Name</i>	Name to assign to the <i>RTSP Camera</i> .
<i>MAC Address</i>	MAC address associated with the <i>RTSP Camera</i> .
<i>Device Code</i>	Value cannot be changed.
<i>Location</i>	Position in the system topology: it is possible to move the device to another topological node by pressing the "Move" button.
<b>RTSP streaming settings</b>	
<i>URI for Streaming</i>	Full URI video streaming. Read-only value. It is automatically compiled by compiling the fields below, respecting the following syntax: rtsp://[<Username>:<Password>@] <IP Address>:<Port>/<Stream> The part between square brackets may not be present if the user name and password are not defined.
<i>IP Address</i>	Camera IP address.
<i>Port</i>	RTSP stream port.
<i>Stream</i>	Address of the stream.
<i>Username</i>	User name to access the camera.
<i>Password</i>	User password for access to the camera.

Table 90: general settings for RTSP Camera



To set the IP address it is recommended to follow what is reported in [APPENDIX F1: How to use customized network settings in IperCom system](#). For RTSP cameras supported by IPerCom system video door phones, follow what is reported in [APPENDIX W1: RTSP Cameras supported by IPerCom video door phones](#).

## RTSP Camera (NVR)

**Create new Device**  
RTSP Camera (NVR)

Name \* \_\_\_\_\_

Identifier \* \_\_\_\_\_

Device Code \* 05 \_\_\_\_\_

Location \* Site 01 \_\_\_\_\_

Streaming URI rtsp://10.10.128.1:/ \_\_\_\_\_

IP Address \* 10.10.128.1 \_\_\_\_\_

Port \* \_\_\_\_\_

Stream \* \_\_\_\_\_

Username \_\_\_\_\_

\* mandatory field

Figure 765: RTSP Camera (NVR) settings (part 1)

**Create new Device**  
RTSP Camera (NVR)

Name \* \_\_\_\_\_

Identifier \* \_\_\_\_\_

Device Code \* 01 \_\_\_\_\_

Location \* Appartamento 01010001 \_\_\_\_\_

Streaming URI rtsp://10.10.128.1:/ \_\_\_\_\_

IP Address \* 10.10.128.1 \_\_\_\_\_

Port \* \_\_\_\_\_

Stream \* \_\_\_\_\_

Username \_\_\_\_\_

Password \_\_\_\_\_

\* mandatory field

Figure 766: RTSP Camera (NVR) settings (part 2)

The following table shows the meaning of the fields for *RTSP Camera (NVR)*.

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

Table 91: general settings for *RTSP Camera (NVR)*

For the use of RTSP Cameras with Urmet NVR devices **1098/324P-326P-328P**, refer to [APPENDIX M2: RTSP Cameras with NVR Urmet device](#).



## APPENDIX B: Differences of functions between 2Voice and IPerCom apartment station

Below is a table with the performances supported and not supported by the IPerCom and 2Voice apartment station. Please note that adding a riser of 2Voice apartment station to an IPerCom system is only possible through the IPerCom-2Voice 1083/59 Gateway.

Function	2Voice apartment station	IPerCom apartment station
Call from IPerCom Call station	YES	YES
Call from 2Voice Call station	YES	NO
Call from IPerCom Door Phone	YES	YES
Call from 2Voice Door Phone	YES (*)	NO (**)
Call to IPerCom Switchboard	YES	YES
IPerCom Call station auto-on	YES	YES
2Voice Call station auto-on	YES	NO
RTSP camera auto-on	NO	YES
Relay activation on 1060/84	YES (#)	YES
Relay activation on 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 92: 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 station are appropriately programmed. On different stairs, it is necessary to pass through the Switchboard.

(\*\*): Only through the Switchboard.

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

(##): Unlike IPerCom Door Phones, 2Voice apartment station ring when an emergency call is sent from the Switchboard.

It is also remembered that:

- if an audio apartment station (IPerCom or 2Voice) with call forwarding function enabled is called from an IPerCom outdoor station, the video stream of the outdoor 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 C: Differences of functions between 2Voice and IPerCom devices with IPerCom Switchboard

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

<b>Function</b>	<b>2Voice device</b>	<b>IPerCom device</b>
Auto-on from Switchboard	2Voice secondary stations (connected to the Gateway): NO	IPerCom stations (any): YES
Interception of calls from IPerCom Switchboard located on 2Voice stairs node	Calls from 2Voice secondary station (connected to the Gateway): NO	Calls from IPerCom secondary station: YES

*Table 93: Differences of functions with IPerCom Switchboard*

## APPENDIX D: IPerCom priority calls

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

- auto-on;
- intercom (call between two apartments);
- call from Call Module/Entry Panel/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-insertion 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](http://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 E: Type of proximity keys that can be read by IPerCom devices with access control function

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
<b>Call Module 1060/12-13-17-18</b>	V	X	V (*)	X
<b>Call Module 1060/23</b>	X	V	V (***)	V
<b>Modular Entry Panel with 1060/48</b>	X	V	V (**)	V
<b>Entry panel 1060/21</b>	X	V	X	X
<b>Key Reader 1060/86</b>	X	V	V (***)	V
<b>Key Reader 1060/45</b>	X	V	V (***)	V

Table 94: Type 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;

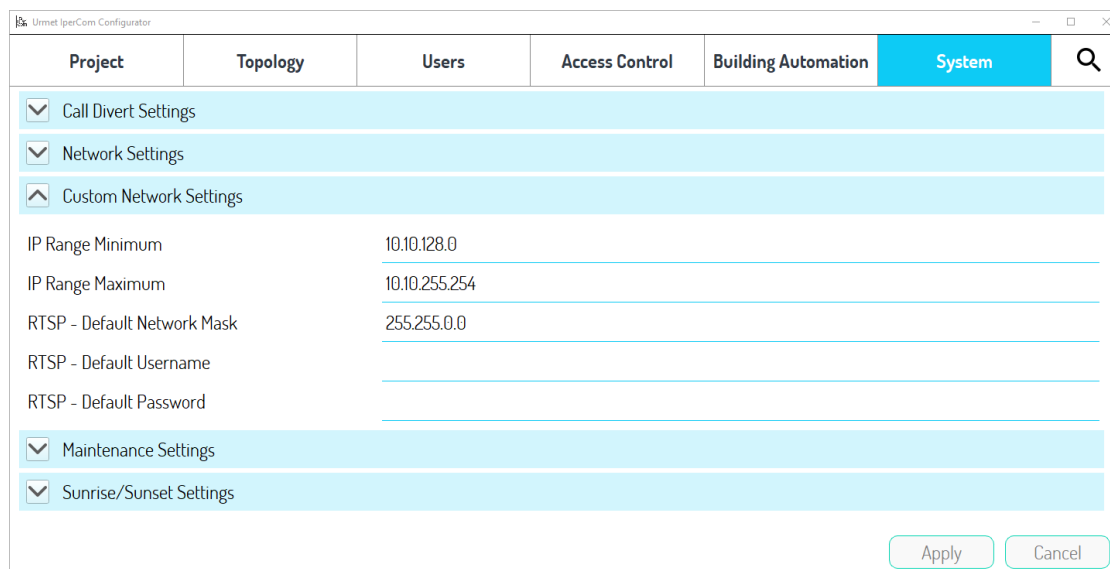
(\*\*\*): with dual technology keys (125KHz/Mifare), only the Mifare component is read.

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 F1: How to use customized network settings in IperCom system

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



The screenshot shows the 'System' tab of the IperCom Configurator. The 'Custom Network Settings' section is expanded, showing the following fields:

IP Range Minimum	10.10.128.0
IP Range Maximum	10.10.255.254
RTSP - Default Network Mask	255.255.0.0
RTSP - Default Username	
RTSP - Default Password	

Other settings visible include Call Divert Settings, Network Settings, Maintenance Settings, and Sunrise/Sunset Settings. 'Apply' and 'Cancel' buttons are at the bottom right.


Figure 767: “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 767](#).

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 call 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 767](#).*

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:

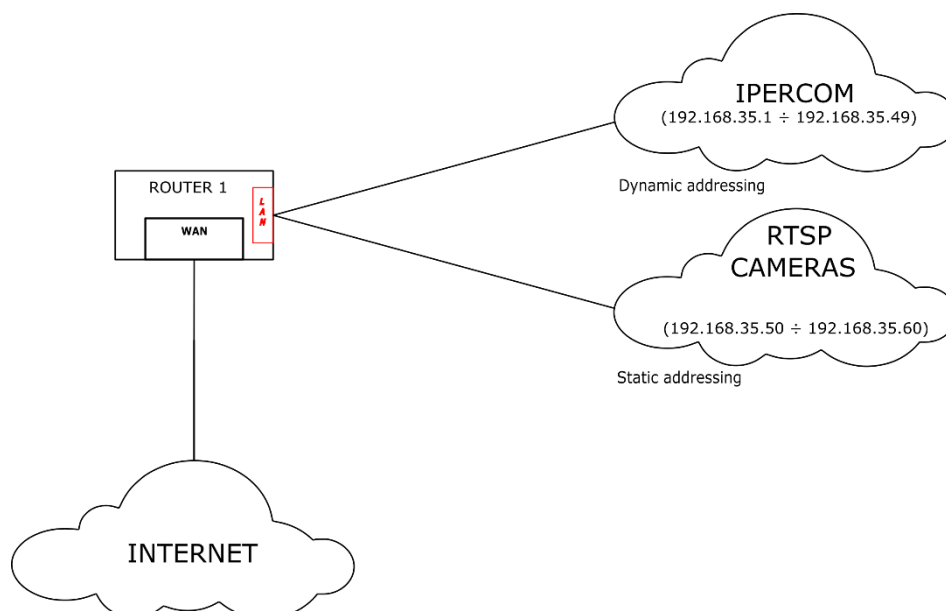


Figure 768: connection diagram for RTSP cameras and IPerCom devices

To create the diagram in [Figure 768](#), 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

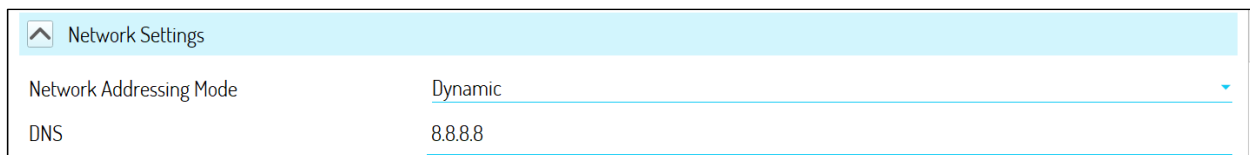
- Set the *RTSP Cameras* addressing in static mode with addresses ranging from 192.168.35.50 to 192.168.35.60

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:

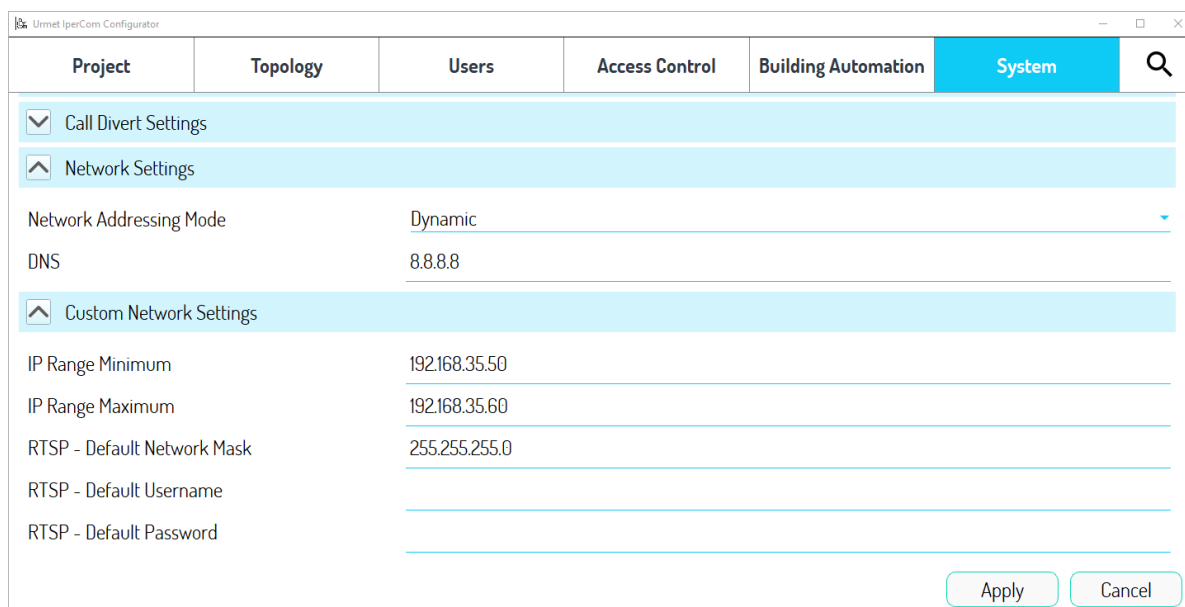


Network Settings	
Network Addressing Mode	Dynamic
DNS	8.8.8.8

Figure 769: 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:



Project	Topology	Users	Access Control	Building Automation	System	
Call Divert Settings						
Network Settings						
Network Addressing Mode	Dynamic					
DNS	8.8.8.8					
Custom Network Settings						
IP Range Minimum	192.168.35.50					
IP Range Maximum	192.168.35.60					
RTSP - Default Network Mask	255.255.255.0					
RTSP - Default Username						
RTSP - Default Password						
					Apply	Cancel

Figure 770: custom IP address range

### 3. Adding an RTSP Camera

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

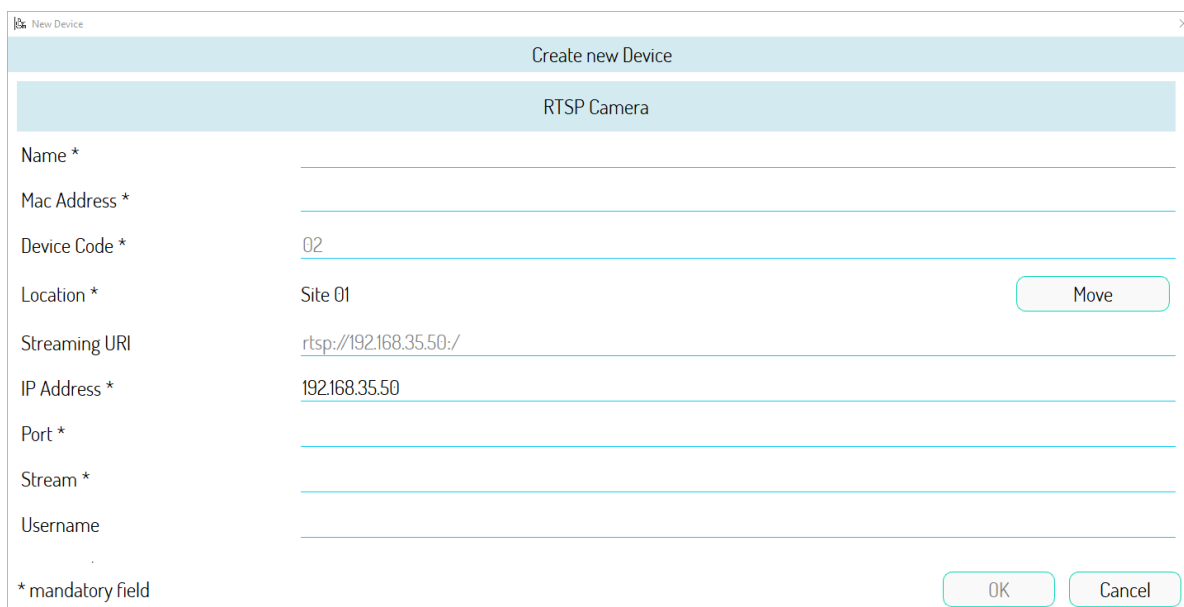


Figure 771: adding an RTSP camera to the IPerCom system

The “*IP Address*” field automatically reports the first available IP address among those present in the range of IP addresses defined in [Figure 770](#).

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 770](#) (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 770](#). 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:

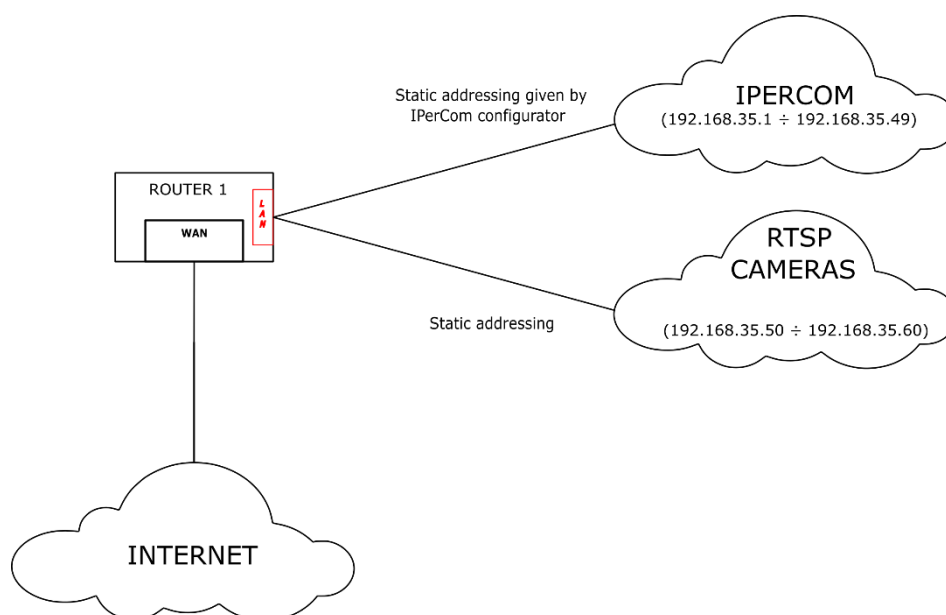


Figure 772: connection diagram for RTSP cameras and IPerCom devices

To create the diagram in [Figure 772](#), 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:

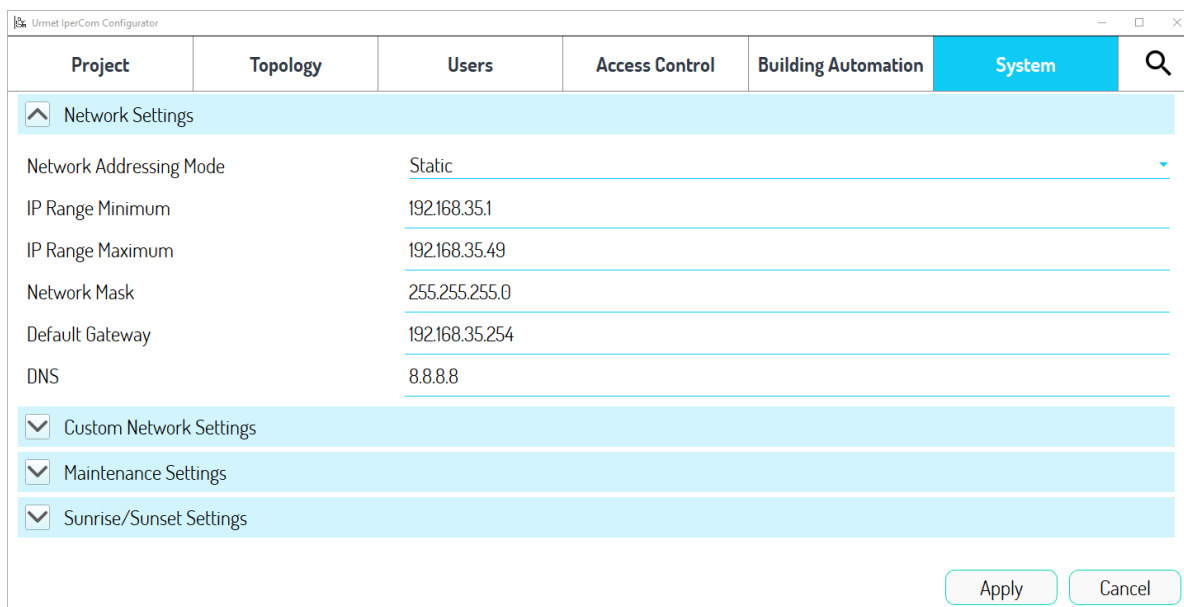


Figure 773: static network settings for IPerCom devices

### 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:

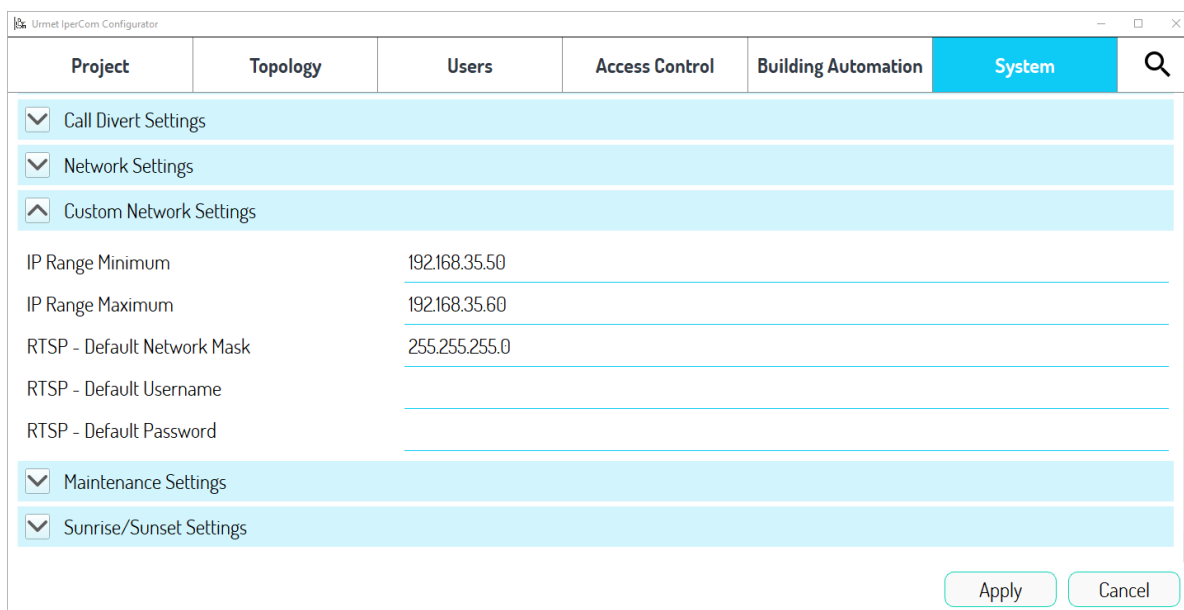


Figure 774: custom IP address range

### 3. Adding an RTSP Camera

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

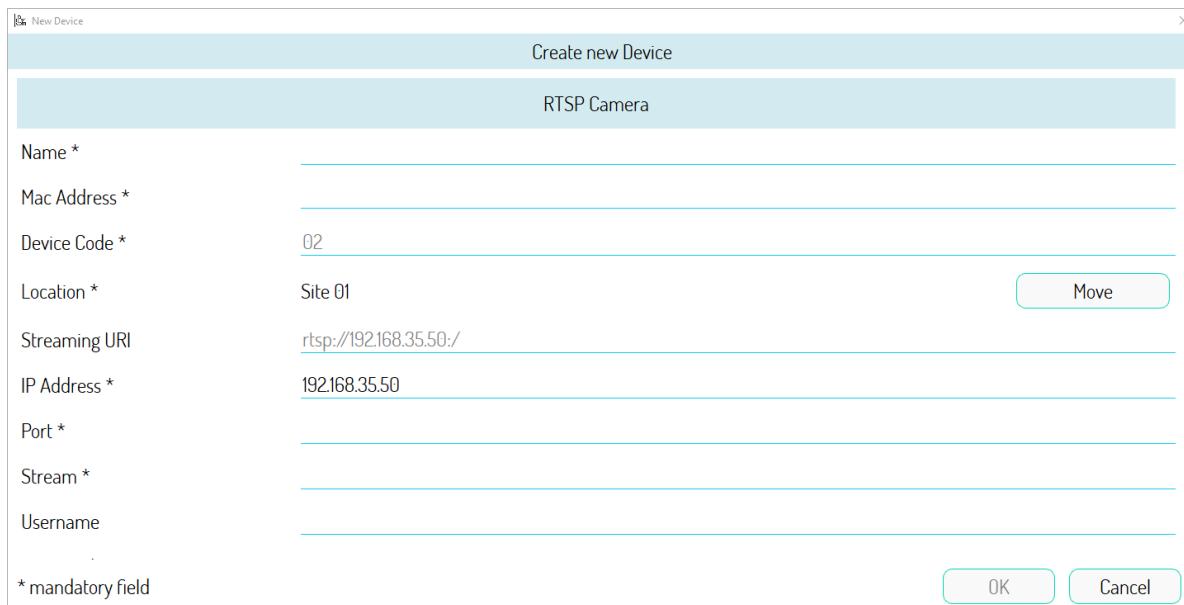


Figure 775: adding an RTSP camera to the IPerCom system

The “*IP Address*” field automatically reports the first available IP address among those present in the range of IP addresses defined in [Figure 774](#).

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 774](#) (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 774](#). 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:

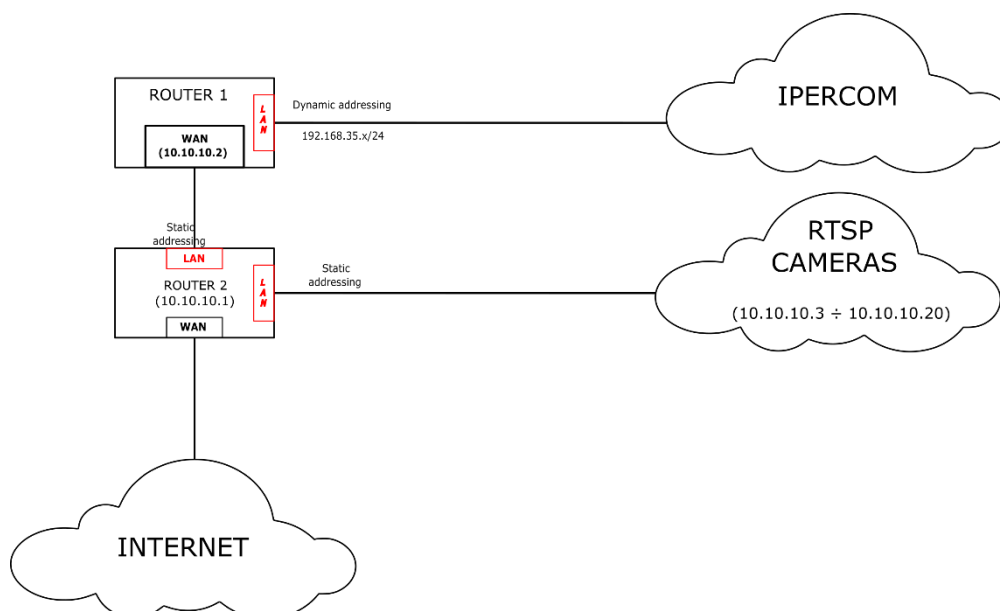


Figure 776: connection diagram for RTSP cameras and IPerCom devices

To create the diagram in [Figure 776](#), 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:

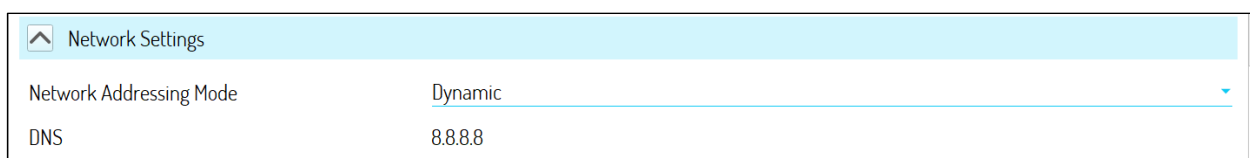


Figure 777: dynamic network settings for IperCom devices

### 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:

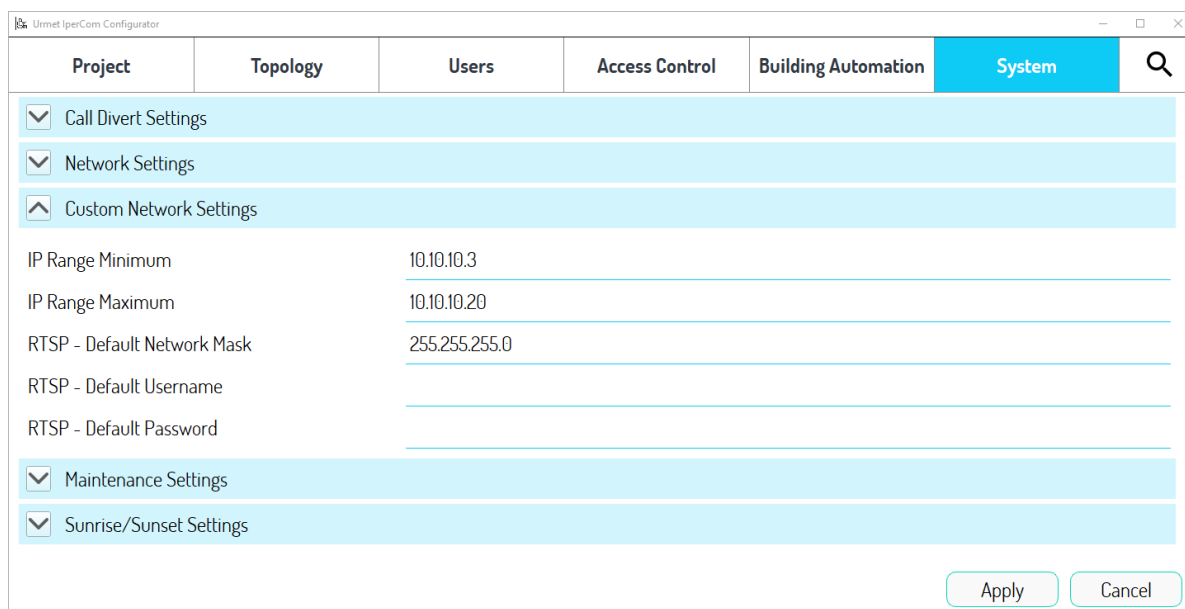


Figure 778: network settings RTSP Cameras

### 3. Adding an RTSP Camera

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

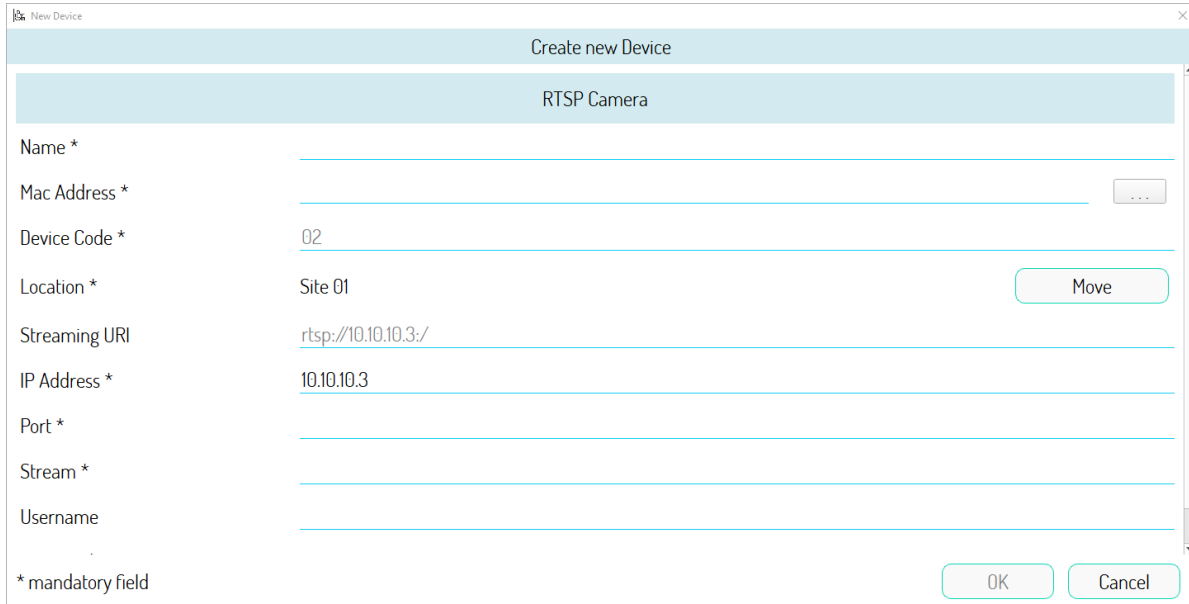


Figure 779: adding an RTSP camera to the IPerCom system

The “*IP Address*” field automatically reports the first available IP address among those present in the range of IP addresses defined in [Figure 778](#).

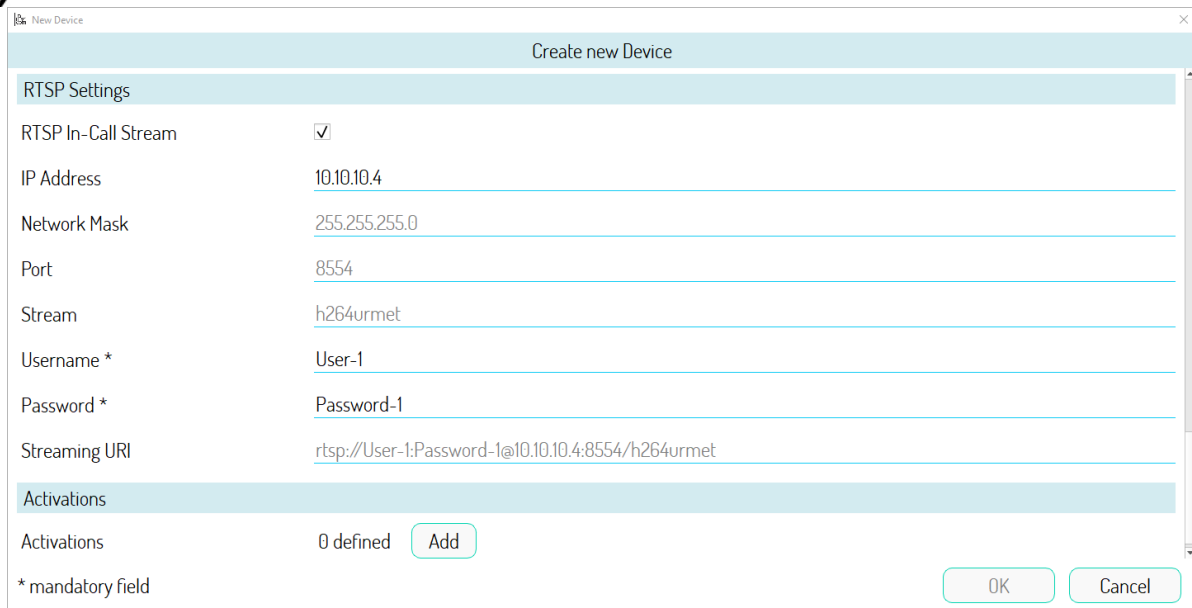
The proposed IP address must be the same as the one manually set in the *RTSP Camera* that you are adding into the configuration: if this is not the case, simply change it in the *configurator*.



The proposed IP address can be changed to another IP address even outside the range set in [Figure 778](#) (provided it has not already been used).



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



The screenshot shows a dialog box titled "Create new Device" with the following fields and values:

RTSP Settings	
RTSP In-Call Stream	<input checked="" type="checkbox"/>
IP Address	10.10.10.4
Network Mask	255.255.255.0
Port	8554
Stream	h264urmet
Username *	User-1
Password *	Password-1
Streaming URI	rtsp://User-1:Password-1@10.10.10.4:8554/h264urmet
Activations	
Activations	0 defined <input type="button" value="Add"/>

\* mandatory field

Buttons: OK, Cancel

Figure 780: enabled RTSP streaming of a calling station

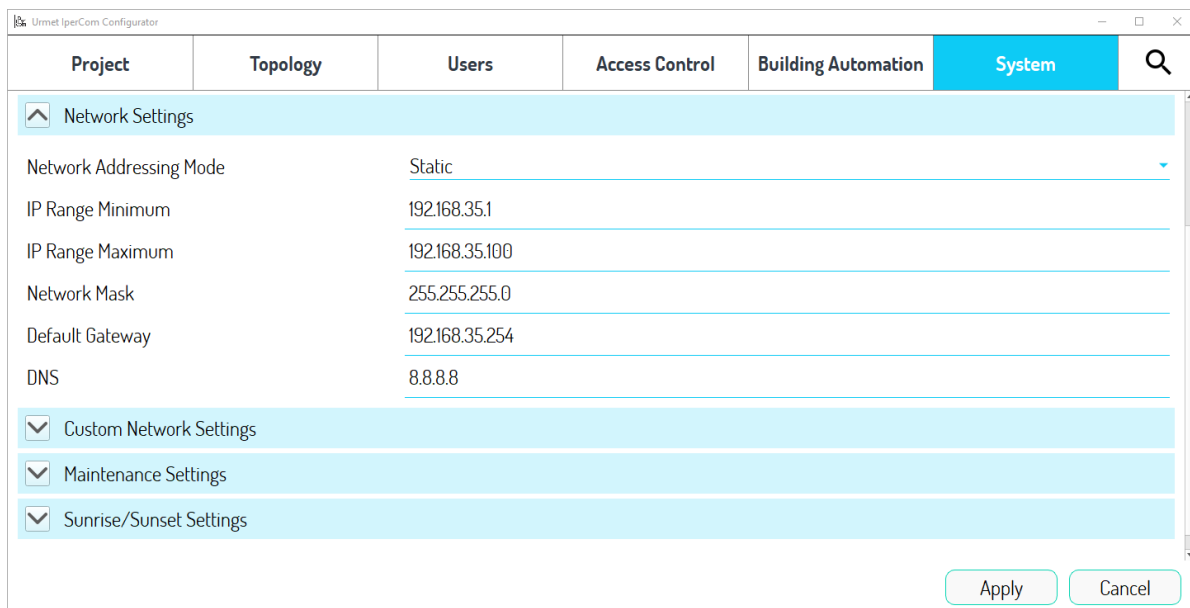
As written above, the "IP address" field automatically reports the first available IP address: this can be modified with another value which in this case, however, must be included in the range set in [Figure 778](#) (and must not already be been used).



The above works even if in [Figure 776](#) the IPerCom devices have static addressing.

