IP DES SYSTEM

Software Manual

RA00193AC_S-01/24-PC

IP DES SYSTEM

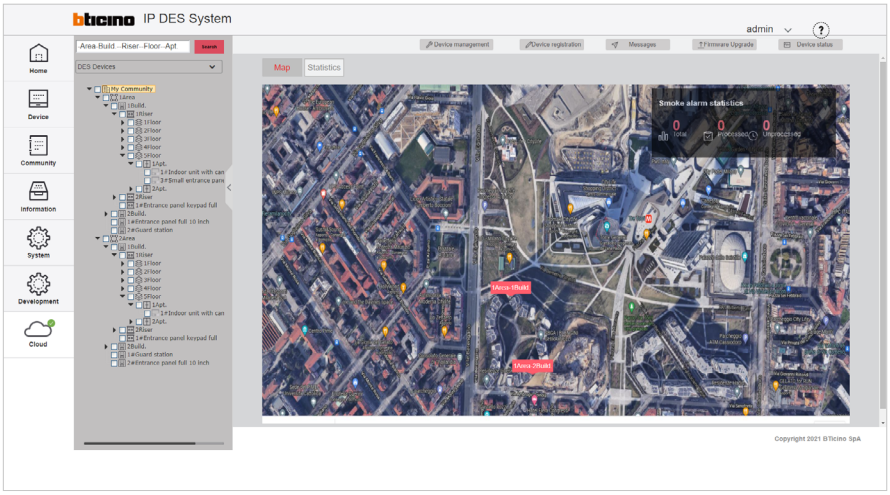
Software Manual

Contents

General description

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.
You can 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 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 IUs.



Acronyms

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

- IU: Indoor Unit
- EP: Entrance Panel
- GS: Guard Station
- SD: Server DES
- SEP: Small Entrance Panel
- AB: Address book
- SW: IP DES System configuration software

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
- To avoid malfunctions when connecting the SD to the cloud, ensure that multicast is enabled on all routers. The name may change depending on the router manufacturer (e.g. "enable multicast" or "igmp snooping").

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 IUs 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.

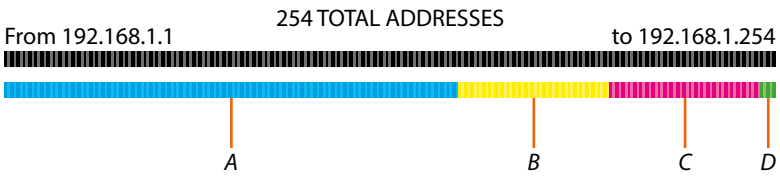
The two address ranges must be separated by configuring the network parameters of the DHCP service and the SD.

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
- addresses available on the network from 192.168.1.1 a 192.168.1.254 : 254 with 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 addresses assigned, DES Server

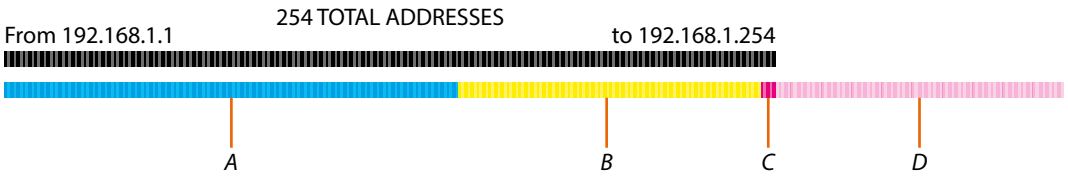
D 4 free addresses

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 addresses assigned DES Server

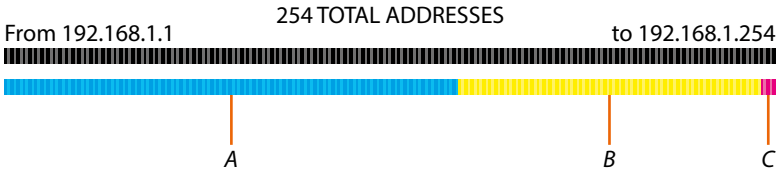
D 96 addresses to assign

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. 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:

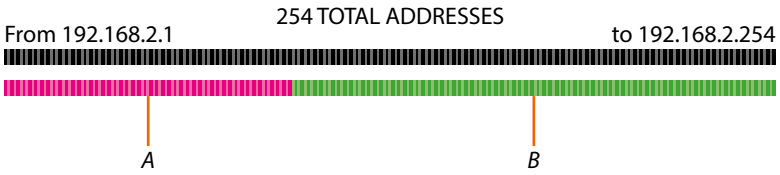
- router DHCP service management for addresses from 192.168.1.1 to 192.168.1.250 (250 addresses available for generic devices and video door entry system devices "1st switch on")
- SD DHCP service management for addresses from 192.168.1.251 to 192.168.1.254 (4 addresses available for video door entry 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 addresses assigned DES Server



A 95 addresses assigned DES Server

B 159 free addresses

Assigning a "privileged" network address to the SD

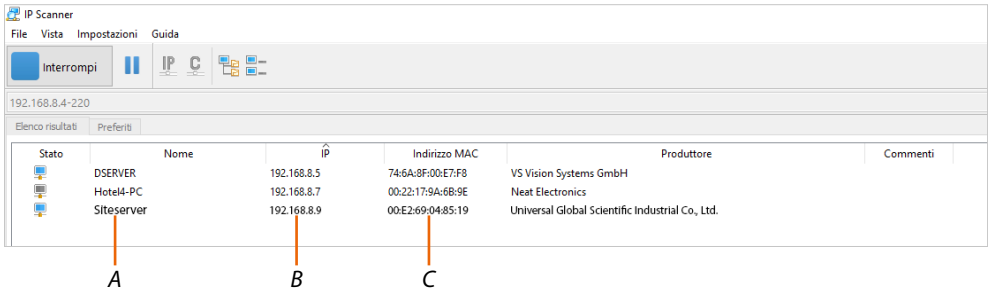
The SD receives the IP address from the DHCP server installed in the network.

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 (method 1)

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".



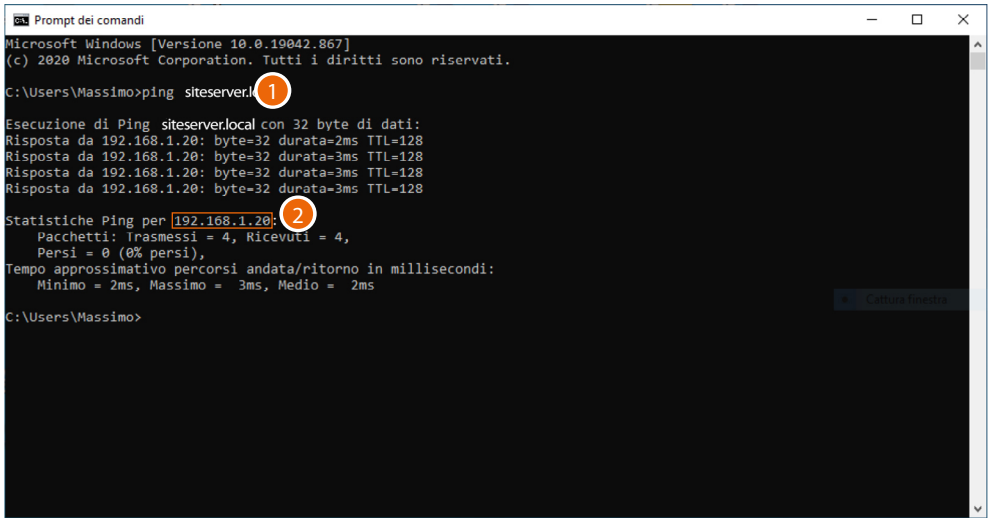
A Device name

B IP address of the SD

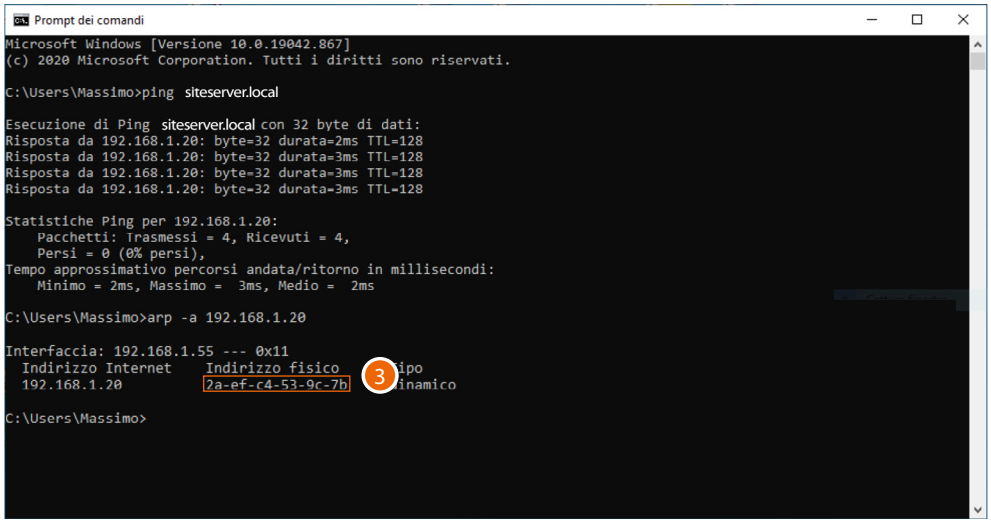
C MAC address of the SD

MAC address identification (method 2)

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

Once configured, the DES server 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 DES Server 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
Server software address management 192.168.1.200 up to 192.168.1.250

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 EPs simultaneously connected to Home + Security in audio/video mode
- A fibre optic line in case of an unlimited number of EPs 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: IU/ EP/GS/SEP.

Community

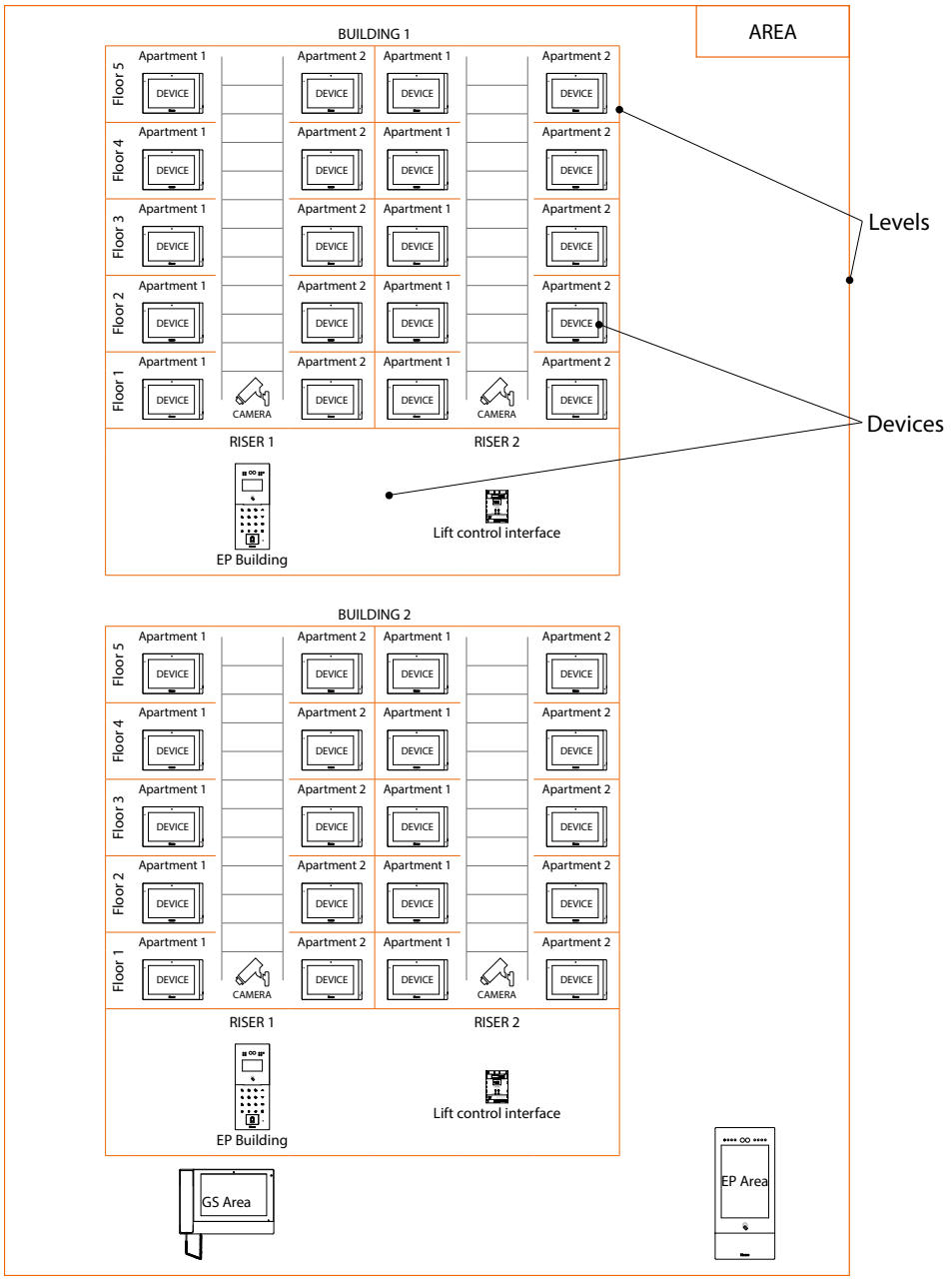
The IP system is designed for the management of installations of medium to large, or even extremely large, sizes.
For this reason, every installation, even a simple apartment, is always included in what is called Community.
Think of a Community as a City split into neighbourhoods (Areas) consisting of Buildings, which are in turn split into Risers, Floors and Apartments.
Each of these levels can then be populated by several devices, such as IU, EP, SEP and GS.
The Community can be saved on the cloud. (strongly recommended).

Plant

Saving of the AB and other data on the cloud

Example of the structure of a community

AREA → BUILDING → RISER → FLOOR → APARTMENT → DEVICE



Address Book

The AB is the project in which Community data are stored.
This data may relate to the Community structure and/or to device parameters.
Changes made to both the structure and the device parameters are stored in the SW.
This data must then be sent to the physical devices in the system.
There are several ways to send the parameters, and therefore to synchronise data between the SW and the physical devices. See the relevant sections.

Call addressing procedures

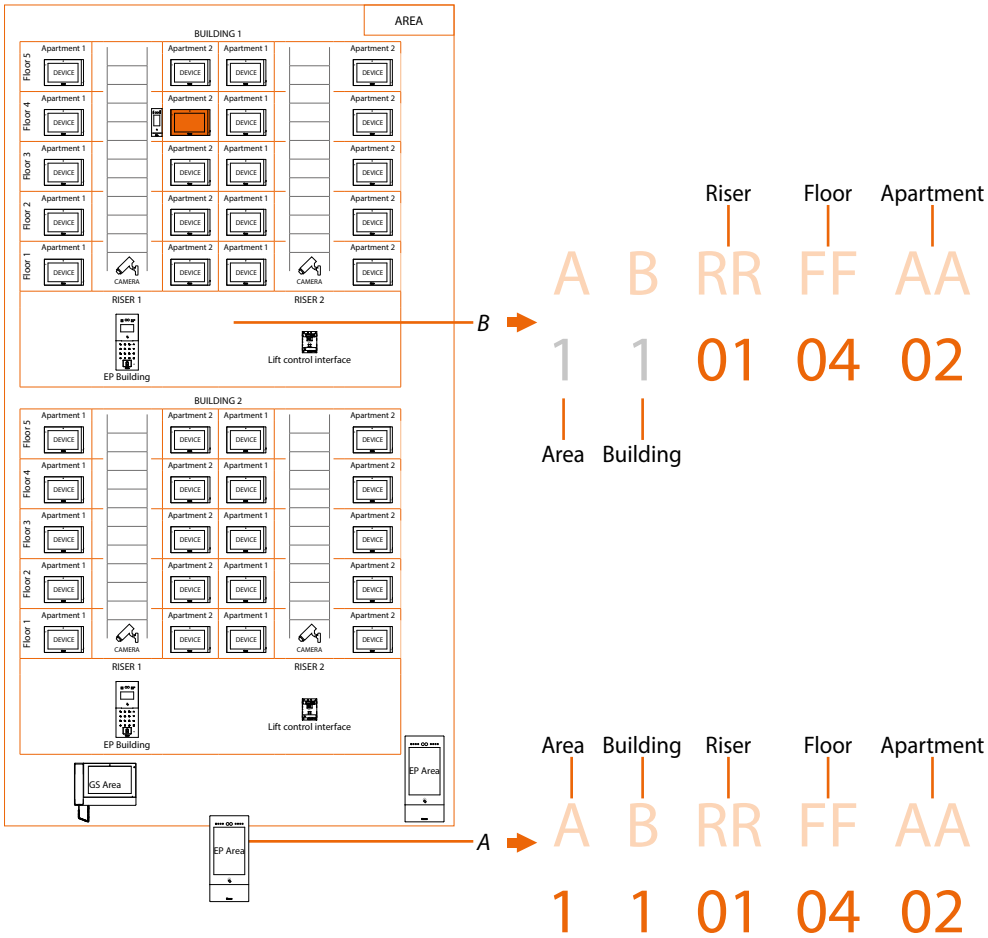
On the basis of data recorded in the system address book and the Community structure the calls can be made using various methods:

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

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 A EP, enter the corresponding address **11010402**;
- to call the IU highlighted in the diagram from the B EP, 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, Building 99, Riser 99, Floor 99, Apartment 99
The limits can be changed using the SD software.

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

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 itsel

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 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 guide (configuration flow)

Step 01
Check your system requirements

Step 02
Authenticate

Step 03
Create the community VLAN network

Step 04
Define the community structure

Step 05
Create the template (Advanced/Configuration of model parameters)

Step 06
Create a new structure

Or

Step 06
Import the existing AB and edit it

Step 07
Register the MAC addresses of the devices

Step 08
Registration of the Community on the installer's Cloud

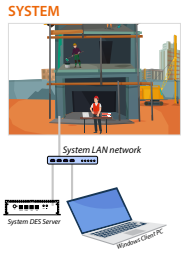
Step 09
Forwarding of the address book to the SD

Step 10
Install the devices, activate and update them (see Examples of system situations)

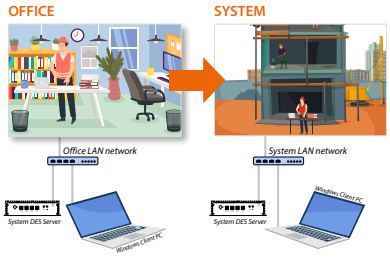
After installing and activating the devices, the SW can be used to:

- 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

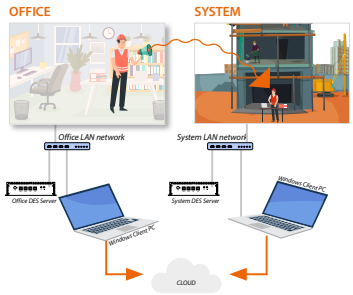
Installation examples



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.

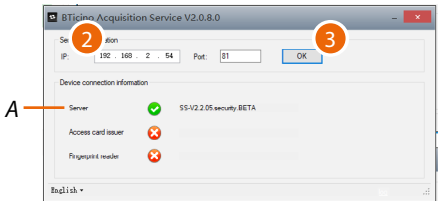
View all the steps required for the example

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.

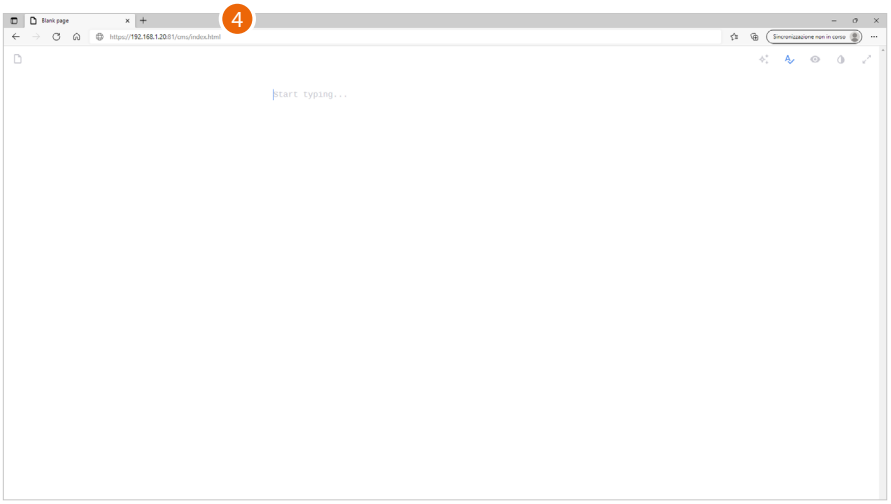
The following screen appears



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 MAC address identification (method 2).

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

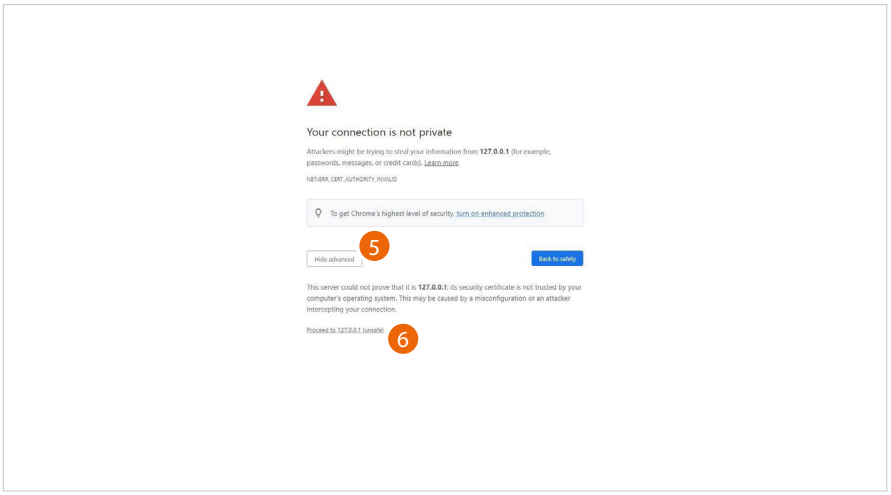


4. Open the browser and enter the http address of the DES Server:

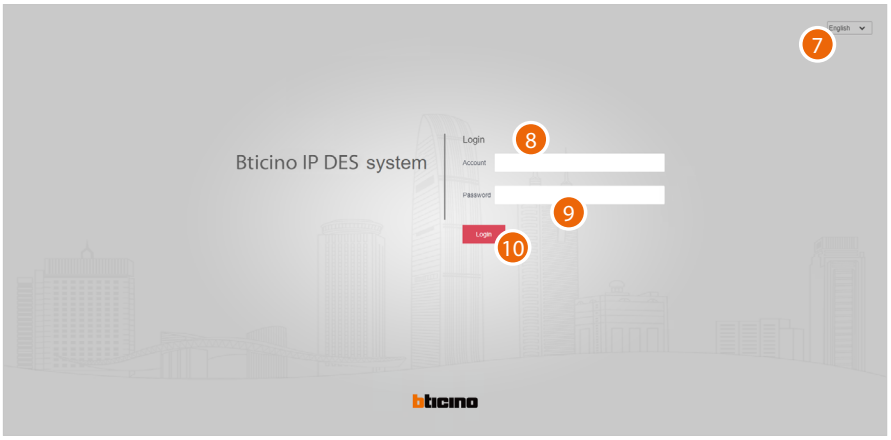
https://SD IP address:81/cms/index.html

Note: *use Crome/Edge browser and a screen with resolution 1920x1080*

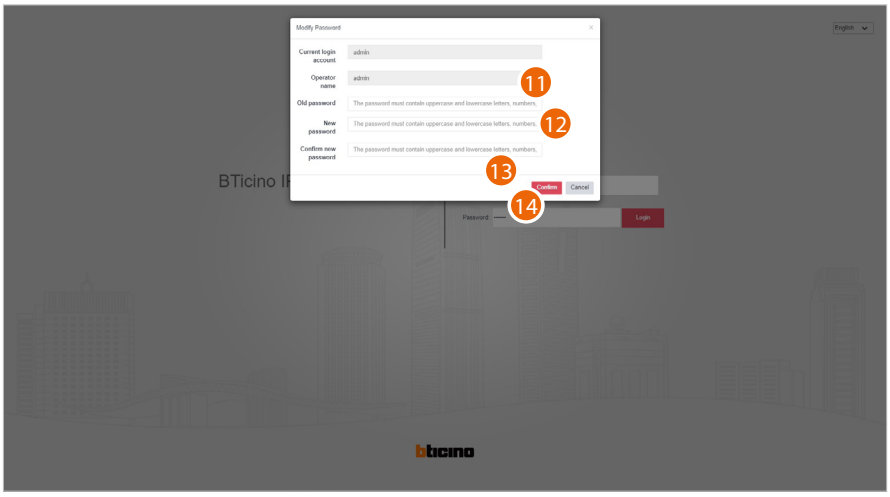
In some cases, the browser may consider the page to be unsafe.



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. Click to confirm

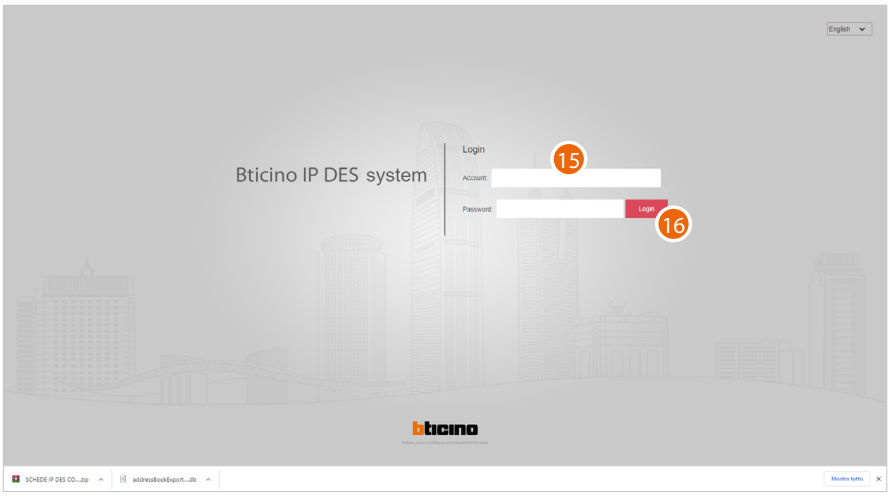


For security reasons, it is mandatory to change the default password; the new password must have the following characteristics:

- 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

***Note**: Store the password in a safe place, as if lost it cannot be recovered*



15. Enter the new data
16. Click to confirm

To change the password, go to the modify password section

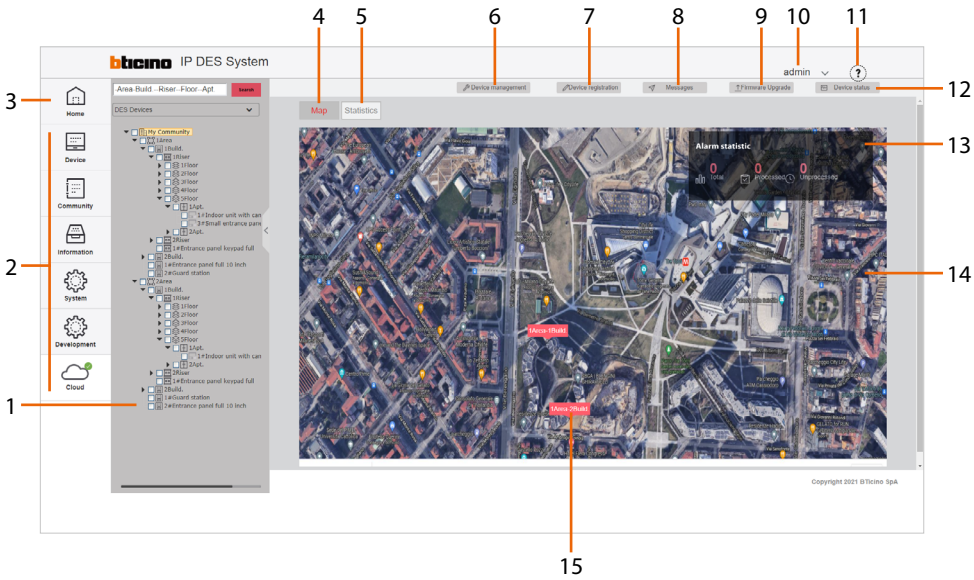
***Note**: The above procedure is completed using the admin profile, which allows full system management.*
Other profiles can be created for different roles on the operator management pages

Home Page

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

- 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.
- a menu tree for the management of the community structure.

In the centre section, in addition to shortcuts for certain functions, is a map page (to make it easier to find community buildings) and a statistics page.



1. Tree menu for creating the community structure and the management of levels and devices.
2. Main menu
3. Returns to the Home Page
4. Displays the map page (to add background images and markers; see map configuration)
5. Displays the statistics page
6. Displays the Device management (*) page
7. Displays the Device registration (*) page
8. Displays the Messages page
9. Displays the firmware update (*) page
10. Opens the logout menu and change password (*)
11. Displays the tutorial page
12. Displays the device status (* page)
13. Displays community alerts summary data
14. Map
15. Markers to identify the managed buildings

* Shortcut button to the sub-menus of the main menu

Statistics page

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

A Displays the percentage quantity of community devices

B Display filter of on/offline devices and registered/unregistered access

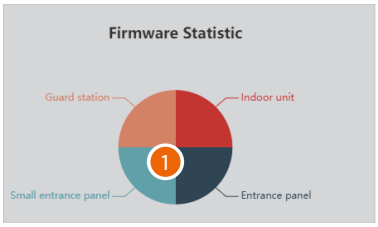
C Displays the percentage quantity of accesses opening types

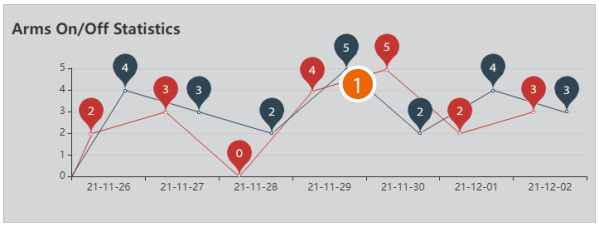
D Displays the percentage quantity of on/offline devices

E Displays how many alarms have occurred and in which dates

F Displays when and how many times the alarm system was armed/disarmed

G Displays the type and number of accesses

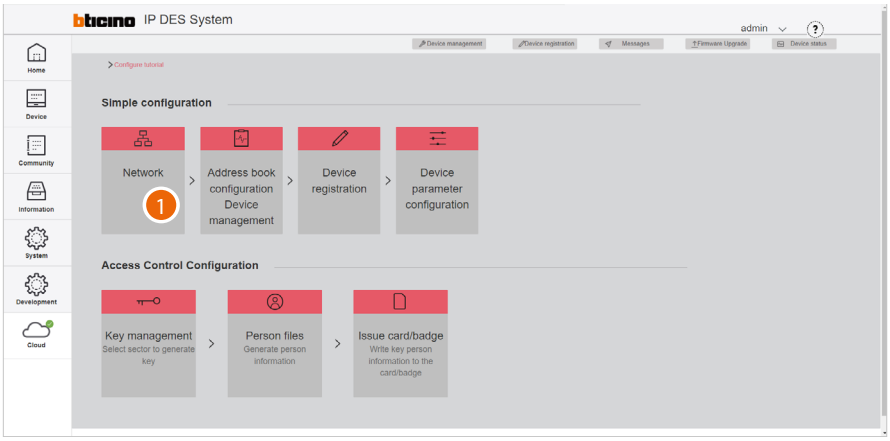




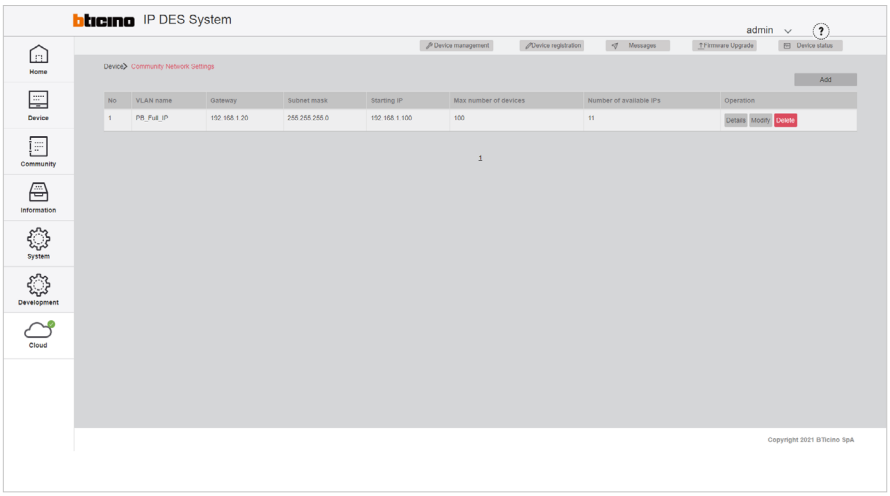
1. Click on the chart to view the numerical data

Configure tutorial

This page shows the essential steps for setting up a community, entering people data and managing entries.

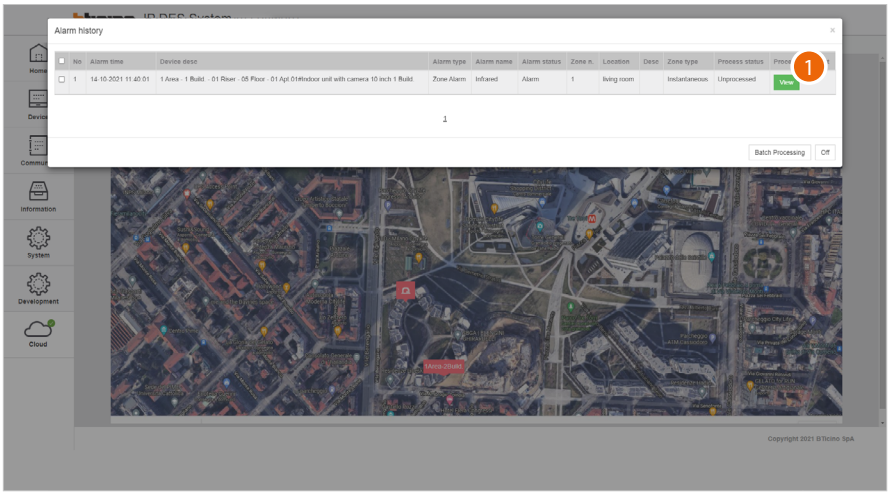


1. Clicking the steps of the procedure opens the relevant pages

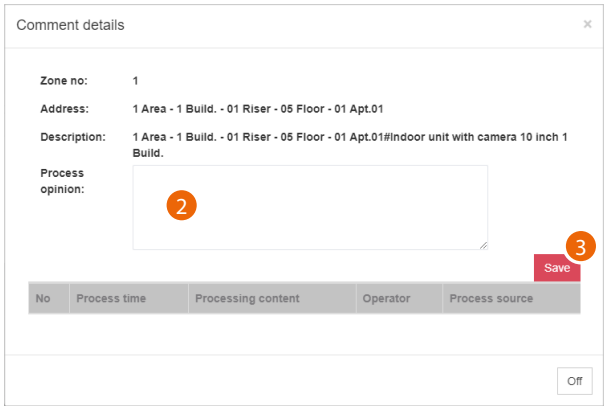


Alarms

When an alarm occurs in the community, a notice appears in the Home Page

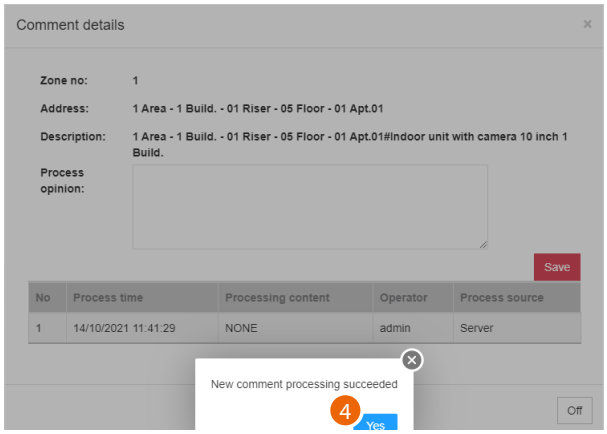


1. Click to display the details

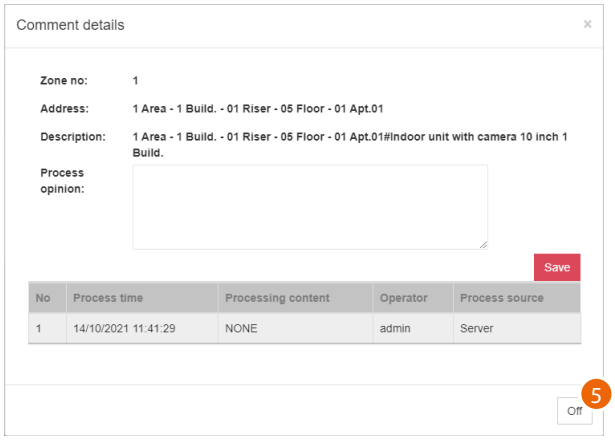


A panel opens, showing some alarm data, with a field for adding comments

2. Add a comment
3. Click to save



4. Click to confirm



5. The comment has been saved, click to confirm

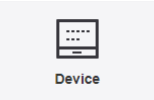
The alarm log is available in the **Information\alarm history** page

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

Main menu

 Home	Home Page	Returns to the Home Page
 Device	Device menu	It manages various aspects linked with community devices, such as the connecting data network, device registration, changing parameters, etc.
 Community	Community menu	Displays and manages community access functions, such as permissions, badges/cards etc.
 Information	Information menu	Displays various information about accesses, calls, alarms and more in the community.
 System	System menu	It displays and manages roles and operators as well as various functions related to the SW.
 Development	Development menu	Menu reserved to advanced developers.
 Cloud	Cloud menu	It allows, after authentication via an Installer account, to save a copy of the Community on the Installer's Cloud.

Device

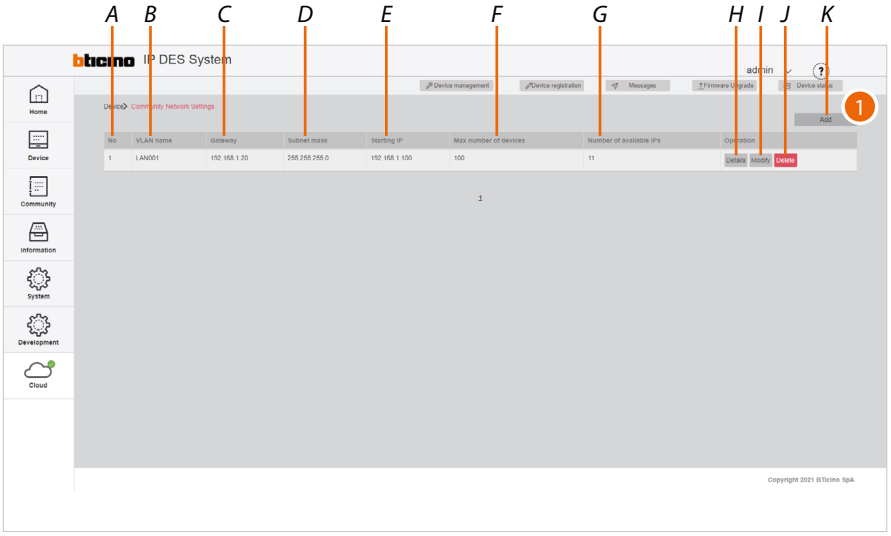


This menu allows to manage various aspects of the community devices, such as the data network that connects them, their registration, the modification of the parameters and so on.
It is also possible to update the firmware of the community devices.

Community Network Settings	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)
Device registration	Associates the MAC addresses of the physical devices with the virtual devices in the community
Standard Call with letters setting	Replaces letters with numbers in the addresses of the devices
Device parameter configuration	Reads/modifies/sends the advanced parameters
Background picture replacement	Imports new Home Page background images in addition to the default ones, and sends them to the device
Firmware Upgrade	Check, imports and sends firmware updates to the devices
Fire linkage	Activates and deactivates the Fire linkage function on the EP
Lift Control Function	Sets the parameters of the Lift Control function

Community Network Settings

This page can be used to create community networks or manage the existing ones.



A Community networks progressive number

B Name of the community VLAN network (letters and numbers without space)

C IP address of the gateway (router) used to access the Internet

D Subnet mask address

E Enter the starting address from which the IP addresses of IP devices will be generated (including Onvif IP cameras and interfaces item 375013) see Assignment of IP address range based on the number of video door entry devices

F Maximum number of IP devices that will be part of the Community

G Maximum number of IP addresses still available for association with new IP DES devices

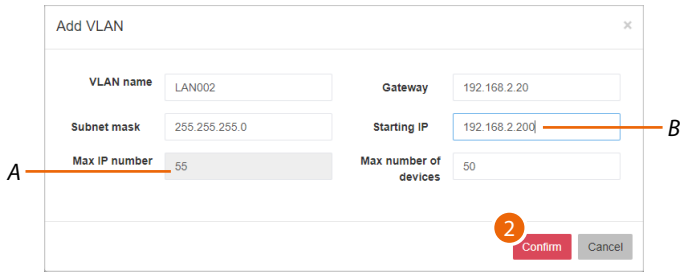
H Network devices

I Edits the network parameters

J Deletes the network

K Creates the network

1. Click to create a new network



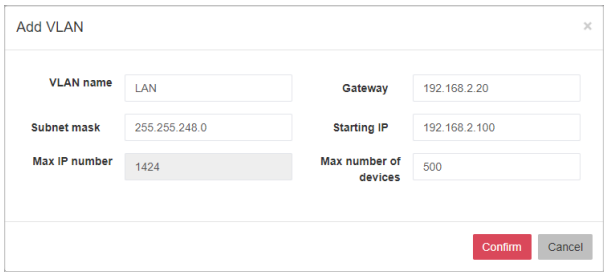
A Maximum number of IP DES devices that can be installed based on the data entered in the starting IP and subnet mask fields

B 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 192.168.2.199
Server software address management 192.168.2.200 up to 192.168.2.250

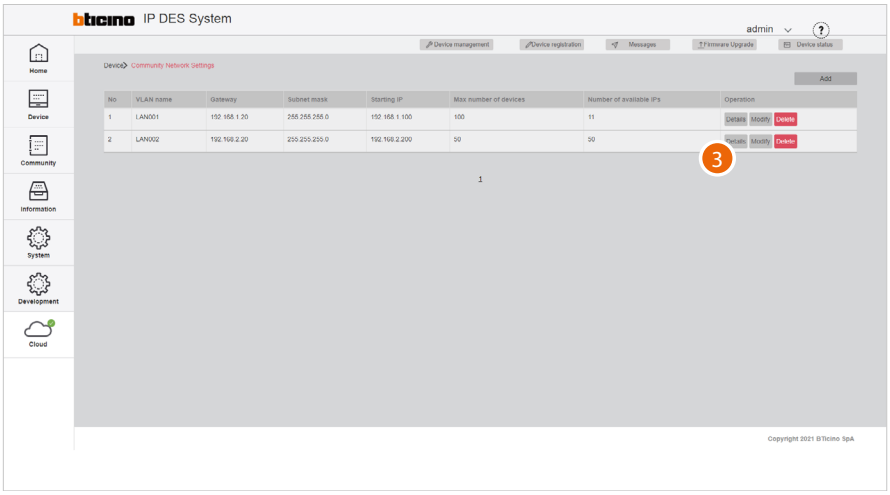
2. Enter the new network parameters and click to confirm.

Configuration examples

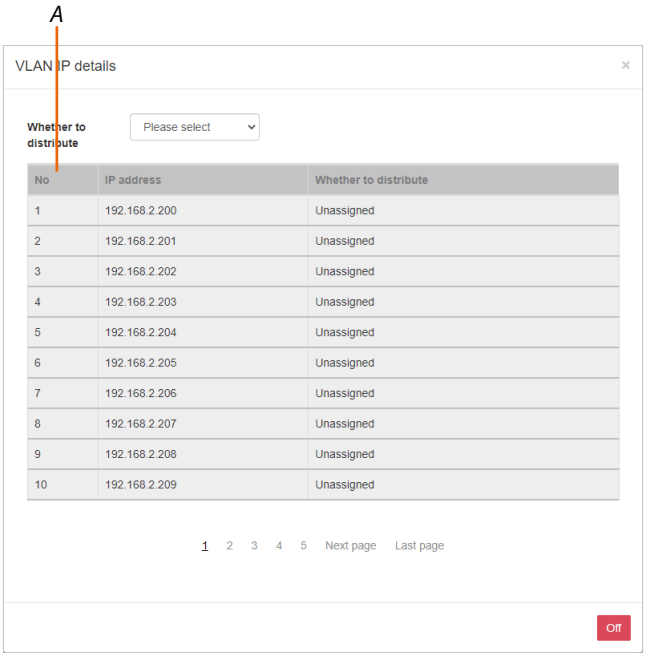
Changes in the network parameters (subnet mask) will also cause changes in the maximum number of addresses available (max IP number) for association with the devices



***Note**: If some IP addresses in the network are already being used by third parties, a network conflict may occur.*
This conflict will be indicated in the home page of the device. To correct it, set a different address; see *Editing of structural and network parameters (Edit)*



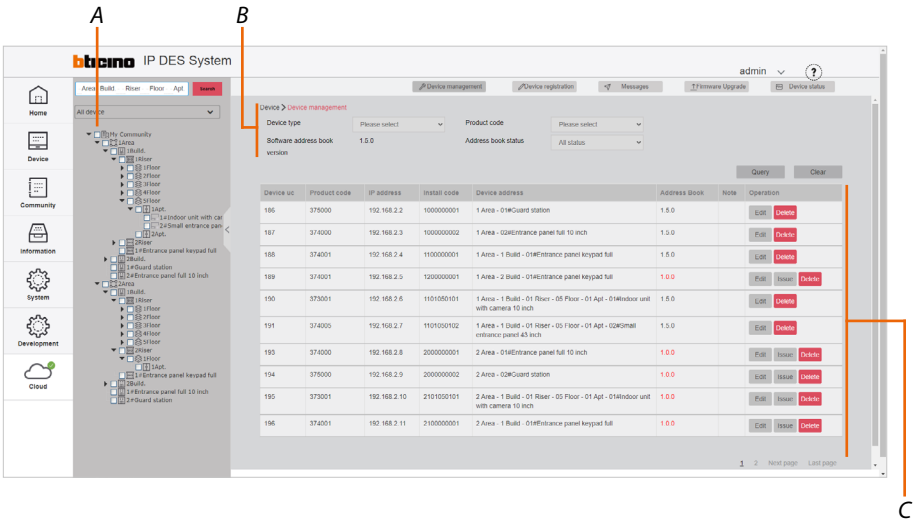
3. Click to display the network details



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

This page can be used to manage the community devices.



