







Guide to reading the manual

Welcome to the manual reading guide.

This section has been created to give you a clear and complete understanding of the contents of this manual.

By following these guidelines, you can maximise the effectiveness of your learning and user experience.

This manual can be read in two main ways:



1 – Full reading of all the chapters

If you want to know in depth every aspect of the system, we recommend the full reading of all the chapters.

This allows to explore each aspect in detail, for a complete and thorough understanding of the system.

You can start with the [interactive index](#), which gives a complete overview of all the topics, and read through the manual in the suggested order, or use the interactive links to go from one section to the next.



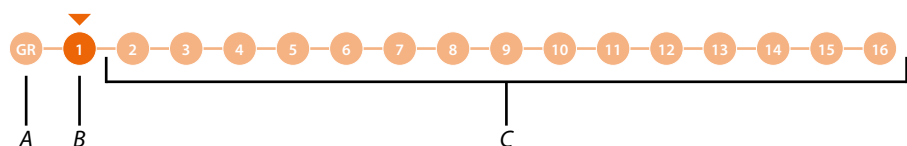
2 – Quick guide to first installation

If you are looking for quick and practical instructions on how to complete your first configuration, follow the “STEPS” in the [Quick Start Guide](#).

By following the step-by-step instructions (STEPS), you can learn the quickest procedure to complete an initial configuration of the system.

The pages of the manual that are part of a STEP contain graphic indications to help with navigation.

Navigation bar:



A. Back to the guide with the description of the steps

B. Current step

C. Next steps, click to navigate through the steps

At the end of each step, there is also a link to the next step:

[GO TO THE NEXT STEP](#) >>

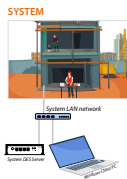
This method is very convenient to enable you to have a working system up and running in no time. However, we recommend that you learn more about the system by reading the entire manual. Although some paragraphs may initially seem less relevant, they may prove useful in the future. In addition, by reading the manual in its entirety, you may discover features you did not know existed and which could significantly improve your use of the system.

Contents

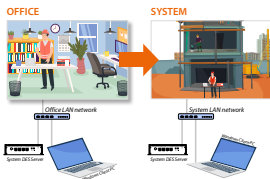
General information	7
Warnings and recommendations	7
Preliminary requirements	8
Network infrastructure adapted to the system	8
Warning for the LAN network	8
Private addresses	8
LAN band size	9
System router requirements	9
Assignment of IP address range based on the number of video door entry devices	10
Assigning a "privileged" network address to the SD	13
Band requirements for Internet connection	14
Fundamental concepts	14
Levels	14
Devices	14
Community	14
System	14
Call addressing procedures	16
Numeric call (using the standard address of the community)	16
Alphanumeric call (using alias)	17
4-DIGIT call	17
Lift function	17
Alphanumeric call (using alphanumeric alias)	18
Alphanumeric call (using contact alias in the address book)	18
Lift Control Function	18
Fire-fighting	18
OnVif IP cameras	18
Quick configuration guide	19
Authentication	21
Forgotten password	24
Home Page	25
Configuration page	26
Statistics page	27
Map page	28
Alarms	29
Edit password	30
Main menu	31
Device	32
Network and VLAN set-up	33
Server information	33
Manage the community networks	34
Device management	36
Creation of levels and devices	37
Device management	52
Send the configuration to the devices	59
Set the system call mode	60
Management of project data	66
Devices status	73
Parameter settings	74
Change the individual device parameters	75
Changing the default parameters of all devices of a certain type	78
Create a new template	81
Background picture replacement	92
Fire linkage	95
Lift control settings	96
Update devices	100
Gate code and installer passwords	105

Cloud	107
First access	108
Manage your account	115
Create a Plant	125
Manage the Plant	127
Import a Plant	135
Community	137
Users profile management	138
<i>Add a person</i>	143
Cards and badges configuration	160
<i>Add badge/card</i>	161
<i>Identify badge/card</i>	162
<i>Delete badge/card</i>	164
<i>Disable badge/card</i>	167
<i>Key sector management</i>	168
Resident user codes	170
Messages	171
<i>Manage the messages</i>	172
History	179
Alarm history	180
Access history	183
Patrol history	184
Call history	185
System	186
Role management	187
Account profile management	191
Map configuration	196
Account operation log	198
System data backup	199
System data recovery	201
<i>Export backup</i>	202
<i>Import backup</i>	203
Server version information	204
Server upgrade	205
Advanced	207
System parameter configuration	208
Device catalogue	212
Device offline log	214
Access control user details	215
Access version debug	216
Diagnostics	219
Factory reset	220

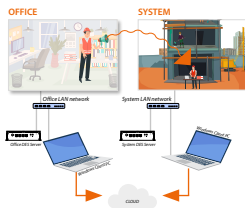
Examples of system situations	221
-------------------------------	-----



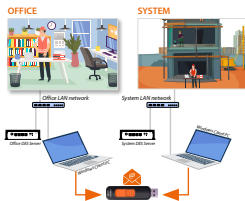
Configuration of the server and IP DES system at the construction site	223
--	-----



Pre-configuration of the server at the office and on-site system configuration	260
--	-----



Project creation at the office and on-site server and system configuration	300
--	-----



Appendix	346
----------	-----

General information

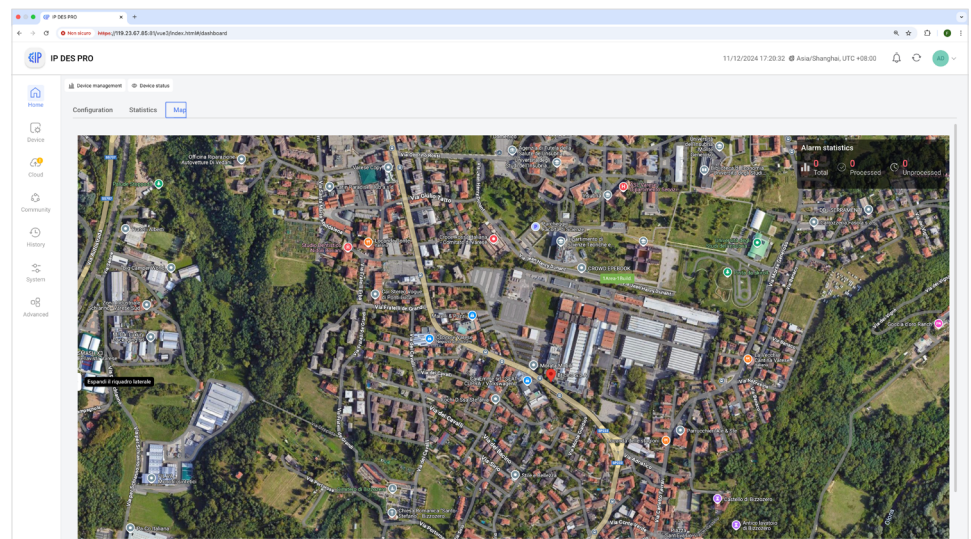
The IP DES SYSTEM allows to manage very wide infrastructures with a high number of apartments. After creating the community and populating it with the devices, with SW it is possible to manage the network settings, the profiles of the people who live in the community and the various people who administer it.

The profile setting will allow to manage the accesses to the different types of gates, according to the profile set.

We suggest to save the Community in the Cloud after creating an Installer account; this allows you to ensure greater security in backing up your data as well as associating the Home+Security app to the IU for remote management of the video door entry system.

It is also possible to:

- display the device status and change the configuration
- send different types of messages to the community (alarm, information and advertising messages)
- monitor accesses, calls, alarms coming from IU.



Acronyms

In this manual, for easy reading, the abbreviated device and function name is used as in the list:

- IU: Internal Unit
- EP: Entrance Panel
- GS: Guard station
- SD: Server DES
- VEPO: Video entrance panel outside the door
- AB: Configuration
- SW: IP DES System configuration software

Warnings and recommendations

It is important to read this manual carefully before proceeding with the installation. The warranty becomes automatically void in case of negligence, improper use, tampering by unauthorised personnel.

CAUTION: The images of this manual are only indicative and therefore may not exactly represent the characteristics of the product.

Preliminary requirements

- Network infrastructure adapted to the system
 - Warning for the LAN network
 - LAN band size
 - Band requirements for Internet connection
 - System router requirements
 - Assignment of IP address range based on the number of video door entry devices
 - Assigning a “privileged” network address to the SD
- DHCP server installed and active on the network
- SD item no. 375001 installed on the same network as the DHCP server and the IP DES system devices
- PC to be used as Client PC (only Windows operating system), as network mask with SD and with BTicinoWare software installed (available for download from www.homesystems-legrandgroup.com)

Network infrastructure adapted to the system

Warning for the LAN network

The IP DES system uses multicast communication to connect system components locally with a single VLAN.

For correct operation proceed as follows:

- Connect all the devices, the SD and the Windows Client PC used to configure/maintain the system to the same LAN.
- Avoid using wireless bridges to connect network segments
- Do not use a virtual VPN to connect different parts of the network.
- The system configured by the DES Server must belong to a network with private addresses
- To avoid malfunctions when connecting the SD to the cloud, ensure that multicast is enabled. The name may change depending on the router manufacturer (e.g. “enable multicast” or “igmp snooping”).

CAUTION: With the DES Server connected, it is recommended to test multicast operation in the local network using the Windows prompt command: “ping siteserver.local”.

Private addresses

The system configured by the DES server must belong to a network with private addresses.

Supported address classes						
RFC 1918 name	IP address range	Number of addresses	Largest CIDR block (subnet mask)	Host ID size	Mask bits	Classful description
16-bit block	192.168.0.0 – 192.168.255.255	65536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks
24-bit block	10.0.0.0 – 10.255.255.255	16777216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
Unsupported address classes						
20-bit block	172.16.0.0 – 172.31.255.255	1048576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks

LAN band size

Size each network segment and LAN switch according to the number of possible simultaneous audio/video connections:

- At least 2.5 Mbit/sec for calls using one-way video and two-way audio (e.g. EP to IU call)
- At least 5 Mbit/sec for calls using two-way video and audio (e.g. intercom between IU with integrated camera)

For example: with an upload speed of 25Mbit/sec, the system can handle up to 10 simultaneous calls from entrance panels to the Home + Security app without audio / video signal deterioration. The following formula can be used to determine the bandwidth:

minimum bandwidth value * number of Entrance Panels * probability of simultaneous calls = Total Upload Bandwidth

2.5/5 Mbit/sec * 10 * 1 = 25/50 Mbit/sec

System router requirements

The system requires a router or a switch managed using a DHCP server with the following characteristics:

- Possibility of dividing the IP address range (subnet mask) into two sets: A – managed by the DHCP Server (dynamic and temporary)
Example: DHCP server managed addresses from 192.168.1.0 to 192.168.1.199 B - free and available for use by the SD
Example: SD managed addresses from 192.168.1.200 to 192.168.1.250
- Possibility of fixing the IP address of the SD within the range managed by the DHCP server. This is necessary because the IP address of the SD must remain fixed within the DHCP range. Some routers may call fixed addresses “reserved addresses” or “static leases”.
- The router and firewall must not block:
 - endpoint: *.netatmo.com e *.netatmo.net, eliotCloudUAMPRD.onmicrosoft.com, *.legrand.com, *eliotbylegrand.com.

For webRTC TURN/STUN: the endpoints are indicated here and depend on the geographical region: <https://www.twilio.com/docs/stun-turn/regions>

 - fixed doors: https/wss: 443 (tcp,udp), netcom: 25050 (tcp) Per TURN: 3478 (tcp,udp), TURN TLS: 443, 5349 (tcp)
 - dynamic ports form multimedia flow and multimedia flow control.

This is the result of the SDP webRTC handshake: not known beforehand.

All unknown ports (non-system ports), above 1024, and incoming/outgoing ports, should remain open, at least in UDP

 - mDNS e multicast, in particular: 239.106.106.255, door 10007 (udp) 224.0.0.251 (or address IPv6 ff02::fb), door 5353 (udp)

Assignment of IP address range based on the number of video door entry devices

Before proceeding with the configuration of the next steps, it is necessary to know the total number of devices in the community, including not only IU,EP,SEP,GS but also OnVif cameras, and to request from the network administrator a range of addresses dedicated to our video door entry system.

The address range should be equal to the number of devices in the video door entry system.

The video door entry system devices will, in the beginning (1st switch on), take an address assigned by the router. Later on (after establishing communication with the SD, which will be in the same network) they will be assigned a FIXED IP address by the SD.

This entails the following requirements:

- the number of IP addresses available in the DHCP service of the router must be equal to the number of devices of the video door entry system.
- the management of the DHCP service of the system router and of the addresses to be managed by the SD must be correctly defined in collaboration with the network administrator, so that the addresses do not overlap.

The two address ranges must be separated by configuring the network parameters of the DHCP service and the SD (see [examples](#)).

Once configured, the SD assigns its own IP address range (VLAN) to IP DES devices, changing the initial IP address assigned by the network's DHCP.

In the case of installation in an existing and shared network, it must be ensured that:

- the network's DHCP server can assign an IP address to each IP DES device (initial IP address)
- the existing network has a number of addresses outside the DHCP allocation available for SD address management (Server address range)

The network parameters must be compatible with the DHCP server settings. The addresses starting from this value will be assigned by the software, therefore they must not be managed by the DHCP server on the LAN.

For example:

DHCP server address management 192.168.1.1 up to 192.168.1.199

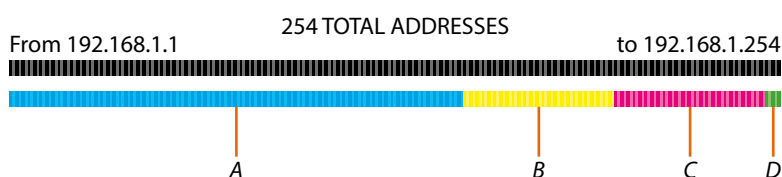
Software server address management 192.168.1.200 up to 192.168.1.250

Example 1 (working case):

- Number of generic addresses already occupied in the system:150
- Total number of devices (IU;EP;SEP;GS; OnVif cameras): 50
- indirizzi disponibili sulla rete da 192.168.1.1 a 192.168.1.254 : 254 con subnet mask: 255.255.255.0

we will apply the following separation:

- router DHCP service management for addresses from 192.168.1.1 to 192.168.1.200 (200 addresses available for generic devices and video door entry system devices "1st switch on")
- SD DHCP service management for addresses from 192.168.1.201 to 192.168.1.254 (54 addresses available for video door system system devices)
- The request of 50 addresses by the SD is met by the 54 addresses available



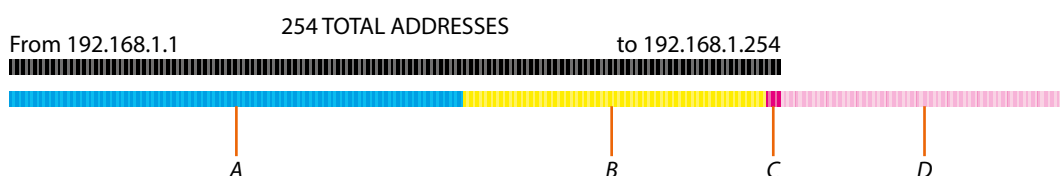
- A. 150 addresses already occupied in the network
- B. 50 addresses assigned by the router automatically during the 1st switching on
- C. 50 DES Server assigned addresses
- D. 4 free addresses

Example 2 (critical case):

- Number of generic addresses already occupied in the system:150
- Total number of devices (IU;EP;SEP;GS; OnVif cameras): 100
- addresses available on the network from 192.168.1.1 a 192.168.1.254 : 254 with subnet mask: 255.255.255.0

Assuming we have a range of available addresses from 192.168.1.1 to 192.168.1.254, we will divide them as follows:

- router DHCP service management for addresses from 192.168.1.1 to 192.168.1.250 (250 addresses available for generic devices and video door entry system devices "1st switch on")
- SD DHCP service management for addresses from 192.168.1.251 to 192.168.1.254 (4 addresses available for video door entry system devices)
- The request of 100 addresses by the SD is NOT met by the 4 addresses available



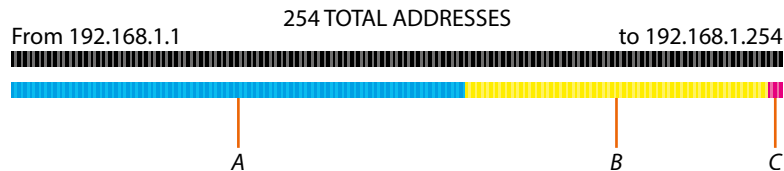
- A. 150 addresses already occupied by the system
- B. 100 addresses assigned by the router automatically during the 1st switching on
- C. 4 DES Server assigned addresses
- D. 96 addresses to assign

Solution for example 2 (critical case):

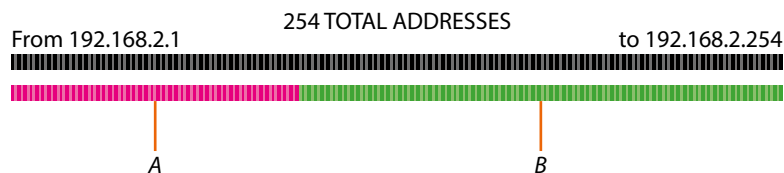
- Number of generic addresses already occupied in the system: 150
- Total number of devices (IU;EP;SEP;GS; OnVif cameras): 100
- addresses available on the network from 192.168.1.1 a 192.168.1.254 + 192.168.2.1 a 192.168.2.254 : 508 with subnet mask: 255.255.254.0

In this case, the network administrator must confirm address availability bearing in mind the "first switch" process of video door entry system devices: available addresses from 192.168.1.1 to 192.168.2.254; we will divide as follows:

- router DHCP service management for addresses from 192.168.1.1 to 192.168.1.250 (250 addresses available for generic devices and video door entry system devices "1st switch on")
- SD DHCP service management for addresses from 192.168.1.251 to 192.168.1.254 (4 addresses available for video door entry system devices)
- +
SD DHCP service management for addresses from 192.168.2.1 to 192.168.2.254 (254 addresses available for video door entry system devices)
- The request of 100 addresses by the SD is met by the 4+254 addresses available



- A. 150 addresses already occupied by the system
- B. 100 addresses assigned by the router automatically during the 1st switching on
- C. 4 DES Server assigned addresses



- A. 95 DES Server assigned addresses
- B. 159 free addresses

Assigning a “privileged” network address to the SD

The SD receives the IP address from the DHCP server installed in the network.

In order to guarantee correct system operation, the SD must maintain its IP address even if the system is restarted.

To be able to guarantee this in a system with a DHCP server, it is necessary to set up a “privileged” assignment (each manufacturer uses its own definition, e.g. fixed, reserved) of the IP address to a specific MAC address on the same DHCP server.

Mac address identification in case of server configuration directly on the system

In this case, you can find the Mac address on the [Network and VLAN set-up](#) page

Mac address identification in case of server pre-configuration at the office

In this case, you can find the Mac address on the label on the server

NOTE: *If the Mac address cannot be found, see [Mac address finder via IP Scanner in case of missing or unreadable label on the server](#) or [Mac address finder via ping command in case of missing or unreadable label on the server](#)*

Band requirements for Internet connection

The system uses the internet connection to perform the backup and maintenance tasks via the cloud and to use the Home + Security app functions. For this reason, the internet connection must have the following characteristics:

- Upload speed of at least 5Mbit/sec for correctly forwarding audio-video calls to Home + Security
- A fast line (VDSL2) in case of a limited number of EP simultaneously connected to Home + Security in audio/video mode
- A fibre optic line in case of an unlimited number of EP simultaneously connected to Home + Security in audio/video mode

for more details see "[LAN band size](#)"

Fundamental concepts

This section explains concepts that will arise in the explanations throughout this manual.

Levels

This term refers to the various levels that make up the community structure: Area, Building, Riser, Floor, Apartment.

Devices

This term refers to the various devices that populate the community structure: UI/EP/GS/VEPO.

Community

The IP system is designed for the management of installations of medium to large, or even extremely large, sizes.

For this reason, every installation, even a simple apartment, is always included in what is called Community.

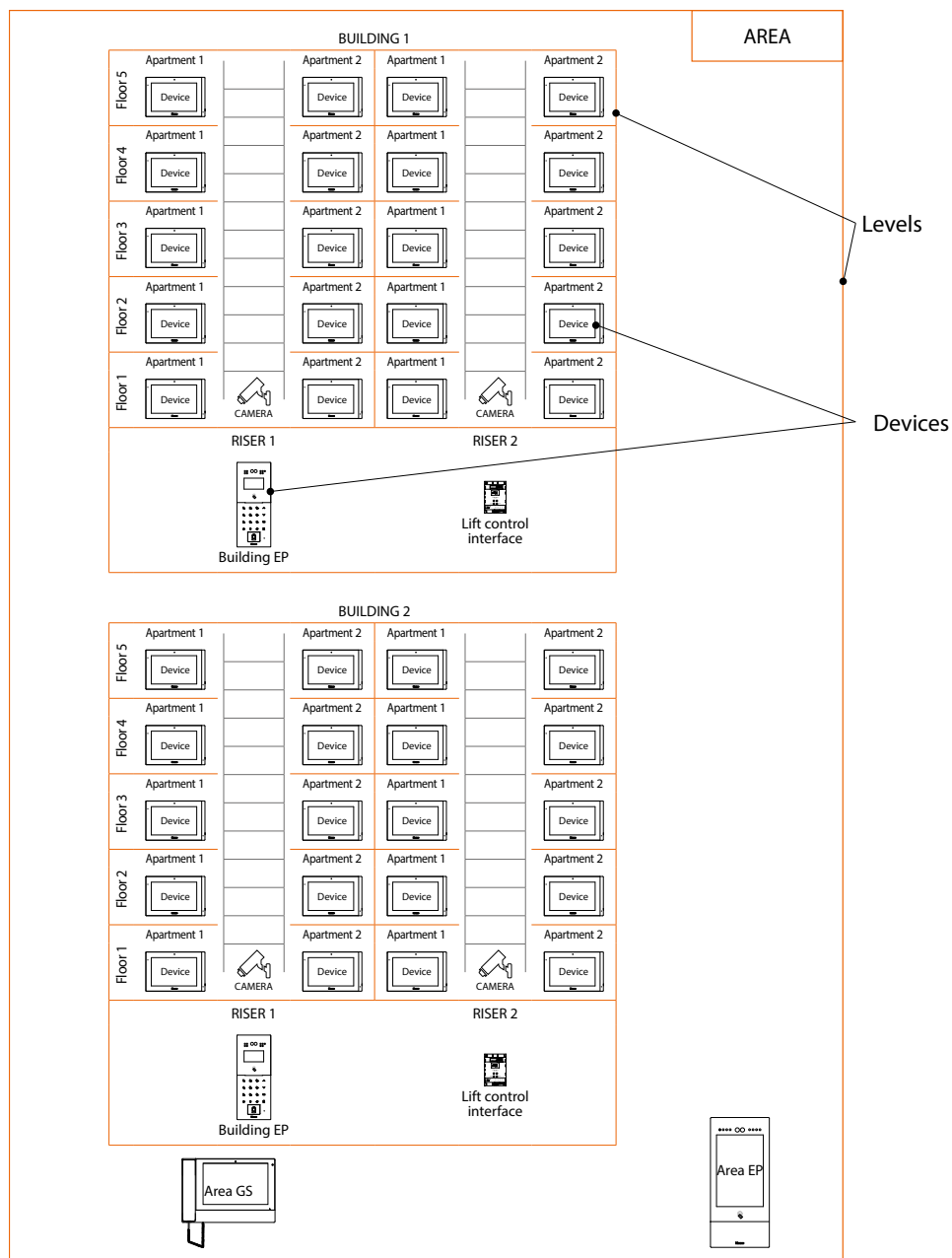
Think of a Community as a City split into neighbourhoods (Areas) consisting of Buildings, which are in turn split into Riser, Floor and Apartment.

Each of these levels can then be populated by several devices, such as UI, EP, VEPO e GS. The Community can be saved on the cloud. (strongly recommended).

System

Saving of the configuration and other data on the cloud

Example of the structure of a community



Call addressing procedures

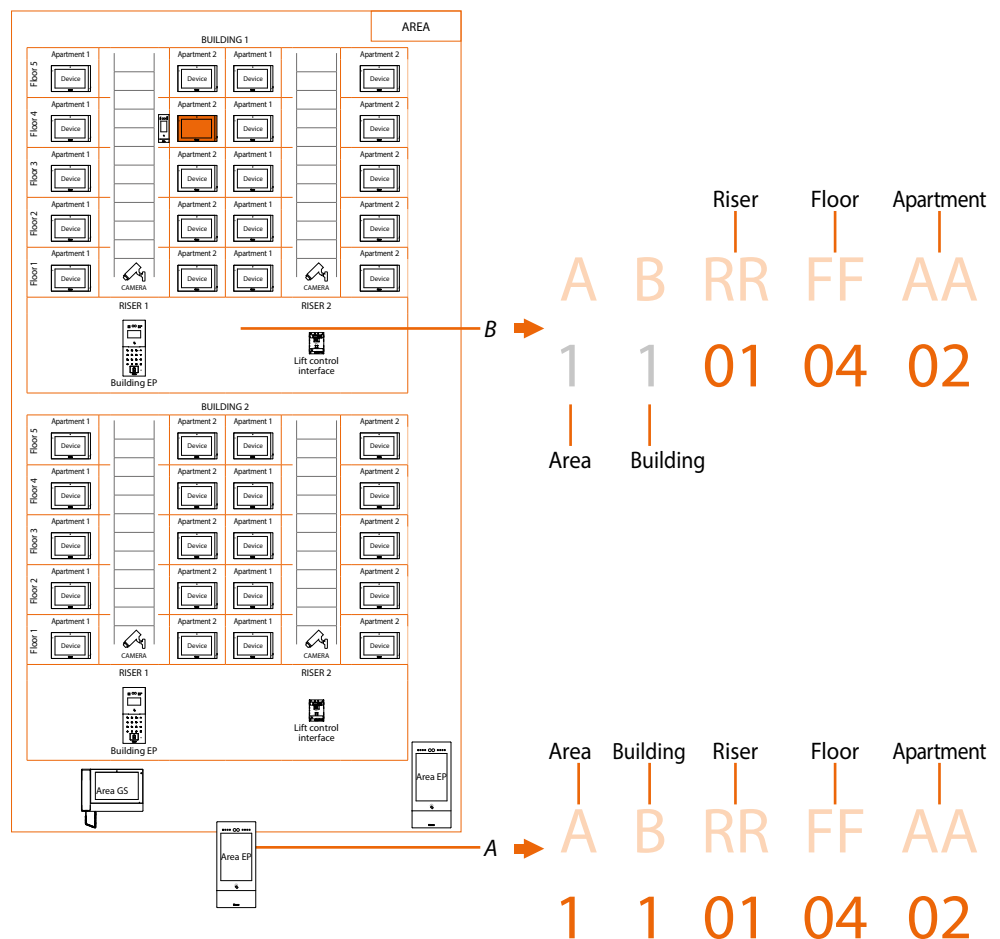
On the basis of data recorded in the configuration and the Community structure the calls can be made using various methods:

- **numeric call (using the standard address of the community);**
- **alphanumeric call (using Alias);**
- **4-DIGIT call;**

Numeric call (using the standard address of the community)

To make this type of call you must know the address of the person being called, which depends on the community structure, for example:

- to call the IU highlighted in the diagram from the EP A, enter the corresponding address **11010402**;
- to call the IU highlighted in the diagram from the EP B, enter the corresponding address **010402**, as the IU is positioned inside Building 1 and therefore it is sufficient to type the Riser, Floor and Apartment number.



NOTE: during the configuration phase, the number of digits to be used for each call sector (Area/ Building/Riser/Floor/Apartment) must be set.

Example: I have to call an apartment inside Building 2

- if there are from 1 to 9 Buildings in the area, I must enter 2 (one digit used for the Building call sector);
- if there are more than 10 Buildings in the area, I must enter 02 (two digits used for the Building call sector);

The system will automatically show the correct number of digits to type and which data to enter on the basis of the EP position you are calling from, for example Area (2 01 06 02) or Building (01 06 02)

System configuration (default)

Areas 9, Buildings 99, Risers 99, Floors 99, Apartments 99

It is possible to modify the limits using SW.

Alphanumeric call (using alias)

The Alias is an alphanumeric code that replaces the community address created through the software.

The default alias is the same as the address in the Community*. However, this can be changed using the SW and can be of two types:



Call using alphanumeric alias

The alphanumeric alias can be used on all entrance panels, internal units and guard stations. To make the call, enter the full alphanumeric alias in the device call menu --> B12

Call using contact alias in the address book

The address book contact alias can be used on all internal units and guard stations, but only on entrance panels with touch display.

To make the call, use the appropriate address book button (icon) in the call menu of the device and select the desired contact (JOHN SMITH), or enter the contact alias using the auto-complete function - -> JOHN SMITH

4-DIGIT call

To make this type of call, you need to know the specific 4-digit code of each apartment.



Lift function

The Lift Control function consists of the ability to interact with the lift system through calls and commands from the DES IP video door entry system.

The operating mode of the lift depends on its control system (BTicino cannot operate the lift but only send commands, which are interpreted and executed).

Safety must be guaranteed by an access control system or by the lift itself.

The lift control function can be realised in two modes:

- The first is through protocol commands on RS485.
Using the interface 375010, the IP DES video door entry system sends commands to the lift control centre to simulate a lift call.
For more information, see the "Lift Interface Software Manual, item. 375010"
- The second mode is through dry contact commands.
The DES IP video door entry system opens and/or closes contacts (output contacts from interface 375013). Lift calls are simulated when these contacts (correctly connected to the lift system) are opened or closed.
Interface 375013 must be added as a device in the Community. After this, it will be necessary to configure the parameters in the [Lift Control function](#) page

You can see some examples of connection diagrams in the manuals of the IP devices.

What discussed in the previous sections is not applicable to all devices. Below is a list showing their applicability.

	Alphanumeric call (using alphanumeric alias)	Alphanumeric call (using contact alias in the address book)	Lift Control Function	Fire-fighting	OnVif IP cameras
373001	✓	✓	✓*	✗	✓
373002	✓	✓	✓*	✗	✓
373003	✓	✓	✓*	✗	✓
373004	✓	✓	✓*	✗	✓
373005	✓	✓	✓*	✗	✓
373006	✓	✓	✓*	✗	✓
373007	✓	✓	✓*	✗	✓
373008	✓	✓	✓*	✗	✓
374000	✓	✓	✓	✓	✗
374001	✓**	✗	✓	✓	✗
374002	✓	✓	✓	✓	✗
374003	✓**	✗	✓	✓	✗
374004	✗	✗	✓***	✓	✗
374005	✓	✓	✓****	✓	✗
374006	✗	✗	✓***	✓	✗
375000	✓	✓	✗	✗	✓

*NOTE: function only valid with lift interface 375010

**NOTE: function only available with numbers and letters between 0-9 and A-I

***NOTE: function only valid with contact interface 375013

****NOTE: function only valid with contact interface 375013 or with interface 375011, but only in SLAVE mode

Quick configuration guide

The following procedure describes the minimum steps for an initial configuration of the system.

In order to program an IP DES system correctly, preliminary steps must be taken:

- [Check your system requirements](#)
- [Authenticate](#)

After this, the basic steps to be performed are:

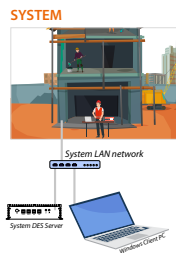
-
- | | | |
|------|---|---|
| Step | 1 | Create the community VLAN network |
|------|---|---|
-
- | | | |
|------|---|--|
| Step | 2 | Set the system call mode |
|------|---|--|
-
- | | | |
|------|---|--|
| Step | 3 | Create a new structure |
|------|---|--|
-
- | | | |
|------|---|---|
| Step | 4 | Create the template (Configuration of parameters) |
|------|---|---|
-
- | | | |
|------|---|---|
| Step | 5 | Register the MAC addresses of the devices |
|------|---|---|
-
- | | | |
|------|---|---|
| Step | 6 | Copy of the Community on the Legrand Commercial Cloud |
|------|---|---|
-
- | | | |
|------|---|---|
| Step | 7 | Send the configuration to the devices |
|------|---|---|
-
- | | | |
|------|---|---|
| Step | 8 | Gate code and installer passwords |
|------|---|---|
-
- | | | |
|------|---|--------------------------------|
| Step | 9 | Update devices |
|------|---|--------------------------------|
-
- | | | |
|------|----|--|
| Step | 10 | Account profile management |
|------|----|--|
-
- | | | |
|------|----|--|
| Step | 11 | Users profile management |
|------|----|--|
-
- | | | |
|------|----|--|
| Step | 12 | Cards and badges configuration |
|------|----|--|
-

Finally, install the devices, activate and update them (see [Examples of system situations](#))

After installing and activating the devices, the SW can be used to:

- **Manage the** Community **people** and **accesses** (badge/card/face and fingerprint)
- Display various types of information relating to messages, alarms, community calls and device status
- Display and manage various SW functions
- **Update the** device **firmware**

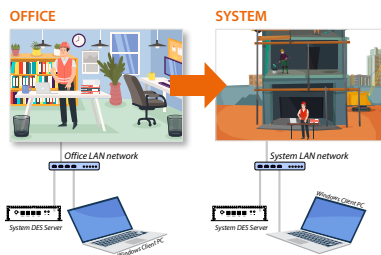
Installation examples



Configuration of the server and IP DES system at the construction site

The system already includes a wired and functioning LAN network. The installer can therefore go on site to complete the configuration using a Windows Client PC connected to the same LAN network as the system SD.

[View all the steps required for the example](#)

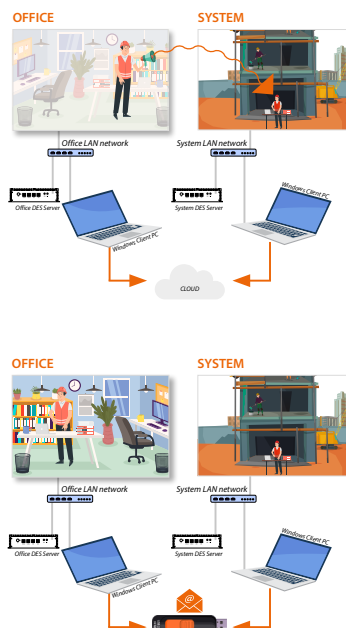


Pre-configuration of the server at the office and on-site system configuration

It is preferred to pre-configure the system SD in advance at the office, connecting it to a Windows Client PC of the office LAN network.

The SD can then be moved to the system and connected to the LAN network of the same.

[View all the steps required for the example](#)



Project creation at the office and on-site server and system configuration

As the system SD is installed in a system far away and is therefore not available, the configuration will have to be carried out on a “test” SD connected to the office LAN.

The configuration can then be sent to the system SD in two ways:

- save the configuration to the cloud and then synchronise.
- download the configuration locally and then send it to the system.

[View all the steps required for the example](#)

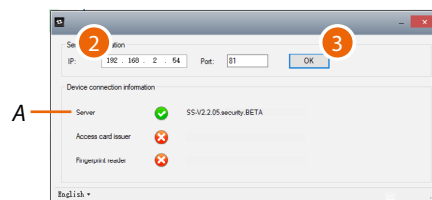
Authentication

To use the SW to configure and manage the BTicino IP DES system, follow the procedure shown below:



1. Run the BTicinoWare software (only for Windows Client PCs) previously installed. The BTicinoWare software is required to:
 - register the badge/card using a badge/card programmer (item 375003)
 - register the fingerprints using a fingerprint reader (item 375004)
 - print labels during the configuration phase.

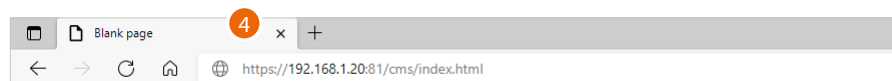
The following screen appears:



2. Enter the **SD address** and check that the port is 81

In order to guarantee correct system operation, the SD (which will take an address assigned by the system router) must maintain its IP address even if the system is restarted. To be able to guarantee this, it is necessary to set up on the system router a “privileged” assignment (each manufacturer uses its own definition: fixed, reserved) of the IP address to a specific MAC address, see [Appendix](#).

3. Press to confirm and check that the flag A is green

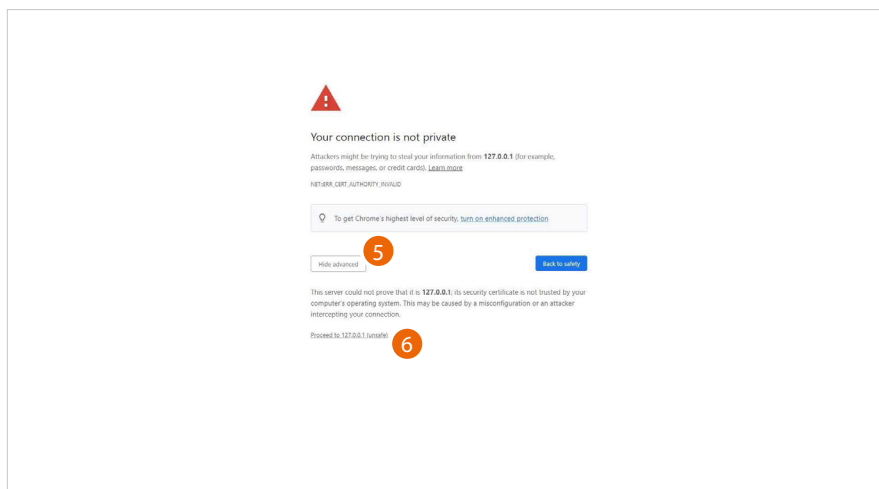


4. Open the browser and enter the http address of the SD:

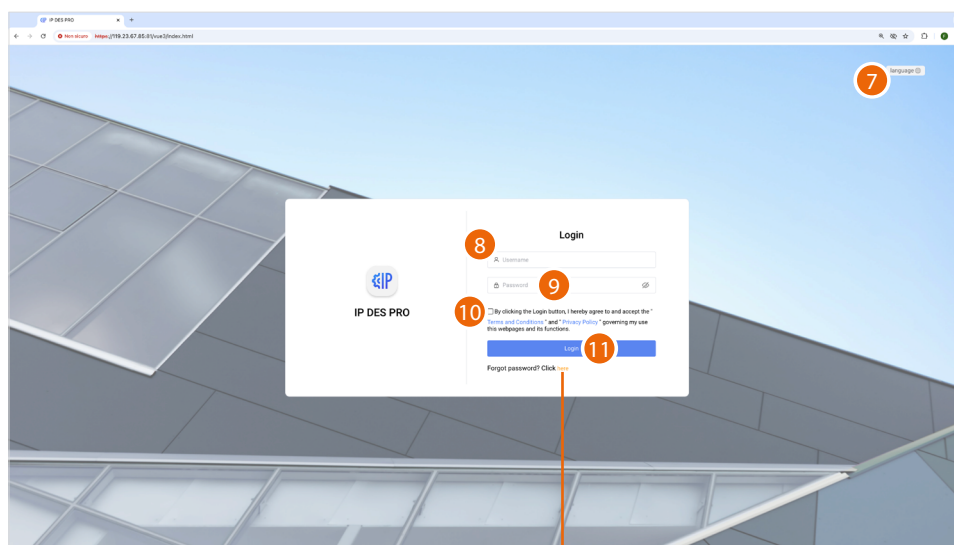
https://IP or siteserver.local:81

NOTE: use Chrome/Edge browser and a screen with resolution 1920x1080

In some cases, the browser may consider the page to be unsafe.

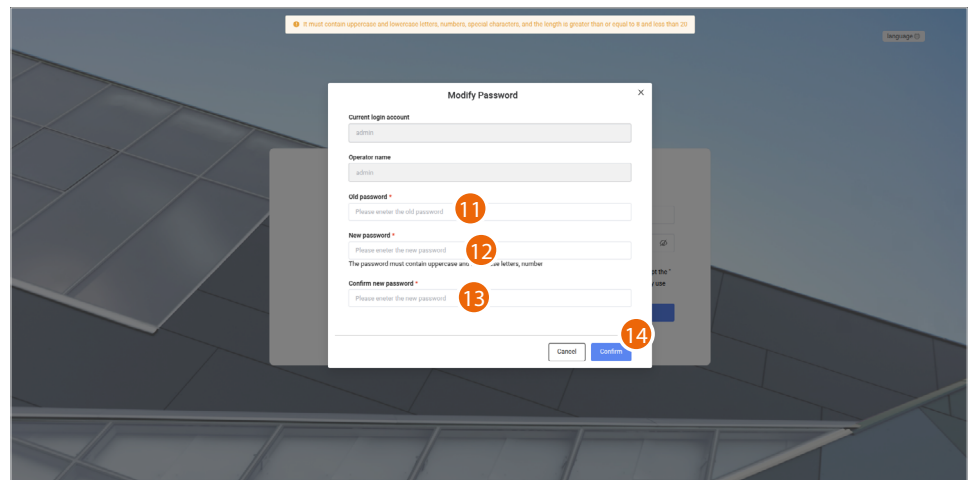


5. Click to display the advanced options
6. Click to ignore the warning and proceed



A

- A Activate the **password recovery** procedure
7. Select the interface language.
 8. Enter the login name (default admin)
 9. Enter the password (default 123456)
 10. Accept the "Terms and Conditions" and the "Privacy Policy" that apply to your use of this website and its functions.
 11. Click to confirm



For security reasons, it is mandatory to change the default password; the new password must have the following characteristics:

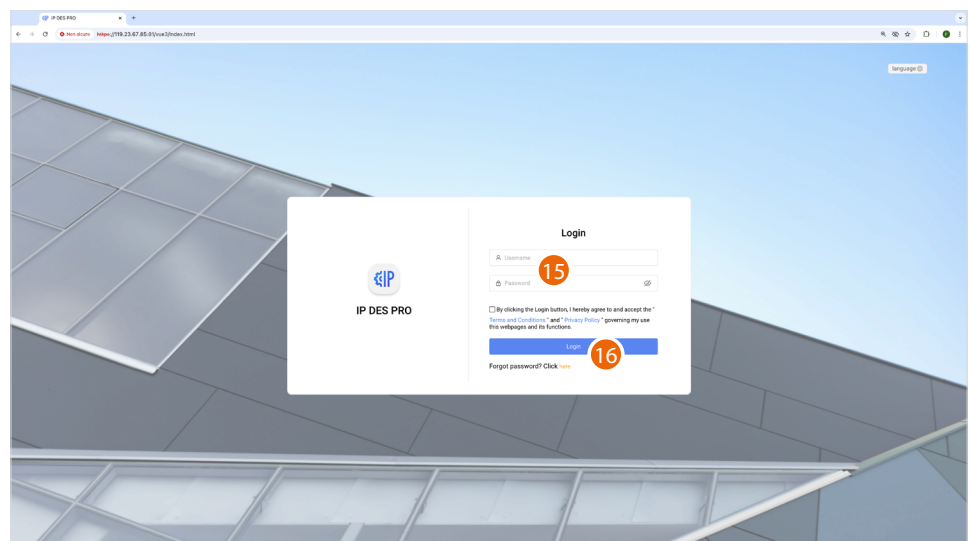
- Number of characters between 5 and 20
- Must contain at least one number, one special character and one upper case letter

11. Enter the default password

12. Enter the new password

13. Repeat the new password

14. Click to confirm



15. Enter the new data

16. Click to confirm

To change the password, go to the **Modify password** section

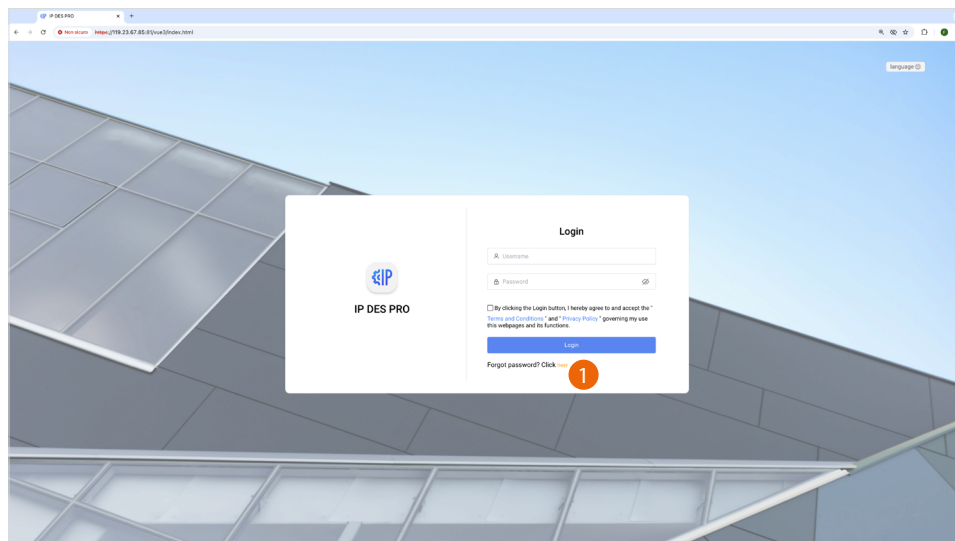
NOTE: the above procedure is completed using the admin profile, which allows full system management.

Other profiles can be created for different roles in the **Role Management** and **Operator Management** pages

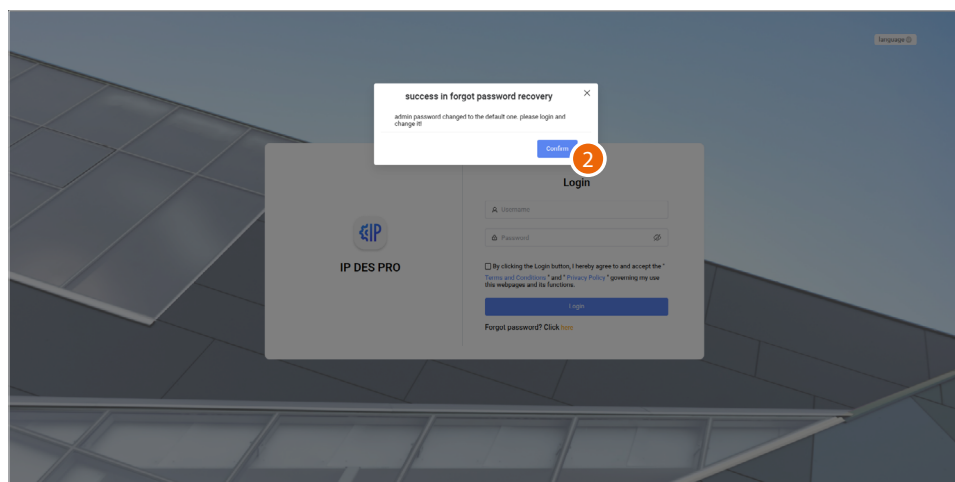
Forgotten password

If you forget your password, you can reset it via the “admin reset password” function on the DES Server label.

If it is not possible to reset the password through the DES Server label:



1. Click to activate the password recovery procedure



2. The password was reset.
The password to be used for authentication is now the default password.

Home Page

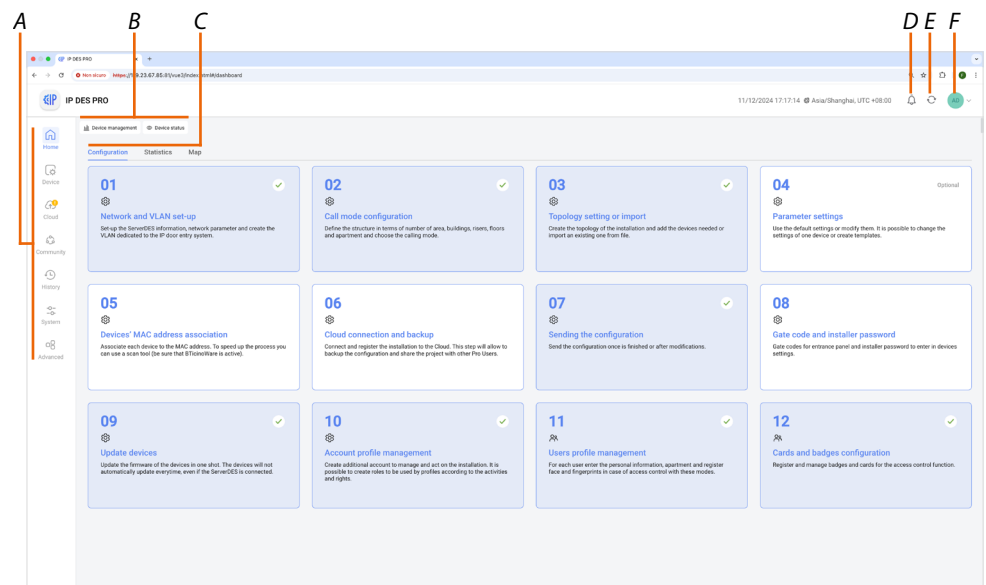
The Home Page contains some tools (menus and buttons) for configuring and managing community levels and devices.

In particular, there is a [main menu](#) for managing devices and programming profiles and accesses to the community, and an information section for recording events, messages and alarms recorded in the community.

There is also a section for [cloud](#) management.

There are also 3 additional pages on the home page:

- the [configuration page](#)
- the [statistics page](#)
- the [maps page](#)



A Main menu

B In this section, when a tab is opened (either from the dashboard or the main menu), the chronology is maintained.

To delete the tab from the chronology, simply press 'X'.

C [Configuration](#), [statistics](#) and [maps](#) pages

D Alarm notifications

E Notifications

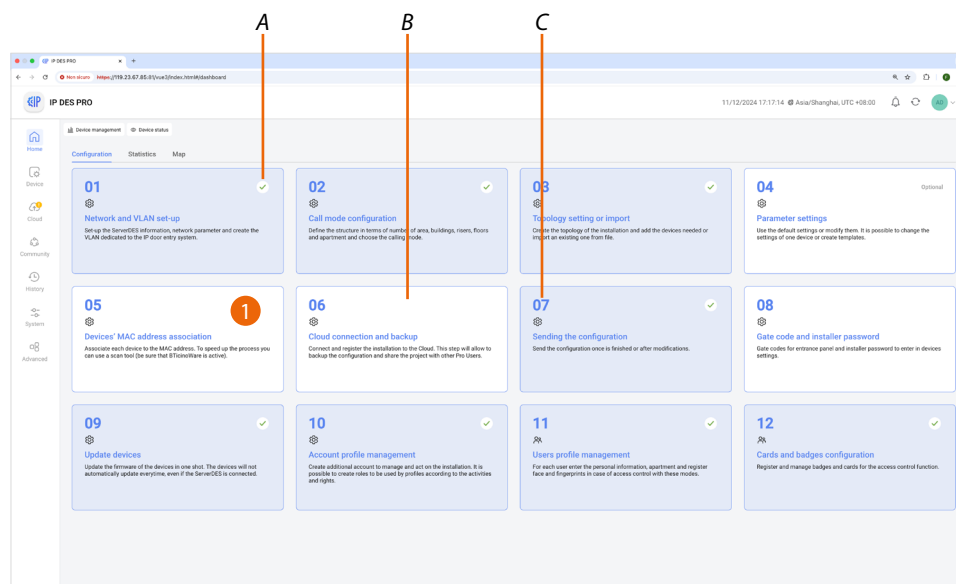
F Opens the logout menu and [Modify password](#)

Configuration page

This dashboard has been designed as a guide for the installer, the order of the tabs suggests a process for the correct and complete configuration of a project.

When a tab is closed, it is possible to return to the home page and go to the next tab.

Tabs do not block the process, it is possible to access all the other sections of the menu at any time



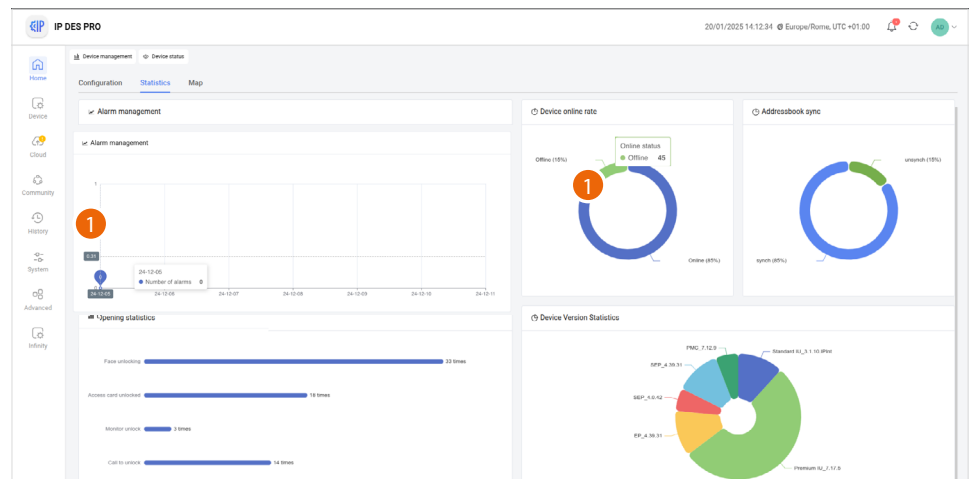
- A The light blue background and tick symbol indicate that the tab has been completed successfully
 - B The white background indicates that the tab has not yet been completed
 - C The 'Sending the configuration' tab does not open any pages but allows to directly send the configuration.
1. Click to enter the configuration page

Statistics page

This page shows statistical data regarding devices, accesses and alarms.



- A Displays how many alarms have occurred and in which dates*
- B Displays the percentage quantity of on/offline devices*
- C Displays the percentage quantity of community devices*
- D Displays the type and number of accesses*
- E Displays the percentage quantity of accesses opening types*

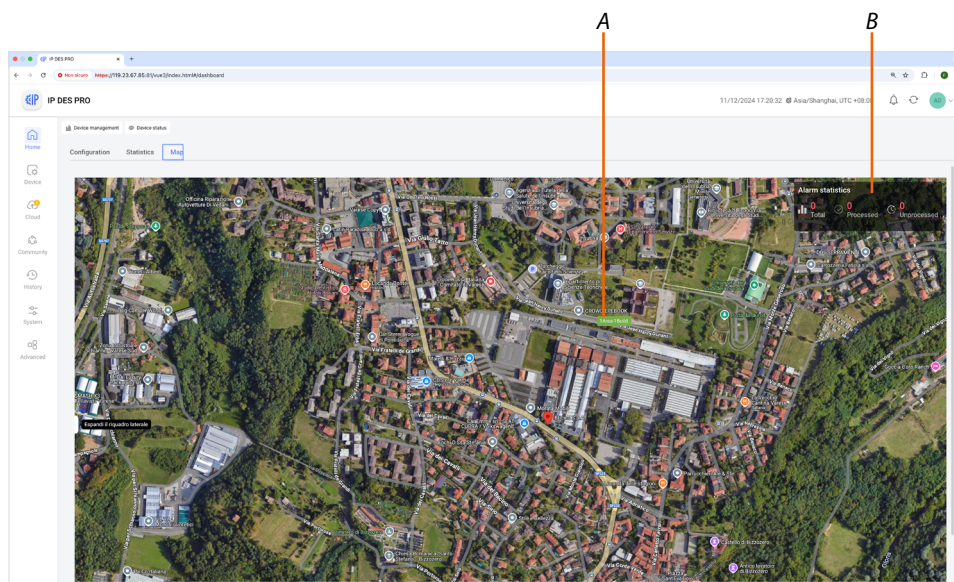


1. Move the mouse on the chart to display the numerical data

Map page

This page serves to facilitate the identification of community Buildings on the map (to insert a background image and markers see [Map Configuration](#)).

It is also possible to display community alerts summary data.

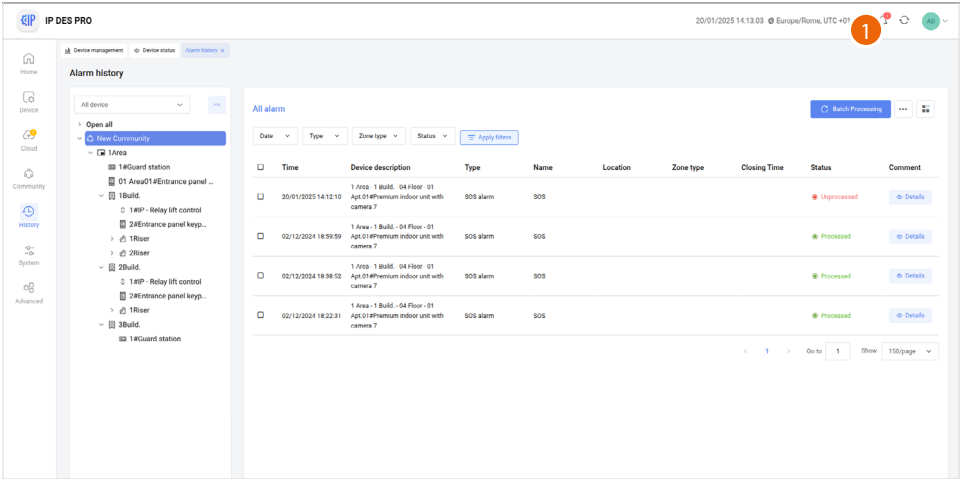


A Markers to identify the managed Buildings

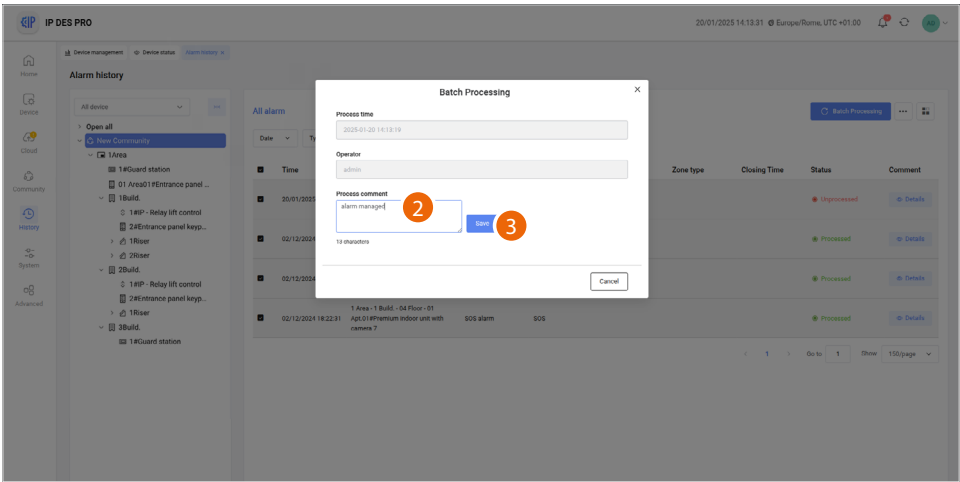
B Displays community alerts summary data

Alarms

When an alarm occurs in the community, a notice appears

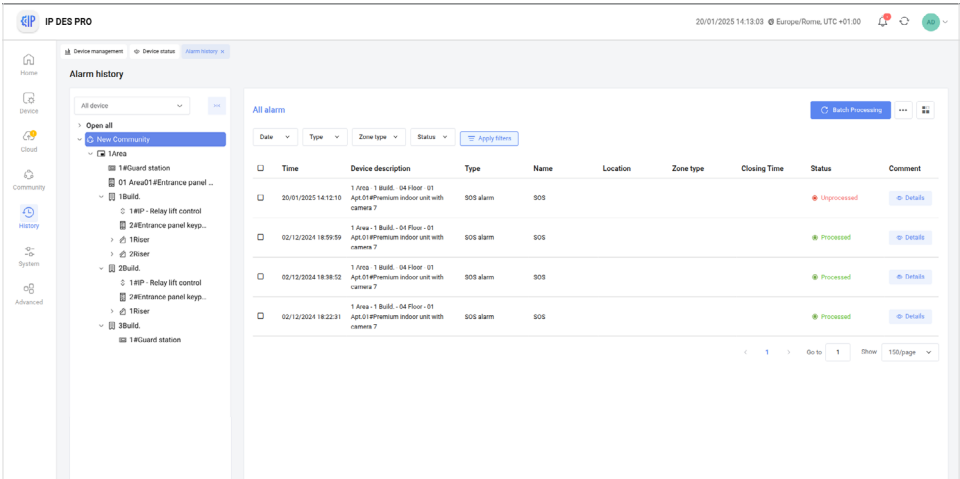


1. Click to display the details



A panel opens, showing some alarm data, with a field for adding comments

- 2. Add a comment
 - 3. Click to save.
- The comment has been saved

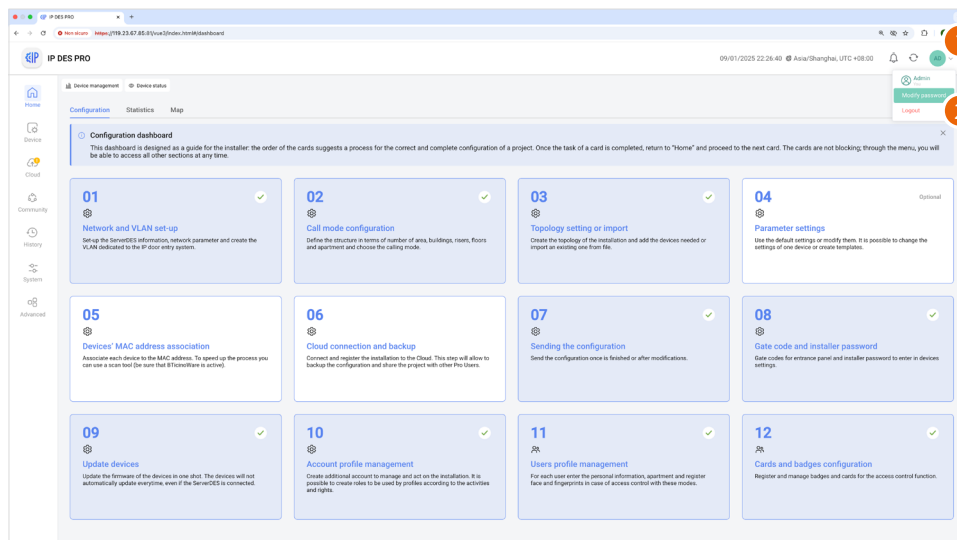


The alarm log is available in the **Alarm history** page

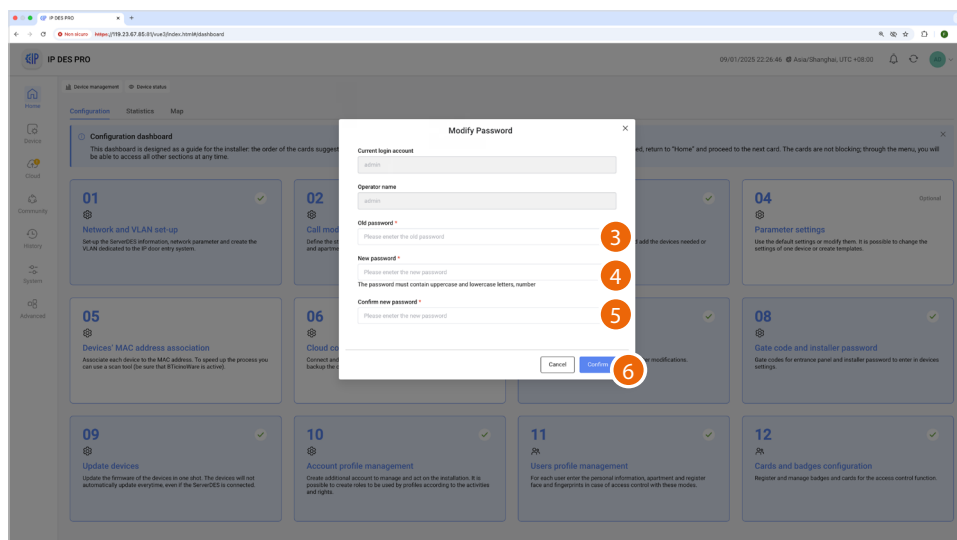
NOTE : the same alarms can be managed by the GS, item 375000

Edit password

This page can be used to change the password of the operator (account) used for accessing the software










1. Click to open the logout and password change menu
2. Click to modify the password



3. Enter the current password
4. Enter the new password (5 to 20 characters, at least one upper case letter, one number and one special character)
5. Enter the new password again
6. Click to confirm

Warning: Save passwords in a safe place that is always accessible.

Main menu

 Home	Home Page	Returns to the Home Page
 Device	<u>Menù</u> <u>Device</u>	It manages various aspects linked with community devices, such as the connecting data network, device registration, changing parameters, etc.
 Cloud	<u>Menù</u> <u>Cloud</u>	It allows, after authentication via an Installer account, to save a copy of the Community on the Legrand Commercial Cloud.
 Community	<u>Menù</u> <u>Community</u>	Displays and manages community access functions, such as permissions, badges/cards etc.
 History	<u>Menù</u> <u>History</u>	Displays various information about accesses, calls, alarms and more in the community.
 System	<u>Menù</u> <u>System</u>	Displays and manages roles and operators as well as various functions related to the SW.
 Advanced	<u>Menù</u> <u>Advanced</u>	Displays and allows the configuration of advanced parameters.

Device



This menu allows to manage various aspects of the community devices, such as the data network that connects them, their registration, the modification of the parameters and so on.

It is also possible to update the firmware of the community devices.

Network and VLAN set-up

Creates and manages the VLAN networks that connect the SD with the community devices.

Device management

Manages the Community devices (add/delete/change the general parameters)

Devices status

Associates the MAC addresses of the physical devices with the virtual devices in the community

Parameter settings

Reads/modifies/sends the advanced parameters of the devices

Background picture replacement

Imports new Home Page background images in addition to the default ones, and sends them to the device.

Fire linkage

Activates and deactivates the Fire linkage function on the EP

Lift control settings

Sets the parameters of the Lift Control function

Update devices

Checks, imports and sends firmware updates to the devices

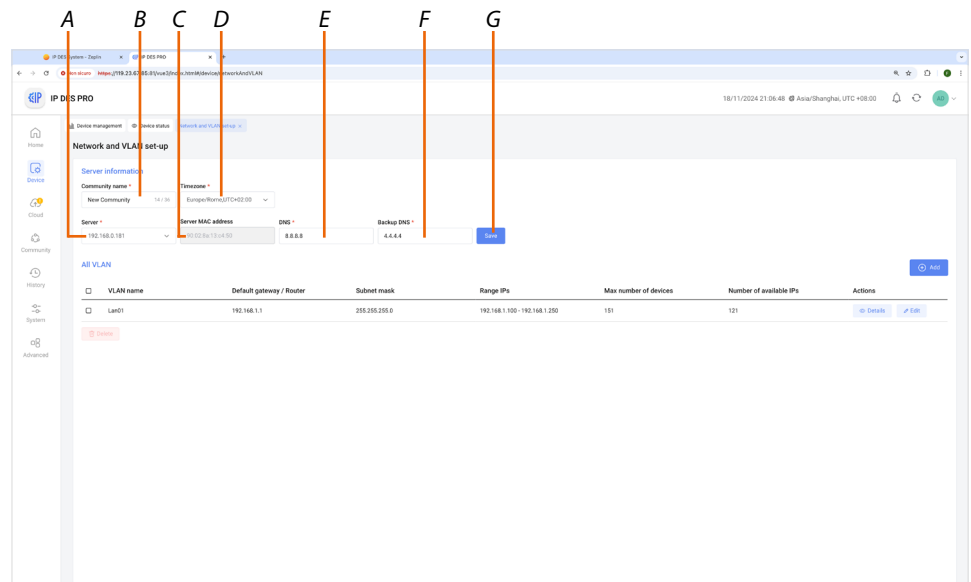
Gate code and installer passwords

Collects all system access codes and installer codes for easy reading

Network and VLAN set-up

This page can be used to set various IP server parameters in the [Server information](#) section and view/edit server information. You can also create VLAN networks in the [Network Management](#) section

Server information



A Selects the Server using the IP address

B Sets the community name

C Displays the Server MAC address

D Sets the time zone

NOTE: The devices do not immediately align date and time, but do so within 24 hours.
To force the new date and time to take effect immediately, restart the devices

E Enters the DNS

F Enters the DNS backup

G Saves the settings

NOTE: When a new system is configured, the devices store in themselves the IP address of the SD that configured them.

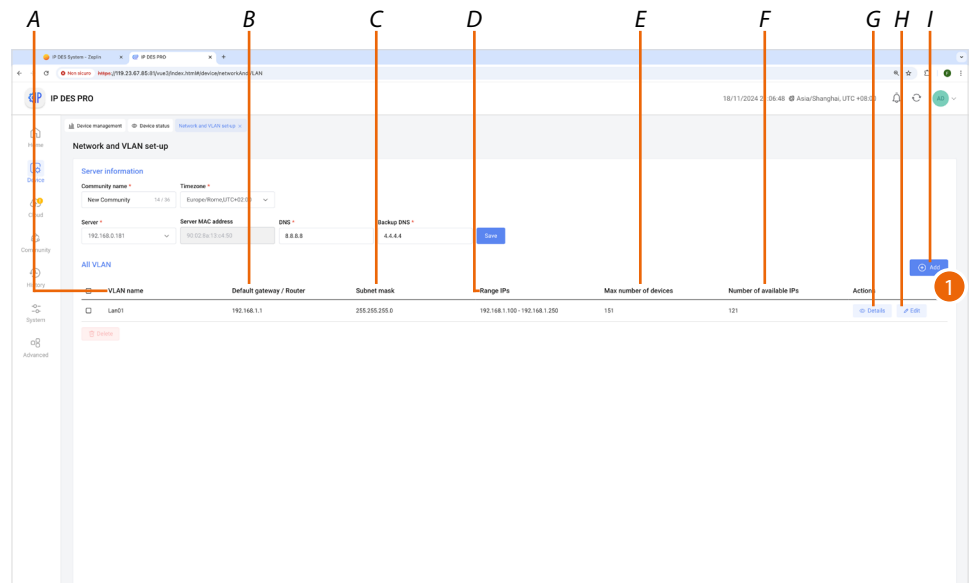
– the SD is replaced with a new one

– the SD is reset to the factory settings

– the SD is configured with parameters not aligned with the existing system

In such cases, the devices will no longer find the association with the SD and will automatically dissociate (unbind) and return to the factory settings, waiting for a new configuration.

Manage the community networks



- A Name of the community VLAN network (letters and numbers without space)
- B IP address of the gateway (router) used to access the Internet
- C Subnet mask address
- D Range of IP addresses occupied by the network
- E Maximum number of devices that it is possible to install in the network
- F Number of devices that can still be installed
- G Network details
- H To edit the network parameters
- I To create the network

1. Click to create a new network

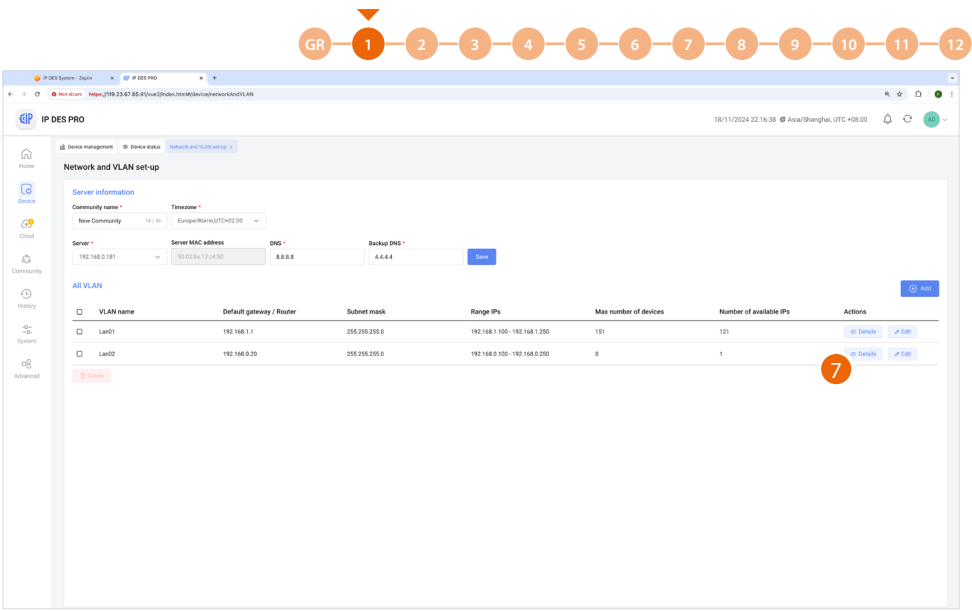
2. Enter the name of the community VLAN network (letters and numbers without space)
3. Enter the Subnet mask address
4. Enter the fixed IP address of the SD given to you by the network administrator
5. Enter the starting and ending IP addresses that will determine the maximum number (A) of devices that can be installed on the network.
6. Click to confirm

NOTE: The network parameters must be compatible with the DHCP server settings. The addresses starting from this value will be assigned by the software, therefore they must not be managed by the DHCP server on the LAN network, see [Assignment of IP address range based on the number of video door entry devices](#).

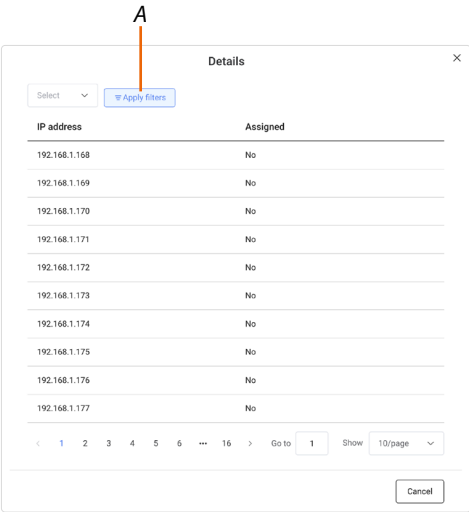
Example:

DHCP server address management 192.168.1.0 up to 192.168.1.199

Software server address management 192.168.1.200 up to 192.168.1.250



7. Click to display the network details

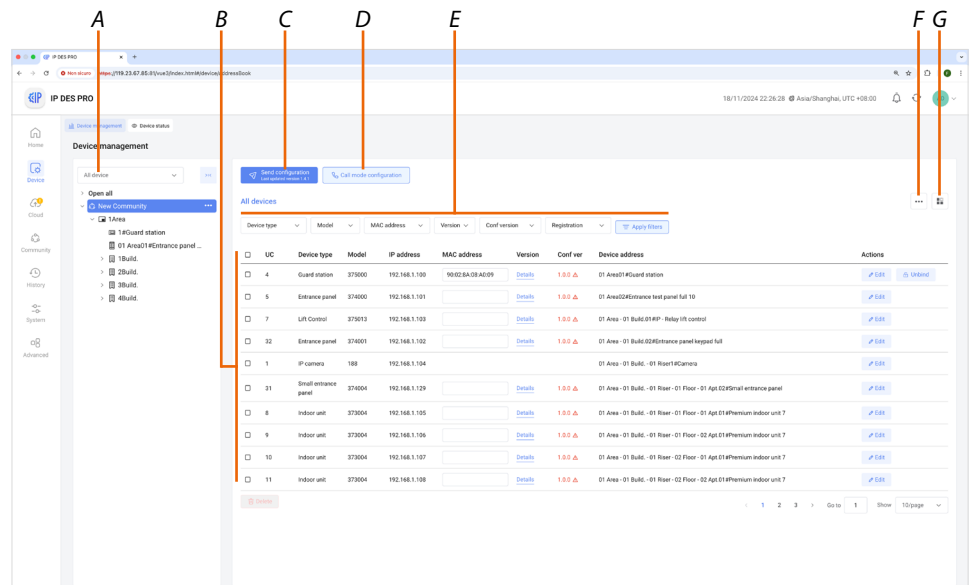


This page shows all the network addresses and related devices. Using the filter (A), it is possible to display only free or only already assigned addresses

Device management

On this page, it is possible to use various functions to create and manage the levels and devices of your system. In particular, you can:

- Reproduce the system defining the structure of the Community through [the levels](#)
- Insert the devices and associate them (using the MAC address) with those on the system.
- Select individual levels/devices, to view and update their parameters
- Set the call mode
- Send the configuration to the system



- A [Creation of levels and devices](#)
- B [Device management area](#)
- C [Send the configuration to the system](#)
- D [Set the system call mode](#)
- E [Select the devices to be managed using filters](#)
- F [Import/Export the device details and structure](#)
- G [Set which information is displayed in the device management area](#)

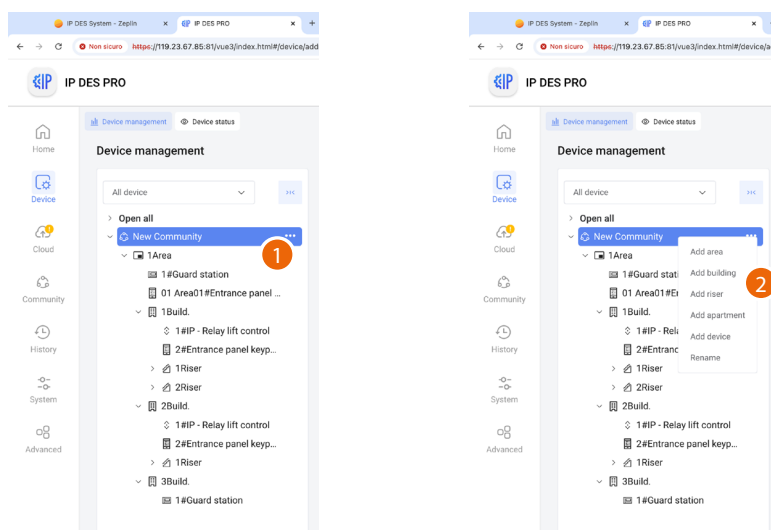
Creation of levels and devices

To create layers and insert devices, use the tree menu.

The tree menu is dynamic, it appears not only on this page but also on the Device Status, parameter settings and Fire linkage pages.

By clicking on a level or device, the button **...** appears

Pressing this key opens a context menu that only displays the functions available for the level/device.



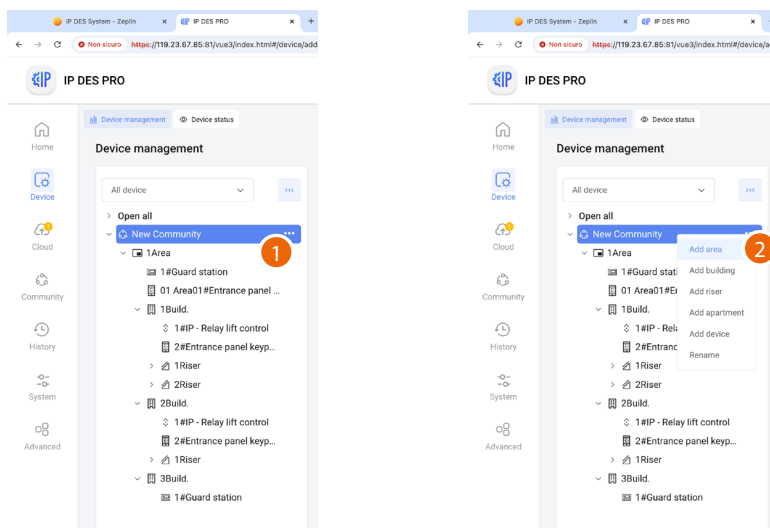
1. Click to open the context menu
2. Click the desired command

FUNCTION	DESCRIPTION	ITEM AVAILABLE FOR
Add area	Add an Area level to the community	Community
Add building	Add a Building level to the community	Community, Area
Add riser	Add a Riser level to the community	Community, Area, Building
Add floor	Add a Floor level to the community	Building, Riser
Add apartment	Add an Apartment level to the community	Community, Area, Building, Floor
Add device	Add a Device to the community	all
Rename	Modify the name of a level or device	all
Delete	Delete a level or device	all

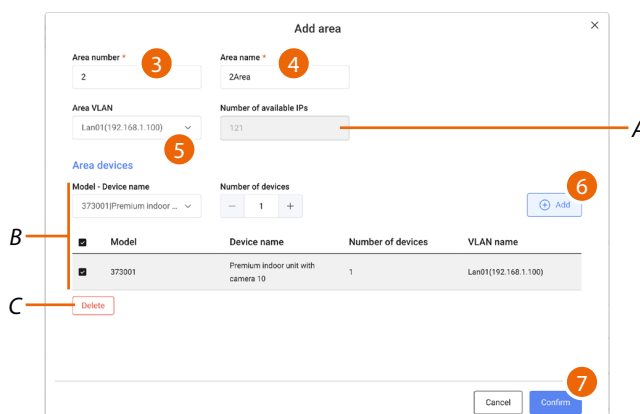
Add an Area

This function can be used to add levels and devices to the community.

While adding a layer, it is also possible to enter at the same time the devices that are relevant for the layer.



1. Click to open the context menu
2. Click to add the Area



- A Maximum number of addresses available (see [Community Network Settings](#))
- B Area for adding the device
- C Delete the selected devices

3. Select the progressive identification number

Please note: changing this parameter also changes the address in the community (see [automatic addressing](#))

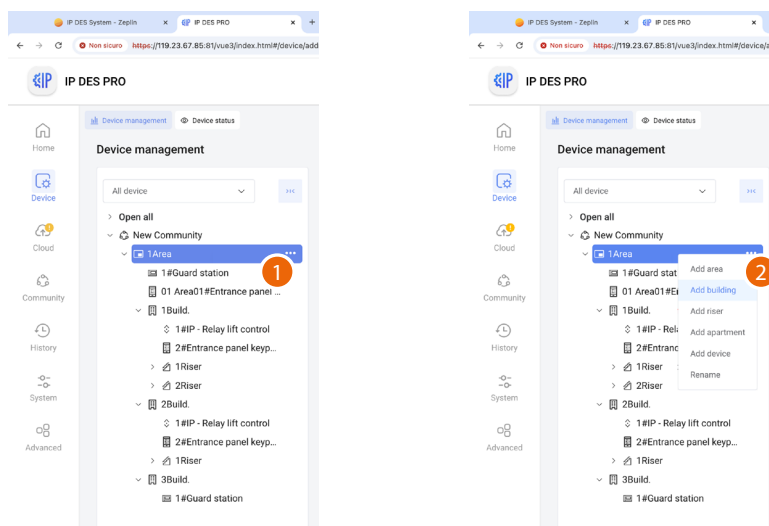
4. Enter a name for the Area
5. Select the VLAN network from those created in the [Community Network Settings](#) page
6. It is now possible to add devices to the area; see [Add device](#)
7. Click to confirm

Add a Building

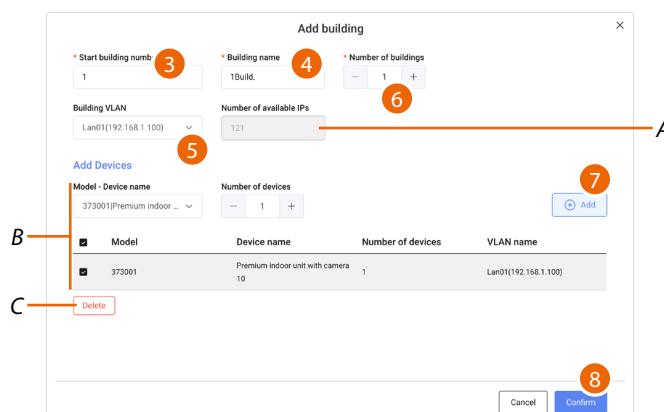
Add a Building **level** to the community.

While adding a level, it is also possible to add the level devices.

For example, when adding a Building, it is possible to also add the EP associated with that Building.



1. Click to open the context menu
2. Click to add the Building



A Maximum number of addresses available (see [Community Network Settings](#))

B Area for adding a Building device

C Delete the selected devices

3. Select the progressive identification number

Please note: changing this parameter also changes the address in the community (see [automatic addressing](#))

4. Enter a name for the Building
5. Select the VLAN network from those created in the [Community Network Settings](#) page
6. Select how many Buildings to add
7. It is now possible to add Building devices, see [Add device](#)
8. Click to confirm

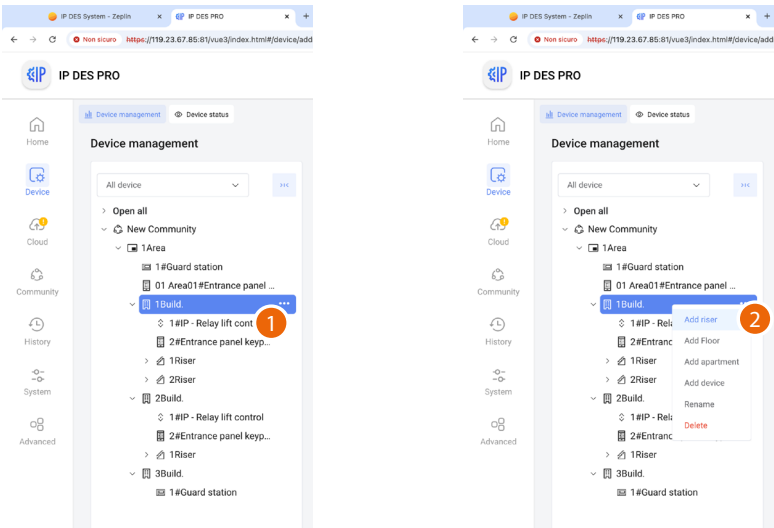


Add a Riser

Add a Riser [level](#) to the community.

While adding a level, it is also possible to add the level devices. For example, when adding a Riser, it is possible to also add the EP associated with that Riser.

When adding a Riser, it is also necessary to define the number of Floor and the number of Apartment for each Floor.



1. Click the level to which you want to add a Riser
2. Click to add a Riser

- A Maximum number of addresses available (see [Community Network Settings](#))
- B Area for adding the devices
- C Delete the selected devices

GR 1 2 3 4 5 6 7 8 9 10 11 12

Add riser

> 1Area 1Build.

* Riser number 3

* Riser name 3Riser

* Start floor number 3

* Number of floors 1

* Number of apartment per floor 1

Riser VLAN Lan01(192.168.1.100)

Number of available IPs 121

Riser devices

Model - Device name 188/Camera

Number of devices 1

Floor devices

Model - Device name 188/Camera

Number of devices 1

Apartment devices

Model - Device name 188/Camera

Number of devices 1

Cancel Confirm

3. Select the progressive identification number

Please note: changing this parameter also changes the address in the community (see [automatic addressing](#))

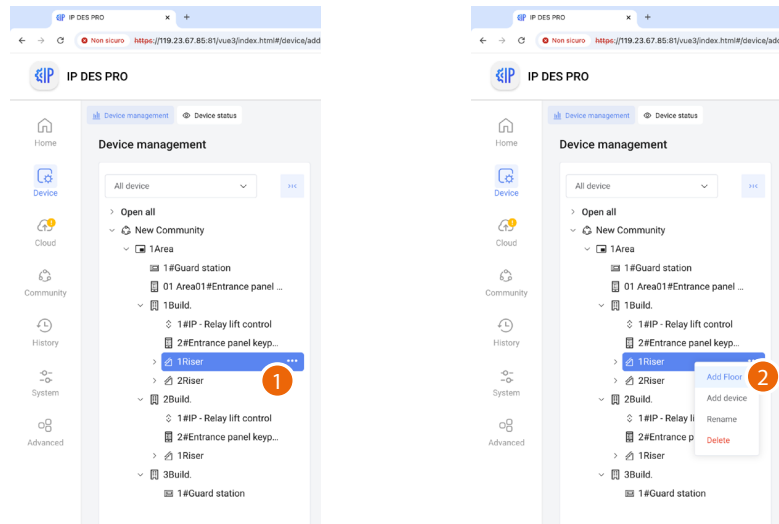
4. Enter the name of the Riser
5. Enter the floor number from which the system starts counting the number of floors.
6. Enter the number of Floors that make up the Riser
7. Enter the number of Apartments for each Floor
8. Select the VLAN network from those created in the [Community Network Settings](#) page.
9. Now it is possible to add the devices of Riser, Floor and Apartment, see [Add device](#)
10. Click to confirm

Add a Floor

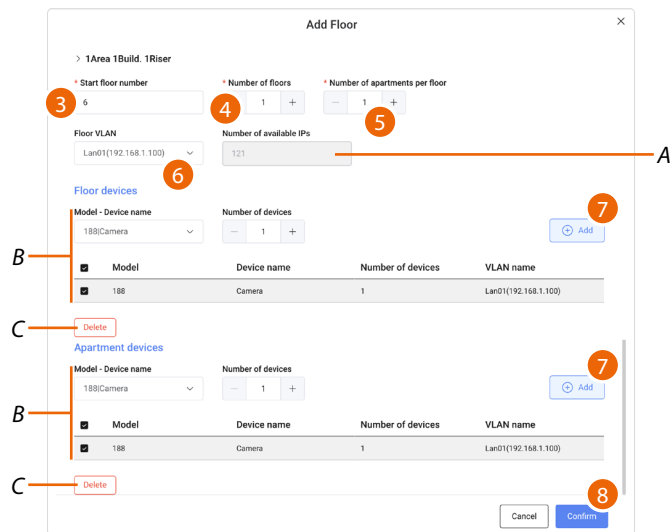
Add a Floor [level](#) to the community.

While adding a level, it is also possible to add the level devices.

For example, when adding a Floor, it is possible to also add the EP associated with that Floor.



1. Click the level to which you want to add a Floor
2. Click to add the Floor



A Maximum number of addresses available (see [Community Network Settings](#))

B Area for adding the devices

C Delete the selected devices

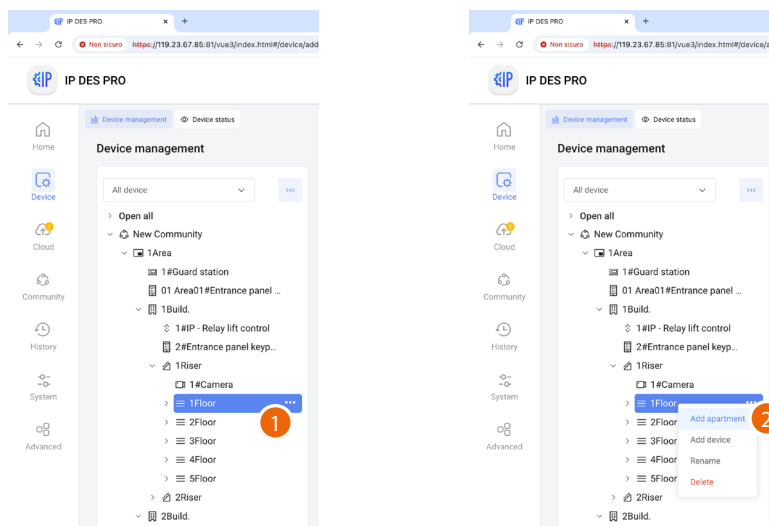
3. Enter the floor number from which the system starts counting the number of floors.
For example, in a building with non-conventional numbering (e.g. mixed-use building in which the residential floors start from the third floor).
4. Enter the number of the Floor
5. Enter the number of the Apartment for each Floor
6. Select the VLAN network from those created in the [Community Network Settings](#) page
7. Now it is possible to add the devices of Riser, Floor and Apartment, see [Add device](#)
8. Click to confirm

Add a new apartment

Add an Apartment **level** to the community.

While adding a level, it is also possible to add the level devices.

For example, when adding a Apartment, it is possible to also add the VEPO associated with that Apartment.



1. Click the level to which you want to add an Apartment
2. Click to add the Apartment

A Maximum number of addresses available (see [Community Network Settings](#))

B Area for adding the device

C Delete the selected devices

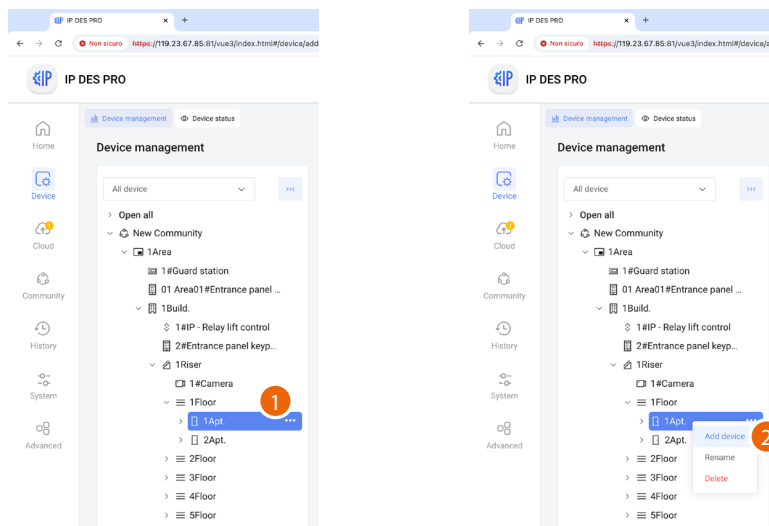
3. Enter the apartment number from which the system starts identifying apartments.
For example, in a building where the numbering of the apartments starts at 100, this parameter must be set to 100.
4. Select the number of apartments to add
5. Select the VLAN network from those created in the [Community Network Settings](#) page
6. It is now possible to add the devices of the apartment
- Or
7. Click to confirm and enter devices later; see [Add device](#)



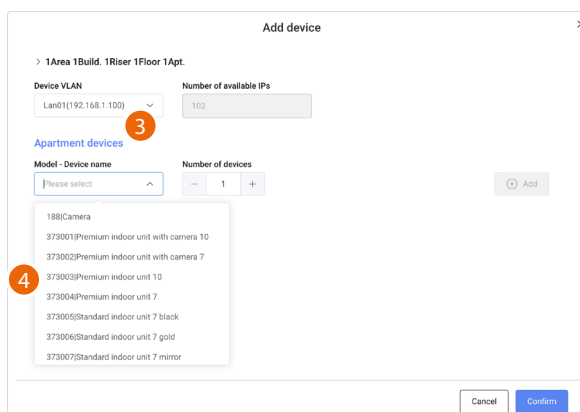
Add device

Adds a device within the selected **level** in the community

NOTE: before carrying out this operation it is recommended to generate a template (see [Parameter configuration](#))



1. Click the level to which you want to add a device
2. Click to add one or more devices



3. Select the VLAN network from those created in the [Community Network Settings](#)
4. Select the device among those suggested, or enter the product code, if known



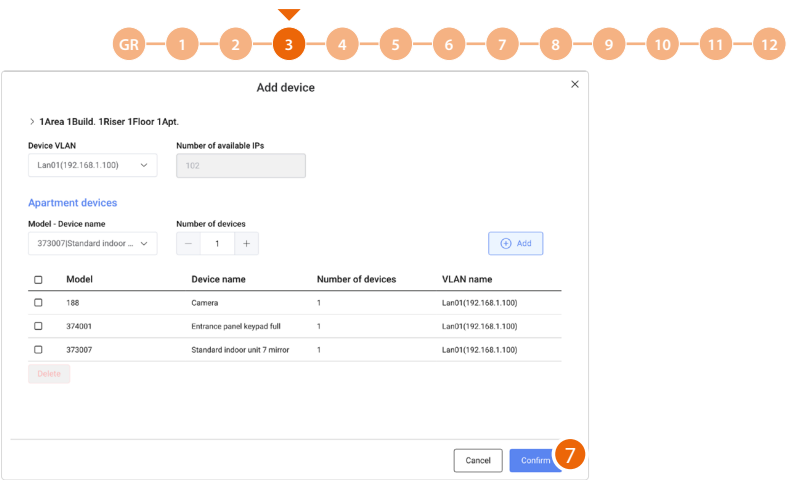
The available devices are:

PE	374000	IP video external pushbutton panel with 10" touch display, face recognition and fingerprint
	374001	IP video external pushbutton panel with 4.3" display, face recognition and fingerprint
	374002	IP video external pushbutton panel with 10" touch display
	374003	IP video external pushbutton panel with 4.3" display
PEF	374004	Small IP video internal pushbutton panel
	374005	IP video external pushbutton panel with 4.3" touch display
	374006	Small external pushbutton panel with badge reader and keys for direct call
PI	373001	IP video internal unit with 10" touch display and internal camera
	373002	IP video internal unit with 7" touch display and internal camera
	373003	IP video internal unit with 10" touch display
	373004	IP video internal unit with 7" touch display
	373005/6/7	Standard IP video internal unit (black / gold / mirror) with 7" touch display
	373008	IP video internal unit with 7" touch display (standard POE power supply)
CDP	375000	IP guard station with 10" touch display and audio handset
ALTRO	188	Camera NOTE: to add this device, see "Add a OnVif IP camera"
	375013	Lift control interface with relay 375013 NOTE: to add this device, see "Add a lift control interface with relay 375013"

NOTE: Not all devices are available for all markets: see the catalogue or contact your dealer

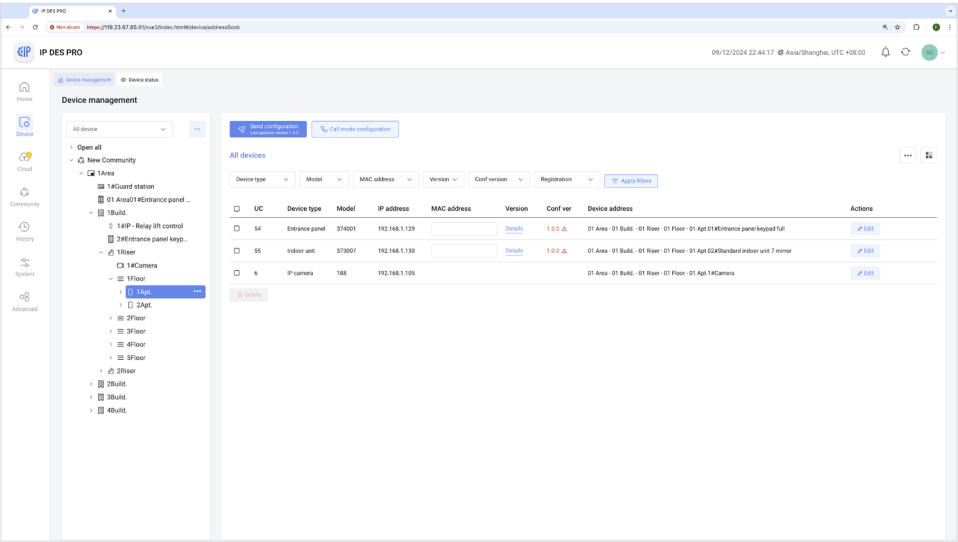
5. Enter the number of devices

6. Click to add



Several devices may be added at the same time

7. Click to confirm



Add a OnVif IP camera

Adds a camera within the selected **level** in the community

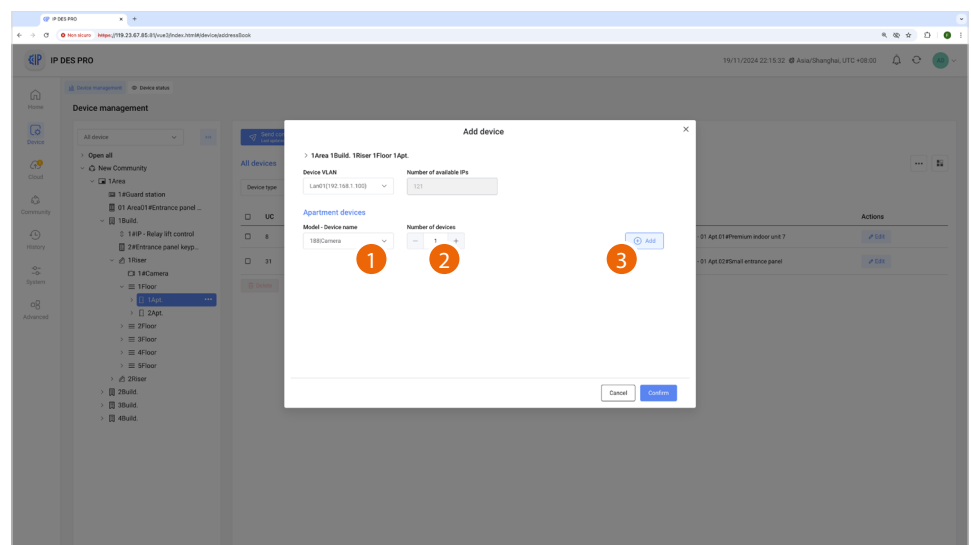
Before completing the final installation, a function test is recommended in order to be sure of compliance.

The BTicino IP video door entry system complies with the ONVIF protocol, check on the website <https://www.onvif.org/conformant-products> that the IP camera you want to use is also compliant.

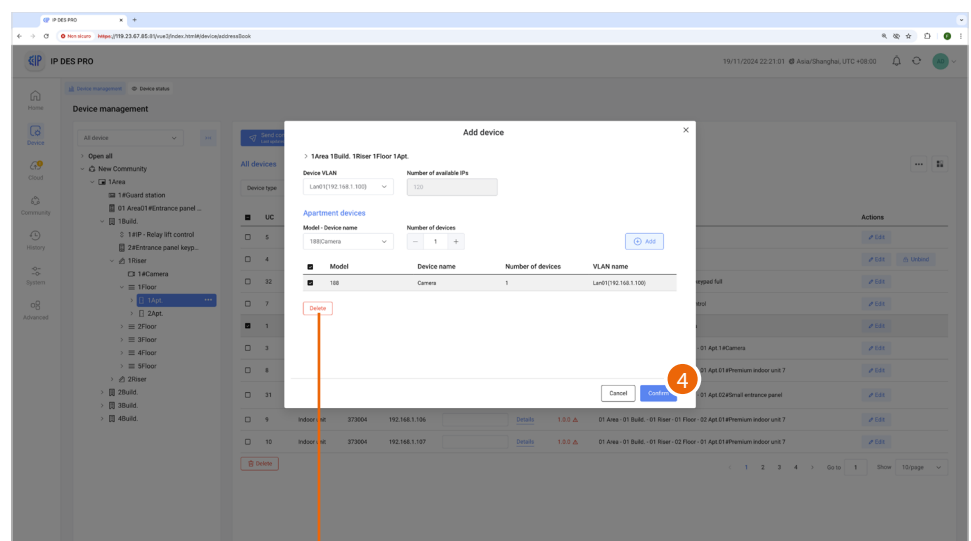
NOTE: Some brands and models may not be compatible.

When choosing and configuring OnVif IP cameras, bear in mind that the video transmitted must meet these parameters:

- resolution: max. 720p
- coding: H264



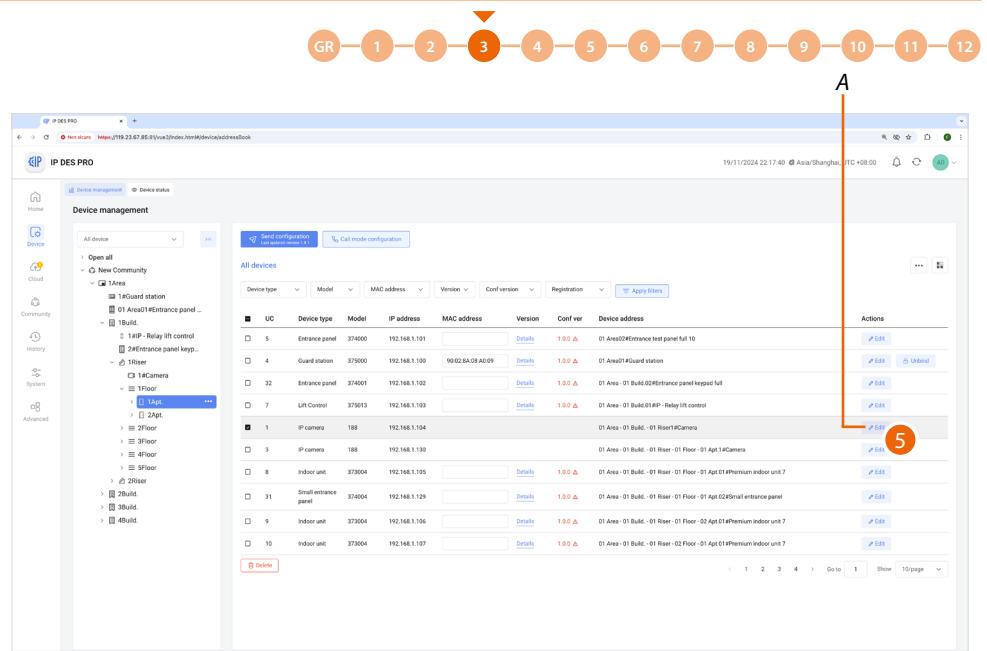
1. Select the camera
2. Select the quantity
3. Click to add



A

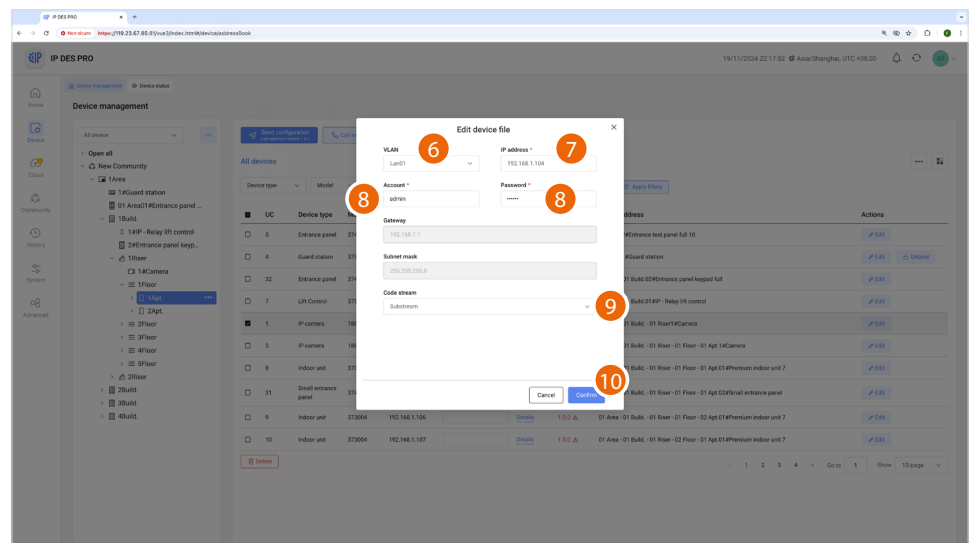
A Delete the camera

4. Click to confirm



A Modify the camera settings

5. Select to modify the camera

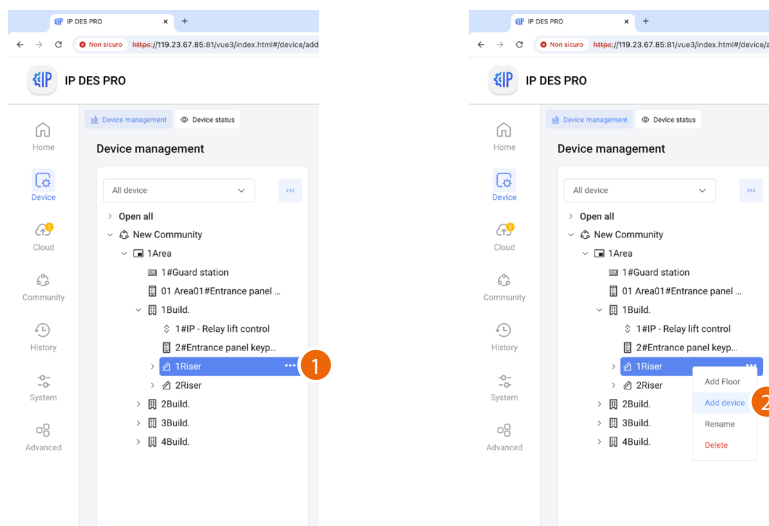


6. Select the network on which the camera is installed (must be the same as the IP video door entry system devices)
7. This address is automatically suggested by the system. Check that the IP camera has this same address
8. Enter the account (*) and password of the camera.
*NOTE: the reference account is the one from which the video stream can be taken
9. Select the type of video streaming that you want to use
10. Click to confirm

Add a lift control interface with relay 375013

Adds a lift control interface with relay 375013 within the selected **level** in the community

NOTE: The lift control interface can only be inserted at riser level



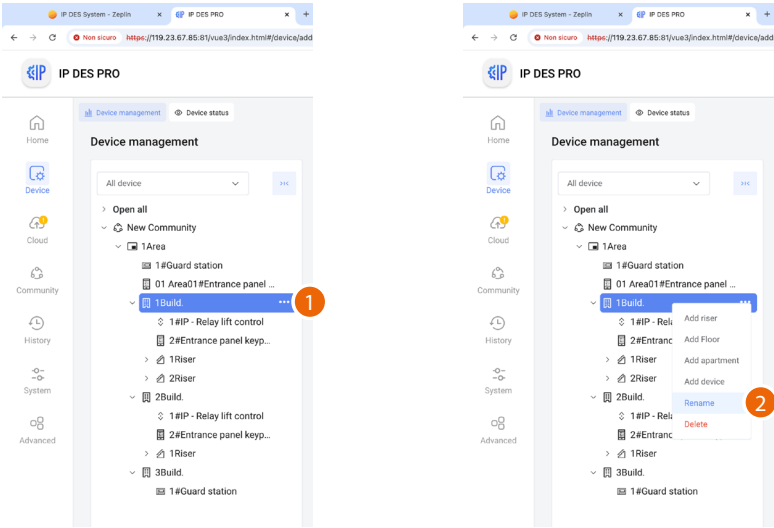
1. Right click the level to which you want to add a Lift control interface with relay 375013
2. Click to add a lift control interface with relay 375013

3. Select the Lift control interface with relay 375013
4. Select the quantity
5. Select the operating mode:
 - **with access control:** this mode allows to set up an exclusive call to a specific floor (e.g. only go to the third floor)
 - **ground floor call:** this mode allows to set the system so that the lift is sent to the floor of the caller.
6. Click to add

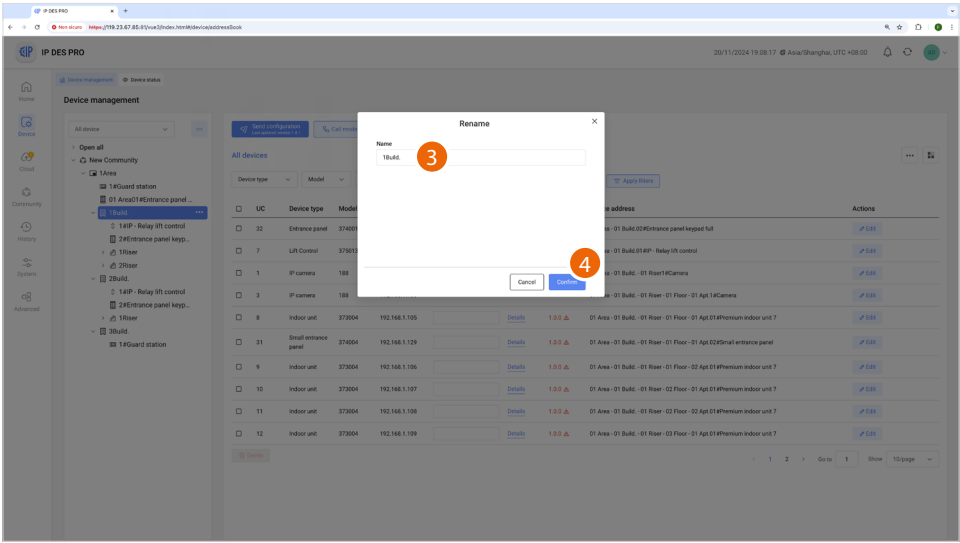
NOTE: If in the community there is an entrance panel at Area or Building level, set the Lift Control Interface with Relay 375013 to NO LIFT

Modify the name

Modify the name of levels and/or devices



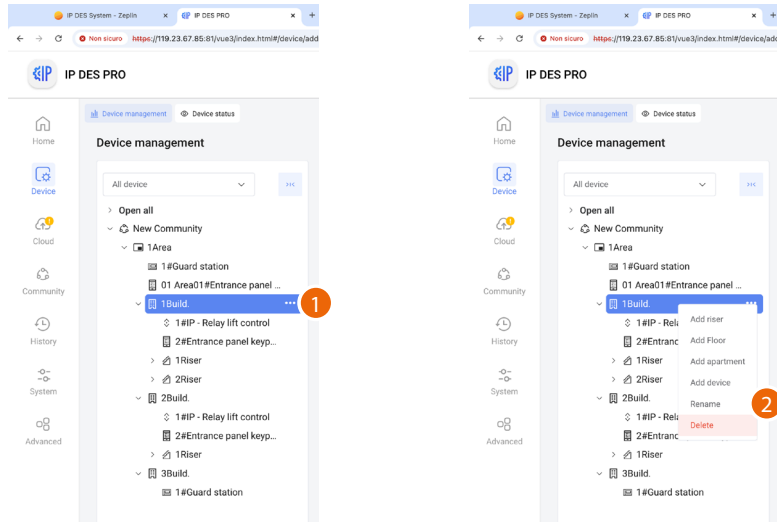
1. Click the level or device to be modified
2. Click to select the command



3. Enter the new name
4. Click to confirm

Delete

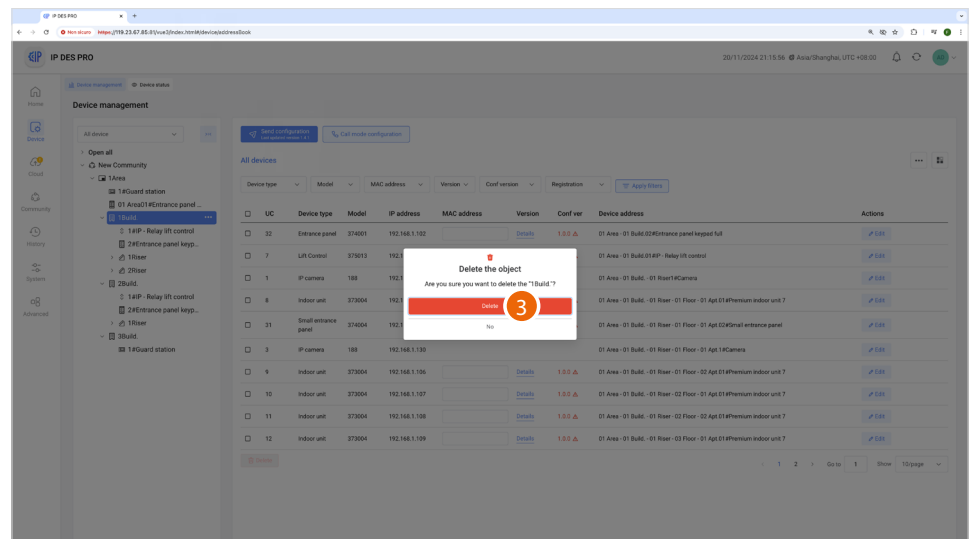
Delete levels and/or devices



1. Click the level or device to be deleted

CAUTION: Selecting a level will also delete its sub-levels

2. Click to select the command



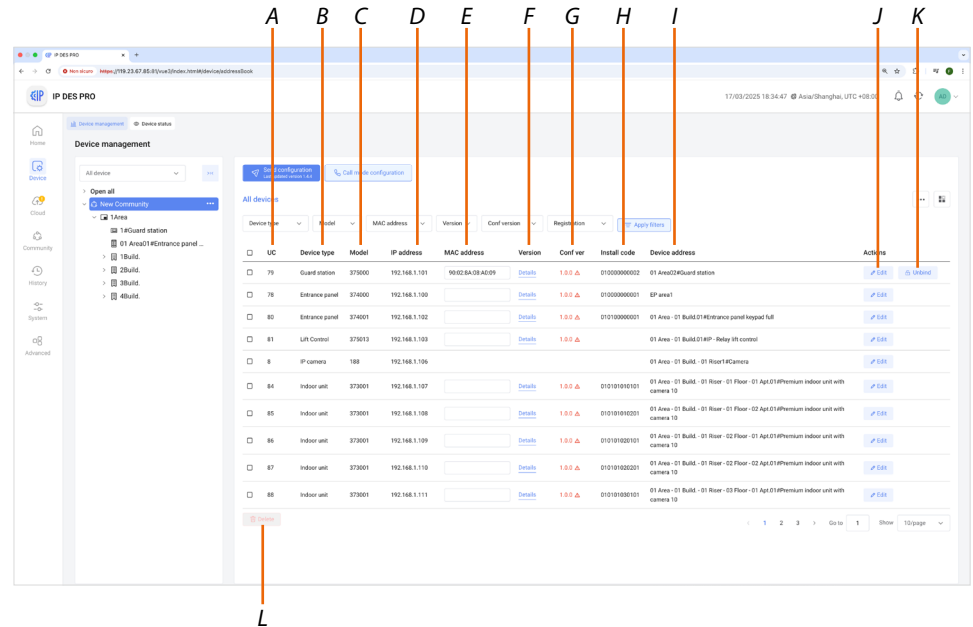
3. Click to confirm.

Performing this operation also dissociates the physical device from the virtual one. The physical device is reset.

ATTENTION: with this procedure, the level/device is permanently deleted. To be able to manage it again, it will be necessary to follow the adding procedure (Add Area/Building/Riser/Floor/Apartment/Device)

Device management

In this area, it is possible to associate the device using the mac address, change its parameters or delete it.



A Progressive number

B Type of device

C Item code

D Device network address

E Device Mac address: to associate the MAC addresses of the physical devices to virtual devices, see [Associate the device](#)

F Displays some [details](#) della configurazione presente sul dispositivo

G Version installed on the physical device.
The colour identifies the synchronisation status of the software and device configuration.
Black = synchronized Red = not synchronized

H. Product installation code, a unique code that can be requested by community devices under certain configuration conditions (see the individual device manuals)

I. Name of the customisable device.
The original name represents [the address of the device in the community](#)

J [Modify the device parameters](#)

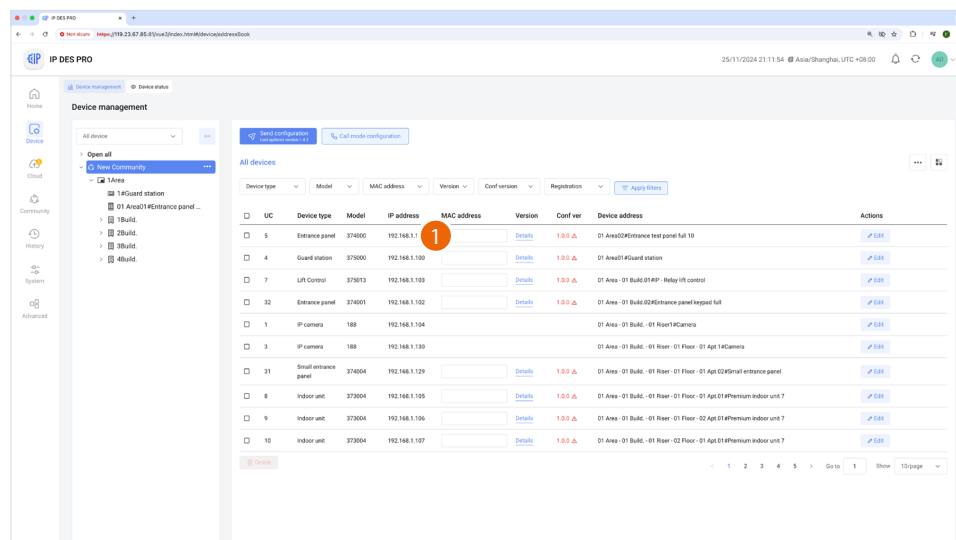
K [Dissociate the device](#)

L Delete the selected devices



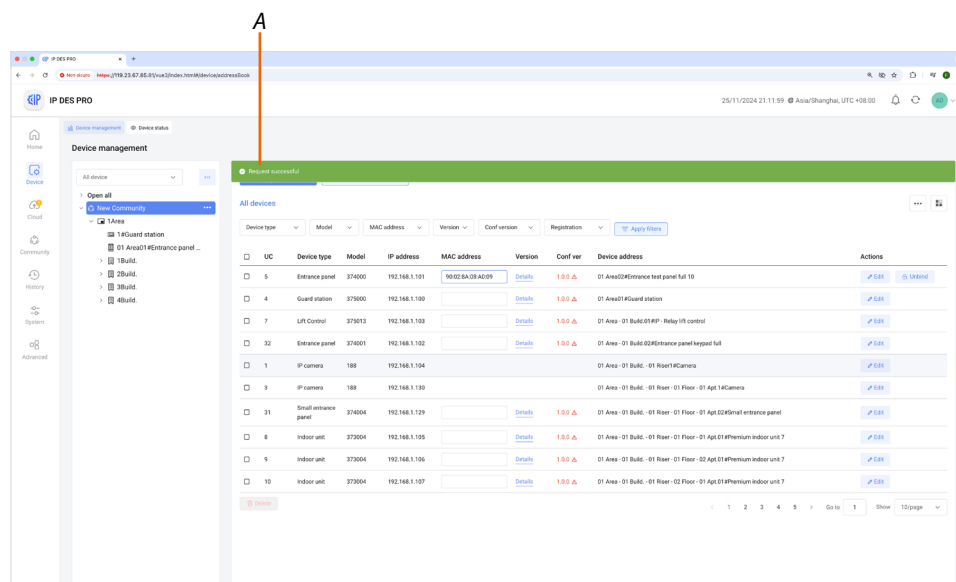
Associate the device

This page can be used to associate the MAC addresses of the physical devices with the virtual devices in the community.



1. Move the cursor inside the field then:

- Using a reader, read the address from the label on the packaging, or the label on the back of the device or
- manually enter the address (including the separation :).



A A message indicates that the association has been carried out

If the printer is the one set as default, it will automatically print the label which must then be applied to the Device box in order to immediately identify the apartment or position in which to install it.

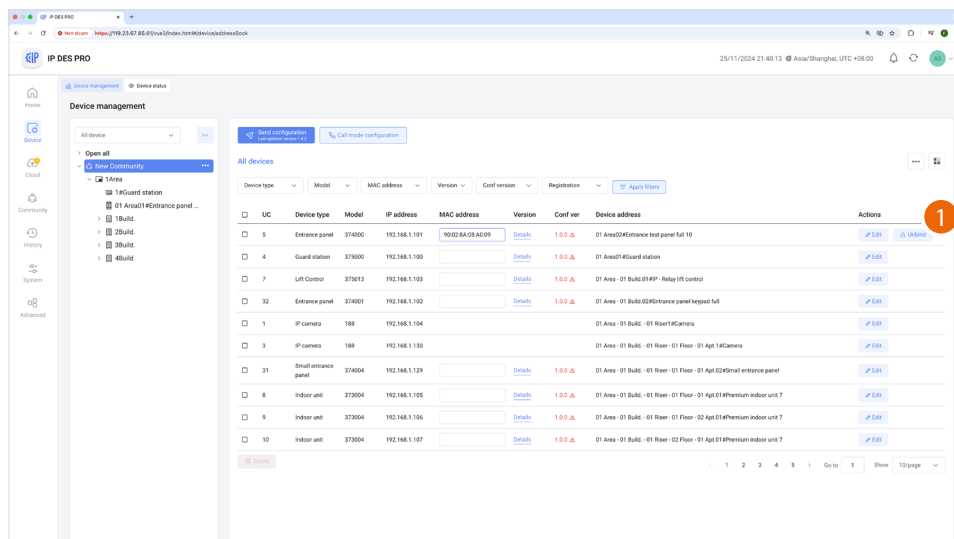
NOTE: the BTicinoWare software must be running.

```

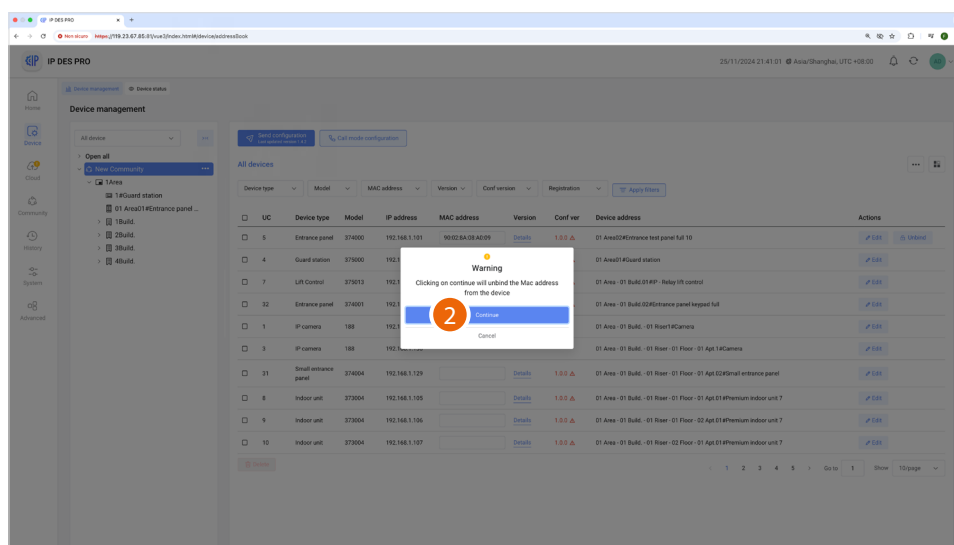
DEVICE INFORMATION:
1area1building01riser01floor01house#10 inch grey iu
DEVICE MODE1: 373001
MAC ADDRESS: 90:02:8A:08:A0:09
PRINT DATE/TIME: 2020-12-09 15:41:05
  
```

Dissociate the device

It is possible to remove the association between the physical and the virtual device

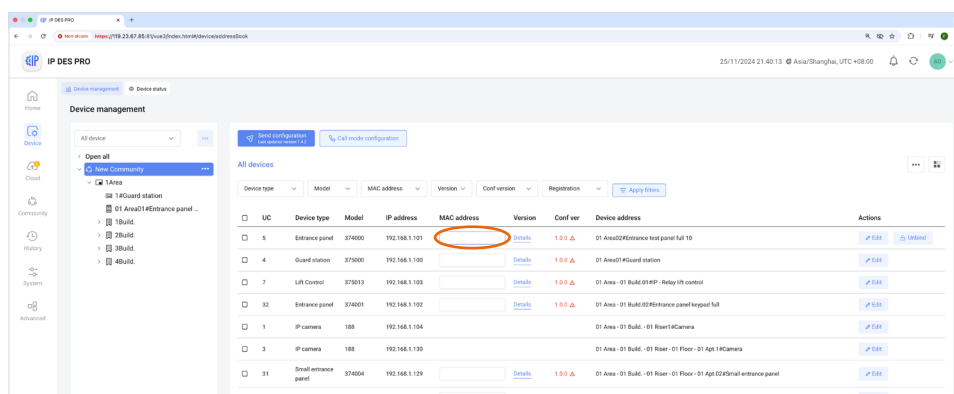


1. Click to dissociate

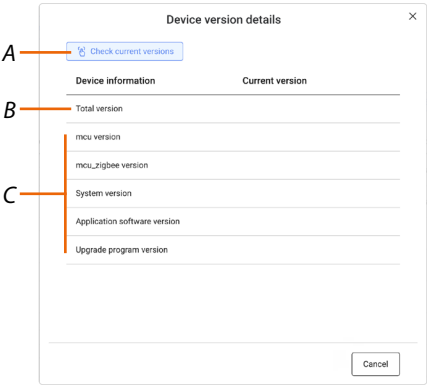


2. Click to confirm

The virtual device can now be associated with another physical device by entering the MAC address.

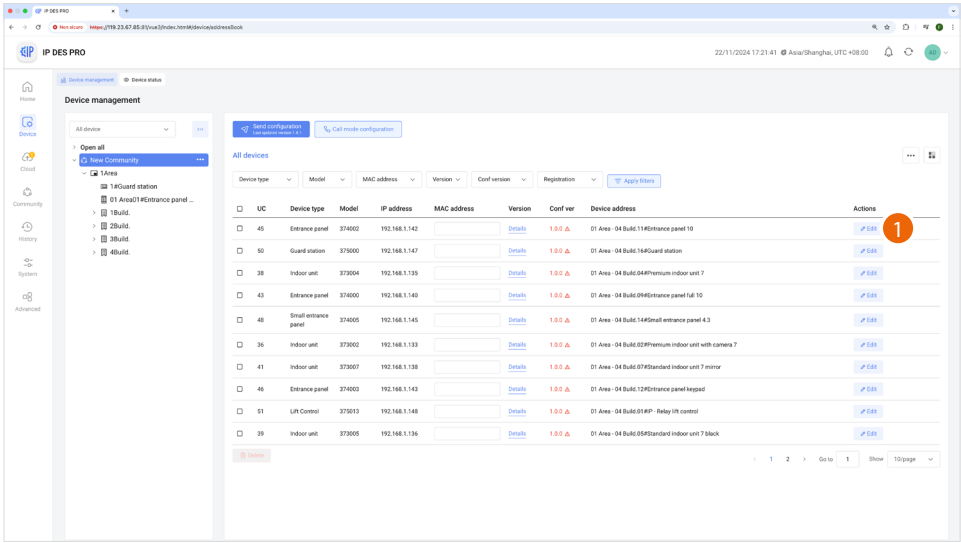


Configuration details



- A Check the current version on the device
- B Device version
- C Information for debug

Modify the device parameters



1. Click to edit.
The parameters vary depending on the device

374000, 374001, 374002, 374003

373001/373002/373003/373004/
373005/373006/373007/373008/
374004/374005/374006/375000/
375013

Edit device file

VLAN: Lan01 IP address: 192.168.1.142

Install code: 010400000011

Device description: 01 Area - 04 Build.11#Entrance panel 10

Device ID: 445-45

Is super: No

Cancel Confirm

Edit device file

VLAN: Lan01 IP address: 192.168.1.147

Install code: 010400000016

Device description: 01 Area - 04 Build.16#Guard station

Device ID: 445-50

Cancel Confirm

- A Edit the device VLAN network
- B Edit the device network address
- C Change the device name in the SW (does not change the call address)
- D Set the database to read from, for face recognition and fingerprint information.
 - No: up to 10,000 faces and up to 5,000 fingerprints (EP database)
 - Yes: more than 10,000 faces or more than 5,000 fingerprints (SW database)

188

188

Edit device file

VLAN: Lan01

IP address *: 192.168.1.131

Account *: admin

Password *: *****

Gateway: 192.168.1.1

Subnet mask: 255.255.255.0

Code stream: Substream

Cancel Confirm

E points to Account/Password fields. *F* points to Code stream field.