## APPENDIX F2: 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:



The screenshot shows the 'System' tab of the 'Urmnet IperCom Configurator' application. The 'Network Settings' section is expanded, showing the following configuration:

Setting	Value
Network Addressing Mode	Static
IP Range Minimum	192.168.35.1
IP Range Maximum	192.168.35.100
Network Mask	255.255.255.0
Default Gateway	192.168.35.254
DNS	8.8.8.8

Below the network settings, there are three expandable sections:

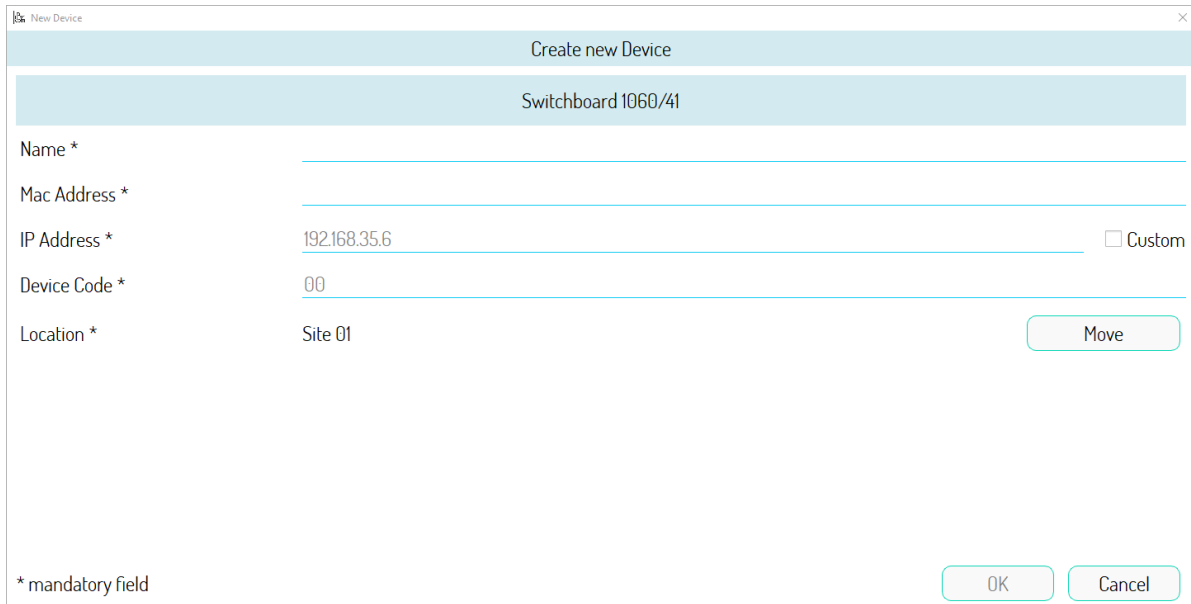
- Custom Network Settings
- Maintenance Settings
- Sunrise/Sunset Settings

At the bottom right of the window, there are 'Apply' and 'Cancel' buttons.

Figure 781: static network settings for IPerCom devices



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



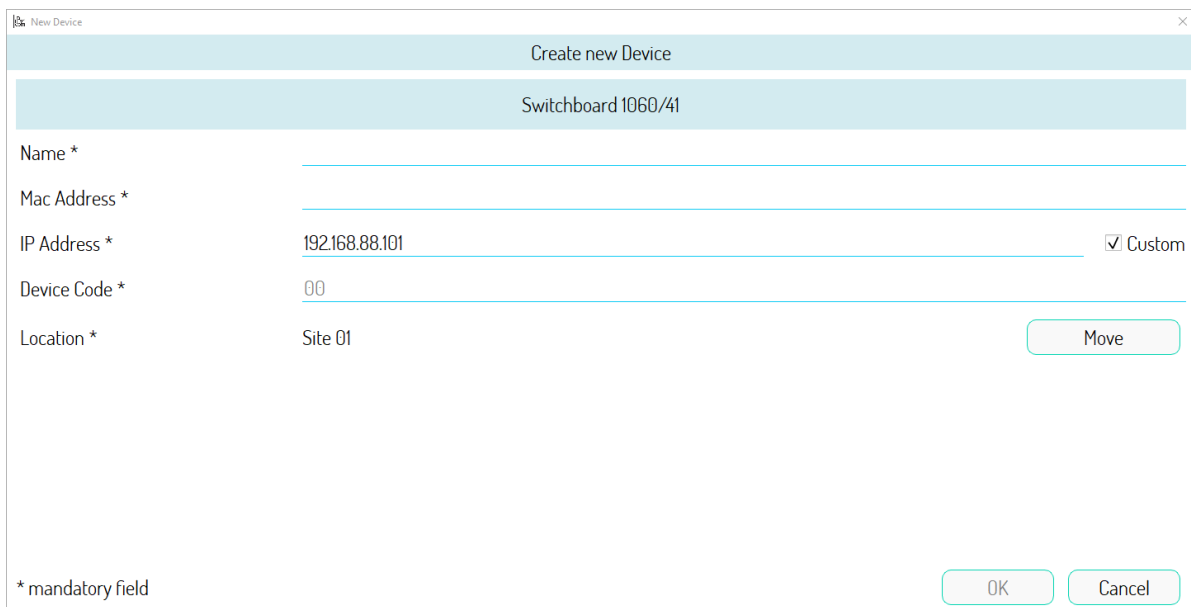
The screenshot shows a dialog box titled "New Device" with a subtitle "Create new Device". Below the subtitle is a header bar for "Switchboard 1060/41". The form contains the following fields:

- Name \*
- Mac Address \*
- IP Address \* with the value 192.168.35.6 and an unchecked checkbox for "Custom".
- Device Code \* with the value 00.
- Location \* with the value Site 01 and a "Move" button.

At the bottom left, there is a note "\* mandatory field". At the bottom right, there are "OK" and "Cancel" buttons.

Figure 782: adding an IPerCom device

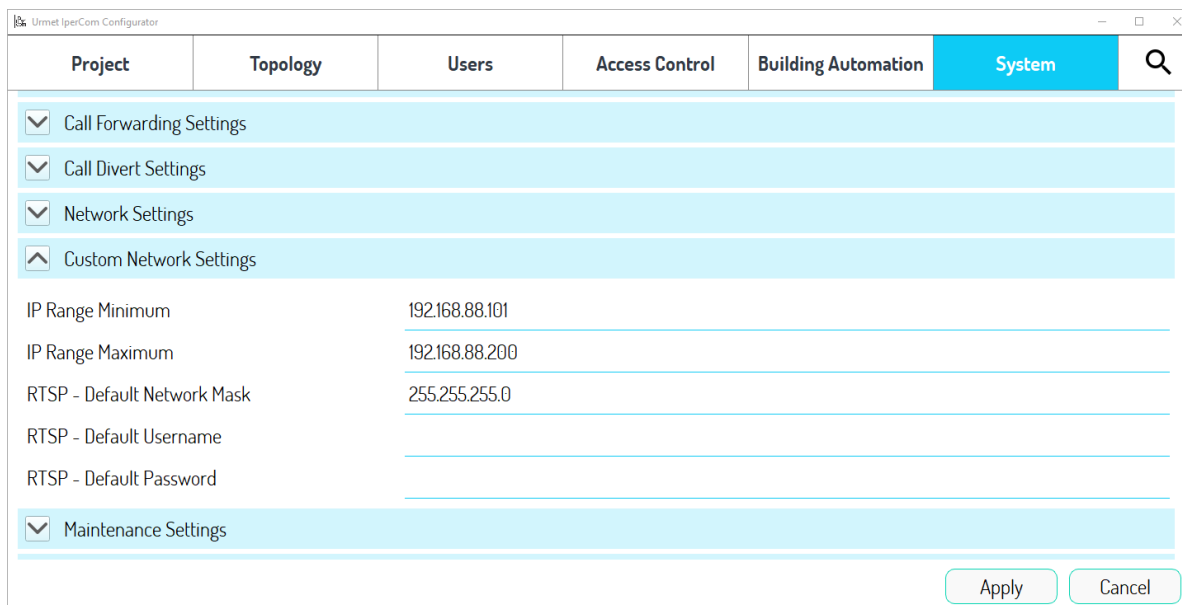
The "IP Address" field automatically reports the first available IP address proposed in the range of IP addresses defined in [Figure 781](#). This IP address can be modified if you select the "Custom" item:



This screenshot is identical to Figure 782, but with the "Custom" checkbox for the IP Address field checked. The IP address value is now 192.168.88.101.

Figure 783: 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:



Project	Topology	Users	Access Control	Building Automation	System
<input checked="" type="checkbox"/> Call Forwarding Settings					
<input checked="" type="checkbox"/> Call Divert Settings					
<input checked="" type="checkbox"/> Network Settings					
<input checked="" type="checkbox"/> Custom Network Settings					
IP Range Minimum		192.168.88.101			
IP Range Maximum		192.168.88.200			
RTSP - Default Network Mask		255.255.255.0			
RTSP - Default Username					
RTSP - Default Password					
<input checked="" type="checkbox"/> Maintenance Settings					

Figure 784: custom IP address range

To be able to modify the “IP address” field of [Figure 783](#) it is necessary to choose a value included in the IP address range of [Figure 784](#).

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 an automatic setting (for example if there is a router in the system) to a manual setting 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:

Network Settings	
Network Settings	Manual
IP Range Minimum	10.10.10.2
IP Range Maximum	10.10.10.200
Network Mask	255.255.255.0
Default Gateway	10.10.10.1
DNS	8.8.8.8

Figure 785: 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:

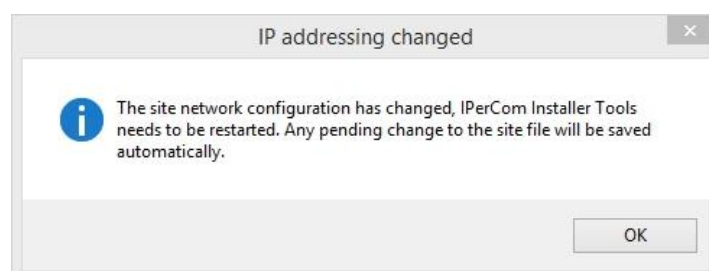


Figure 786: message on the modification of network parameters



*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 the following screen:

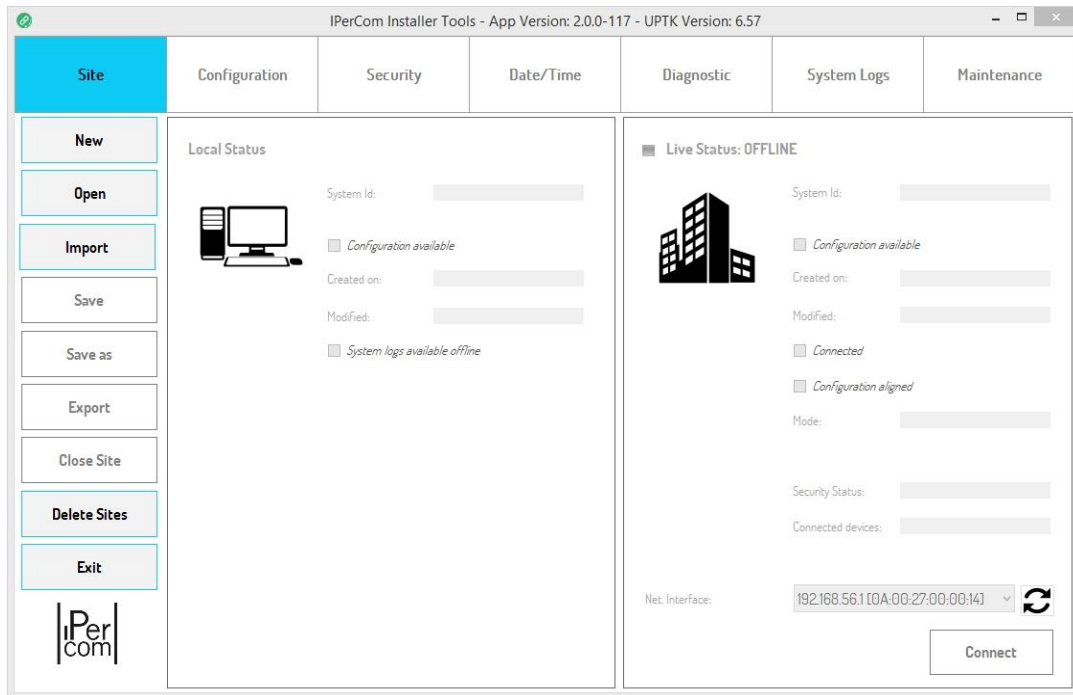


Figure 787: *iPerCom Installer Tools* screen after restart

Now it is necessary to open the project associated with the system and connect to it. When you press the "Connect" 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:

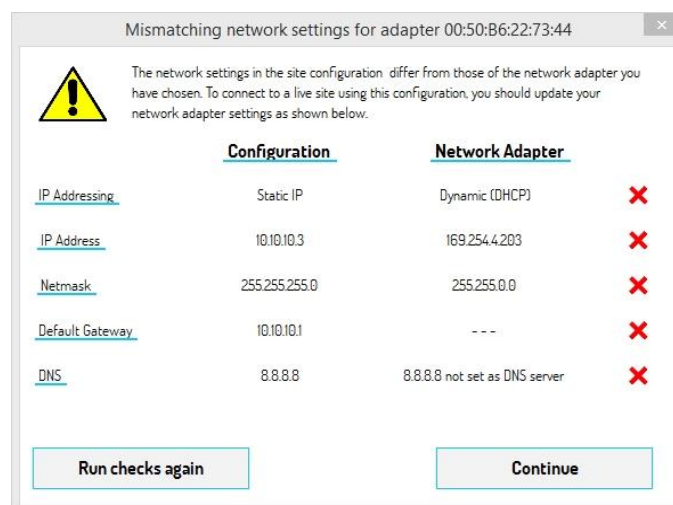





Figure 788: invalid network parameters

 If you press the **Continue** key 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:

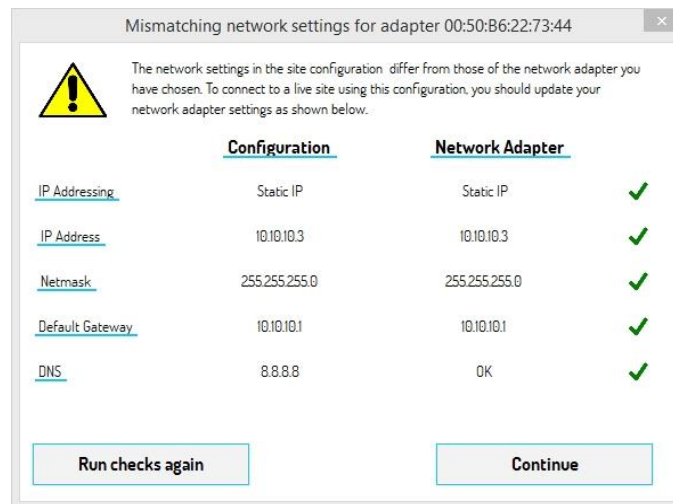


Figure 789: valid network parameters

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

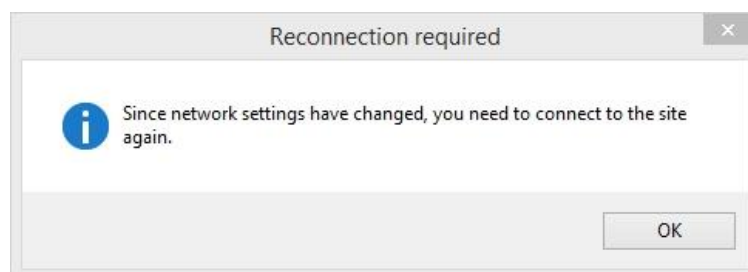


Figure 790: request for new connection to the system

Press OK, in the drop-down menu with the list of network cards with MAC and IP address you can find the previously modified network interface, i.e. the one with MAC address 00:80:80:8A:4C:4A and IP address 10.10.10.200. Once this interface has been selected, press the Connect button to reactivate the connection to the system.

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

As described in the previous paragraphs, during the commissioning of an IPerCom system it is necessary to correctly set the date and time. This can be done through *MAX video door phone* or *IPerCom Clock Module* or by simply connecting the system to the Internet via a router. Also the *IPerCom Installer Tools* application allows you to request the date and time from the system and, if they are wrong, set the right ones (i.e. those of the PC where the application is installed).

Correct date and time are essential for the *MAX video door phone* and the *IPerCom Installer Tools* application, as these are the only 2 tools that can distribute the configuration to the whole system and because date and time are used to identify which configuration file is more up-to-date than the current date.

If the distribution of the configuration on a system is mistakenly made by a *MAX video door phone* or 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 correctly reset, 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 after 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:

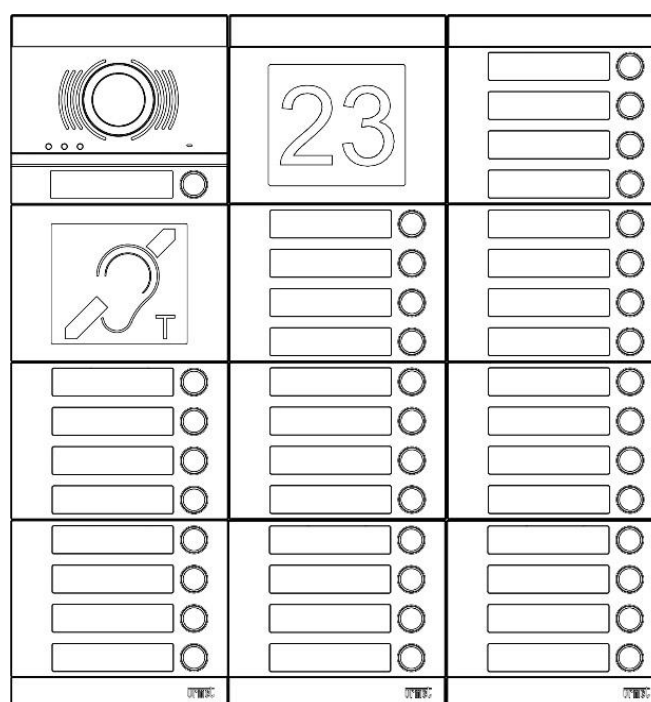
- export the configuration from the system to SD card (via *MAX video door phone*);
- make a change to the configuration and save: in this way the configuration setting is the current date and time;
- from the Maintenance tab of *IPerCom Installer Tools* press the Delete Configuration from Devices button;

Once the devices have finished deleting the configuration (e.g. the QR code is displayed on *MAX video door phones*), always import the previously saved configuration from *MAX video door phones* and distribute it.

If there are no *MAX video door phones* in the system, the same operation can be done with *IPerCom Installer Tools*. Simply import the configuration from the system and associate it to a project, save with the correct date, delete the configuration on the system and distribute the configuration with the current date.

## APPENDIX I: Modular entry panel with 1060/48 Alpha

Modular entry panel with a robust, essential, and advanced design that offers easy access to a full range of functions. The system, with modular elements, consists of modules (with or without white or black or gray plastic front units) that can be inserted on special wall frames. Its impact resistance is rated IK08, its protection against the infiltration of liquids and fine dust is rated IP55. Using special spacers, it is possible to couple the flush-mounting boxes or wall-mounting housings, so that entry panels of any type and configuration can be made, with a reduced number of components and consequently of cards to be managed in stock; the advantage is thus reflected both on the wholesaler and on the installer. The modules can be installed in a simple way, thanks to the connection cables (with connectors) supplied.



The figure above is an example consisting of the following products:

- IP audio video external unit module (Ref. 1060/48) with 1-key front unit (Ref. 1168/141).
- 4-key modules (Ref. 1168/4) with 4-key front unit (Ref. 1168/14).
- Optional building number module (Ref. 1168/50).
- ILA module and optional voice synthesis (Ref. 1168/48).

## Performance

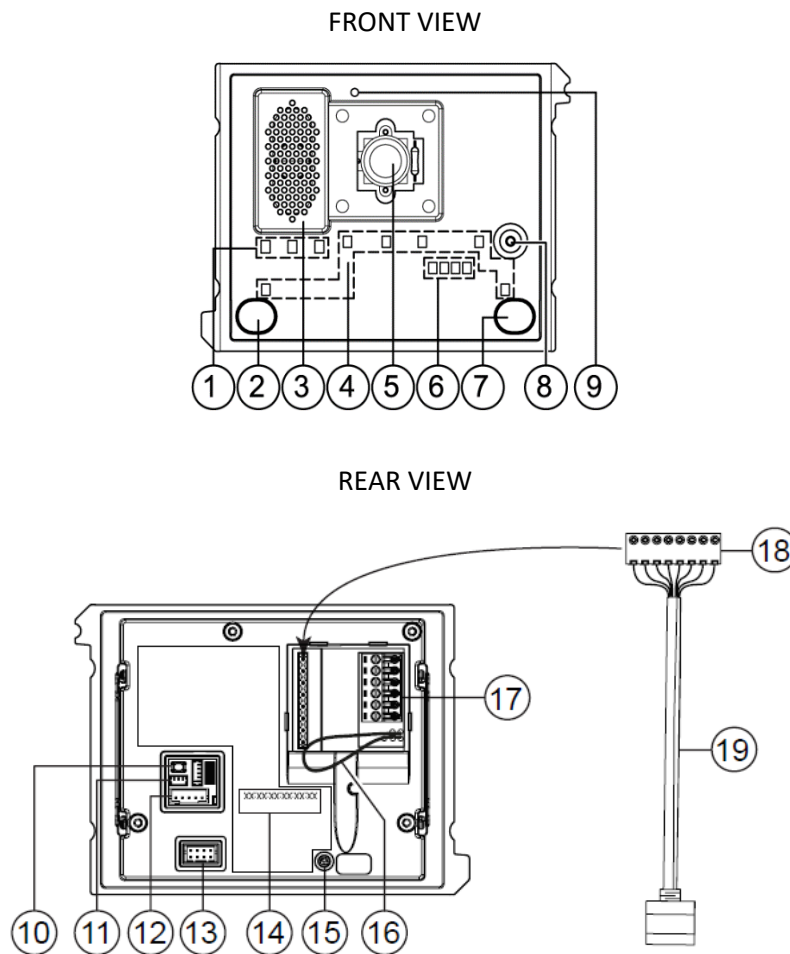
- Audio/video IP outdoor station module Ref. 1060/4.
- Possibility to supply a maximum of 12 modules in total:
  - Only one IP audio video external unit with its front unit (black or white or gray) with 0.1 or 2 keys;
  - ILA module with optional black, white, or grey speech synthesis.
  - only one optional proximity key reader module black or white or gray;
  - maximum 11 4-key add-on modules (Ref. 1168/4) with relevant front units (black or white or gray) from 1 to 4 keys, for a maximum of 45 keys on one row.
  - maximum 11 8-key add-on modules (Ref. 1168/8) with 4 to 8 keys with relevant front units (black or white or gray), for a maximum of 90 keys on two rows;
  - maximum 11 optional building number modules black or white or gray;
- Entry panel configuration through the *Ipercom Installer Tools* application.
- POE connector for LAN connection.
- Protection system against incorrect wiring of the single module.
- Optical signals via system status LEDs (DDA).
- Pedestrian electric lock actuation by capacitive discharge and holding current.
- Pedestrian electric lock actuation programmable from 1 to 90 seconds.
- Entrance hall button.
- Driveway (gate) electric lock actuation with clean contacts.
- Input for door status sensor.
- Speaker sound level adjusting trimmer.
- Name tag activation with twilight sensor that can be deactivated.
- Wide-Angle colour camera.
- Camera lighting LED.

Below is the description of the modules that make up the modular entry panel with 1060/48 ALPHA. About the item numbers available in different colours, reference will be made to those in black. A list of all item numbers (including those available in various colours) is given below.



## Audio video external unit IP Ref. 1060/48







### Structure



1. DDA LED
2. "USER 0" calling button
3. Speaker
4. Name tag and button light LED
5. Camera
6. Camera lighting LED
7. "USER 1" calling button
8. Microphone
9. Dusk sensor for automatically switching on the name tag lighting
10. Reboot/reset to default settings button (RESET)

11. Connector for hearing aid coil (ILA) Ref. 1168/48
12. USB connector for connecting to display module 1168/1
13. Module connection wire connector (OUT)
14. Label with MAC ADDRESS of the device
15. Trimmer for adjusting speaker volume (RV1)
16. Jumper provided to connect the door state sensor
17. Terminal board
18. POE connector for connecting to the LAN.
19. RJ45 adapter for connection to the POE connector

## Description of terminals

 	 	<b>PA</b>	Hall button
 	 	<b>SE2</b>	Garage relay contacts
		<b>SE -</b>	Pedestrian electrical lock with capacitance discharge actuation negative
		<b>SE +</b>	Pedestrian electrical lock with capacitance discharge actuation positive

## Technical specifications







Power voltage POE: .....	<b>37÷54 V<sup>~</sup></b>
Consumption @ 48V	
Standby: .....	<b>&lt; 40 mAcc</b>
Full rate: .....	<b>&lt; 270 mAcc</b>
LAN maximum operating distance: .....	<b>100 m con CAT5</b>
Dimensions (WxHxD): .....	<b>119 x 89 x 32 mm</b>
Working temperature range: .....	<b>-10 °C ÷ + 50 °C</b>

## Operation

### Calls

Up to 90 users max. can be called by pressing the respective buttons of the push button panel associated to the camera.

## DDA (Disability Discrimination Act) led actuation - system status indication

- The system state is shown by the following indications which appear on the door unit front:
- call in progress: LED  on green and voice message "CALL IN PROGRESS".
- line engaged: LED  on red and voice message "THE LINE IS BUSY".
- off-hook waiting time expired: voice message "THE USER IS NOT ANSWERING":
- conversion in progress: LED  on orange;
- conversation paused by the switchboard: LED  on green and LED  fl ashing orange;
- door open: LED  green and "THE DOOR IS OPEN" voice message".

## Pedestrian lock actuation

The door unit has two terminals for managing the pedestrian door lock (SE+ and SE-).

The electric lock is operated in the following cases:

- whenever the hall button is pressed (terminals PA);
- when a door open command is received from an apartment station according to the configuration ("free" or "privacy").

## Garage gate lock actuation

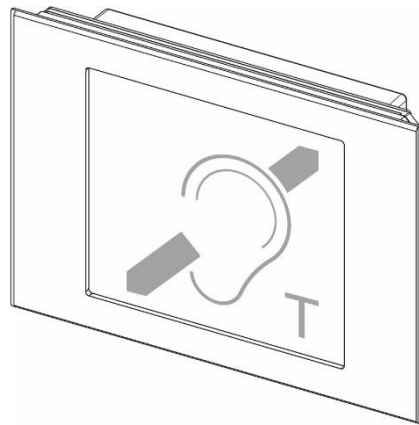
The IP audio-video door units have two terminals (SE2) connected to the contacts of a normally open relay which can be used to control a gate opening control unit (\*). The relay is operated for 1 second after receiving the garage door opening command according to the operating mode ("free" or "privacy") as the door lock.

(\* ) *The relay is NOT suitable to control direct power loads and can only be used as control relay.*


## Volume adjustment

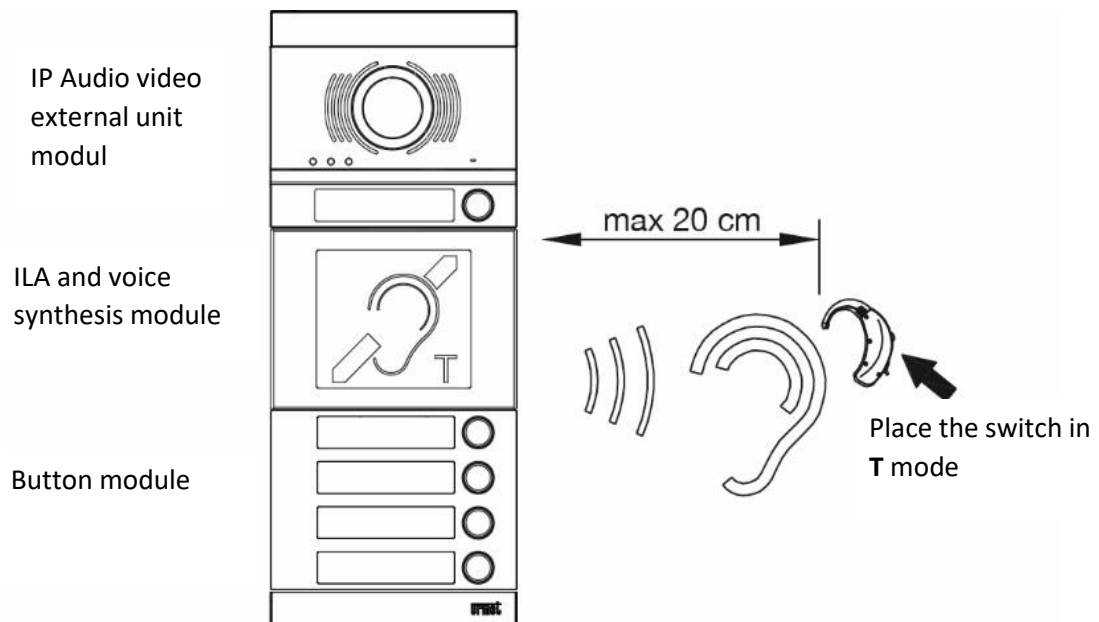
Volume levels are calibrated by default so not to require adjustments in most cases. Use a screwdriver to adjust the speaker volume (15), if required.

ILA and voice synthesis module ref. 1168/48



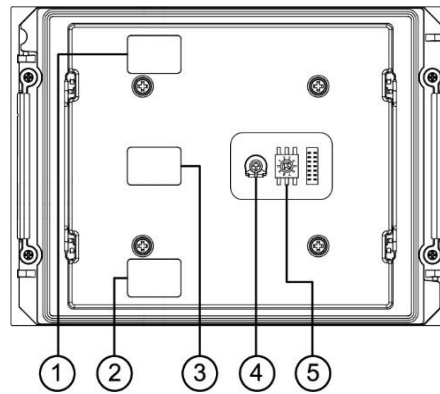
The ILA and voice synthesis module is a modular device designed to allow hearing aid users to hear the door unit audio and be notified of system state by means of auditory indications.

To interface with the calling unit, the user must approach the hearing aid (with T function) to the front part of the device, no further than 20 cm, near the name tag 



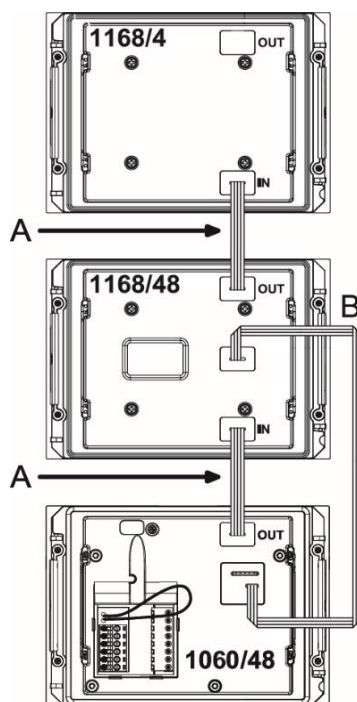
## Structure

REAR VIEW



1. Module connection wire connector (IN)
2. Module connection wire connector (OUT)
3. Audio wire connector (ILA)
4. Potentiometer for adjusting the speech synthesis volume
5. Rotary selector for selecting speech synthesis

## Installation



The ILA module must be positioned immediately near the door unit. The modules must be connected by means of the three-wire audio cord provided.

<b>A</b>	8 cm long cord provided with button module and expansion unit Ref. 1168/4 of the ILA and voice synthesis module Ref. 1168/48.
<b>B</b>	20-cm cord provided with ILA and voice synthesis module Ref. 1168/48

## Speech synthesis language selection

The language is selected by means of the rotary selector (5) in the rear part of the module as shown in the following table.

Rotary selector position	Associated language
1	Italian (default)
2	English
3	Franch
4	German
5	Spanish
6	Dutch
0 – 7 – 8 – 9	Vocal messages deactivated



*To make the programming changes active, power supply to the device must be disconnected and powered up again.*

## Speech synthesis volume adjustment

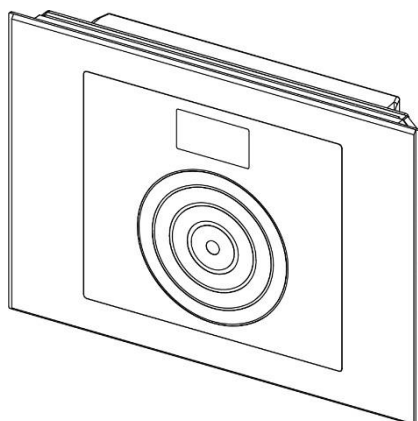
Volumes are calibrated by default so not to require adjustments in most cases. Use a screwdriver to adjust the volume, if required.

## Technical specifications

Voice message acoustic pressure: ..... **80 dB a 10 cm**

Working temperature range: ..... **-25 ÷ 40° C**

## Proximity key reader module Ref. 1168/45



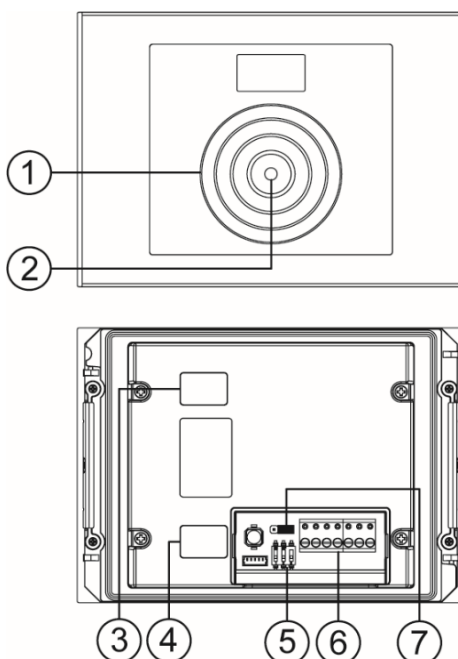
The device Ref. 1168/45 is the proximity key reader. It has following operating modes:

- Audio-video door IP unit Ref. 1060/48



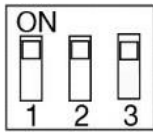
Only one module 1168/45 can be installed for each call station.

## Structure



1. Proximity key sensor
2. Two colour LED (red/green)
3. Module connection cable connector (IN)
4. Module connection cable connector (OUT)
5. Configuration dip switches used for:





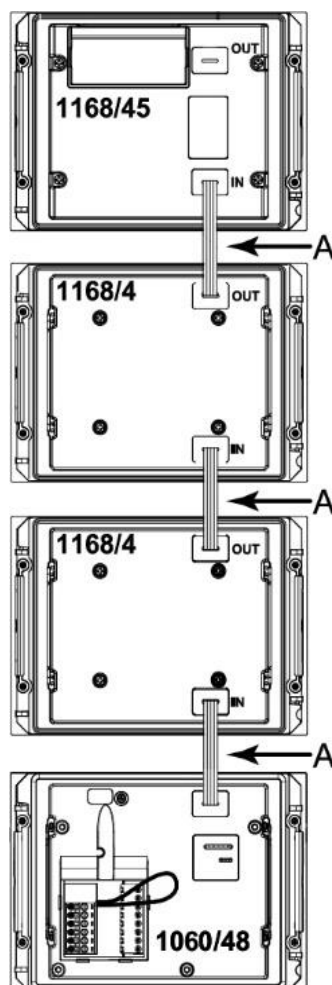
1. **indicating LED state:** ON enable (default)  
OFF disable
2. **Do not change the arrangement of this dip switch**
3. RS485 BUS: Ipercom mode

6. Terminal board
7. Jumper for power from Ipercom system

The device must be positioned as the last module on the panel. Respect the installation constraint of maximum **12** modules of which only one is a 1168/45 module. The pedestrian lock activation time must be programmed on the door unit.

The keys configuration must be configured through the *configurator*, refer to the following paragraphs: [Residents](#) and [Not residents](#).

## Installation



<b>A</b>	8 cm long cord provided with modules Ref. 1168/xx.
----------	--

## Performance

Permits timed opening (from 0 to 99 seconds) when a user proximity key is placed close to the front panel.


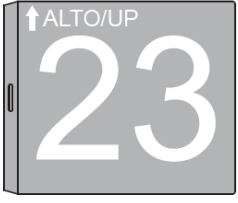
The two-color LED, if enabled, displays the recognition of a proximity key approached to the front by changing color (from red to green).

## Building number module Ref. 1168/50

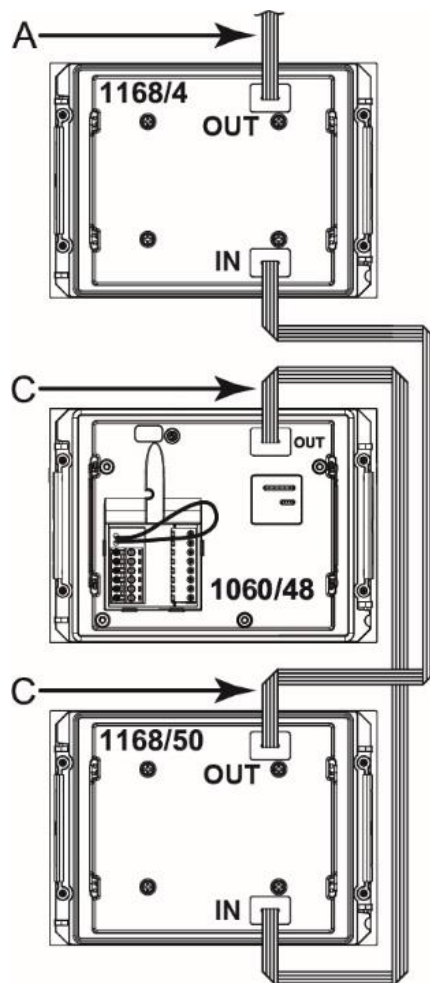


Below is a list of the name tags that come with the product according to the different colours available.

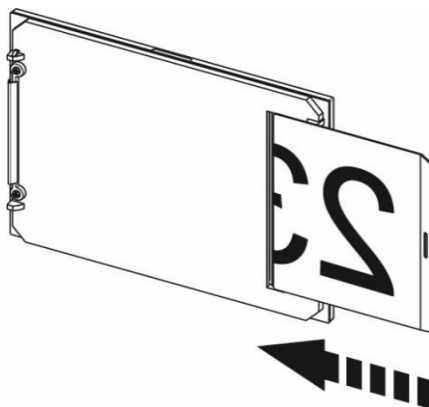
<p><b>Ref.1168/50-50W-50G:</b> Temporary transparent name tag.</p>	
<p><b>Ref.1168/50:</b> Black name tag supplied with the module; the name tag can be written by engraving.</p>	

<p><b>Ref.1168/50W:</b> Opaline white name tag supplied with the module; the name tag can be written by means of decals.</p>	
<p><b>Ref. 1168/50G:</b> grey name tag supplied with the module; name tags are engraved.</p>	

## Installation

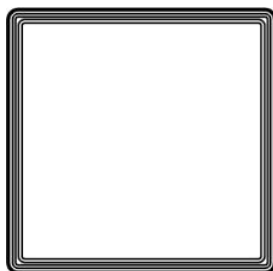


<b>A</b>	8 cm long cord provided with button module and expansion unit Ref. 1168/4 or 1168/8 of the building number module Ref. 1168/50
<b>B</b>	38 cm long cord provided with building number module Ref. 1168/50.



*The name tag can only be fitted or replaced after the front unit of the module has been removed.*

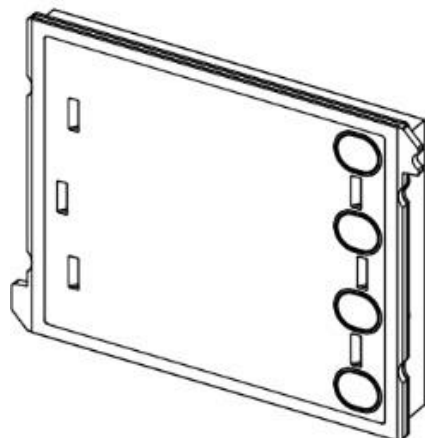
### Blind module Ref. 1168/59



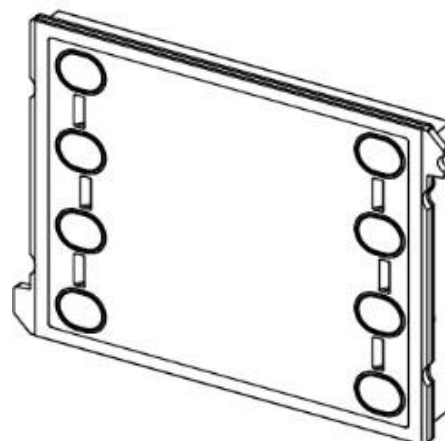
This module is used to fill in spaces which are not used in modular applications as required.