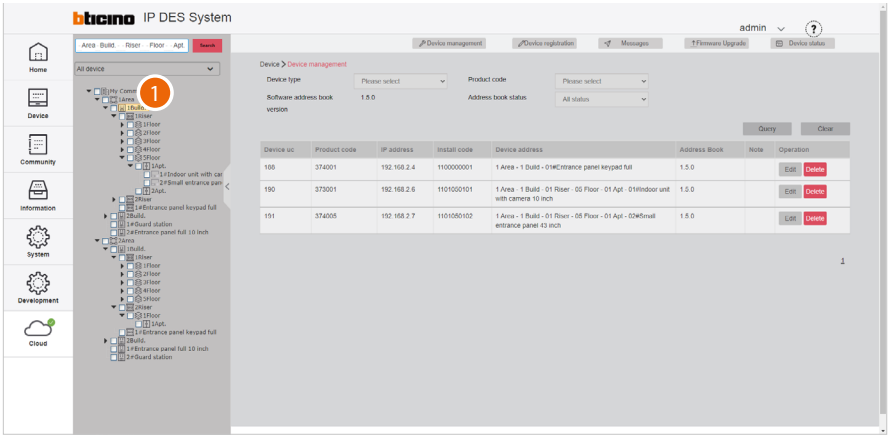
A Tree menu

B Device filters

C Device management zone

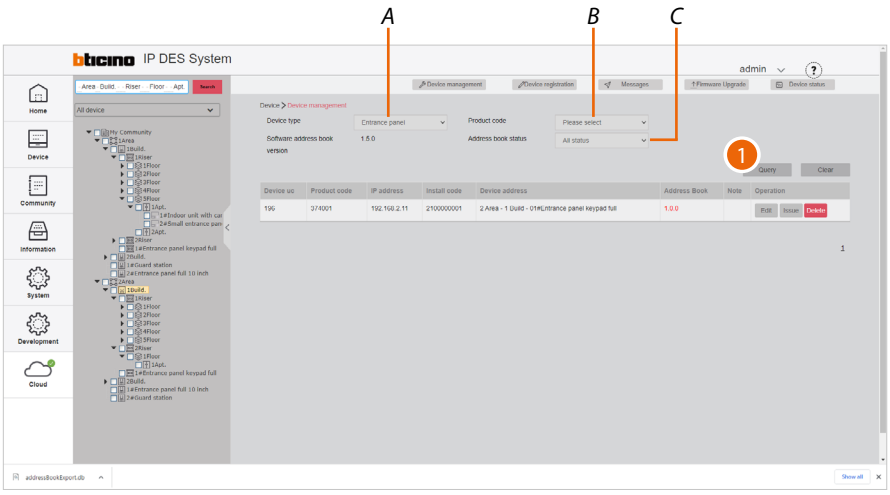
After adding the devices (see AddDevice), it will be possible to edit some of their data, send any changes to the physical devices, or delete them.

Selection of the devices to be managed using filters



1. Click to select the community level containing the device.
   The right-hand area shows all the devices present (e.g. Building 1 devices)

It is possible to use the filters to narrow down the search



A Type filter (EP, IU, etc.)

B Item code filter

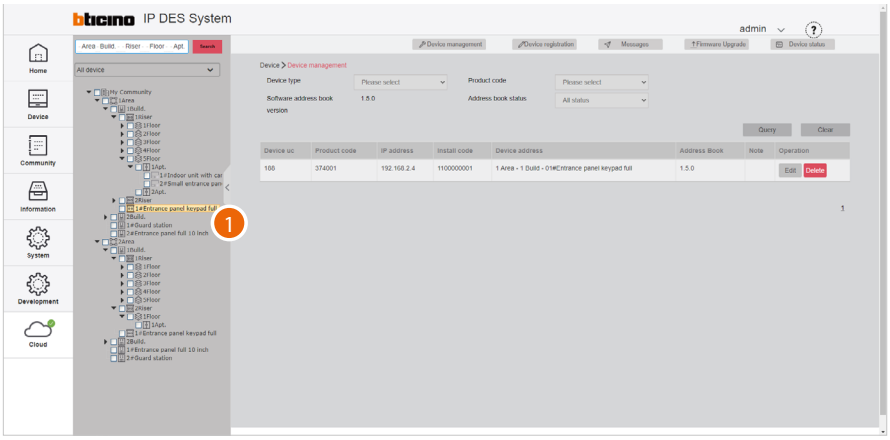
C AB status filter (AB synchronised with physical device, not synchronised, or both)

1. Click to apply

The system will only display devices meeting the filter criteria; in the example, EPs from Building 1

Direct selection of the device

If the location of the device is known, this can be selected directly from the tree menu



1. Navigate through the menu to the desired position and click to select the device

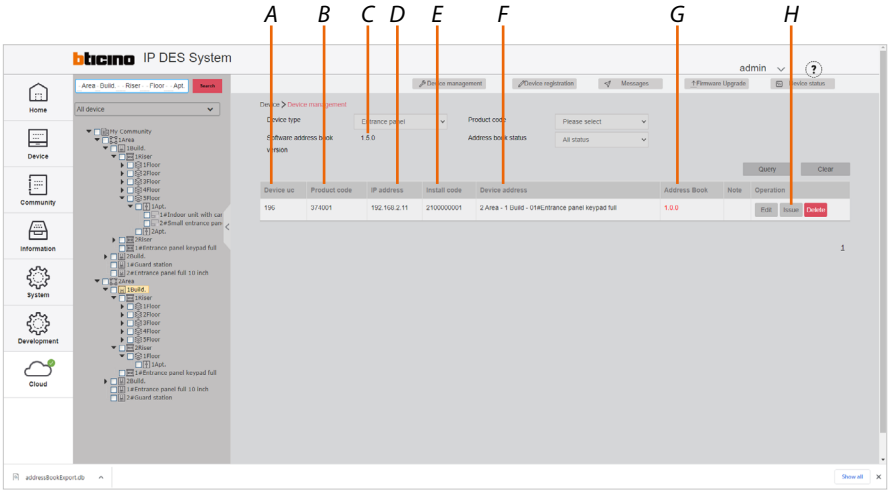
Device management

In this area it is possible to:

– Display and edit the structure and network parameters of the devices

– Update the AB of the single device

– Delete the devices



A Progressive number

B Item code

C AB version in the SW (see AB)

D Device network address

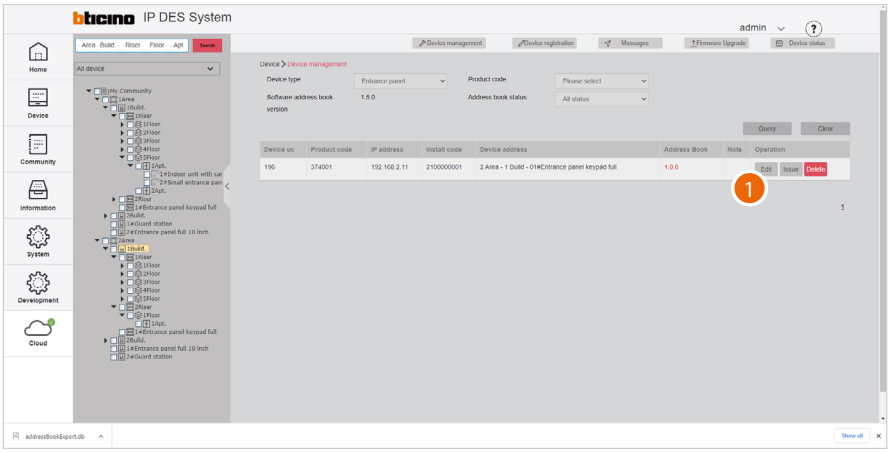
E Product installation code, a unique code that can be requested by community devices under certain configuration conditions (see the individual device manuals)

F Name of the device (customisable).
The original name represents the address of the device in the community.

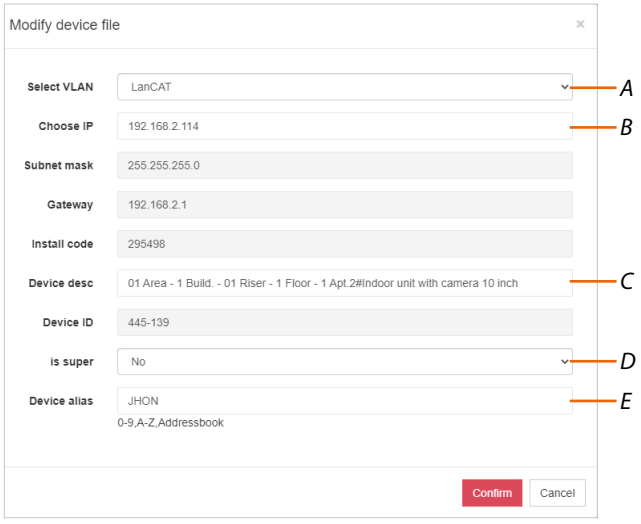
G AB version in the physical device.
The colour identifies the synchronisation status of the software and device AB.
Black = synchronized
Red = not synchronized

H Device management keys

Edit the structure and network parameters (Edit)



1. Click to edit



A Edit the device VLAN network

B Edit the device network address

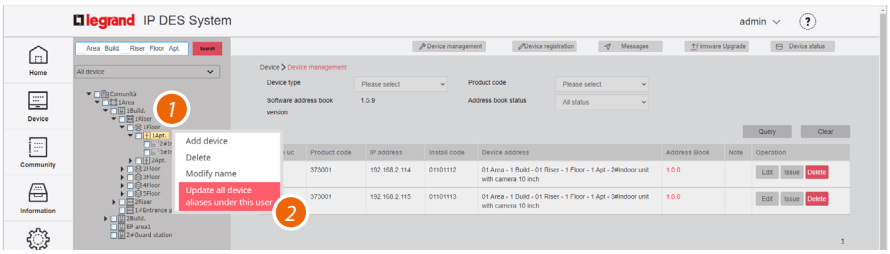
C Change the device name in the SW (does not change the call address)

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)

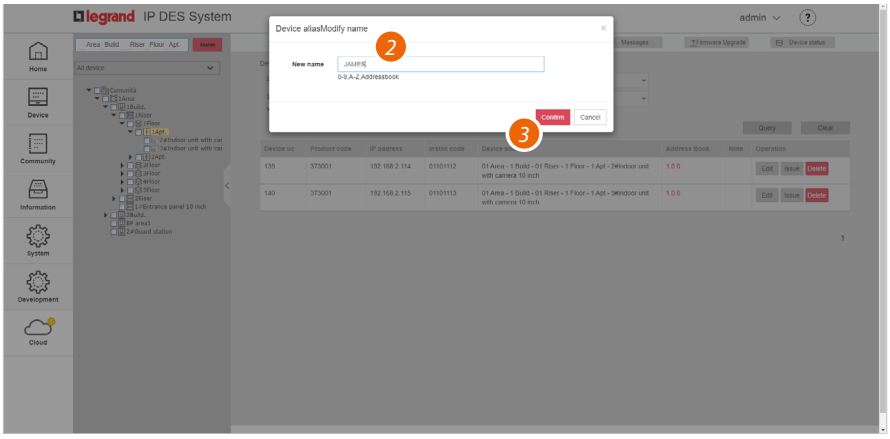
***Note**: parameter available only for EP*

E Modify the alias

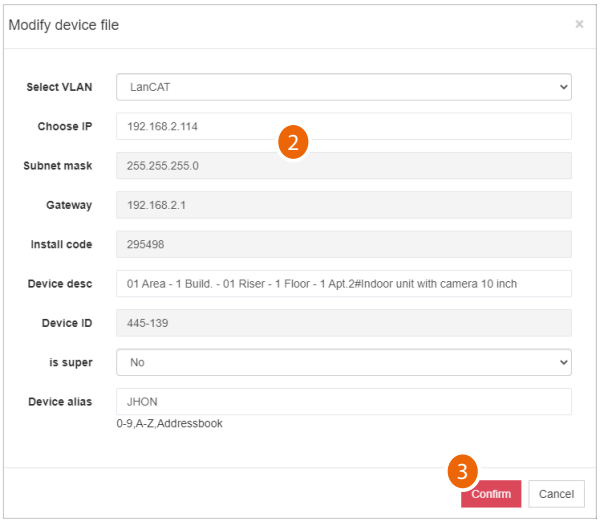
If you want to change the alias of all the devices inside the same apartment:



1. Right click the apartment
2. Click to change the alias of all the devices inside the same apartment



3. Modify the alias
4. Click to confirm

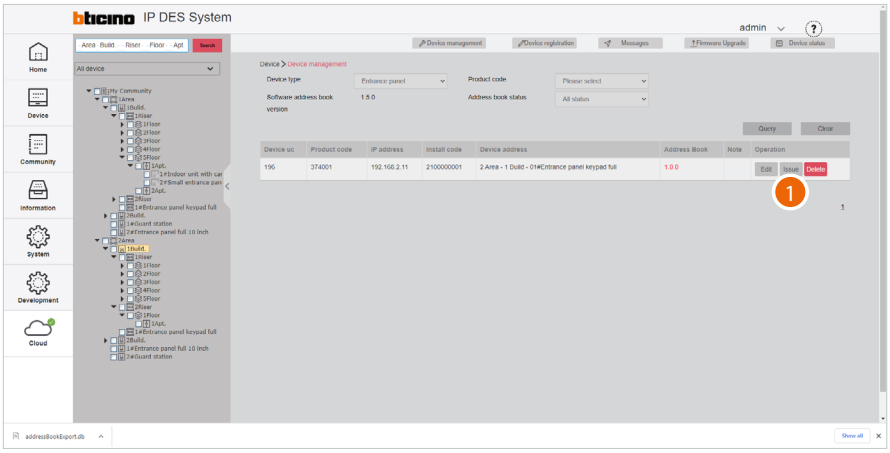


2. Edit the parameter
3. Click to confirm

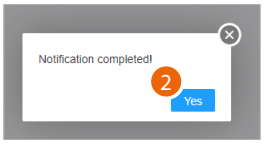
To **change the advanced device parameters** (e.g. ring volume, installer password etc.), see Device parameter configuration

***Please note**: after changing these parameters, it will be necessary to restart the device.*

Send parameters to the physical devices (Issue)

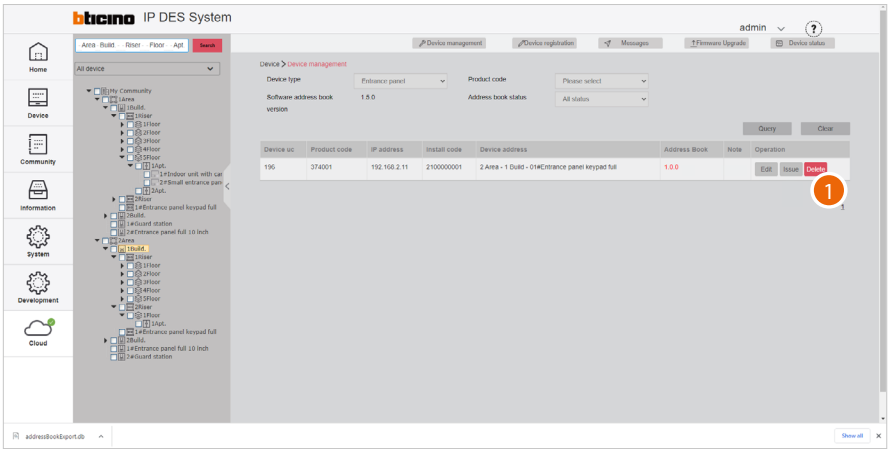


1. Click to send the parameters to the physical device

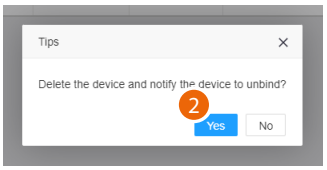


2. Click to confirm

Delete the devices



1. Click to delete the device

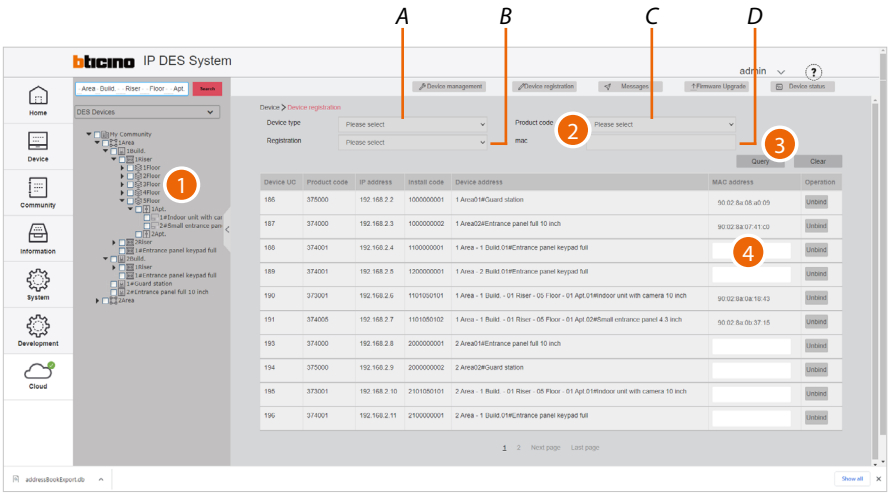


2. Click to confirm

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

Device registration

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



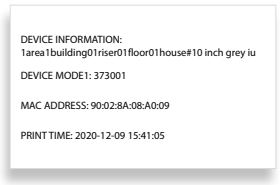
1. Select the community branch that contains the devices to be associated
2. If necessary, use the filters to narrow down the selection:

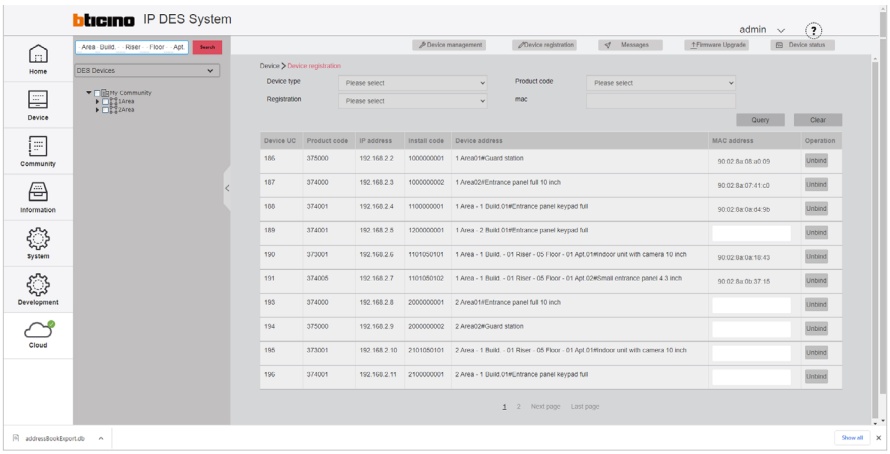
A *Type of device*
B *Registered/unregistered devices*
C *Item code*
D *MAC address (to directly select a device when the MAC address is known)*

3. Click to apply the filter
4. 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 :).

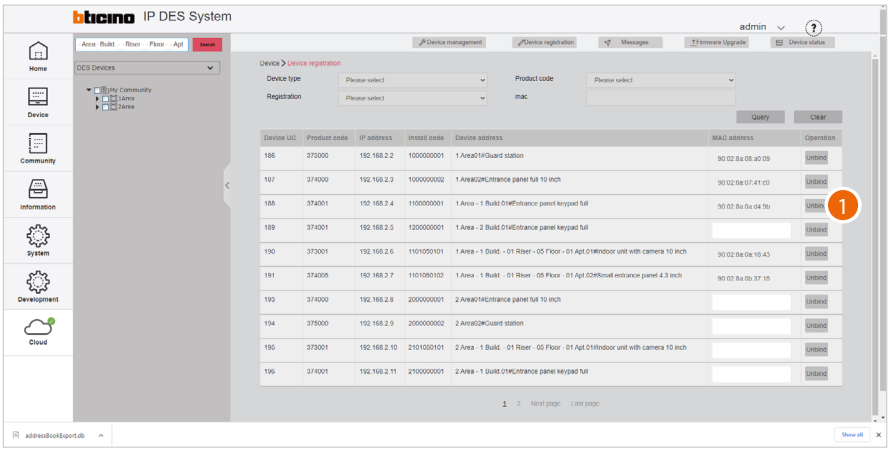
If the printer is connected to the network and set up, it will automatically print the label which must then be applied to the device box in order to immediately identify the apartment or position in which to install it.





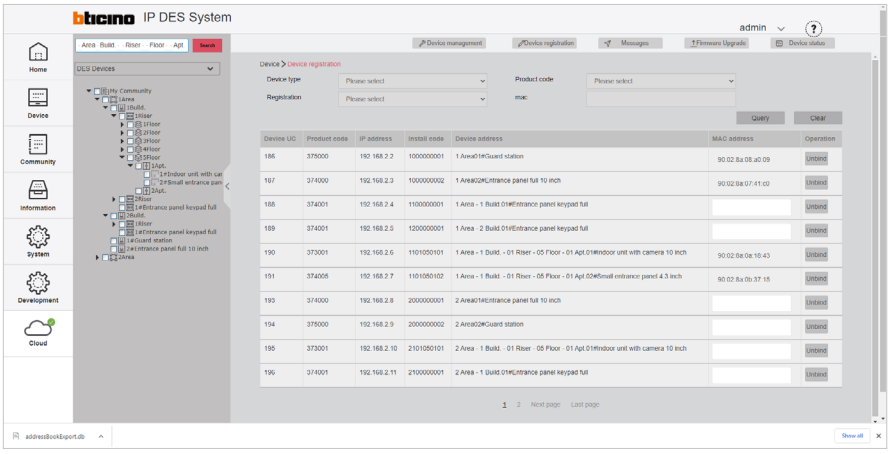
Dissociate the device

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



1. Click to dissociate

2. Click to confirm
3. Click to continue

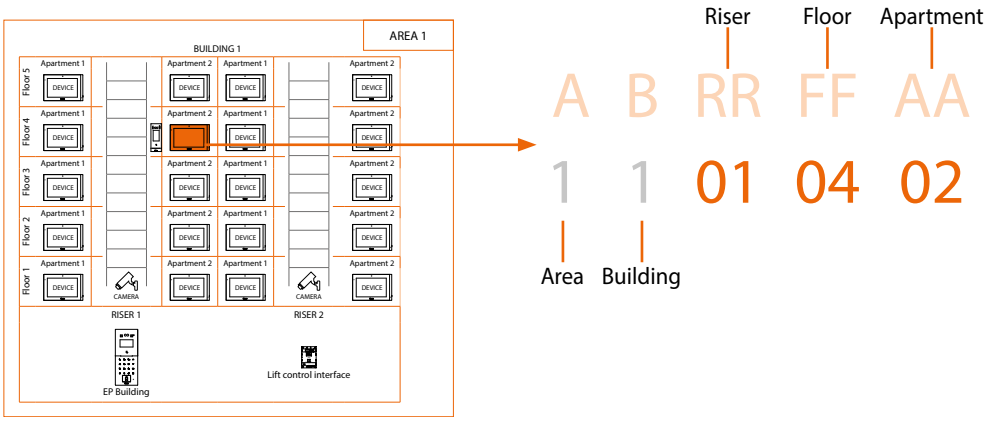


The virtual device can now be associated with another physical device by entering the MAC address.

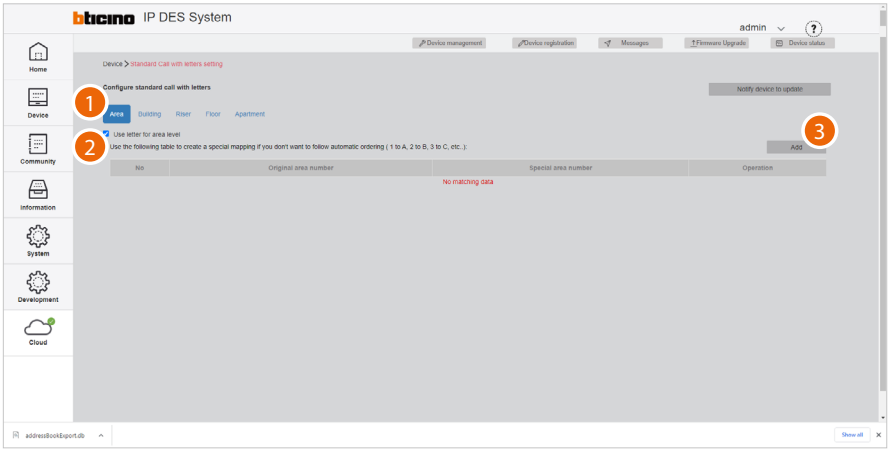
Standard Call with letters setting

Community devices are identified with an address based on their position within the structure. This address is used in the communications between devices (e.g. call from EP to IU, call between IUs etc.).
By default, the system uses numbers to identify the various levels of the structure.

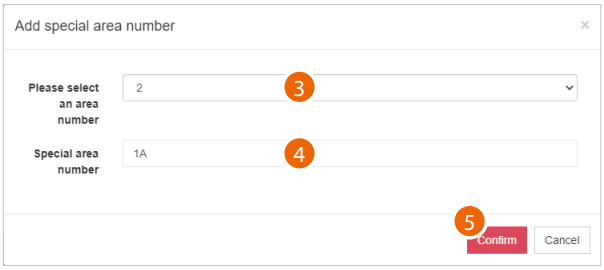
Example:



This page can be used to **replace numbers with letters** (e.g. numbers that cannot be used for cultural reasons).

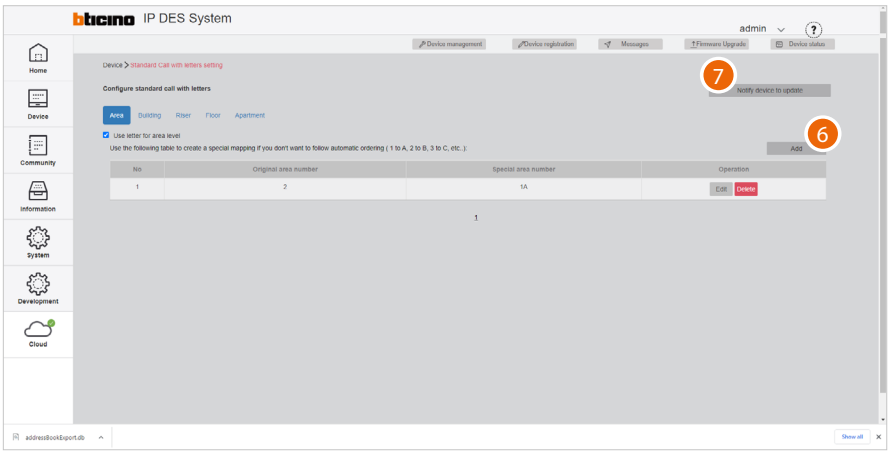


1. Click the level.
2. Click to define the use of letters for the level
3. Click to continue



Since the number of floors is normally very high, and therefore letters replacing numbers may not be enough, a combination of numbers and letters may also be used.

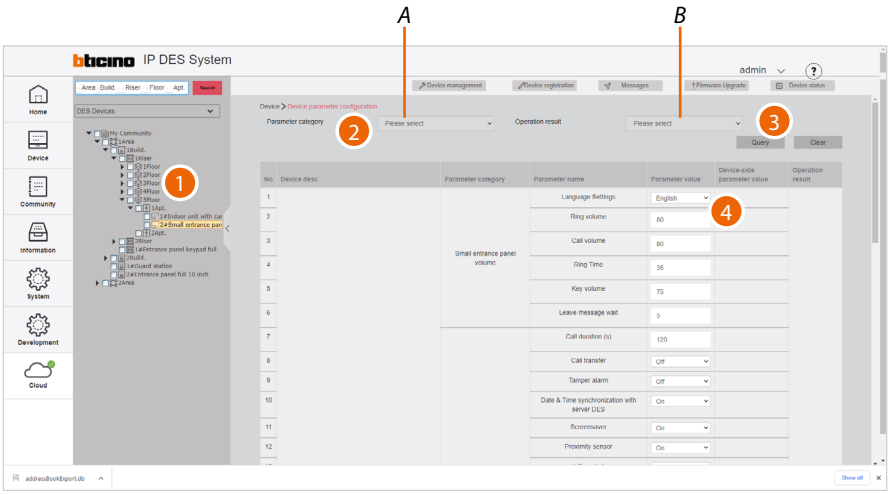
3. Select the number of Floors to be replaced with a combination of numbers and letters.
4. The system suggests a combination, which can be replaced with a letter or another combination of your choice.
5. Click to confirm



6. Click to add another combination
7. Click to send the configuration to the devices

Device parameter configuration

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.



1. Select the community branch containing the devices to be modified
2. If necessary, use the filters to narrow down the selection:

A *Type of parameters*

B *Indicates if the last operation (reading or writing) was completed successfully*

3. Click to apply the filter
4. On the right-hand side, a table with all editable parameters is displayed for each device (example: if building 1 is selected in the tree menu and IU in the filters, the tables of all IU in building 1 will be displayed)

You can now use the context sub-menu:

– Read the parameters on the physical devices

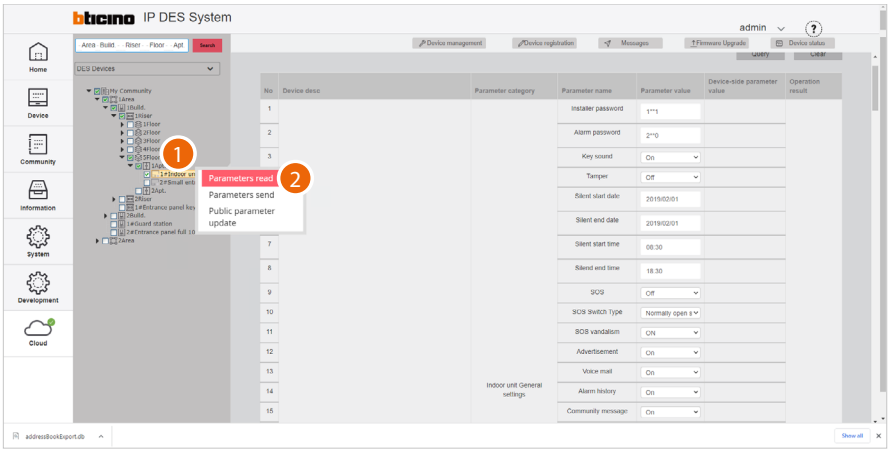
– Edit the parameters

– Send them to the system

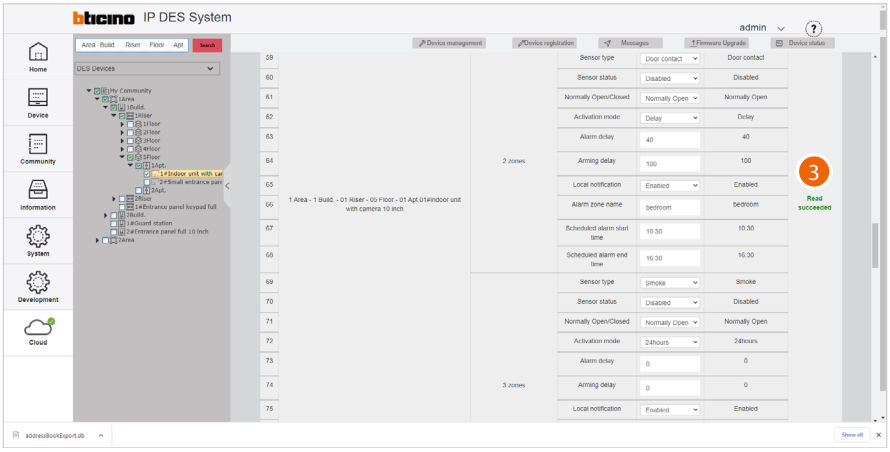
– Edit the public parameters

Read the parameters

This function allows to view the parameters set on the physical device.



1. Tick the device of which you want to read the parameters
2. Click to send the command



3. A message will be displayed if the operation is successful

Edit the parameters
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 adjustable parameters depend on the type of device (see the specific tables of the devices):

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

Note: *the new added devices will use the set parameters by default*

373001/02/03/04/05/06/07 IU PARAMETERS				
Parameter category	**Parameter name**	**Function description**	**Values**	**Position in the device menus**
Indoor Unit General settings	*Installer password*	*Set the password to access the installer menu **	*1111*	*Settings/Installation/**installation access code***
	Alarm password	*Set the password for the management and configuration of the alarms **	*2000*	*Settings/Access code/**alarm password***
	Key sound	*Enable / Disable the confirmation tone of the display icons*	*on / off*	*Settings/Preferences/function/**the key sound***
	Tamper	*Enable / Disable local tamper*	*close / on*	*Settings/Installation/function/**tamper***
	Silent start date	*Set the start date of the DO NOT DISTURB mode in conjunction with the time*	*date*	*Settings/shortcut/**silent mode***
	Silent end date	*Set the end date of the DO NOT DISTURB mode in conjunction with the time*	*date*	*Settings/shortcut/**silent mode***
	Silent start time	*Set the start time of the DO NOT DISTURB mode in conjunction with the date*	*time*	*Settings/shortcut/**silent mode***
	Silend end time	*Set the end time of the DO NOT DISTURB mode in conjunction with the date*	*time*	*Settings/shortcut/**silent mode***
	SOS	*Enable / Disable the SOS GND input in the alarm terminal block*	*on / off*	*Settings/Installation/alarm setting/advanced/**SOS enable***
	SOS Switch Type	*Set the status of the SOS GND input in the alarm terminal block*	*Normally open switch / Normally closed switch*	*Settings/Installation/alarm setting/advanced/**open normally***
	SOS vandalism	*Set if the SOS GND input in the alarm terminal block checks for short circuits and wire cuts in addition to the alarm signal*	*yes / no*	*Settings/Installation/alarm setting/advanced/**SOS vandalism***
	Advertisement	*Enable / Disable the display of incoming advertising information from the Guard Station*	*on / off*	*Settings/Installation/function/**advert***
	Voice mail	*Enable / Disable the display of video answering system messages*	*on / off*	*Settings/Installation/function/**leave message***
	Alarm history	*Enable / Disable the display of the alarm log*	*on / off*	*Settings/Installation/function/**alarm message***
	Community message	*Enable / Disable the display of service information from the software*	*on / off*	*Settings/Installation/function/**community message***
	Access history	*Enable / Disable the display of entrance access information*	*on / off*	*Settings/Installation/function/**access message***
	Family Message	*Enable / Disable the display of messages from family members*	*on / off*	*Settings/Installation/function/**family message***
	Emergency message	*Enable / Disable the display of incoming emergency information from the software*	*on / off*	*Settings/Installation/function/**emergency message***
	Call	*Enable / Disable the CALL in HOMEPAGE function*	*on / off*	*Settings/Installation/function/**call***
	Message	*Enable / Disable the MESSAGE in HOMEPAGE function*	*on / off*	*Settings/Installation/function/**message***

*see the "make the password visible" procedure

373001/02/03/04/05/06/07 IU PARAMETERS				
Parameter category	**Parameter name**	**Function description**	**Values**	**Position in the device menus**
Indoor Unit General settings	*Camera*	*Enable / Disable the CAMERA in HOMEPAGE function*	*on / off*	*Settings/Installation/function/**camera***
	Alarm	*Enable / Disable the ALARM in HOMEPAGE function*	*on / off*	*Settings/Installation/function/**alarm***
	Lift control	*Enable / Disable the LIFT CONTROL function in the shortcut page*	*on / off*	*Settings/Installation/function/**lift***
	Common areas camera	*Enable / Disable the display of the COMMON AREA in the room page*	*on / off*	*Settings/Installation/function/**common area***
	Call apt.	*Enable / Disable the display of the ENTRANCE PANEL in the room page*	*on / off*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Setting	*Enable/disable the display of the Settings on the Home page*	*on / off*	*Settings/Installation/function/**Setting***
	Block all the intercom	*Enable/disable call block for all IUs*	*on / off*	*Call/Blacklist/**Block all the intercom***
	Blacklist	*Enable/disable blacklist display on the call-page*	*on / off*	*Settings/Installation/function/**Blacklist***
Indoor unit call and display	*Screen brightness*	*Set the screen brightness level*	*10 – 100*	*Settings/preference/display/**brightness***
	Screensaver Time	*Set the screen saver activation delay*	*10 – 120*	*Settings/preference/display/**screensaver***
	Ring volume	*Set the ringtone level*	*0 – 100*	*Settings/preference/ringtone/**ring volume***
	Call Volume	*Set the audio level*	*0 – 100*	***PARAMETER THAT CAN BE ADJUSTED DURING THE CALL***
	Ring Time	*Set the ringtone time*	*19 – 35*	*Settings/preference/ringtone/**ring time***
	Ringback tone	*Select the call confirmation ringtone*	*ring 1.wav ring 6.wav*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Apt. entrance panel ringtone	*Select the ringtone for EP calls*	*ring1.wav ring6.wav*	*Settings/ringtone/Entrance panel/**ringing tone***
	Entrance panel ringtone	*Select the ringtone for SEP calls*	*ring1.wav ring6.wav*	*Settings/ringtone/apartment entrance panel/**ringing tone***
	Indoor unit ringtone	*Select the ringtone for IU calls*	*ring1.wav ring6.wav*	*Settings/ringtone/indoor unitl/**ringing tone***
	Guard station ringtone	*Select the ringtone for GS calls*	*ring1.wav ring6.wav*	*Settings/ringtone/guard station/**ringing tone***
	Language Settings	*Select the menu language*	*english - CHN traditional CHN simplified*	*Settings/**language***
	Video intercom	*Enable / Disable the video internal unit camera*	*on / off*	*Settings/Preferences/function/**local camera***
	Call duration	*Set the conversation time*	*60 – 120*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Shortcut key display	*maximum number of shortcuts available on the homepage*	*1#2#3#4*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
Zone Configuration	*Day start time*	*Set the start time of the daytime period for the CHECK ACTIVITY function*	*time*	*Settings/Installation/alarm setting/advanced/**day time***
	Night start time	*Set the start time of the night time period for the CHECK ACTIVITY function*	*time*	*Settings/Installation/alarm setting/advanced/**night time***
	Day time	*Set the time during which the CHECK ACTIVITY function indicates an alarm in case of non-detection in the daytime period*	*1 – 12*	***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*	*1 – 12*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Zone vandalism	*It sets the type of alarm detection (from F1 to F8), which can be of two types*	*on Enabled (Detection of open - closed - cable cutting - short circuit)*	*Settings/Installation/alarm setting/**Zone vandalism***
			off Disabled (Detection of open - closed)	

373001/02/03/04/05/06/07 IU PARAMETERS				
Parameter category	**Parameter name**	**Function description**	**Values**	**Position in the device menus**
Background image configuration	*Background picture*	*Select the device background*	*Background 1 – 5*	*Settings/preference/display/**background picture***
1-8 zone	*Sensor type*	*Select the type of sensor based on the device*	*Infrared / Magnetic contact / Smoke / Gas / SOS / Others*	*Settings/Installation/alarm setting/edi alarm zone/**sensor type***
	Sensor status	*Enable / Disable the terminal block input for the sensor*	*Disabled / Enabled*	*Settings/Installation/alarm setting/edit alarm zone/ **sensor enable***
	Normally Open/ Closed	*Select the sensor input status*	*Normally open / Normally closed*	*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*	*24-hoir zone*	*Settings/Installation/allarm setting/edit allarm zone/ **activation mode***
		The alarm is notified with a delay in relation to the occurring of the condition (set value in alarm delay) The alarm is notified with a delay in relation to the command given by the user (set the value in arming delay)	*Delayed*	
		The alarm is immediately communicated	*instantaneous*	
		The alarm is communicated immediately, if the sensor does not detect activities for a preset time	*Activity check*	
		Scheduled activation	*Scheduled allarm*	
	Alarm delay	*Set the alarm notification delay (see the IU manual)*	*0 – 255*	*Settings/Installation/allarm setting/edit allarm zone/ activation mode/**alarm delay***
	Arming delay	*Set the alarm activation delay (see the IU manual)*	*0 – 255*	*Settings/Installation/allarm setting/edit allarm zone/ activation mode/**arm delay***
	Local notification	*Enable or disable the sound trigger in case of alarm*	*Enabled / Disabled*	*Settings/Installation/allarm setting/edit allarm zone/**local notificaions***
	Alarm zone name	*Set the sensor name*	*Nome (es living room)*	*Settings/Installation/allarm setting/edit allarm zone/ **alarm zone name***
	Zone status	*Set the zone default status*	*Arms / Alarm / Arm delay status / Alarm delay status / disabled / disarm*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Scheduled alarm start time	*Set the scheduled alarm start time*	*Time*	*Settings/Installation/allarm setting/edit allarm zone/ activation mode/**scheduled***
	Scheduled alarm end time	*Set the scheduled alarm end time*	*Time*	*Settings/Installation/allarm setting/edit allarm zone/ activation mode/**scheduled***

375000 GS PARAMETERS				
Parameter category	**Parameter name**	**Function description**	**Values**	**Position in the device menus**
Guard station Transfer settings	Installer password	Set the password to access the installer menu *	1111	Settings/Installation/**password**
	Entrance panel	Enable/disable the "Quick Absence" function. When it is active the call is not intercepted by the GS but transferred directly to the IU to which it was originally addressed.	off / on	Absence/Quick absence/Direct to IUs
	Call transfer	Do not transfer calls	do not transfer	Settings/transfer settings/**no selection**
		Transfer calls if engaged in another call	transfer when busy	Settings/transfer settings/**busy transfer**
		Transfer calls if not answered within 30 seconds	do not answer transfers after 30 s	Settings/transfer settings/**no answer time**
		Transfer calls if engaged in another call or if not answered within 30 seconds	busy or not answering transfers after 30 s	Settings/transfer settings/**busy transfer + no answer time**
	No answer transfer time	Set the time after which to transfer the unanswered call	6 – 29 s	Settings/transfer settings/**no answer time**
	UC of the target guard station for scheduled absence	Select the guard station to which to transfer the call in case of scheduled absence for a long time	GS list	Settings/absence settings/**scheduled absence**
	UC of the target guard station for quick absence	Select the guard station to which to transfer the call in case of brief absence	GS list	Settings/absence settings/**quick absence**
	Transfer Call Mode	Select the absence mode	determinated by day and night time / always absent / always present	Settings/absence settings/**scheduled absence**
	Scheduled call transfer start time	Set the scheduled call transfer start time	time	Settings/absence settings/quick absence/**start time**
	Scheduled call transfer end time	Set the scheduled call transfer end time	time	Settings/absence settings/quick absence/**end time**
Guard station call and display	Screen brightness	Set the screen brightness level	10 – 100	Settings/display/**brightness**
	Ring volume	Set the ringtone level	1 – 100	Settings/ringtone/**volume of ring**
	Call volume	Set the audio level	1 – 100	**PARAMETER THAT CAN BE ADJUSTED DURING THE CALL**
	Ring Time	Set the ringtone time	15 – 35	**PARAMETER THAT CANNOT BE SET FROM THE DEVICE**
	Apartment entrance panel ringtone	Select the ringtone for entrance panel calls	ring1.wav ring6.wav	Settings/ringtone/apartment entrance panel/**ring tone**
	Unit VTO call ringtone file	Select the ringtone for SEP calls	ring1.wav ring6.wav	Settings/ringtone/apartment entrance panel/**ring tone**
	Indoor unit ringtone	Select the ringtone for internal unit calls	ring1.wav ring6.wav	Settings/ringtone/Indoor unit/**ring tone**
	Guard station ringtone	Select the ringtone for guard station calls	ring1.wav ring6.wav	Settings/ringtone/Guard station /**ring tone**
	Language Settings	Select the menu language	english - CHN traditional CHN simplified	Settings/**language**
	Screensaver time	Select the screen saver activation delay	10 – 120	Settings/display/**screensaver**
Background image configuration	Background picture	Select the device background	Background 1 – 5	Settings/display/**background picture**

*see the "make the password visible" procedure

374000/01/02/03 EP PARAMETERS				
Parameter category	**Parameter name**	**Function description**	**Values**	**Position in the 374000 device menus**
EP synchronization configuration	*Language Settings*	*Select the menu language*	*english - CHN traditional CHN simplified*	*Settings/**language***
	Ring volume	*Set the ringtone level*	*0 – 100*	*Settings/display & volume/**ringtone***
	Call volume	*Set the audio level*	*0 – 100*	*Settings/display & volume/**call***
	Ring time	*Set the call time duration*	*10 - 60*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Key volume	*Set the display icon/key pressing confirmation sound level*	*0 – 100*	*Settings/display & volume/**key tone***
	Leave message wait	*Duration of the message left on the video door entry system answering machine*	*5 -35*	*Settings/display & volume/**Leave message wait***
EP Engineering Configuration	*Call duration (s)*	*Set the conversation time*	*60 – 300*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Call transfer	*Enable/Disable forwarding of calls*	*off / on*	*Settings/setting/**tamper alarm enable***
	Tamper alarm	*Enable/Disable the tamper function*	*on / off*	*Settings/setting/**call forwarding enable***
	Date & Time synchronization with server DES	*Enable / Disable automatic synchronisation of date and time with the DES Server*	*on / off*	*Settings/date and time/**automatically sinc date and time***
	Local access code	*Enable / Disable the opening of the door lock with dedicated password for this entrance panel only **	*on / off*	*Settings/setting/**local access code***
	Screensaver	*Enable/Disable the screen saver*	*on / off*	*Settings/setting/**screen saver enable***
	Proximity sensor	*Enable/Disable the proximity sensor*	*on / off*	*Settings/setting/**proximity sensor enable***
	Lift control	*Enable / Disable the automatic lift call*	*on / off*	*Settings/setting/**lift control enable***
	Lift control mode	*Select the automatic lift call connection type and speed*	*9600 / 115200 / network / IP-Relay*	*Settings/lift control/**mode***
	Lift control protocol	*Display the lift protocol*	*bticino*	*Settings/Lift control/**lift control protocol***
	Lowest Floor	*Set the lowest structure floor level that can be reached by the lift*	*-5 / 5*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Number of lifts	*Set the number of lifts to manage*	*1 – 8*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Floor Number	*Set the number of floors*	*1 / 99*	***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*	*enter the address*	*Settings/lift control/mode/network/**master IP***
	Interlocked contact	*Select the status of the input contact for the Door status function*	*Normally open / Normally closed / not used*	*Settings/door lock/**door status***
	Electric Lock Setting	*Select if contact closure is impulsive or maintained*	*Impulsive lock / timed lock*	*Settings/door lock/**door lock***
	Unlock time	*Select the time during which the contact is maintained*	*2 – 255*	*Settings/door lock/**unlock time***
	Face recognition	*Enable/Disable the face recognition***	*on / off*	*Settings/setting/**face enable***
	Call management center machine	*It sets the EP reference GS*	*Enter the EP address*	*Settings/**Guard station***

*see the "make the password visible" procedure

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

374000/01/02/03 EP PARAMETERS				
Parameter category	**Parameter name**	**Function description**	**Values**	**Position in the 374000 device menus**
EP User Settings	*Installer password*	*Set the password to access the installer menu **	*2000*	*Settings/access code/**settings***
	EP local access code	*Set the local access code for this entrance panel*	*111111*	*Settings/access code/**local***
	Screen brightness	*Set the screen brightness level*	*10 – 100*	*Settings/display & volume/**brightness***
	Screensaver time	*Select the screen saver activation delay*	*30 / 60 / 120 / 300 / 600 s*	*Settings/display & volume/**screen saver***
	Ad play time	*Select the switch off time of the display*	*30 / 60 / 120 / 300 / 600 s*	*Settings/display & volume/**screen saver time***
Background image configuration	*Background*	*Select the display background*	*Background 1 – 5*	*Settings/**background***

374004/05 SEP PARAMETERS				
Parameter category	**Parameter name**	**Function description**	**Values**	**Position in the device menus**
Small entrance panel volume	*Language Settings*	*Select the menu language*	*english - CHN traditional CHN simplified*	*Settings/**language***
	Ring volume	*Set the ringtone level*	*0 – 100*	*Settings/display & volume/**ringtone***
	Call volume	*Set the audio level*	*0 – 100*	*Settings/display & volume/**call***
	Ring time			
	Key volume	*Set the display icon/key pressing confirmation sound level*	*0 – 100*	*Settings/display & volume/**key tone***
	Leave message wait			
Small entrance panel general settings	*Call duration (s)*	*Set the conversation time*	*60 – 300*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Call transfer	*Enable/Disable forwarding of calls*	*on / off*	*Settings/setting/**call forwarding enable***
	Tamper alarm	*Enable/Disable the tamper function*	*on / off*	*Settings/setting/**tamper alarm enable***
	Date & Time synchronization with server DES	*Enable / Disable automatic synchronisation of date and time with the DES Server*	*on / off*	*Settings/Date and time/**automatically sinc date and time***
	Screensaver	*Enable/Disable the screen saver*	*on / off*	*Settings/setting/**screen saver enable***
	Proximity sensor	*Enable/Disable the proximity sensor*	*on /off*	*Settings/setting/**proximity sensor enable***
	Lift control	*Enable / Disable the automatic lift call*	*on / off*	*Settings/setting/**lift control enable***
	Lift control mode	*Select the automatic lift call connection type and speed*	*9600 / 115200 / network / IP-Relay*	*Settings/Lift control/**mode***