E Edit the account (*) and password of the camera

***NOTE:** the reference account is the one from which the video stream can be taken

F Edit the type of video streaming that you want to use

If you want to change the alias of all the devices inside the same apartment:

2

Edit device file

VLAN: Lan01

IP address *: 192.168.1.142

Install code: 010403000011

Device description *: 01 Area - 04 Build 11#Entrance panel 10

Device ID: 445-45

Is super: No

Cancel **3** Confirm

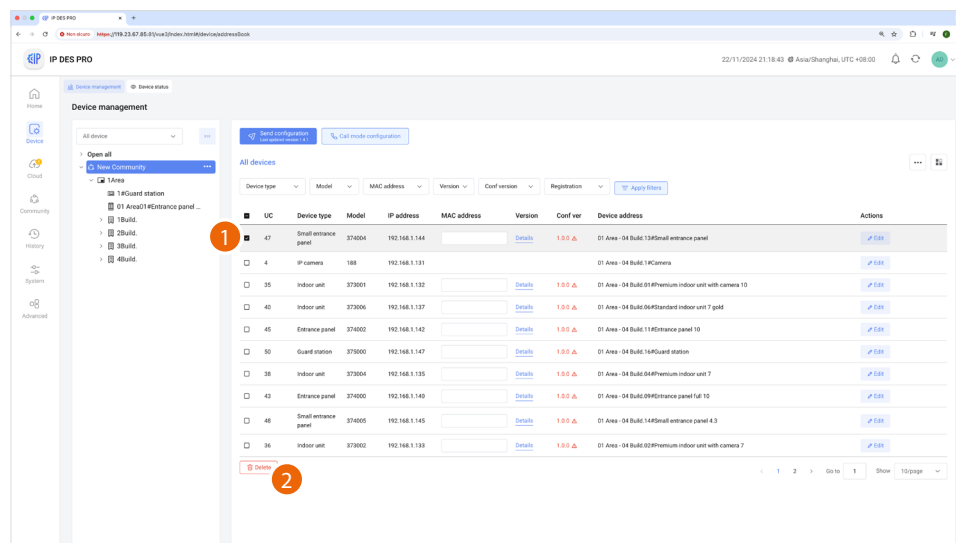
2. Edit the parameter

3. Click to confirm

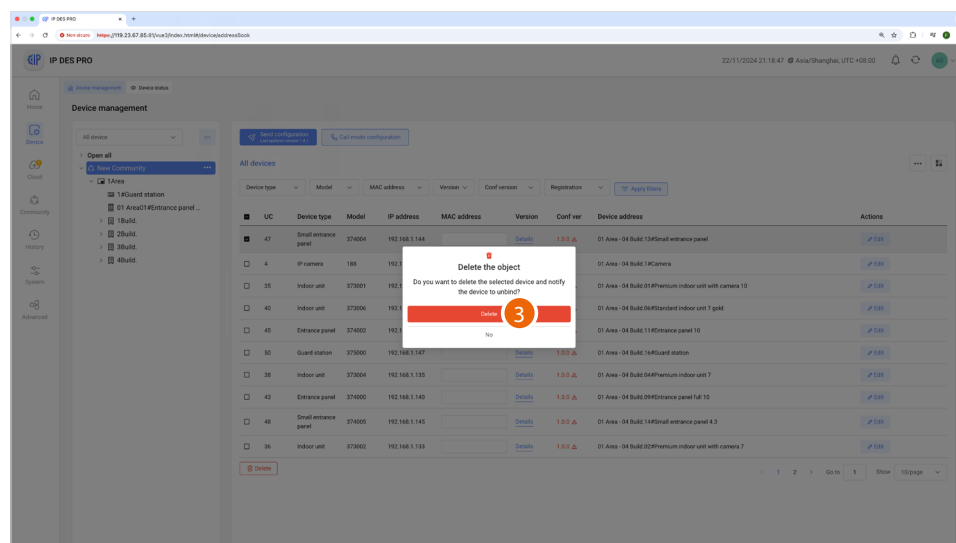
To change the advanced device parameters (e.g. ring volume, installer password etc.), see [Parameters configuration](#)

CAUTION: After changing these parameters, it will be necessary to restart the device.

Delete the devices



1. Click to select the device to be deleted
2. Click to delete the device

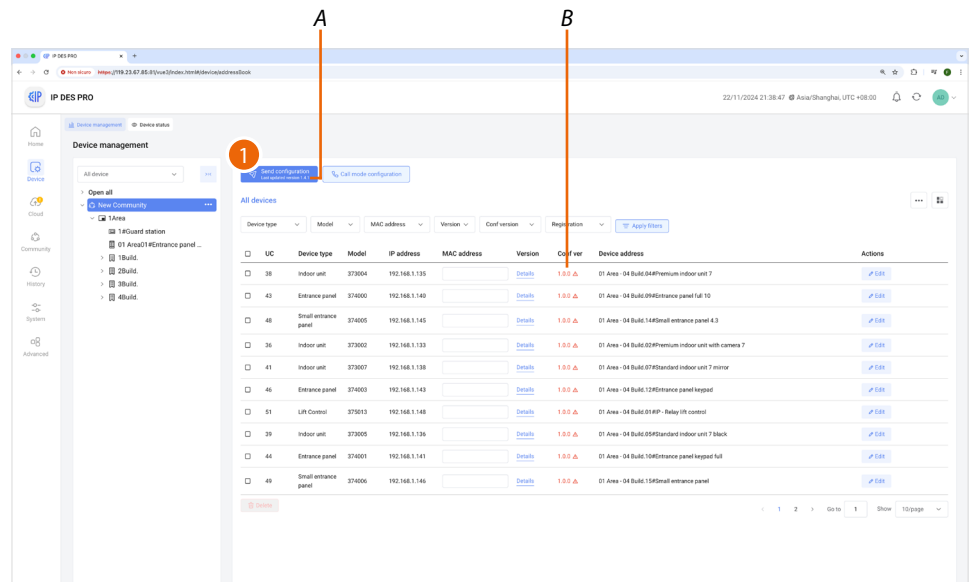


3. Click to confirm

Warning: this procedure will permanently delete the device. To manage it again, it will be necessary to **re-enter** it and **register it**

Send the configuration to the devices

With this function it is possible to send the configuration.
Each time this is done, the configuration version will be updated.

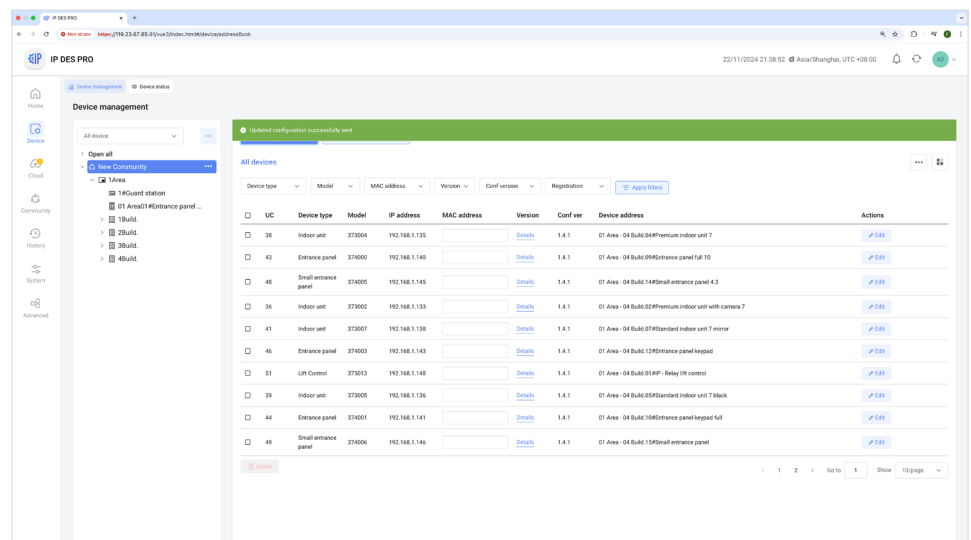


A Configuration version on the SW

B Configuration version on the device

1. Click to send the configuration to the devices

NOTE: in case of unexpected device behaviour during use, check that the SW configuration is the same as the device configuration



Complete the configuration with devices switched off. When first switched on, the devices will automatically load the configuration

In the event of a change to the configuration, the devices will only accept the changes without further action if they remain in the same position they were the previous time the configuration was sent.

If a device has been incorrectly placed in an apartment and needs to be moved, it will need to be reset (see device manuals) before uploading the new configuration.

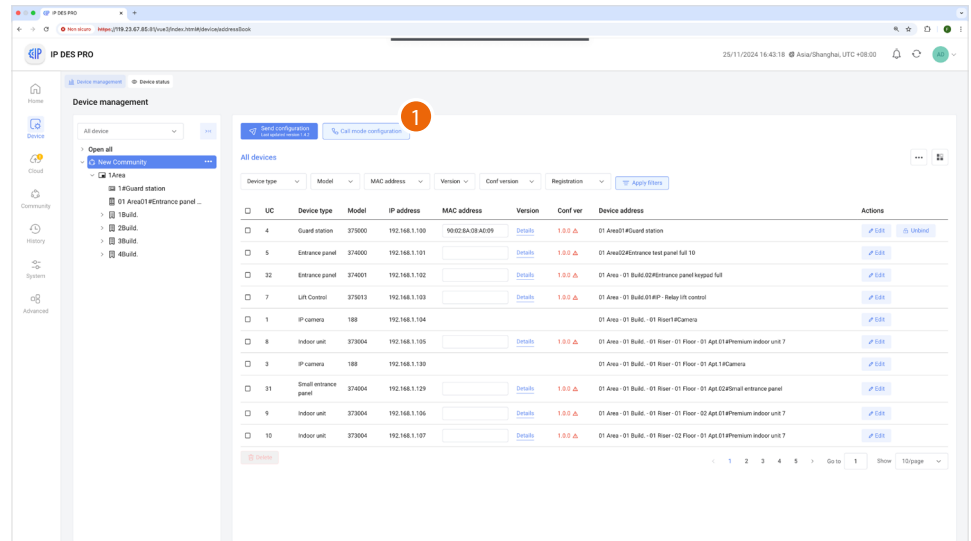
The configuration is now saved in the SD. To avoid accidental data loss, it is also possible to **save it in an archive file**

Set the system call mode

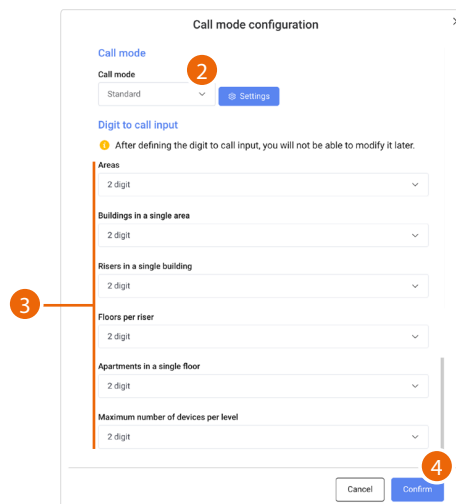
This function allows to choose how to address a call.
The available modes are:

- [Standard call](#)
- [Alphanumeric call](#)
- [4-digit call](#)

For details, see [Fundamental concepts](#).



1. Click to open the page



2. Set the type of call ([standard](#), [alphanumeric](#), [4-digit](#))
3. Set the number of digits to be used for each call sector (Area/Building/Riser/Floor/Apartment)
CAUTION: After setting these parameters for the first time, it will no longer be possible to change them.
In order to change these parameters, restore the factory settings.
4. Touch to confirm



Standard call

1. Click to set the standard call parameters

2. Select the level to be configured
3. Click to define the use of letters for the level
4. Since the number of Floors is normally high, and therefore letters replacing numbers may not be enough, a combination of numbers and letters may also be used.
Click to add a combination
5. Select the number of Floor to be replaced with a combination of numbers and letters
6. The system suggests a combination, which can be replaced with a letter or another combination of your choice.
7. Click to save the setting.

Alphanumeric call

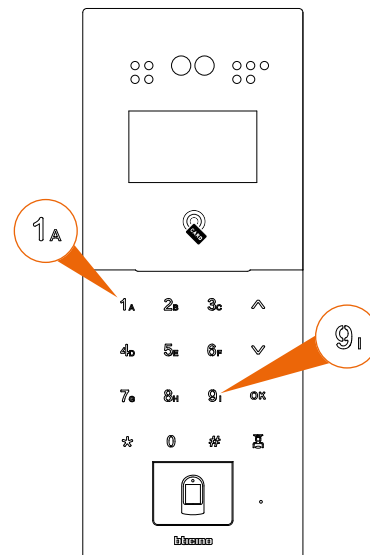
1. Click to define the type of alphanumeric call based on the EP in the system:
2. Select the type based on the devices present in the system:
 - Devices with “0-9; A-I” type keypad (available for all devices)
 - Devices with “0-9; A-Z” type keypad (not available for 374001/03)
 - Devices with “A-Z” type keypad with address book (available only for devices with touch display)

NOTE: if even one single EP has an “0-9, AI” type keypad, select the “0-9, AI” option

EP with “0-9, AZ” type keypad



EP with “0-9, AI” type keypad

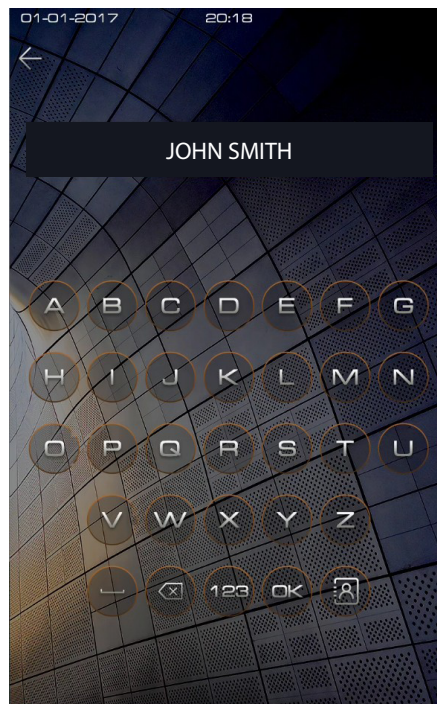


7. Enter the parameters
8. Click to confirm

By default, to call an apartment, enter the address in the community (e.g. 101010102 from an EP).
To call the apartment by entering an alias (e.g. JOHN SMITH):

- | A | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|----|------|------|--------|-------|---------|-------------|-------------|-----------|---------------|--------------|--------------|----------------|--------------|-------------|-------------|--------------|------|---|---|---|---|---|---|---|
| # | Area | Bldg | Room | Floor | Appt | Device desc | Device code | VLAN name | Interface | Serial code | Address Book | Device address | Device uid | Device name | Device type | MAC address | | | | | | | | |
| 44 | 1 | Area | 01Bldg | 1Rm | 01Floor | 01Appt | 44-4 | Lan-01 | 192.168.1.100 | 010000000002 | 01 | 192.168.1.100 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 45 | 1 | Area | 01Bldg | 1Rm | 02Floor | 01Appt | 44-5 | Lan-01 | 192.168.1.101 | 010000000002 | 01 | 192.168.1.101 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 46 | 1 | Area | 01Bldg | 1Rm | 03Floor | 01Appt | 44-6 | Lan-01 | 192.168.1.102 | 010000000002 | 01 | 192.168.1.102 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 47 | 1 | Area | 01Bldg | 1Rm | 04Floor | 01Appt | 44-7 | Lan-01 | 192.168.1.103 | 010000000002 | 01 | 192.168.1.103 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 48 | 1 | Area | 01Bldg | 1Rm | 05Floor | 01Appt | 44-8 | Lan-01 | 192.168.1.104 | 010000000002 | 01 | 192.168.1.104 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 49 | 1 | Area | 01Bldg | 1Rm | 06Floor | 01Appt | 44-9 | Lan-01 | 192.168.1.105 | 010000000002 | 01 | 192.168.1.105 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 50 | 1 | Area | 01Bldg | 1Rm | 07Floor | 01Appt | 44-10 | Lan-01 | 192.168.1.106 | 010000000002 | 01 | 192.168.1.106 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 51 | 1 | Area | 01Bldg | 1Rm | 08Floor | 01Appt | 44-11 | Lan-01 | 192.168.1.107 | 010000000002 | 01 | 192.168.1.107 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 52 | 1 | Area | 01Bldg | 1Rm | 09Floor | 01Appt | 44-12 | Lan-01 | 192.168.1.108 | 010000000002 | 01 | 192.168.1.108 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 53 | 1 | Area | 01Bldg | 1Rm | 10Floor | 01Appt | 44-13 | Lan-01 | 192.168.1.109 | 010000000002 | 01 | 192.168.1.109 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 54 | 1 | Area | 01Bldg | 1Rm | 11Floor | 01Appt | 44-14 | Lan-01 | 192.168.1.110 | 010000000002 | 01 | 192.168.1.110 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 55 | 1 | Area | 01Bldg | 1Rm | 12Floor | 01Appt | 44-15 | Lan-01 | 192.168.1.111 | 010000000002 | 01 | 192.168.1.111 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 56 | 1 | Area | 01Bldg | 1Rm | 13Floor | 01Appt | 44-16 | Lan-01 | 192.168.1.112 | 010000000002 | 01 | 192.168.1.112 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 57 | 1 | Area | 01Bldg | 1Rm | 14Floor | 01Appt | 44-17 | Lan-01 | 192.168.1.113 | 010000000002 | 01 | 192.168.1.113 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 58 | 1 | Area | 01Bldg | 1Rm | 15Floor | 01Appt | 44-18 | Lan-01 | 192.168.1.114 | 010000000002 | 01 | 192.168.1.114 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 59 | 1 | Area | 01Bldg | 1Rm | 16Floor | 01Appt | 44-19 | Lan-01 | 192.168.1.115 | 010000000002 | 01 | 192.168.1.115 | 010000000002 | 01 | Area-01 | 010000000001 | 7F00 | | | | | | | |
| 60 | 1 | Area | 01Bldg | 1Rm | 17Floor | 01Appt | 44-20 | Lan-01 | 192.168.1.116 | 010000000002 | 01 | 192.168.1.116 | 0100000000 | | | | | | | | | | | |

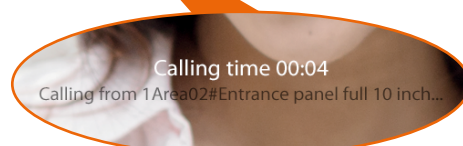
- NOTE:** The alias must be all in upper cases.



Now it is possible to use the alias JOHN SMITH to call the apartment



If the alias of an EP is changed, when receiving a call the alias will be displayed instead of the system address





4-digit call

In this mode, there are no further parameters to set

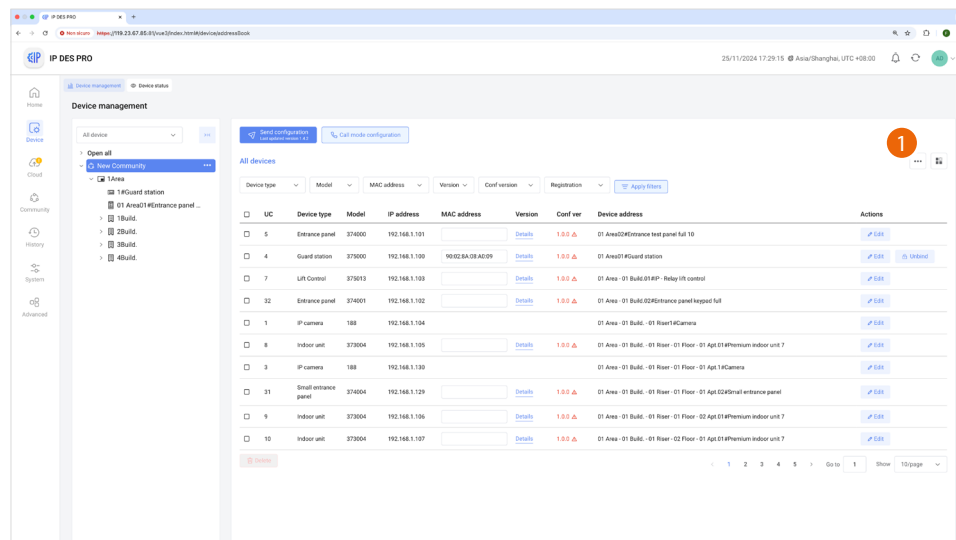
A dialog box titled "Call mode configuration" with a close button (X) in the top right corner. It contains several sections with dropdown menus:

- Call mode**: A dropdown menu showing "4 digit".
- Digit to call input**: A section with a warning icon and text: "After defining the digit to call input, you will not be able to modify it later."
- Areas**: A dropdown menu showing "2 digit".
- Buildings in a single area**: A dropdown menu showing "2 digit".
- Risers in a single building**: A dropdown menu showing "2 digit".
- Floors per riser**: A dropdown menu showing "2 digit".
- Apartments in a single floor**: A dropdown menu showing "2 digit".
- Maximum number of devices per level**: A dropdown menu showing "2 digit".

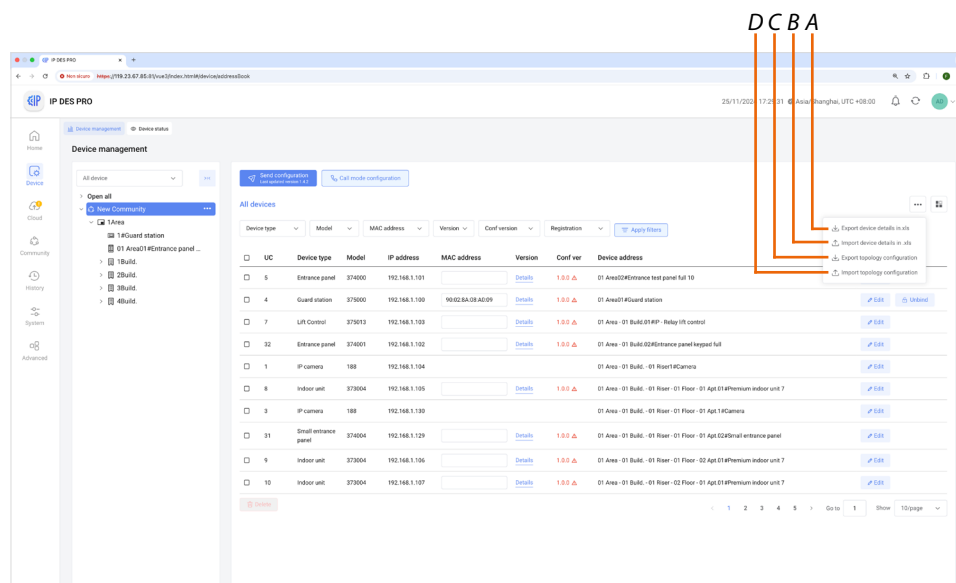
At the bottom right, there are two buttons: "Cancel" and "Confirm".

Management of project data

The data stored in the project can be imported or exported for various purposes. The data are of 2 types: device detail data and structure configuration data.



1. Touch to open the data management menu.



- A Export the device detail data in .xls format
- B Import the device detail data in .xls format
- C Export the structure configuration data in database format
- D Import the structure configuration data in database format

The file contains the characteristic data of each device. One of these data is the Alias. The Alias is a customisable alphanumeric code that replaces the community address. The alias may be of two types:

- **Alphanumeric Alias:** this type of Alias can be used on all entrance panels, internal units and guard stations.
- **Address book Alias:** this type of Alias can be used on all internal units and guard stations, but only on entrance panels with touch display.

Open

← → ↑ ↓ ↻ 🔍 This PC > Windows (C:) Search alias list

Organise ▾ New folder

Name	Date modified	Type	Size
OneDrive			
This PC			
3D Objects			
Desktop			
Documents			
Downloads			
Music			
Pictures			
1			
Windows (C:)			
Microsoft			

File name: Device_list_1639490895487.xls All Files (*.*)

2 Save Cancel

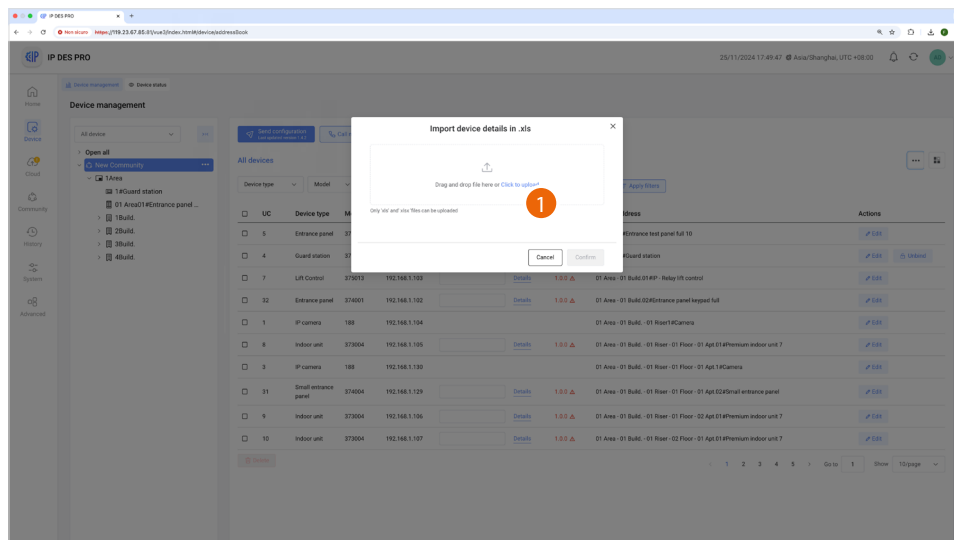
- [illegible]

67

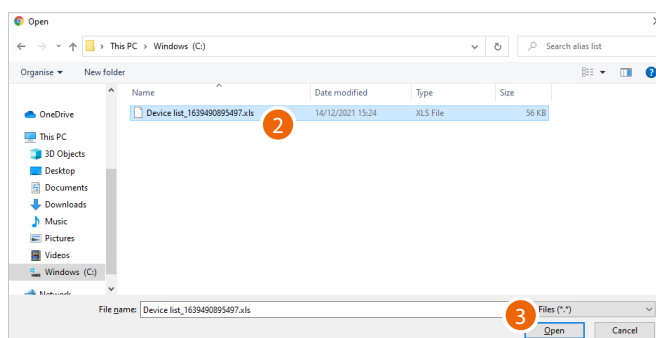
Import the device detail data

This function can be used to import device detail data previously stored in Excel® format using the **Export device list to Excel®** function.

This function is useful for **creating aliases**.

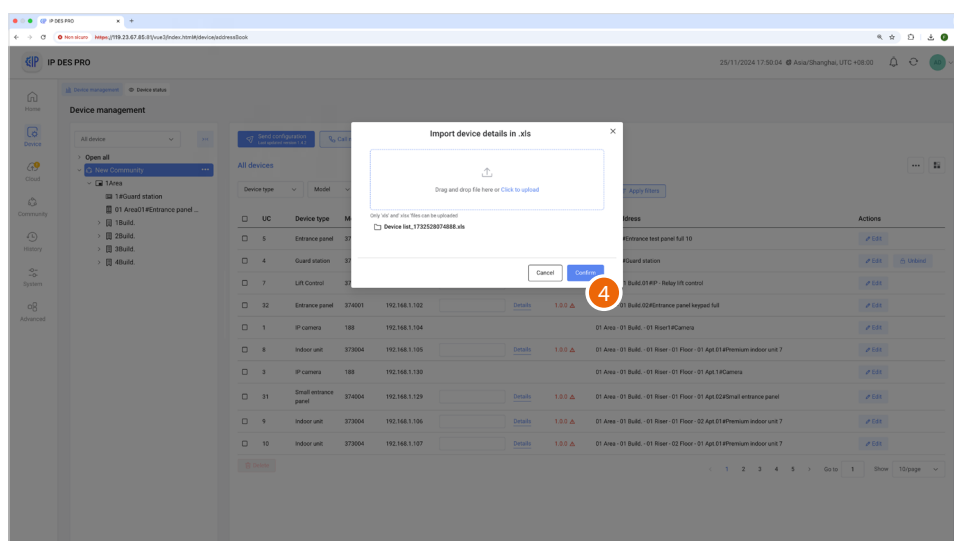


1. Click to select the Excel® file

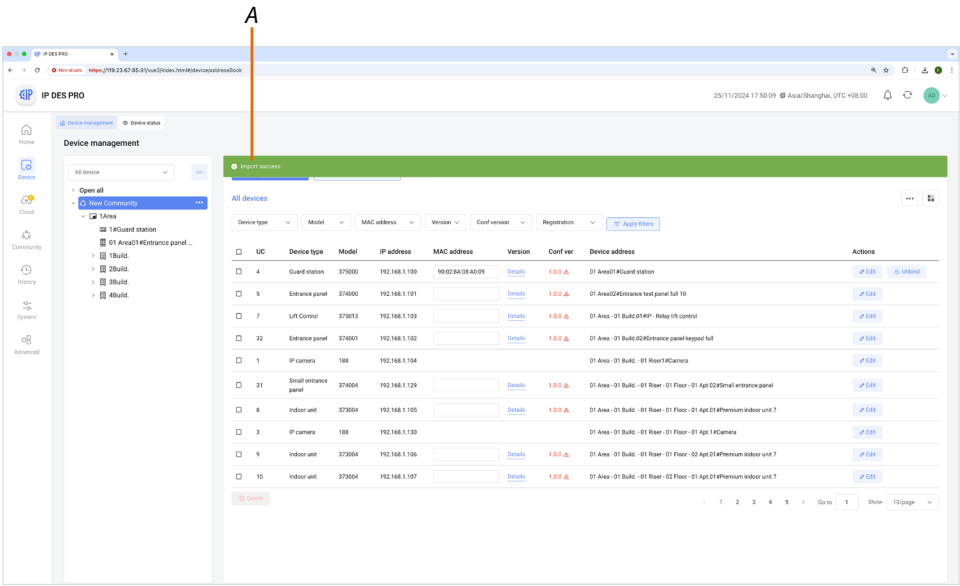


2. Select the file (.xlsx)

3. Click to open



4. Click to confirm

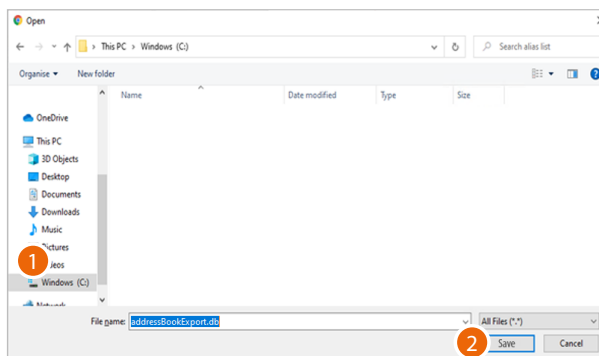


A A message indicates that the device detail data have been imported

Export configuration

This function allows to export the configuration stored in the SW.

This function can be useful in order to file a configuration for use at a later date using the [Import configuration](#) function

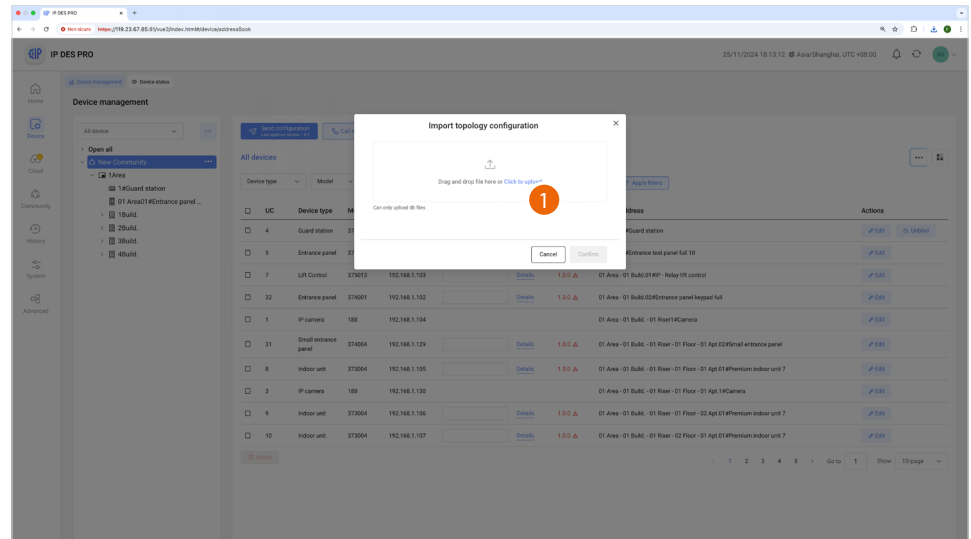


1. Select the location where to save the file (.db)
2. Click to save

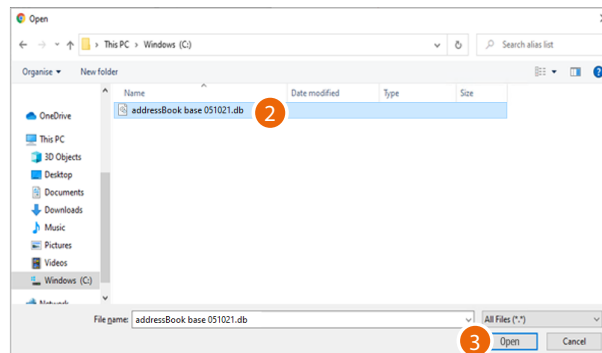
Import configuration

This function allows to import a previously saved configuration using the [Export configuration](#) function.

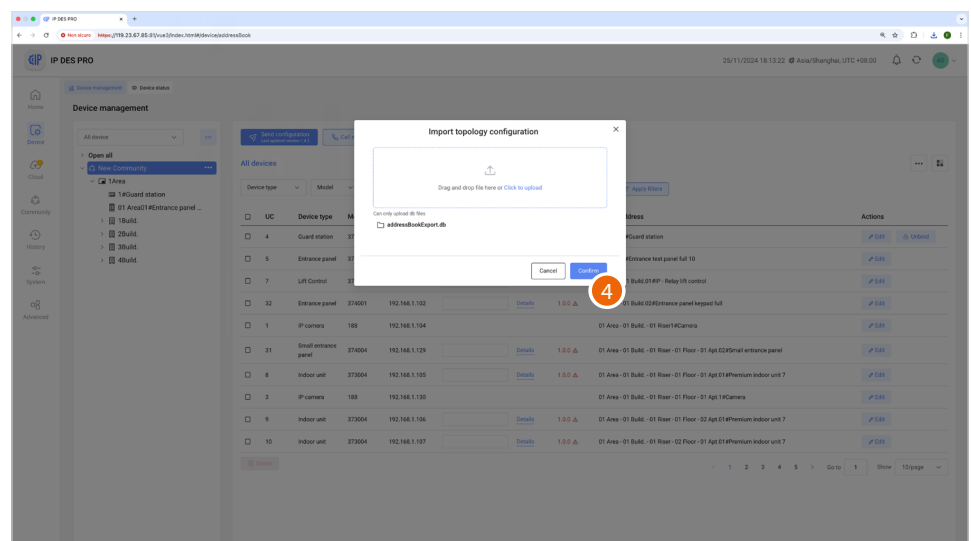
This function can be useful to start a new configuration from an existing one.



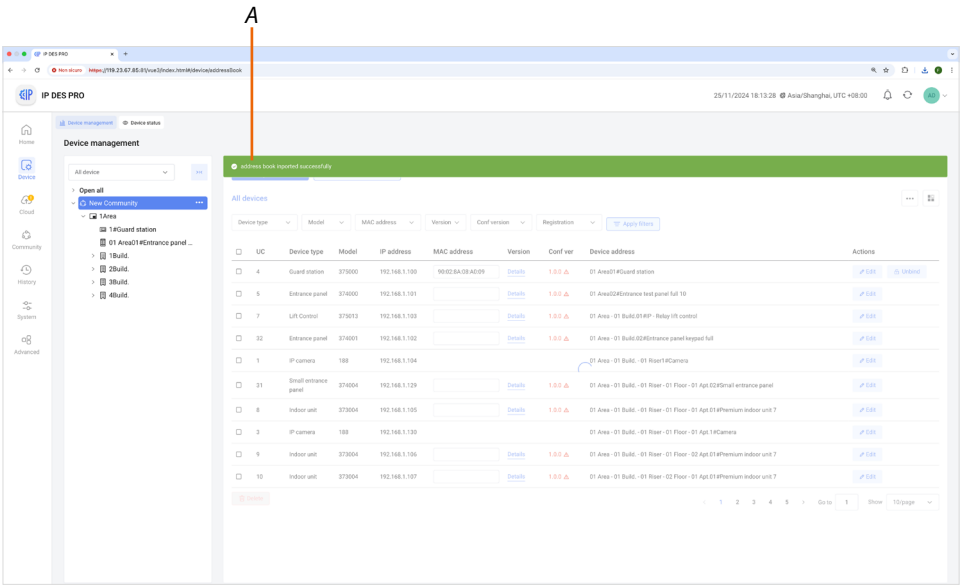
1. Click to select the AB file (.db)



2. Select the file (.db)
3. Click to open



4. Click to confirm



A A message indicates that the configuration has been imported

Devices status

This page can be used to display the device status.

For correct operation of the devices, online status is required (green colour)

UC	Device type	Model	MAC address	Device address	IP address	Last online	Last offline	Uptime	Status
1	Entrance panel keypad full	374001	90:02:8a:0c:f1:5d	01 Riser - 01#Entrance panel keypad full	192.168.2.200	15/06/2023 09:46:01		00:47 h	Online
4	Indoor unit 7 inch mirror	373007	90:02:8a:11:a8:44	01 Riser - 02#Floor - 01 Apt. 01#Indoor unit 7 inch mirror	192.168.2.352	15/06/2023 09:49:01	15/06/2023 10:49:01	01:00 h	Offline
7	Entrance panel 10 inch	374002	90:02:8a:0c:4e:4a	Entrance panel 10 inch	192.168.3.201	15/06/2023 09:46:02		00:47 h	Online
1	Entrance panel keypad full	374001	90:02:8a:0c:f1:5d	01 Riser - 01#Entrance panel keypad full	192.168.3.202	15/06/2023 09:46:01		00:47 h	Online
4	Indoor unit 7 inch mirror	373007	90:02:8a:11:a8:44	01 Riser - 02#Floor - 01 Apt. 01#Indoor unit 7 inch mirror	192.168.3.201	15/06/2023 09:49:01		00:47 h	Online
7	Entrance panel 10 inch	374002	90:02:8a:0c:4e:4a	Entrance panel 10 inch	192.168.3.201	15/06/2023 09:46:02	15/06/2023 11:16:45	01:30 h	Offline
1	Entrance panel keypad full	374001	90:02:8a:0c:f1:5d	01 Riser - 01#Entrance panel keypad full	192.168.3.204	15/06/2023 09:46:01		00:47 h	Online
4	Indoor unit 7 inch mirror	373007	90:02:8a:11:a8:44	01 Riser - 02#Floor - 01 Apt. 01#Indoor unit 7 inch mirror	192.168.3.205	15/06/2023 09:49:01		00:47 h	Online
7	Entrance panel 10 inch	374002	90:02:8a:0c:4e:4a	Entrance panel 10 inch	192.168.3.206	15/06/2023 09:46:02		00:47 h	Online
1	Entrance panel keypad full	374001	90:02:8a:0c:f1:5d	01 Riser - 01#Entrance panel keypad full	192.168.3.207	11/06/2023 09:16:01		1 week	Online

A Filters

A Progressive number

B Type of device

C Item code

D Mac address

E Name of the customisable device.

The original name represents **the address of the device in the community.**

G Device network address

H Last date/time the device was online

I Last date/time the device was offline

J Duration of online status

K Device status

L Update then data

1. Select the community branch for which you want to view the status of the devices
2. If necessary, use the filters to narrow down the selection
3. Click to apply the filter

Filters

A Type of device filter (IU, EP, etc.)

B Item code filter

C Device status filter (online/offline)

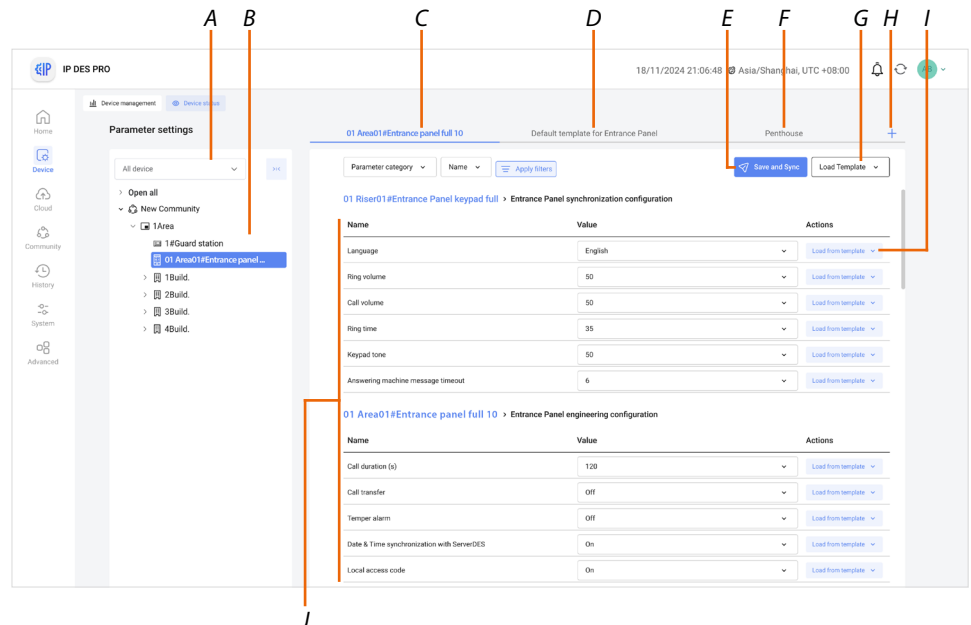
Parameter settings

This page can be used to make more advanced changes to the device parameters than the options available in the menus of the physical devices.

It is possible to change the parameters in different ways:

- Change the parameters of the **individual device**
- Change the **default parameters of all devices** of a given type

The parameters can be entered directly, or they can be loaded from a previously created **template**



A Device selection filter

B Selected device

C Open the page of the parameters of the individual device selected

D Open the page of the parameters of the default template of all the devices of a certain type

NOTE: the new added devices will use the parameters set in this page by default

E Save the changes and send the parameters to the system

F Open the parameter page of a customised template

G Upload all the parameters from a template

H Create a new template

I Load the single parameter from a template

J Device parameters

NOTE: The default and the customised templates vary depending on the device selected.

NOTE: Some described parameters are only available for certain devices.

It is possible to modify the device parameters from the fields displayed in the central area.

The parameters that can be changed depend on the type of device (see specific device tables):

- **IU** (373001/02/03/04/05/06/07/08);
- **GS** (375000);
- **EP** (374000/01/02/03 e 374005);
- **VEPO** (374004/06).

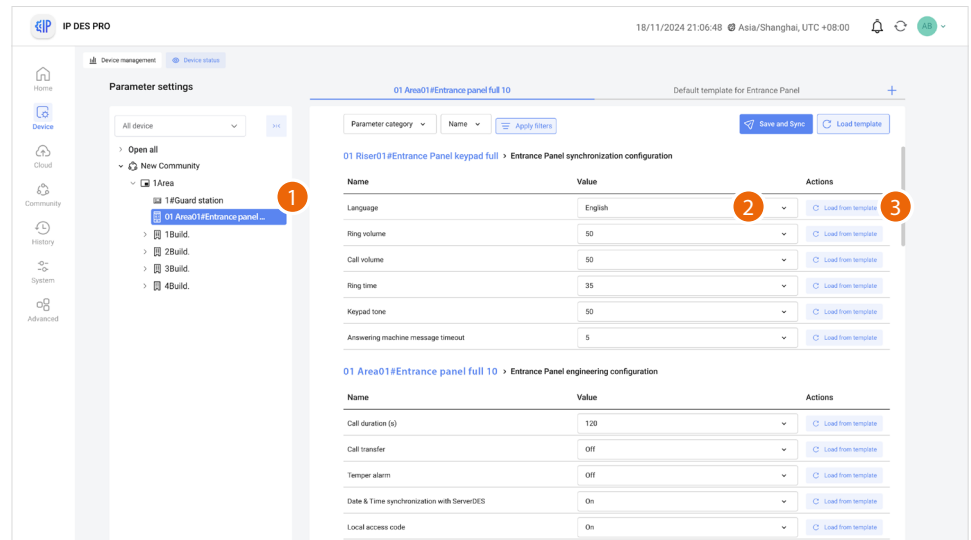
When finished, to confirm the modifications on the existing objects, it will be necessary to **send the parameters** to the physical devices.

NOTE: for safety reasons, modify the codes for accesses or for Installer menu

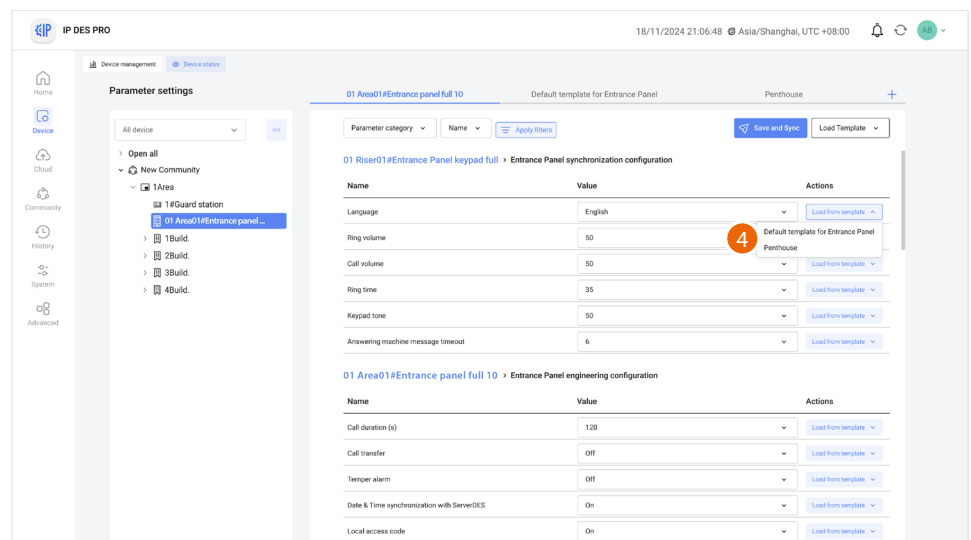
Change the individual device parameters

This page can be used to change the parameters of the individual devices selected in the tree menu.

It is possible to modify the parameters directly or use the parameters saved in the templates.



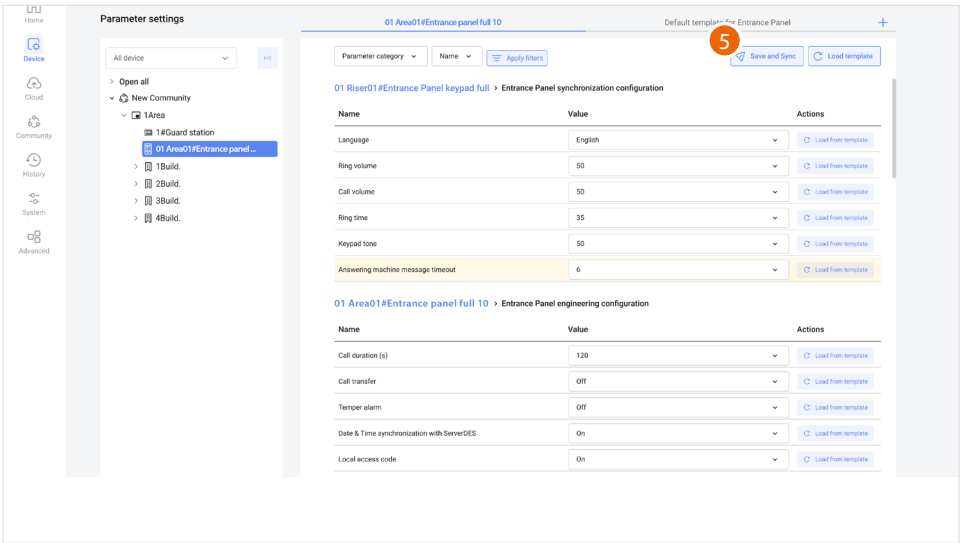
1. Select the device from the tree menu
2. Directly modify the parameter or
- Or
3. Upload the parameter value from a template



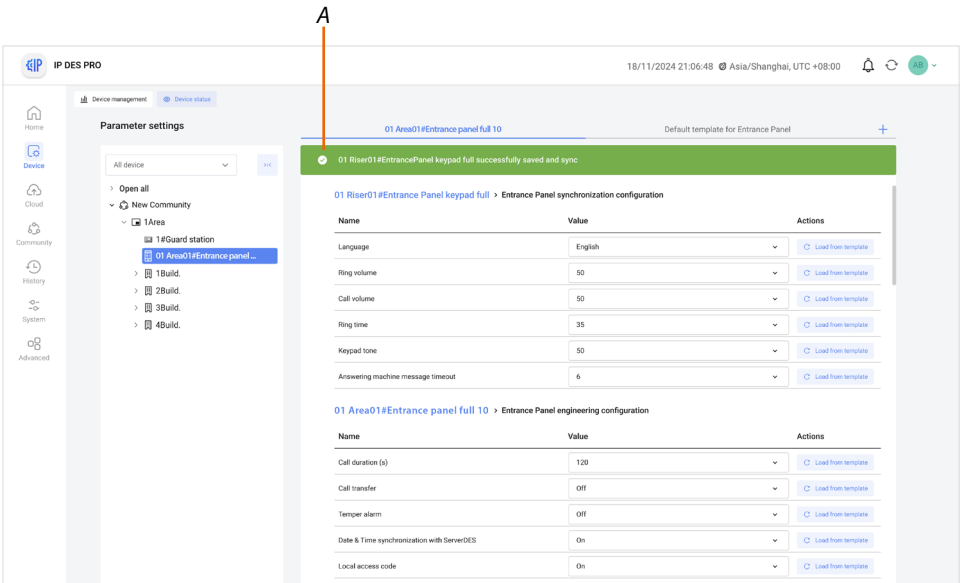
4. Define whether to load the parameter value from the default template or from a previously created specific one

GR 1 2 3 4 5 6 7 8 9 10 11 12

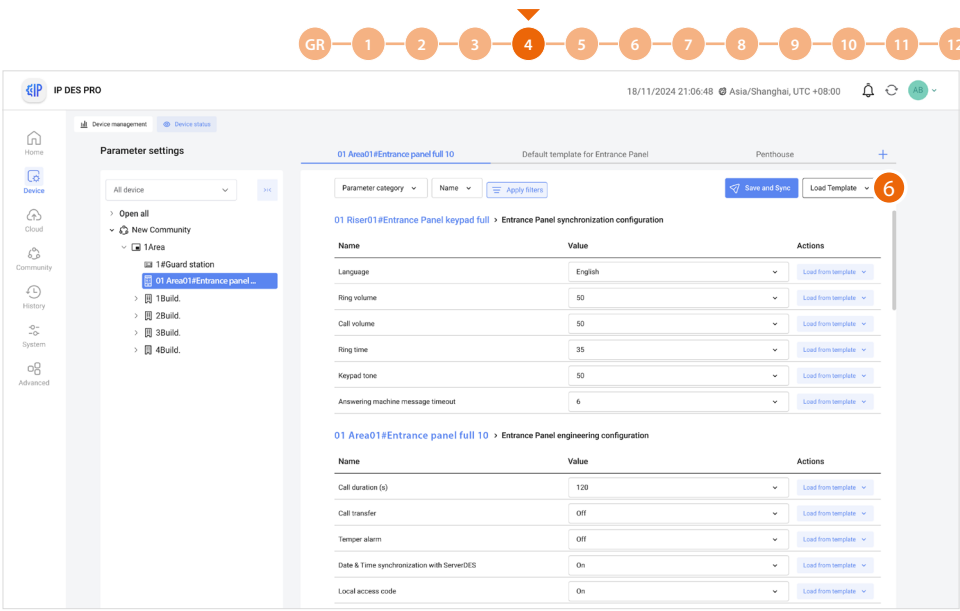
After editing/loading the new value, the line is highlighted to indicate that the device has not yet been updated



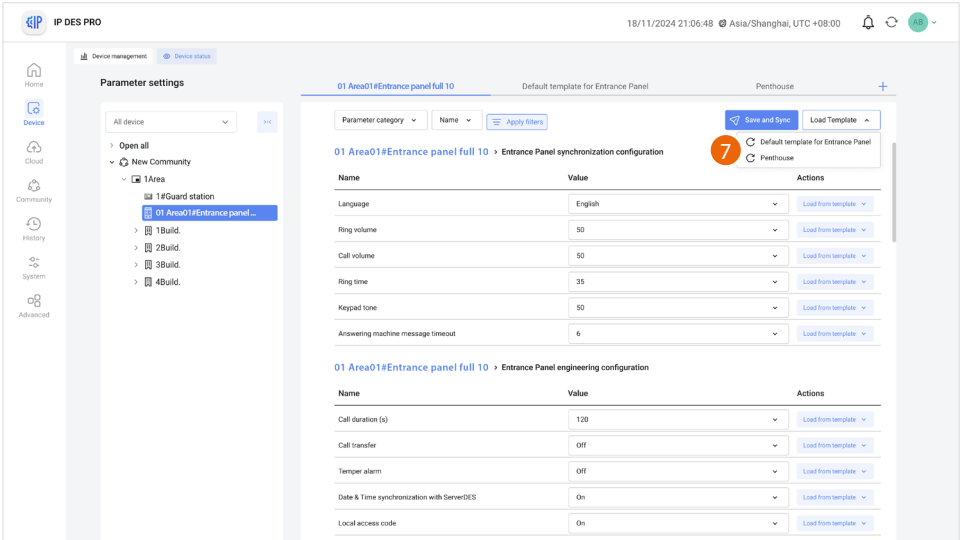
5. Click to send the configuration and synchronise the device with the new values.



A message (A) indicates successful synchronisation



6. You can also edit all the parameters simultaneously by loading them from a template



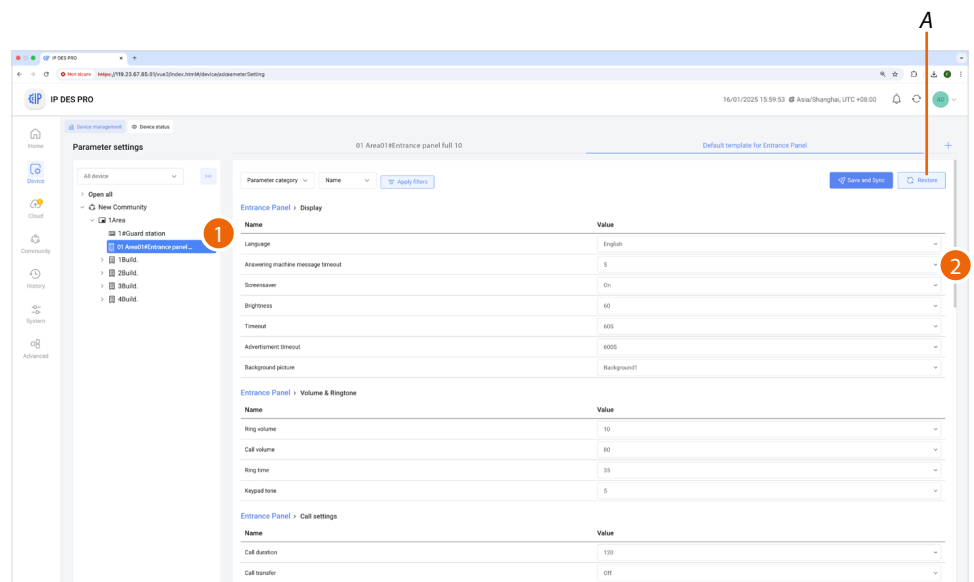
7. Define whether to load the values of all parameters from the default template or from a previously created specific one. Then save and synchronise as indicated in [step 5](#).

Changing the default parameters of all devices of a certain type

This page is shown by default and displays the template of all device parameters for devices of the same type as the one selected in the tree menu.

The values displayed are the default values. When they are changed, newly added devices will acquire the updated values.

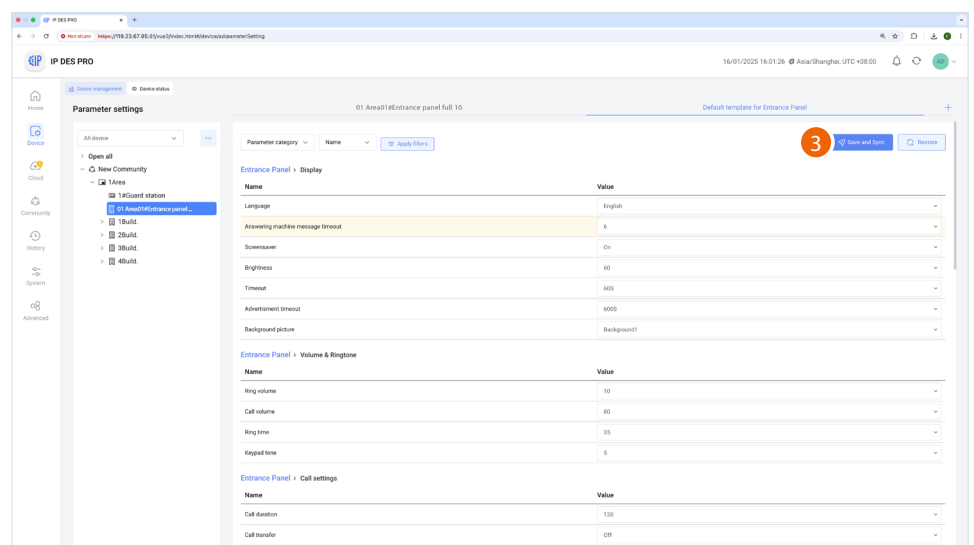
After changing the parameters, it is also possible to select whether to apply them only to certain devices or to all the devices of the same type.



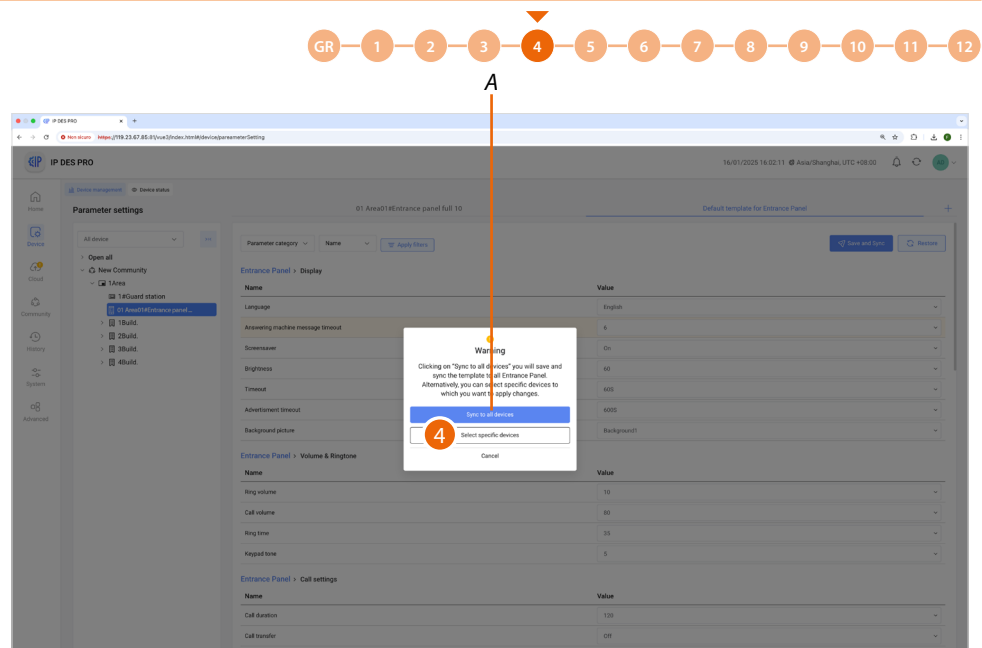
1. Select the device from the tree menu
2. Edit the parameter

CAUTION: If the new parameters set are correct, the default values can be reset by clicking the reset key (A).

After changing the new value, the line is highlighted to indicate that the device has not yet been updated



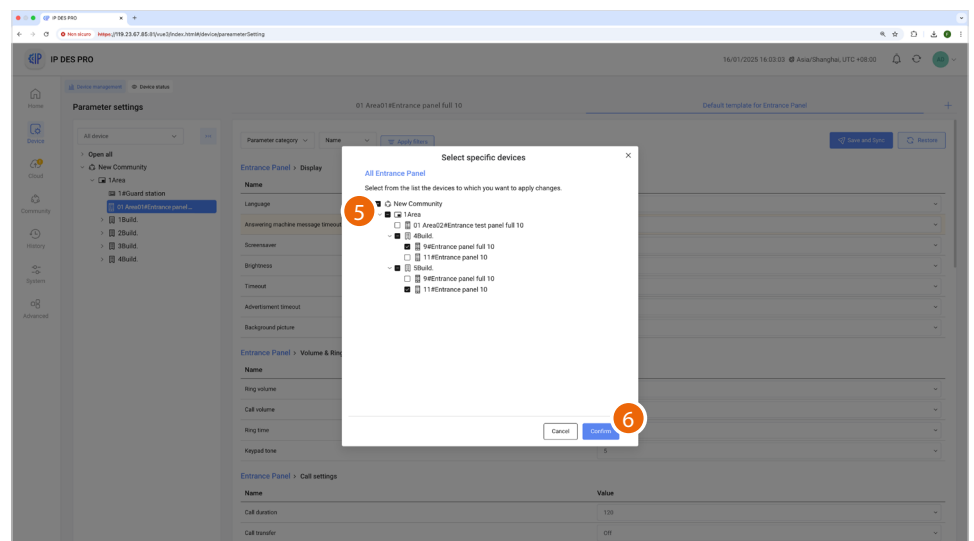
3. Click to send the configuration and synchronise the devices with the new values.



You can synchronise all the devices of the selected type (e.g. all EP) by clicking the (4) key

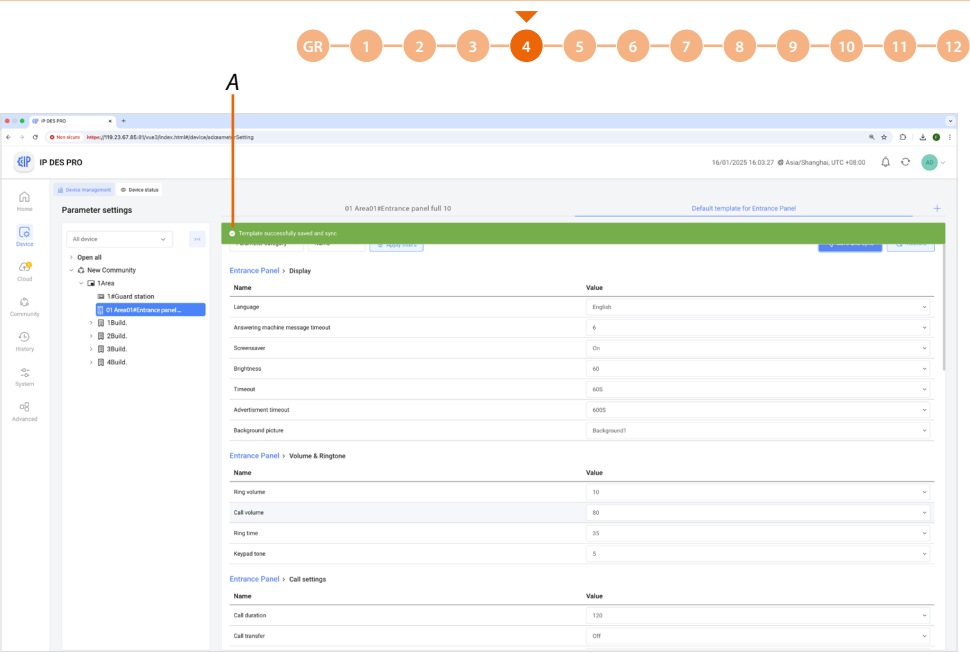
Or

4. Click to select some specific devices



5. Click to select the devices

6. Click to confirm



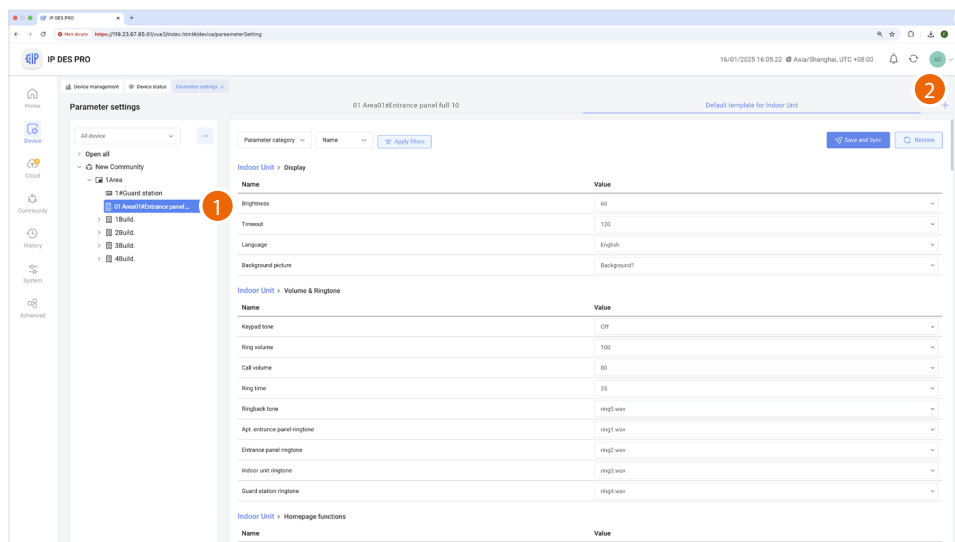
A message (A) indicates successful synchronisation

Create a new template

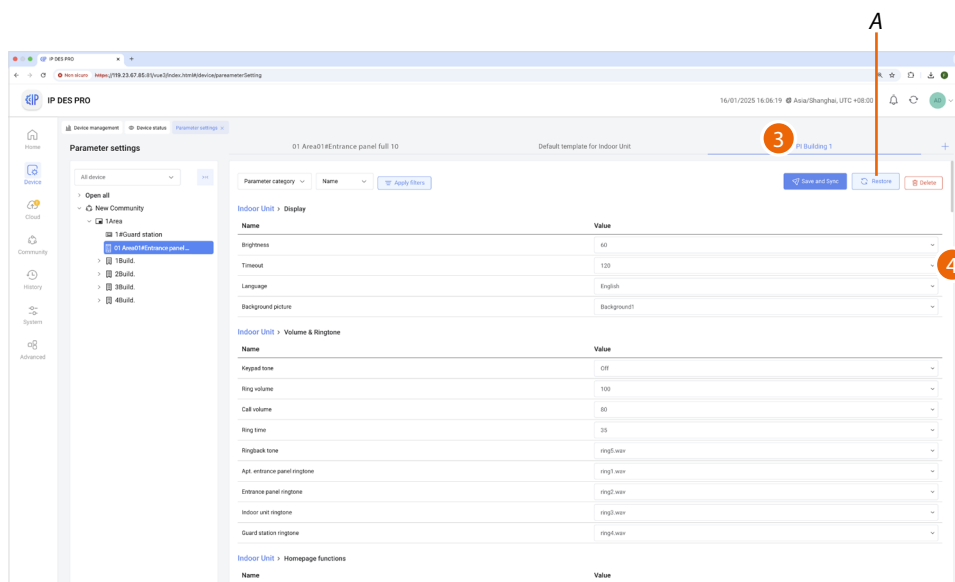
This function allows to create a new template to be used as template for configuring various devices in a similar way.

The parameter values of the new template are the default values for the selected device type. Change the values and rename the template to create a new one to be applied to other devices of the same type.

For example, create a template called "Building 1 IU", change the values of certain parameters and then apply them and the template to all the IU of Building 1.

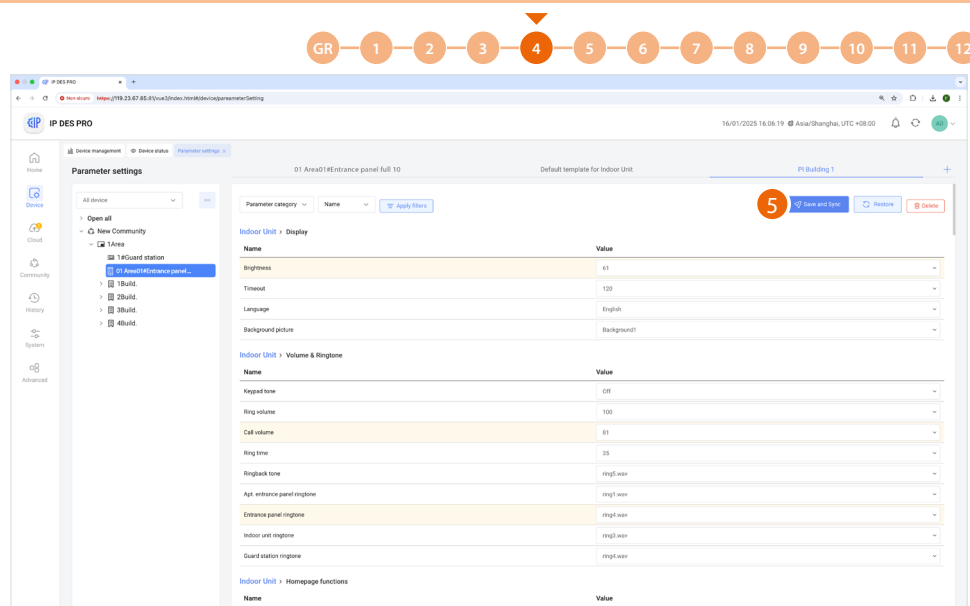


1. Select the device from the tree menu
2. Click to create a template

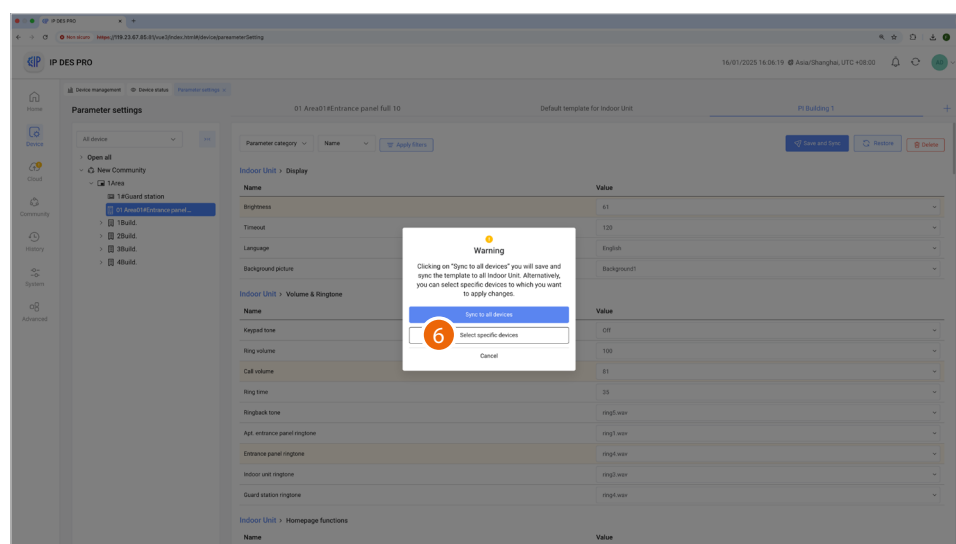


3. Click and enter a name for the template
4. Change one or more parameters

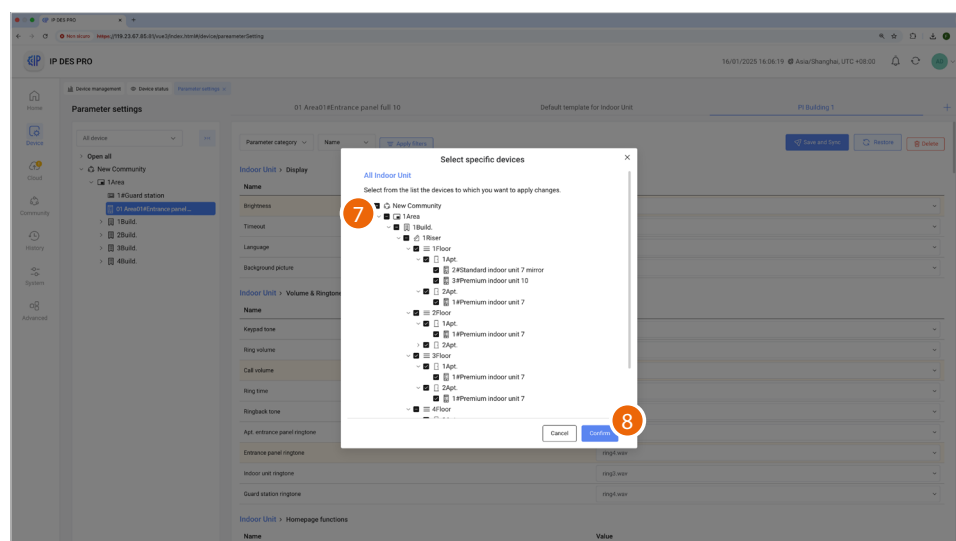
CAUTION: If the new parameters set are correct, the default values can be reset by clicking the reset key (A).



5. Click to synchronise the system devices with these parameters

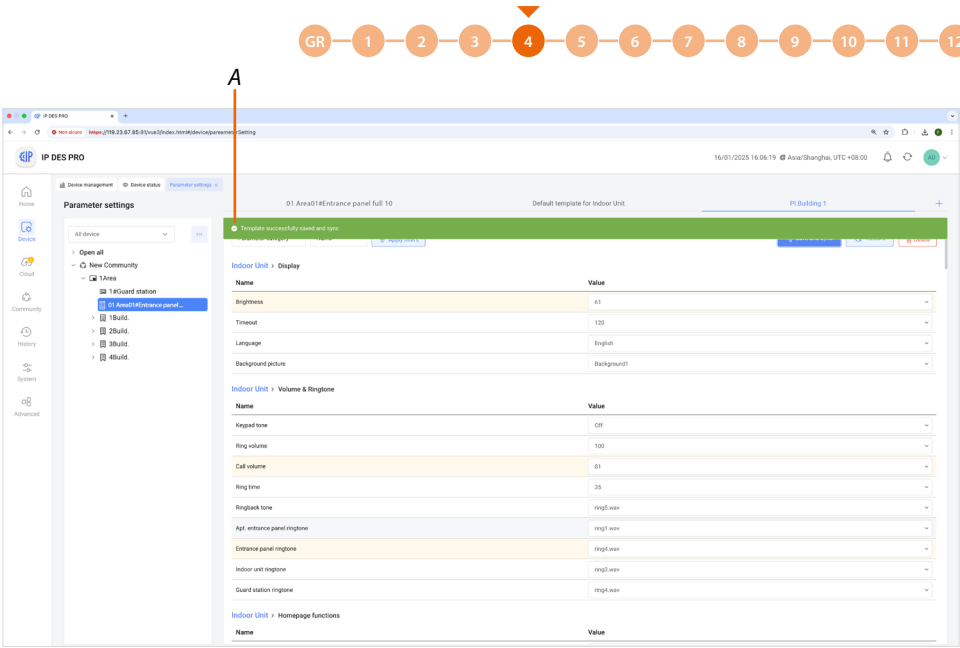


6. Click to select some devices

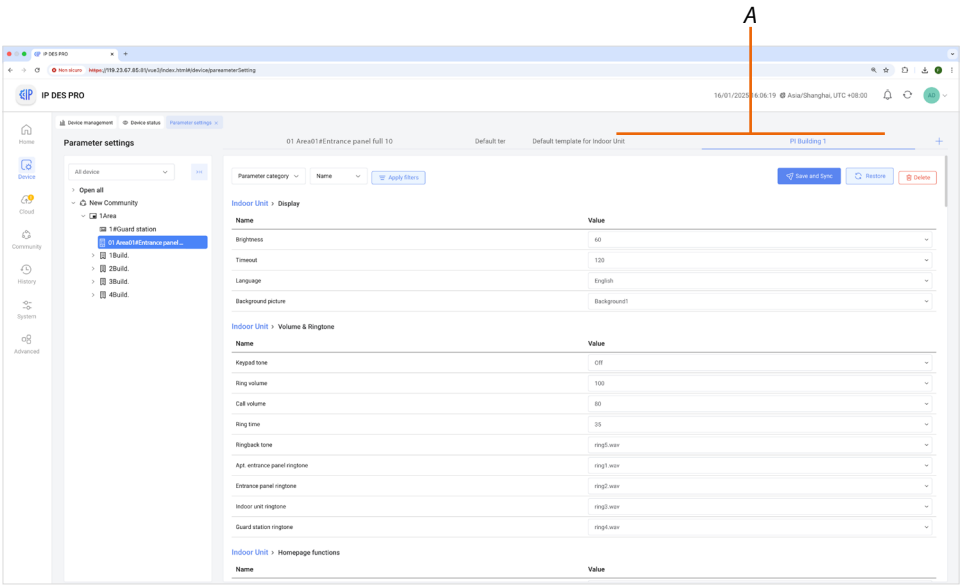


7. Select the devices (e.g.: all the IU of building 1)

8. Click to confirm



A message (A) indicates successful synchronisation



For each device type, it is possible to create various templates (A), which will remain available for later application in the **parameters page of the individual device selected**.

Device parameters

IU PARAMETERS 373001/02/03/04/05/06/07			
Parameter category	Parameter name	Function description	Position in the device menus
Display	Brightness	Set the screen brightness level	Settings/preference/display/brightness
	Timeout	Set the timeout to turn the screen off	
	Language	Select the menu language	Settings/language
	Background picture	Select the device background	Settings/preference/display/background picture
Volume & Ringtone	Keypad tone	Set the volume of the keypad tones	
	Ring volume	Set the ringtone level	Settings/preference/ringtone/ring volume
	Call volume	Set the audio level	PARAMETER THAT CAN BE ADJUSTED DURING THE CALL
	Ring time	Set the ringtone time	Settings/preference/ringtone/ring time
	Ringback tone	Select the call confirmation ringtone	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Apt. entrance panel ringtone	Select the ringtone for EP calls	Settings/ringtone/Entrance panel/ringing tone
	Entrance panel ringtone	Select the ringtone for VEPO calls	Settings/ringtone/apartment entrance panel/ringing tone
	Indoor unit ringtone	Select the ringtone for IU calls	Settings/ringtone/indoor unit/ringing tone
	Guard station ringtone	Select the ringtone for GS calls	Settings/ringtone/guard station/ringing tone
	Call section	Enable / Disable the CALL in HOMEPAGE function	Settings/Installation/function/call
	Message section	Enable / Disable the MESSAGE in HOMEPAGE function	Settings/Installation/function/message
	Camera section	Enable / Disable the CAMERA in HOMEPAGE function	Settings/Installation/function/camera
Homepage functions	Alarm section	Enable / Disable the ALARM in HOMEPAGE function	Settings/Installation/function/alarm
	Lift Control shortcut	Enable / Disable the LIFT CONTROL function in the shortcut page	Settings/Installation/function/lift
	Setting section	Enable/disable the display of the Settings on the Home page	Settings/Installation/function/Setting
	Lift control mode	Select the automatic lift call connection type and speed	Settings/lift control/mode
	Silent start time	Set the start date of the DO NOT DISTURB mode in conjunction with the time	Settings/shortcut/silent mode
	Silent end date	Set the end date of the DO NOT DISTURB mode in conjunction with the time	Settings/shortcut/silent mode
	Silent start date	Set the start time of the DO NOT DISTURB mode in conjunction with the date	Settings/shortcut/silent mode
	Silend end time	Set the end time of the DO NOT DISTURB mode in conjunction with the date	Settings/shortcut/silent mode
	Shortcut key display	Maximum number of shortcuts available on the homepage	PARAMETER THAT CANNOT BE SET FROM THE DEVICE

CONTINUE ➔

IU PARAMETERS 373001/02/03/04/05/06/07			
Parameter category	Parameter name	Function description	Position in the device menus
App	App enable	Enable / disable the connection with the app	Settings/Installation/Function/App
	Monitor entrance panel	Enable/disable entrance panel monitoring from the app	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	App Ice Transport Policy	Default is "All" other options to solve issues in H+S streaming	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
Call settings	Answering machine	Enable / Disable I Video door entry answering machine	Settings/Installation/Function/Voice mail
	Call apt.	Enable / Disable the display of the ENTRANCE PANEL in the room page	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Block all intercoms	Enable / disable call block for all IU	Call/Blacklist/Block all the intercom
	Blacklist	Enable/disable blacklist display on the call-page	Settings/Installation/function/Blacklist
	Video intercom	Enable / disable the video internal unit camera	Settings/Preferences/function/local camera
	Call duration	Set the conversation time	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
Message section details	Advertisement	Enable / Disable the display of incoming advertising information from the Guard Station	Settings/Installation/function/advert
	Community message	Enable / Disable the display of service information from the software	Settings/Installation/function/community message
	Access history	Enable / Disable the display of entrance access information	Settings/Installation/function/access message
	Family message	Enable / Disable the display of messages from family members	Settings/Installation/function/family message
	Emergency message	Enable / Disable the display of incoming emergency information from the software	Settings/Installation/function/emergency message
Cameras section details	Common area cameras	Enable / Disable the display of the COMMON AREA in the room page	Settings/Installation/function/common area
Advanced alarm settings	Alarm history	Enable / Disable the display of the alarm log	Settings/Installation/function/alarm message
	Start day time	Set the start time of the daytime period for the CHECK ACTIVITY function	Settings/Installation/alarm setting/advanced/day time
	Start night time	Set the start time of the night time period for the CHECK ACTIVITY function	Settings/Installation/alarm setting/advanced/day time
	Day time	Set the time during which the CHECK ACTIVITY function indicates an alarm in case of non-detection in the daytime period	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Night time	Set the time during which the CHECK ACTIVITY function indicates an alarm in case of non-detection in the night time period	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Zone vandalism	Set the type of alarm detection (from F1 to F8), which can be of two types	Settings/Installation/alarm setting/Zone vandalism

CONTINUE ➔

*see the "make the password visible" procedure

IU PARAMETERS 373001/02/03/04/05/06/07

Parameter category	Parameter name	Function description	Position in the device menus
Zone 1/8 alarm	Sensor type	Select the type of sensor based on the device	Settings/Installation/alarm setting/edit alarm zone/sensor type
	Sensor status	Enable / Disable the terminal block input for the sensor	Settings/Installation/alarm setting/edit alarm zone/sensor enable
	Normally Open/ Closed	Select the sensor input status	Settings/Installation/alarm setting/edit alarm zone/normally open
	Activation mode	The sensor is always active and the alarm is given at a certain time after the triggering condition occurs	Settings/Installation/allarm setting/edit allarm zone/activation mode
		The alarm is given at a certain time after the triggering condition occurs (set the value in alarm delay). The alarm is given at a certain time after the user gives the command (set the value in arming delay)	
		The alarm is immediately communicated	
		The alarm is communicated immediately, if the sensor does not detect activities for a preset time	
		Scheduled activation	
	Alarm delay	Set the alarm notification delay (see the IU manual)	Settings/Installation/allarm setting/edit allarm zone/activation mode/alarm delay
	Arming delay	Set the alarm activation delay (see the IU manual)	Settings/Installation/allarm setting/edit allarm zone/activation mode/alarm delay
Others	Notification on IU	Enable or disable the sound trigger in case of alarm	Settings/Installation/allarm setting/edit allarm zone/local notifications
	Zone name	Set the sensor name	Settings/Installation/allarm setting/edit allarm zone/alarm zone name
	Scheduled alarm start time	Set the scheduled alarm start time	Settings/Installation/allarm setting/edit allarm zone/activation mode/scheduled
	Scheduled alarm end time	Set the scheduled alarm end time	Settings/Installation/allarm setting/edit allarm zone/activation mode/scheduled
	Installer password	Set the password to access the installer menu.*	Settings/Installation/installation access code
	SOS	Enable / Disable the SOS GND input in the alarm terminal block	Settings/Installation/alarm setting/advanced/SOS enable
	SOS switch status	Set the status of the SOS GND input in the alarm terminal block	Settings/Installation/alarm setting/advanced/open normally
	SOS vandal mode	Set if the SOS GND input in the alarm terminal block checks for short circuits and wire cuts in addition to the alarm signal	Settings/Installation/alarm setting/advanced/SOS vandalism
	Low voltage alarm	Enable/disable the alarm when power supply is insufficient?	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Alarm code	Set the password for the management and configuration of the alarms*	Settings/Access code/alarm password
	Tamper alarm	Enable/disable the alarm in case of physical removal of the part	Settings/Installation/Function/Tamper

*see the "make the password visible" procedure

GS PARAMETERS 375000

Parameter category	Parameter name	Function description	Position in the device menus
Display	Brightness	Set the screen brightness level	Settings/preference/display/brightness
	Timeout	Set the timeout seconds to turn off the screen	Settings/preference/display/screensaver
	Language	Select the menu language	Settings/language
	Background picture	Select the device background	Settings/preference/display/background picture
	Ring volume	Set the ringtone level	Settings/preference/ringtone/ring volume
	Call volume	Set the audio level	PARAMETER THAT CAN BE ADJUSTED DURING THE CALL
	Ring time	Set the ringtone time	Settings/preference/ringtone/ring time
	Apt. entrance panel ringtone	Select the ringtone for EP calls	Settings/ringtone/Entrance panel/ringing tone
	Entrance panel ringtone	Select the ringtone for VEPO calls	Settings/ringtone/apartment entrance panel/ringing tone
	Indoor unit ringtone	Select the ringtone for IU calls	Settings/ringtone/indoor unit/ringing tone
	Guard station ringtone	Select the ringtone for GS calls	Settings/ringtone/guard station/ringing tone
	Call transfer mode	Select the absence mode	Settings/absence settings/scheduled absence
Transfer call setting	No answer transfer delay	Set the time after which to transfer the unanswered call	Settings/transfer settings/no answer time
	The target guard station for transfer	Select the guard station to which to transfer the calls	Settings/absence settings/scheduled Absence
Absence setting	Quick absence	Enable/disable the "Quick Absence" function	Settings/absence settings/scheduled Absence
Others	Installer password	Set the password to access the installer menu.*	Settings/Installation/installation access code

*see the "make the password visible" procedure

EP PARAMETERS 374000/01/02/03			
Parameter category	Parameter name	Function description	Position in the device menus
Display	Language	Select the menu language	Settings/language
	Answering machine message timeout	Duration of the message left on the video door entry system answering machine	Settings/display & volume/Leave message wait
	Screensaver	Enables/disables the screen saver	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Brightness	Set the screen brightness level	Settings/display & volume/brightness
	Timeout	Set the screen timeout	
	Advertisement timeout	Set the display advertising timeout (10" display only)	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
Volume & Ringtone	Background picture	Select the display background	Settings/background
	Ring volume	Set the ringtone level	Settings/display & volume/ringtone
	Call volume	Set the audio level	Settings/display & volume/call
	Ring time	Set the call time duration	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
Call settings	Keypad tone	Set the display icon/key pressing confirmation sound level	Settings/display & volume/key tone
	Call duration	Set the conversation time	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Call transfer	Enable/Disable forwarding of calls	Settings/setting/tamper alarm enable
Panel Access code	Call to Guard station	Select the guard station to be called with the dedicated pushbutton	Settings/Guard station
	Enable gate code	enable/disable the opening of the door using a code	Settings/Local access code
Access settings	Gate code	Enter a code for releasing the door lock	Settings/Gate code
	Proximity sensor	Enable/Disable the proximity sensor	Settings/setting/proximity sensor enable
	Lock status	Select the door lock status (NO/NC/not used)	Settings/door lock/door status
	Electric lock mode	Select if contact closure is impulsive or maintained	Settings/door lock/door lock
	Lock activation time	Select the time during which the contact is maintained	Settings/door lock/unlock time
	Face recognition	Enable/Disable the face recognition**	Settings/setting/face enable

CONTINUE ➔

*see the "make the password visible" procedure

**NOTE: La funzione Riconoscimento facciale è disponibile solo con la chiave USB di abilitazione 375011 da acquistare separatamente. La chiave USB deve essere collegata permanentemente al SD

EP PARAMETERS 374000/01/02/03

Parameter category	Parameter name	Function description	Position in the device menus
Face Recognition	Face recognition mode	Select the face recognition mode	Settings/Face settings
	Sensitivity threshold	*Sets the level of face recognition accuracy	Settings/Face settings
	Recognition distance	Set the distance from which facial recognition is activated	Settings/Face settings
	Recognition points	Select the number of facial recognition reference points	
	Quality	Select the image quality	
	Face angle yaw	Maximum angle of face rotation	Settings/Face settings
	Face angle pitch	Maximum angle of left/right face inclination	
	Face angle roll	Maximum angle of up/down face inclination	
	Induction time setting	Time to start face recognition when the screen turns on	Settings/Face settings
	Proximity sensing distance	Set the proximity sensor activation distance	Settings/Face settings
Lift control	Lift control	Enable / Disable the automatic lift call	Settings/setting/lift control enable
	Lift control mode	Select the automatic lift call connection type and speed	Settings/lift control/mode
	Lowest Floor	Set the lowest structure floor level that can be reached by the lift	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Number of lifts	Set the number of lifts to manage	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Floor Number	Set the number of floors	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Entrance panel IP address for lift control connection	Set the number of the Master entrance panel for the automatic lift call function	Settings/lift control/mode/network/master IP
Others	Low voltage alarm	Enable/disable the alarm when power supply is insufficient?	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Tamper alarm	Enable/Disable the tamper function	Settings/setting/call forwarding enable
	Date & Time synchronization with ServerDES	Enable / disable automatic synchronisation of date and time with the SD	Settings/date and time/automatically sync date and time
	Installer password	Set the password to access the installer menu.*	Settings/access code/settings

NOTE: In case of several entrance panels in the system, those not controlling the lift must have the "Lift control" parameter set to "Off"

*see the "make the password visible" procedure

****NOTE:** The Face recognition function is only available with USB enable stick 375011, to be purchased separately. The USB stick must be permanently connected to the SD

VEPO PARAMETERS 374004/05/06

Parameter category	Parameter name	Function description	Position in the device menus
Display	Language	Select the menu language	Settings/language
	Answering machine message timeout	Duration of the message left on the video door entry system answering machine	Settings/display & volume/Leave message wait
	Screensaver	Enable/disable the screen saver (only for 374005)	
	Brightness	Set the screen brightness level	Settings/display & volume/brightness
	Timeout	Set the screen timeout (only for 374005)	
	Advertisement timeout	Set the display advertising timeout (374005 display only)	
	Background picture	Select the display background	Settings/background
Volume & Ringtone	Ring volume	Set the ringtone level	Settings/display & volume/ringtone
	Call volume	Set the audio level	Settings/display & volume/call
	Ring time	Set the call time duration	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Keypad tone	Set the display icon/key pressing confirmation sound level	Settings/display & volume/key tone
Call settings	Call duration	Set the conversation time	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Call transfer	Enable/Disable forwarding of calls	Settings/setting/tamper alarm enable
	Call to Guard station	Select the guard station to be called with the dedicated pushbutton	Settings/Guard station
	Gate code	Enter a code for releasing the door lock	Settings/Gate code
Access settings	Proximity sensor	Enable/Disable the proximity sensor	Settings/setting/proximity sensor enable
	Lock status	Select the door lock status (NO/NC/not used)	Settings/door lock/door status
	Electric lock mode	Select if contact closure is impulsive or maintained	Settings/door lock/door lock
	Lock activation time	Select the time during which the contact is maintained	Settings/door lock/unlock time
	Face recognition	Enable/Disable the face recognition**	Settings/setting/face enable
Face Recognition	Face recognition mode	Select the face recognition mode	Settings/Face settings
	Sensitivity threshold	*Sets the level of face recognition accuracy	Settings/Face settings
	Recognition distance	Set the distance from which facial recognition is activated	Settings/Face settings
	Recognition points	Select the number of facial recognition reference points	
	Quality	Select the image quality	Settings/Face settings
	Face angle yaw	Maximum angle of face rotation	
	Face angle pitch	Maximum angle of left/right face inclination	
	Face angle roll	Maximum angle of up/down face inclination	
	Induction time setting	Time to start face recognition when the screen turns on	Settings/Face settings
	Proximity sensing distance	Set the proximity sensor activation distance	Settings/Face settings

VEPO PARAMETERS 374004/05/06

Parameter category	Parameter name	Function description	Position in the device menus
Lift control	Lift control	Enable / Disable the automatic lift call	Settings/setting/lift control enable
	Lift control mode	Select the automatic lift call connection type and speed	Settings/lift control/mode
	Lowest Floor	Set the lowest structure floor level that can be reached by the lift	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Number of lifts	Set the number of lifts to manage	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Floor Number	Set the number of floors	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Entrance panel IP address for lift control connection	Set the number of the Master entrance panel for the automatic lift call function	Settings/lift control/mode/network/master IP
Others	Low voltage alarm	Enable/disable the alarm when power supply is insufficient	PARAMETER THAT CANNOT BE SET FROM THE DEVICE
	Tamper alarm	Enable/Disable the tamper function	Settings/setting/call forwarding enable
	Date & Time synchronization with ServerDES	Enable / disable automatic synchronisation of date and time with the SD	Settings/date and time/automatically sinc date and time
	Installer password	Set the password to access the installer menu.*	Settings/access code/settings
Direct call to other IU (only for 374004 / 06)	Indoor unit Area	Set the address of the IU to call	FUNCTION NOT AVAILABLE
	Indoor unit Build		
	Indoor unit Riser		
	Indoor unit Floor		
	Indoor unit Apt.		

*see the "make the password visible" procedure

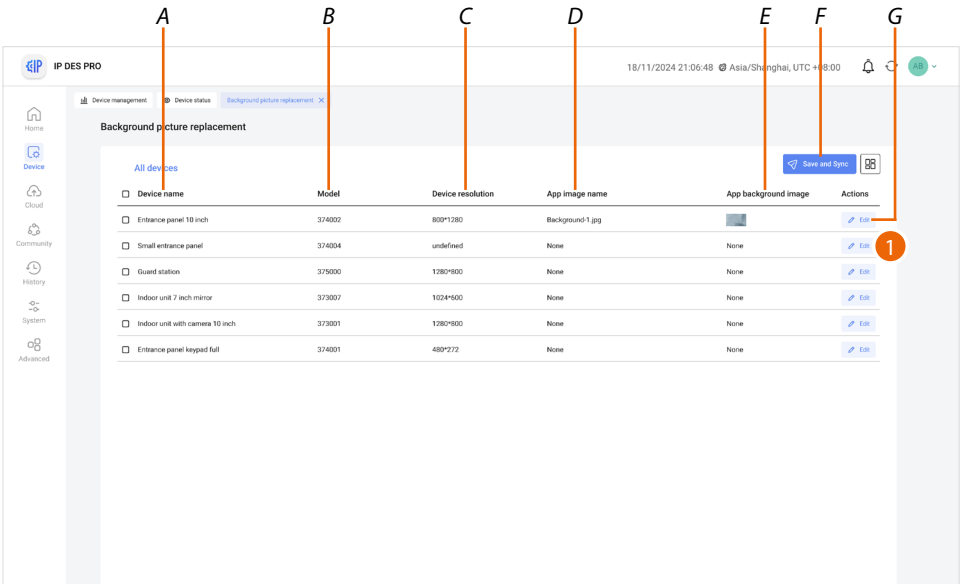
**NOTE: The Face recognition function is only available with USB enable stick 375011, to be purchased separately. The USB stick must be permanently connected to the SD

Background picture replacement

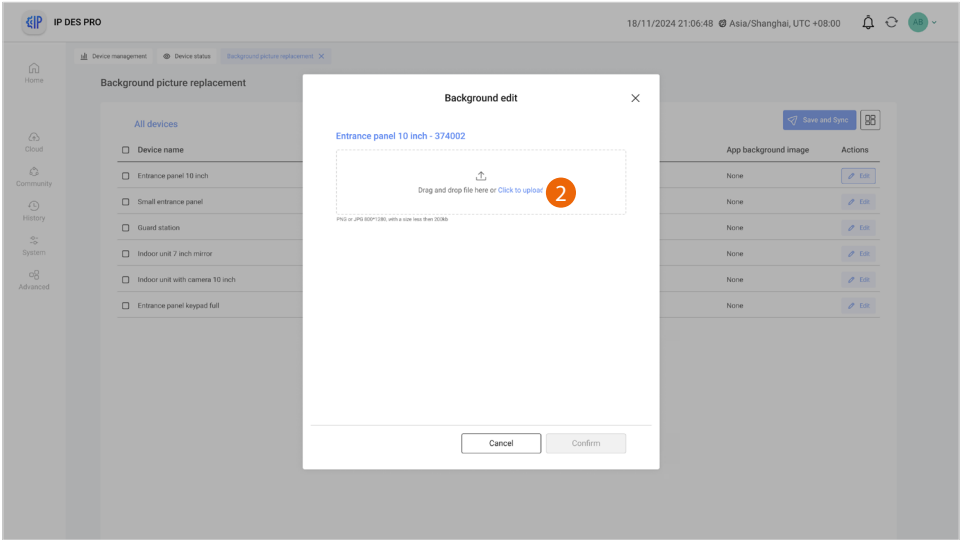
This page can be used to set the Home Page background of the devices.

The imported image will remain available on the device, in addition to the default images.

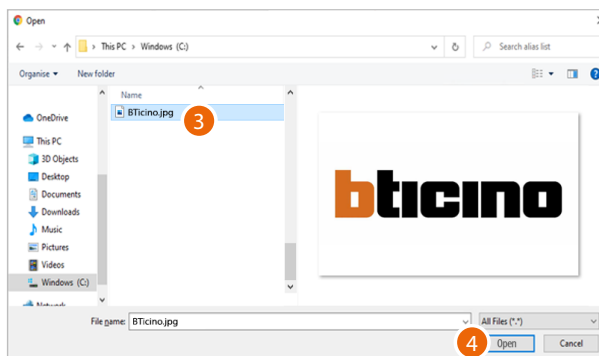
This function is only available for registered devices.



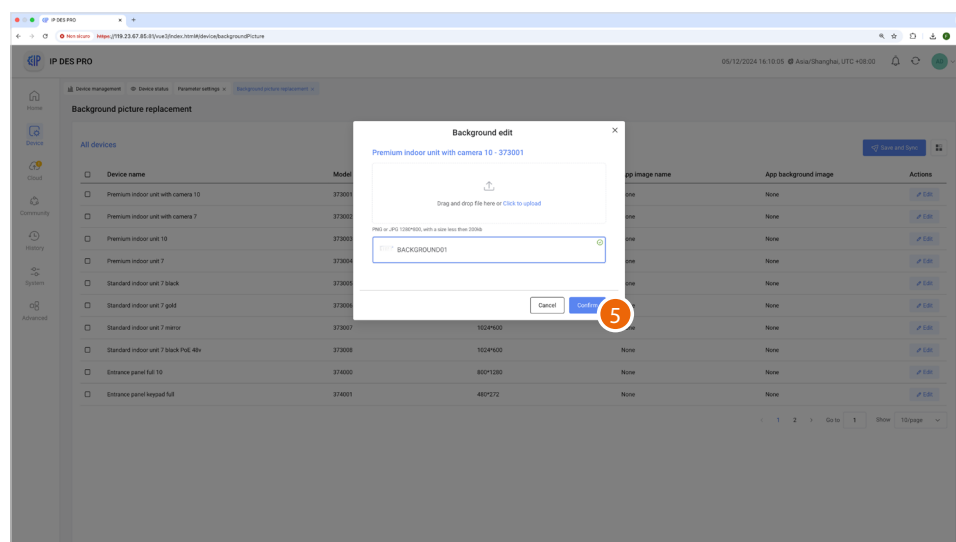
- A Type of device
 - B Item code
 - C Size of background image to be imported
 - D Image name
 - E Image preview
 - F Sends images to device
 - G Opens the image loading panel
1. Click to open the image loading panel



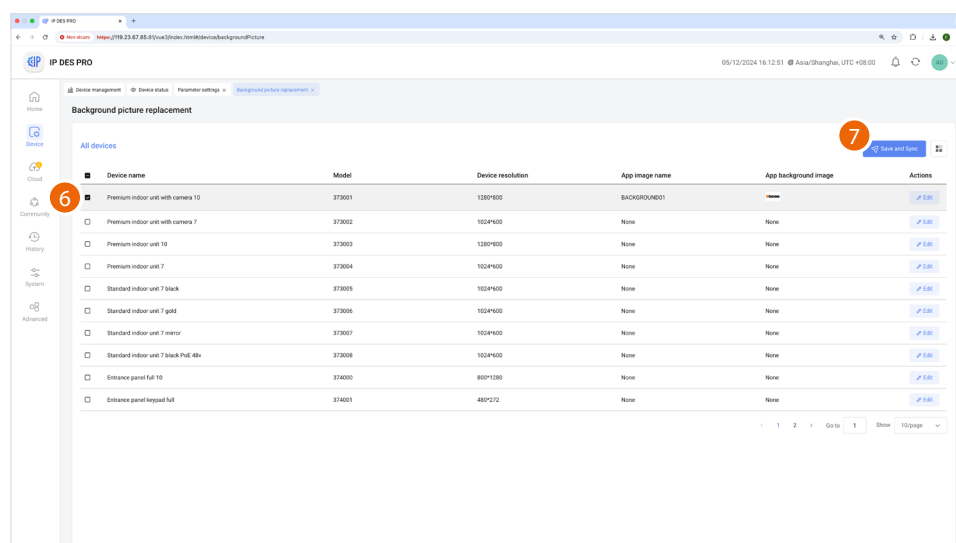
2. Click to select an image



3. Select the image that meets the characteristics
4. Click to load the image

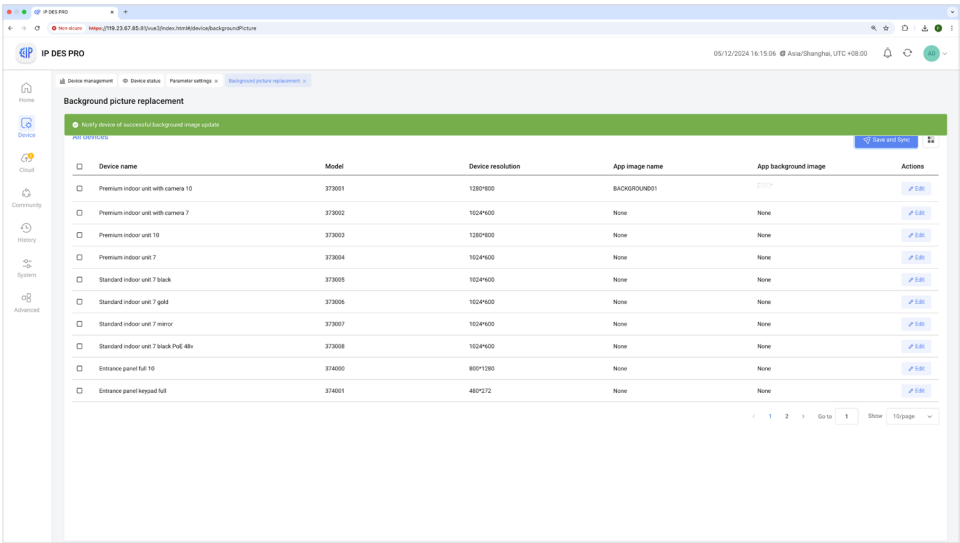


5. Click to confirm



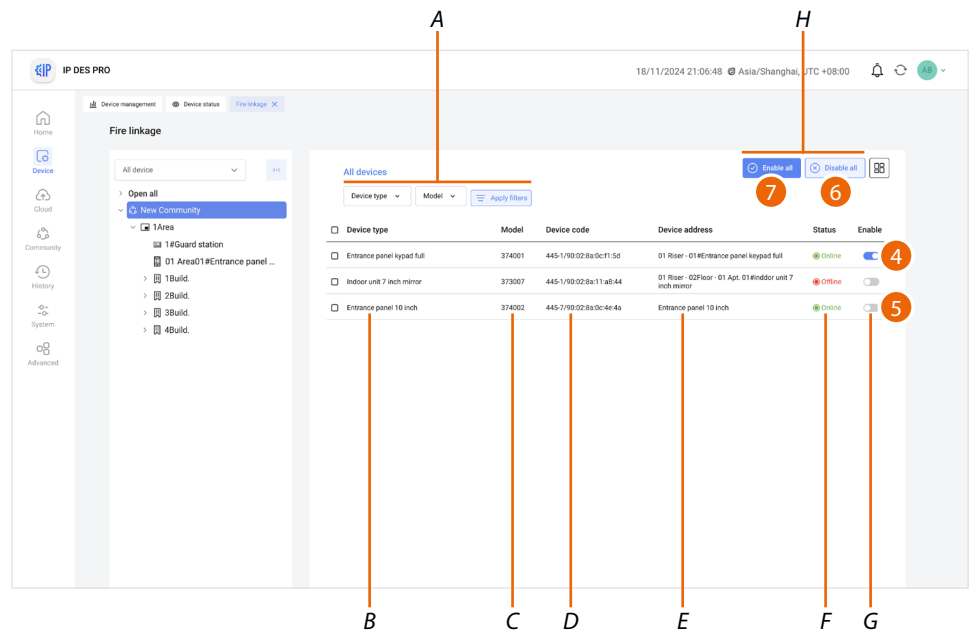
6. Select the device to which to send the previously selected image
7. Click to send

The image will now be the active background of the device and will remain available in the corresponding menu.



Fire linkage

On this page, you can use the Fire linkage function to enable the opening of the locks of the EP of the community in the event of a fire.
The use of this function requires a clean contact in the GND Fire linkage input clamp from the fire fighting system.



- A **Filters**
- B *Type of device*
- C *Item code*
- D *Mac address*
- E *Name of the customisable device.*
*The original name represents **the address of the device in the community.***
- F *Device status (online/ offline)*
- G *Single device on/off key (online devices only)*
- H *On/off keys for all devices*

For the single device:

- 4. Click to deactivate the Fire linkage function
- 5. Click to activate the Fire linkage function:

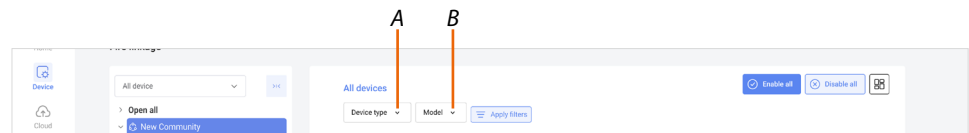
For all devices:

- 6. Click to deactivate the Fire linkage function
- 7. Click to activate the Fire linkage function



- 8. Click to confirm

Filters



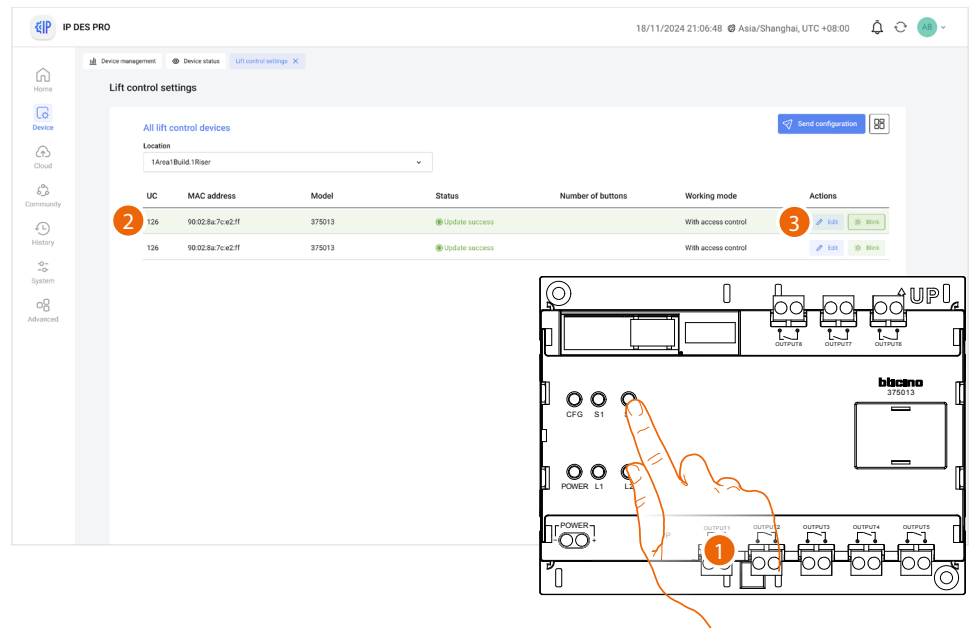
- A *Device type filter*
- B *Item code filter*

Lift control settings

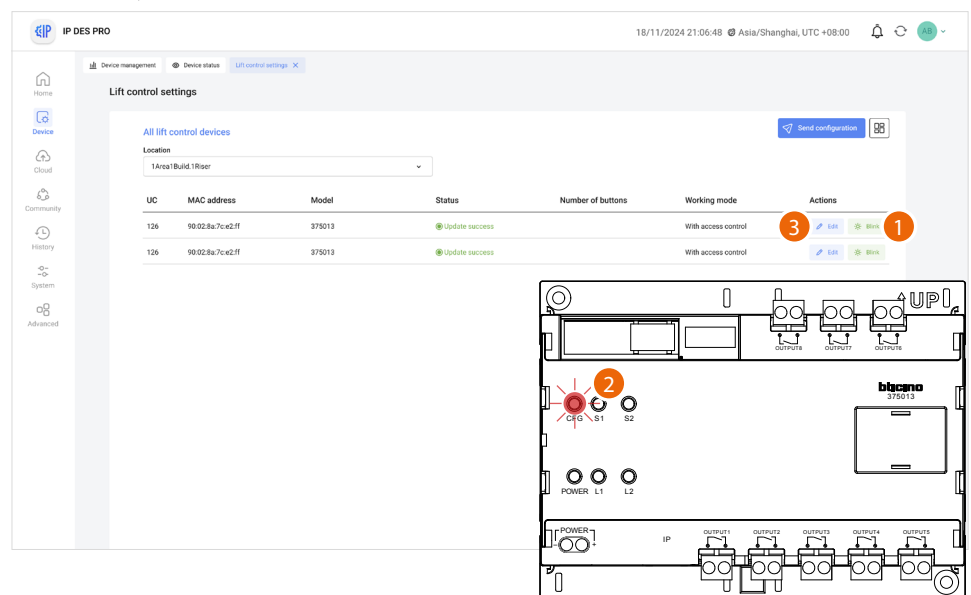
On this page, you can use the lift control interface with relay 375013 to set the parameters of the lift control function.

This function allows to send commands to the lift control centre, through dry contacts, to simulate a lift call.

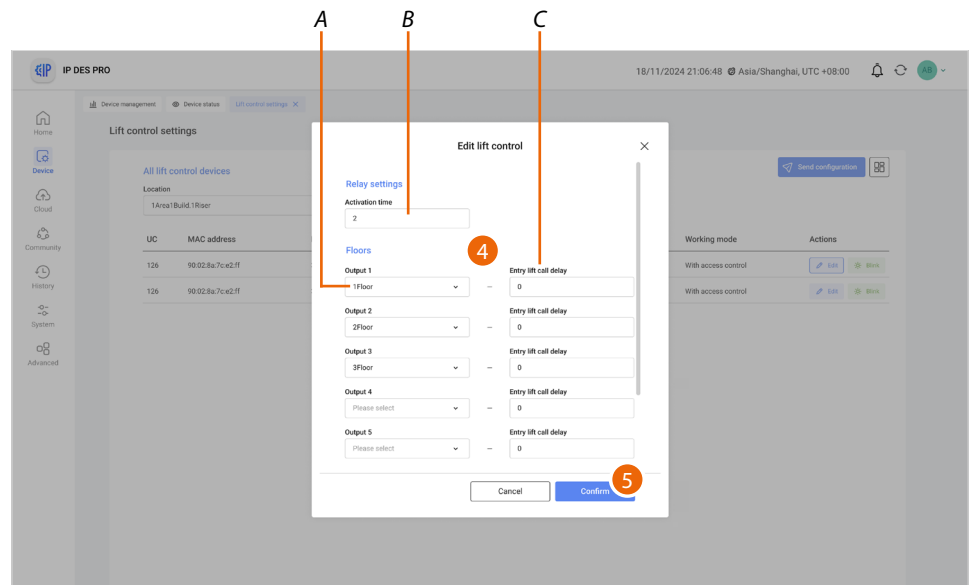
NOTE: In case of several entrance panels in the system, those not controlling the lift must have the **"Lift control" parameter set to "Off"**



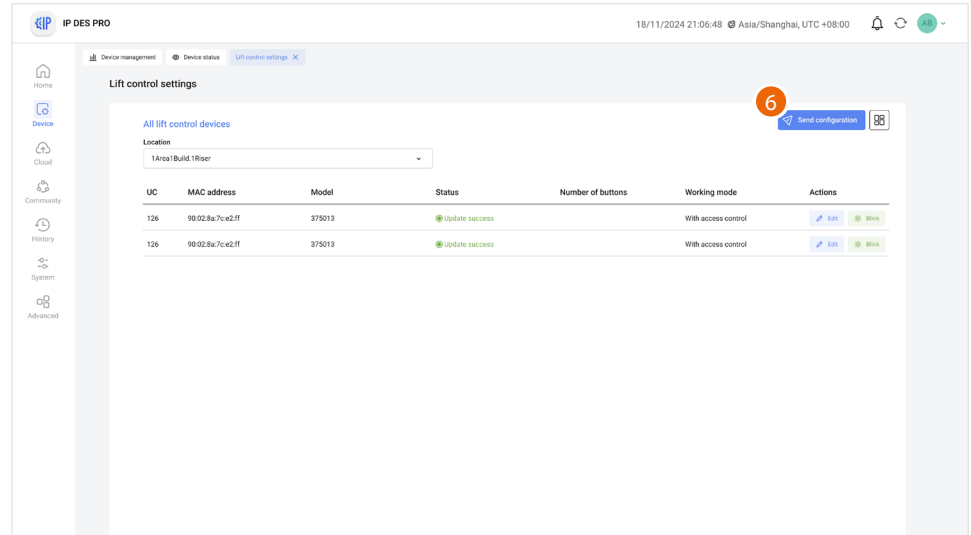
1. After adding the lift control interface with relay 375013, briefly press the button on the device to identify the device among those present in the structure in the Lift control function page of the Software.
2. The line of the lift control interface with relay 375013 of the Software will flash
3. Click to modify the device settings or alternatively



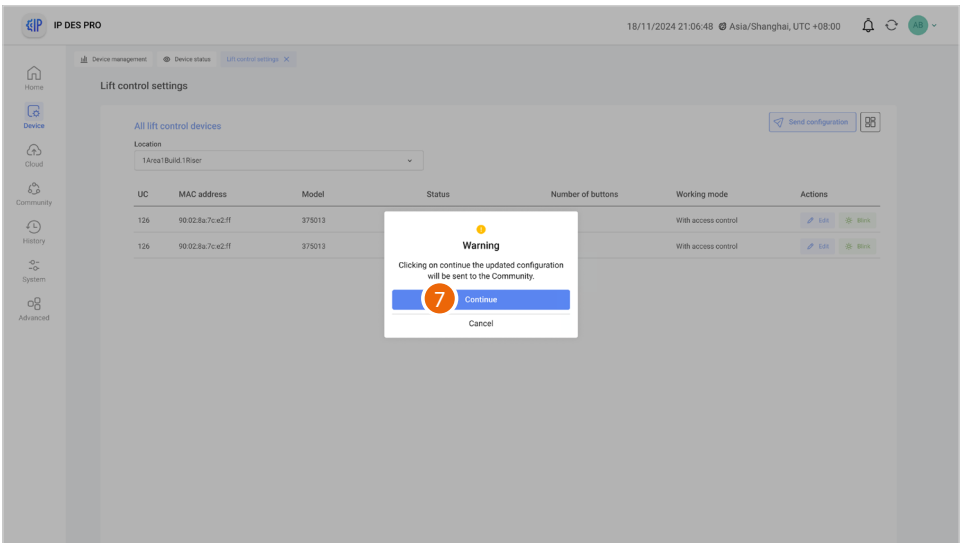
1. In the Lift control function page of the Software, click the button to locate which system interface is selected.
2. On the system, the LED of the lift control interface with relay 375013 will flash
3. Click to modify the device settings



- A. Selection of the floor for which output 1 to 8 is activated.
- B. Time during which the contact remains switched
- C. Contact switching activation delay time
4. Modify the data
5. Click to confirm

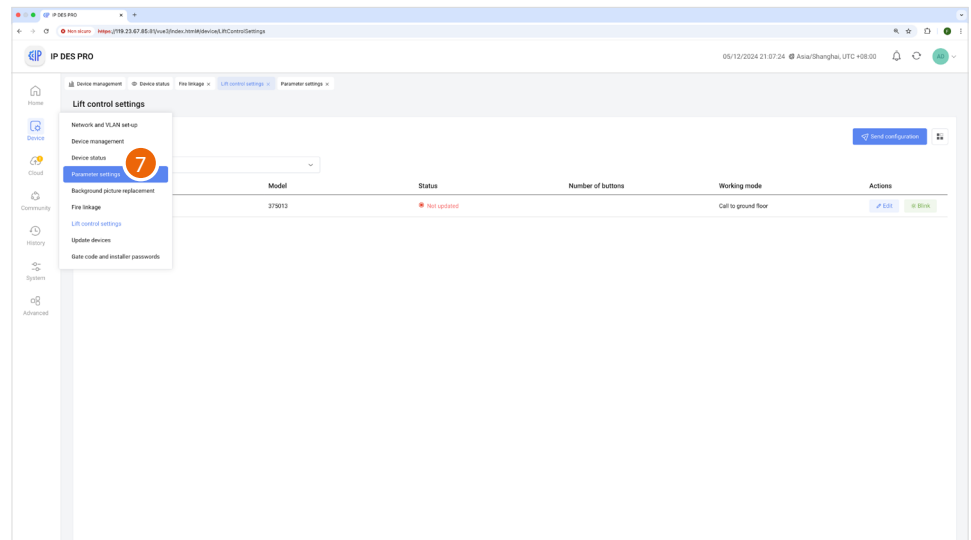


6. Click to send the modifications to the device

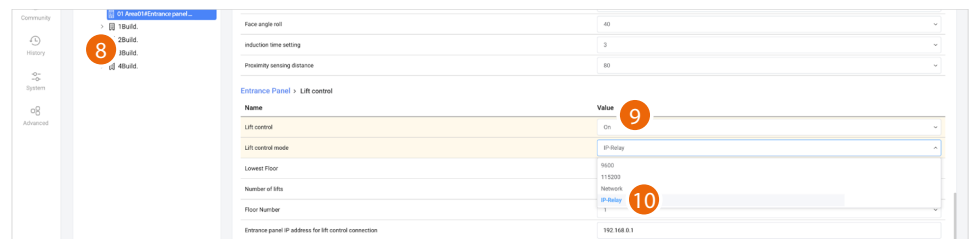


7. Click to confirm

After configuring the lift control functions, it will be appropriate to configure the type of protocol used by the devices that use the lift control function.



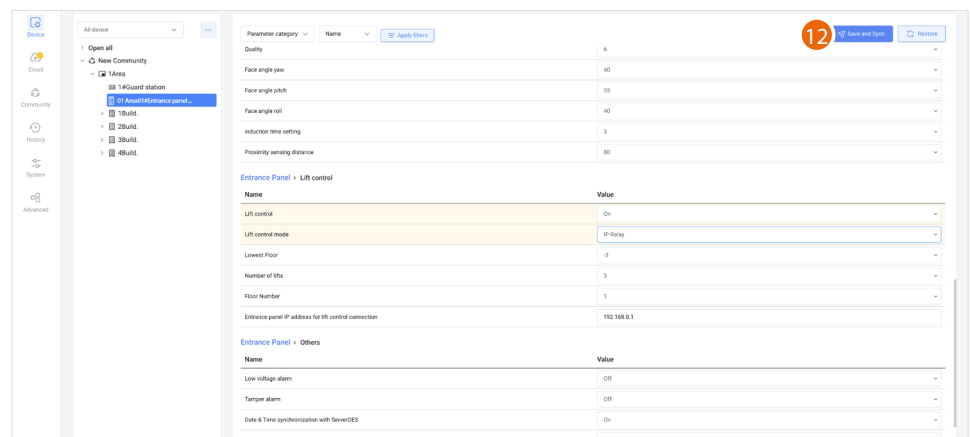
7. Click to open the configuration parameters



8. Select the entrance panel on which to set the lift control function parameters

9. Select the "ON" setting

10. Select the "IP-Relay" mode



11. Click to send the configuration

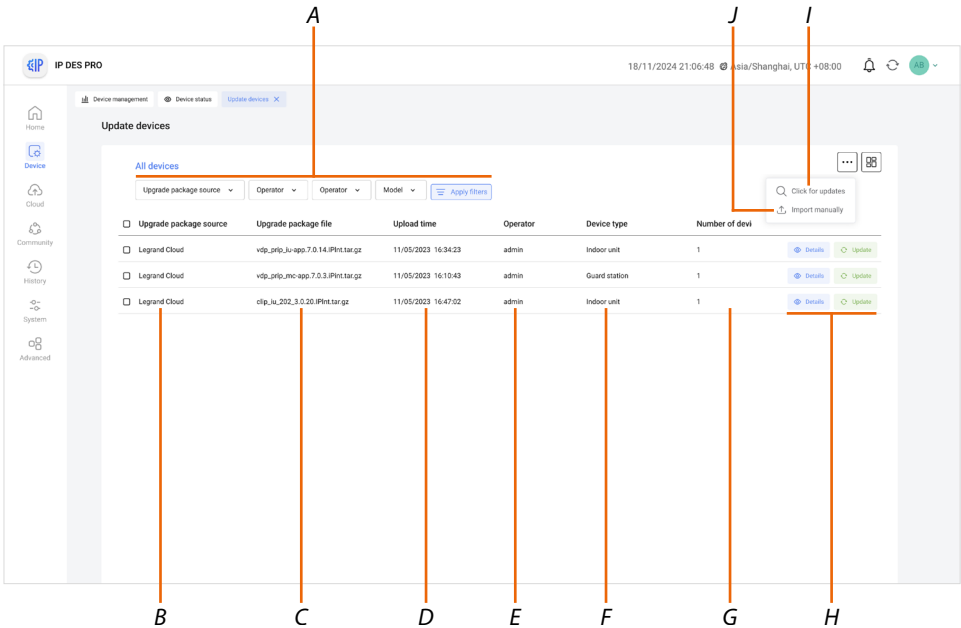
Update devices

This page can be used to view the firmware updates of the devices and import and perform new updates.

When the page is opened, the system checks for firmware updates for the devices in the Community.

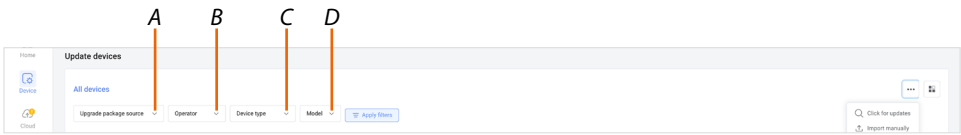
If the search shows that updates are available, these will be downloaded automatically.

Attention: the search for new firmware only takes place if the last downloaded updates have already been deleted. The page must be empty..



- A Update selection filters
- B Update package source: local import or download from cloud
- C Update file name (.gz)
- D Time date of the system update
- E Name of the account that carried out the update
- F Devices affected
- G Number of affected community devices
- H Update management keys
- I Check and download the update package from the cloud if available (if the system is connected to the internet)
- J Import update package (to be used if an update file is available)

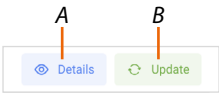
Filters



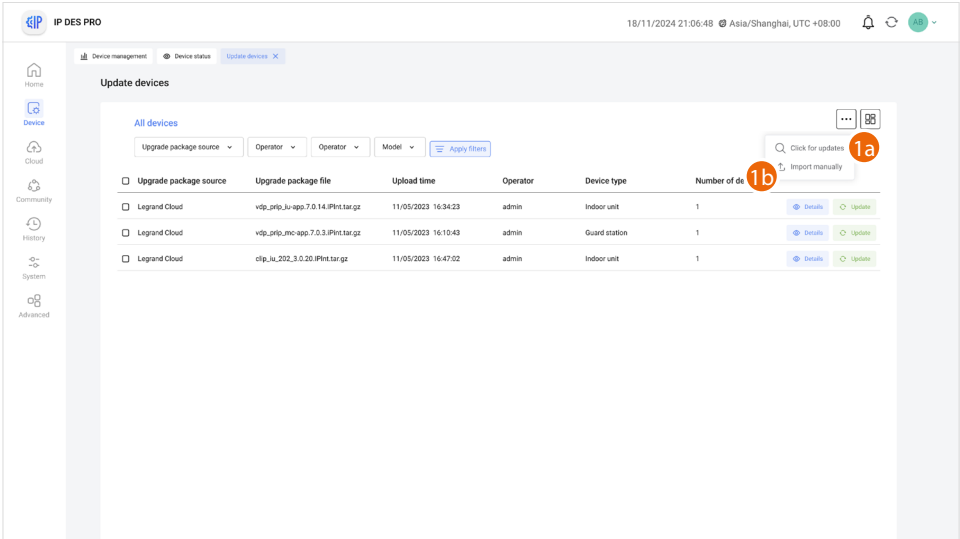
- A Origin of the update
- B Account that completed the update (enter the name)
- C Type of devices
- D Select the code of the product affected by the firmware update (in case of firmware that can be applied to several devices)



Update management keys



- A Information about the update
- B Open the panel to send the update to the system



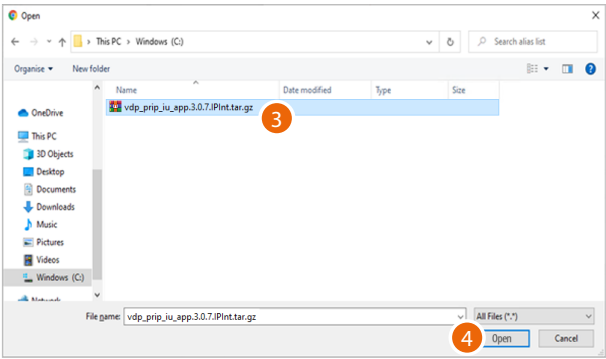
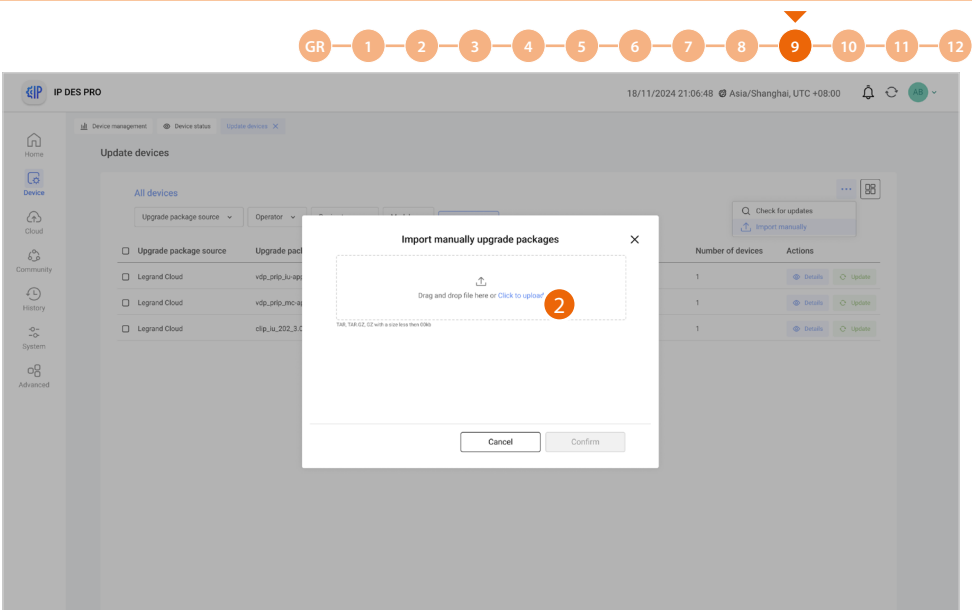
- 1a. Click to check for updates on the cloud. If there are updates, these will be downloaded and available for installation

NOTE: firmware updates will only be downloaded if the last installed updates have already been deleted: the page must be empty.

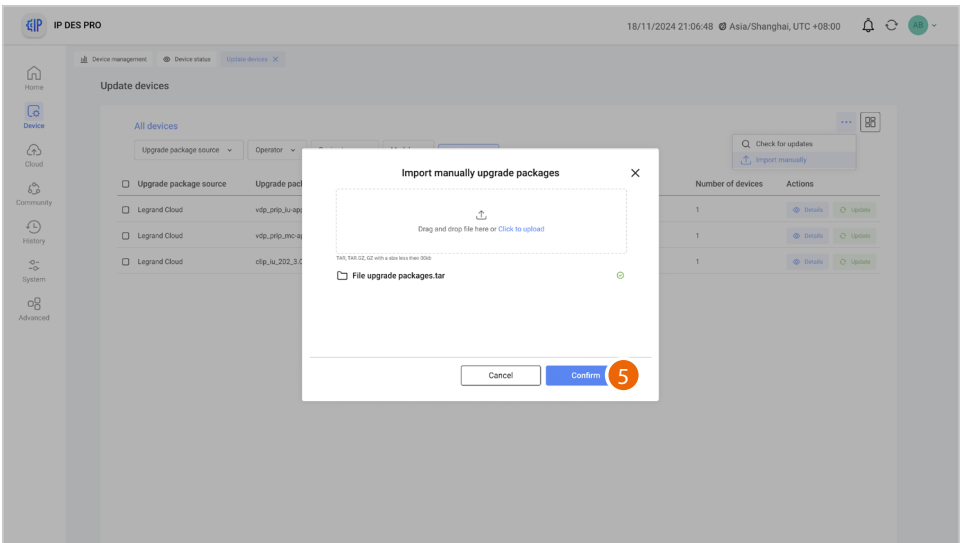
or

- 1b. Click to import the update package from the local system (see item 2)

NOTE: the updates are not distributed by BTicino and this function is only intended for technical support.