## 4-Button module Ref. 1168/4 and 8-Button module Ref. 1168/8

4-BUTTON MODULE



8-BUTTON MODULE



The 4-button or 8-button modules can be used to expand the number of users on the panel. Up to 88 buttons can be connected (in addition to the two already present on the door unit), using up to 11 button modules Ref. 1168/8.

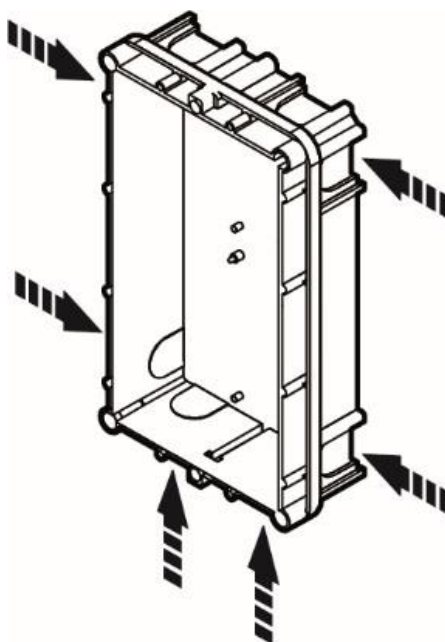
### Flush-mounted panel accessories

#### Flush-mounting boxes

For different versions of flush-mounting boxes for ALPHA range products are provided according to the number of modules to be housed:

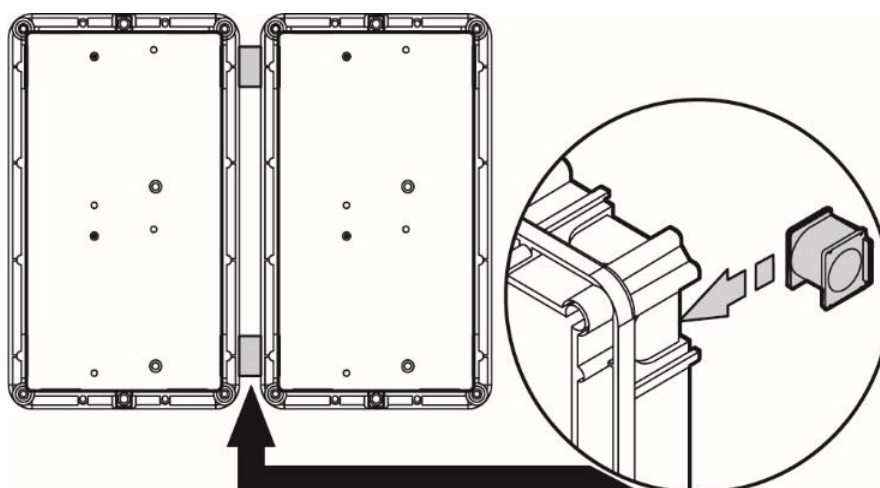
- For 1 module **Sch. 1145/51**
- For 2 modules **Sch. 1145/52**
- For 3 modules **Sch. 1145/53**
- For 4 modules **Sch. 1145/54**

System wires lead into the boxes through the openings on the sides and bottom of the box. All openings are shut by removable closures.



### Joining flush-mounting boxes

Flush mounting boxes can be assembled with suitable spacers, also used as wire hole. Up to 3 4-module flush-mounting boxes can be assembled (12 modules in total). If wall cover frames are used, instead, up to 3 3-module boxes (9 modules in total) can be assembly, joining them on the longer side. All spacers are empty, to allow the passage of wires from a box to another one.



## Module holder frames

The module holder frames allow quick and easy ALPHA module assembly (either single or double). A hinge is provided in the lower part of the frame to tip the modules and facilitate wiring and adjustment.

Available versions are:

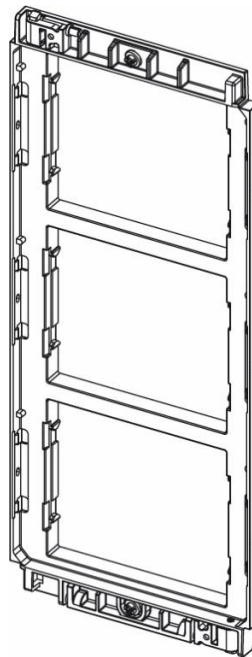
- For 1 module
- For 2 modules
- For 3 modules
- For 4 modules

**Sch. 1168/61**

**Sch. 1168/62**

**Sch. 1168/63**

**Sch. 1168/64**



## Wall cover frame

These frames are used to conceal irregularities of the wall in the flush mounting area surrounding the panel; insert the cover frames between modules and wall.

The following anodised aluminium frames are provided:

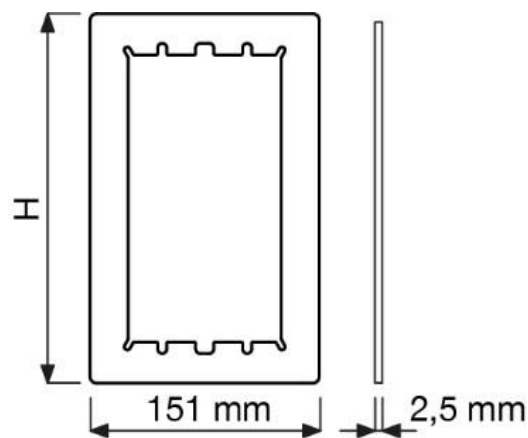
- 1-row frame for 1 module
- 1-row frame for 2 modules
- 1-row frame for 3 modules
- 1-row frame for 4 modules

Sch. 1168/611

Sch. 1168/612

Sch. 1168/613

Sch. 1168/614

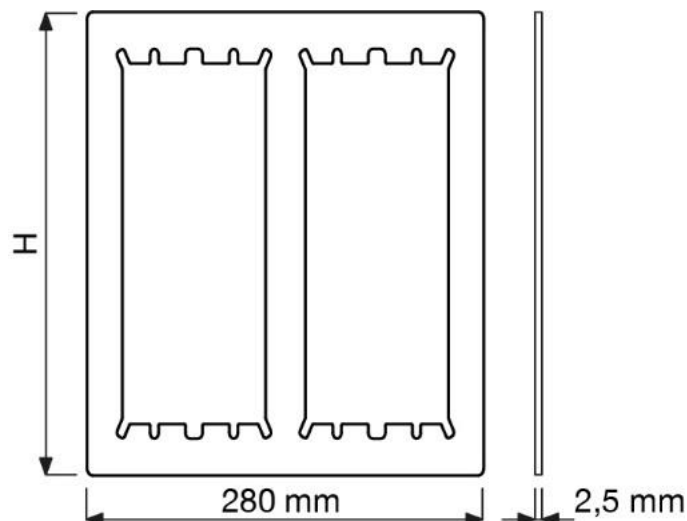


H is 148, 238, 328 and 418 mm for the 1, 2, 3 and 4 module versions, respectively.

- 2-row frame for 4 modules
- 2-row frame for 6 modules

Sch. 1168/624

Sch. 1168/626

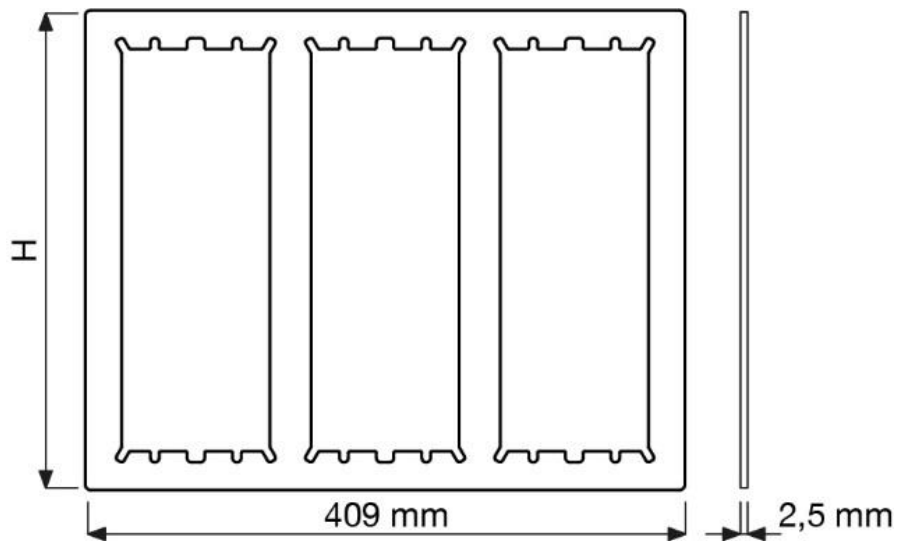


H is 238 and 328 mm for 2 and 3 module versions, respectively.



- 3-row frame for 9 modules

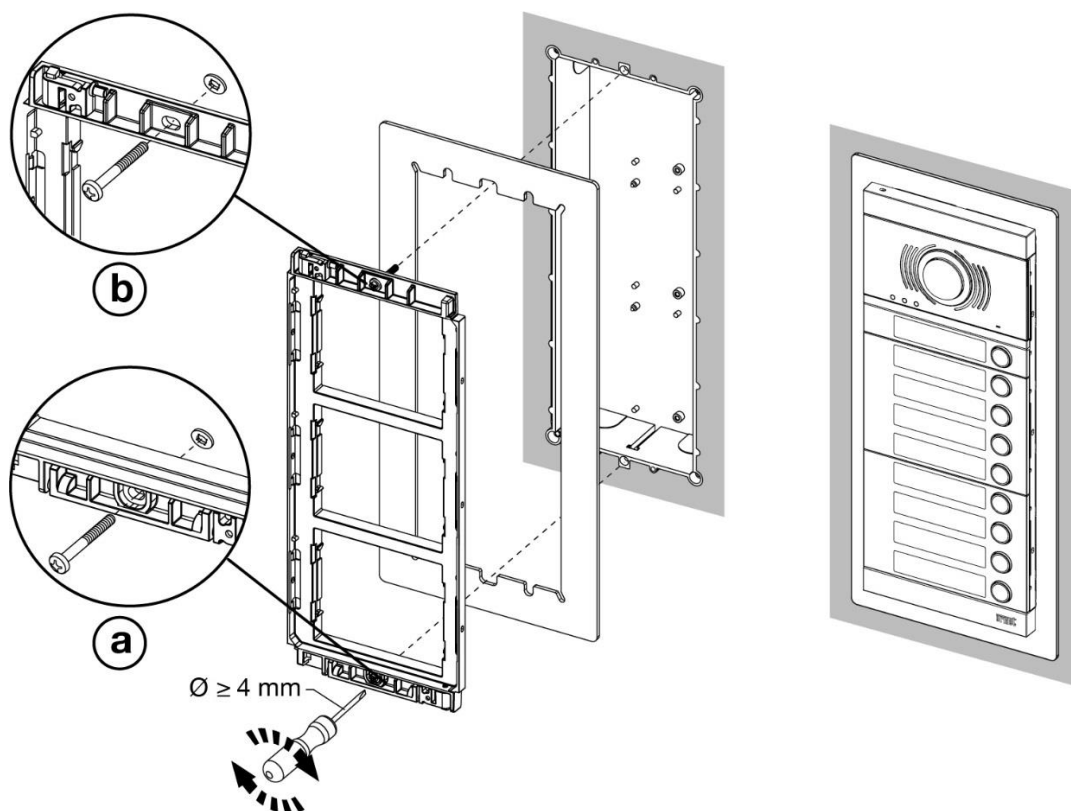
Sch. 1168/639



H is 328 mm for 3 module versions.

### Wall frame cover installation

Embed the flush mounting box in the wall, position the wall cover frame and fasten the module holder lower screw. Frame fastening is completed by tightening the upper frame screw last.



## Wall-mounted panel accessories

### Casings with frame

The casings can be used for wall-mounted installations without embedding.

The following versions are provided with module holder frame:

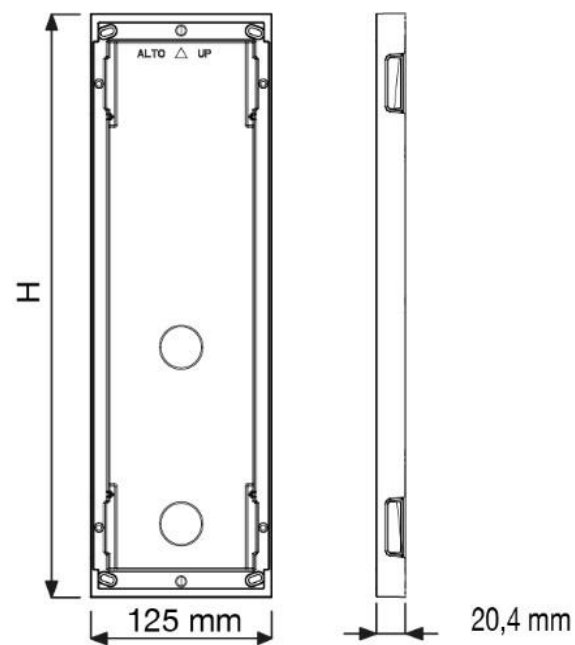
- For 1 module
- For 2 modules
- For 3 modules
- For 4 modules

**Sch. 1168/311**

**Sch. 1168/312**

**Sch. 1168/313**

**Sch. 1168/314**

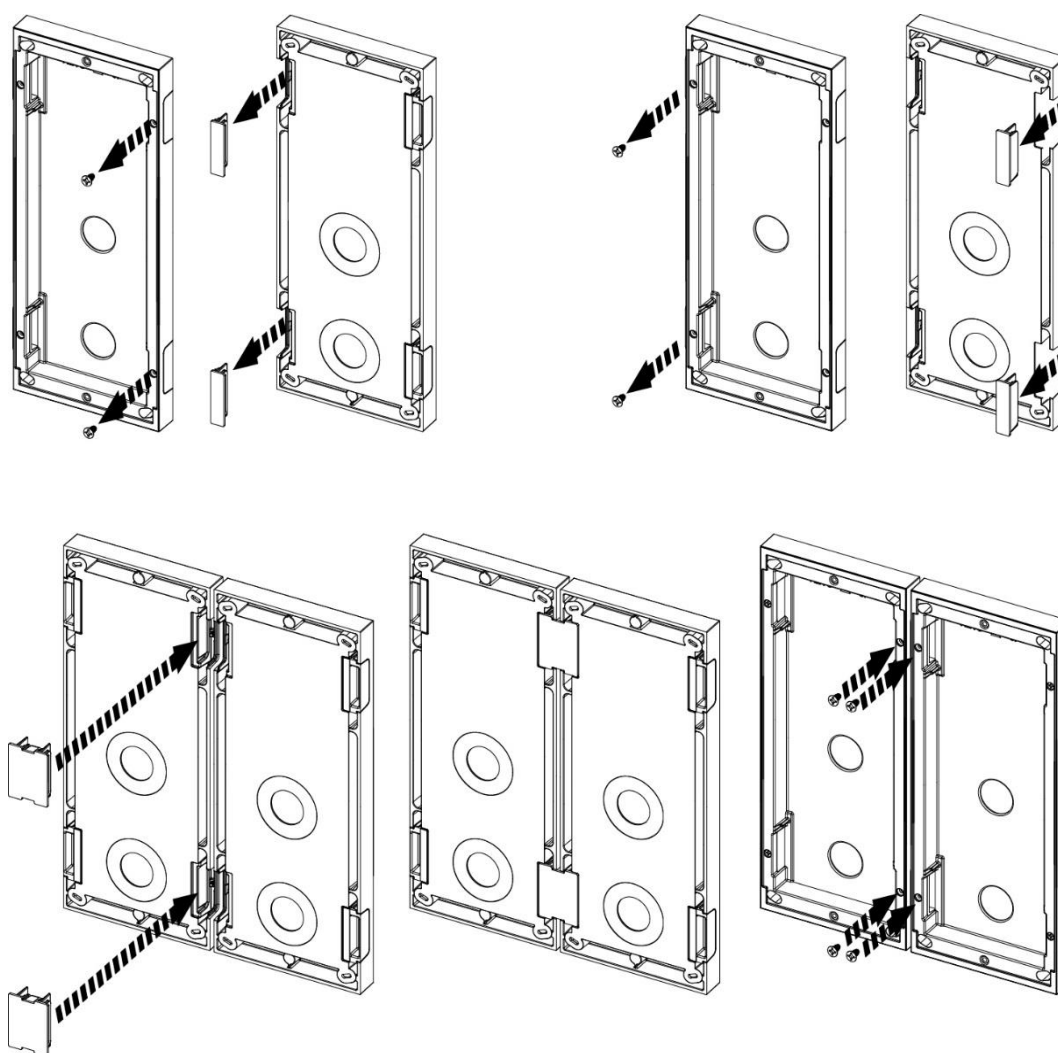


H is 126, 217, 306 and 396 mm for the 1, 2, 3 and 4 module versions, respectively.

## Casing and frame joiner

The casings with frames may be joined by means of shims which double as spacers. Up to 3 4-module flush-mounting boxes can be assembled (12 modules in total).

All shims are hollow to allow the passage of wires from one box to the other.



## Panel accessory in common to both versions

### Rain hood cover

They are useful to make the panel installation weatherproof.

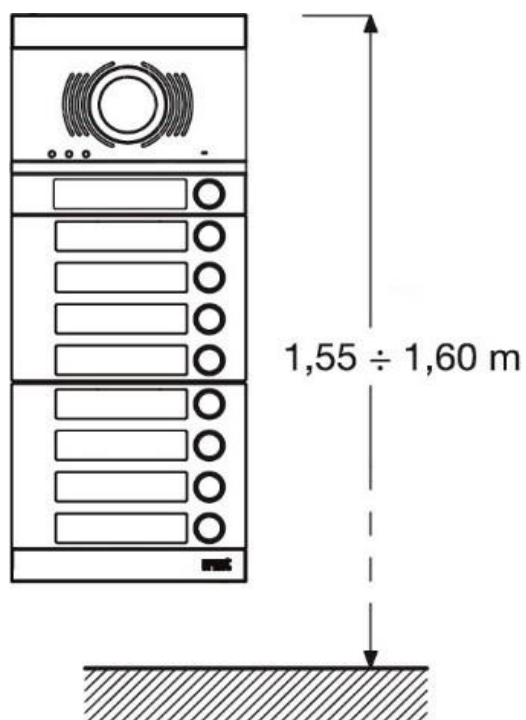
- For 1 module

Sch. 1168/401

The hoods are inserted instead of the upper headers.

## Alpha entry panel with 1060/48 installation

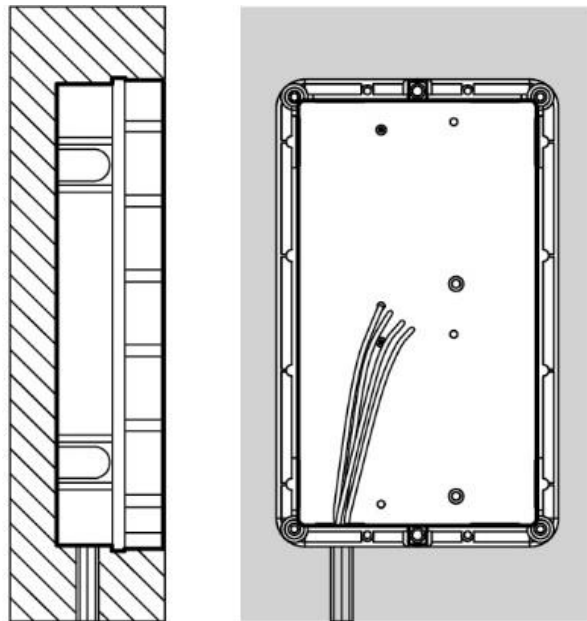
It is suggested to install the modules at the height shown below, according to the system to be realized.



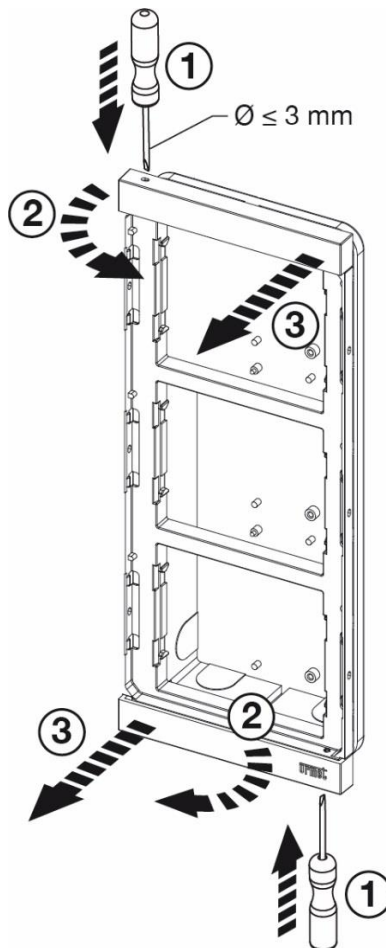
However, for complex systems with several modules, for a correct installation consider the height shown in the figure to fix the camera. If the system is a door phone, height refers to the door unit.

## Flush-mounted version

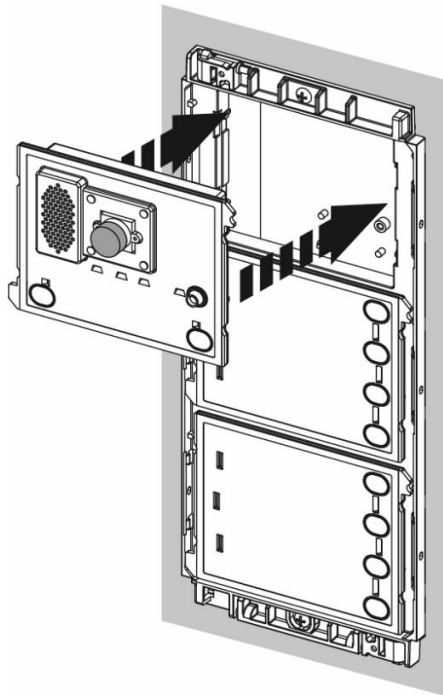
- Prepare the flush-mounting hole for the passages of the connecting wires.
- Install the flush mounting box: it must not jut out of the wall.



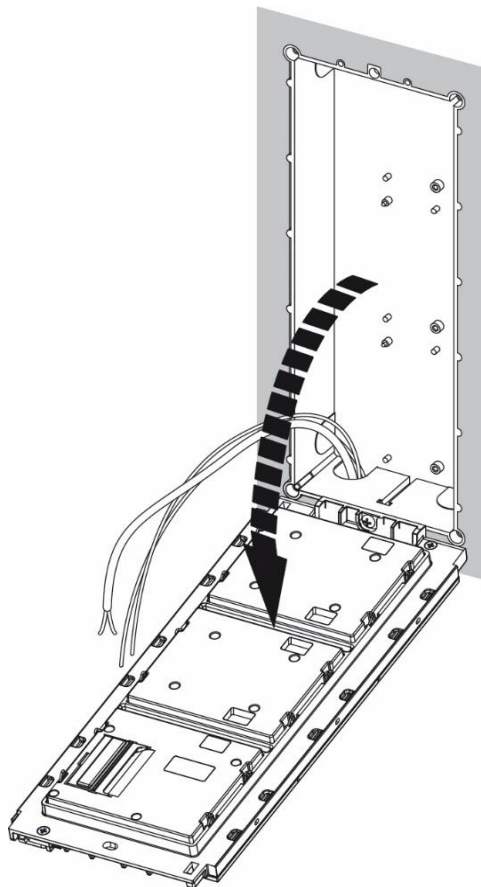
- Remove the upper header and the lower header from the frame using a flat screwdriver at the tip 0.



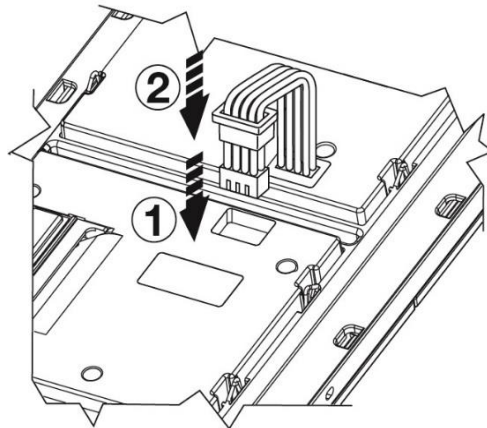
- Fit the module holder frame



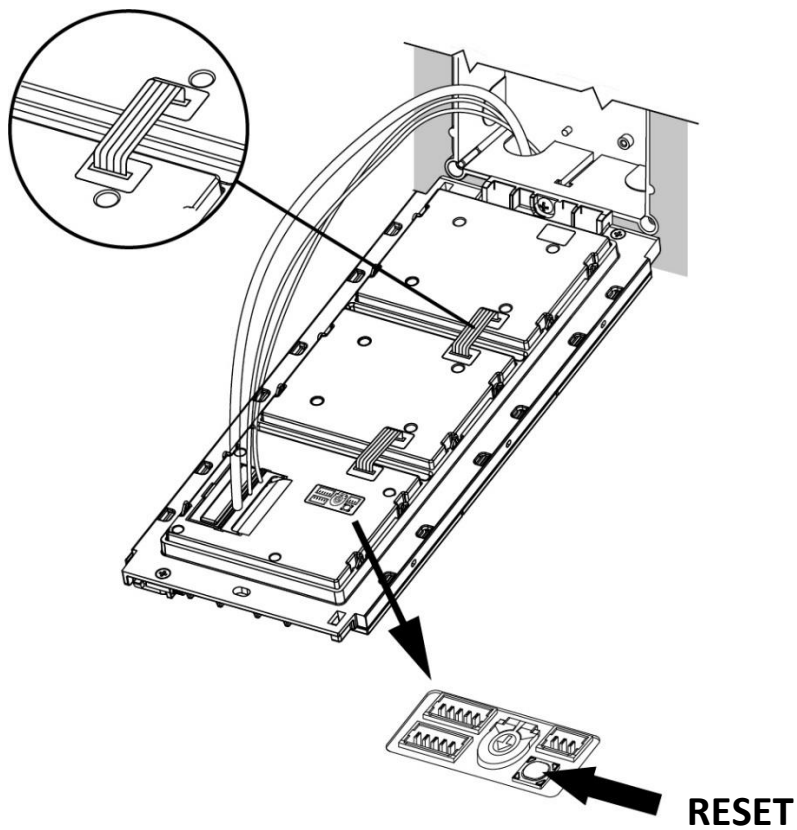
- Tip the holder frame and connect the wires.



- Adjust correct perpendicularity of the panel.
- Establish the connections between the various modules with the wires provided before powering the system.

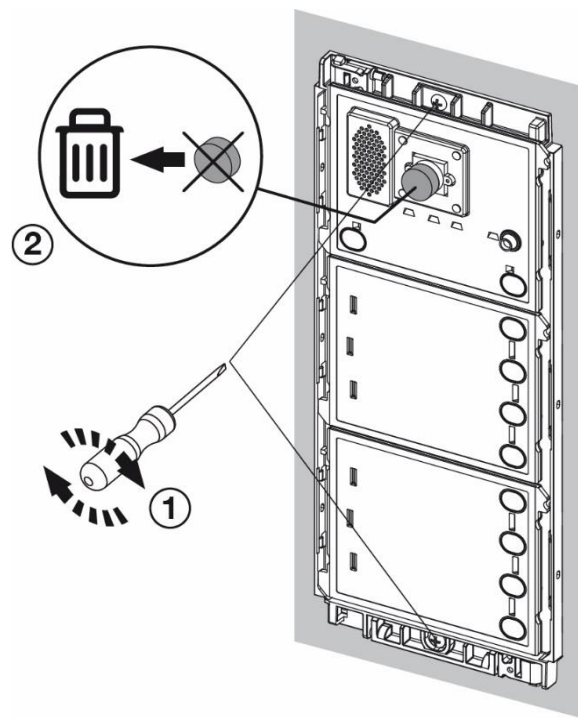


- Use the cord provided with the frame to connect modules belonging to frames arranged side by side.
- On the last module be sure to protect the OUT connector using the cap provided.





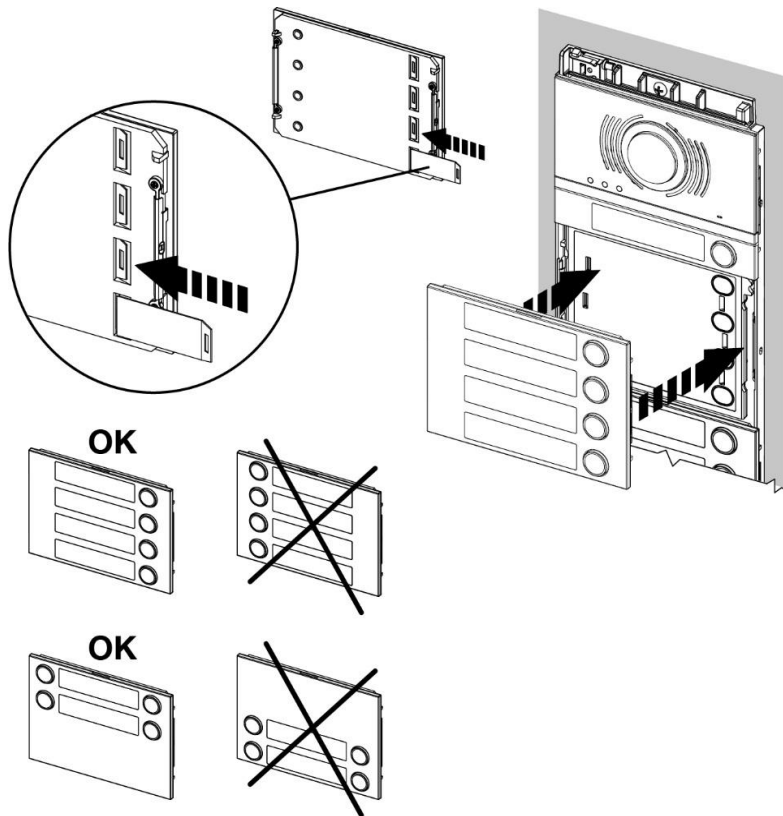
- On the rear of the external unit there is the RESET key which must be pressed to restart or reset the device to factory settings.
- Close the frame by tightening the screws.



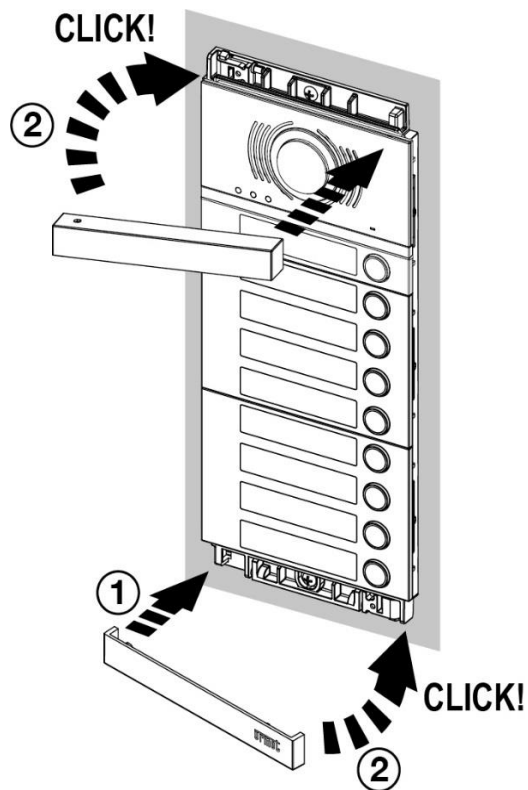
- Insert the name tags in the front panels Clip the front panels onto the frame.



*When hooking the front unit to the wall frame, make sure to keep the buttons on the right side of the entry panel.*

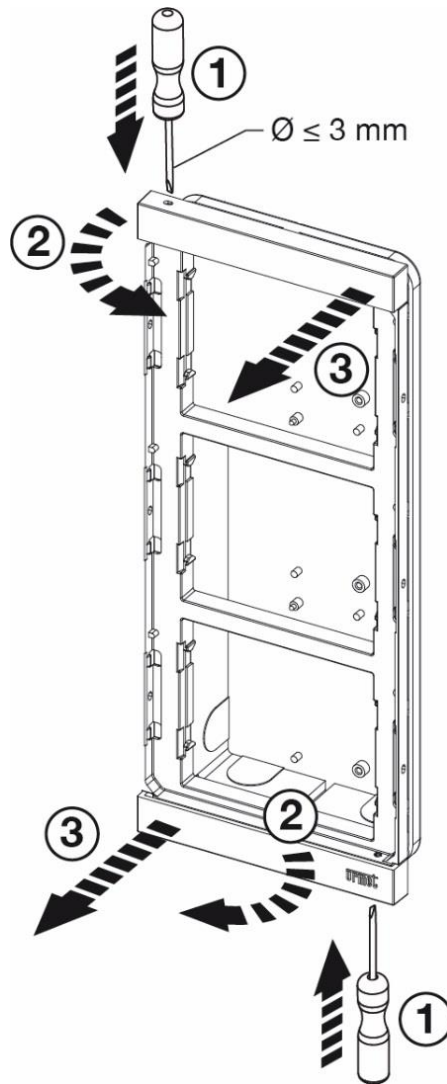


- Attach upper header and lower the frame.



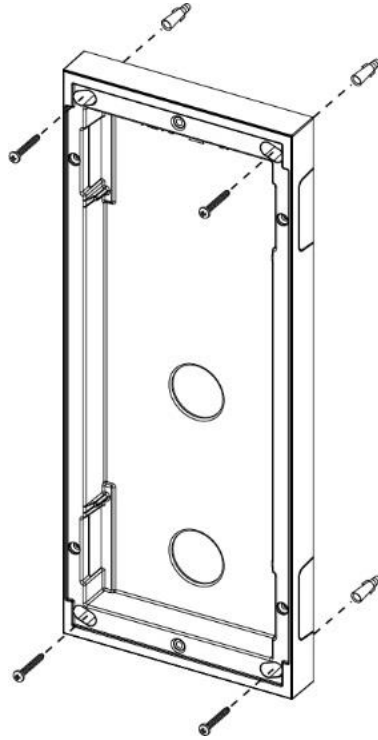
## Wall-mounted version

- Remove the upper header and the lower header from the frame using a flat screwdriver at the tip 0.

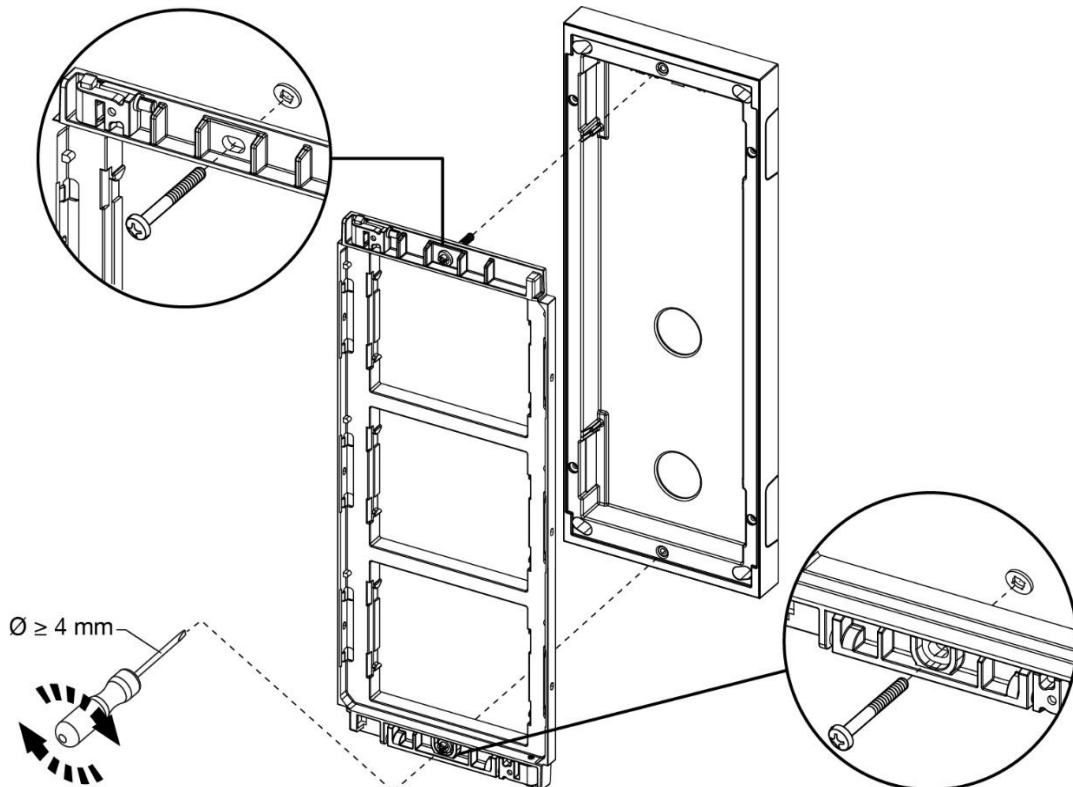


- Remove the module holder frame from the casing.

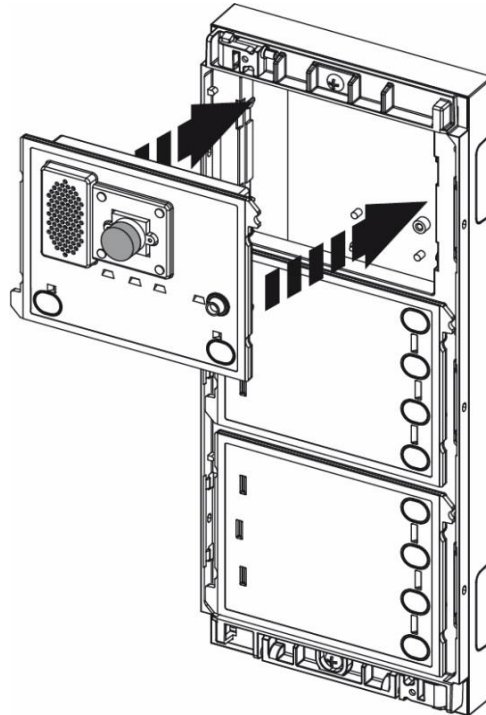
- Secure the casing with screws to the wall.



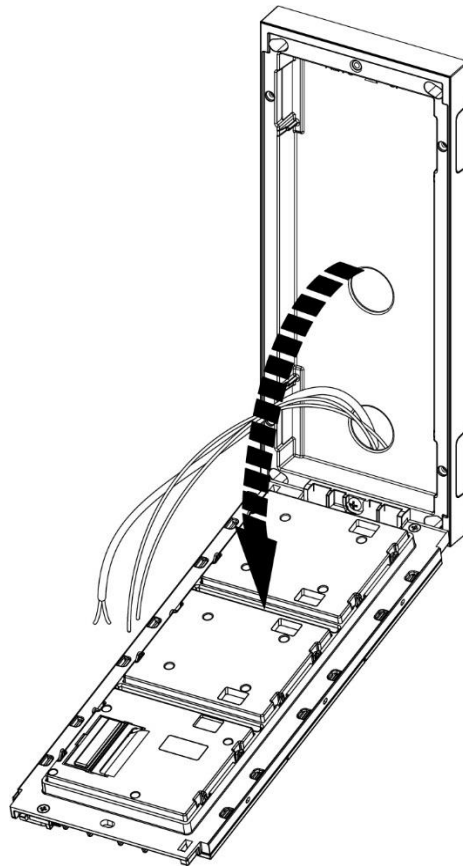
- Fit the module holder frame.