*see the "make the password visible" procedure

374004/05 SEP PARAMETERS				
Parameter category	**Parameter name**	**Function description**	**Values**	**Position in the device menus**
Small entrance panel general settings	*Lift control protocol*	*Display the lift protocol*	*bticino*	*Settings/Lift control/**Lift control protocol***
	Lowest Floor	*Set the lowest structure floor level that can be reached by the lift*	*- 5 / 5*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Number of lifts	*Set the number of lifts to manage*	*1– 8*	***PARAMETER THAT CANNOT BE SET FROM THE DEVICE***
	Floor Number	*Set the number of floors*	*1 / 99*	***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*	*enter the address*	*Settings/Lift control/mode/network/**master IP***
	Interlocked contact	*Select the status of the input contact for the Door status function*	*Normally open / Normally closed / not used*	*Settings/door lock/**door status***
	Electric Lock Setting	*Select if contact closure is impulsive or maintained*	*Impulsive lock/ timed lock*	*Settings/door lock/**door lock***
	Unlock time	*Select the time during which the contact is maintained*	*2 – 255*	*Settings/door lock/**unlock time***
	Face recognition	*Enable/Disable the face recognition***	*on / off*	*Settings/setting/**face enable***
	Scan QR Prompt Tone	*FUNCTION NOT AVAILABLE*	*off / on*	***FUNCTION NOT AVAILABLE***
	Call management center machine	*It sets the EP reference GS*	*Enter the EP address*	*Settings/**Guard station***
	Resident Area	*Set the address of the IU to call*	*0 – 999*	***FUNCTION NOT AVAILABLE***
	Resident Build			
	Resident Riser			
	Resident Floor			
	Resident Apt.			
Small entrance panel display	*Installer password*	*Set the password to access the installer menu **	*2000*	*Settings/access code/**settings***
	Screen brightness	*Set the screen brightness level*	*10 – 100*	*Settings/display & volume/**brightness***
	Screensaver time	*Select the screen saver activation delay*	*30 / 60 / 120 / 300 / 600s*	*Settings/display & volume/**screen saver***
	Ad play time	*Select the switch off time of the display*	*30 / 60 / 120 / 300 / 600 s*	*Settings/display & volume/**screen saver time***
	door code	*Set the access code to enter the building*	*Enter the code*	*Settings/access code/local*
Background image configuration	*Background*	*Select the display background*	*Background 1 – 5*	*Settings/**background***

*see the "make the password visible" procedure

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

Make the password visible

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

The randomly assigned passwords are:

IU installer password

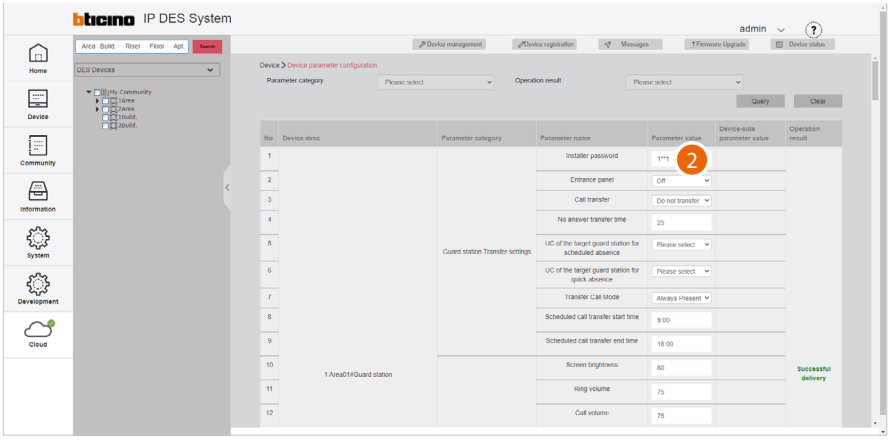
IU **alarm password** (to be communicated to the user)

GS installer password

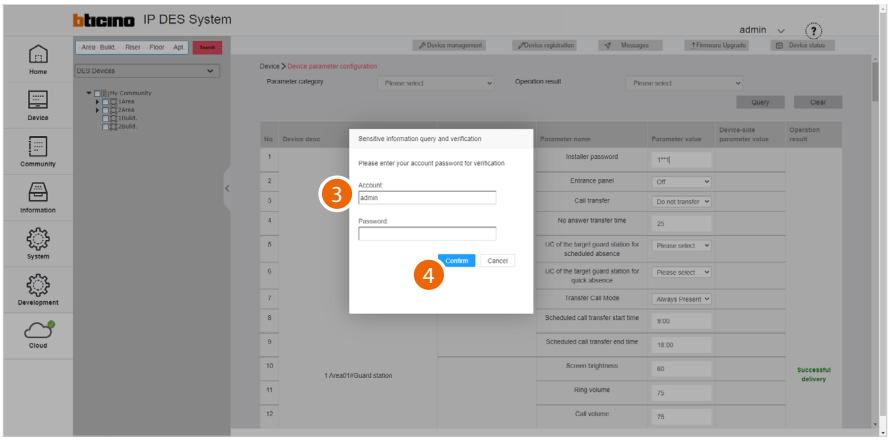
EP installer password – EP local access code

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

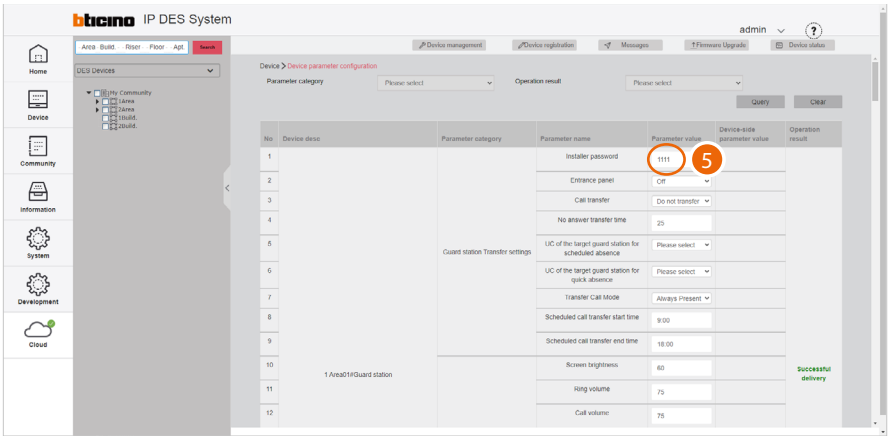
1. Go to the Device/Device parameter configuration menu



2. Click the password field of any of the devices



3. Enter the software authentication details
4. Click to confirm



5. The passwords are now visible.
   This operation reveals the passwords of all the devices.
   If you leave the page and then come back, the passwords will no longer be visible and you will have to repeat the operation.

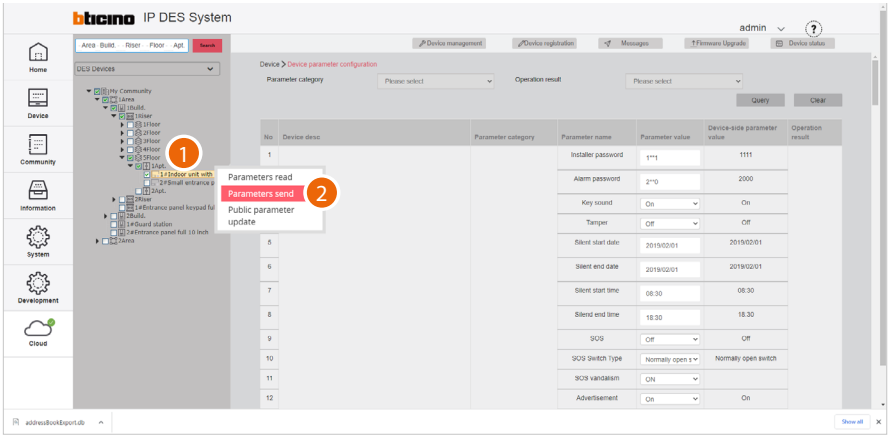
***Caution**: Save passwords in a safe place that is always accessible (Cloud backup activation recommended).*
If both the SD and the backup are unavailable, it will not be possible to retrieve the passwords.

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

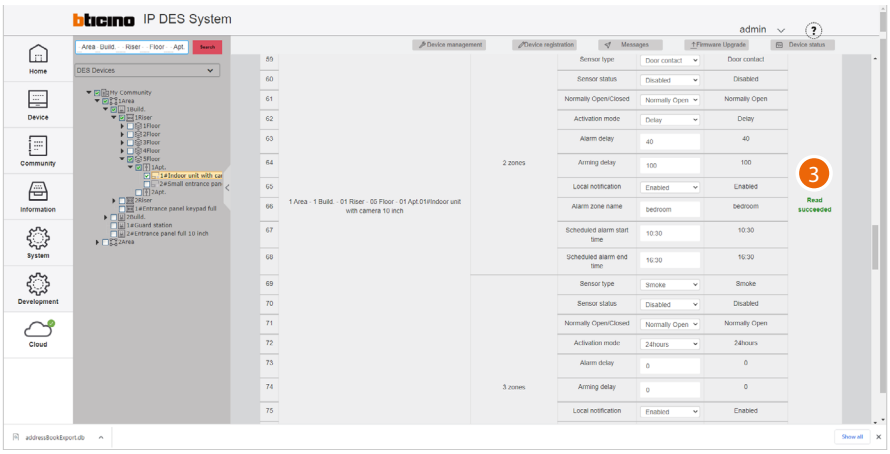
***NOTE**: The passwords of the devices incorrectly activated in DEMO mode are: 2000 (EP) and 1111 (IU and GS)*

Send the parameters

After changing the device parameters, they must be sent to the physical devices



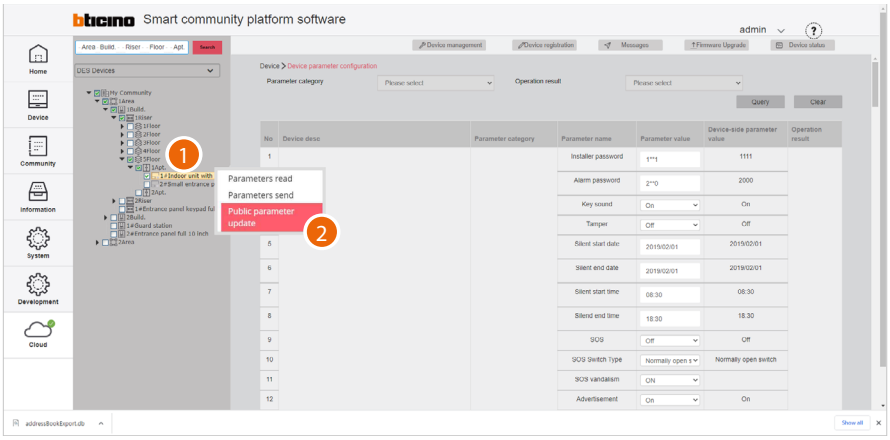
1. Tick the device to which you want to send the parameters
2. Click to send the command



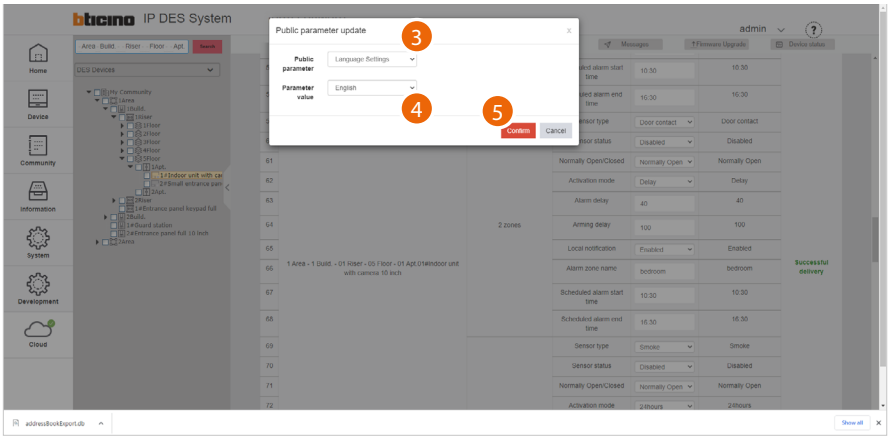
3. A message will be displayed if the operation is successful

Public parameter update

This page can be used to modify, with a single action, certain **parameters for all the devices** in the community.
It is possible to define which parameters to make available for editing, by setting them in the development/parameter template configuration page



1. Select the part of the community that contains the devices whose parameters you want to change
2. Click to send the command



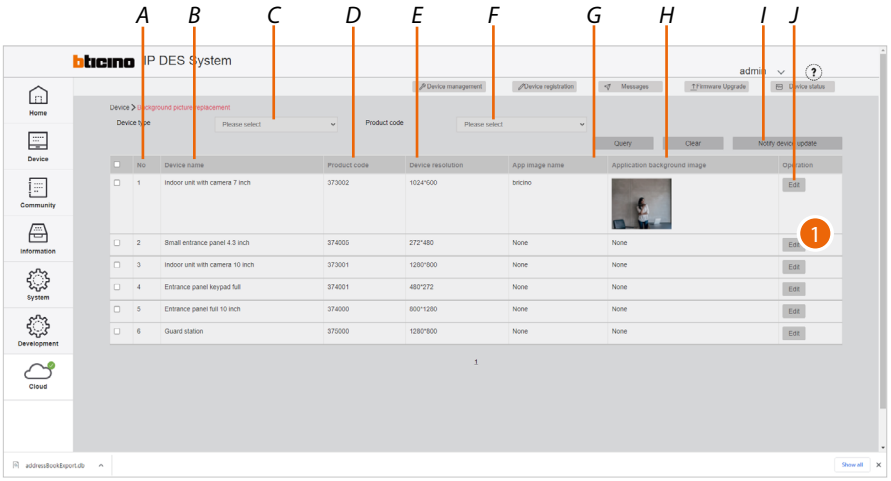
3. Select the parameter
4. Select the value
5. Click to confirm

The English language will be set on all devices in the community

Background picture replacement

This page can be used to set the Home Page background of the devices.
The imported image will remain available for selection on the device, in addition to the default images.

This function is only available for registered devices.



A Progressive number

B Type of device

C Type of device filter

D Item code

E Size of the background image to be imported

F Item code filter

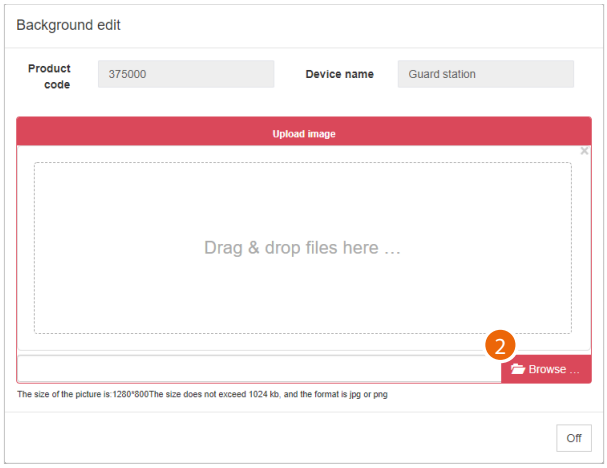
G Image name

H Image preview

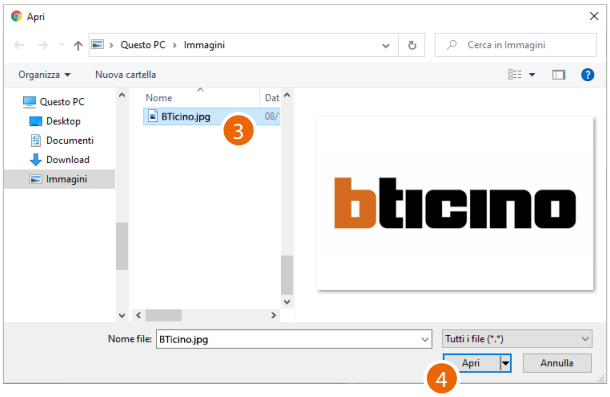
I Sends images to the device

J Opens the image loading panel

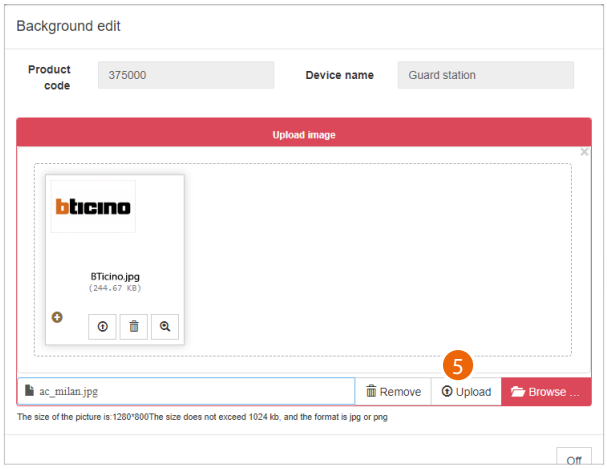
1. Click to open the image loading panel

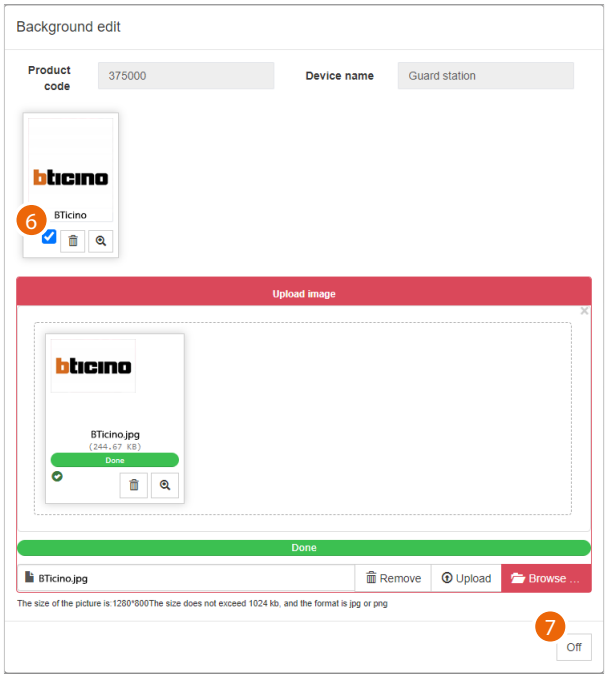


2. Click to select an image

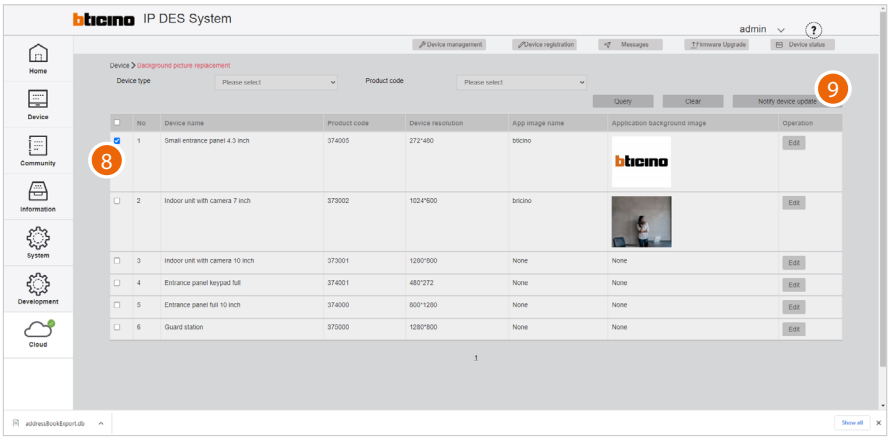


3. Select the image that meets the characteristics
4. Click to continue

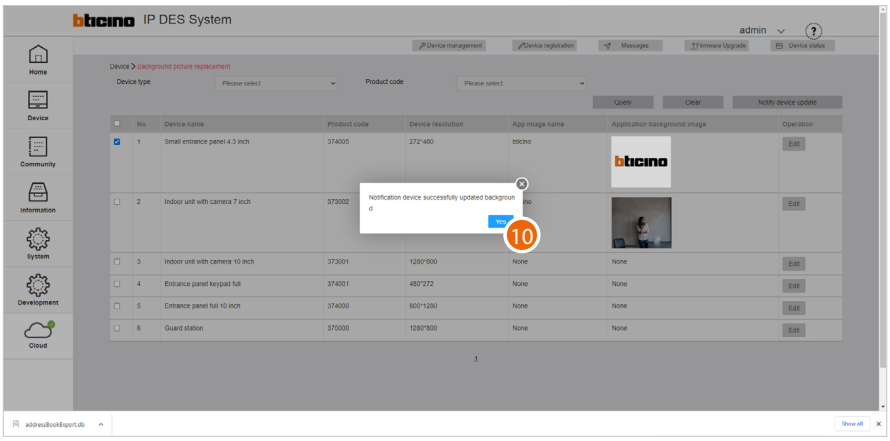




5. Click to load the image
6. Select the image
7. Click to finish



8. Select the device to which to send the previously selected image
9. Click to send

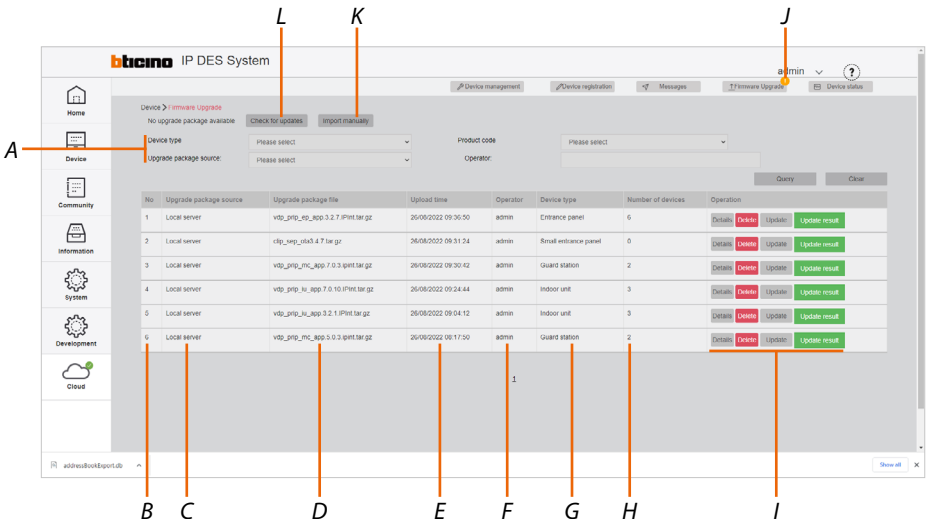


10. Click to finish

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

Firmware Upgrade

This page can be used to view the firmware updates of your 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 Progressive number

C Update package source: local import or download from cloud

D Update file name (.gz)

E Time and date of the plant update

E Name of the account that carried out the update

D Devices affected

H Number of affected community devices

I Update management keys

J Indication of availability of update packages on the cloud

K Import update package
(to be used if an update file is available)

L Check and download the update package from the cloud if available
(if the plant is connected to the internet)

Filters

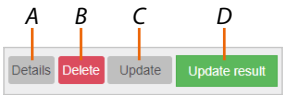
A Type of devices

B Origin of the update

C Select the code of the product affected by the firmware update (in case of firmware that can be applied to several devices)

D Account that completed the update (enter the name)

Update management keys

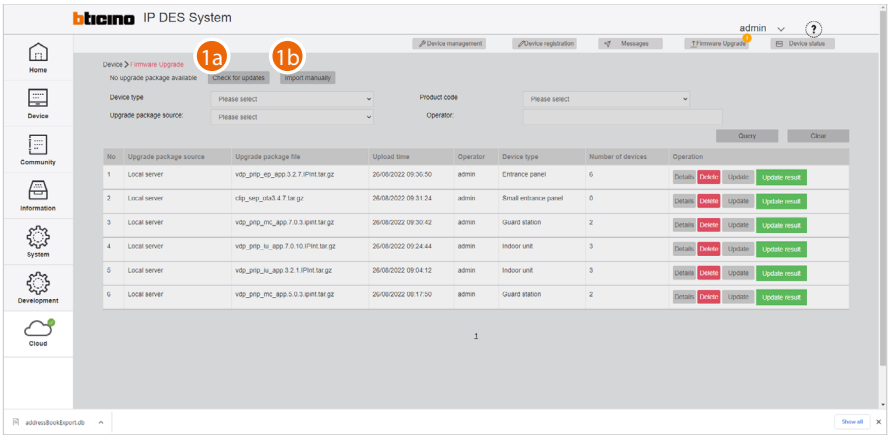


A Information about the update

B Delete the update

C Open the panel to send the update to the installation

D Display the panel with the update report for each device

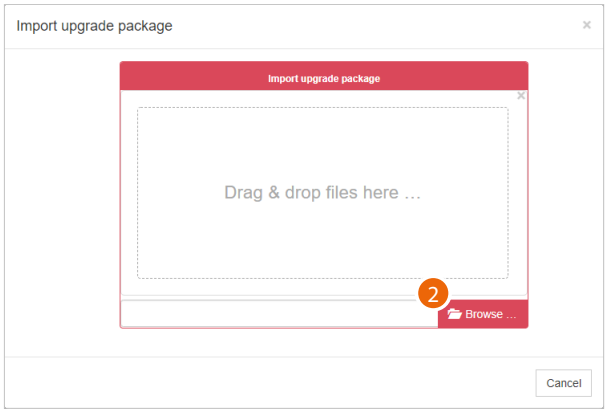


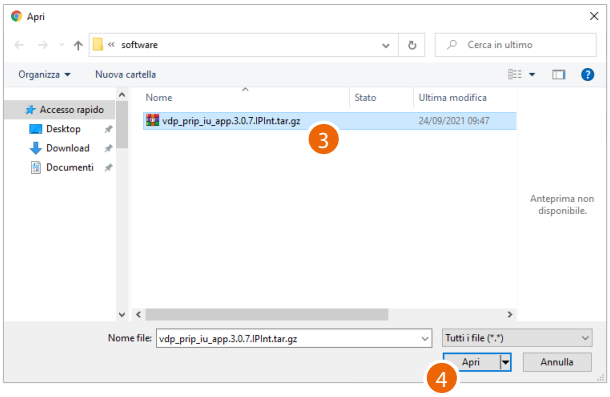
1a. Click to check for updates on the cloud. If there are updates, these will be downloaded and available for installation
***NOTE**: firmware updates will only be downloaded if the last installed updates have already been deleted: the page must be empty.*

or

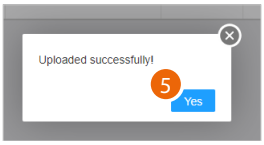
1b. Click to import the update package from the local system (see item 2)

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

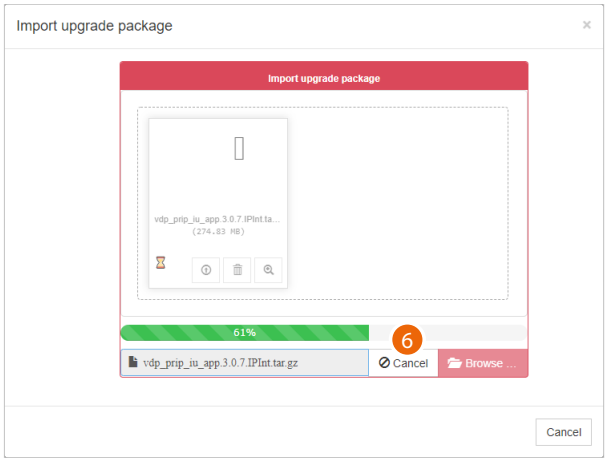




2. Click to select the update package
3. Select the .gz file
4. Click to continue

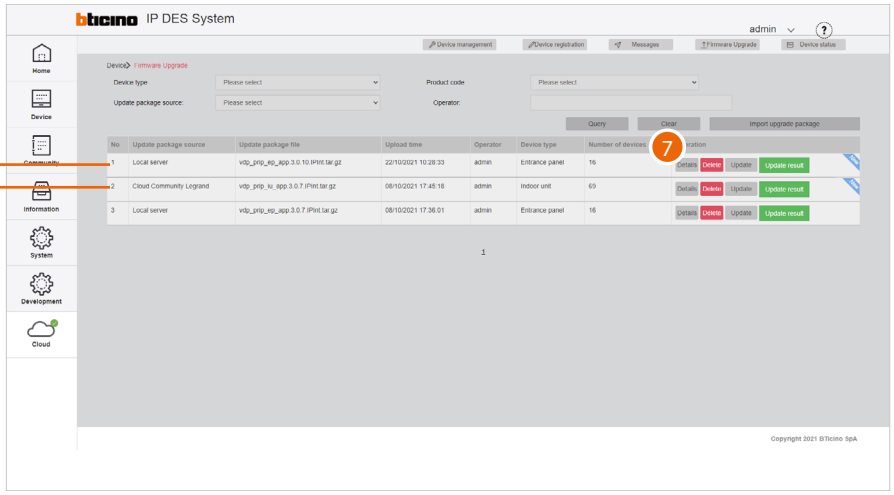


5. Click to continue



6. Start the process of loading the package into the SD server, click to abort if necessary

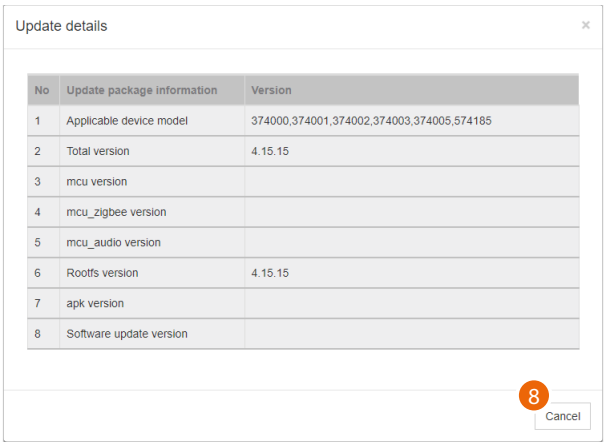
The package has been imported and is available to be sent to the devices



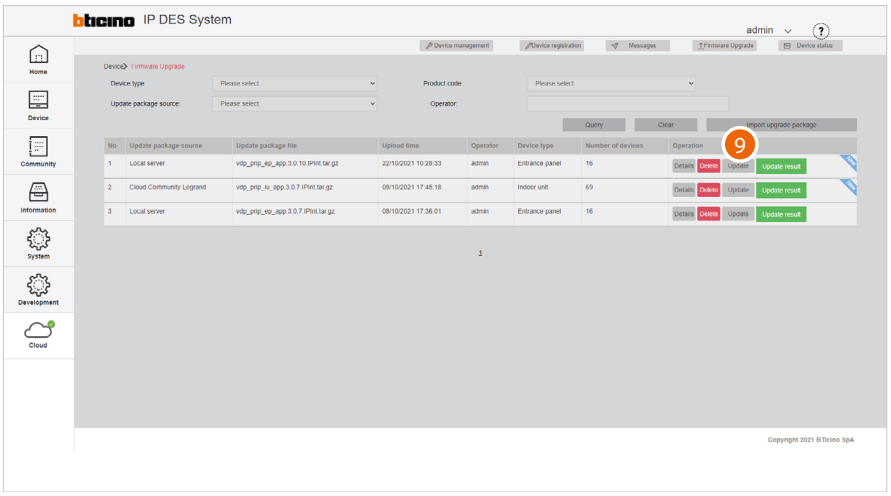
A *Update package from local system*

B *Update package from Cloud*

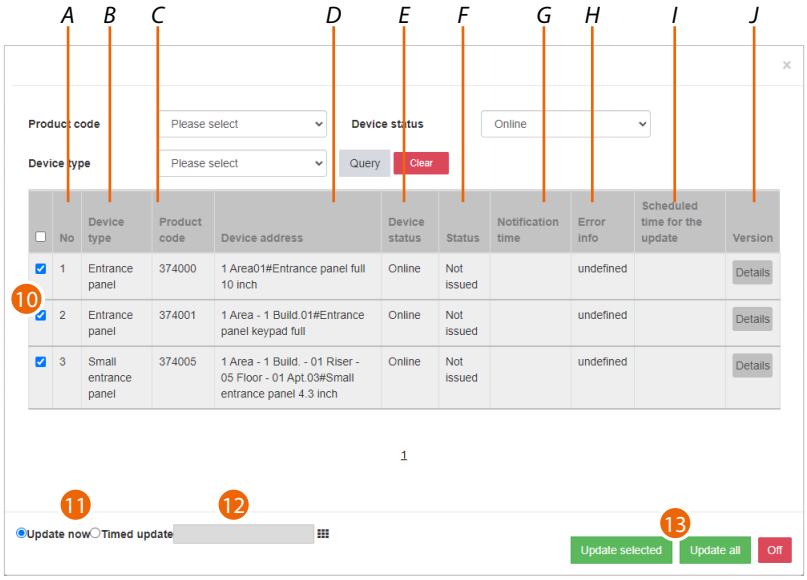
7. Click to see some of the update data



8. Click to close



9. Click to send the update to the plant



A Progressive number

B Type of device

C Item code

D Name of the device (customisable).
The original name represents the address of the device in the community.

E On line/off line device

F Sent/not sent

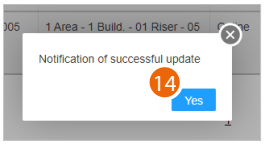
G Send time

H Log in case of error

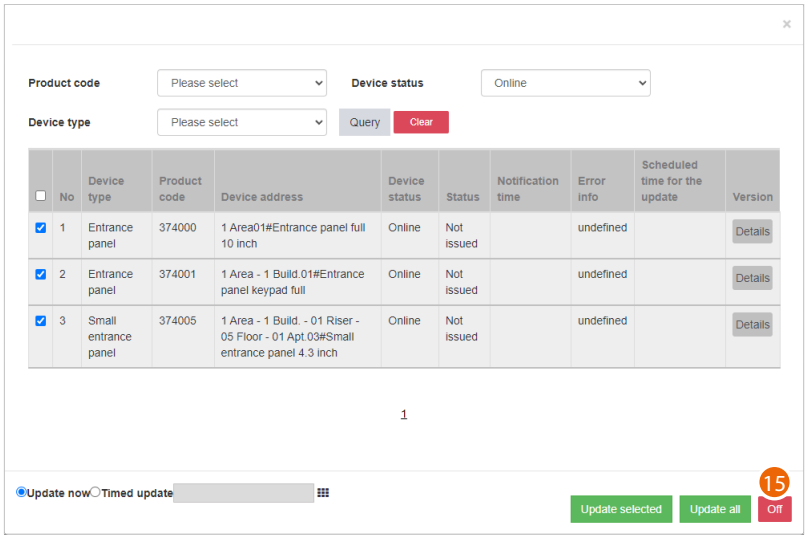
I Update schedule time

J Update details

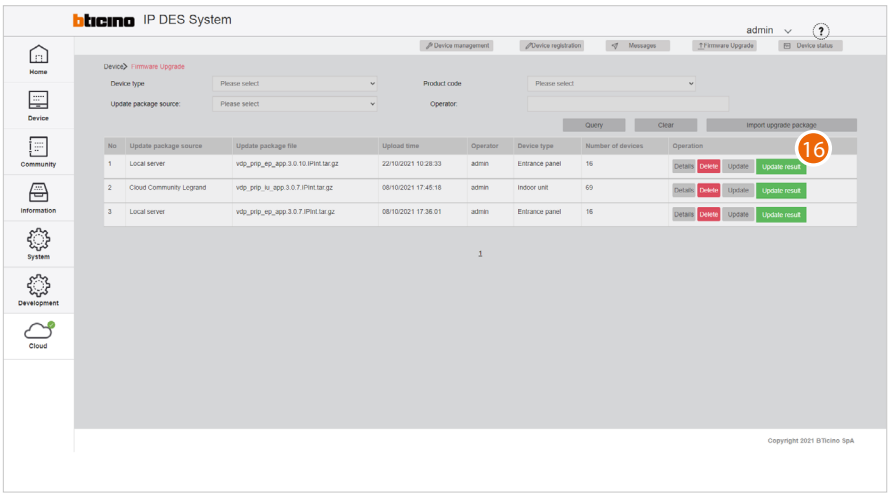
10. After using the filters to display the relevant devices, select them
11. Decide whether to perform the update immediately or
12. Schedule an update, setting the date and time
13. Start the update for the selected devices or for all the devices



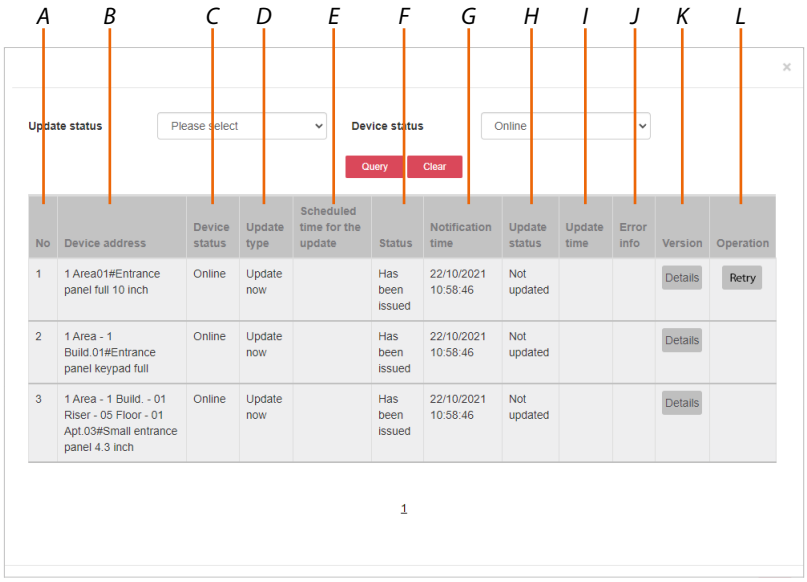
14. Click to finish



15. Click to close the panel



16. Click to view the results of the update



A Progressive number

B Name of the device (customisable)
The original name represents the address of the device in the community.

C On line/off line device

D Immediate/scheduled update mode

E Update schedule time

F Update status

G Update send time and date

H Update result

I Update time and date

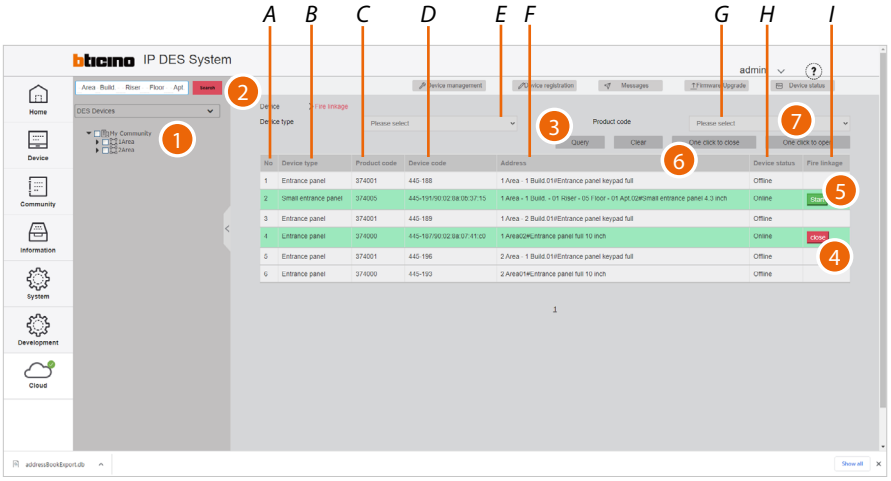
J Error report

K Update version details

L Send the update again

Fire linkage

On this page, you can use the Fire linkage function to enable the opening of the locks of the EPs 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.



E *Type of device filter*

G *Item code filter (first select the type of device)*

A *Progressive number*

B *Type of device*

C *Item code*

D *Mac address*

F *Name of the device (customisable)*
The original name represents the address of the device in the community.

H *Device status (on line/ off line)*

I *On/off button (online devices only)*

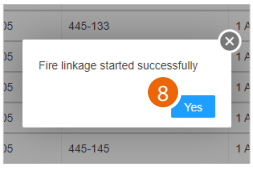
1. Select the community branch that contains the EPs concerned
2. If necessary, use the filters to narrow down the selection
3. Click to apply the filter

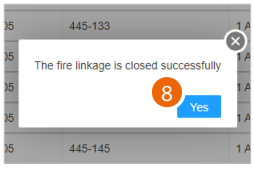
For the single device:

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

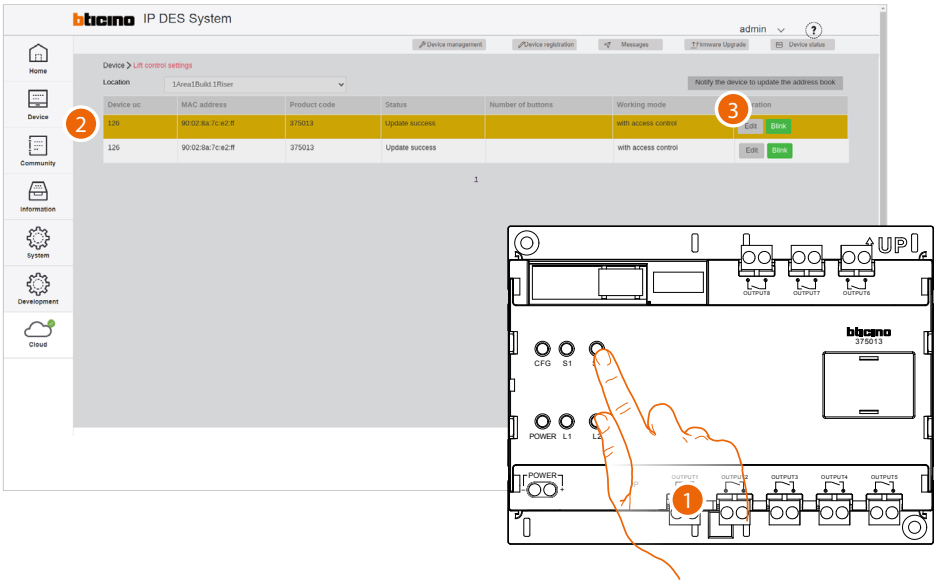




8. Click to finish

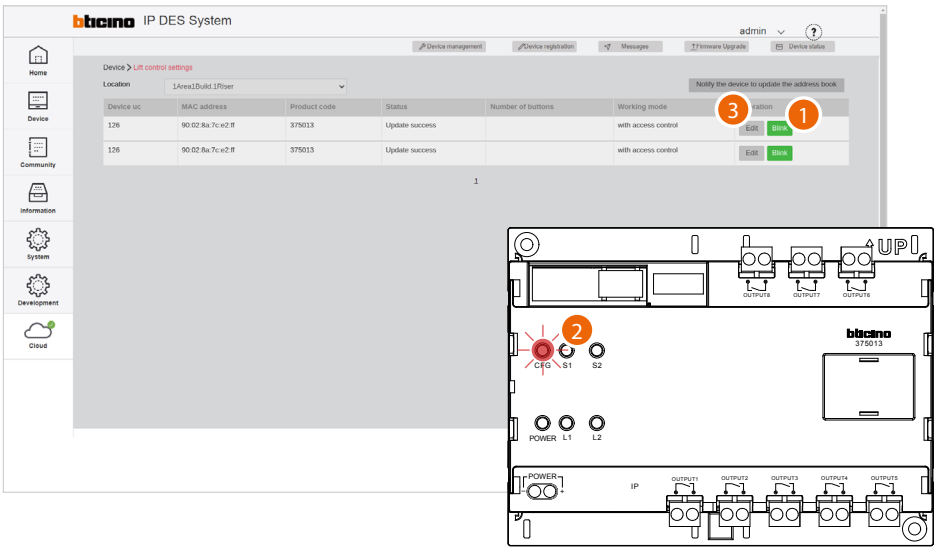
Lift control function

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.

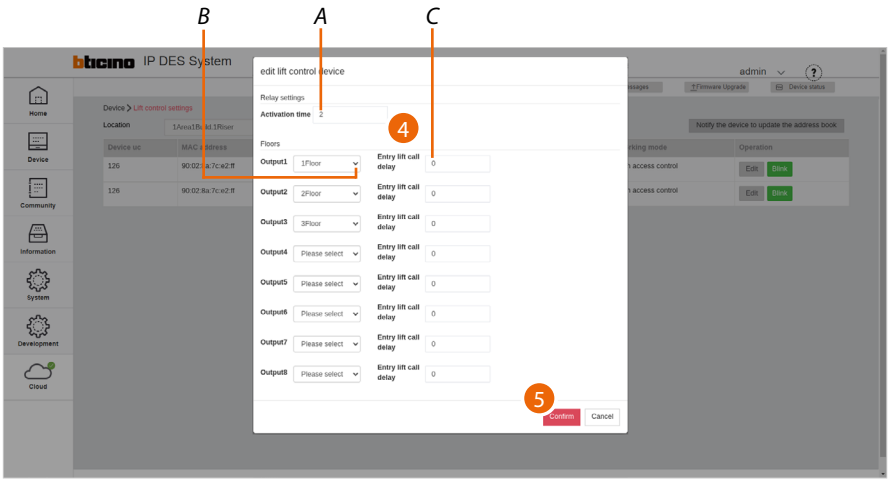


1. After adding the lift control interface with relay 375013, briefly press the button on the device to identify the device among those present in the structure in the Lift control function page of the Software.
2. The line of the lift control interface with relay 375013 of the Software will flash
3.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

as an alternative



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



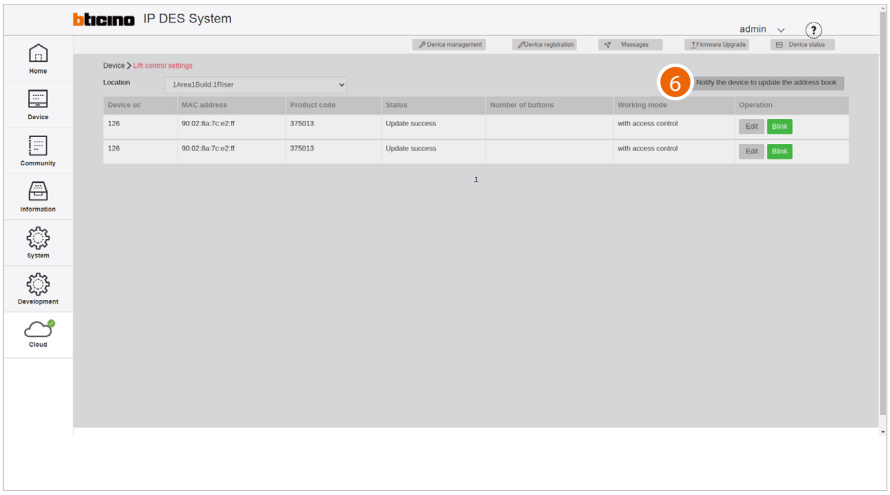
A Time during which the contact remains switched

B Selection of the floor for which output 1 to 8 is activated.