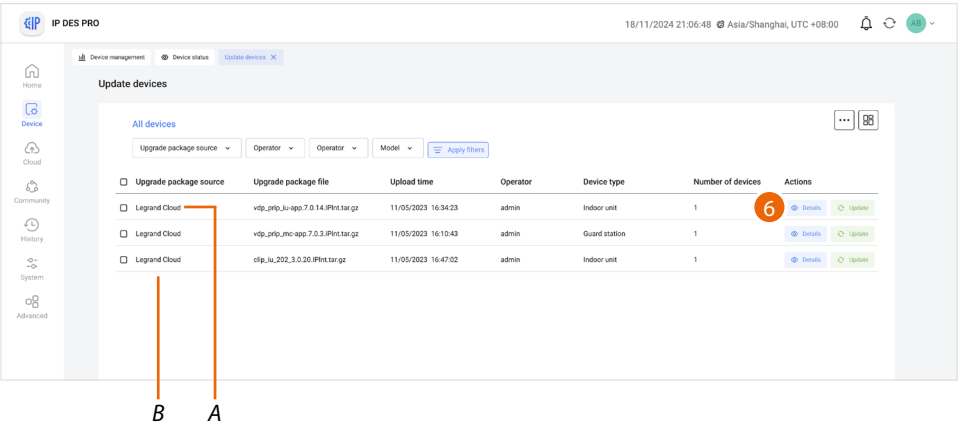
2. Click to select the update package
3. Select the .gz file
4. Click to continue



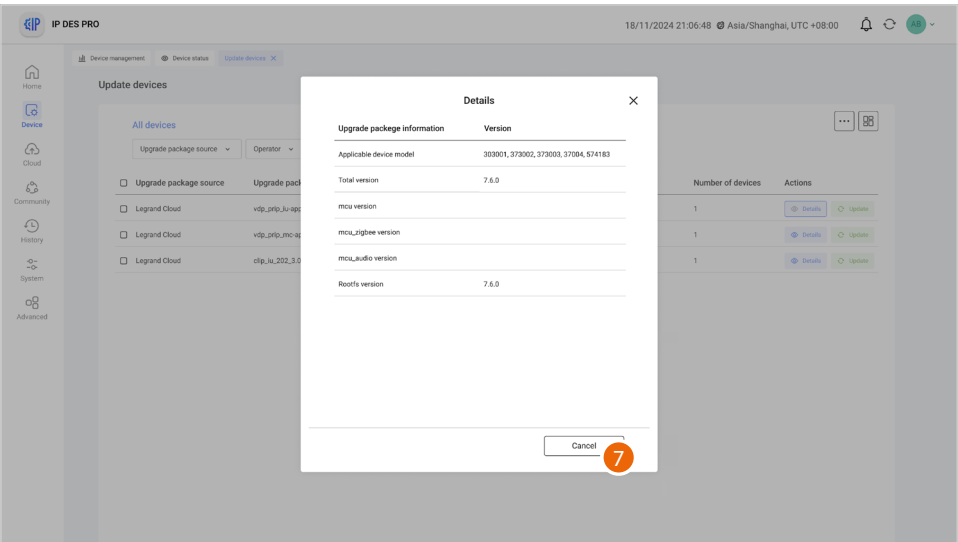
5. Click to confirm



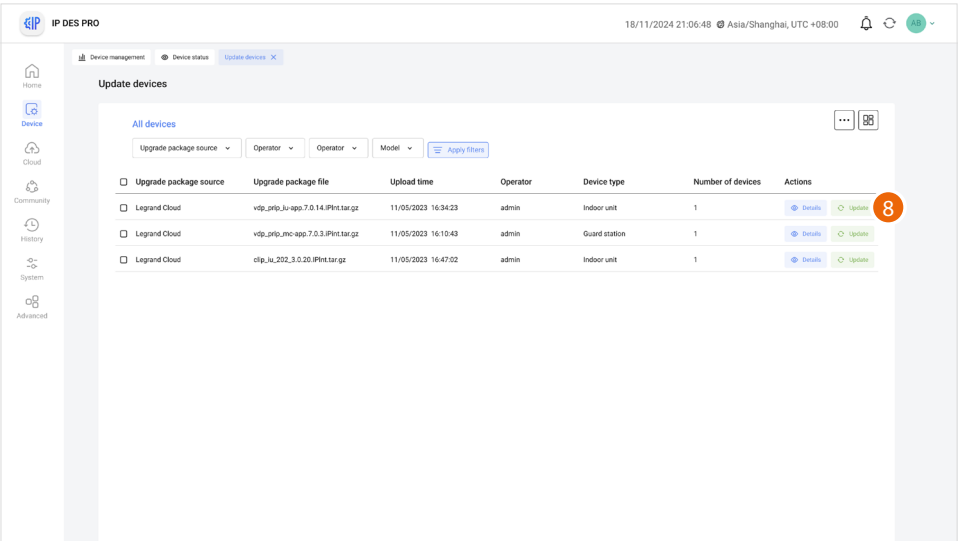
The package has been imported and is available to be sent to the devices



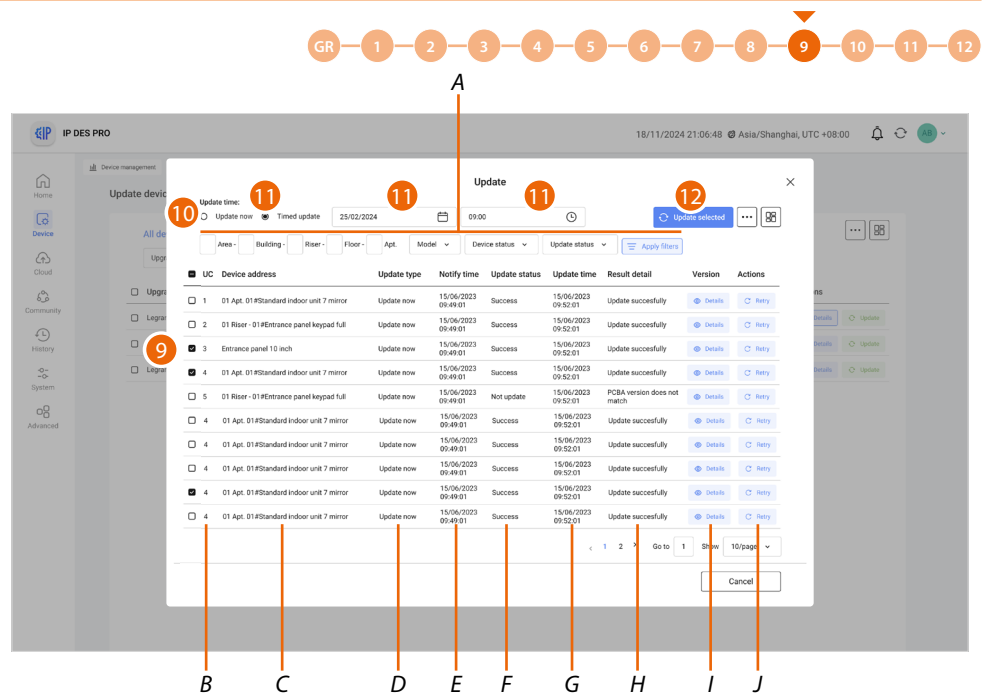
- A. Update package from Cloud
- B. Update package from local system
- 6. Click to see some of the update data



- 7. Click to close



- 8. Click to send the update to the plant



A Filters for displaying the devices affected by the update

B Progressive number

C Name of the customisable device.

The original name represents **the address of the device in the community.**

D Indicates whether the update is performed immediately or is scheduled

E Send time

F Sent/not sent

G Update schedule time

H Update result

I Update details

J Try again

9. After using the filters, select the relevant devices

10. Decide whether to perform the update immediately or
or

11. Schedule an update, setting the date and time

12. Start the update for the selected devices or for all the devices

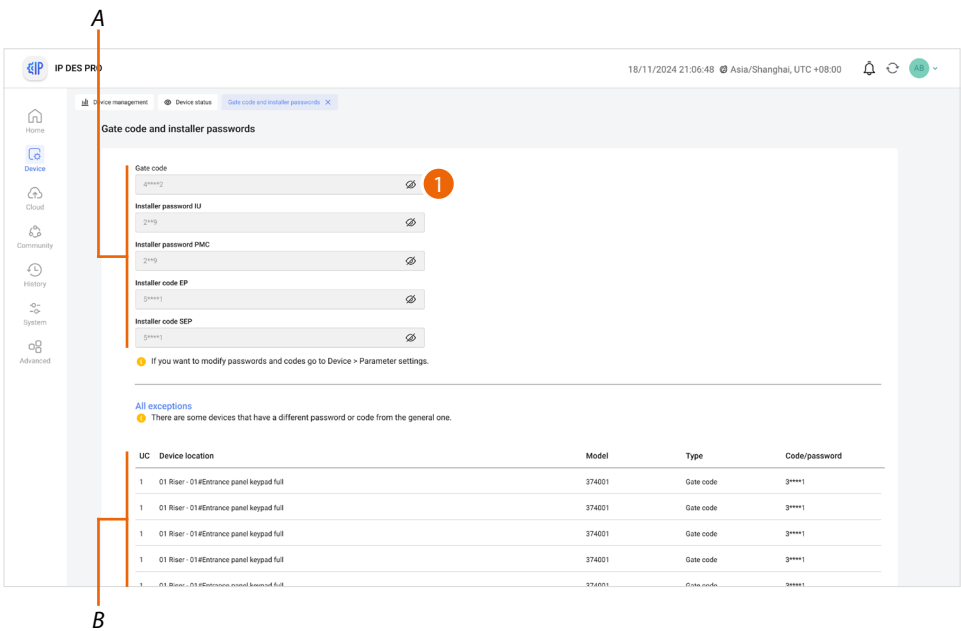
Gate code and installer passwords

For security reasons, after the first installation, the device passwords and codes are generated automatically (with random characters) and uniquely for each type of device (one for IU and GS, one for EP and VEPO).

The randomly assigned passwords are:

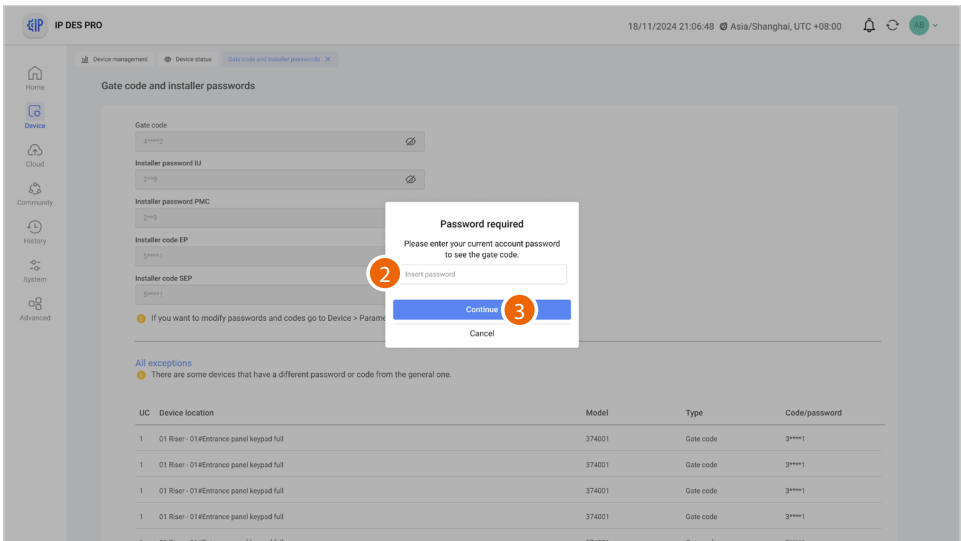
- Gate code – Local access code
- IU installer password – IU installer password
- PMC installer password – GS installer password
- EP installer code – EP password
- VEPO installer code – VEPO password

To know these passwords, you must make them visible using the following procedure:

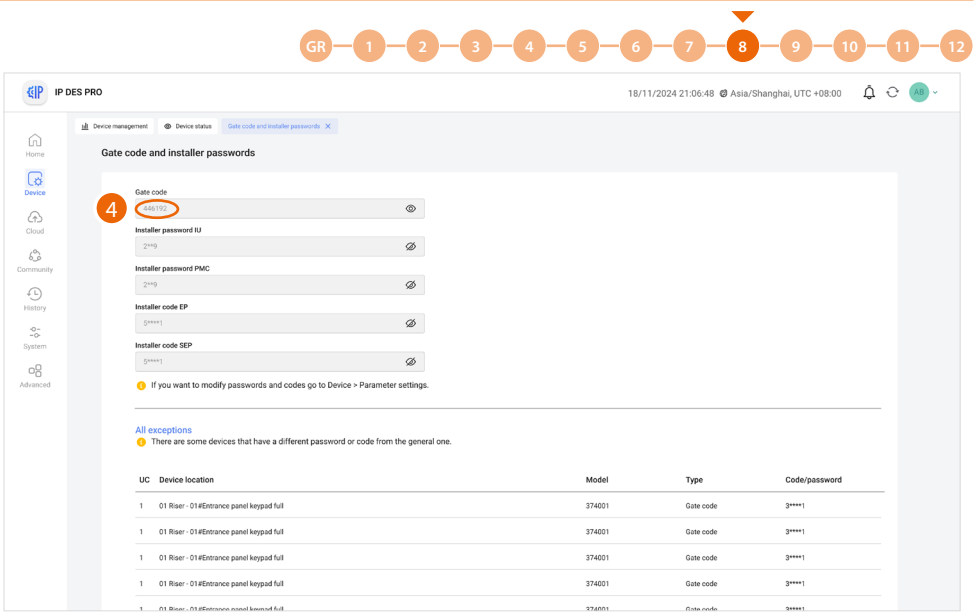


- A Default passwords and codes
- B List of devices for which codes and passwords have been changed.
To modify codes and passwords see [Parameter settings](#)

1. Click the password field of any of the devices



2. Enter the software [authentication](#) password
3. Click to confirm



4. The passwords are now visible.
If you leave the page and then come back, the passwords will no longer be visible and you will have to repeat the operation.

Warning: Save passwords in a safe place that is always accessible (Cloud backup activation recommended).

If both the SD and the backup are unavailable, it will not be possible to retrieve the passwords.

NOTE: the passwords of the devices incorrectly activated in DEMO mode are: 2000 (EP) and 1111 (IU and GS)

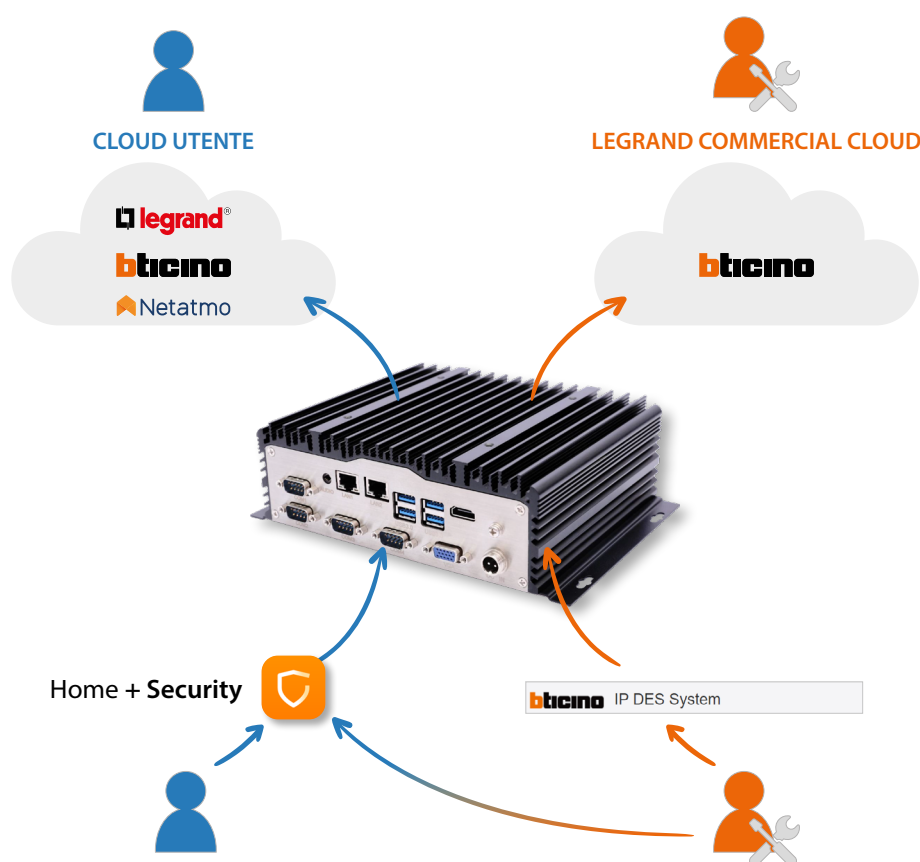
Cloud

This menu allows, after authentication via an Installer account, to save a copy of the configuration + other data to the Legrand Commercial Cloud.

This operation allows to:

- installation synchronisation and import of the pre-configured system
- increased data backup security
- download the FW to update the system
- share access with another member of your team
- associate the Home+Security app to the IU, for remote management of the video door entry system.

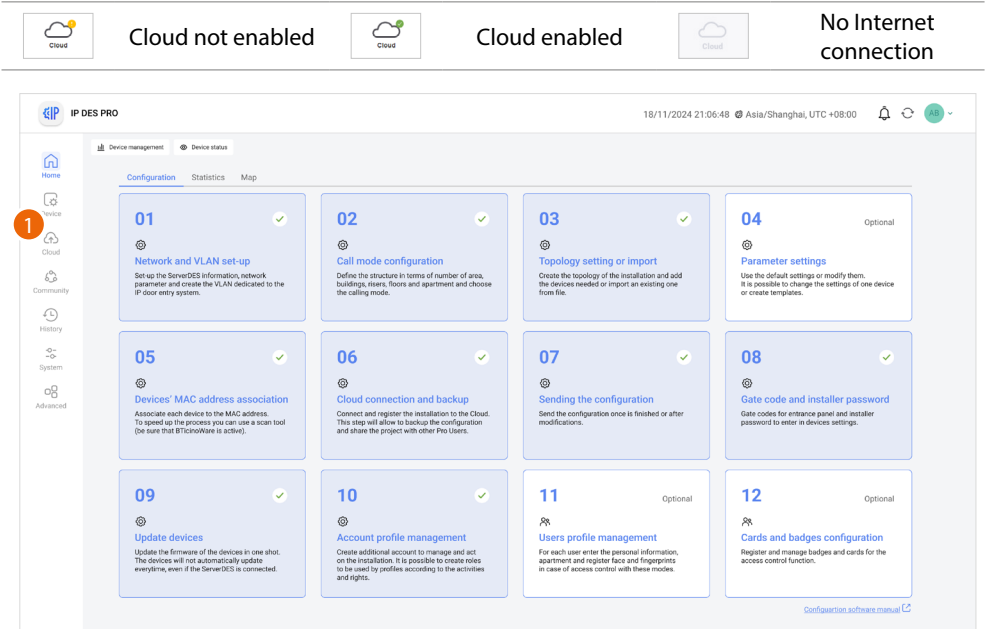
To use this function, you must have an Installer account or create one.



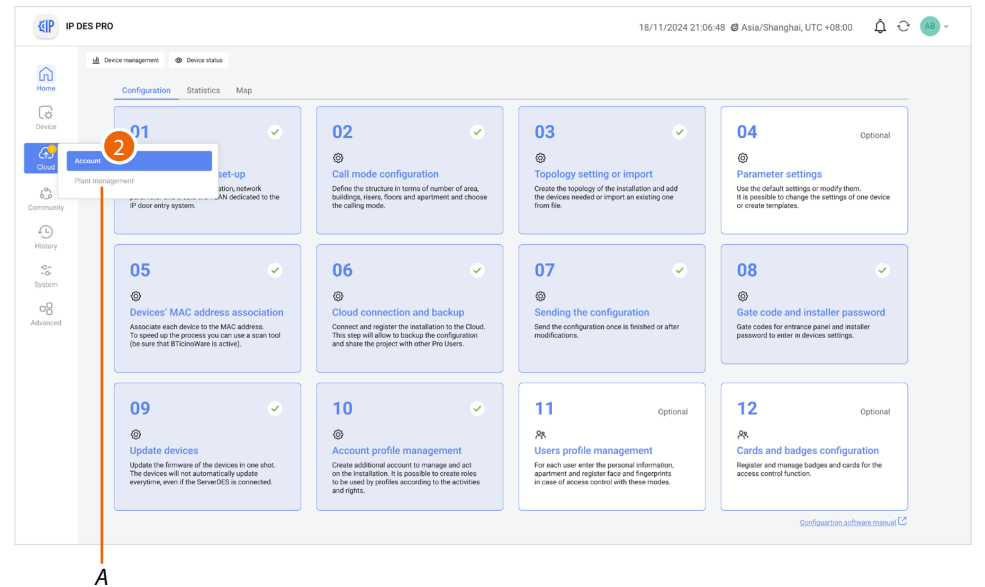
NOTE: With a single building Internet connection, it is also possible to manage the forwarding of calls from all entrance panels to the enabled internal units.

First access

The first time you access the cloud menu, the authentication/account creation page is displayed

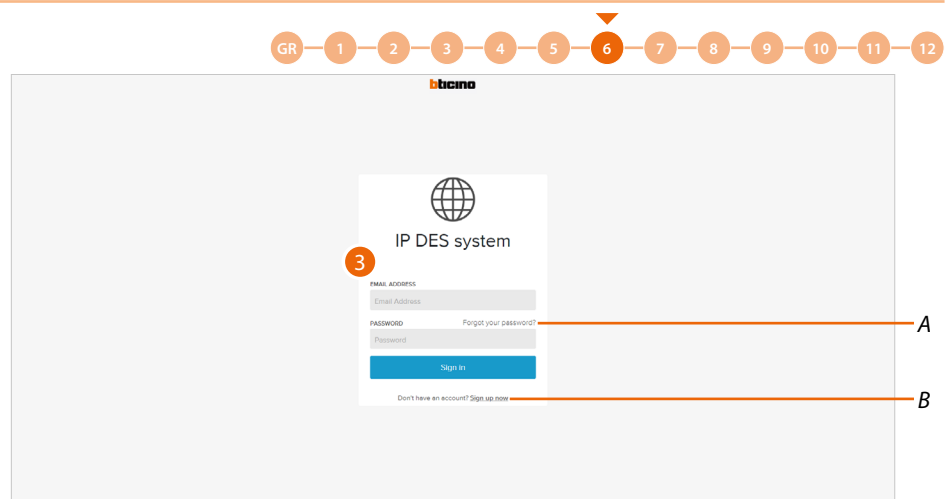


1. Click to enter the menu



2. Click to complete the Legrand Commercial Cloud authentication process.

A The plant management key is not active because the community has not yet been created on the cloud.

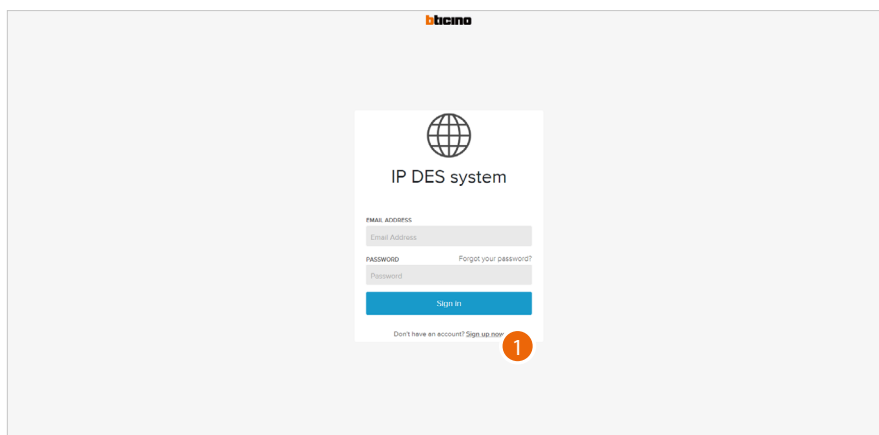


3. If you are already registered, run the [authentication](#) process, or [register a new account](#) (B).

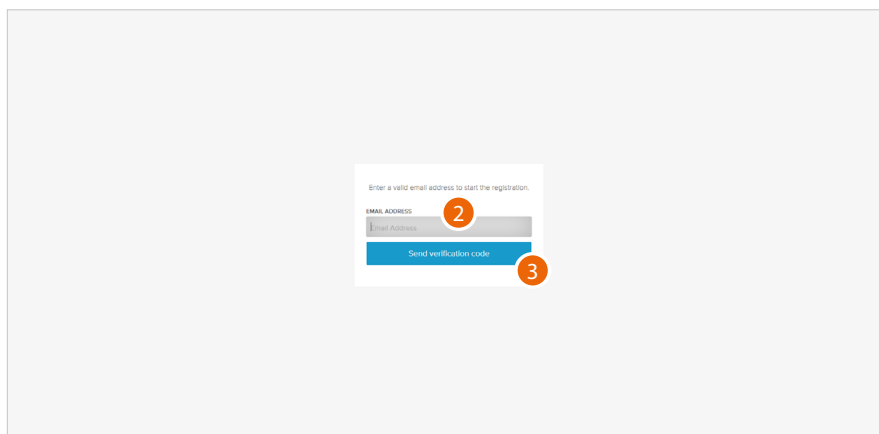
A Recover the [forgotten password](#)

Registration of the account on the Legrand Commercial Cloud

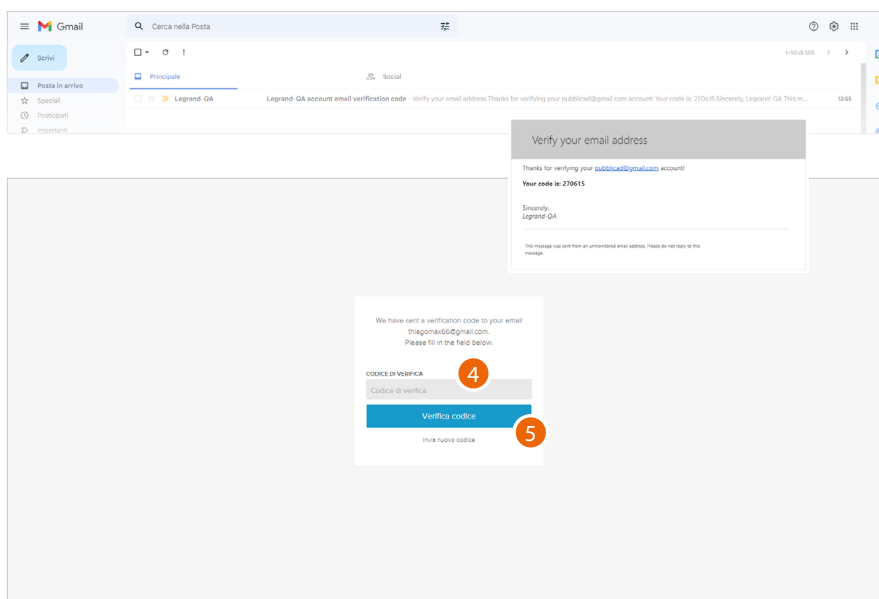
In order to use the cloud you must first register. To register, follow the instructions:



1. Click to register and create an account



2. Enter the email address where the system can send a verification code
3. Click to confirm the forwarding of the verification code



4. Enter the verification code received by e-mail
5. Click to confirm

GR 1 2 3 4 5 6 7 8 9 10 11 12

Fill in the fields below to complete the creation of your account.

6 **PASSWORD**

CONFIRM PASSWORD

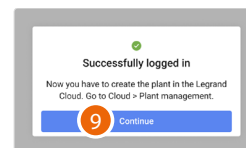
NAME James **SURNAME** Smith
COUNTRY Italia
DISPLAYED NAME James Smith

7 ☒ I have read and accept the Terms and Conditions of use and the Data protection declaration
☒ Stay in contact to receive e-mail news regarding Legrand
☒ Participate to the product improvement program by sharing the application use data

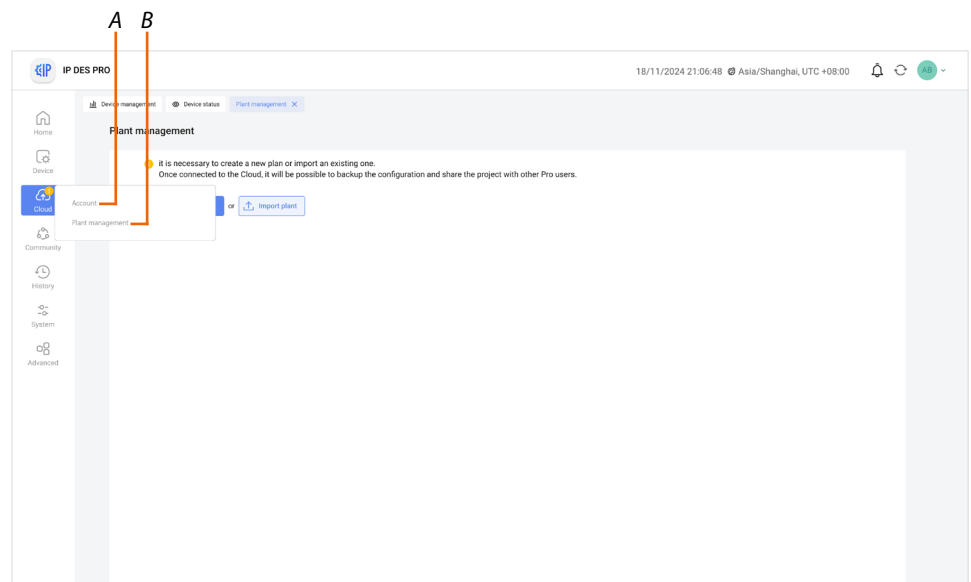
8 **Create**

6. Enter a password and fill the fields with your details.
7. Tick to accept the terms and conditions of use laid down in the associated text (obligatory).
8. Click to continue.

The account has been correctly created



9. Click to finish.



Now it is possible to:

- A **Manage your account**
- B **Create e and manage your plant**

Authentication

After registering with the portal, you can authenticate by entering email and password.

1. Enter email and password
2. Click to access

3. Tick the boxes to accept/reject the privacy terms and conditions of use, inclusion in the Legrand e-mail list and sharing of data for the purpose of improving the software.
4. Click to confirm

5. Click to confirm.

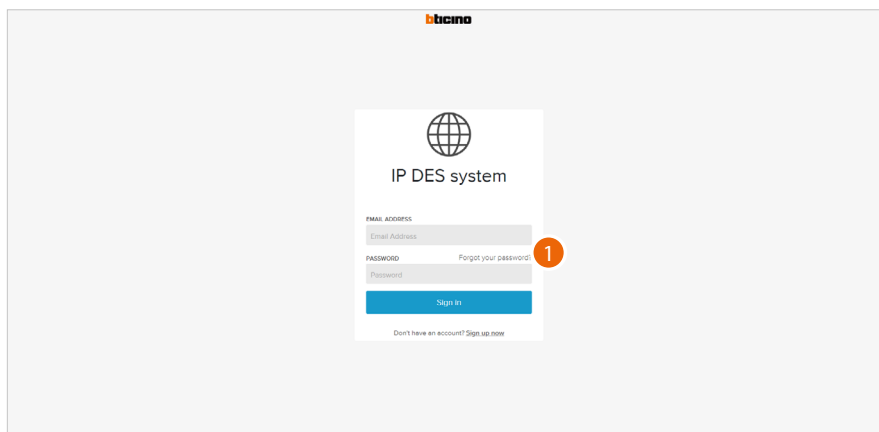
Login not performed system not yet created
 Synchronisation in progress
 Synchronisation KO
 Synchronisation OK

Now it is possible to:

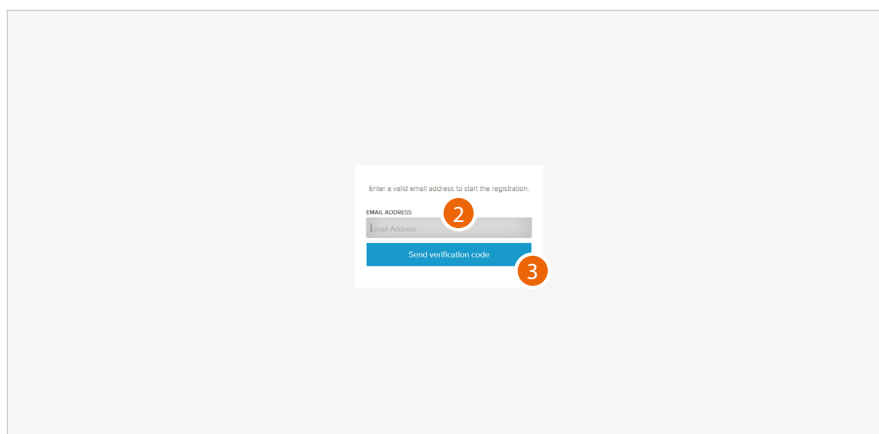
- A **Manage your account**
- B **Create and manage your plant**

Forgotten password

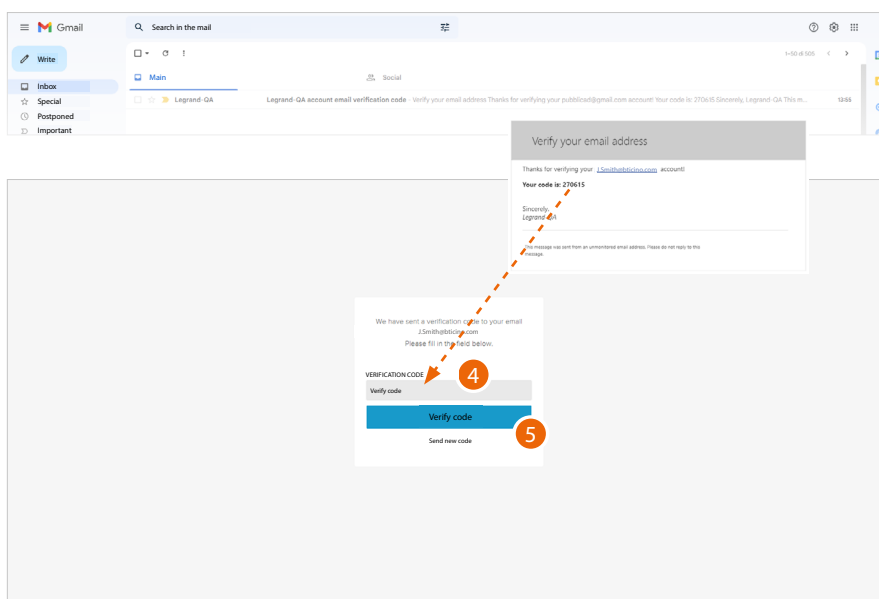
When you have forgotten the password:



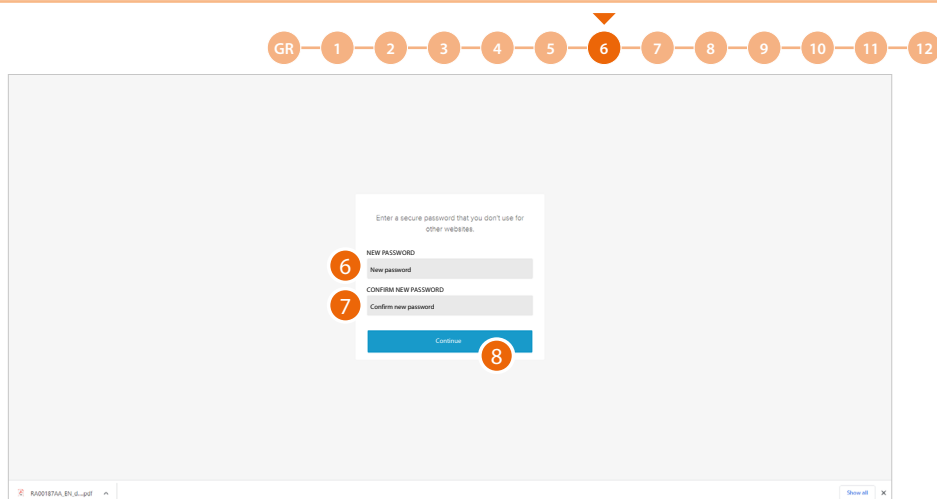
1. Click to activate the password recovery procedure



2. Enter the email address where the system can send a verification code
3. Click to confirm the forwarding of the verification code



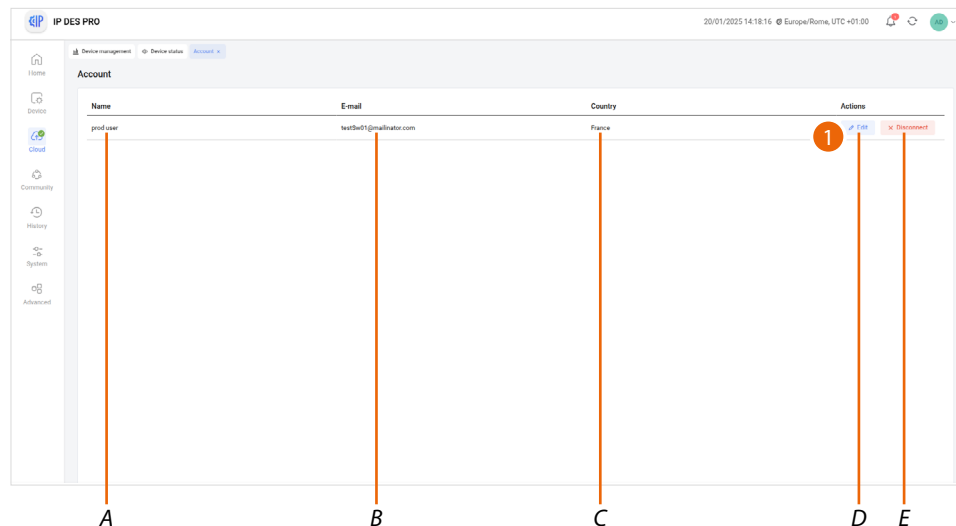
4. Enter the verification code received by e-mail
5. Click to confirm



6. Enter the new password.
For security reasons enter a new password with these features:
 - minimum length 8 characters;
 - must contain at least one letter and one number;
 - it must be different from the last 5 passwords used.
7. Enter the password again.
8. Click to confirm. The Home Page will be displayed so that the authentication procedure can be completed.

Manage your account

In this section, it is possible to view and display some functions regarding your account.



- A Display the name used for the account
- B Current email/account
- C Display the country
- D Manage your account
- E Disconnect the account
- 1 Click to enter the account management section



- A Login mail address
- B Display/edit your Legrand account **registration details**
- C Modify some **safety parameters** of your account, such as password and disconnection from all objects
- D Authorise the sharing of data to help **improve the product.**
- E Manage your communication **authorisations** and other aspects of your personal details
- F Display **contract terms and conditions** regarding the Legrand apps that you are using
- G Manage **partner apps** to which your account is connected (e.g. Google Home etc.)

Profile

This section may be used to change some data of the account or to replace it with another registered Legrand account.

bticino Personal data

Name	James	A
Surname	Smith	B
Show name	James Smith	C
E-mail	J.Smith@bticino.com	D
Country	United Kingdom	E
Language	We will send you our communications in this language (email, ...)	F
Language	English	F
Delete the account		G

Termini e Condizioni | Informativa sulla Privacy | Legrand © 2019

RA00187AA_EN_d...pdf Show all

- A View/edit the name used for the account
- B Display/edit the surname used for the account
- C Show/edit the name used for the account
- D View/edit the device management email/account
- E Display the country
- F Display/select the language in which to receive communications
- G Delete the account

Show name (edit name)

bticino Personal data

Name	James	1
Surname	Smith	
Show name	James Smith	
E-mail	J.Smith@bticino.com	
Country	United Kingdom	
Language	We will send you our communications in this language (email, ...)	
Language	English	
Delete the account		

Termini e Condizioni | Informativa sulla Privacy | Legrand © 2019

RA00187AA_EN_d...pdf Show all

1. Click to edit the name

bticino Change the name shown

Show name	James Smith	2
Maximum 30 characters		

Termini e Condizioni | Informativa sulla Privacy | Legrand © 2019

RA00187AA_EN_d...pdf Show all

2. Enter the name that will be used in the system e-mail communications.

Email/account (change of the device management email/account)

To change the access email address:

bticino Personal data

Name	James
Surname	Smith
Show name	James Smith
E-mail	J.Smith@bticino.com
Country	United Kingdom
Language	English
Delete the account	

Tarmini e Condizioni | Informativa sulla Privacy | Legrand © 2019

RA00187AA_EN_d..pdf Show all

1. Click to edit the email address

bticino Change e-mail

New email	J.Brown@bticino.com
Confirm the new email	J.Brown@bticino.com
Password	*****

Confirm

Tarmini e Condizioni | Informativa sulla Privacy | Legrand © 2019

RA00187AA_EN_d..pdf Show all

2. Enter the login details (email and password) of the new registered Legrand account to be used to manage the device

3. Click to confirm

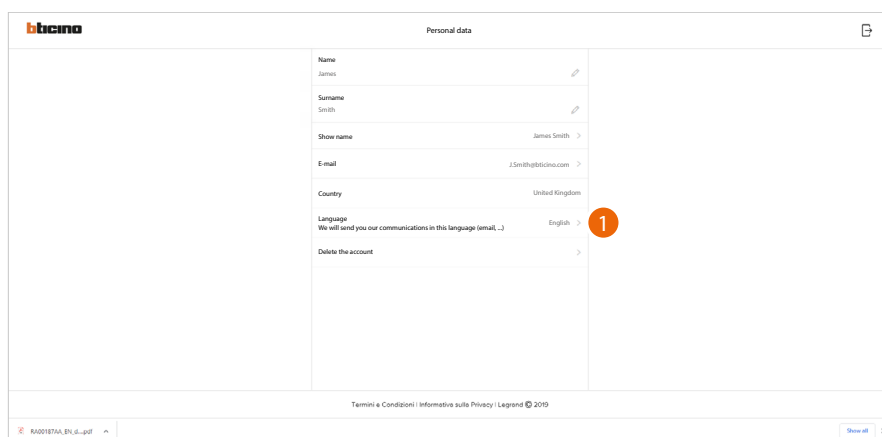
bticino Personal data

Name	James
Surname	Smith
Show name	James Brown
E-mail	J.Brown@bticino.com
Country	United Kingdom
Language	English
Delete the account	

Tarmini e Condizioni | Informativa sulla Privacy | Legrand © 2019

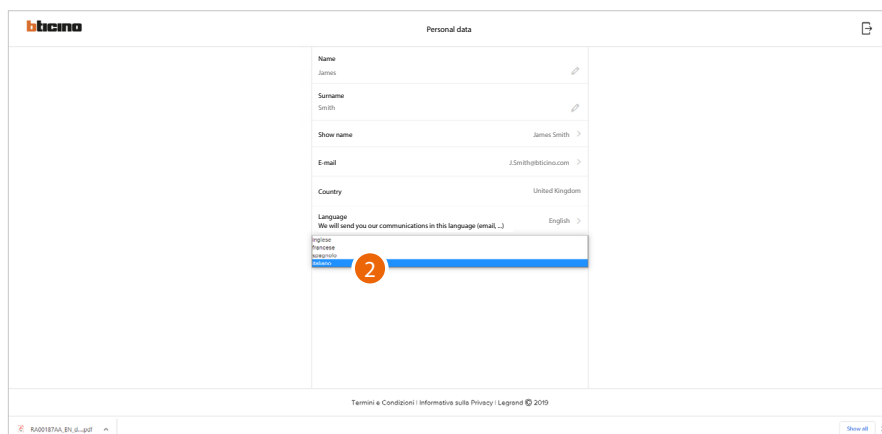
RA00187AA_EN_d..pdf Show all

Language



The screenshot shows the 'Personal data' form in the bticino system. The form includes fields for Name, Surname, Show name, E-mail, Country, and Language. The 'Language' field is highlighted with a red circle and the number 1, indicating it should be clicked to edit. The form also includes a 'Delete the account' link and a footer with 'Termini e Condizioni', 'Informativa sulla Privacy', and 'Legenda'.

1. Click to edit the language in which to receive communications



The screenshot shows the 'Personal data' form in the bticino system. The 'Language' dropdown menu is open, showing options: English, Italiano, Francese, Spagnolo, and Deutsch. The 'Deutsch' option is highlighted with a red circle and the number 2, indicating it should be selected. The form also includes a 'Delete the account' link and a footer with 'Termini e Condizioni', 'Informativa sulla Privacy', and 'Legenda'.

2. Select the language

Delete the account

In this page it is possible to permanently delete your Legrand account, which can therefore no longer be used for the Applications to which it was associated.

NOTE : When deleting the account, all the data associated with the Applications will also be lost

bticino Personal data

Name James

Surname Smith

Show name James Smith

E-mail J.Smith@bticino.com

Country United Kingdom

Language We will send you our communications in this language (email, ...) English

Delete the account 1

Tamini & Condipoli | Informativa sulla Privacy | Legrand © 2019

RA00187AA_EN_d...pdf Show all

1. Click to delete your Legrand account definitively

bticino Delete the account

When deleting your account, you will not be able to use the SiteServer_QH application.

All the data associated with the applications will also be lost.
If you know what you are doing, enter your password and confirm your choice.

Password Your password 2

Yes, delete my account 3

Tamini & Condipoli | Informativa sulla Privacy | Legrand © 2019

RA00187AA_EN_d...pdf Show all

1. Enter the password
2. Click to delete the account

bticino Delete the account

When deleting your account, you will not be able to use the SiteServer_QH application.

All the data associated with the applications will also be lost.
If you know what you are doing, enter your password and confirm your choice.

Password Your password

Account deleted successfully
Your account has been correctly deleted.
You will now be disconnected from this application.

Continue 4

Yes, delete my account

Tamini & Condipoli | Informativa sulla Privacy | Legrand © 2019

RA00187AA_EN_d...pdf Show all

4. Click to confirm
At the end of the procedure you will be disconnected from the application.

Safety

In this page it is possible to edit the password of your account and to disconnect it from all devices. The disconnection of your account from all devices is useful in case one of your devices is lost or stolen.

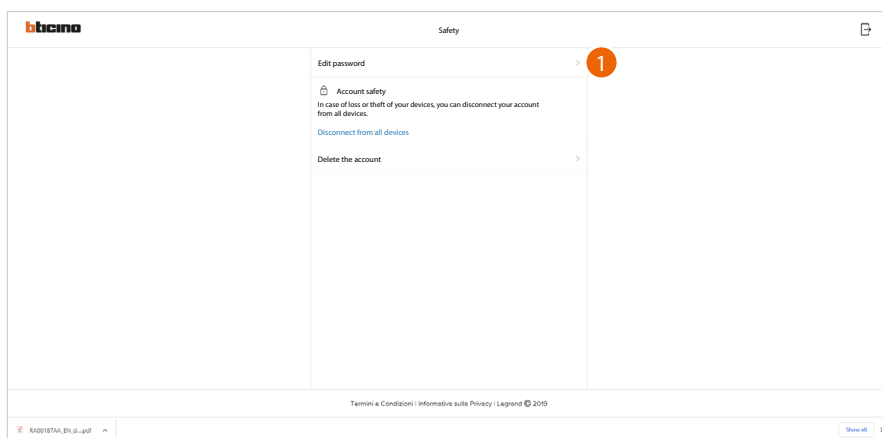


A Complete the password change procedure

B Disconnect from all devices

C Delete the account

Edit password



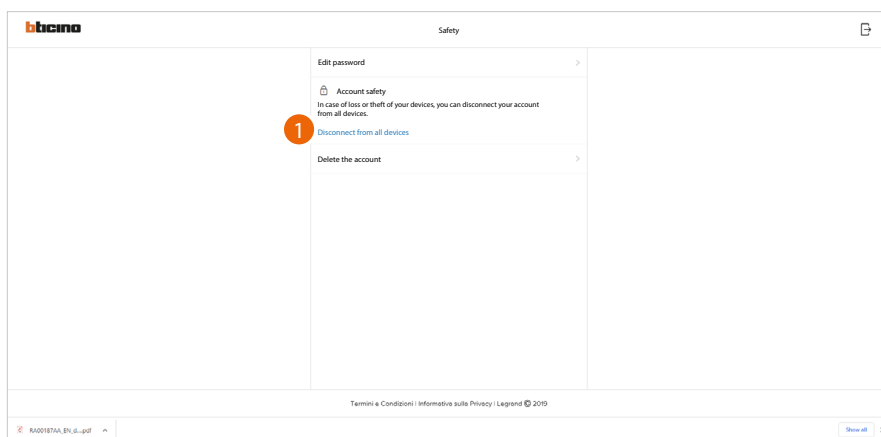
1. Click to modify the password

The screenshot shows the 'btcino' Safety page. At the top, a progress bar indicates steps 1 through 12, with step 6 highlighted. The page title is 'Safety'. The user is logged in as 'j.smith@btcino.com'. The 'Current password' field is marked with a red circle 2. Below it is a 'Continue' button marked with a red circle 3. The footer contains the text 'Termini e Condizioni | Informativa sulla Privacy | Legend © 2019'.

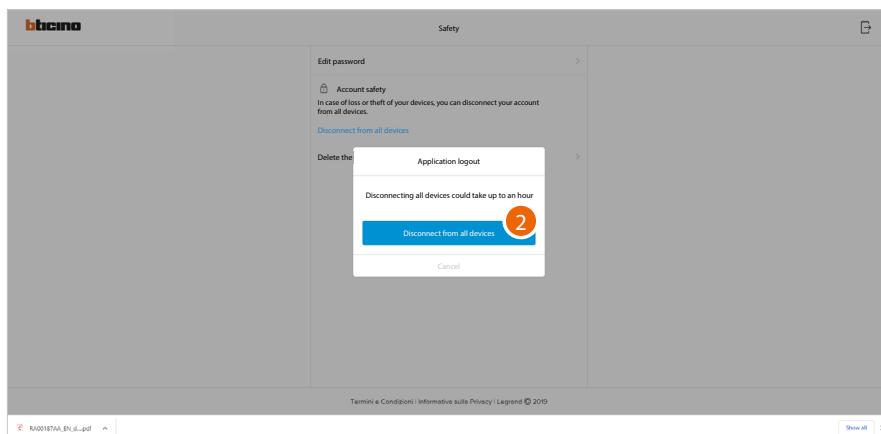
2. Enter the current password
3. Click to continue

The screenshot shows the 'btcino' Safety page. At the top, a progress bar indicates steps 1 through 12, with step 6 highlighted. The page title is 'Safety'. The user is logged in as 'j.smith@btcino.com'. The 'New password' field is marked with a red circle 4. Below it is a 'Continue' button marked with a red circle 5. The footer contains the text 'Termini e Condizioni | Informativa sulla Privacy | Legend © 2019'.

4. Enter the new password, which must meet the following requirements:
 - at least 8 characters;
 - at least one lower case letter (e.g. a);
 - at least one upper case letter (e.g. A);
 - at least one number (e.g. 1);
 - at least one special character (e.g. \$);
5. Click to confirm

Disconnect from all devices

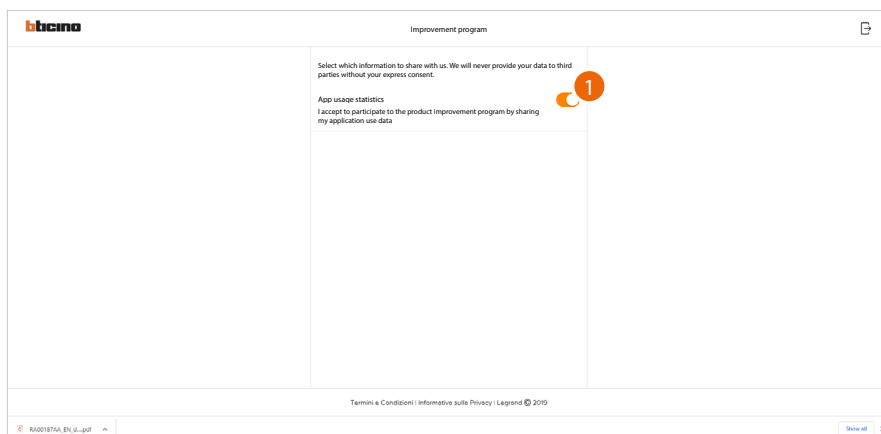
1. Click to activate the procedure



2. Click to disconnect your account from all the devices and all the third-party applications. The system automatically logs out from the application.

Improvement program

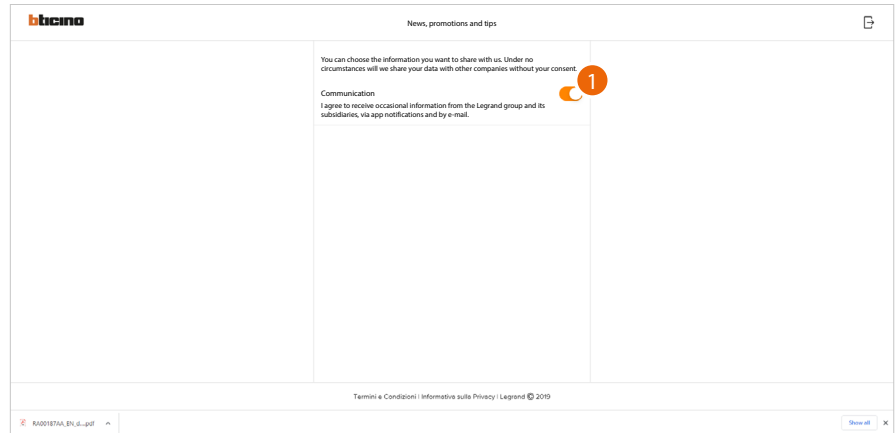
This section can be used to enable the sharing of the app usage data.



1. Click to enable the sharing of the app usage data.

Communication preferences

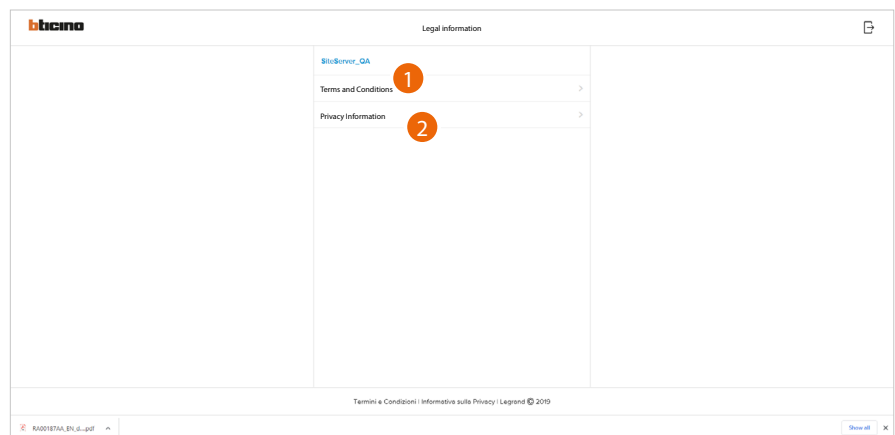
This section can be used to enable the reception of communications from Legrand



1. Click to accept communications from Netatmo/Legrand/BTicino

Legal information

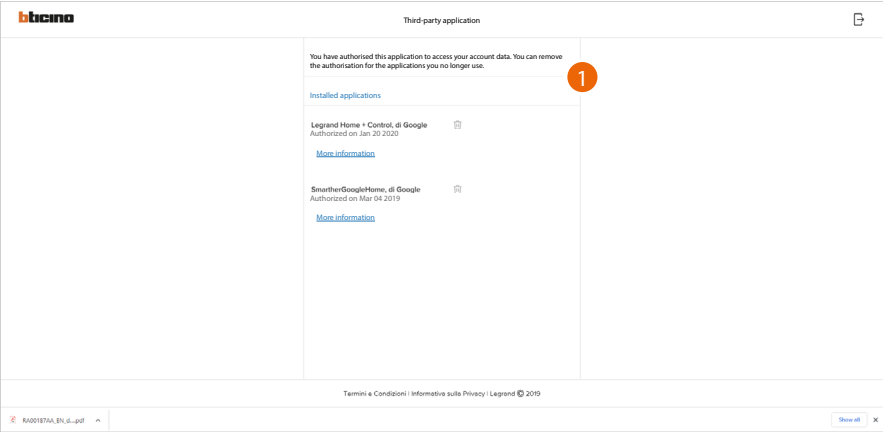
Using this section you will be able to view terms and conditions of use and privacy information for each App to which your Legrand account is associated



1. Click to display Terms and Conditions
2. Click to display Privacy information

Partner apps

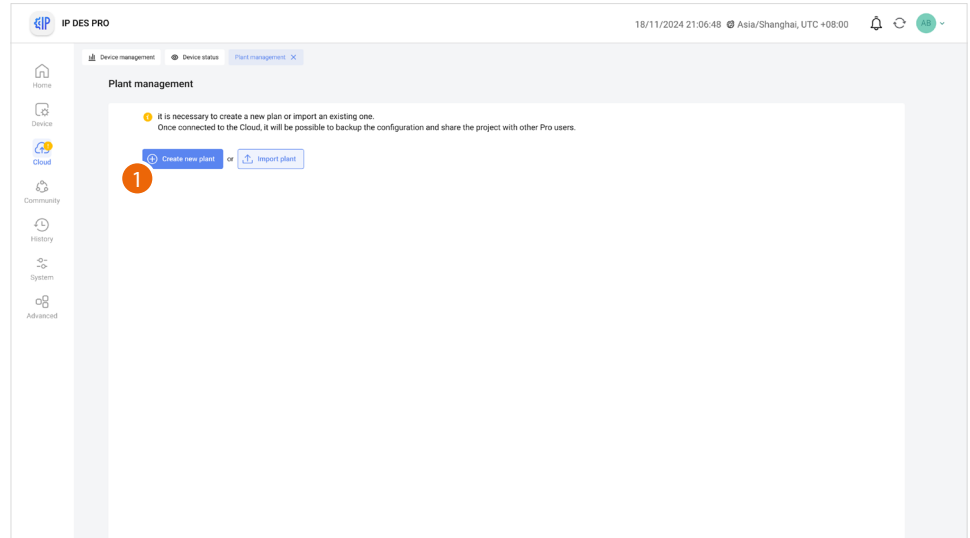
In this section you can display all the third parties to whom you granted rights to operate on your connected devices.



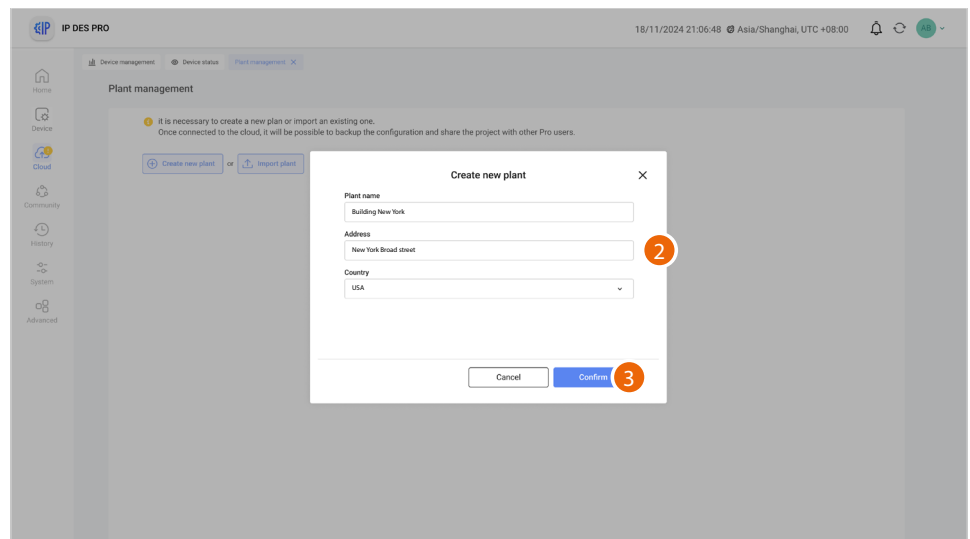
1. Click to remove the authorisation to access your details for this application.
- A Displays more information regarding the access to your home by partner Apps.

Create a Plant

This page can be used to create a Plant, saving it on the cloud; this function can be useful in order to file a configuration for use at a later date.



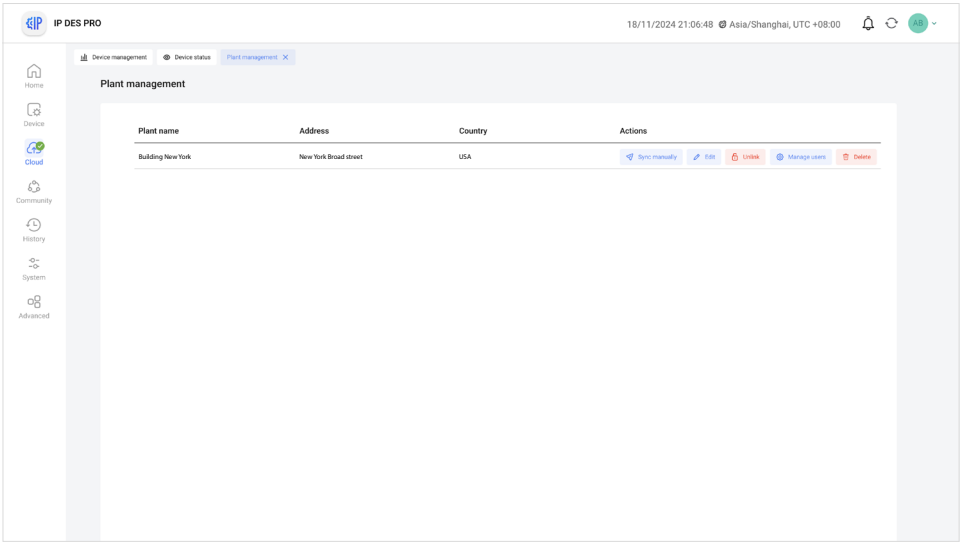
1. Click to create a new Plant



2. Enter the details of the Plant you are creating (name, address and country)
3. Click to save

GR 1 2 3 4 5 6 7 8 9 10 11 12

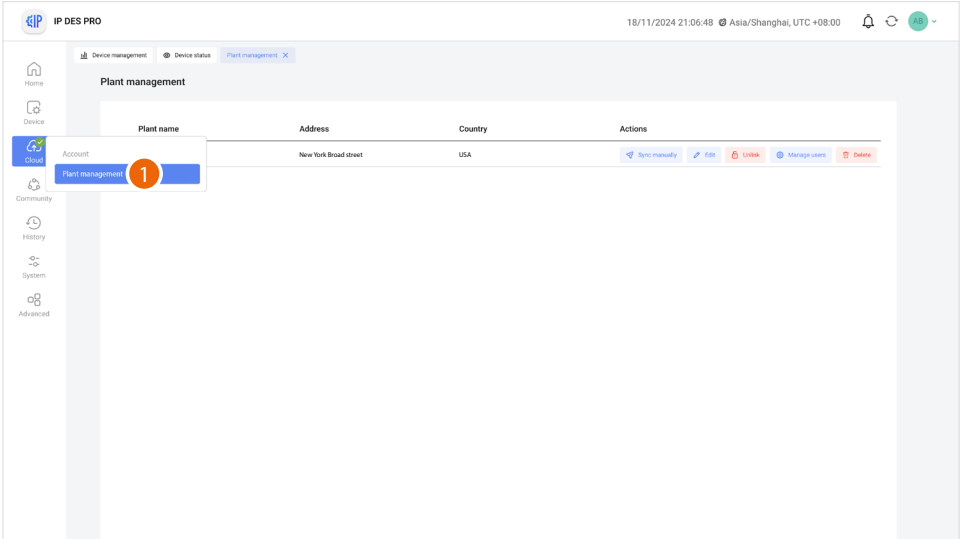
The plant is automatically synchronised



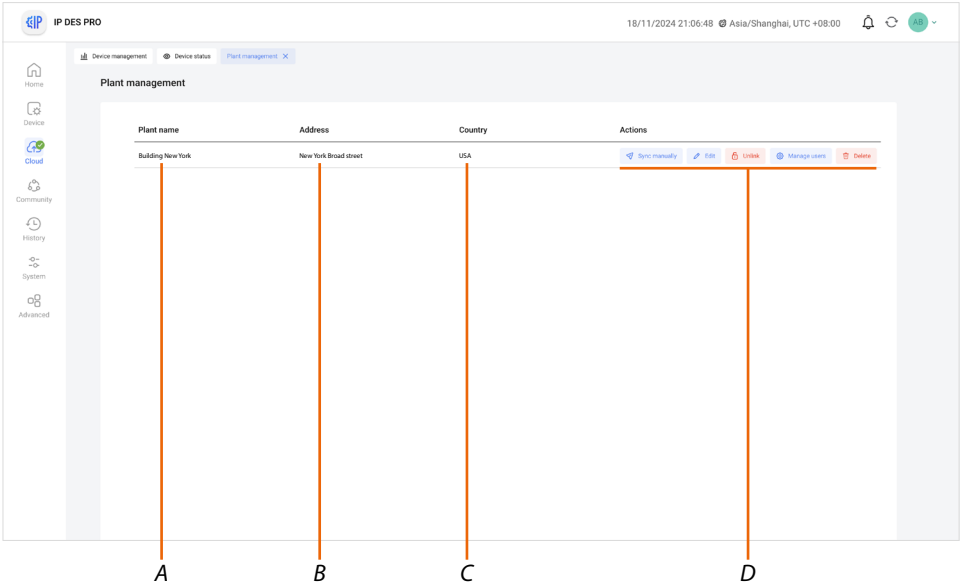
Once created, the plant remains available on the cloud.
If disconnected (unlink button), it can be retrieved from the cloud using the [Import a Plant](#) function.
If [deleted](#), it will also be deleted from the cloud.

Manage the Plant

After creation, the Plant can be managed using a number of functions on this page.



1. After completing the [authentication](#) and [creating your Plant](#), a key will become active, which when clicked will take to the Plant management page



- A Plant Name
B Plant Address
C Plant Country
D [Plant management bar](#)

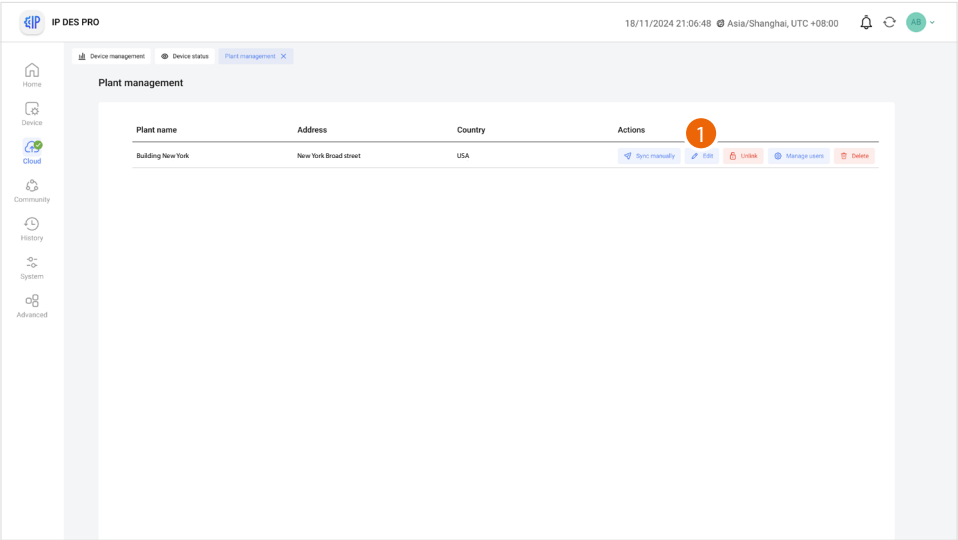
Plant management bar



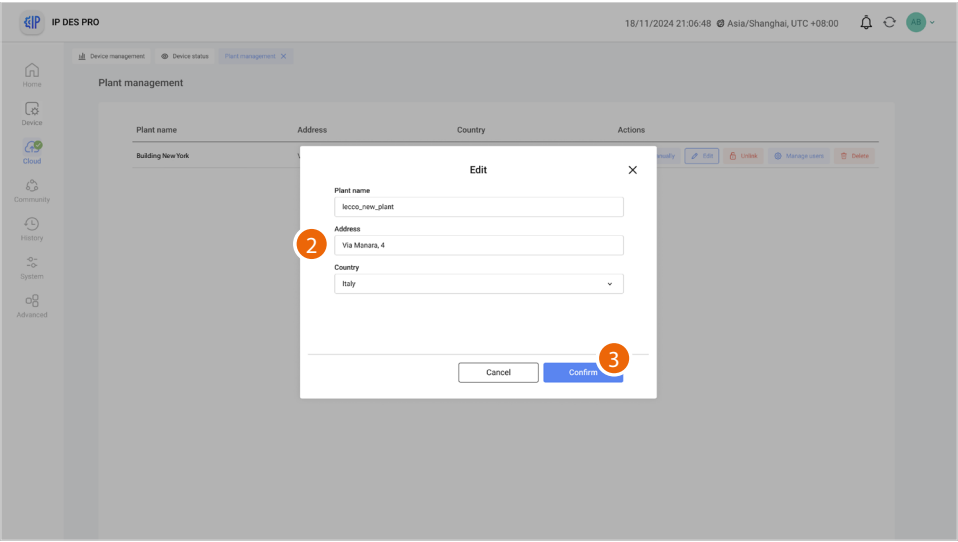
- A Synchronises the local plant with the plant stored on the cloud.
CAUTION: This operation is necessary every time changes are made to the plant.
B [Edit the plant](#)
C [Disconnect](#)
D [Manage the users](#)
E [Delete the plant](#)

Edit the Plant

This function allows to edit a Plant



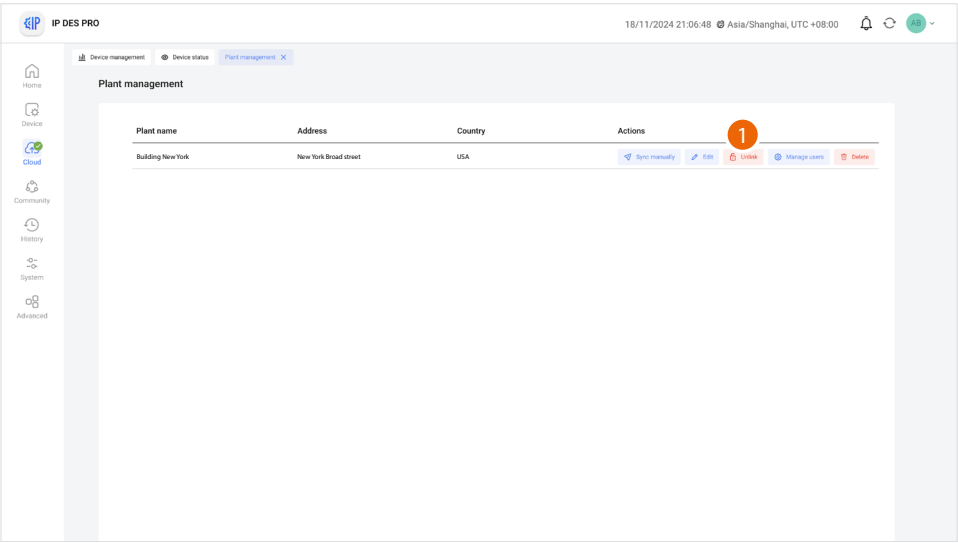
1. Click to edit the plant



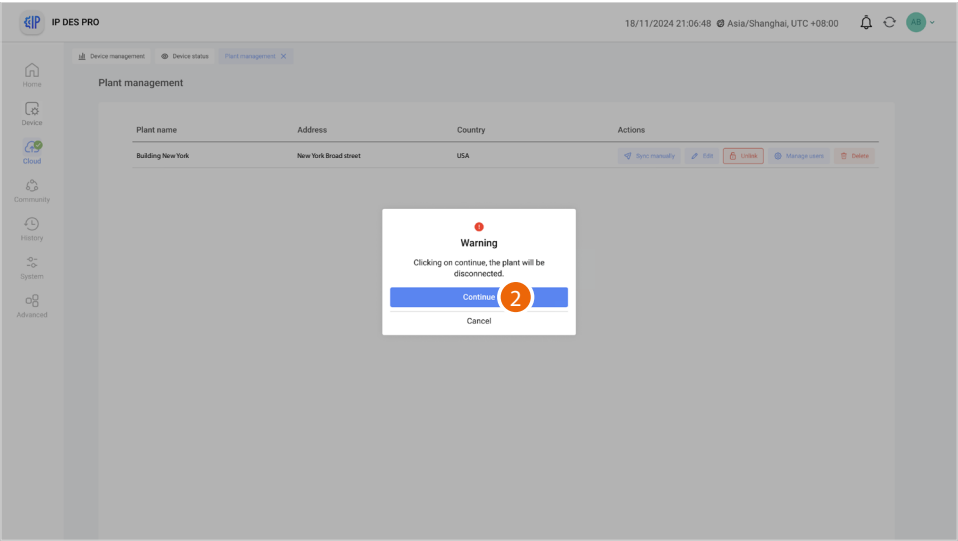
2. Edit Plant data (name, plant and country)

3. Click to save

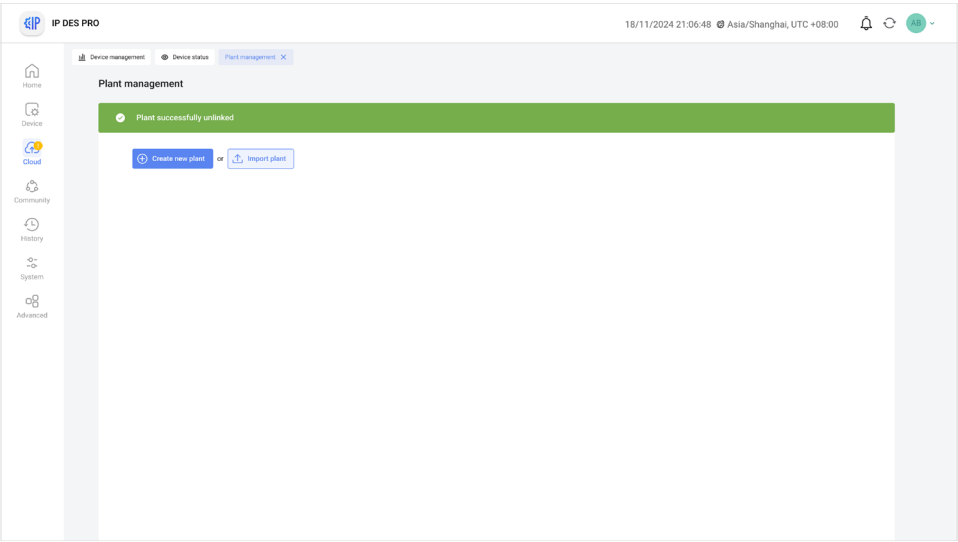
Disconnect the Plant
This function allows to disconnect a Plant from the cloud



1. Click to disconnect the plant from the cloud



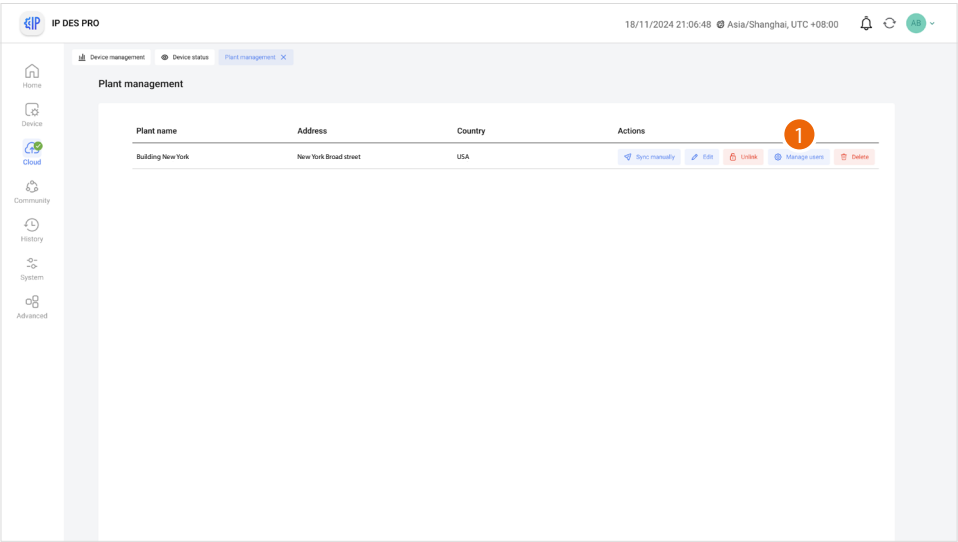
1. Click to continue and disconnect the plant
Now the plant is disconnected from the cloud, it is possible to create a new one or select and import one saved on the cloud



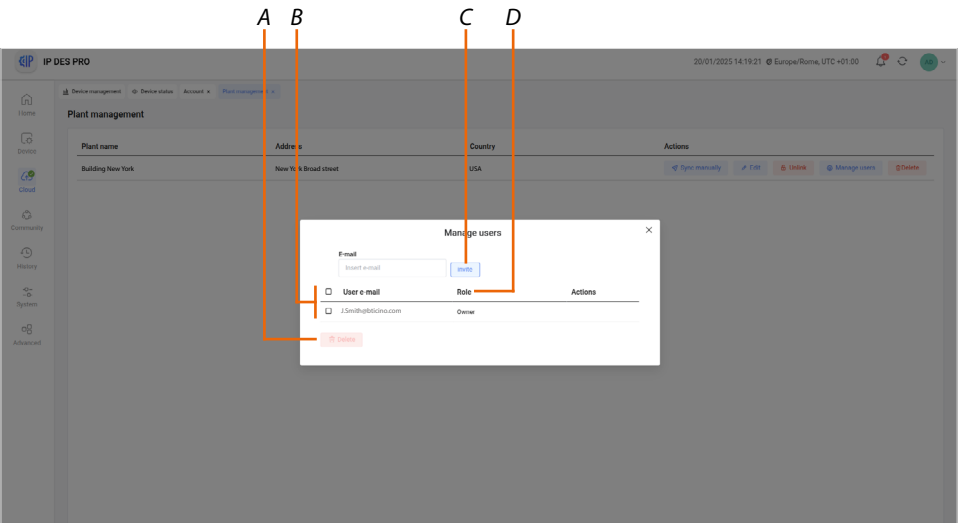
Manage the users

In this section it is possible to display the users who can interact with your plant, invite new ones or if necessary delete them (the user will not be deleted, just the possibility of interacting with this plant).

NOTE: If the Cloud includes several plants, the invited users will have the possibility of interacting with all of them.

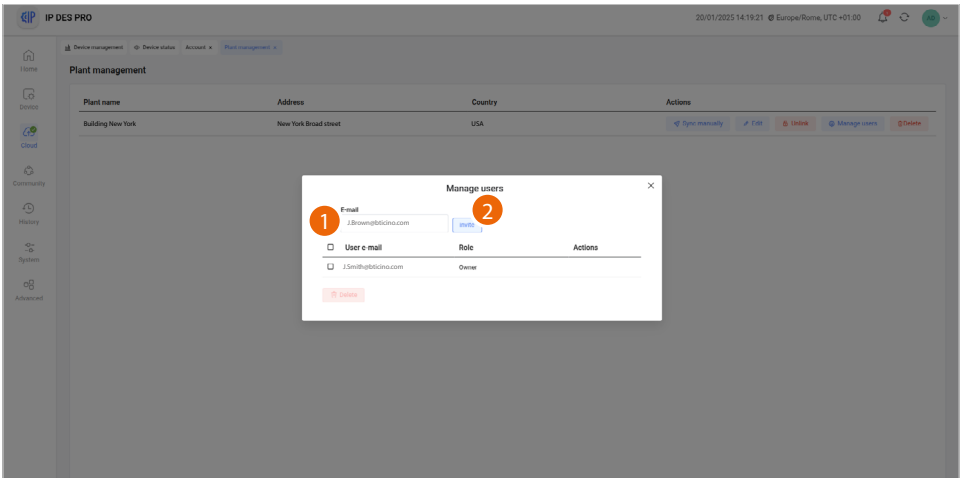


1. Click to access the guest management section

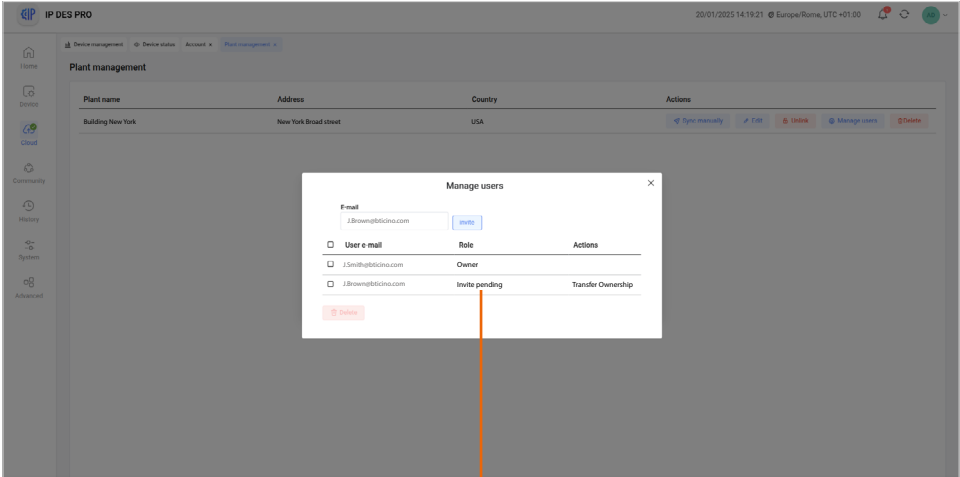


- A Delete a user
- B List of users
- C Invite a user
- D User role

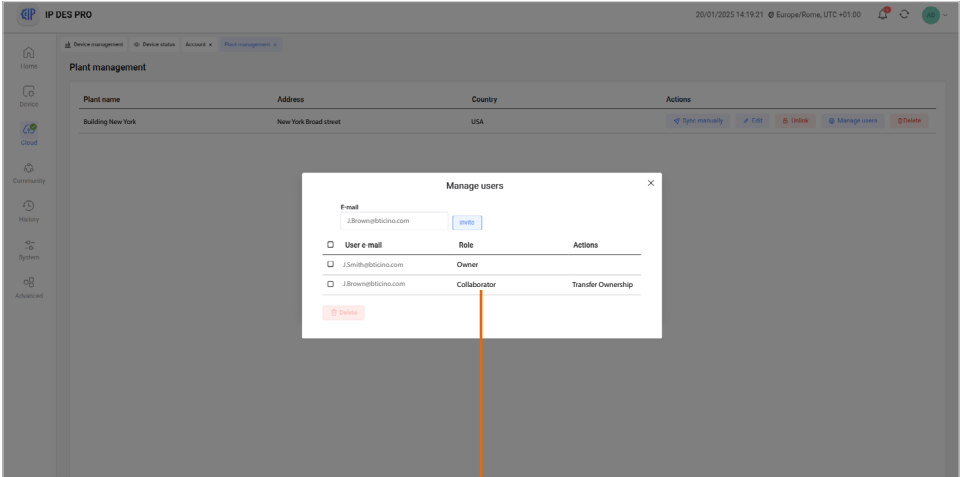
Invite a user



- 1. Insert email address of the person you want to invite
- 2. Click to confirm the invitation

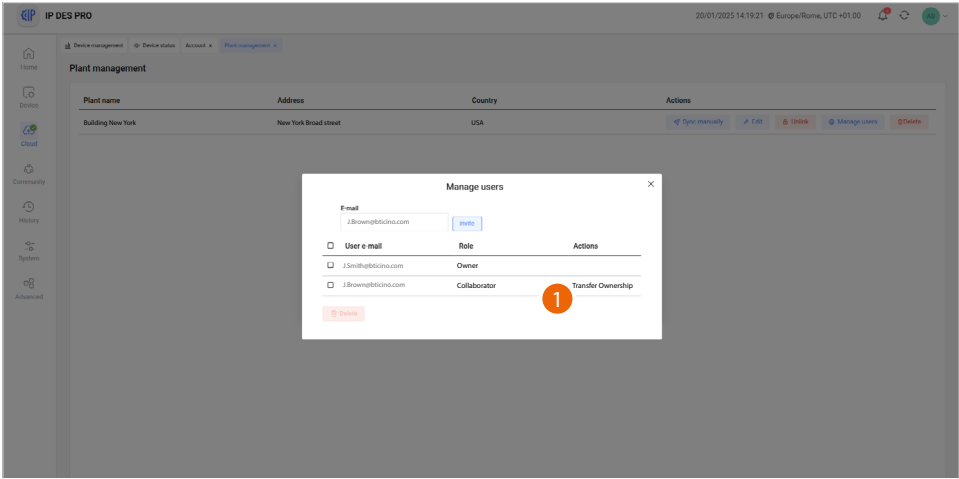


The invitation was sent.
The invited user will receive an e-mail with the invitation to check the plant. The invited user must complete the server authentication procedure using their own profile and must be registered in the Legrand Commercial Cloud. Until the invited user has completed the authentication procedure, they will appear in the list as “invited, pending” (A).

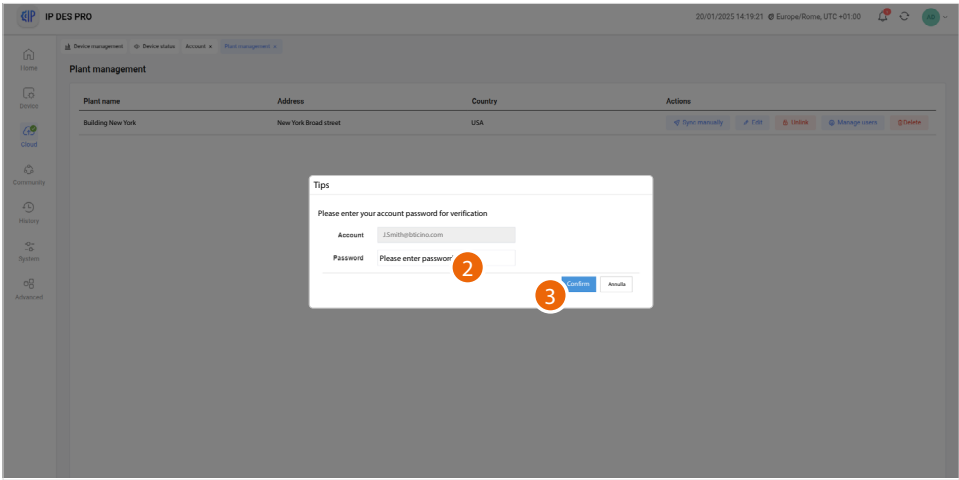


After authentication, the user will be associated to the plant and will appear in the list as “collaborator” (B).

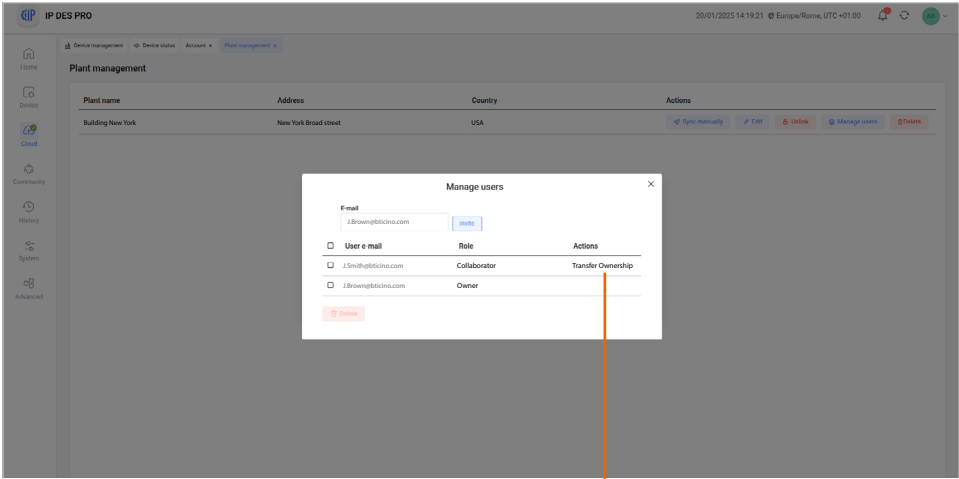
Change the user role
This function can be used to change the role of users from “Collaborator” to “Owner”



1. Click to change the role to “Owner”



2. Enter the password of the “Owner” user
3. Click to confirm



A The role of the user has been changed from “Collaborator” to “Owner”

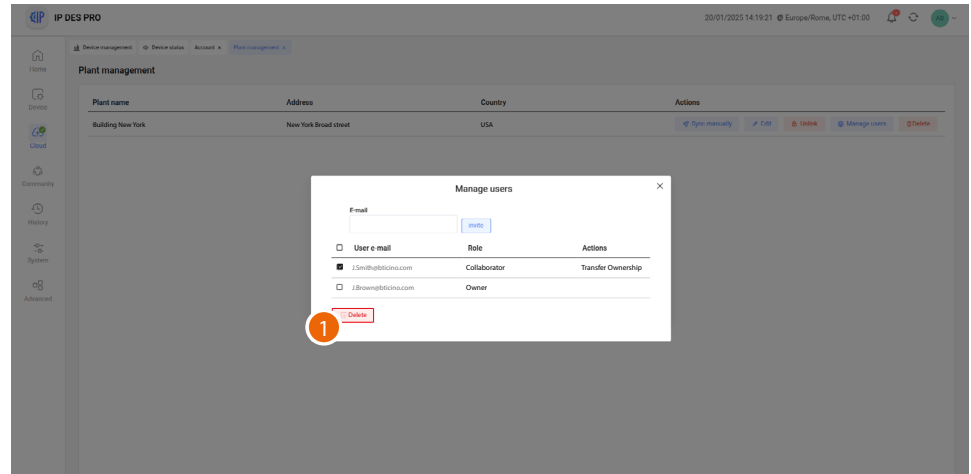
GR 1 2 3 4 5 6 7 8 9 10 11 12

Delete a user

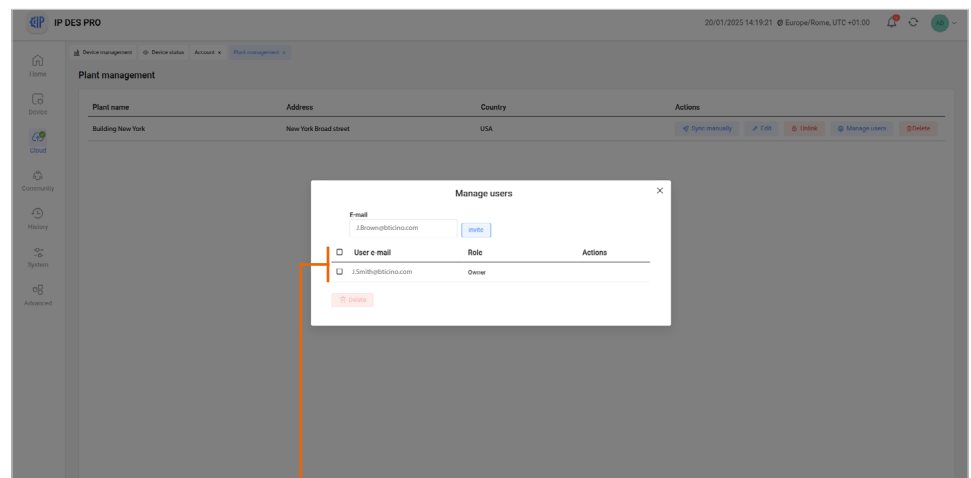
This function can be used to remove a user from plant management

NOTE: "Owner" users cannot be removed. It will be necessary to first change their role. See [Change User Role](#)

NOTE: A "Collaborator" user can only remove "Collaborator" users.



1. Click to remove a user from plant management



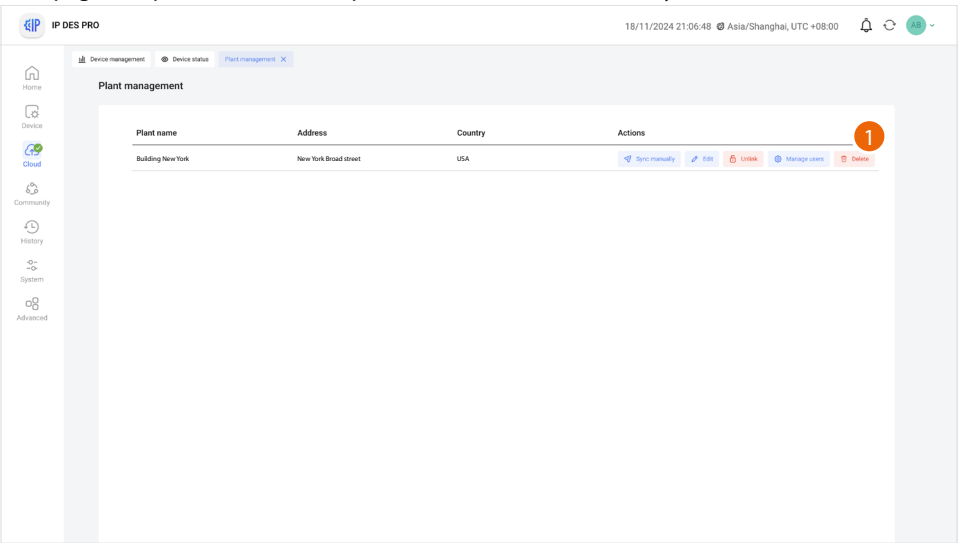
A

A The user has been correctly removed

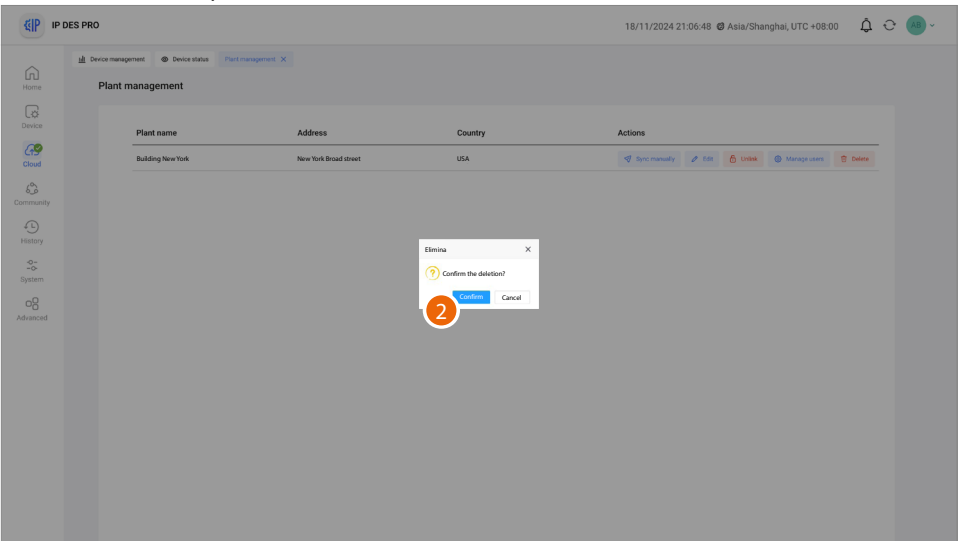
GR 1 2 3 4 5 6 7 8 9 10 11 12

Delete a Plant

In this page, it is possible to delete a plant from the Cloud definitively

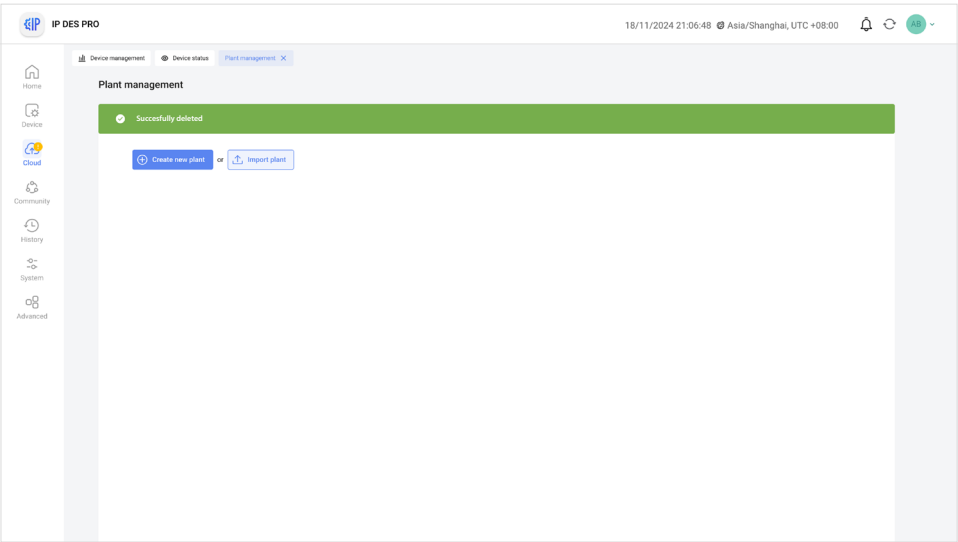


1. Click to delete the plant



2. Click to confirm

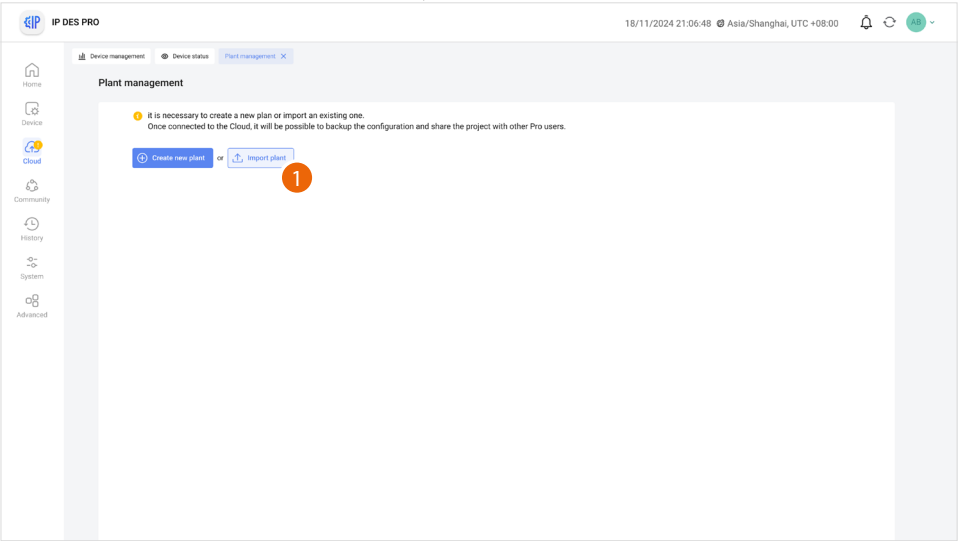
CAUTION: All the data will be lost



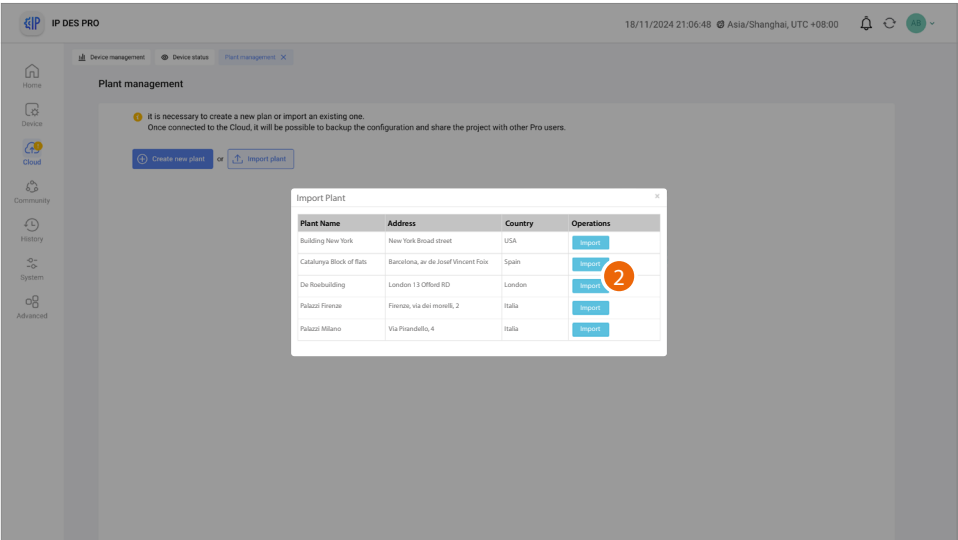
The plant was deleted from the cloud. Therefore, it is now necessary to create a new one or import another plant among those saved on the cloud.

Import a Plant

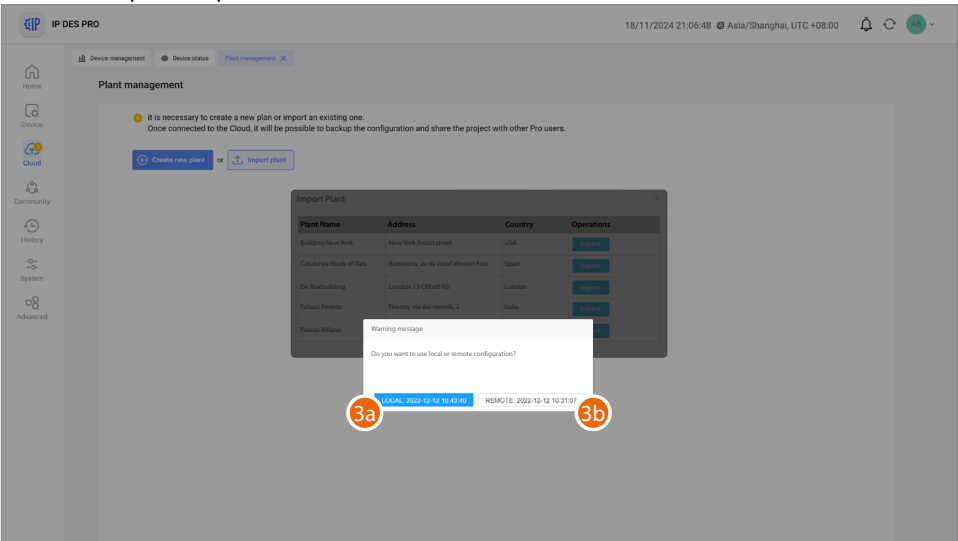
This page can be used to import a previously saved plant from the cloud



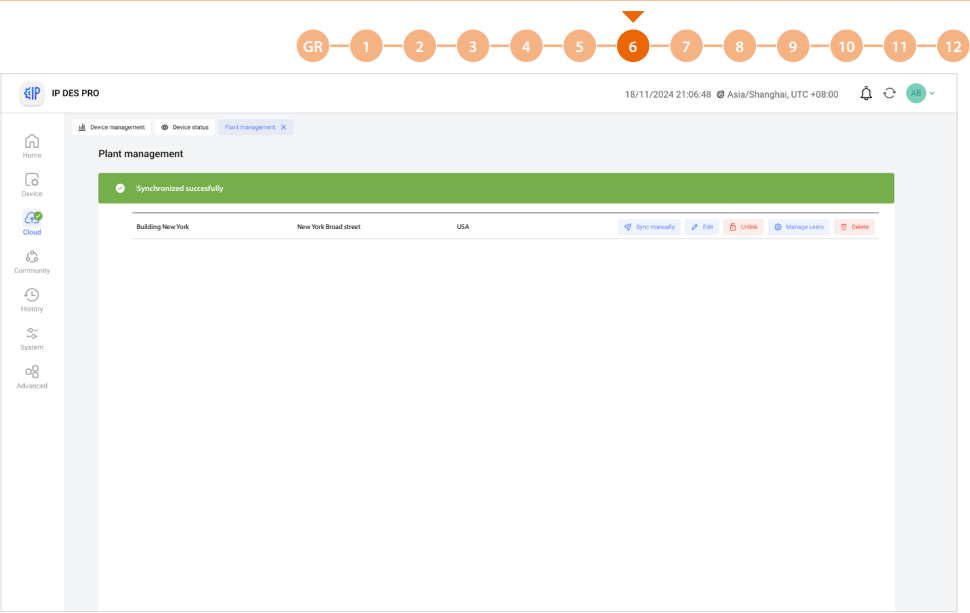
1. Click to import a Plant from those saved on the cloud.



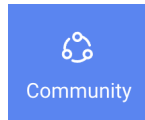
2. Click to import the plant



3a. Click to import the plant version stored on the SD or
3b. Click to import the plant version stored on the cloud
In both cases, the date and time of the last synchronisation will be indicated



The Plant has been imported

Community

This menu can be used to view and manage functions related to community accesses, such as permissions, badge/card etc.

Users profile management

Creates people in the community and associates the apartments to which they have access through personal code, fingerprint, facial recognition and card/badge.

Cards and badges configuration

Create and manages new badges for one or more people and manages the key sector

Resident user codes

Resets the Personal Access Code and the Emergency Access Code of the IU.

Messages

Creates and sends messages to devices within the community

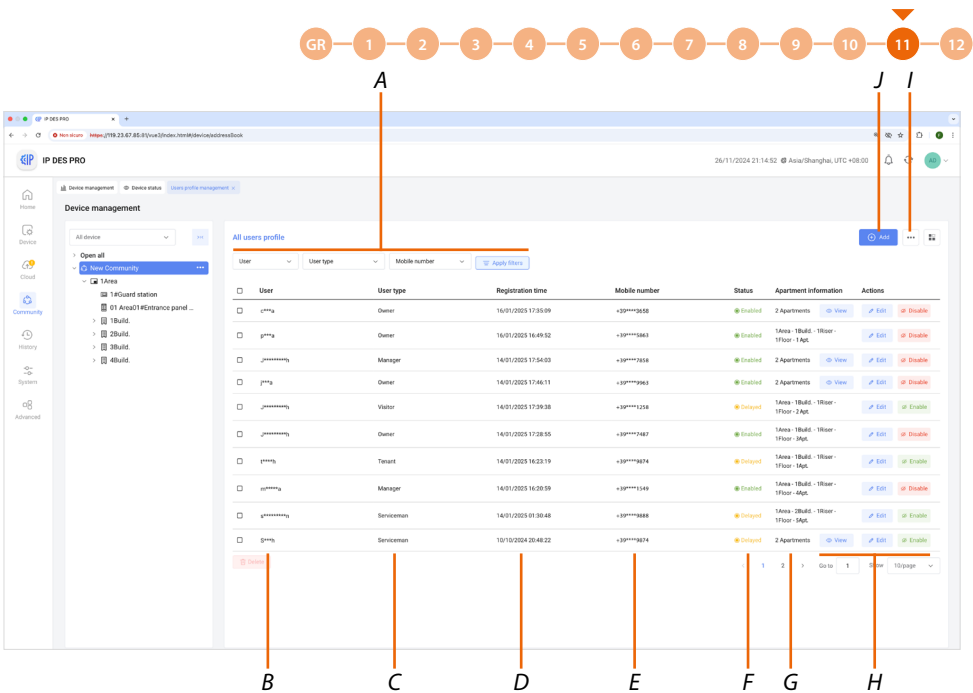
Users profile management

This page can be used to add/manage community people and give them permissions to access the structure.

When configuring the person in Personal data, the relevant apartment is defined.

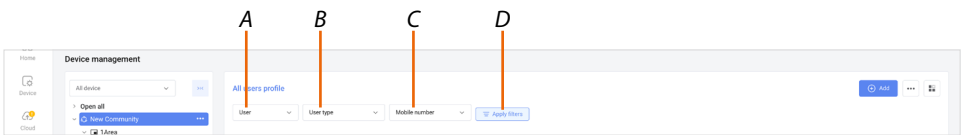
The other sub-pages are used to configure fingerprint, facial recognition and card/badge access. Default access permissions are created depending on type (see table). Other permissions can always be added or removed.

Person type	Accesses allowed by default
Owner	All accesses to reach the relevant apartment
Tenant	All the accesses to reach the relevant apartment
Visitor	All the accesses to reach the relevant apartment
Manager	All the common accesses
Cleaner	All the common accesses
Security	All the common accesses
Serviceman	No access



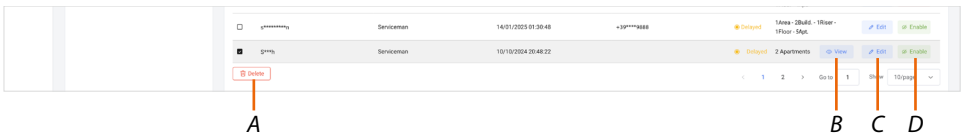
- A **Person selection filters**
- B **Name of the person**
- C **Type of person**
- D **Registration date and time**
- E **Telephone number**
- F **Person status (enabled/disabled)**
- G **Apartment address to which the person has access**
- H **Person management keys**
- I **Export users list in .xls: exports a file containing the details of the residents**
[Download the template/Import users list in .xls](#)
- J **Add a new person**

Filters



- A **Name and surname**
- B **Type of person**
- C **Telephone number**
- D **Apply the filters**

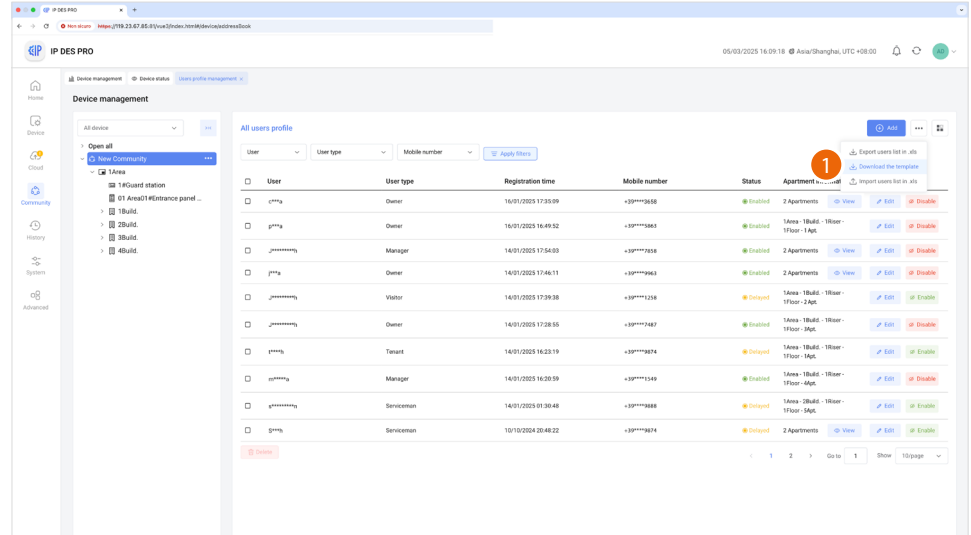
Person management keys



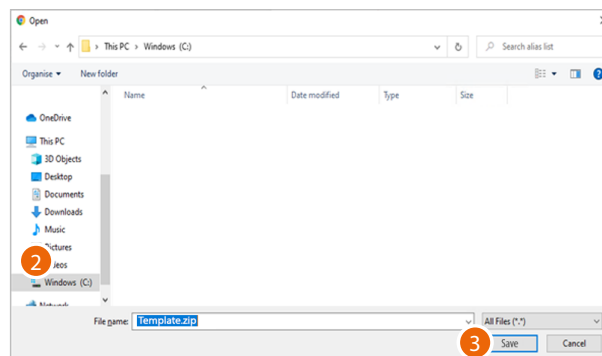
- A **Delete the selected person**
- B **View the apartments to which the person has access.**
The key only appears if access to more than one apartment is granted.
- C **Open the person management panel**
- D **Disable the person.**
In this case, the person is still present but cannot access the apartment

Creation of multiple residents at the same time

This procedure can be used to create multiple residents at the same time, also including face recognition biometric data.



1. Click to download the template in .zip format



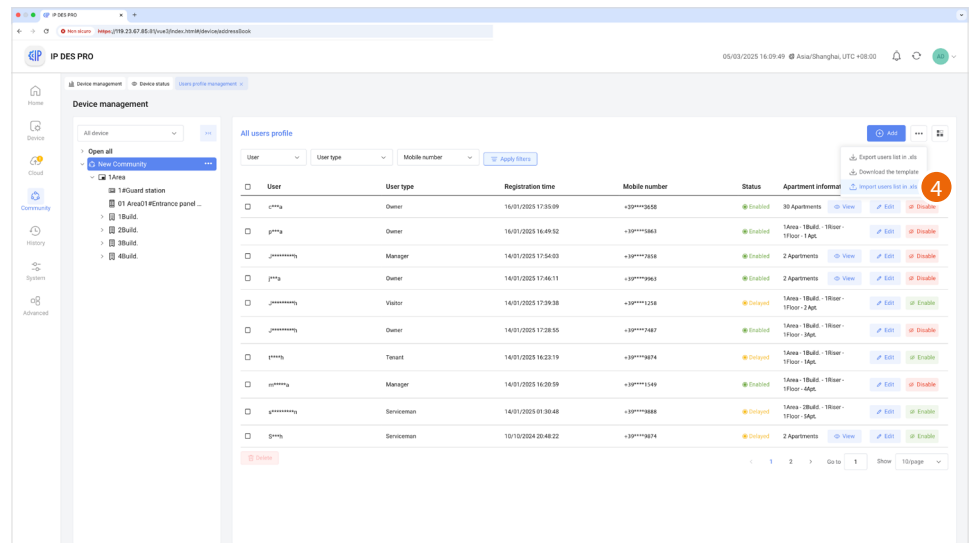
2. Select the location where to save the file
3. Click to save

A .zip folder is downloaded, containing an .xlsx file and a folder with 2 example images inside. The .xlsx file needs to be used as a base, entering the data of the new residents to be imported, while the actual images of the residents must be saved in the folder (the one containing the 2 example images).

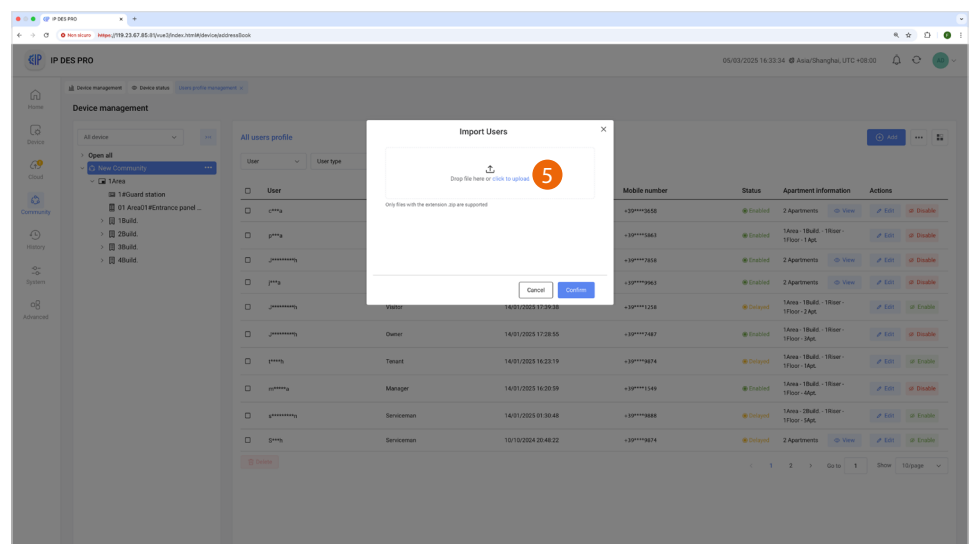
NOTE: The image must be:

- 200 x 200 pixels;
- use a front image with a pale background;
- the background should be free of any shadows;
- there must be nothing in the image covering facial features and the person must not wear heavy makeup.
- The face in the image must not be wearing spectacles with anti-reflective lenses or blue light sensitive lenses
- The image should have even light and a natural expression

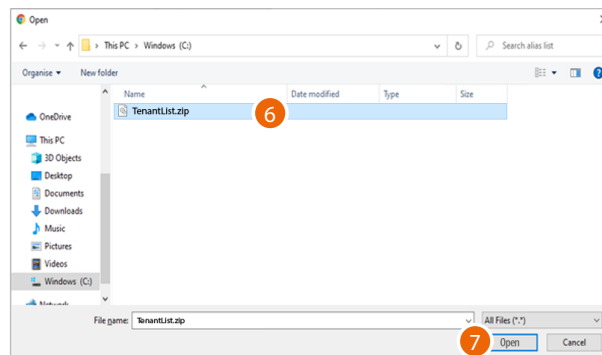
After completing all these steps, it will be necessary to recreate a .zip folder just like the one downloaded.



4. Click to import the template in .zip format

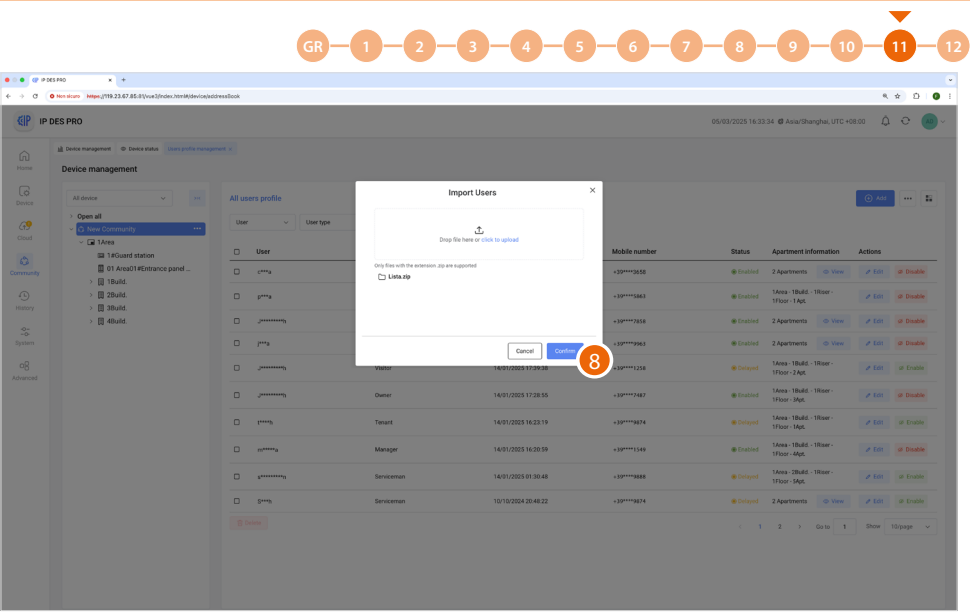


5. Click to upload the .zip file



6. Select the file (.zip)

7. Click to open

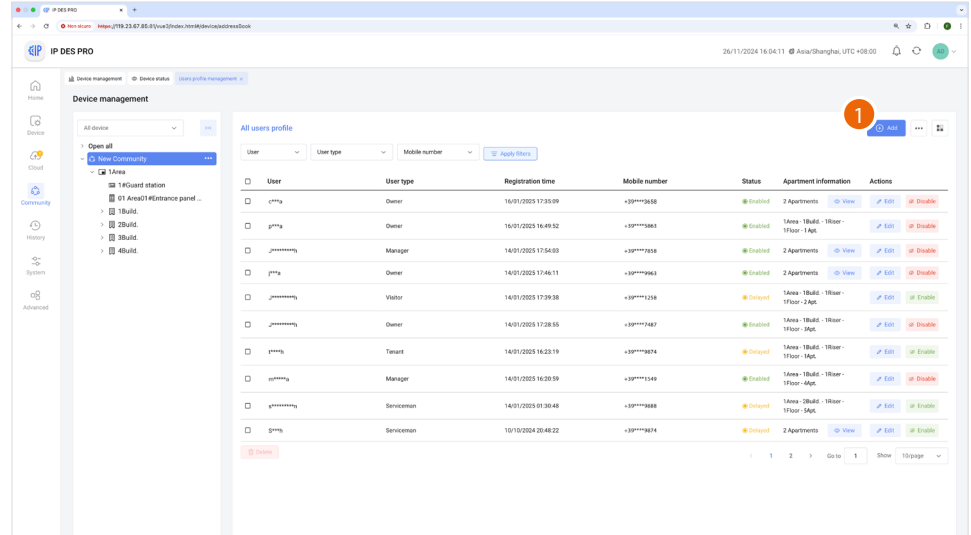


8. Click to import the data

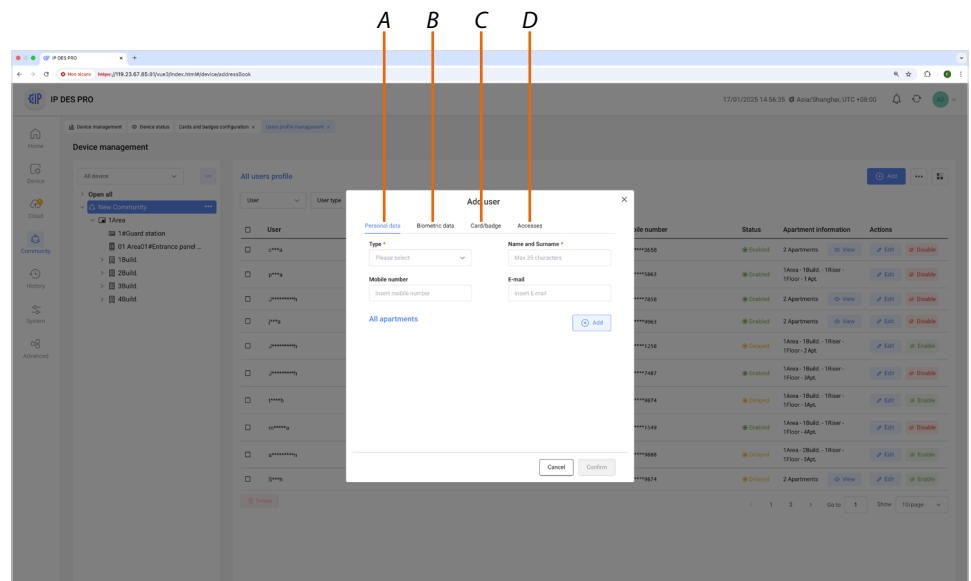
NOTE: If the import is not successful, check the configuration again

Add a person

This page can be used to create a person and define which tools they can use to access the associated apartment.



1. Click to add a new person.



- A **Sets the personal data** of the person and defines the apartments to which they have access
- B **Fingerprint and face registration** for fingerprint and face recognition access
- C **Creates and manages cards/badges** in an advanced manner and manages key sectors
- D **Manages the accesses** defined in Personal data

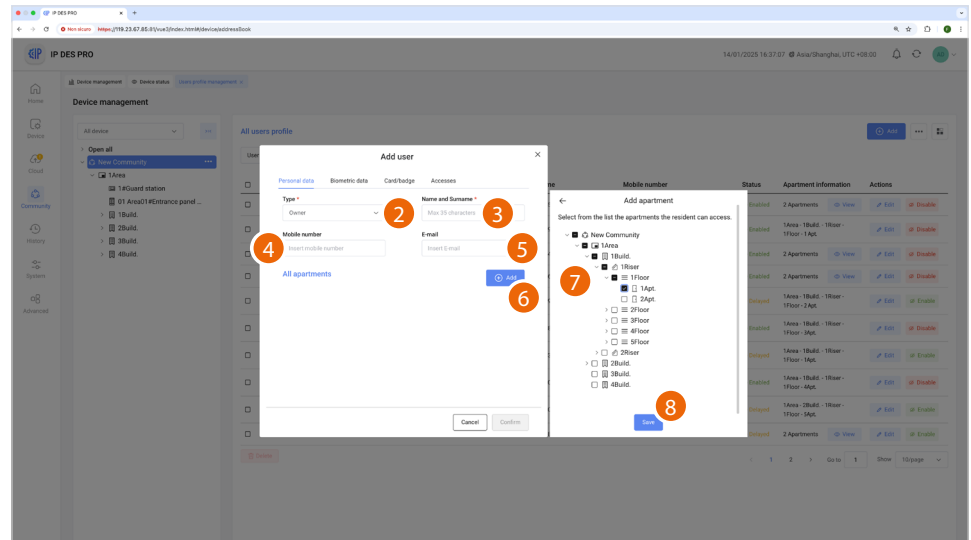
Personal Data

To begin with, it will be necessary to enter the account details and type, followed by the indication of the associated apartment.

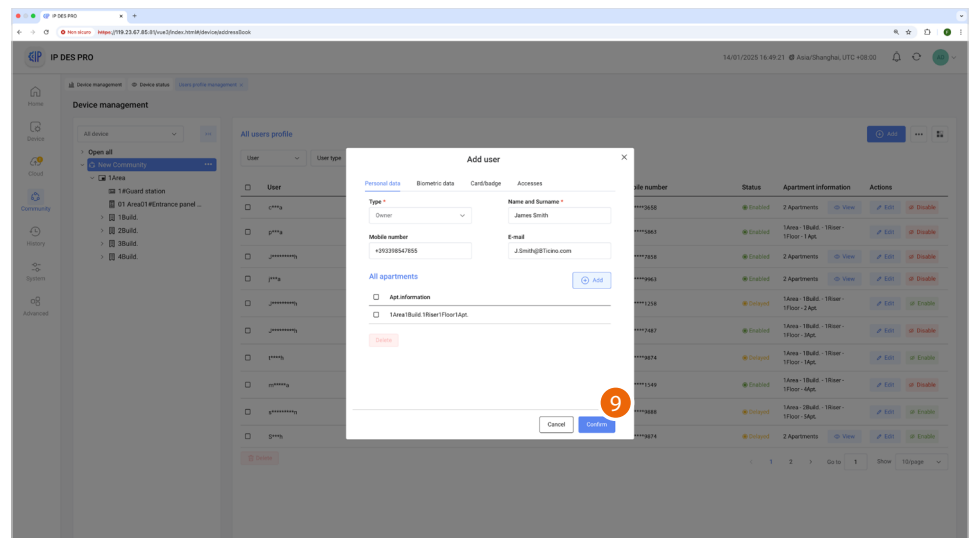
The configuration of this page allows to access the apartment via a personal code.

NOTE: The configuration of the tools depends on the type of person; the differences in configuration according to the type of person are highlighted below for each subpage.

Owner



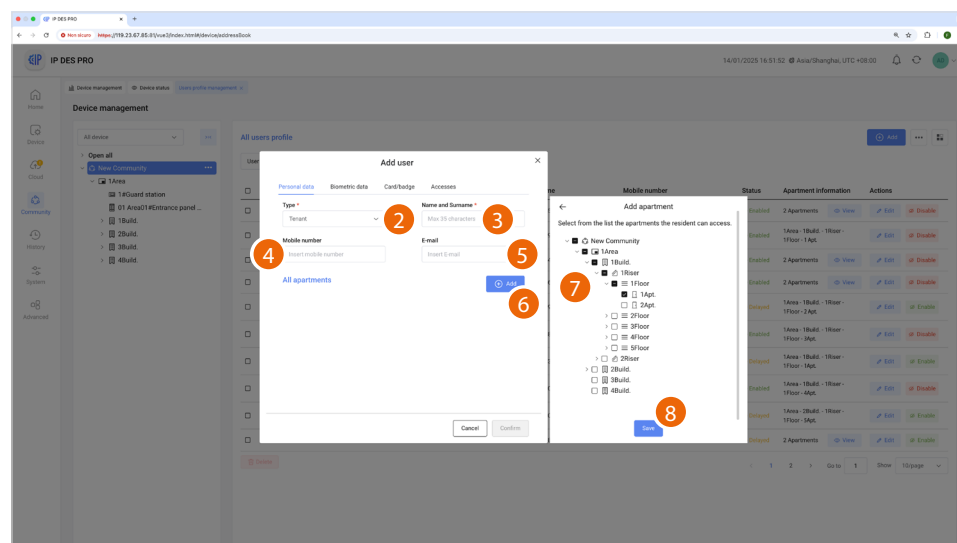
2. Select the type of person
3. Enter the name and surname of the person
4. Enter the telephone number of the person
5. Enter the email address of the person
6. Click to open the panel showing the Community structure
7. Select the person's apartment
8. Click to save



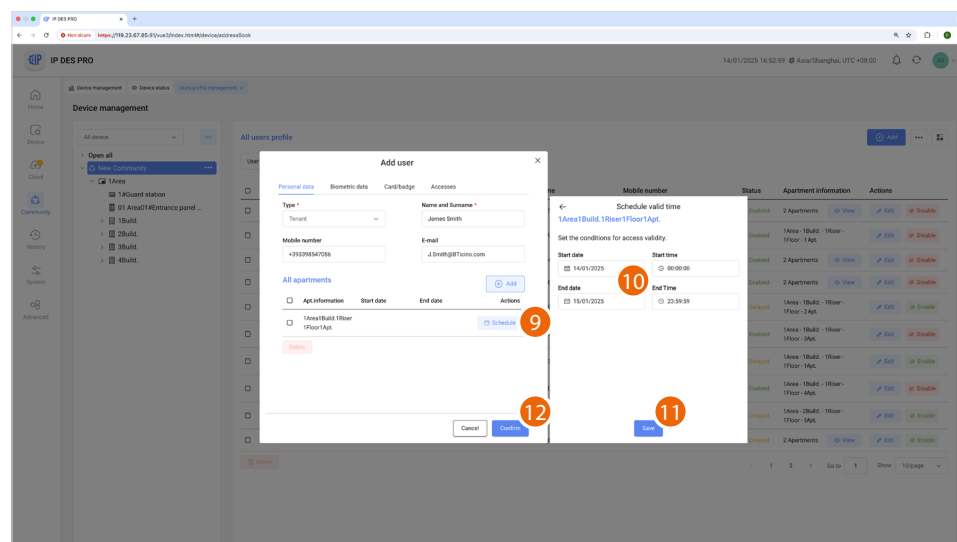
9. Click to add the person

NOTE: To access the Biometric data, Card/badge and Accesses sections, the person must first be added.

Tenant, Visitor



2. Select the type of person
3. Enter the name and surname of the person
4. Enter the telephone number of the person
5. Enter the email address of the person
6. Click to open the panel showing the Community structure
7. Select the person's apartment
8. Click to save

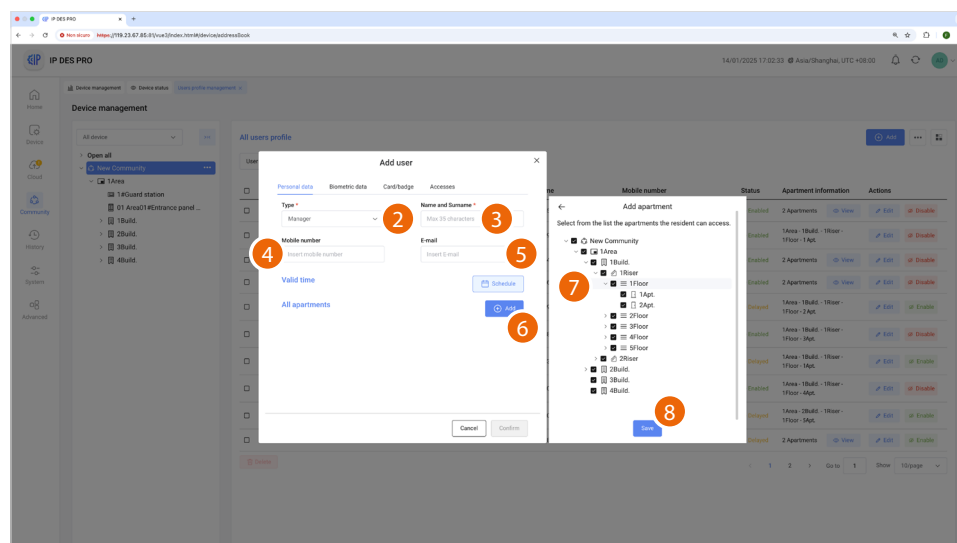


For this type, it is possible to define a time interval during which the user can access all apartments.