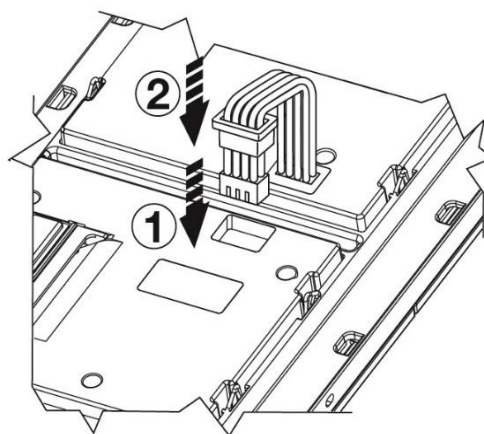
- Fit the modules in the frame.



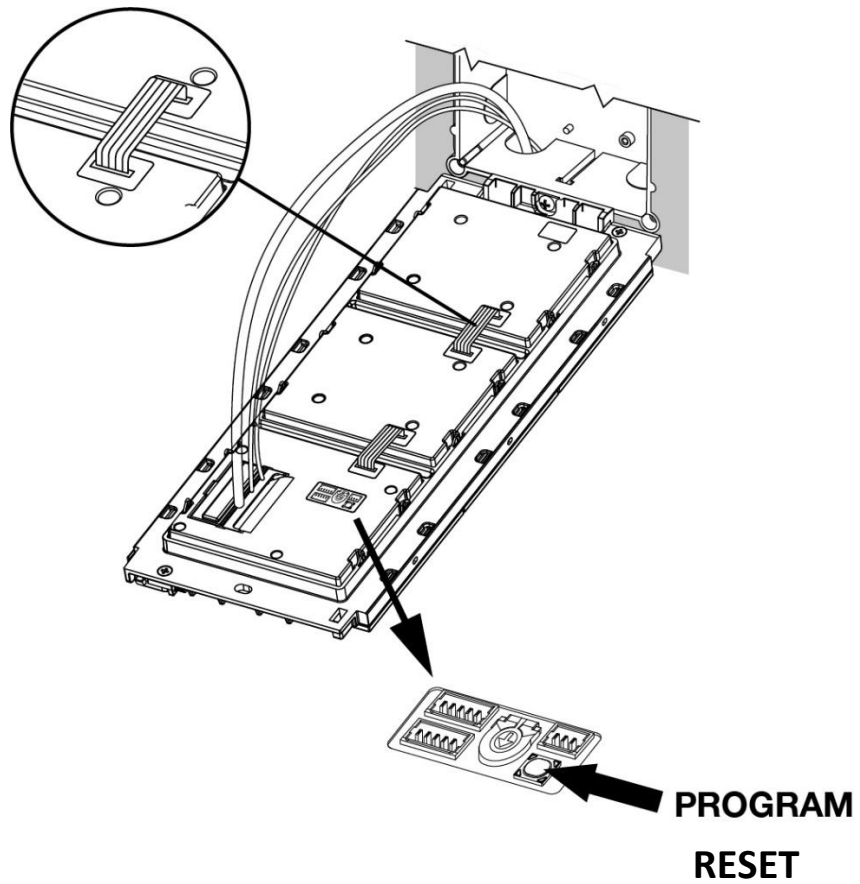
- Tip the frame and connect the wires.



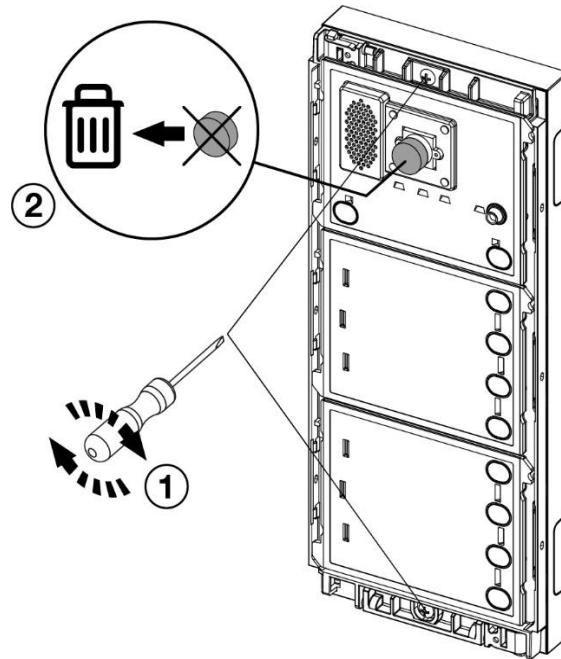
- Adjust correct perpendicularity of the panel.
- Establish the connections between the various modules with the wires provided before powering the system.



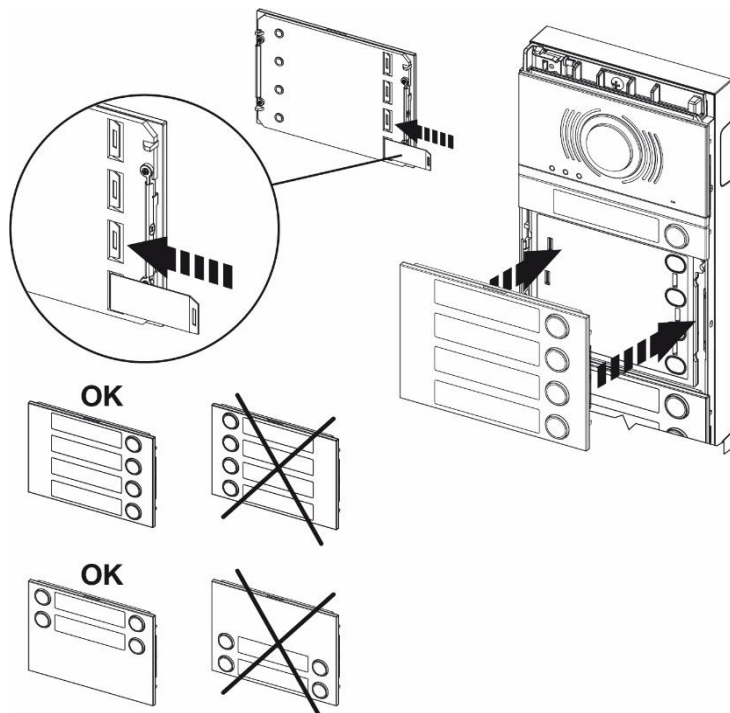
- Use the cord provided with the frame to connect modules belonging to frames arranged side by side
- On the last module be sure to protect the OUT connector using the cap provided.




- On the rear of the external unit there is the RESET key which must be pressed to restart or reset the device to factory settings.
- Attach upper header and lower the frame.



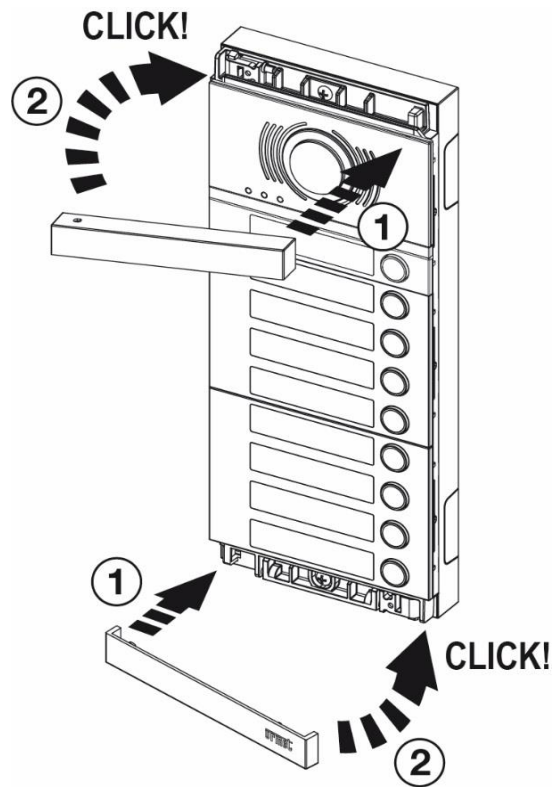
- Insert the name tags in the front panels Clip the front panels onto the frame.



 *When hooking the front unit to the wall frame, make sure to keep the buttons on the right side of the entry panel.*

- Attach upper header and lower the frame.





## Complementary products list

### DOOR UNIT

Audio video IP door unit **Ref. 1060/48**

### MODULES

4-Button module **Ref. 1168/4**

8-Button module **Ref. 1168/8**

ILA and voice synthesis module (\*) **Ref. 1168/48-48W-48G**

Building number module (\*) **Ref. 1168/50-50W-50G**

Name directory module (\*) **Ref. 1168/51-51W-51G**

Blind module **Ref. 1168/59-59W-59G**

### FRONT FRAME FOR PANEL AND DOOR UNIT (\*)

1 Button front frame on 1 row **Ref. 1168/11-11W-11G**

2 Button front frame on 1 row **Ref. 1168/12-12W-12G**

3 Button front frame on 1 row **Ref. 1168/13-13W-13G**

4 Button front frame on 1 row **Ref. 1168/14-14W-14G**

4 Button front frame on 2 row **Ref. 1168/24-24W-24G**

8 Button front frame on 2 row **Ref. 1168/28-28W-28G**

0 PB front frame for audio video IP door unit **Ref. 1168/140-140W-140G**

1 PB front frame for audio video IP door unit **Ref. 1168/141-141W-141G**

2 PB front frame for audio video IP door unit **Ref. 1168/142-142W-142G**

### FLUSH-MOUNTING BOXES

For 1 module **Ref. 1145/51**

For 2 modules **Ref. 1145/52**

For 3 modules **Ref. 1145/53**

For 4 modules **Ref. 1145/54**

### **MODULE HOLDER FRAMES**

Frame for 1 module	<b>Ref. 1168/61</b>
Frame for 2 modules	<b>Ref. 1168/62</b>
Frame for 3 modules	<b>Ref. 1168/63</b>
Frame for 4 modules	<b>Ref. 1168/64</b>

### **WALL COVER FRAME**

1-row frame for 1 module	<b>Ref. 1168/611</b>
1-row frame for 2 modules	<b>Ref. 1168/612</b>
1-row frame for 3 modules	<b>Ref. 1168/613</b>
1-row frame for 4 modules	<b>Ref. 1168/614</b>
2-row frame for 4 modules	<b>Ref. 1168/624</b>
2-row frame for 6 modules	<b>Ref. 1168/626</b>
3-row frame for 9 modules	<b>Ref. 1168/639</b>

### **CASINGS WITH FRAME**

1-row frame for 1 module	<b>Ref. 1168/311</b>
1-row frame for 2 modules	<b>Ref. 1168/312</b>
1-row frame for 3 modules	<b>Ref. 1168/313</b>
1-row frame for 4 modules	<b>Ref. 1168/314</b>

### **RAIN HOOD COVER**

For 1 module	<b>Ref. 1168/401</b>
--------------	----------------------

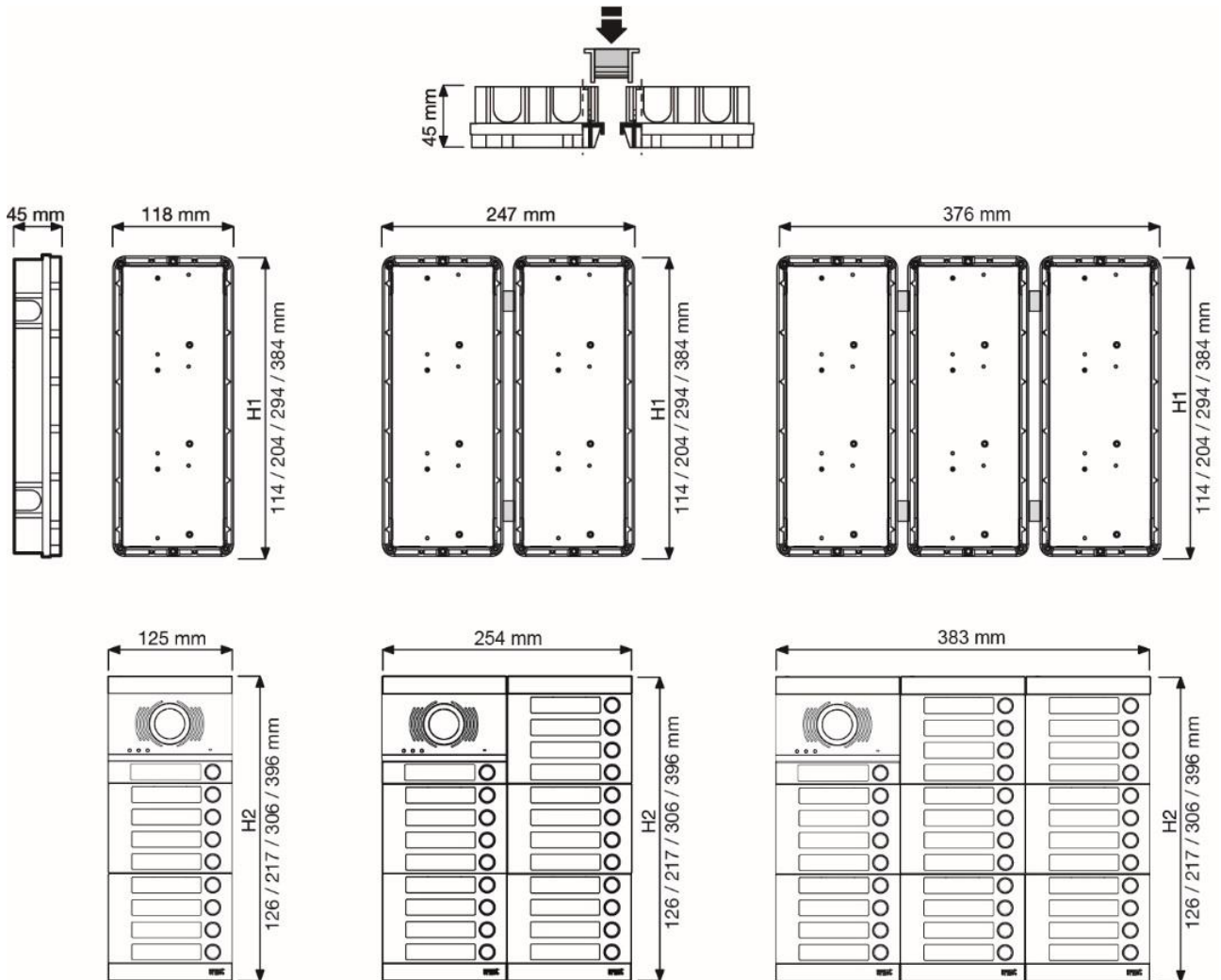
### **NAME TAGS**


Set name tags Alpha single PB black	<b>Ref. 1168/100</b>
Set name tags Alpha single PB white	<b>Ref. 1168/101</b>
Set name tags Alpha double PB black	<b>Ref. 1168/102</b>
Set name tags Alpha double PB white	<b>Ref. 1168/103</b>

(\*) Black, white or gray

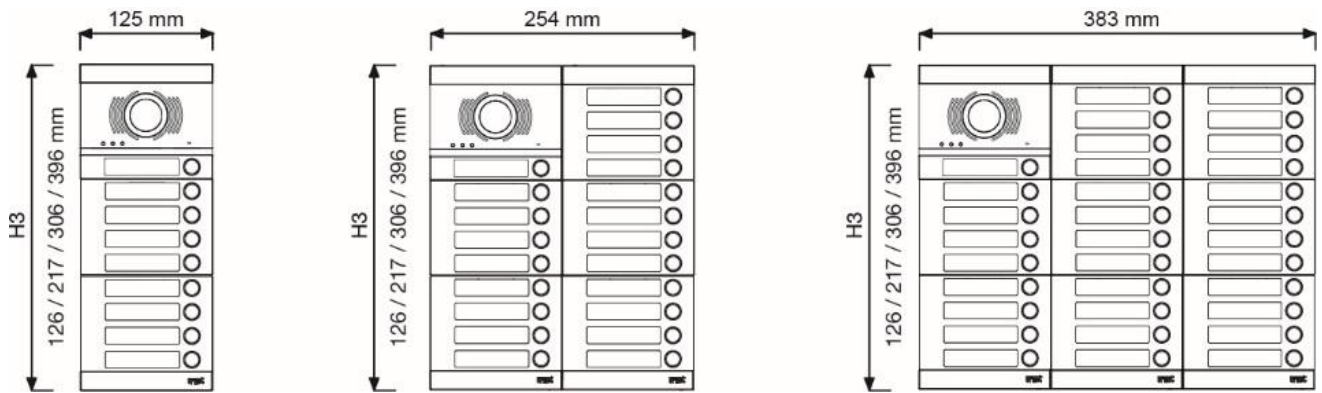
## Overall dimensions

### Flush-mounted version



 Dimensions H1= 114, 204, 294, 384 refers to the flush-mounting height and H2= 126, 217, 306, 396 refers to the total height, for the 1, 2, 3, 4 module versions, respectively.

### Wall-mounted version



*The H3 dimensions related to the total height can have different values depending on the number of modules that the housing can accommodate.*

Modularity examples for different system dimensions (single push button black color)

Video door phones			BUTTONS NUMBER															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Common products	A/V door IP unit module	1060/48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Front frame for A/V IP door unit	1168/140				1		1	1	1		1	1	1		1	1	
		1168/141	1		1		1				1				1			
		1168/142		1														
	4-Button module	1168/4			1	1	1	2	2	2	2	3	3	3	3	4	4	
	Front frame for push button panel	1168/11																
		1168/12			1			1				1				1		
		1168/13							1				1					1
		1168/14				1	1	1	1	2	2	2	2	3	3	3	3	3
Building number module	1168/50																	
Blind module	1168/59															1	1	
Rain hood cover	1168/401	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	
Flush mounting (#)	Flush-mounting boxes	1145/51	1	1														
		1145/52			1	1	1											
		1145/53						1	1	1	1						2	2
		1145/54										1	1	1	1			
	Module holder frames	1168/61	1	1														
		1168/62			1	1	1											
		1168/63						1	1	1	1						2	2
		1168/64										1	1	1	1			
	Wall cover frame (*)	1168/611	1	1														
		1168/612			1	1	1											
		1168/613						1	1	1	1							
		1168/614																
		1168/624										1	1	1	1			
1168/626																1	1	
1168/639																		
Wall mounting (#)	Casings with frame	1168/311	1	1														
		1168/312			1	1	1											
		1168/313						1	1	1	1						2	2
		1168/314										1	1	1	1			
			<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>	<b>10</b>	<b>11</b>	<b>12</b>	<b>13</b>	<b>14</b>	<b>15</b>	
			<b>BUTTONS NUMBER</b>															

(#) in alternative, (\*) optional

Video door phones			BUTTONS NUMBER														
			16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Common products	A/V door IP unit module	1060/48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	Front frame for A/V IP door unit	1168/140	1		1	1	1		1	1	1		1	1	1		1
		1168/141		1				1				1				1	
		1168/142															
	4-Button module	1168/4	4	4	5	5	5	5	6	6	6	6	7	7	7	7	8
	Front frame for push button panel	1168/11															
		1168/12			1				1				1				1
		1168/13				1				1				1			
		1168/14	4	4	4	4	5	5	5	5	6	6	6	6	7	7	7
Building number module	1168/50																
Blind module	1168/59	1	1					1	1	1	1						
Rain hood cover	1168/401	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	
Flush mounting (#)	Flush-mounting boxes	1145/51															
		1145/52															
		1145/53	2	2	2	2	2	2									3
		1145/54							2	2	2	2	2	2	2	2	
	Module holder frames	1168/61															
		1168/62															
		1168/63	2	2	2	2	2	2									3
		1168/64							2	2	2	2	2	2	2	2	
	Wall cover frame (*)	1168/611															
		1168/612															
		1168/613															
		1168/614															
		1168/624															
1168/626		1	1	1	1	1	1										
1168/639																	
Wall mounting (#)	Casings with frame	1168/311															
		1168/312															
		1168/313	2	2	2	2	2	2									3
		1168/314							2	2	2	2	2	2	2	2	
			<b>16</b>	<b>17</b>	<b>18</b>	<b>19</b>	<b>20</b>	<b>21</b>	<b>22</b>	<b>23</b>	<b>24</b>	<b>25</b>	<b>26</b>	<b>27</b>	<b>28</b>	<b>29</b>	<b>30</b>
			<b>BUTTONS NUMBER</b>														

(#) in alternative

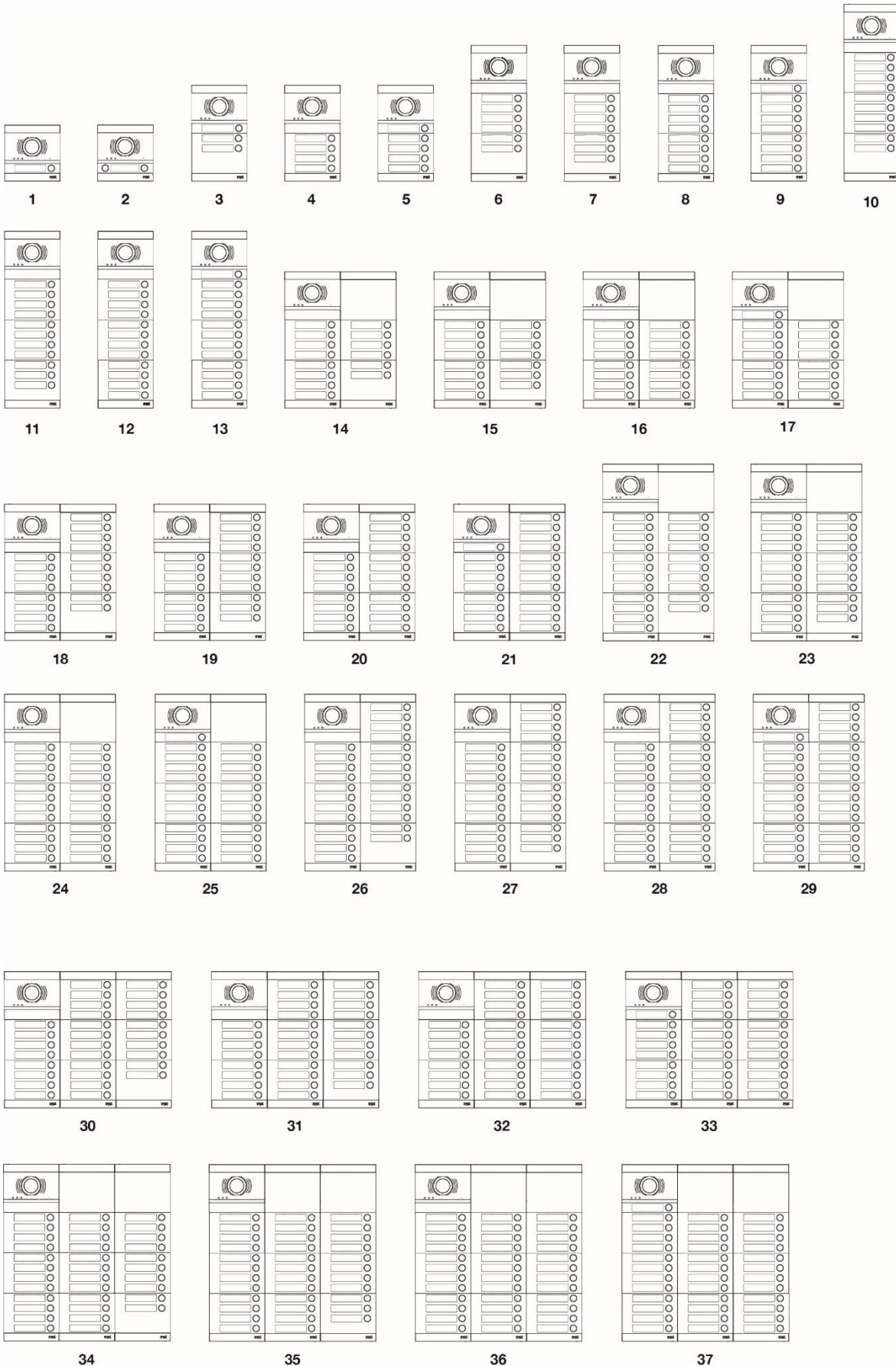
(\*) optional

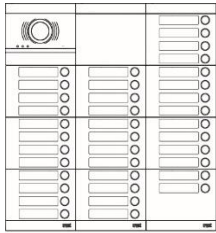
Video door phones			BUTTONS NUMBER														
			31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
Common products	A/V door IP unit module	1060/48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	Front frame for A/V IP door unit	1168/140	1	1		1	1	1		1	1	1		1	1	1	
		1168/141			1				1				1			1	
		1168/142															
	4-Button module	1168/4	8	8	8	9	9	9	9	10	10	10	10	11	11	11	
	Front frame for push button panel	1168/11															
		1168/12				1				1				1			
		1168/13	1				1				1				1		
		1168/14	7	8	8	8	8	9	9	9	9	10	10	10	10	11	11
	Building number module	1168/50															
Blind module	1168/59				2	2	2	2	1	1	1	1					
Rain hood cover	1168/401	3	3	3	3	3	3	3	3	3	3	3	3	3	3		
Flush mounting (#)	Flush-mounting boxes	1145/51															
		1145/52															
		1145/53	3	3	3												
		1145/54				3	3	3	3	3	3	3	3	3	3	3	3
	Module holder frames	1168/61															
		1168/62															
		1168/63	3	3	3												
		1168/64				3	3	3	3	3	3	3	3	3	3	3	3
	Wall cover frame (*)	1168/611															
		1168/612															
		1168/613															
		1168/614															
		1168/624															
1168/626																	
1168/639	1	1	1														
Wall mounting (#)	Casings with frame	1168/311															
		1168/312															
		1168/313	3	3	3												
		1168/314				3	3	3	3	3	3	3	3	3	3	3	3
			<b>31</b>	<b>32</b>	<b>33</b>	<b>34</b>	<b>35</b>	<b>36</b>	<b>37</b>	<b>38</b>	<b>39</b>	<b>40</b>	<b>41</b>	<b>42</b>	<b>43</b>	<b>44</b>	<b>45</b>
<b>BUTTONS NUMBER</b>																	

(#) in alternative

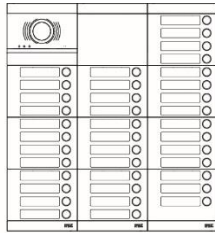
(\*) optional



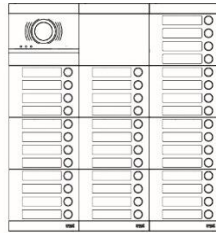




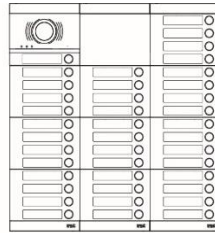
38



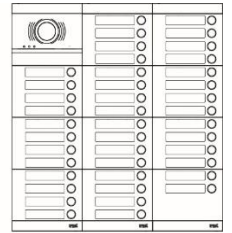
39



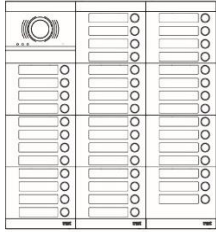
40



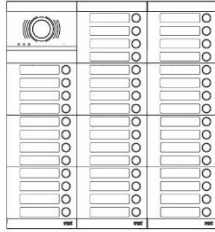
41



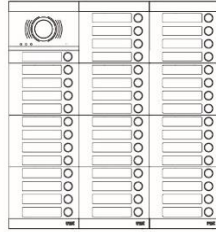
42



43



44



45

Modularity examples for different system dimensions (double push button black color)

Video door phones			BUTTONS NUMBER														
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Common products	A/V door IP unit module	1060/48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	Front frame for A/V IP door unit	1168/140			1	1			1	1			1	1			1
		1168/141	1														
		1168/142		1			1	1			1	1			1	1	
	4-Button module	1168/8			1	1	1	1	1	1	1	2	2	2	2	2	
	Front frame for push button panel	1168/24			1	1	1	1					1	1	1	1	
		1168/28							1	1	1	1	1	1	1	1	2
	Building number module	1168/50															
	Blind module	1168/59															
Rain hood cover	1168/401	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Flush mounting (#)	Flush-mounting boxes	1145/51	1	1													
		1145/52			1	1	1	1	1	1	1	1					
		1145/53												1	1	1	1
		1145/54															
	Module holder frames	1168/61	1	1													
		1168/62			1	1	1	1	1	1	1	1	1				
		1168/63												1	1	1	1
		1168/64															
	Wall cover frame (*)	1168/611	1	1													
		1168/612			1	1	1	1	1	1	1	1					
		1168/613												1	1	1	1
		1168/614															
		1168/624															
		1168/626															
		1168/639															
Wall mounting (#)	Casings with frame	1168/311	1	1													
		1168/312			1	1	1	1	1	1	1	1					
		1168/313												1	1	1	1
		1168/314															
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
			<b>BUTTONS NUMBER</b>														

(#) in alternative

(\*) optional

Video door phones			BUTTONS NUMBER														
			16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Common products	A/V door IP unit module	1060/48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	Front frame for A/V IP door unit	1168/140	1			1	1			1	1			1	1		
		1168/141															
		1168/142		1	1			1	1			1	1		1	1	
	4-Button module	1168/8	2	2	2	3	3	3	3	3	3	3	3	4	4	4	
	Front frame for push button panel	1168/24				1	1	1	1					1	1	1	
		1168/28	2	2	2	2	2	2	2	2	3	3	3	3	3	3	
	Building number module	1168/50															
Blind module	1168/59												1	1	1		
Rain hood cover	1168/401	1	1	1	1	1	1	1	1	1	1	1	2	2	2		
Flush mounting (#)	Flush-mounting boxes	1145/51															
		1145/52															
		1145/53	1	1	1									2	2	2	
		1145/54				1	1	1	1	1	1	1	1				
	Module holder frames	1168/61															
		1168/62															
		1168/63	1	1	1									2	2	2	
		1168/64				1	1	1	1	1	1	1	1				
	Wall cover frame (*)	1168/611															
		1168/612															
		1168/613	1	1	1												
		1168/614				1	1	1	1	1	1	1	1				
		1168/624															
1168/626													1	1	1		
Wall mounting (#)	Casings with frame	1168/311															
		1168/312															
		1168/313	1	1	1									2	2	2	
		1168/314				1	1	1	1	1	1	1	1				
			<b>16</b>	<b>17</b>	<b>18</b>	<b>19</b>	<b>20</b>	<b>21</b>	<b>22</b>	<b>23</b>	<b>24</b>	<b>25</b>	<b>26</b>	<b>27</b>	<b>28</b>	<b>29</b>	<b>30</b>
			<b>BUTTONS NUMBER</b>														

(#) in alternative

(\*) optional

Video door phones			BUTTONS NUMBER														
			31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
Common products	A/V door IP unit module	1060/48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	Front frame for A/V IP door unit	1168/140	1	1			1	1			1	1			1	1	
		1168/141															
		1168/142			1	1			1	1			1	1			1
	4-Button module	1168/8	4	4	4	4	5	5	5	5	5	5	5	5	6	6	6
	Front frame for push button panel	1168/24					1	1	1	1					1	1	1
		1168/28	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5
	Building number module	1168/50	1	1	1	1										1	1
Blind module	1168/59																
Rain hood cover	1168/401	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	
Flush mounting (#)	Flush-mounting boxes	1145/51															
		1145/52															
		1145/53	2	2	2	2	2	2	2	2	2	2	2	2	2		
		1145/54														2	2
	Module holder frames	1168/61															
		1168/62															
		1168/63	2	2	2	2	2	2	2	2	2	2	2	2	2		
		1168/64														2	2
	Wall cover frame (*)	1168/611															
		1168/612															
		1168/613															
		1168/614															
		1168/624															
1168/626																	
Wall mounting (#)	Casings with frame	1168/639	1	1	1	1	1	1	1	1	1	1	1	1	1		
		1168/311															
		1168/312															
		1168/313	2	2	2	2	2	2	2	2	2	2	2	2	2		
		1168/314															
			<b>31</b>	<b>32</b>	<b>33</b>	<b>34</b>	<b>35</b>	<b>36</b>	<b>37</b>	<b>38</b>	<b>39</b>	<b>40</b>	<b>41</b>	<b>42</b>	<b>43</b>	<b>44</b>	<b>45</b>
			<b>BUTTONS NUMBER</b>														

(#) in alternative

(\*) optional

Video door phones			BUTTONS NUMBER															
			46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	
Common products	A/V door IP unit module	1060/48	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
	Front frame for A/V IP door unit	1168/140		1	1				1	1			1	1			1	1
		1168/141																
		1168/142	1			1	1				1	1			1	1		
	4-Button module	1168/8	6	6	6	6	6	7	7	7	7	7	7	7	7	8	8	
	Front frame for push button panel	1168/24	1						1	1	1	1					1	1
		1168/28	5	6	6	6	6	6	6	6	6	6	7	7	7	7	7	7
	Building number module	1168/50	1	1	1	1												
Blind module	1168/59																	
Rain hood cover	1168/401	2	2	2	2	2	2	2	2	2	2	2	2	2	2	3	3	
Flush mounting (#)	Flush-mounting boxes	1145/51																
		1145/52																
		1145/53															3	3
		1145/54	2	2	2	2	2	2	2	2	2	2	2	2	2	2		
	Module holder frames	1168/61																
		1168/62																
		1168/63															3	3
		1168/64	2	2	2	2	2	2	2	2	2	2	2	2	2	2		
	Wall cover frame (*)	1168/611																
		1168/612																
		1168/613																
		1168/614																
		1168/624																
1168/626																		
1168/639																1	1	
Wall mounting (#)	Casings with frame	1168/311																
		1168/312																
		1168/313															3	3
		1168/314	2	2	2	2	2	2	2	2	2	2	2	2	2	2		
			<b>BUTTONS NUMBER</b>															

(#) in alternative

(\*) optional

Video door phones			BUTTONS NUMBER														
			61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
Common products	A/V door IP unit module	1060/48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	Front frame for A/V IP door unit	1168/140			1	1				1	1			1	1		1
		1168/141															
		1168/142	1	1			1	1				1	1			1	1
	4-Button module	1168/8	8	8	8	8	8	8	9	9	9	9	9	9	9	10	
	Front frame for push button panel	1168/24	1	1						1	1	1	1				1
		1168/28	7	7	8	8	8	8	8	8	8	8	9	9	9	9	9
	Building number module	1168/50															
	Blind module	1168/59								2	2	2	2	2	2	2	1
Rain hood cover	1168/401	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	
Flush mounting (#)	Flush-mounting boxes	1145/51															
		1145/52															
		1145/53	3	3	3	3	3	3									
		1145/54								3	3	3	3	3	3	3	3
	Module holder frames	1168/61															
		1168/62															
		1168/63	3	3	3	3	3	3									
		1168/64								3	3	3	3	3	3	3	3
	Wall cover frame (*)	1168/611															
		1168/612															
		1168/613															
		1168/614															
		1168/624															
		1168/626															
	1168/639	1	1	1	1	1	1										
Wall mounting (#)	Casings with frame	1168/311															
		1168/312															
		1168/313	3	3	3	3	3	3									
		1168/314								3	3	3	3	3	3	3	3
			61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
			BUTTONS NUMBER														

(#) in alternative

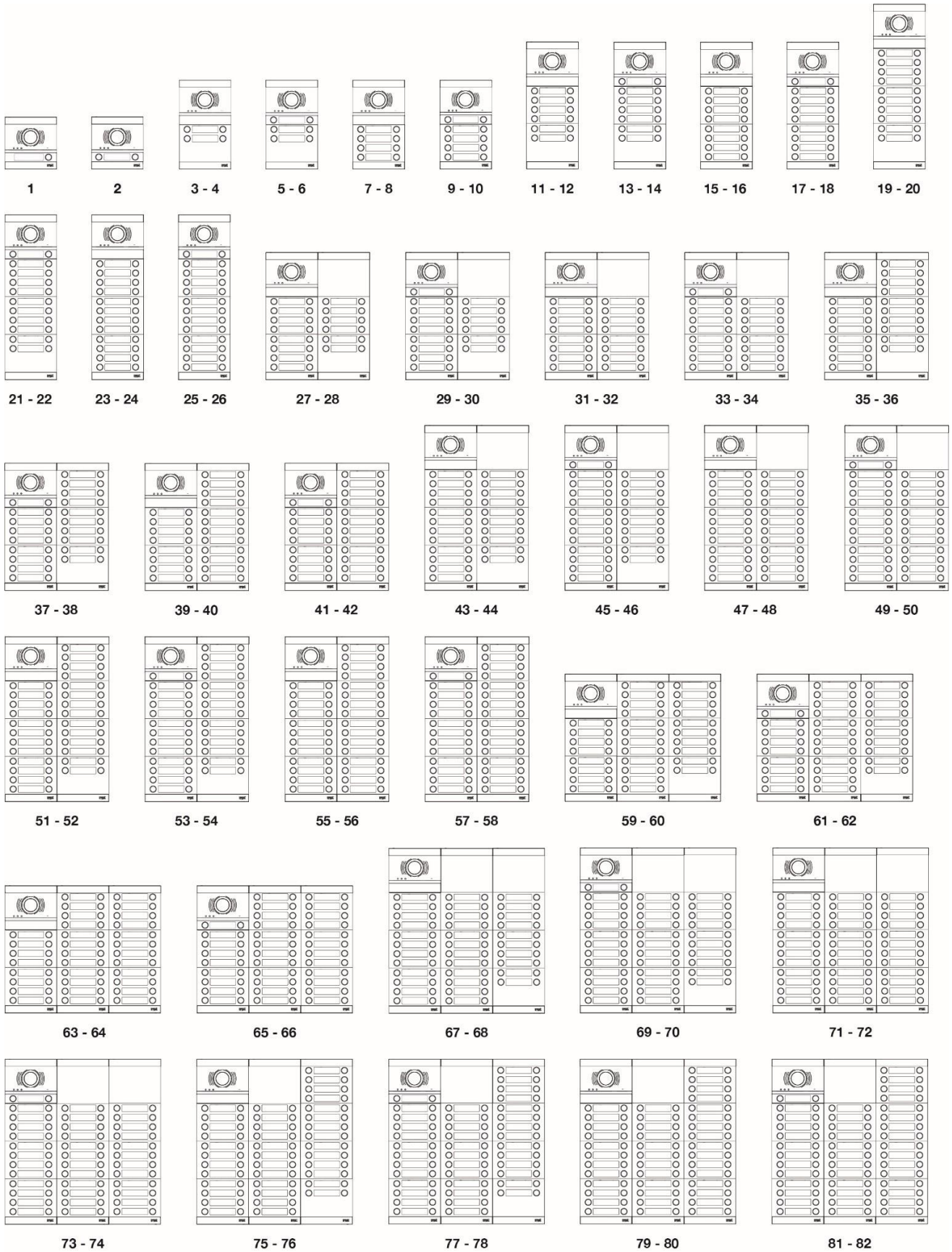
(\*) optional

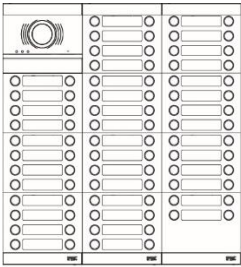
Video door phones			BUTTONS NUMBER														
			76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
Common products	A/V door IP unit module	1060/48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
	Front frame for A/V IP door unit	1168/140	1			1	1			1	1			1	1		
		1168/141															
		1168/142		1	1				1	1			1	1		1	1
	4-Button module	1168/8	10	10	10	10	10	10	10	11	11	11	11	11	11	11	
	Front frame for push button panel	1168/24	1	1	1					1	1	1	1				
		1168/28	9	9	9	10	10	10	10	10	10	10	10	11	11	11	11
	Building number module	1168/50															
	Blind module	1168/59	1	1	1	1	1	1	1								
Rain hood cover	1168/401	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	
Flush mounting (#)	Flush-mounting boxes	1145/51															
		1145/52															
		1145/53															
		1145/54	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	Module holder frames	1168/61															
		1168/62															
		1168/63															
		1168/64	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	Wall cover frame (*)	1168/611															
		1168/612															
		1168/613															
		1168/614															
		1168/624															
		1168/626															
		1168/639															
Wall mounting (#)	Casings with frame	1168/311															
		1168/312															
		1168/313															
		1168/314	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
			<b>76</b>	<b>77</b>	<b>78</b>	<b>79</b>	<b>80</b>	<b>81</b>	<b>82</b>	<b>83</b>	<b>84</b>	<b>85</b>	<b>86</b>	<b>87</b>	<b>88</b>	<b>89</b>	<b>90</b>
			<b>BUTTONS NUMBER</b>														

(#) in alternative

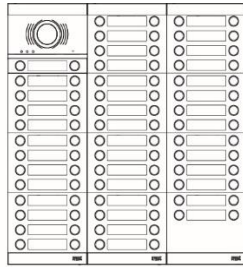
(\*) optional



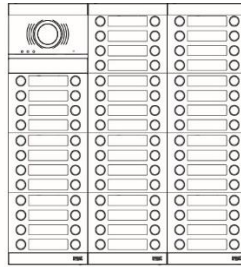




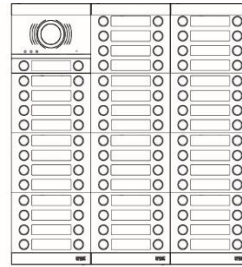
83 - 84



85 - 86



87 - 88



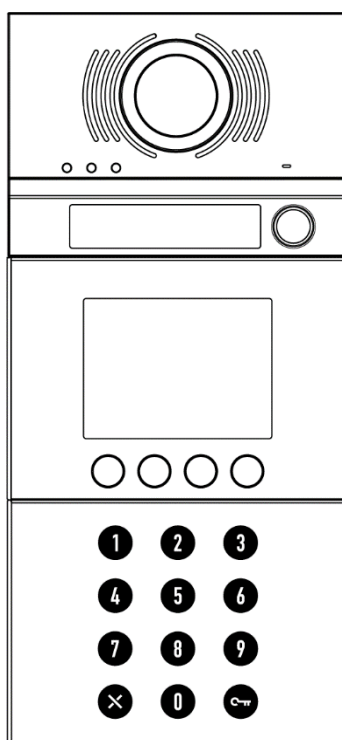
88 - 90

## APPENDIX L: Alpha call module 1168

The ALPHA call module with sturdy, streamline and modern design is for use in 2Voice systems. It offers simple access to a full range of functions. The system consists of black or grey modules which can be inserted on specific frames. The system has IK08 shock resistance and IP55 resistance to penetration of liquids and micro-dust.