C Contact switching activation delay time

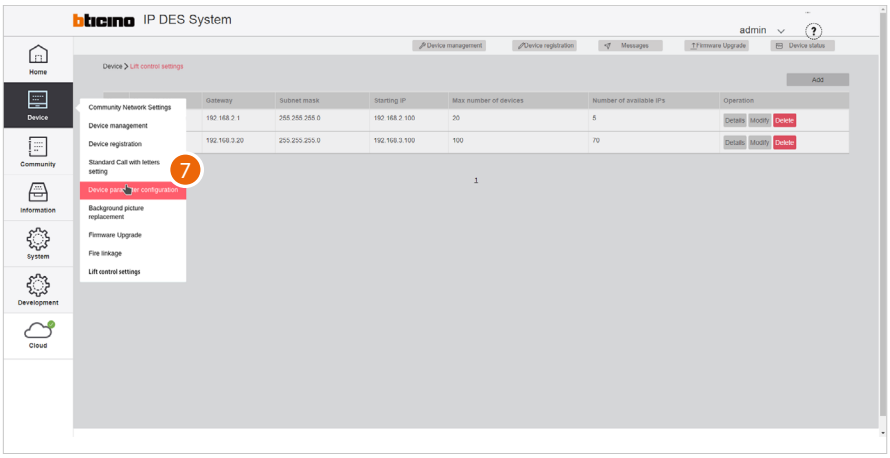
4. Modify the data

5. Click to confirm

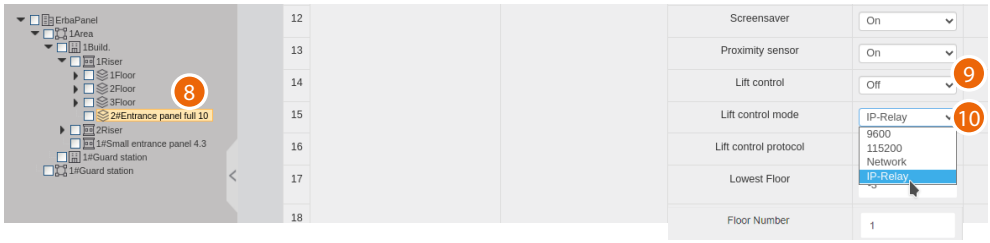


6. Click to send the modifications to the device

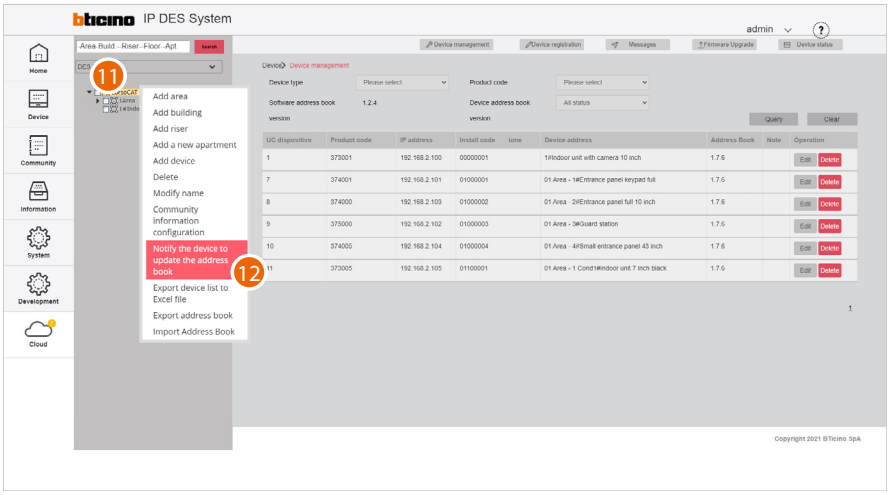
After configuring the lift control functions, it will be appropriate to configure the type of protocol used by the devices that use the lift control function.



7. Click to open the configuration parameters

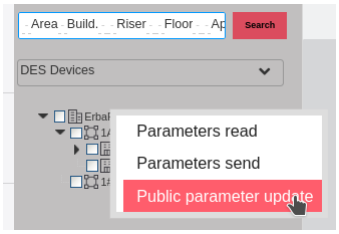


8. Select the entrance panel on which to set the lift control function parameters
9. Select the "ON" setting
10. Select the "IP-Relay" mode

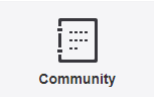


11. Right click the community
12. Click to select the command

The configuration can be performed using public parameters, see Modifying public parameters



Community



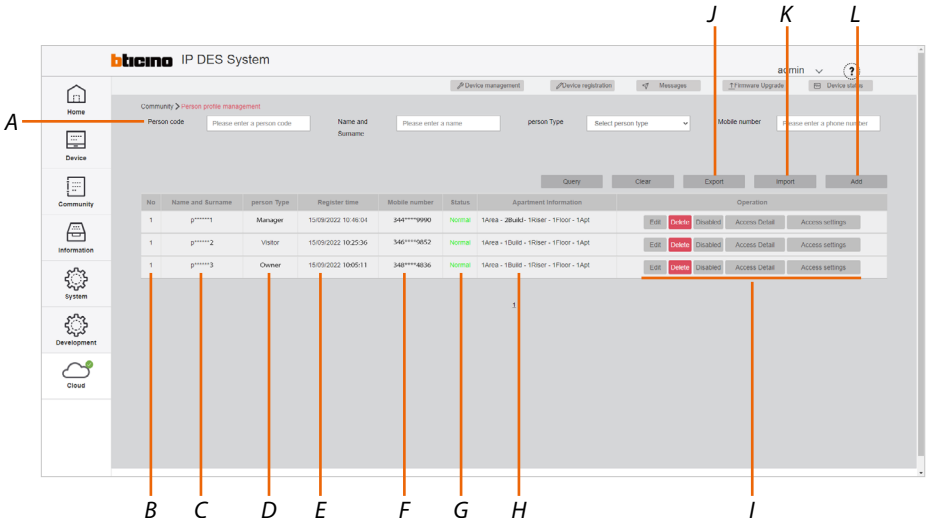
This menu can be used to view and manage functions related to community accesses, such as permissions, badges/cards etc.

Person profile management	Creates and manages the relevant people in the community, access permissions, personal data registrations, etc
Sector Key Management	Defines which sector keys to use for data storage in community badges/cards
Access control card management	It registers community cards or badges and assigns them to the relevant people
Access code	Resets the personal access code and panic access code of the IUs. The codes will be reset to their default values.
EP Registered Person Query	Displays for each person the EPs they have access to
Access version query	Displays data and events relating to community EP fingerprint and face recognition registrations

Person profile management

This page can be used to add/manage community people and give them permissions to access the structure.
Depending on the type of person, different access permissions may be assigned.
Default access permissions are created depending on type (see table).
Other permissions can always be added or removed.

Type of person	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
Security	All the common accesses
Cleaner	All the common accesses
Tester	No access
Service man	No access



A Person selection filters
B Progressive number
C Name of the person
D Type of person
E Registration date and time
F Telephone number
G Person status (enabled/disabled)
H Apartment address to which the person has access
I Person management keys
J Export the people list in .xls format
K Import the people list in .xls format
L Add a new person

Filters

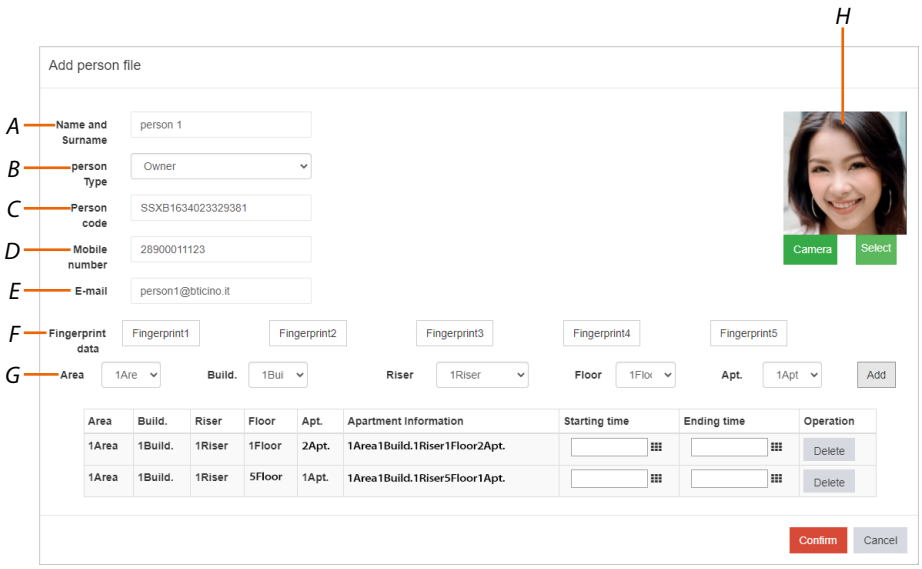
A Personal code
B Name and surname
C Type of person
D Telephone number

Person management keys

A Opens the person management panel
B Deletes the person
C Disables the person.
In this case, the person is still present but cannot access the apartment
D Displays details with access status and list of accesses controlled by the person
E Displays the tree menu for managing access permissions

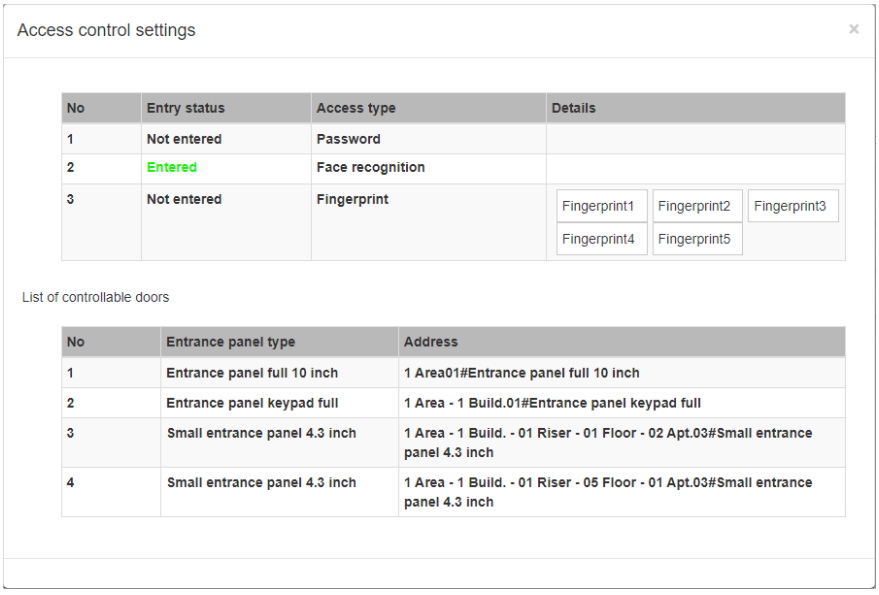
Person management (Edit)

This page can be used to edit personal data, and the fingerprint and face recognition records defined when adding individuals.



A Name of the person
B Type of person
C Unique person identifier
D Telephone number
E Email address
F Fingerprints stored for Fingerprint access
G Address of the apartments to which the person has access
H Image of the person used for Face Recognition access

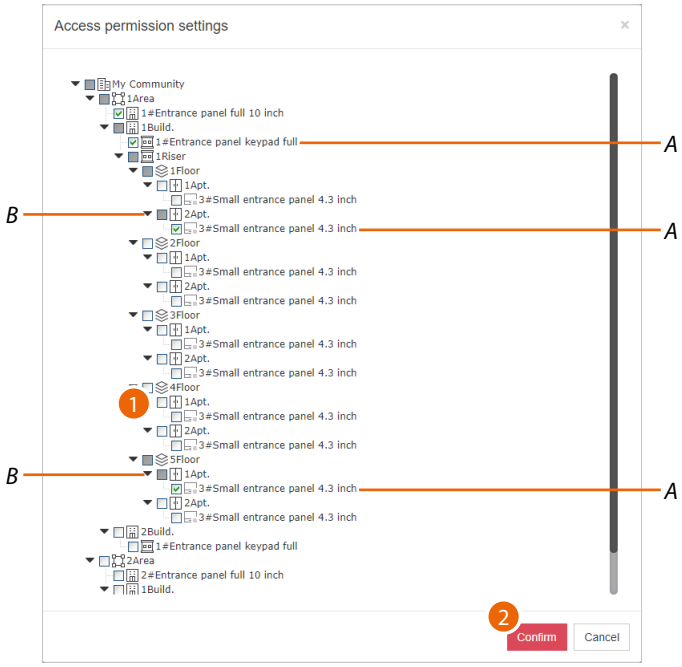
Access details



This page can be used to view the access status of the person.
It is possible to see if and how the person has accessed the community (Entry stratus is green).
The purpose of this page is to check that all access solutions are working properly.

Access settings

This page can be used to view, in a tree structure, the access permissions of the person.
The EPs for which the person has access permissions to reach the relevant apartment are displayed in the structure with a tick.



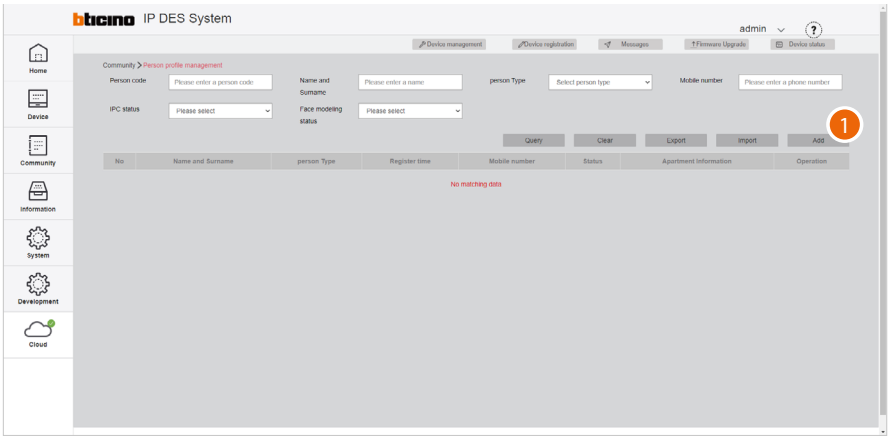
A *Accessible EPs*

B *Apartments that can be accessed by the person*

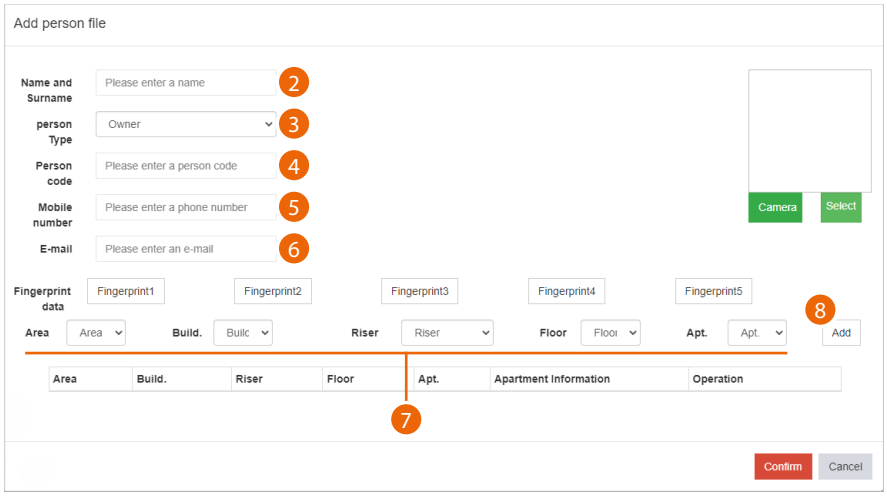
1. Click to enable/disable access to other apartments
2. Click to confirm

***Note**: access permissions also depend on the type of person set during the creation stage*

Create a person



1. Click to add a new person



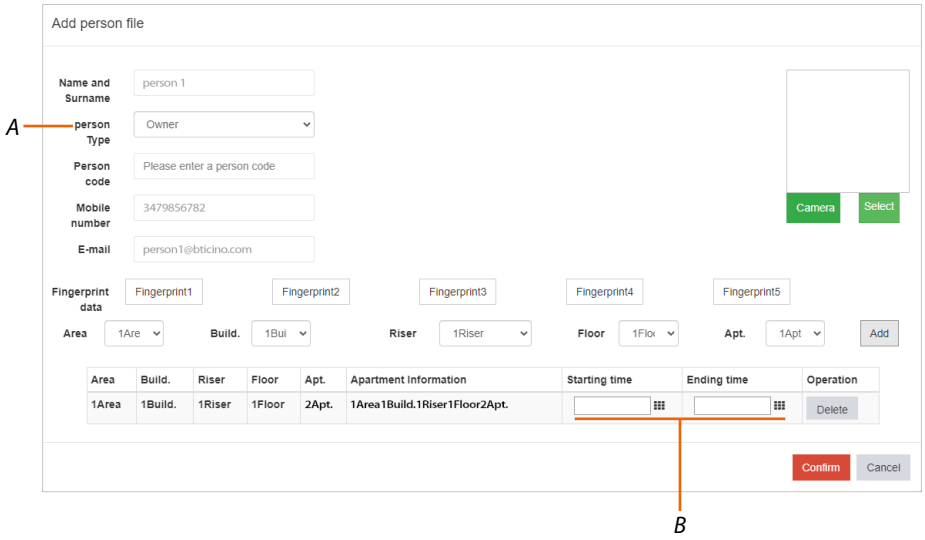
2. Enter the name and surname of the person
3. Select the type of person

Note: *some parameters may change depending on the type of person*

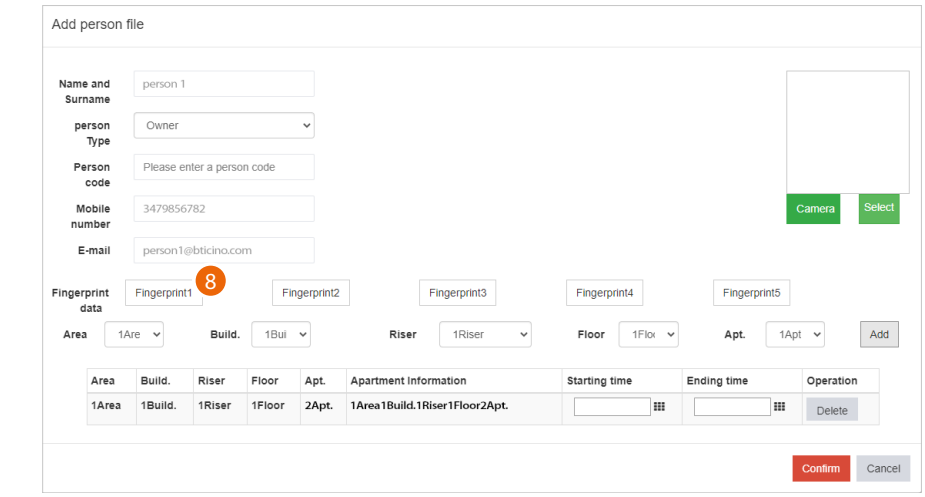
4. Person code
5. Enter the telephone number of the person
6. Enter the email address of the person

Now enter the relevant address of the apartment for the person

7. Select the relevant area/building/riser/floor/apartment for the person
8. Click to add



For the Visitor type (*A*), it is possible to set a duration for the access permission by entering the start and end date of the permission (*B*)

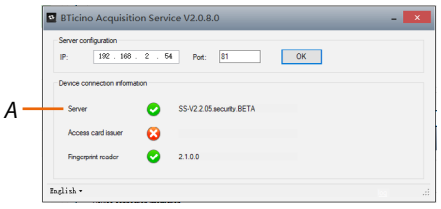


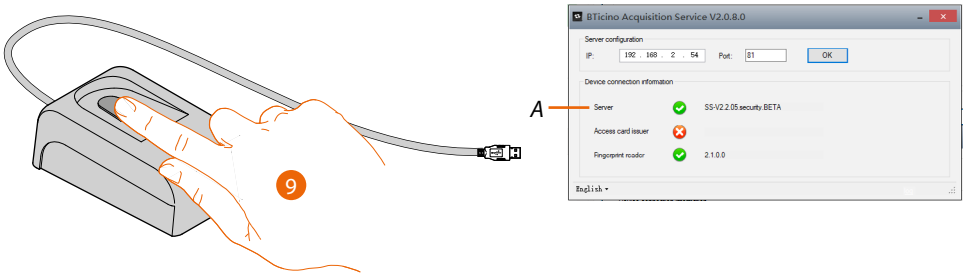
Access is now allowed using the Personal code.
Depending on the type of EP, it may also be possible to enable fingerprint and face recognition* access.

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

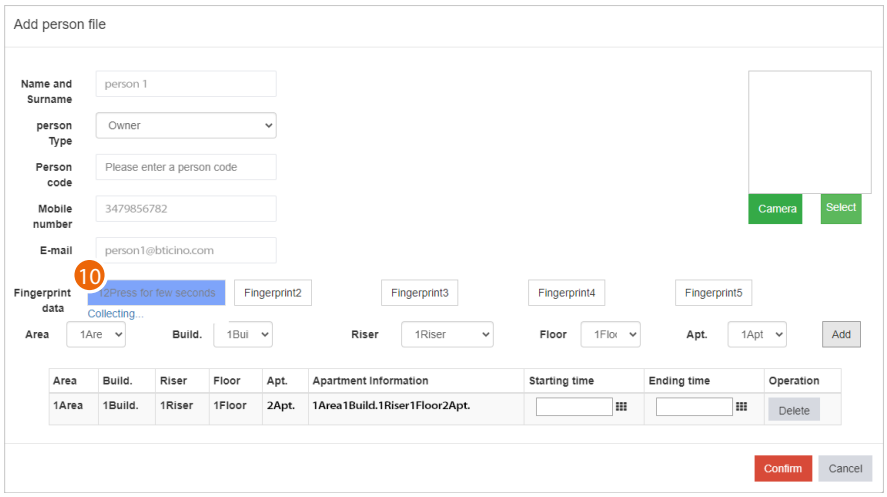
***Note**: the registration of fingerprints requires the installation of the BTicino ware software in the system. Also make sure that the Server A flag is green.*

***Nota**: La funzione Face Recognition è disponibile solo con la chiave USB di abilitazione 375011 da acquistare separatamente. La chiave USB deve essere collegata permanentemente all'SD*

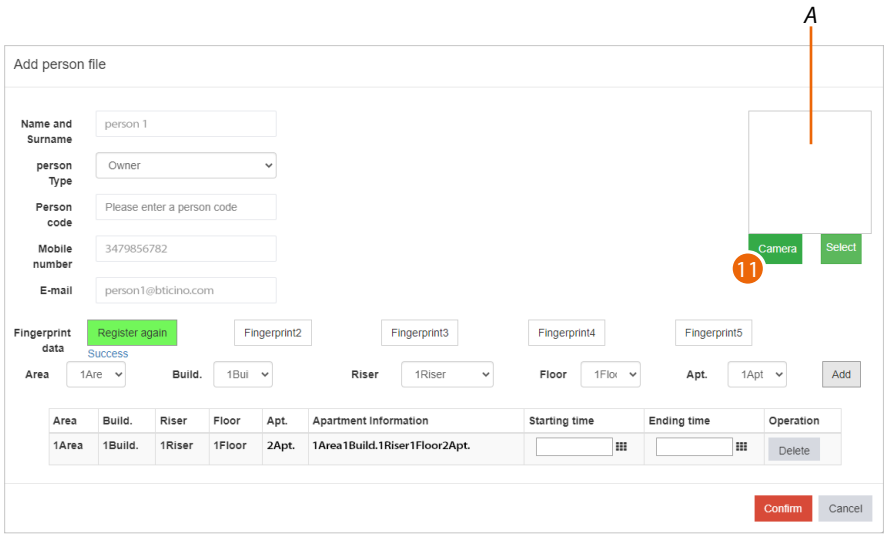




9. Connect a fingerprint reader (item 375004) to the Windows Client PC and check that the Server A flag is green



10. Click and then place the finger to be recorded on the reader, raising and lowering the tip until the box on the software turns green



Register other fingerprints or click to register the image used for face recognition* (*A*)

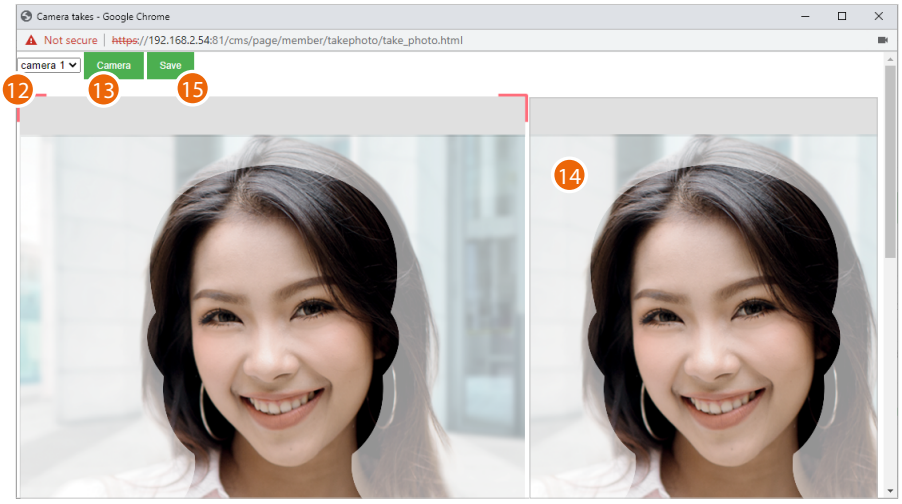
The image can be recorded in 2 ways:

– capture the image using the Windows Client PC camera, or

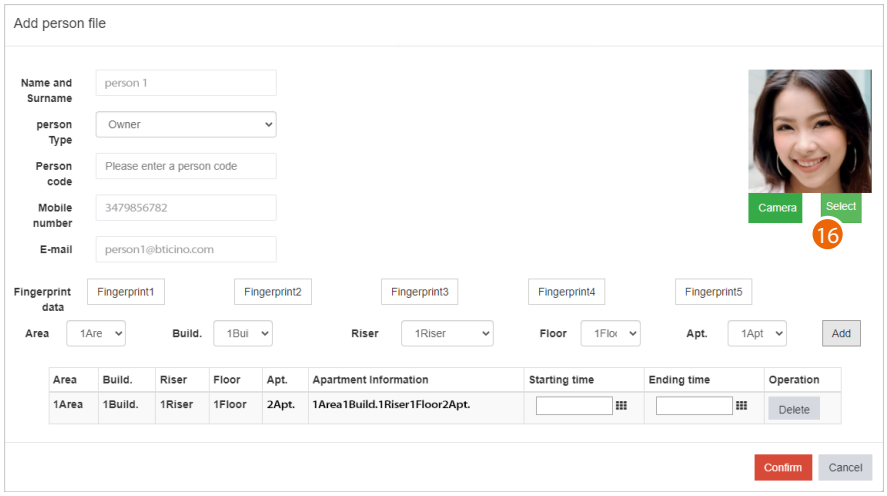
– import an image previously saved in the Windows Client PC

11. Click to record using the camera

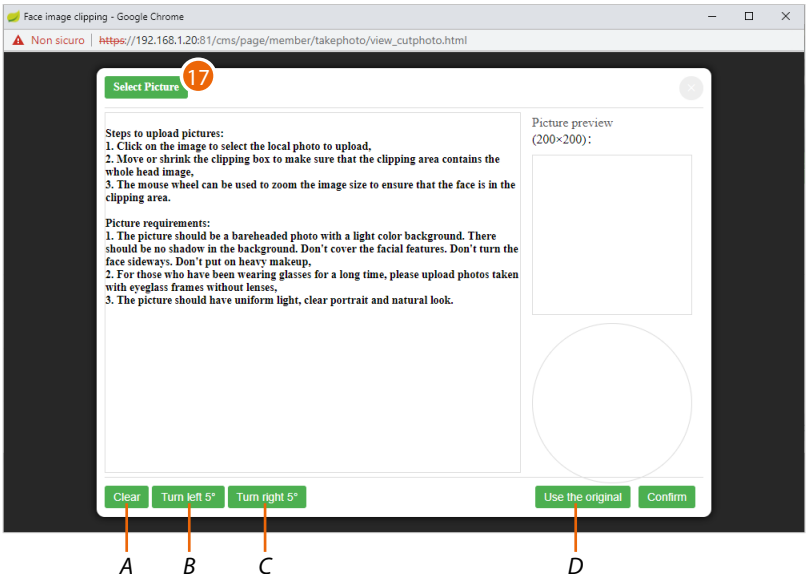
***Nota**: La funzione Face Recognition è disponibile solo con la chiave USB di abilitazione 375011 da acquistare separatamente. La chiave USB deve essere collegata permanentemente all'SD*



12. 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 glasses 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
13. Click to acquire the image
14. Check the preview
15. Click to save it



16. Alternatively, click to import an image from disk



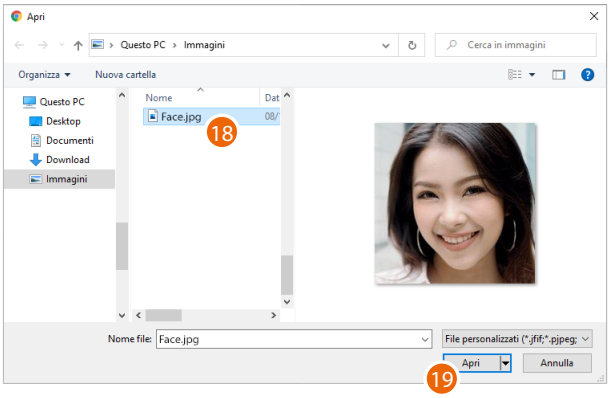
A Delete changes

B Rotate image 5° to the left

C Rotate image 5° to the right

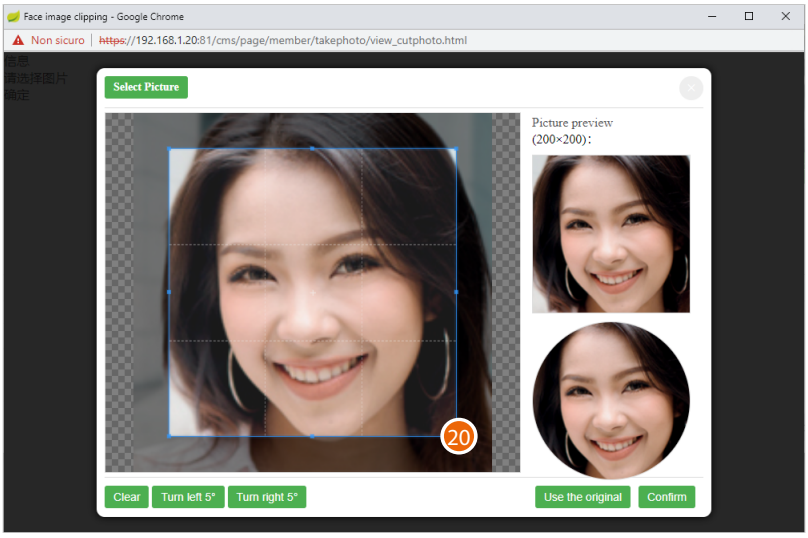
D Use the original image without changes

17. Click to select an image from disc
    – The image must be 200 x 200 pixels
    – See *warnings for camera captured images*

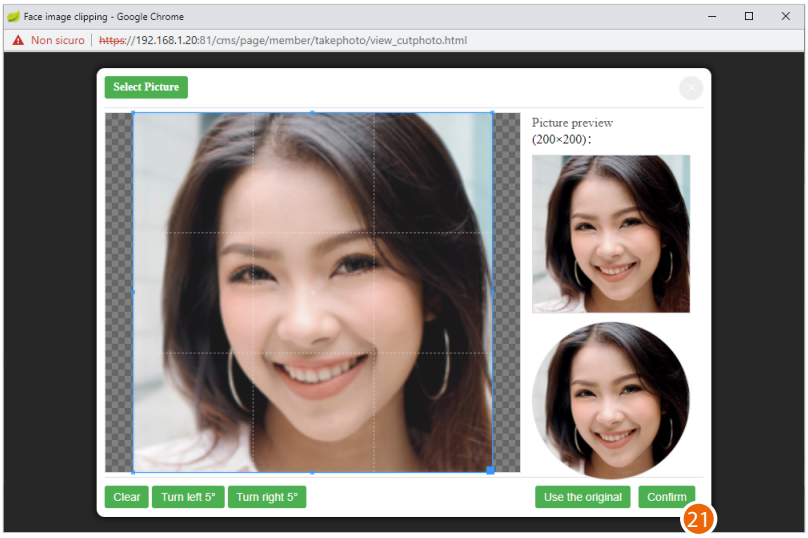


18. Select an image

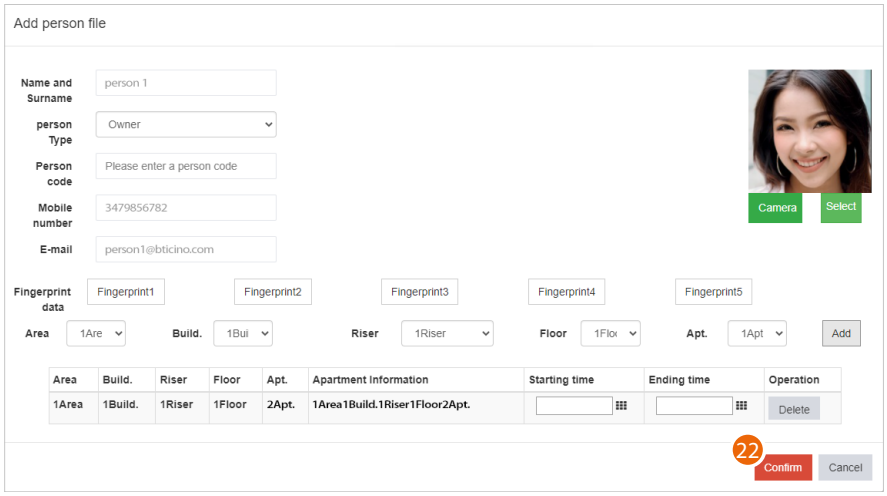
19. Click to open



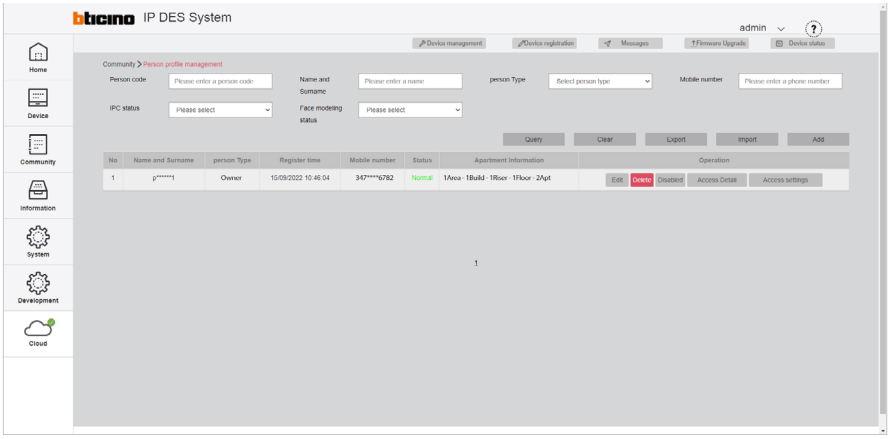
20. Using the anchor points, modify the selection box to obtain correct framing



21. Click to finish



22. Click to finish creating the person



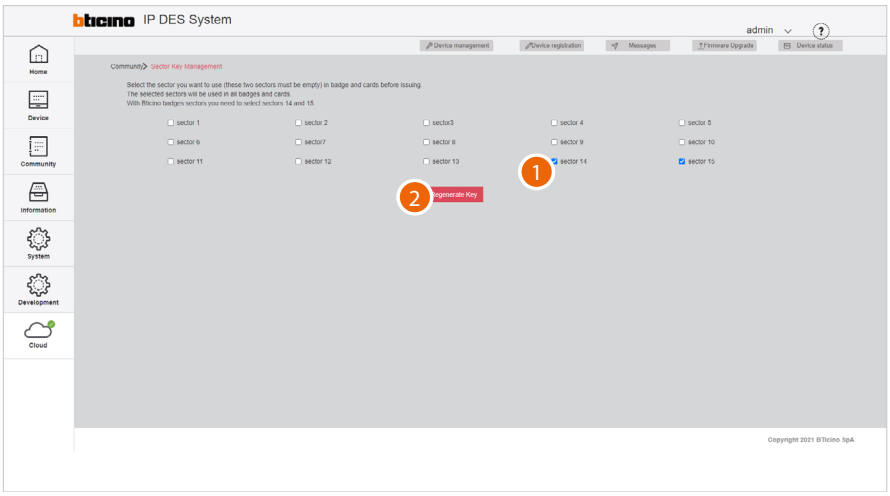
The person is now available on the management page

Sector Key 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 and the manufacturer.

BTicino Badge = sector keys 14,15
Other brands = sector keys not used

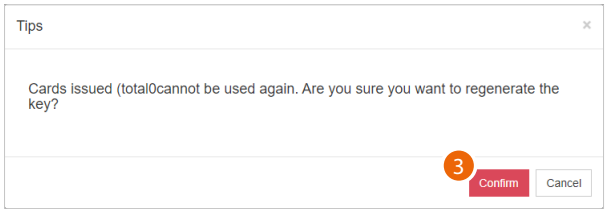
***Note**: some data of the community AB to which you are associating them are stored in the badges/ cards. Every time a new AB is generated, the above data changes, so the same badges cannot be used with different ABs and consequently on two different systems.*



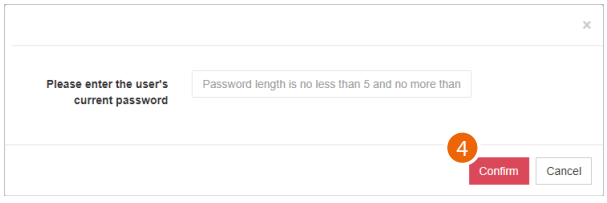
1. Select the sector keys

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

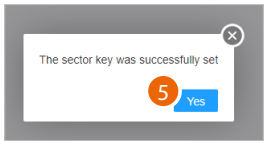
2. Click to record



3. Click to confirm



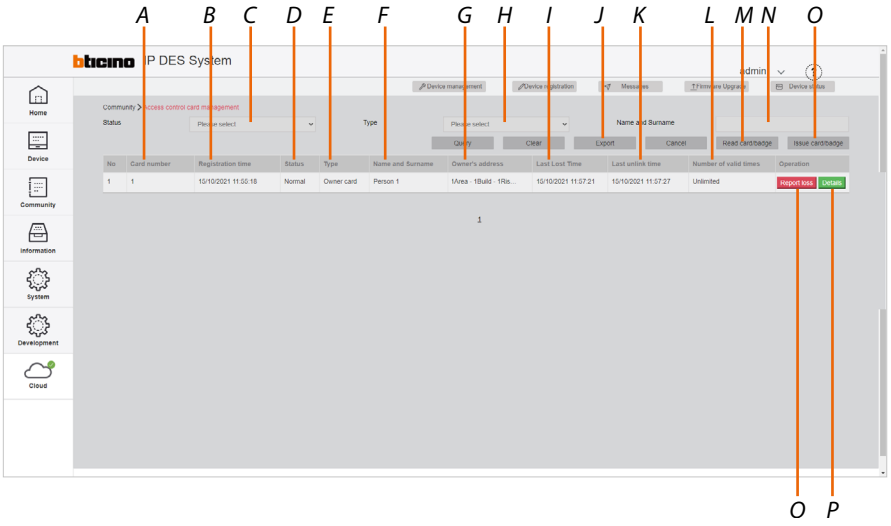
4. Enter the SD server authentication password



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

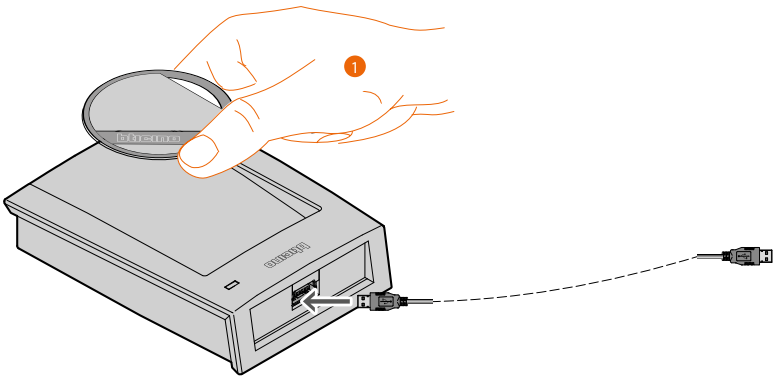
Access control card management

This page can be used to register cards/badges and associate them with people.
It is also possible to view the badge/card details and set the badge status to lost.
To read or register a badge/card, the connection of a badge reader, item 375003, is required.

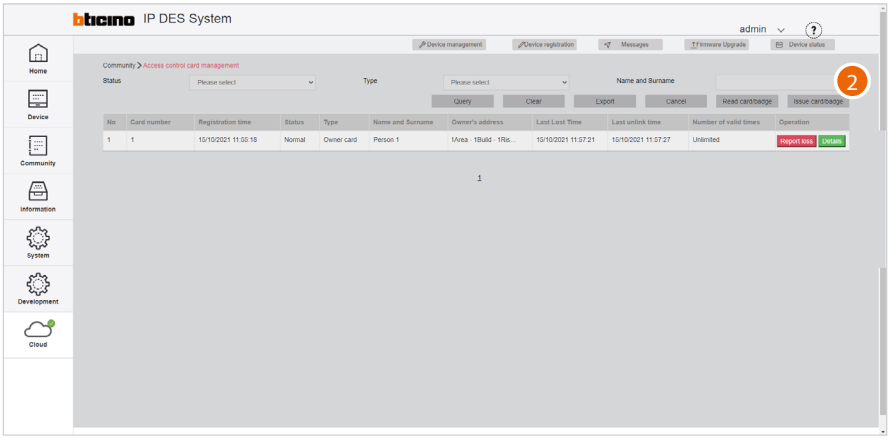


A Badge identifier
B Badge registration and assigning date
C Badge/card status filter (normal/reported lost/cancelled)
D Operation status
E Badge/card type based on the person (owner/security/manager...)
F Name of the person
G Apartment address
H Badge/card type filter based on the person
I Date reported as lost
J Export to an Excel® file
K Date found
L Number of times the badge/card can be used
M Read badge/card (requires a connected badge reader)
N Person name filter
O Register badge card (requires a connected badge reader)
P Badge/card details
Q Lost badge/card function button/status:
Reportloss=badge/card lost
Reportfound=badge/card found

Register a badge/card

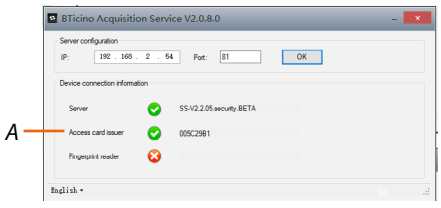


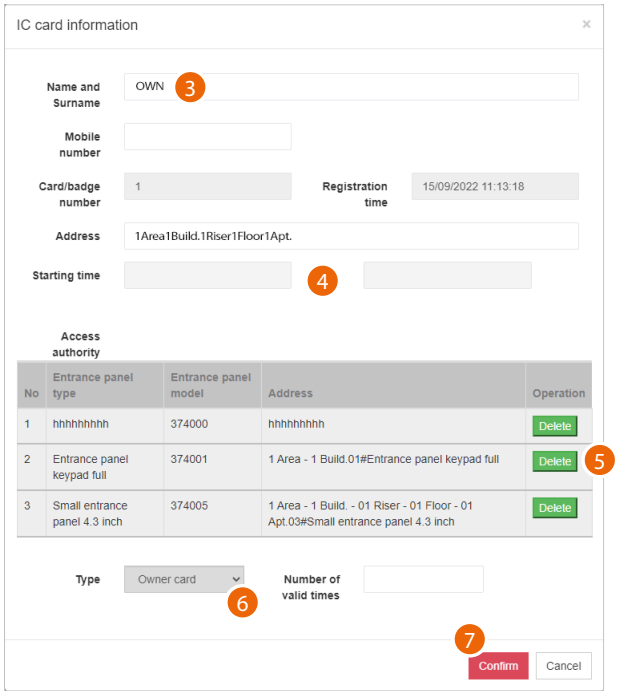
1. Connect a badge/card programmer (item 375003) to the Windows Client PC
   Place the badge/card to read on the reader



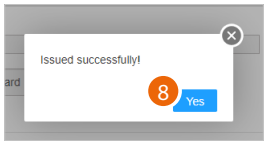
2. Click to record a badge/card

***Note**: the registration of a badge/card requires the installation of the BTicino ware software, available at www.homesystems-legrandgroup.com. Also make sure that the A flag is green.*

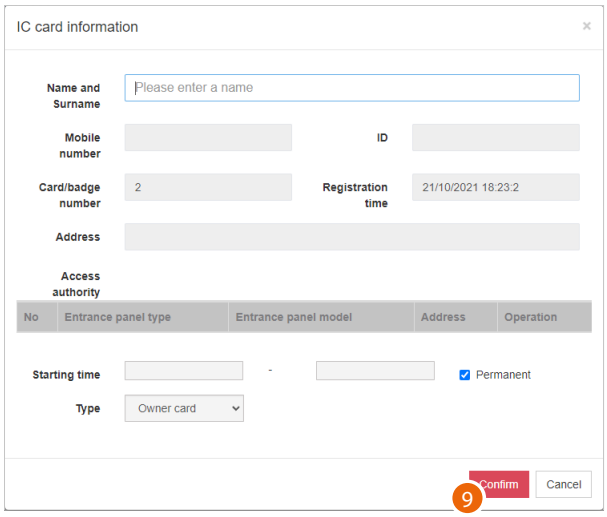




3. Enter the name or part of the name (a list is displayed) of the person to be associated with the badge. The person must already have been created in the Person profile management page
4. Select a validity period for the badge/card or
5. The display shows the list of EPs to which the person has access. Accesses may be deleted as required
6. Displays the type of badge/card. If the person is someone responsible for Security, Patrol or Property Manager can also be selected.
   The patrol badge does not open the lock but has a specific function; see Patrol record.
7. Click to record



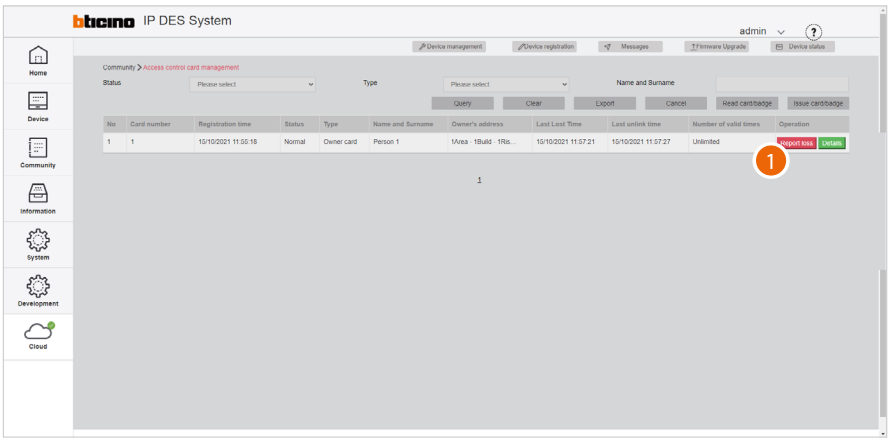
8. A sound and a message indicate that the registration has been successful, click to finish



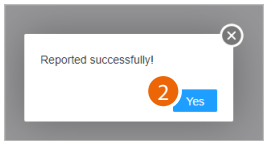
9. Register another badge or click to end the process

Disable the badge

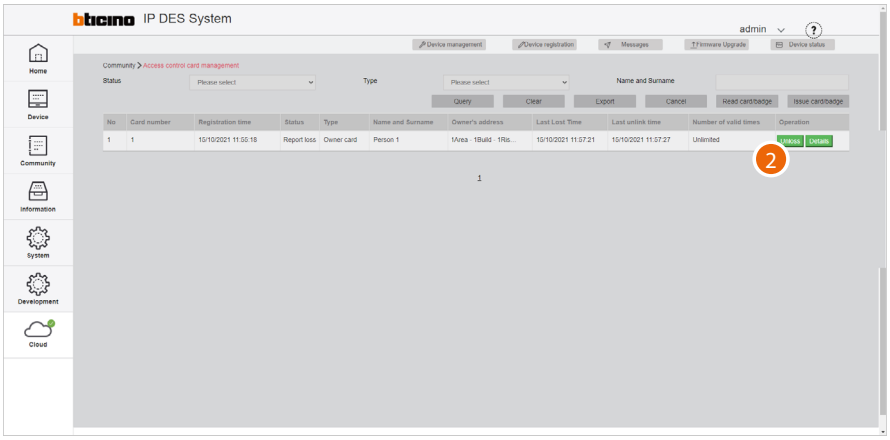
Lost badges can also be disabled.
Once found again, the badge can be reactivated.