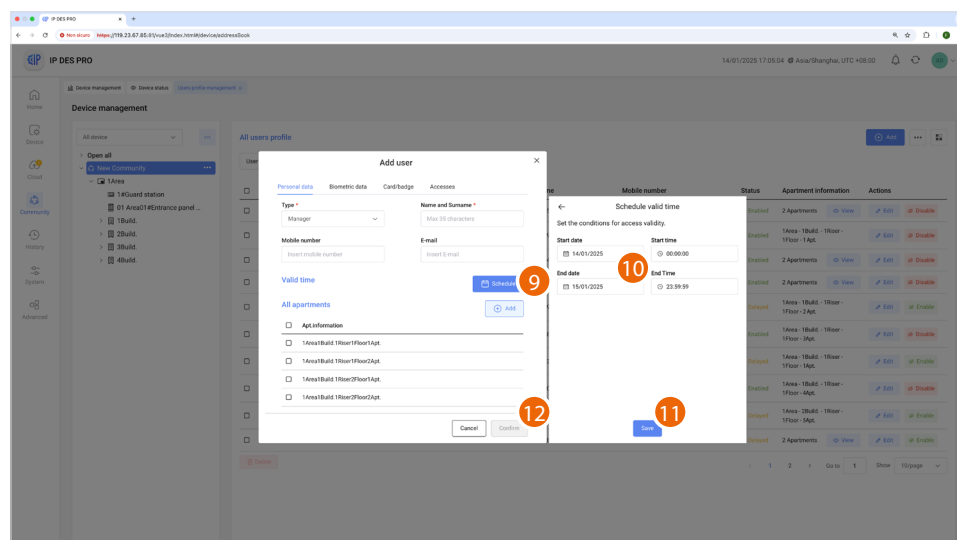
9. Click to open the scheduling panel
10. Define the access time interval
11. Click to save
12. Click to add the person

NOTE: To access the Biometric data, Card/badge and Accesses sections, the person must first be added

Manager, Cleaner, Security, Serviceman



2. Select the type of person
3. Enter the name and surname of the person
4. Enter the telephone number of the person
5. Enter the email address of the person
6. Click to open the panel showing the Community structure
7. Select the person's apartment
8. Click to save



For this type, it is possible to define a time interval during which the user can access all apartments.

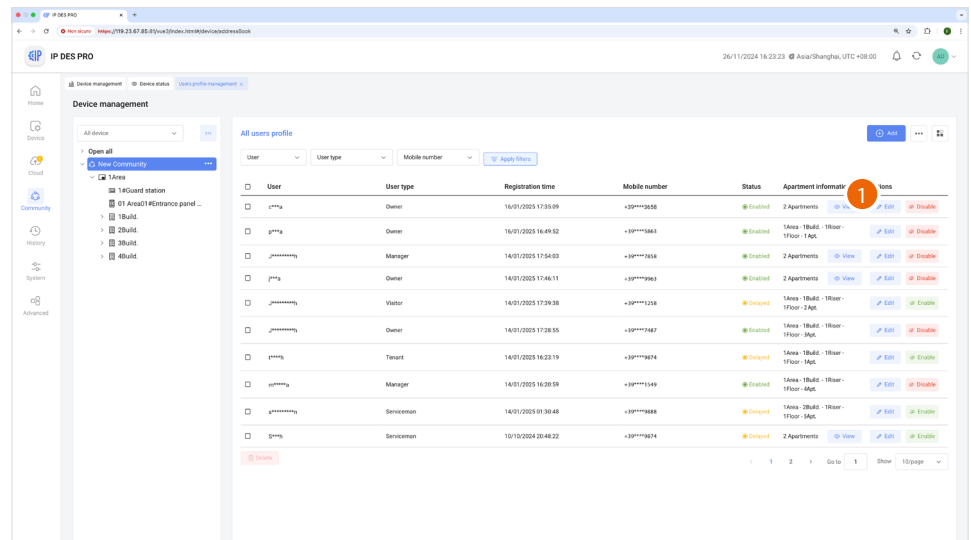
9. Click to open the scheduling panel
10. Define the access time interval
11. Click to save
12. Click to add the person

NOTE: To access the Biometric data, Card/badge and Accesses sections, it will first be necessary to add the person.

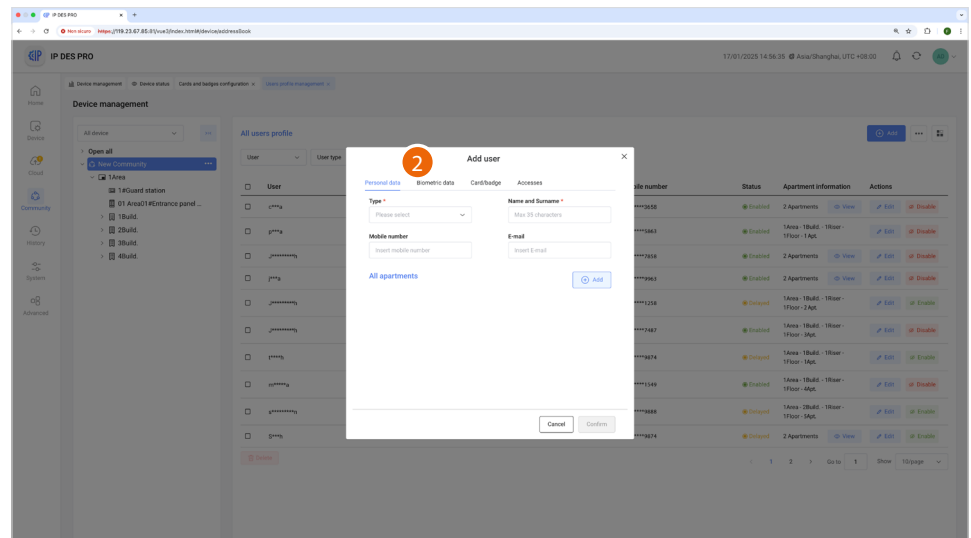
Biometric Data

This page can be used to enable fingerprint and Facial Recognition* access, based on EP type

***NOTE:** The Face recognition function is only available with USB enable stick 375011, to be purchased separately. The USB stick must be permanently connected to the SD



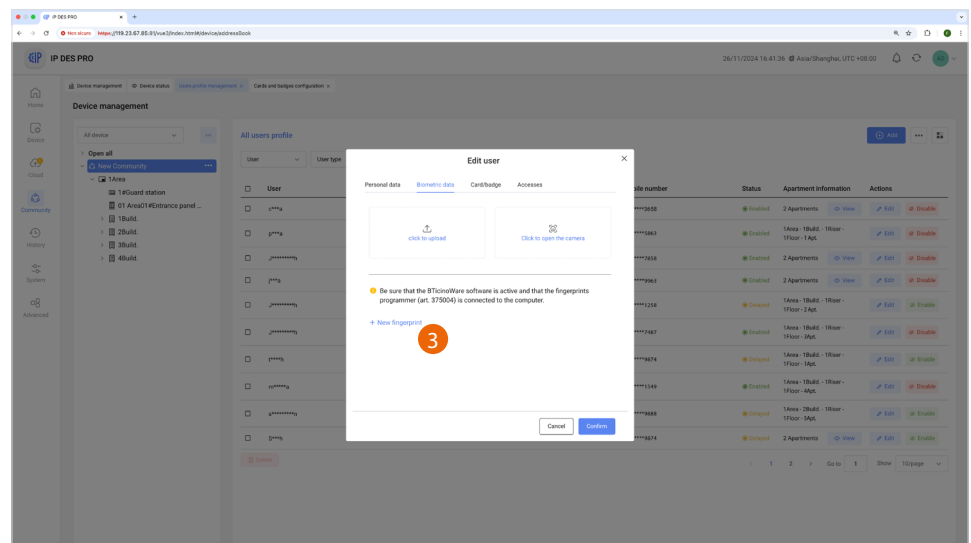
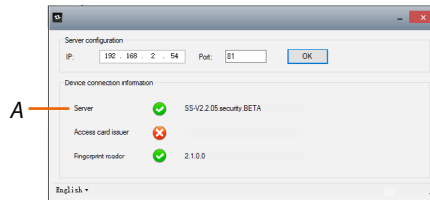
1. Click to modify the person



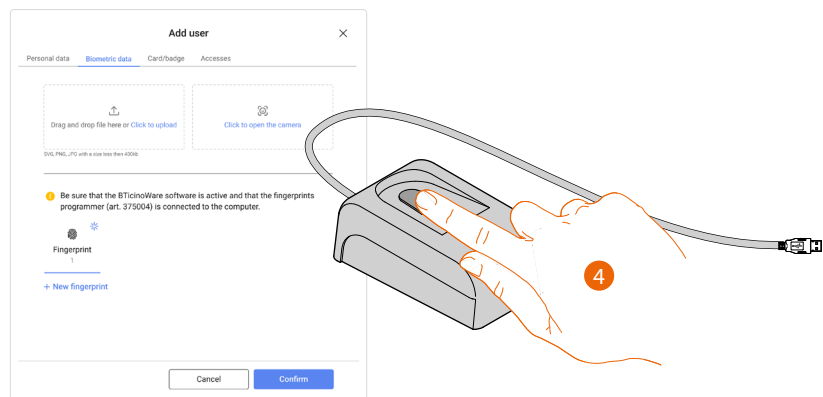
2. Click to open the section for registering one or more fingerprints.

GR 1 2 3 4 5 6 7 8 9 10 11 12

NOTE: the registration of fingerprints requires the installation of the BTicino ware software in the system. Also make sure that a fingerprint reader (item 375004) is connected to the Windows Client PC. Check that the Server A flag is green.

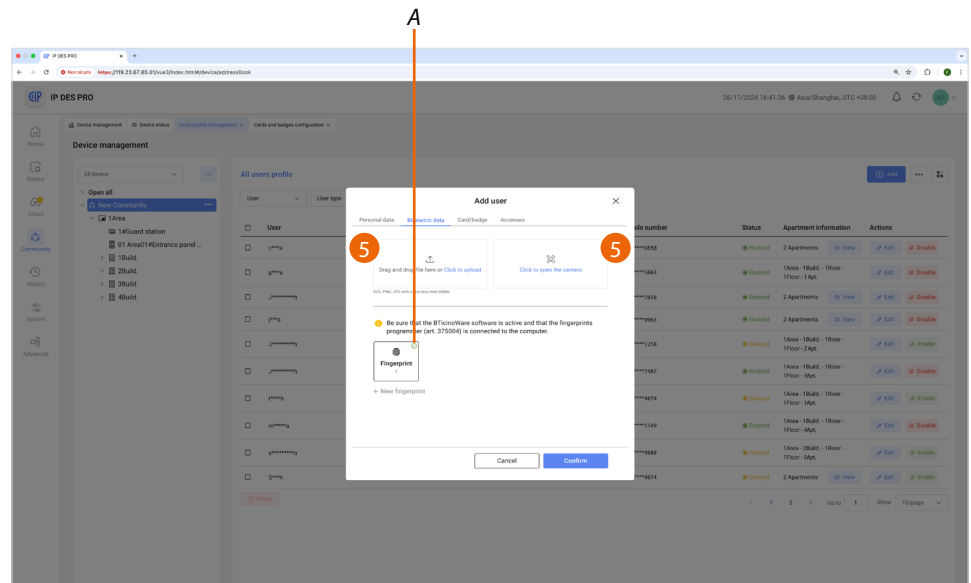


- Click to register one or more fingerprints (max. 5) to access the apartment using fingerprint recognition



- Place the finger to be registered on the reader, raising and lowering the tip until the box on the software turns green

Fingerprints registered correctly (A)



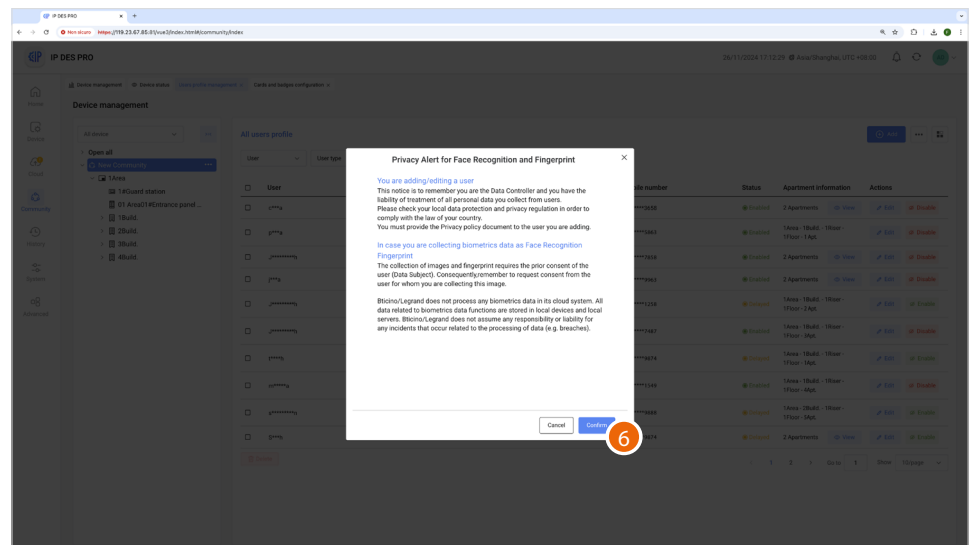
5. Click to register the image used for Facial Recognition*.

The image can be registered in 2 ways:

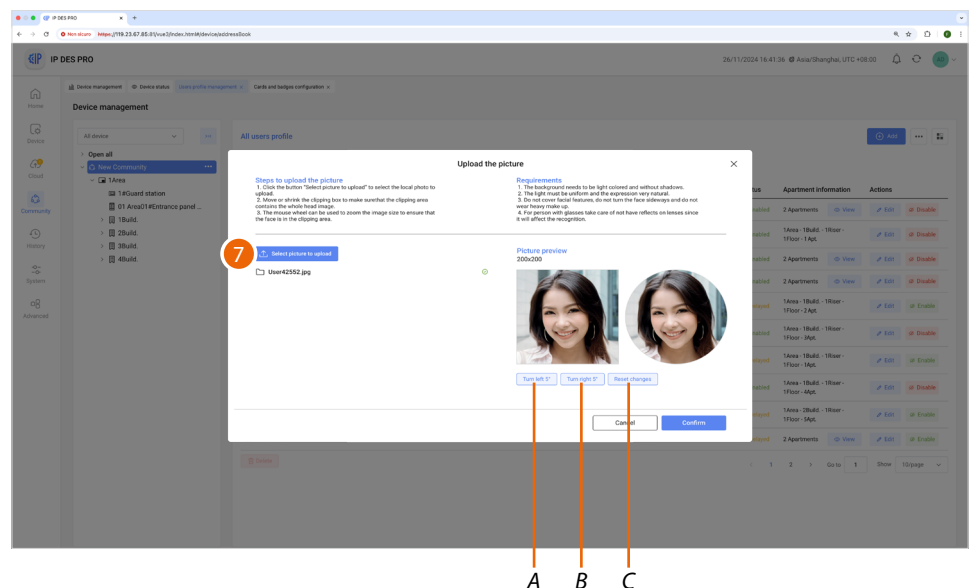
- **import an image** previously saved in the Windows Client PC.
- **capture the image using the** Windows Client PC **camera**

***NOTE:** The Face recognition function is only available with USB enable stick 375011, to be purchased separately. The USB stick must be permanently connected to the SD

Import an image



6. Click to give consent to data processing



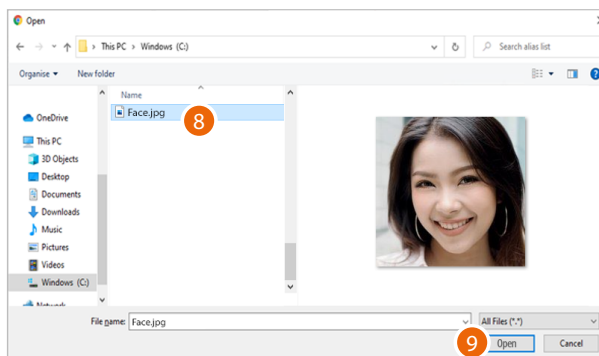
A Rotate image 5° to the left

B Rotate image 5° to the right

C Delete changes

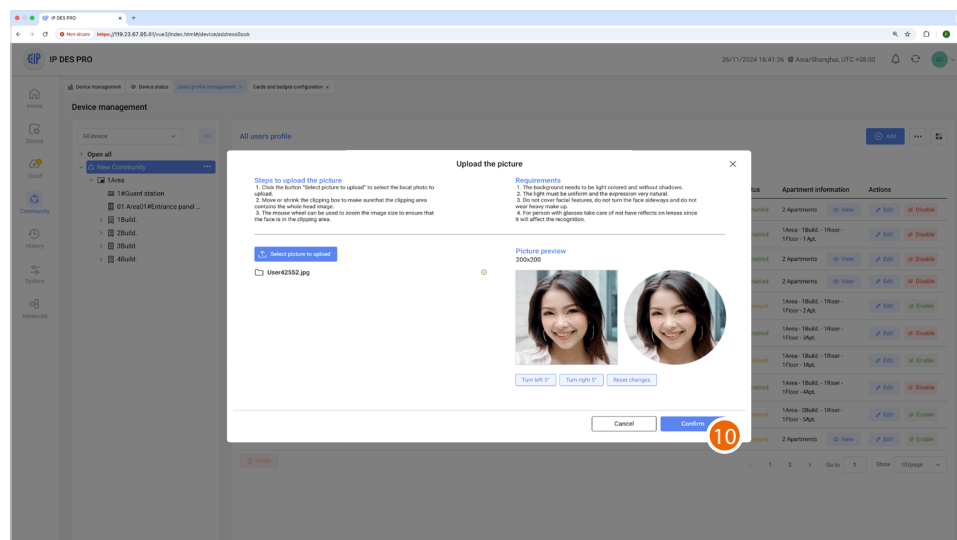
7. Click to select an image from disc
 - The image must be 200 x 200 pixels
 - Face the camera, looking at the lens
 - Use a front image with a pale background
 - The background should be free of any shadows; do not cover facial features and do not wear heavy make-up
 - Do not wear spectacles with anti-reflective lenses or blue light sensitive lenses
 - The image should have even light and a natural expression
 - Move your face near the camera so that the contour of the face matches the sample shape on the screen

GR 1 2 3 4 5 6 7 8 9 10 11 12

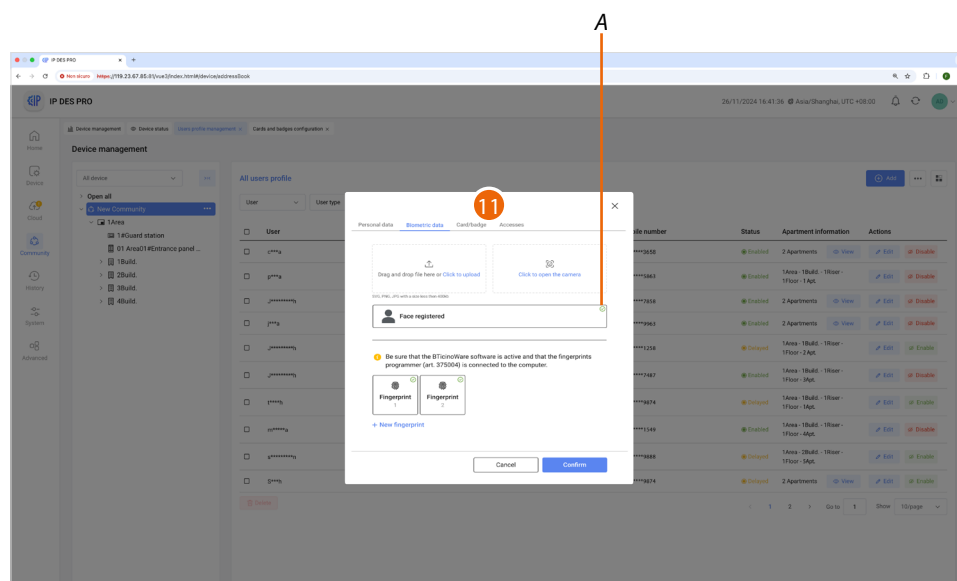


8. Select an image

9. Click to open



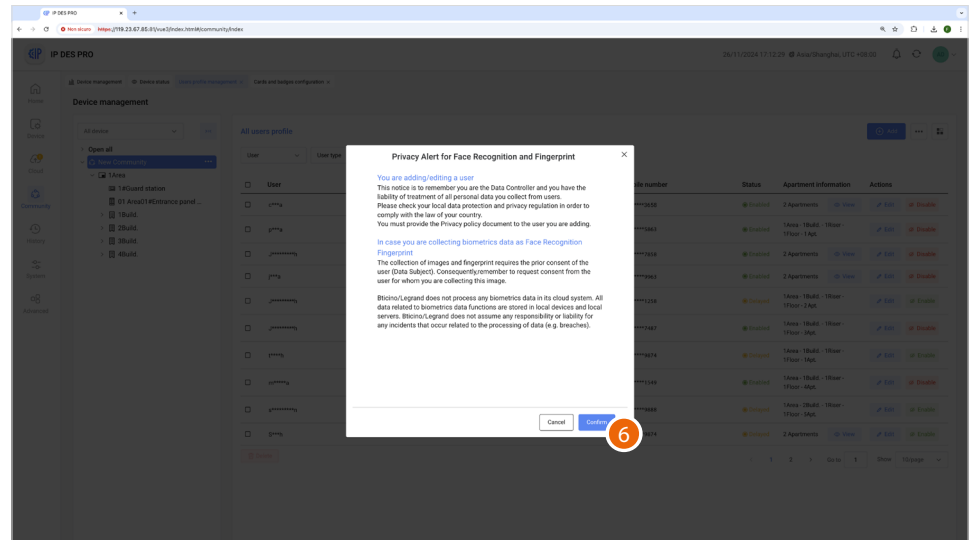
10. Click to finish



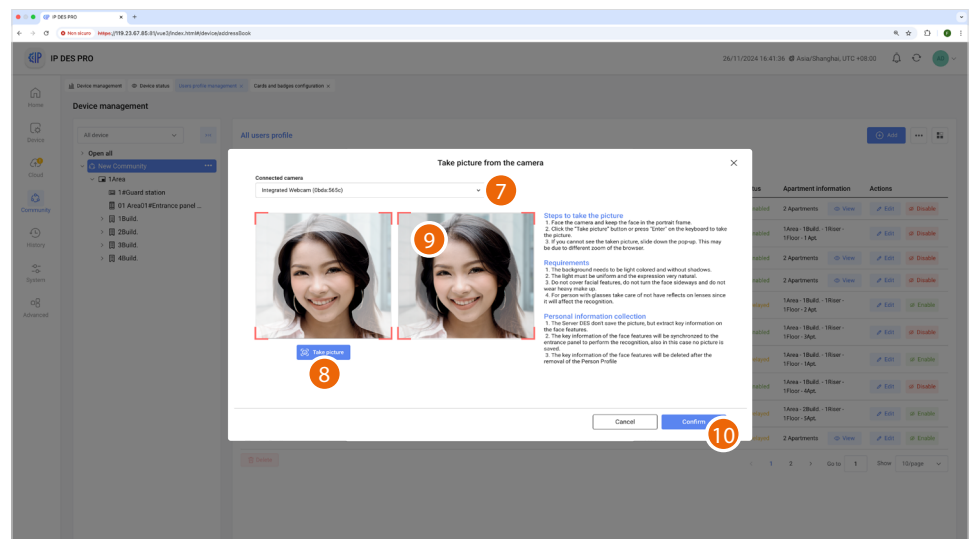
A Face registered correctly

11. Click to open the section for the **registration of one or more cards/badges**.

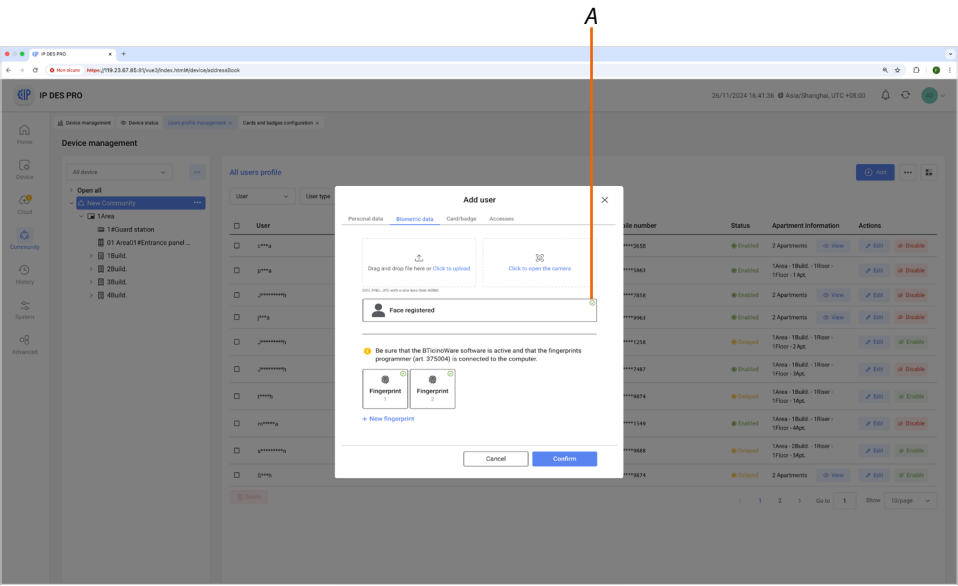
Capture the image using the camera



6. Click to give consent to data processing



7. Select the camera
 - Face the camera, looking at the lens
 - Use a front image with a pale background
 - The background should be free of any shadows; do not cover facial features and do not wear heavy make-up
 - Do not wear spectacles with anti-reflective lenses or blue light sensitive lenses
 - The image should have even light and a natural expression
 - Move your face near the camera so that the contour of the face matches the sample shape on the screen
8. Click to acquire the image
9. Check the preview
10. Click to save it



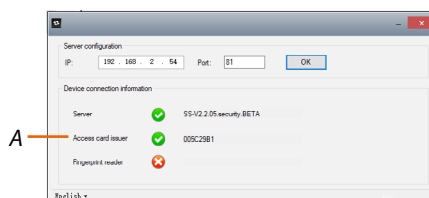
A Face registered correctly

Card/badge

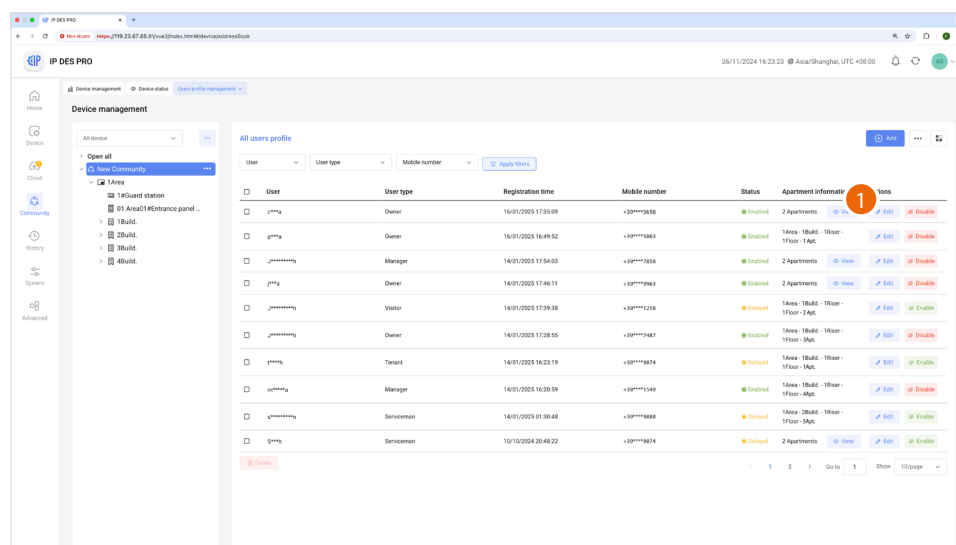
This page can be used to enable badge/card access.

NOTE: The configuration of the tools depends on the type of person; the differences in configuration according to the type of person are highlighted below for each subpage.

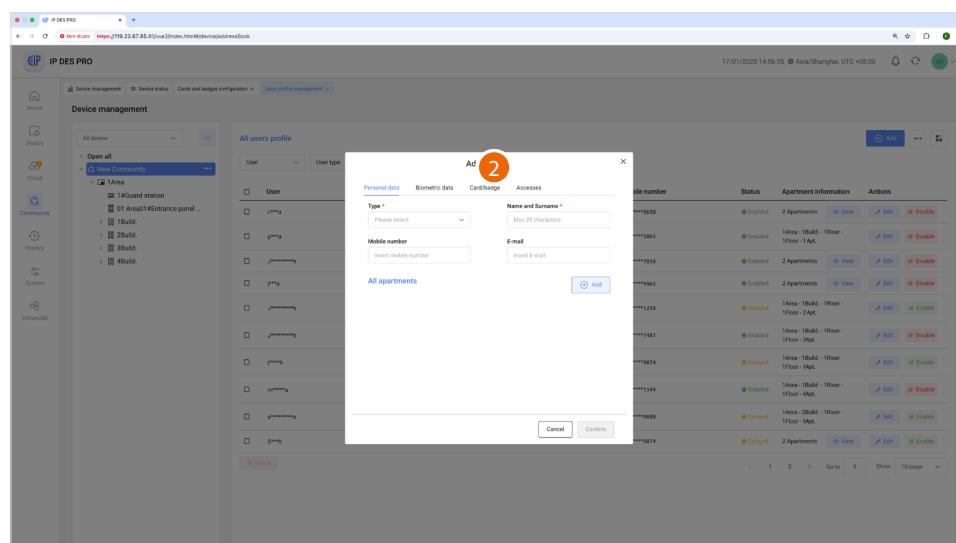
NOTE: the registration of badge/card requires the installation of the BTicino ware software in the system. Also make sure that a badge/card reader (item 375003) is connected to the Windows Client PC. Check that the Server A flag is green.



Some parameters may change depending on the type of person.

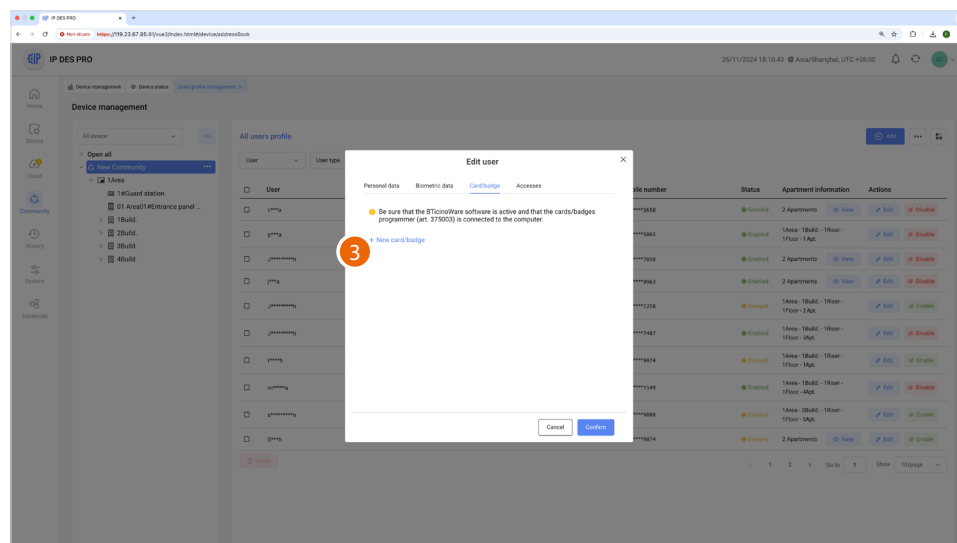


1. Click to modify the person

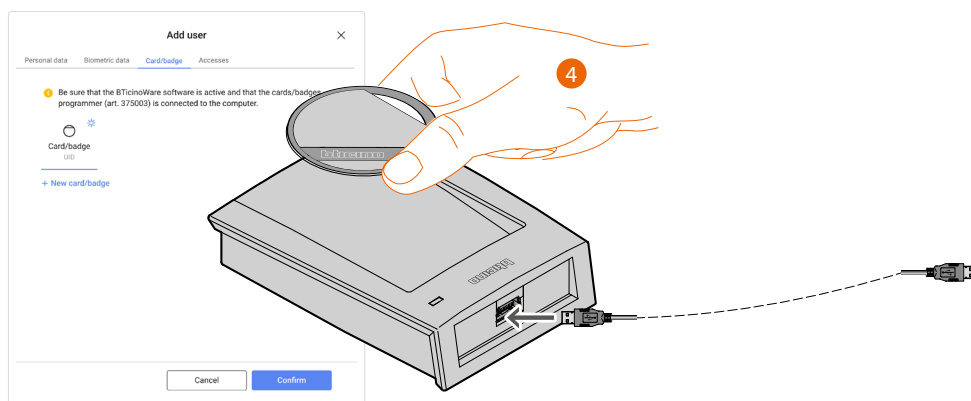


2. Click to open the section to add cards/badges

Owner, Tenant

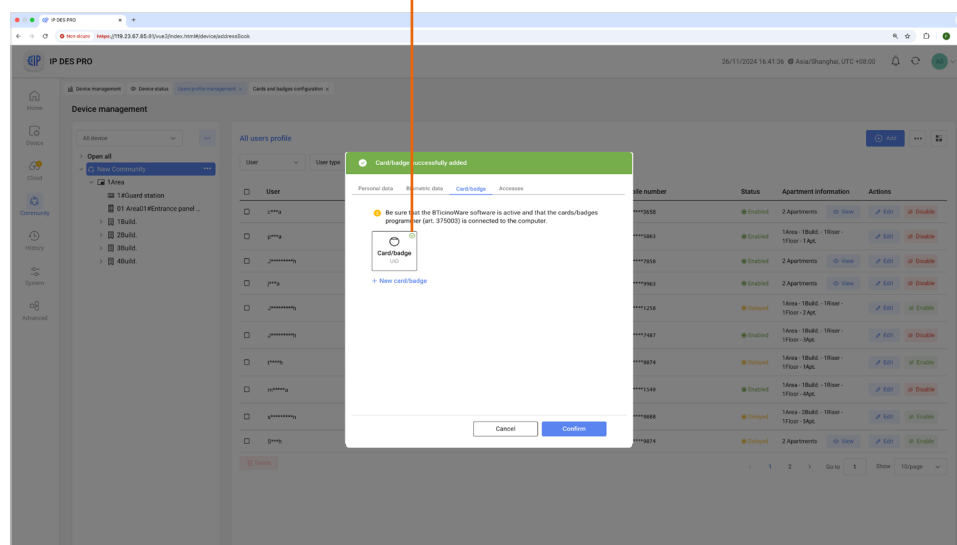


3. Click to register a badge/card.



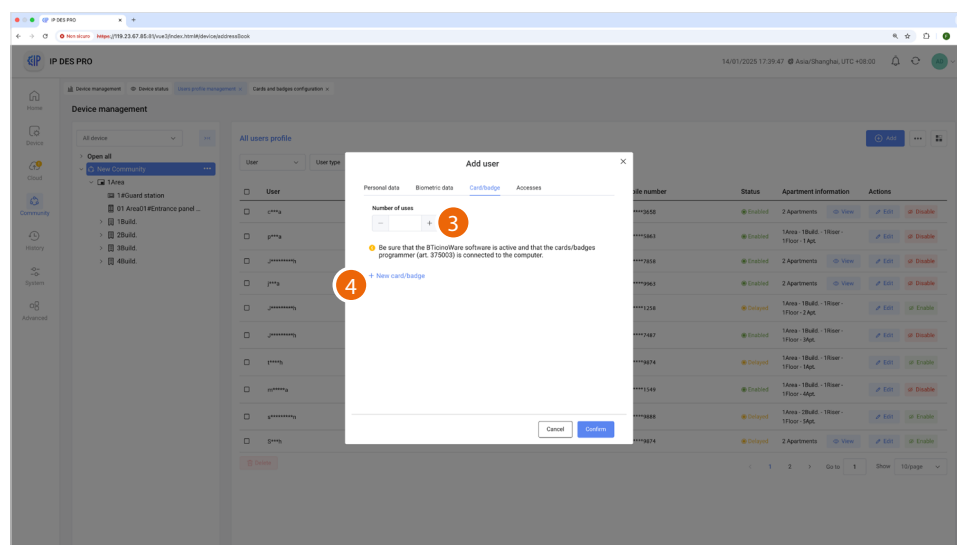
4. Place the badge/card to be registered on the reader

A



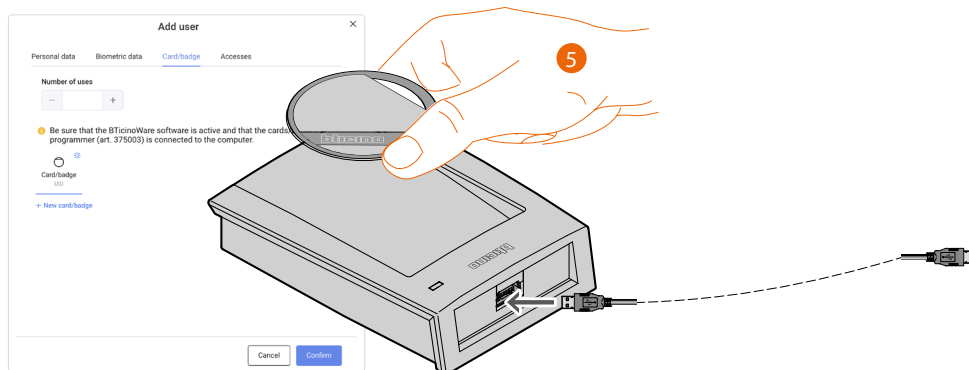
A The badge/card has been correctly registered

Visitor, Serviceman, Cleaner

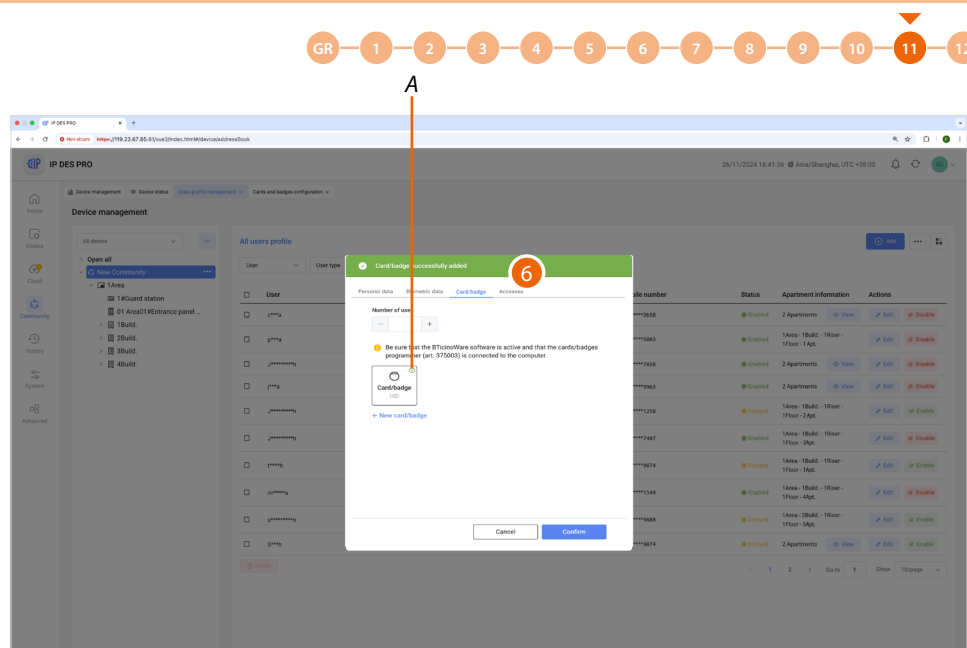


3. Select the number of uses to associate with the badge/card

4. Click to register a badge/card



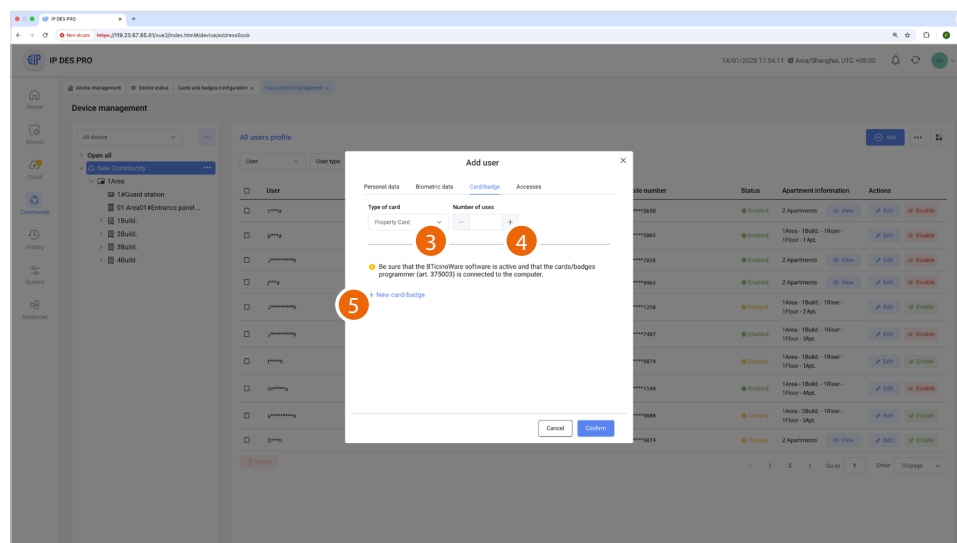
5. Place the badge/card to be registered on the reader



A The badge/card has been correctly registered

6. Click to open the Access section

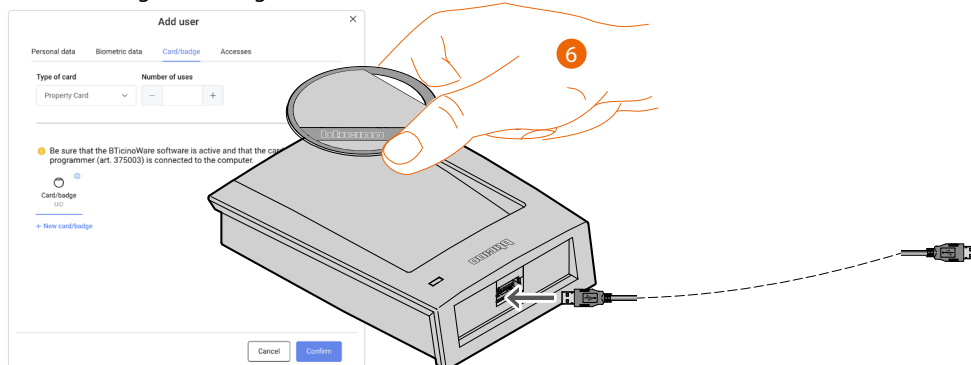
Manager, Security



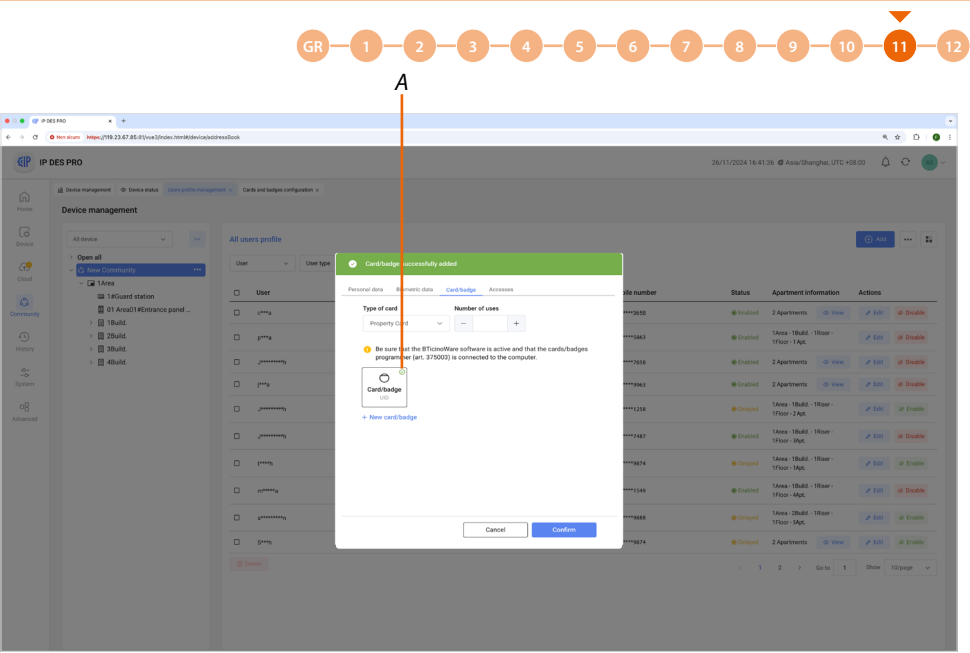
3. Select the card/badge type, either patrol card or property card

4. Select the number of uses to be associated with the card/badge (property card only)

5. Click to register a badge/card.



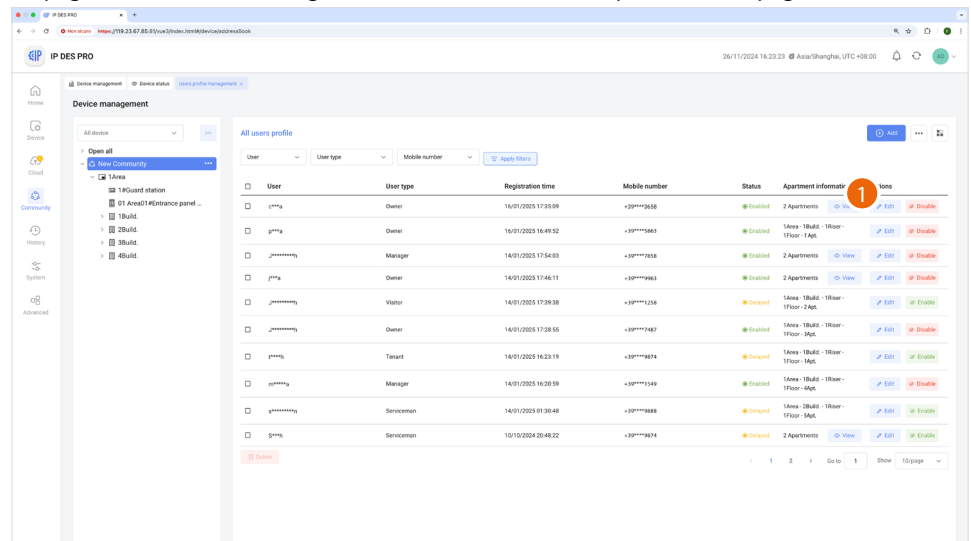
6. Place the badge/card to be registered on the reader



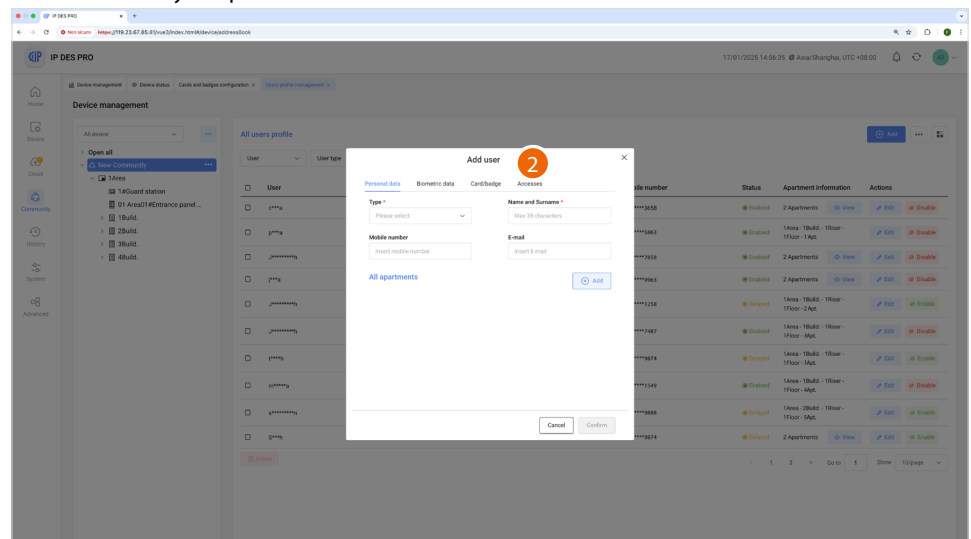
A The badge/card has been correctly registered

Accesses

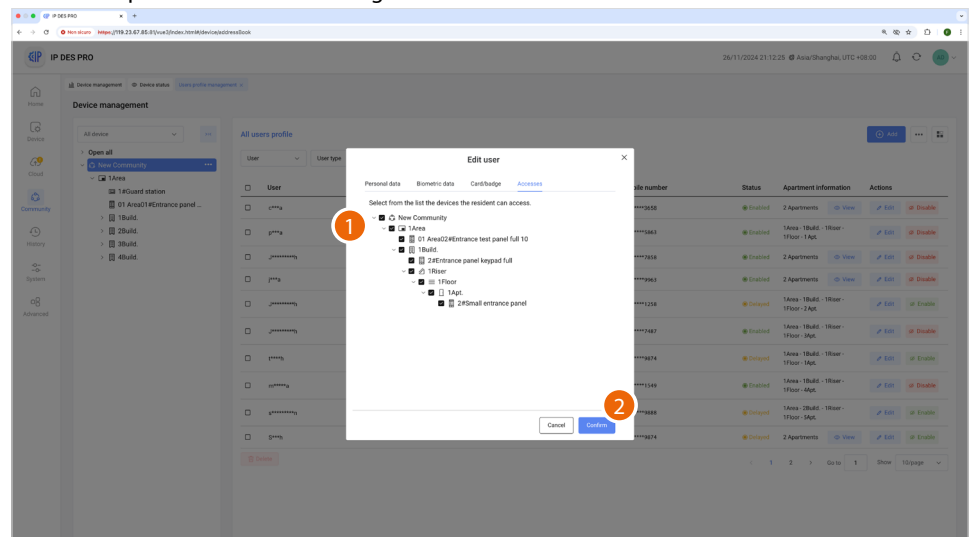
This page can be used to manage the accesses enabled in the personal data page



1. Click to modify the person



2. Click to open the section to manage the accesses



1. Select the apartment to which the person will have access

2. Click to save

Cards and badges configuration

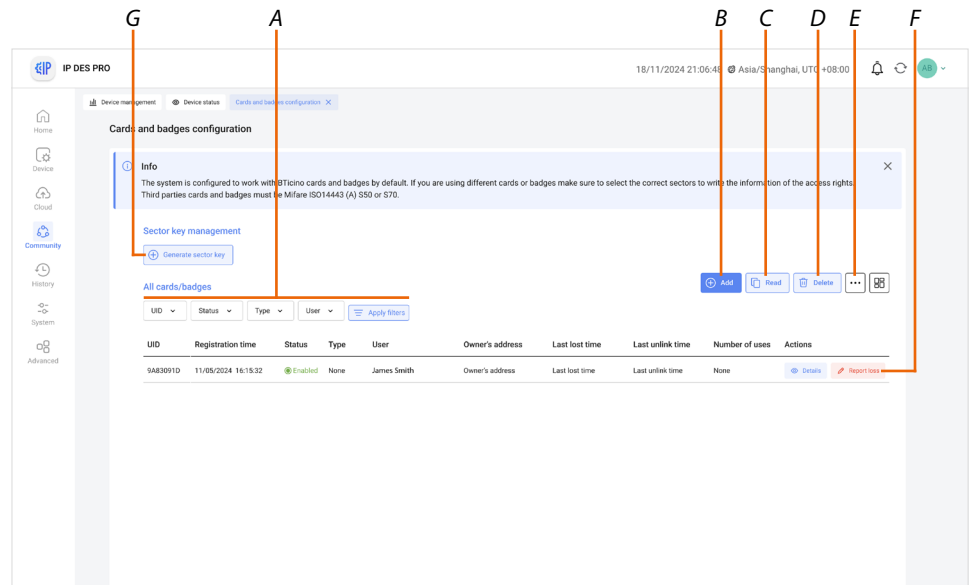
In this page it is possible to:

- [create new badges](#) for one or more persons and manage those already created previously on the card/badge page.
- [identify](#), [activate/deactivate](#) or [delete a card/badge](#).
- [Manage the key sector](#)

CAUTION: By default, the system is configured to work with BTicino cards/badges.

If you use different cards/badges, make sure to select the correct sectors to write the access rights information.

Third-party cards/badges must be Mifare ISO14443 (A) S50 or S70.



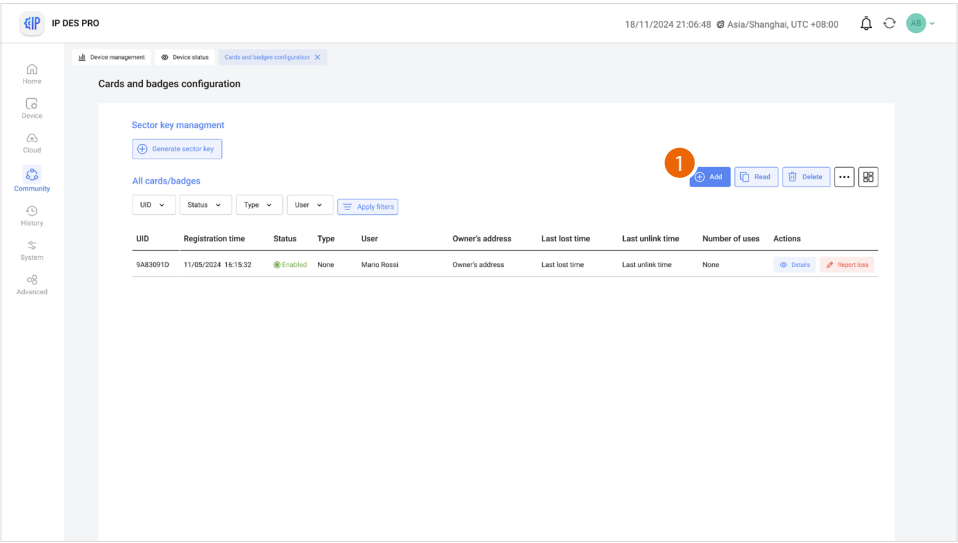
- A [Filters](#) selezione cards e badges
- B [Add badge/card](#)
- C [Identify badge/card](#)
- D [Delete badge/card](#)
- E [Export the list of cards and badges in .xls format](#)
- F [Disable/enable badge/card](#)
- G [Key sector management](#)

Filters

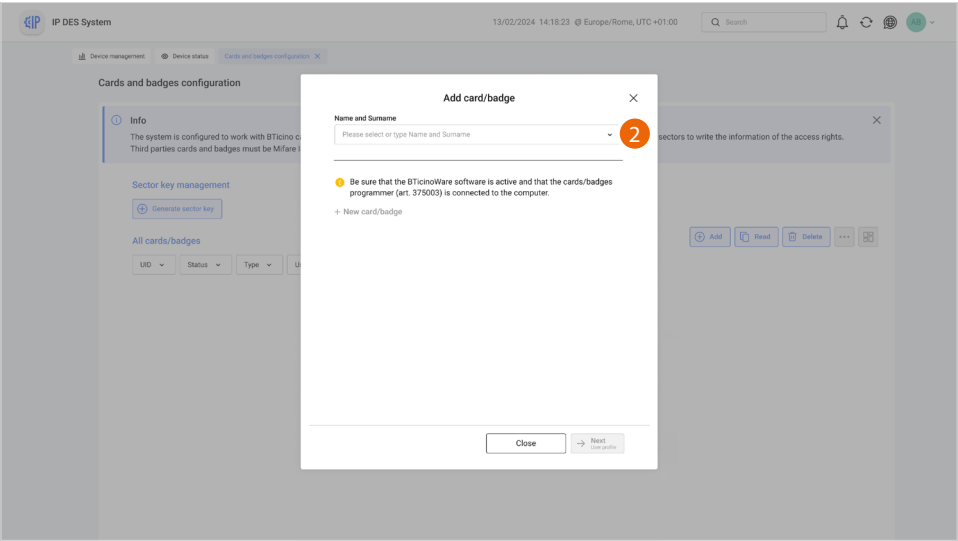


- A [Badge/card ID](#)
- B [Badge/card status filter](#)
- C [Badge/card type filter based on the person](#)
- D [Person name filter](#)

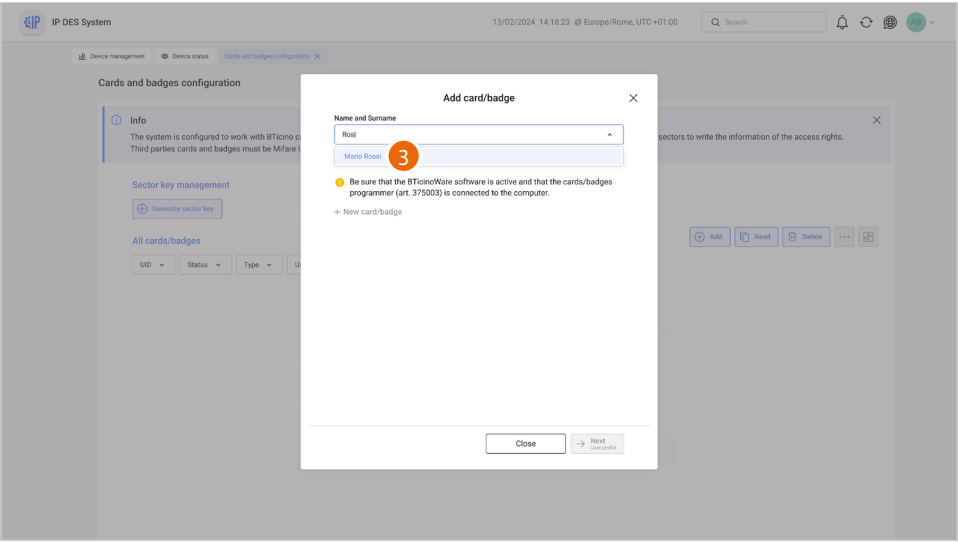
Add badge/card



1. Click to assign a badge/card to a person



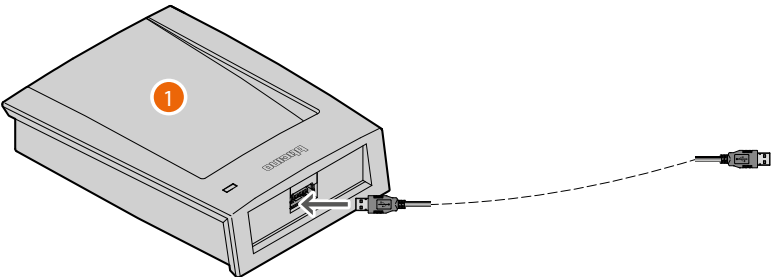
2. Click to select the person



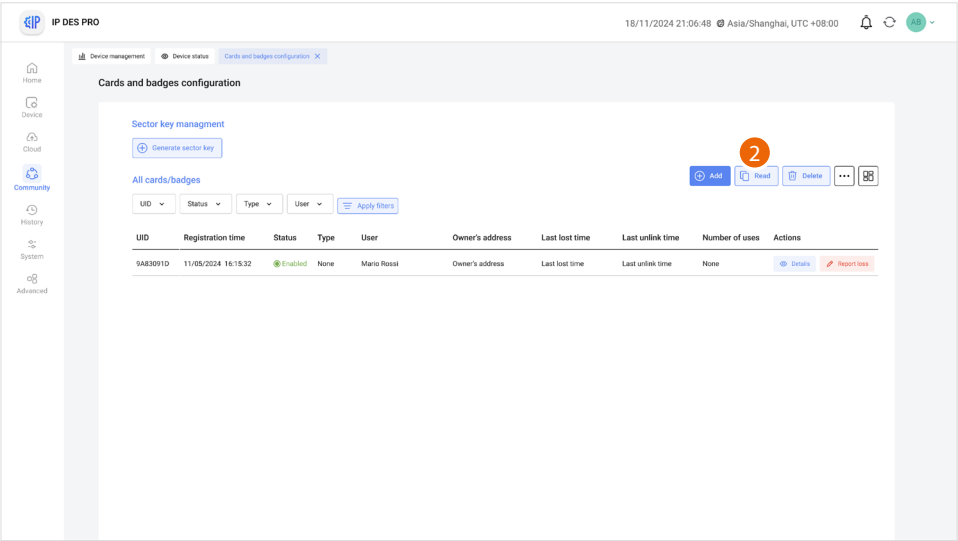
3. Select the person to whom to assign a badge/card, see [Register a badge/card](#)

Identify badge/card

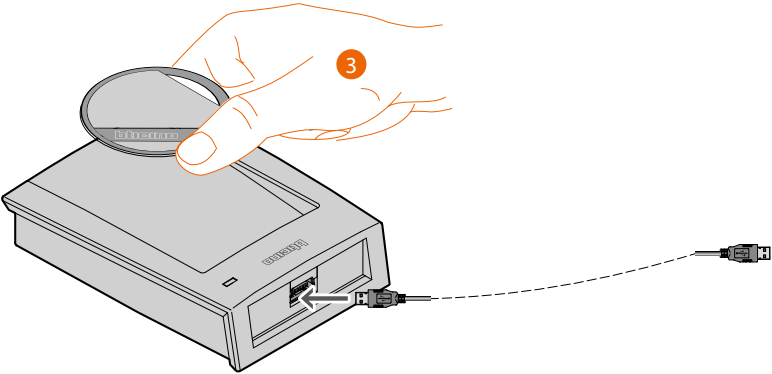
This function allows to read the data contained in a badge/card; for example, to identify it when found.



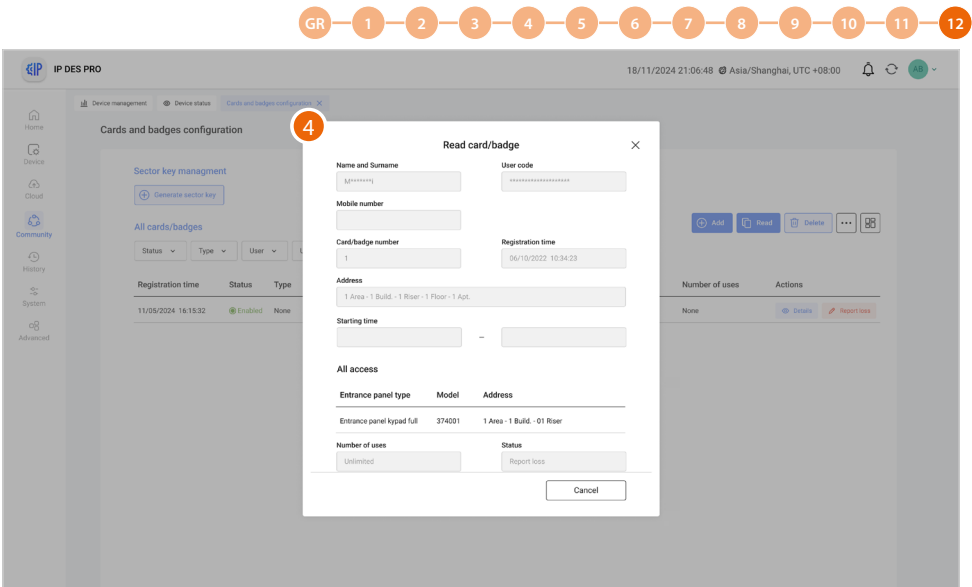
1. Connect a badge/card programmer (item 375003) to the Windows Client PC



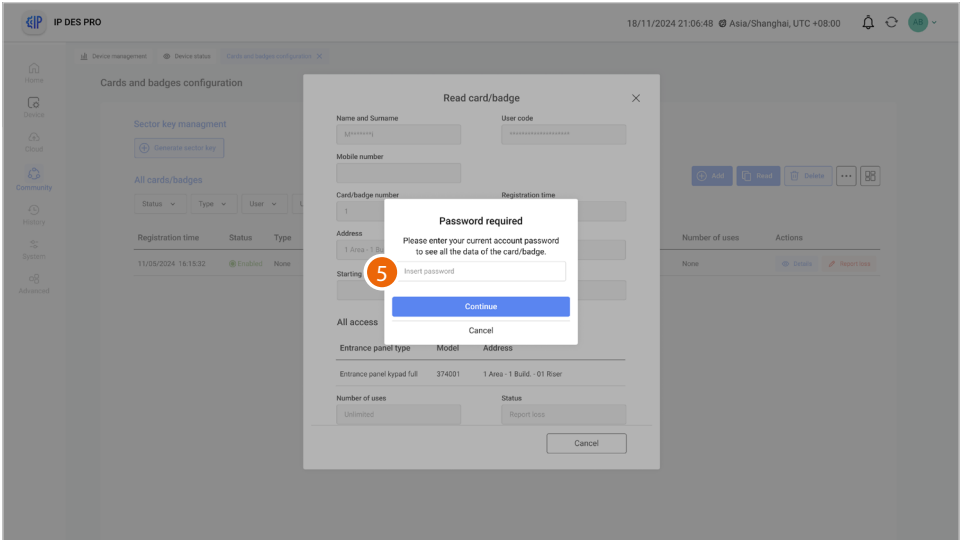
2. Click to read a badge/card



3. Place the badge/card to be read on the reader

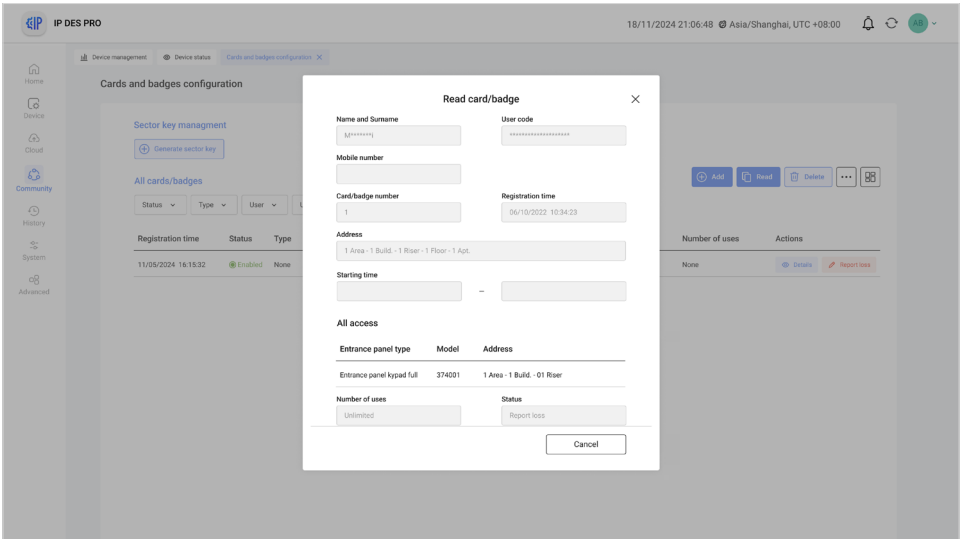


4. The panel displays the data of the badge/card owner badges



5. Enter the password

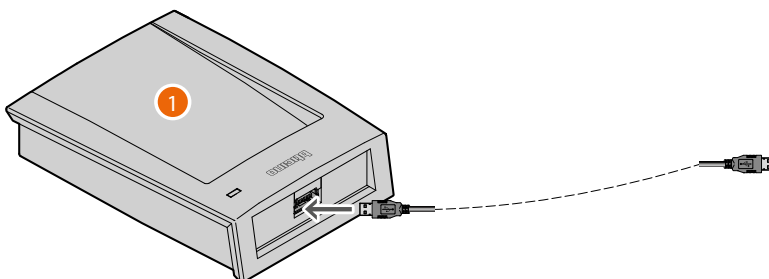
6. Click to confirm



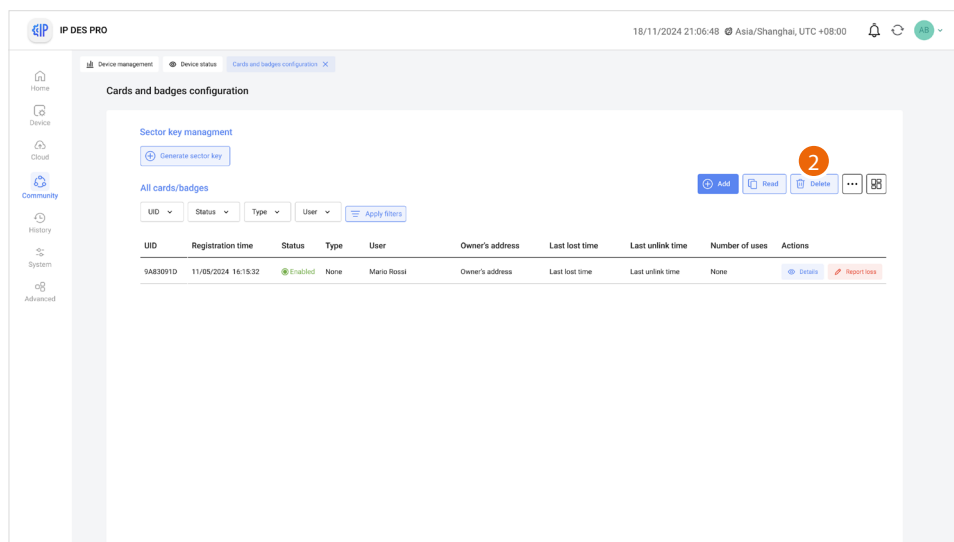
Delete badge/card

This function allows to erase the registered owner of a badge/card.

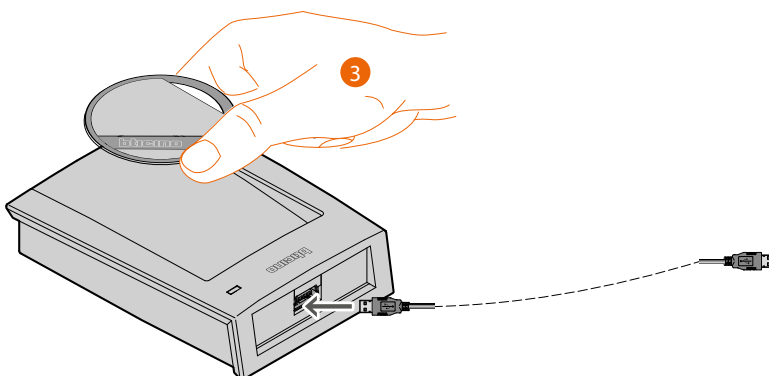
After this operation, the data of the person will be deleted and the badge/card will be ready for association with someone else



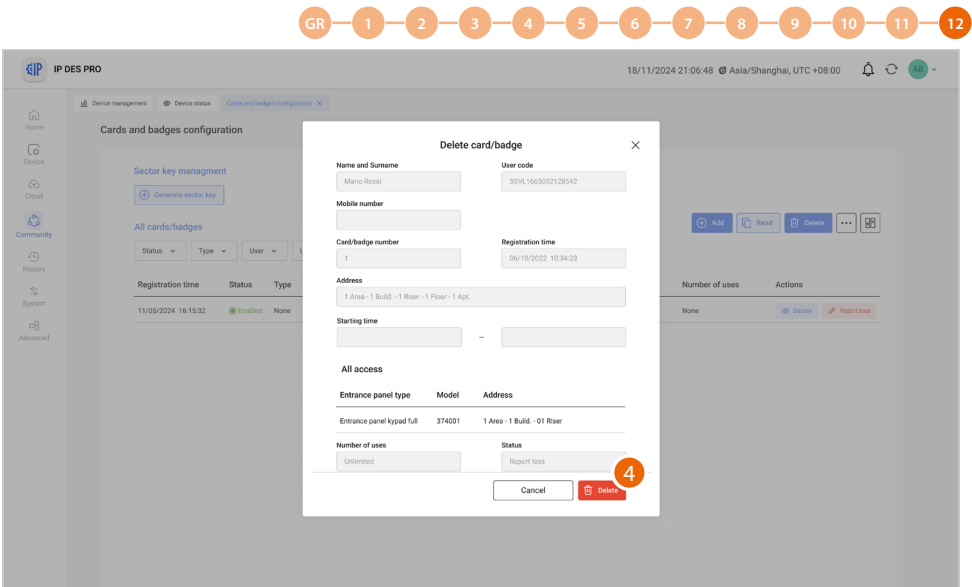
1. Connect a badge/card programmer (item 375003) to the Windows Client PC



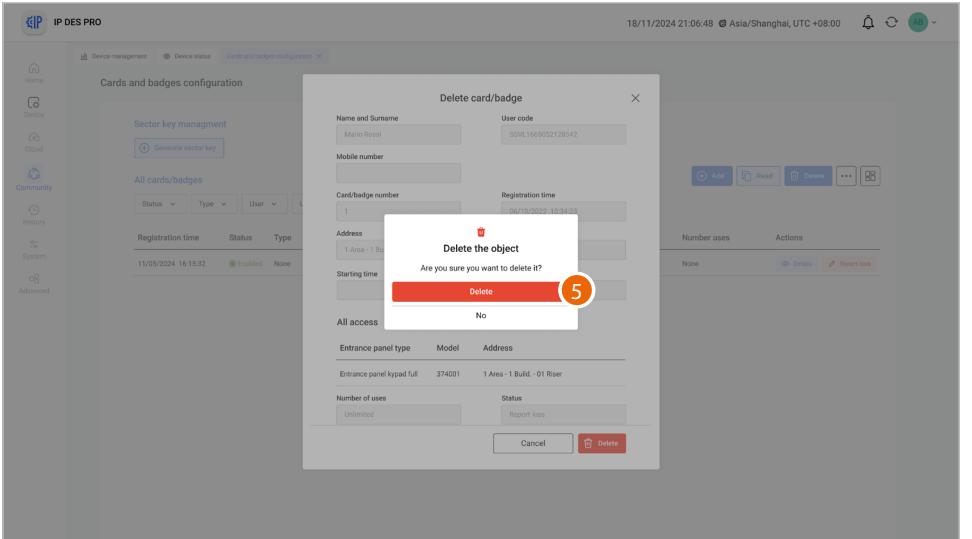
2. Click to delete a badge/card



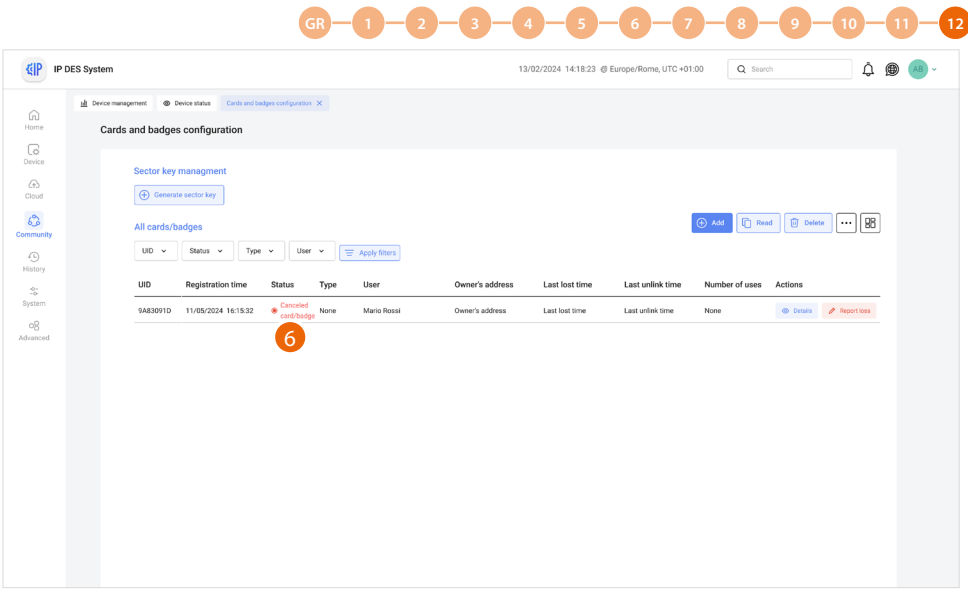
3. Place the badge/card to be deleted on the reader



4. The panel displays the data of the person registered on the badge/card; click to proceed



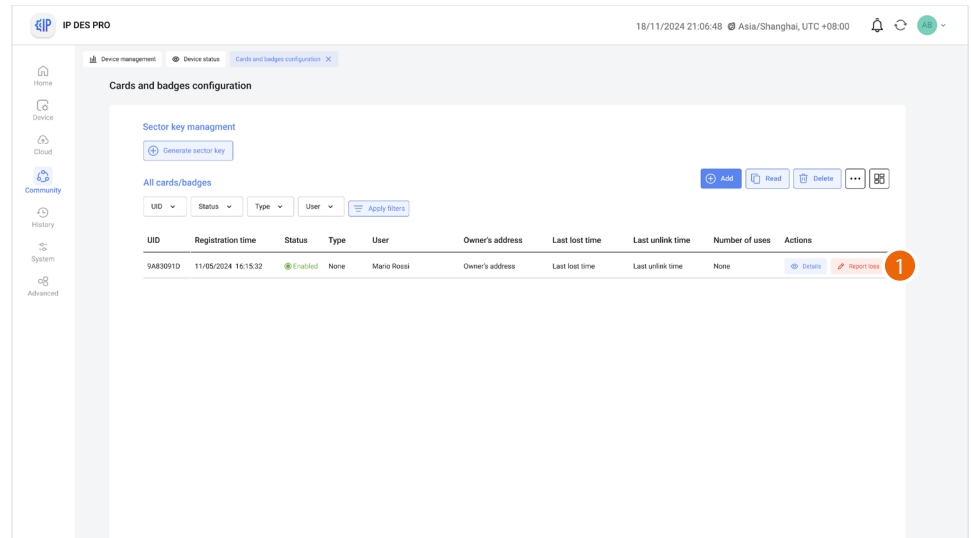
5. Click to confirm: all the details of the person will be erased from the badge/card



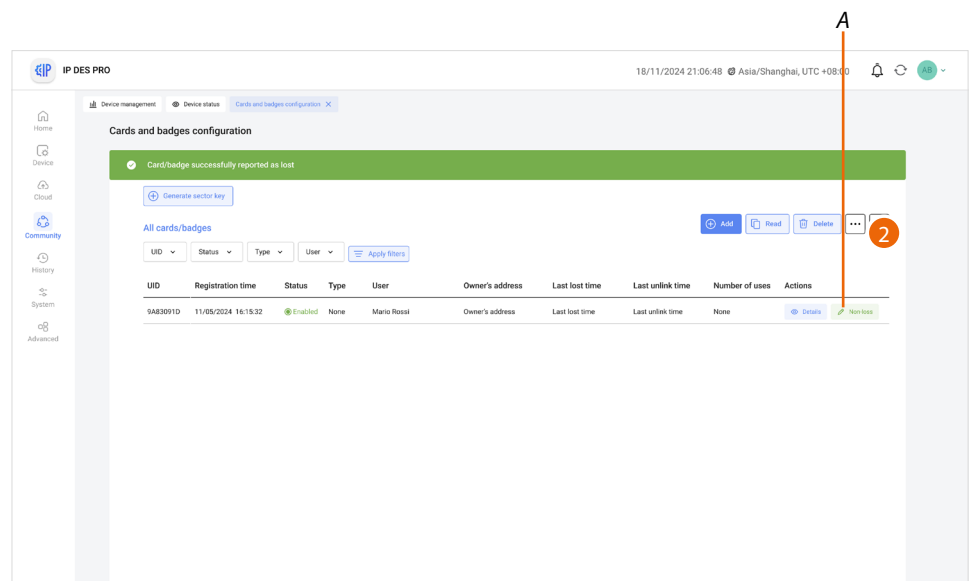
6. The status field shows the badge/card erased indication

Disable badge/card

Lost badges/cards can also be disabled.
Once found again, the badge can be reactivated.



1. Click to confirm that the badge/card has been lost



- A The badge/card is now disabled; click to continue
2. Click to activate the badge again if found

Key sector management

In this page, it will be necessary to indicate which sector keys will be used to store the IP system/gate/entry data on badge/card used for access.

Sector keys are the memory spaces inside badges and cards. There are 15 sector keys.

The sector keys that can be selected depend on the type of badge/card and the manufacturer..

BTicino badge/card = key sector 14,15

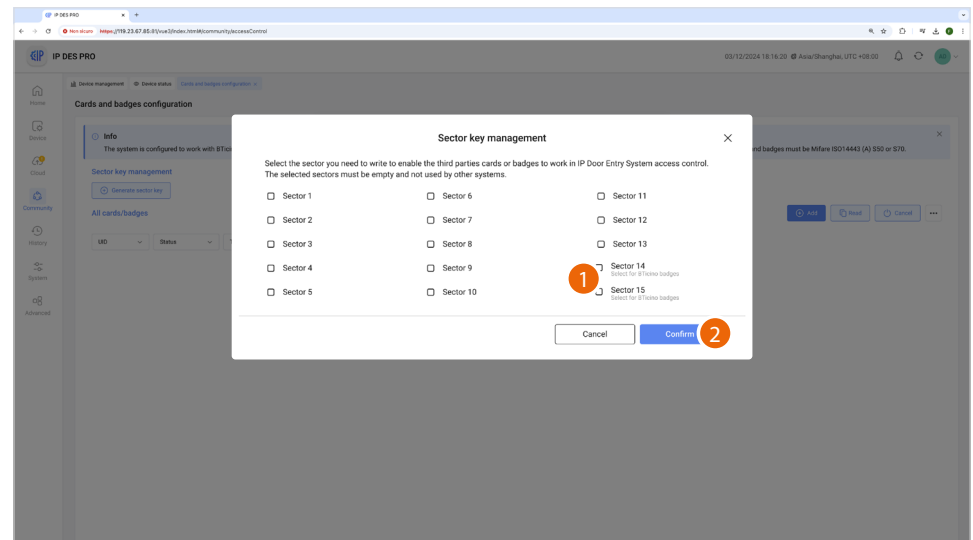
Other brands= key sector not used

NOTE: Some data of the community AB to which you are associating them are stored in the badges/cards.

Every time a new AB is generated, the above data changes, so the same badges/cards cannot be used with different ABs and consequently on two different systems.

NOTE: The system is set by default to work with BTicino badges.

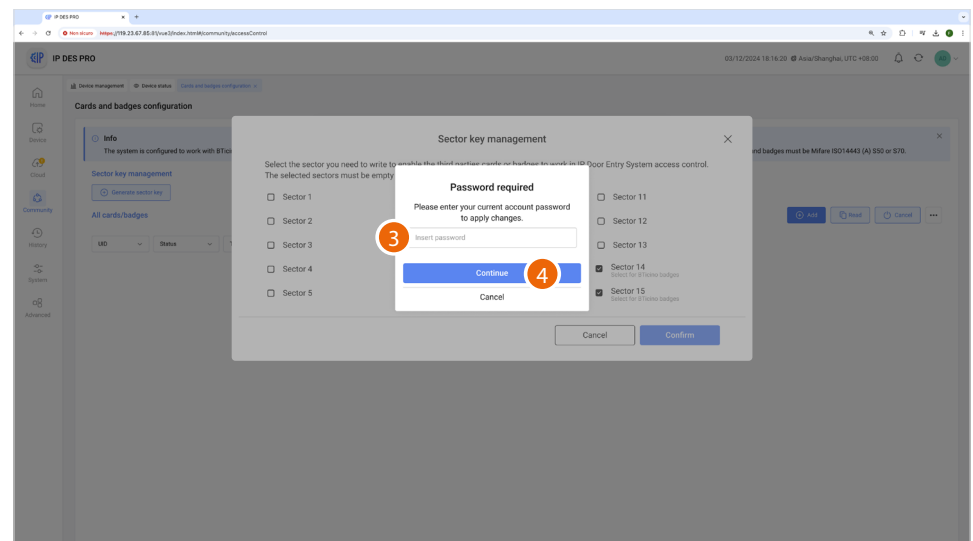
Third-party badges/cards may work with the same sectors. If not, it will be necessary to select the sectors to use, particularly if the same badge is used for other services.



1. Select the sector keys

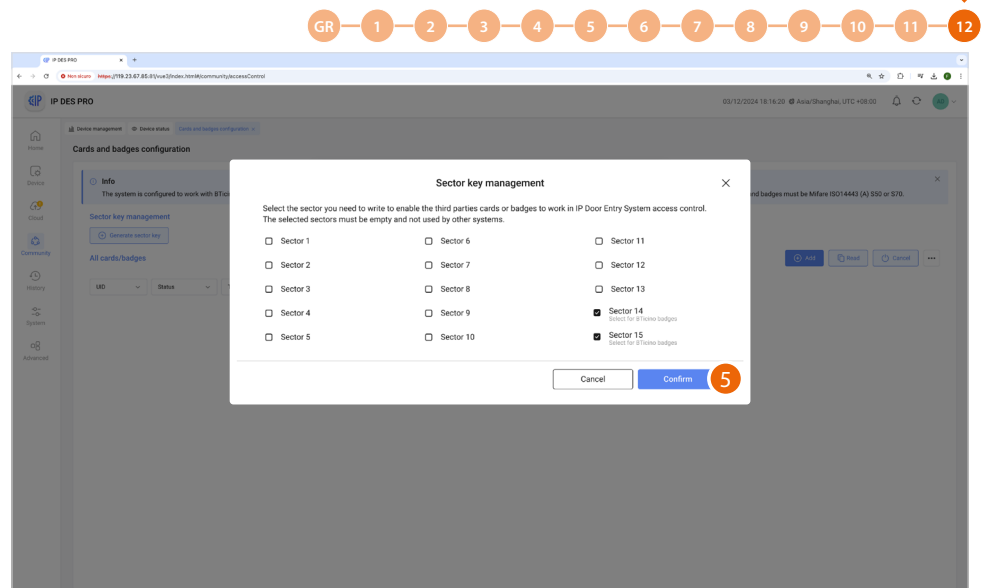
Attention: if the system includes mixed badges/cards (BTicino and other brands), ensure that the badges/cards of other brands have free sector keys 14,15.

2. Click to confirm



3. Enter the SD server authentication password

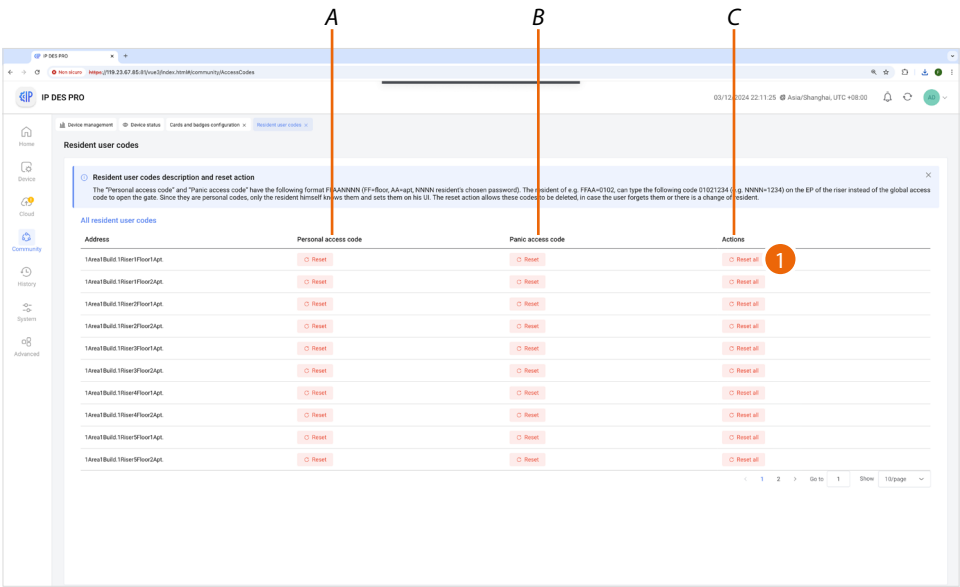
4. Click to continue



5. Click to finish. The information is stored in the SW and then linked to the badge/card through the reader

Resident user codes

This page can be used to reset the Personal Access Code and the IU Emergency Access Code. The codes will be reset to their default values. This function can be used if the user has lost the passwords.



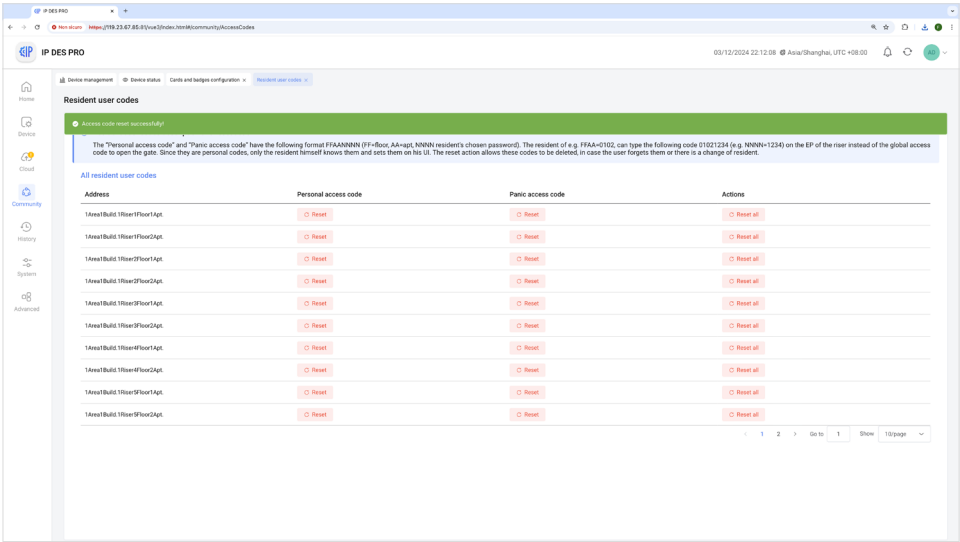
A Reset the personal access code

B Reset the emergency access code

C Resets both the personal access code and the emergency access code

1. Touch to reset the personal access code and the emergency access code

Warning: The codes will be reset immediately without further confirmation.



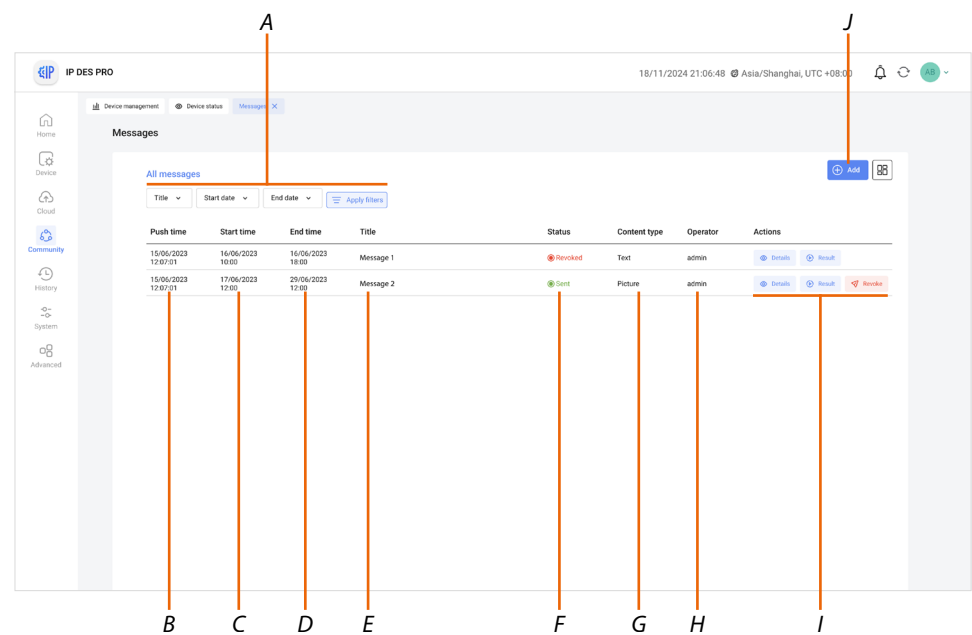
Messages

This page can be used to view and manage the messages sent to the Community and/or send new messages. The types of message are:

- Community Message: messages about the Community
- Advertisement: messages showing advertising content.
- Emergency Notifications: emergency messages

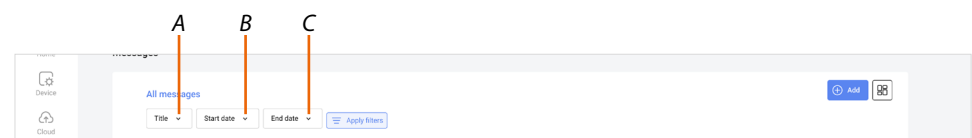
Messages will be displayed on the devices (depending on the parameters entered in “Message location” and the type of device) in one or more locations:

- Screen Saver
- Call waiting page



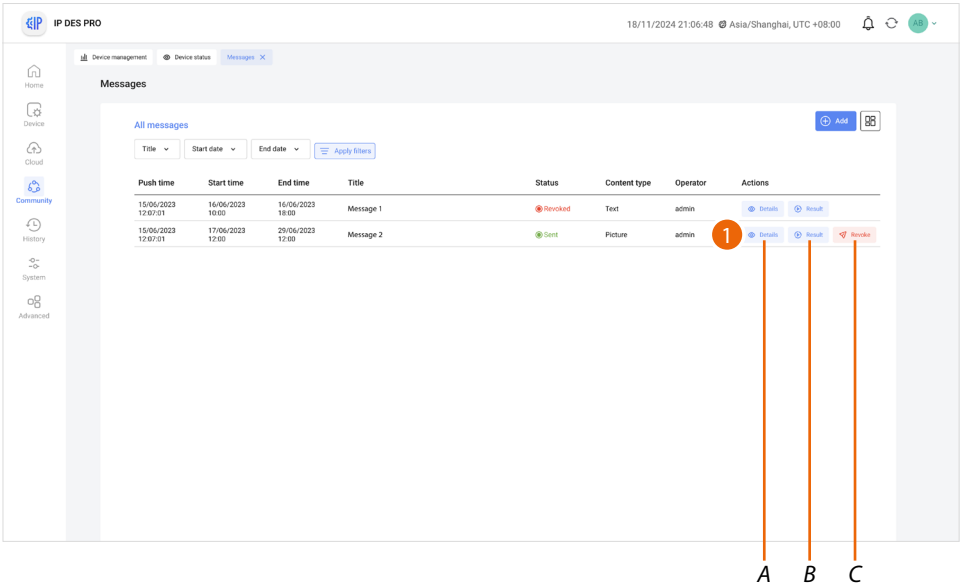
- A Message filters
- B Date and time of creation of the message
- C Start of message
- D End of message
- E Message title
- F Message status
- G Type of content
- H User who posted the message
- I Message management pushbuttons
- J Create a new message

Filters



- A Message title filter
- B Publication start date/time filter
- C Publication end date/time filter

Manage the messages



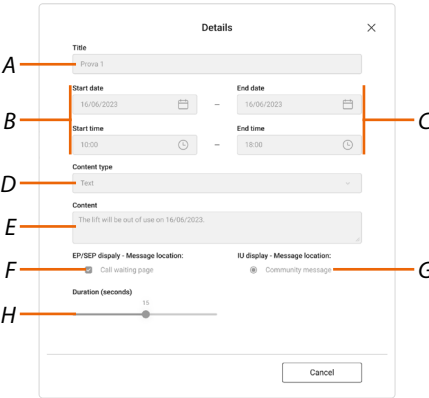
A View [the details of the message](#) sent

B View [the message publishing details](#)

C [Stop the sending of the message](#)

1. Click to view the message details

Message details



A Message title

B Publication start date/time

C Publication end date/time

D Type of message (text message, photo, video)

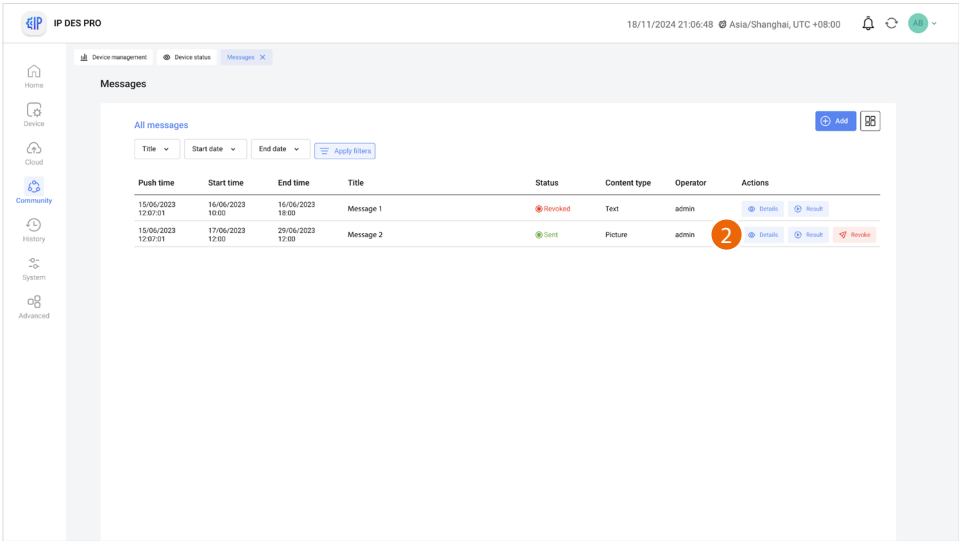
E Message text

F Location where the message is displayed on the devices (EP / VEPO)

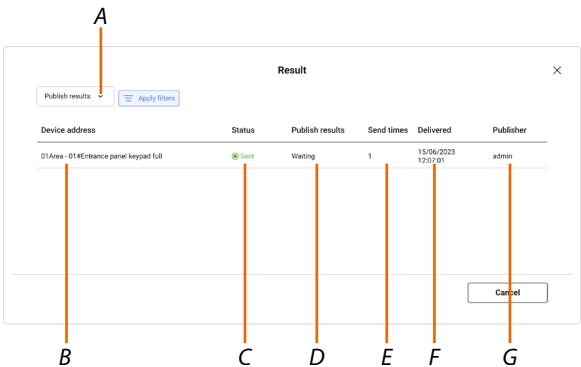
G Location where the message is displayed on the devices (IU)

H Message length

Message publication details

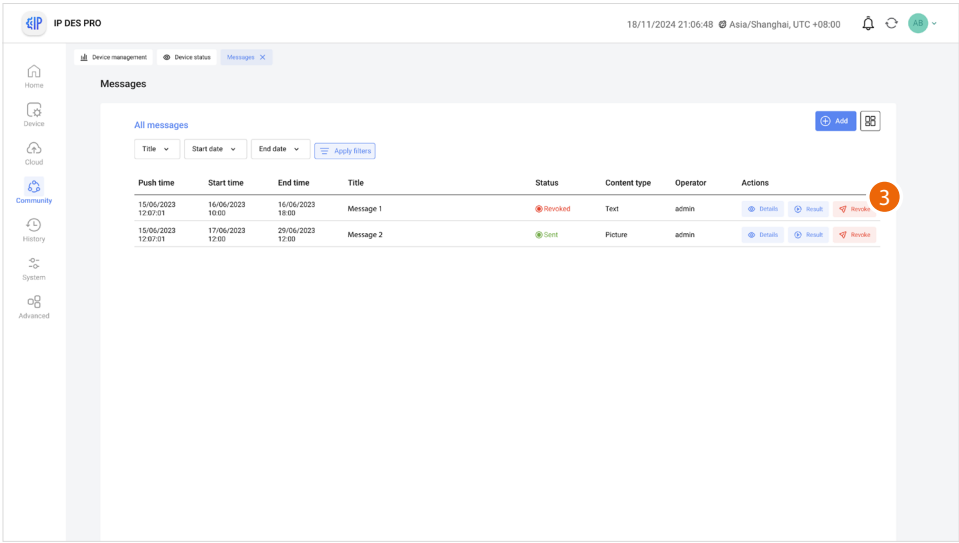


2. Click to view the message publication details

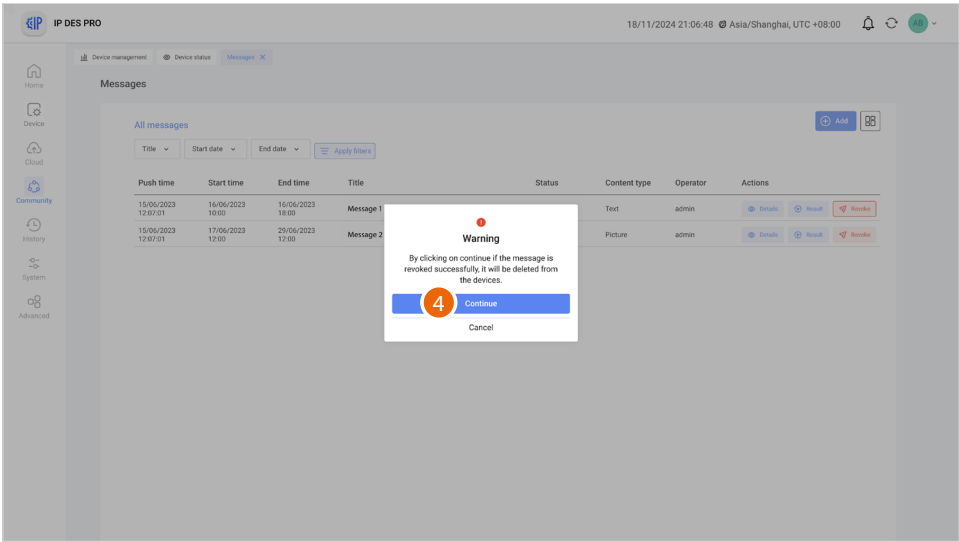


- A Select the successful/failed messages filter
- B Address of the device to which the message was sent
- C Message status (not sent/sent)
- D Publication status (executed/not executed)
- E Number of transmissions
- F Date/time sent
- G Account that sent it

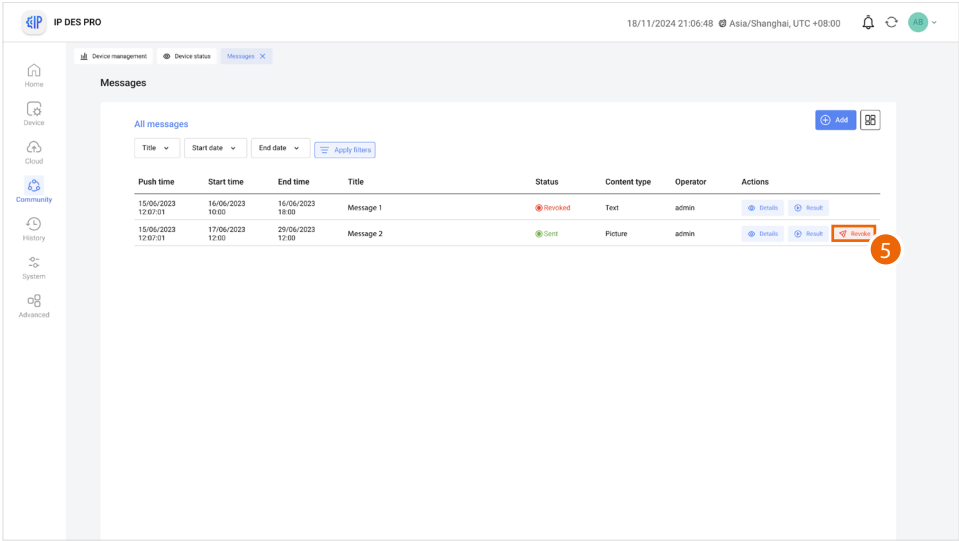
Revoke the message



3. Click to revoke the message

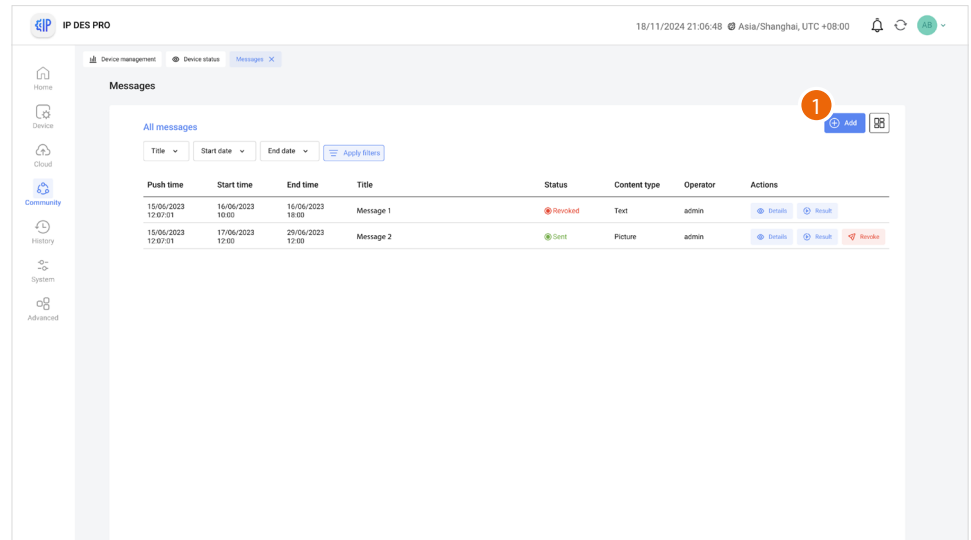


4. Click to confirm, the message will no longer be displayed in the community

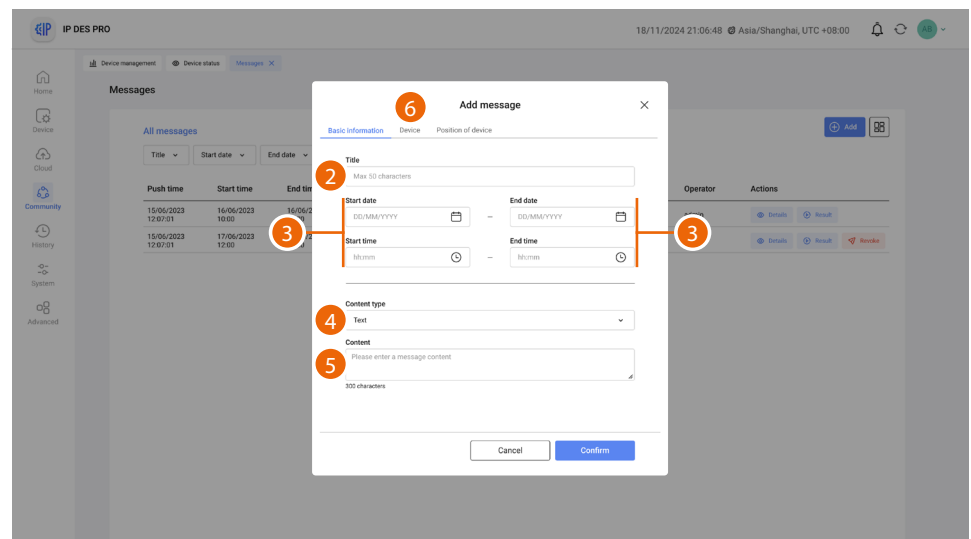


5. The message has been revoked

Create a new message

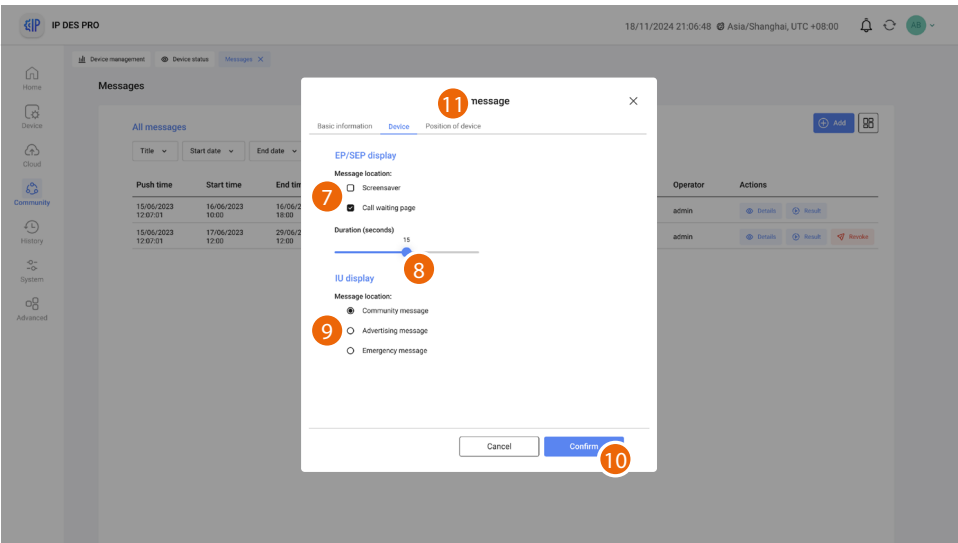


1. Click to create a new message

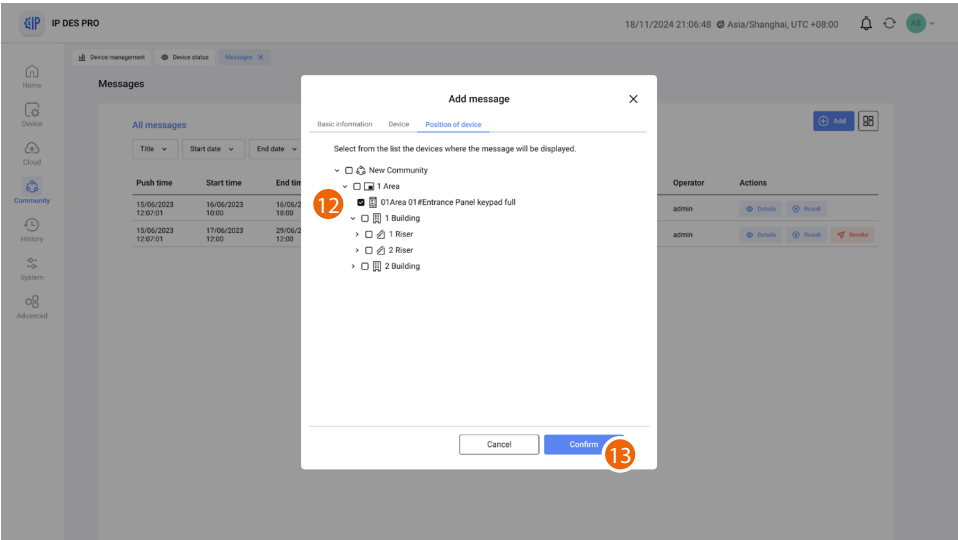


Start by entering the basic information for composing the message

2. Enter a title for the message
3. Enter a publication start and end date
4. Select the type (text message, photo, video)
5. Enter the text of the message (for sending photos or videos [see the relevant section](#))
6. Click to define how the message will appear on the devices and the duration

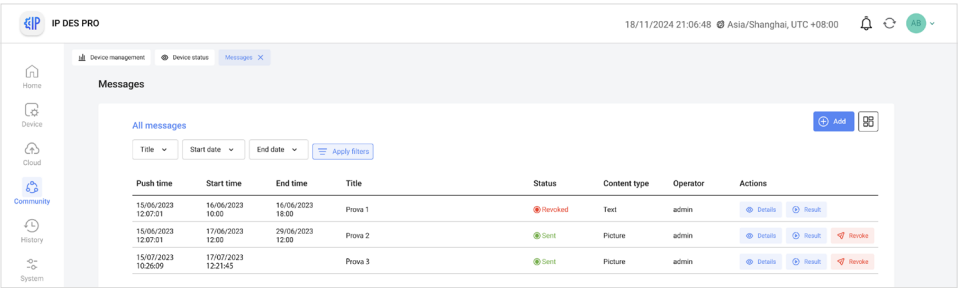


7. Select where to display messages on the EP (screen saver/call waiting page)
8. Select the duration of the message
9. Select the type of message (Community/Advertising Message/Emergency Notifications) and the IU pages where they will be displayed (message section).
10. Click to send
11. Click to select which devices will display the message

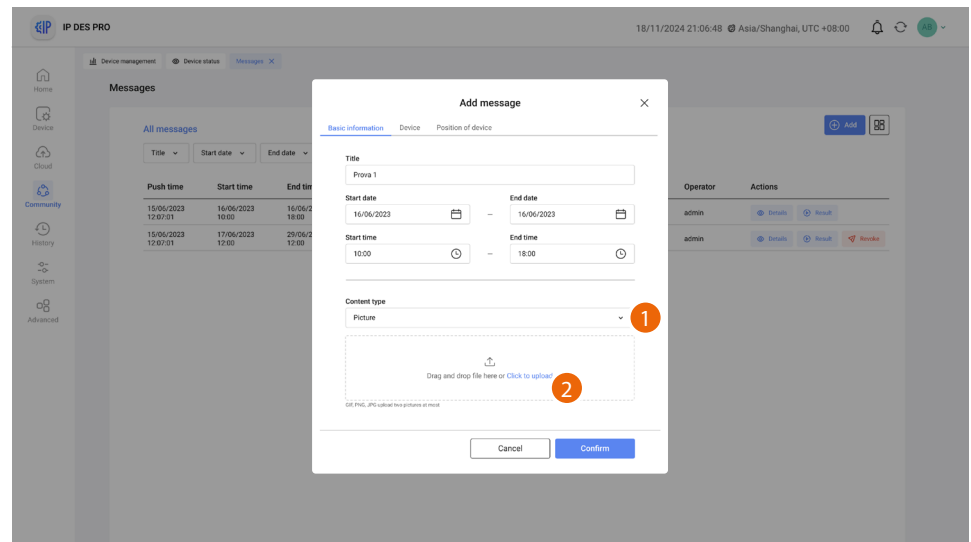


12. Select the community branch you want to send messages to
13. Click to finish

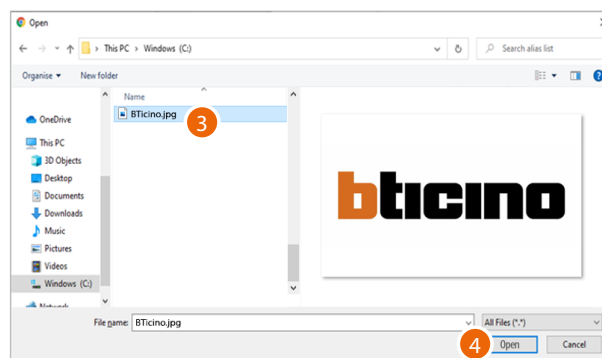
The message has been published



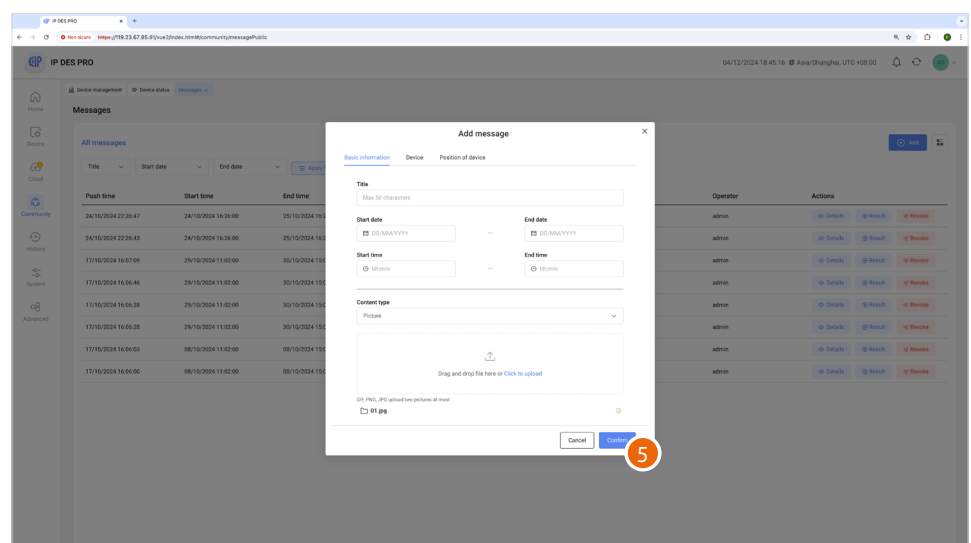
Send messages containing images or videos



1. Select image/video as content type
2. Click to select the content

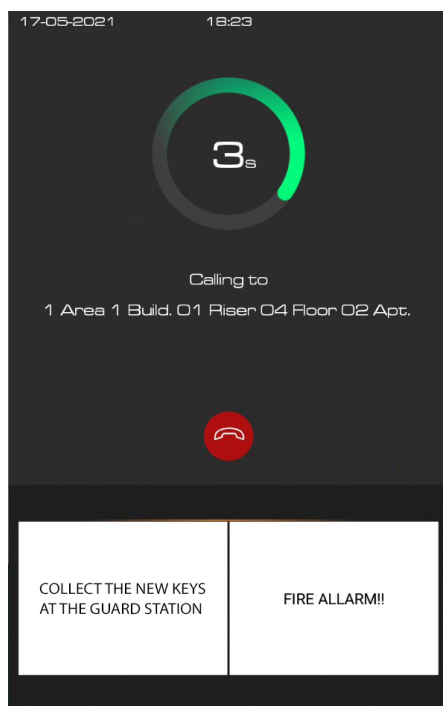


3. Select an image
4. Click to load the image

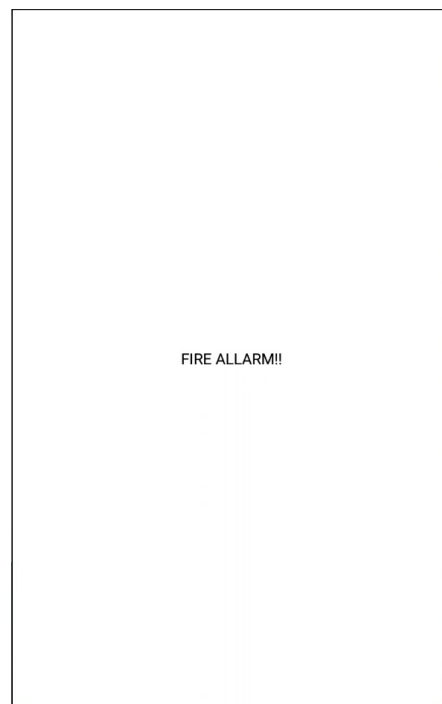


5. Click to publish the message

The message has been published



Messages displayed during a call



Messages displayed as screen saver

Sent messages will be displayed on the devices (e.g. EP item 374000)

History



This menu allows to display various information about accesses, calls, alarms and more in the community.

Alarm history

Displays all the alarms from community devices

Access history

Displays all the community logins and registrations

Patrol history

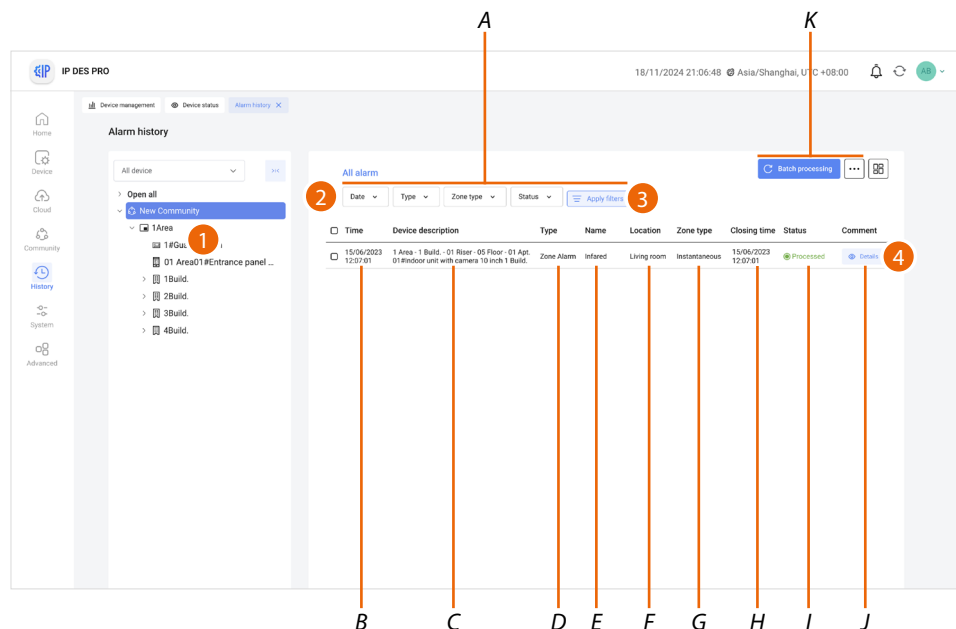
Displays the history of the patrols carried out in the community

Call history

Displays the community call history

Alarm history

This page can be used to view alarms from IU and EP (Emergency Alarm and Tampering Alarm)



A **Alarm filters**

B Date and time of the alarm

C Name of the device that generated the alarm (customisable).
The original name represents **the address of the device in the community**

D Type of alarm

E Type of sensor

F Name of the alarmed zone

G Type of alarm zone

H Process closing date and time

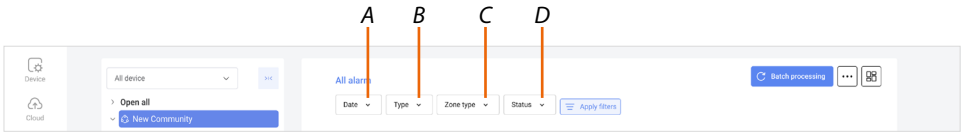
I Management status

J Alarm details

K **Alarm management keys**

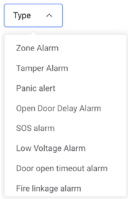
1. Select the community branch that contains the EP concerned
2. If necessary, use the filters to narrow down the selection
3. Click to apply the filter
4. Click to view the details of the alarm and to process it if required

Filters



A Alarm monitoring period

B Type of alarm

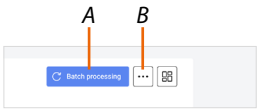


C Type of zone

24 hours	The probe is always active, even if the alarms are totally deactivated
Instantaneous	The alarm is immediately communicated
Delay	The alarm is given at a certain time after the triggering condition occurs
Activity Control	The alarm is communicated immediately, if the sensor does not detect activities for a preset time
Programmed	Scheduled activation

D Status (processed/not processed)

Alarm management keys



A Process several alarms simultaneously

B Export the alarm list to an Excel® file

Details

Zone number

1

Address

1 Area - 1 Build. - 01 Riser - 05 Floor - 01 Apt.

Device description

1 Area - 1 Build. - 01 Riser - 05 Floor - 01 Apt. 01#Indoor unit with camera 10 inch 1 Build.

Comment

Please enter a comment

5

Save

6

n characters

All comments

Time	Comment	Operator	Process source
12/03/2024 12:32:09	Seen	admin	Server

Cancel

A panel opens, showing some alarm data, with a field for adding comments

- 5. Add a comment
- 6. Click to save

Details

Zone number

1

Address

1 Area - 1 Build. - 01 Riser - 05 Floor - 01 Apt.

Device description

1 Area - 1 Build. - 01 Riser - 05 Floor - 01 Apt. 01#Indoor unit with camera 10 inch 1 Build.

Comment

Please enter a comment

Save

n characters

All comments

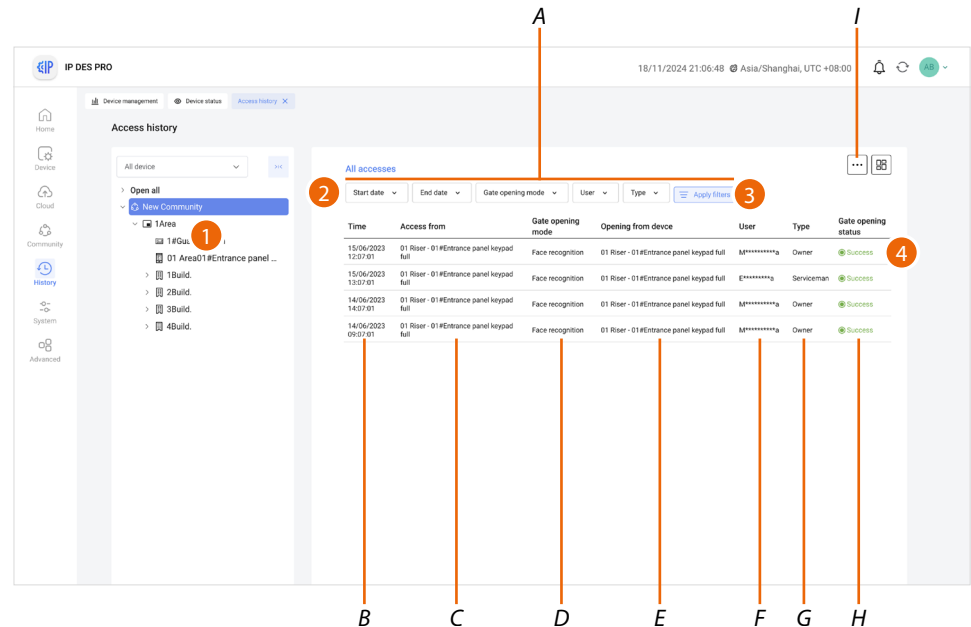
Time	Comment	Operator	Process source
12/03/2024 12:32:09	Seen	admin	Server
12/03/2024 12:32:09	Seen	admin	Server

Cancel

The comment has been added

Access history

This page can be used to view and export community accesses in a list



A **Filters**

B Access time and date

C Name of the device used for the access (customisable).
The original name represents **the address of the device in the community**

D Access mode

E Name of the device that opened the entrance (customisable).
The original name represents **the address of the device in the community**

F Name of the person who entered

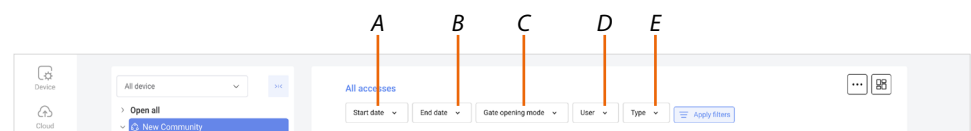
G Type of person who entered

H Opening outcome

I Export the access list to an Excel® file

1. Select the community branch that contains the EP concerned
2. If necessary, use the filters to narrow down the selection
3. Click to apply the filter

Filters



A Access start time/date filter

B Access end time/date filter

C Entrance opening mode filter

D Person who completed the access filter

E Type of person who completed the access filter

Patrol history

This page can be used to view patrol security check point records.
Whenever a Patrol badge is moved near an EP reader, the reading is recorded.

NOTE: in order to keep track of inspections, it is necessary to configure the badges/cards as Patrol or System Manager types.

The screenshot shows the 'Patrol history' page in the IP DES PRO application. The interface includes a sidebar with navigation options (Home, Device, Cloud, Community, History, System, Advanced) and a main content area. The main area has a 'Patrol history' tab selected, showing a table of patrol records. Above the table are filter buttons for 'Patrol date', 'Device type', and 'User', along with an 'Apply filters' button. In the top right corner, there are icons for a menu, a notification bell, and a user profile. Labels A through H point to specific elements: A points to the filter buttons, B points to the 'Patrol date' column, C points to the 'Patrol time' column, D points to the 'Device type' column, E points to the 'Device address' column, F points to the 'User' column, G points to the 'Mobile number' column, and H points to the export icon (a document with a plus sign).

Patrol date	Patrol time	Device type	Device address	User	Mobile number
15/06/2023	13:07:01	Small entrance panel	01 Riser - 01 Entrance panel keypad full	S***	3395987496
15/06/2023	13:07:01	Small entrance panel	01 Riser - 01 Entrance panel keypad full	S***	3396589696
15/06/2023	13:07:01	Small entrance panel	01 Riser - 01 Entrance panel keypad full	S***	3395969696

- A **Filters**
- B Check point date
- C Check point time
- D Type of device
- E Name of the customisable device.
The original name represents **the address of the device in the community**.
- F Name of the property Manager or Security Personnel (persons with Property Manager or Security Personnel status)
- G Telephone number of the Property Manager or Security Personnel (persons with Property Manager or Security Personnel status)
- H Export the list to an Excel® file

Filters

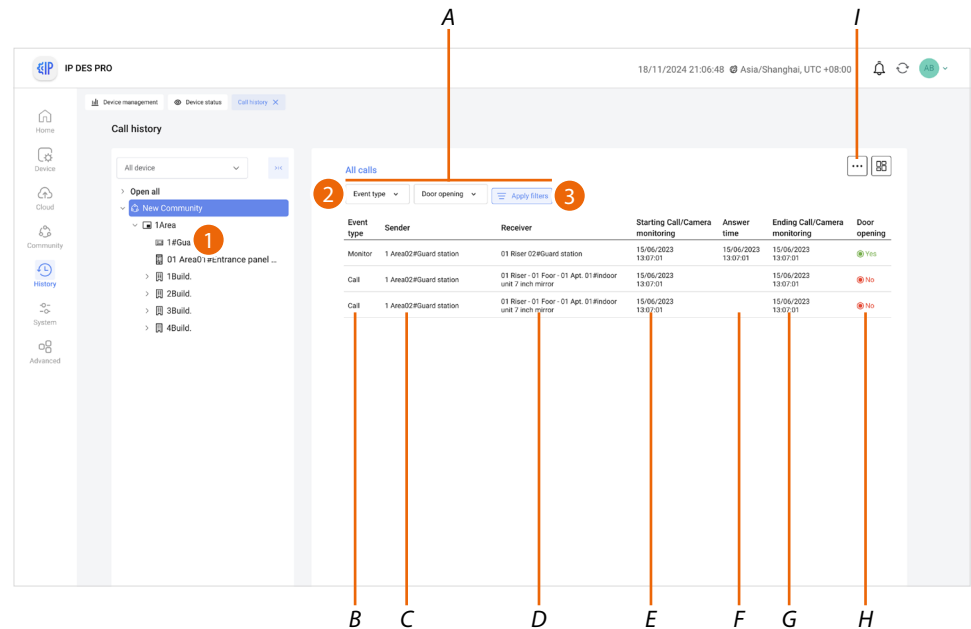
The screenshot shows the filter section of the 'Patrol history' page. It includes three dropdown menus labeled A, B, and C. Label A points to the 'Patrol date' dropdown, label B points to the 'Device type' dropdown, and label C points to the 'User' dropdown. There is also an 'Apply filters' button to the right of the dropdowns.

Patrol date	Device type	User
Patrol date	Device type	User

- A Inspection registration date filter
- B Inspection registration device filter
- C Inspector filter

Call history

This page can be used to view the list of calls between community devices



A **Filters**

B **Type of event (call to IU or GS/monitoring of EP)**

C **Name of calling device (customisable).**

The original name represents **the address of the device in the community**

D **Name of the receiving device (customisable).**

The original name represents **the address of the device in the community**

E **Call or monitoring start date/time**

F **Date/time the call was answered.**

If empty, it means missed call or busy device.

G **Call or monitoring end date/time**

H **Door opening after call**

I **Export the call list to an Excel® file**

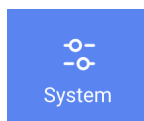
1. Select the community branch of which you want to monitor the calls
2. If necessary, use the filters to narrow down the selection
3. Click to apply the filter

Filters



A **Type of event (call to IU or GS/monitoring of EP) filter**

B **Call with door opening filter (yes/no)**

System

This menu allows to view and manage various SW-related functions.