The display module together with the audio video IP door unit Ref. 1060/48 and the keypad form a standard calling module configuration.

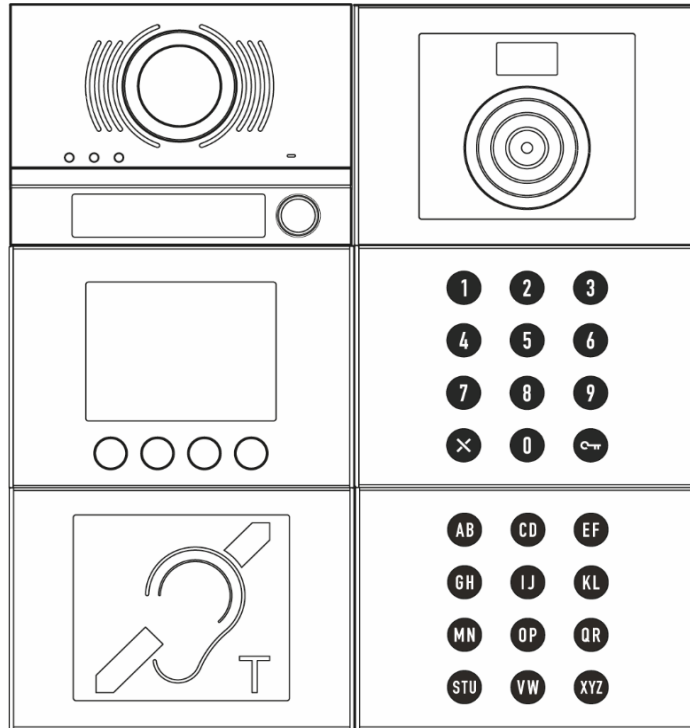
### STANDARD CONFIGURATION



The calling module can be expanded with further additional modules, e.g.:

- ILA and voice synthesis module
- Alphabetic keyboard module
- Proximity key reader module

**EXTENDED CONFIGURATION**



Apart from the IP 1060/48 audio video outdoor station, all the other modules listed above can be black or grey. The IP 1060/48 audio video outdoor station must be fitted with a black or grey faceplate (with 0, 1 or 2 keys) depending on the colour chosen. In listing the features of the various modules, reference is made to those in black (the corresponding grey modules differ only in colour). A list of all item numbers (both black and grey, when available) is given below.

## Features

Possibility of powering up to 12 modules in total:

CONFIGURATIONS								
Modules	Description	Maximum number of modules						
		1	2	3	4	5	6	7
1060/48	IP Door unit modules	1	1	1	1	1	1	1
1168/1	Display module	1	1	1	1	1	1	1
1168/46	Numeric keypad module	1	1	1	1	1	1	1
1168/45	Proximity key reader module		1			1	1	1
1168/48	ILA and voice synthesis module			1		1		1
1168/49	Alphaphetic keypad module				1		1	1
1168/50 – 1168/4 – 1168/8	Door number module or 4-buttons module or 8-buttons module	9	8	8	8	7	7	6

### AUDIO VIDEO EXTERNAL UNIT MODULE IP 1060/48

- Connection on LAN cable with dedicated connector (no RJ45) and power supply via POE.
- Wide-Angle colour camera.
- Camera lighting LED.
- Pedestrian electric lock actuation by capacitive discharge and holding current.
- Pedestrian electric lock actuation programmable from 1 to 90 seconds.
- Driveway (gate) electric lock actuation with clean contacts.
- Management of free or secret electric locks.
- Loudspeaker sound level adjustment.
- Entrance hall button.
- Input for door status sensor

### DISPLAY MODULE 1168/1

- 16-character 3.5-inch LCD display module.
- 4 soft touch keys on display module.
- Complete customisation of the display Homepage.
- Management of up to 10000 names in the address book (if there is a server 1060/1 in the system).
- Name search by address book.
- Possibility to call all potential users of the system by entering the code.
- Advanced configuration of the display buttons for switchboard call or special function.

## PROXIMITY KEY READER MODULE 1168/45

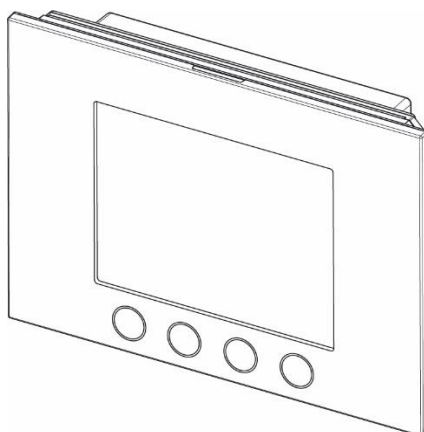
- The door can be opened using a transponder key if the proximity key reader module is present.

Below is the description of the modules that make up the *ALPHA* call module.


For the description of the following modules see [APPENDIX M1](#):

- Audio/video external unit module IP Ref. 1060/48
- Proximity key reader module Ref. 1168/45
- ILA module and voice synthesis Ref. 1168/48
- Building number module Ref. 1168/50
- Blank module Ref. 1168/59
- 4- and 8-key module Ref. 1168/4 and 1168/8

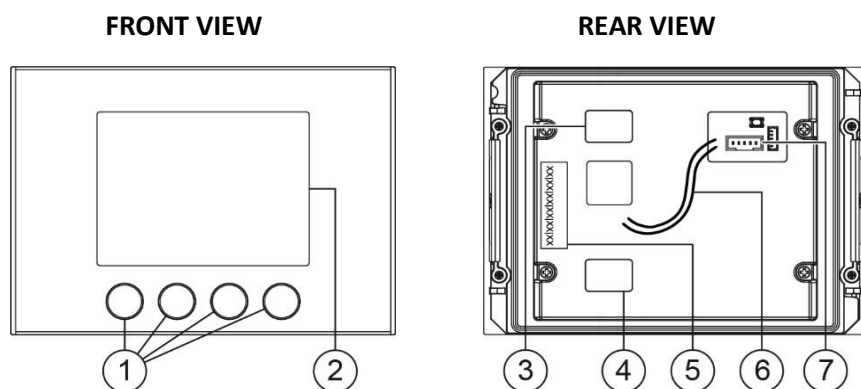
## Display module Ref. 1168/1



The display module Ref. 1168/1 allows you to display the graphical interface of the *ALPHA* call module. It is equipped with address book that can store up to 10000 users (in presence of at least one 1060/1 *Server*). It has 4 soft touch keys that allow you to use the functions of the call module.

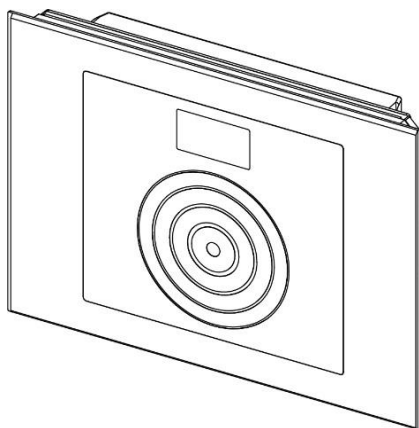
 *The device must always be placed under the external unit module Ref. 1060/48 and connected to it through a USB cable supplied with the product.*

## Structure



1. 4 context soft touch keys on backlighting
2. 3.5-inch LCD display
3. Connector for module connection cable (IN)
4. Connector for module connection cable (OUT)
5. Label with MAC ADDRESS of the device
6. Cables preset for connection to the external presence sensor (optional)
7. USB connector for connection to external unit module 1060/48

## Proximity key reader module Ref. 1168/45



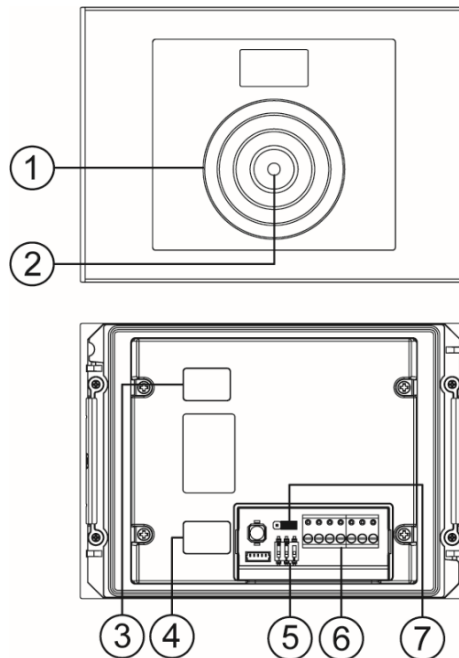
The device Ref. 1168/45 is the proximity key reader for modular door unit Mod.1168. It has following operating modes:

- Audio-video door IP unit Ref. 1060/48
- Display module Ref. 1168/1
- Numeric keypad module Ref. 1168/46

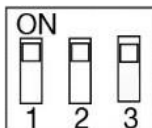


*Only one Sch. module 1168/45 can be installed for each call station.*

## Structure



- 8. Proximity key sensor
- 9. Two colour LED (red/green)
- 10. Module connection cable connector (IN)
- 11. Module connection cable connector (OUT)
- 12. Configuration dip switches used for:



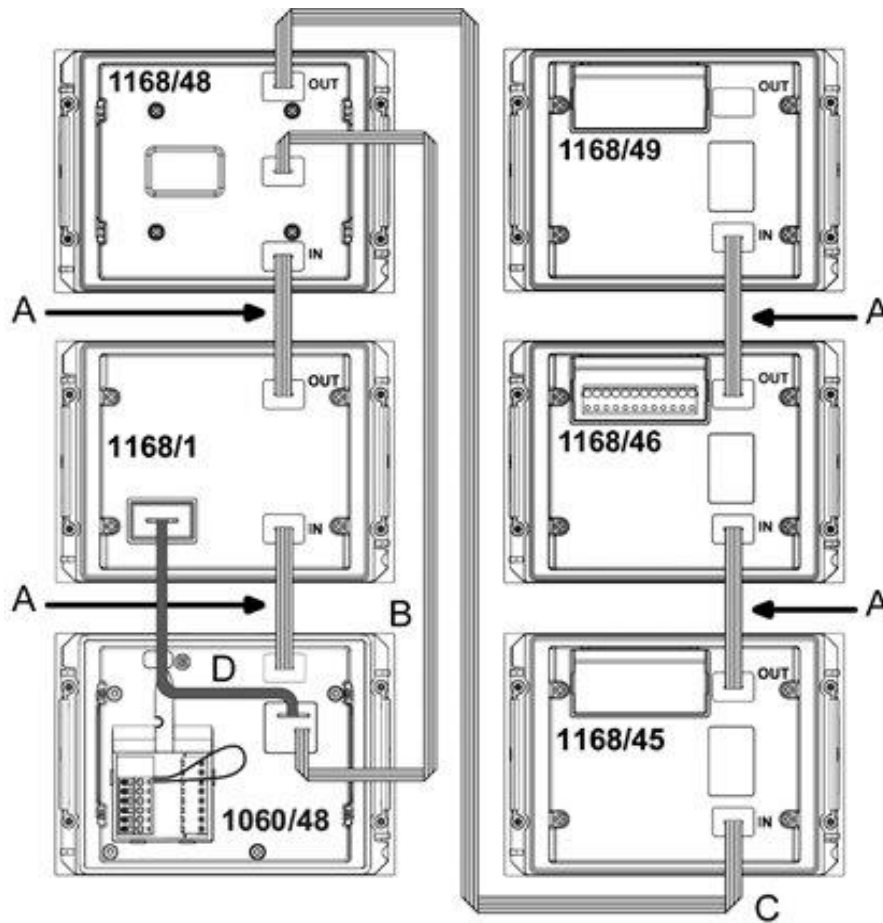
- 1. **indicating LED state:** ON enable (default)
- 2. **Do not change the arrangement of this dip switch**
- 3. RS485 BUS: IPerCom mode

- 13. Terminal board
- 14. Jumper for power from Ipercom system

The keys configuration must be configured through the *configurator*, refer to the following paragraphs: [Residents](#) and [Not residents](#).



## Installation



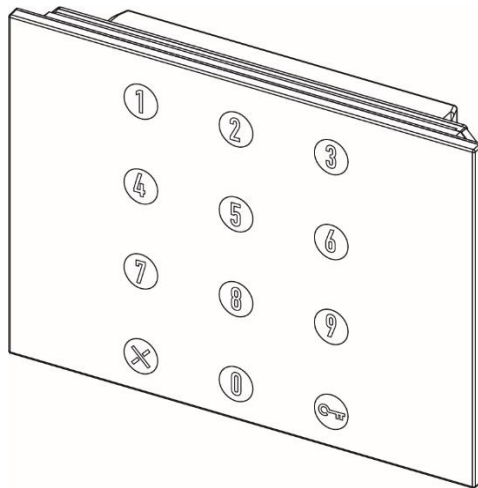
<b>A</b>	8-cm long cord provided with the following modules: display Ref. 1168/1, keypads Ref. 1168/46 and /49, proximity key reader Ref. 1168/45 and door number Ref. 1168/50.
<b>B</b>	82-cm cord provided with ILA and voice synthesis module Ref. 1168/48.
<b>C</b>	58-cm long cord provided with three or four-module frame Ref. 1168/63 or and of one-row casings with three or four-module frame (Ref. 1168/313 or 1168/314).
<b>D</b>	13 cm long USB cable supplied with the IP door unit module (Ref. 1060/48).

## Performance

Permits timed opening (from 0 to 99 seconds) when a user proximity key is placed close to the front panel.

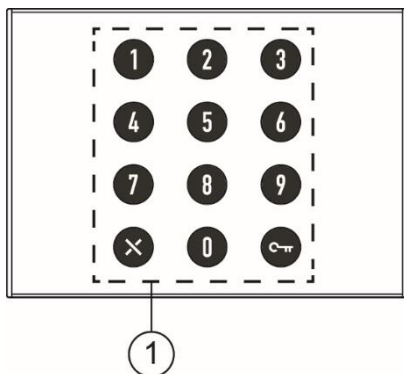
The two-color LED, if enabled, displays the recognition of a proximity key approached to the front by changing color (from red to green).

## Numeric keypad module Ref. 1168/46

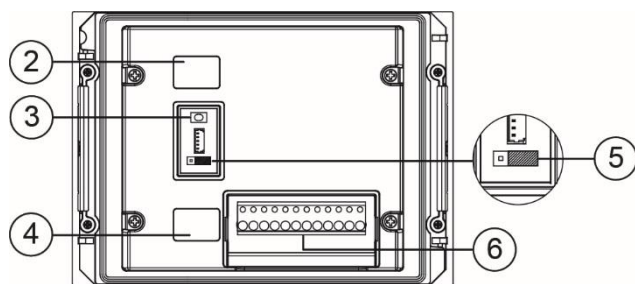


The numeric keypad module Ref. 1168/46 allows you to make a call using a numerical, logical, topological code or enter a door opener code to open an access point.

**FRONT VIEW**

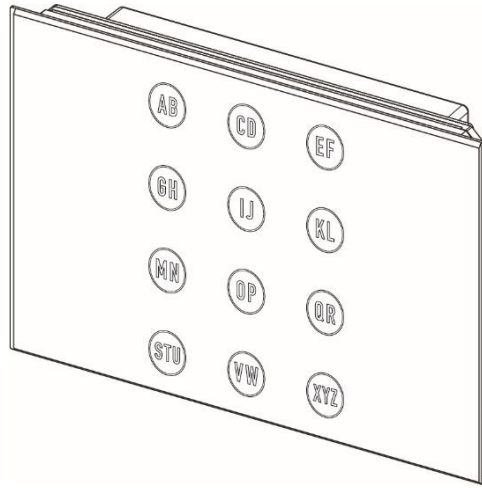


**REAR VIEW**



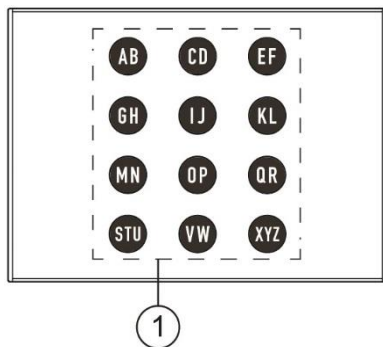
1. 12 soft-touch shortcut keys with backlighting
2. Module connection wire connector (IN)
3. Reset button (PROGRAM)
4. Module connection wire connector (OUT)
5. Terminal board
6. Jumpers for operation in Ipecom systems

## Alphabetic keypad module Ref. 1168/49

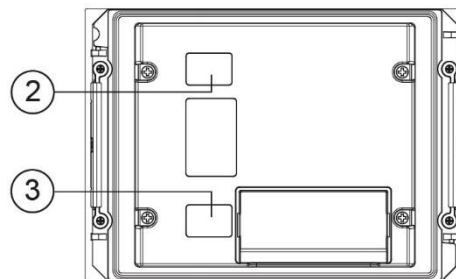


The alphabetic keypad module Ref. 1168/46 is a keypad dedicated to IperCom call modules.

**FRONT VIEW**



**REAR VIEW**

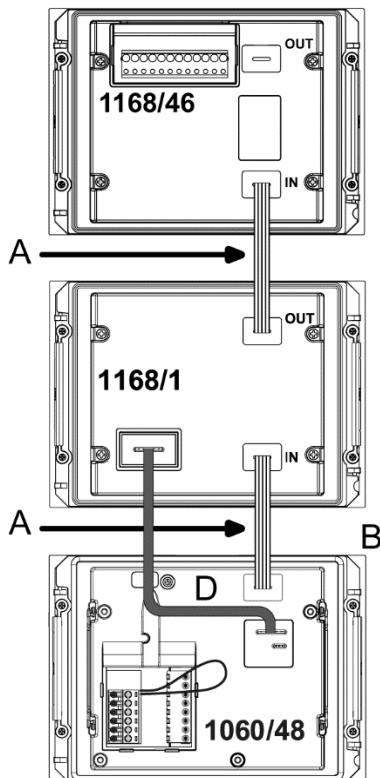


1. 12 soft-touch shortcut keys with backlighting
2. Module connection wire connector (IN)
3. Module connection wire connector (OUT)

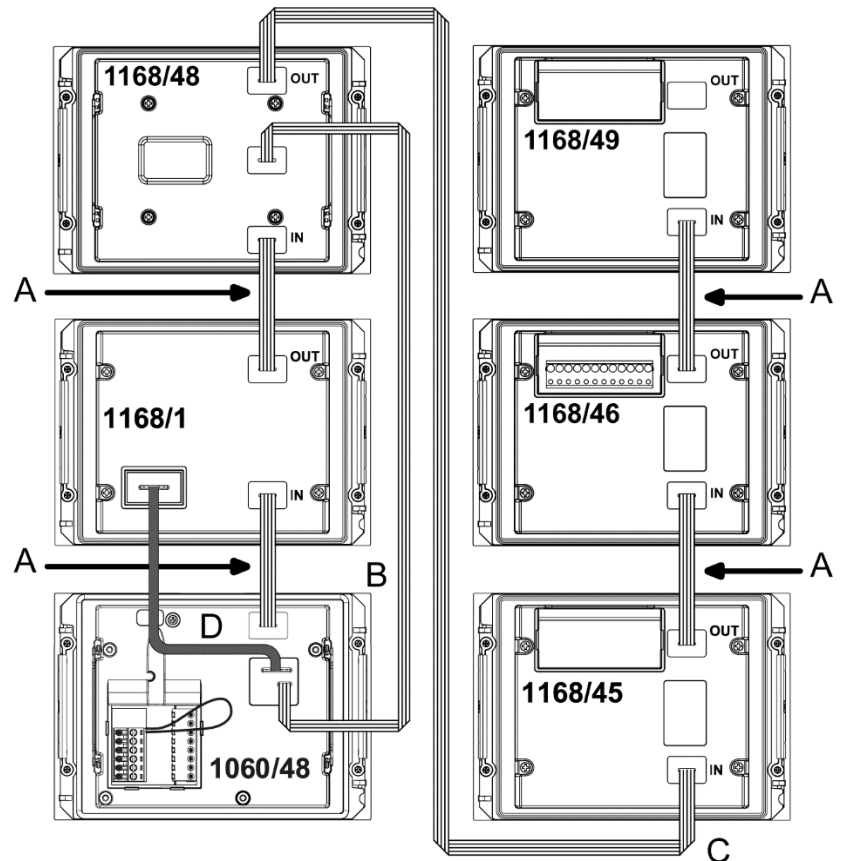
## Connecting the call module

The connection of a call module with standard and extended configuration is shown below.

### STANDARD CONFIGURATION



### EXTENDED CONFIGURATION



<b>A</b>	8-cm long cord provided with the following modules: display Ref. 1168/1, keypads Ref. 1168/46 and /49, proximity key reader Ref. 1168/45 and door number Ref. 1168/50.
<b>B</b>	82-cm cord provided with ILA and voice synthesis module Ref. 1168/48.
<b>C</b>	38-cm long cord provided with two-module frame Ref. 1168/62 and with casing with two-module frame Ref. 1168/312. 58-cm long cord provided with three or four-module frame Ref. 1168/63 or and of one-row casings with three or four-module frame (Ref. 1168/313 or 1168/314).
<b>D</b>	13 cm long USB cable supplied with the IP door unit module (Ref. 1060/48).

## Complementary products list

### DOOR UNIT

Audio video IP door unit **Ref. 1060/48**

### MODULES

Display module **Ref. 1168/1-1G**  
 4-Button module **Ref. 1168/4**  
 8-Button module **Ref. 1168/8**  
 Numeric keypad module **Ref. 1168/46-46G**  
 Alphabetic keypad module **Ref. 1168/49-49G**  
 Proximity key reader module **Ref. 1168/45-45G**  
 ILA and voice synthesis module **Ref. 1168/48-48G**  
 Building number module **Ref. 1168/50-50G**  
 Blind module **Ref. 1168/59-59G**

### FRONT FRAME FOR PANEL AND DOOR UNIT

1 Button front frame on 1 row **Ref. 1168/11**  
 2 Button front frame on 1 row **Ref. 1168/12**  
 3 Button front frame on 1 row **Ref. 1168/13**  
 4 Button front frame on 1 row **Ref. 1168/14**  
 4 Button front frame on 2 row **Ref. 1168/24**  
 8 Button front frame on 2 row **Ref. 1168/28**  
 0 PB front frame for audio video IP door unit **Ref. 1168/140-140G**  
 1 PB front frame for audio video IP door unit **Ref. 1168/141-141G**  
 2 PB front frame for audio video IP door unit **Ref. 1168/142-142G**

### FLUSH-MOUNTING BOXES

For 1 module **Ref. 1145/51**  
 For 2 modules **Ref. 1145/52**  
 For 3 modules **Ref. 1145/53**  
 For 4 modules **Ref. 1145/54**

### **MODULE HOLDER FRAMES**

Frame for 1 module	<b>Ref. 1168/61</b>
Frame for 2 modules	<b>Ref. 1168/62</b>
Frame for 3 modules	<b>Ref. 1168/63</b>
Frame for 4 modules	<b>Ref. 1168/64</b>

### **WALL COVER FRAME**

1-row frame for 1 module	<b>Ref. 1168/611</b>
1-row frame for 2 modules	<b>Ref. 1168/612</b>
1-row frame for 3 modules	<b>Ref. 1168/613</b>
1-row frame for 4 modules	<b>Ref. 1168/614</b>
2-row frame for 4 modules	<b>Ref. 1168/624</b>
2-row frame for 6 modules	<b>Ref. 1168/626</b>
3-row frame for 9 modules	<b>Ref. 1168/639</b>

### **CASINGS WITH FRAME**

1-row frame for 1 module	<b>Ref. 1168/311</b>
1-row frame for 2 modules	<b>Ref. 1168/312</b>
1-row frame for 3 modules	<b>Ref. 1168/313</b>
1-row frame for 4 modules	<b>Ref. 1168/314</b>

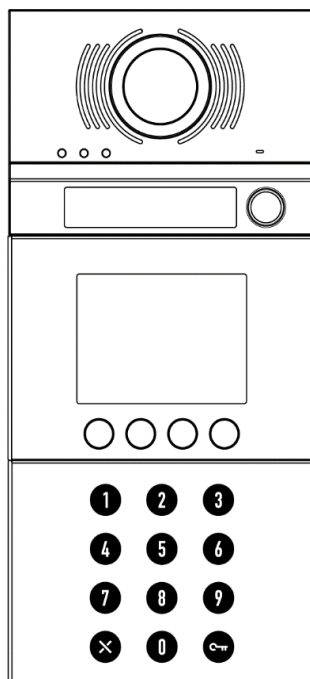
### **RAIN HOOD COVER**

For 1 module	<b>Ref. 1168/401</b>
--------------	----------------------

### **NAME TAGS**

Set name tags Alpha single PB black	<b>Ref. 1168/100</b>
Set name tags Alpha double PB black	<b>Ref. 1168/102</b>
Grey single-key Alpha name tag set	<b>Ref. 1168/104G</b>
Grey double-key Alpha name tag set	<b>Ref. 1168/105G</b>

## Modularity examples

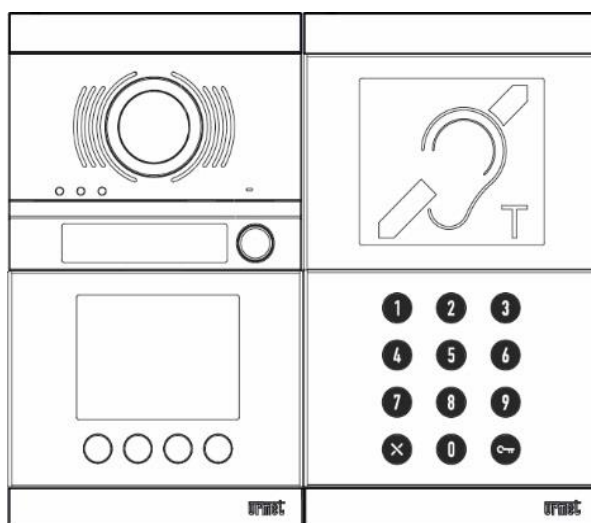


Ref.	Description	N°	Note
1060/48	Audio video IP door unit	1	
1168/141 (§)	1 PB front frame for audio video IP door unit	1	
1168/1	Display module	1	
1168/46	Numeric keypad module	1	
1145/53	Flush-mounting boxes	1	Flush-mounted
1168/63	Module holder frames	1	
1168/613	Wall cover frame (*)	1	
1168/313	Casings with frame	1	Wall-mounted installation
1168/401	Rain hood cover (*)	1	

(\*) optional

(§) in alternative: 1168/140 or 1168/142

(&) in alternative: 1168/130 or 1168/132

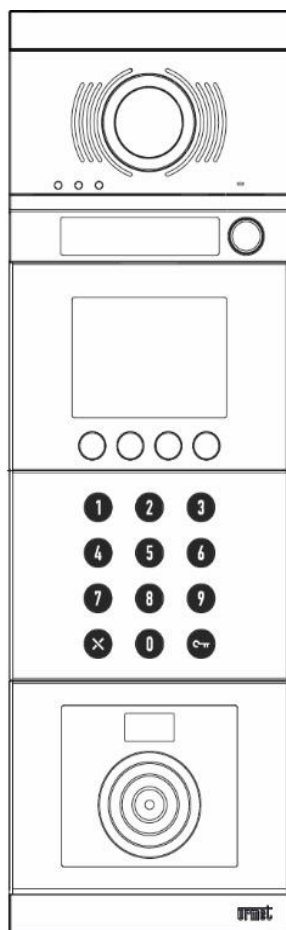


Ref.	Description	N°	Note
1060/48	Audio video IP door unit	1	
1168/141 (§)	1 PB front frame for audio video IP door unit	1	
1168/48	ILA and voice synthesis module	1	in alternative: 1168/50 1168/49 1168/45 1168/8 1168/4
1168/1	Display module	1	
1168/46	ILA and voice synthesis module	1	
1145/52	Flush-mounting boxes	2	Flush-mounted
1168/62	Module holder frames	2	
1168/624	Wall cover frame (*)	1	
1168/312	Casings with frame	2	Wall-mounted installation
1168/401	Rain hood cover (*)	2	

(\*) optional

(§) in alternative: 1168/140 or 1168/142

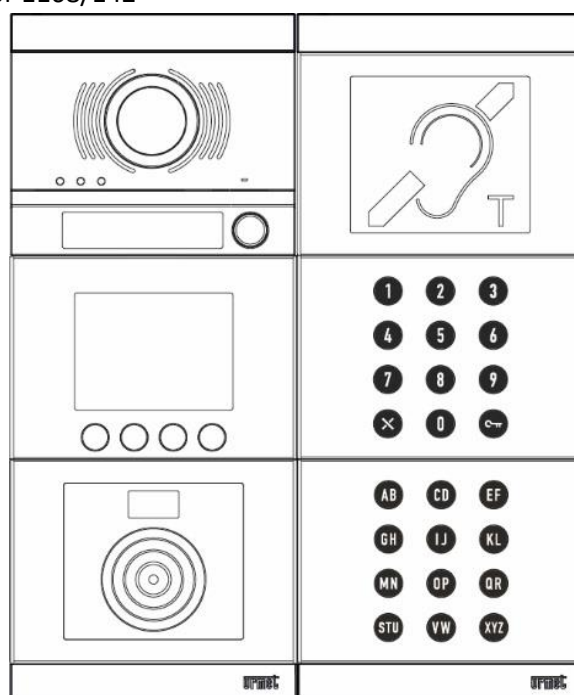




Ref.	Description	N°	Note
1060/48	Audio video IP door unit	1	
1168/141 (§)	1 PB front frame for audio video IP door unit	1	
1168/1	Modulo display	1	
1168/46	Display module	1	
1168/45	Proximity key reader module	1	in alternative: 1168/50 1168/49 1168/48 1168/8 1168/4
1145/54	Flush-mounting boxes	1	Flush-mounted
1168/64	Module holder frames	1	
1168/614	Wall cover frame (*)	1	
1168/314	Casings with frame	1	Wall-mounted installation
1168/401	Rain hood cover (*)	1	

(\*) optional

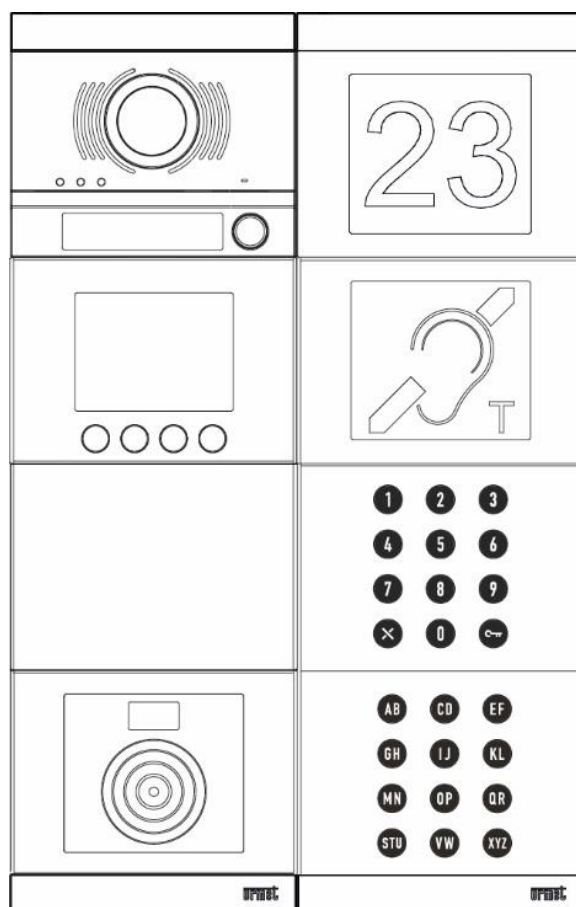
(§) in alternative: 1168/140 or 1168/142



Ref.	Description	N°	Note
1060/48	Audio video IP door unit	1	
1168/141 (§)	1 PB front frame for audio video IP door unit	1	
1168/48	ILA and voice synthesis module	1	
1168/45	Proximity key reader module	1	
1168/1	Display module	1	
1168/46	Numeric keypad module	1	
1168/49	Alphabetic keypad module	1	
1145/53	Flush-mounting boxes	2	Flush-mounted
1168/66	Module holder frames	2	
1168/626	Wall cover frame (*)	1	
1168/313	Casings with frame	2	Wall-mounted installation
1168/401	Rain hood cover (*)	2	

(\*) optional

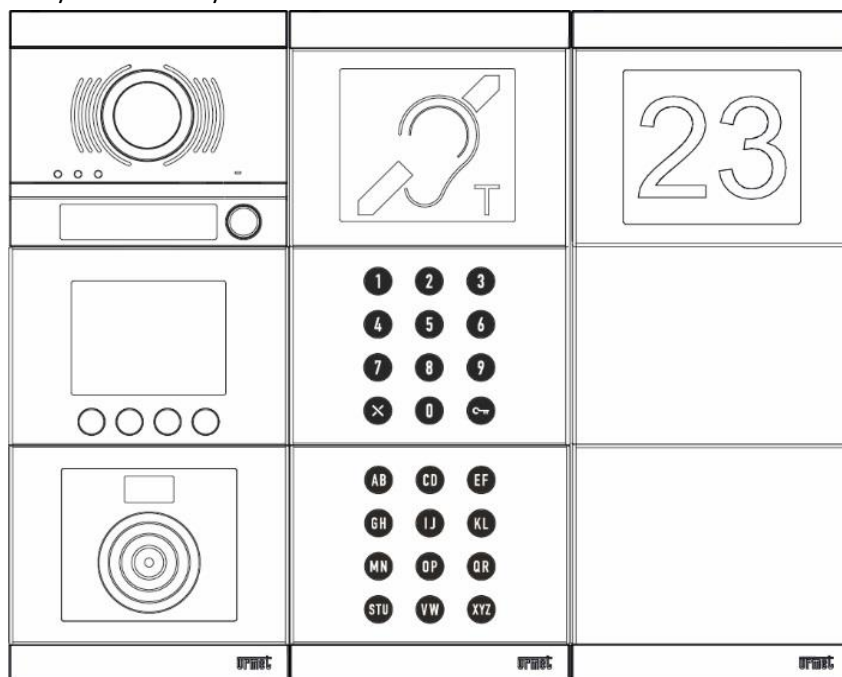
(§) in alternative: 1168/140 or 1168/142



Ref.	Description	N°	Note
1060/48	Audio video IP door unit	1	
1168/141 (§)	1 PB front frame for audio video IP door unit	1	
1168/1	Display module	1	
1168/59	Blind module	1	in alternative: 1168/4 / 1168/8
1168/45	Proximity key reader module	1	
1168/50	Building number module	1	
1168/48	ILA and voice synthesis module	1	
1168/46	Numeric keypad module	1	
1168/49	Alphabetic keypad module	1	
1145/54	Flush-mounting boxes	2	Flush-mounted
1168/66	Module holder frames	2	
1168/626	Wall cover frame (*)	1	
1168/313	Casings with frame	2	Wall-mounted installation
1168/401	Rain hood cover (*)	2	

(\*) optional

(§) in alternative: 1168/140 or 1168/142



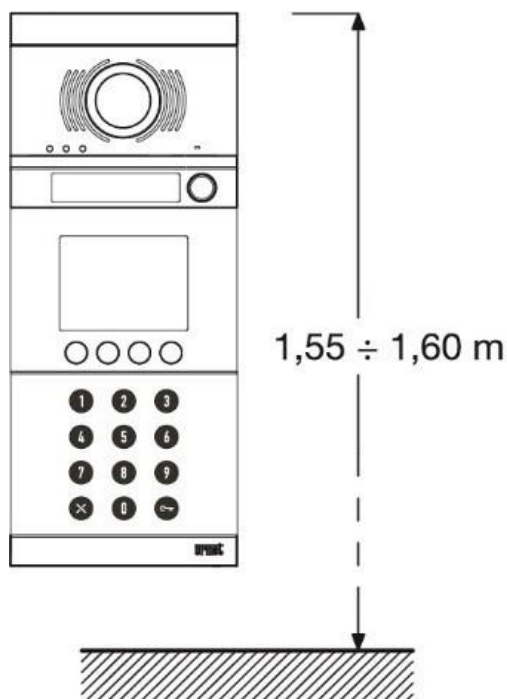
Ref.	Description	N°	Note
1060/48	Audio video IP door unit	1	
1168/141 (§)	1 PB front frame for audio video IP door unit	1	
1168/1	Display module	1	
1168/45	Proximity key reader module	1	
1168/48	ILA and voice synthesis module	1	
1168/46	Numeric keypad module	1	
1168/49	Alphabetic keypad module	1	
1168/50	Building number module	1	in alternative: 1168/4 1168/8
1168/59	Blind module	2	
1145/54	Flush-mounting boxes	3	Flush-mounted
1168/66	Module holder frames	3	
1168/626	Wall cover frame (*)	1	
1168/313	Casings with frame	3	Wall-mounted installation
1168/401	Rain hood cover (*)	3	

(\*) optional

(§) in alternative: 1168/140 or 1168/142

## Call module installation

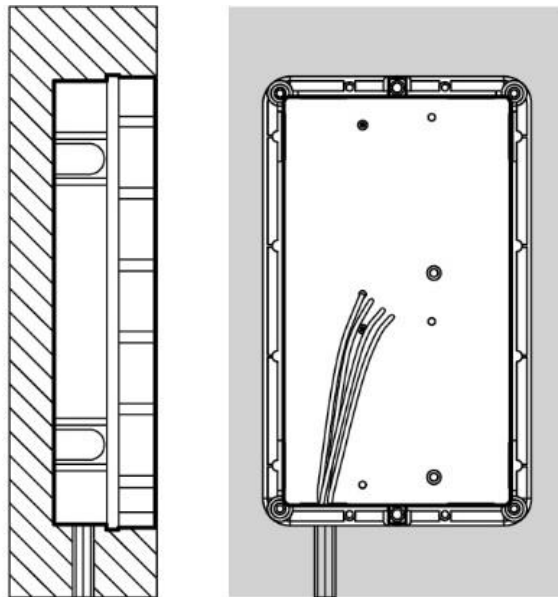
It is suggested to install the modules at the height shown below, according to the system to be realized.