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



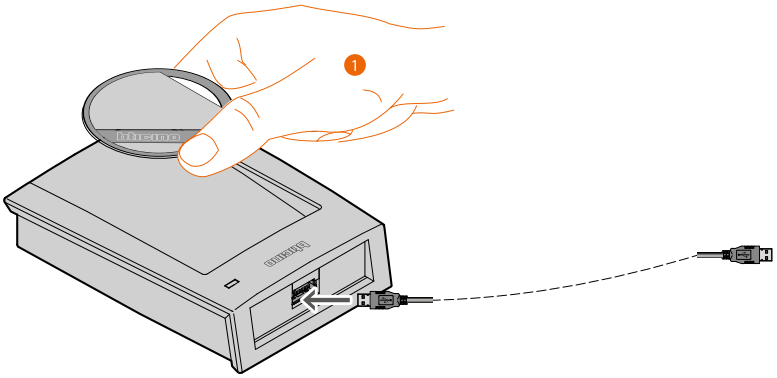
2. The badge/card is now disabled; click to continue



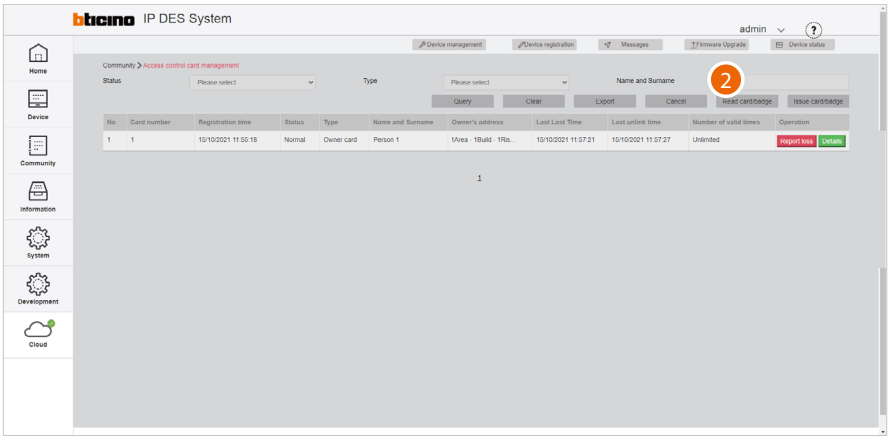
3. Click to activate the badge again if found

Identify the badge

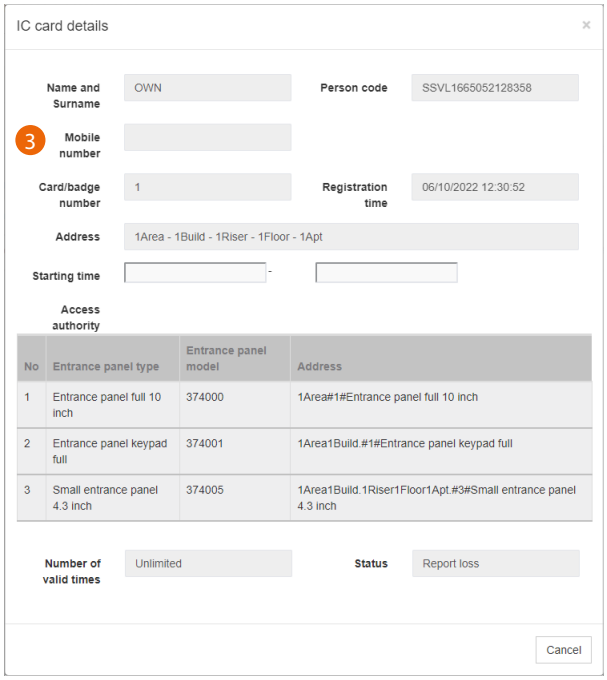
This function allows to read the data contained in a badge/card; for example, to identify it when found.



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



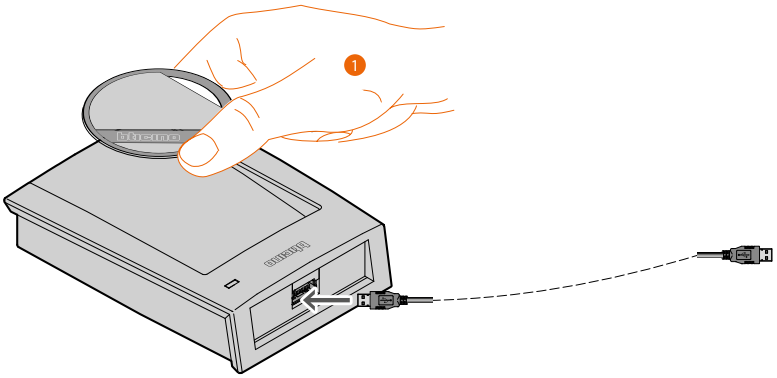
2. Click to read a card/badge



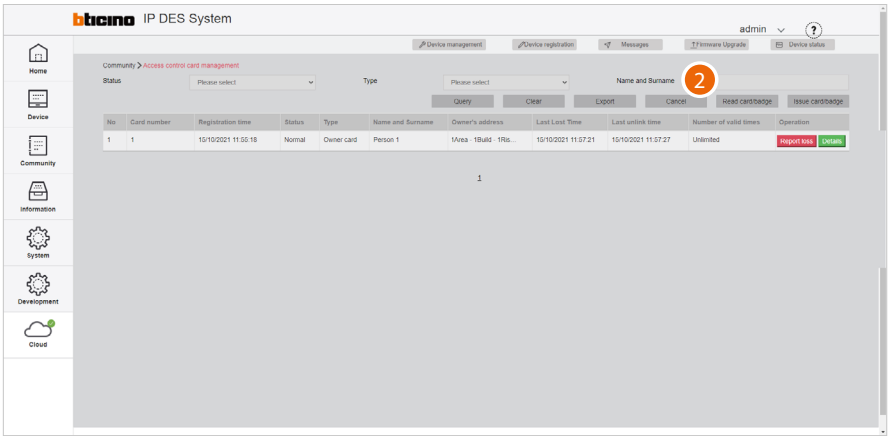
3. The panel displays the data of the badge owner

Delete a badge

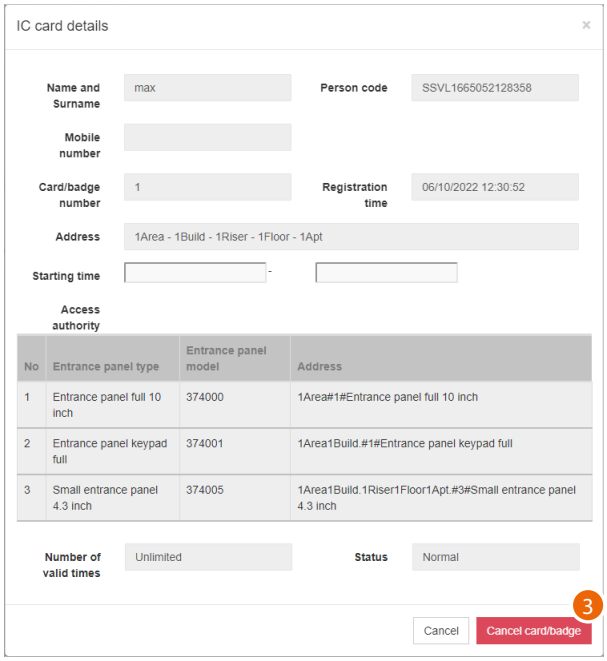
This function allows to erase the registered owner of a badge/card.After this operation, the data of the person will be deleted and the badge/card will be ready for association with someone else.



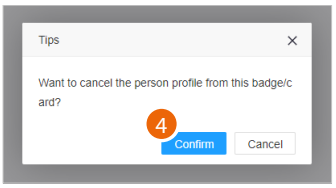
1. Connect a badge/card programmer (item 375003) to the Windows Client PC
   Place the badge/card to read on the reader



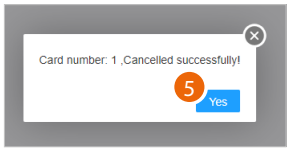
2. Click to erase a card/badge



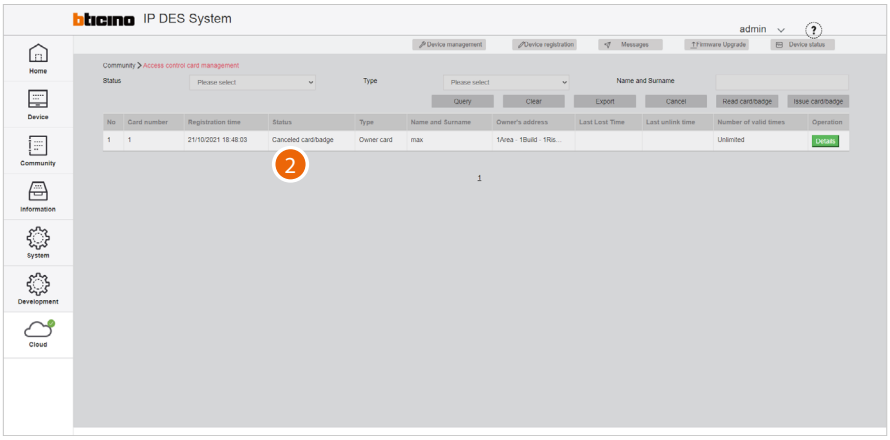
3. The panel displays the data of the person registered on the badge/card; click to proceed



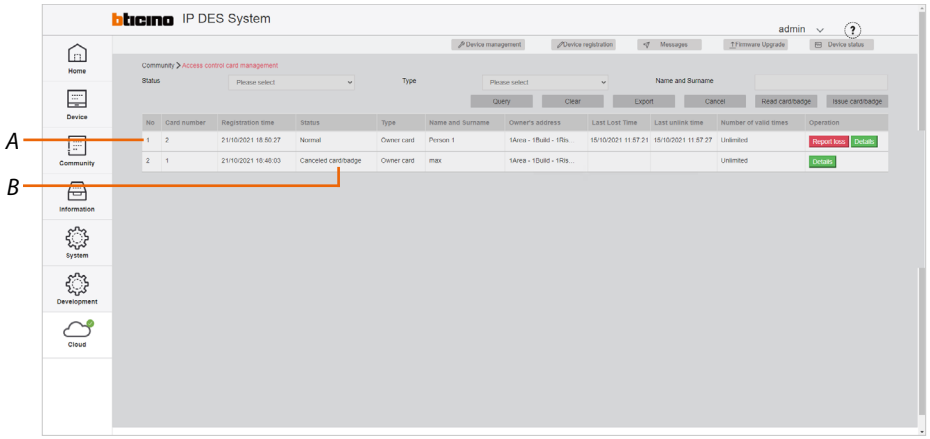
4. Click to confirm: all the details of the person will be erased from the badge/card



5. Click to continue



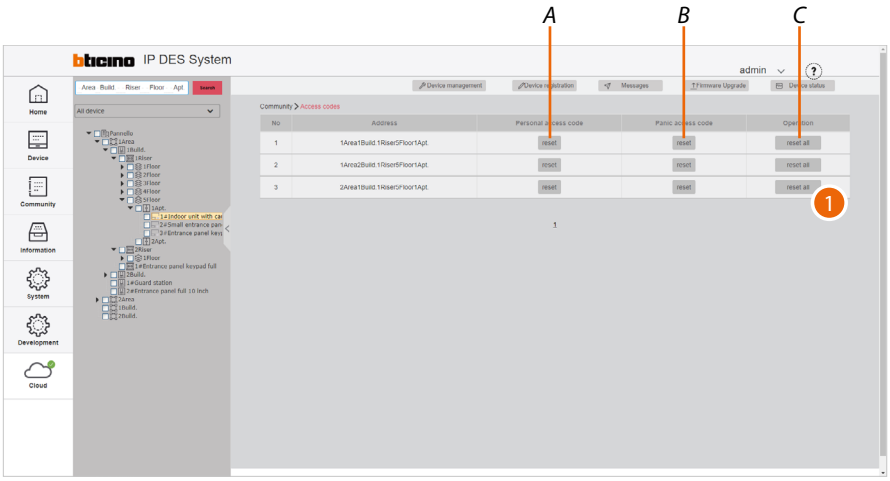
6. The status field shows the badge erased indication



It is now possible to associate another person to the badge (*A*). The previous registration will still be present in the page, with the status showing as erased (*B*)

Access code

This page can be used to reset the Personal access code and the Panic access code of the IUs.
The codes will be reset to their default values.
This function can be used if the user has lost the passwords.



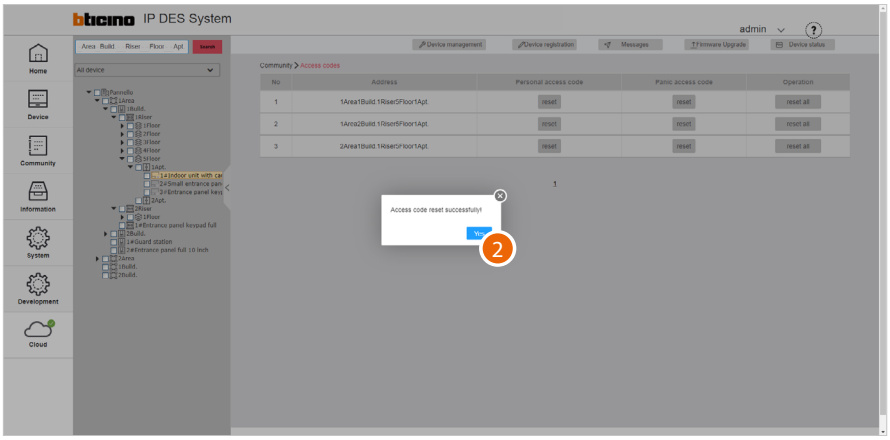
A It resets the Personal access code

B It resets the Panic access code

C It resets both the Personal access code and the Panic access code

1. Tap to reset the Personal access code and the Panic access code

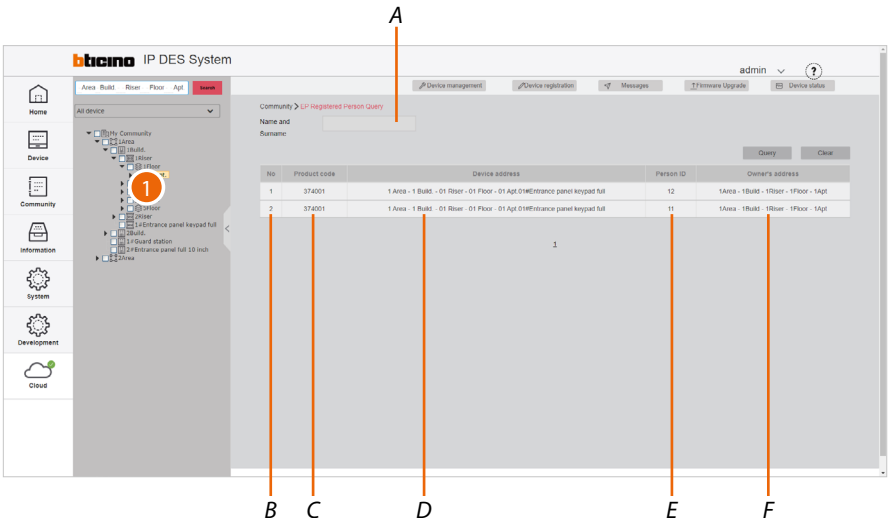
***Caution**: The codes will be reset immediately without further confirmation.*



2. Touch to close

EP Registered Person Query

This page can be used to view, for each person, which EPs they have access to. It is also possible to select an EP to display which individuals have access to it.



A Contact name filter

B Progressive number

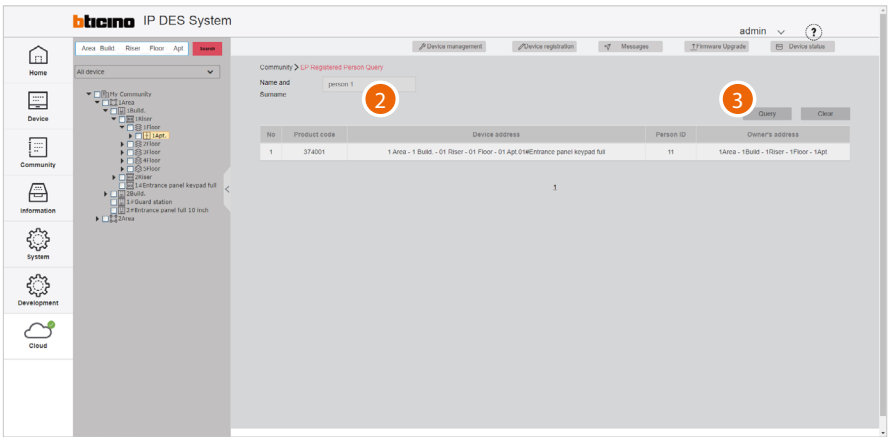
C Item code

D Name of the device (customisable).
The original name represents the address of the device in the community.

E Person identification number generated in personal file management
(see Person profile management)

F Apartment address

1. Select the EP from the tree menu to see the people with access permissions (F), or

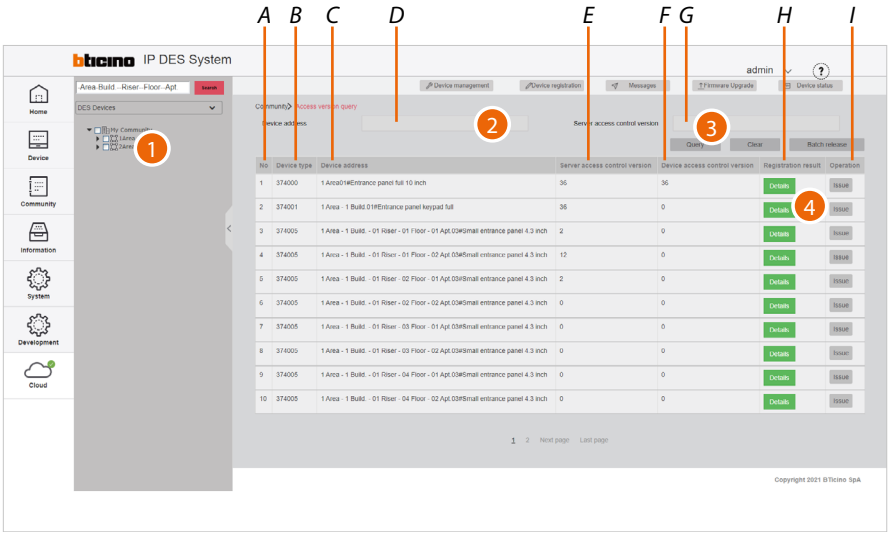


2. Enter the name of the person whose permissions you wish to view
3. Click to continue; the EPs the person has access to will be displayed

Access version query

This page can be used to view data and events related to community EP fingerprint and face recognition registrations.

Note: *and EP row highlighted in red indicates a fingerprint or face recognition error.*



D Device name filter (type the name of the device or part of it)

G SD database version filter (enter the version number)

A Progressive number

B EP item code

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

E Database version in the SD

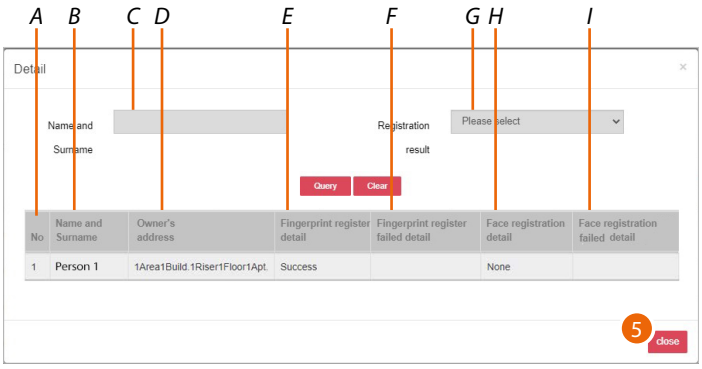
F Database version in the EP

H Details of fingerprint and face recognition registrations

I Send database to the EP

Note: *In case of unexpected behaviour of the devices during use, check that the database version in the SD (F) is the same as that of the device (G)*

1. Select the community branch that contains the EPs concerned
2. If necessary, use the filters to narrow down the selection
3. Click to apply the filter
   For filtered EPs, the database versions present on the SDs and EPs are displayed.
4. Click to view the access details



A Progressive number

B Name of the person

C Person name filter

D Name of the device (customisable).
The original name represents the address of the device in the community.

E Finger registration successful/failed/not carried out

F Details in case of failure

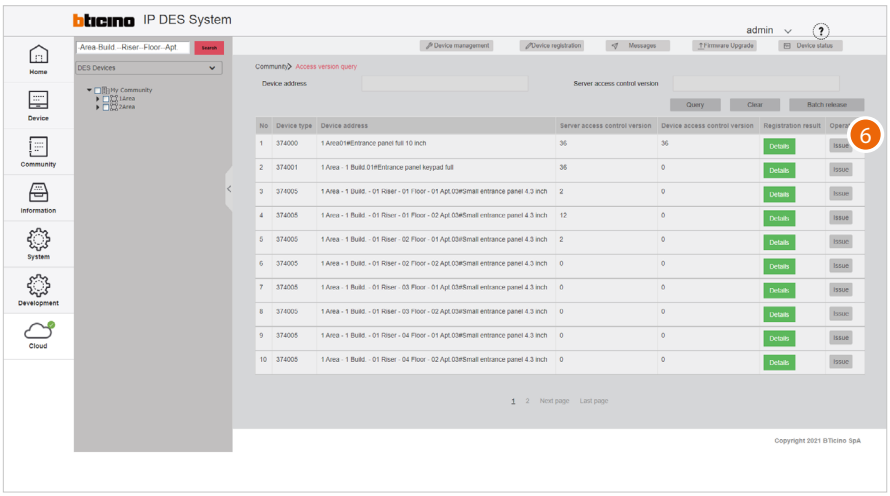
*G Completed/failed registration filter**

H Face recognition registration successful/failed

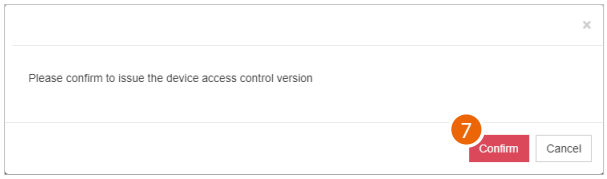
I Details in case of failure

5. Click to close

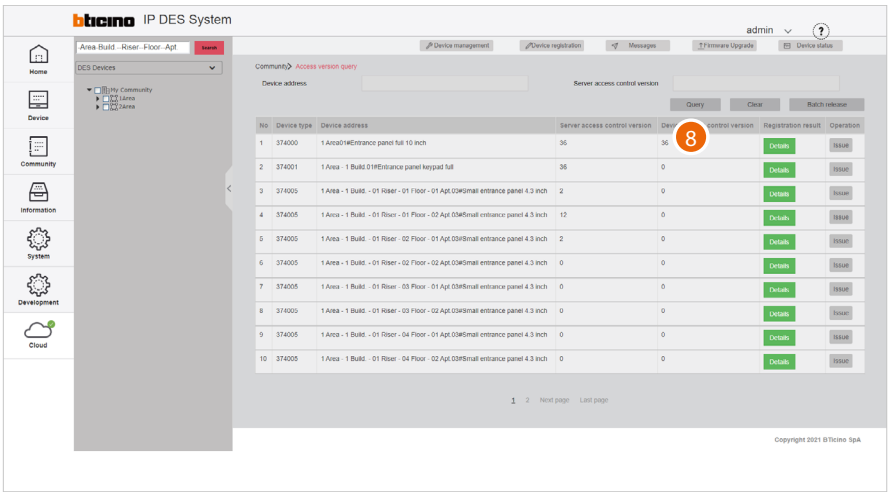
** failed accesses will be displayed by default*



6. Click to force the alignment of the database in the SD and the device



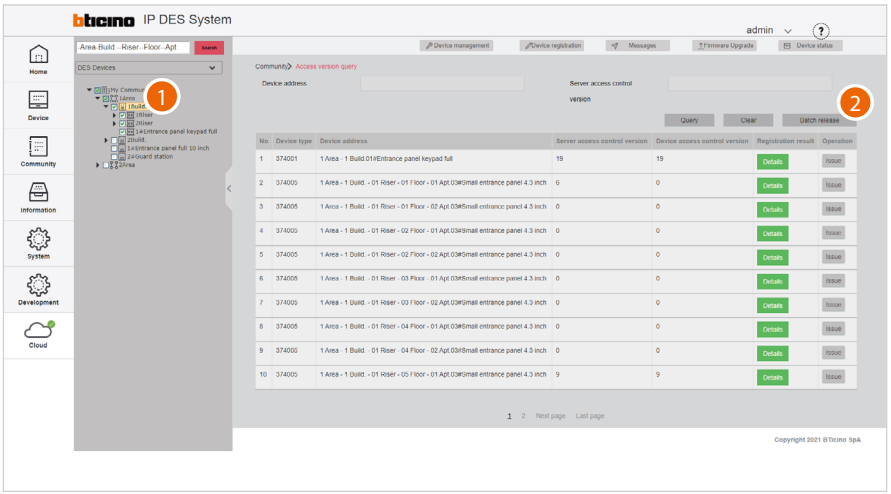
7. Click to confirm



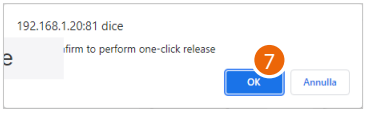
8. The database are now aligned

Batch update

It is possible to update several devices at the same time using the batch command.

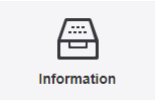


1. In the tree menu, select and tick the level for which you want to update the devices (e.g. all the devices of building 1)
2. Click to run the batch update



3. Click to confirm

Information



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

Messages	Creates and sends messages to devices within the community
Alarm history	Displays all the alarms from community devices
Access history	Displays all the community logins and registrations
Call history	Displays the community call history
Device status	Displays the status of the community devices
Device off line log	Displays the history of the community devices (online/offline)
Patrol record	Displays the history of the patrols carried out in the community
Map Configuration	Creates and manages the community Home Page map

Messages

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

– Community Message: messages about the Community

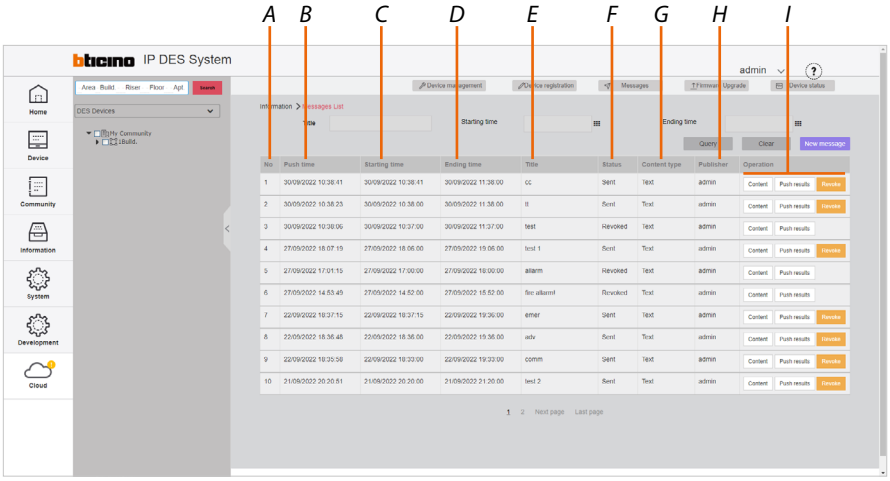
– Advertisement: messages showing advertising content.

– Emergency Notifications: emergency messages

Messages will be displayed on the devices (depending on the parameters entered in "messagelocation" and the type of device) in one or more locations:

– Screen Saver

– Call waiting page



A Progressive number

B Date and time of creation of the message

C Start of message

D End of message

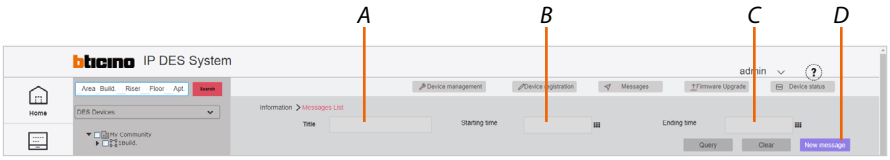
E Message title

F Message status

G Type of content

H User who published the message

I ***Message management buttons***



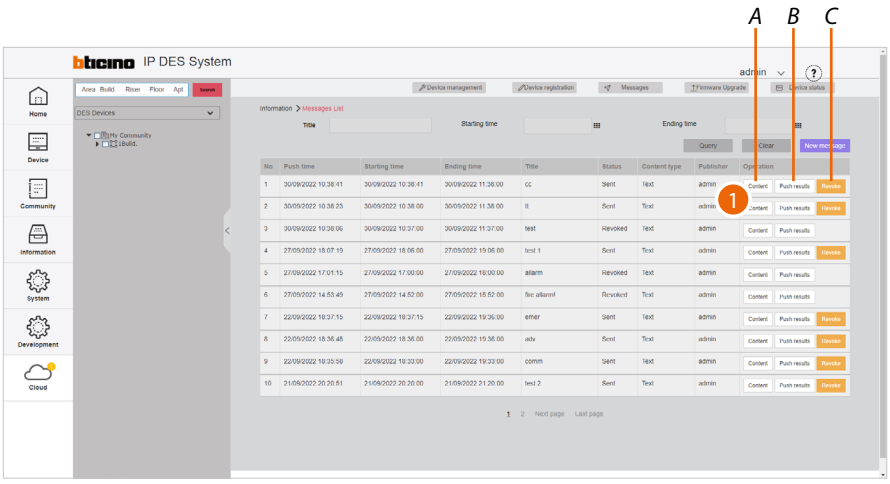
A Message title filter

B Publication start date/time filter

C Publication end date/time filter

D ***Send a new message***

Manage the messages



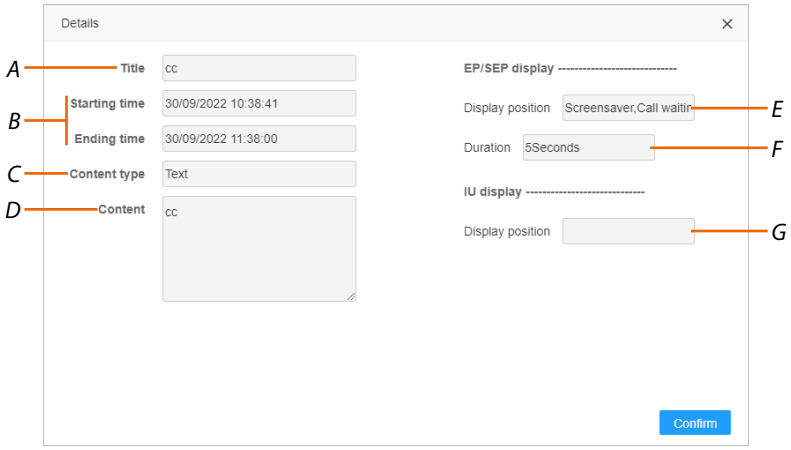
A View the details of the message sent

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 and end date

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

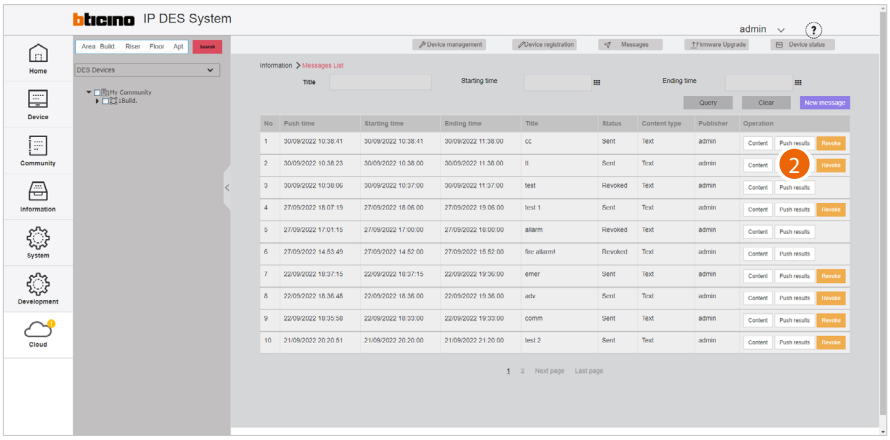
D Message text

E Location where the message is displayed on the devices (EP / SEP)

F Message length

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

Message publication details



2. Click to view the message publication details

A Progressive number

B Address of the device to which the message was sent

C Select the successful/failed messages filter

D Message status (not sent/sent)

E Publication status (executed/not executed)

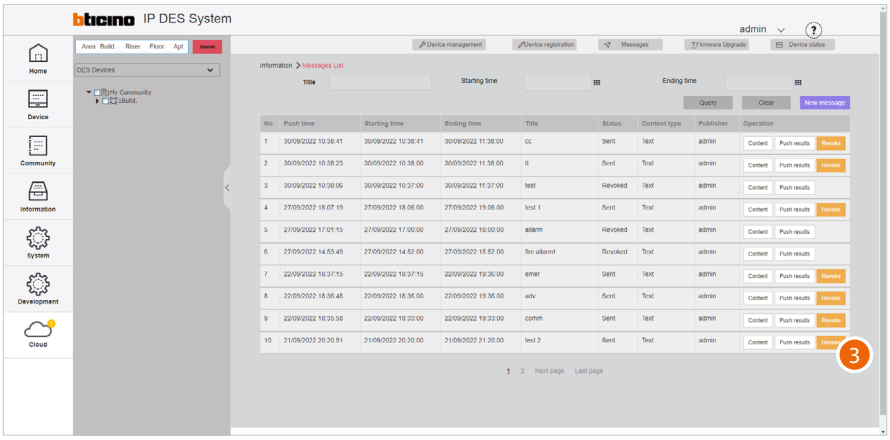
F Number of transmissions

G Date/time sent

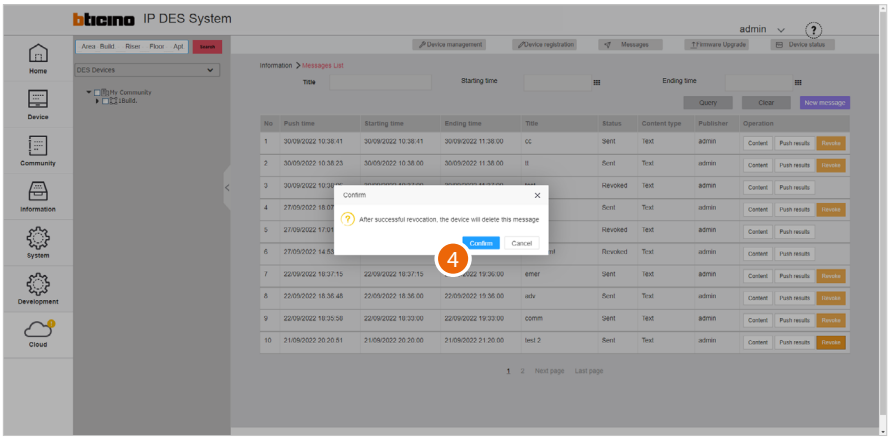
H Account that sent it

I Send again if first sending failed

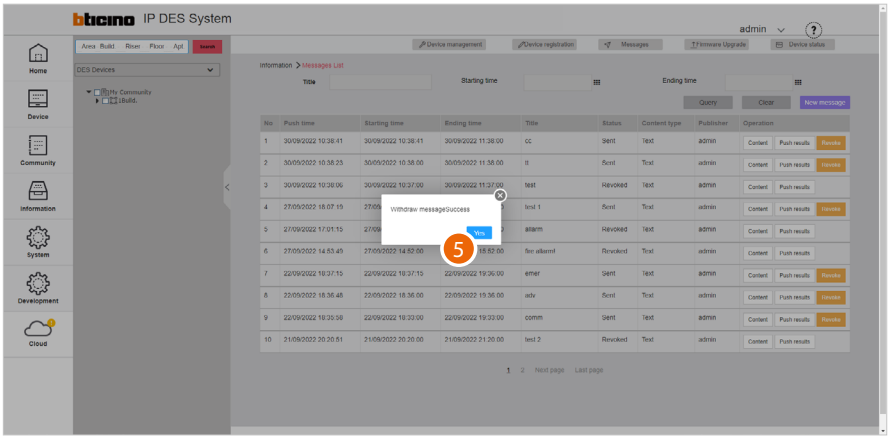
Revoke the message



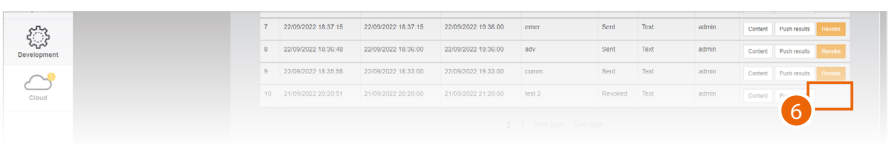
3. Click to revoke the message



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

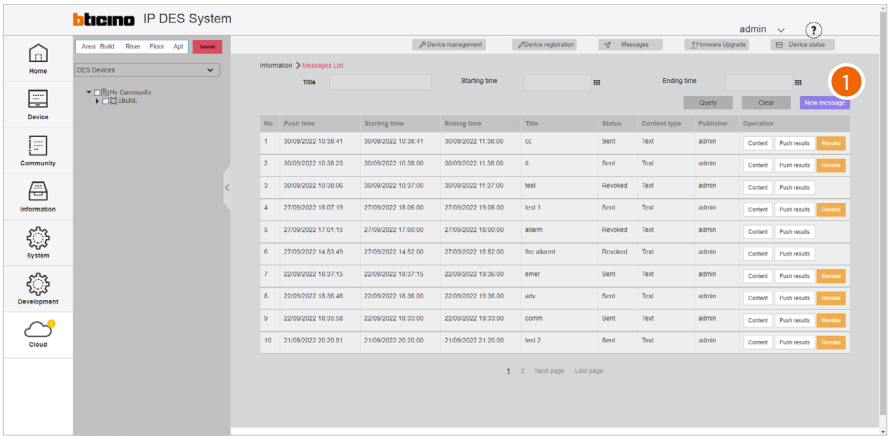


5. Click to finish

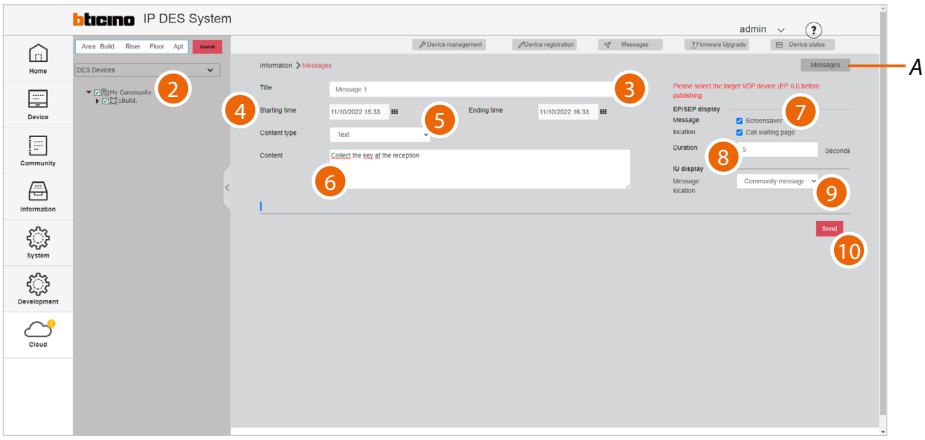


6. The message has been revoked

Create a new message

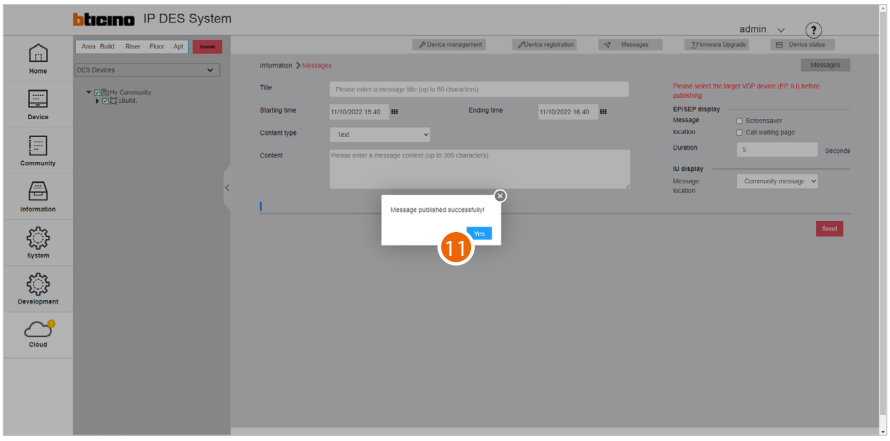


1. Click to create a new message



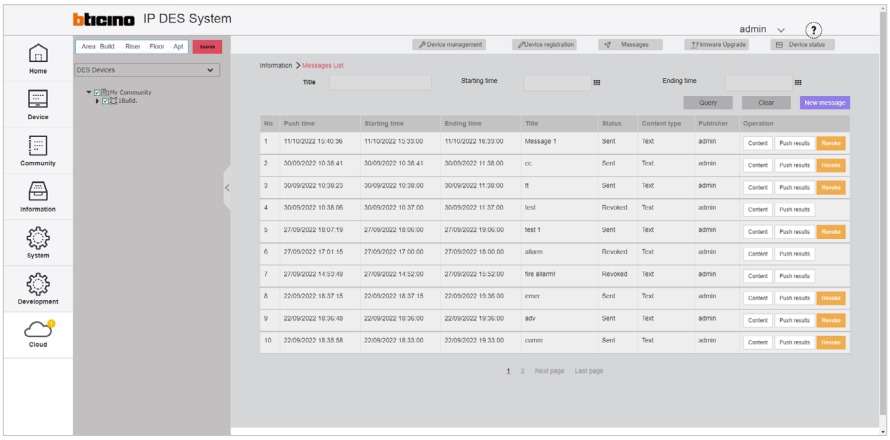
A *View the published messages history*

2. Select the community branch you want to send messages to
3. Enter a title for the message
4. Enter a publication start and end date
5. Select the type (text message, photo, video)
6. Enter the text of the message (for sending photos or videos see the relevant section)
7. Select where to display messages on the EPs (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

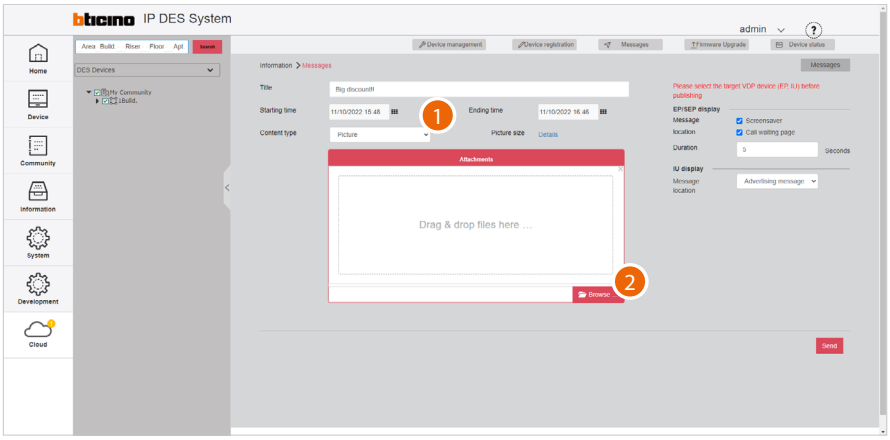


11. Click to finish

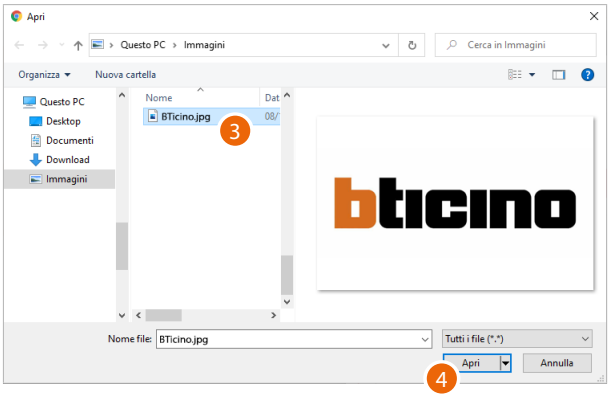
The message has been published



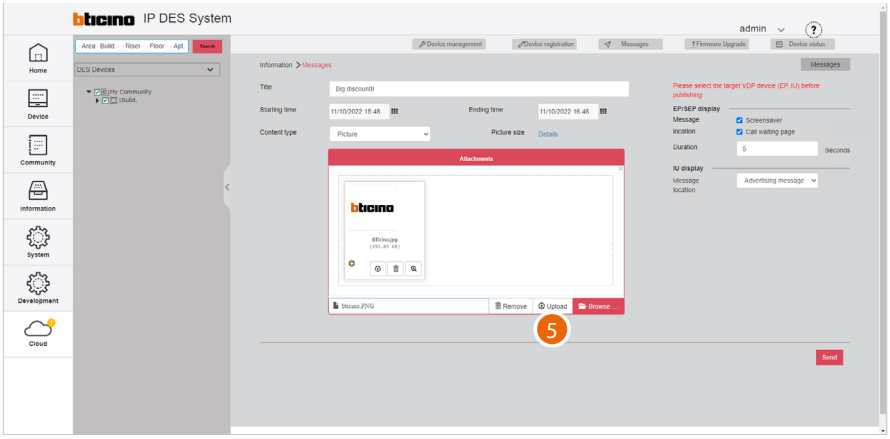
Send messages containing images or videos



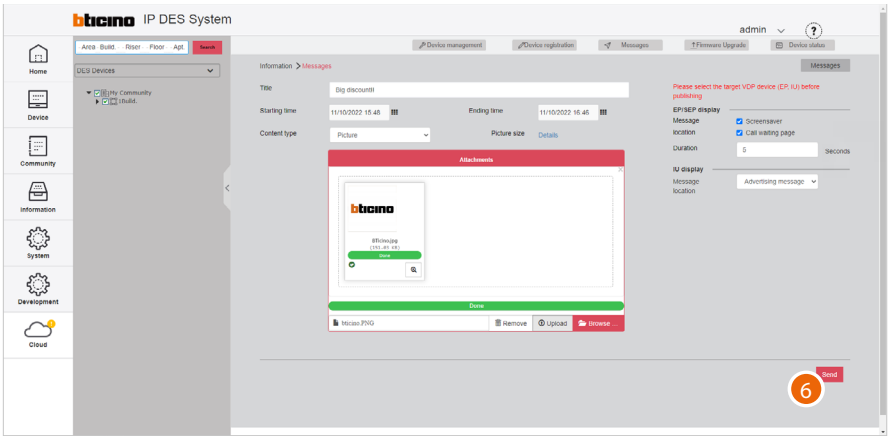
1. Select image/video as content type
2. Click to select the content