Role managment

Creates and manages the roles of the **accounts** of the SW

Account profile management

Creates and assigns roles to **accounts** to perform configurations using the SW

Map configuration

Creates and manages the community Home Page map

Account operation log

Displays the list of the operations carried out by the **accounts**

System data backup

Performs the system backup

System data recovery

Restores the saved backups

Server version information

Displays information concerning the installed SW versions

Server upgrade

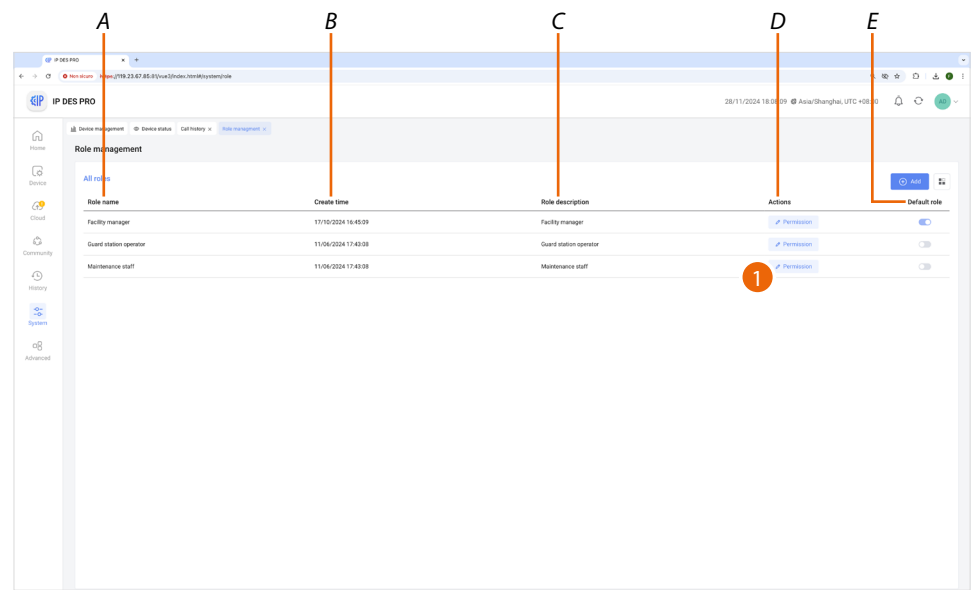
Updates the SD software and operating system (future use)

Role management

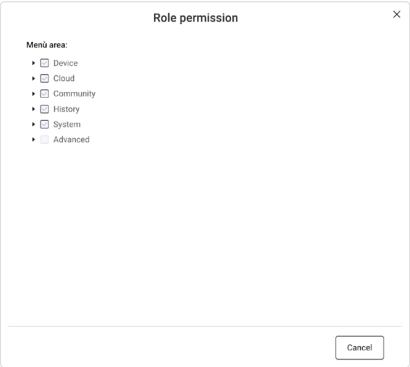
This page can be used to manage the roles to be assigned to the SW accounts. Roles are defined, allowing access to certain items in the main menu. It is possible to associate the role to an account (see [Operator management](#)). There are 3 default roles for which permissions cannot be changed:

- Facility manager = main role, access enabled to all items
- Guard station operator = Access enabled for the following: Community and History
- Maintenance staff = Access enabled for the following: Device, Cloud, Community and History.

It is also possible to [create roles](#) with specific permissions according to specific needs



- A Role name
 - B Time/date of role creation
 - C Role description
 - D Open the permission display/setup panel
 - E Set the role as default
1. Click to view/change the permissions of a role

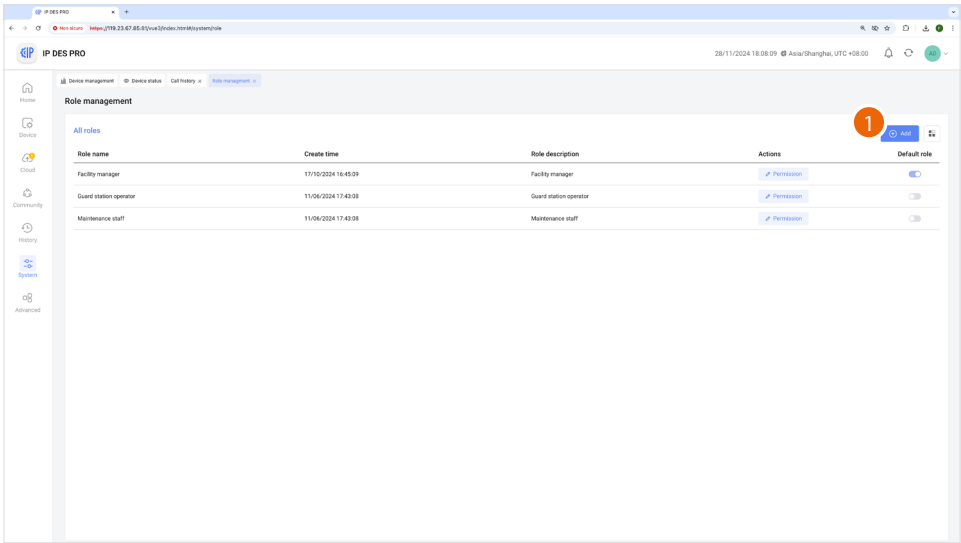


PERMISSION TABLE

Menù area:

▶ <input checked="" type="checkbox"/> Device	Device menu
▶ <input checked="" type="checkbox"/> Cloud	Cloud Menu
▶ <input checked="" type="checkbox"/> Community	Community Menu
▶ <input checked="" type="checkbox"/> History	Menu History
▶ <input checked="" type="checkbox"/> System	Menu System
▶ <input type="checkbox"/> Advanced	Menu Advanced

Create a role



1. Click to create a new role

Add role

Role name

Man Badge

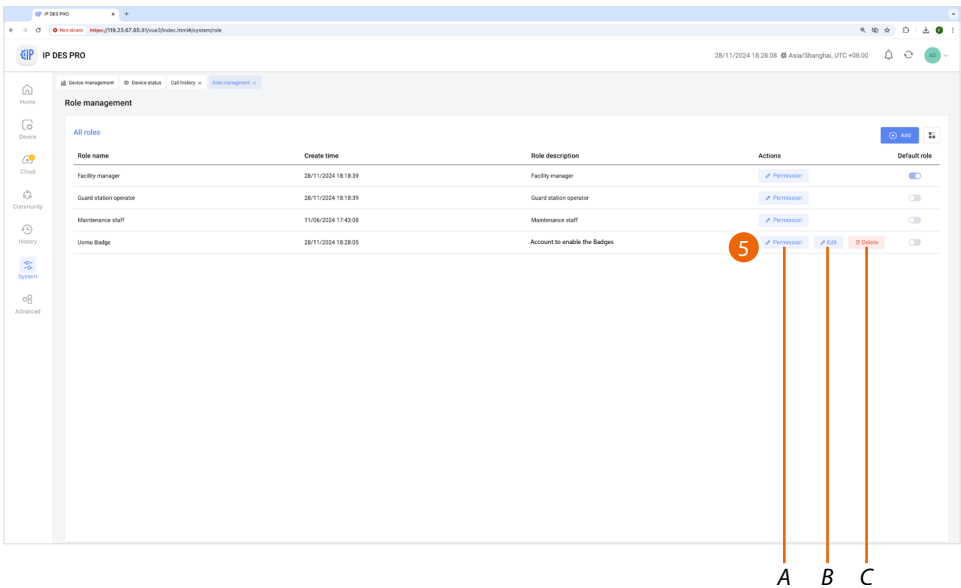
Role description

Account to enable the Badges

Cancel

Confirm

2. Enter the role name
3. Enter a description for the role
4. Click to confirm

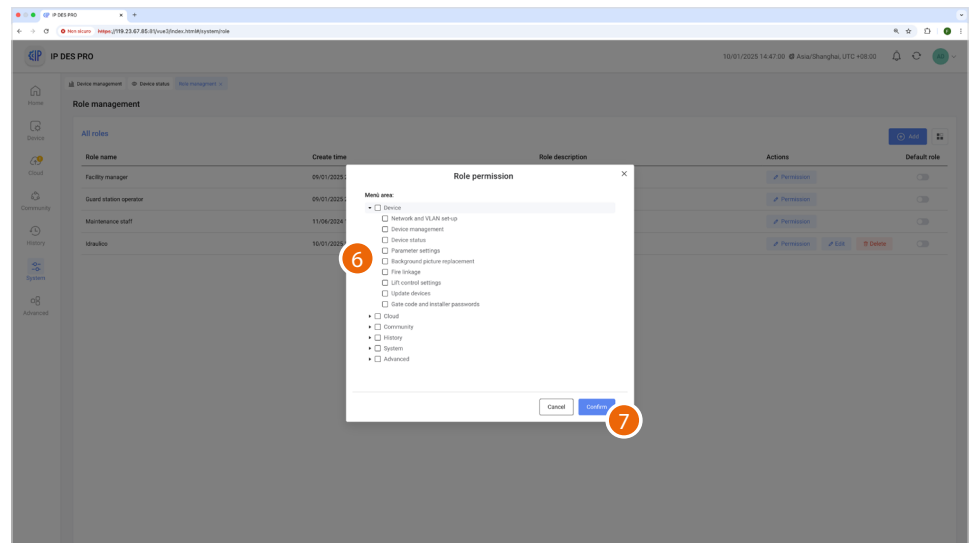


The role has been created and the role management buttons appear

- A Edit the permissions
- B Edit the role name and description
- C Delete the role

NOTE: to delete the role, it will first be necessary to delete the **associated accounts**

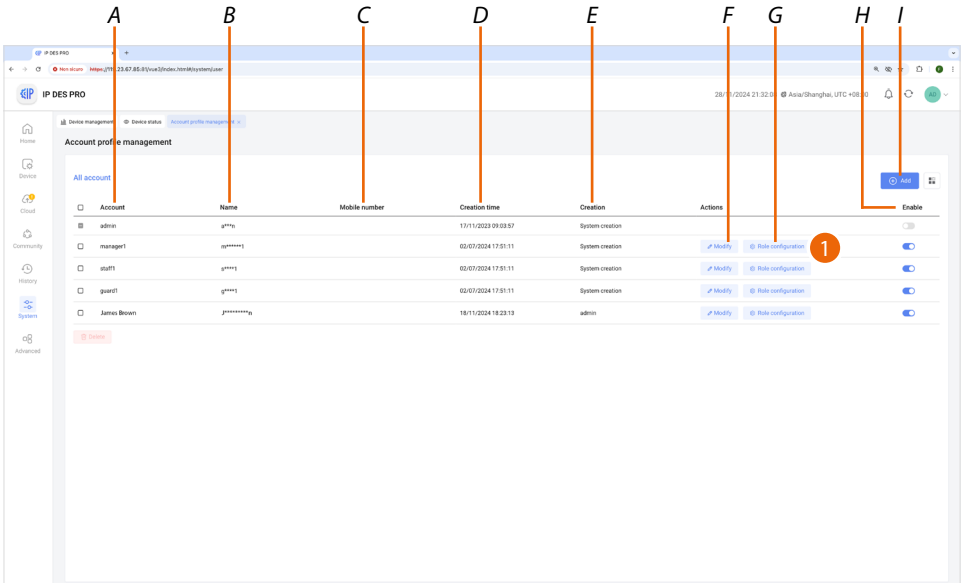
5. Click to define which menus this role will have access to



6. Select the menus
7. Click to confirm

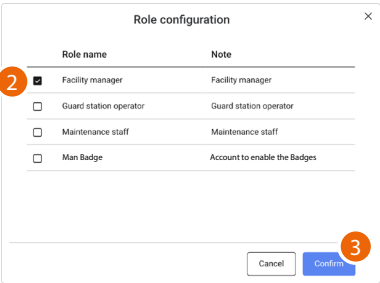
Account profile management

This page can be used to manage the SW operators by assigning them roles created in the [Role Management](#) page

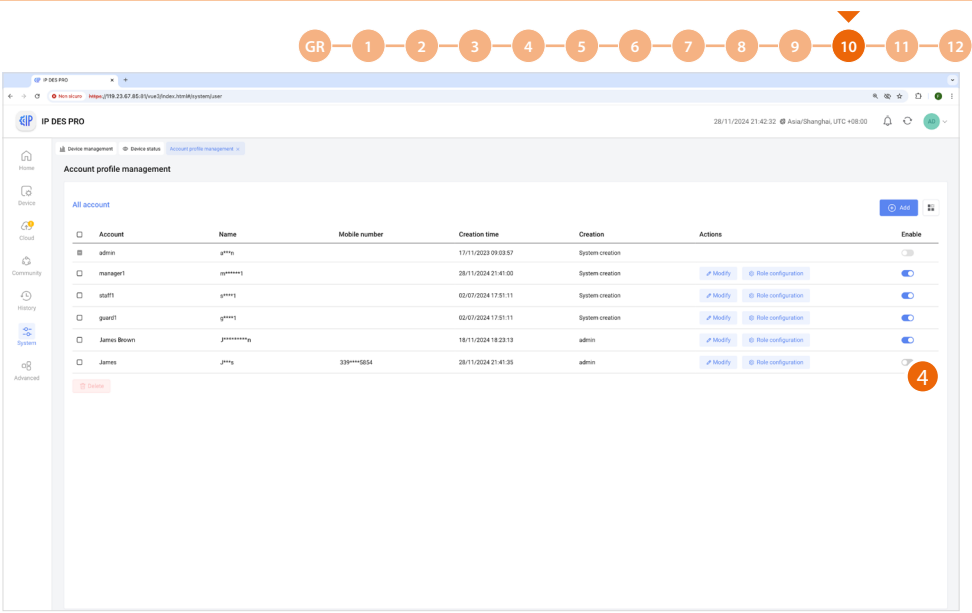


- A Account name
 - B Account user name
 - C Account telephone number
 - D Date of creation
 - E Account creation type:
System creation: created by default by the system
Admin: created from an account
 - F Modify account data
 - G Open the panel to manage account roles
 - H Enable/disable account
- NOTE: during the first enable, the password must be changed
- I Create an account

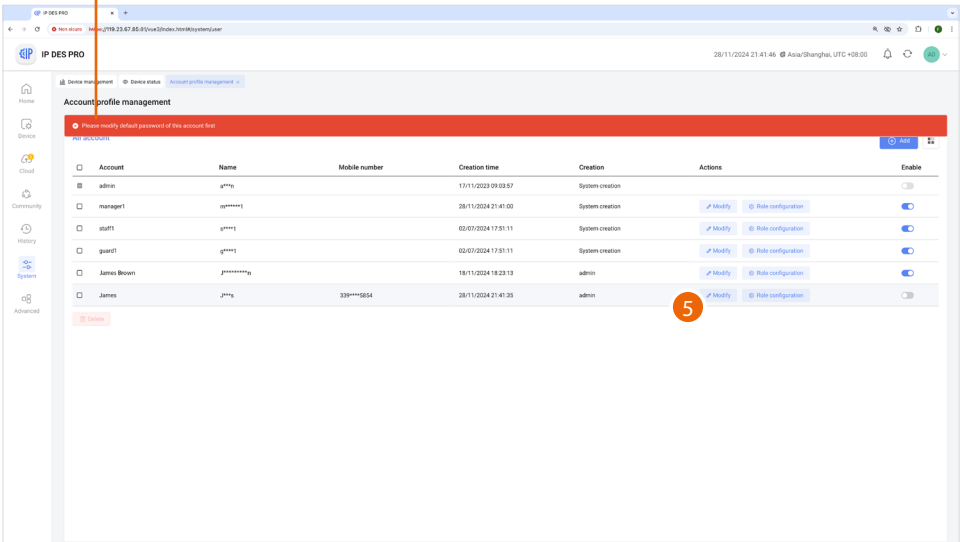
1. Click to display/modify the account roles



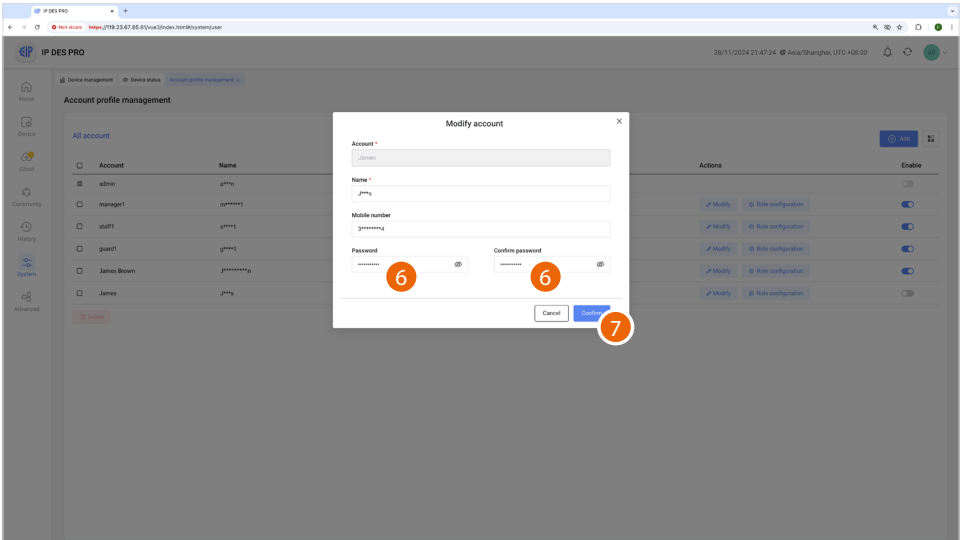
2. Select one or more roles
3. Click to confirm



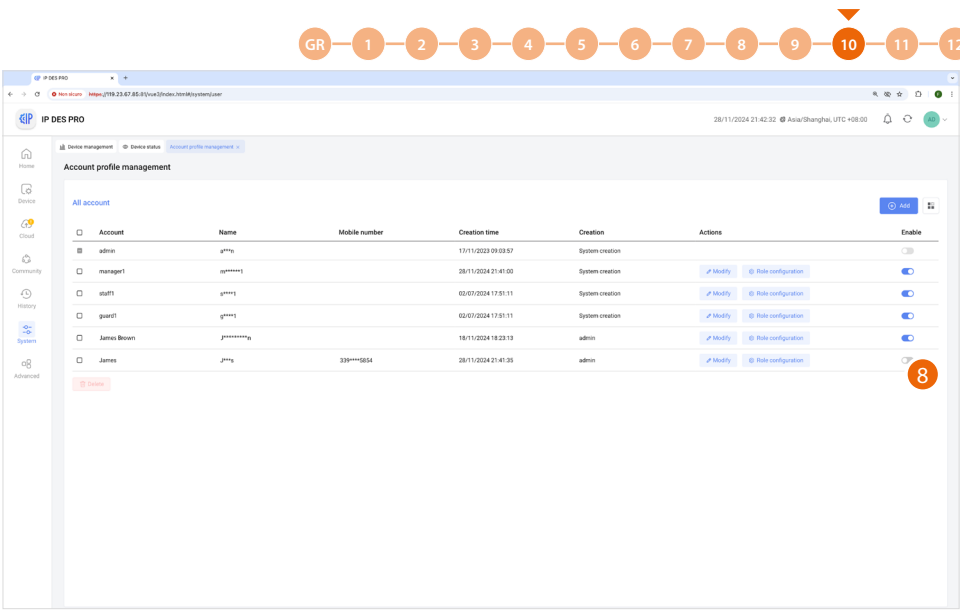
4. Click to enable the account
During the first enable, the password must be changed (A)



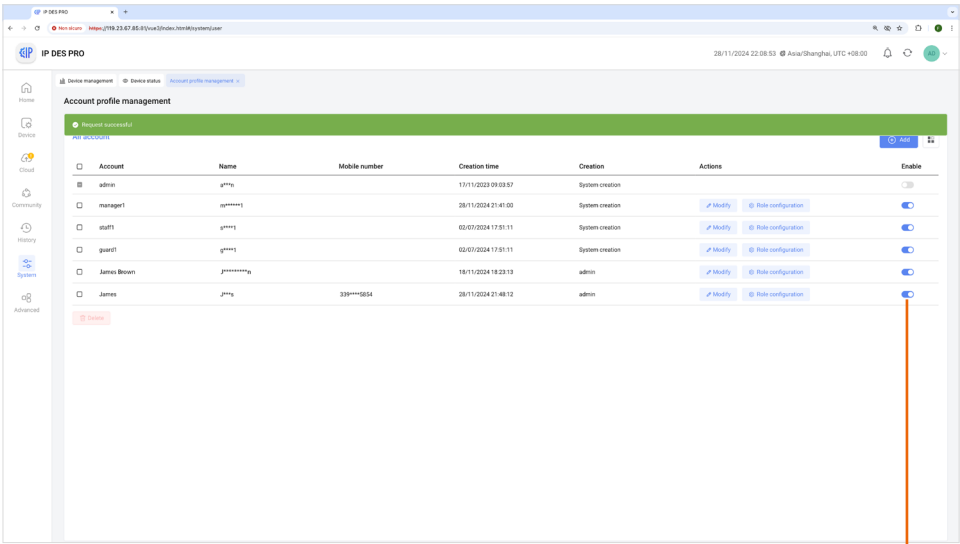
5. Click to continue and change the password



6. Enter and confirm the new password
7. Click to continue

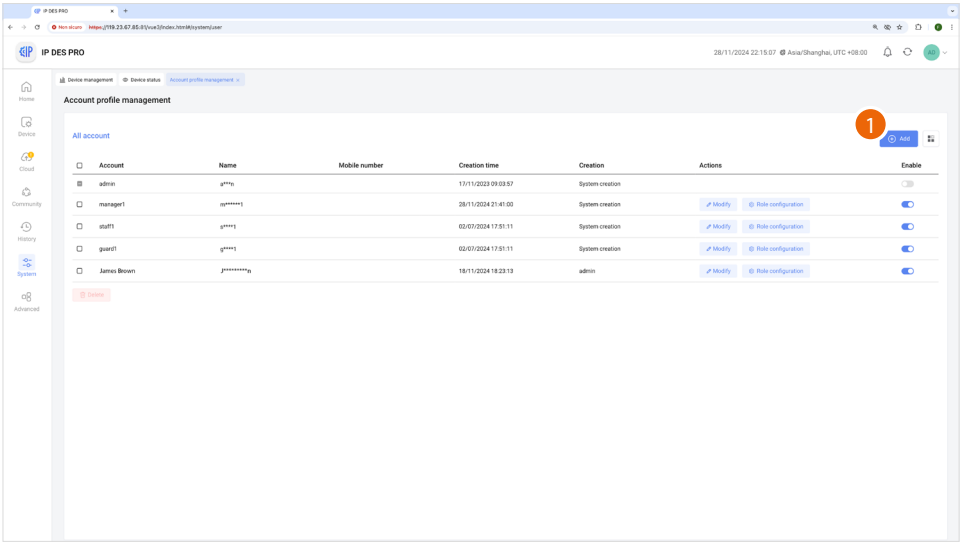


8. Click to enable the account



A The account has been enabled

Create an account



1. Click to create a new account

Add account

Account *

Max 20 characters

Name *

Max 20 characters

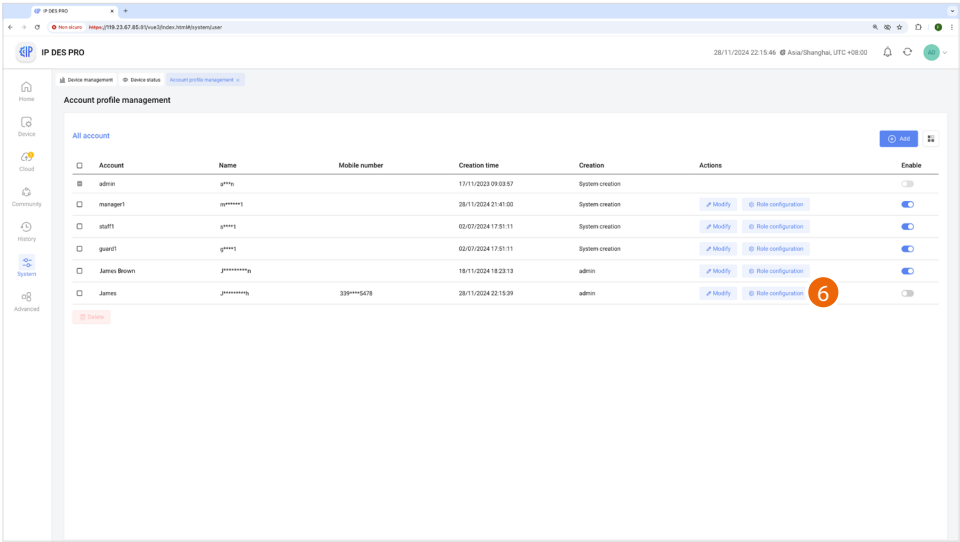
Mobile number

Please enter a mobile number

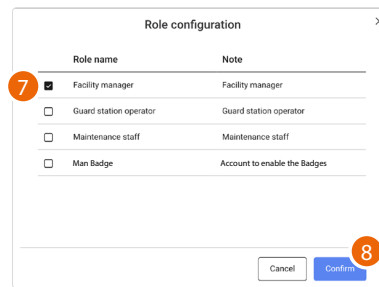
Cancel

Confirm

2. Enter the account name
3. Enter the name of the person using the account
4. Enter the telephone number
5. Click to confirm



6. The account has been created; click to assign a role to the same



A dialog box titled "Role configuration" with a close button (X) in the top right corner. It contains a table with two columns: "Role name" and "Note". The table lists four roles: "Facility manager" (checked), "Guard station operator", "Maintenance staff", and "Man Badge". A red circle with the number 7 is next to the first row. At the bottom right, there are "Cancel" and "Confirm" buttons, with a red circle and the number 8 next to the "Confirm" button.

Role name	Note
<input checked="" type="checkbox"/> Facility manager	Facility manager
<input type="checkbox"/> Guard station operator	Guard station operator
<input type="checkbox"/> Maintenance staff	Maintenance staff
<input type="checkbox"/> Man Badge	Account to enable the Badges

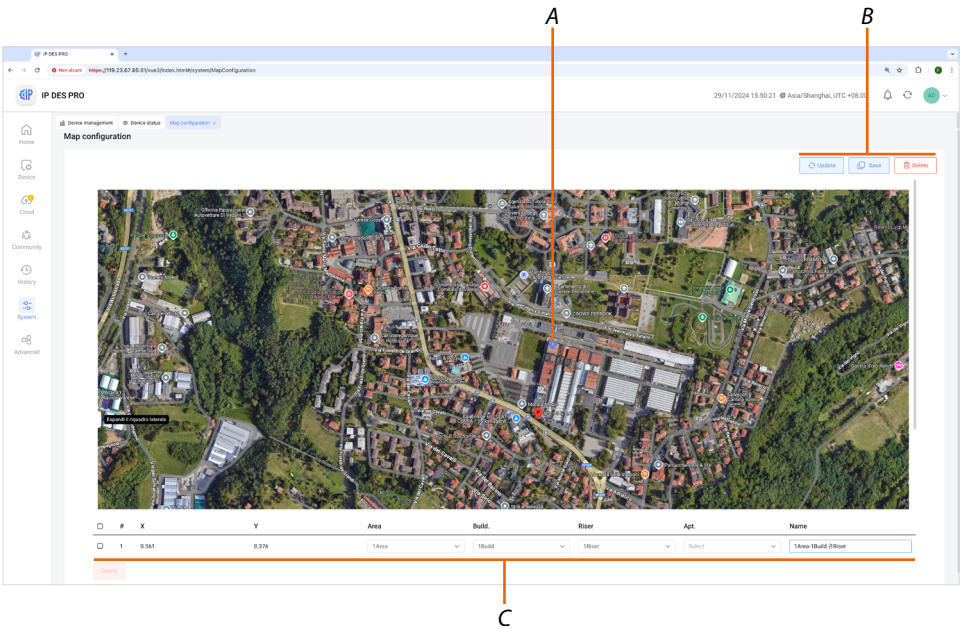
Cancel Confirm

7. Select one or more roles to be associated

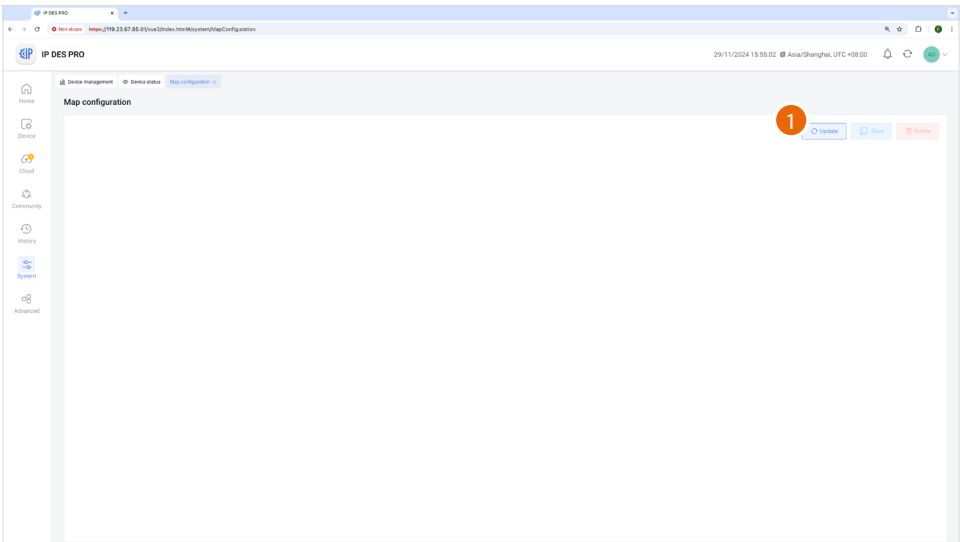
8. Click to confirm

Map configuration

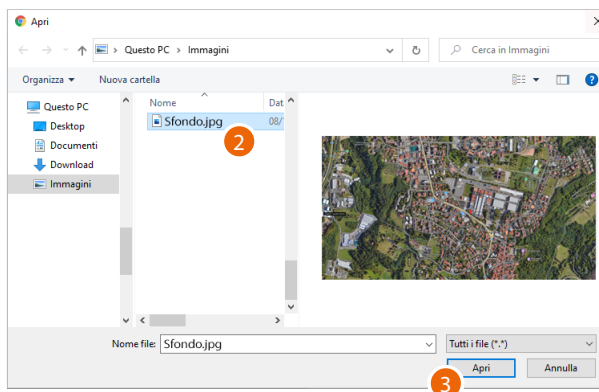
This page can be used to set up a background map for the Home Page and some markers, to make it easier to find the community Buildings



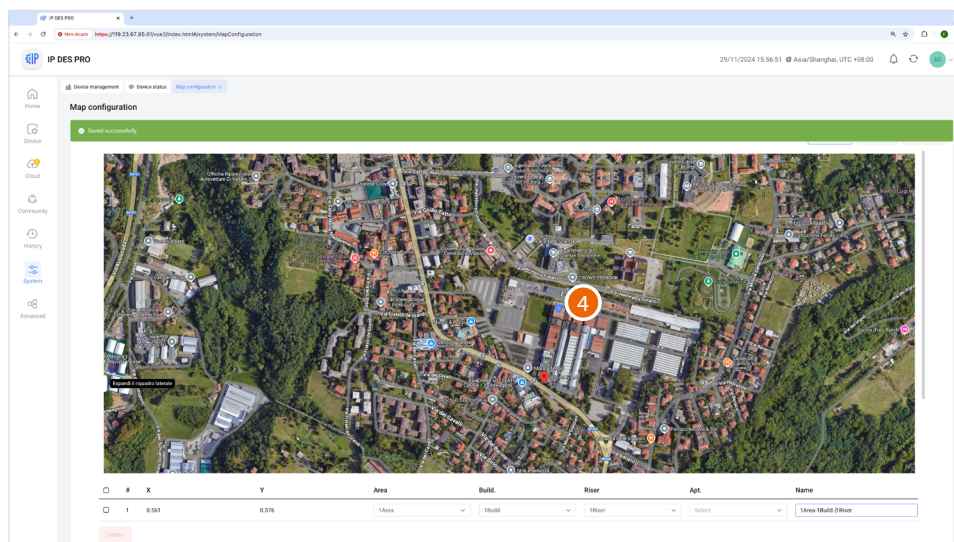
- A Markers
- B Map management keys
- C Marker management



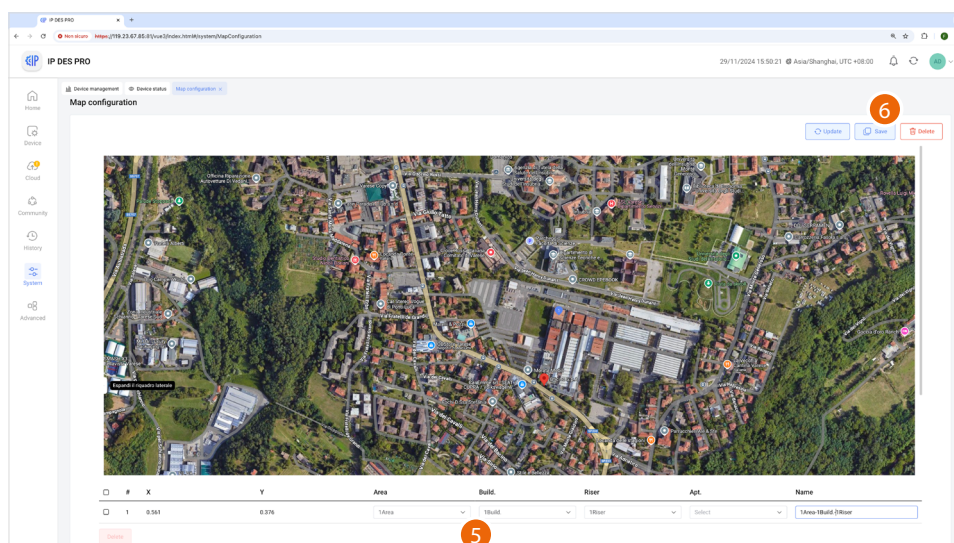
1. Click to load an image to use as map



2. Click to select an image
3. Click to open



5. Click on the map to add a marker corresponding to a community Building



6. Select the area and the Building of your community that you want to include
7. Click to save

Account operation log

This page can be used to view the list of operations carried out by the operators, with the corresponding details.

The screenshot shows the 'Account operation log' page in the IP DES PRO system. It features a table with columns for Time, Operator, Operation IP, Module, Type, Content, and Status. Above the table are filter buttons for Operator, Module, Start time, and End Time, along with an 'Apply filters' button. On the right side, there are icons for export and refresh. Labels A through I point to the following elements:

- A: Filter buttons (Operator, Module, Start time, End Time)
- B: Time column
- C: Operator column
- D: Operation IP column
- E: Module column
- F: Type column
- G: Content column
- H: Status column
- I: Export/Refresh icons

Time	Operator	Operation IP	Module	Type	Content	Status
29/11/2024 17:44:39	admin	2.196.113.19	Operator Management	User login	Operator login: operator name is [admin]	Success
29/11/2024 17:44:39	admin	2.196.113.19	Operator Management	User login agreement	Admin user have read and agree «Terms and Conditions» «Privacy Policy»	Success
29/11/2024 17:44:39	admin	2.196.113.19	Operator Management	User login	Operator login: operator name is [admin]	Success
29/11/2024 15:40:23	admin	2.196.113.19	Operator Management	User login	Operator login: operator name is [admin]	Success
29/11/2024 15:40:23	admin	2.196.113.19	Operator Management	User login agreement	Admin user have read and agree «Terms and Conditions» «Privacy Policy»	Success
29/11/2024 15:39:54	admin	2.196.113.19	Operator Management	User login	Operator login: operator name is [admin]	Success
29/11/2024 15:39:54	admin	2.196.113.19	Operator Management	User login agreement	Admin user have read and agree «Terms and Conditions» «Privacy Policy»	Success
29/11/2024 15:39:54	admin	2.196.113.19	Operator Management	User login	Operator login: operator name is [admin]	Success
29/11/2024 15:39:48	admin	2.196.113.19	Operator Management	User login	Operator login: operator name is [admin]	Success

A Filters

B Date/time of operation

C Account name

D IP addresses from which the change was made

E Configuration category

F Type of operation

G Description of the operation

H Operation result

I Export the list to an Excel® file

Filters

The screenshot shows the filter section of the 'Account operation log' page. Labels A through D point to the following elements:

- A: Operator filter button
- B: Module filter button
- C: Start time filter button
- D: End Time filter button

Operator	Module	Start time	End Time
----------	--------	------------	----------

A Account name filter

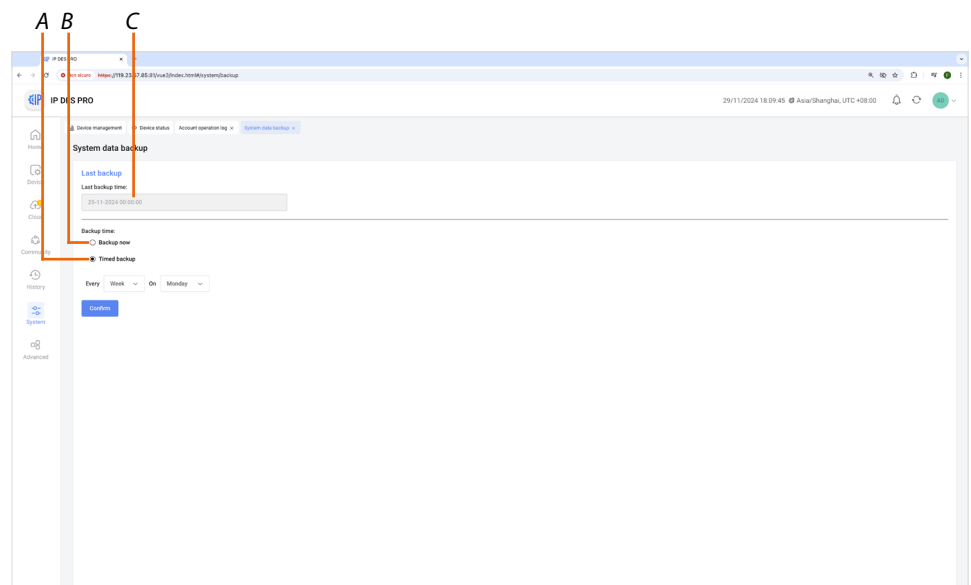
B Category configuration filter

C Operation start date/time filter

D Operation end date/time filter

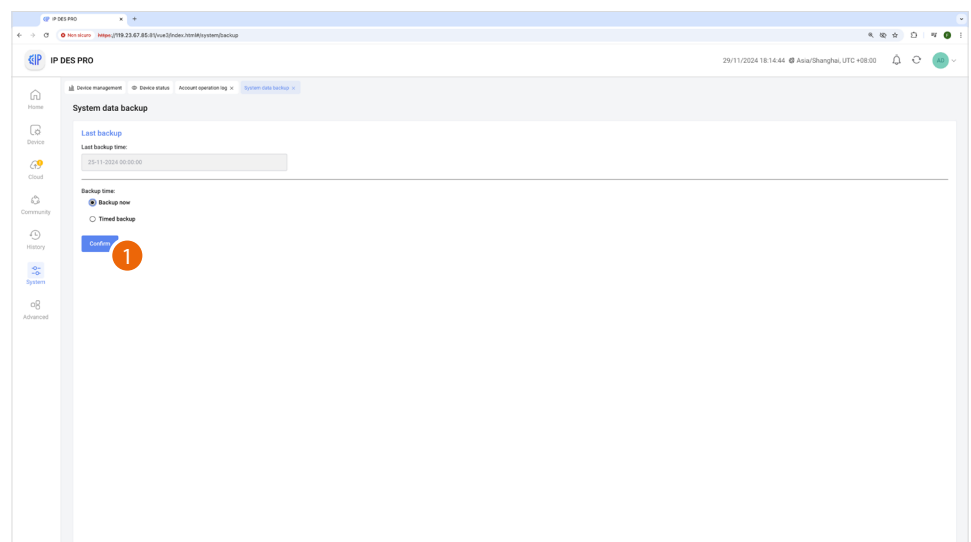
System data backup

This page can be used to backup the system
Date can be restored from the [System Data Recovery](#) page

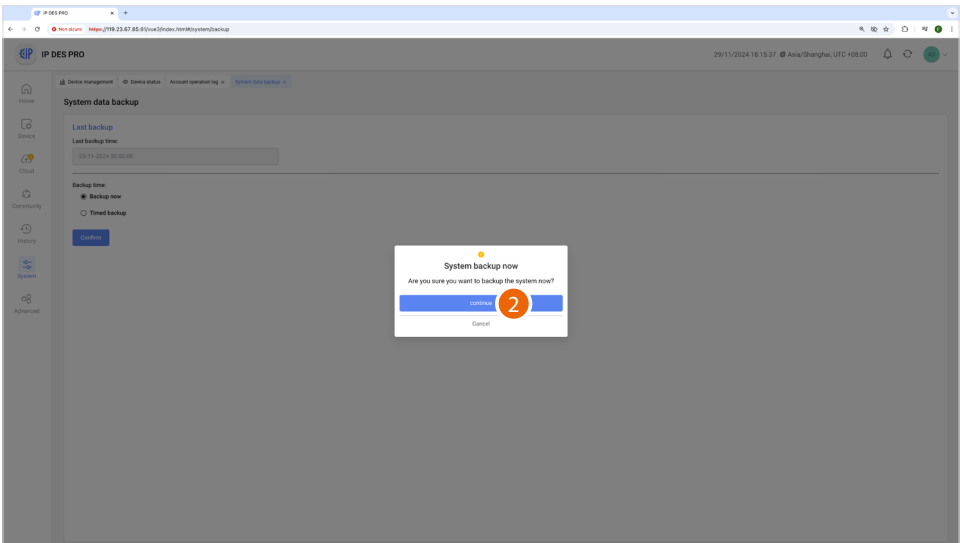


- A [Select scheduled backup](#)
- B [Immediate backup commands](#)
- C [Date and time of last backup completed](#)

Immediate backup



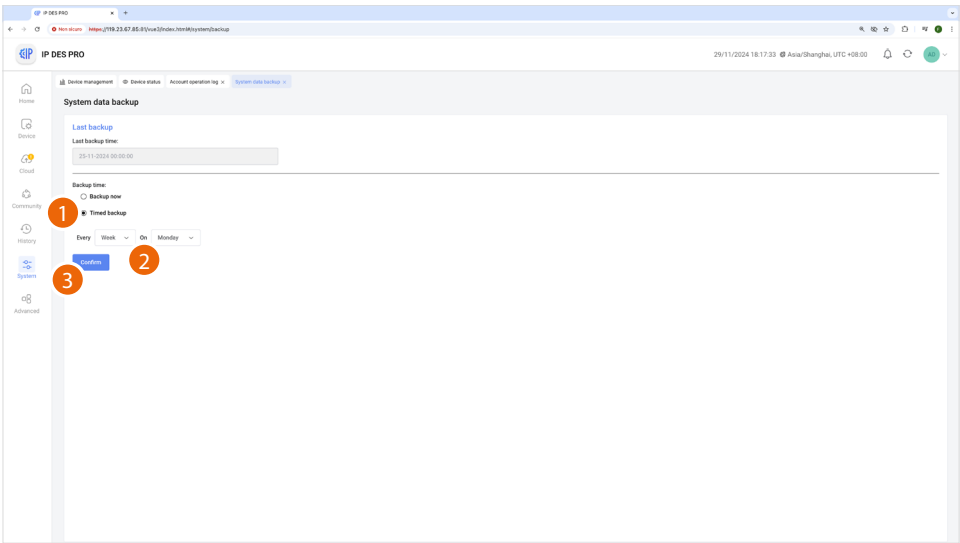
1. Click to immediately start the backup



2. Click to confirm, the backup will be available in the [System Data Recovery](#) page

Scheduled backup

This function allows you to set up a backup to be carried out on a regular basis

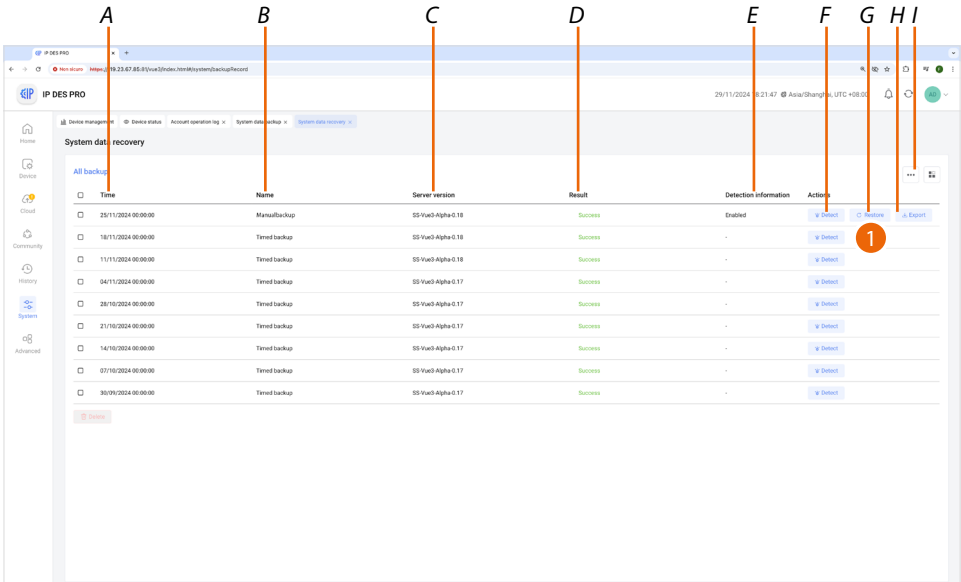


1. Click to set the backup parameters
2. Set the period
3. Click to confirm; the backup will be available in the [System Data Recovery](#) page

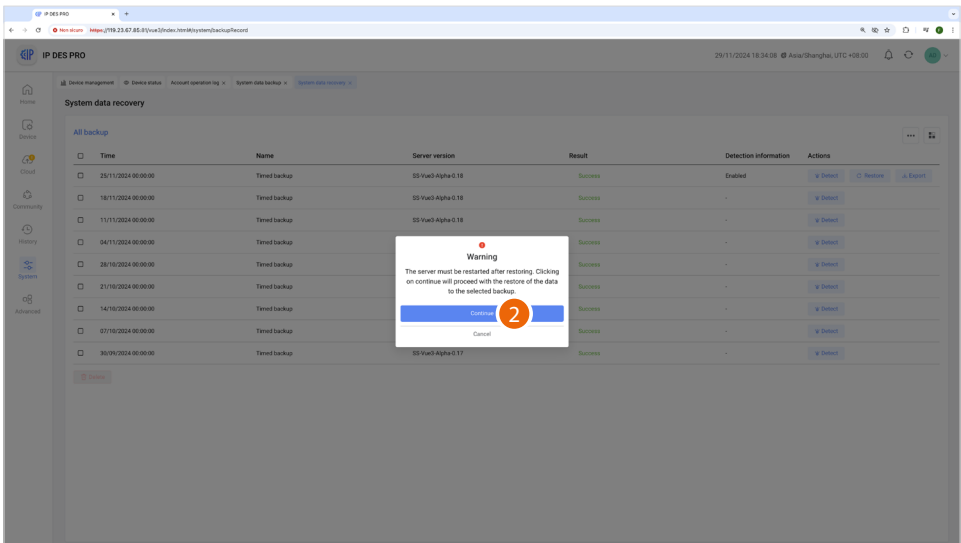
Backup period	
Every day	The backup will be carried out every day
Weekly	Select day of the week on which the backup will be carried out
Monthly	Select from 1 to 28 days; the backup will be repeated for the selected number of days

System data recovery

This page can be used to restore backups saved on the [System data backup](#) page

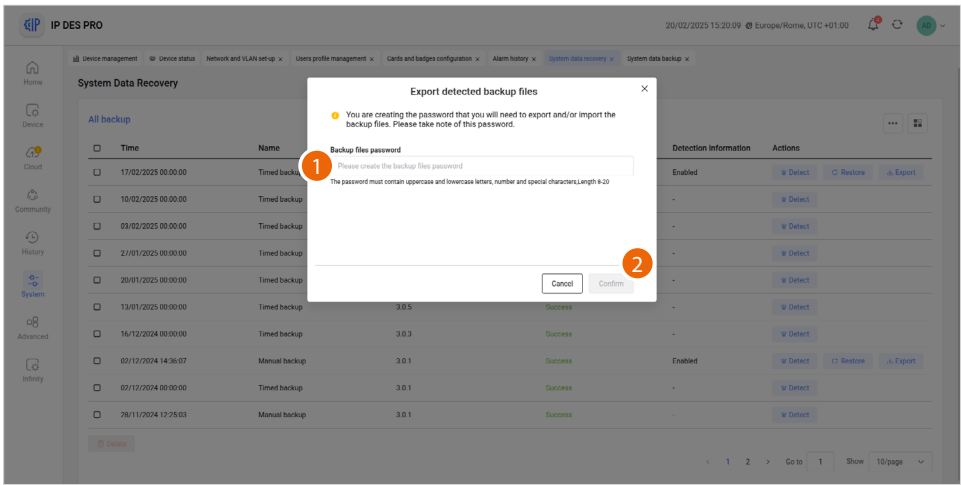


- A Backup date/time
 - B Backup type: manual or automatic
 - C SD version on which the backup was saved
 - D Backup result
 - E Availability of the backup file on the DES server
 - F Backup presence and integrity check.
If the check is successful, the Restore (G) and Export (H) buttons appear
 - G Restore backup
 - H [Export backup](#)
 - I [Import backup](#)
1. Click to restore the data

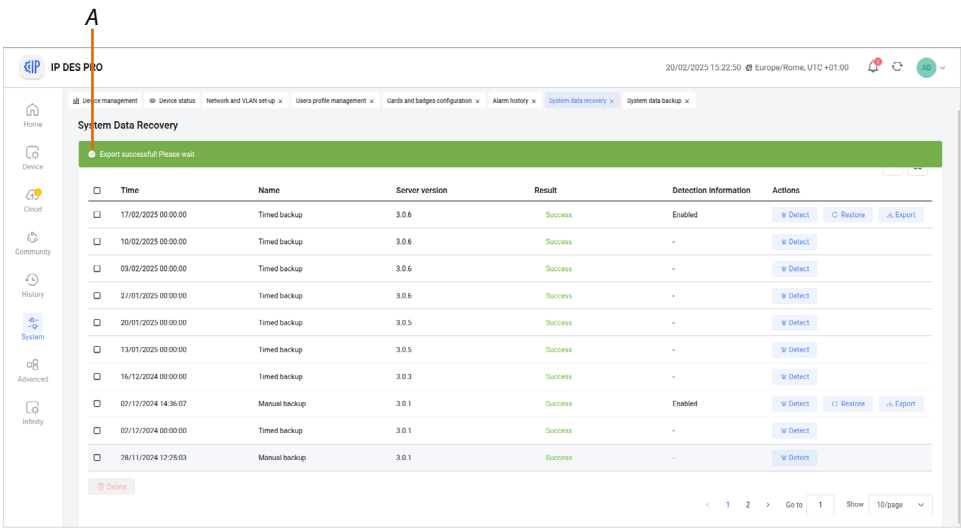
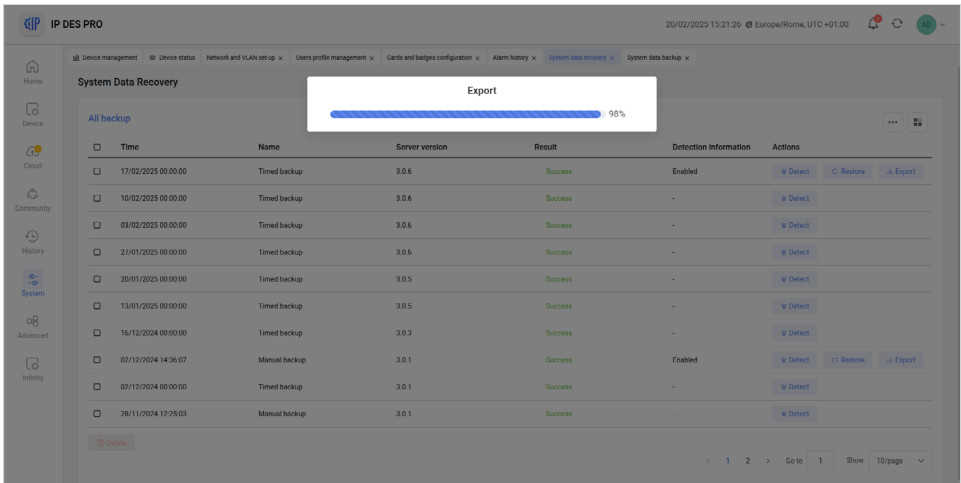


2. Click to confirm
- Caution:** the existing data will be overwritten

Export backup

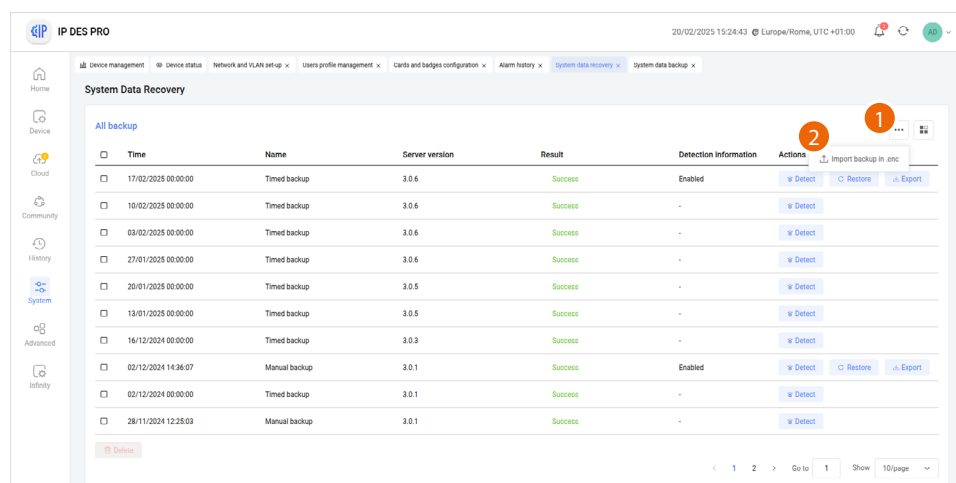


1. Click to create a password that will be needed later when importing the backup
2. Click to confirm

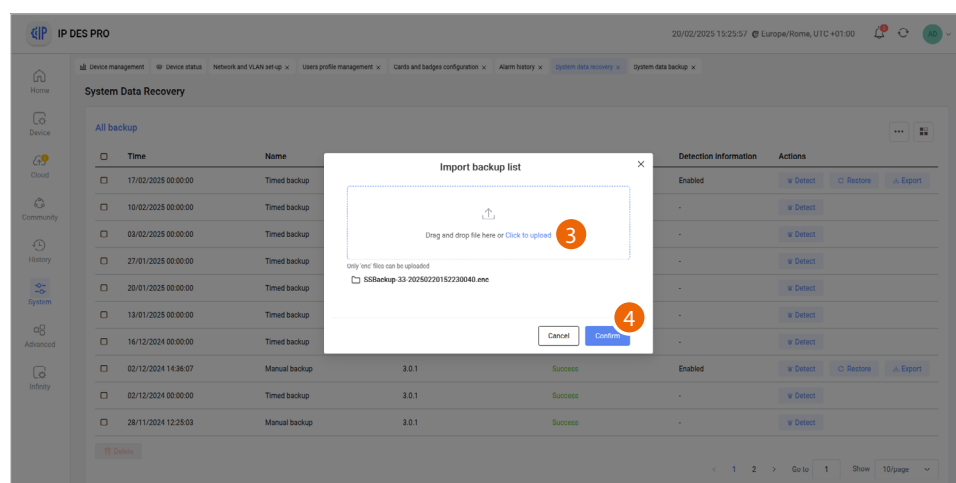


A The message indicates that the backup has been correctly exported

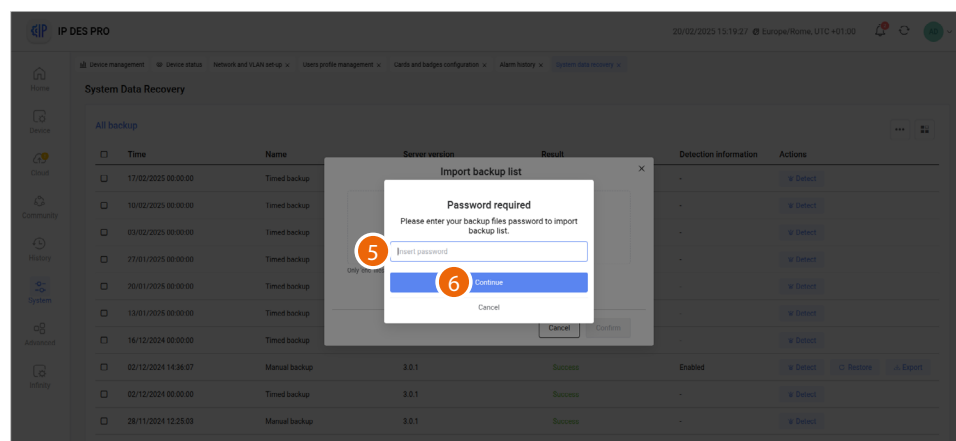
Import backup



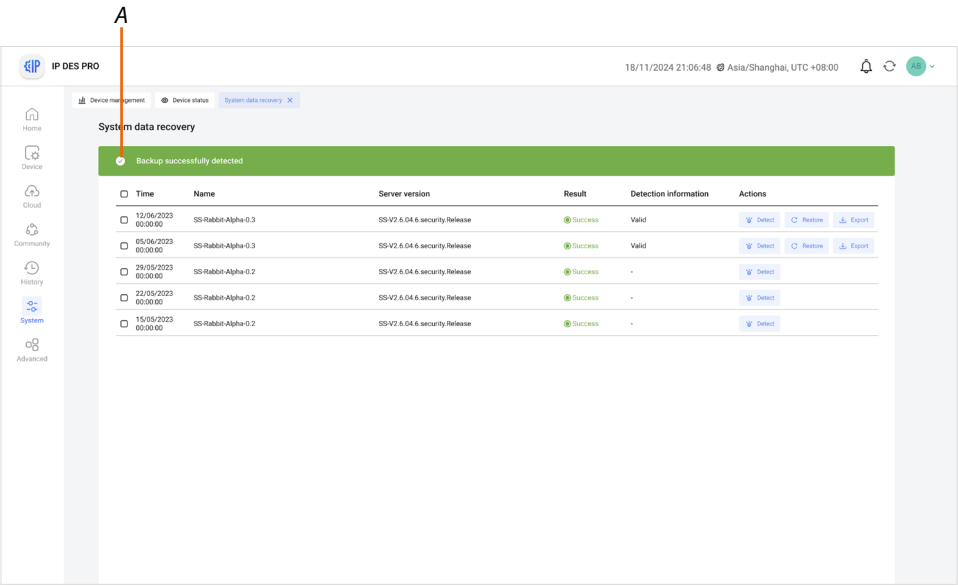
1. Click to open the menu and import a backup
2. Click to import a backup



3. Click to select the backup that you want to import
4. Click to confirm



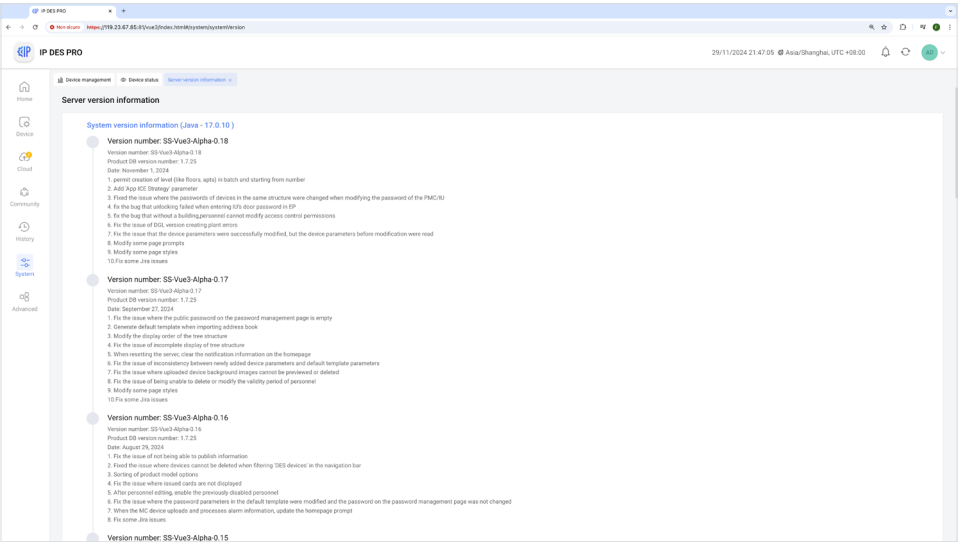
5. Enter the password previously created when exporting the backup
6. Click to continue



A The message indicates that the backup has been correctly exported

Server version information

This page can be used to view the history of the software versions installed. The one currently installed is the first on the list.

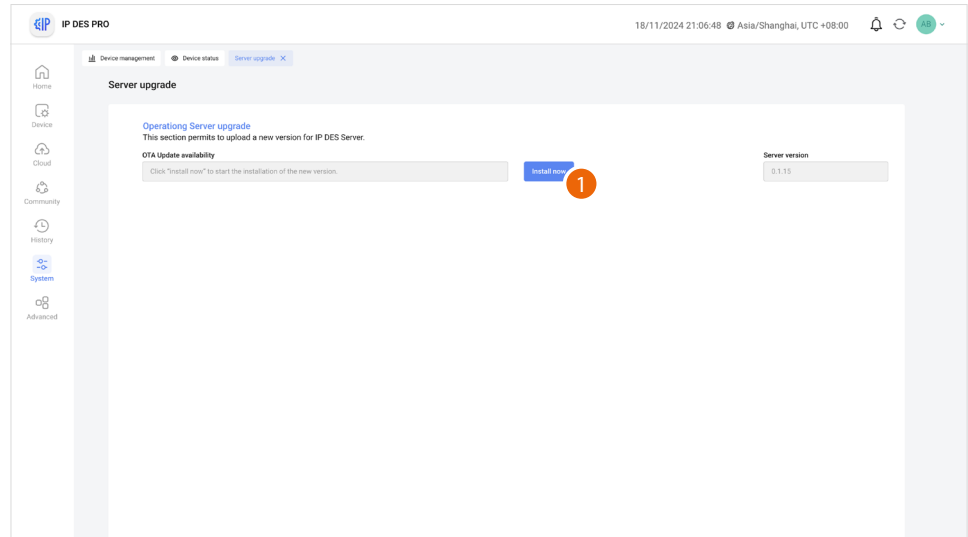


Server upgrade

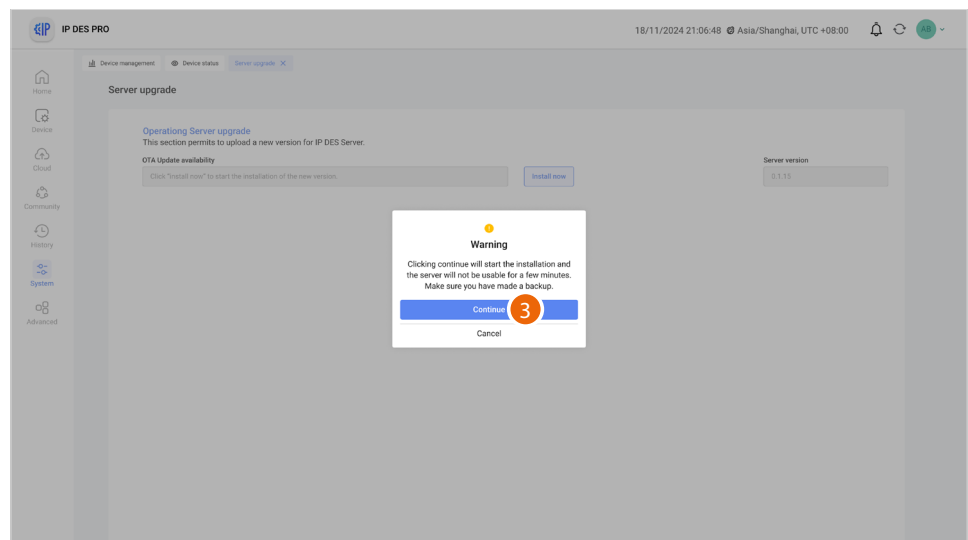
This page can be used to update the IP DES software.

It does not update the complete operating system but only this software, applying any new features and bug fixes

If a new IP DES software version is available, the key to start the installation appears.



2. Click to start the update procedure

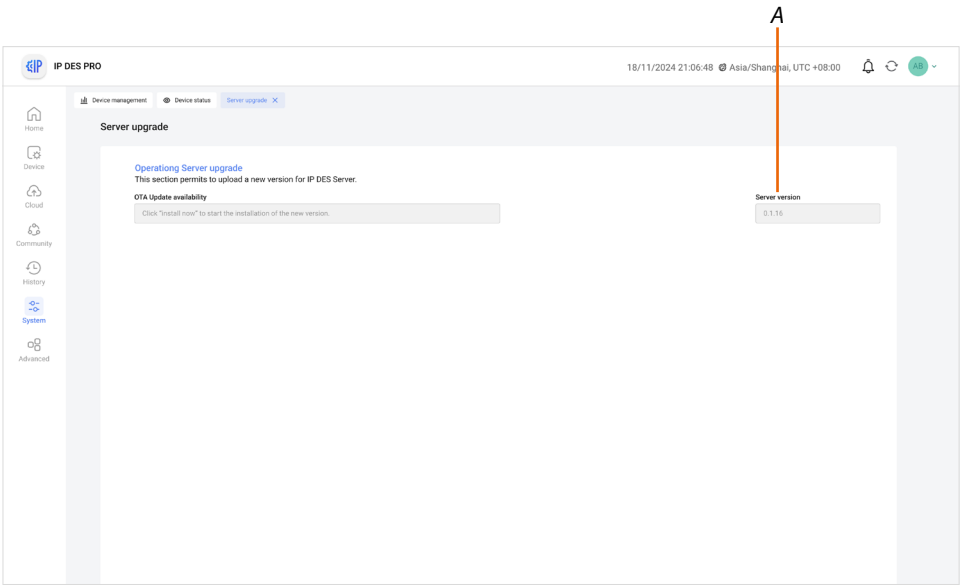


3. Click to start the installation

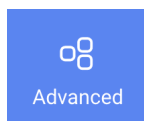
NOTE: The server will be unavailable for a few minutes.

NOTE: Make sure a backup has been made.

Installation successful.



A Current software version

Advanced

Menu reserved to advanced developers.

System parameter configuration

View and change some configuration parameters

Device catalogue

View the catalogue of devices managed by the IP DES Server, check their details and import a new catalogue.

Device offline log

View the device online and offline status history

Access control user details

View the list of users who can access certain entrance panels.

Access version debug

It allows to check that the access database version in the entrance panels is the same as the database on the IP DES Server. It also allows to force the alignment or regenerate the database.

Diagnostics

It allows to download a DES IP Server .log file for use in case of advanced technical support.

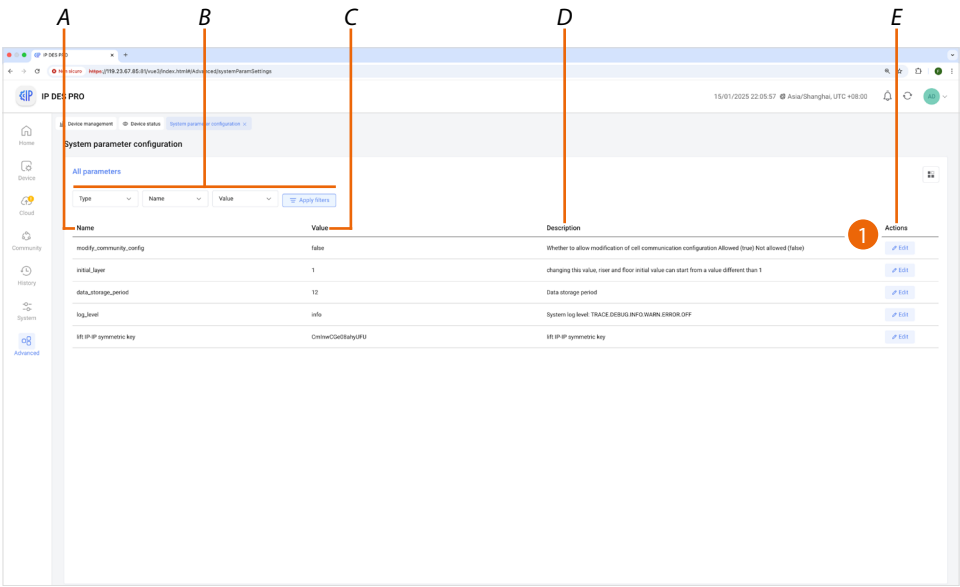
Factory reset

Restore the factory settings of the IP DES Server

System parameter configuration

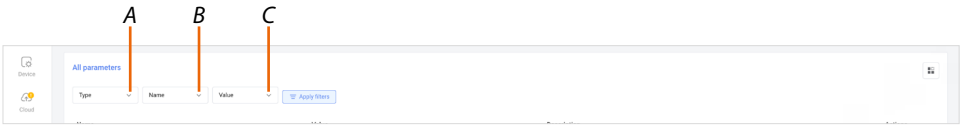
In this page it is possible to display and modify some configuration parameters such as:

- [modify_community_config](#)
- [initial_layer](#)
- [data_storage_period](#)
- [log_level](#)
- [lift IP-IP symmetric key](#)



- A Parameter name
 - B [Filters](#)
 - C Parameter value
 - D Parameter description
 - E Actions available for each parameter
1. Click to open the modification screen

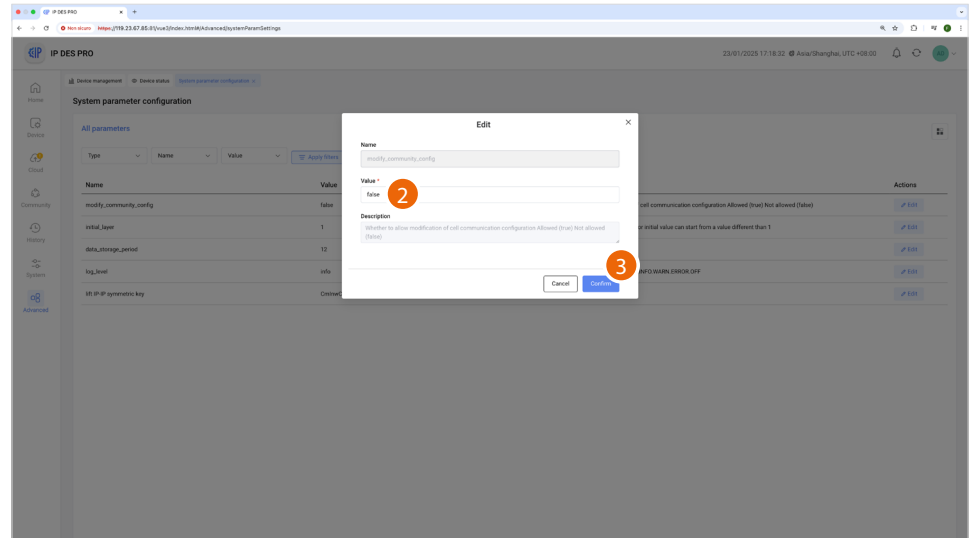
Filters



- A Parameter type filter
- B Parameter name filter
- C Value type filter

Modify_community_config

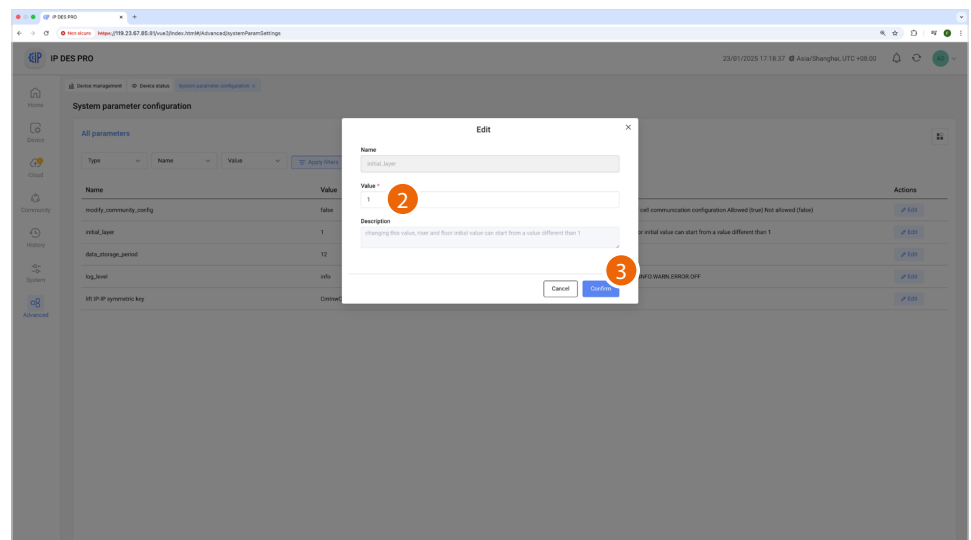
After completing the configuration, this function allows to enable/disable the possibility of changing the number of digits that make up the level names.



2. Click to enable (true) or disable (false).
The default function has been disabled.
3. Click to confirm.

Initial_layer

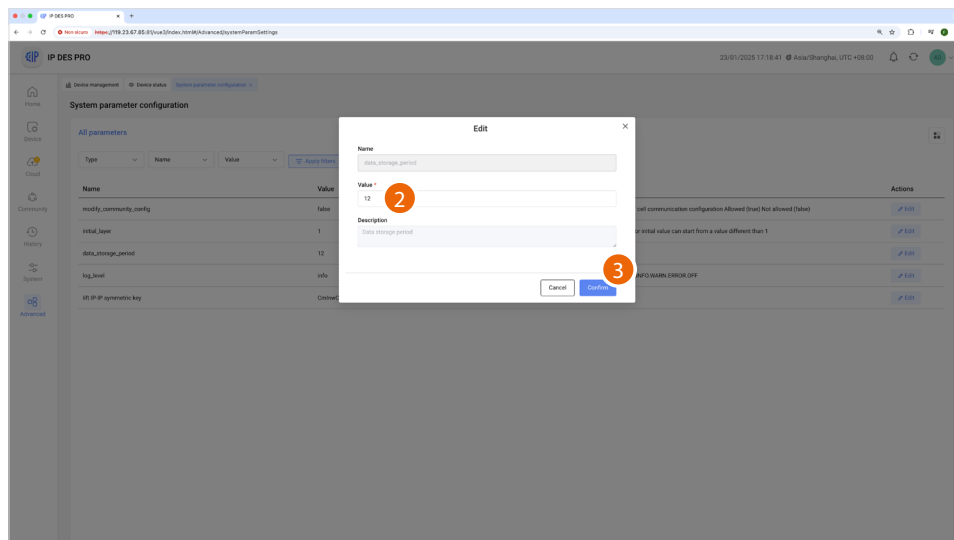
This function can be used to change the initial number of floor and riser levels, which normally starts at 1.



2. Click to set the initial value from which to count the levels.
3. Click to confirm.

Data_storage_period

Configure the period (in months) during which data will be stored (logs, call history, accesses, etc.). After this period, the data will be overwritten by new ones.



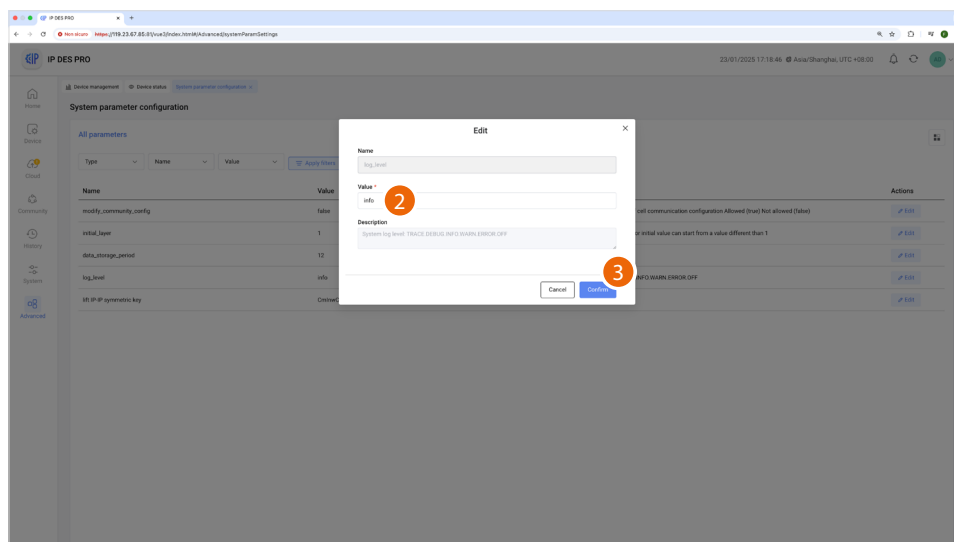
2. Click to set the number of months.

NOTE: Set the duration in a manner compatible with the regulations in force in the country where the IP DES Server is installed

3. Click to confirm.

Log_level

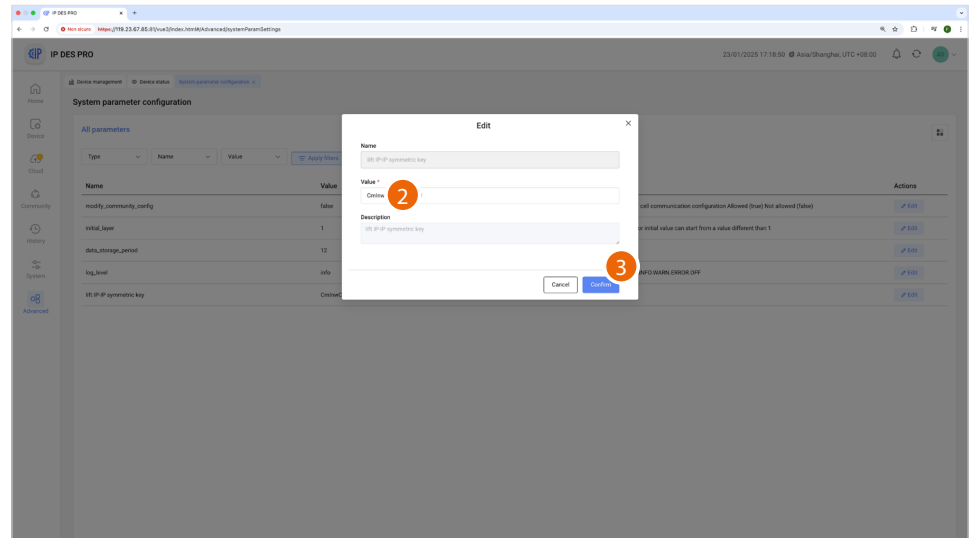
Set the level of details of the system logs, meaning the detail level of the information recorded by the system.



2. Click to select the detail level in ascending order between ERROR, WARNING, INFO AND DEBUG.
3. Click to confirm.

Lift IP-IP symmetric key

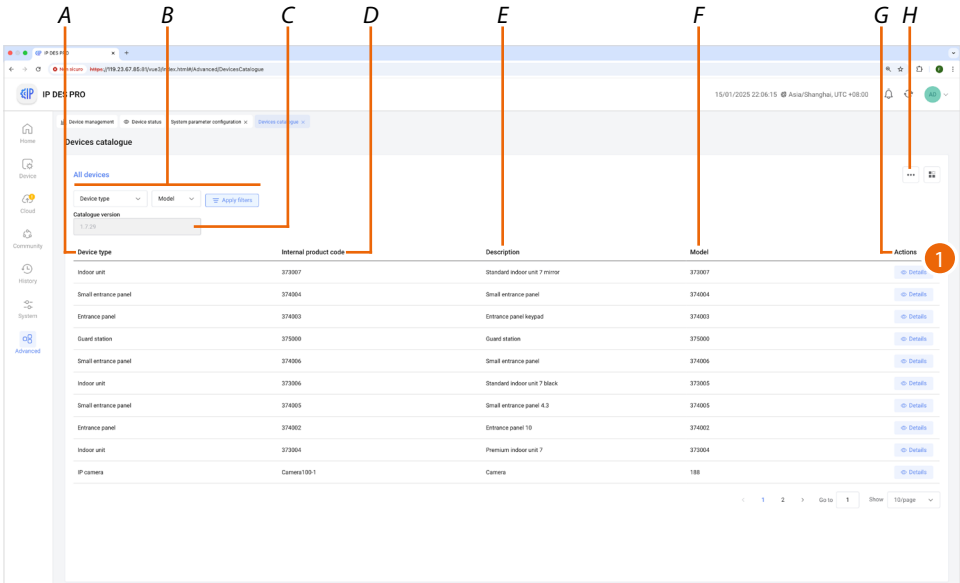
Set the symmetric key for IP-IP integrations with other lift systems.



2. Click to enter the symmetric key.
3. Click to confirm.

Device catalogue

This page can be used to view the catalogue of devices managed by the IP DES Server, check their details and [import a new catalogue](#).



A Type of device

B [Filters](#)

C Current catalogue version

D Internal item code of the product

E Device type description

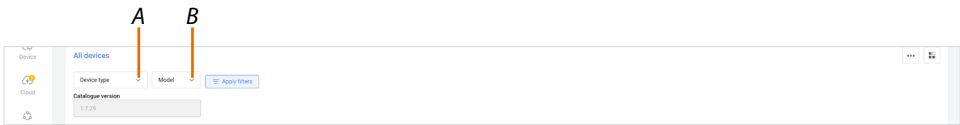
F Item code

G Device details

H [Import catalogue](#)

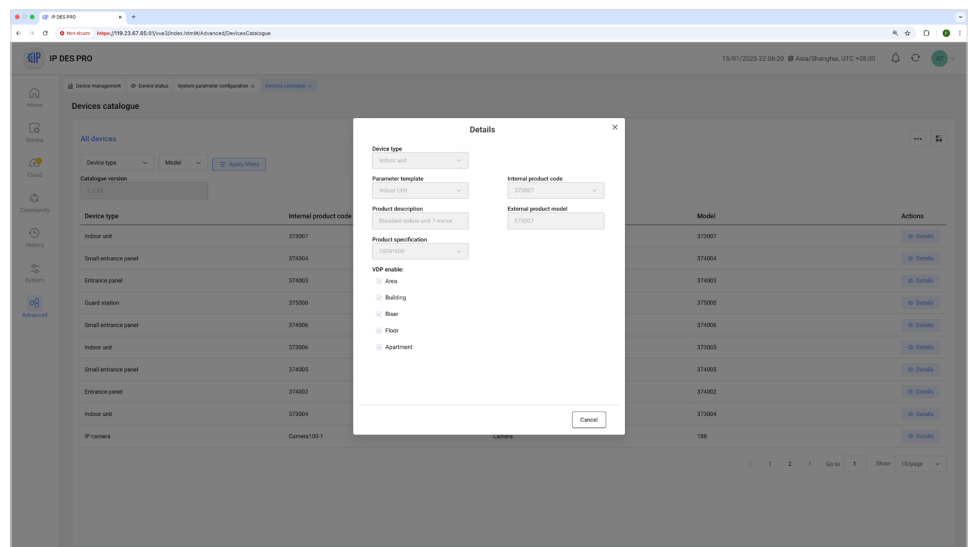
1. Click to view the details of the selected device

Filters

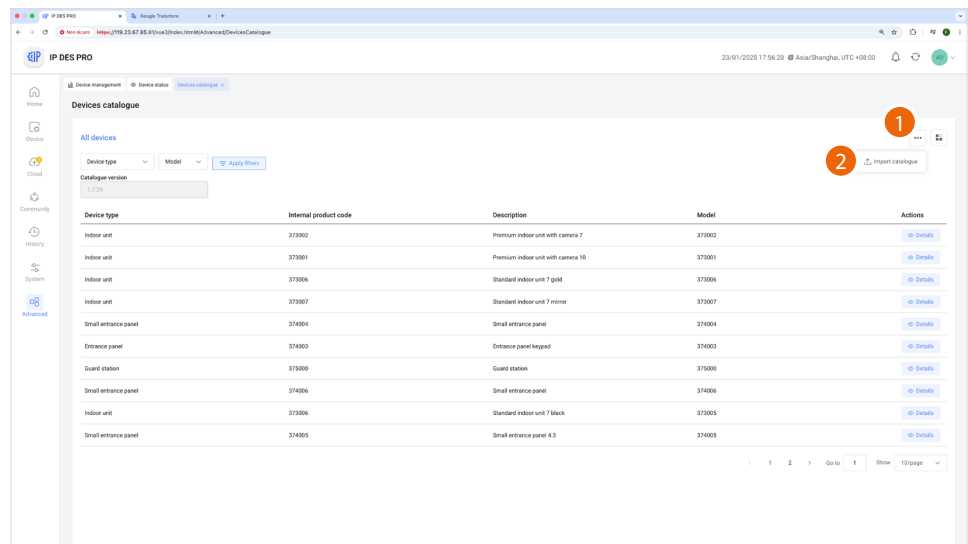


A Device type filter

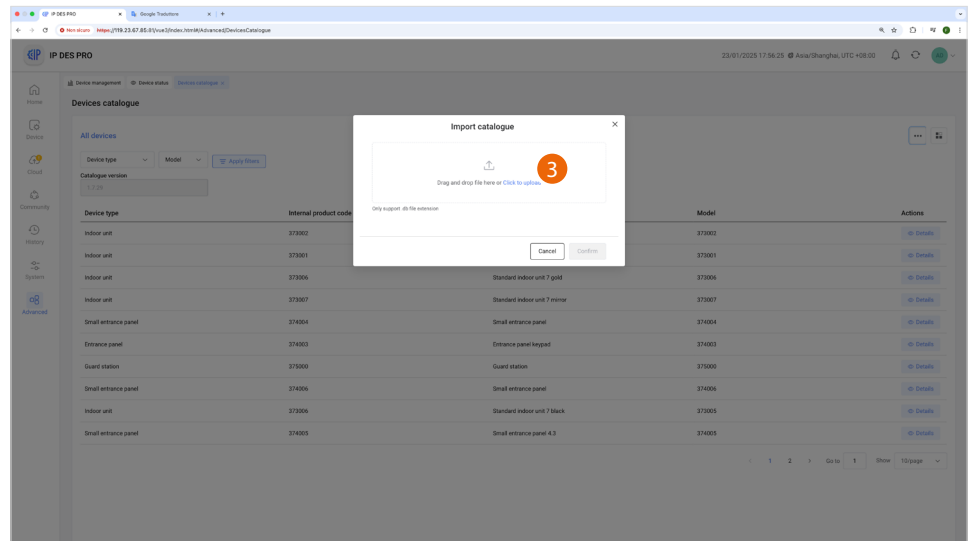
B Device model filter



Import catalogue



1. Click to select the catalogue import.
2. Click to import a catalogue.



3. Import a catalogue

Device offline log

This page can be used to view the device online and offline status history

The screenshot shows the 'Device offline log' page in the IP DES PRO software. The interface includes a sidebar with a tree view of communities (1 Area, 1 Gas, 01 Area, 1 Build, 2 Build, 3 Build, 4 Build). The main area displays a table of device logs. Above the table are filters for Device type, Model, and Device code. The table columns are labeled A through I: UC, Device type, Model, Device code, Device address, Time, and Type. The table contains several rows of data with status indicators (Online or Offline).

A Progressive number

B Type of device filter (IU, EP, etc.)

C Type of device

D Item code filter

E Item code

F Community ID + Unique code + Mac address

G Name of the customisable device.

The original name represents **the address of the device in the community.**

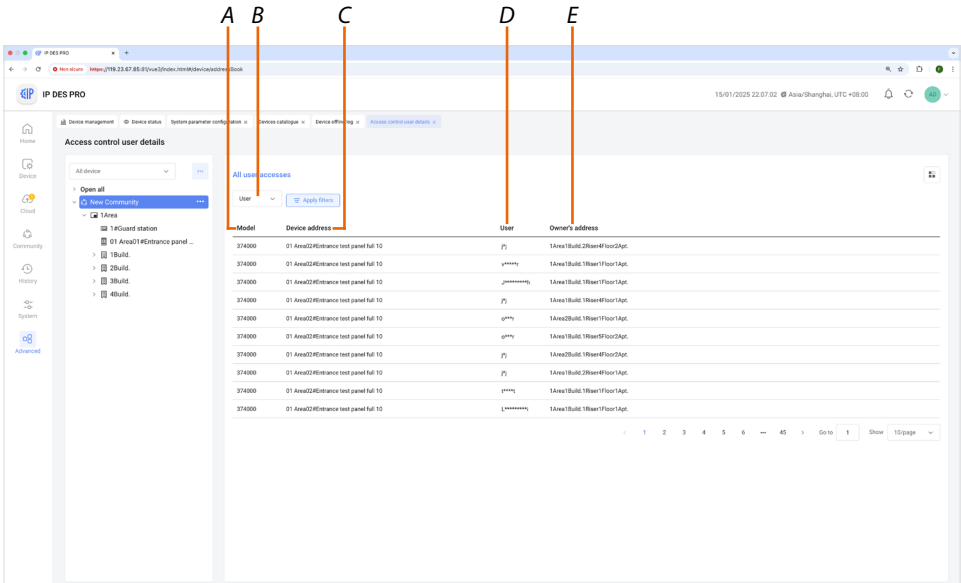
H. Status start date/time

I. Device status

1. Select the community branch for which you want to view the device history
2. If necessary, use the filters to narrow down the selection
3. Click to apply the filter

Access control user details

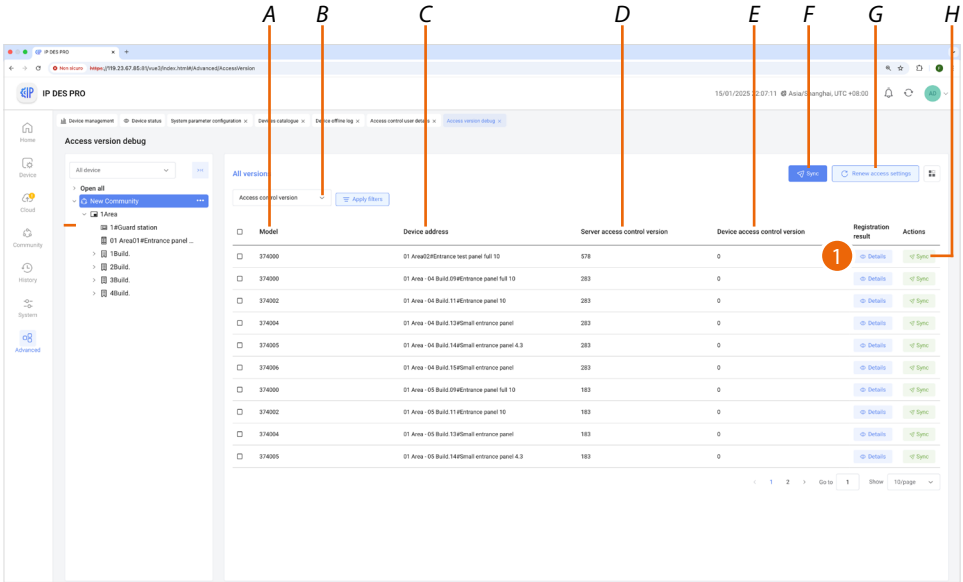
This page can be used to view the list of users who can access certain entrance panels.



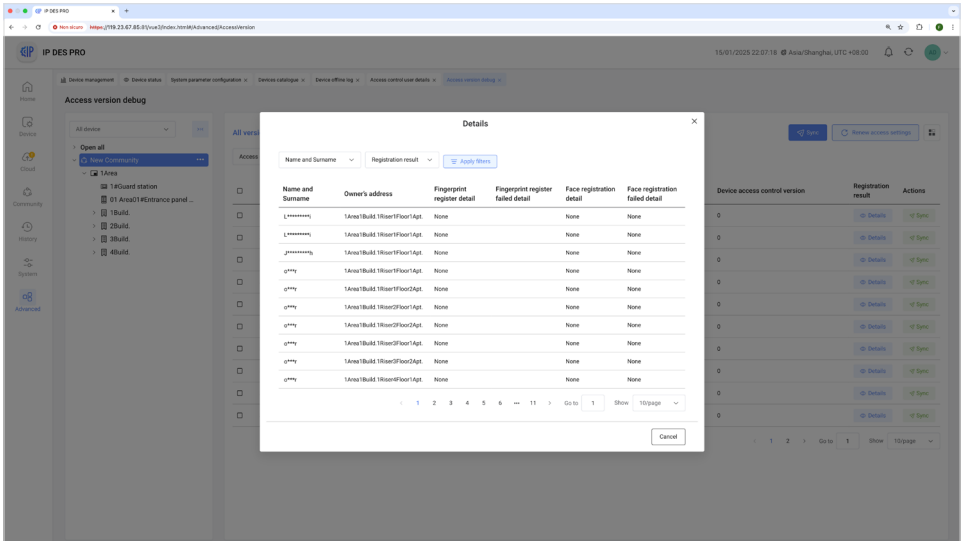
- A Item code
- B Filter by person's surname and first name
- C Name of the customisable device.
The original name represents the the address of the device in the community
- D Name of the person
- E Apartment address

Access version debug

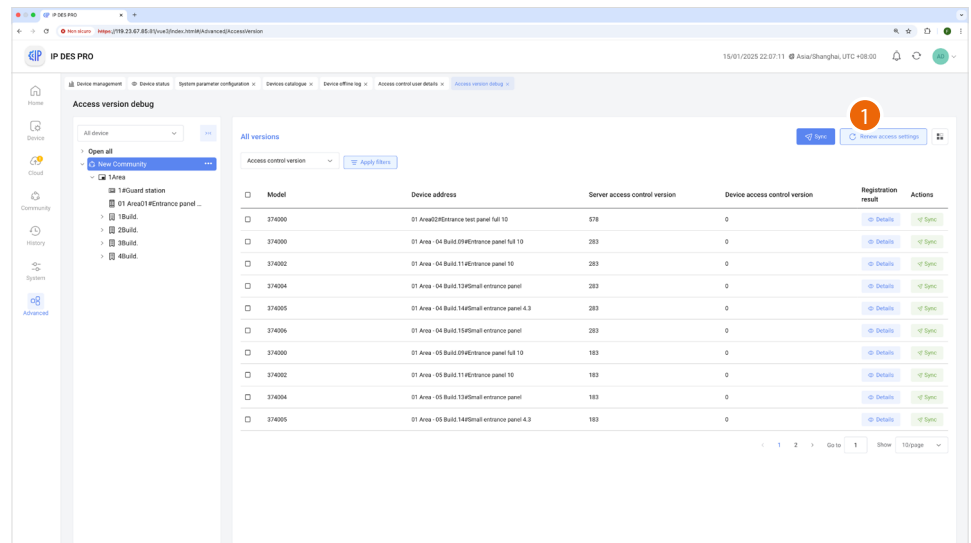
This page can be used to check that the access database version in the entrance panels is synchronised with the database version on the IP DES Server.
It is also possible to force the alignment or regenerate the database.



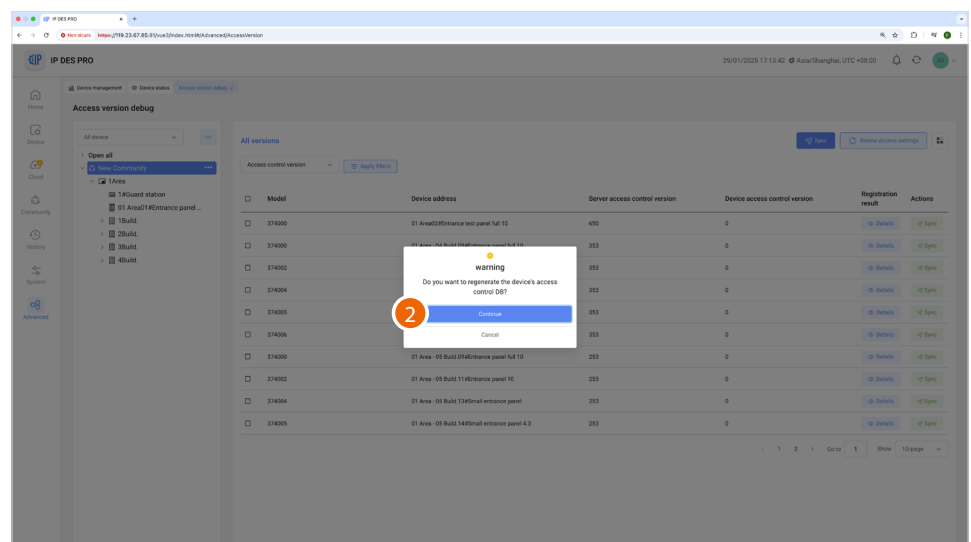
- A Item code
 - B Access control version filter
 - C Name of the customisable device.
The original name represents the *the address of the device in the community*.
 - D Version of the access database on the server
 - E Version of the access database in the EP
 - F Align the database in all EP
 - G *Regenerate the database*
 - H *Align the database in selected EP*
1. Click to display the details



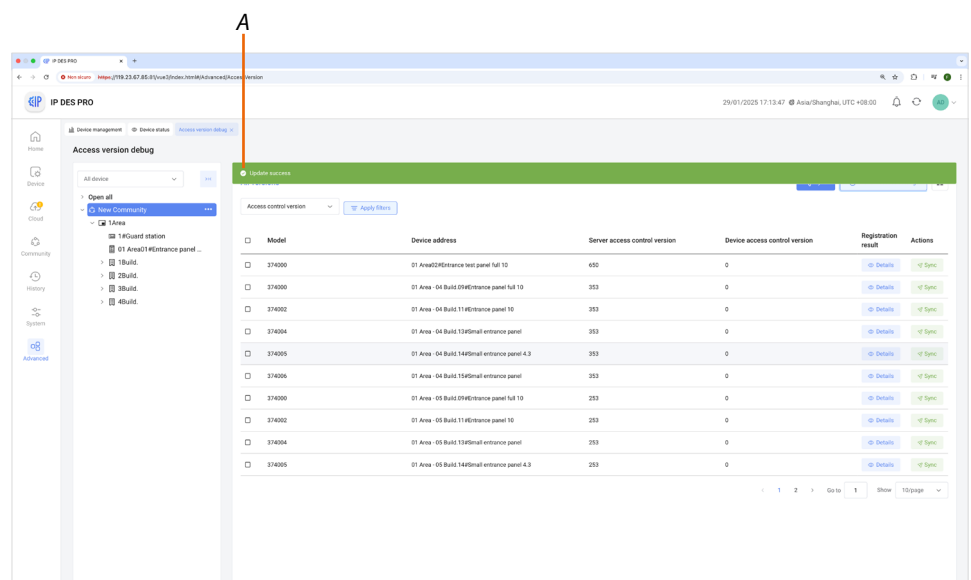
Database regeneration



1. Click to regenerate the database

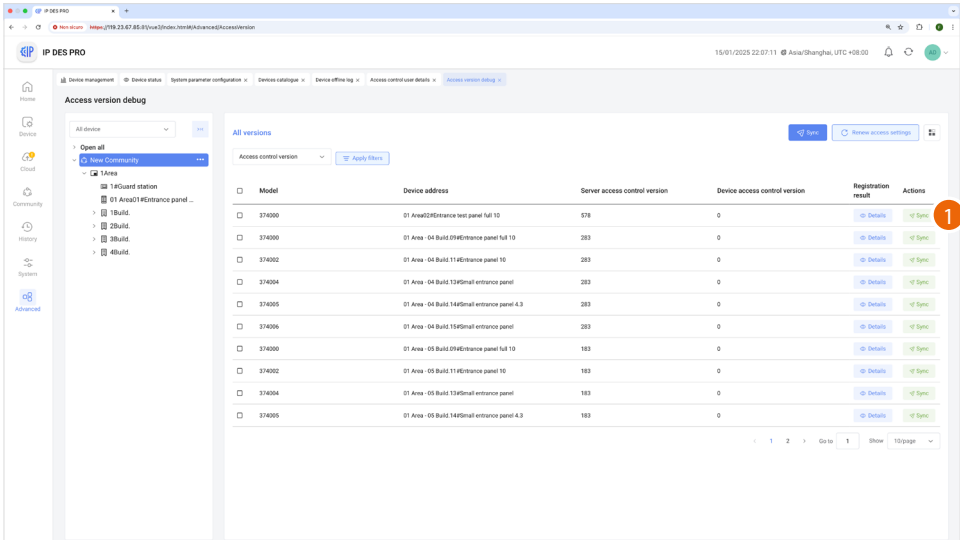


2. Click to confirm

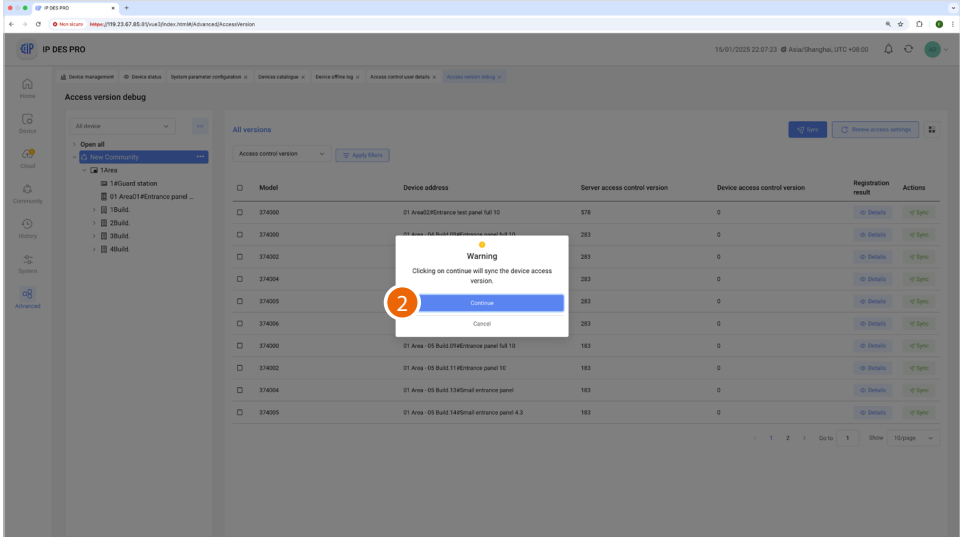


A A message indicates that the operation has been carried out

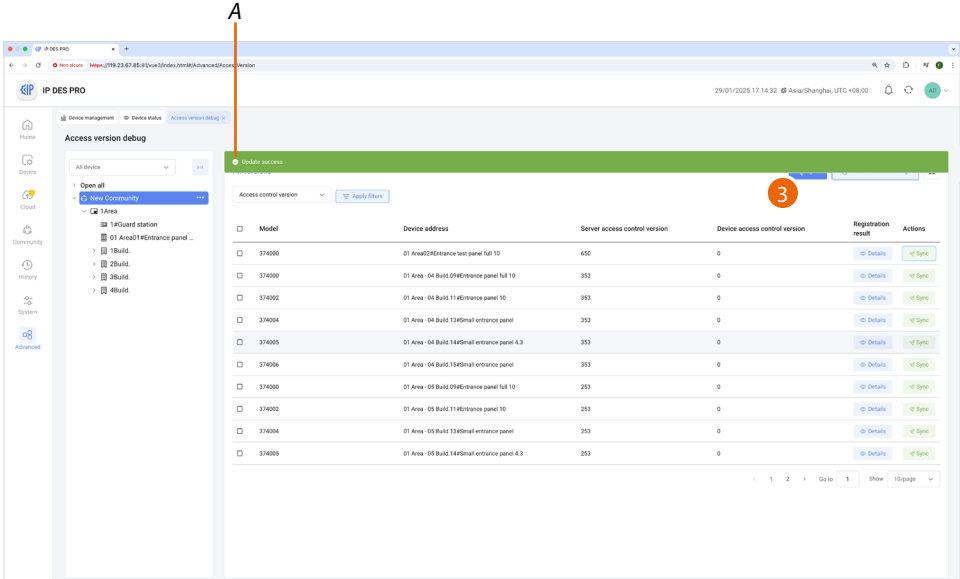
Database alignment



1. Click to align the database to the selected EP



2. Click to confirm

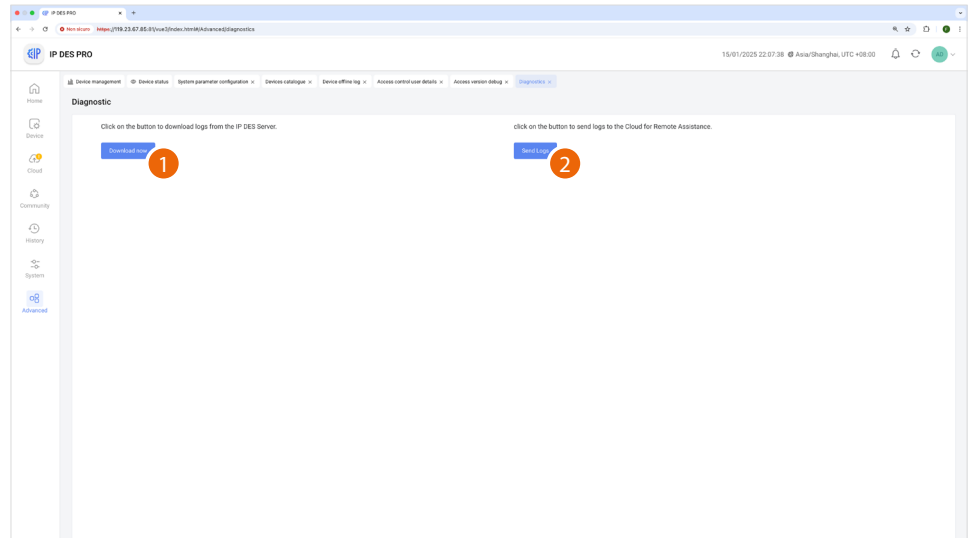


A A message indicates that the operation has been carried out

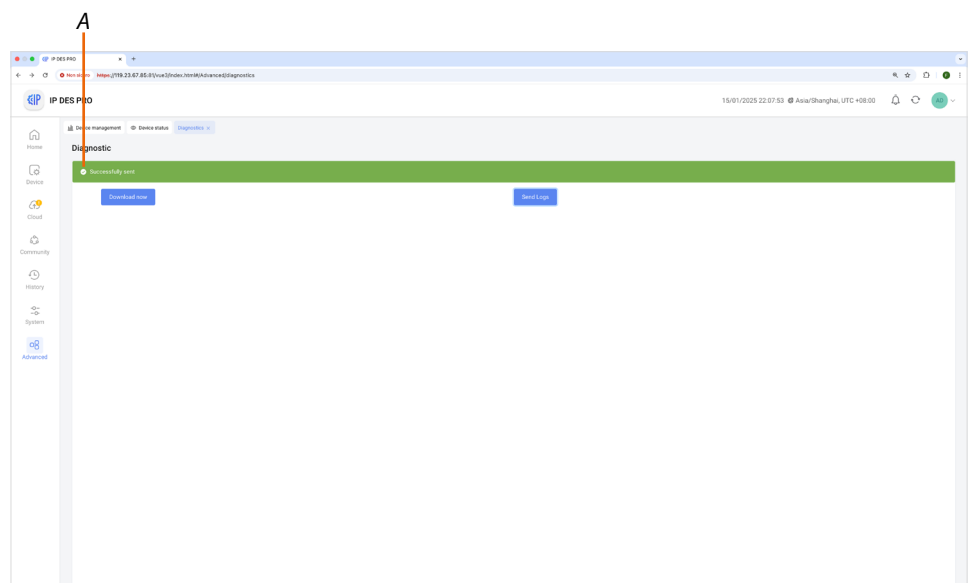
3. Click to align all EP

Diagnostics

This page can be used to download a DES IP Server log file to be sent to technical support for advanced technical support.



1. Click to download the file
2. Click to send .log files to technical support



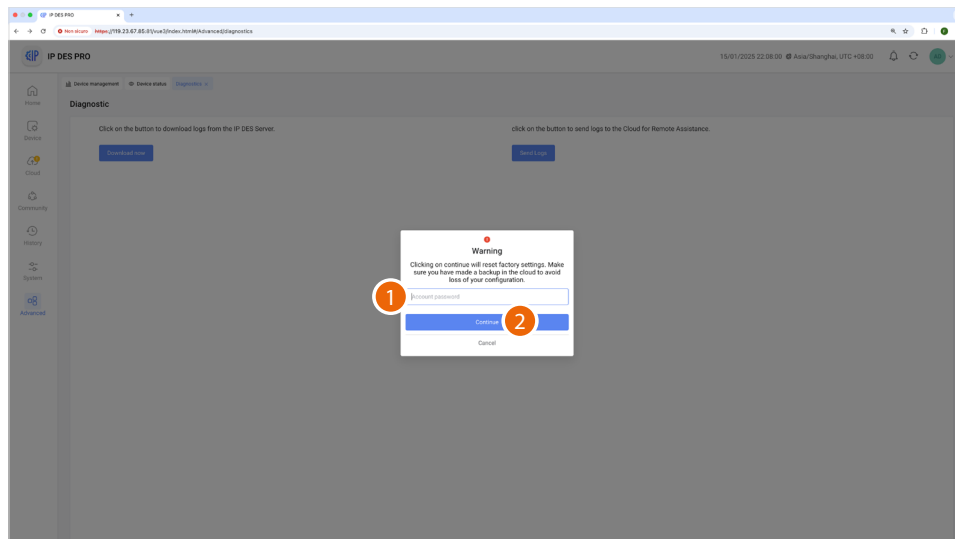
A A message indicates that the operation has been carried out

Factory reset

In this page it is possible to restore the factory settings of the IP DES Server.

NOTE: Make sure to complete a cloud backup to avoid losing your configuration..

CAUTION: When the IP DES Server is reset to the factory settings, all the devices will lose their configuration. For more information [see](#).



1. Enter the software authentication password
2. Click to restore the factory settings

Examples of system situations

This section will illustrate three IP DES system installation situation examples.

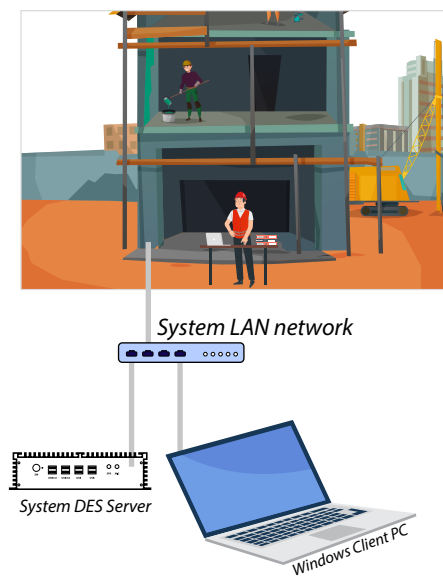
For each situation, the steps required to set up a functioning IP DES system will be described in sequential order.

EXAMPLE 1: Configuration of the server and IP DES system at the construction site

In this case, the system already has a wired LAN network connected to the Internet. Therefore, the installer can perform the configuration on site using a Windows Client PC connected to the same LAN network as the system SD.

[View all the steps required for the example](#)

SYSTEM



EXAMPLE 2: Pre-configuration of the server at the office and on-site system configuration

In this case, the SD is configured before it is installed in the system, using a Windows Client PC and connecting it to the office LAN.

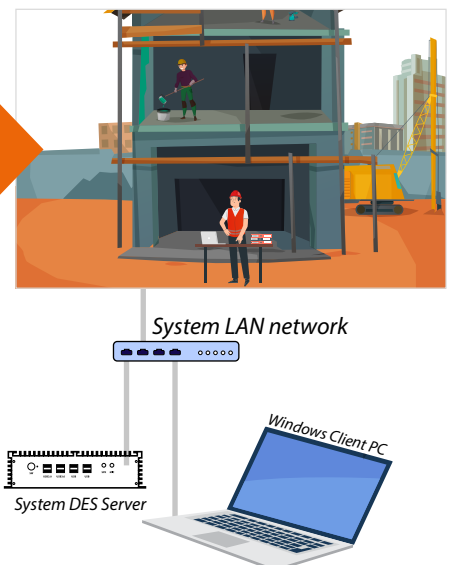
The SD is then taken on site and connected to the system LAN.

[View all the steps required for the example](#)

OFFICE



SYSTEM

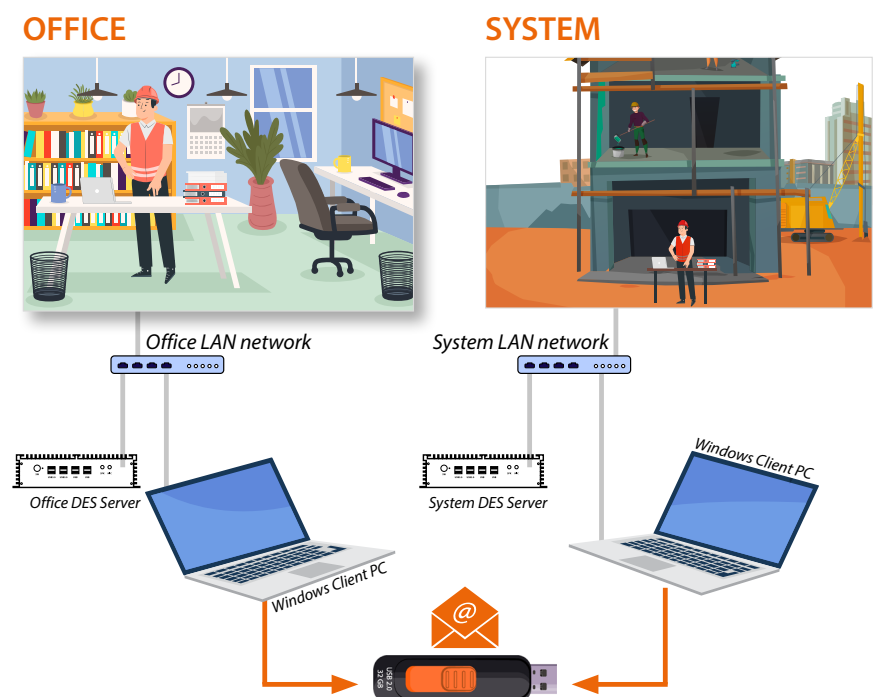
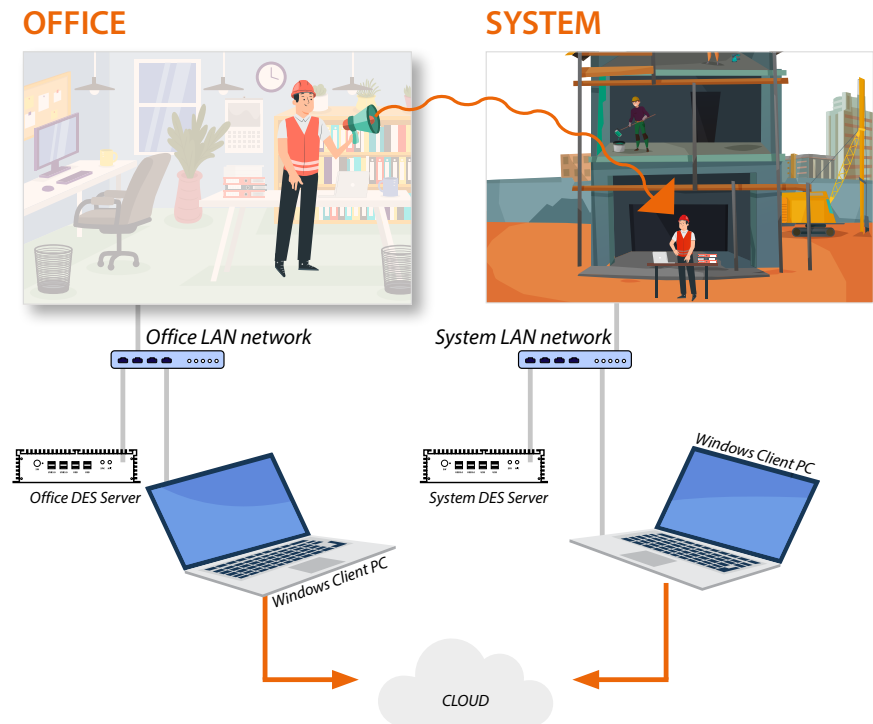


EXAMPLE 3: Creation of the project at the office, on-site server and system configuration

As the system SD is installed in a system far away and is therefore not available, the configuration in this case will have to be carried out on a "test" SD connected to the office LAN.

The configuration completed at the office will then be sent to the system SD by saving it on the cloud and then sending it to the system server using the synchronisation procedure.

[View all the steps required for the example](#)



Configuration of the server and IP DES system at the construction site

- Step 1 [Community VLAN network creation](#)
- Step 2 [Call mode setting and community structure definition](#)
- Step 3 [Community structure creation](#)
- Step 4 [Device MAC address registration](#)
- Step 5 [Community customisation](#)
- Step 6 [Registration of the Community on the Legrand Commercial Cloud](#)
- Step 7 [Send configuration to the DES Server](#)
- Step 8 [Saving of passwords](#)
- Step 9 [Installation of the devices](#)
- Step 10 [Activation of the devices](#)
- Step 11 [System test](#)
- Step 12 [Update of the devices](#)

SYSTEM



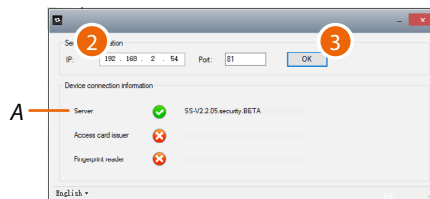
Community VLAN network creation

To configure the community network, it will first be necessary to configure the system by following the steps below:



1. Run the BTicinoWare software (on the Windows Client PC) previously installed

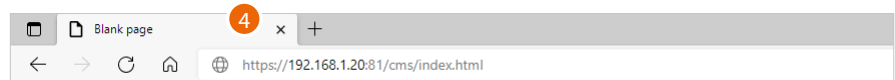
The following screen appears:



2. Enter the **SD address** and check that the port is 81

In order to guarantee correct system operation, the SD (which will take an address assigned by the system router) must maintain its IP address, see [Assigning a "privileged" network address to the SD](#).

3. Press to confirm and check that the flag A is green

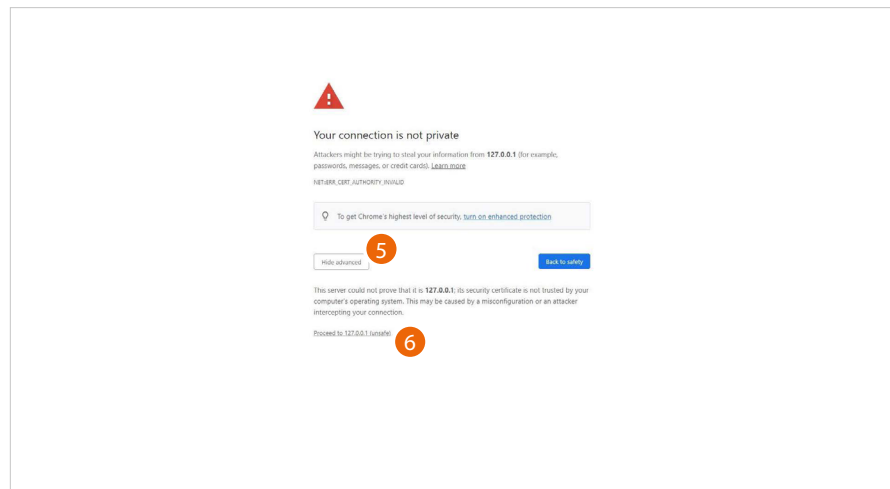


4. Open the browser and enter the http address of the SD:

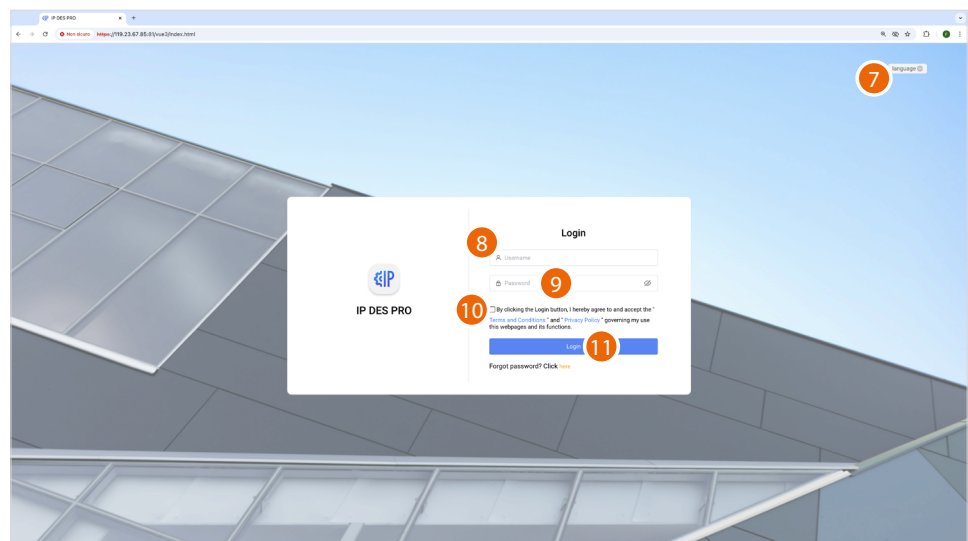
https://IP or siteserver.local:81

NOTE: use Chrome/Edge browser and a screen with resolution 1920x1080

In some cases, the browser may consider the page to be unsafe.

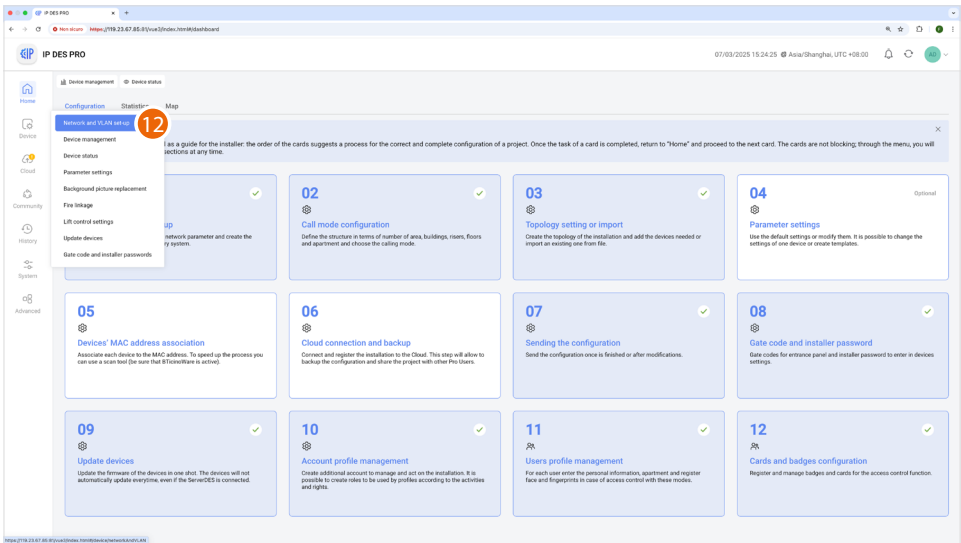


5. Click to display the advanced options
6. Click to ignore the warning and proceed

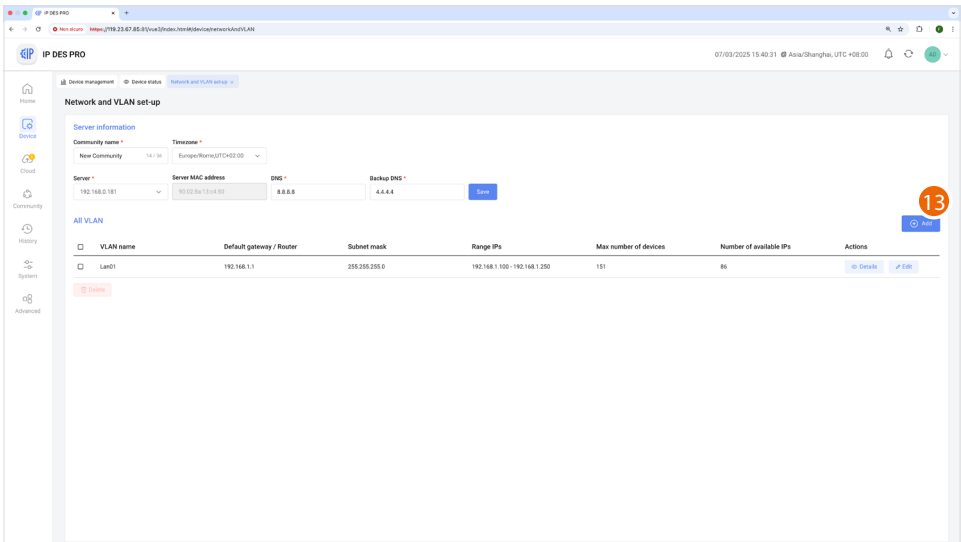


7. Select the interface language.
8. Enter the login name (default admin)
9. Enter the password (default 123456)
10. Accept the "Terms and Conditions" and "Privacy Policy" that govern your use of this website and its functions.
11. Click to confirm

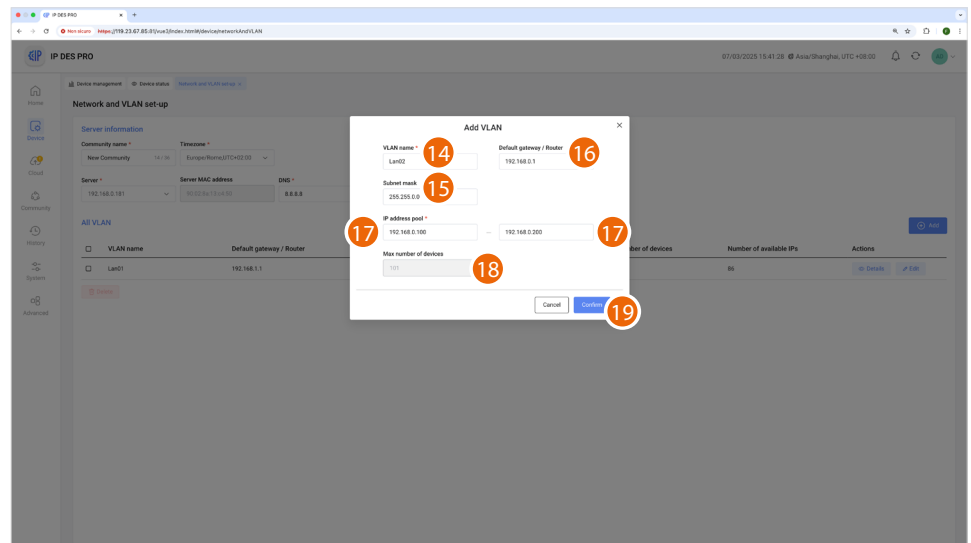
NOTE: For safety reasons, it is mandatory to modify the default password.



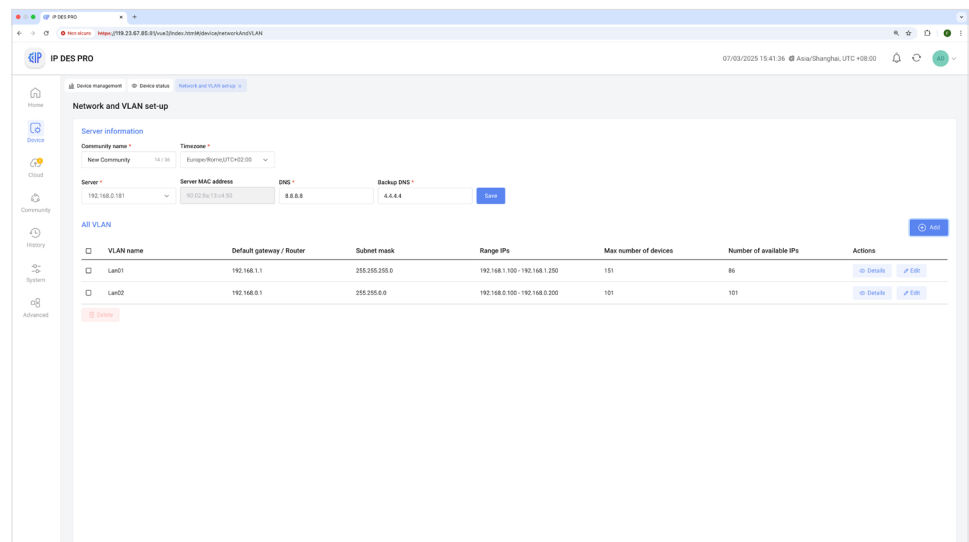
12. Click to open the section where it is possible to create your new community VLAN network



13. Click to create the community VLAN network



14. Enter the name of the community VLAN network (letters and numbers without space)
15. Enter the Subnet mask address
16. Enter the fixed IP address of the SD given to you by the network administrator
17. Enter the starting and ending IP addresses that will determine the maximum number of devices that can be installed on the network.
18. It displays the maximum number of IP devices that can be installed based on the previously entered data
19. Click to confirm

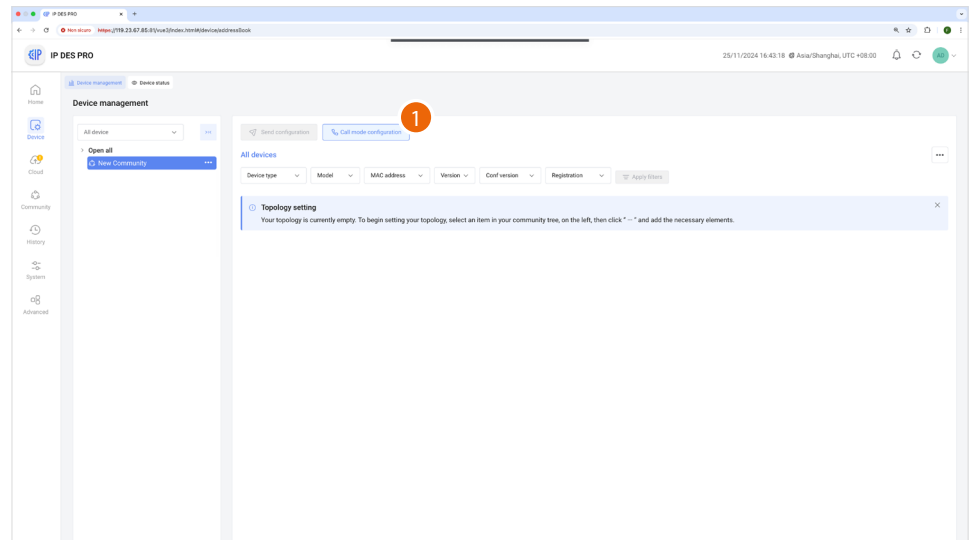


The community VLAN network has been created

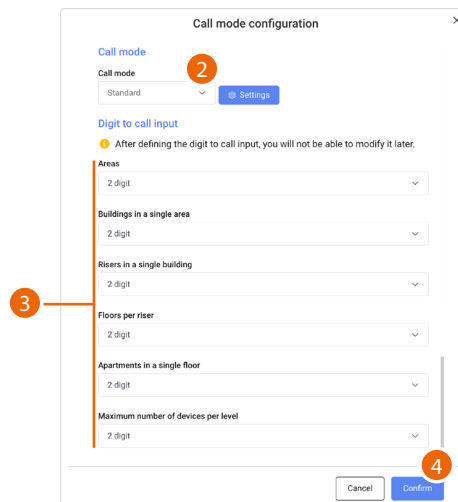
Call mode setting and community structure definition

It is now necessary to define parameters like number of Areas, Buildings, Risers and so on, as well as other parameters that will define the structure of the Community.