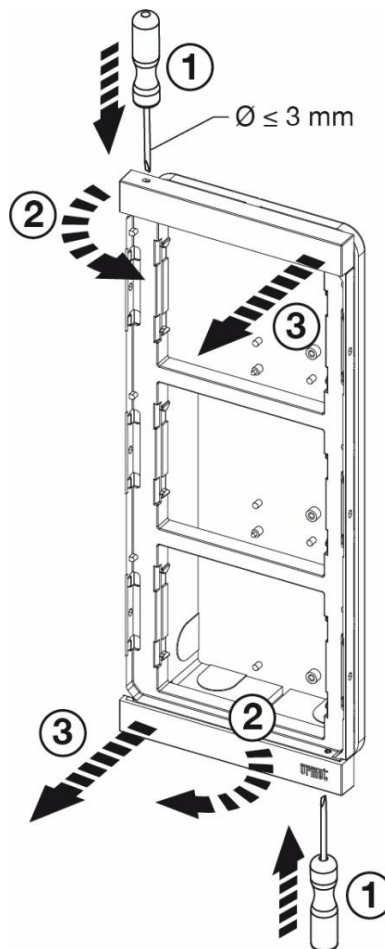
However, for complex systems with several modules, for a correct installation consider the height shown in the figure to fix the camera. If the system is a door phone, height refers to the door unit.

## Flush-mounted version

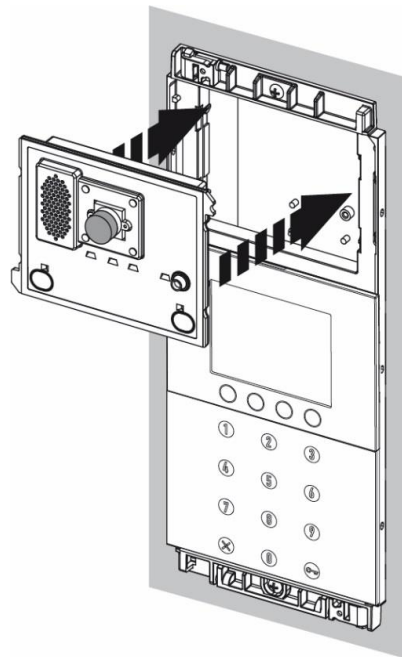
- Prepare the flush-mounting hole for the passages of the connecting wires.
- Install the flush mounting box: it must not jut out of the wall.



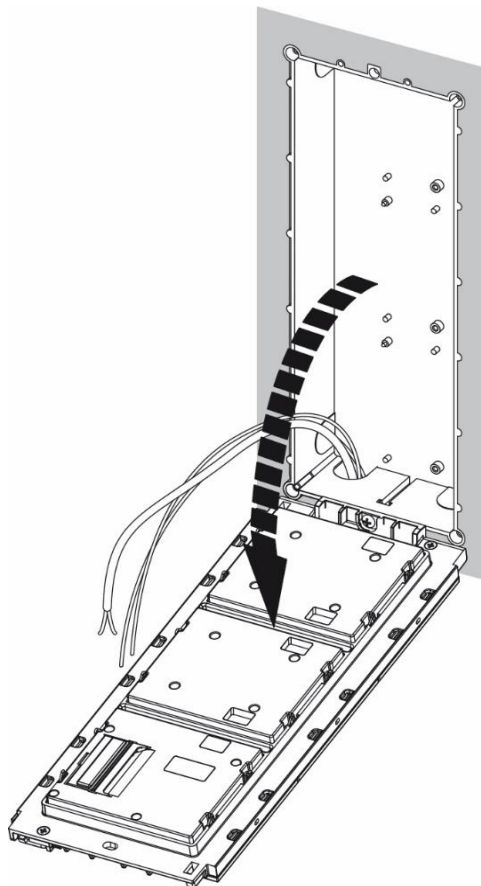
- Remove the upper header and the lower header from the frame using a flat screwdriver at the tip 0.



- Fit the module holder frame.

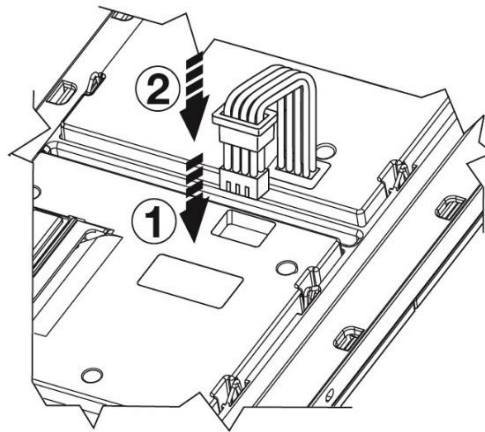


- Tip the holder frame and connect the wires.

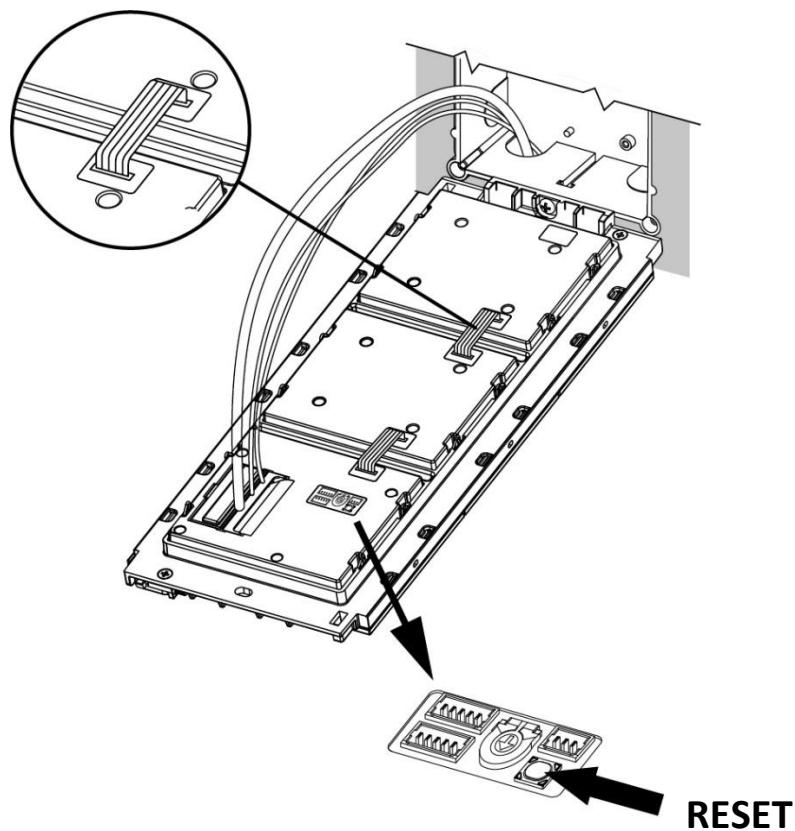


- Adjust correct perpendicularity of the call module.

- Establish the connections between the various modules with the wires provided before powering the system.



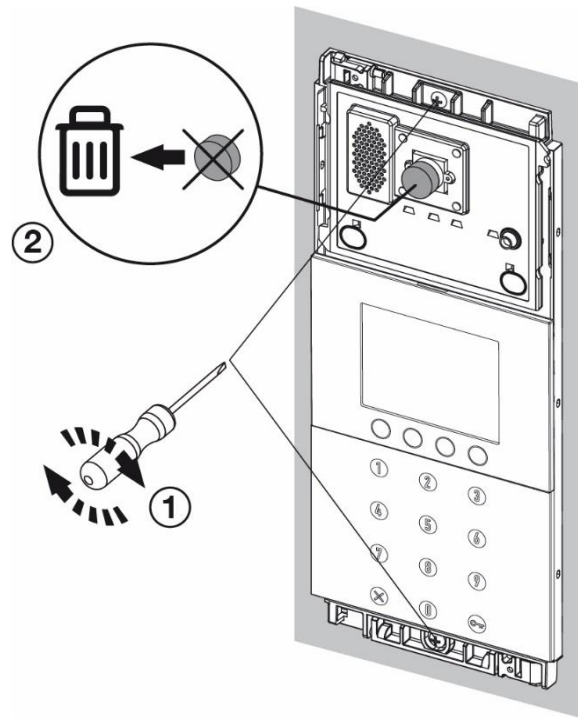
- Use the cord provided with the frame to connect modules belonging to frames arranged side by side.
- On the last module be sure to protect the OUT connector using the cap provided.



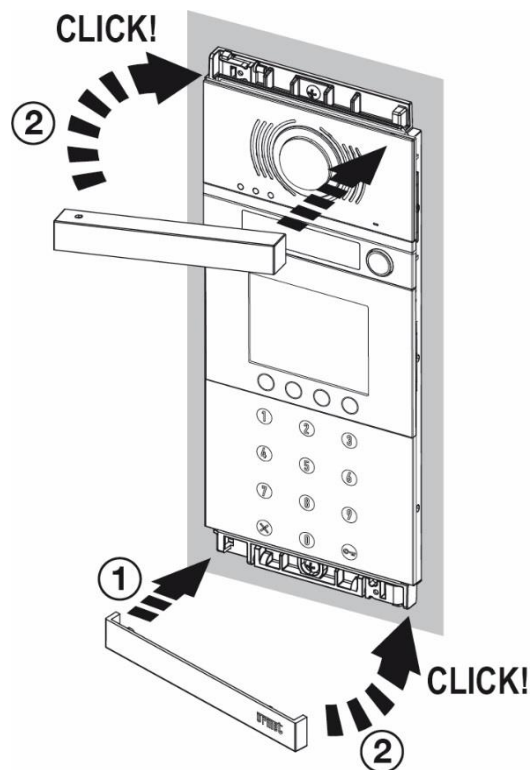
- On the rear of the external unit there is the RESET key which must be pressed to restart or reset the device to factory settings.



- Close the frame by tightening the screws.

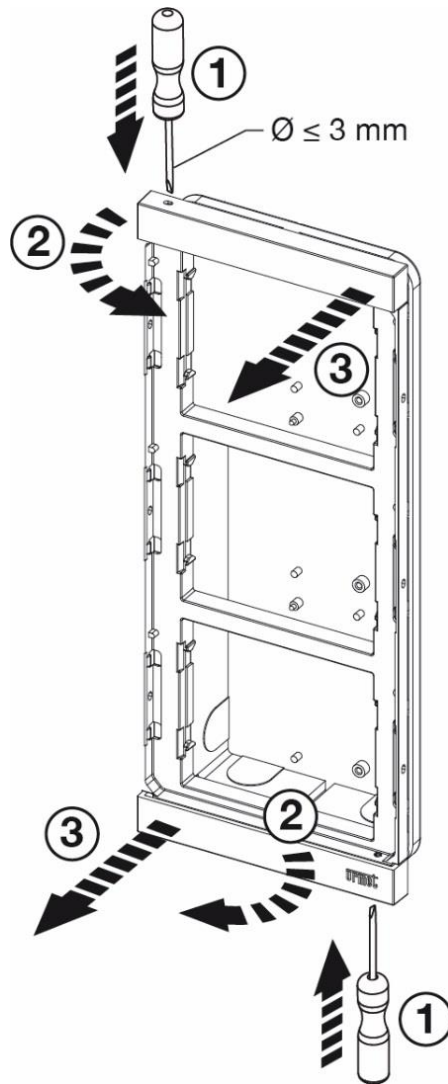


- Attach upper header and lower the frame.



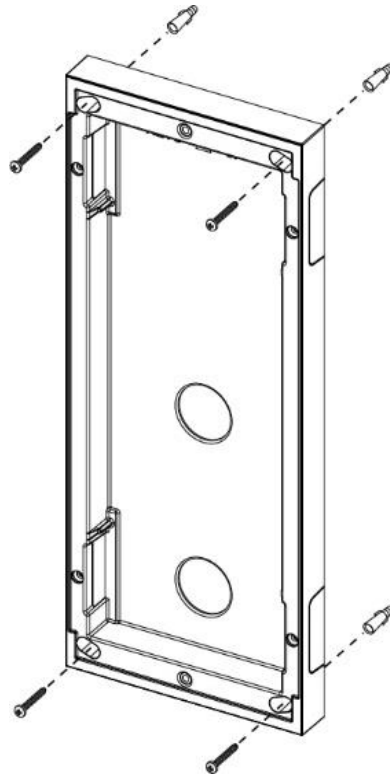
## Wall-mounted version

- Remove the upper header and the lower header from the frame using a flat screwdriver at the tip 0.

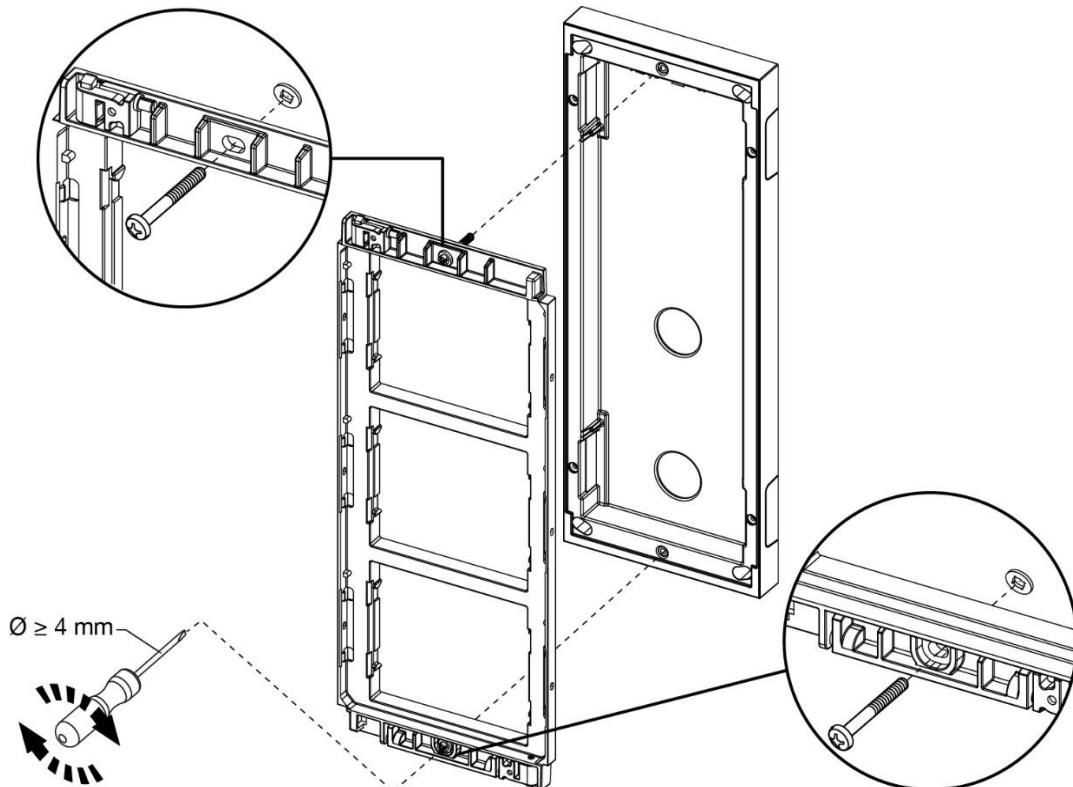


- Remove the module holder frame from the casing.

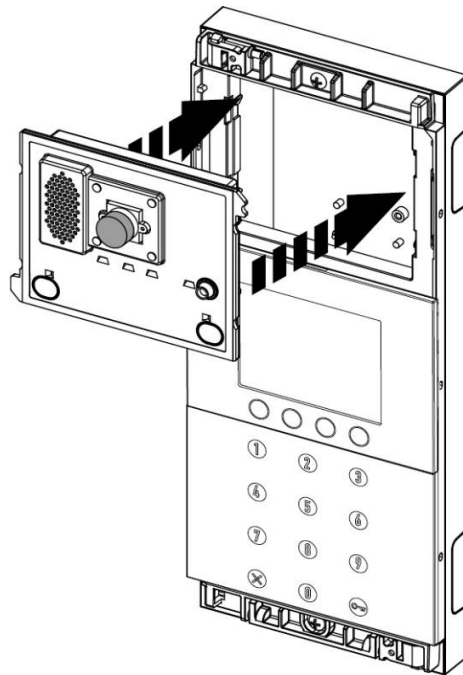
- Secure the casing with screws to the wall.



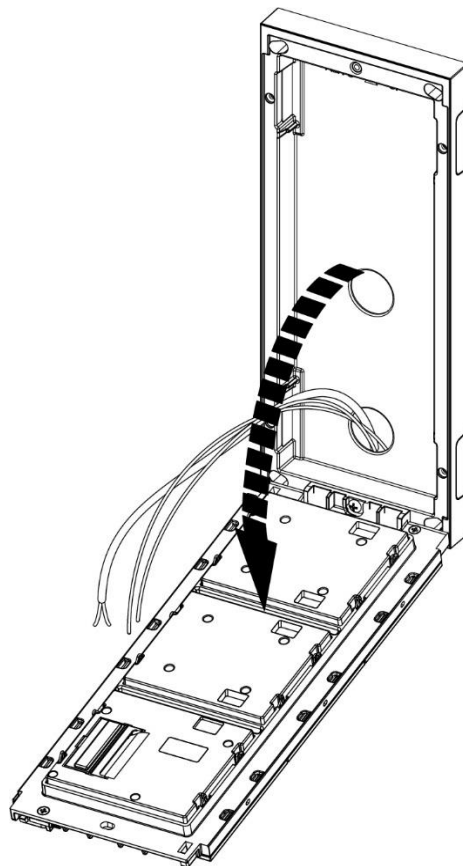
- Fit the module holder frame.



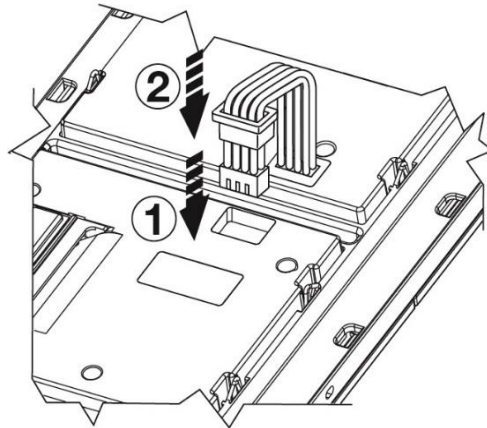
- Fit the modules in the frame.



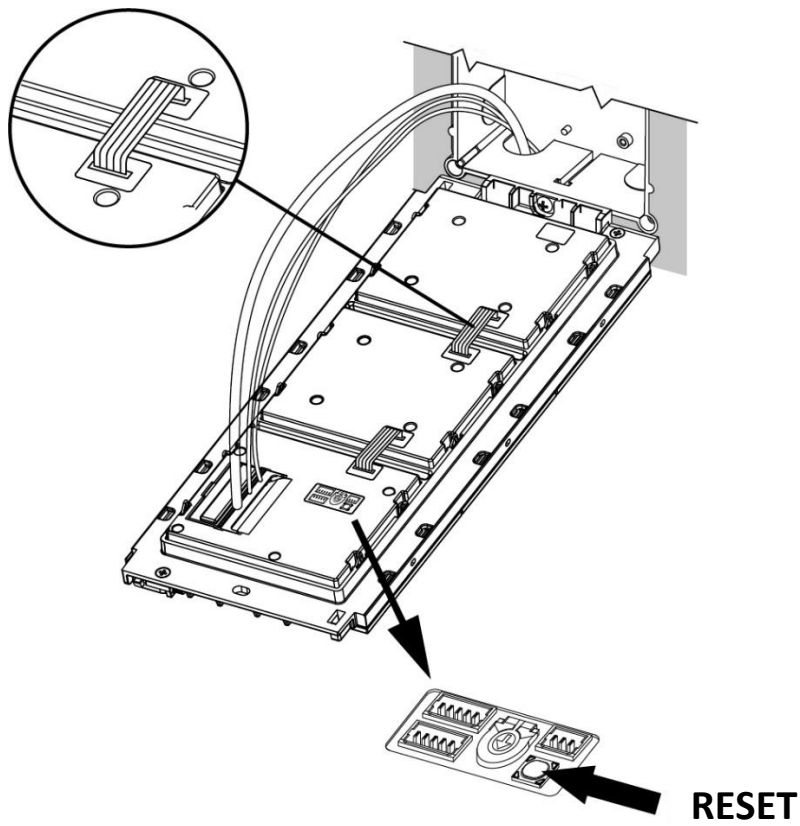
- Tip the frame and connect the wires.



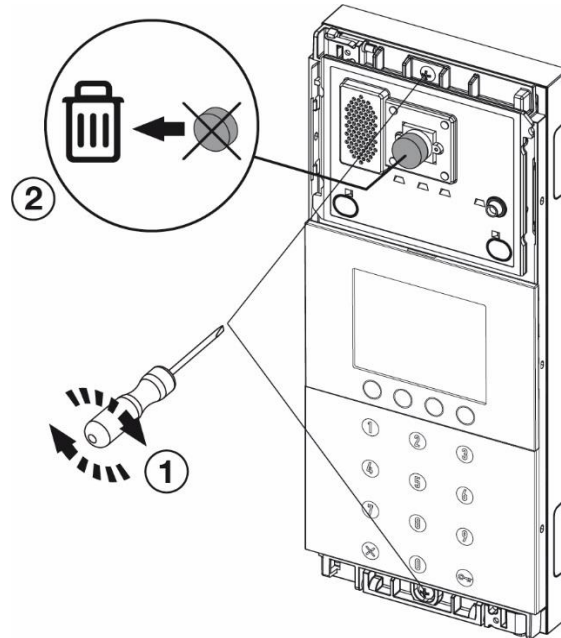
- Adjust correct perpendicularity of the panel.
- Establish the connections between the various modules with the wires provided before powering the system.



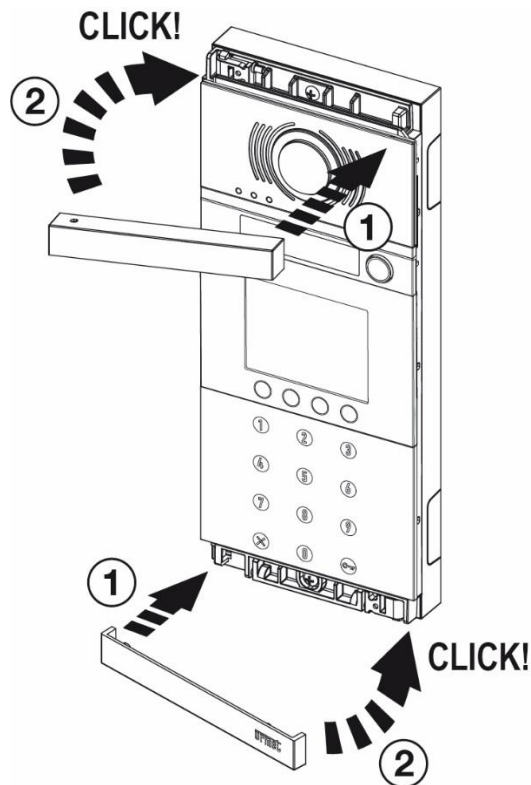
- On the last module be sure to protect the OUT connector using the cap provided.



- On the rear of the external unit there is the RESET key which must be pressed to restart or reset the device to factory settings.
- Attach upper header and lower the frame.



- Attach upper header and lower the frame.



## APPENDIX M1: 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:

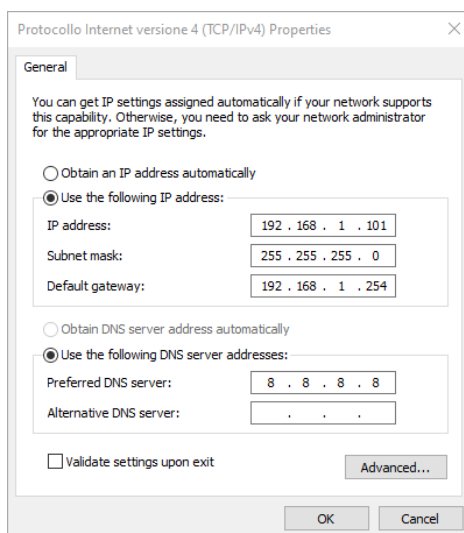


Figure 791: static IP address assignment

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 792: 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 793: password accepted

After pressing the “OK” button, the login window appears:

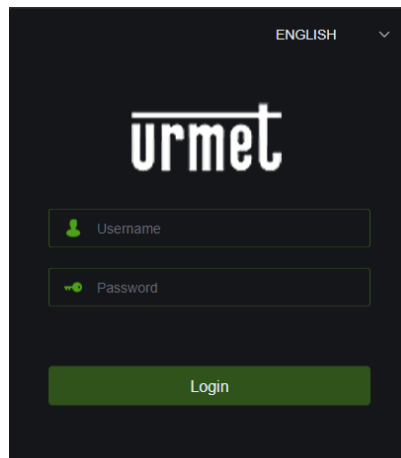


Figure 794: login window

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

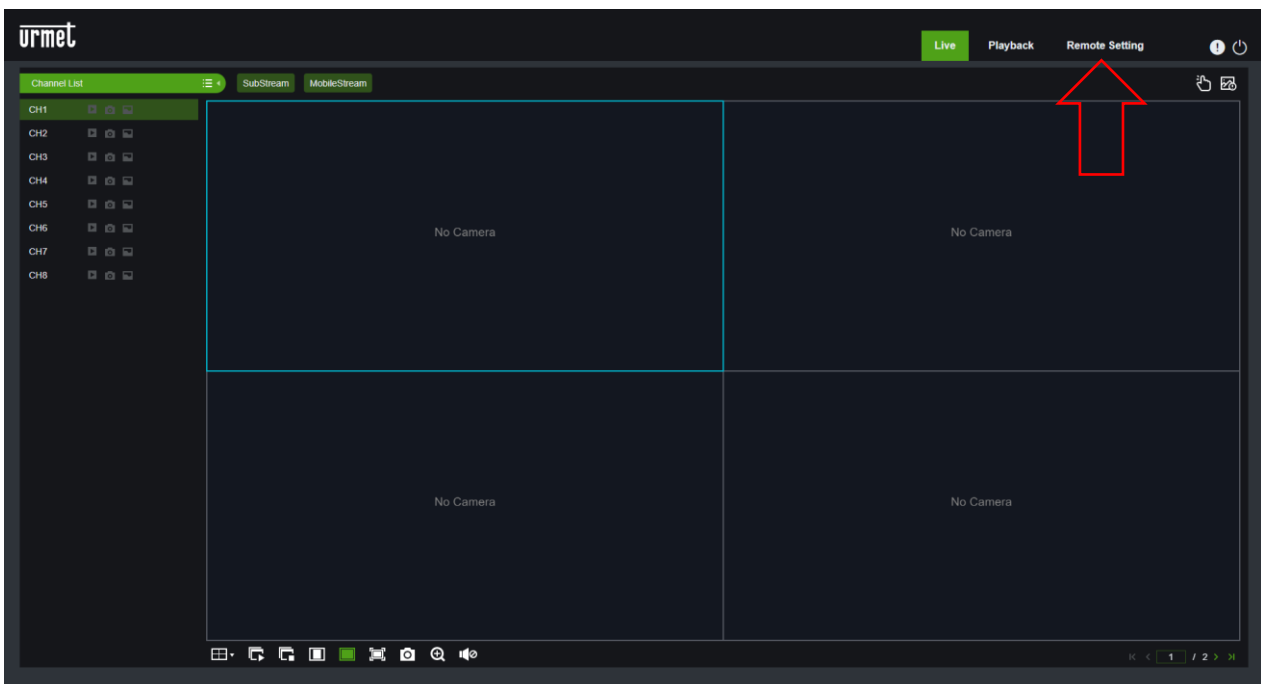


Figure 795: access to the NVR device

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

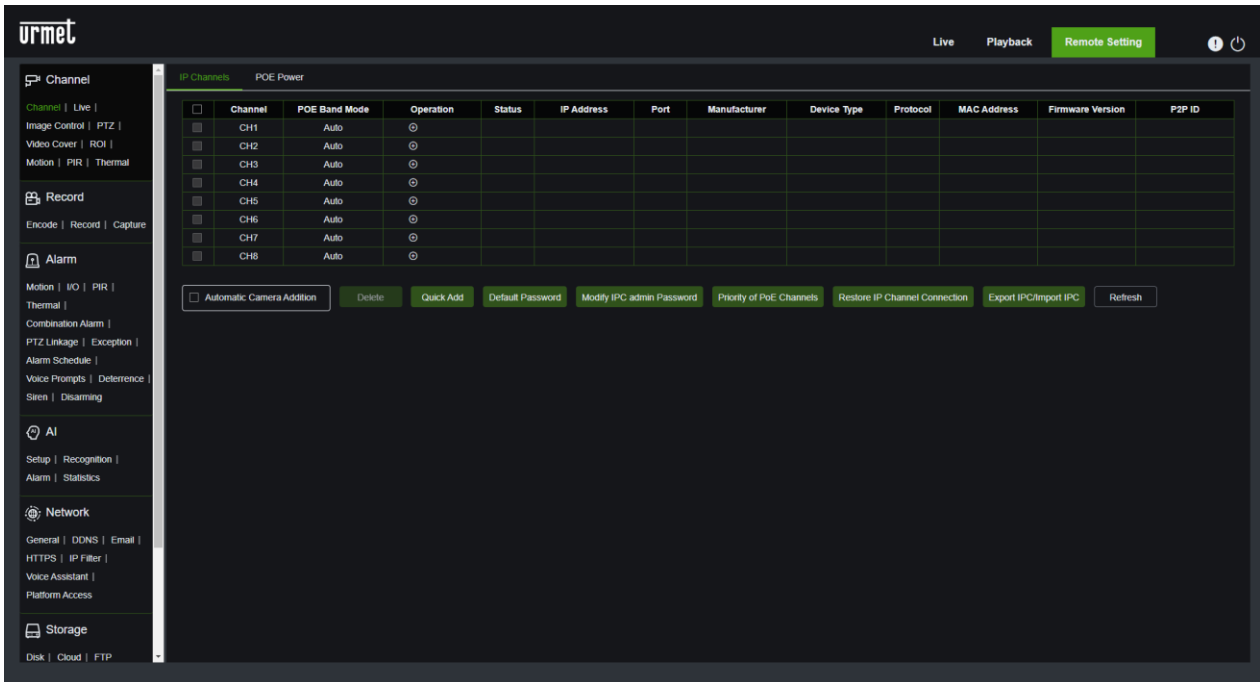


Figure 796: tab “Remote Setting”

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):

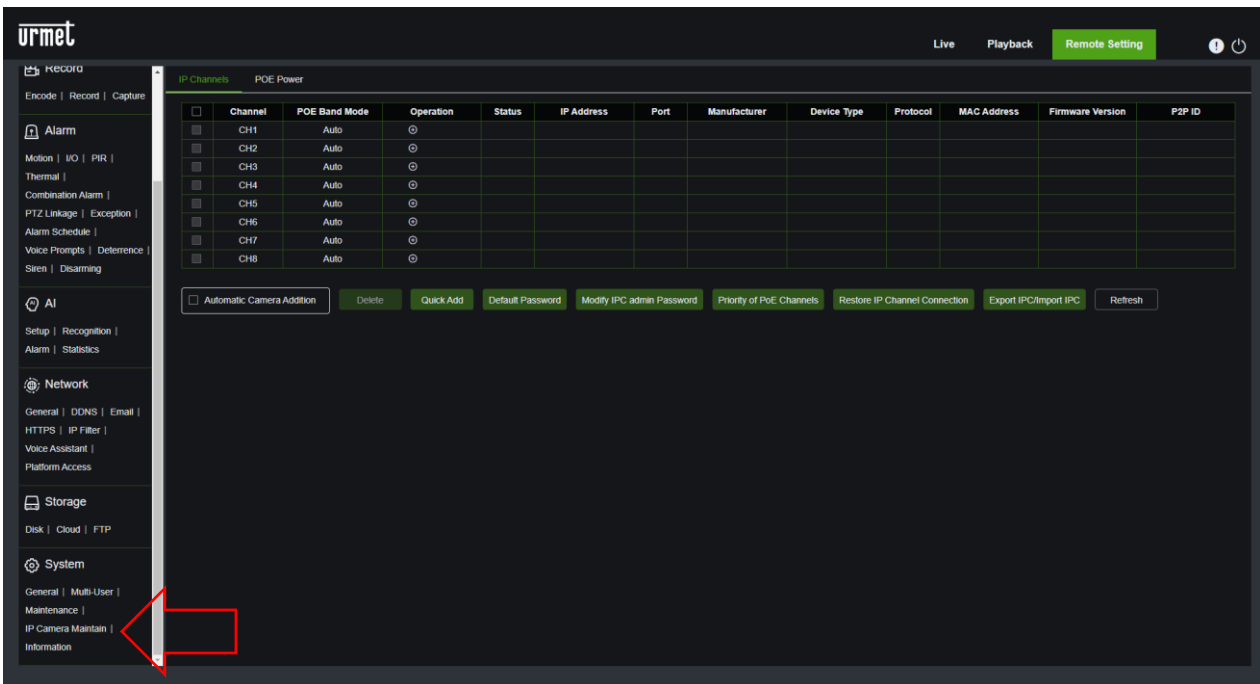


Figure 797: tab “Remote Setting” - section “System”

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

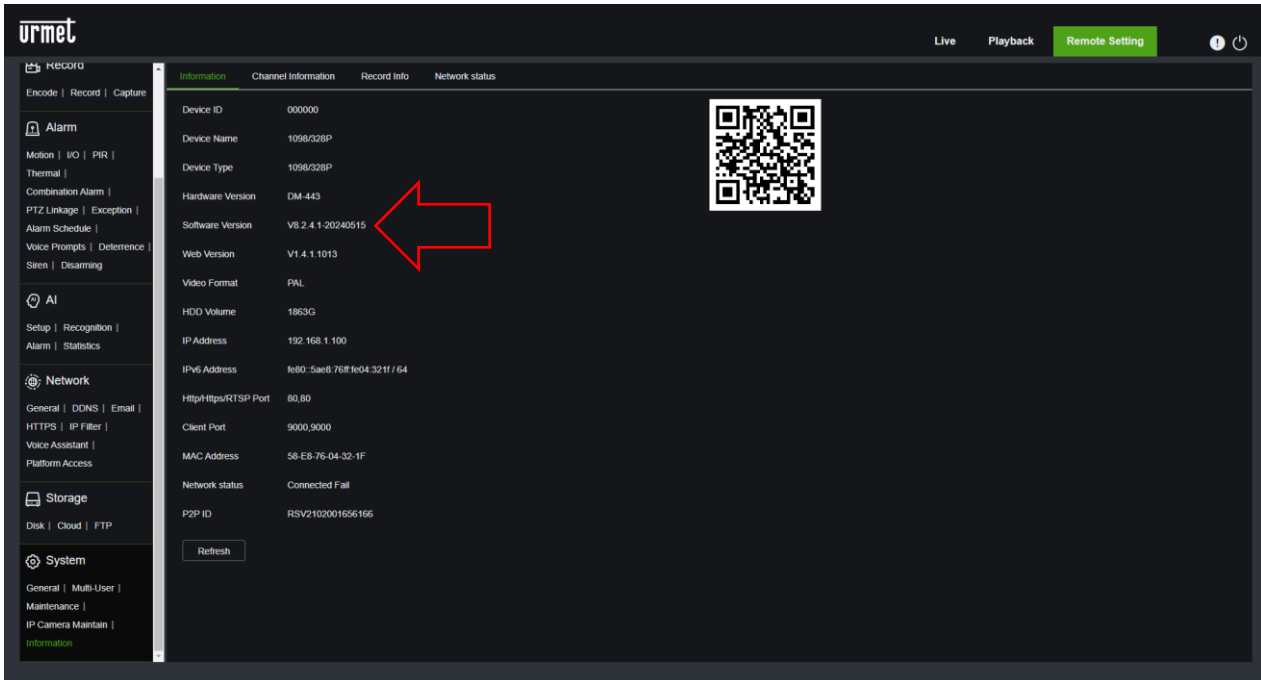


Figure 798: tab “Remote Setting” - section “System” ---> “Information”



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 default value of 5 minutes.