3. Select an image
4. Click to open

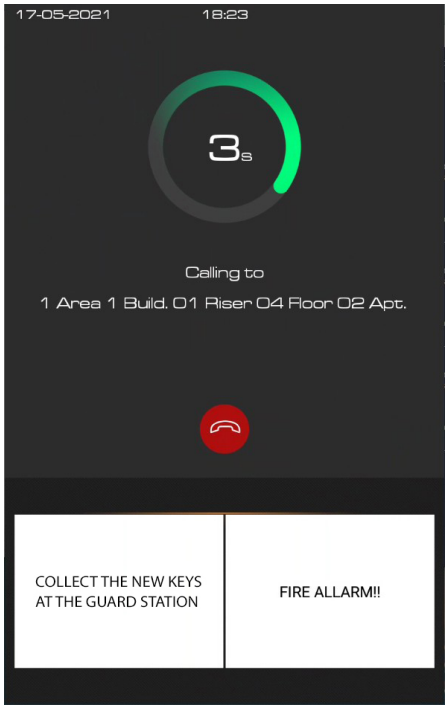


5. Click to load the image

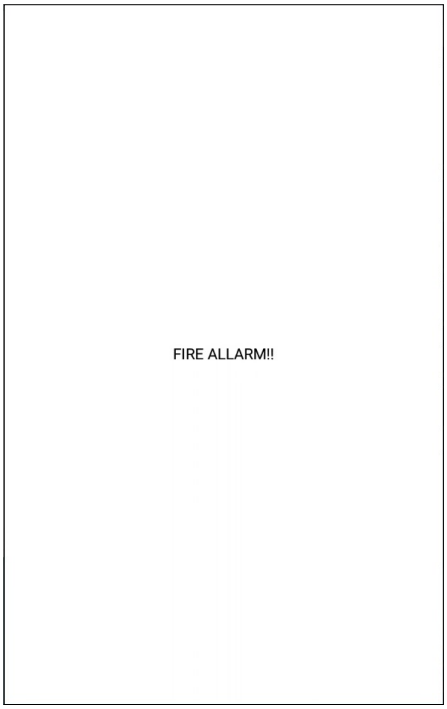


6. Click to publish the message

The message has been published; click to finish



Messages displayed during a call

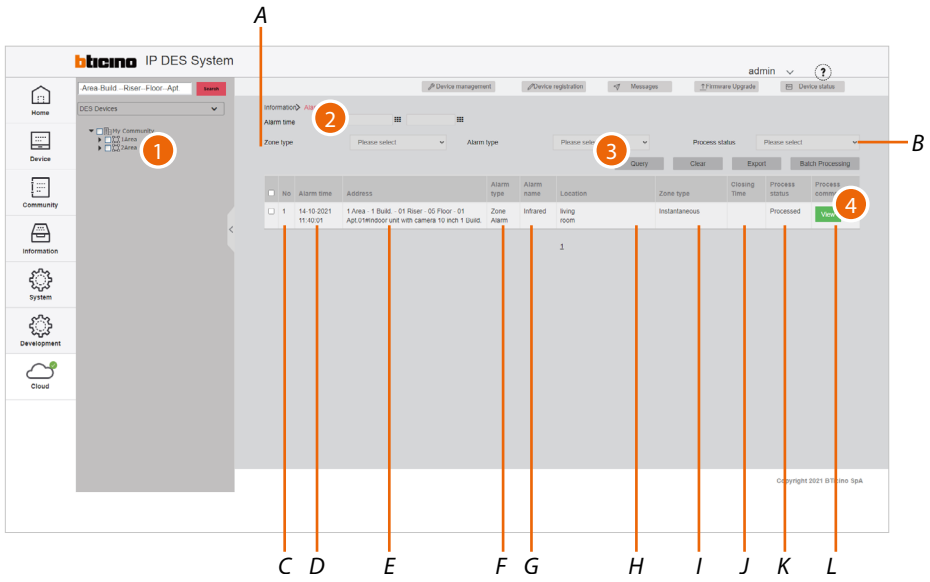


Messages displayed as screen saver

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

Alarm history

This page can be used to view IU and EP alarms (panic and tamper)



A Alarm filters

B Alarm management keys

C Progressive number

D Date and time of the alarm

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

F Type of alarm

G Type of sensor

H Name of the alarmed zone

I Type of alarm zone

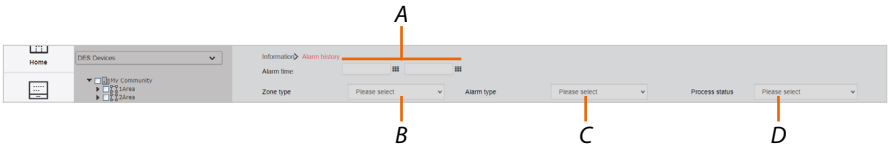
J Process closing date and time

K Management status

L Alarm management comments

1. Select the community branch that contains the EPs 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

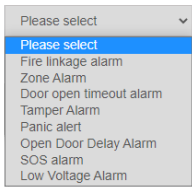


A Alarm monitoring period

B Type of zone

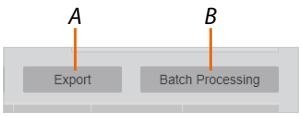
24hours	The probe is always active, even if the alarms are totally deactivated
Instantaneous	The alarm is immediately communicated
Delay	The alarm is given at a certain time after the triggering condition occurs
Activity check	The alarm is communicated immediately, if the sensor does not detect activities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

C Type of alarm



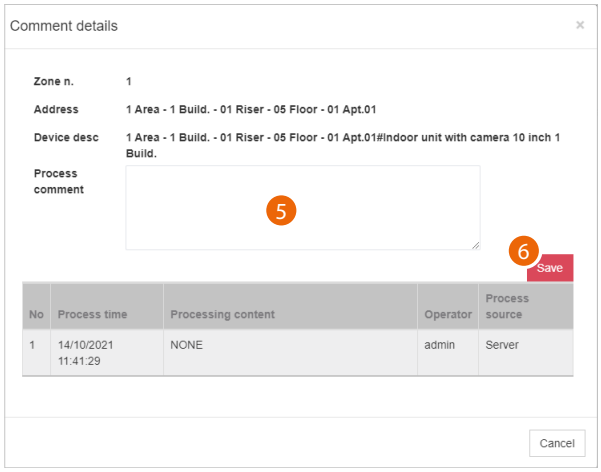
D Status (processed/not processed)

Alarm management keys



A Export the alarm list to an Excel® file

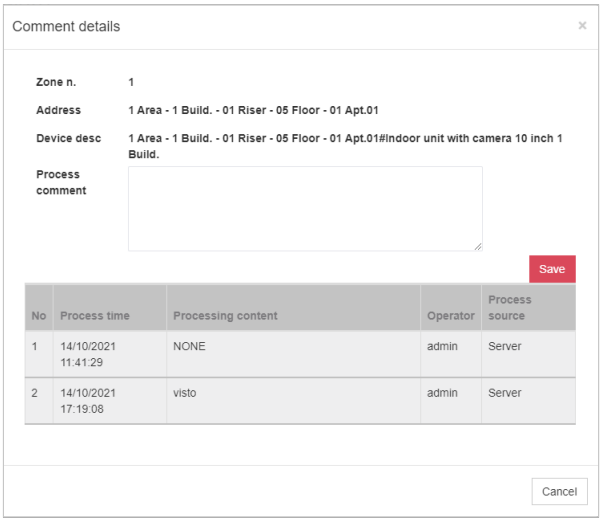
B Process several alarms simultaneously



A panel opens with some alarm details, a field for entering comments and the list of previous management activities (*A*)

5. Add a comment
6. Click to save

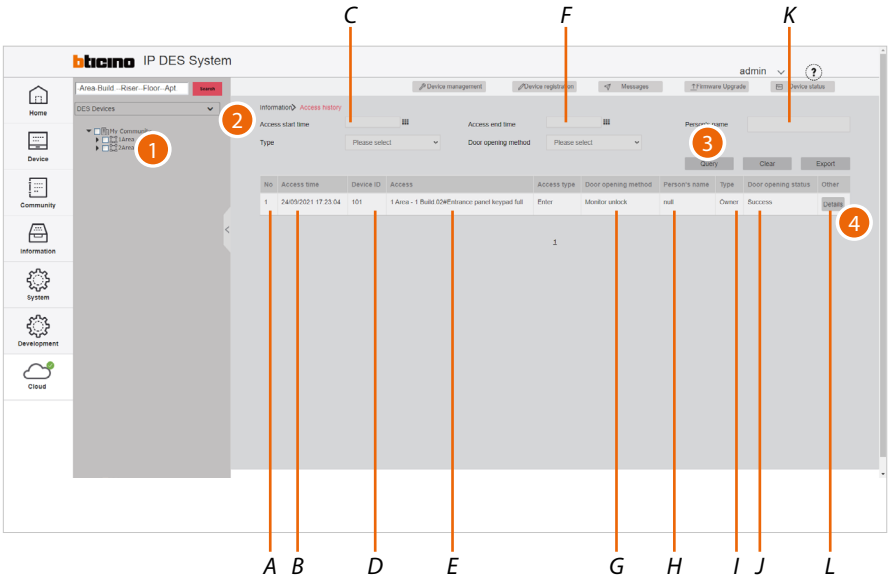
7. Click to continue



The comment has been added

Access history

In questa pagina puoi visualizzare ed esportare in una lista gli accessi effettuati nella community



A Progressive number

B Access time and date

C Access start time/date filter

D Univocal code

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

F Access end time/date filter

G Lock opening method

H Name of the person who completed the access (e.g. person associated with the card/badge used)

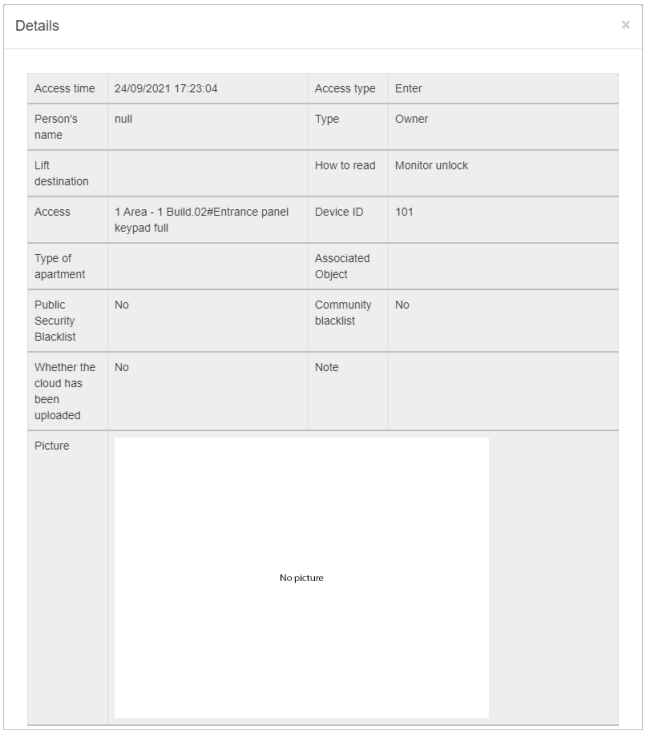
I Type of person who completed the access

J Opening outcome

K Person who completed the access filter

L Access details

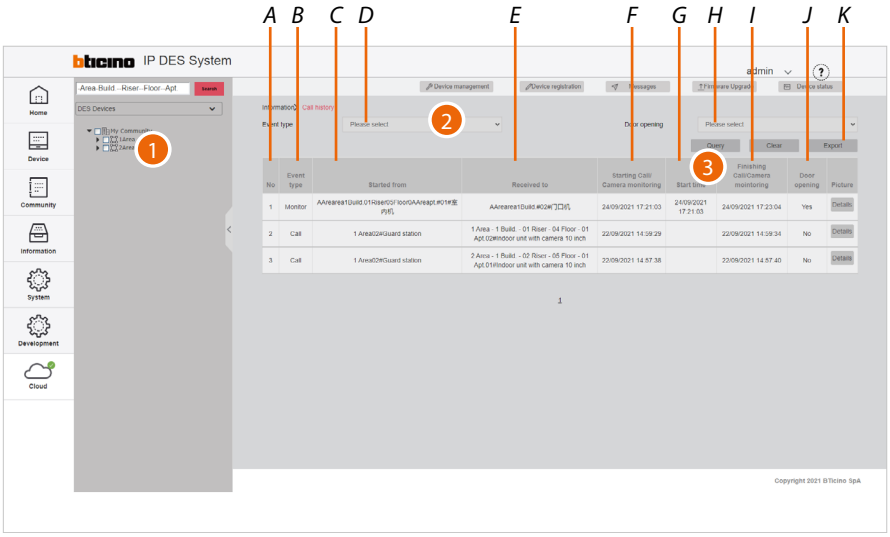
1. Select the community branch that contains the EPs concerned
2. If necessary, use the filters to narrow down the selection
3. Click to apply the filter
4. Click to display the access details



Some details are displayed.

Call history

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



A Progressive number

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

C Name of the receiving device (customisable).
The original name represents the address of the device in the community

D Event type filter (call to IU or GS/monitoring of EP)

E Name of calling device (customisable).
The original name represents the address of the device in the community

F Call or monitoring start date/time

G Date/time the call was answered. If empty, it means missed call or busy device.

H Call with door opening filter (yes/no)

I Call or monitoring end date/time

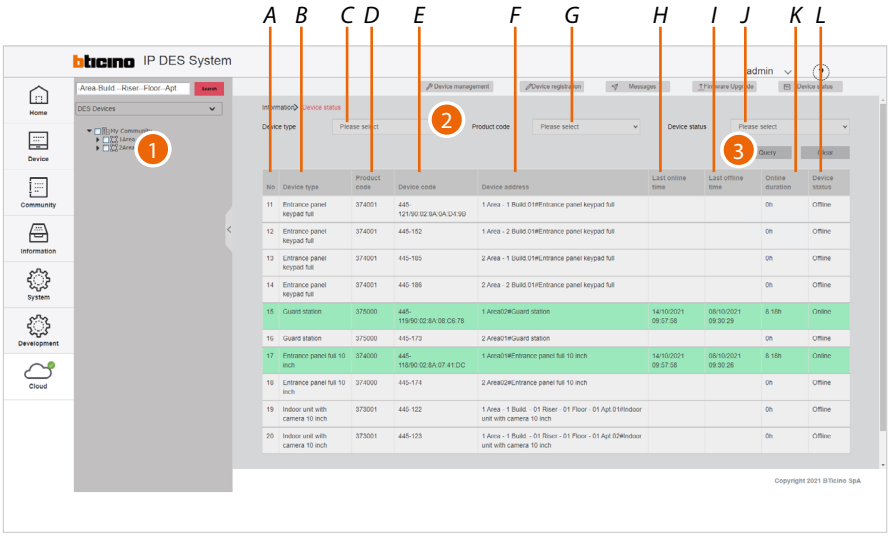
J Opening of door after call

K 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

Device status

This page can be used to display the device status.
For correct operation of the devices, online status is required (green colour)



A Progressive number

B Type of device

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

D Item code

E Community ID + Unique code + Mac address

F Name of the device (customisable).
The original name represents the address of the device in the community.

G Item code filter

H Last date/time the device was online

I Last date/time the device was offline

J Device status filter (online/offline)

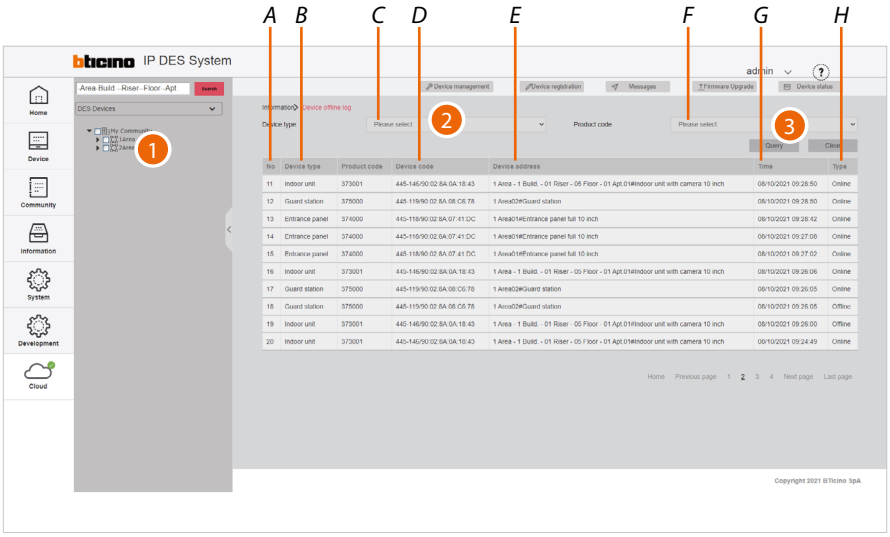
K Duration of online status

L Device status

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

Device off line log

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



A Progressive number

B Type of device

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

D Item code

E Community ID + Unique code + Mac address

F Item code filter

G Name of the device (customisable).
The original name represents the address of the device in the community.

H Status start date/time

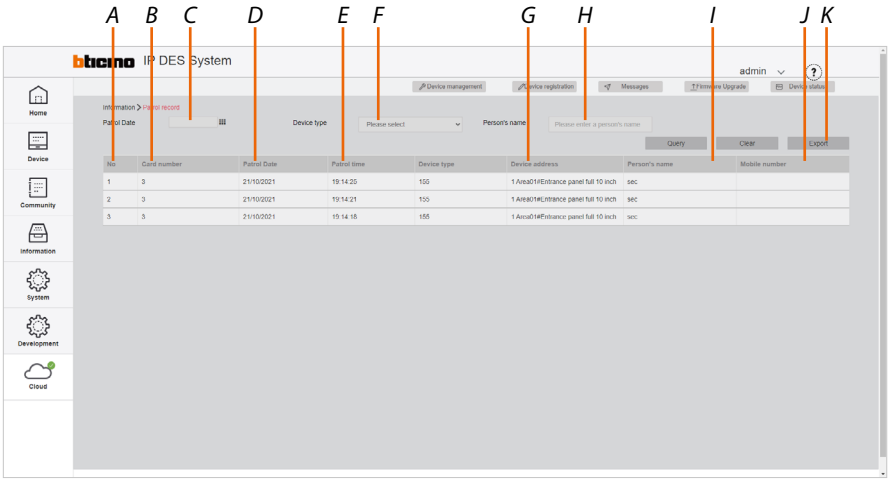
I Device status

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

Patrol record

This page can be used to view patrol security check point records.

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



A Progressive number

B Badge/card ID

C Check point date filter

D Check point date

E Check point time

F Device filter

G Name of the device (customisable).
The original name represents the address of the device in the community.

H Check point responsible person filter

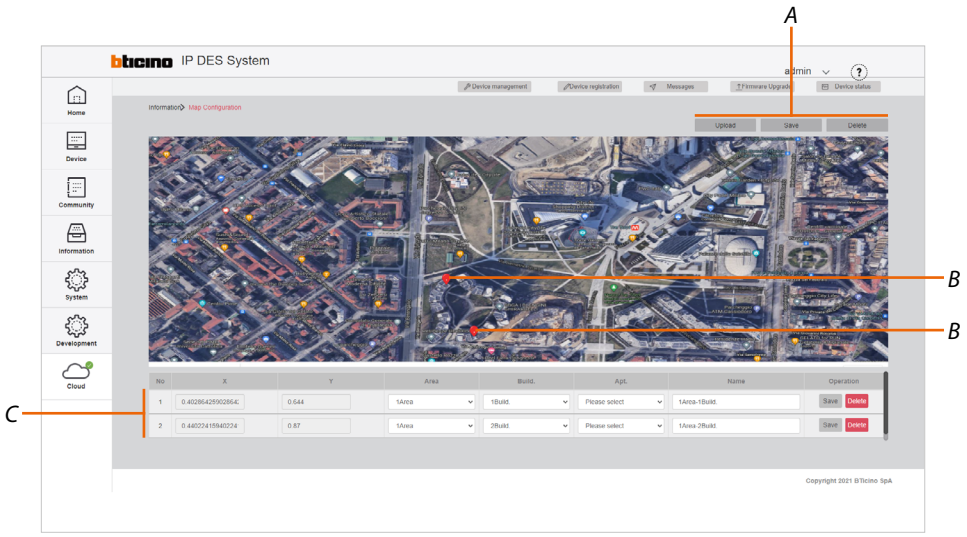
I Name of manager or security (persons with manager or security status)

J Telephone number of manager or security (persons with manager or security status)

K Export the list to an Excel® file

Map Configuration

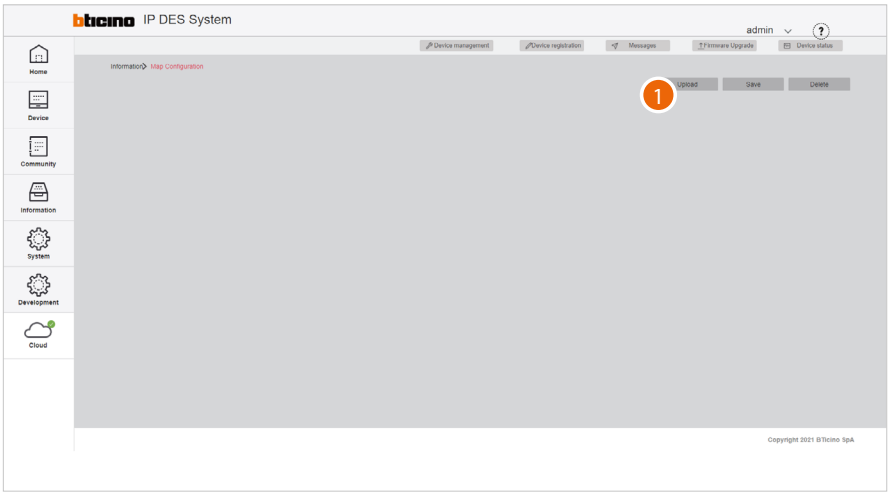
This page can be used to set up a background map for the Home Page and some markers, to make it easier to find the community buildings



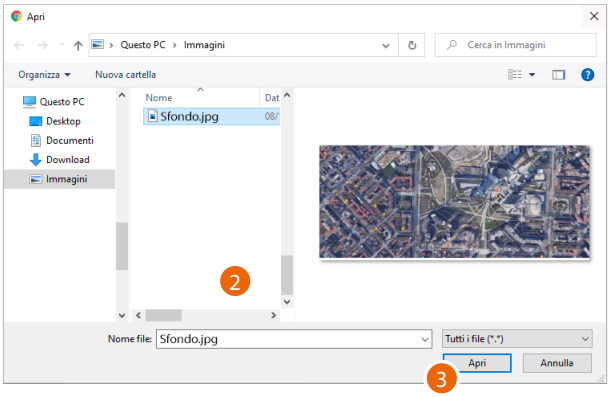
A Map management keys

B Markers

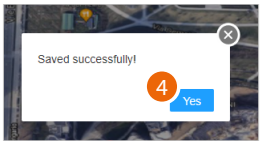
C Marker management



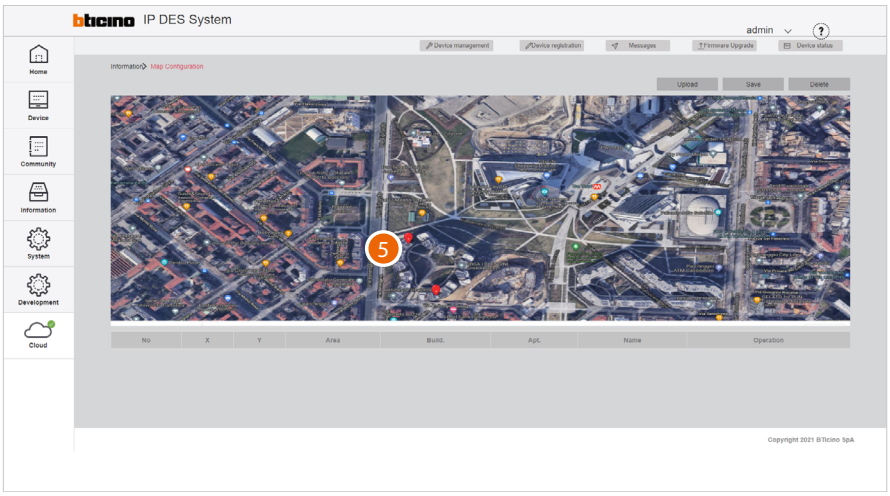
1. Click to load an image to use as map



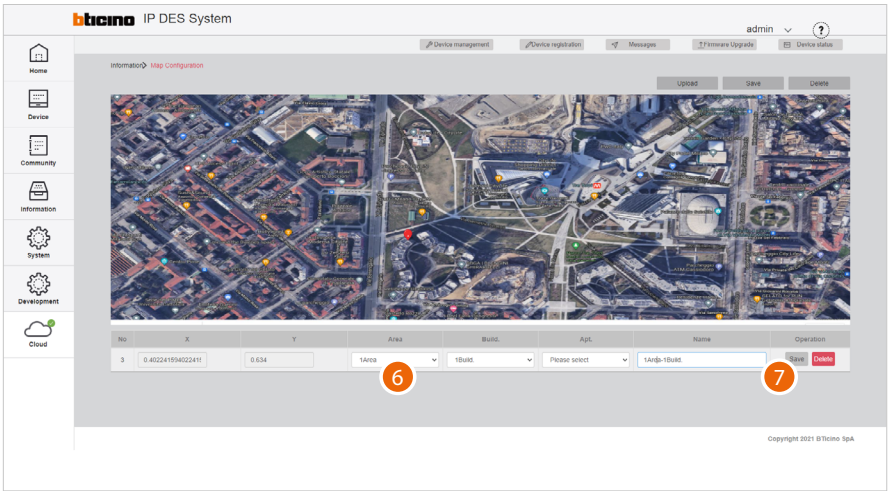
2. Click to select an image
3. Click to open



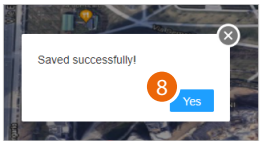
4. Click to finish



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



8. Click to finish

System

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

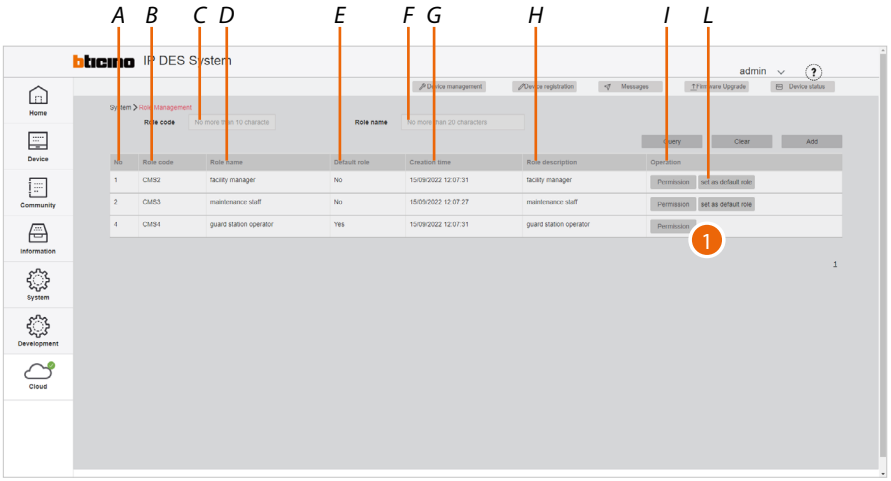
Role Management	Creates and manages the roles of the accounts of the SW
Operator Management	Creates and assigns roles to accounts, to perform configurations using the SW
Modify Password	Modifies the password of the current account
System operation log	Displays the list of the operations carried out by the accounts
System data backup	Performs the system backup
System Data Recovery	Restores the saved backups
System version information	Displays information concerning the installed SW versions
Diagnostic	Save the DES Server logs in a file
Upgrade	Update the DES Server 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 4 default roles for which permissions cannot be changed:

- Admin = main role, access enabled for all items (not displayed in the page)
- Technical staff = Access enabled for the following: Home, Device, Community and Information
- Facility manager= Access enabled for the following: Home, Device, Community, Information and System.
- GS = Access enabled for the following: Home, Community and Information.

It is also possible to create roles with specific permissions according to specific needs



A Progressive number

B Role code

C Role code filter

D Role name

E Indicates the default role.
The permissions set for this role will be assigned to all newly created roles.

F Role name filter

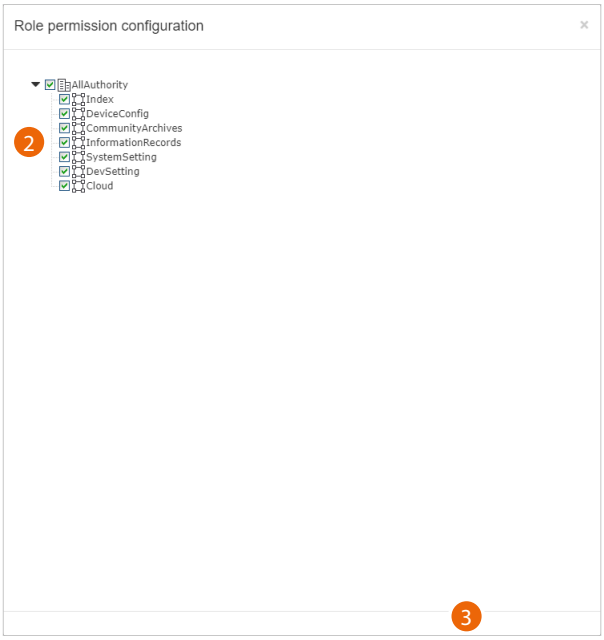
G Time/date of role creation

H Role description

L Set the role as default

I Opens the permission display/setup panel

1. Click to view/change the permissions of a role

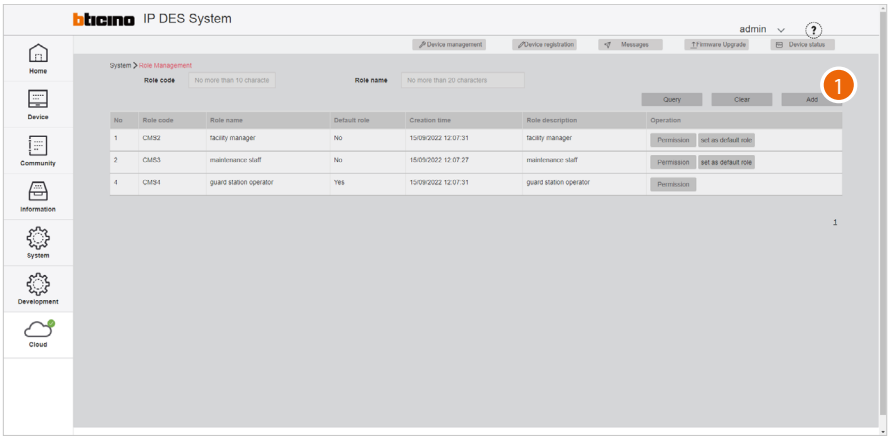


2. Tick the permissions to be assigned to the role
3. Click to confirm

PERMISSION TABLE

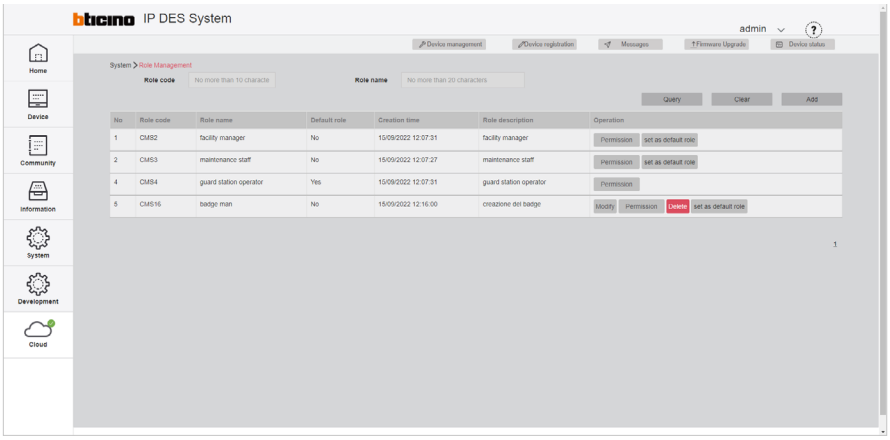
AllAuthority	
Index	home menu activation
DeviceConfig	device menu activation
CommunityArchives	community menu activation
InformationRecords	information menu activation
SystemSetting	system menu activation
DevSetting	development menu activation
Cloud	Cloud menu activation

Create a role



1. Click to create a new role

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 Modify the role name and description

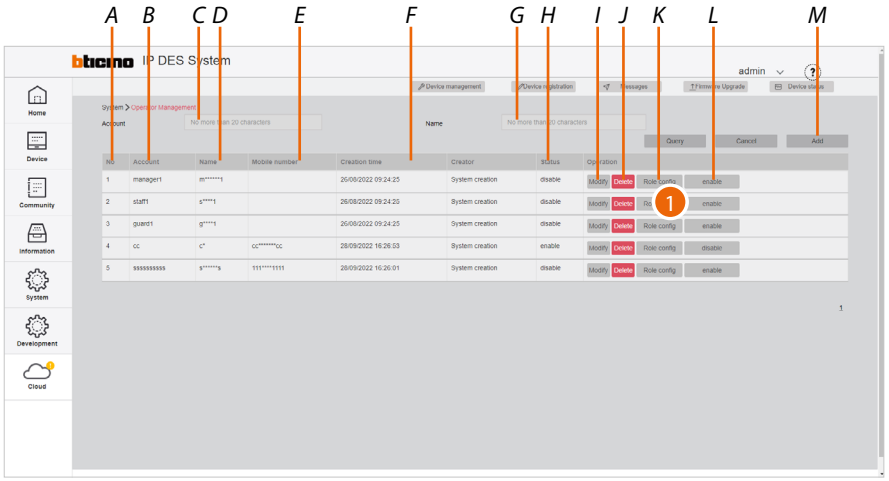
B Edit the permissions

C Delete the role

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

Operator Management (account)

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



A Progressive number

B Account name

C Account filter

D Account user name

E Account telephone number

F Date of creation

G Account user name filter

H Account status

I Modify the account data

J Delete the account (name and password)

K Open the panel to manage account roles

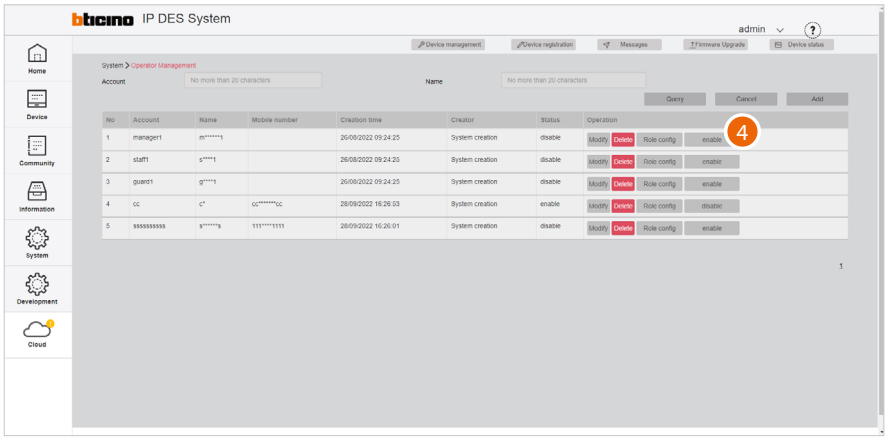
L Enable/disable the account

***Note**: during the first enable, the password must be changed*

M Create an account

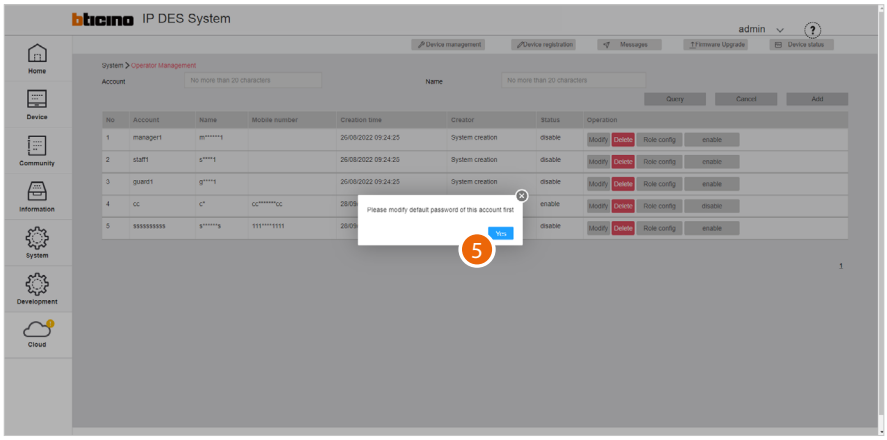
1. Click to display/modify the account roles

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

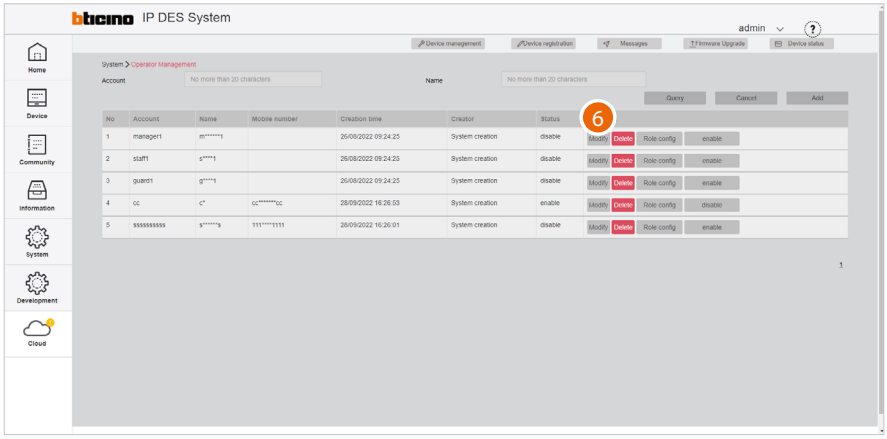


4. Click to enable the account

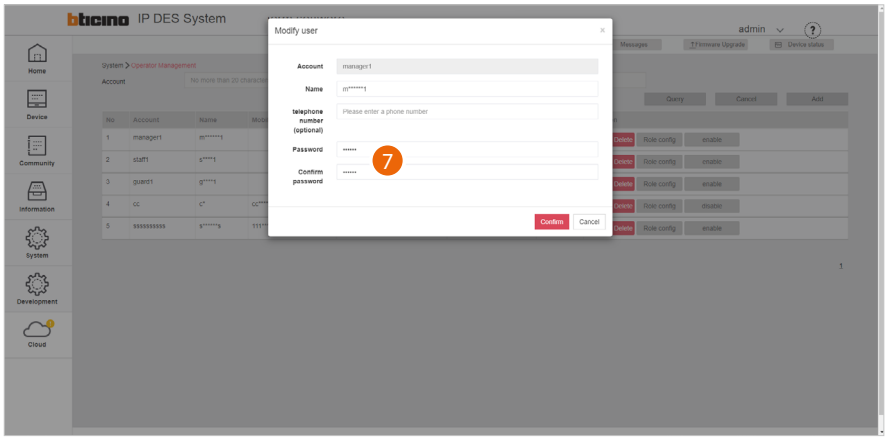
During the first enable, the password must be changed



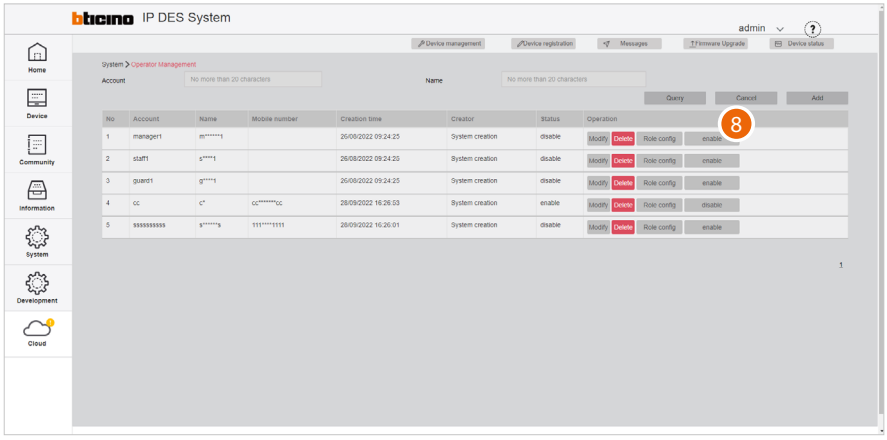
5. Click to continue and change the password



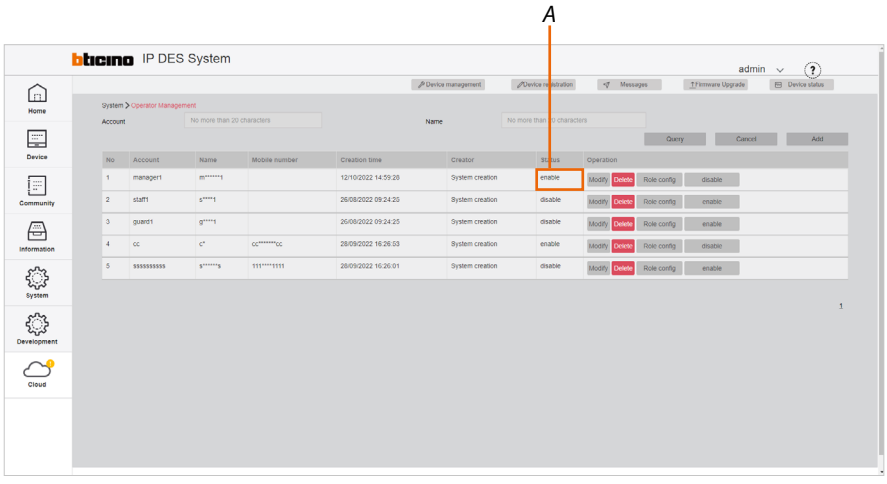
6. Click to modify the password



7. Enter and confirm the new password

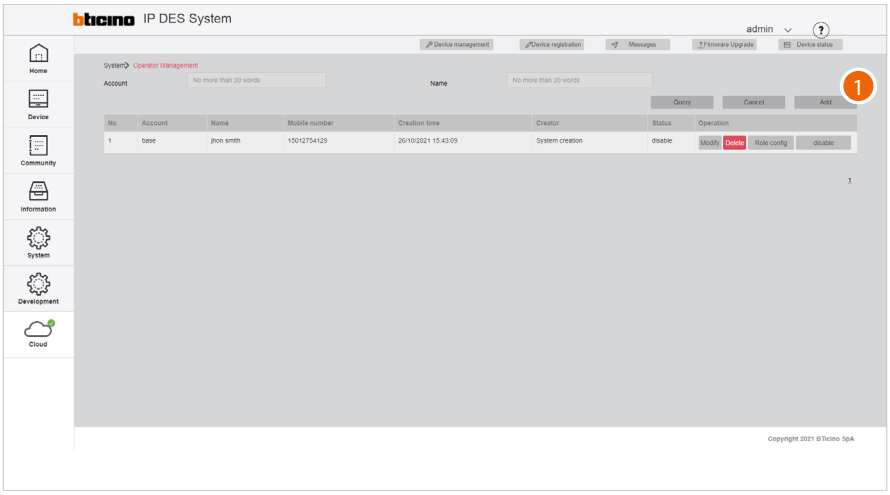


8. Click to enable the account



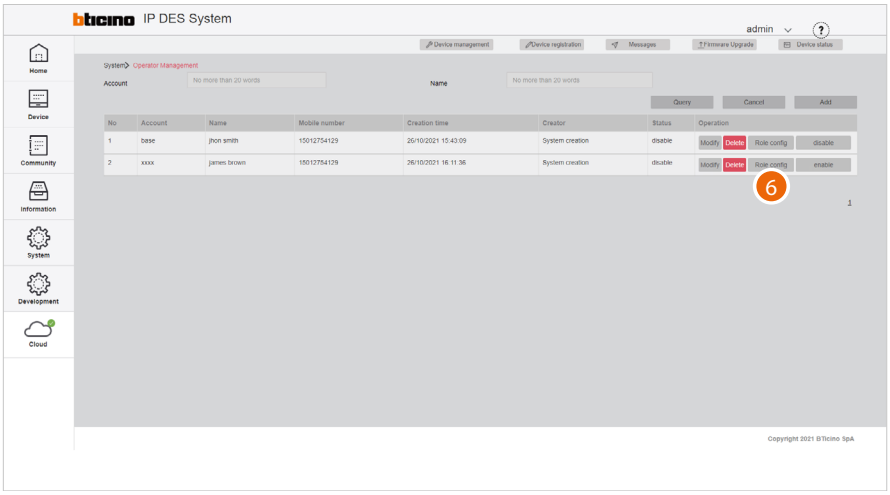
A The account has been enabled

Create an account

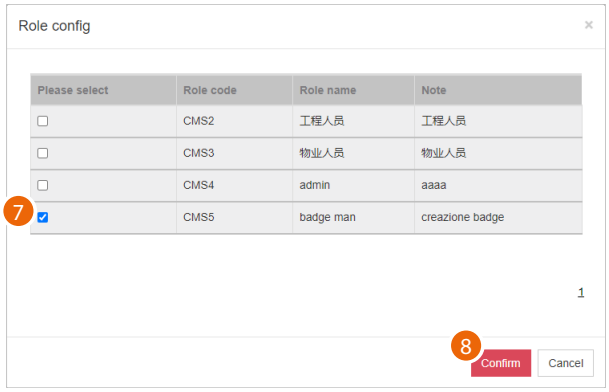


1. Click to create a new account

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



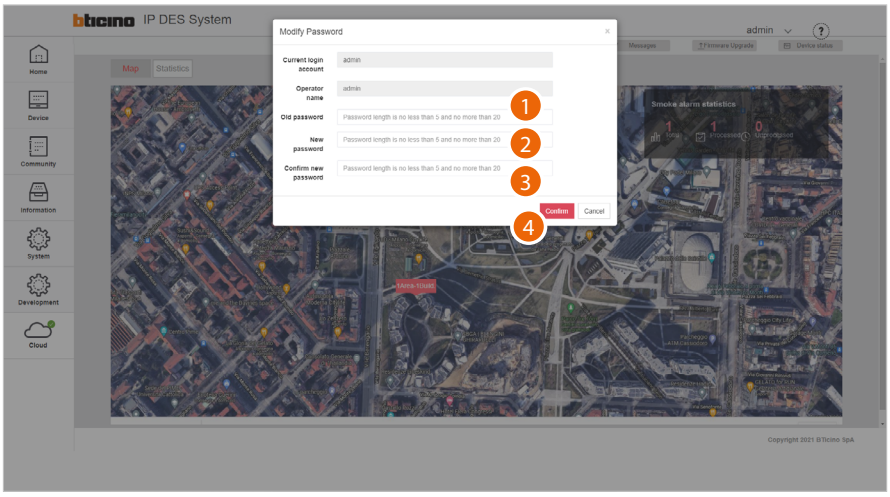
6. The account has been created; click to assign a role to the same



7. Select the role to be associated
8. Click to confirm

Modify password

This page can be used to modify the Operator (account) password with which the software was accessed