In this section, it is also necessary to define the type of call that will be used for all Community calls.



1. Click to open the page



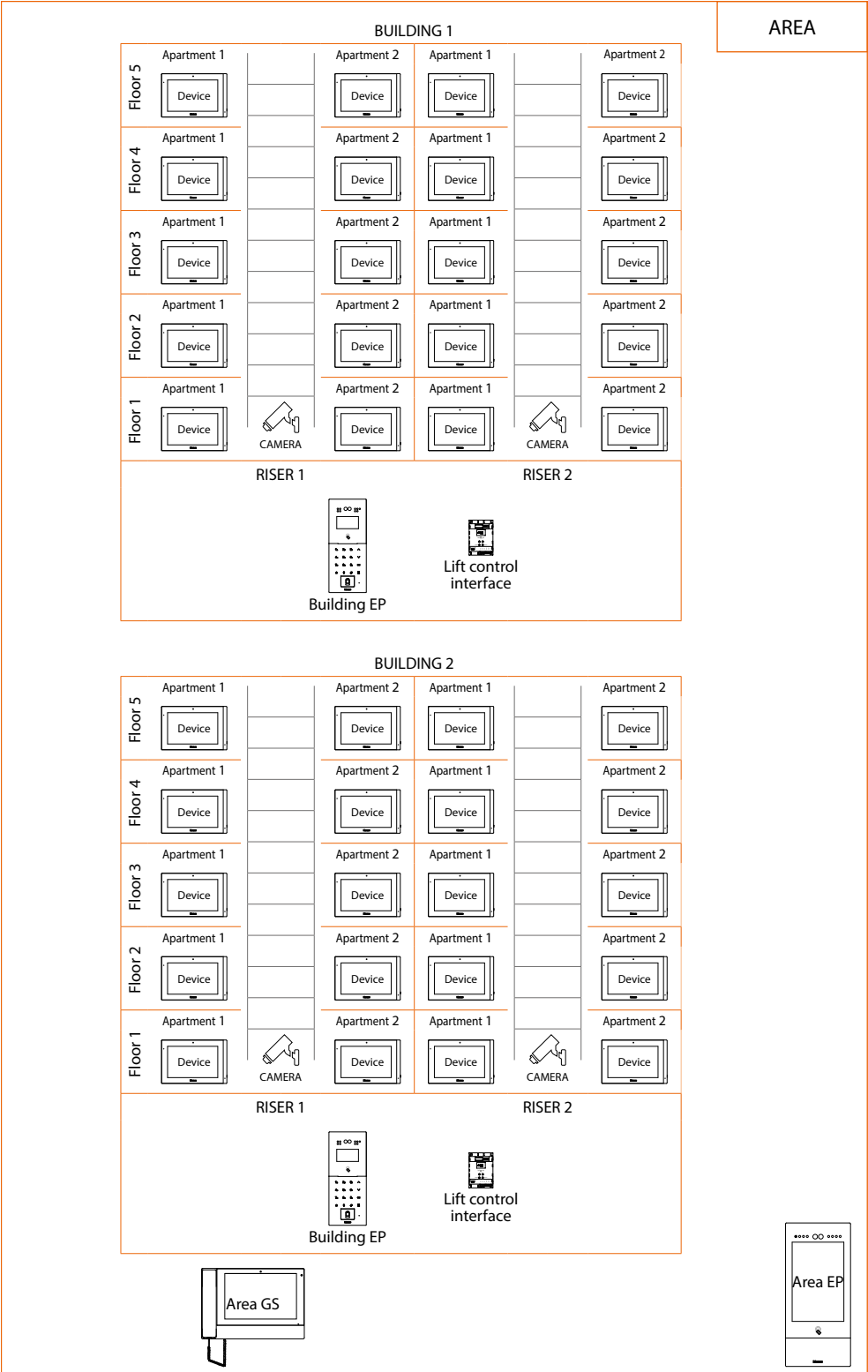
2. Select the **call mode** and configure the relevant parameters
3. Set the number of digits to be used for each call sector (Area/Building/Riser/Floor/Apartment)
ATTENTION: After setting these parameters for the first time, it will no longer be possible to change them.
In order to change these parameters, restore the factory settings
4. Touch to confirm

Community structure creation

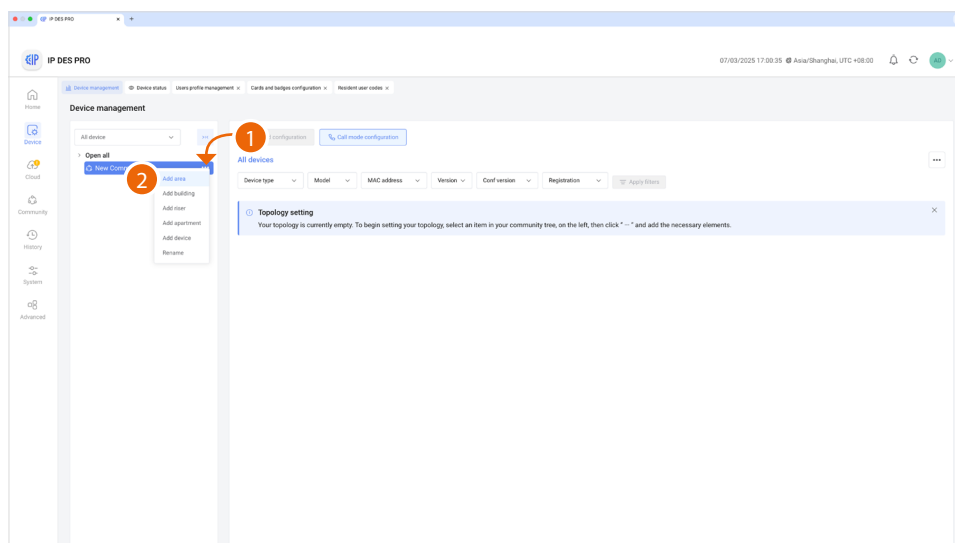
Depending on how your Community is composed, you will need to hierarchically enter:



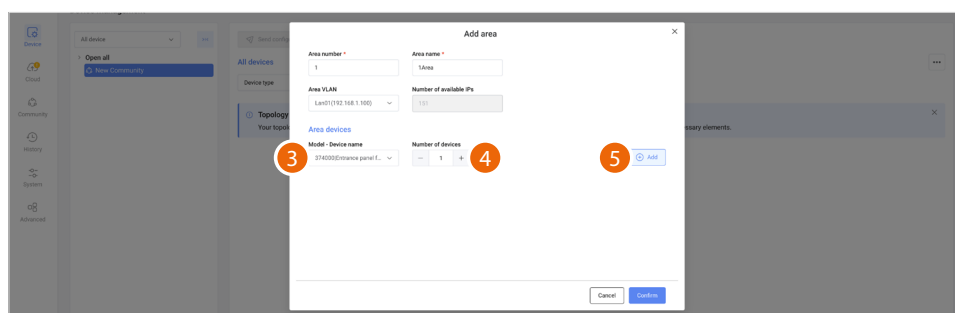
This document will show the creation of a sample structure composed as follows:



Caution: The configuration operations illustrated below are those required to create the example structure.

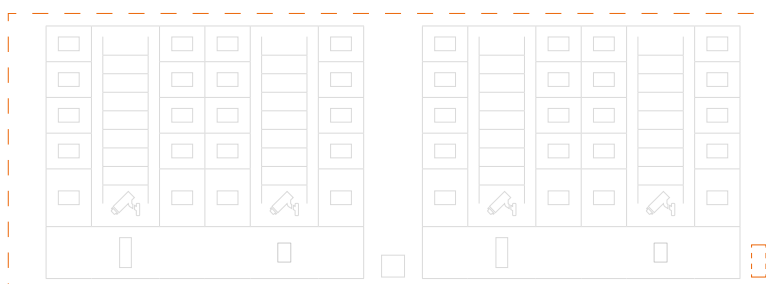


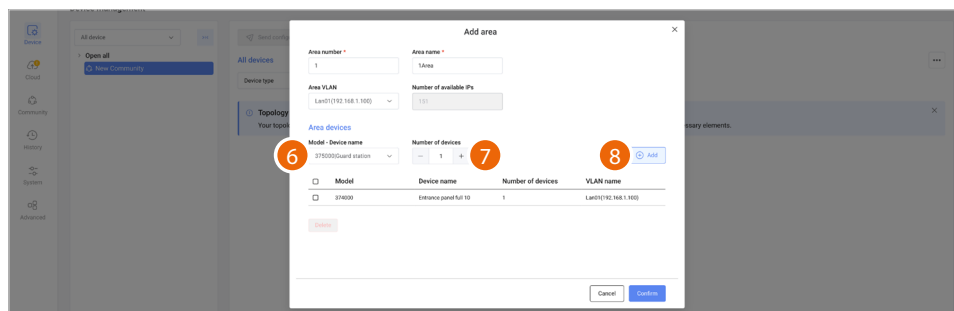
1. Click the Community to open the context menu, a drop-down menu will appear with the commands for its configuration
2. Click to add a new Area



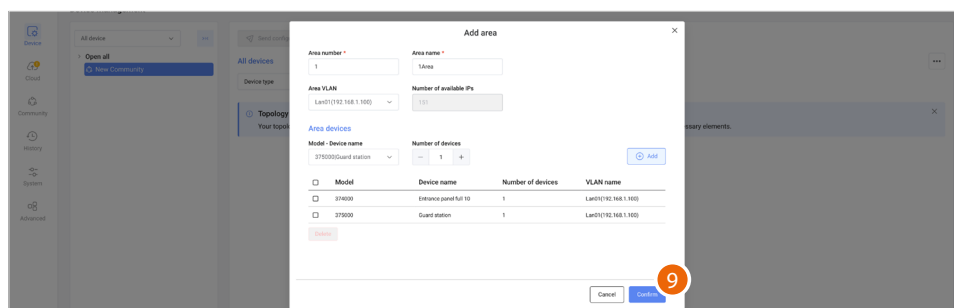
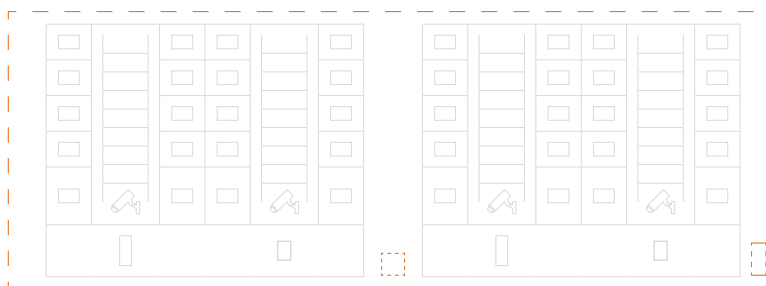
3. Select the area device (Area EP)*
4. Select the quantity
5. Click to add

***NOTE:** Before proceeding with the addition of the devices, remember to check that all the device parameters comply with the requirements, see [Configuration Parameters](#)

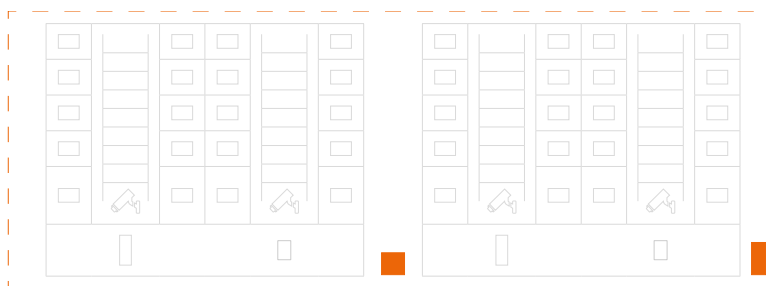


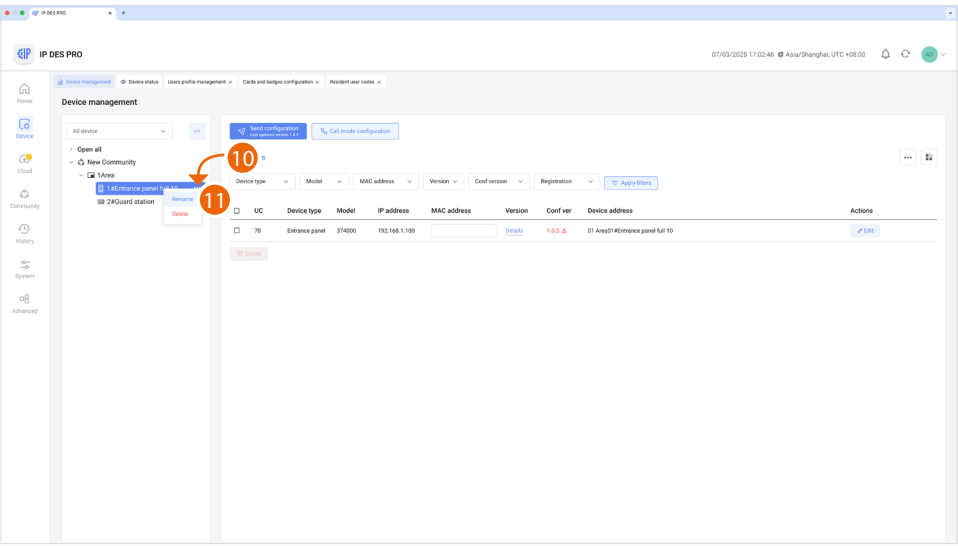


6. Select the second area device (Area GS)
7. Select the quantity
8. Click to add

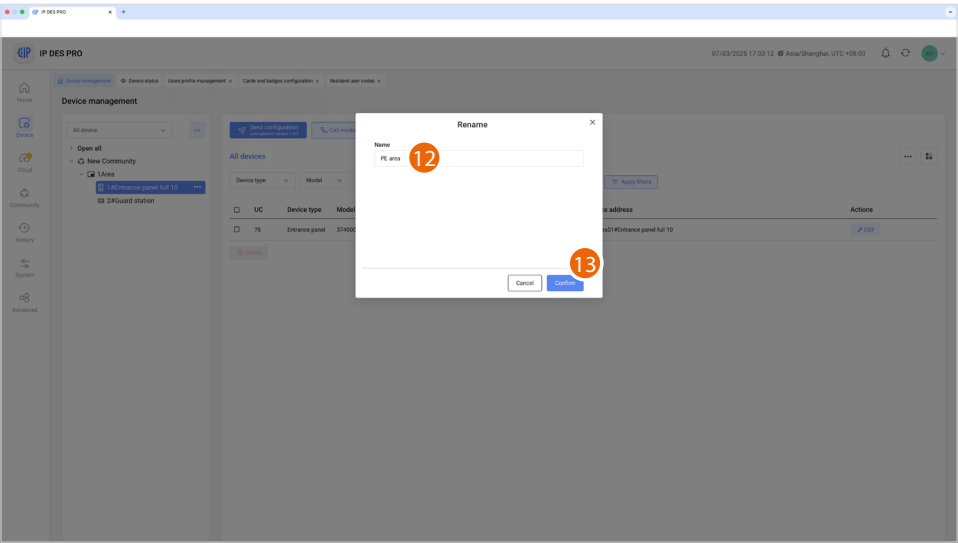


9. Click to confirm

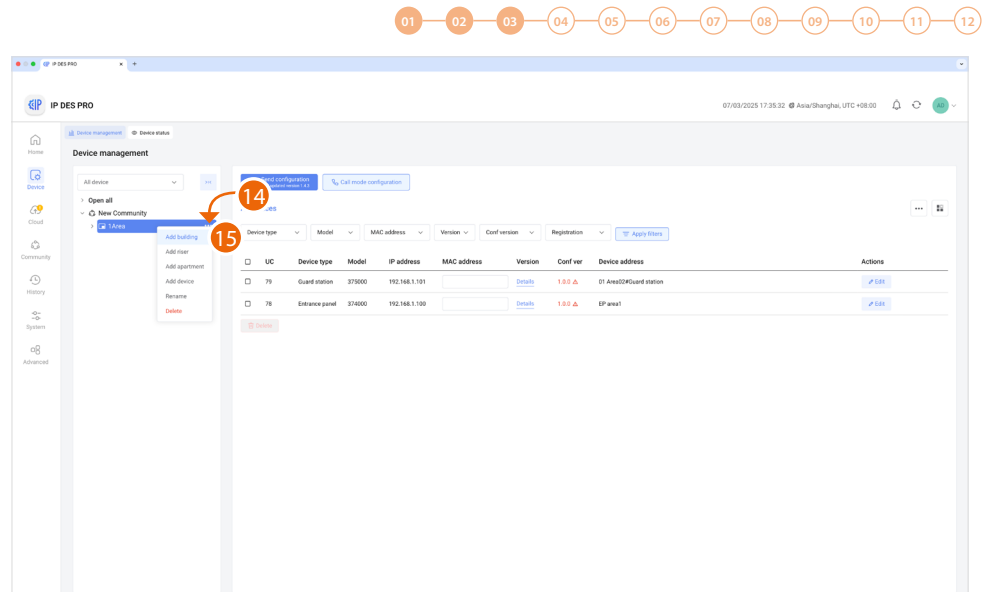




- After inserting the devices, you will be able to customize their name
10. With the right mouse button click the device that you want to rename: a drop-down menu will appear
11. Click to open the edit window

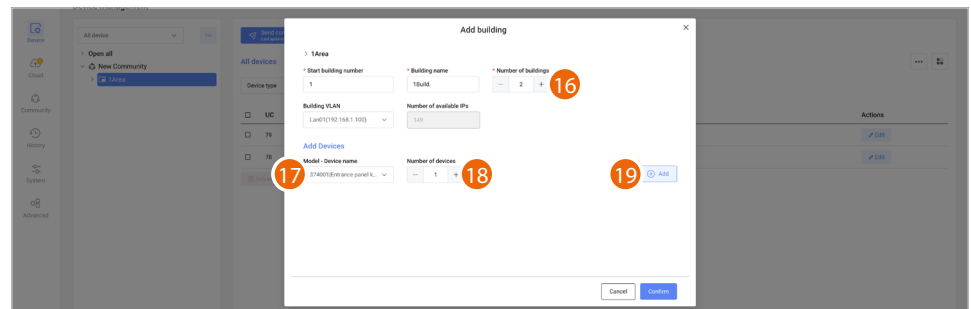
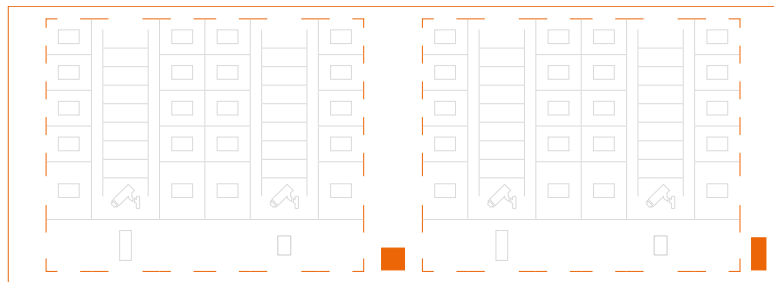


12. Enter the new name
13. Click to confirm



14. Click the Area with the right mouse button. This will open a drop-down menu

15. Click to add the Buildings



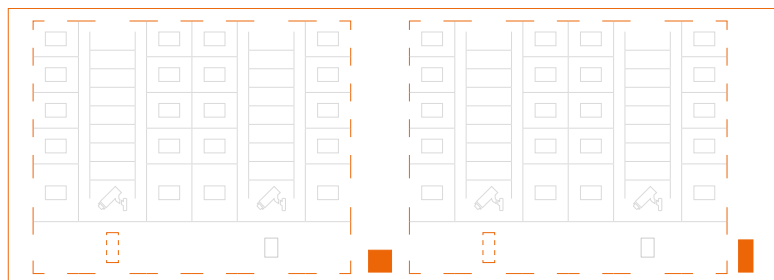
16. Select the number of Buildings to add

17. Select the Building device (Building EP)

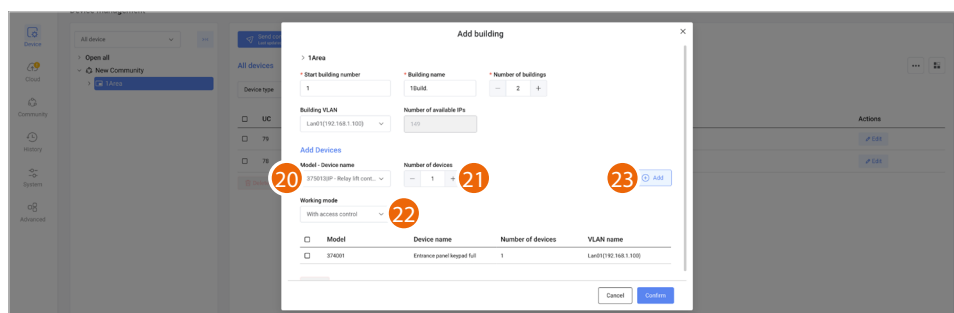
NOTE: the software automatically applies a filter to only show devices that are consistent with the component that you are adding

18. Select the quantity

19. Click to add



01 02 03 04 05 06 07 08 09 10 11 12



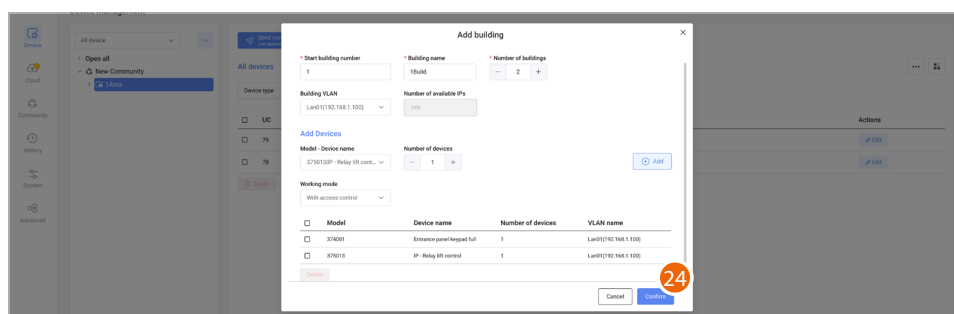
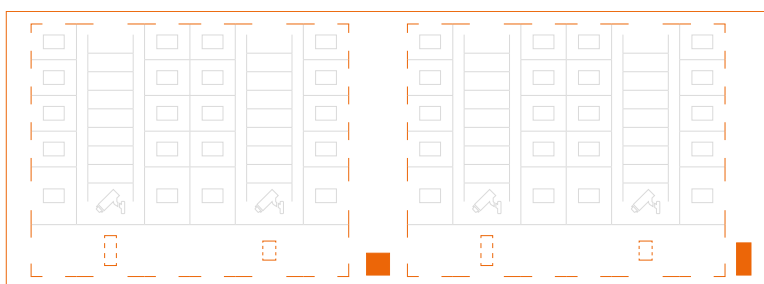
20. Select the device to add (lift control interface with relay 375013)

21. Select the quantity

22. Select the operating mode:

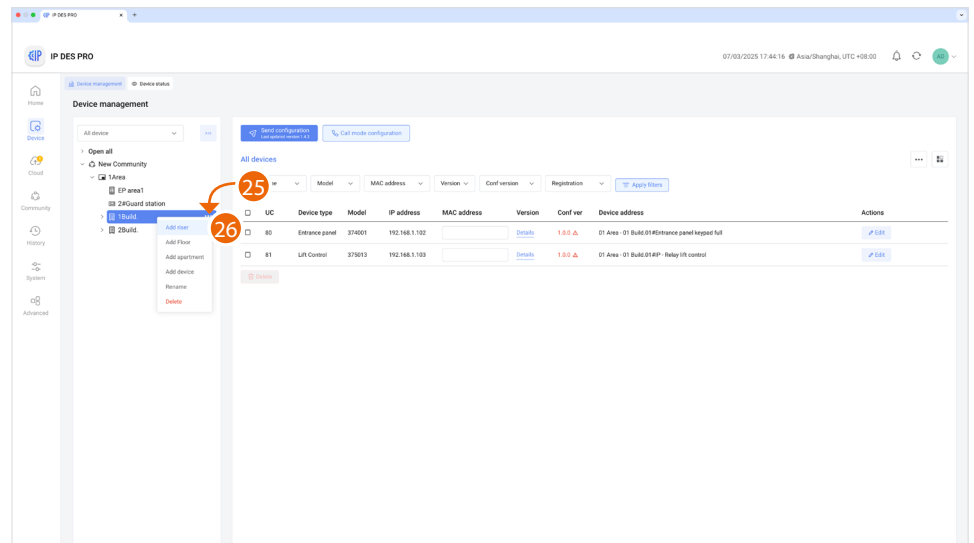
- **with access control:** this mode allows to set up an exclusive call to a specific floor (e.g. only go to the third floor)
- **ground floor call:** this mode allows to set the system so that the lift is sent to the floor of the caller.

23. Click to add



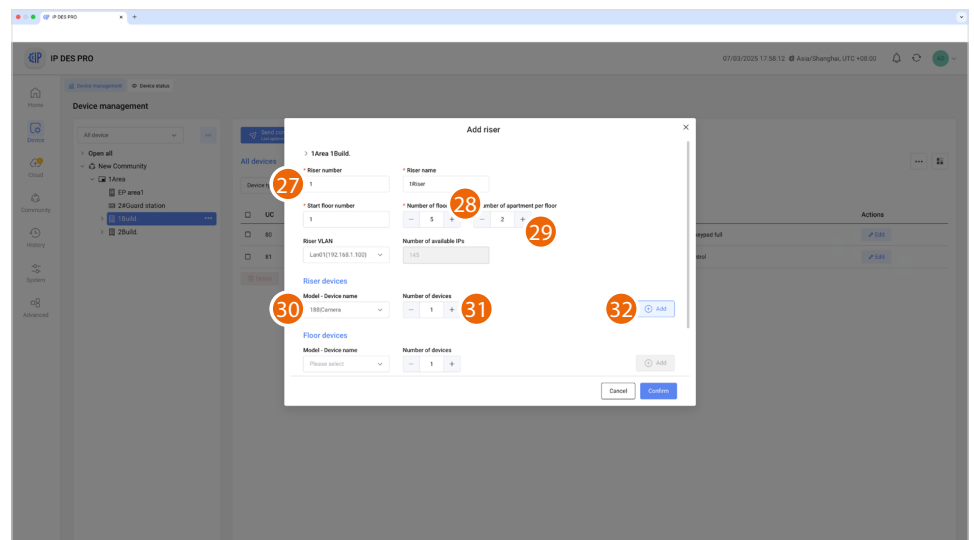
24. Click to confirm





25. Click the Building with the right mouse button. This will open a drop-down menu

26. Click to add a new Riser



27. Enter the progressive Riser number

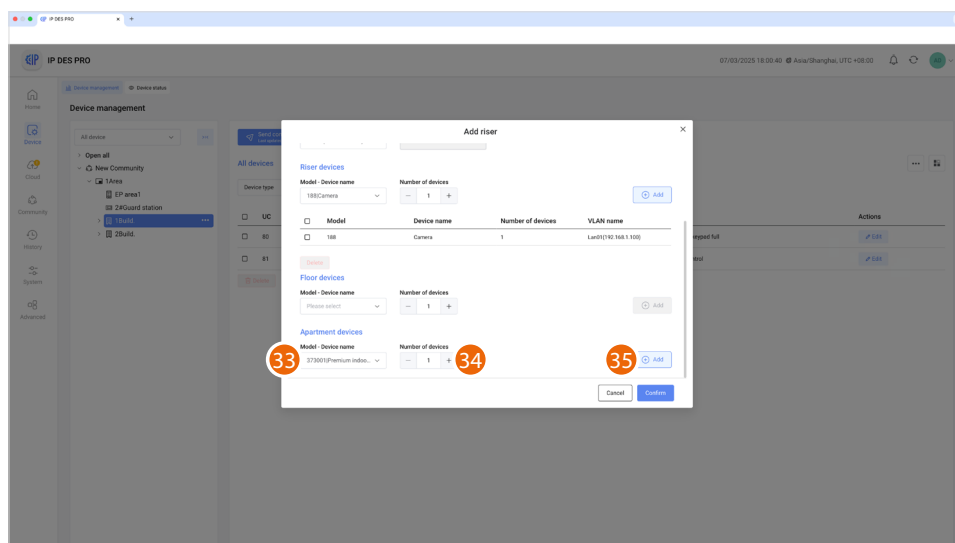
28. Select the Building Floor number (5)

29. Select the number of Apartments for each Floor (2)

30. Select the OnVif IP Camera

31. Select the quantity

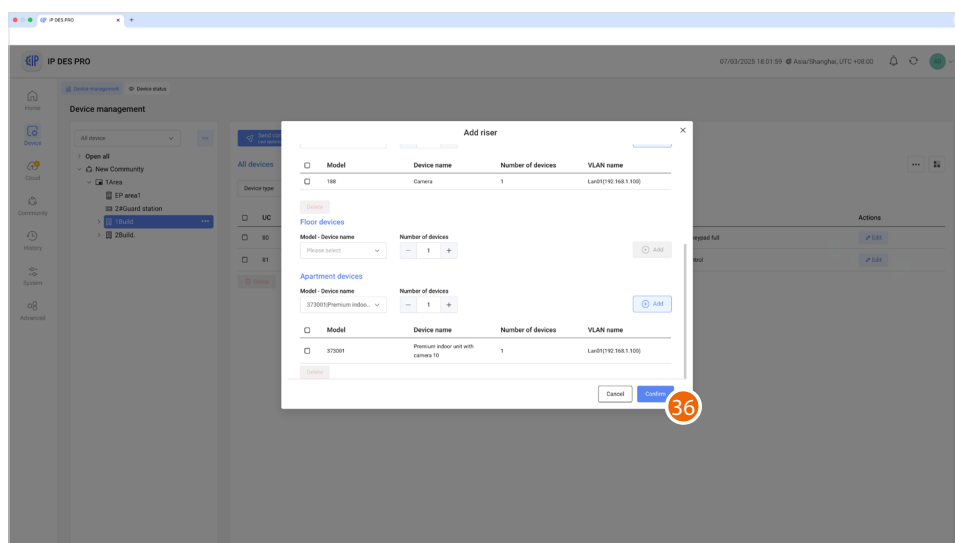
32. Click to add



33. Select the apartment device

34. Select the quantity

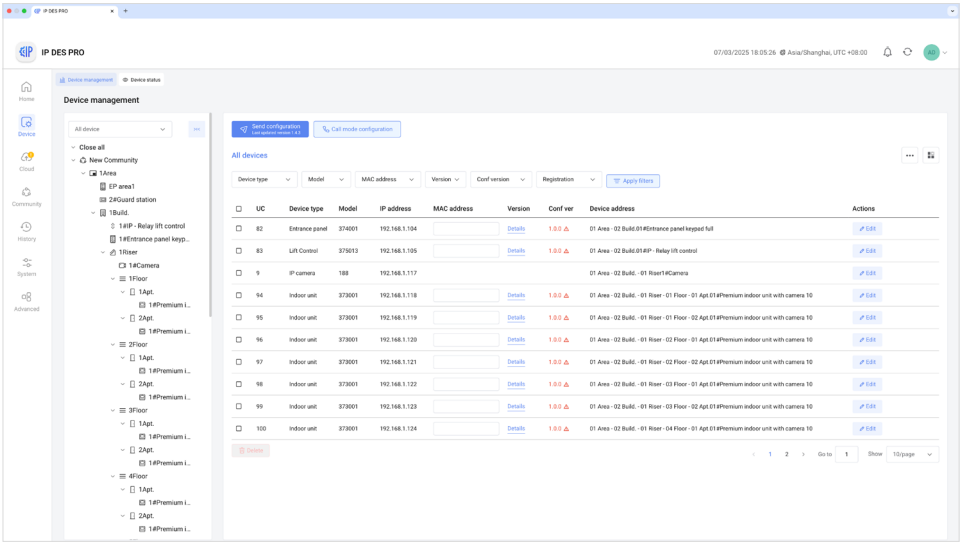
35. Click to add



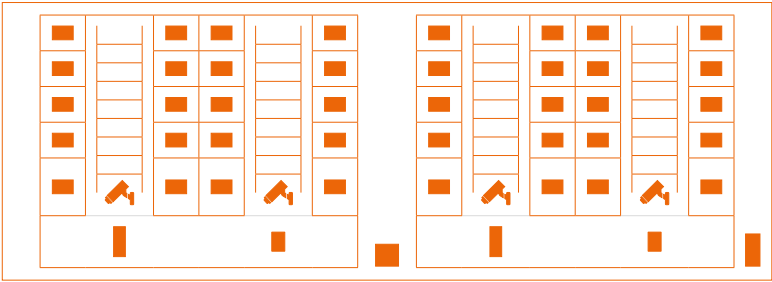
36. Click to confirm



Repeat the same steps for Riser 2

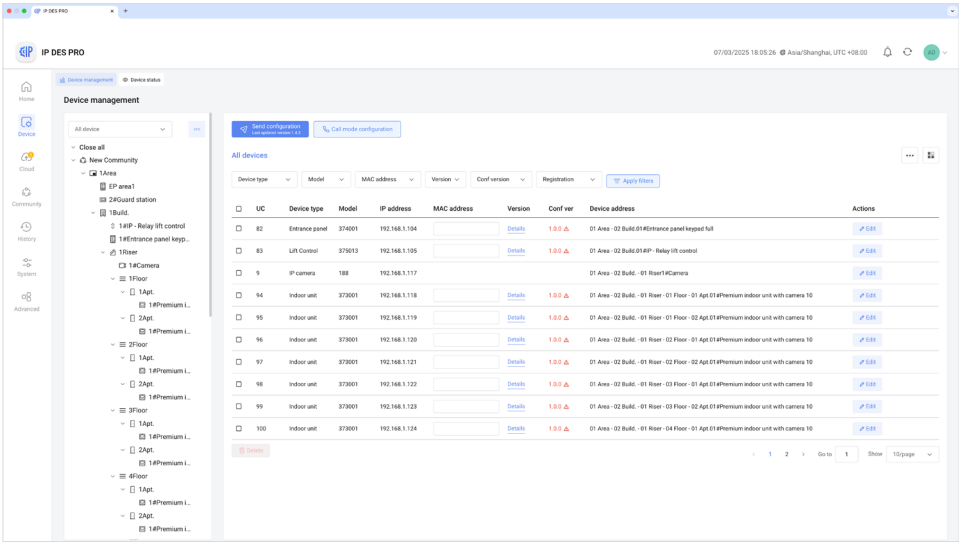


Repeat from step 21 also for Building 2

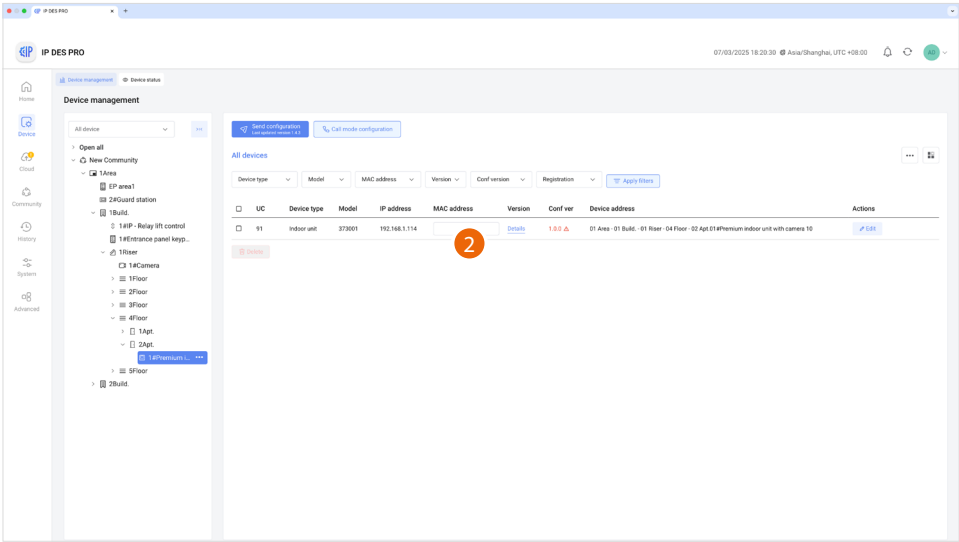


Device MAC address registration

Now that the structure is complete, you will need to associate the MAC addresses of the physical devices with the virtual ones included earlier in the structure.

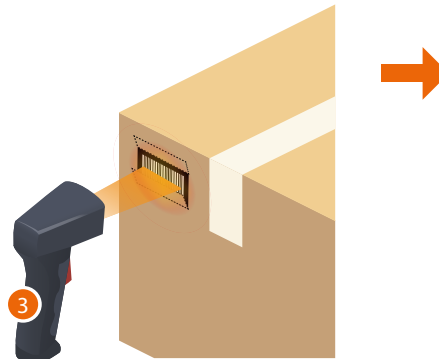


This section includes all the devices to associate. The MAC address can be entered directly from this screen



Alternatively, it is possible to select a branch and only view the devices belonging to that branch. It is also possible to select a device from the menu tree and enter the MAC address individually. The advantage of this second method, is that it is easy to identify devices based on their geographical location.

2. Move the cursor inside the field



Version ▾	Conf version ▾
MAC address	Version
90:02:8A:08:A0:09	Details



3. With a bar code scanner, read the label on the back of the device. To get to the label, open the pre-punched hole on the enclosure.
The code may also be entered manually.
The video door entry system devices must be available in the same configuration room.

NOTE: the BTicinoWare software must be running.

The MAC address will appear in the field and the printer will automatically print a label that you will need to apply to the package
The printed label contains the following data:

- A Where to place the device based on the previously created structure
- B Device model
- C MAC address
- D Date and time the label was printed

A INFORMAZIONI DISPOSITIVO:
1area1building01riser01floor01house#10 inch grey PI

B MODELLO DI DISPOSITIVO: 373001

C MAC ADDRESS: 90:02:8A:08:A0:09

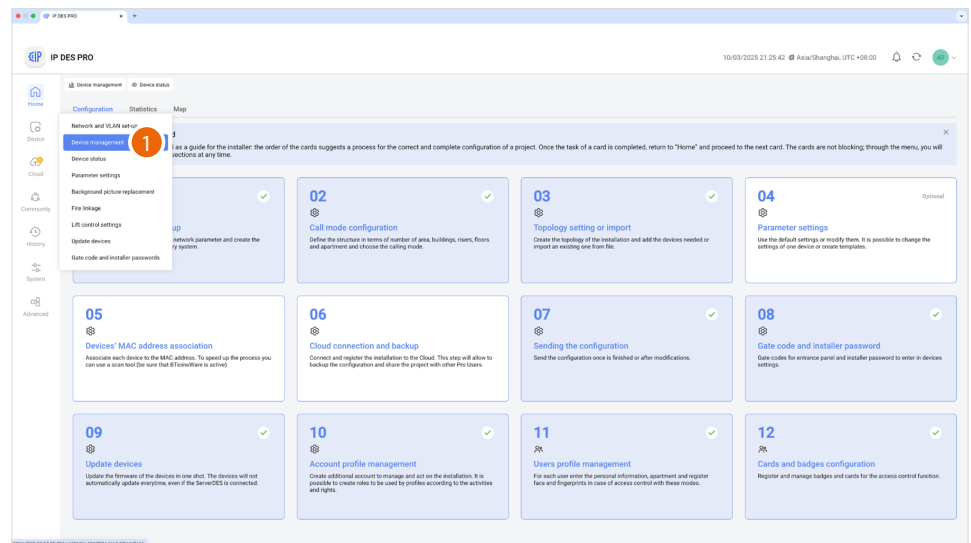
D PRINT DATE/TIME: 2020-12-09 15:41:05

If the printer is connected to the network and ready, the label will be printed automatically
Repeat for all devices

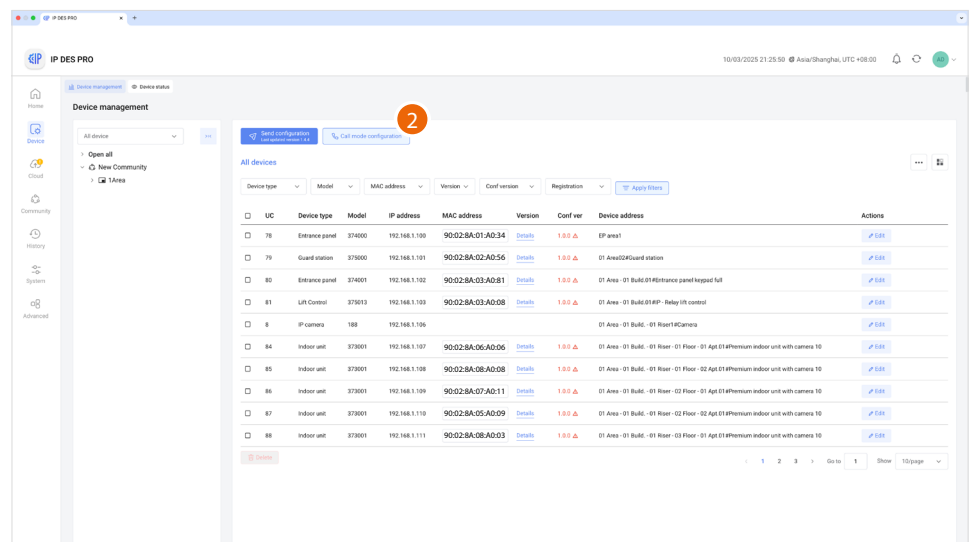
Community customisation

Before sending the configuration to the SD, we can customise the Community by e.g. **modifying the call mode** and/or by **enabling access to the Community for certain individuals**. To use a different call mode, (e.g. call mode via phonebook) to call residents, it will be necessary to:

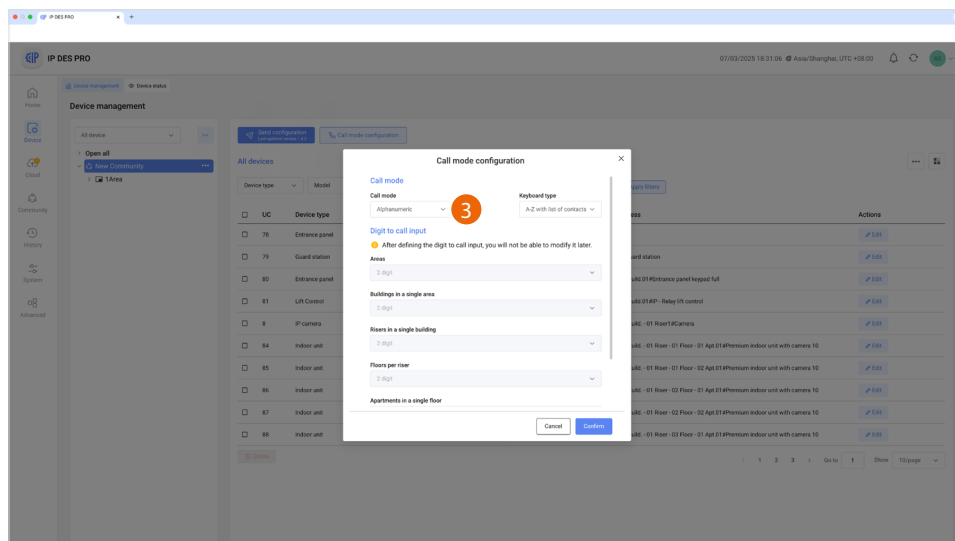
- Change call type to alphanumeric/address book
- replace **the address in the community with an alias** to facilitate recognition of the called party. This function renames the apartment to a different name (alias). The call to this apartment will be made using this new name. E.g. JOHN SMITH



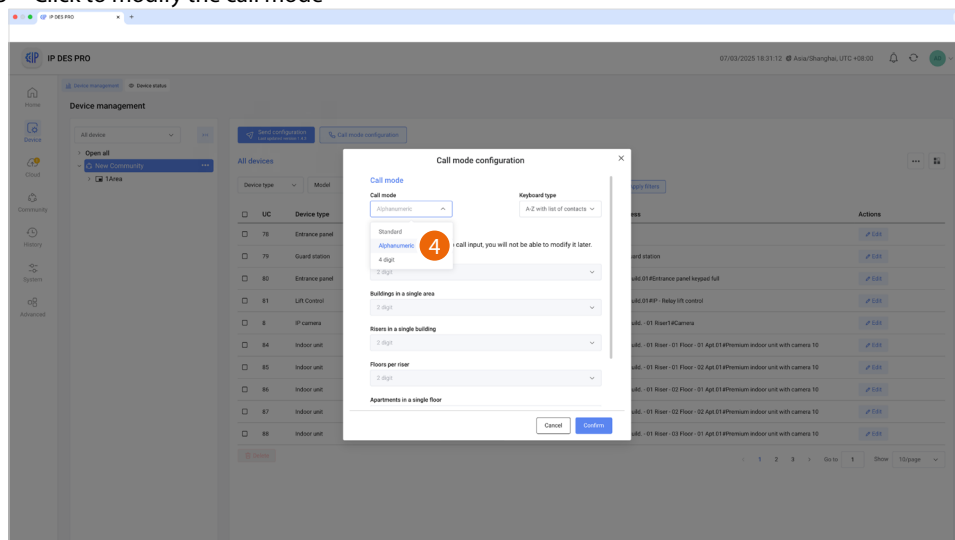
1. Select Device/Device management



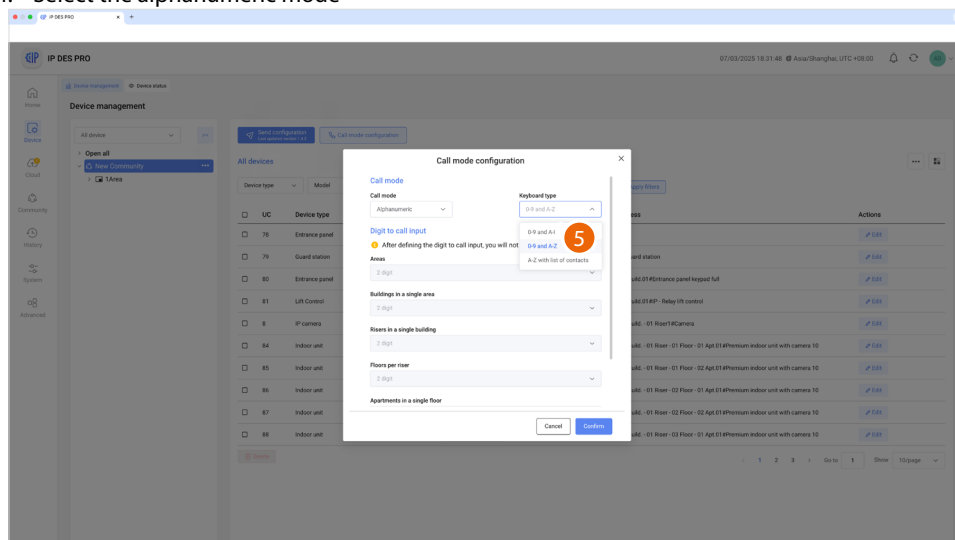
2. Click to select the command



3 Click to modify the call mode



4. Select the alphanumeric mode

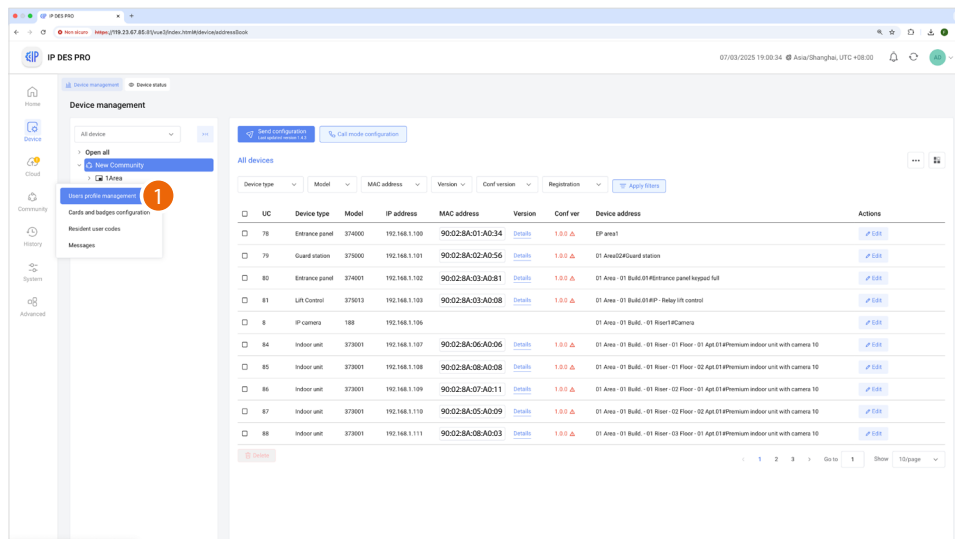


5. Select address book as entry type

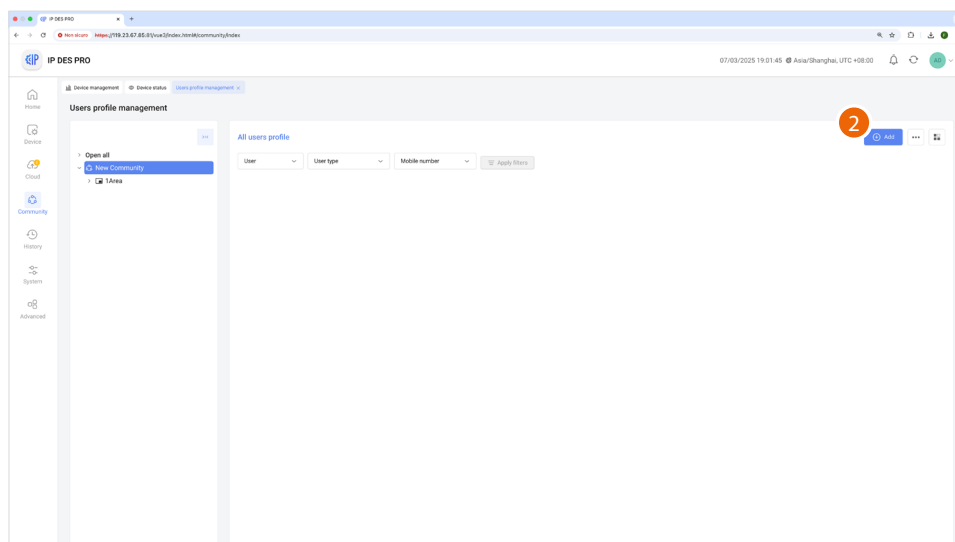
After sending the configuration to the SD, it will be possible to call IU using custom names (aliases). When changing the name of a GS or EP, this will be identified with this name on the receiving device when the call is made.

NOTE: This alias format (Address Book) is not supported by entrance panels 374001/03

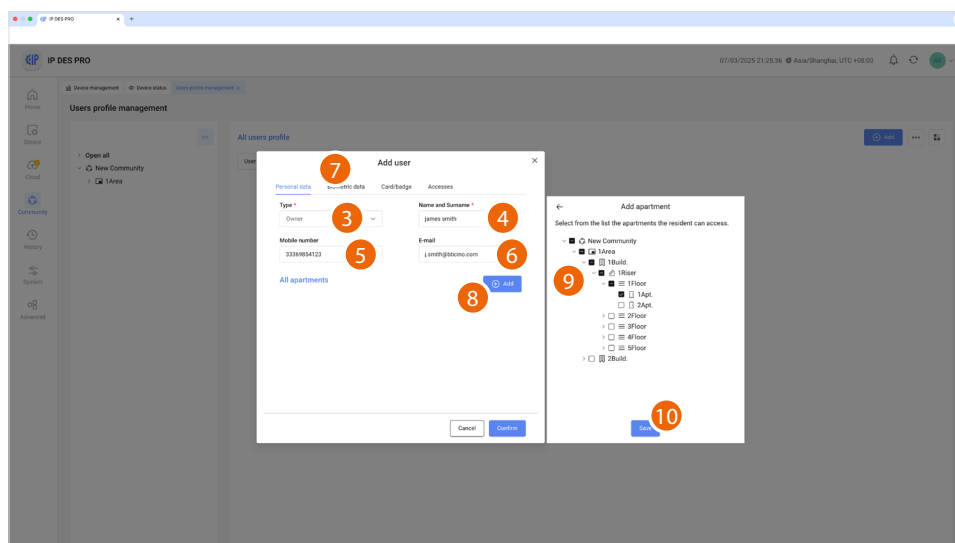
Now it is possible to add community people and give them permissions to access the structure. Depending on the type of person, different access permissions may be assigned, see [Person profile management](#).



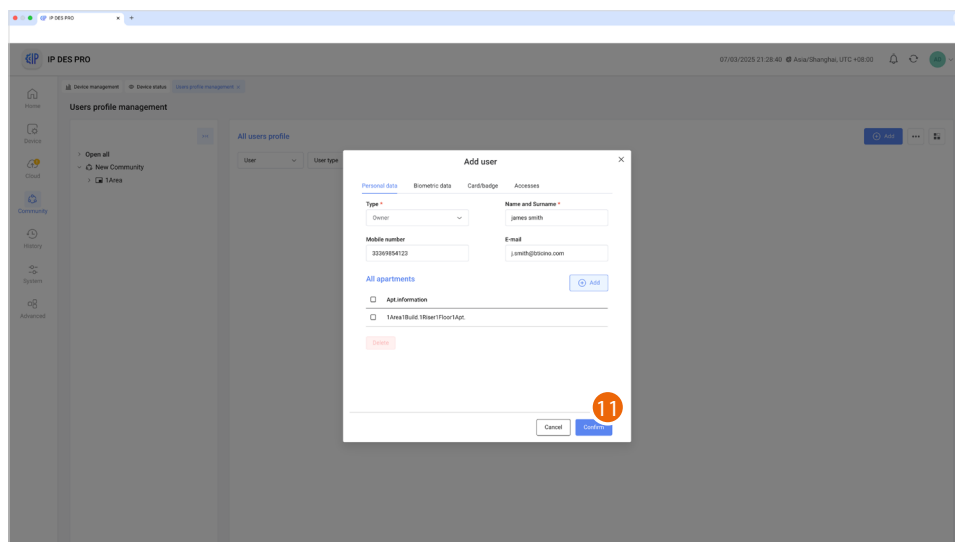
1. Select Community/Users profile management



2. Click to create a new person



3. Select the type of person
4. Enter the name and surname of the person
- NOTE:** some parameters may change depending on the type of person
5. Inserisci il numero di telefono della persona
6. Inserisci la mail della persona
7. [Registra un'impronta digitale](#)
8. Ora devi indicare l'indirizzo dell'appartamento di pertinenza della persona
9. Seleziona area/Condominio/Scala/Piano/Appartamento di pertinenza della persona
10. Clicca per aggiungere



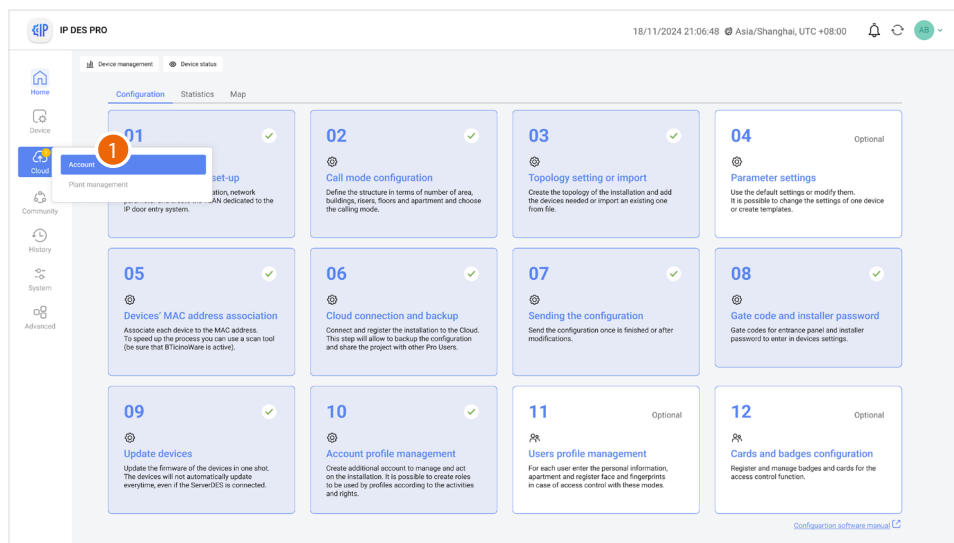
11. Click to finish; the person can now access the community using the code and/or fingerprint reading. To use a badge/card to access the community, this must be registered; see [Access control card management](#)

Registration of the community on the Installer's Cloud

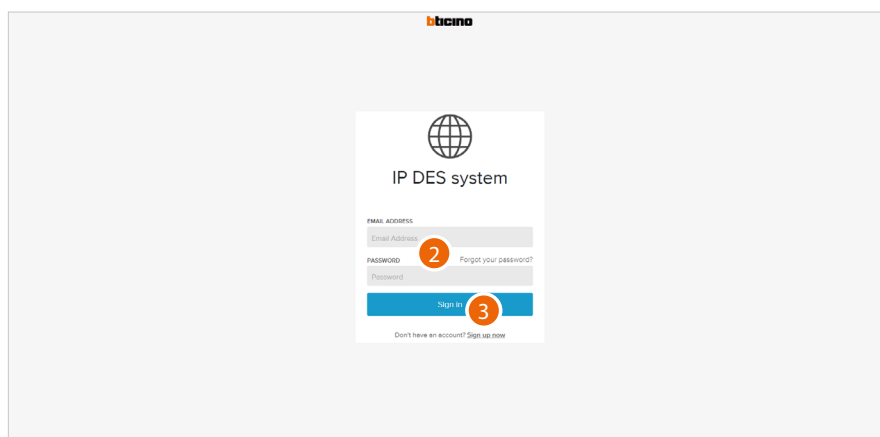
After completing the registration process and creating an Installer account, it is possible to save a copy of the Community on the Installer's Cloud.

Having a copy of the Community on the Installer's Cloud allows you to:

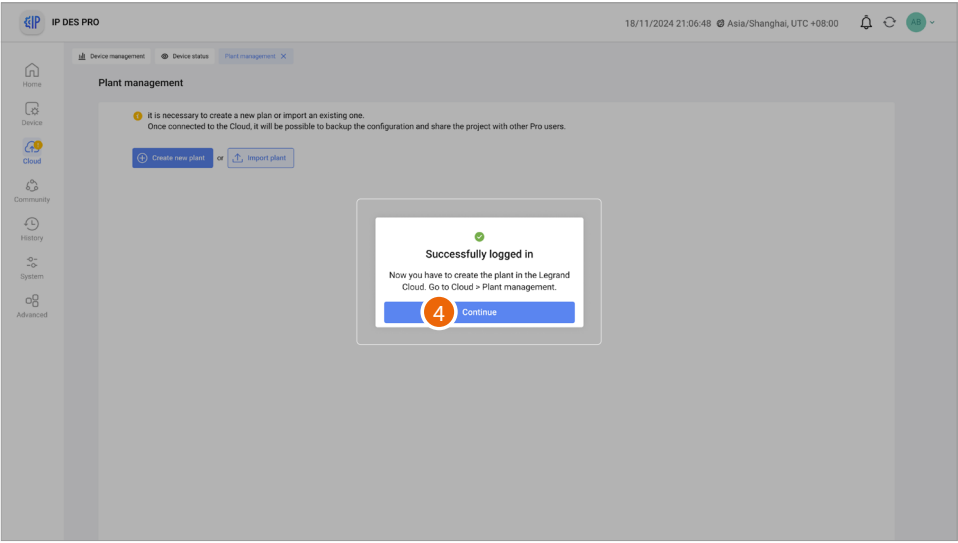
- have greater security in the event of local data loss
- associate the Home+Security app to the IU, for remote management of the video door entry system



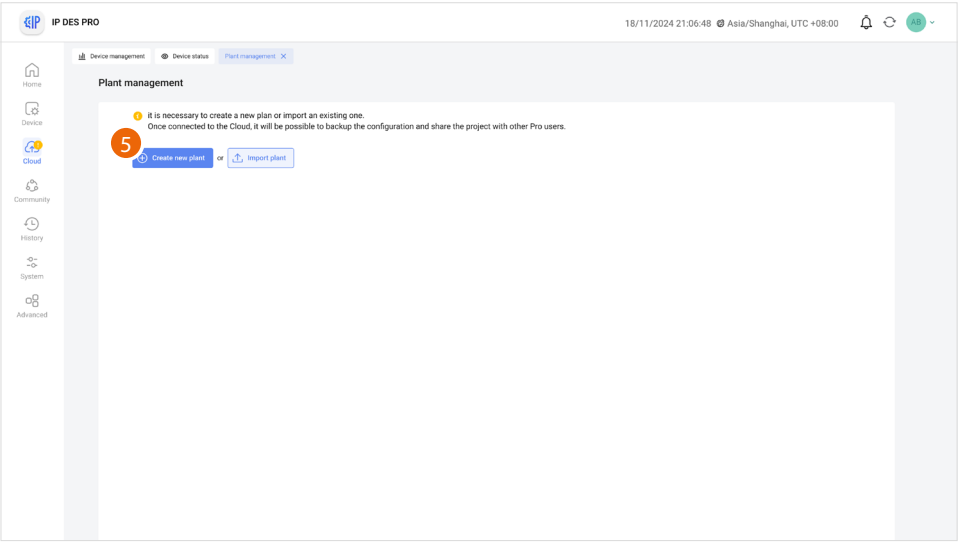
1. Click to complete the Installer's Cloud authentication process



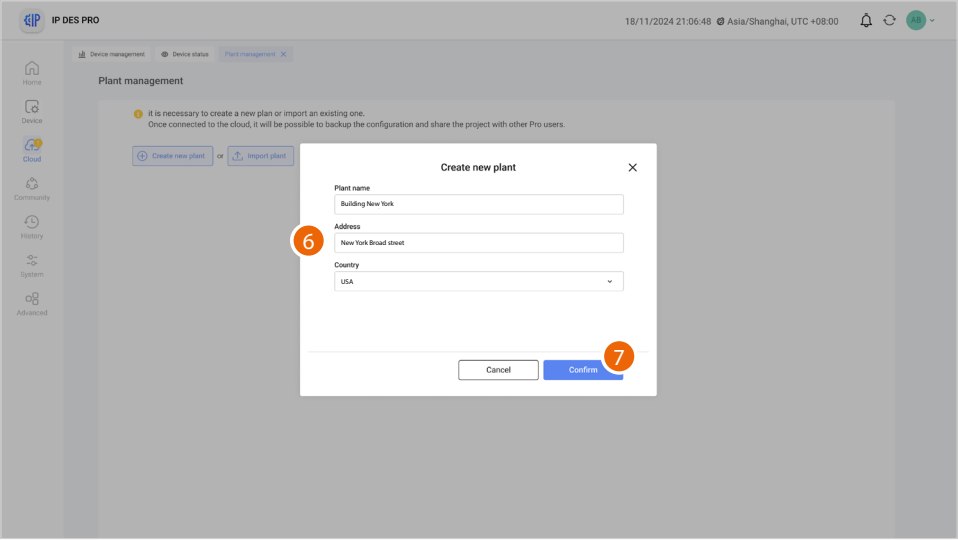
2. Enter email and password
3. Click to access



4. Click to confirm



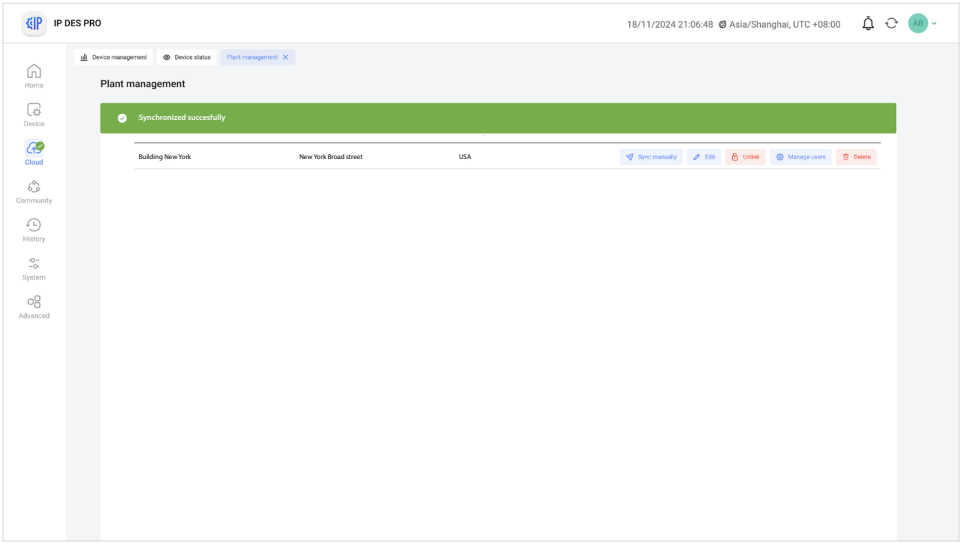
5. Click to create a new Plant



6. Enter the details of the Plant you are creating (name, address and country)

7. Click to save

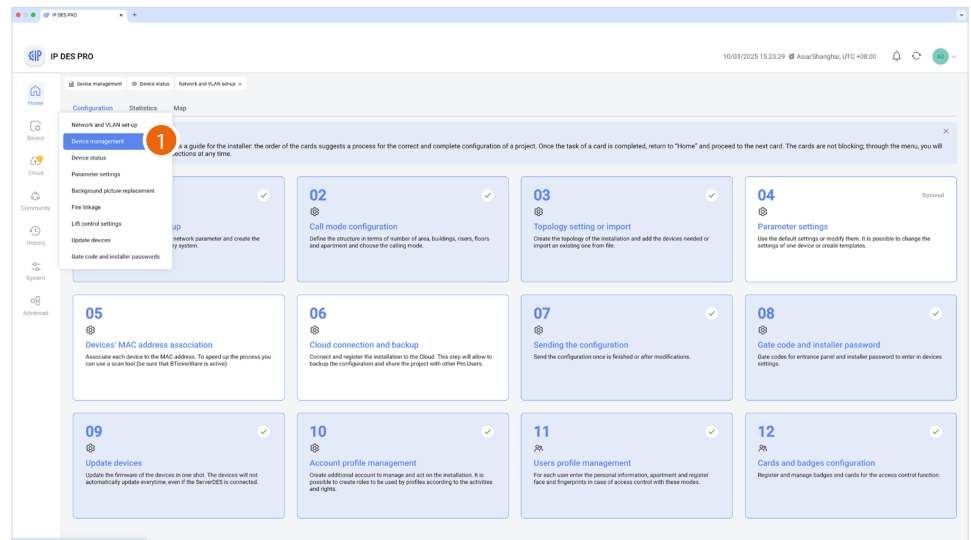
The plant is automatically synchronised



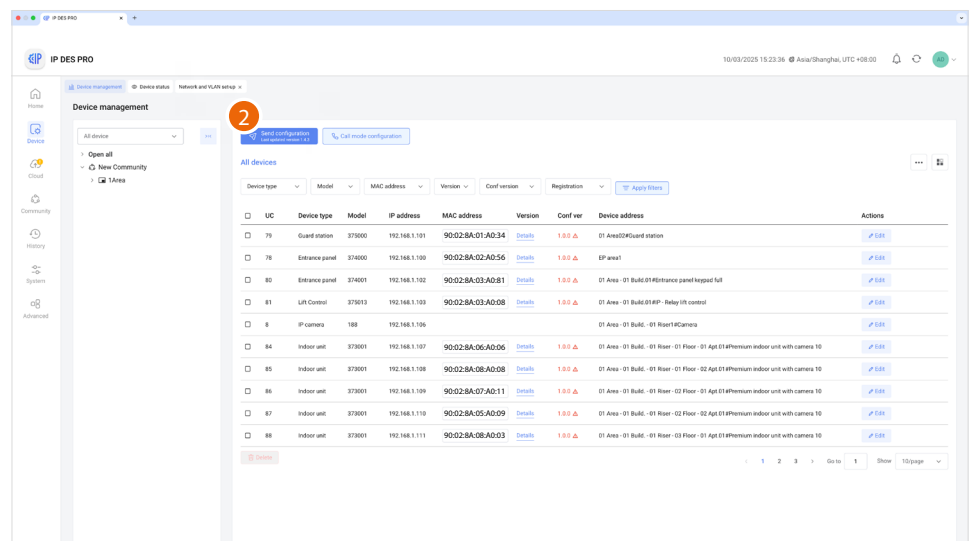
Once created, the plant remains available on the cloud.
If disconnected (unlink button), it can be retrieved from the cloud using the [Import a Plant](#).
If **deleted**, it will also be deleted from the cloud.

Send configuration to the DES Server

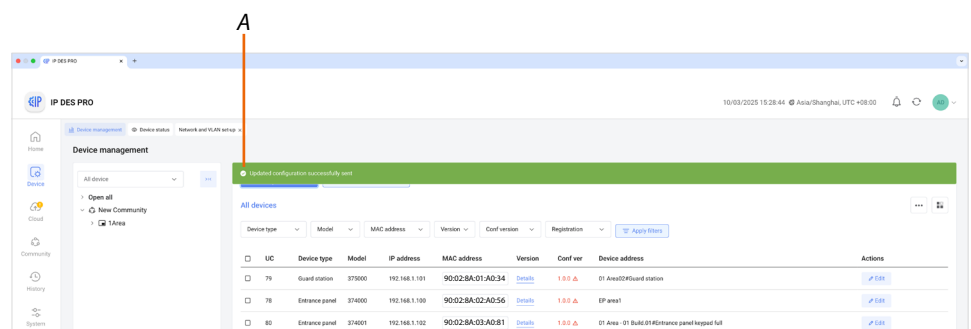
After creating the structure and configuring the virtual devices, it will be necessary to forward the configuration to the system, therefore “instructing” the system to use this configuration.



1. Select Device/Device management

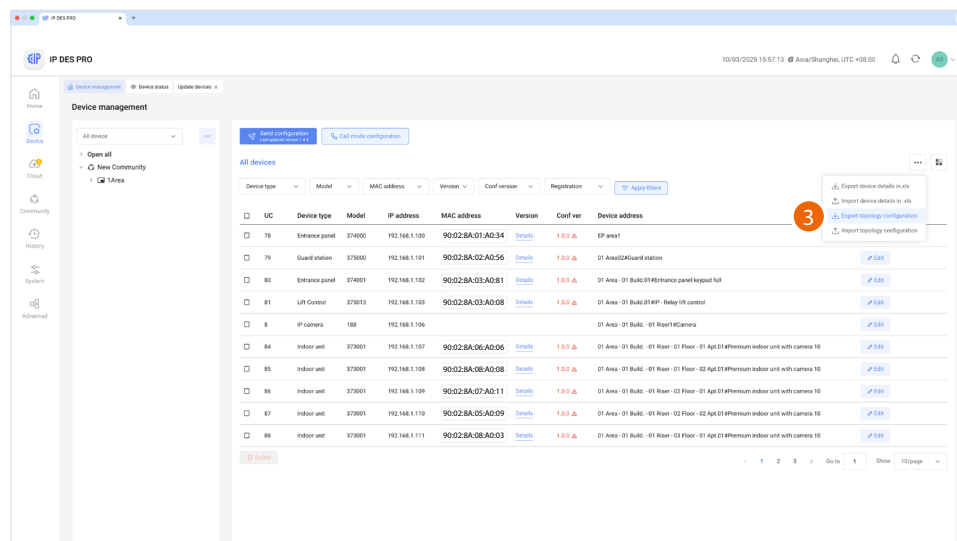


2. Click to send the configuration to the devices

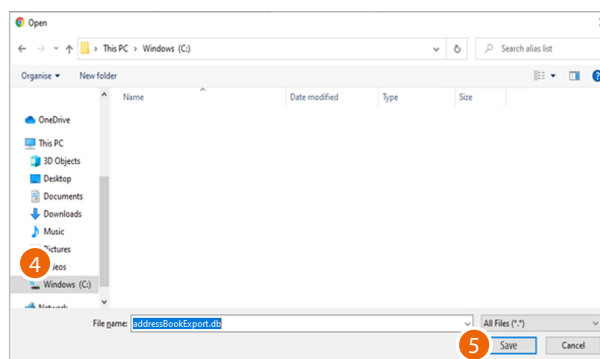


A A message indicates that the configuration has been sent correctly

The configuration is now saved in the DES Server. To avoid accidental loss, it is also possible to save it in an archive file.



3. Click to export the configuration to a file



1. Select the location where to save the file (.db)
2. Click to save

Saving of passwords

Installer passwords are generated automatically (with random digits) and uniquely for the two types of devices:

- entrance panels (with 6 digits)
- internal units and guard stations(with 4 digits).

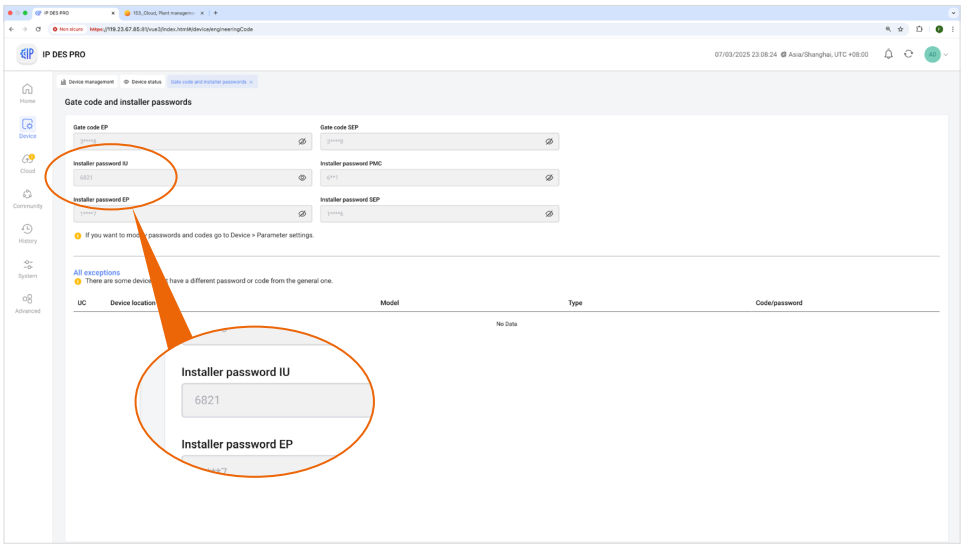
The access codes for opening the door locks of entrance panels are also generated in the same way.

For security reasons, it is recommended to save passwords in a safe place that is always accessible (Cloud backup activation recommended).

If both the SD and the backup are unavailable, it will not be possible to retrieve the passwords.

NOTE : The passwords of the devices incorrectly activated in DEMO mode are: 2000 (EP) and 1111 (IU and GS)

Make passwords visible; see “**Make passwords visible**”



1

INSTALLER PASSWORD
Internal units and guard
stations

INSTALLER PASSWORD
Entrance panels

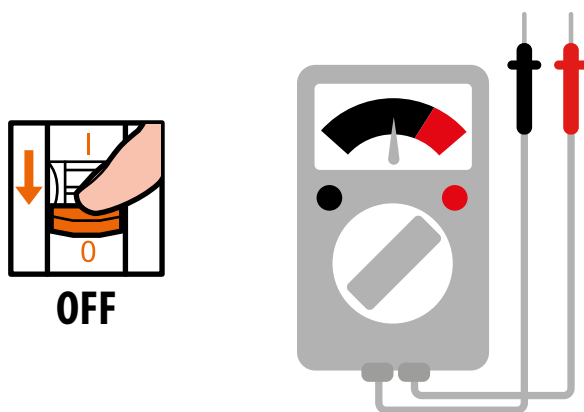
Door lock release
code

1. Write down the passwords in a safe place that is always accessible.

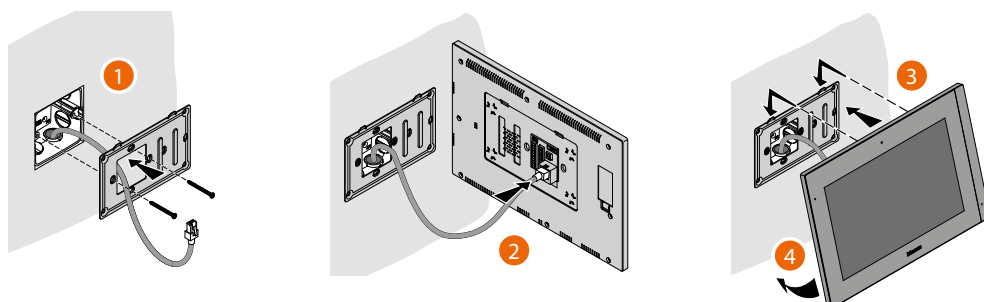
Installation of the devices

To transfer the configuration to the devices, these must be installed and powered

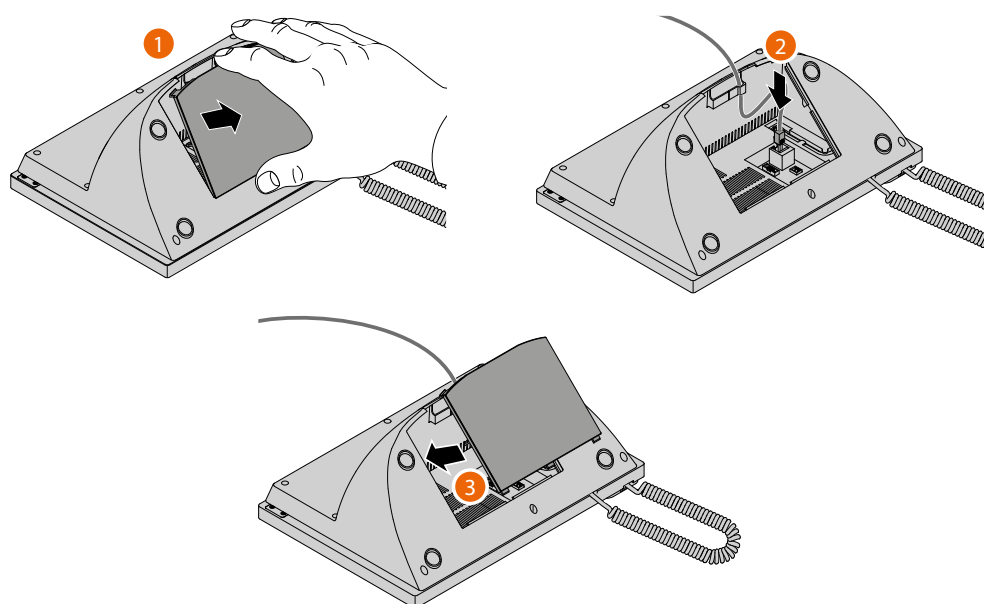
Switch off the power supply to the system and check that there is no voltage



Install the devices

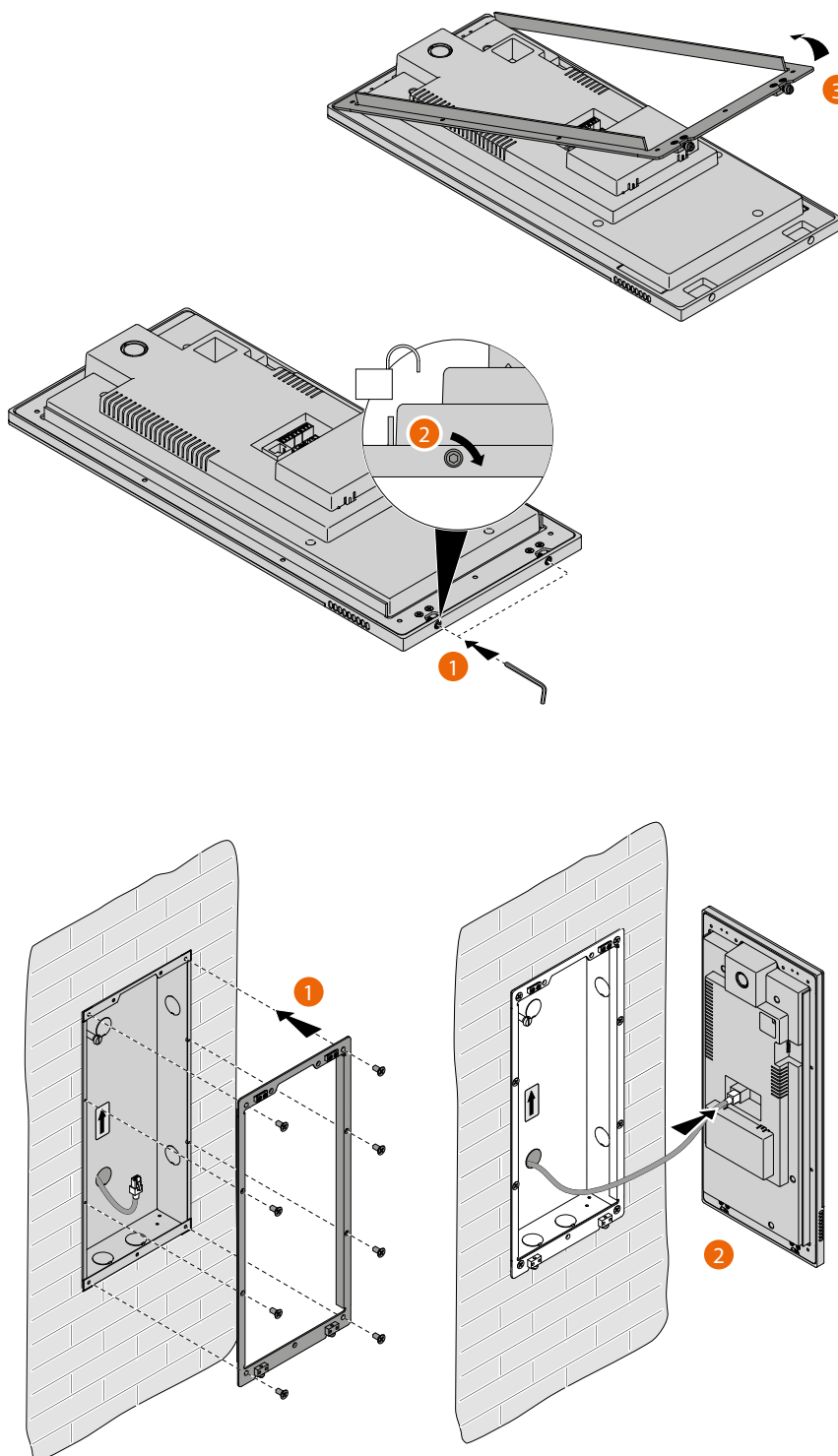


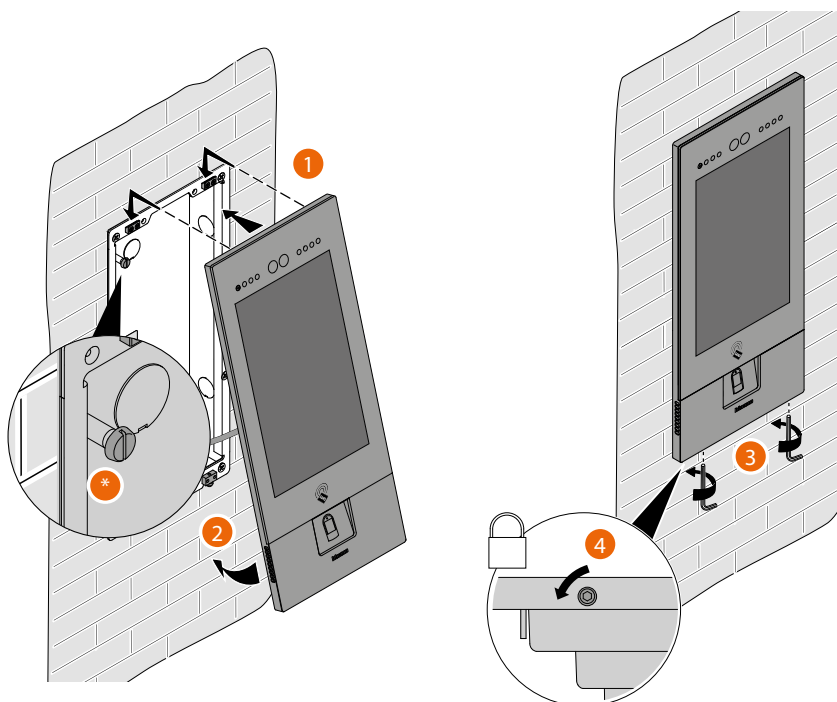
The RJ45 cable must be at least 200 mm long





The wrong wiring of the Ethernet cable connecting the device to the Poe Switch 375002 could damage the device itself.
The RJ45 cable must be at least 200 mm long.





- * Adjust the tamper screw so that it presses the tamper switch of the device and activates the anti-theft function in case of removal, by sending an alarm to the guard station.

Warning: the EP installation shown is representative of all EP.
For more details, see the specific instructions in the package

Reconnect the power supply

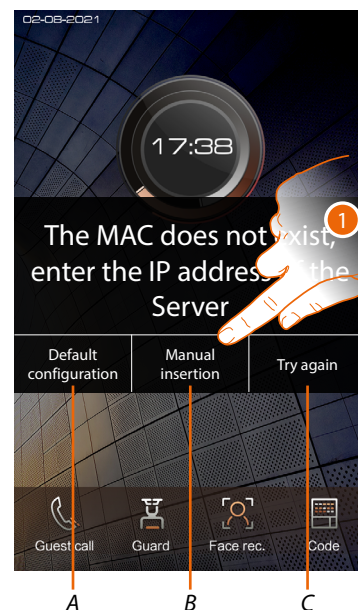
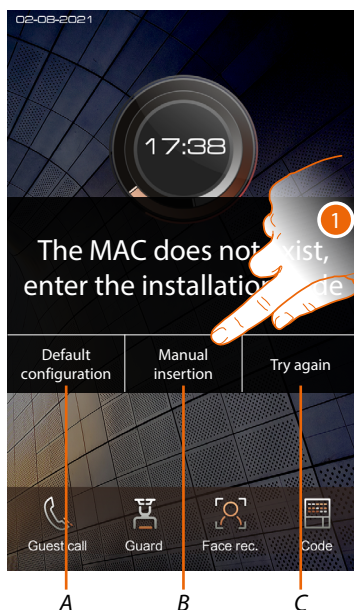


Activation of the devices

Thanks to the previously entered MAC address, once powered, the devices check that a configuration is available on the SD, and if so acquire it.

NOTE: devices that were already configured in the past must be reset.
After rebooting, they will configure themselves

If the automatic activation of the device is unsuccessful, warning messages and manual activation modes may appear.



A Not to be used

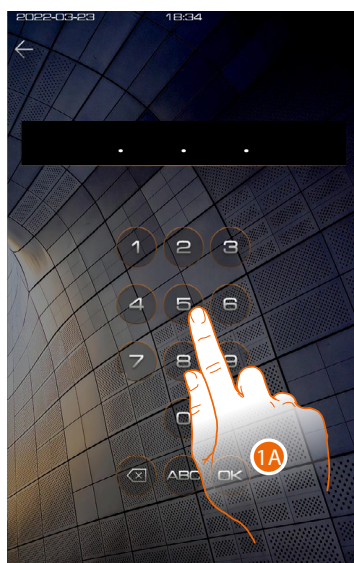
B Button for the manual entry **of the server IP address** or installation code. By entering one of the two described parameters, it is possible to force the configuration of the device by putting it into forced communication with the server.

NOTE: to display the IP address, see [Manage the community networks](#), to display the installation code, see [Installation code](#)

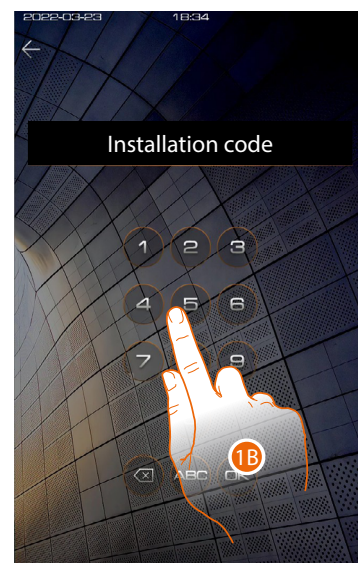
C Button to test the activation of the device

1. Click to manually enter the server IP address or the system access code IP address

IP address



Installation code

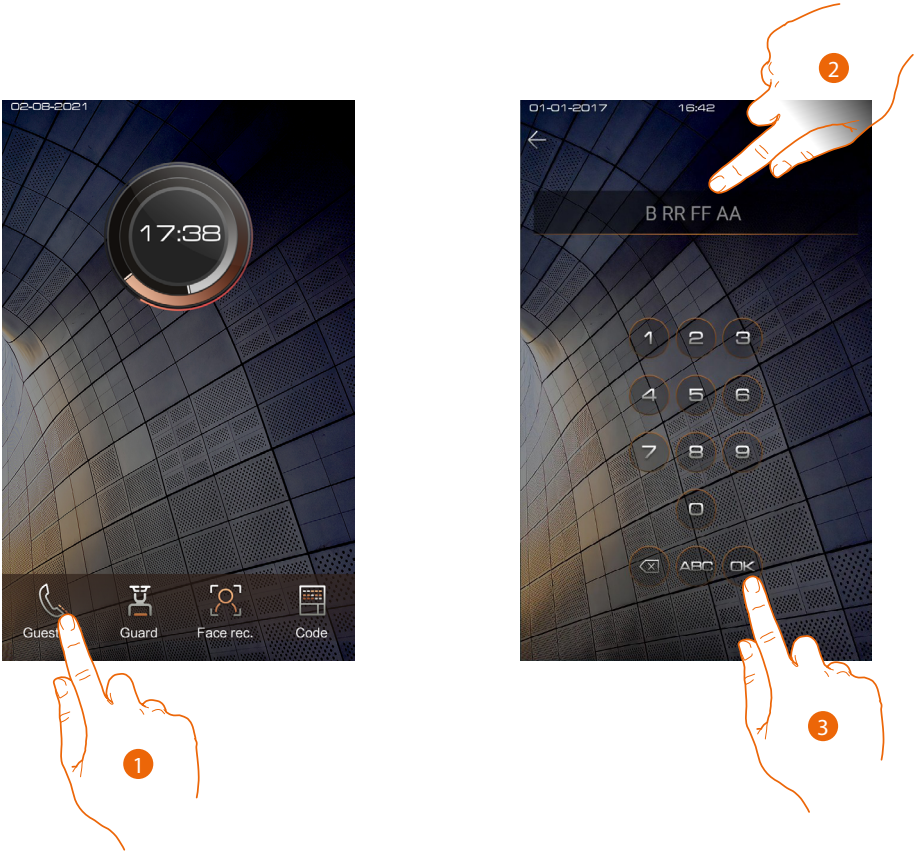


1A. Inserisci l'indirizzo IP del server

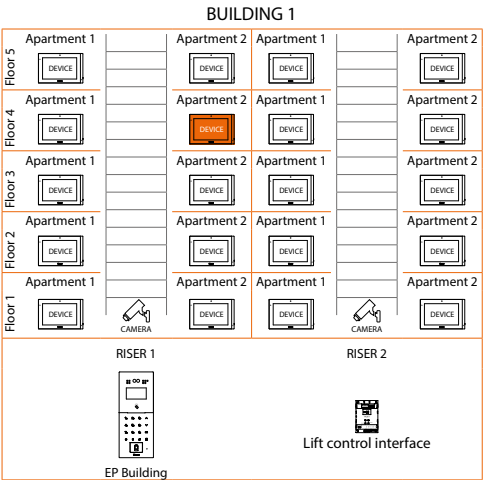
1B. Inserisci il codice installazione

System test

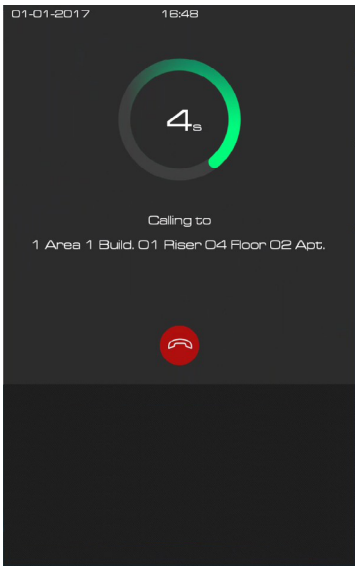
It is now possible to test the system, for example by making a call from the EP



- 1. Touch to make the call
- 2. Enter the IU address

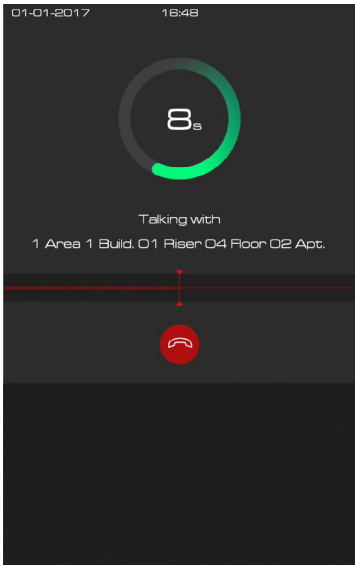


- 3. Touch to send the call



the call is in progress

4. Reply from the IU



Test the audio signal on the EP



Test the audio/video signal on the IU



5. Touch to capture an image of the screen



A confirmation message appears.

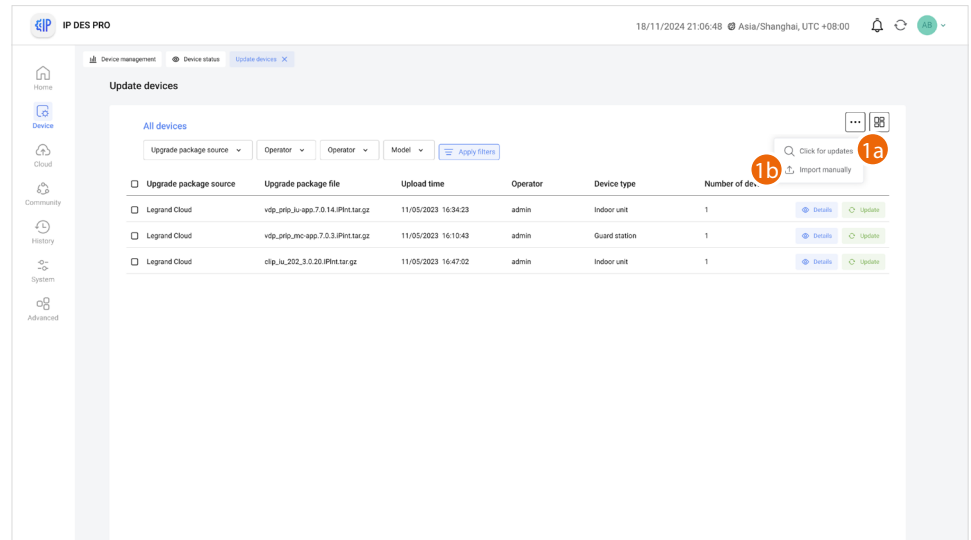
6. Touch to open the EP door lock



A confirmation message appears

7. Tap to adjust the volume
8. Touch to end the call

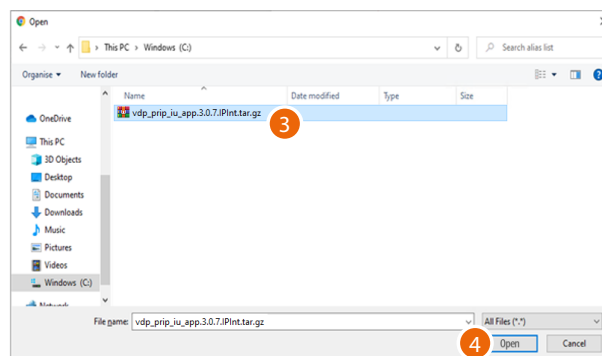
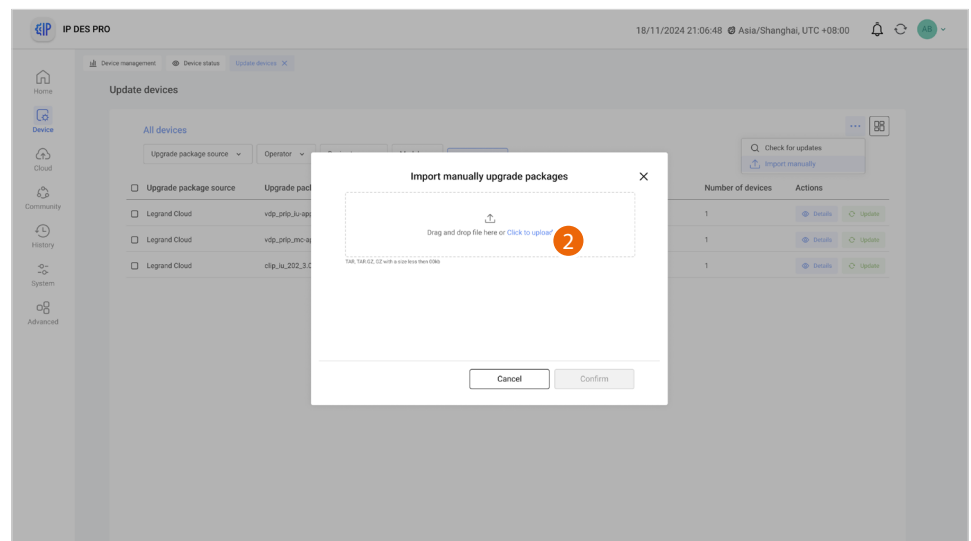
Update of the devices



1a. Click to check for updates on the cloud. If there are updates, these will be downloaded and available for installation

or

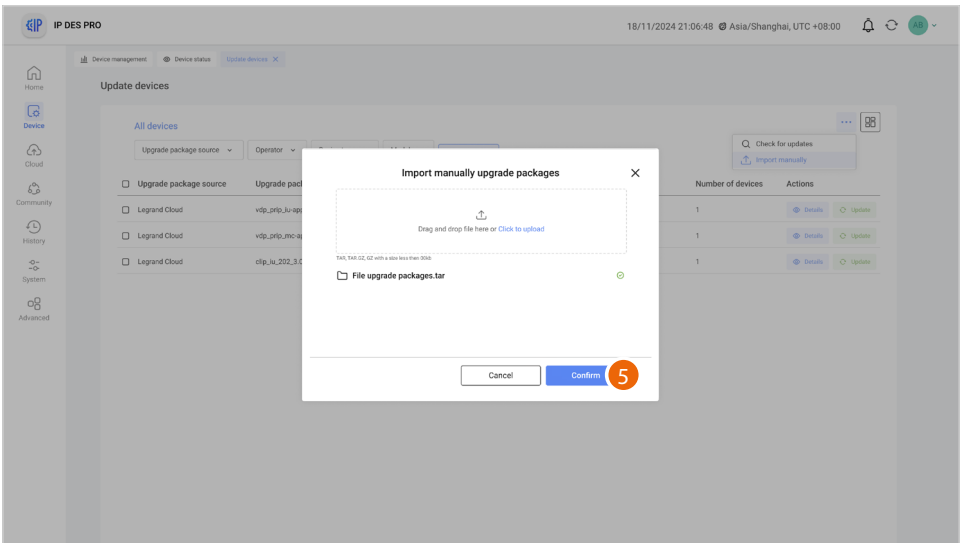
1b. Click to import the update package from the local system (see item 2)



2. Click to select the update package

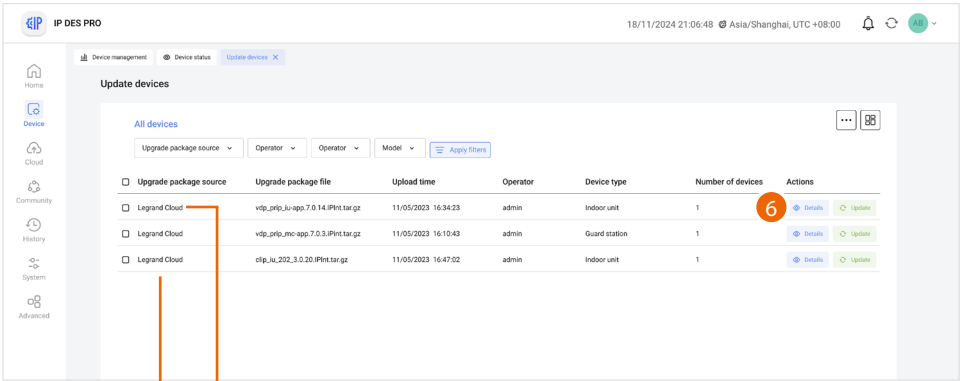
3. Select the .gz file

4. Click to continue



5. Click to confirm

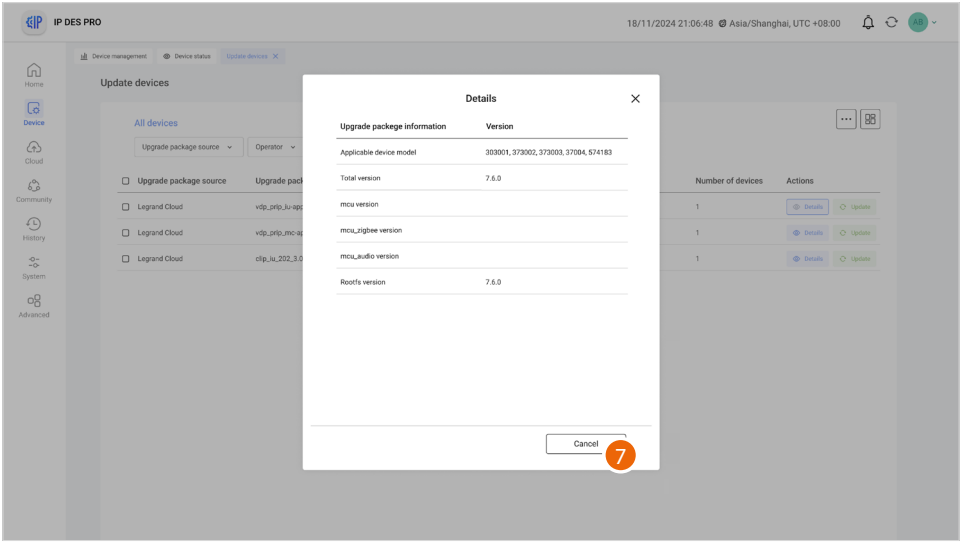
The package has been imported and is available to be sent to the devices



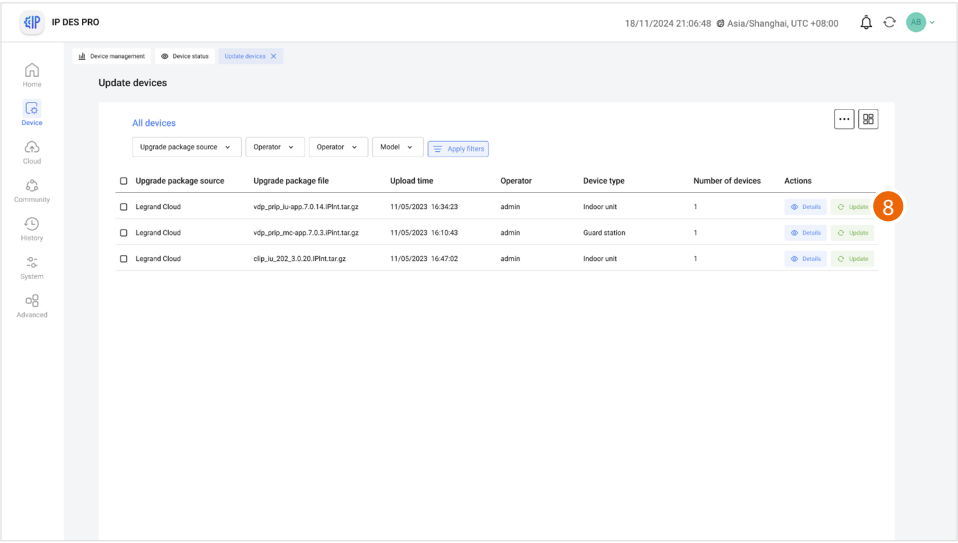
A Update package from Cloud

B Update package from local system

6. Click to see some of the update data



7. Click to close



8. Click to send the update to the plant

Pre-configuration of the server at the office and on-site system configuration

SYSTEM

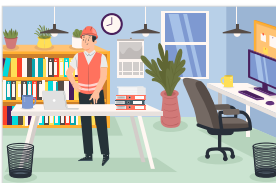


Step **1** Creation of a list of all devices present with their corresponding item codes and MAC ADDRESS, and recovery of the SD from the system, to take to the office

Step **2** Community VLAN network creation

Step **3** Call mode setting and community structure definition

OFFICE



Step **4** Community structure creation

Step **5** Device MAC address registration

Step **6** Community customisation

Step **7** Registration of the Community on the Legrand Commercial Cloud

Step **8** Send configuration to the DES Server

Step **9** Saving of passwords

Step **10** Take the DES server back to system

Step **11** Setup of the fixed DES Server address on the system router

SYSTEM



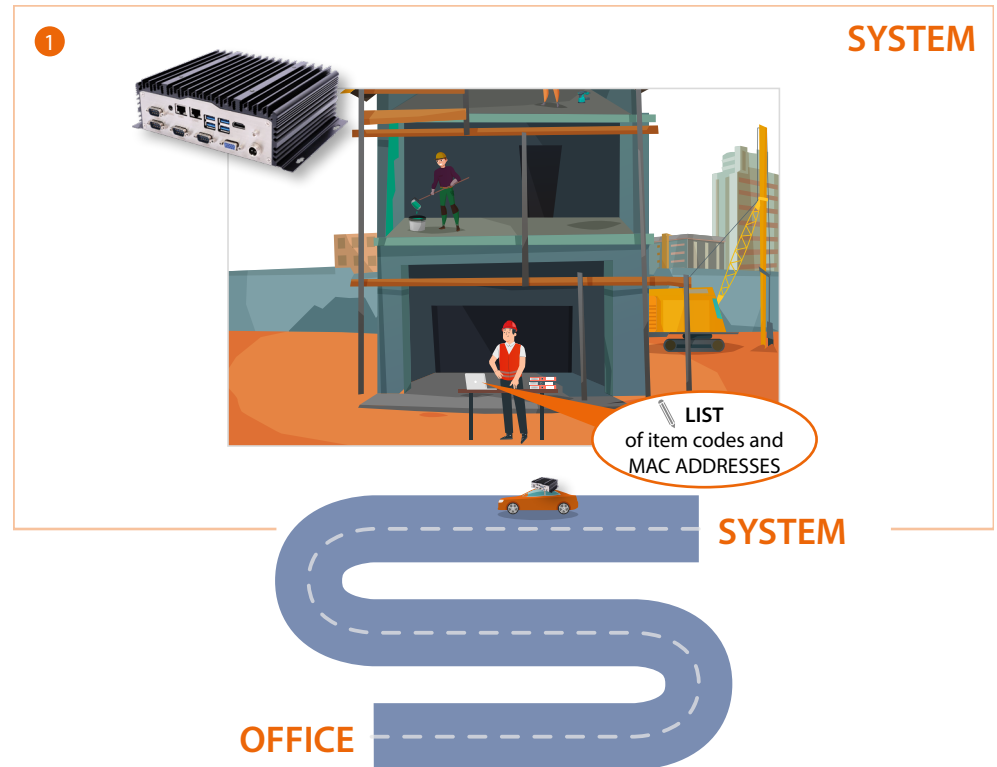
Step **12** Installation of the devices

Step **13** Activation of the devices

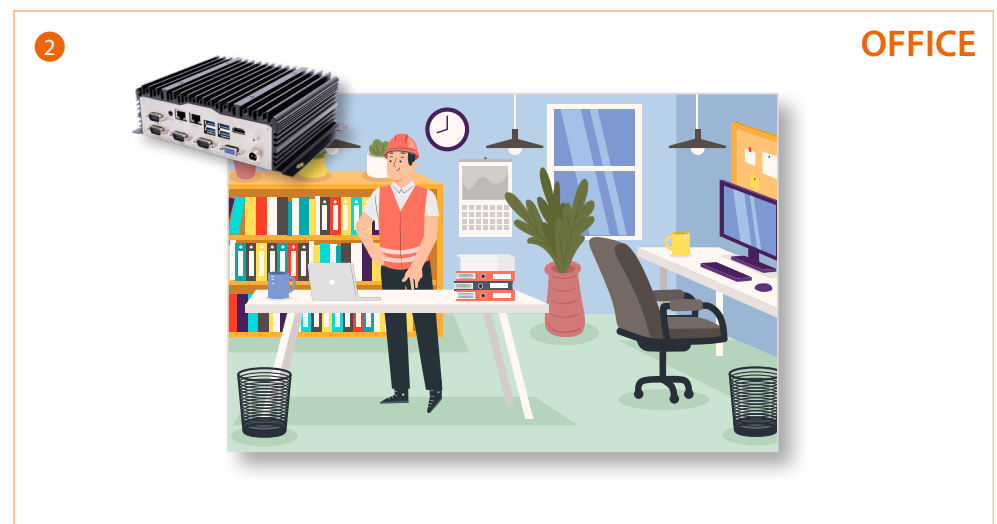
Step **14** System test

Step **15** Update of the devices

Creation of a list of all devices present with their corresponding item codes and MAC ADDRESS, and recovery of the SD from the system, to take to the office



1. Go to the system and create a list of all the devices present with their corresponding item codes and MAC ADDRESSES (these will be needed later when registering the **Mac address**). Take the SD to the office for the configuration.



2. When back at the office, connect the SD to the LAN network and start the configuration.

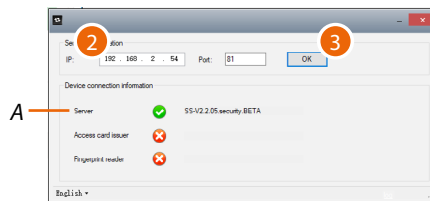
Community VLAN network creation

To configure the community network, it will first be necessary to configure the system by following the steps below:



1. Run the BTicinoWare software (on the Windows Client PC) previously installed

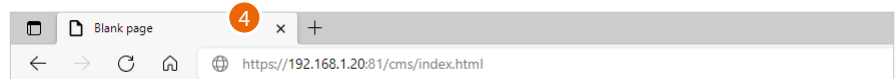
The following screen appears:



2. Enter the **SD address** and check that the port is 81

In order to guarantee correct system operation, the SD (which will take an address assigned by the system router) must maintain its IP address, see [Assigning a "privileged" network address to the SD](#).

3. Press to confirm and check that the flag A is green



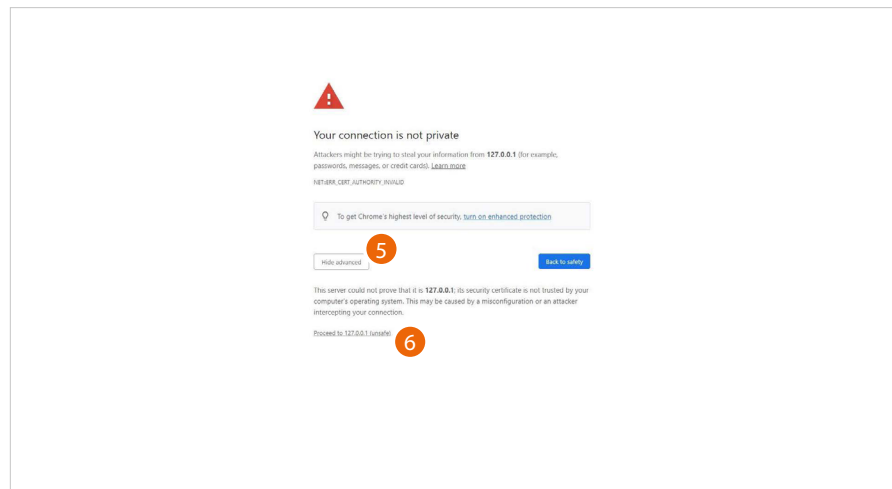
4. Open the browser and enter the http address of the SD:

https://IP or siteserver.local:81

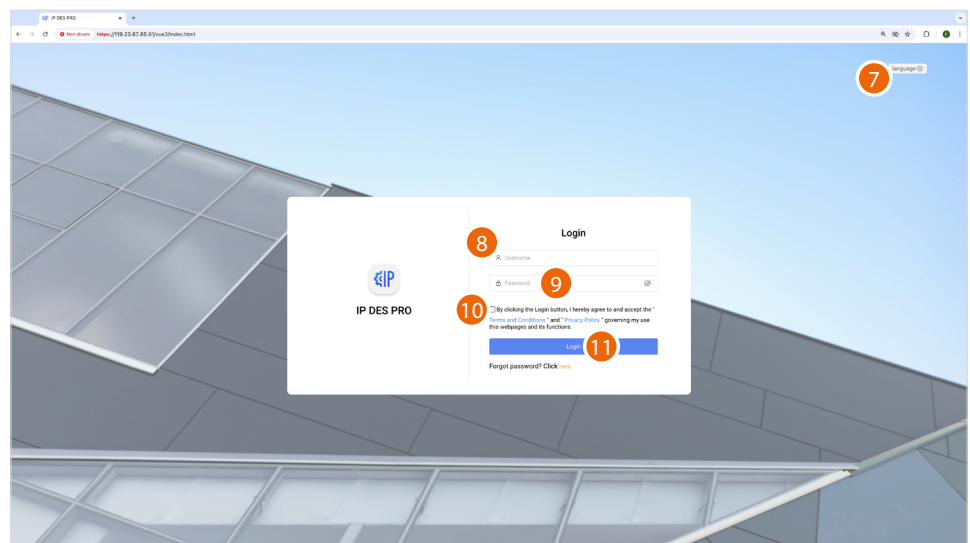
NOTE: use Chrome/Edge browser and a screen with resolution 1920x1080



In some cases, the browser may consider the page to be unsafe.

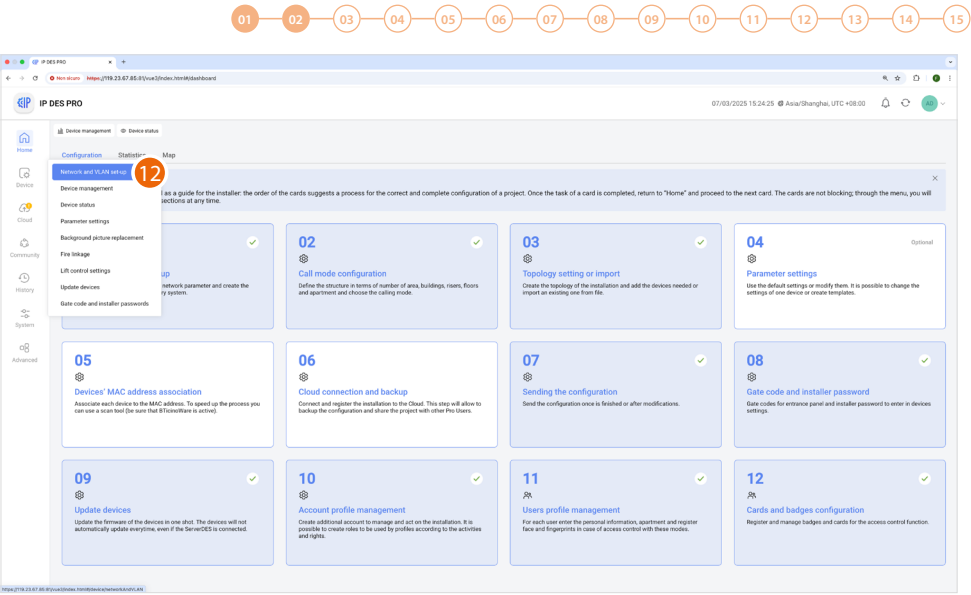


5. Click to display the advanced options
6. Click to ignore the warning and proceed

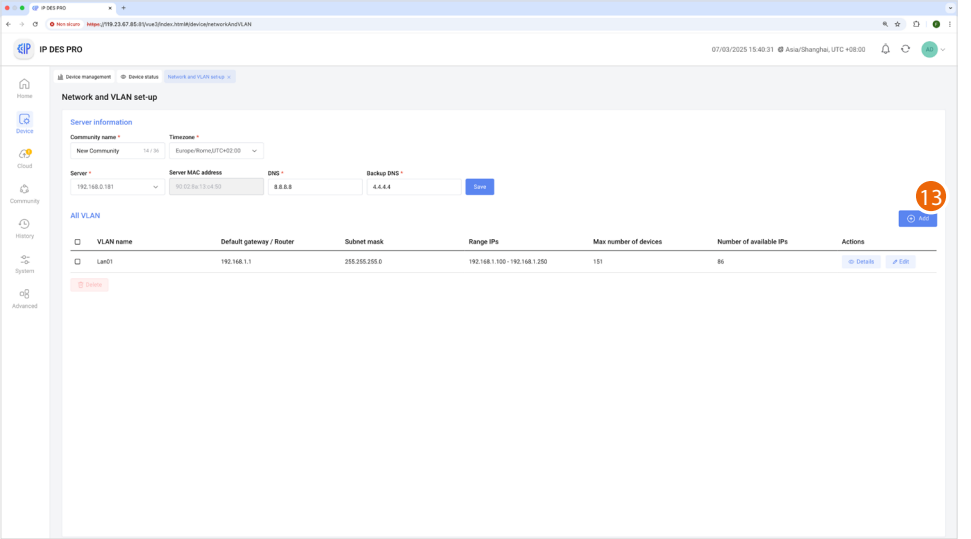


7. Select the interface language.
8. Enter the login name (default admin)
9. Enter the password (default 123456)
10. Accept the "Terms and Conditions" and "Privacy Policy" that govern your use of this website and its functions.
11. Click to confirm

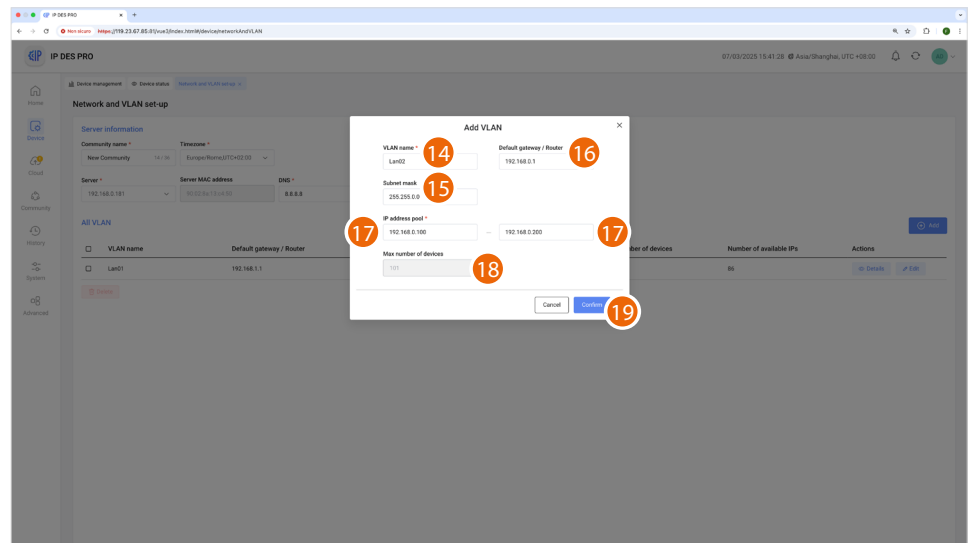
NOTE: For safety reasons, it is mandatory to modify the default password.



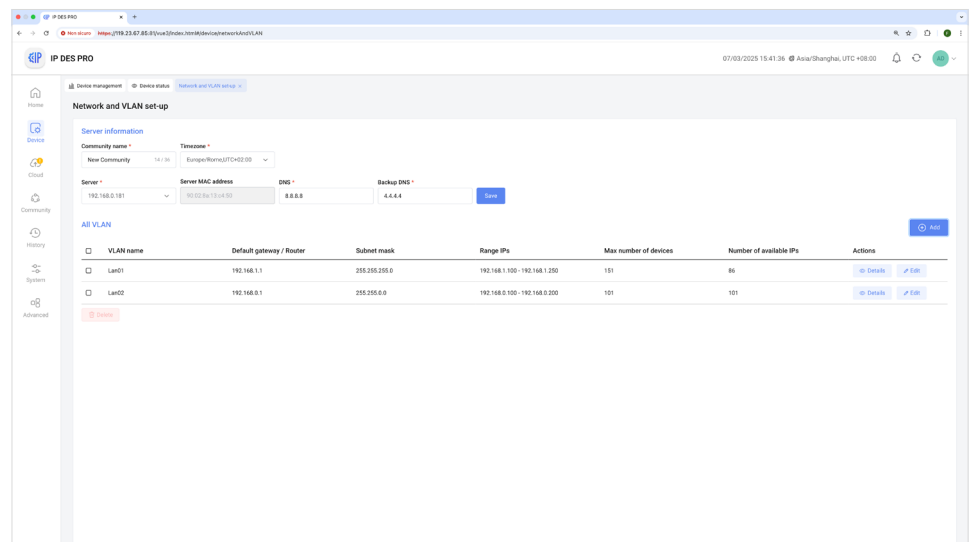
12. Click to open the section where it is possible to create your new community VLAN network



13. Click to create the community VLAN network



14. Enter the name of the community VLAN network (letters and numbers without space)
15. Enter the Subnet mask address
16. Enter the fixed IP address of the SD given to you by the network administrator
17. Enter the starting and ending IP addresses that will determine the maximum number of devices that can be installed on the network.
18. It displays the maximum number of IP devices that can be installed based on the previously entered data
19. Click to confirm

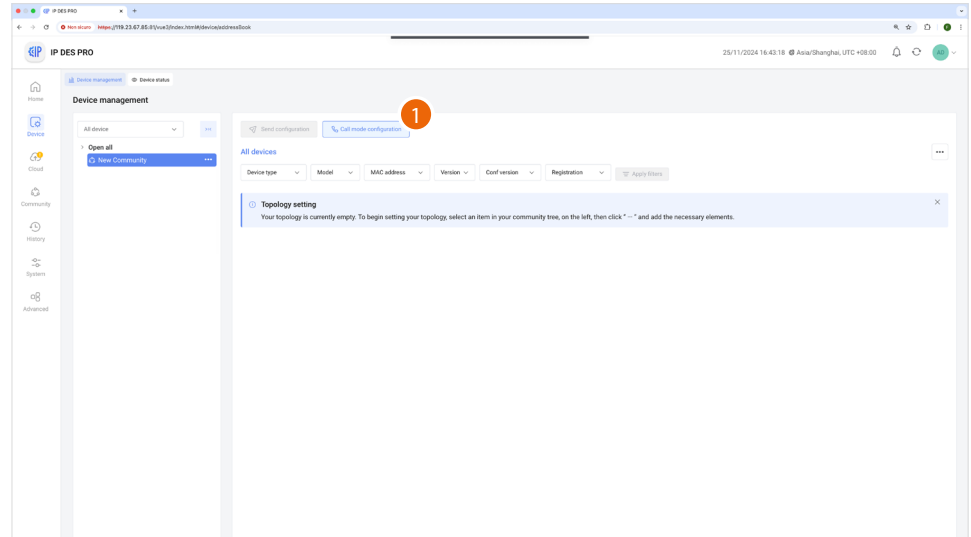


The community VLAN network has been created

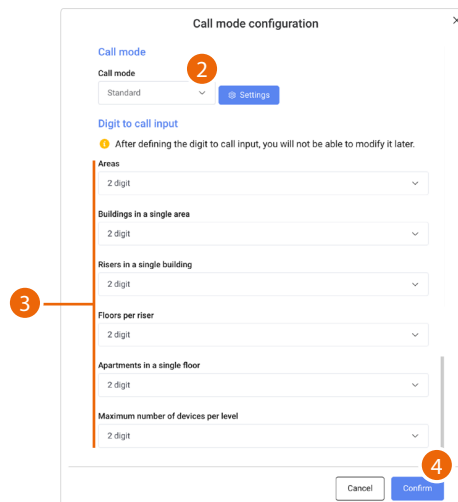
Call mode setting and community structure definition

It is now necessary to define parameters like number of Areas, Buildings, Risers and so on, as well as other parameters that will define the structure of the Community.

In this section, it is also necessary to define the type of call that will be used for all Community calls.



1. Click to open the page



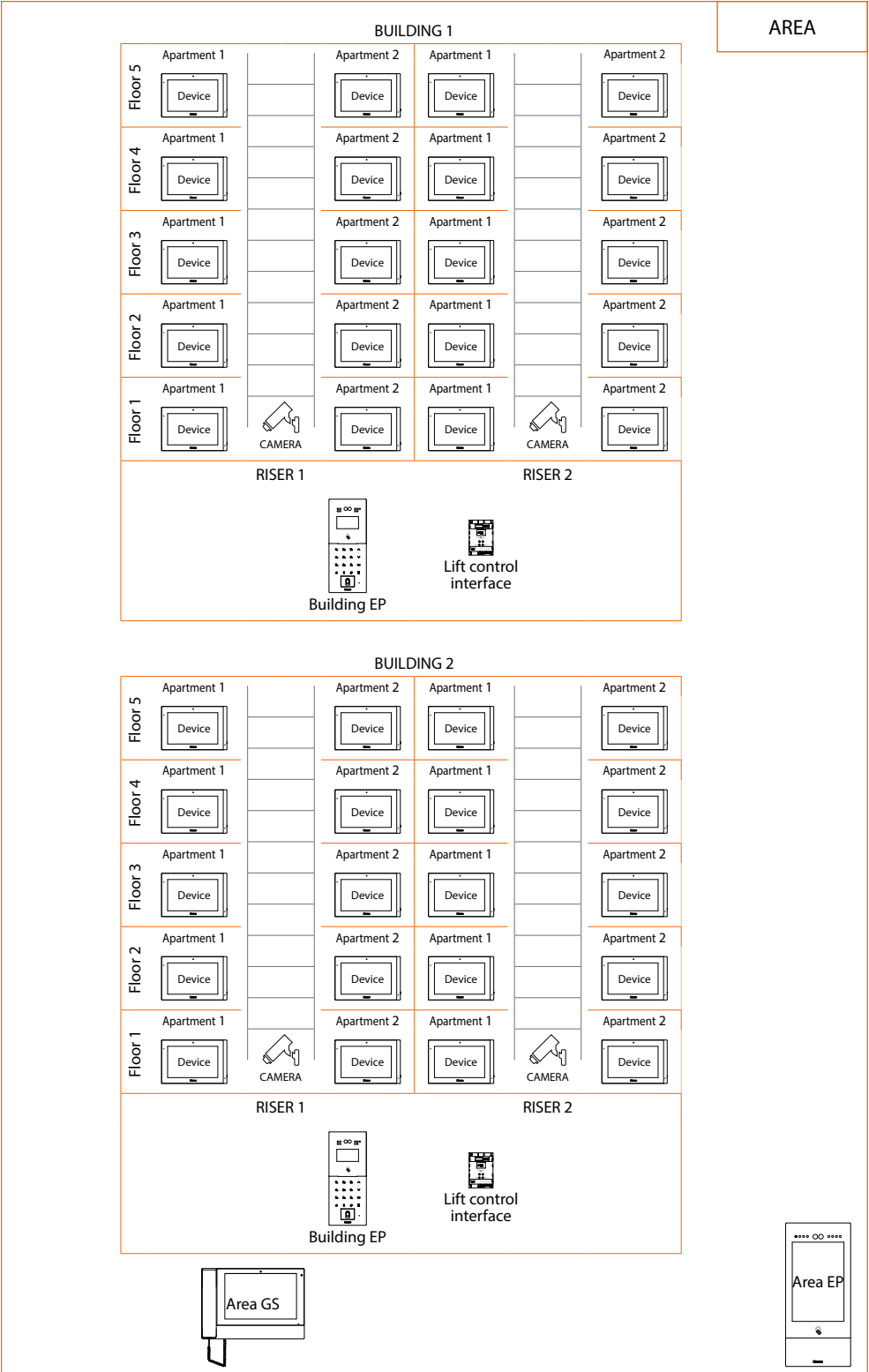
2. Select the **call mode** and configure the relevant parameters
3. Set the number of digits to be used for each call sector (Area/Building/Riser/Floor/Apartment)
ATTENTION: After setting these parameters for the first time, it will no longer be possible to change them.
In order to change these parameters, restore the factory settings
4. Touch to confirm

Community structure creation

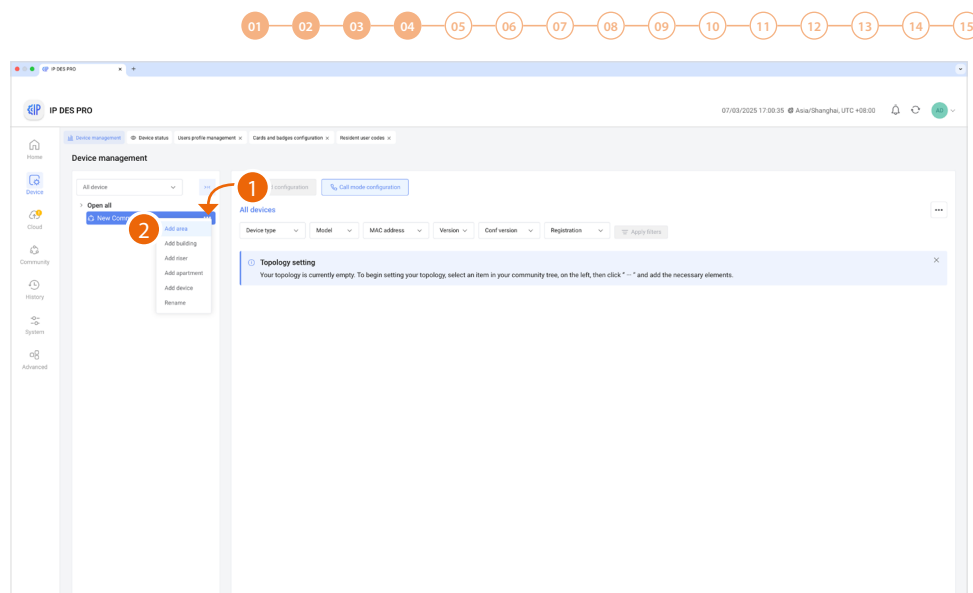
Depending on how your Community is composed, you will need to hierarchically enter:



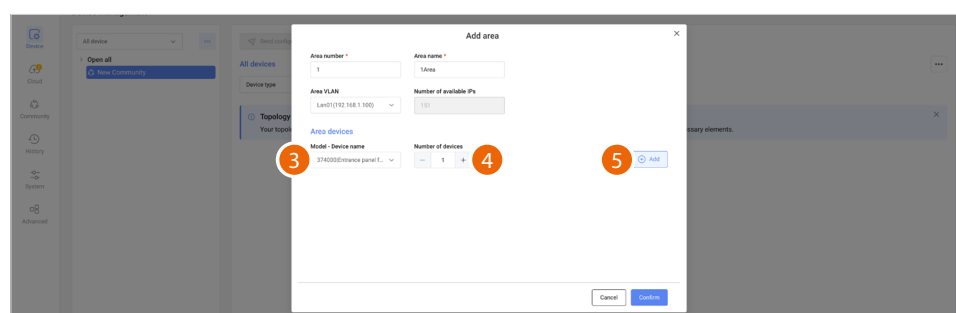
This document will show the creation of a sample structure composed as follows:



Caution: The configuration operations illustrated below are those required to create the example structure.