## 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](http://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:

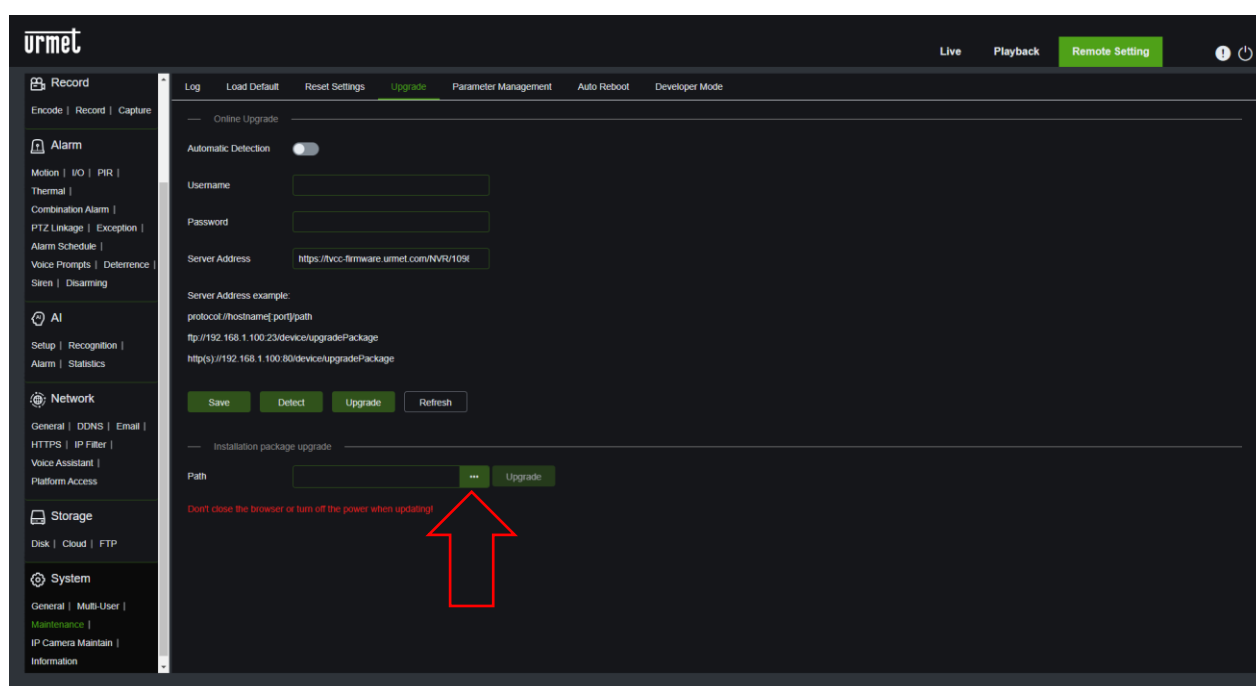



Figure 799: button to upload the software update file

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:

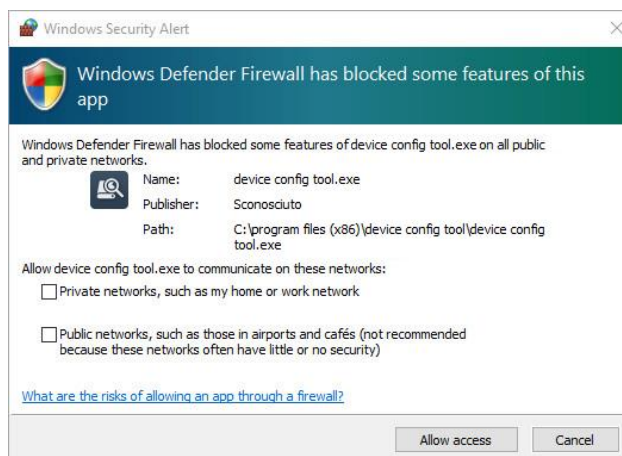
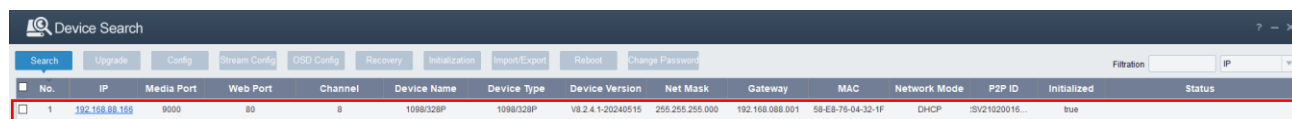


Figure 800: Windows Firewall block for Device Config Tool application

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



No.	IP	Media Port	Web Port	Channel	Device Name	Device Type	Device Version	Net Mask	Gateway	MAC	Network Mode	P2P ID	Initialized	Status
1	192.168.88.168	9000	80	8	1098328P	1098328P	V8.2.4.1-20240515	255.255.255.000	192.168.088.001	58-E8-76-04-32-1F	DHCP	SV21020016	true	

Figure 801: 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):

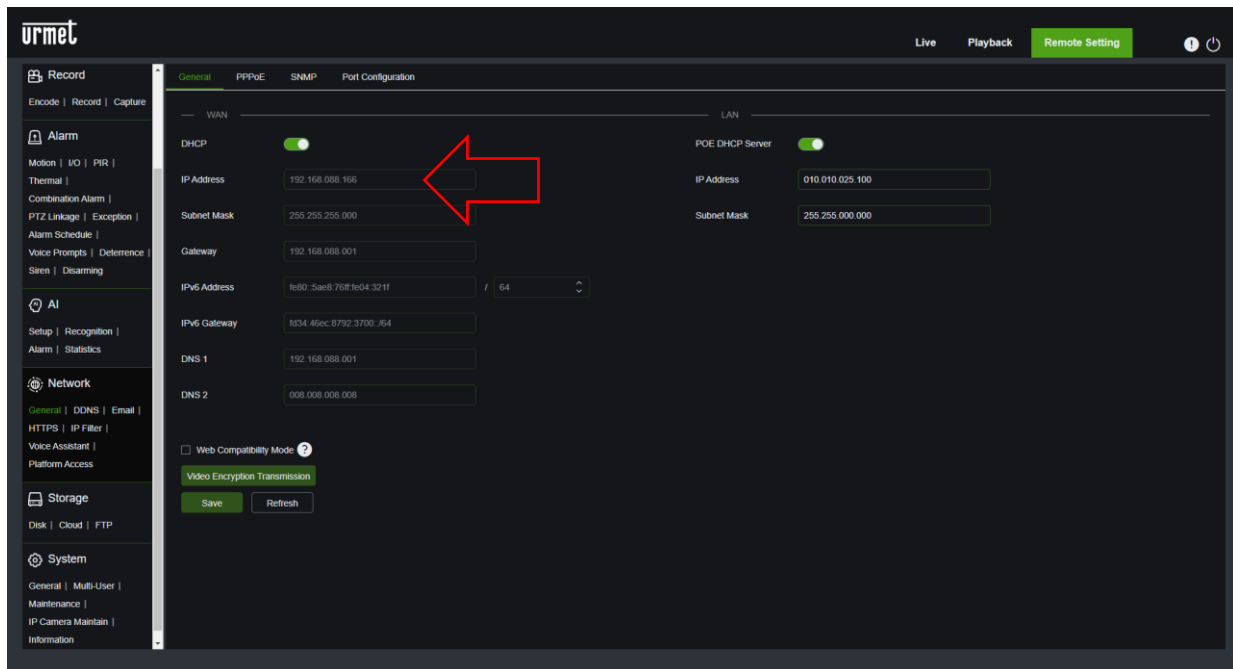


Figure 802: tab “Remote Setting” - section “Network” --- > “General”

## 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:

The screenshot shows a 'New Device' configuration window with the following fields:

Field	Value
RTSP In-Call Stream	<input checked="" type="checkbox"/>
IP Address	10.10.128.0
Network Mask	255.255.0.0
Port	8554
Stream	h264urmet
Username *	urmet
Password *	1937
Streaming URI	rtsp://urmet:1937@10.10.128.0:8554/h264urmet

At the bottom, there are 'OK' and 'Cancel' buttons, and a note: '\* mandatory field'.

Figure 803: 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:

The screenshot shows the 'System' tab in the 'Urmet IperCom Configurator' with the following settings:

Section	Field	Value
Custom Network Settings	IP Range Minimum	10.10.128.0
	IP Range Maximum	10.10.255.254
	RTSP - Default Network Mask	255.255.0.0
	RTSP - Default Username	
	RTSP - Default Password	
Call Divert Settings		
Maintenance Settings		
Sunrise/Sunset Settings		

At the bottom, there are 'Apply' and 'Cancel' buttons.

Figure 804: 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:

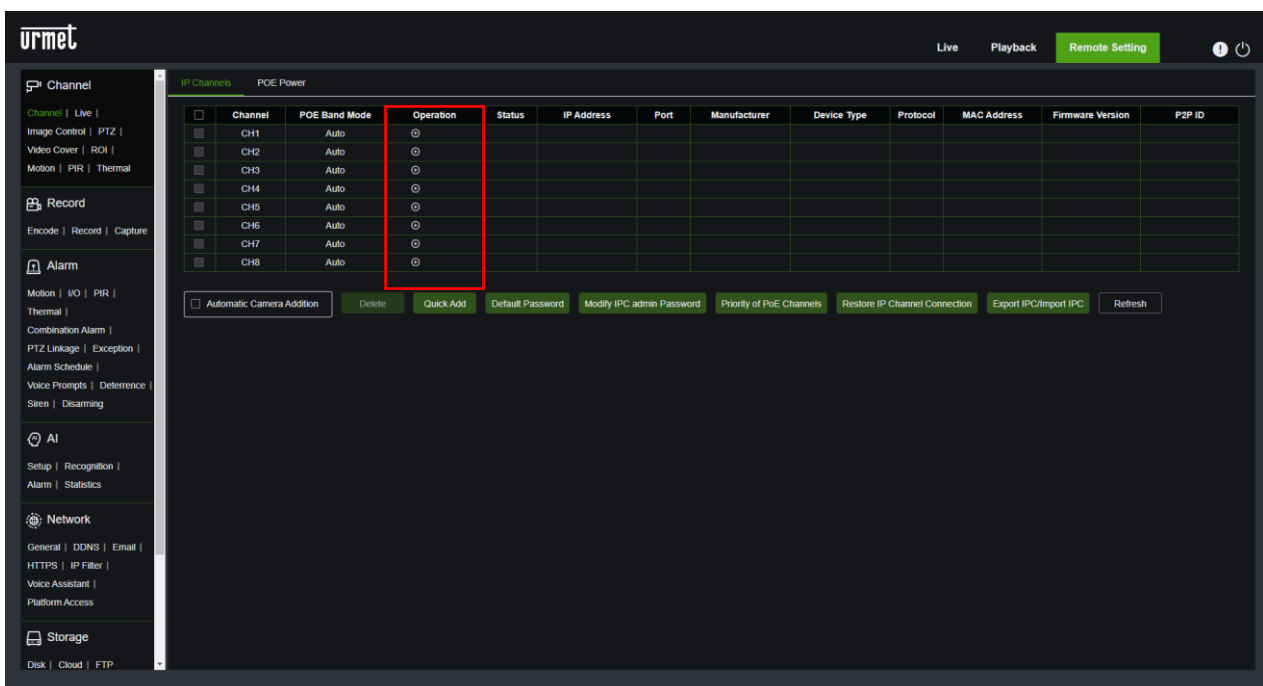



Figure 805: tab “Remote Setting” - section “Channel” --- > “Channel”

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

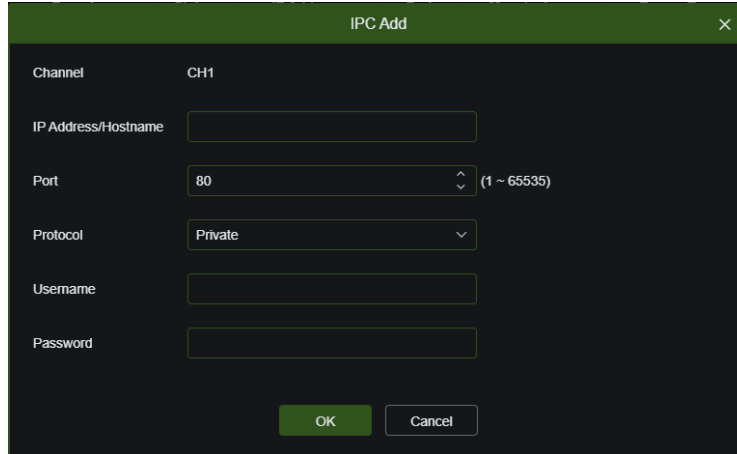


Figure 806: parameters for setting the channel

In the “Protocol” field, select the “RTSP” item. The following screen appears:

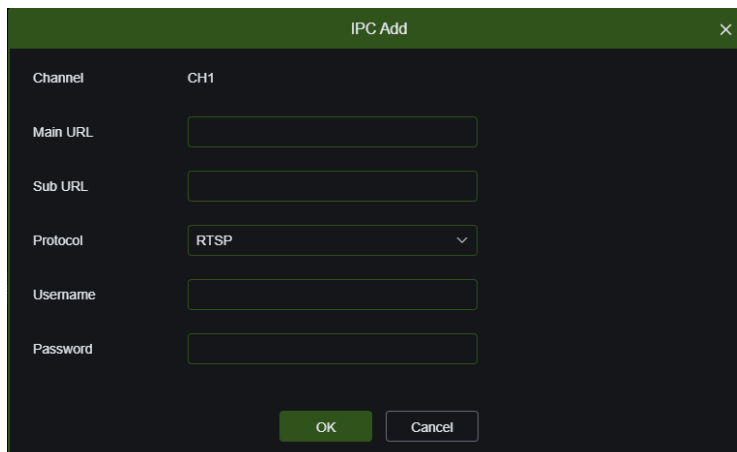


Figure 807: RTSP protocol setting on CH1 channel

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

Figure 808: 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:

Channel	POE Band Mode	Operation	Status	IP Address	Port	Manufacturer	Device Type	Protocol	MAC Address	Firmware Version	P2P ID
CH1	Auto	⊕	⊕	10.10.128.0	8554			RTSP			
CH2	Auto	⊕									
CH3	Auto	⊕									
CH4	Auto	⊕									
CH5	Auto	⊕									
CH6	Auto	⊕									
CH7	Auto	⊕									
CH8	Auto	⊕									

Figure 809: 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:

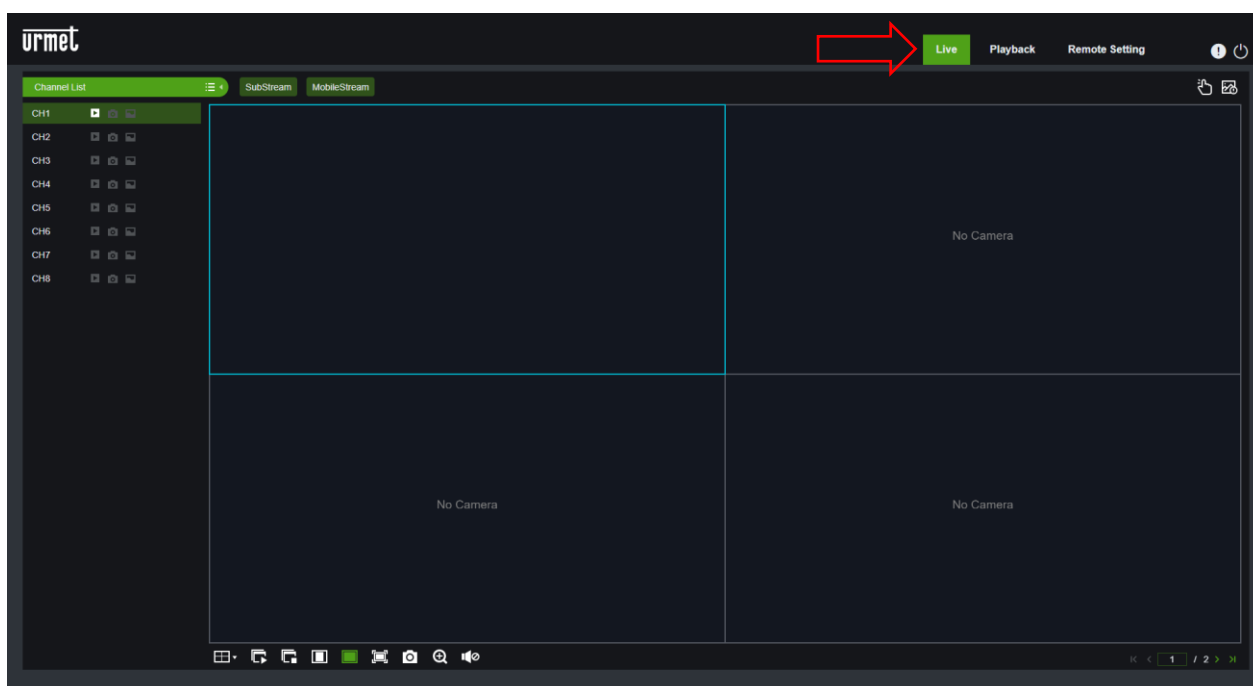


Figure 810: “Live” tab to view the streaming video

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:

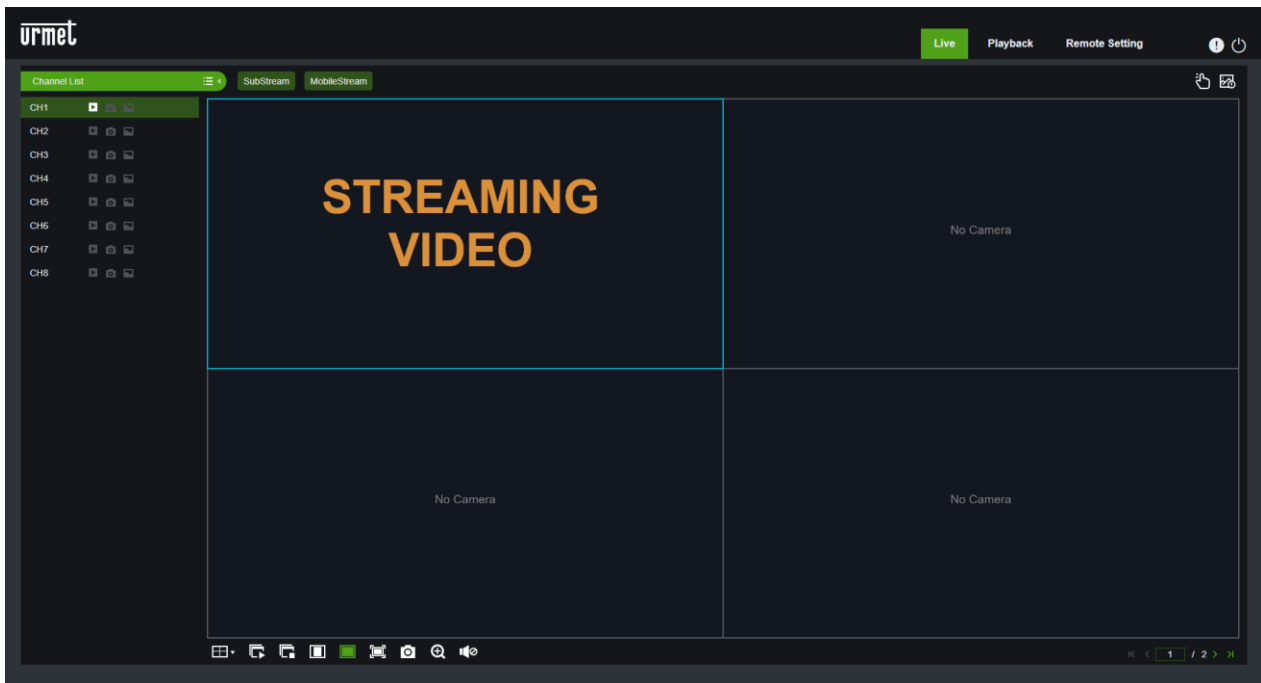


Figure 811: streaming video during calls from the calling station or auto-on from the video door phone

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:

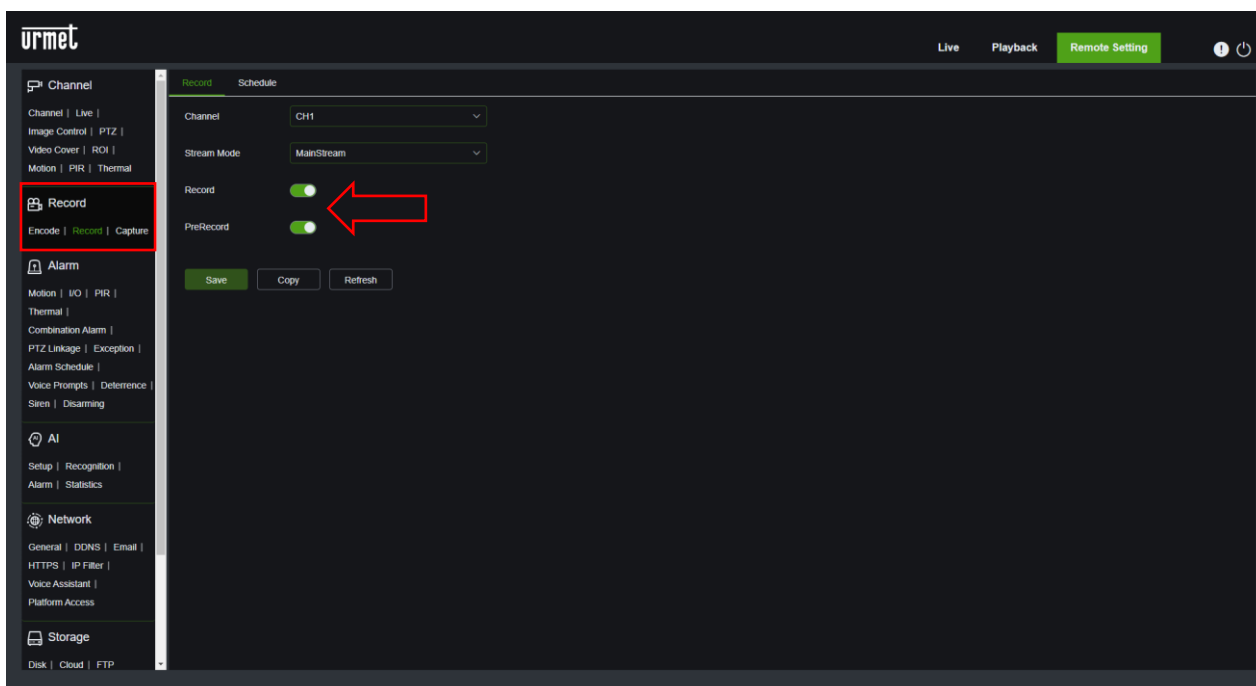


Figure 812: tab “Remote Setting” - section “Record” --- > “Record”

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 813: “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:

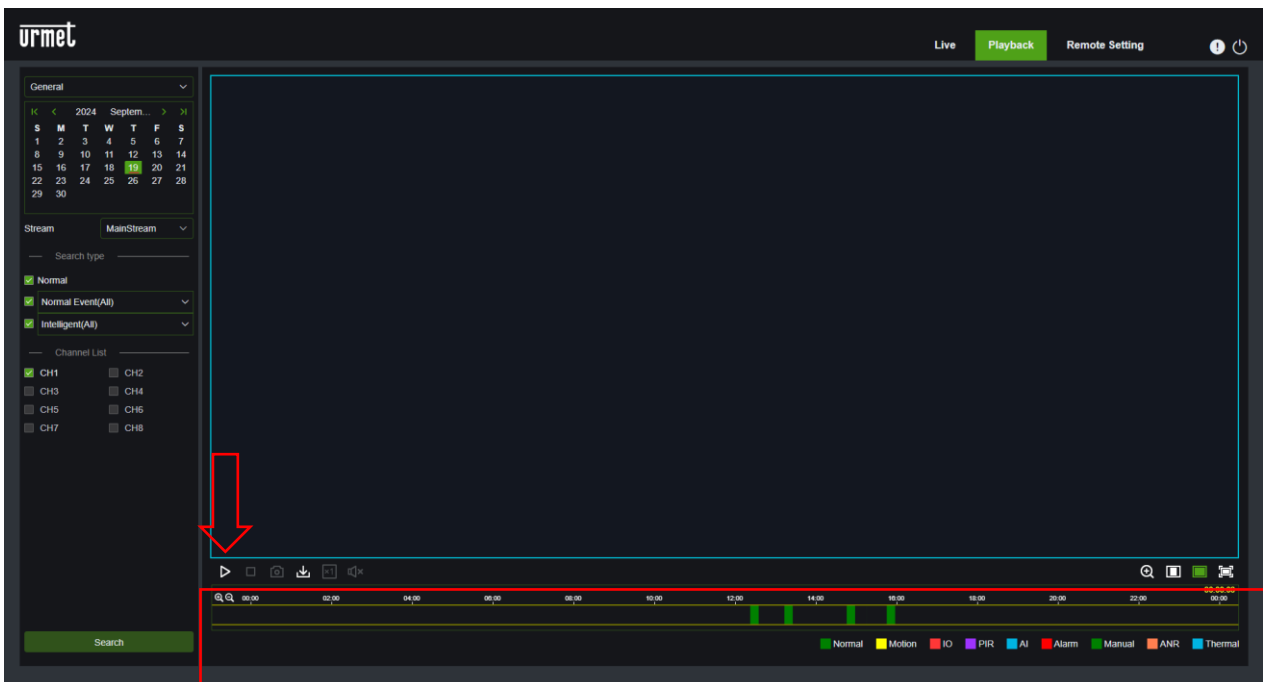



Figure 814: channel selection in the “Playback” tab

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:

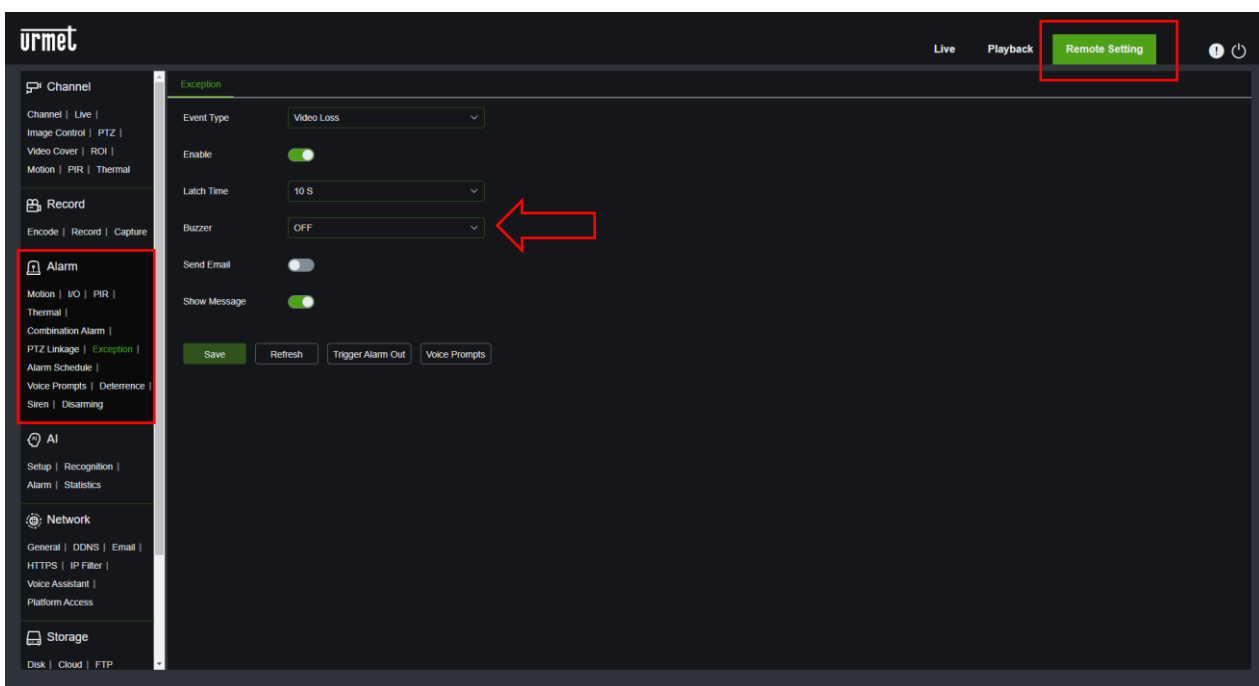


Figure 815: enable the acoustic signal in case of video loss (tab “Remote setting” - section “Alarm” --- > “Exception”)

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 M2: 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:

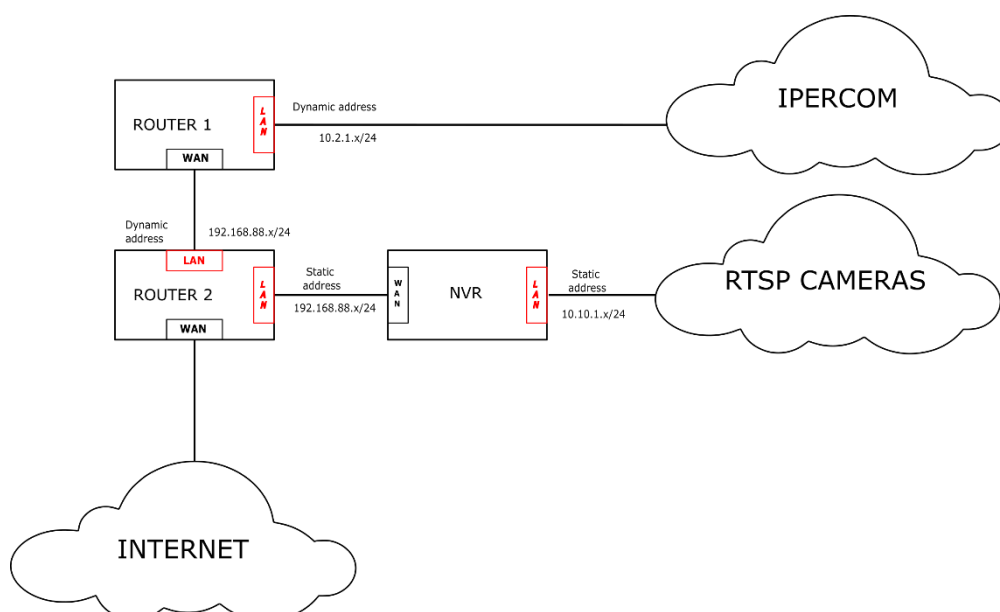



Figure 816: connection diagram for RTSP cameras and Urmet NVR device

 **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:

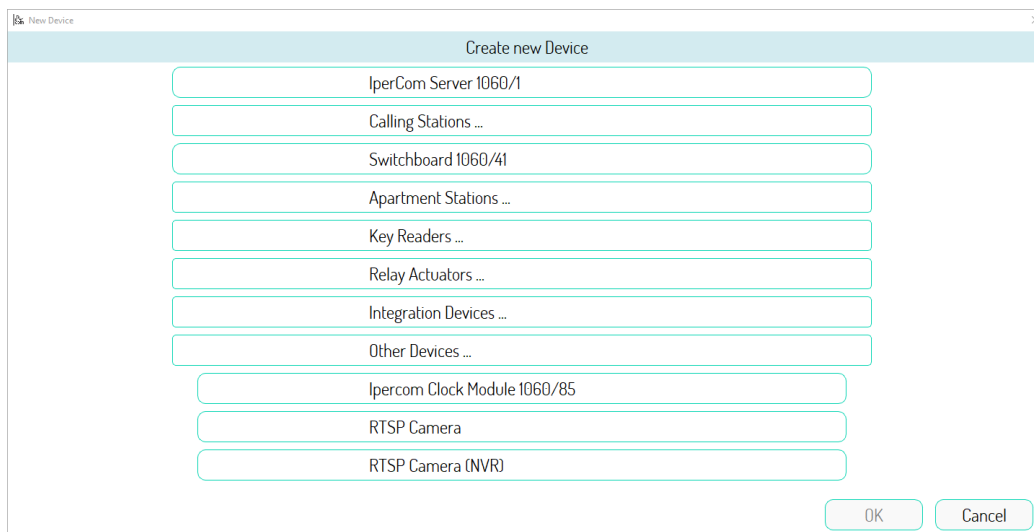


Figure 817: “RTSP Camera (NVR)” device

The following screen appears:

Figure 818: “RTSP Camera (NVR)” device configuration page

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

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

Table 95: 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 N: “Site name” and “Global site 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.

The *CallMe Manager* application is present only if the relevant item is enabled in the *configurator*: in this case the "Global site ID" parameter also comes into play, as explained after.

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):

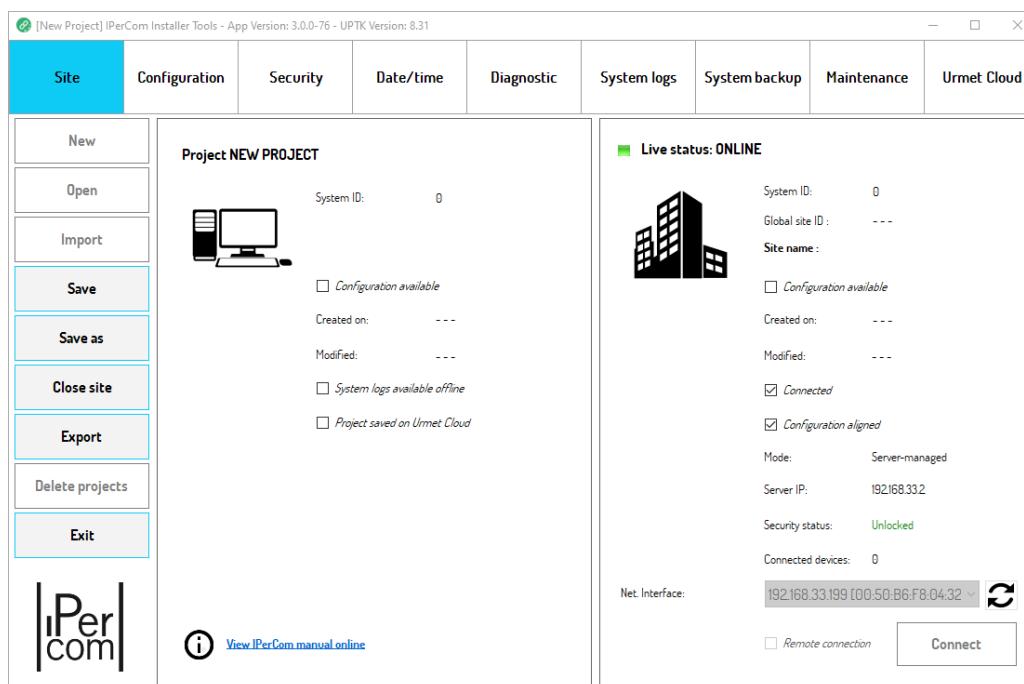


Figure 819: “Site name” field not filled in yet

The “Site name” field has not yet been filled in.

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

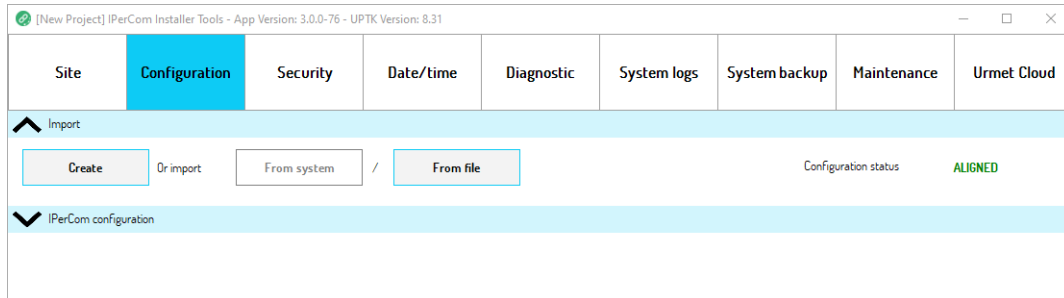


Figure 820: creation of a new configuration

The screen that appears is the following:

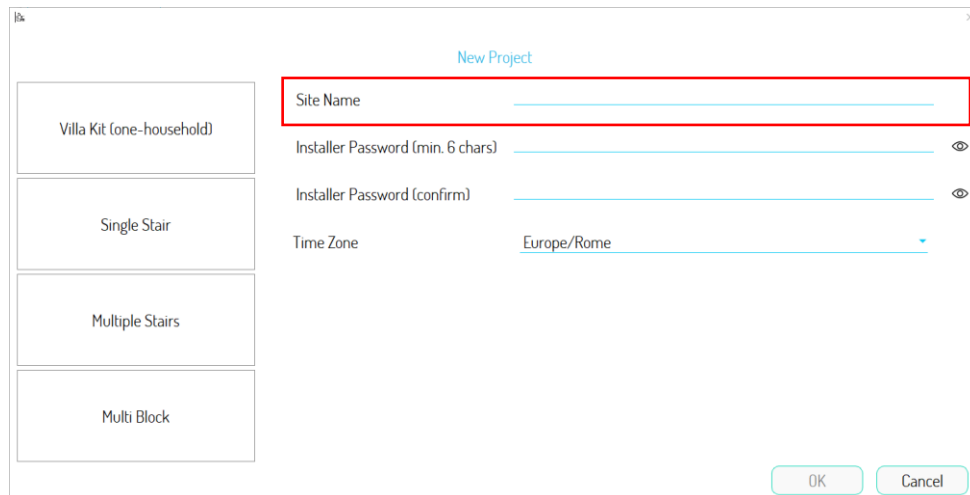


Figure 821: "Site name" field when creating a configuration

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

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

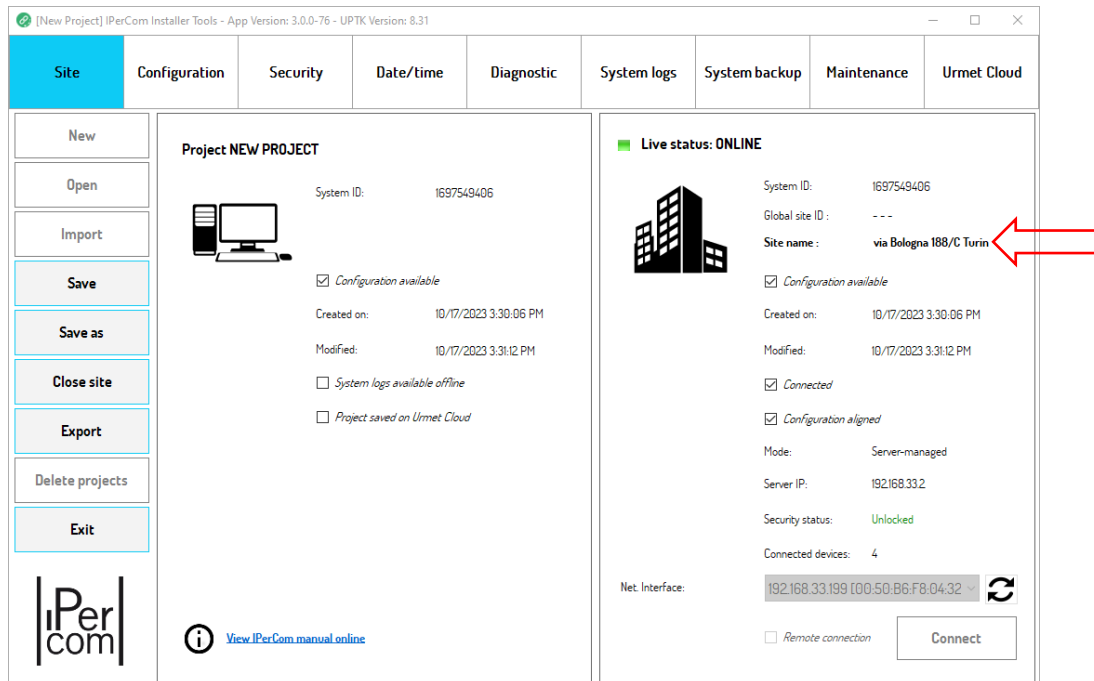


Figure 822: “Site name” field filled in in *iPerCom Installer Tools*

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).