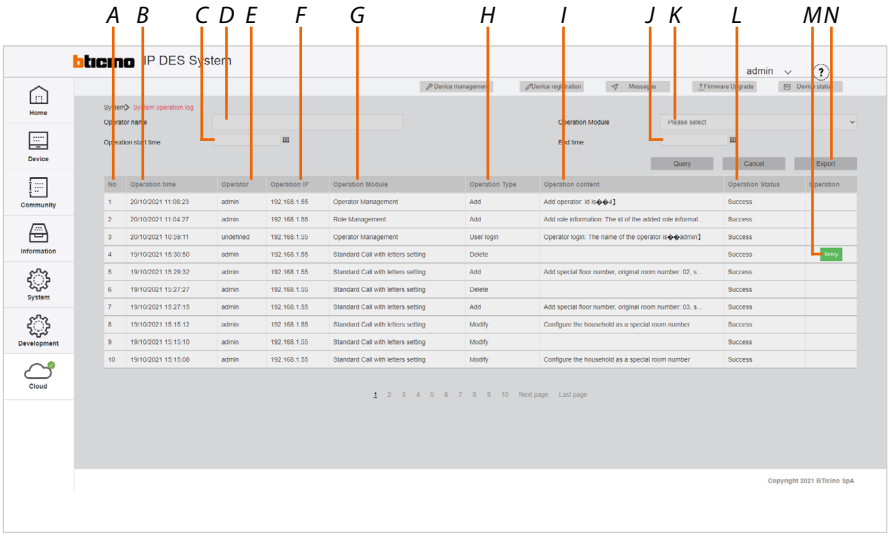


1. Enter the current password
2. Enter the new password (5 to 20 characters, at least one upper case letter, one number and one special character)
3. Enter the new password again
4. Click to confirm

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

System operation log

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



A Progressive number

B Date/time of operation

C Operation start date/time filter

D Account name filter

E Account name

F IP addresses from which the change was made

G Configuration category

H Type of operation

I Description of the operation

J Operation end date/time filter

K Category configuration filter

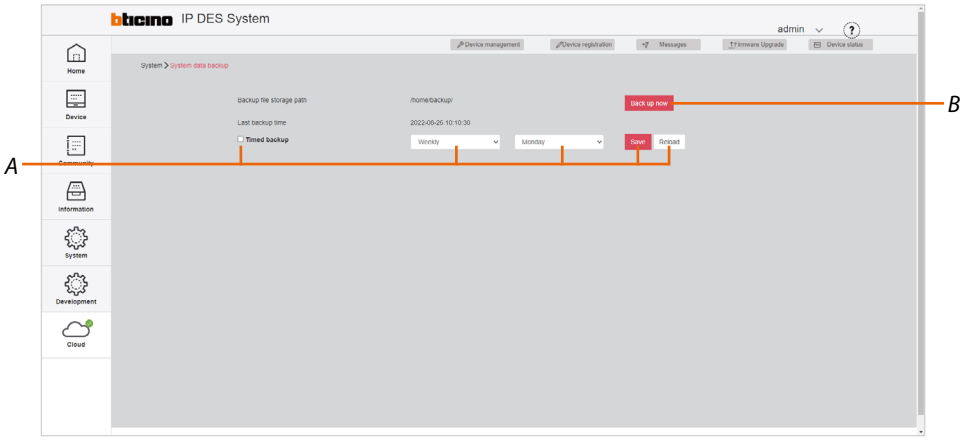
L Operation result

M Repeat the operation if it fails

N Export the list to an Excel® file

System data backup

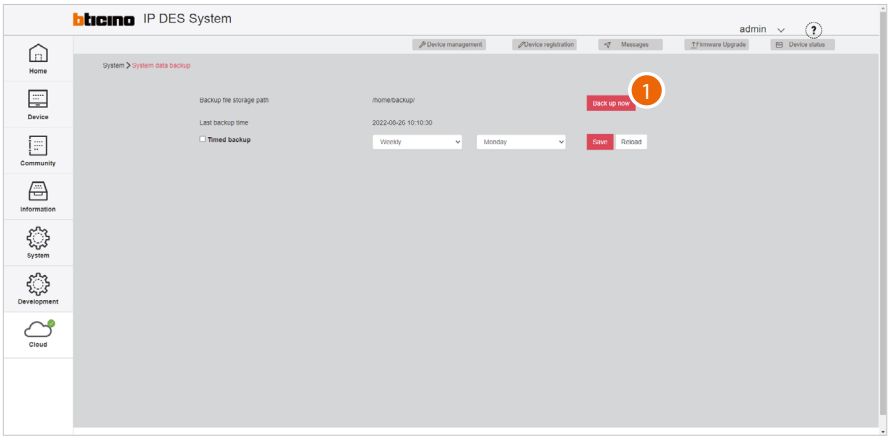
This page can be used to backup the system.
Date can be restored from the System Data Recovery page



A Scheduled backup commands

B Immediate backup commands

Immediate backup

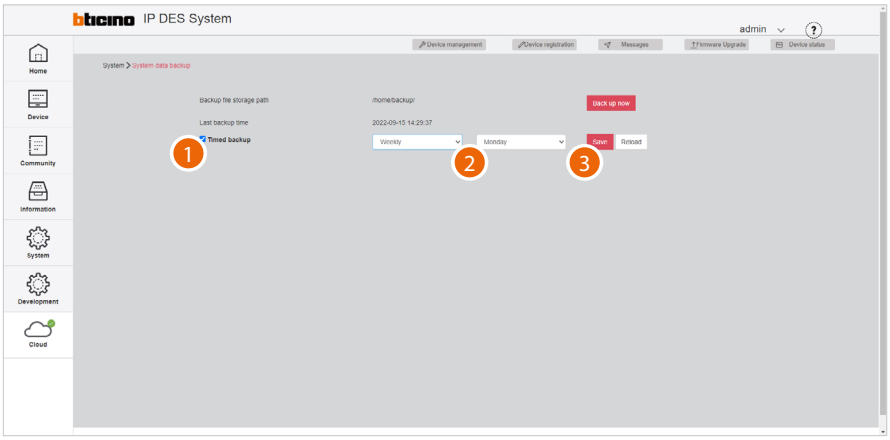


1. Click to immediately start the backup

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 Progressive number

B Backup date/time

C Backup name

D SD version on which the backup was saved

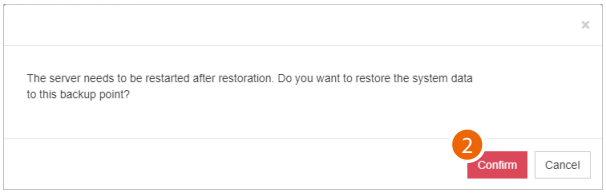
E Backup result

F Backup description

G Backup presence and integrity check.
If the check is successful, the Restore button appears (H)

H Backup restore

1. Click to restore the data

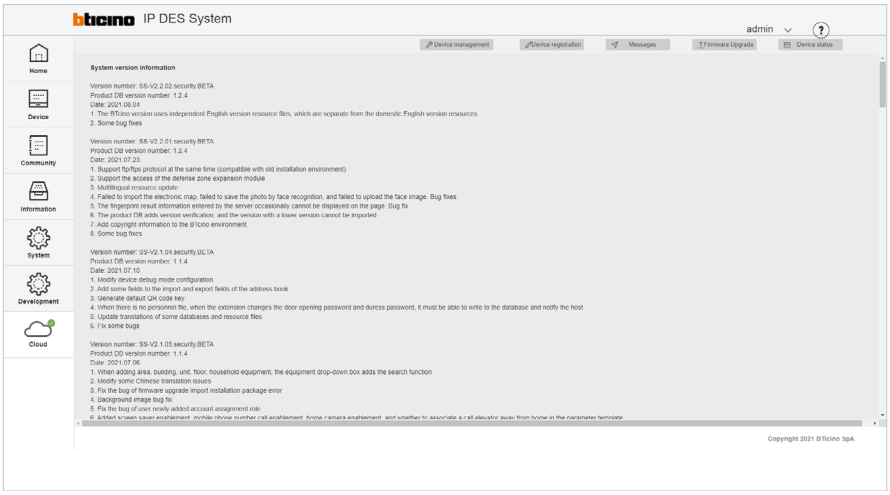


2. Click to confirm

***Caution**: the existing data will be overwritten*

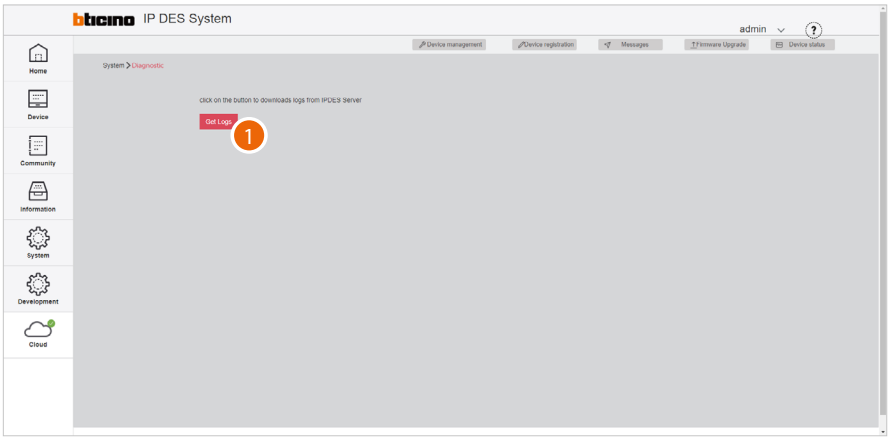
System version information

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



Diagnostic

This page can be used to save the IPDES server logs in a file (what kind?)

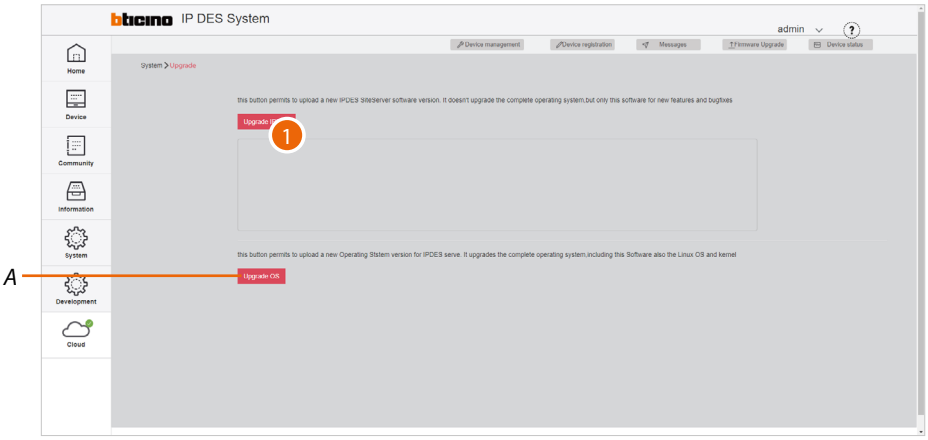


1. Click to download the file

Update the IP DES software

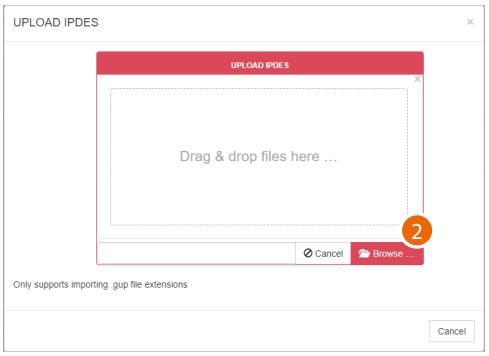
This page permits to upload a new IP DES Site Server software version. It dosen't upgrade the complete operating system, but only this software for new features and bugfixes

Aggiorna software IP DES

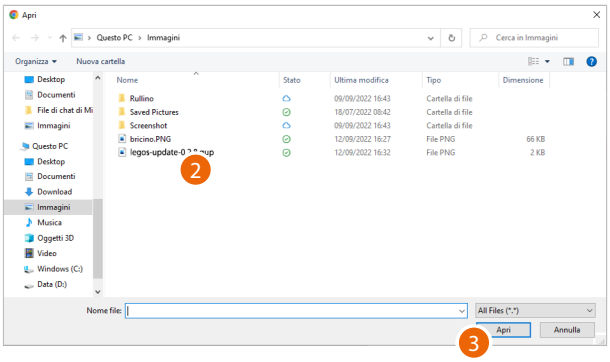


A *Linux and Kernel Update (future uses)*

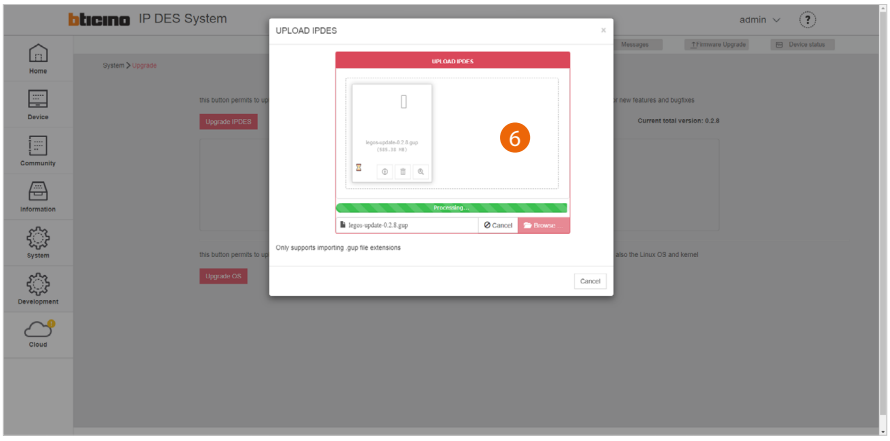
1. Click to upload the file



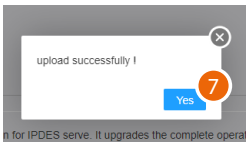
2. Click to search for the file



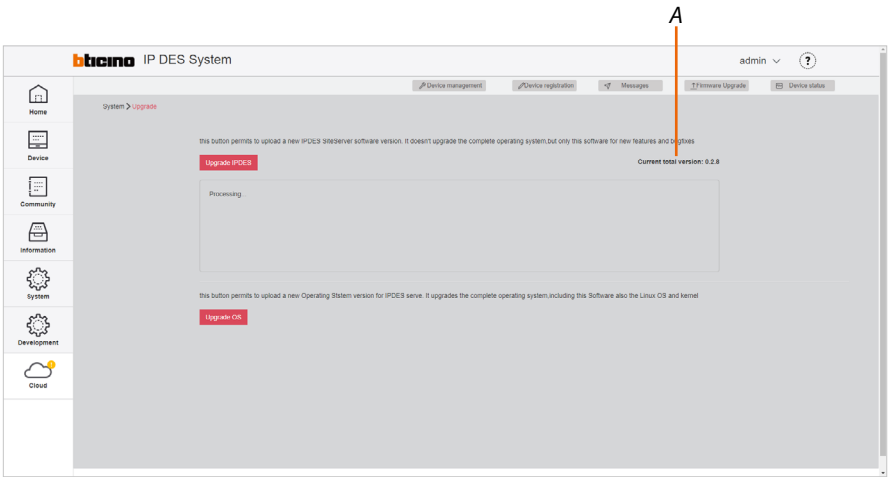
3. Select the file
4. Click to confirm



6. The update procedure starts



7. Click to continue



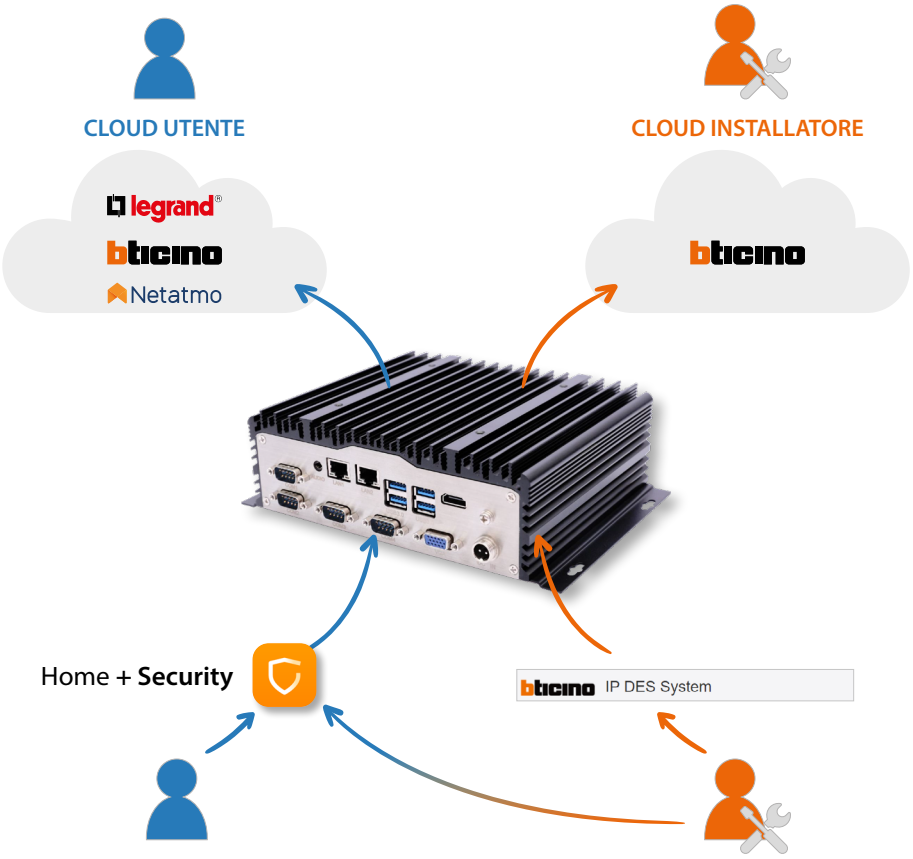
A Current software version

Cloud

This menu allows, after authentication via an Installer account, to save a copy of the AB + other data to the Installer's Cloud.
This operation allows to:

- sync of the installation and import pre-configured plant
- greater data backup security
- download FW to update the system
- share access to other 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.

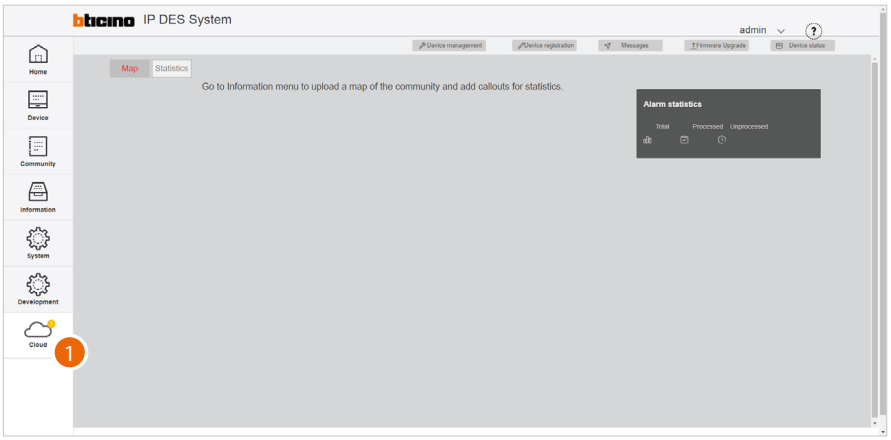


***NOTE**: With a single apartment block Internet connection, it is also possible to manage the forwarding of calls from all entrance panels to the enabled internal units.*

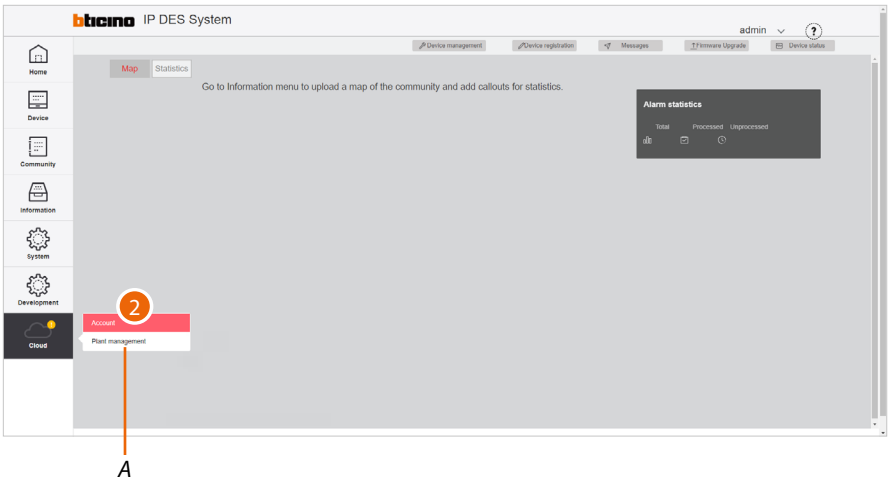
First access

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

Cloud not enabled	Cloud enabled	No Internet connection

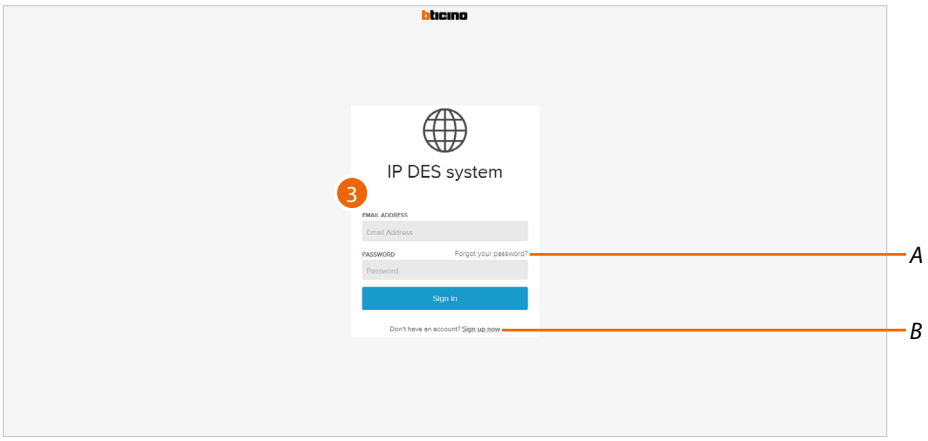


1. Click to enter the menu



2. Click to complete the Installer's Cloud authentication process.

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

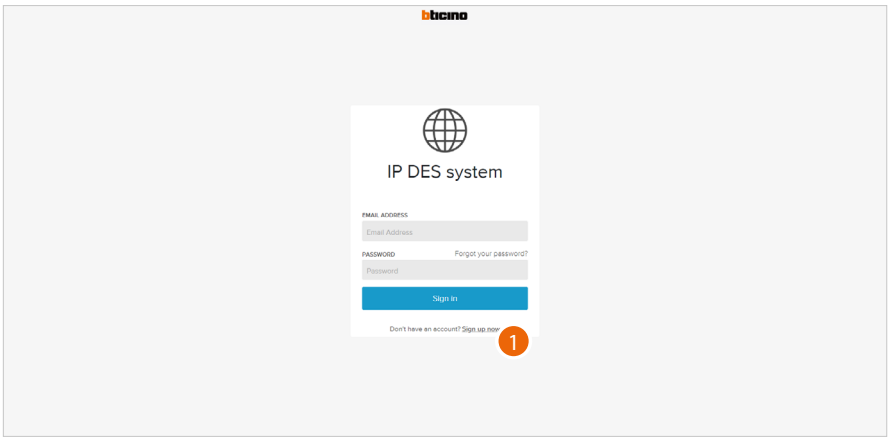


3. If you are already registered, run the authentication process, or register a new account (*B*).

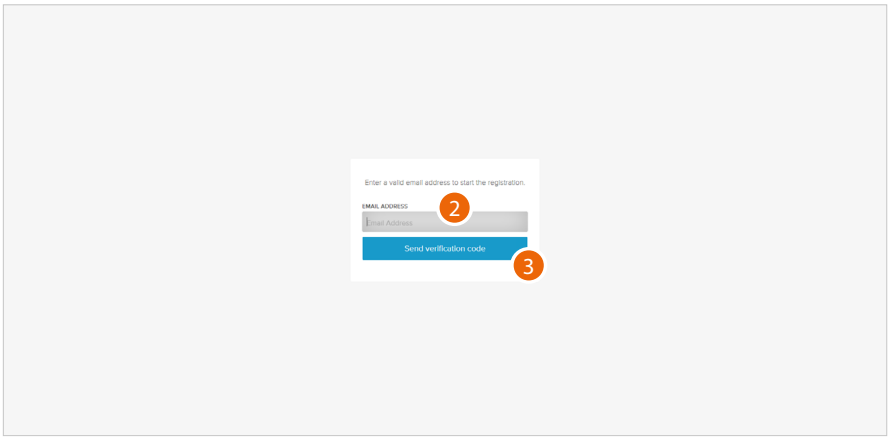
A Recover the forgotten password

Account registration on the Legrand Commercial Cloud

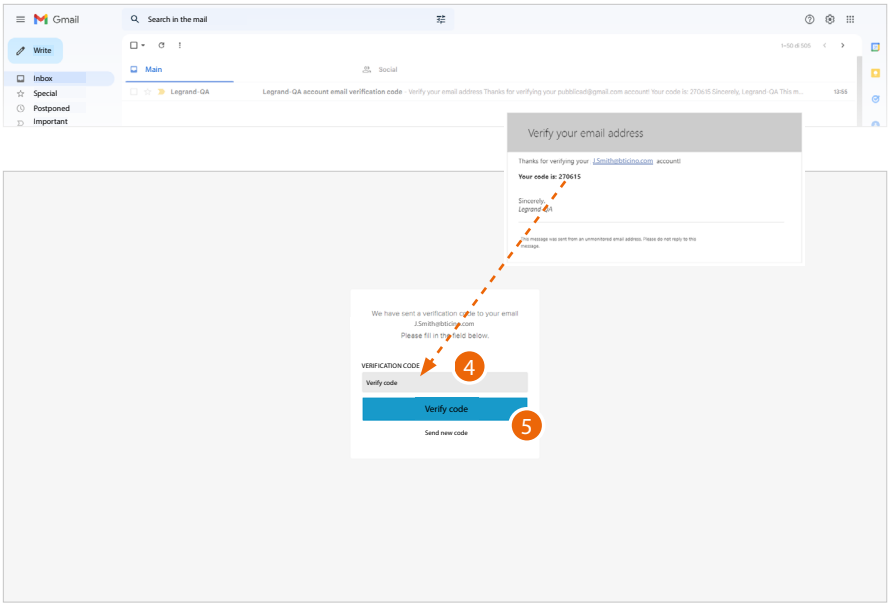
In order to use the cloud you must first register. To register, follow the instructions:



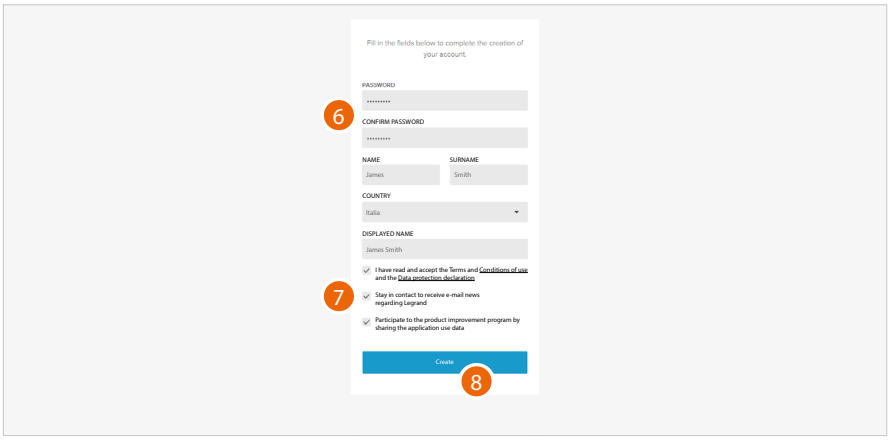
1. Click to register and create an account



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

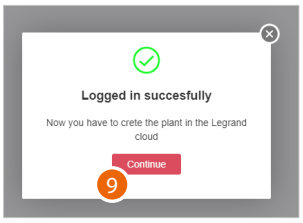


4. Enter the verification code received by e-mail
5. Click to confirm

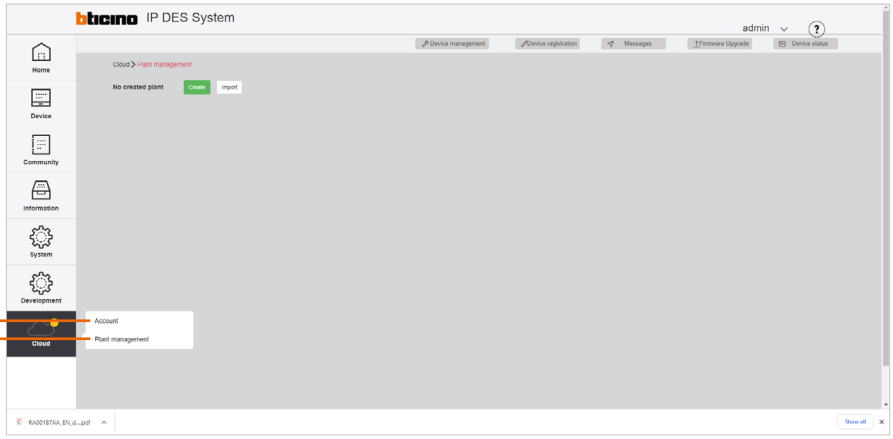


6. Enter a password and fill the fields with your details.
7. Tick to accept the terms and conditions of use laid down in the associated text (obligatory).
8. Click to continue.

The account has been correctly created



9. Click to finish.



Now it is possible to:

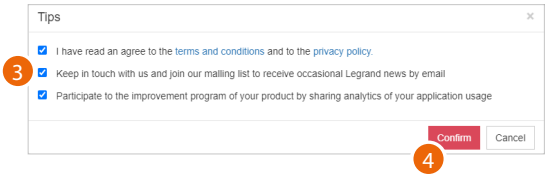
A *Manage your accountt*

B *Create* and *manage your plant*

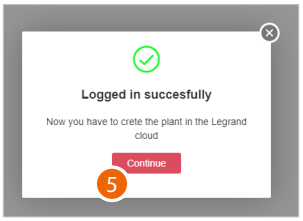
Authentication

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

1. Enter email and password
2. Click to access

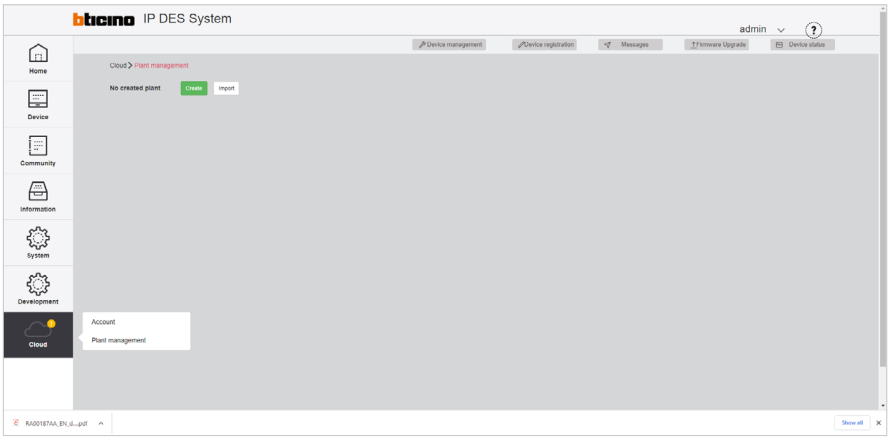


3. Tick the boxes to accept/reject the privacy terms and conditions of use, inclusion in the Legrand e-mail list and sharing of data for the purpose of improving the software.
4. Click to confirm



5. Click to confirm.

Not logged plant not created yet	Sync Progress	Sync KO	Sync OK



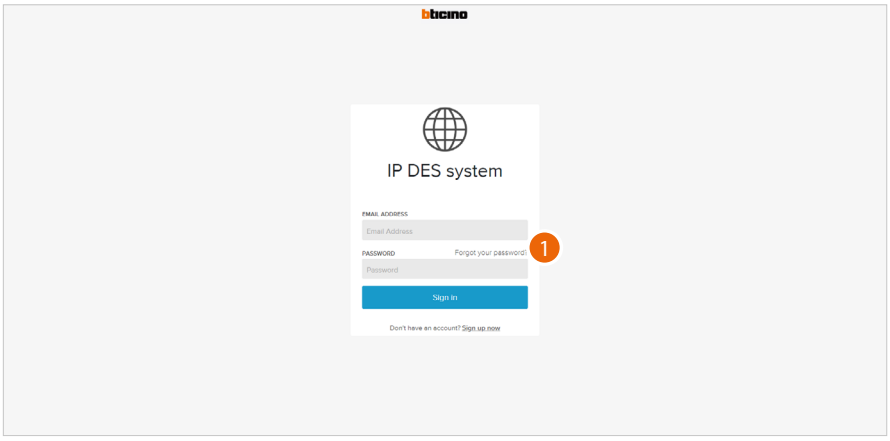
Now it is possible to:

A *Manage your account*

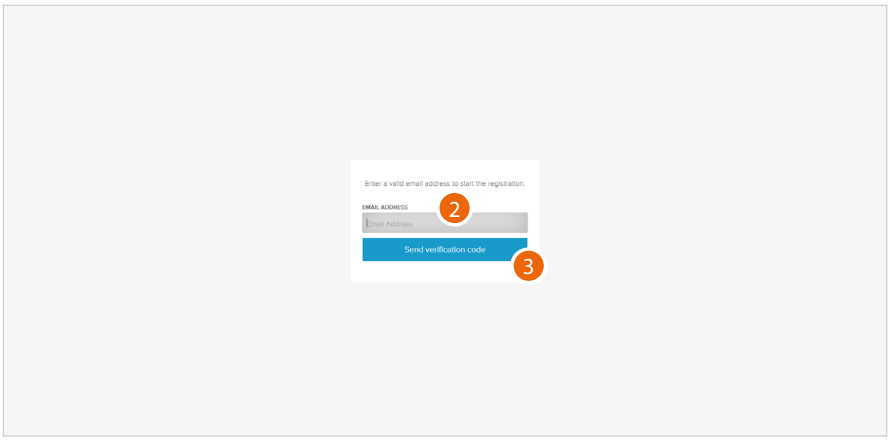
B *Create* and *manage your plant*

Forgotten password

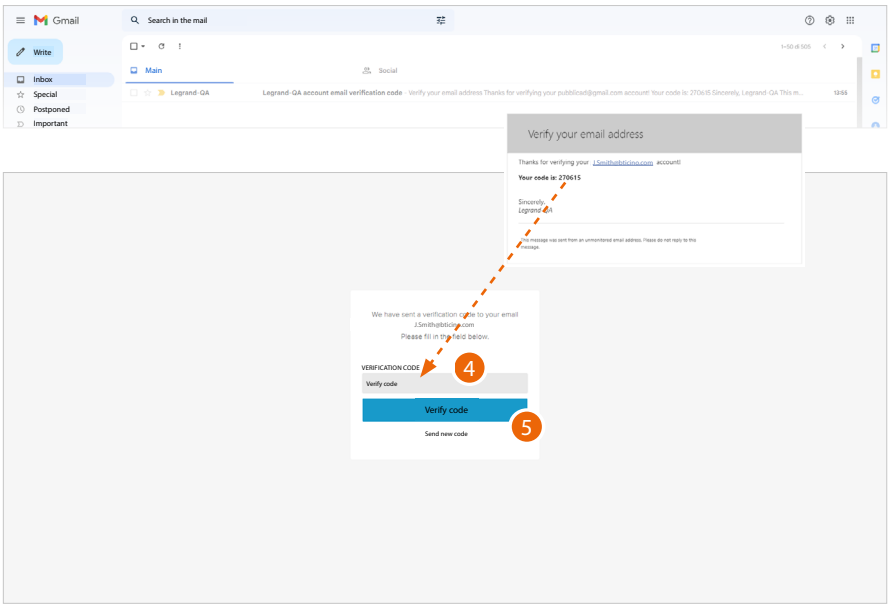
When you have forgotten the password:



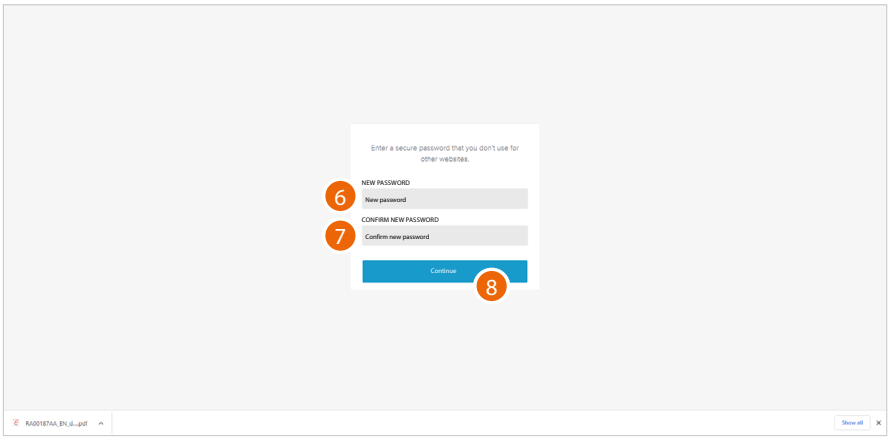
1. Click to activate the password recovery procedure



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



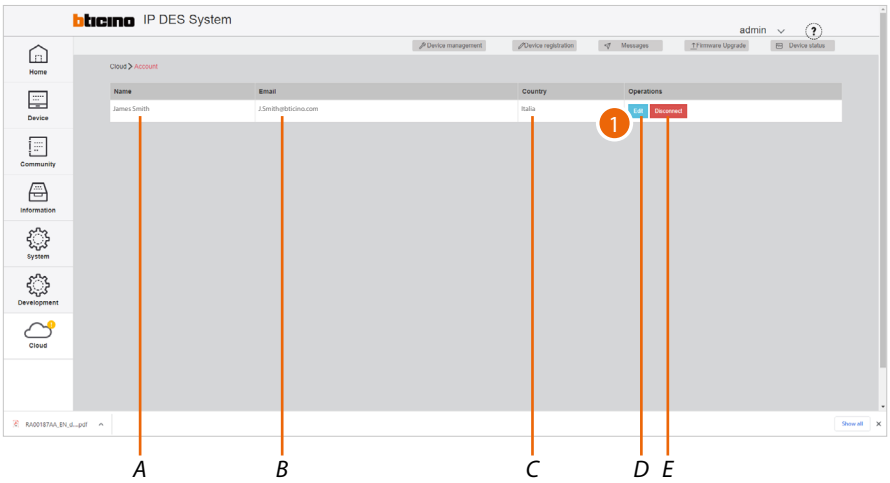
4. Enter the verification code received by e-mail
5. Click to confirm



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

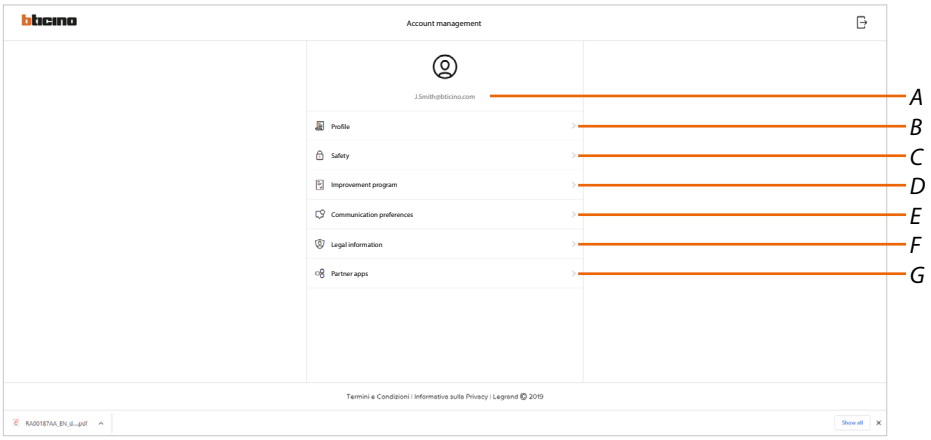
B Current email/account

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/modify 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.

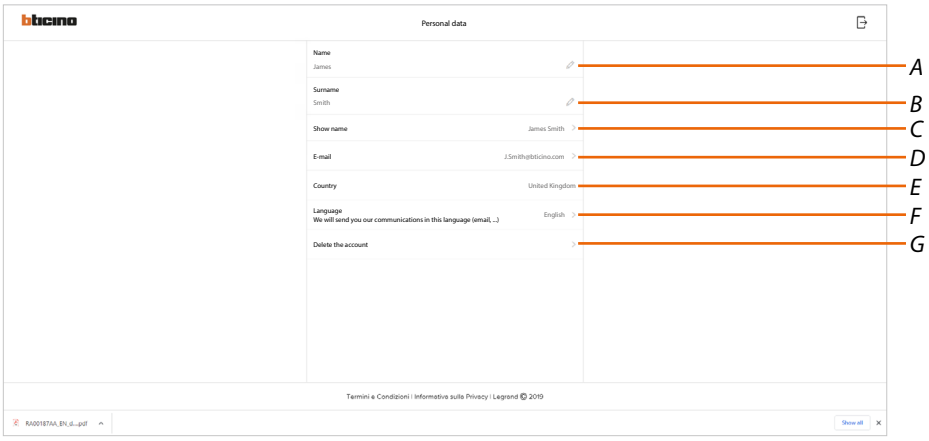
E Manage your communication authorisations and other aspects of your personal details

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.



A *Display/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***

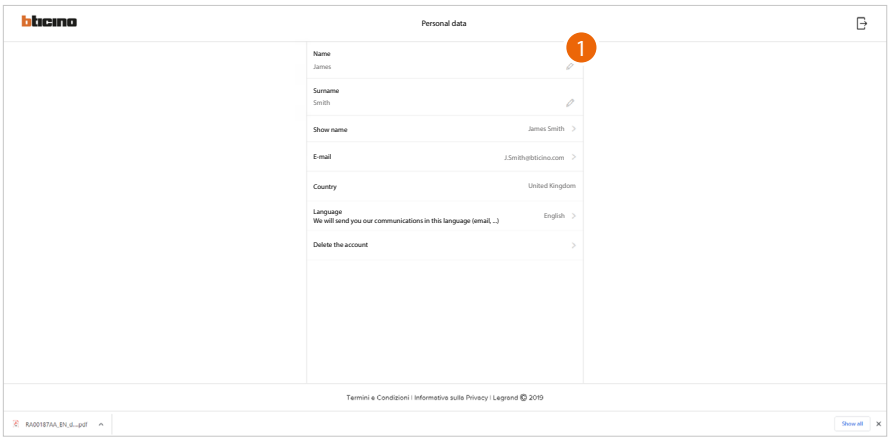
D ***Display/edit the device management email/account***

E *Display the country*

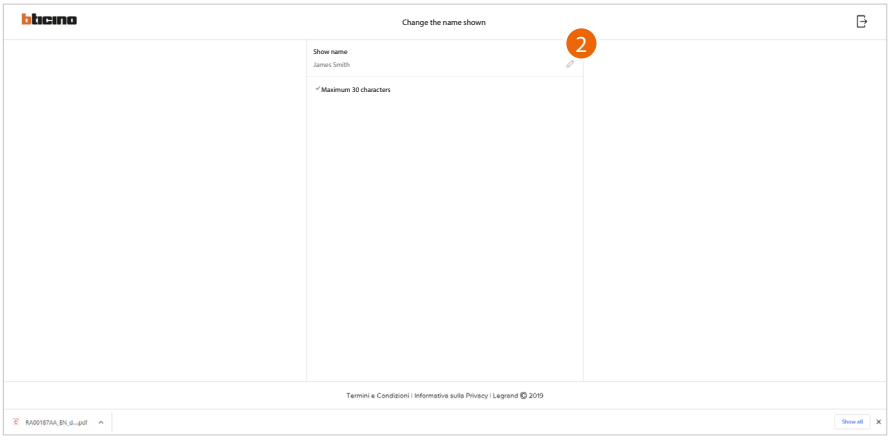
F ***Display/select the language in which to receive communications***

G ***Delete the account***

Show name (edit name)



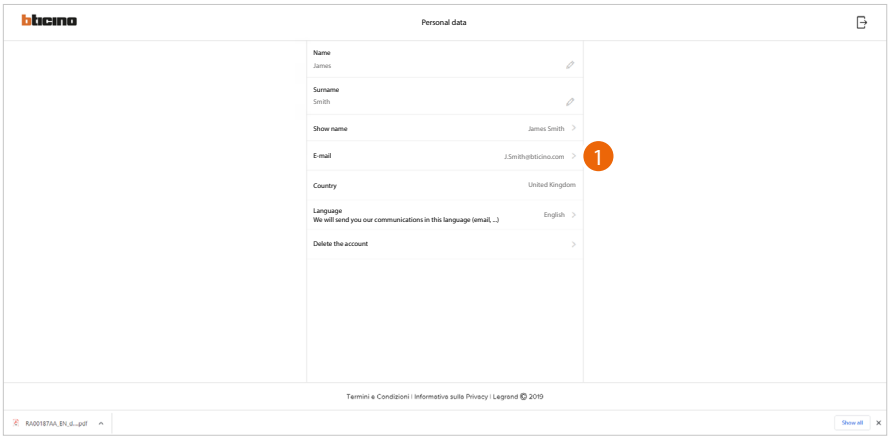
1. Click to edit the name



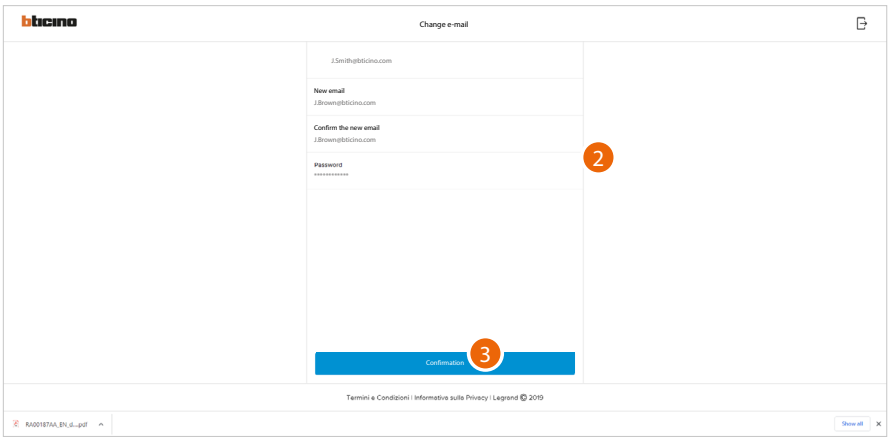
2. Enter the name that will be used in the system e-mail communications.