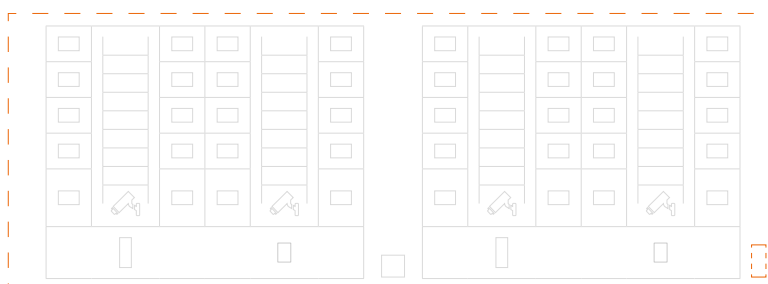


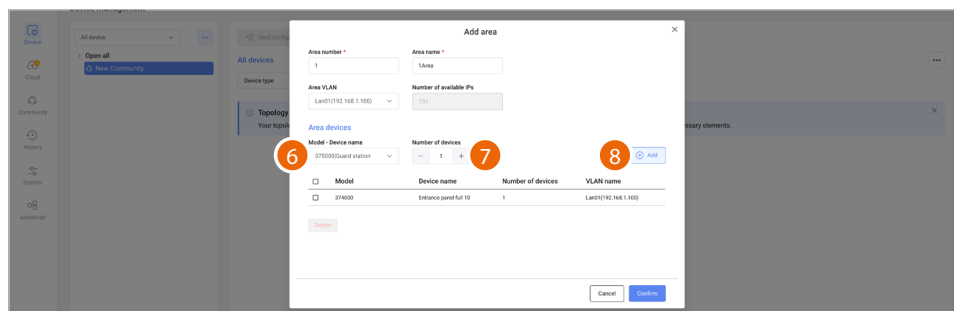
1. Click the Community to open the context menu, a drop-down menu will appear with the commands for its configuration
2. Click to add a new Area



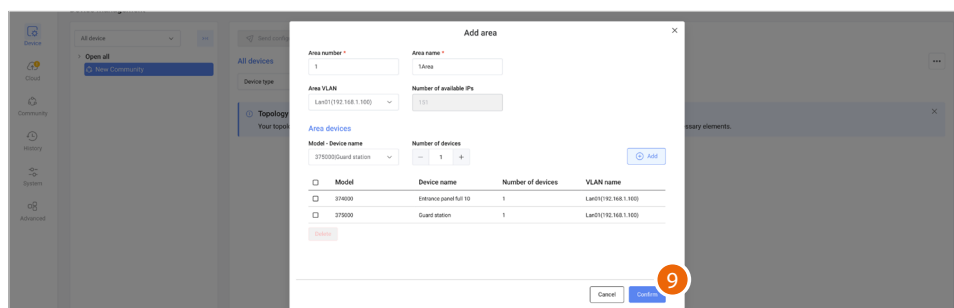
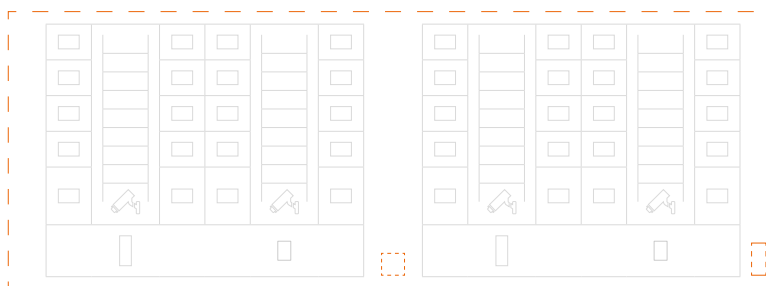
3. Select the area device (Area EP)*
4. Select the quantity
5. Click to add

***NOTE:** Before proceeding with the addition of the devices, remember to check that all the device parameters comply with the requirements, see [Configuration Parameters](#)

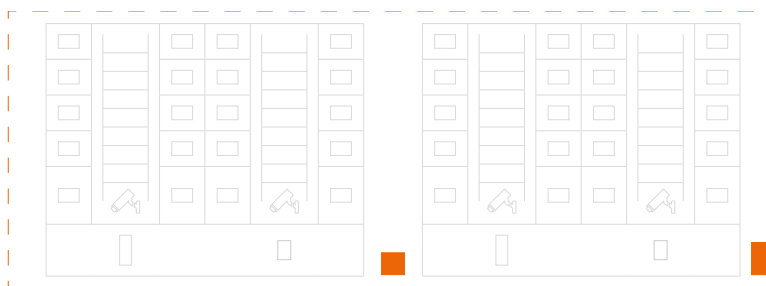


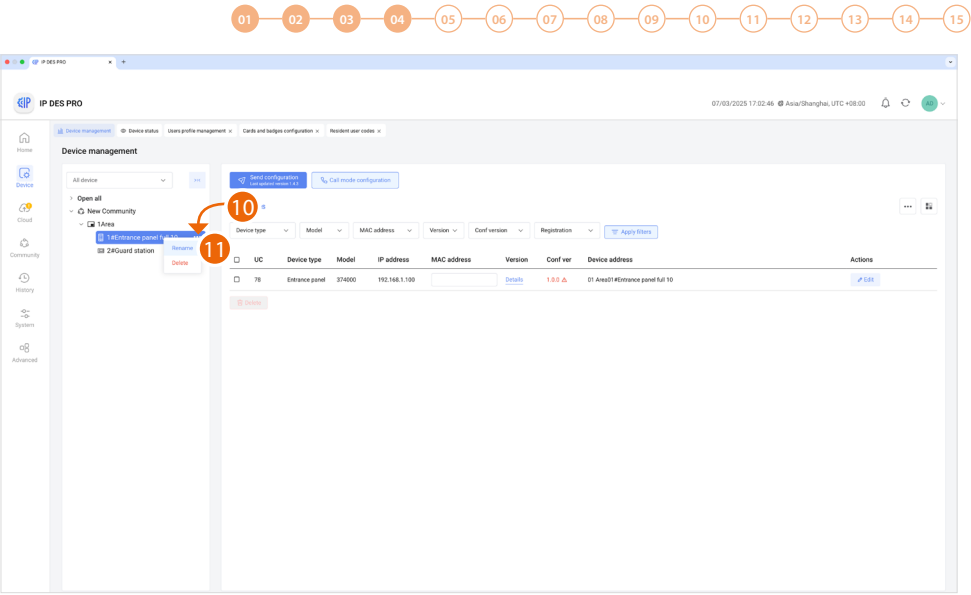


6. Select the second area device (Area GS)
7. Select the quantity
8. Click to add



9. Click to confirm

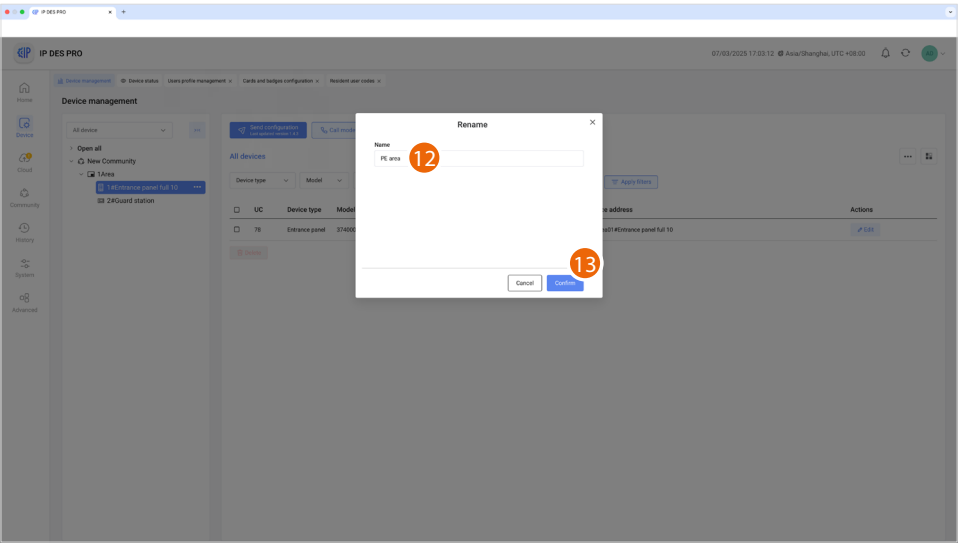




After inserting the devices, you will be able to customize their name

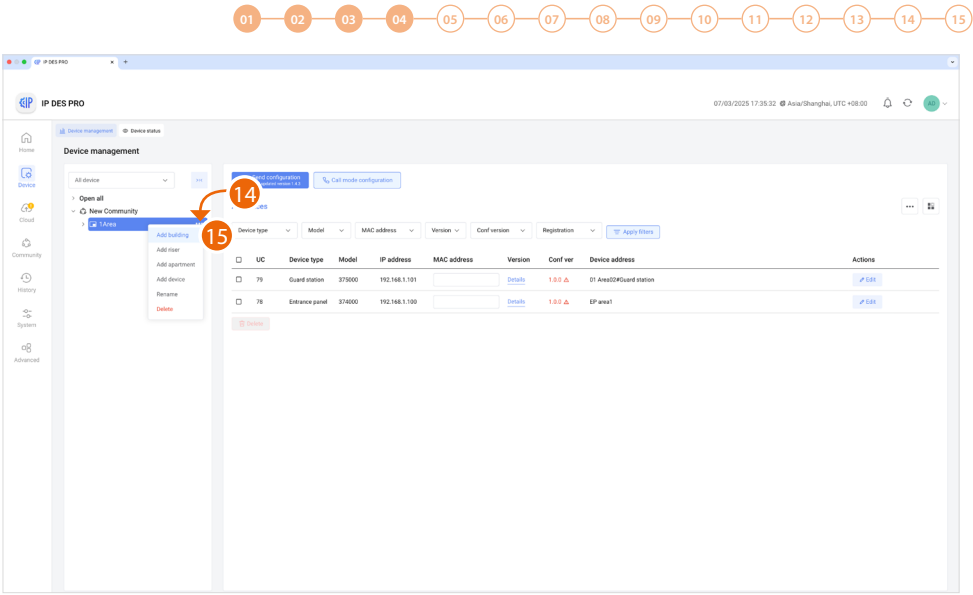
10. With the right mouse button click the device that you want to rename: a drop-down menu will appear

11. Click to open the edit window

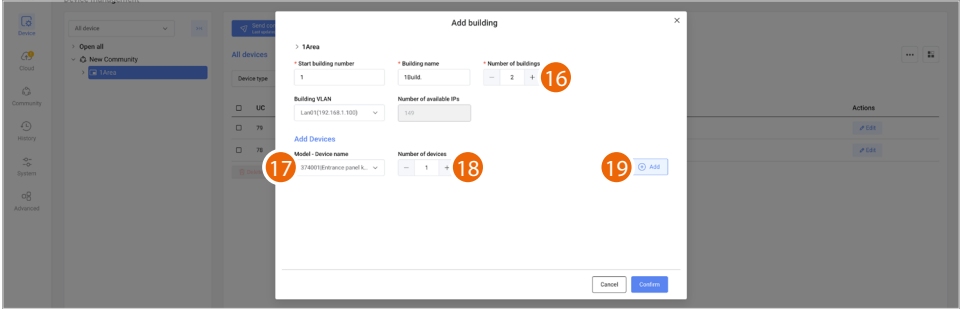
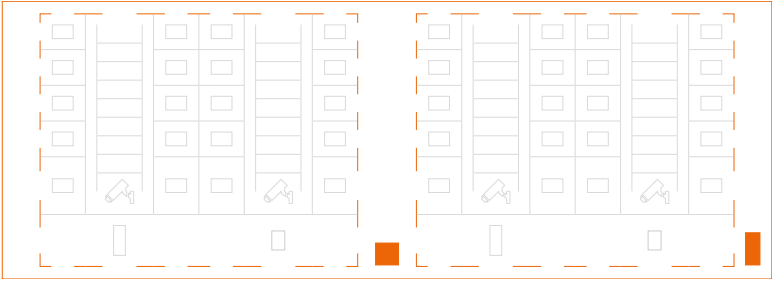


12. Enter the new name

13. Click to confirm



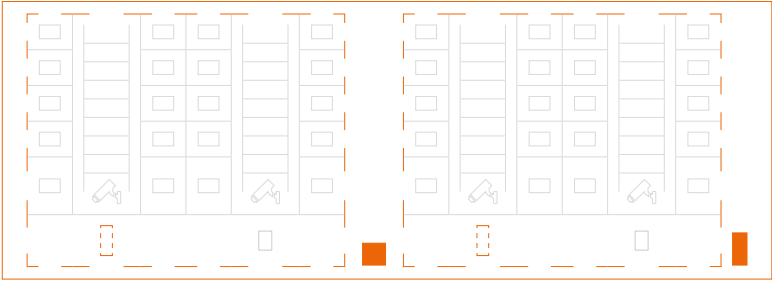
14. Click the Area with the right mouse button. This will open a drop-down menu
15. Click to add the **Buildings**

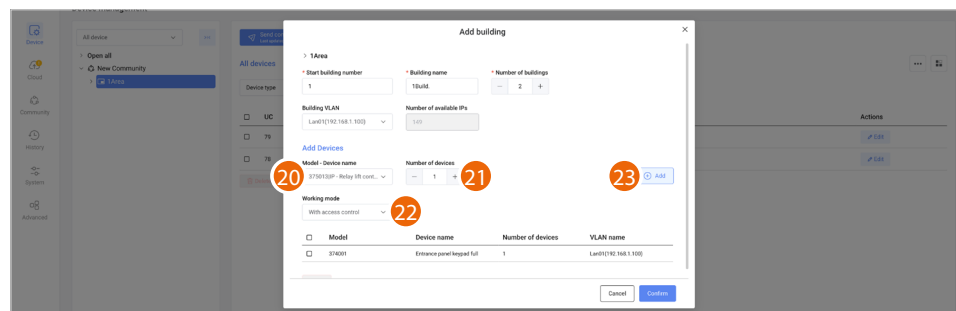


16. Select the number of Buildings to add
17. Select the Building device (Building EP)

NOTE: the software automatically applies a filter to only show devices that are consistent with the component that you are adding

18. Select the quantity
19. Click to add





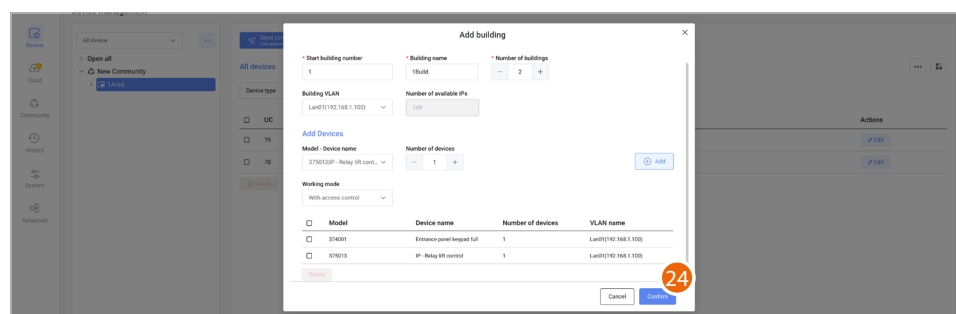
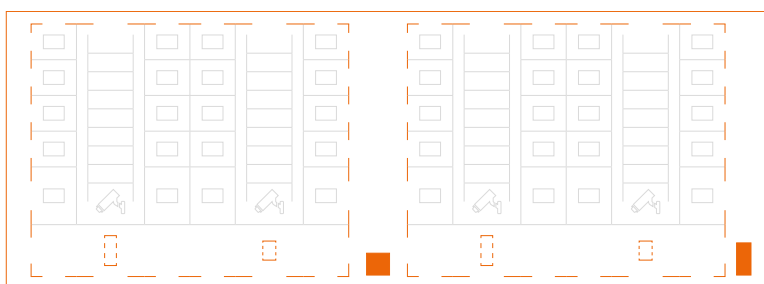
20. Select the device to add (lift control interface with relay 375013)

21. Select the quantity

22. Select the operating mode:

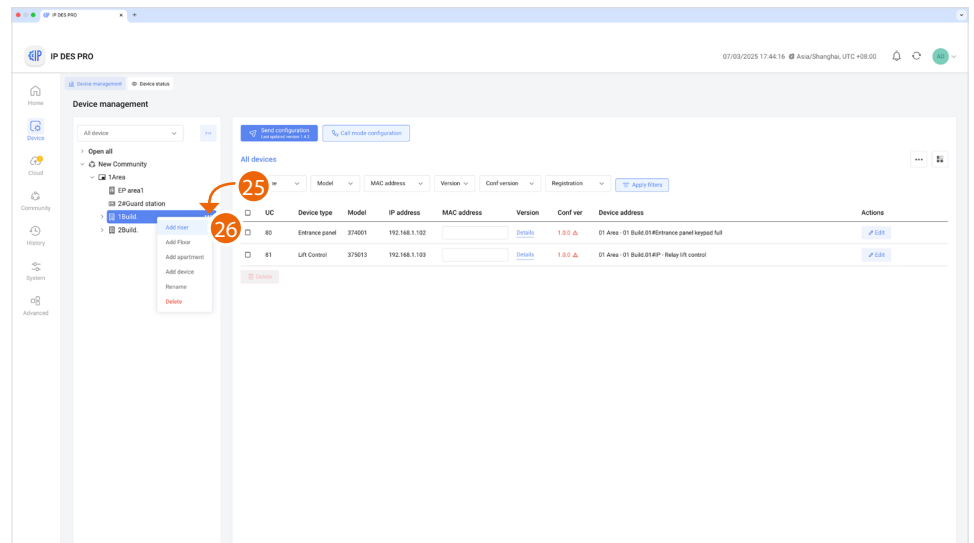
- **with access control:** this mode allows to set up an exclusive call to a specific floor (e.g. only go to the third floor)
- **ground floor call:** this mode allows to set the system so that the lift is sent to the floor of the caller.

23. Click to add



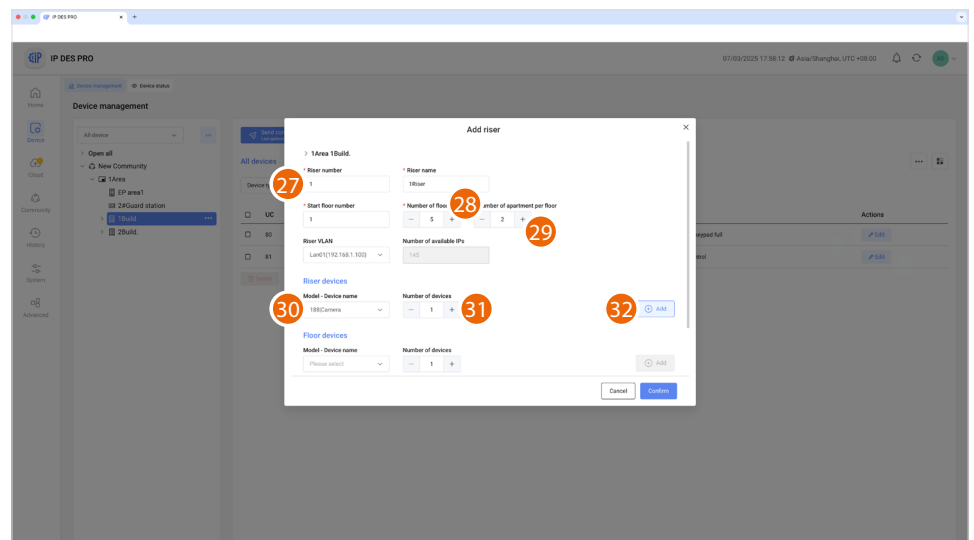
24. Click to confirm





25. Click the Building with the right mouse button. This will open a drop-down menu

26. Click to add a new Riser



27. Enter the progressive Riser number

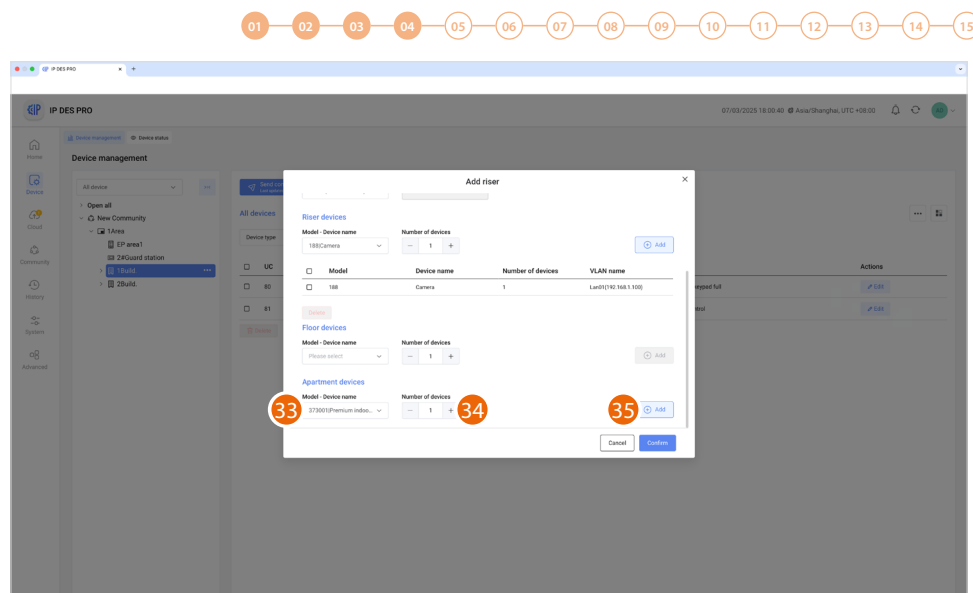
28. Select the Building Floor number (5)

29. Select the number of Apartments for each Floor (2)

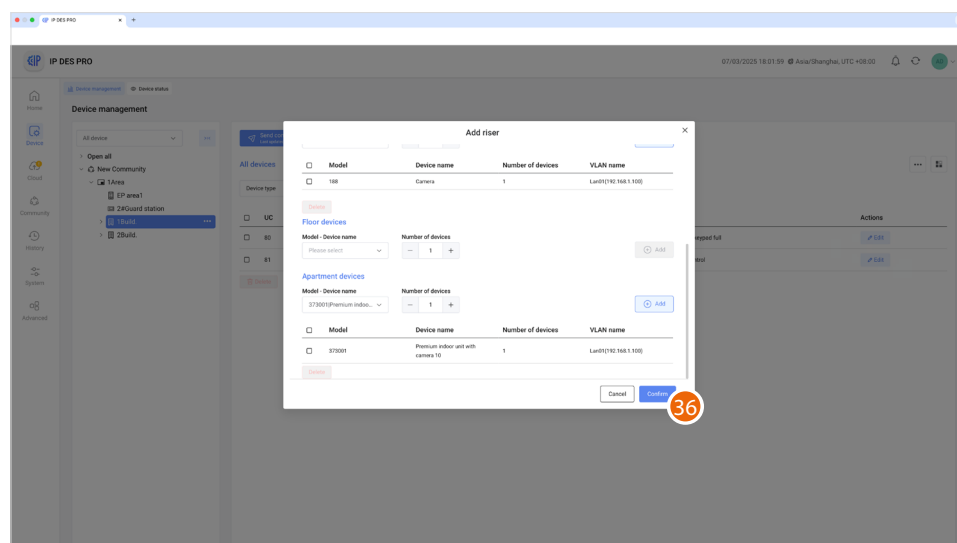
30. Select the OnVif IP Camera

31. Select the quantity

32. Click to add



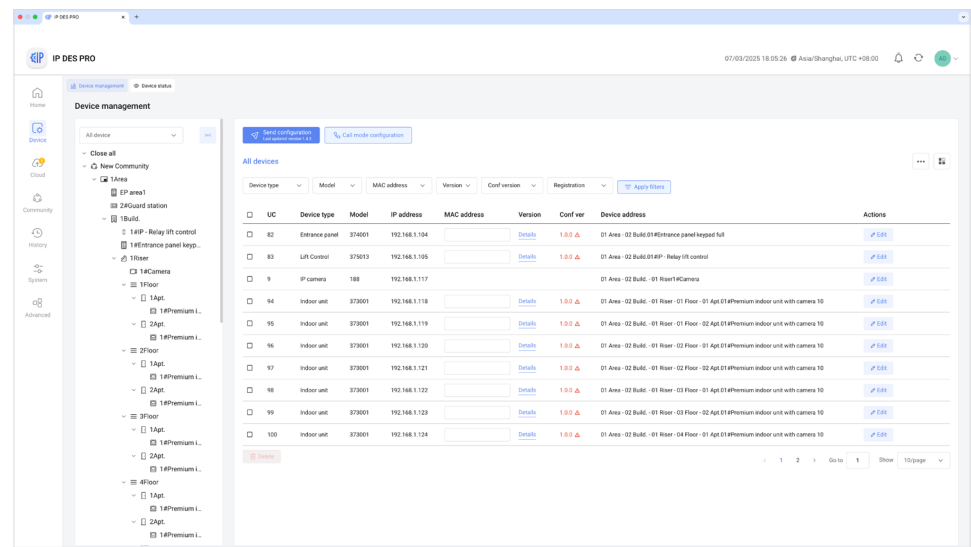
33. Select the apartment device
34. Select the quantity
35. Click to add



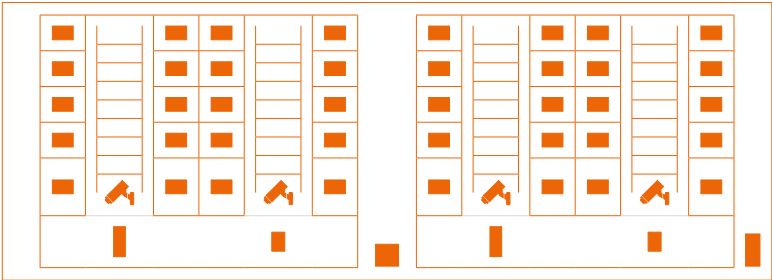
36. Click to confirm



Repeat the same steps for Riser 2



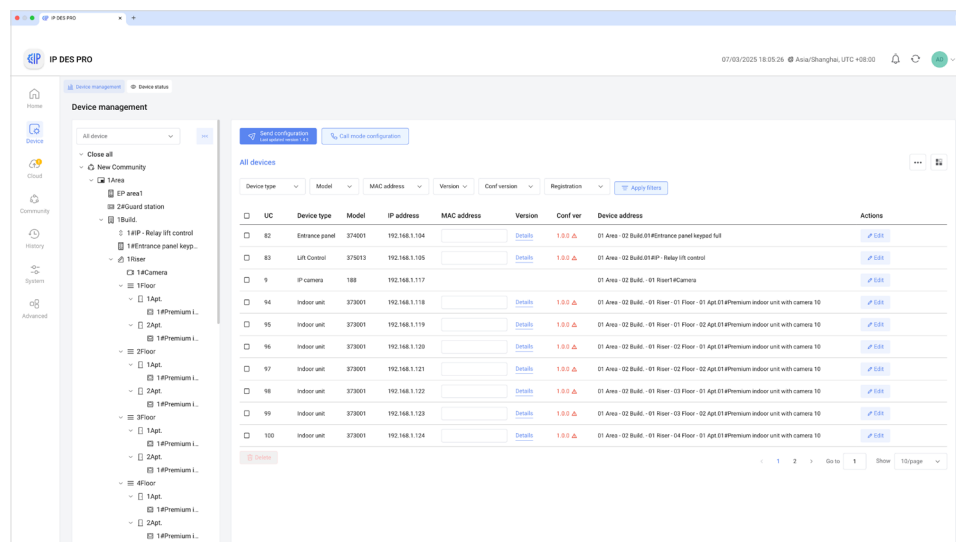
Repeat from step 21 also for Building 2



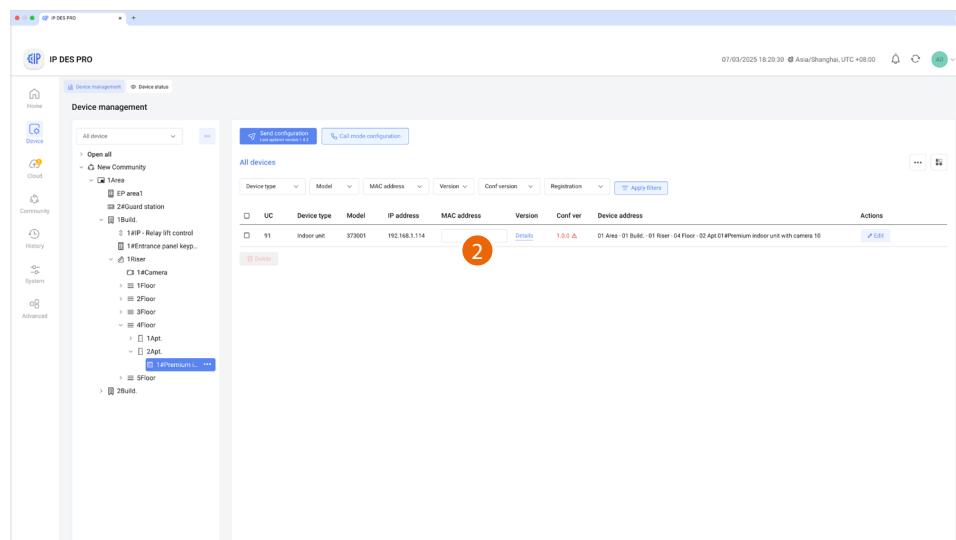
Device MAC address registration

Now that the structure is complete, you will need to associate the MAC addresses of the physical devices with the virtual ones included earlier in the structure.

The device MAC ADDRESSES can be obtained from the list previously created on the system.



This section includes all the devices to associate. The MAC address can be entered directly from this screen



Alternatively, it is possible to select a branch and only view the devices belonging to that branch. Select a device from the tree menu and enter the MAC address individually. The advantage of this method, is that it is easy to identify devices based on their geographical location.

2. Enter the MAC address

Repeat for all devices

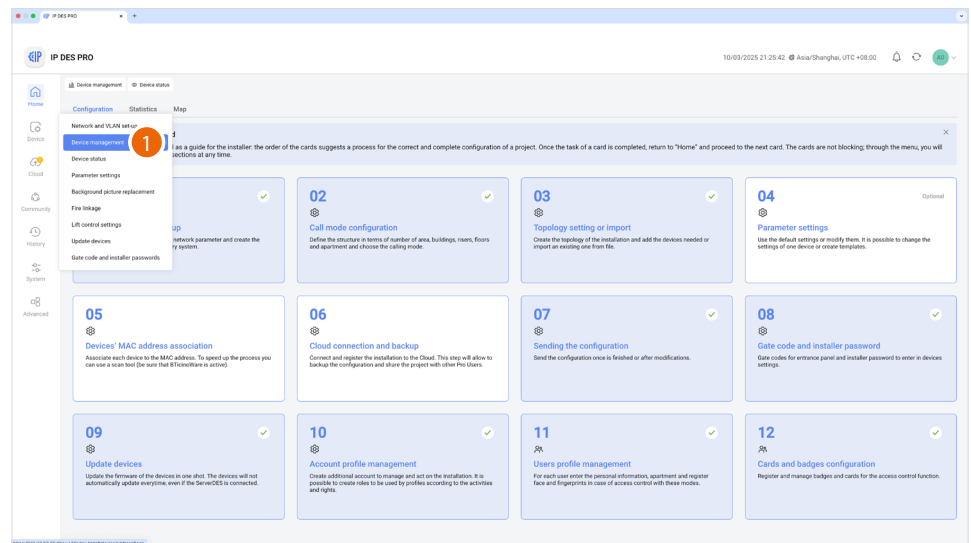


Community customisation

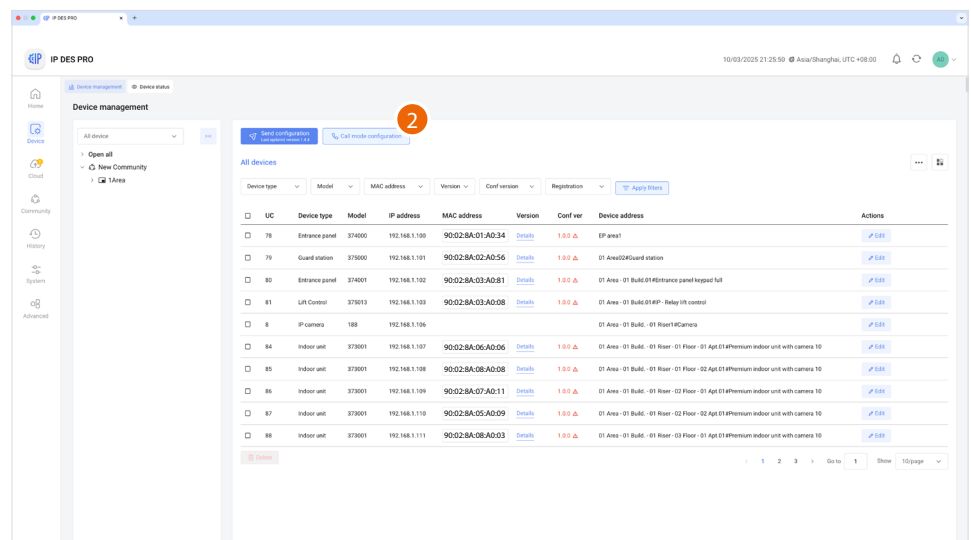
Before sending the configuration to the SD, we can customise the Community by e.g. **modifying the call mode** and/or by **enabling access to the Community for certain individuals**.

To use a different call mode, (e.g. call mode via phonebook) to call residents, it will be necessary to:

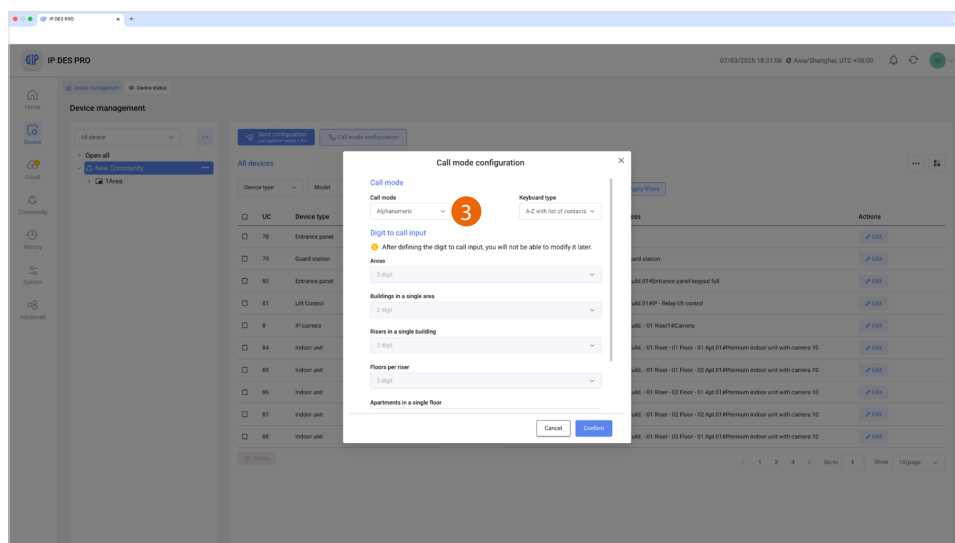
- Change call type to alphanumeric/address book
- replace **the address in the community with an alias** to facilitate recognition of the called party.
This function renames the apartment to a different name (alias). The call to this apartment will be made using this new name. E.g. JOHN SMITH



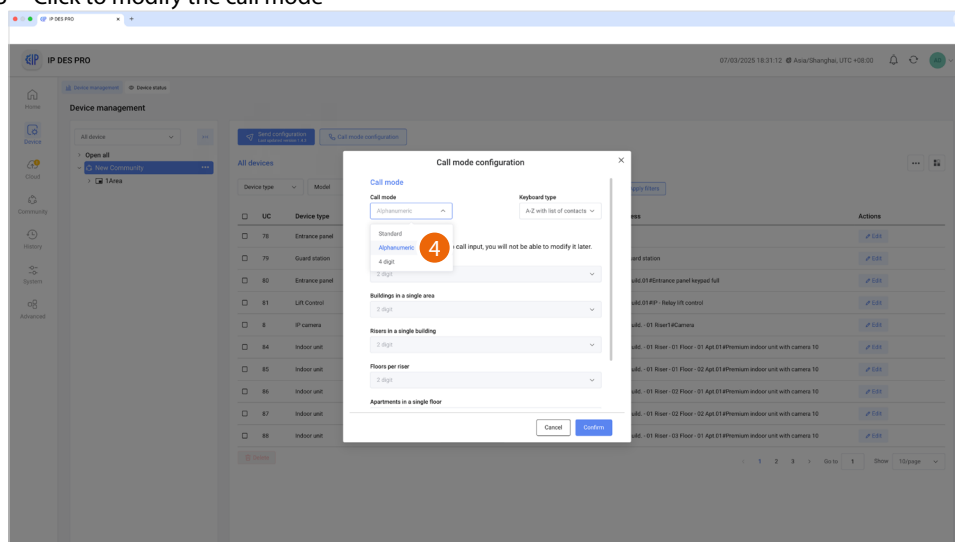
1. Select Device/Device management



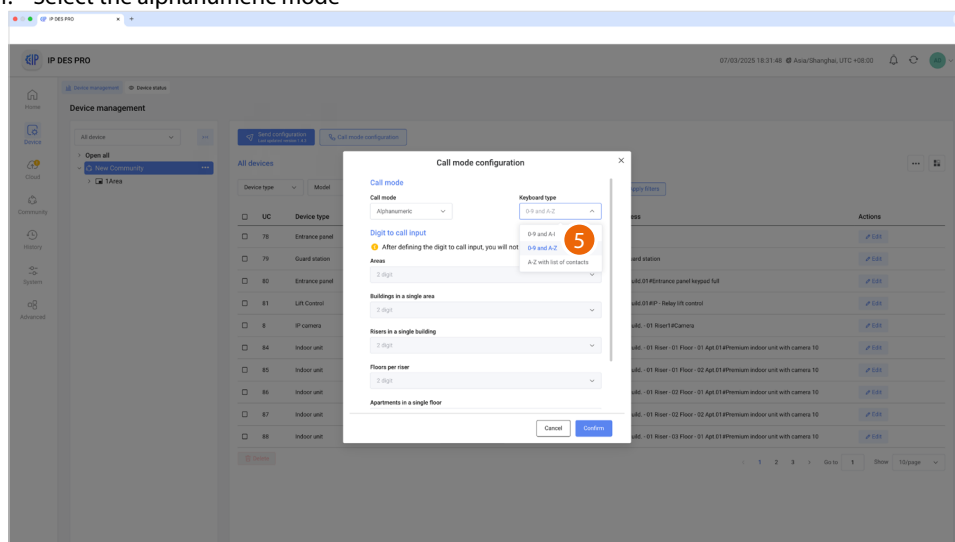
2. Click to select the command



3 Click to modify the call mode



4. Select the alphanumeric mode



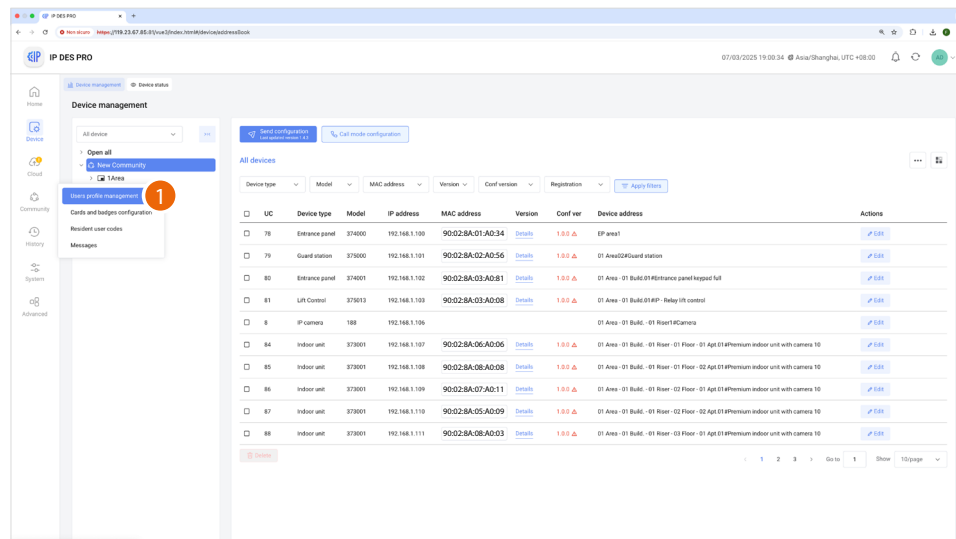
5. Select address book as entry type

After sending the configuration to the SD, it will be possible to call IU using custom names (aliases). When changing the name of a GS or EP, this will be identified with this name on the receiving device when the call is made.

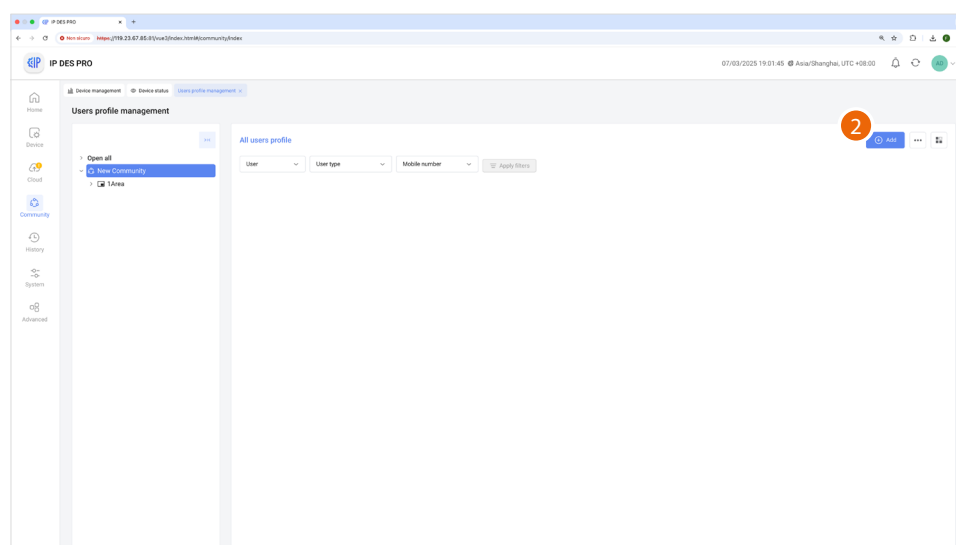
NOTE: This alias format (Address Book) is not supported by entrance panels 374001/03

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

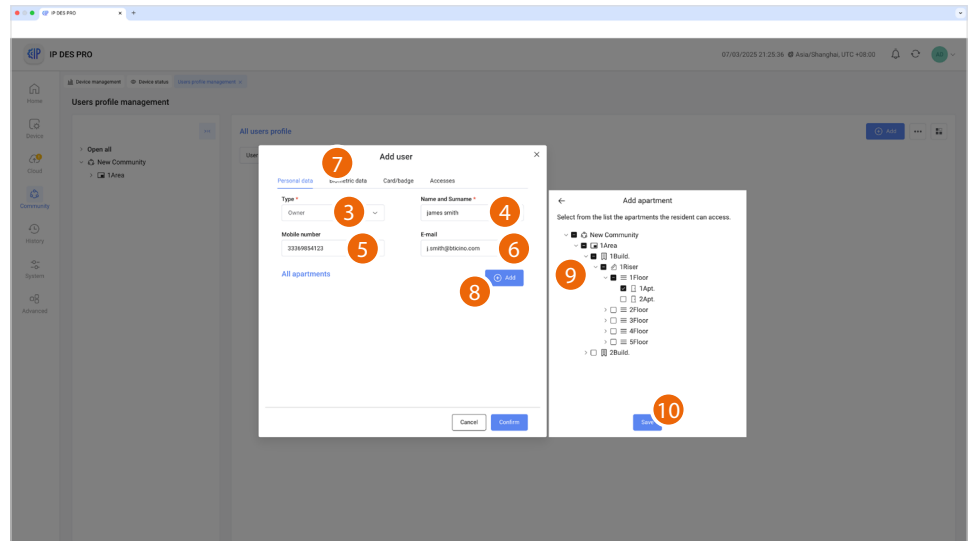
Now it is possible to add community people and give them permissions to access the structure. Depending on the type of person, different access permissions may be assigned, see [Person profile management](#).



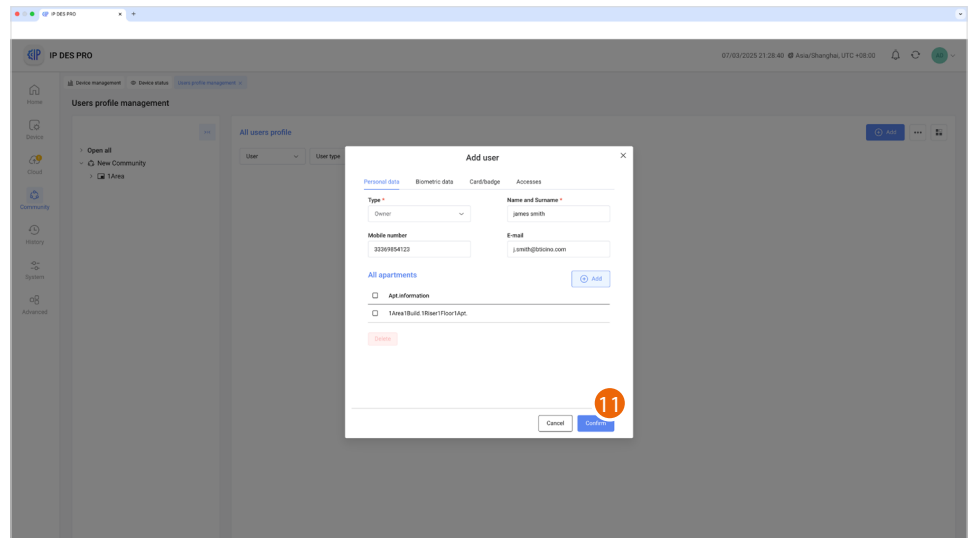
1. Select Community/Users profile management



2. Click to create a new person



3. Select the type of person
4. Enter the name and surname of the person
- NOTE:** some parameters may change depending on the type of person
5. Enter the telephone number of the person
6. Enter the email address of the person
7. [Register a fingerprint](#)
8. Now enter the relevant address of the apartment for the person
9. Select the relevant Area/Building/Riser/Floor/Apartment for the person
10. Click to add



11. Click to finish; the person can now access the community using the code and/or fingerprint reading. To use a badge/card to access the community, this must be registered; see [Access control card management](#)

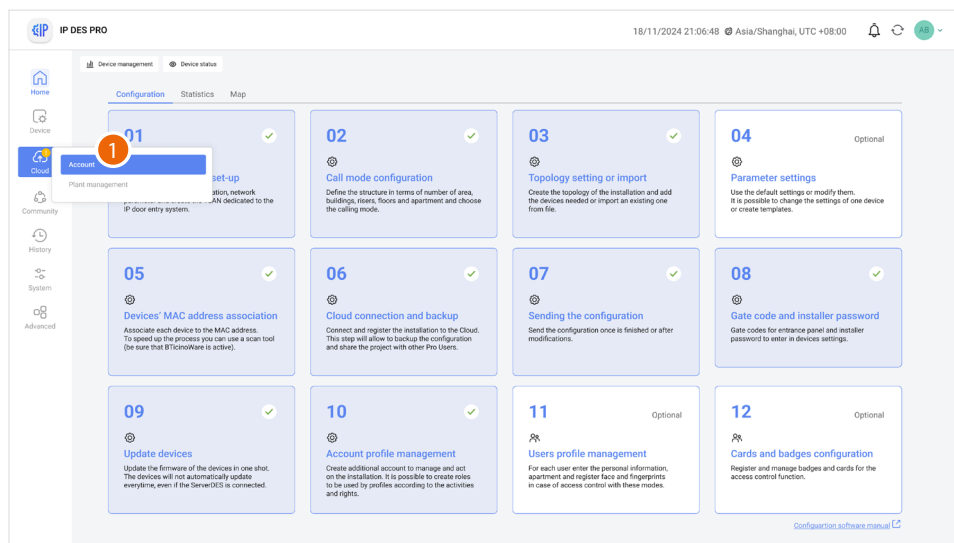


Registration of the community on the Installer's Cloud

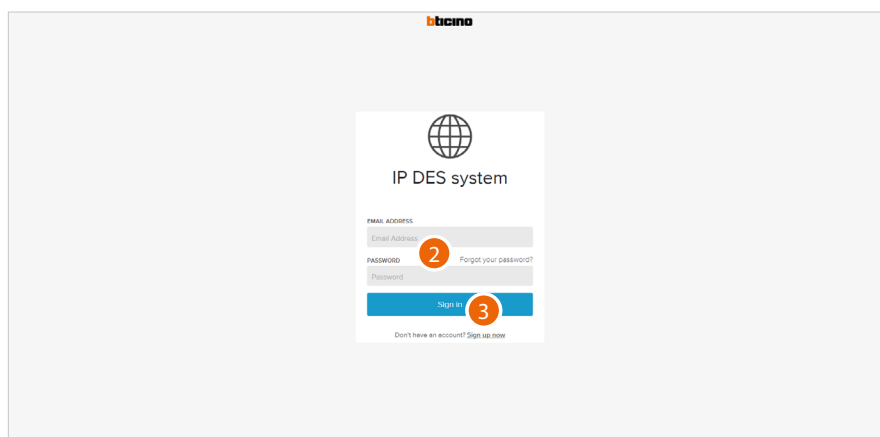
After completing the registration process and creating an Installer account, it is possible to save a copy of the Community on the Installer's Cloud.

Having a copy of the Community on the Installer's Cloud allows you to:

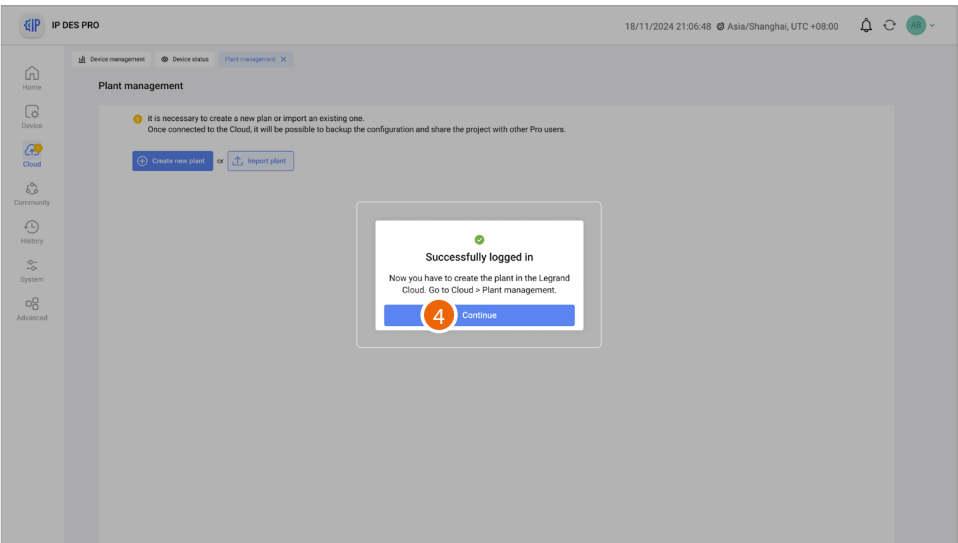
- have greater security in the event of local data loss
- associate the Home+Security app to the IU, for remote management of the video door entry system



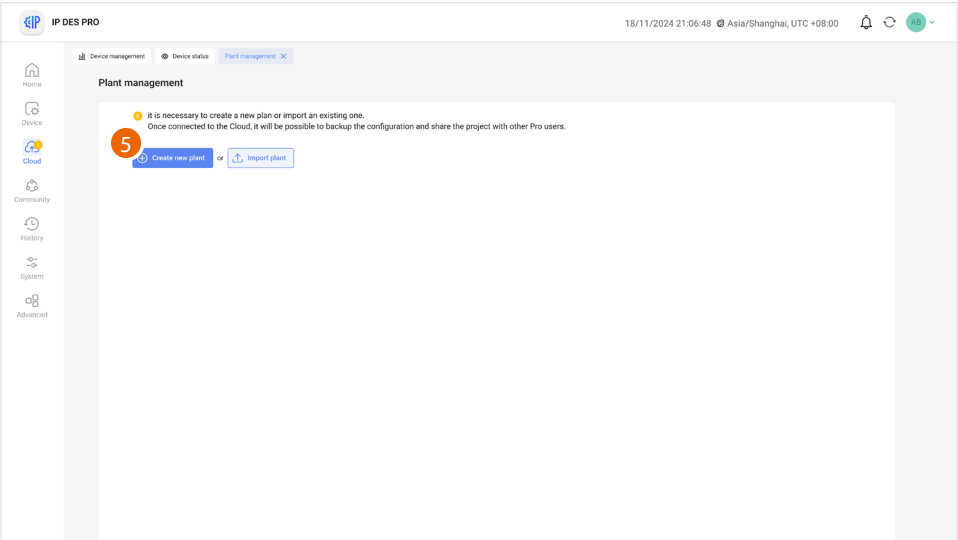
1. Click to complete the Installer's Cloud authentication process



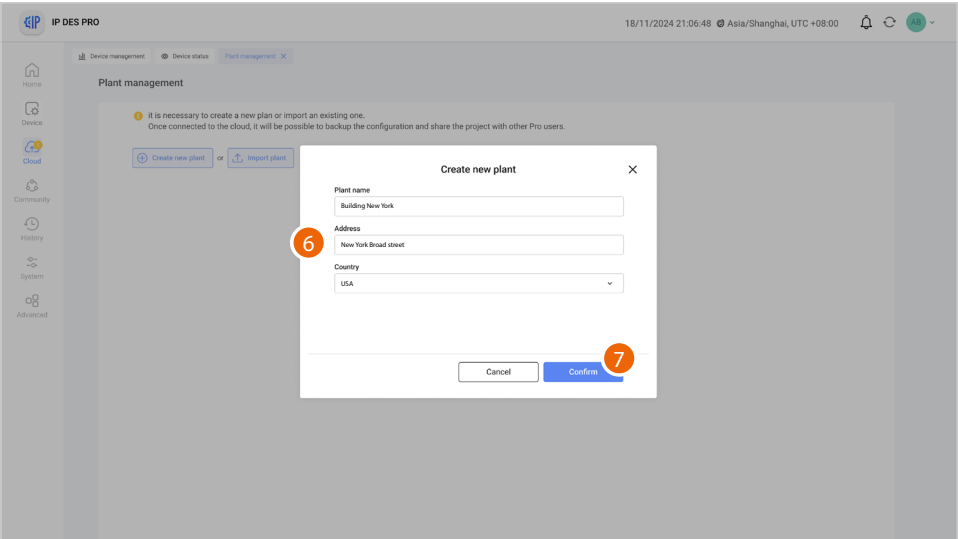
2. Enter email and password
3. Click to access



4. Click to confirm



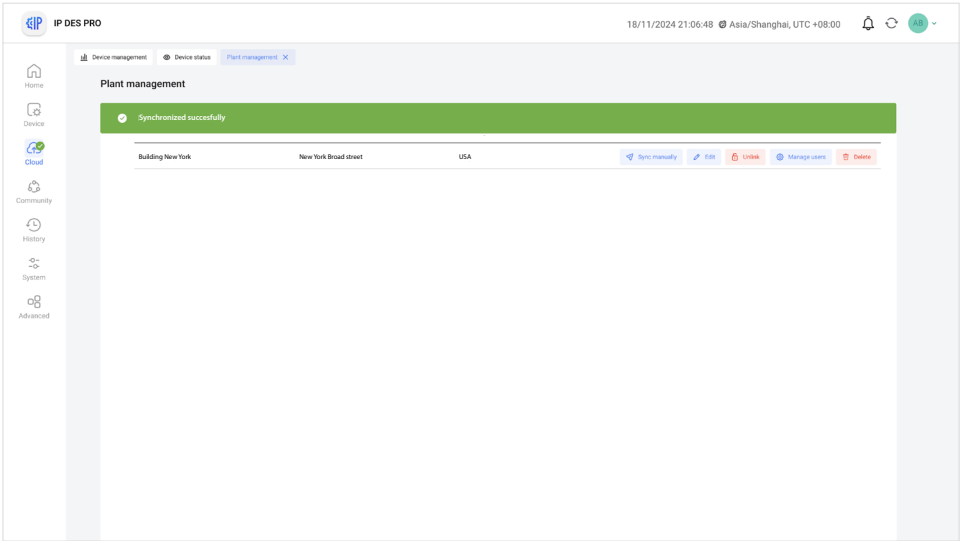
5. Click to create a new Plant



6. Enter the details of the Plant you are creating (name, address and country)

7. Click to save

The plant is automatically synchronised

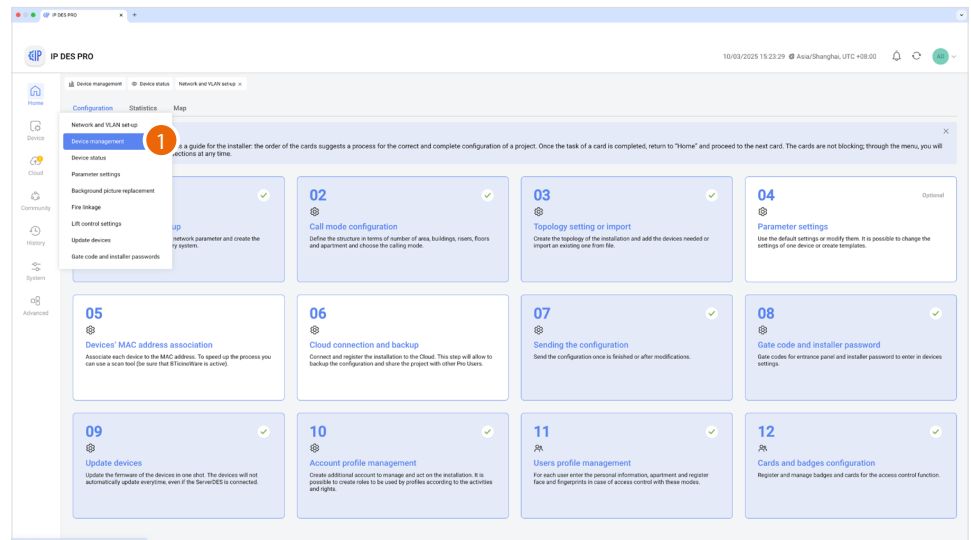


Once created, the plant remains available on the cloud.
If disconnected (unlink button), it can be retrieved from the cloud using the **Import a Plant**.
If **deleted**, it will also be deleted from the cloud.

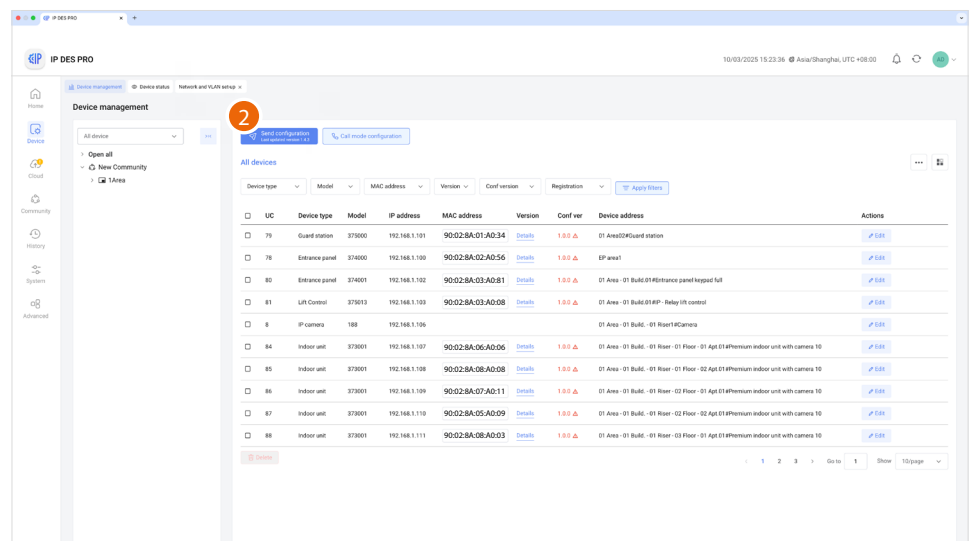


Send configuration to the DES Server

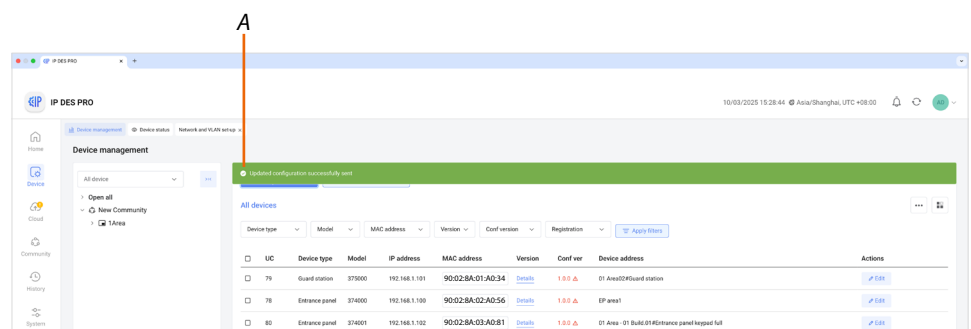
After creating the structure and configuring the virtual devices, it will be necessary to forward the configuration to the system, therefore “instructing” the system to use this configuration.



1. Select Device/Device management



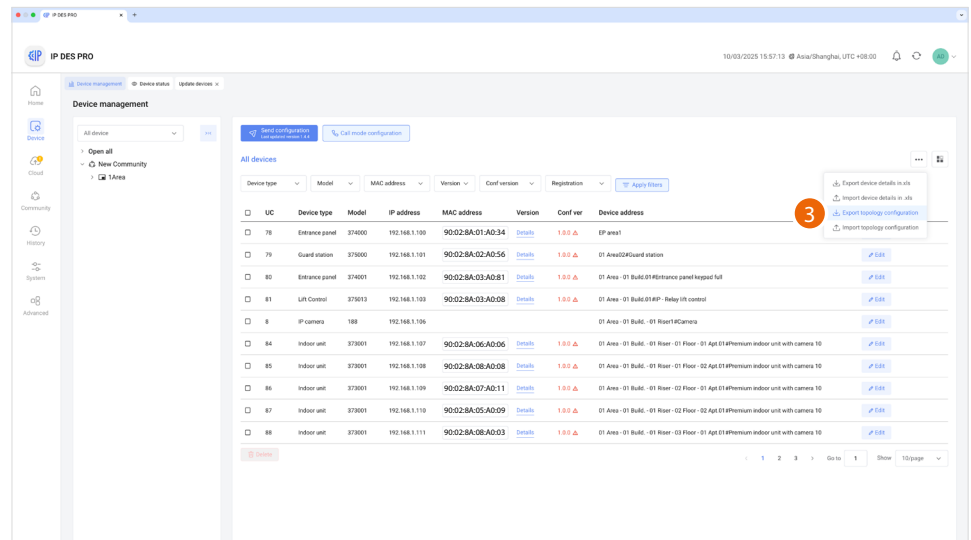
2. Click to send the configuration to the devices



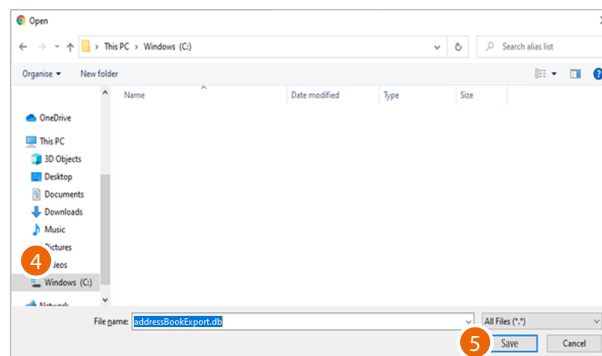
A A message indicates that the configuration has been sent correctly



The configuration is now saved in the DES Server. To avoid accidental loss, it is also possible to save it in an archive file.



3. Click to export the configuration to a file



1. Select the location where to save the file (.db)
2. Click to save

Saving of passwords

Installer passwords are generated automatically (with random digits) and uniquely for the two types of devices:

- entrance panels (with 6 digits)
- internal units and guard stations (with 4 digits).

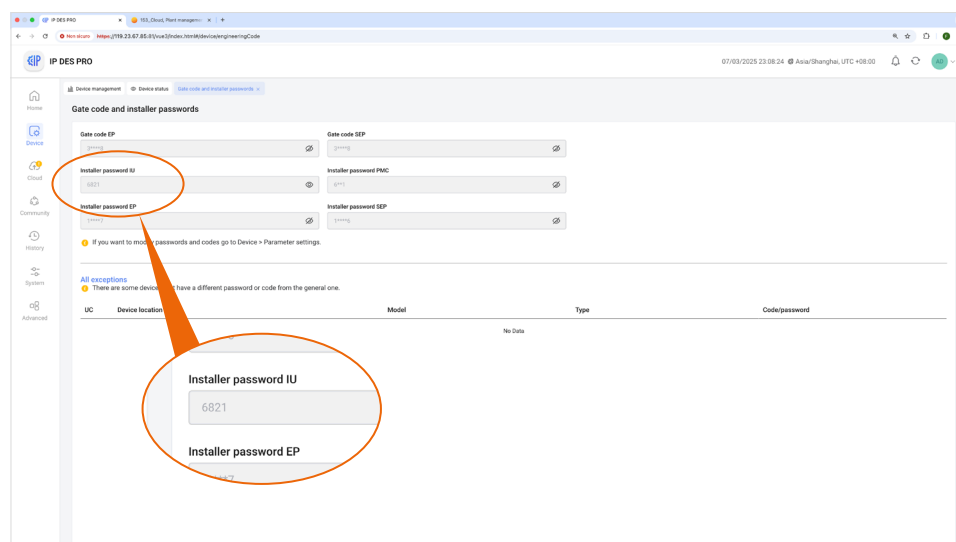
The access codes for opening the door locks of entrance panels are also generated in the same way.

For security reasons, it is recommended to save passwords in a safe place that is always accessible (Cloud backup activation recommended).

If both the SD and the backup are unavailable, it will not be possible to retrieve the passwords.

NOTE: The passwords of the devices incorrectly activated in DEMO mode are: 2000 (EP) and 1111 (IU and GS)

Make passwords visible; see **"Make passwords visible"**



1

INSTALLER PASSWORD

Internal units and guard stations

.....

INSTALLER PASSWORD

Entrance panels

.....

Door lock release code

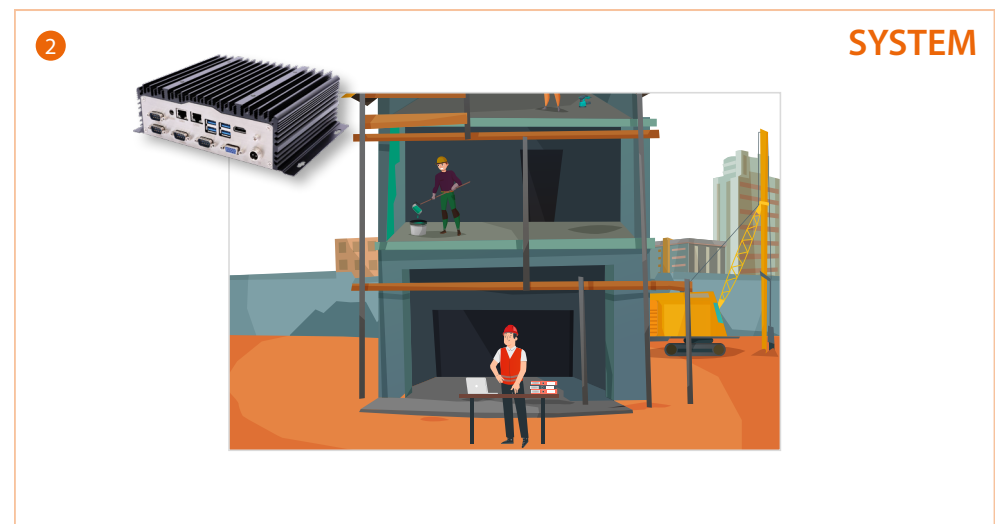
.....

1. Write down the passwords in a safe place that is always accessible.

Take the DES server back to system



1. Disconnect the SD from the office LAN network and take it to the on-site system



2. Reconnect the SD to the system LAN network

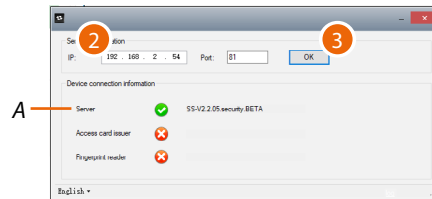


Setup of the fixed DES Server address on the system router



1. Run the BTicinoWare software (on the Windows Client PC) previously installed

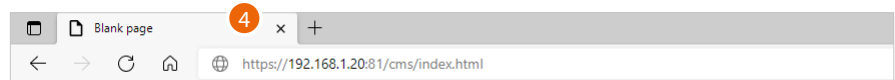
The following screen appears:



2. Enter the **SD address** and check that the port is 81

In order to guarantee correct system operation, the SD (which will take an address assigned by the system router) must maintain its IP address, see [Assigning a "privileged" network address to the SD](#).

3. Press to confirm and check that the flag A is green



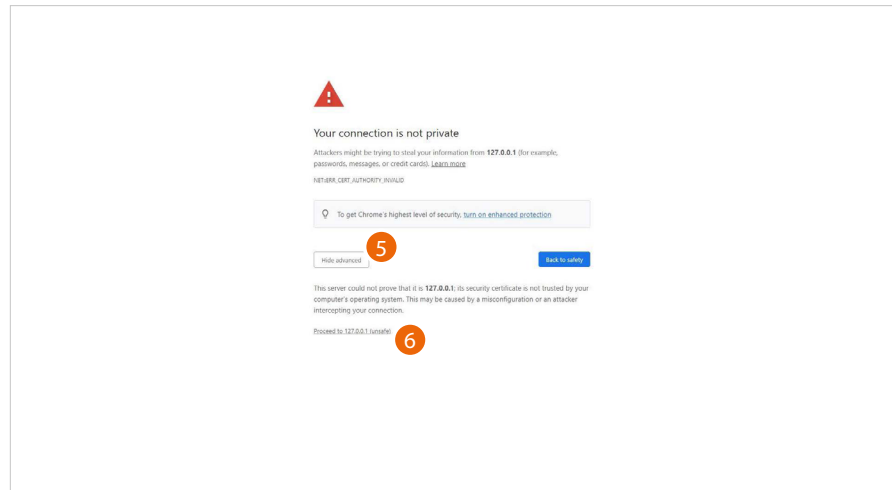
4. Open the browser and enter the http address of the SD:

https://IP or siteserver.local:81

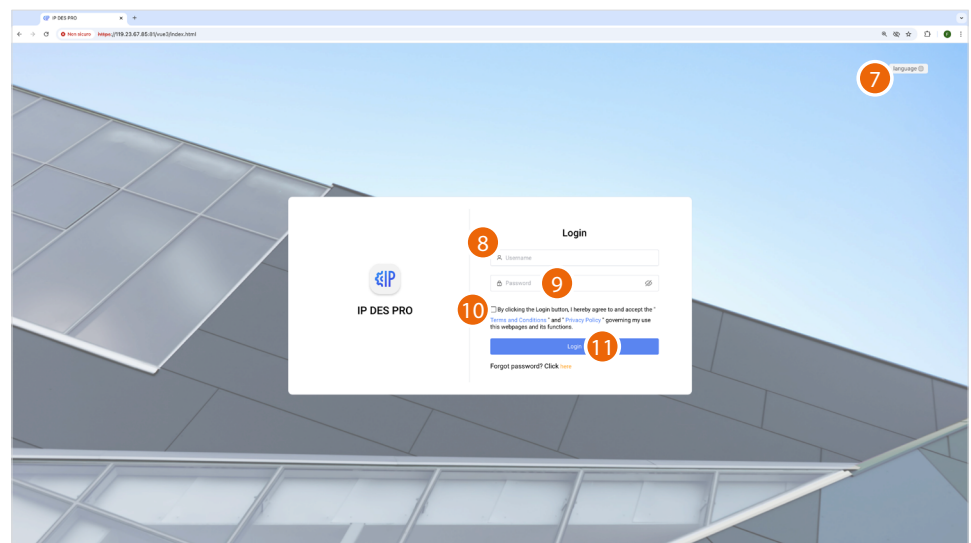
NOTE: use Chrome/Edge browser and a screen with resolution 1920x1080



In some cases, the browser may consider the page to be unsafe.



5. Click to display the advanced options
6. Click to ignore the warning and proceed



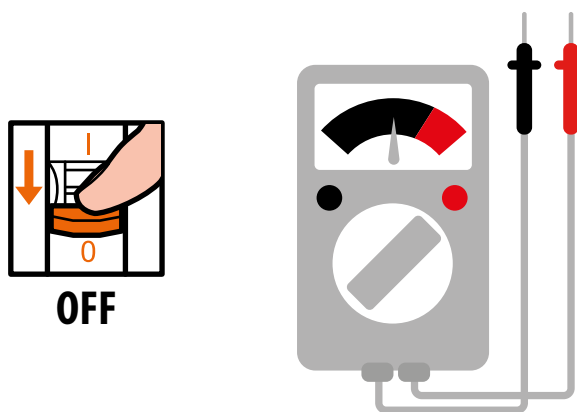
7. Select the interface language.
8. Enter the login name (default admin)
9. Enter the password (default 123456)
10. Accept the "Terms and Conditions" and "Privacy Policy" that govern your use of this website and its functions.
11. Click to confirm

NOTE: For safety reasons, it is mandatory to modify the default password.

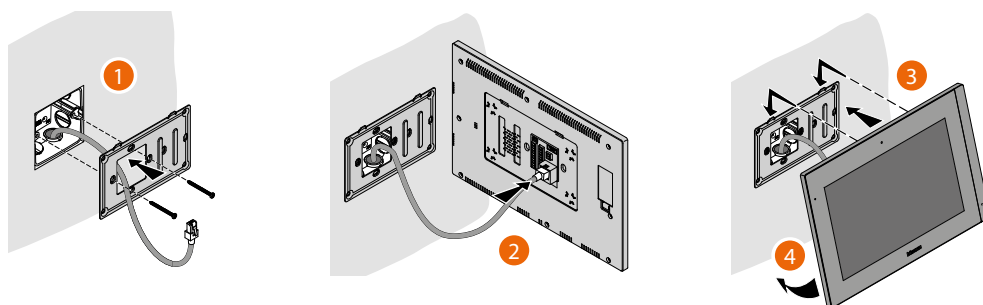
Installation of the devices

To transfer the configuration to the devices, these must be installed and powered

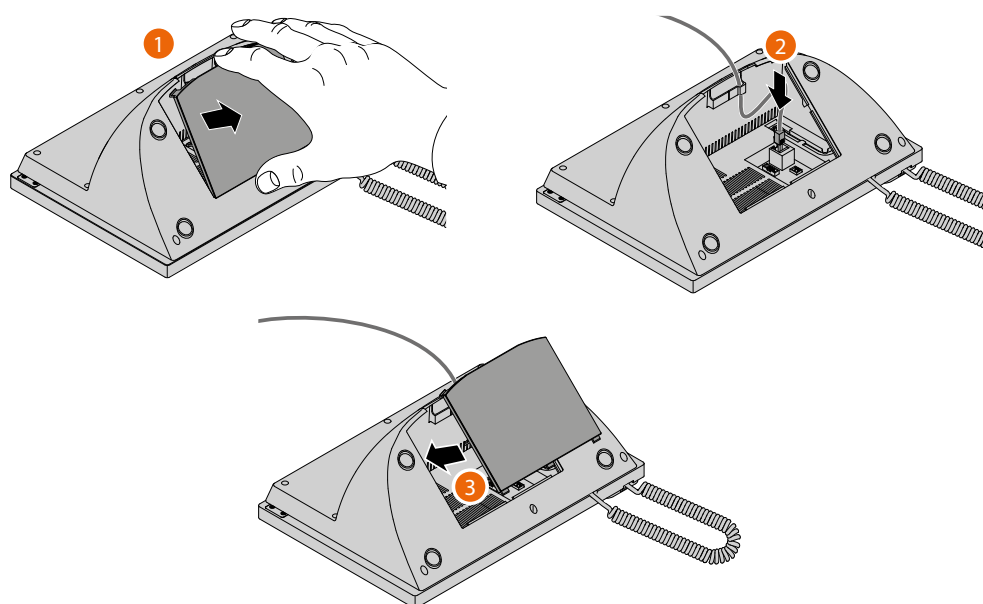
Switch off the power supply to the system and check that there is no voltage



Install the devices

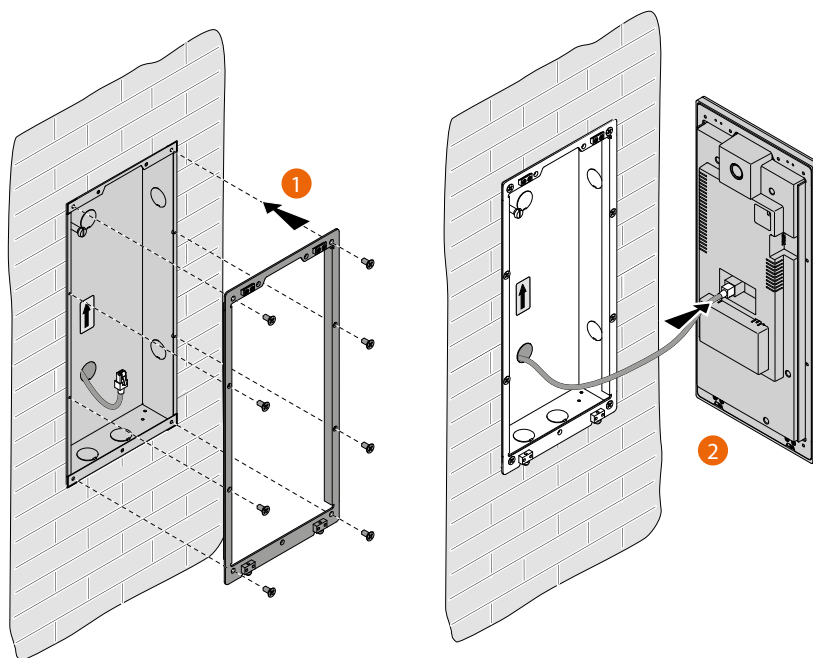
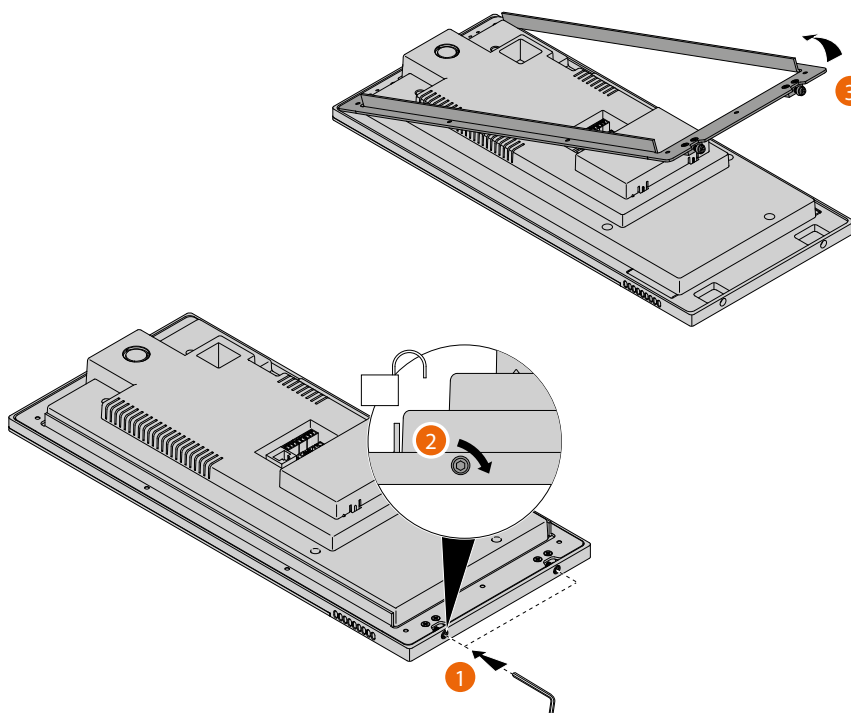


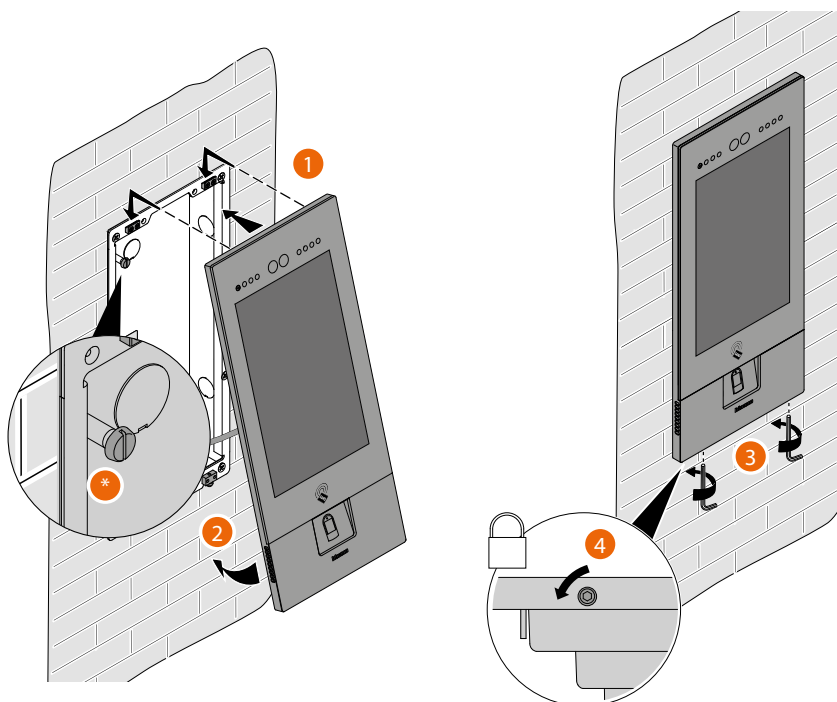
The RJ45 cable must be at least 200 mm long





The wrong wiring of the Ethernet cable connecting the device to the Poe Switch 375002 could damage the device itself.
The RJ45 cable must be at least 200 mm long.





- * Adjust the tamper screw so that it presses the tamper switch of the device and activates the anti-theft function in case of removal, by sending an alarm to the guard station.

Warning: the EP installation shown is representative of all EP.
For more details, see the specific instructions in the package

Reconnect the power supply

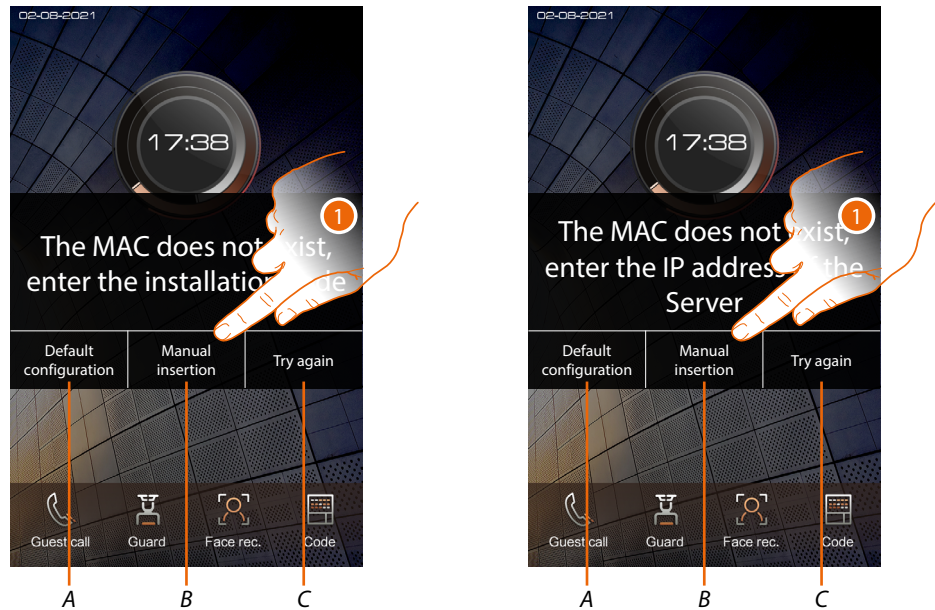


Activation of the devices

Thanks to the previously entered MAC address, once powered, the devices check that a configuration is available on the SD, and if so acquire it.

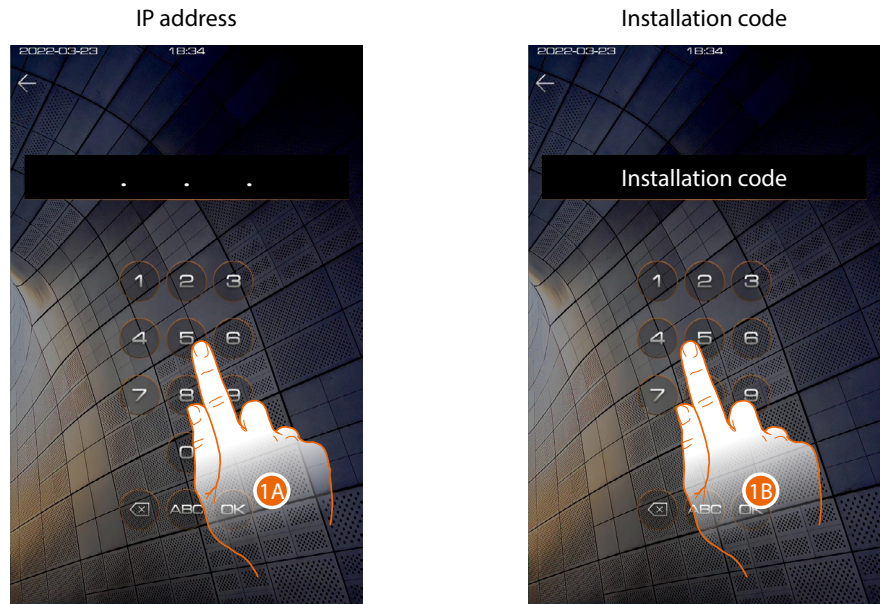
NOTE: devices that were already configured in the past must be reset. After rebooting, they will configure themselves

If the automatic activation of the device is unsuccessful, warning messages and manual activation modes may appear.



- A Not to be used
- B Button for the manual entry of the server IP address or installation code. By entering one of the two described parameters, it is possible to force the configuration of the device by putting it into forced communication with the server.
NOTE: to display the IP address, see Manage the community networks, to display the installation code, see Installation code
- C Button to test the activation of the device

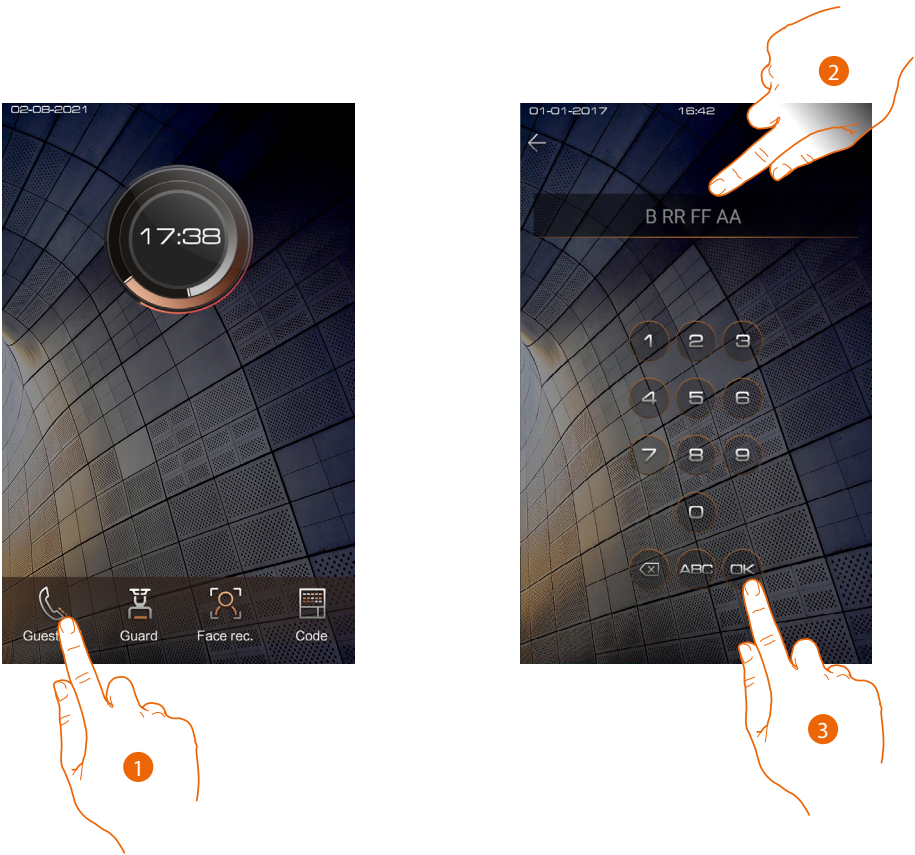
1. Click to manually enter the server IP address or the system access code IP address



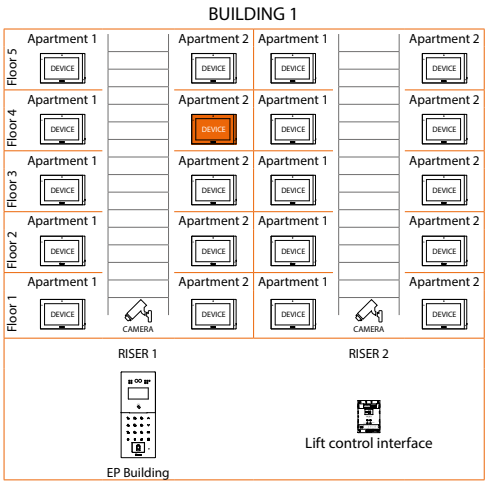
- 1A. Enter the IP address of the server
- 1B. Enter the installation code

System test

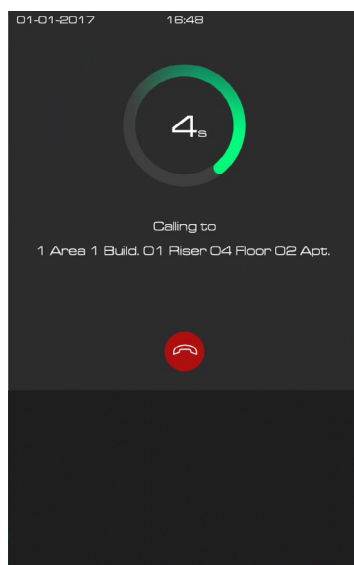
It is now possible to test the system, for example by making a call from the EP



1. Touch to make the call
2. Enter the IU address

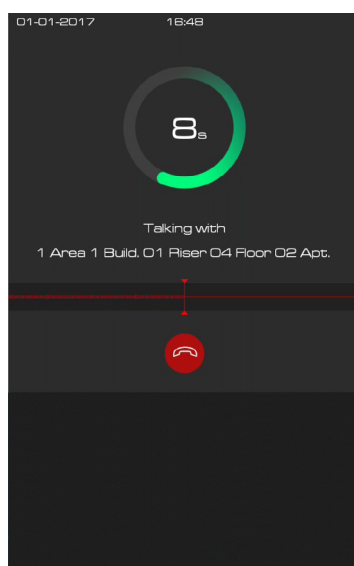


3. Touch to send the call

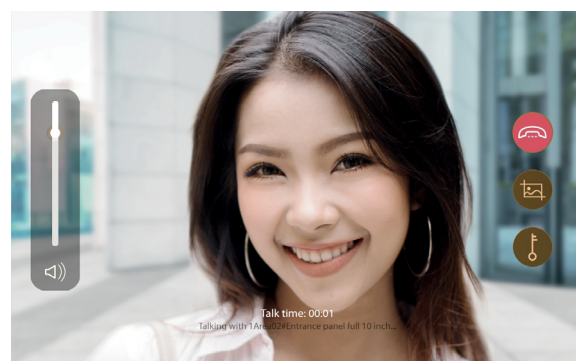


the call is in progress

4. Reply from the IU



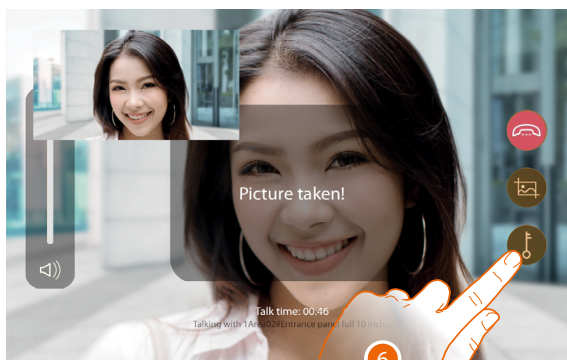
Test the audio signal on the EP



Test the audio/video signal on the IU

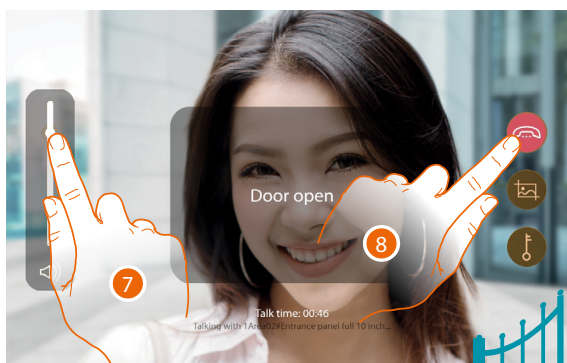


5. Touch to capture an image of the screen



A confirmation message appears.

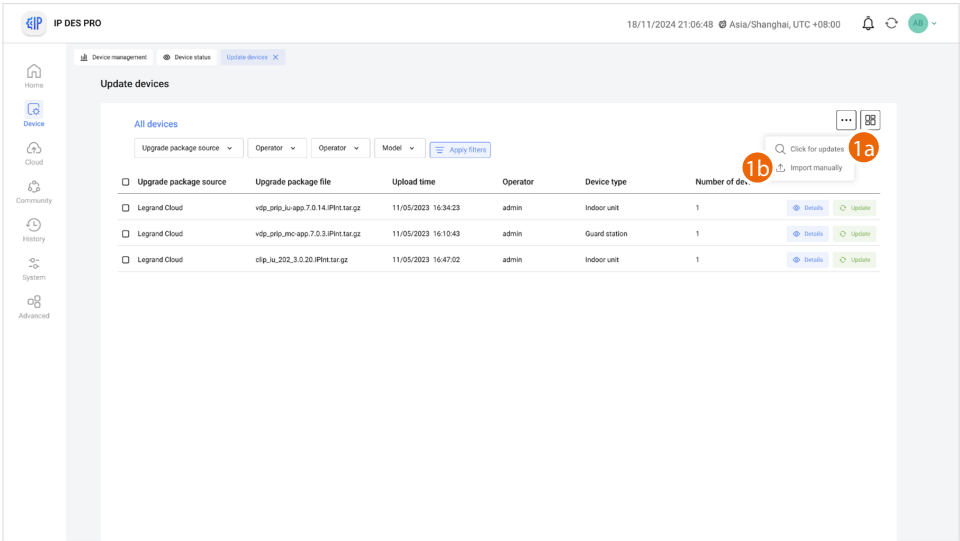
6. Touch to open the EP door lock



A confirmation message appears

7. Tap to adjust the volume
8. Touch to end the call

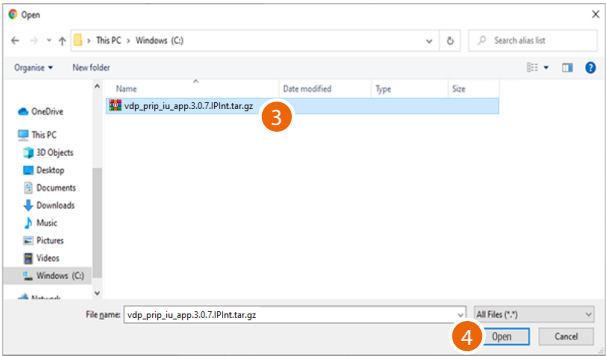
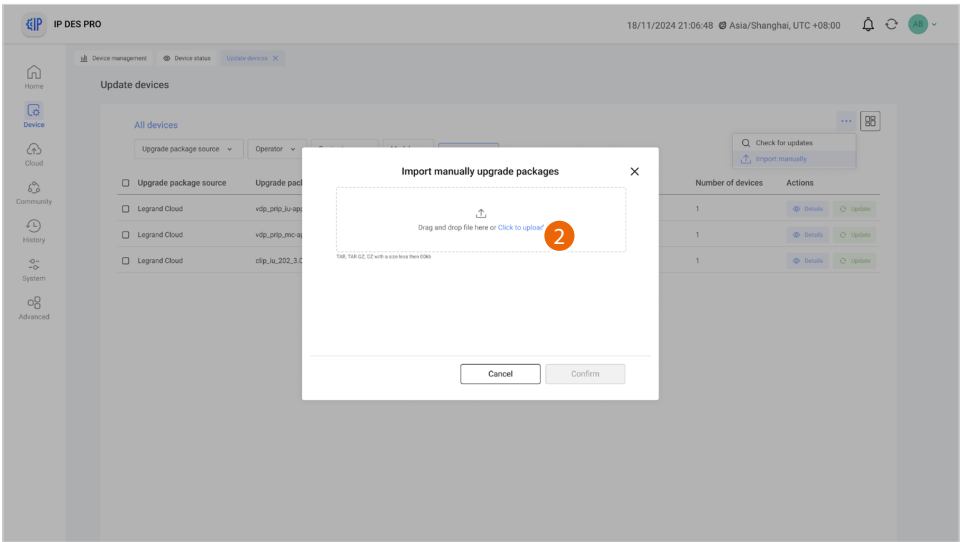
Update of the devices



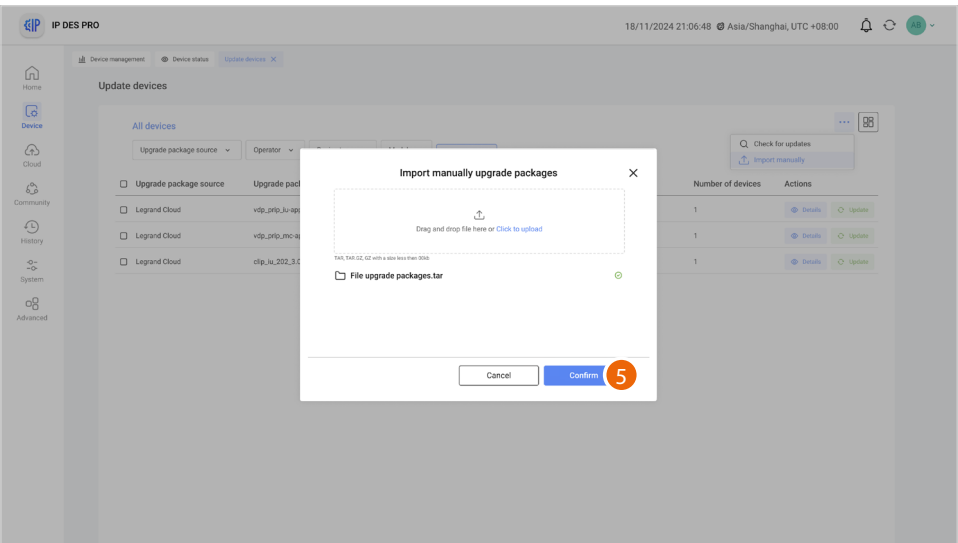
1a. Click to check for updates on the cloud. If there are updates, these will be downloaded and available for installation

or

1b. Click to import the update package from the local system (see item 2)

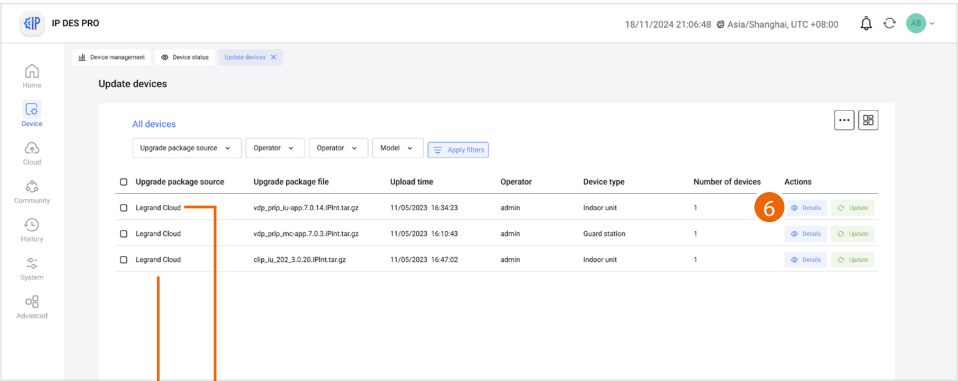


- 2. Click to select the update package
- 3. Select the .gz file
- 4. Click to continue



5. Click to confirm

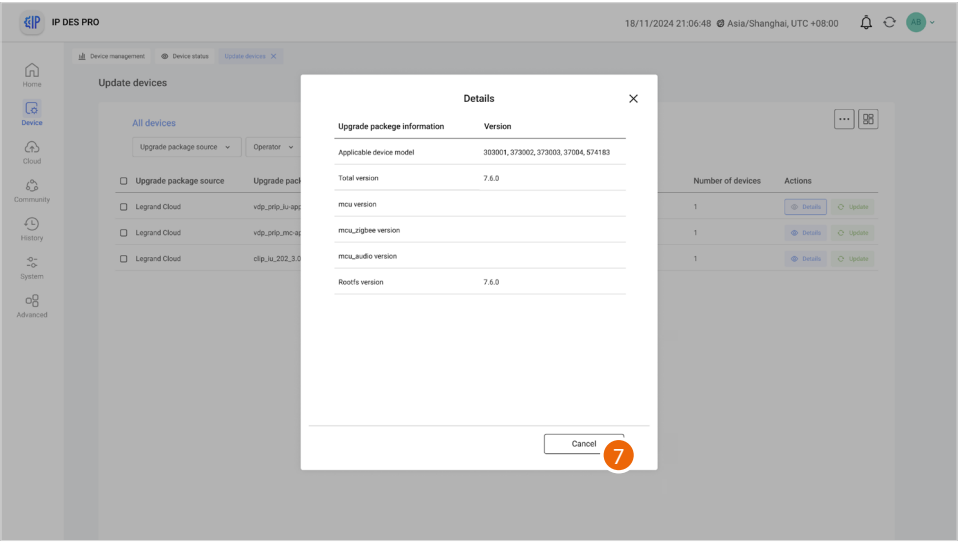
The package has been imported and is available to be sent to the devices



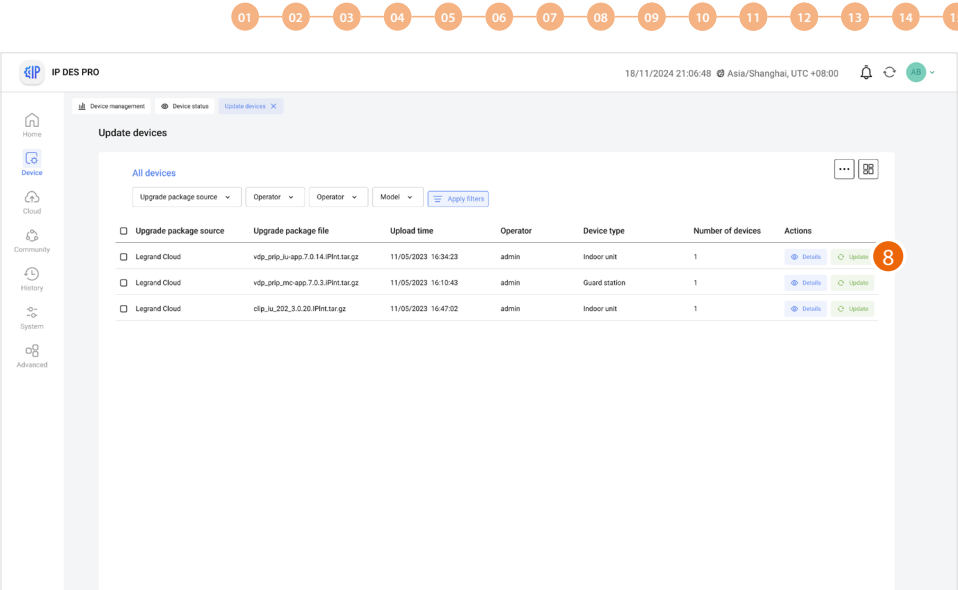
A Update package from Cloud

B Update package from local system

6. Click to see some of the update data



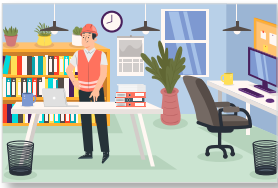
7. Click to close




8. Click to send the update to the plant

Project creation at the office and on-site server and system configuration

OFFICE



- Step **1** [Community VLAN network creation](#)
- Step **2** [Call mode setting and community structure definition](#)
- Step **3** [Community structure creation](#)
- Step **4** [Device MAC address registration](#)
- Step **5** [Community customisation](#)
- Step **6** [Registration of the Community on the Legrand Commercial Cloud](#)
- Step **7** [Send configuration to the DES Server](#)
- 8** [Saving of passwords](#)
- Step **9a**  [Notification to the system that the Plant has been saved to the cloud](#)

Oppure

- Step **9b**  [Send the configuration file to the system.](#)

- Step **10** [Connection of the DES Server on the system](#)
- Step **11** [Setup of the fixed DES Server address on the system router](#)

- Step **12a**  [Plant authentication and synchronisation on the cloud](#)

SYSTEM



Oppure

- Step **12b**  [Import the configuration file](#)

- Step **13** [Installation of the devices](#)

- Step **14** [Activation of the devices](#)

- Step **15** [System test](#)

- Step **16** [Update of the devices](#)



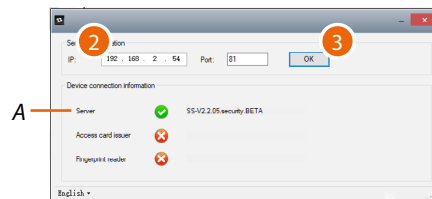
Community VLAN network creation

To configure the community network, it will first be necessary to configure the system by following the steps below:



1. Run the BTicinoWare software (on the Windows Client PC) previously installed

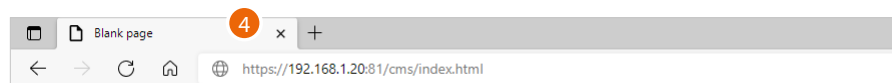
The following screen appears:



2. Enter the **SD address** and check that the port is 81

In order to guarantee correct system operation, the SD (which will take an address assigned by the system router) must maintain its IP address, see [Assigning a "privileged" network address to the SD](#).

3. Press to confirm and check that the flag A is green



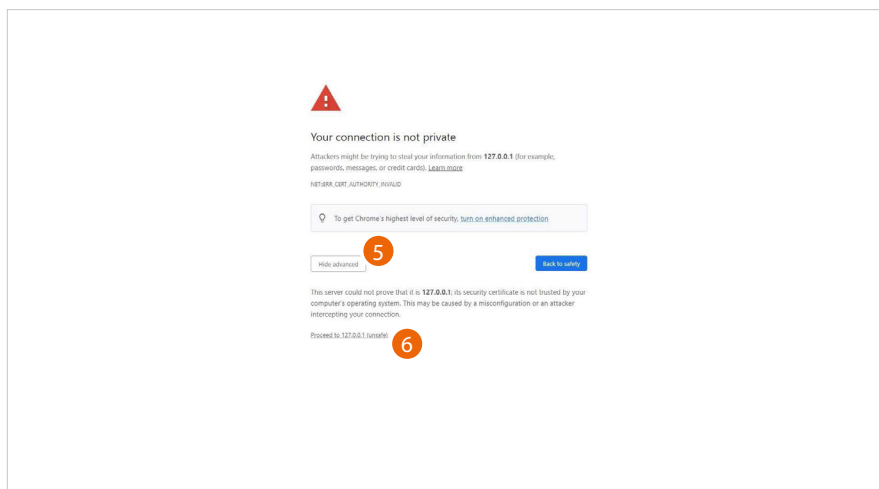
4. Open the browser and enter the http address of the SD:

<https://IP> or siteserver.local:81

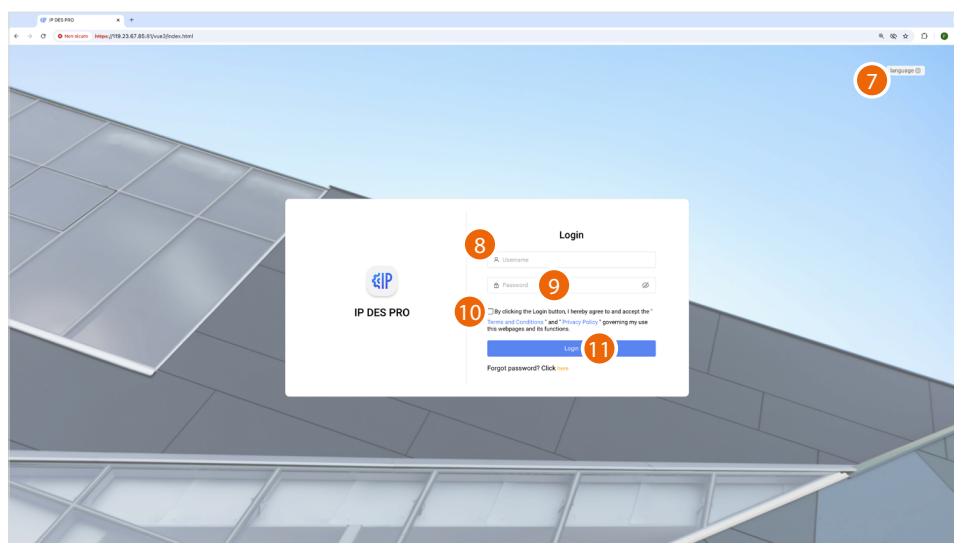
NOTE: use Chrome/Edge browser and a screen with resolution 1920x1080



In some cases, the browser may consider the page to be unsafe.

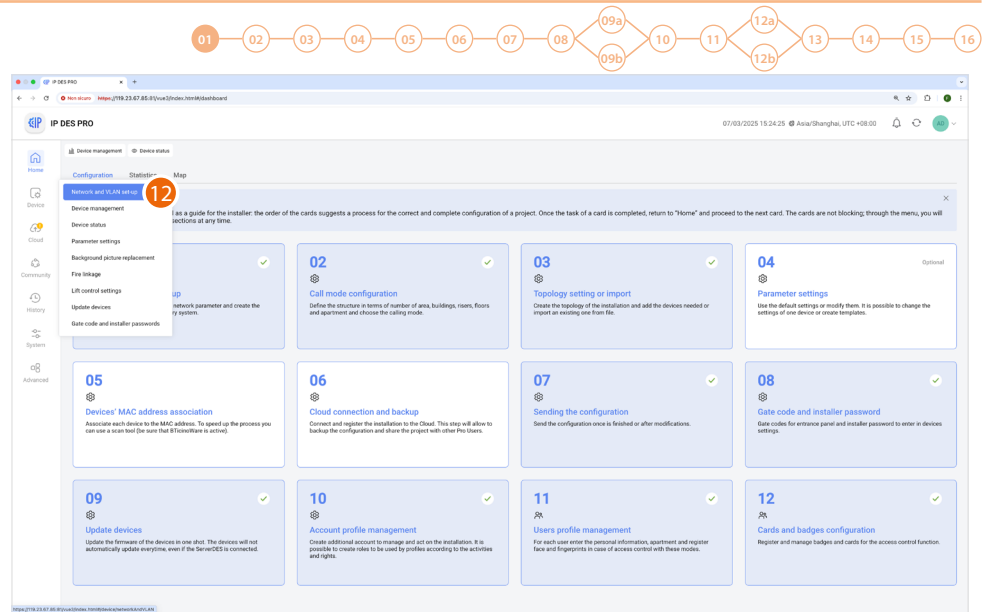


5. Click to display the advanced options
6. Click to ignore the warning and proceed

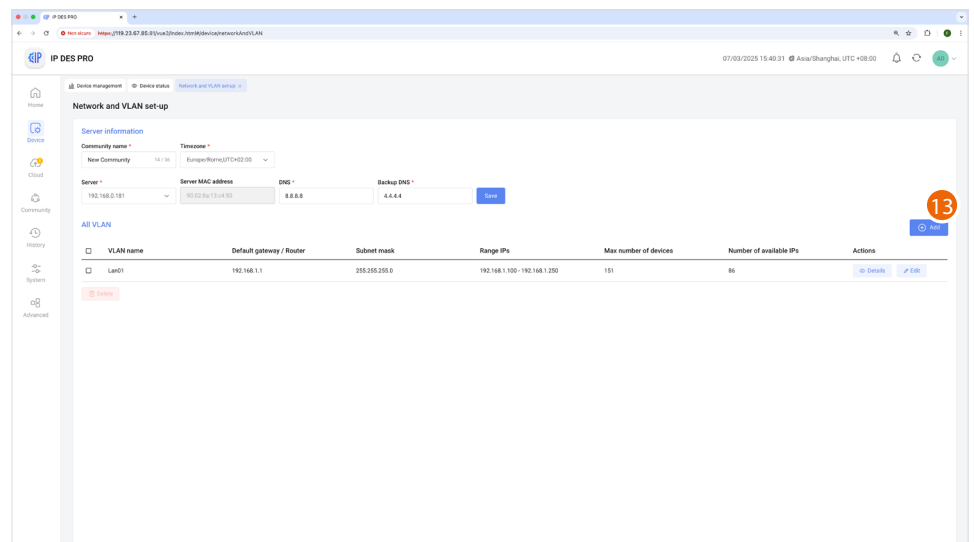


7. Select the interface language.
8. Enter the login name (default admin)
9. Enter the password (default 123456)
10. Accept the "Terms and Conditions" and "Privacy Policy" that govern your use of this website and its functions.
11. Click to confirm

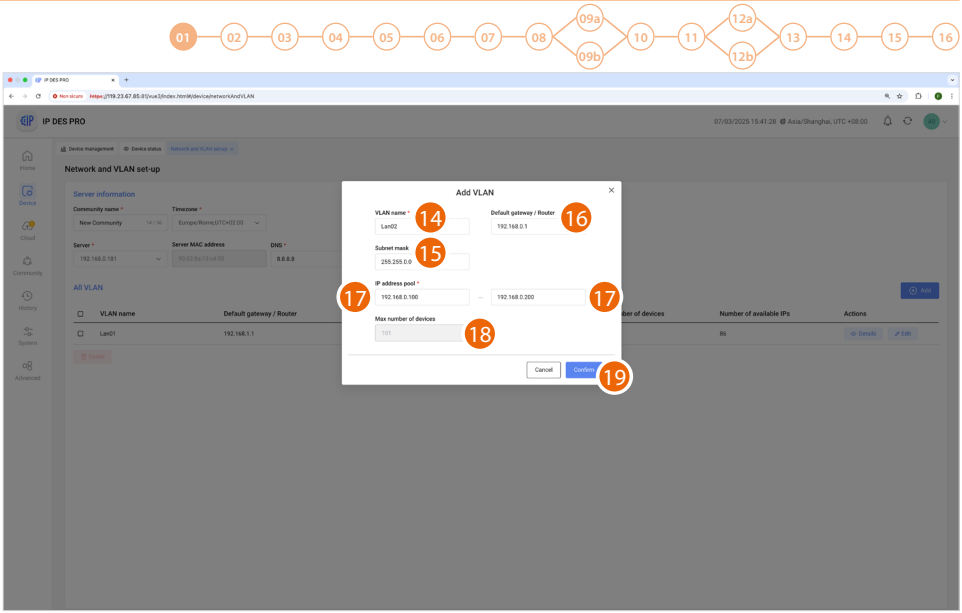
NOTE: For safety reasons, it is mandatory to modify the default password.



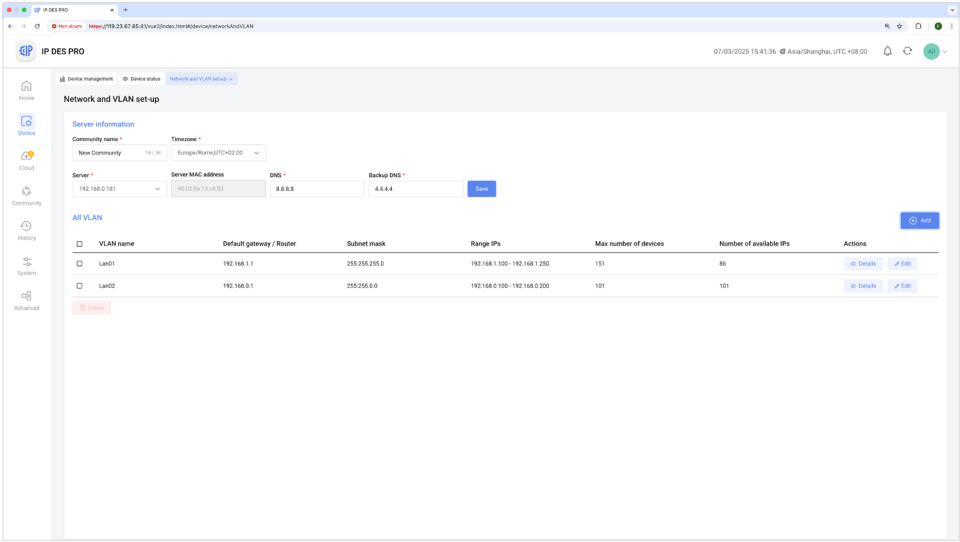
12. Click to open the section where it is possible to create your new community VLAN network



13. Click to create the community VLAN network



- 14. Enter the name of the community VLAN network (letters and numbers without space)
- 15. Enter the Subnet mask address
- 16. Enter the fixed IP address of the SD given to you by the network administrator
- 17. Enter the starting and ending IP addresses that will determine the maximum number of devices that can be installed on the network.
- 18. It displays the maximum number of IP devices that can be installed based on the previously entered data
- 19. Click to confirm



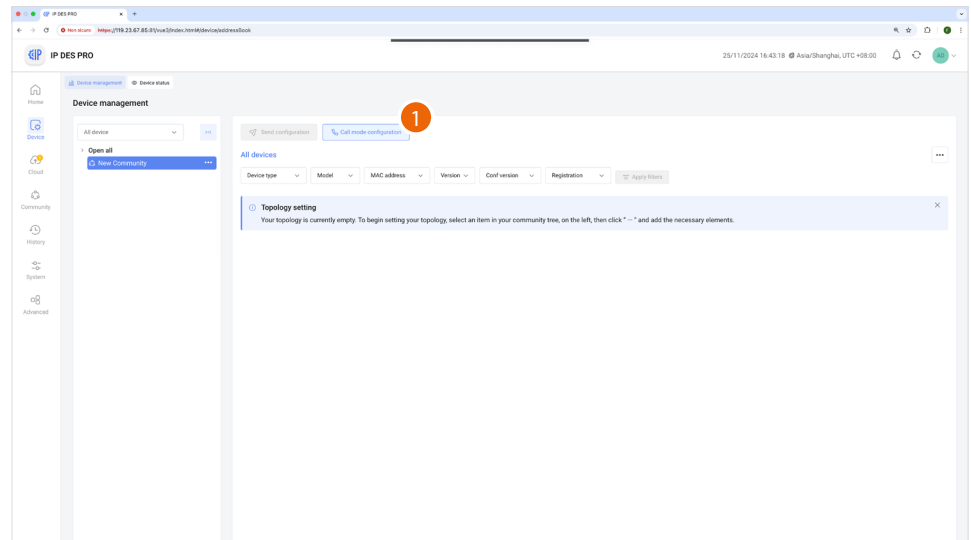
The community VLAN network has been created



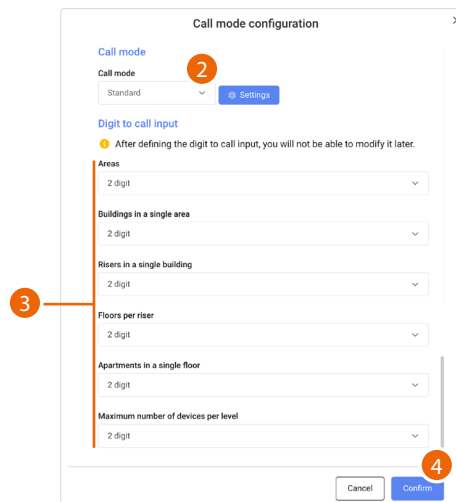
Call mode setting and community structure definition

It is now necessary to define parameters like number of Areas, Buildings, Risers and so on, as well as other parameters that will define the structure of the Community.

In this section, it is also necessary to define the type of call that will be used for all Community calls.



1. Click to open the page



2. Select the **call mode** and configure the relevant parameters
3. Set the number of digits to be used for each call sector (Area/Building/Riser/Floor/Apartment)
ATTENTION: After setting these parameters for the first time, it will no longer be possible to change them.
In order to change these parameters, restore the factory settings
4. Touch to confirm

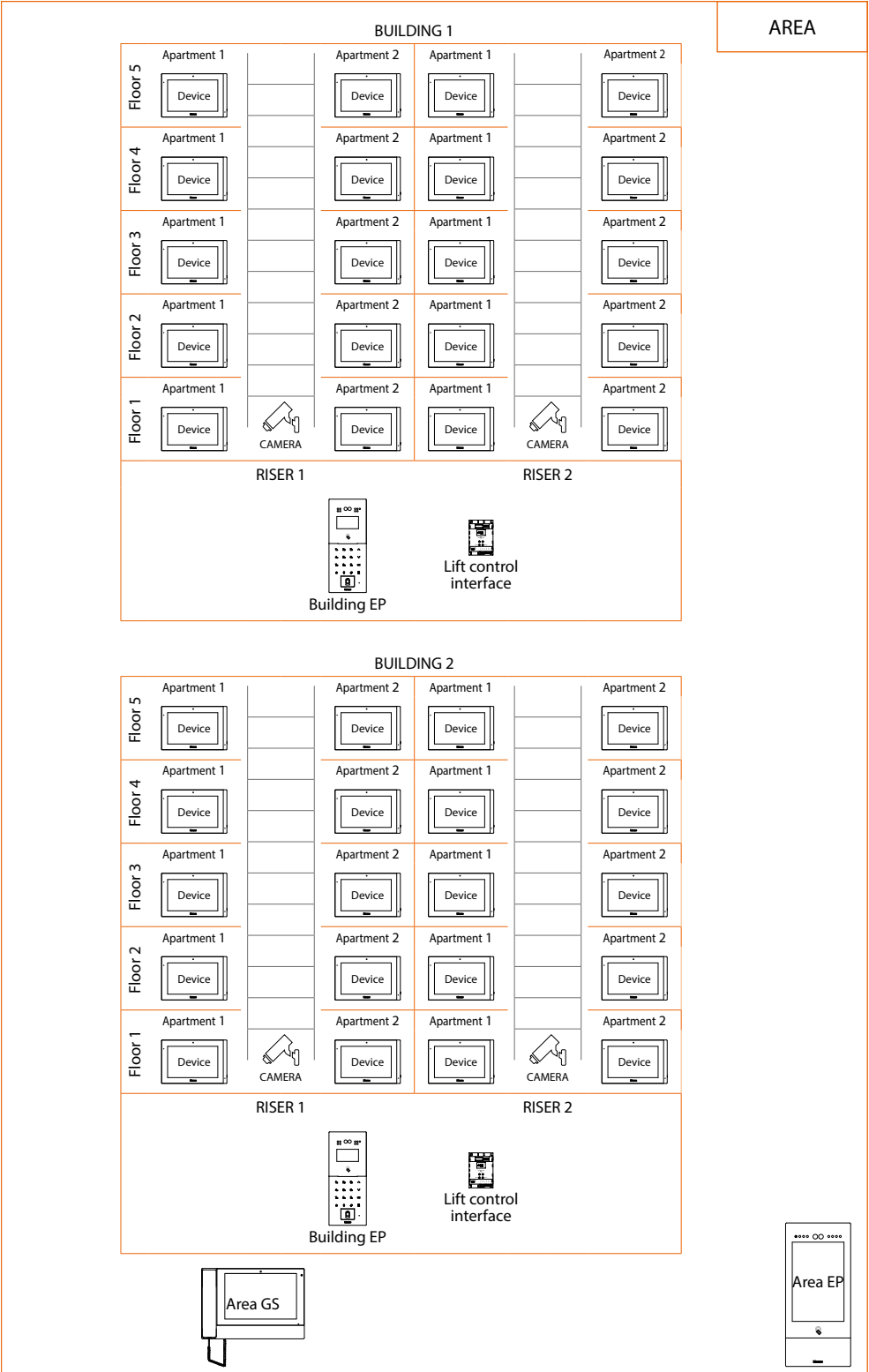


Community structure creation

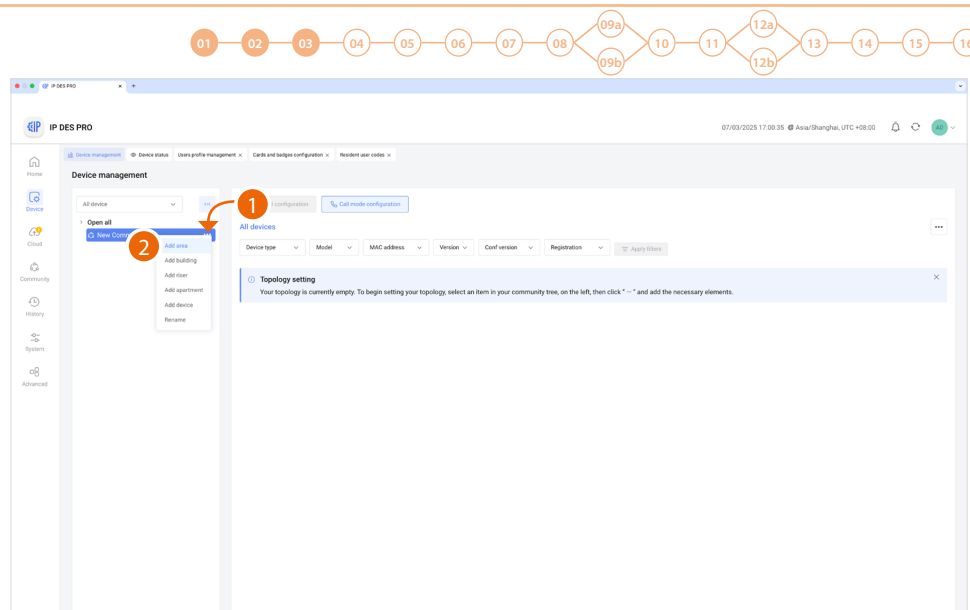
Depending on how your Community is composed, you will need to hierarchically enter:



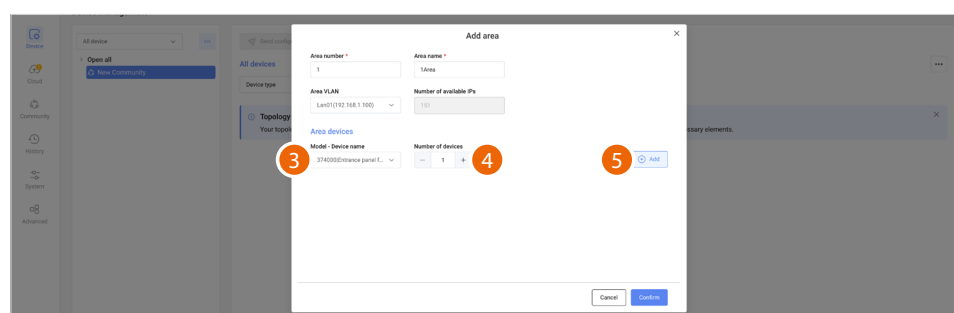
This document will show the creation of a sample structure composed as follows:



Caution: The configuration operations illustrated below are those required to create the example structure.