If *CallMe Manager* support is enabled from the *configurator*, the "Global site ID" field is also filled in in the screen above (after having applied the configuration):

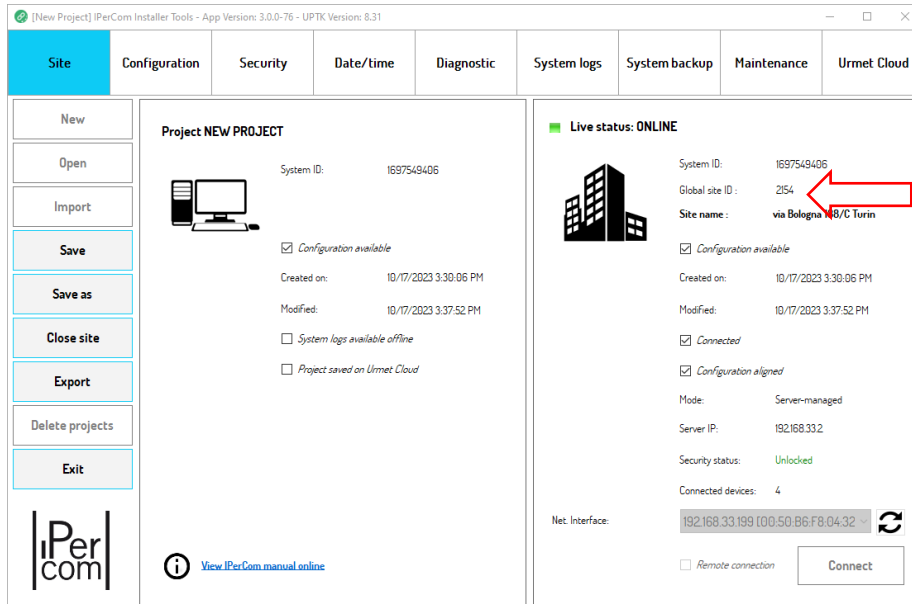


Figure 823: "Global site ID" filled in

In the *CallMe Manager* application, once the site has been imported, the "Site name" field reports what is reported in *IPerCom Installer Tools* while the "ID" field reports the "Global site ID" and "System ID" values also from *IPerCom Installer Tools*:

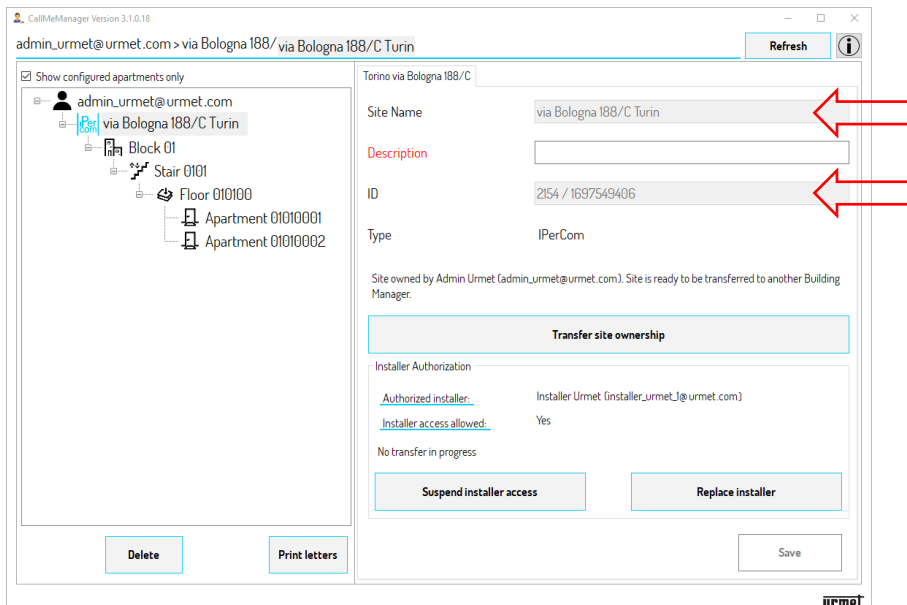


Figure 824: "Global site ID" and "Site name" fields in CallMe Manager

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



## APPENDIX O: IPassan integration with IPerCom

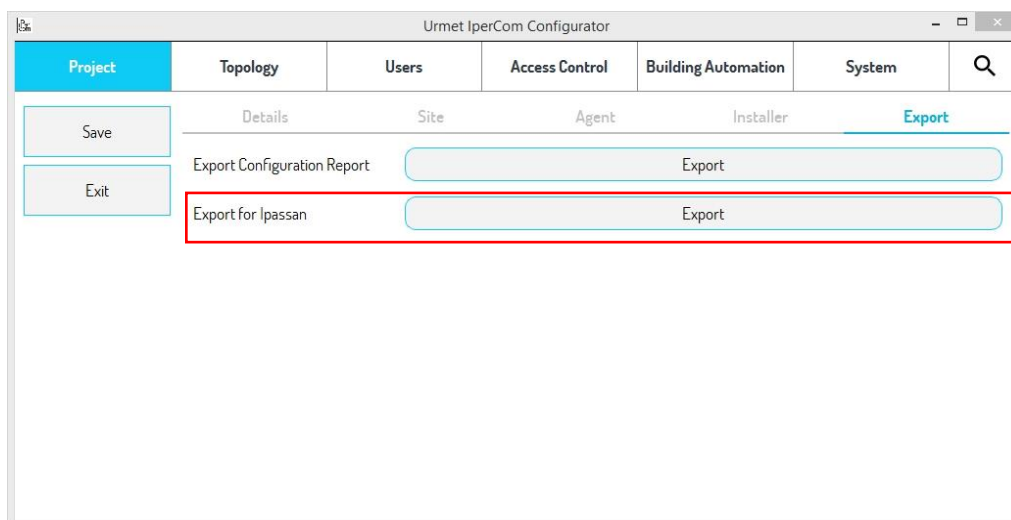
The integration of the IPassan system with the IPerCom system is carried out as follows.

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:



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 P1: 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:



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

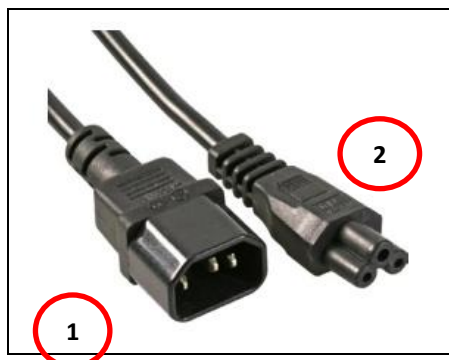
With the LED green, briefly press the button shown in the figure above and wait for the LED to turn yellow. The 1060/1 Server is off and only now you can disconnect the power cord.

## APPENDIX P2: 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):



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:

- Versione UPTK: 6.31

Operazione completata

Sicurezza

agnostica

	APC : 001,046,1104		
	DATE : 2020-01-30 15:47:53 +0100		
	HOSTNAME : IPERCOM		
	VERSION : 3.14.14 (31 May 2016) debian		
	UPSNAME : IPERCOM		
	CABLE : USB Cable		
	DRIVER : USB UPS Driver		
	UPS.MODE : Stand Alone		
	STARTTIME: 2020-01-29 14:20:24 +0100		
	MODEL : Back-UPS CS 650		
	STATUS : ONBATT		Configurat
	LINEV : 0.0 Volts	0.136	30/01/202
	LOADPCT : 1.0 Percent		
_3_8_R6_ROOT	BCHARGE : 23.0 Percent	0.110	30/01/202
_3_8_R6_ROOT	TIMELFT : 10.2 Minutes	0.109	30/01/202
_3_8_R6_ROOT	MBATTCHG : 5 Percent	0.112	30/01/202
	MINTIMEL : 3 Minutes		
	MAXTIME : 0 Seconds		
	OUTPUTV : 230.0 Volts	0.105	30/01/202
	SENSE : Medium		
36	DWAKE : 0 Seconds	0.101	30/01/202
36	DSHUTD : 0 Seconds		
36	LOTRANS : 180.0 Volts	0.108	30/01/202
36	HITRANS : 266.0 Volts		
	RETPCT : 0.0 Percent	0.102	30/01/202
	ITEMP : 29.2 C		
	ALARMDEL : 30 Seconds	0.103	30/01/202
36	BATTV : 12.3 Volts		
	LINEFREQ : 50.0 Hz	0.107	30/01/202
_3_8_R6_ROOT	LASTXFER : Low line voltage	0.111	30/01/202
	NUMXFERS : 2		
	XONBATT : 2020-01-30 14:50:48 +0100	0.106	30/01/202
	TONBATT : 3426 Seconds	0.137	30/01/202
	CUMONBATT: 4009 Seconds		
	XOFFBATT : 2020-01-29 16:54:25 +0100	0.113	01/01/1970
	SELFTST : NO		

## APPENDIX P3: 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 *IPerUpgrade*;
- 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 Q: 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 *IPerUpgrade*, upgrade the *Server 1060/1* (or *Servers 1060/1*) to the required IPerCom firmware version (IPerUpgrade application and user manual available at [www.urmet.com](http://www.urmet.com));



*The Servers 1060/1 are upgraded on a network where, in addition to the Servers, there is only one PC where the IPerUpgrade 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:

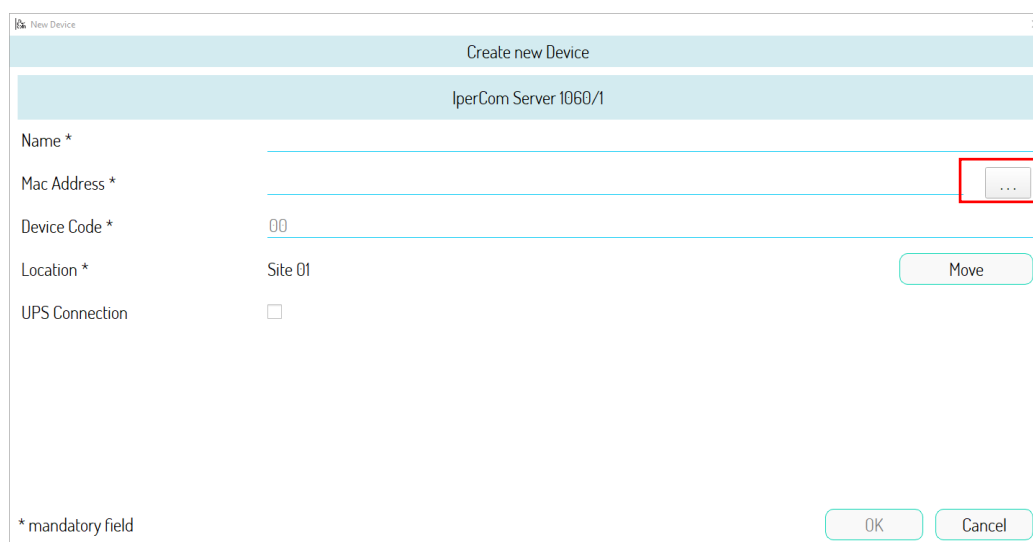


Figure 825: IperCom Server 1060/1

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

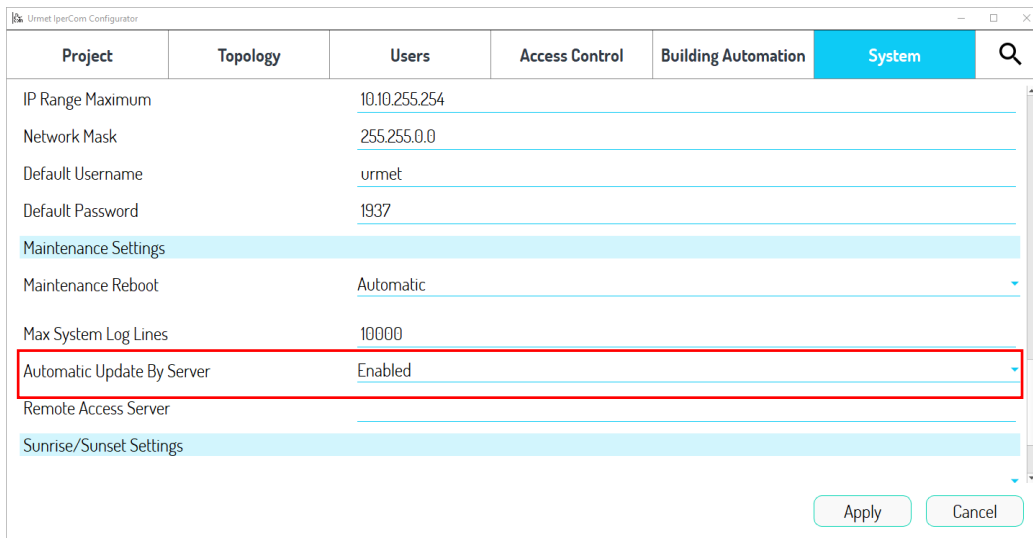


Figure 826: automatic update via IperCom server

- 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 R: Call to several Switchboard applications each connected to a CallMe app

### 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:

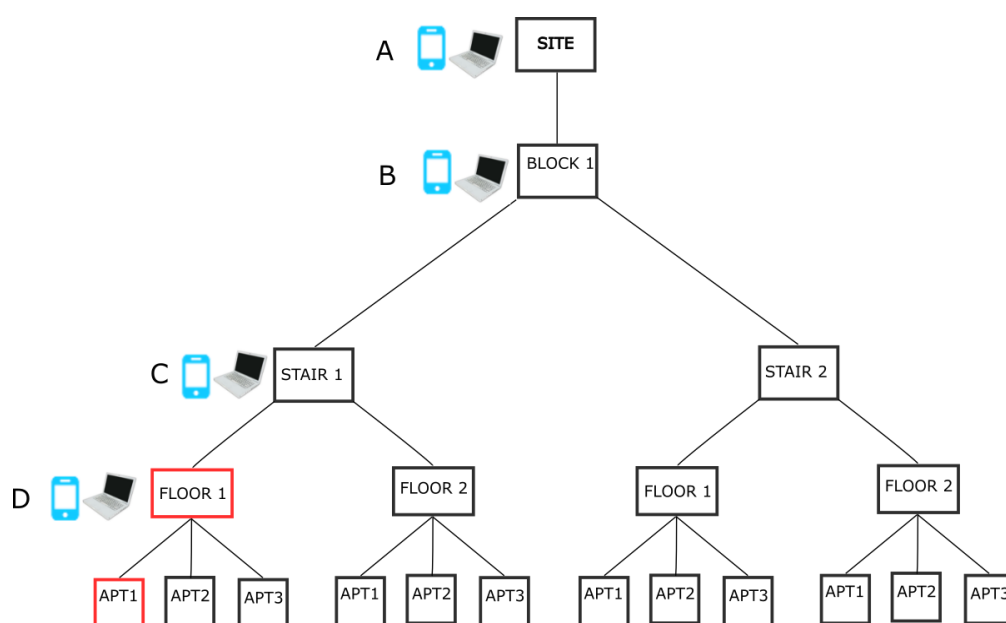



Figure 827: Topological structure with several switchboards

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:



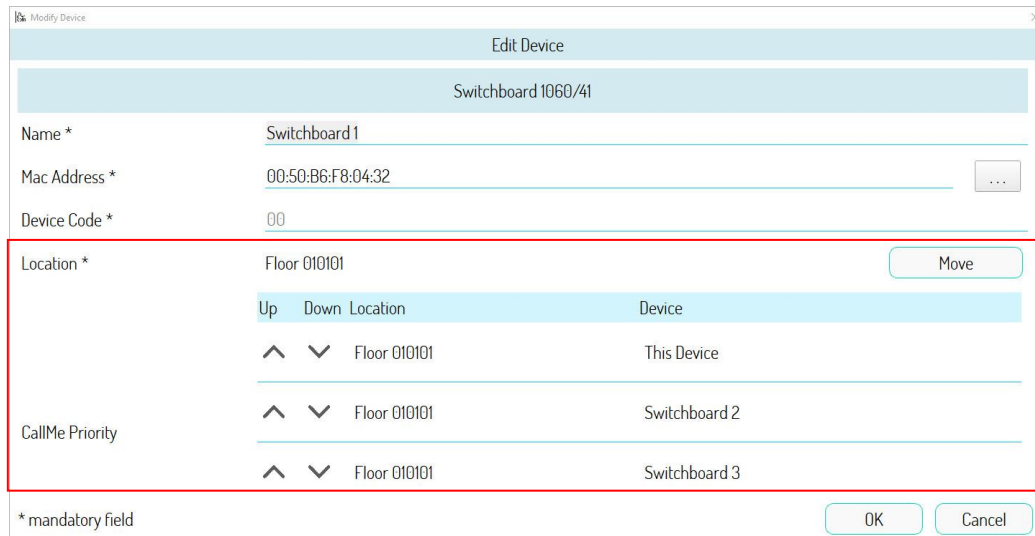


Figure 828: Configuration page with several Switchboard applications on the plant

The list can be modified using the and 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:

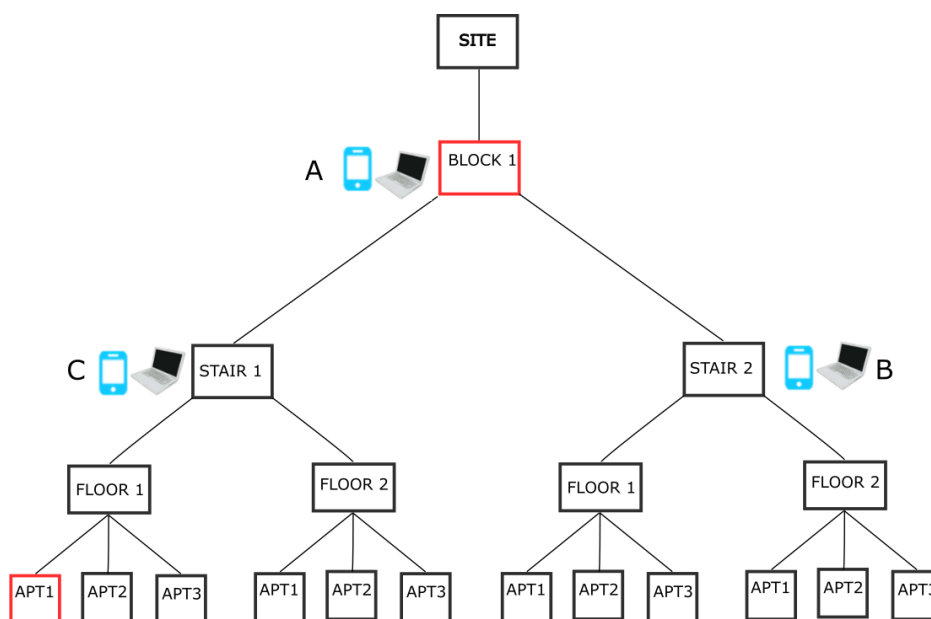


Figure 829: Topological structure with several switchboards

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:

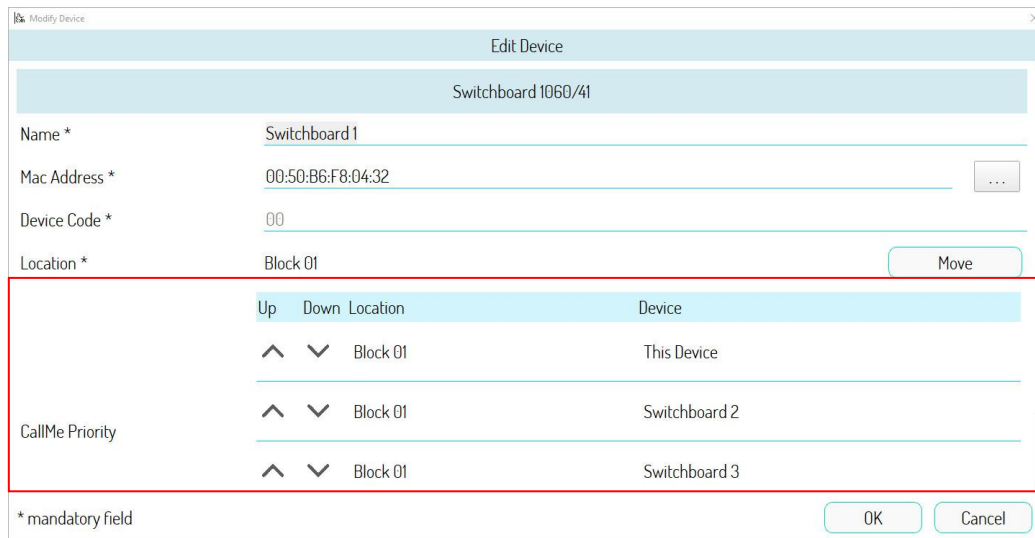


Figure 830: Configuration page with several Switchboard applications on the plant

The list can be modified using the and 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 S: 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:

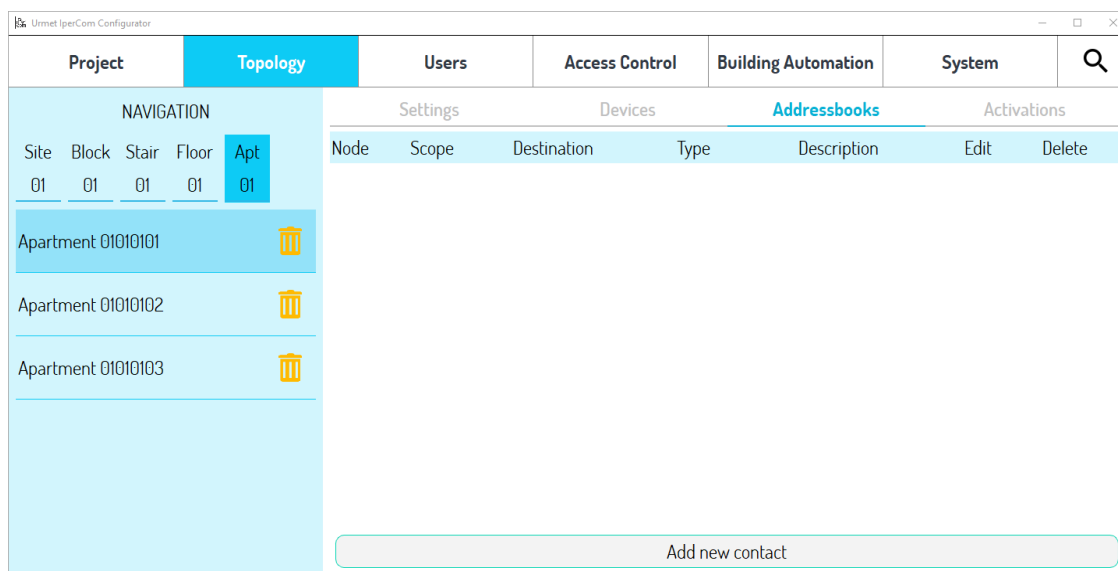


Figure 831: Topological structure with tab "Addressbooks"

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):

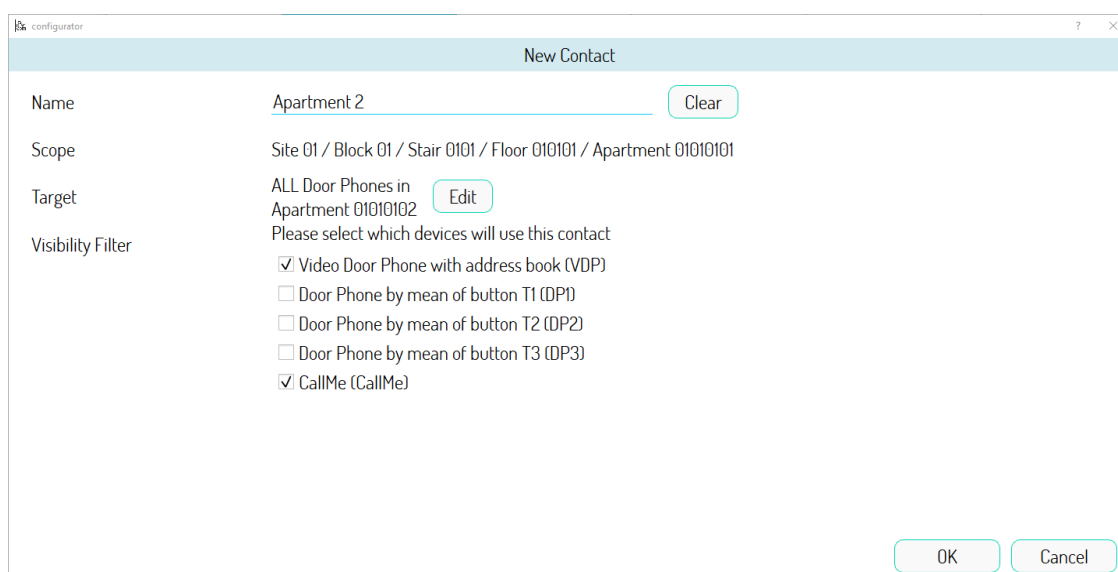


Figure 832: Checkbox "CallMe" selected

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

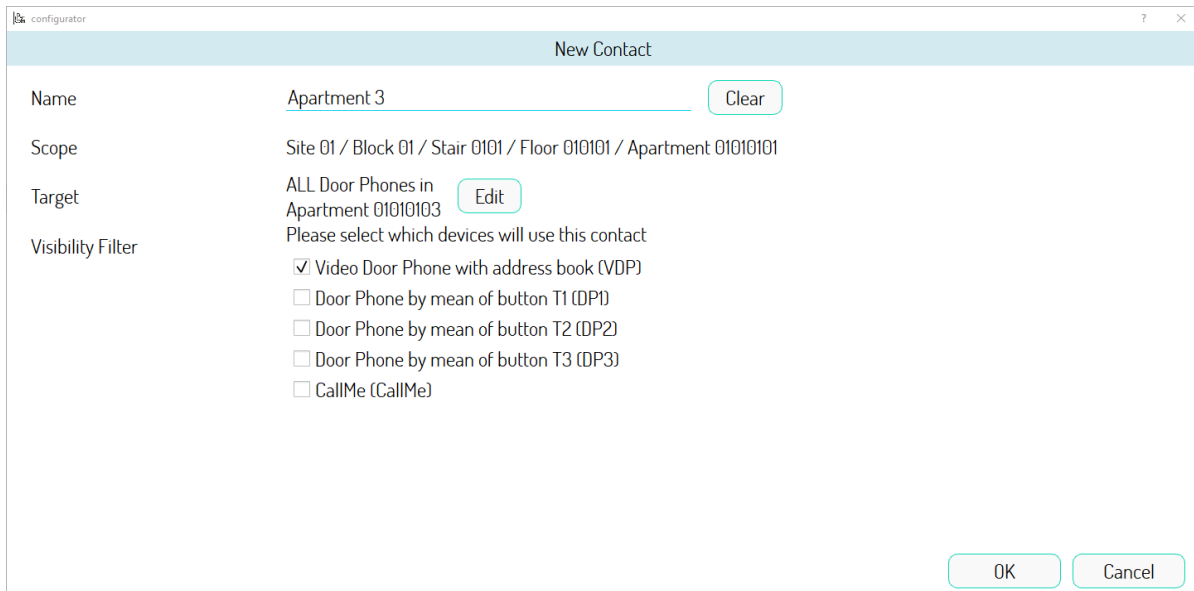


Figure 833: Checkbox "CallMe" not selected

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

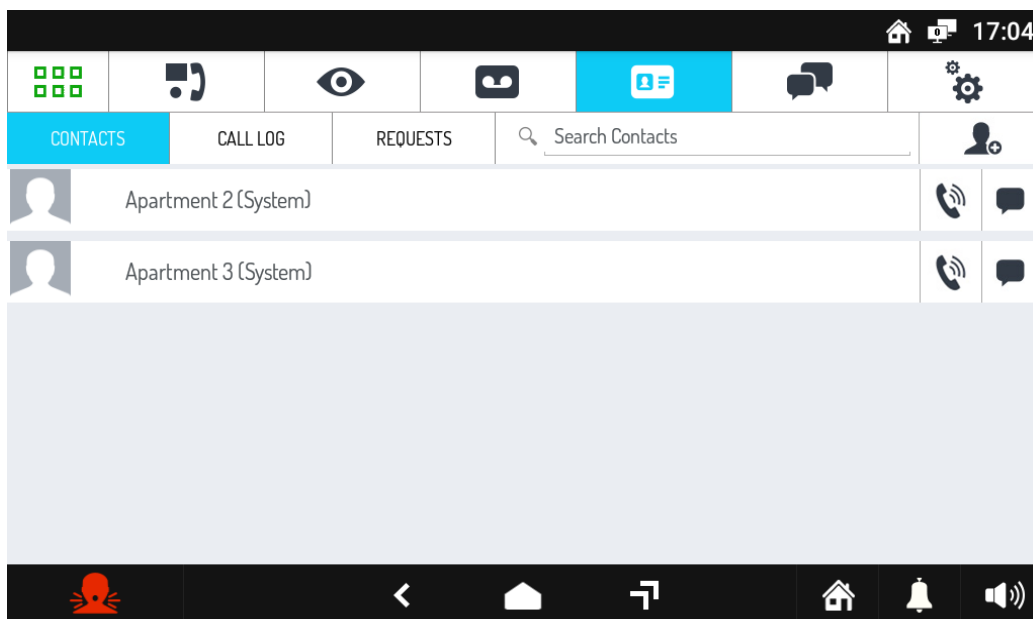


Figure 834: Contacts on video door phone

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

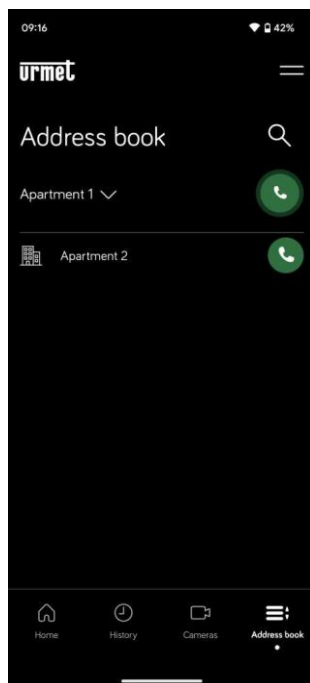


Figure 835: App CallMe contacts



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 T: Consumption in watts of IPerCom devices

A table is shown where next to each IPerCom device the relative consumption in Watts 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
1060/48	Modular Calling Station Alpha	12 (*)
1060/71-74-75-78	Modular Entry Panel Sinthesi S2	9,6 (*)
1060/21	Entry Panel Mikra	3,5
1060/22	Floor Entry Panel	3,5
1060/33-34	Entry Panel Mikra Plus/Digital	12 (*)
1761/31-32-33	7'' VOG <sup>7</sup> video door phone	12
1761/6	5'' VOG <sup>5</sup> video door phone	4,5
1761/15-16-18-19	Video door phone 5'' VOG <sup>5+</sup>	4,5
1717/31-32-33-34-41	7'' MAX video door phone	12
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 96: 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.

## APPENDIX U: Types of system/performance for which the presence of the 1060/1 Server is required

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 97: 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 *Modular Calling Station with 1060/48* or *Entry Panel 1060/33-34* or *Entry Panel 1060/21*,

or

- several IPerCloud apartments greater than 200,

or

- only *Entry Panels 1060/33-34* with several IPerCloud apartments greater than 32,

or

- 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 V: Device compatibility table

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	Code	Ver.	IPERCOM versions										3.0.0 oct-23	3.1.0 jul-24
			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		
			dec-18	dec-18	apr-19	sep-19	nov-19	dec-20	oct-21	apr-22	may-22	dec-22		
VDP IP 7"	1717/3x	A31S	V	V	V	V	V	V	X	X	X	X	X	X
VDP IP 7"	1717/4x	A31S	V	V	V	V	V	V	X	X	X	X	X	X
KEY READER	1060/82		V	V	V	V	V	V	V	V	V	X	X	X
CM ELEKTA	1060/1x		V	V	V	V	V	V	V	V	V	V	V	V
EP SYNTHESI	1060/7x		V	V	V	V	V	V	V	V	V	V	V	V
SWITCHBOARD	1060/41		V	V	V	V	V	V	V	V	V	V	V	V
VDP IP 7"	1717/3x	A64	V	V	V	V	V	V	V	V	V	V	V	V
VDP IP 7"	1717/4x	A64	V	V	V	V	V	V	V	V	V	V	V	V
RELAY ACTUATOR	1060/84	2.07	V	V	V	V	V	V	V	V	V	V	V	V
RTSP CAMERAS			V	V	V	V	V	V	V	V	V	V	V	V
DOOR PHONE	1160/3		X	V	V	V	V	V	V	V	V	V	V	V
CLOCK MODULE	1060/85		X	V	V	V	V	V	V	V	V	V	V	V
EP MIKRA2	1060/21		X	X	X	V	V	V	V	V	V	V	V	V
PRIVATE EP MIKRA2	1060/22		X	X	X	V	V	V	V	V	V	V	V	V
RELAY ACTUATOR	1060/84	3.04	X	X	X	V	V	V	V	V	V	V	V	V
GATEWAY IP-2VOICE	1083/59		X	X	X	V	V	V	V	V	V	V	V	V
SERVER	1060/1		X	X	X	X	X	V	V	V	V	V	V	V
EP ALPHA	1060/48		X	X	X	X	X	V	V	V	V	V	V	V
KEY READER	1060/86		X	X	X	X	X	V	V	V	V	V	V	V
RELAY ACTUATOR	1060/84	4.05	X	X	X	X	X	V	V	V	V	V	V	V
SERVER iPerTalk	1375/1x		X	X	X	X	X	V	V	V	V	V	V	V
CONTROL. IPASSAN			X	X	X	X	X	V	V	V	V	V	V	V
LIFT INTERFACE	1060/37		X	X	X	X	X	V	V	V	V	V	V	V
CM ELEKTA STEEL	1060/23		X	X	X	X	X	X	V	V	V	V	V	V
VDP 7" IP VOG7	1761/3x		X	X	X	X	X	X	V	V	V	V	V	V
VDP 5" VOG5	1761/6		X	X	X	X	X	X	V	V	V	V	V	V
VDP MAX 10"	1717/2x		X	X	X	X	X	X	V	V	V	V	V	V
VDP 7" BASIC	1741/1-2		X	X	X	X	X	X	V	V	V	V	V	V
VDP 7" BASIC	1741/3		X	X	X	X	X	X	X	X	X	X	V	V
IPERCOM CLIENT	1060/43		X	X	X	X	X	X	V	V	V	V	V	V
1060.WIN			X	X	X	X	X	X	X	V	V	V	V	V
EP MIKRA PLUS	1060/33		X	X	X	X	X	X	X	X	X	V	V	V
EP MIKRA DIGITAL	1060/34		X	X	X	X	X	X	X	X	X	V	V	V
VDP IP 5" VOG5+	1761/1x		X	X	X	X	X	X	X	X	X	V	V	V
SERVER iPerTalk	1375/1x	V1	X	X	X	X	X	X	X	X	X	V	V	V
VCT 7" IP VOG7	1761/3xU		X	X	X	X	X	X	X	X	X	X	X	V
VCT MAX 10"	1717/2xU		X	X	X	X	X	X	X	X	X	X	X	V
VCT IP 5" VOG5+	1761/1xU		X	X	X	X	X	X	X	X	X	X	X	V
Key reader	1060/45		X	X	X	X	X	X	X	X	X	X	X	V

*Table 98: Device compatibility with IPerCom versions*

## APPENDIX W1: *RTSP Cameras* supported by IPerCom video door phones

### **VOG<sup>5+</sup> 1761/15-16-17-18 e VOG<sup>5</sup> 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<sup>7</sup>, 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 W2: 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<sup>7</sup>, MAX and Basic* video door phones and *IPerCom Client* application (for the *Switchboard* application there is a dedicated item in the *Tools* menu).

## APPENDIX X: CallMe operating mode for VOG<sup>7</sup>, MAX 1717/3x and 1717/2x video door phones

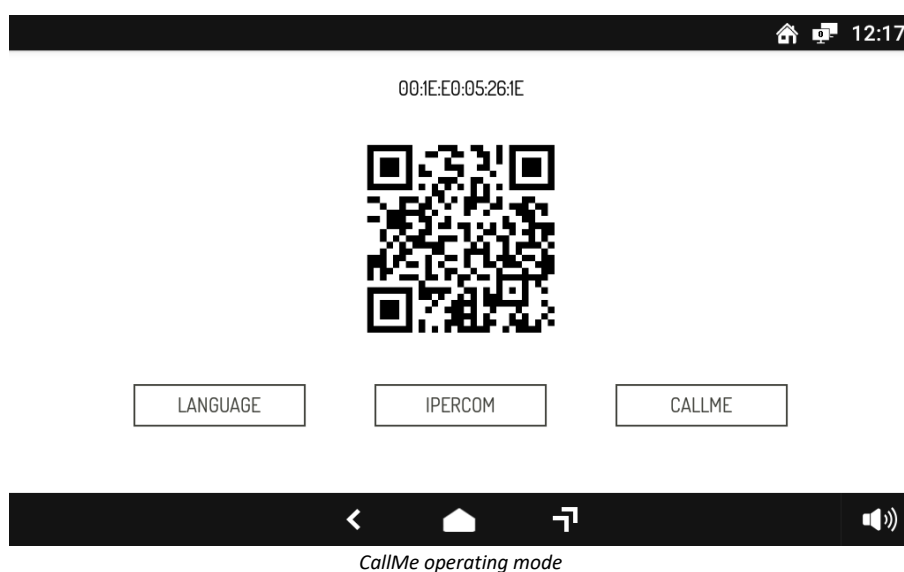
VOG<sup>7</sup> 1761/3x and MAX 1717/2x, 3x video door phones can work in *CallMe* mode.

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.

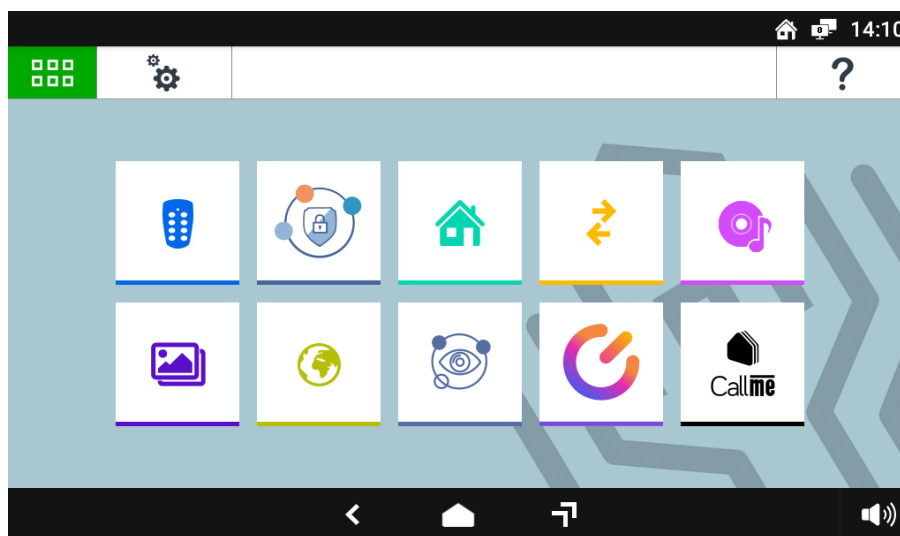
This new operating mode can be set when the video door phone is not configured and switched on. The screen that appears in this case is shown in the figure below:



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:



*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<sup>7</sup>* and *MAX* supports IPerCom and IPerCloud apartments.

The *VOG<sup>7</sup>* and *MAX* video door phones in *CallMe* mode do not have any video door phone function.