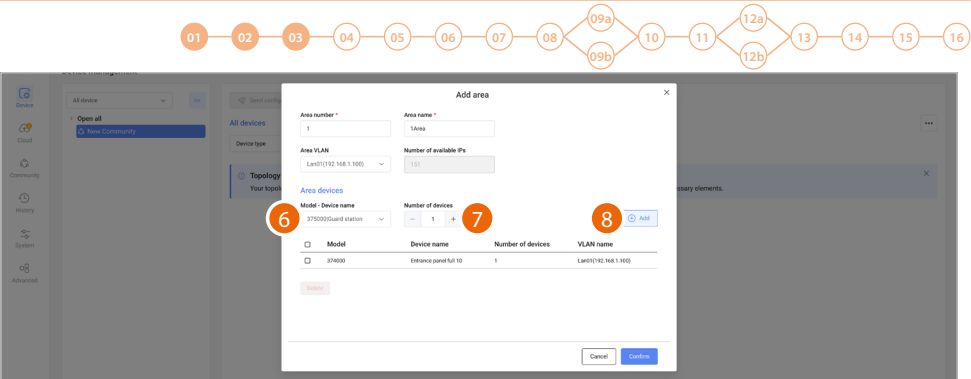
1. Click the Community to open the context menu, a drop-down menu will appear with the commands for its configuration
2. Click to add a new Area



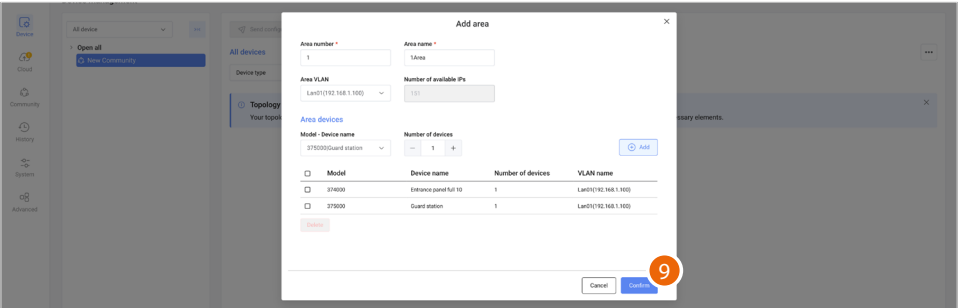
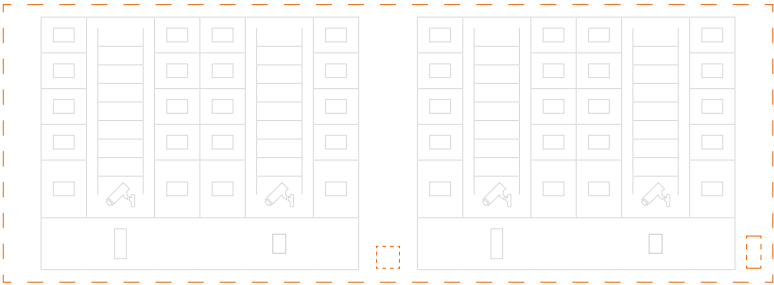
3. Select the area device (Area EP)*
4. Select the quantity
5. Click to add

***NOTE:** Before proceeding with the addition of the devices, remember to check that all the device parameters comply with the requirements, see [Configuration Parameters](#)

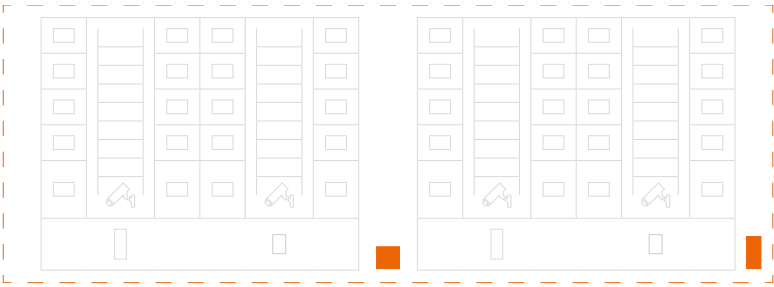


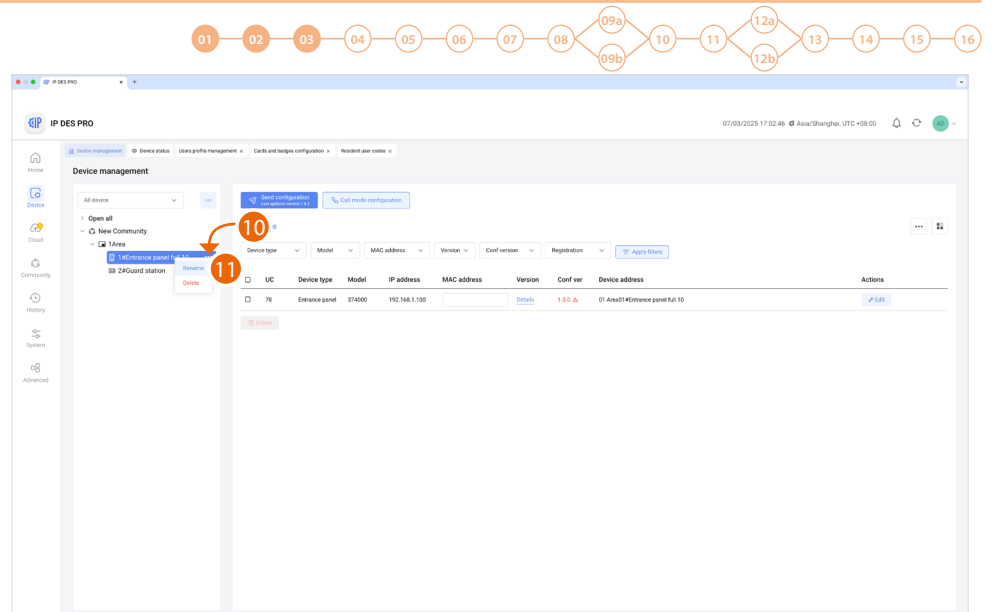


6. Select the second area device (Area GS)
7. Select the quantity
8. Click to add



9. Click to confirm

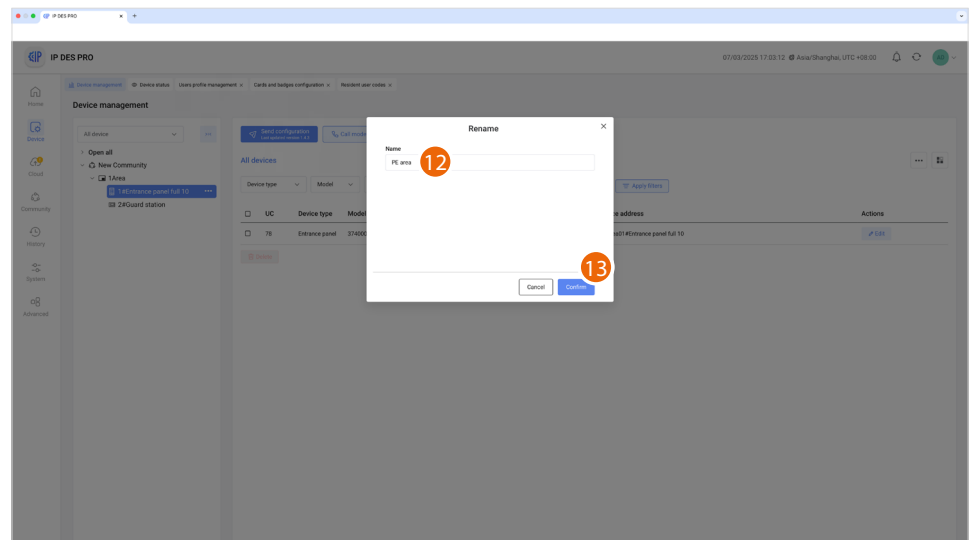




After inserting the devices, you will be able to customize their name

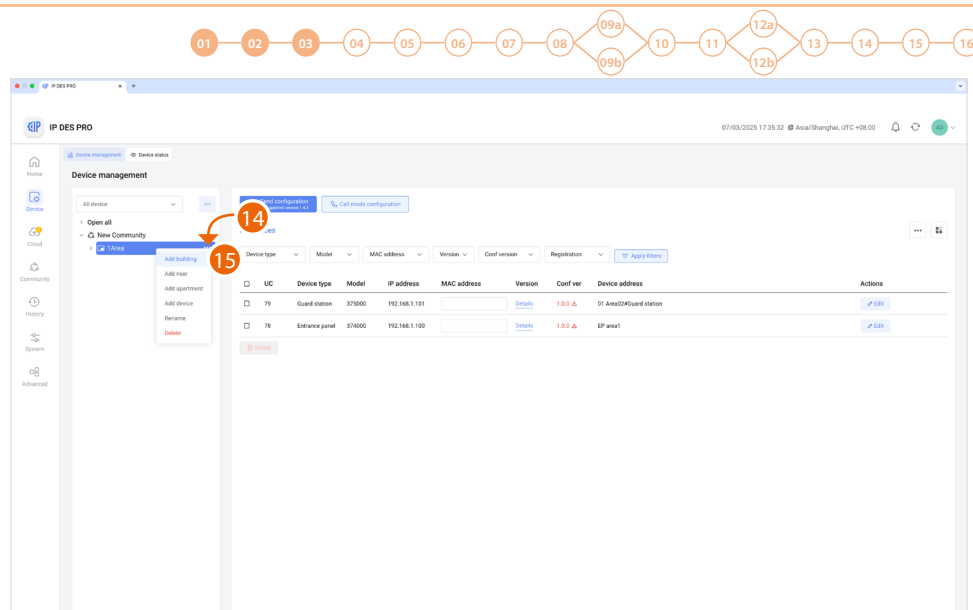
10. With the right mouse button click the device that you want to rename: a drop-down menu will appear

11. Click to open the edit window



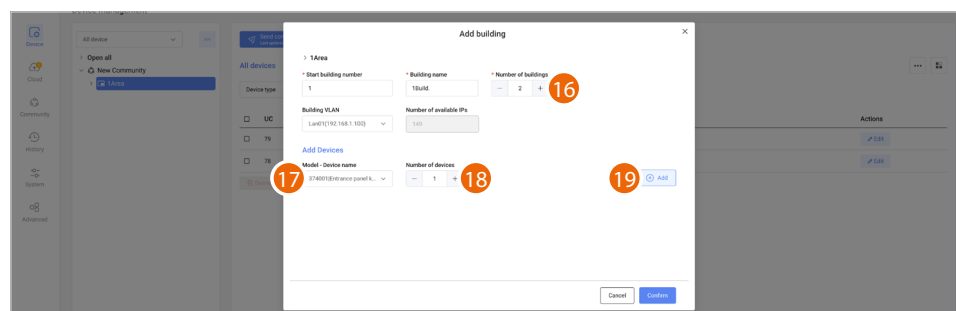
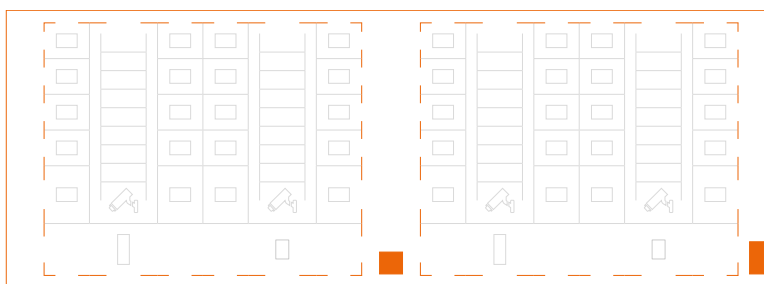
12. Enter the new name

13. Click to confirm



14. Click the Area with the right mouse button. This will open a drop-down menu

15. Click to add the **Buildings**



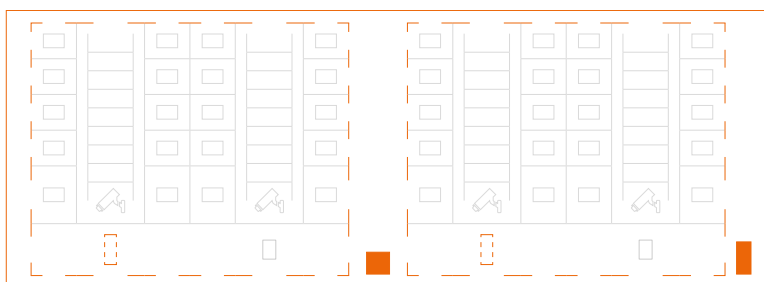
16. Select the number of Buildings to add

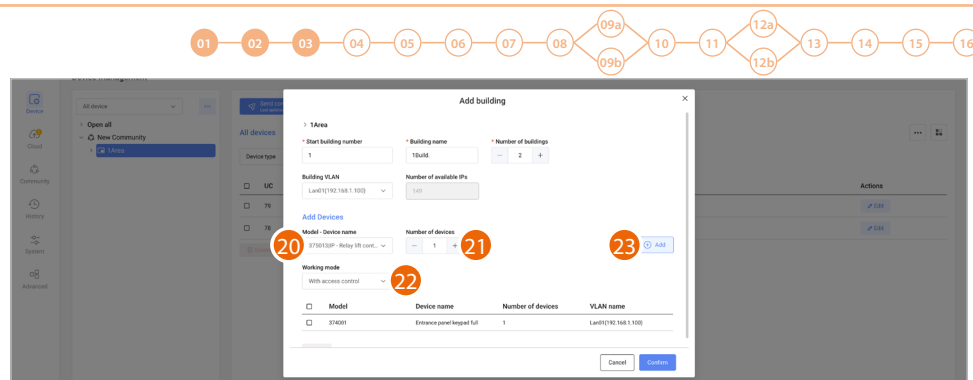
17. Select the Building device (Building EP)

NOTE: the software automatically applies a filter to only show devices that are consistent with the component that you are adding

18. Select the quantity

19. Click to add





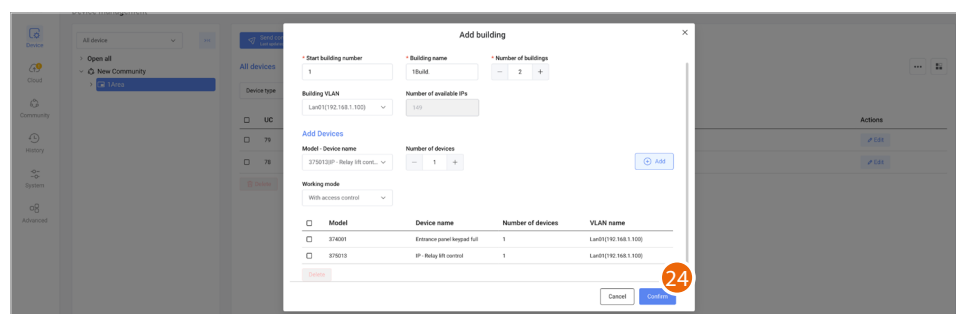
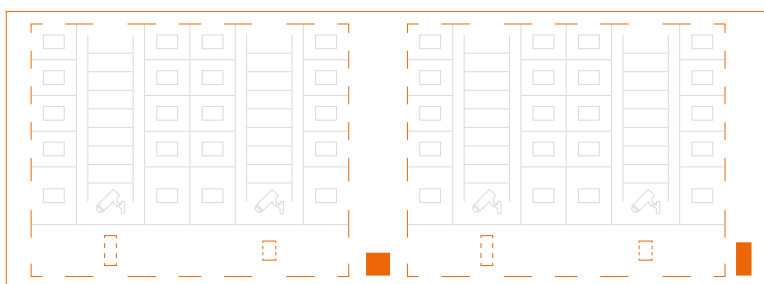
20. Select the device to add (lift control interface with relay 375013)

21. Select the quantity

22. Select the operating mode:

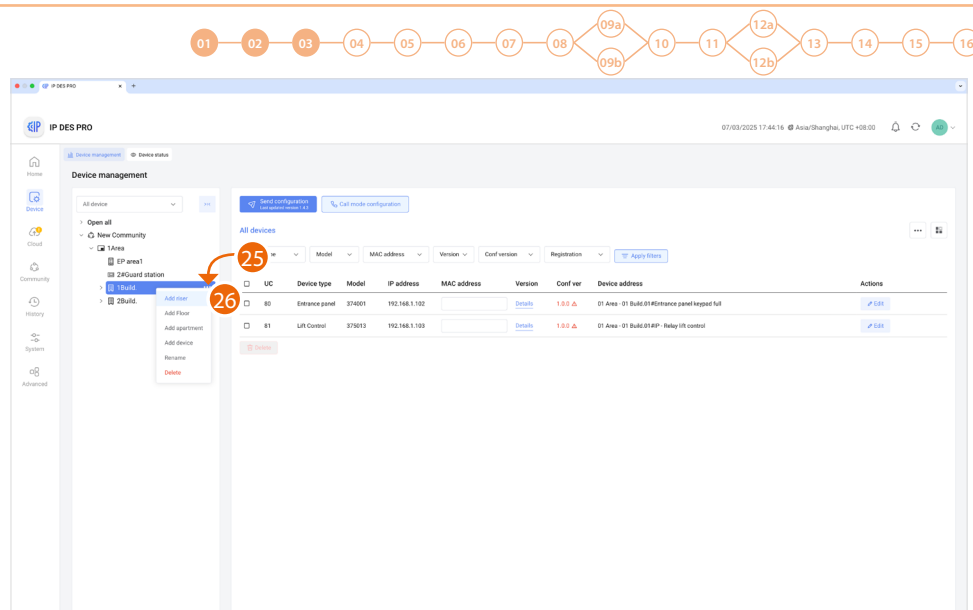
- **with access control:** this mode allows to set up an exclusive call to a specific floor (e.g. only go to the third floor)
- **ground floor call:** this mode allows to set the system so that the lift is sent to the floor of the caller.

23. Click to add



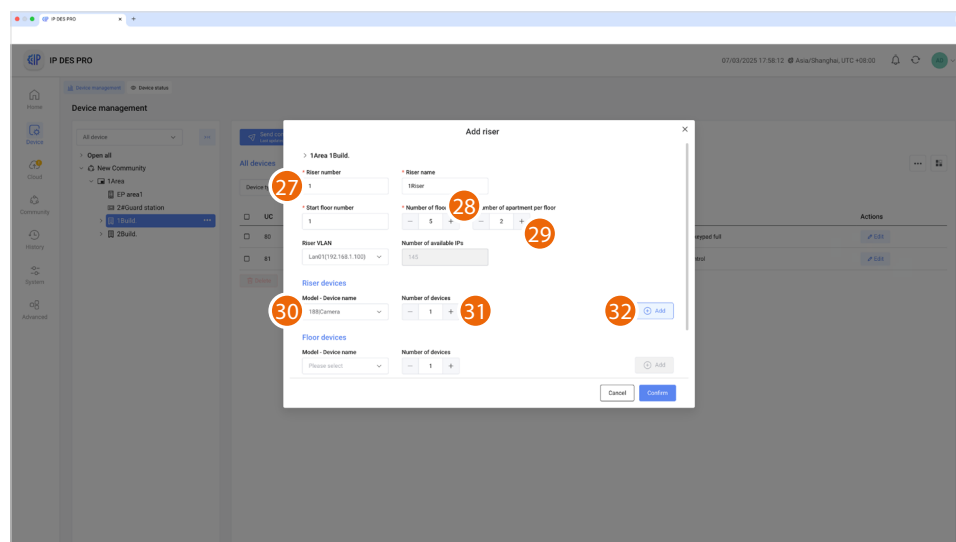
24. Click to confirm





25. Click the Building with the right mouse button. This will open a drop-down menu

26. Click to add a new Riser



27. Enter the progressive Riser number

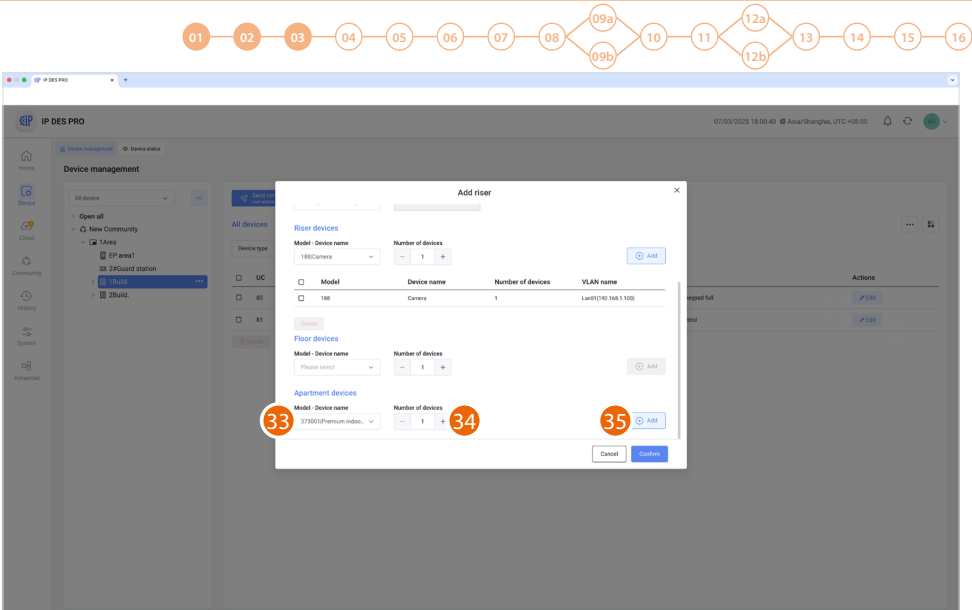
28. Select the Building Floor number (5)

29. Select the number of Apartments for each Floor (2)

30. Select the OnVif IP Camera

31. Select the quantity

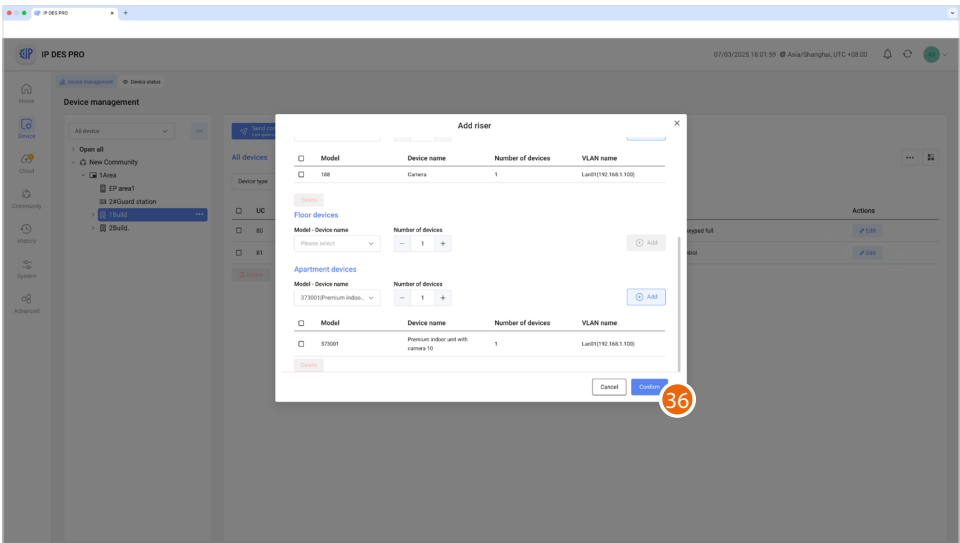
32. Click to add



33. Select the apartment device

34. Select the quantity

35. Click to add

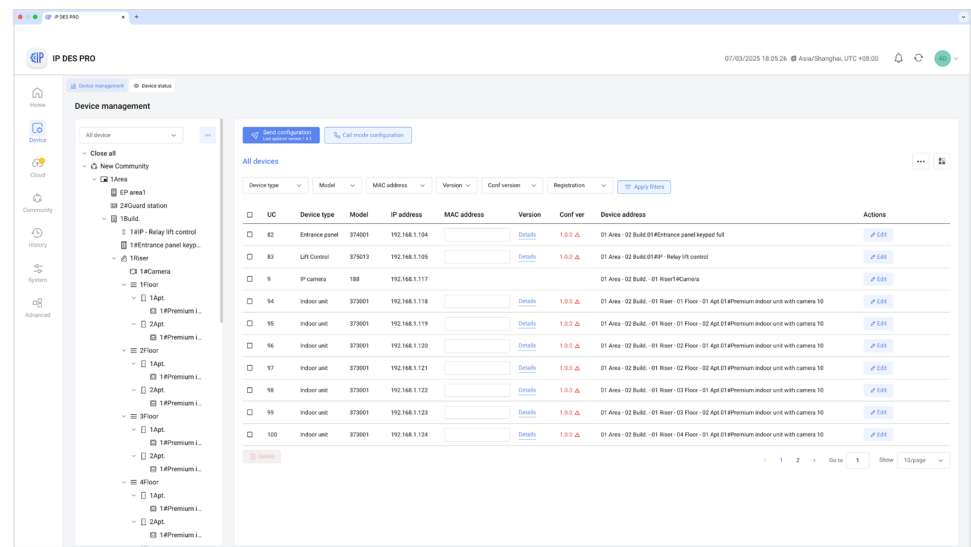


36. Click to confirm

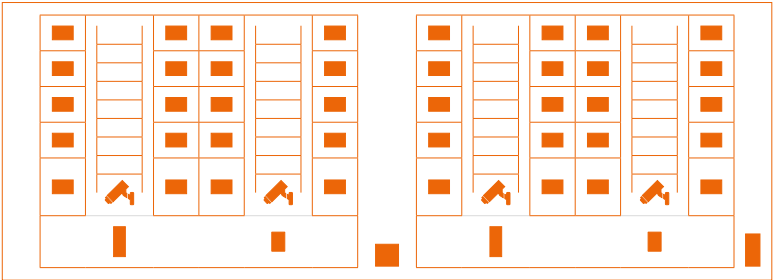




Repeat the same steps for Riser 2



Repeat from step 21 also for Building 2

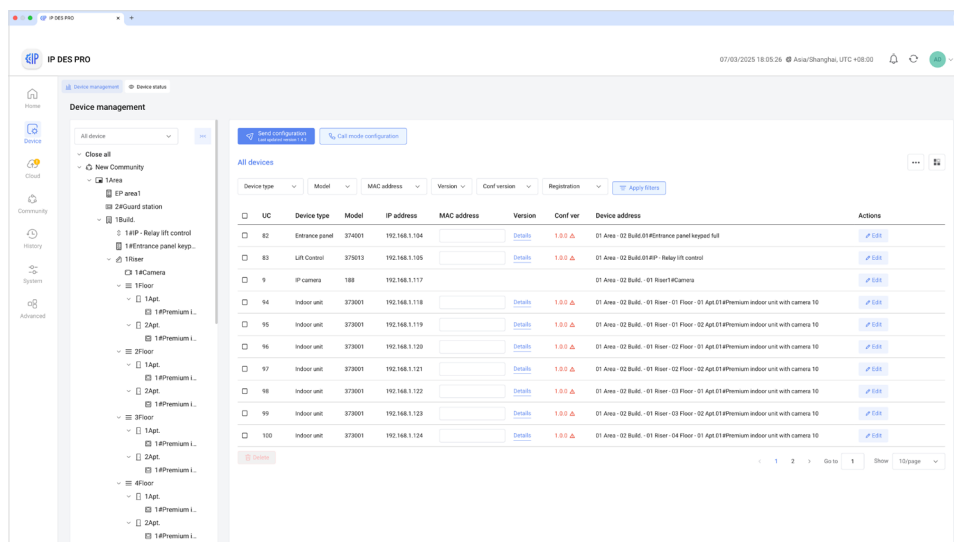




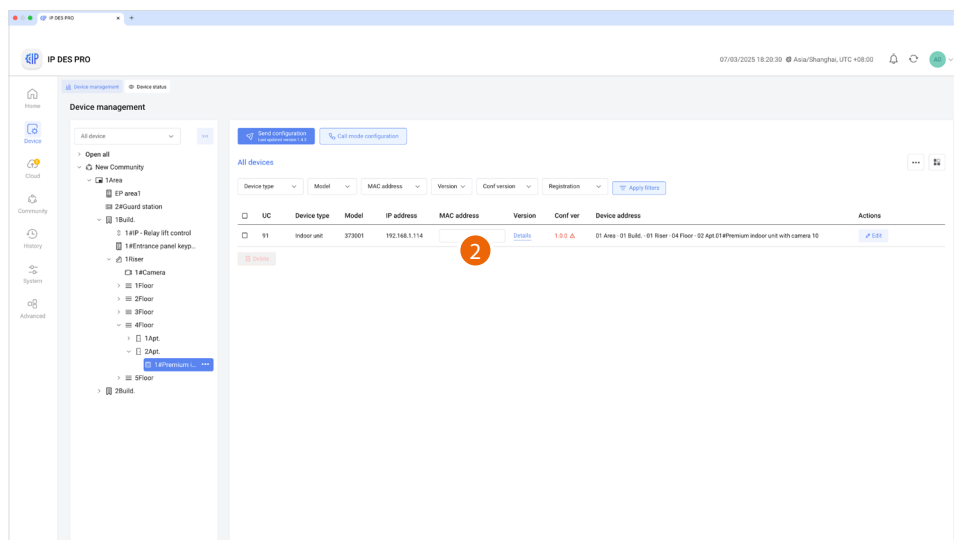
Device MAC address registration

Now that the structure is complete, you will need to associate the MAC addresses of the physical devices with the virtual ones included earlier in the structure.

The device MAC ADDRESSES can be obtained from the list previously created on the system.



This section includes all the devices to associate. The MAC address can be entered directly from this screen



Alternatively, it is possible to select a branch and only view the devices belonging to that branch. Select a device from the tree menu and enter the MAC address individually. The advantage of this method, is that it is easy to identify devices based on their geographical location.

2. Enter the MAC address

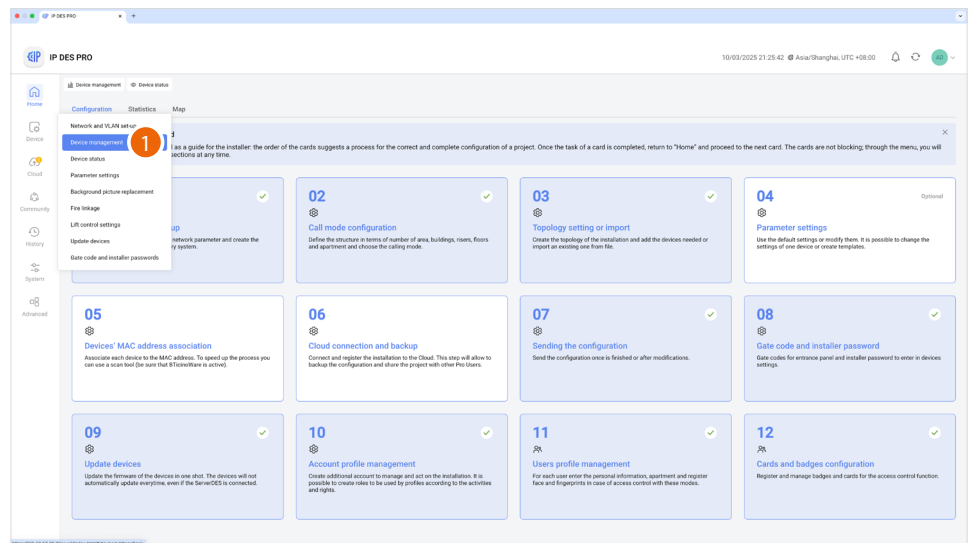
Repeat for all devices



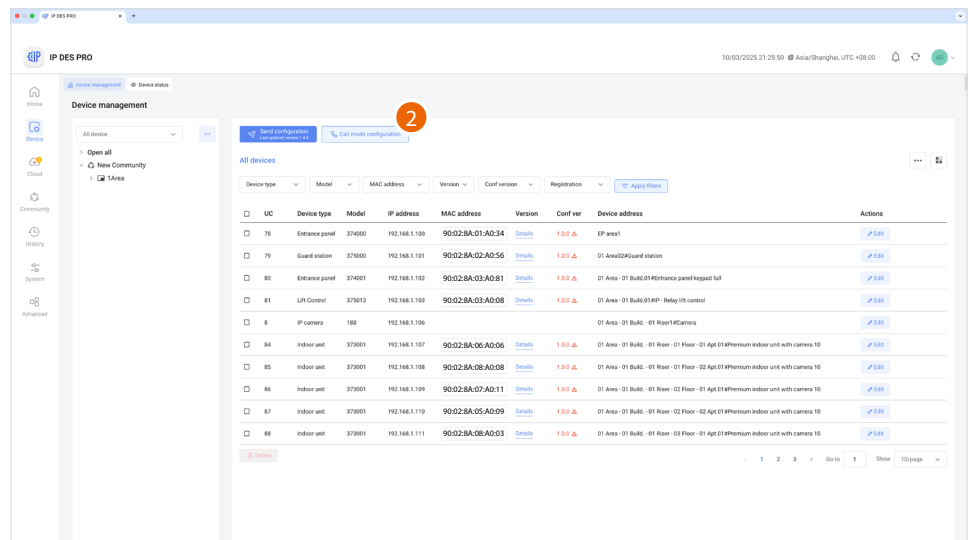
Community customisation

Before sending the configuration to the SD, we can customise the Community by e.g. **modifying the call mode** and/or by **enabling access to the Community for certain individuals**. To use a different call mode, (e.g. call mode via phonebook) to call residents, it will be necessary to:

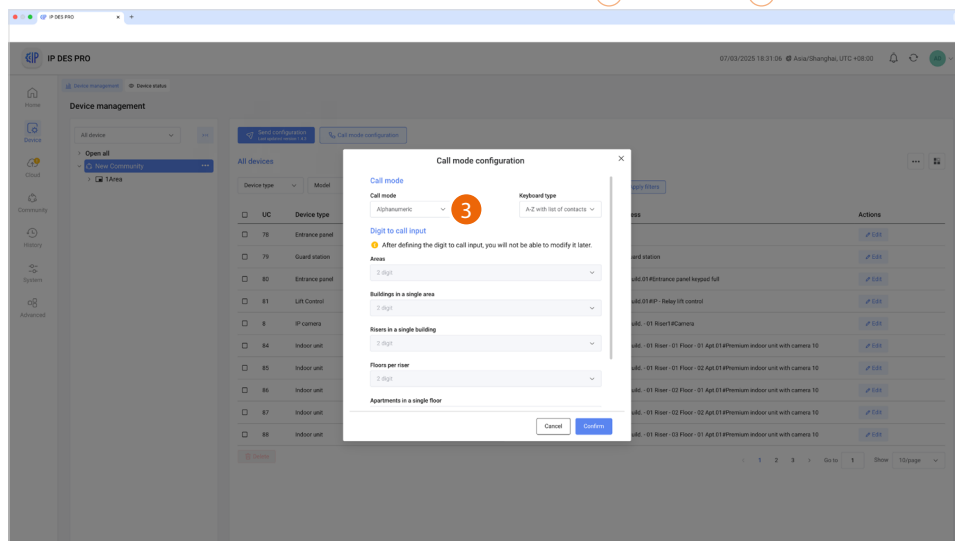
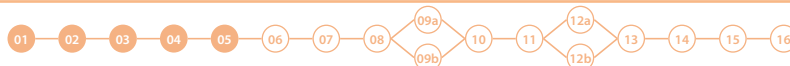
- Change call type to alphanumeric/address book
- replace **the address in the community with an alias** to facilitate recognition of the called party. This function renames the apartment to a different name (alias). The call to this apartment will be made using this new name. E.g. JOHN SMITH



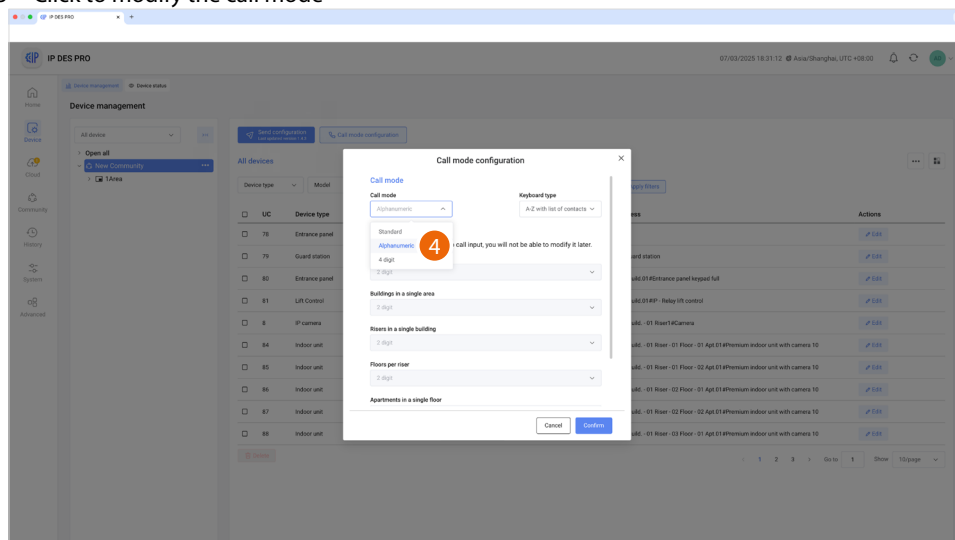
1. Select Device/Device management



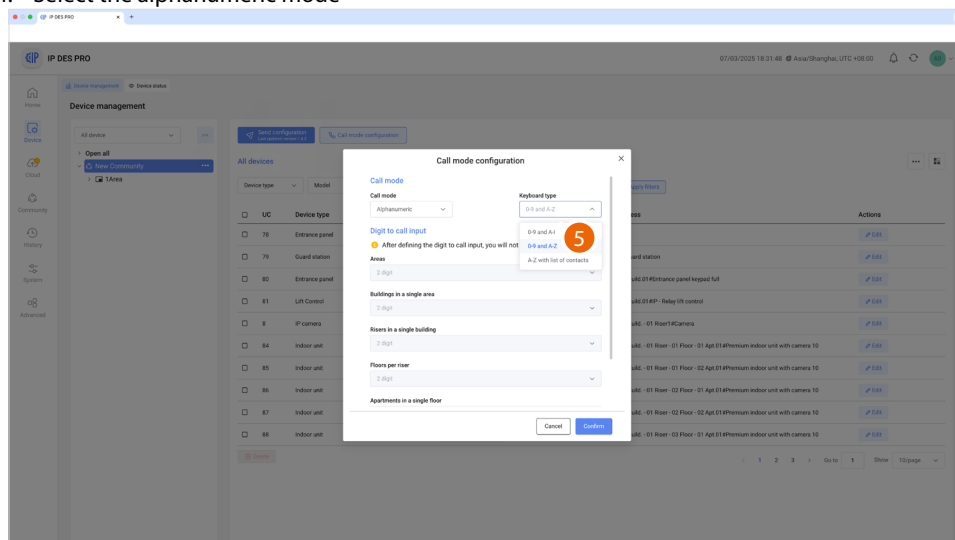
2. Click to select the command



3 Click to modify the call mode



4. Select the alphanumeric mode



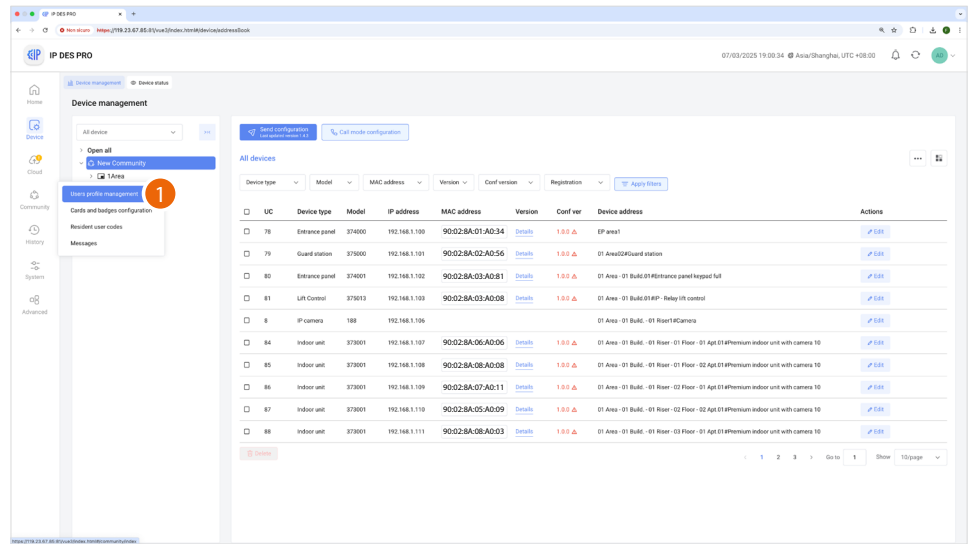
5. Select address book as entry type

After sending the configuration to the SD, it will be possible to call IU using custom names (aliases). When changing the name of a GS or EP, this will be identified with this name on the receiving device when the call is made.

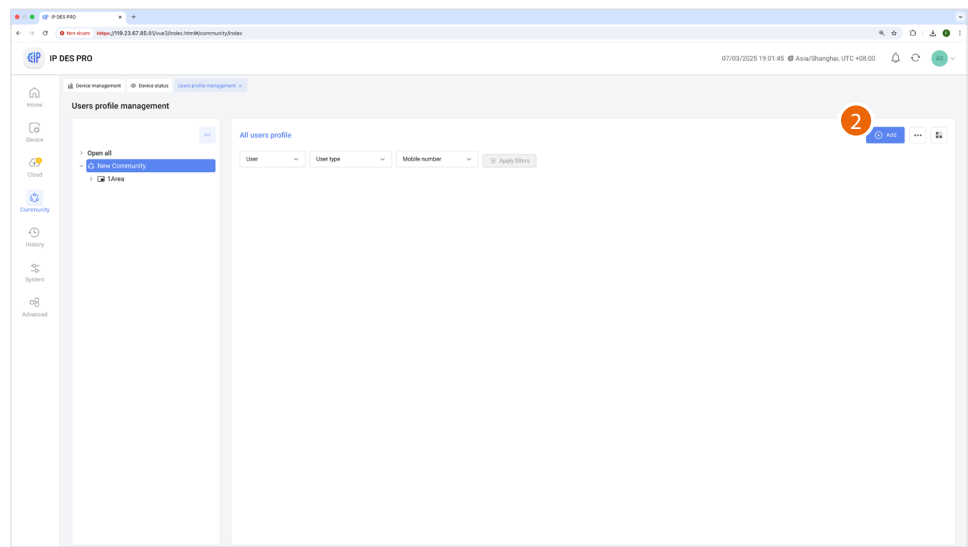
NOTE: This alias format (Address Book) is not supported by entrance panels 374001/03



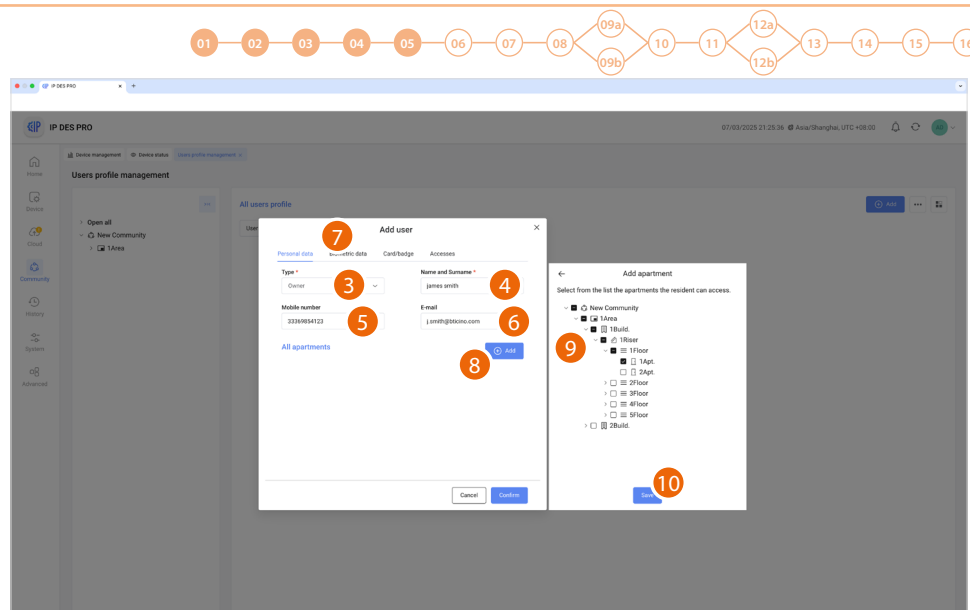
Now it is possible to add community people and give them permissions to access the structure. Depending on the type of person, different access permissions may be assigned, see [Person profile management](#).



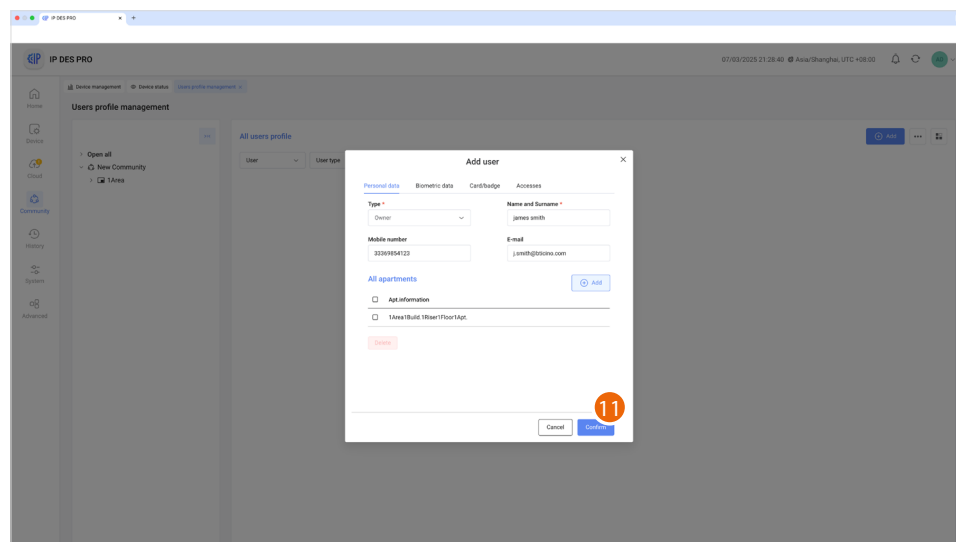
1. Select Community/Users profile management



2. Click to create a new person



3. Select the type of person
4. Enter the name and surname of the person
- NOTE:** some parameters may change depending on the type of person
5. Enter the telephone number of the person
6. Enter the email address of the person
7. [Register a fingerprint](#)
8. Now enter the relevant address of the apartment for the person
9. Select the relevant Area/Building/Riser/Floor/Apartment for the person
10. Click to add



11. Click to finish; the person can now access the community using the code and/or fingerprint reading. To use a badge/card to access the community, this must be registered; see [Access control card management](#)

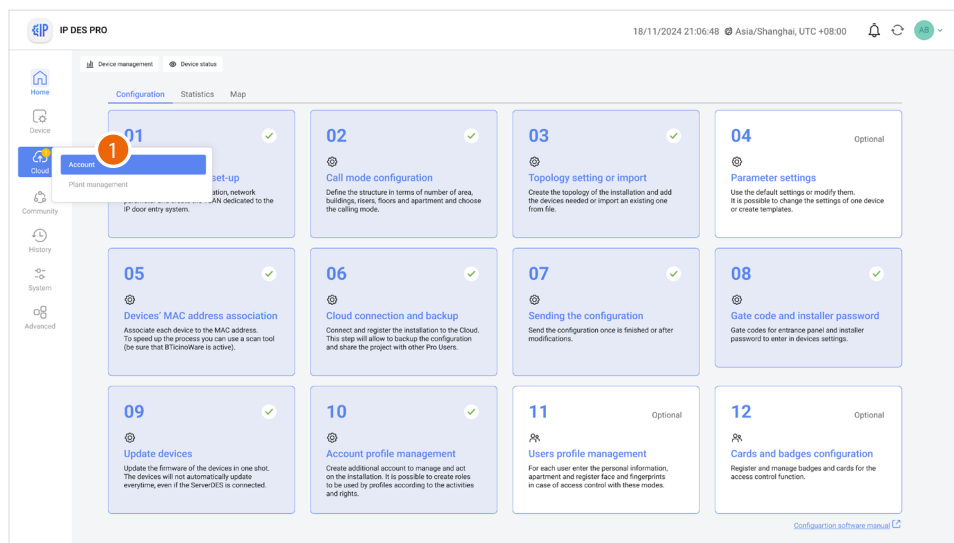


Registration of the community on the Installer's Cloud

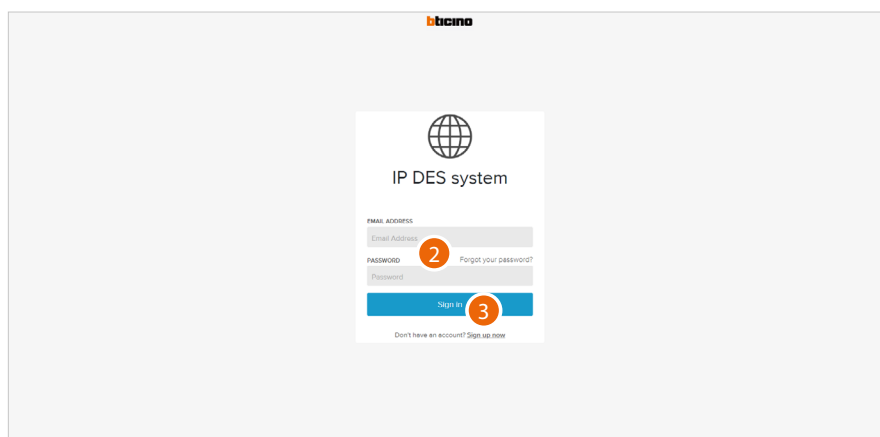
After completing the registration process and creating an Installer account, it is possible to save a copy of the Community on the Installer's Cloud.

Having a copy of the Community on the Installer's Cloud allows you to:

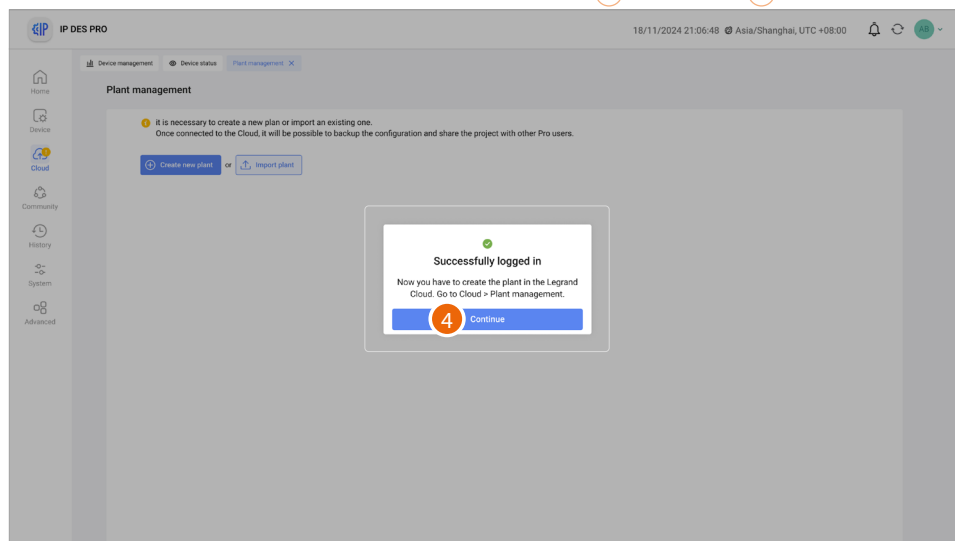
- have greater security in the event of local data loss
- associate the Home+Security app to the IU, for remote management of the video door entry system



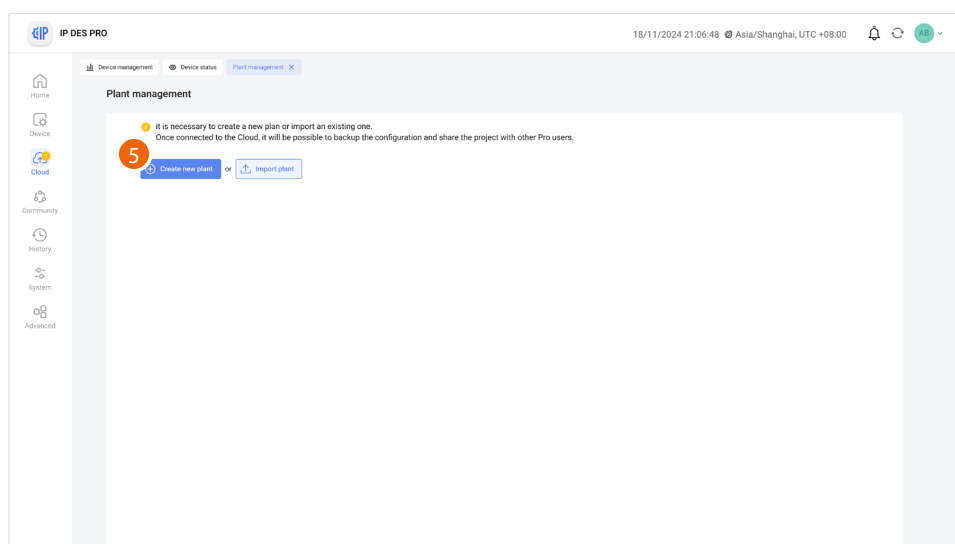
1. Click to complete the Installer's Cloud authentication process



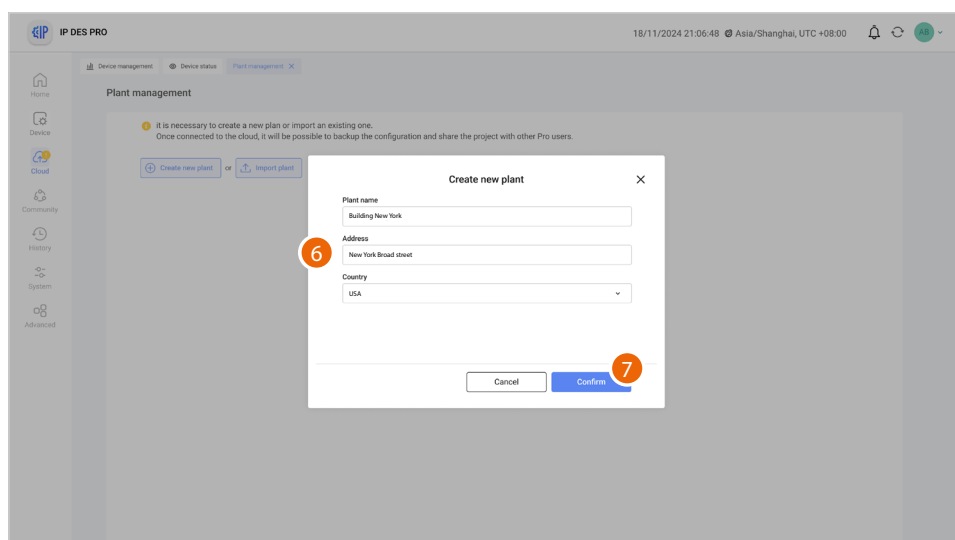
2. Enter email and password
3. Click to access



4. Click to confirm



5. Click to create a new Plant

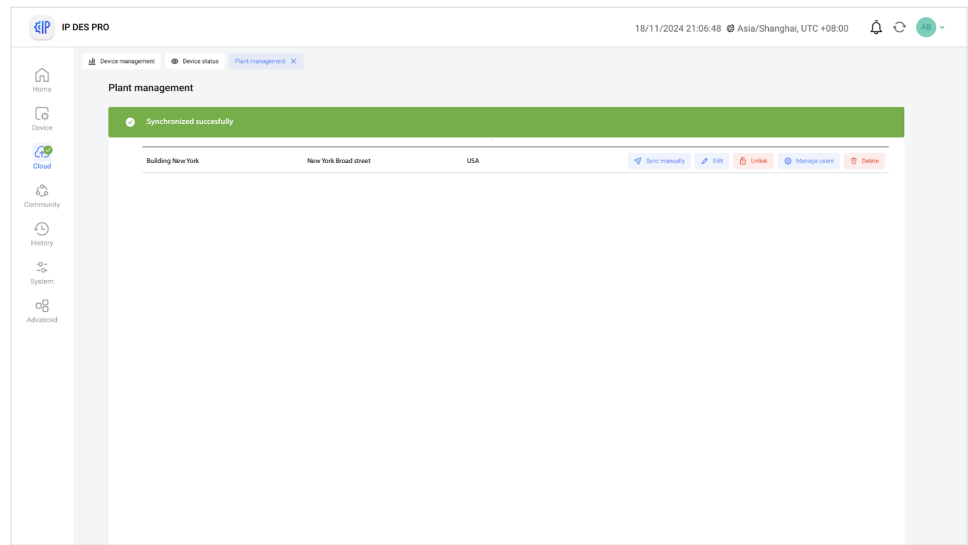


6. Enter the details of the Plant you are creating (name, address and country)

7. Click to save



The plant is automatically synchronised

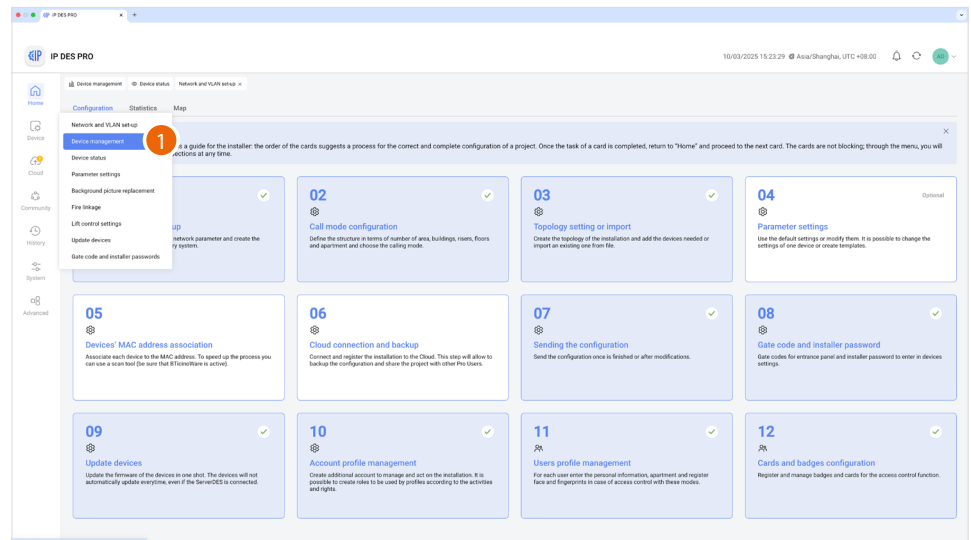


Once created, the plant remains available on the cloud.
If disconnected (unlink button), it can be retrieved from the cloud using the [Import a Plant](#).
If [deleted](#), it will also be deleted from the cloud.

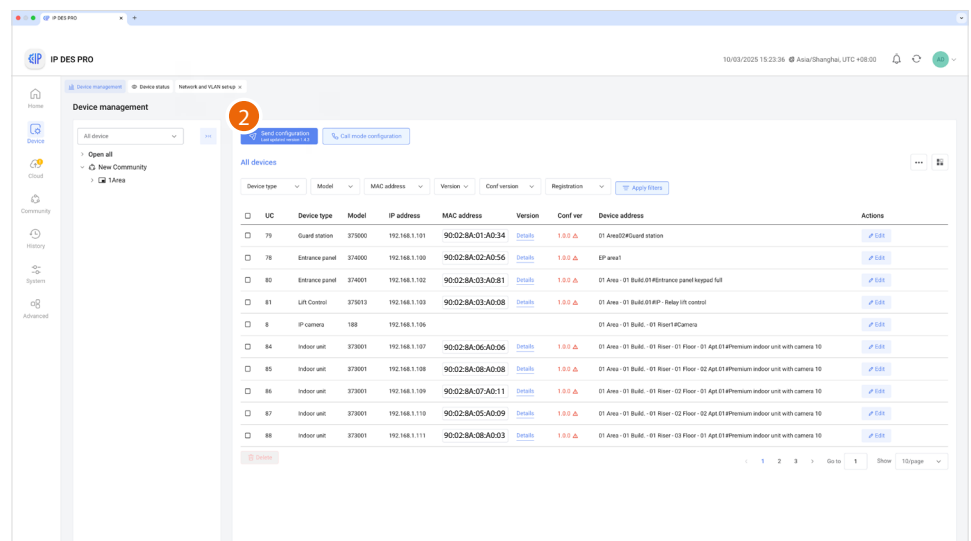


Send configuration to the DES Server

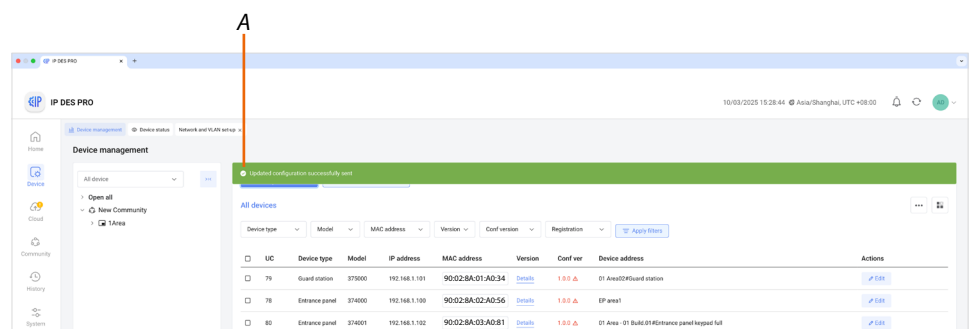
After creating the structure and configuring the virtual devices, it will be necessary to forward the configuration to the system, therefore “instructing” the system to use this configuration.



1. Select Device/Device management



2. Click to send the configuration to the devices

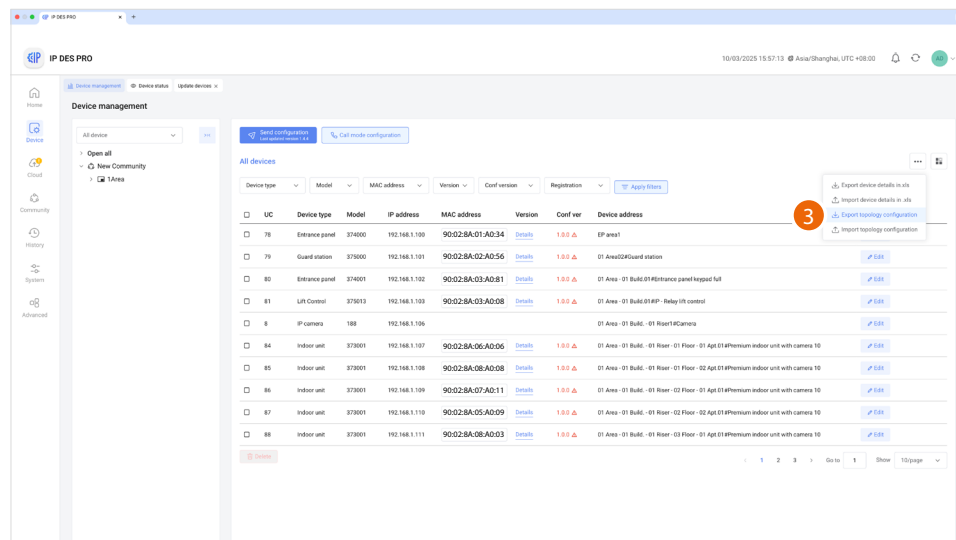


A A message indicates that the configuration has been sent correctly

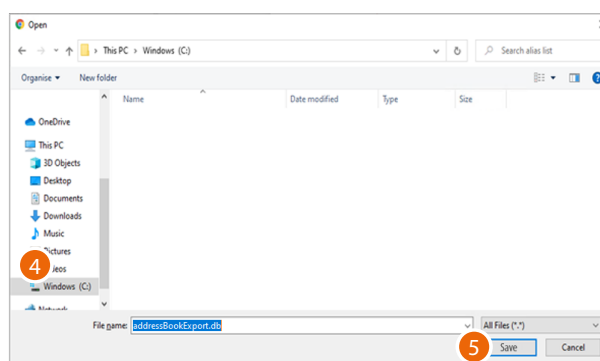


The configuration is now saved in the DES Server.

To avoid accidental loss, it is possible to save it in an archive file or [send the configuration file directly to the system](#).



3. Click to export the configuration to a file



1. Select the location where to save the file (.db)

2. Click to save



Saving of passwords

Installer passwords are generated automatically (with random digits) and uniquely for the two types of devices:

- entrance panels (with 6 digits)
- internal units and guard stations(with 4 digits).

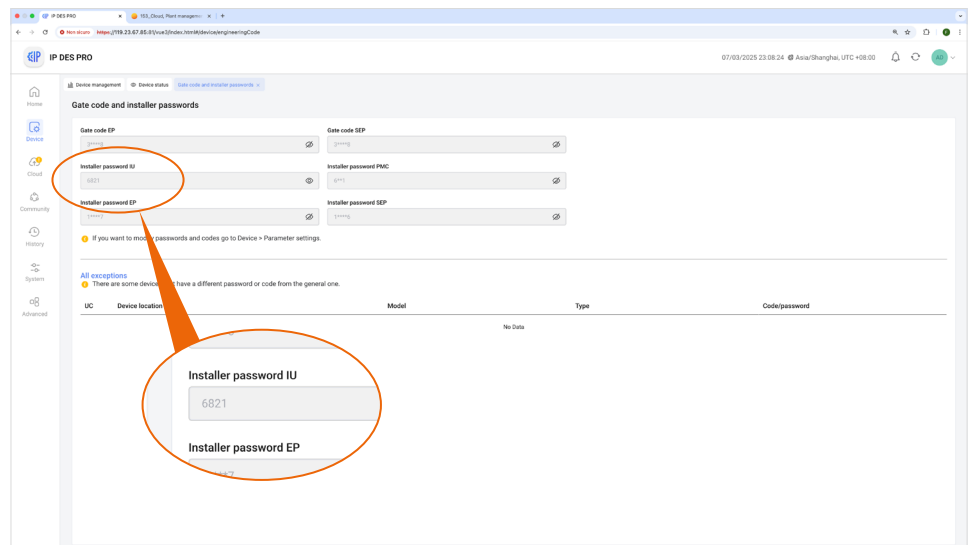
The access codes for opening the door locks of entrance panels are also generated in the same way.

For security reasons, it is recommended to save passwords in a safe place that is always accessible (Cloud backup activation recommended).

If both the SD and the backup are unavailable, it will not be possible to retrieve the passwords.

NOTE: The passwords of the devices incorrectly activated in DEMO mode are: 2000 (EP) and 1111 (IU and GS)

Make passwords visible; see “**Make passwords visible**”



1

INSTALLER PASSWORD
Internal units and guard
stations

INSTALLER PASSWORD
Entrance panels

Door lock release
code

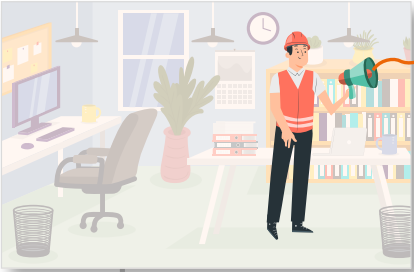
1. Write down the passwords in a safe place that is always accessible.



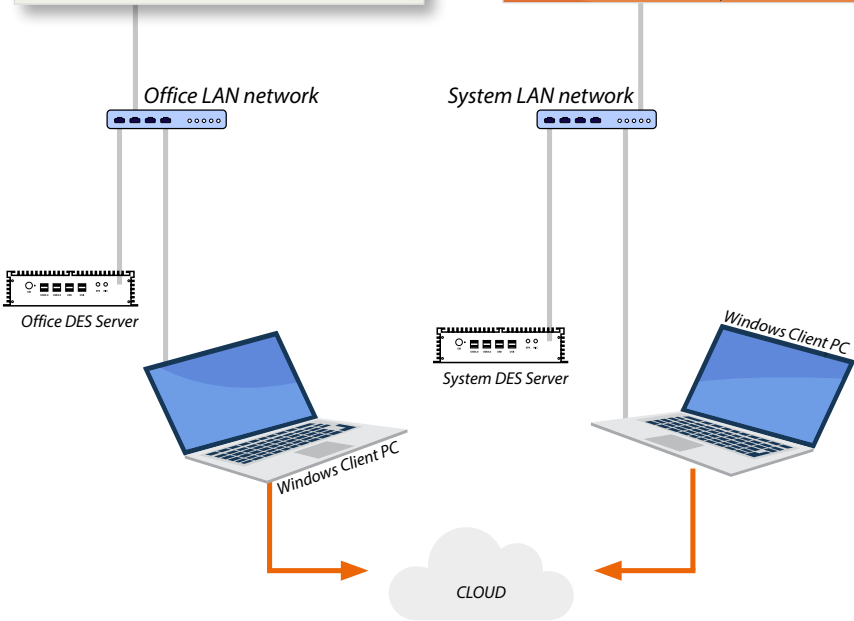
Notification to the system that the Plant has been saved to the cloud

After synchronising the Plant on the Cloud, it will be necessary to notify the installer on the system that the synchronisation has been completed

OFFICE



SYSTEM

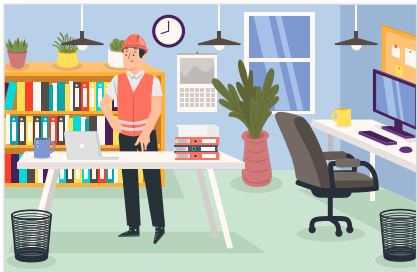




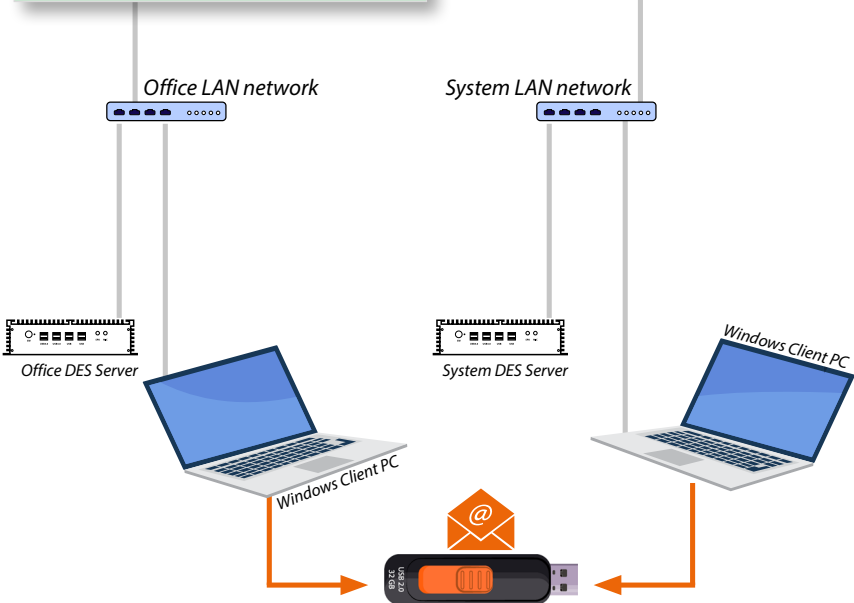
Send the configuration file to the system

After saving the configuration file locally, this can be sent to the system

OFFICE

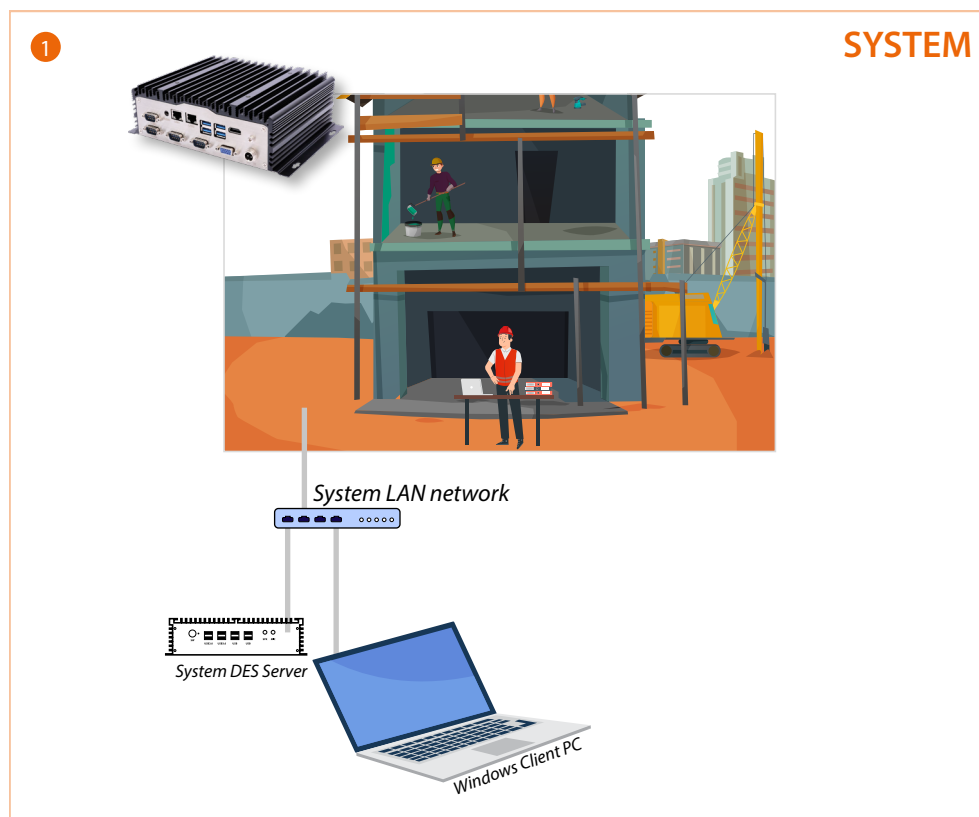


SYSTEM





Connection of the DES Server on the system



1. Connect the SD to the system LAN network

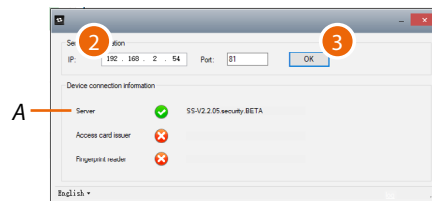


Setup of the fixed DES Server address on the system router



1. Run the BTicinoWare software (on the Windows Client PC) previously installed

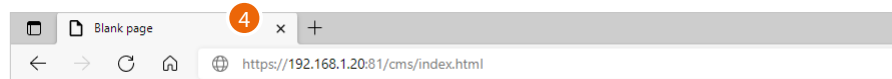
The following screen appears:



2. Enter the **SD address** and check that the port is 81

In order to guarantee correct system operation, the SD (which will take an address assigned by the system router) must maintain its IP address, see [Assigning a "privileged" network address to the SD](#).

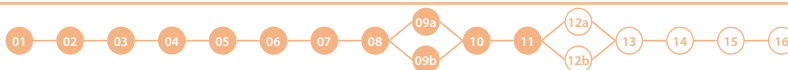
3. Press to confirm and check that the flag A is green



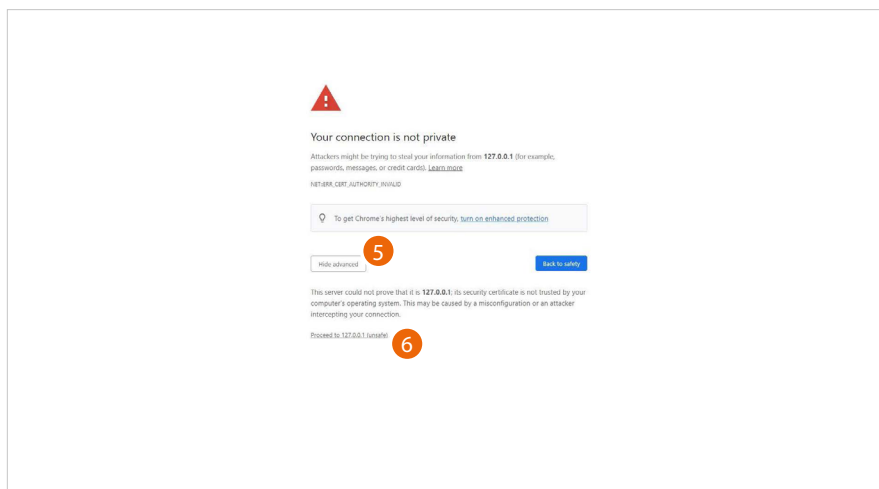
4. Open the browser and enter the http address of the SD:

https://IP or siteserver.local:81

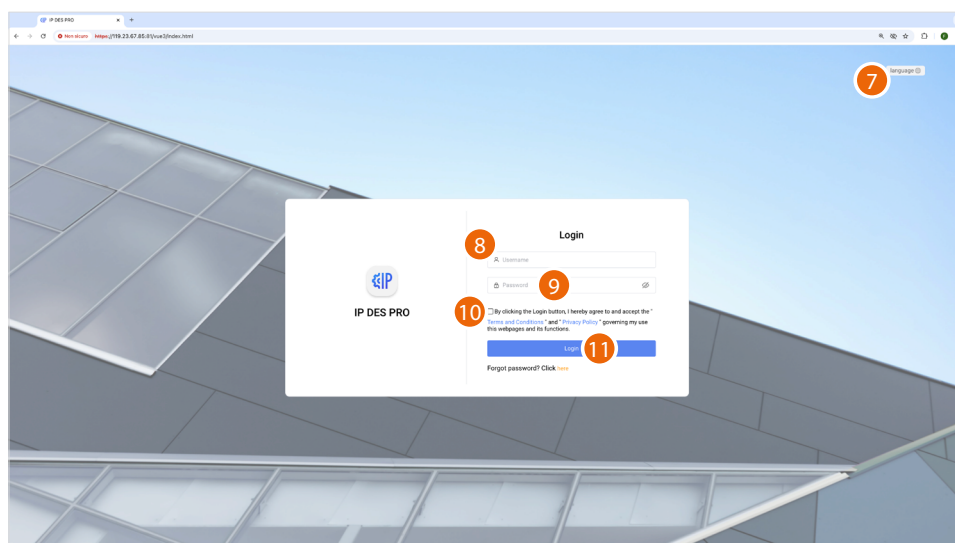
NOTE: use Chrome/Edge browser and a screen with resolution 1920x1080



In some cases, the browser may consider the page to be unsafe.



5. Click to display the advanced options
6. Click to ignore the warning and proceed



7. Select the interface language.
8. Enter the login name (default admin)
9. Enter the password (default 123456)
10. Accept the "Terms and Conditions" and "Privacy Policy" that govern your use of this website and its functions.
11. Click to confirm

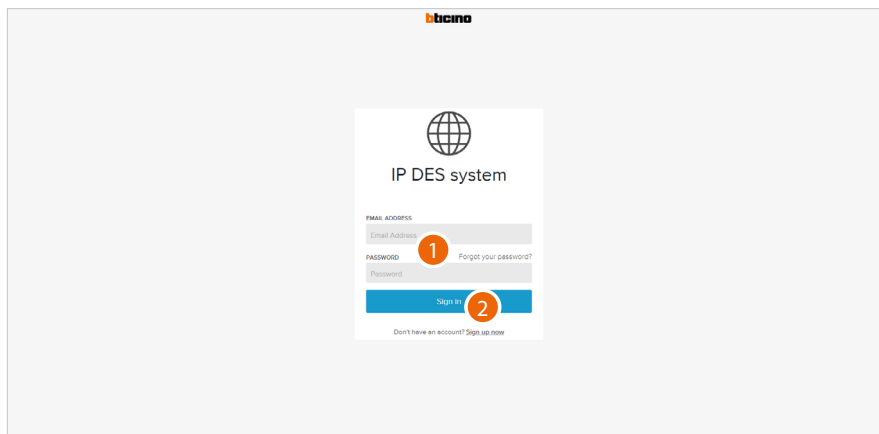
NOTE: For safety reasons, it is mandatory to modify the default password.



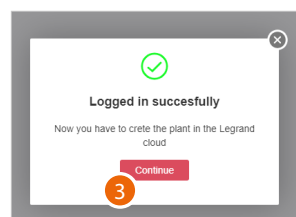
Plant authentication and synchronisation on the cloud

After logging in with the credentials provided by the office, it is possible to synchronise the Plant on the cloud

Authentication



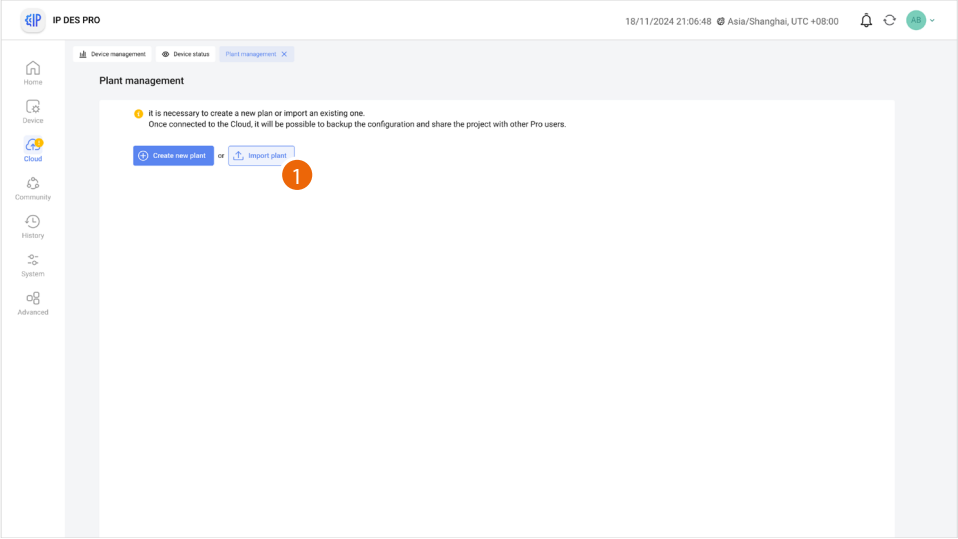
1. Enter email and password
2. Click to access



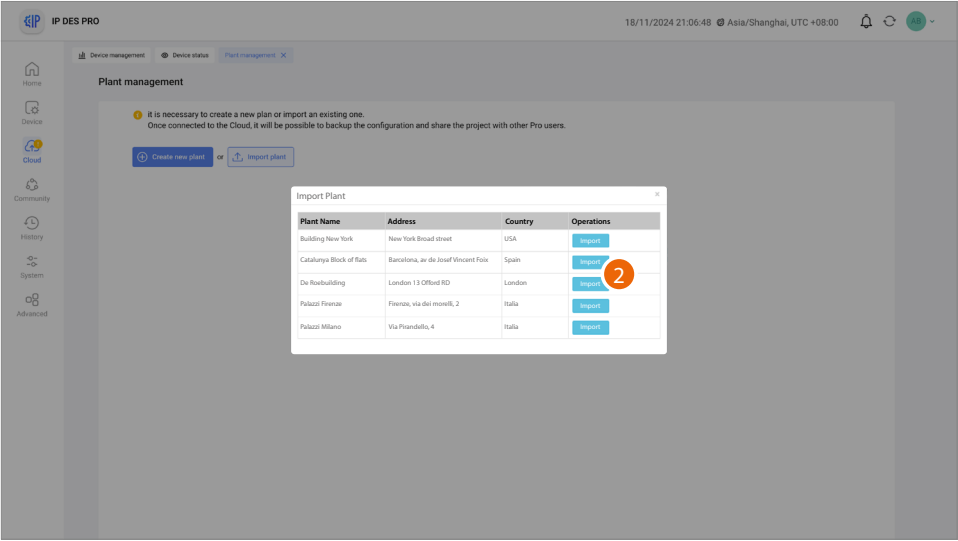
3. Click to confirm.



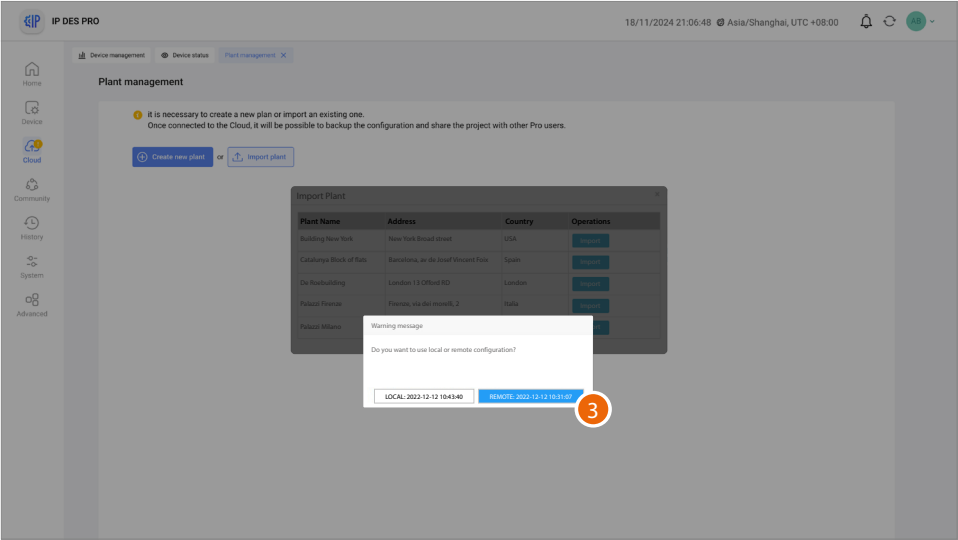
Import the Plant from the cloud
Now it is possible to import the Plant saved on the cloud from the office
To access the Cloud see [First access](#)



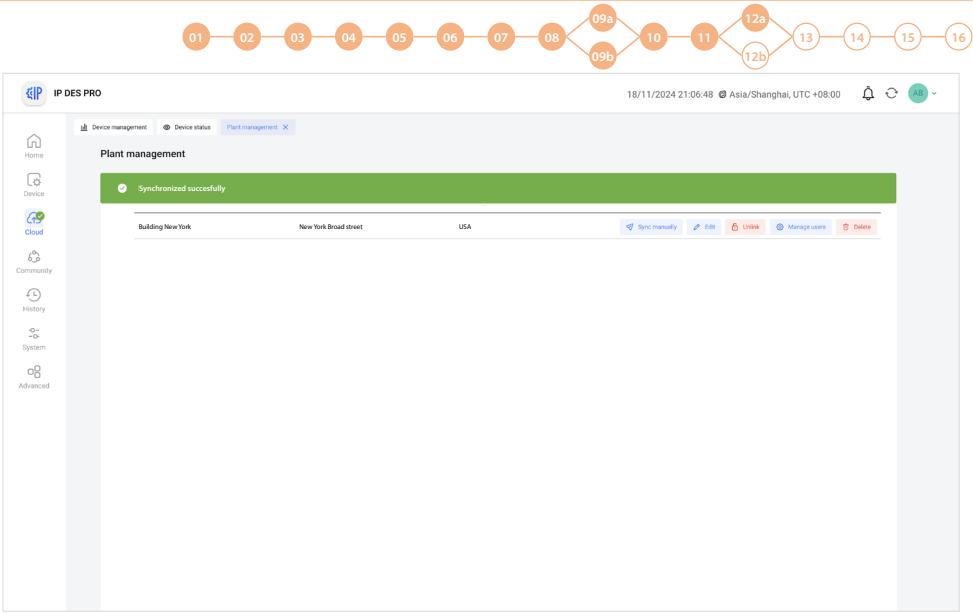
1. Click to import the Plant from those saved.



2. Click to import the plant



3. Click to import the plant version stored on the cloud
Attention: it is important to select the remote version created at the office.

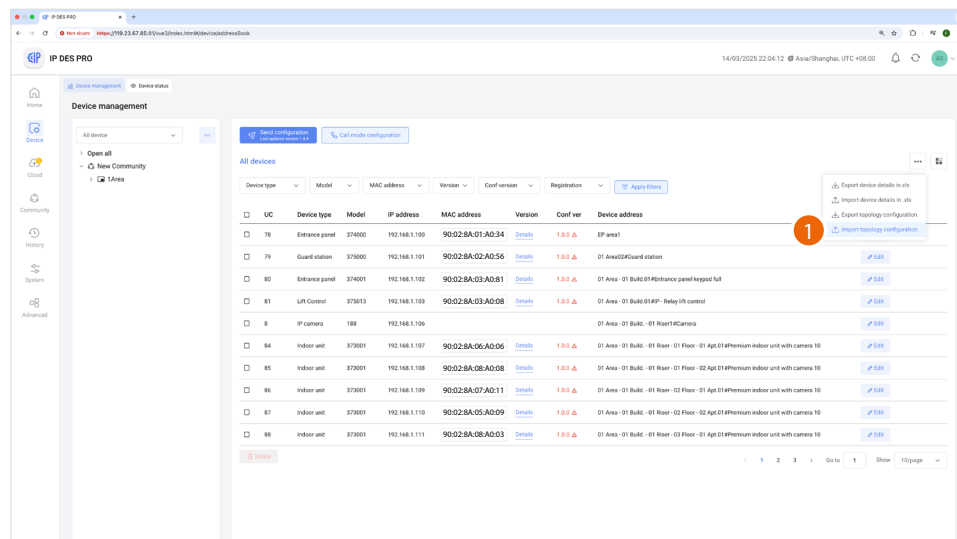


The Plant has been imported

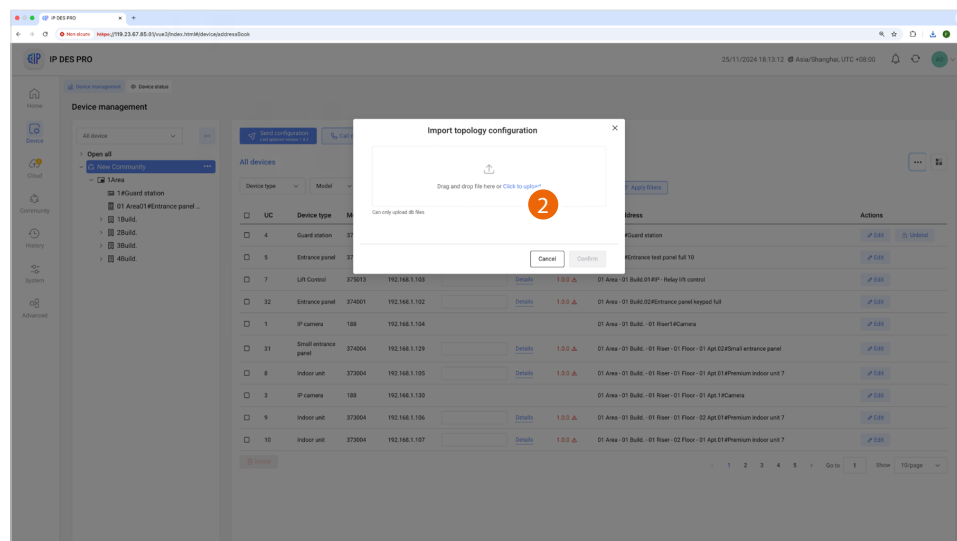


Import the configuration file

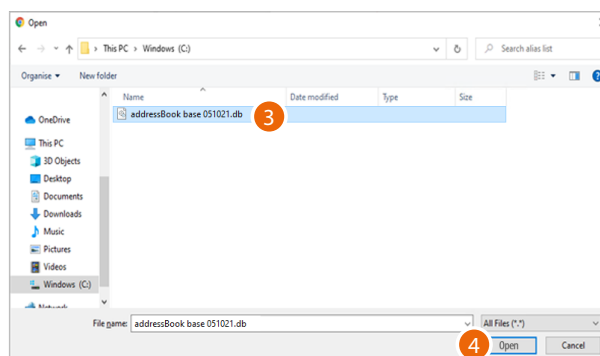
The configuration can now be imported



1. Click to import the configuration(.db)

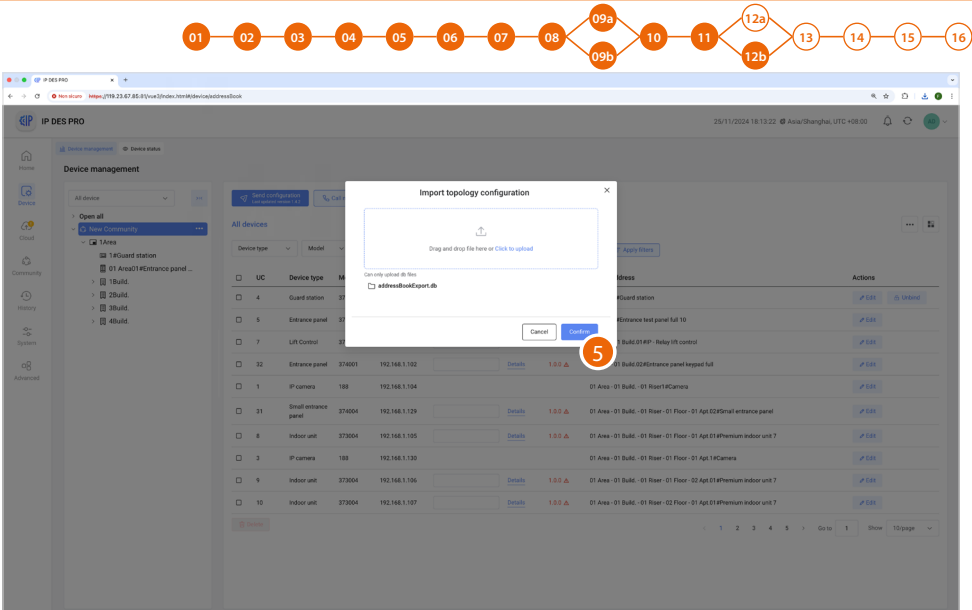


2. Click to select the AB file (.db)

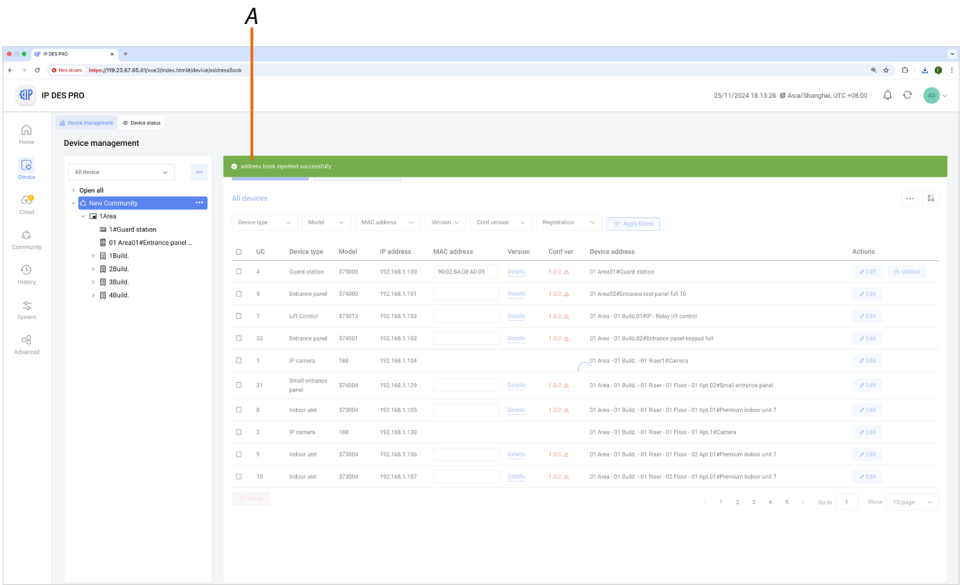


3. Select the file (.db)

4. Click to open



5. Click to confirm



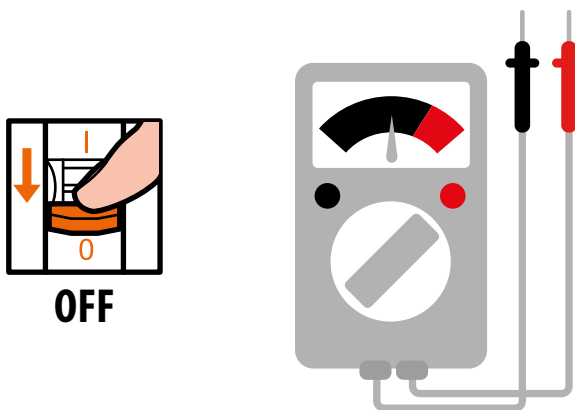
A A message indicates that the configuration has been imported



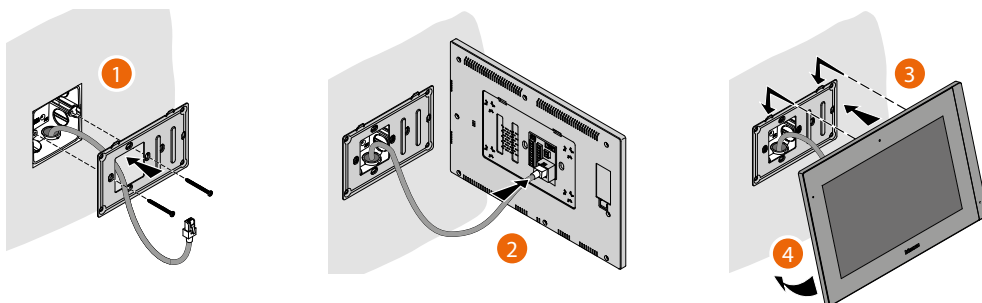
Installation of the devices

To transfer the configuration to the devices, these must be installed and powered

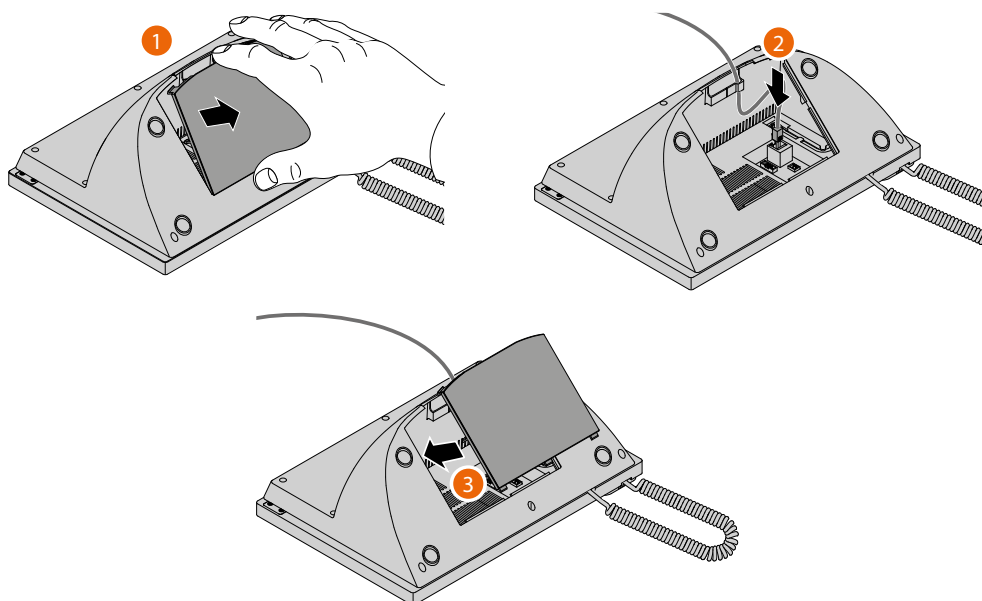
Switch off the power supply to the system and check that there is no voltage



Install the devices

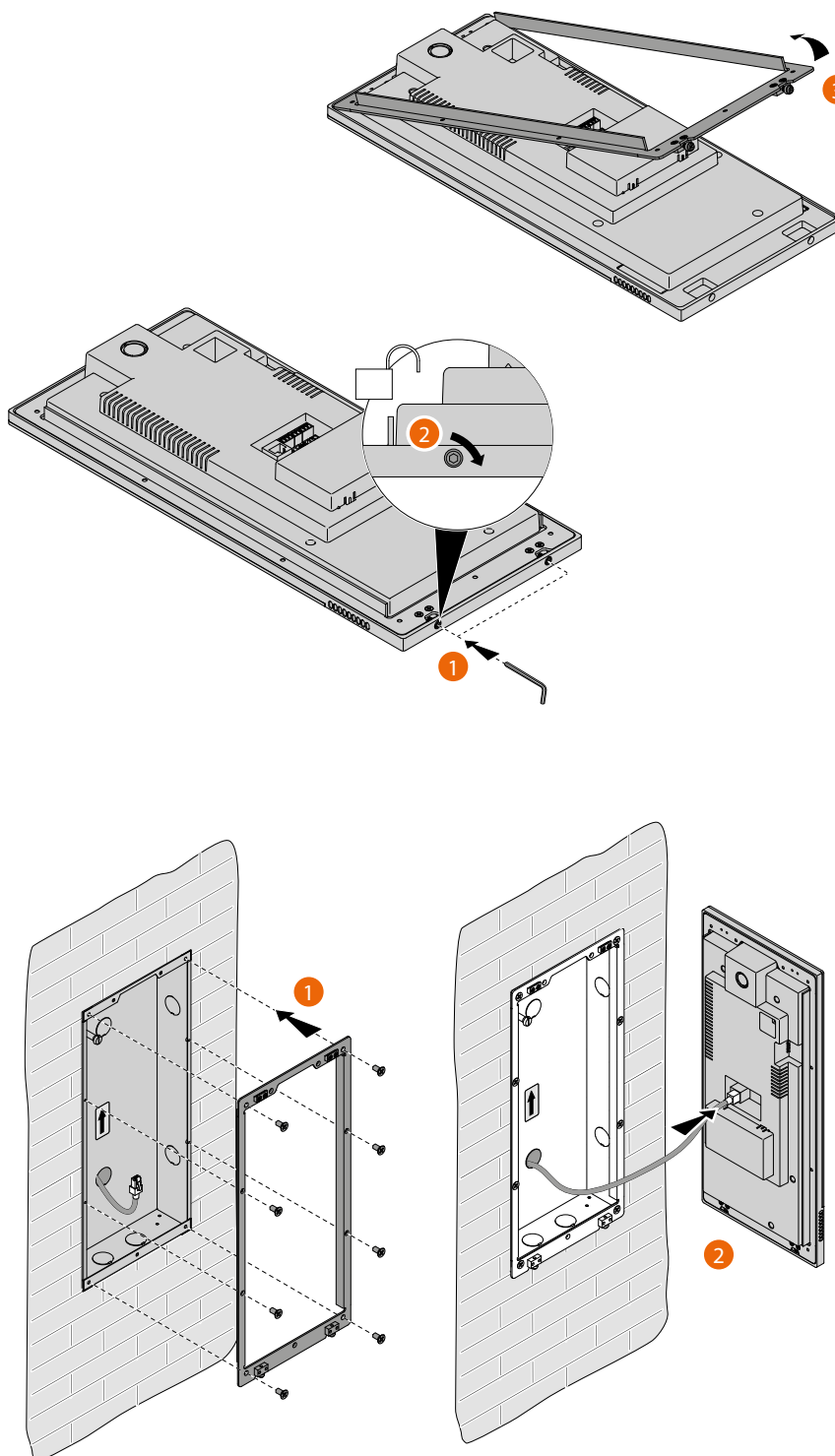


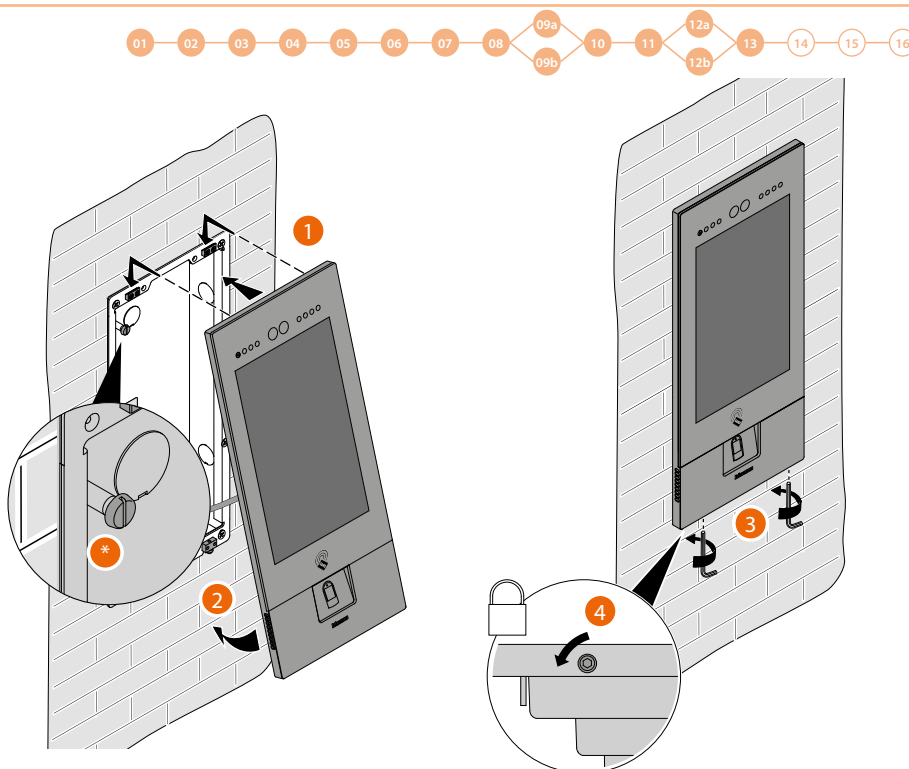
The RJ45 cable must be at least 200 mm long





The wrong wiring of the Ethernet cable connecting the device to the Poe Switch 375002 could damage the device itself.
The RJ45 cable must be at least 200 mm long.

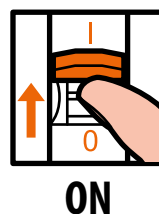




- * Adjust the tamper screw so that it presses the tamper switch of the device and activates the anti-theft function in case of removal, by sending an alarm to the guard station.

Warning: the EP installation shown is representative of all EP.
For more details, see the specific instructions in the package

Reconnect the power supply



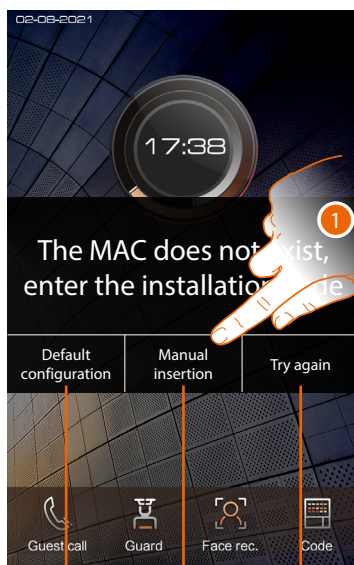
Activation of the devices

Thanks to the previously entered MAC address, once powered, the devices check that a configuration is available on the SD, and if so acquire it.

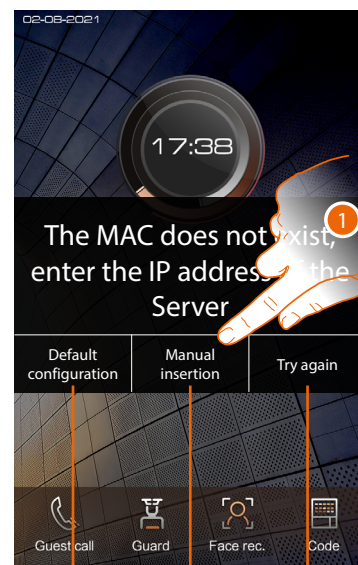
NOTE: devices that were already configured in the past must be reset. After rebooting, they will configure themselves



If the automatic activation of the device is unsuccessful, warning messages and manual activation modes may appear.



A B C



A B C

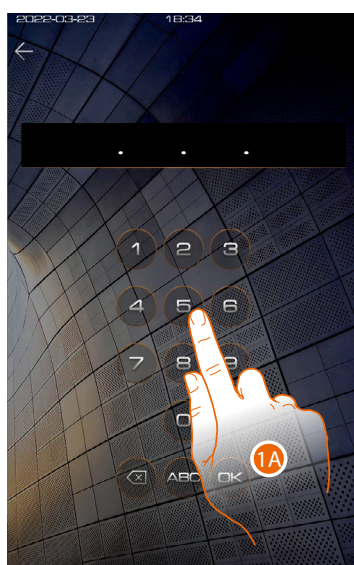
A Not to be used

B Button for the manual entry of the server IP address or installation code. By entering one of the two described parameters, it is possible to force the configuration of the device by putting it into forced communication with the server.
NOTE: to display the IP address, see Manage the community networks, to display the installation code, see Installation code

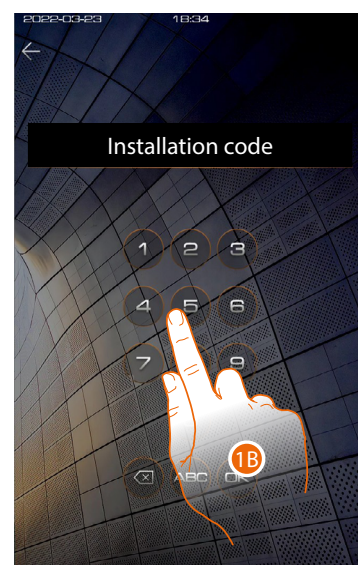
C Button to test the activation of the device

1. Click to manually enter the server IP address or the system access code IP address

IP address



Installation code



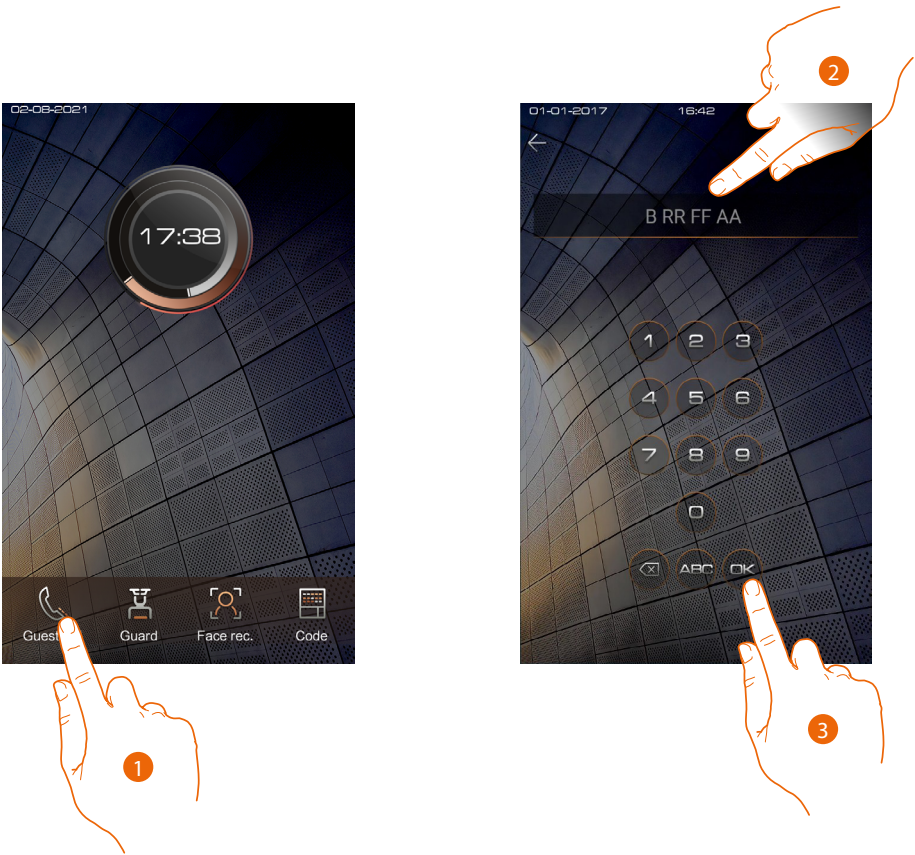
1A. Enter the IP address of the server

1B. Enter the installation code

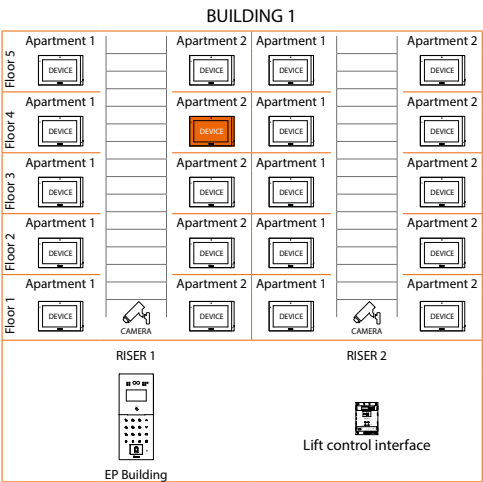
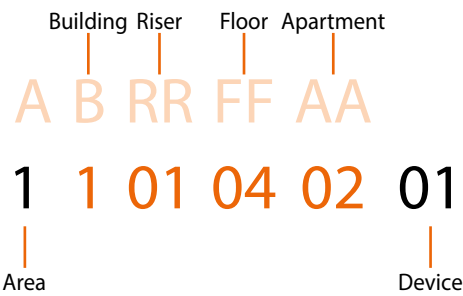


System test

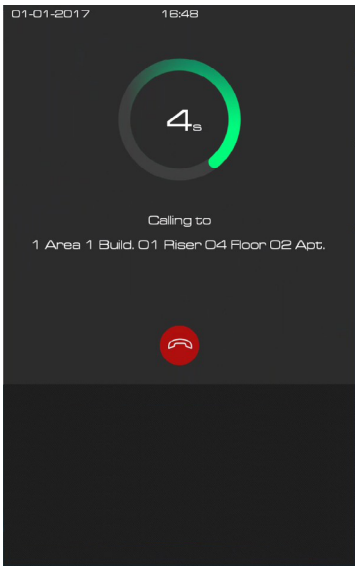
It is now possible to test the system, for example by making a call from the EP



- 1. Touch to make the call
- 2. Enter the IU address

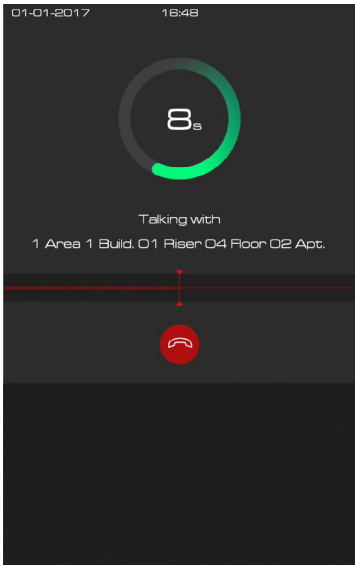


- 3. Touch to send the call



the call is in progress

4. Reply from the IU



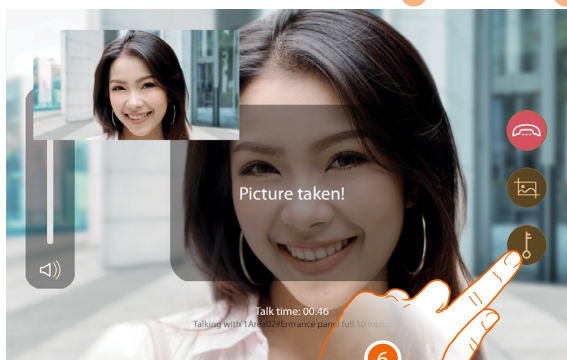
Test the audio signal on the EP



Test the audio/video signal on the IU

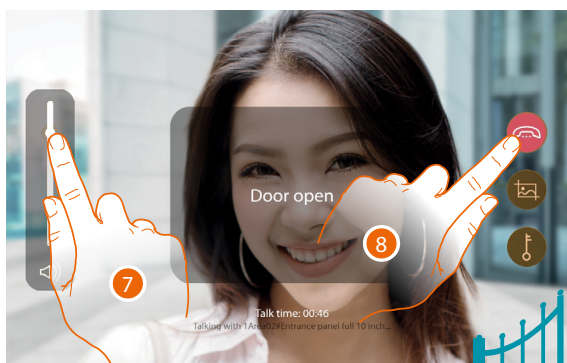


5. Touch to capture an image of the screen



A confirmation message appears.

6. Touch to open the EP door lock

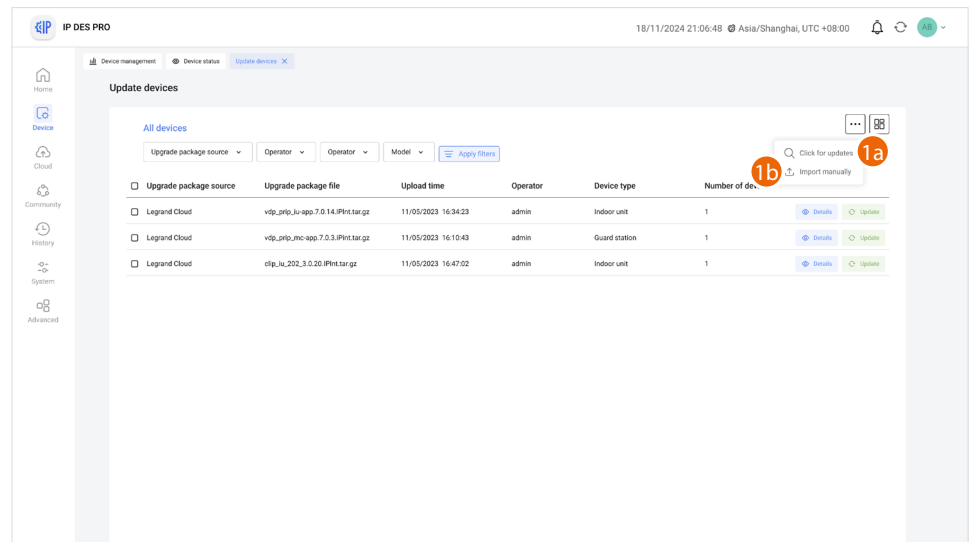


A confirmation message appears

7. Tap to adjust the volume
8. Touch to end the call



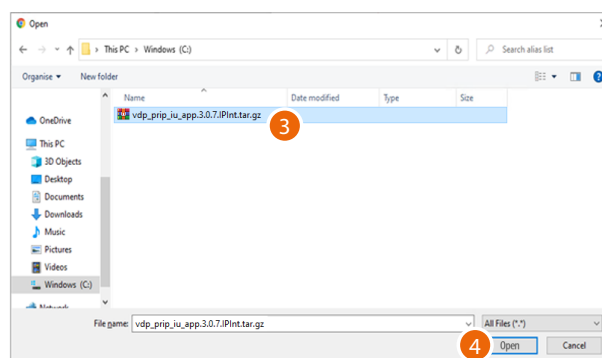
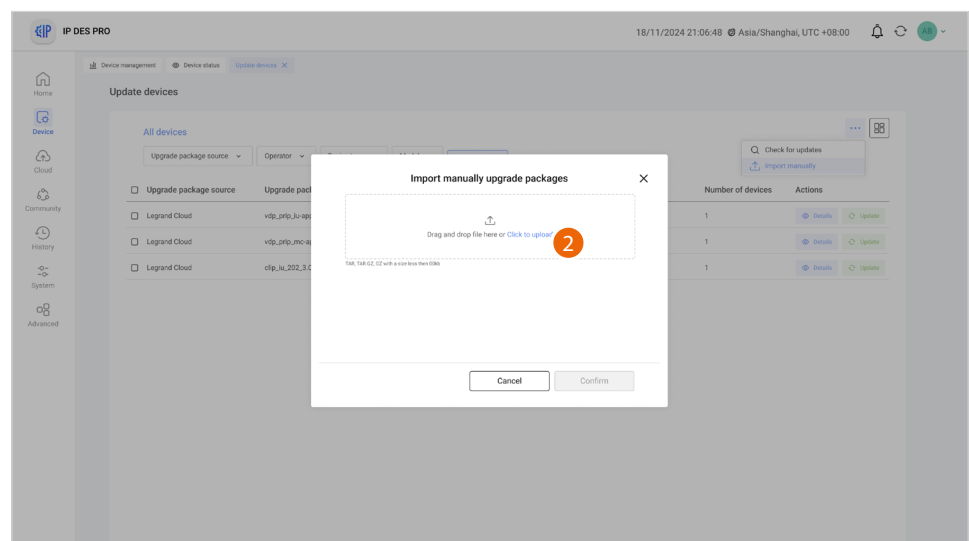
Update of the devices



1a. Click to check for updates on the cloud. If there are updates, these will be downloaded and available for installation

or

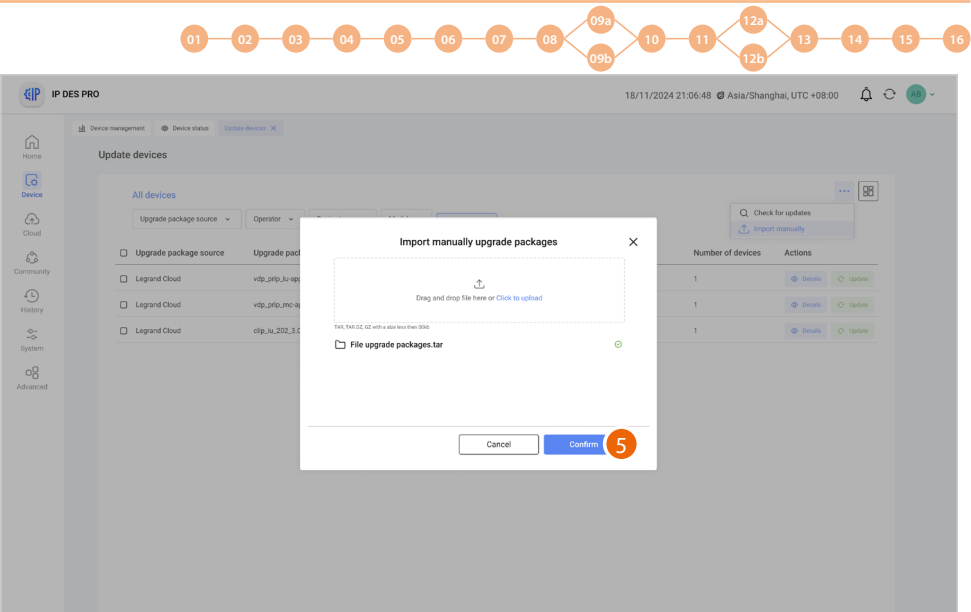
1b. Click to import the update package from the local system (see item 2)



2. Click to select the update package

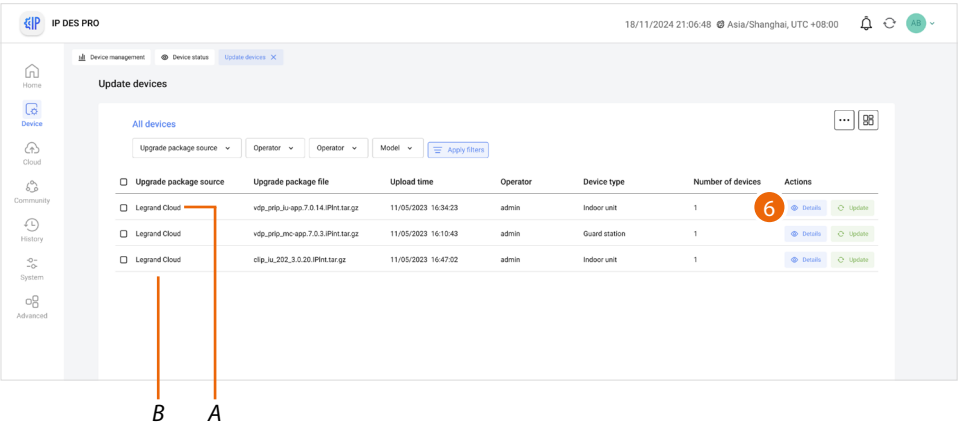
3. Select the .gz file

4. Click to continue



5. Click to confirm

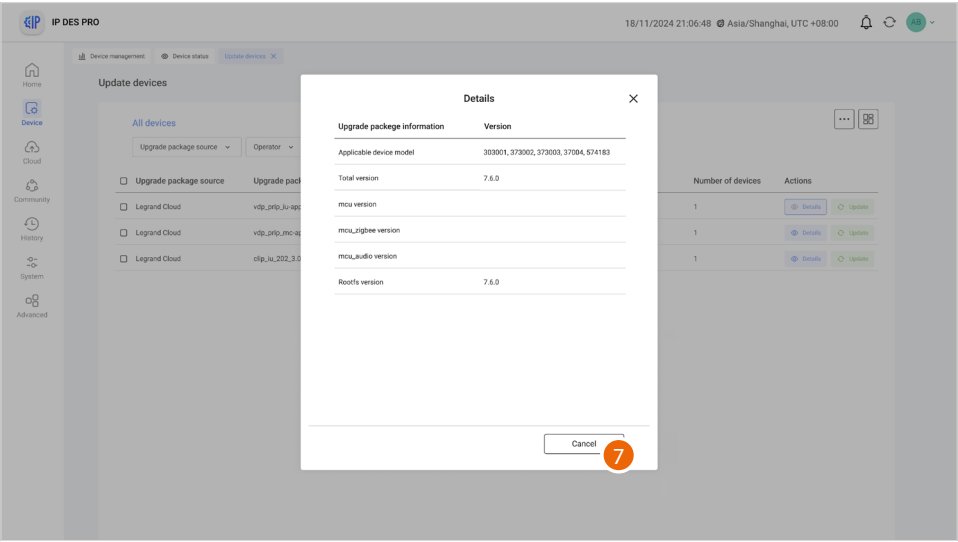
The package has been imported and is available to be sent to the devices



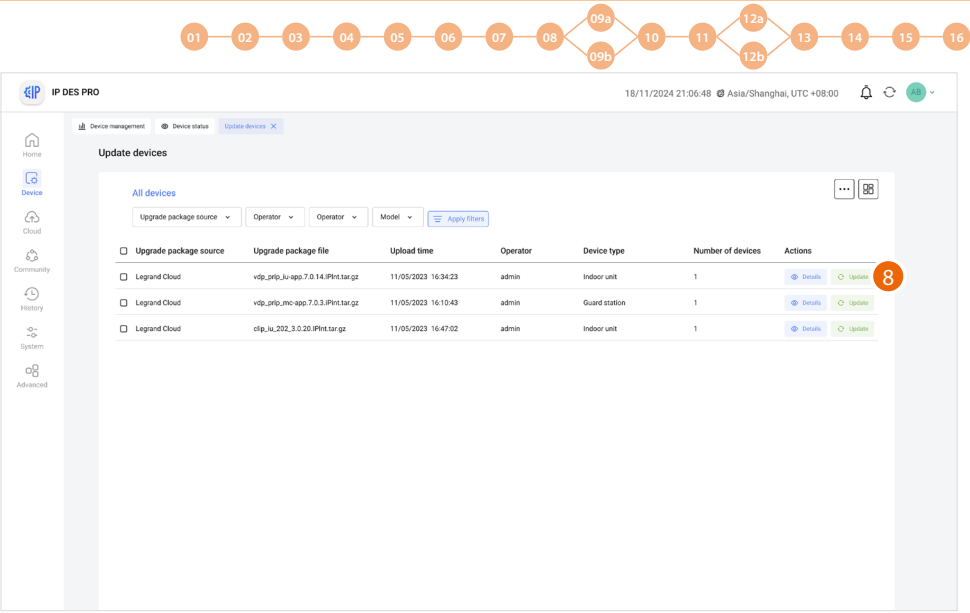
A Update package from Cloud

B Update package from local system

6. Click to see some of the update data



7. Click to close



8. Click to send the update to the plant

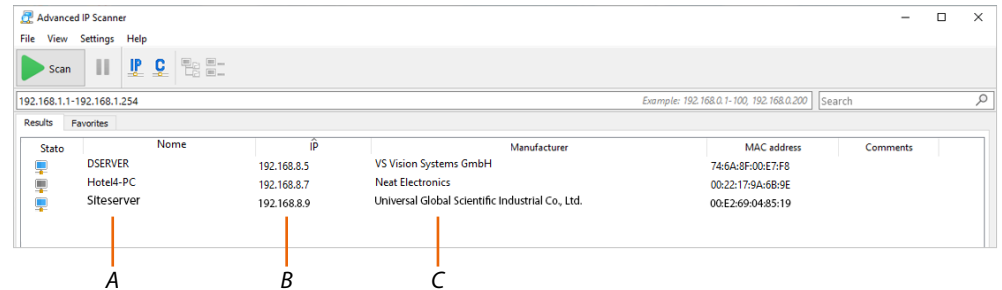
Appendix

Mac address detection via IP Scanner in case of missing or illegible labels on the server

One way to be able to identify the mac address of the SD is to use IP scanners (available on the network) that also show the name and mac address of the devices.

When searching by name, the name Siteserver generally appears in the interface.

If the device has a different name, it can still be identified from the MAC address, which starts with "00:E2:69:xx:xx:xx".



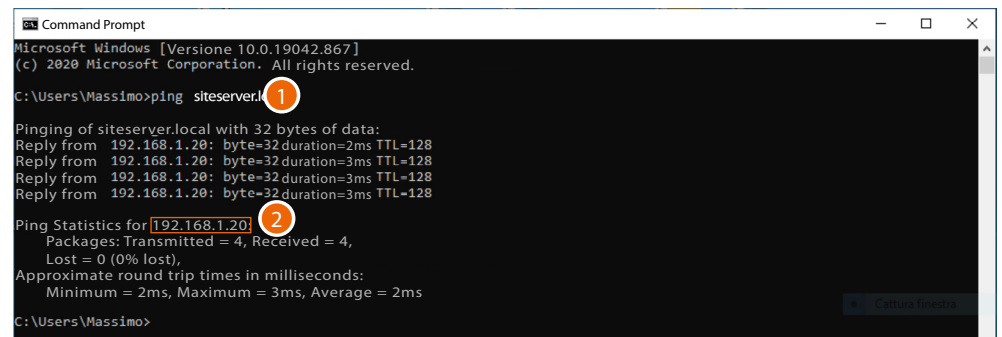
A Name of the device

B IP address of the SD

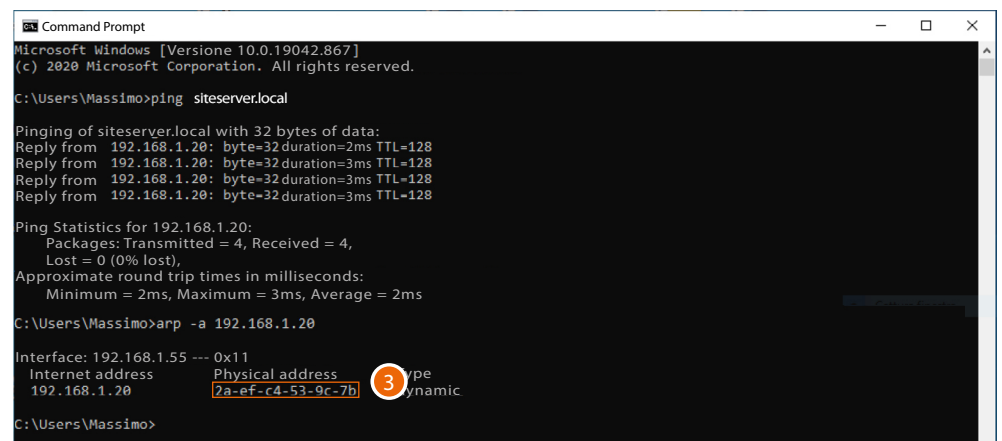
C MAC address of the SD

Mac address detection via ping command in case of missing or illegible label on the server

The device takes 2 minutes to start, after which it remains visible in the network for another 2 minutes. Perform the following activation procedure while the device is still visible.



1. On the Windows Client PC, connected to the same data network as the SD, open the DOS prompt and enter: "ping siteserver.local"
2. Note down the IP address



3. Enter: "arp -a 192.168.1.20 (IP address identified in step 2)" to find the MAC address to use to make the IP address reserved