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

To change the access email address:

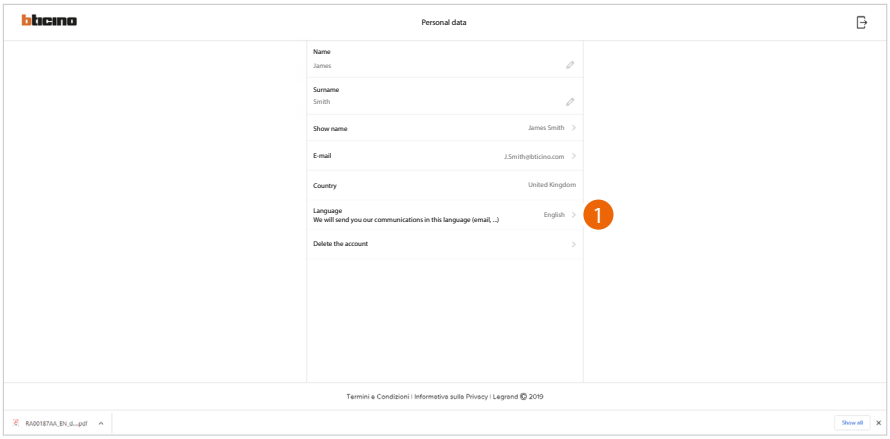


1. Click to edit the email address

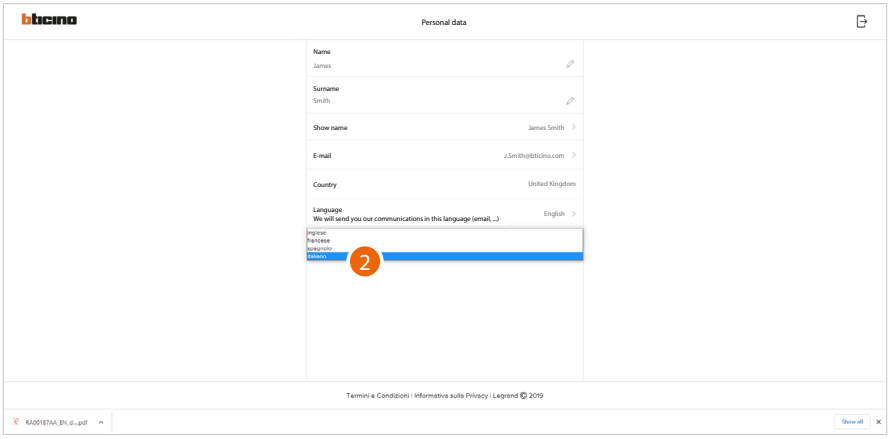


2. Enter the login details (email and password) of the new registered Legrand account to be used to manage the device
3. Click to confirm

Language



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

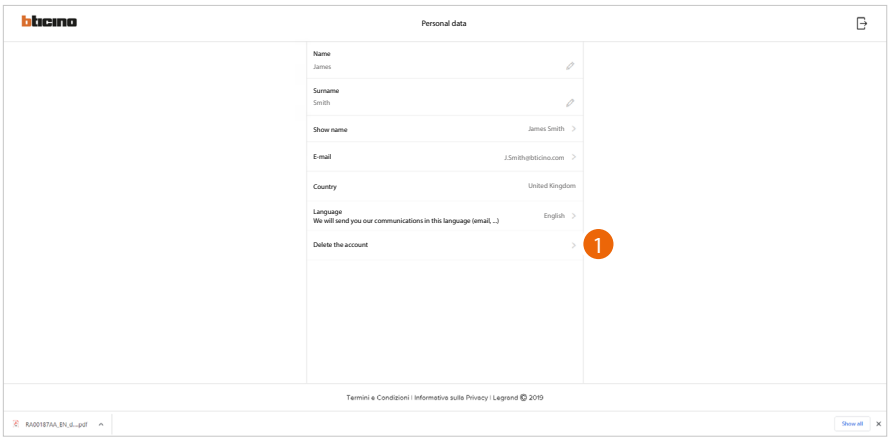


2. Select the language

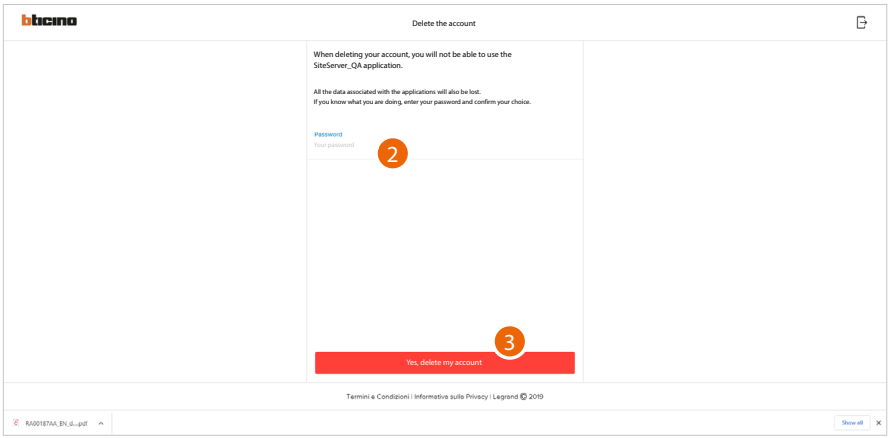
Delete the account

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.

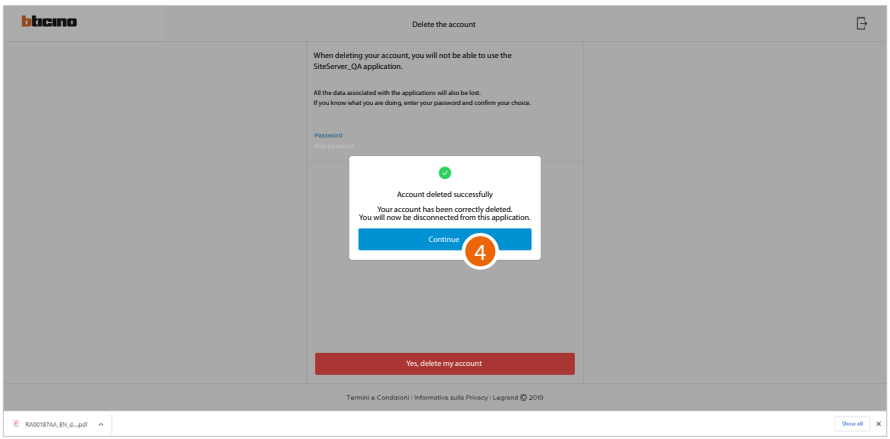
***NOTE**: When deleting the account, all the data associated with the Applications will also be lost*



1. Click to delete your Legrand account definitively



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



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

Safety

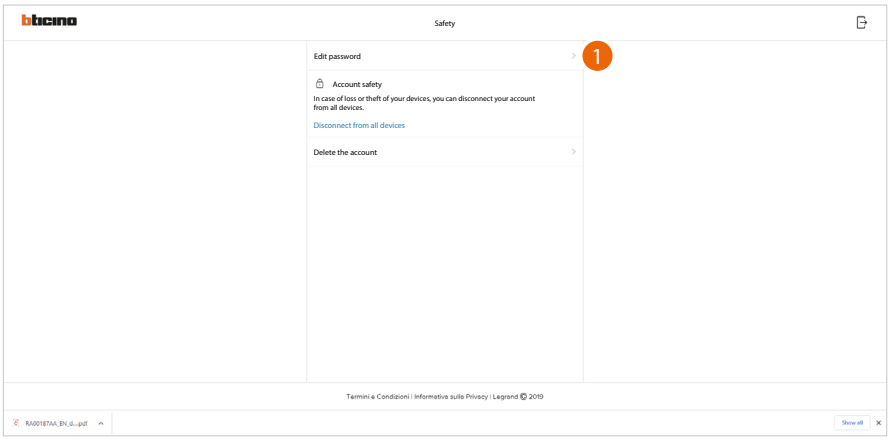
In this page it is possible to edit the password of your account and to disconnect it from all devices. The disconnection of your account from all devices is useful in case one of your devices is lost or stolen.

A Complete the password change procedure

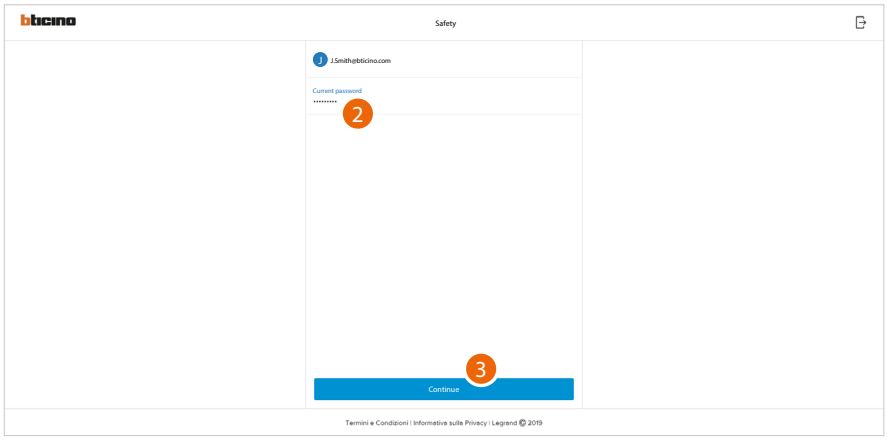
B Disconnect from all devices

C Delete the account

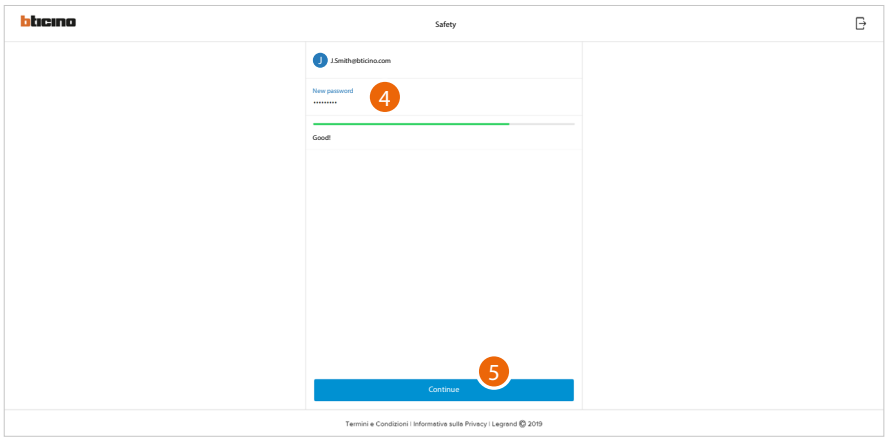
Edit password



1. Click to modify the password

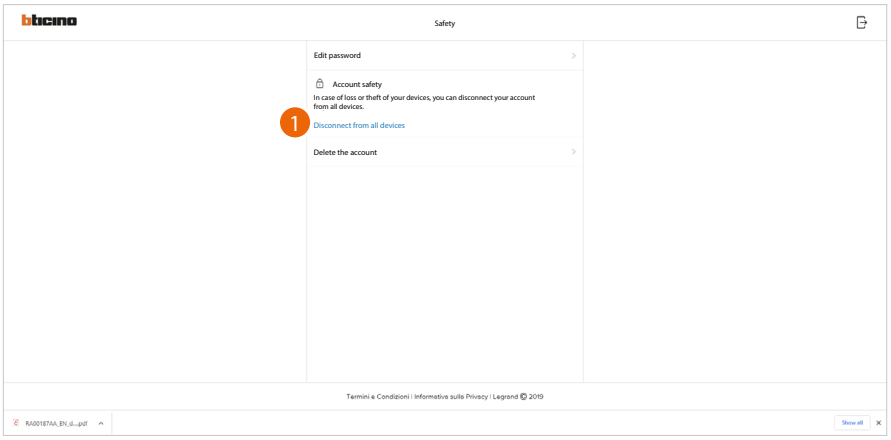


2. Enter the current password
3. Click to continue

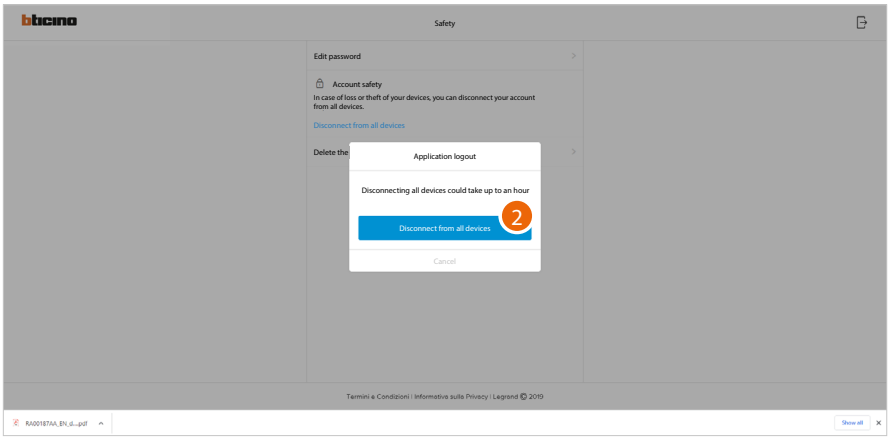


4. Enter the new password, which must meet the following requirements:
   – at least 8 characters;
   – at least one lower case letter (e.g. a);
   – at least one upper case letter (e.g. A);
   – at least one number (e.g. 1);
   – at least one special character (e.g. $);
5. Click to confirm

Disconnect from all devices



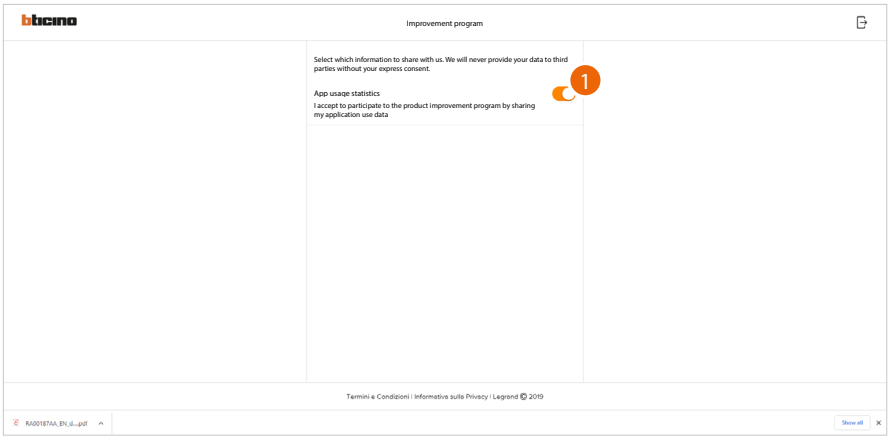
1. Click to activate the procedure



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

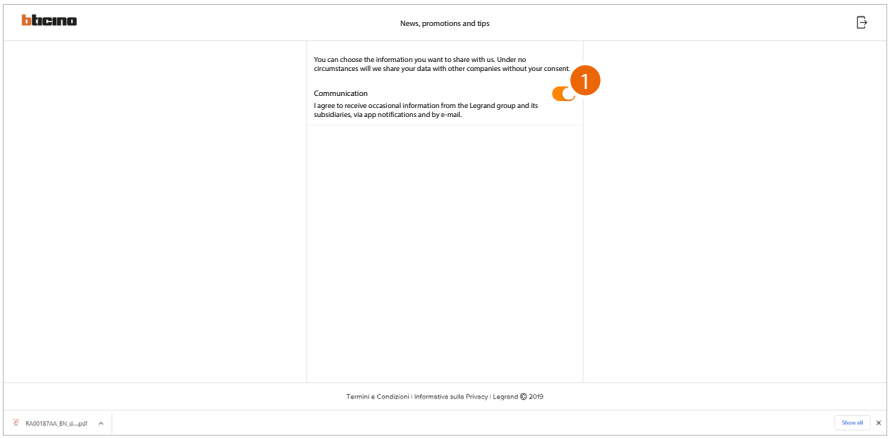
This section can be used to enable the sharing of the app usage data.



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

Communication preferences

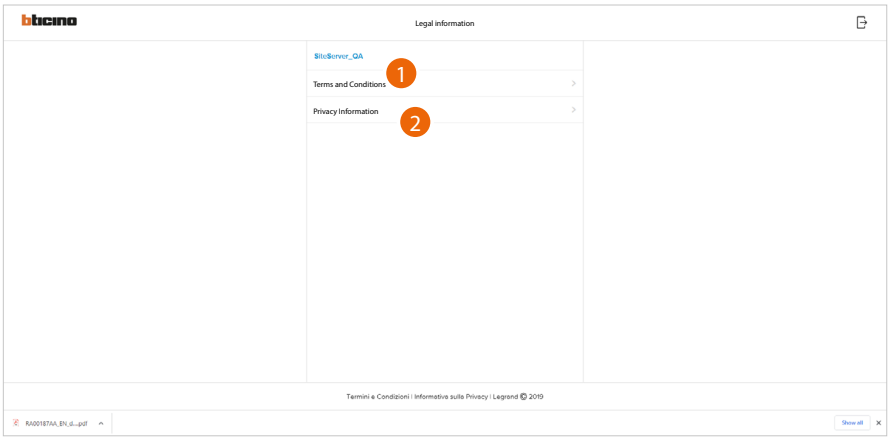
This section can be used to enable the reception of communications from Legrand



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

Legal information

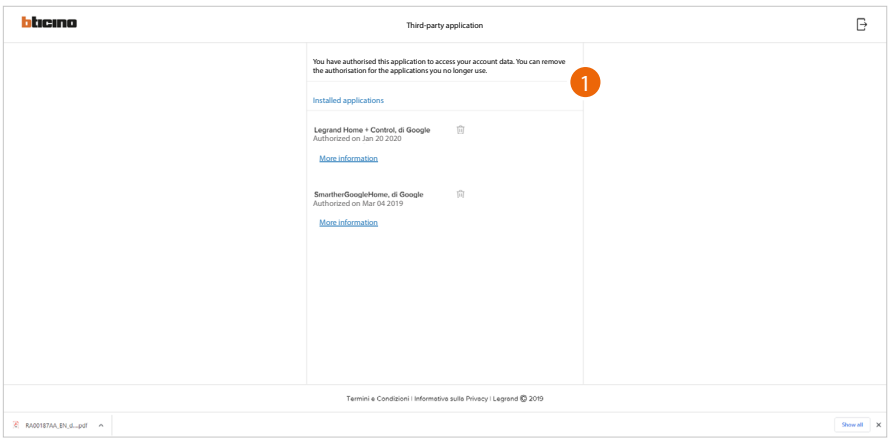
Using this section you will be able to view terms and conditions of use and privacy information for each App to which your Legrand account is associated



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.

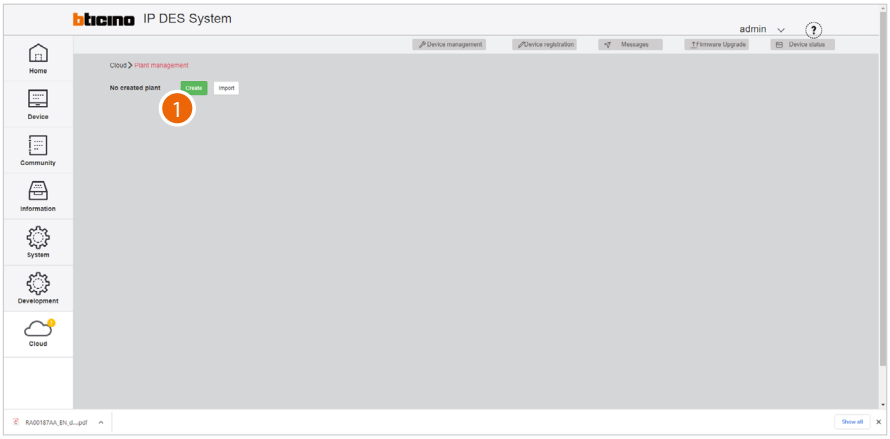


1. Click to remove the authorisation to access your details for this application.

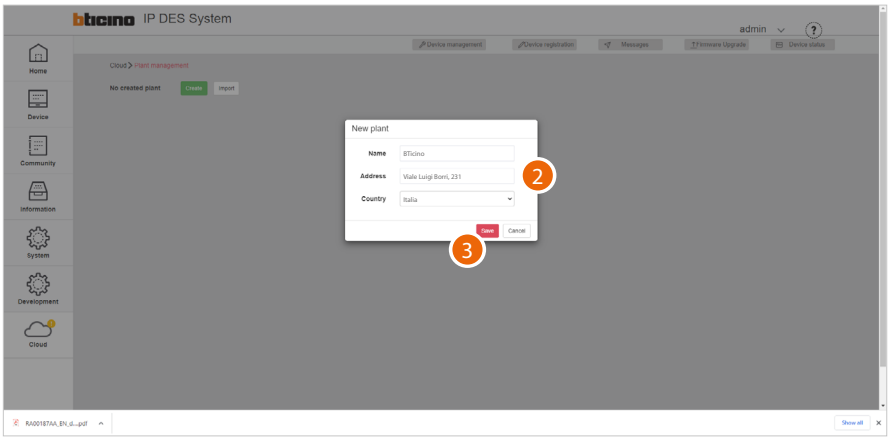
A Display more information regarding the access to your home by partner Apps.

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.

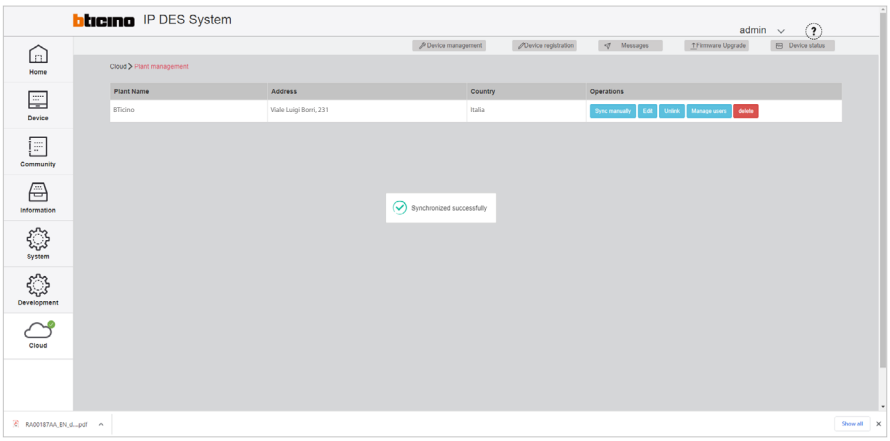


1. Click to create a new Plant



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

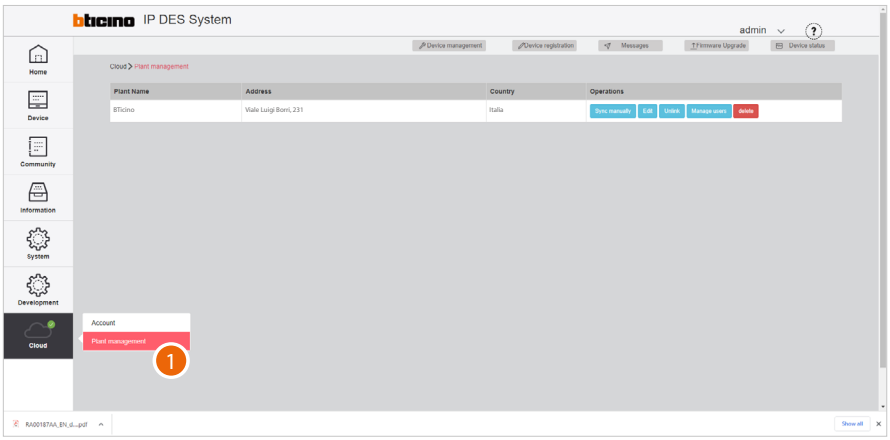
The plant is automatically synchronised



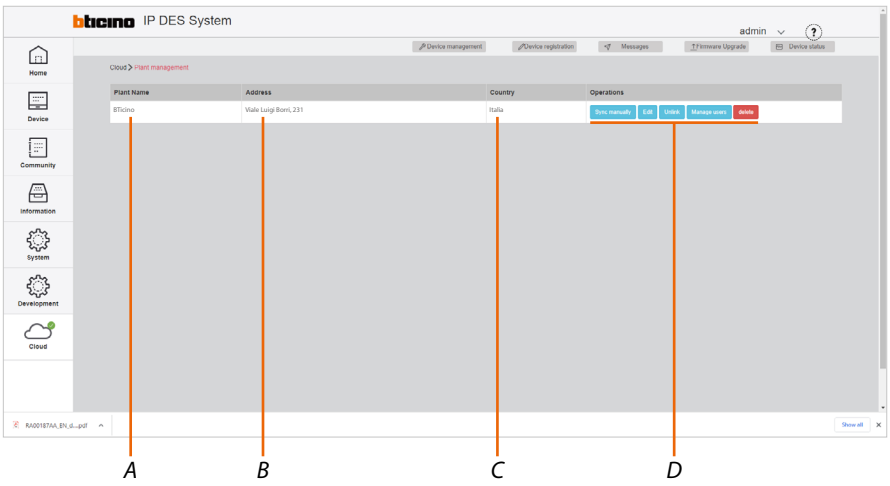
Once created, the plant remains available on the cloud.
If disconnected (unlink button), it can be retrieved from the cloud using the Import a Plant function.
If deleted, it will also be deleted from the cloud.

Manage the Plant

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

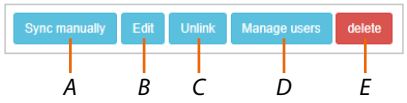


1. After completing the authentication and creating your Plant, a key will become active, which when clicked will take to the Plant management page



A Plant Name
B Plant Address
C Plant Country
D Plant management bar

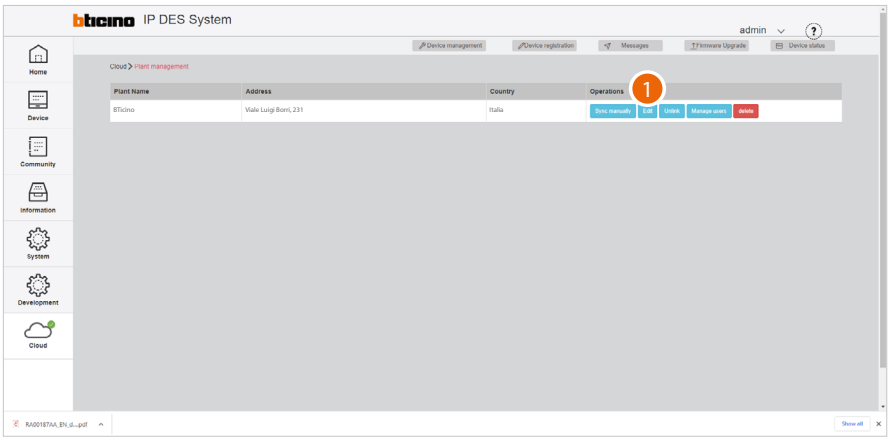
Plant management bar



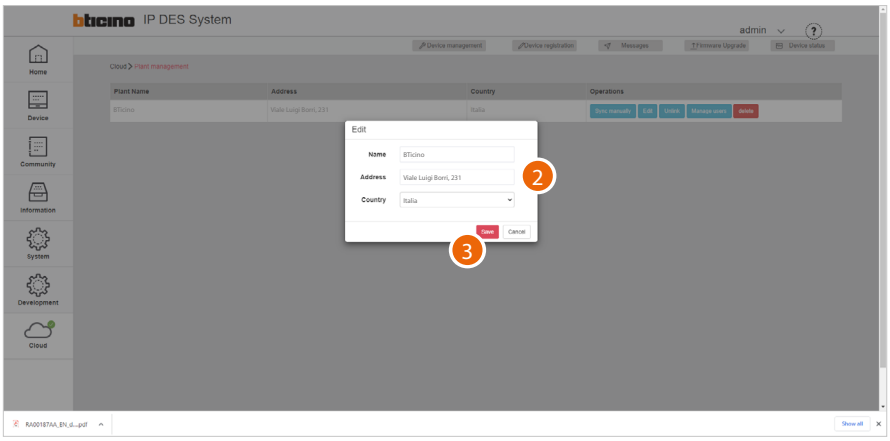
A Synchronises the local plant with the plant stored on the cloud.
***CAUTION**: This operation is necessary every time changes are made to the plant.*
B Edit the plant
C Disconnect
D Manage the users
E Delete the plant

Edit the Plant

This function allows to edit a Plant



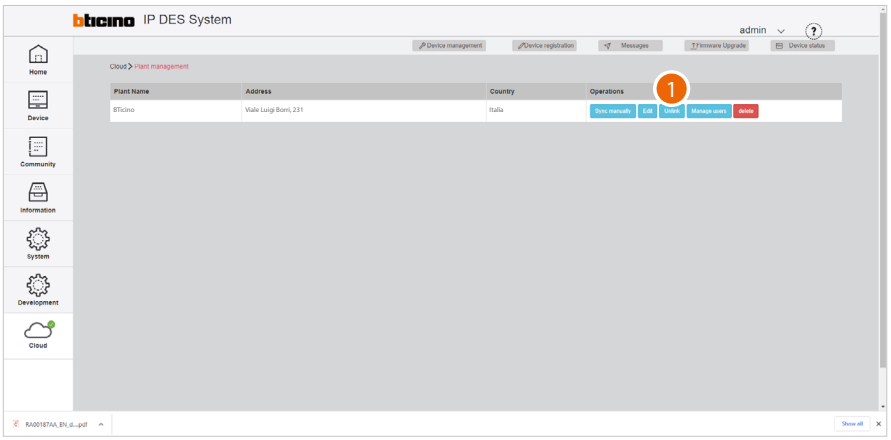
1. Click to edit the plant



2. Edit Plant data (name, plant and country)
3. Click to save

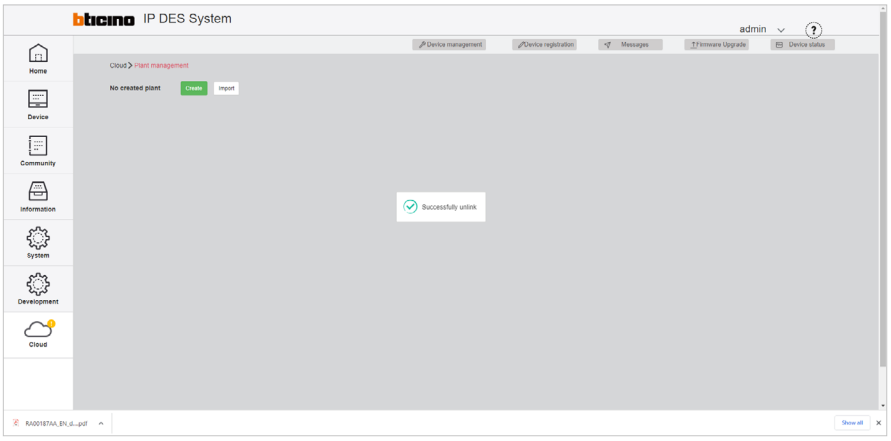
Disconnect the Plant

This function allows to disconnect a Plant from the cloud



1. Click to disconnect the plant from the cloud

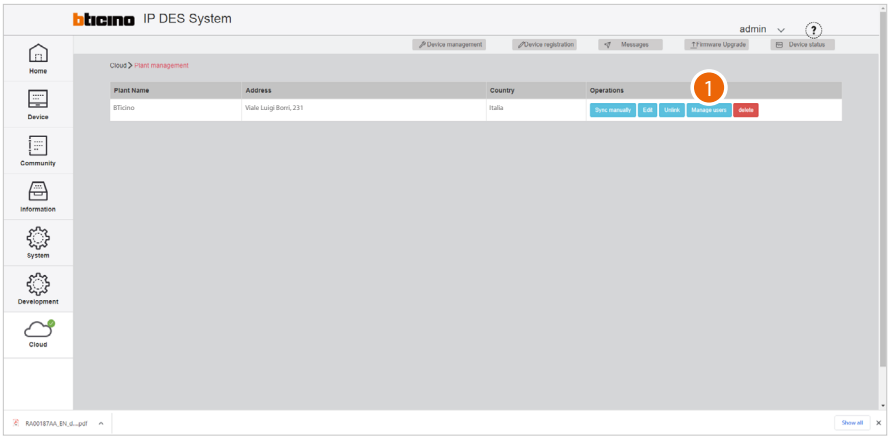
Now the plant is disconnected from the cloud, it is possible to create a new one or select and import one saved on the cloud



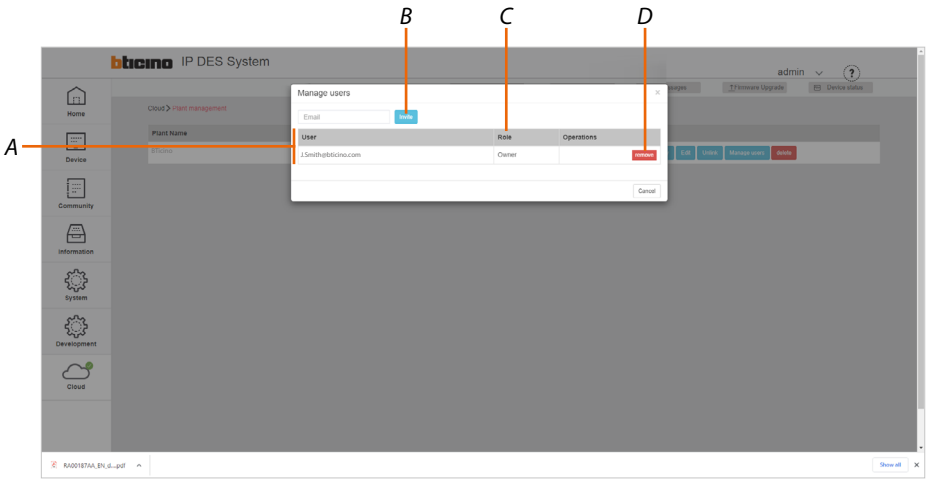
Manage the users

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



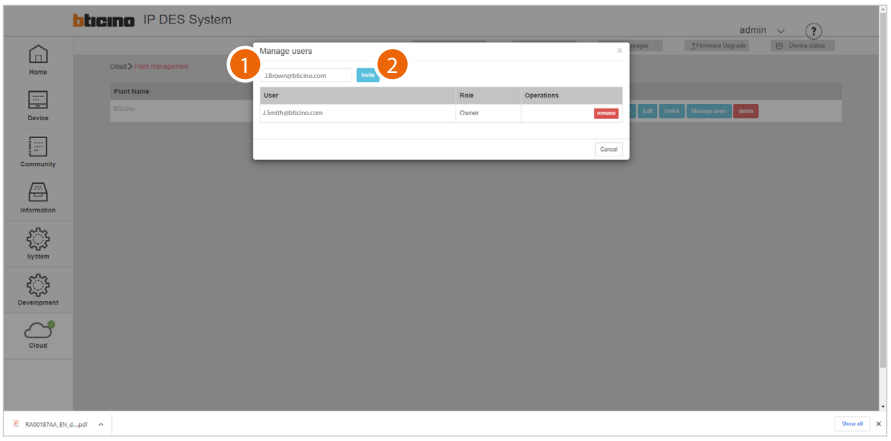
A *List of users*

B *Invite a user*

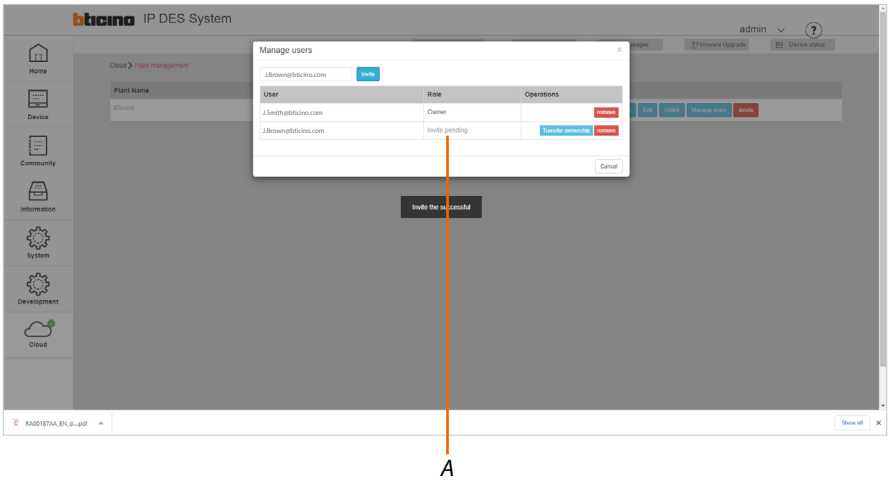
C *User role*

D *Delete a user*

Invite a user

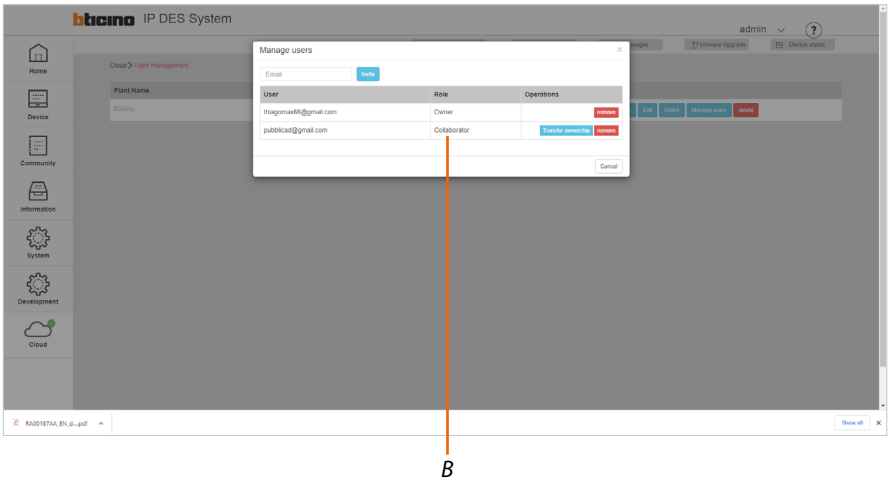


1. Insert email address of the person you want to invite
2. Click to confirm the invitation



The invitation was sent.
The invited user will receive an e-mail with the invitation to check the plant.

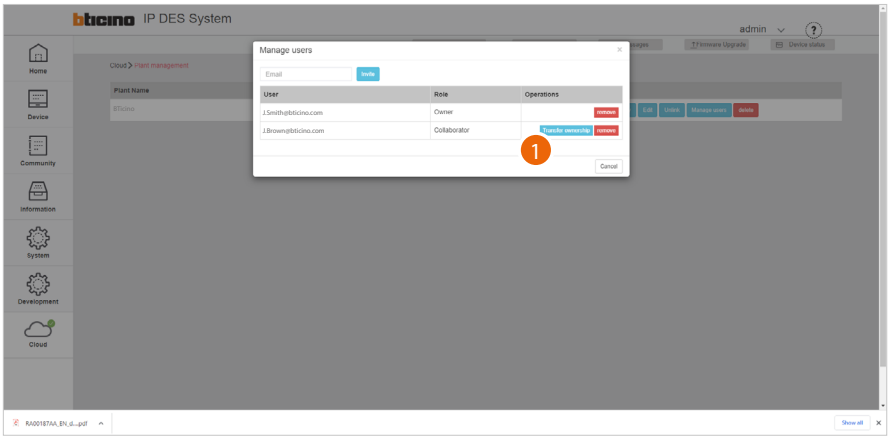
The invited user must complete the server authentication procedure using their own profile and must be registered in the installer cloud.
Until the invited user has completed the authentication procedure, they will appear in the list as "invited, waiting" (*A*).



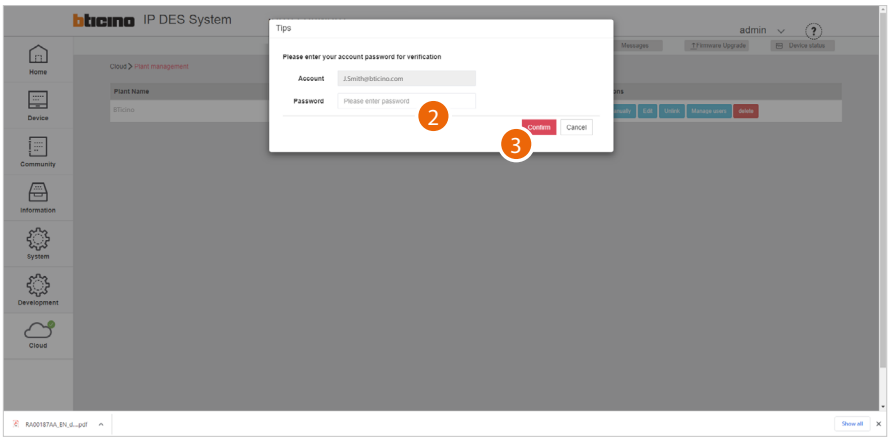
After authentication, the user will be associated to the plant and will appear in the list as "collaborator" (*B*).

Change the user role

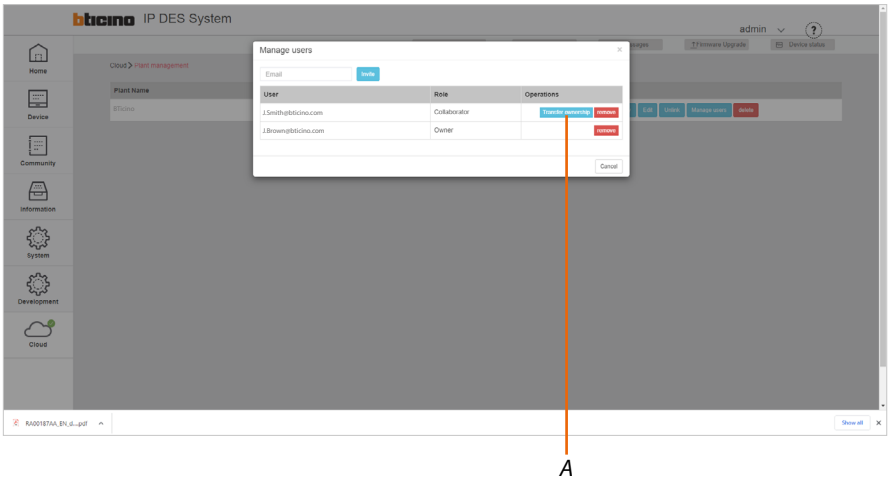
This function can be used to change the role of users from “Collaborator” to “Owner”



1. Click to change the role to “Owner”



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



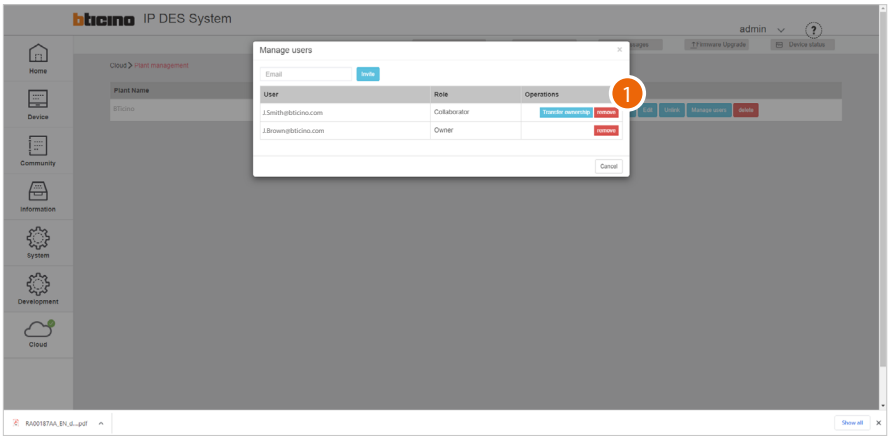
A The role of the user has been changed from “Collaborator” to “Owner”

Delete a user

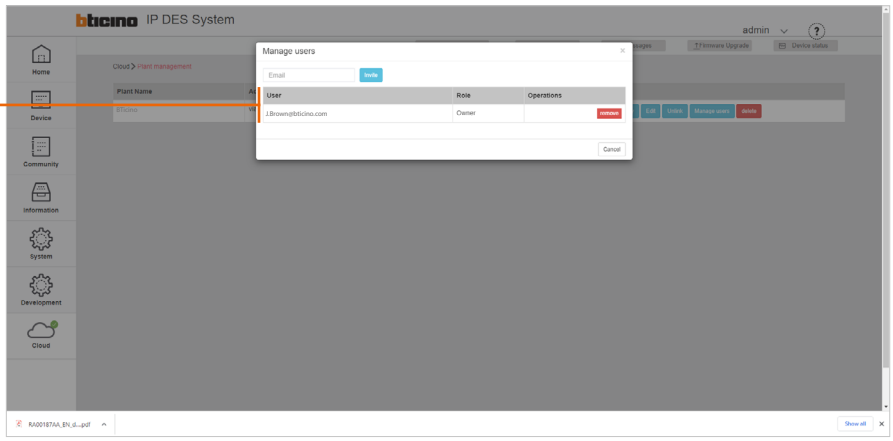
This function can be used to remove a user from plant management

NOTE: *"Owner" users cannot be removed. It will be necessary to first change their role. See* ***Change User Role***

NOTW: *The role of the user has been changed from "Collaborator" to "Owner"*



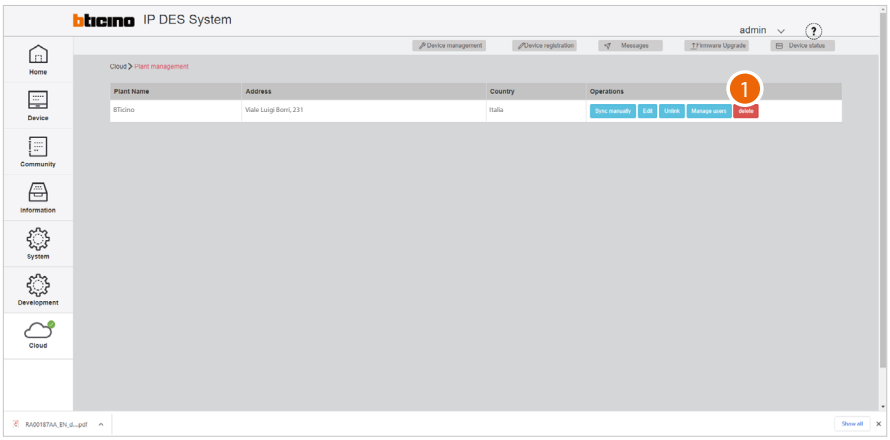
1. Click to remove a user from plant management



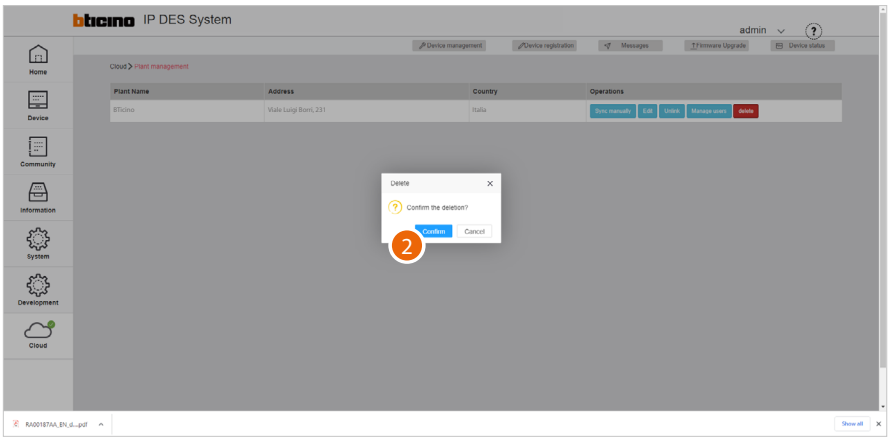
A The user has been correctly removed

Delete a Plant

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

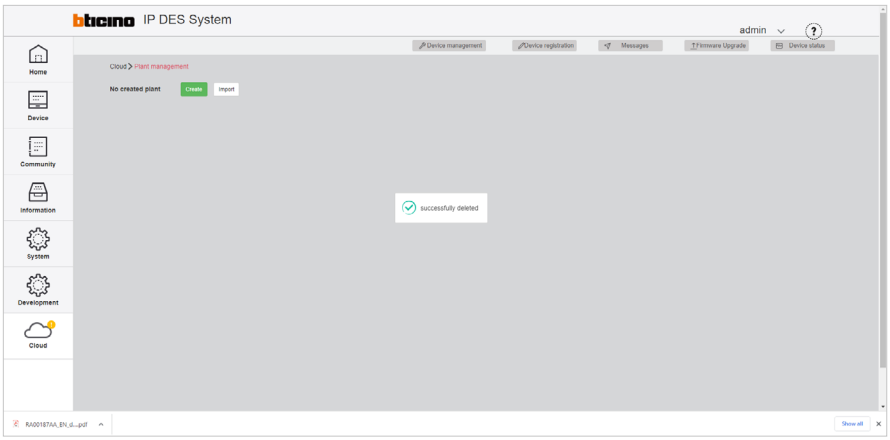


1. Click to delete the plant



2. Click to confirm

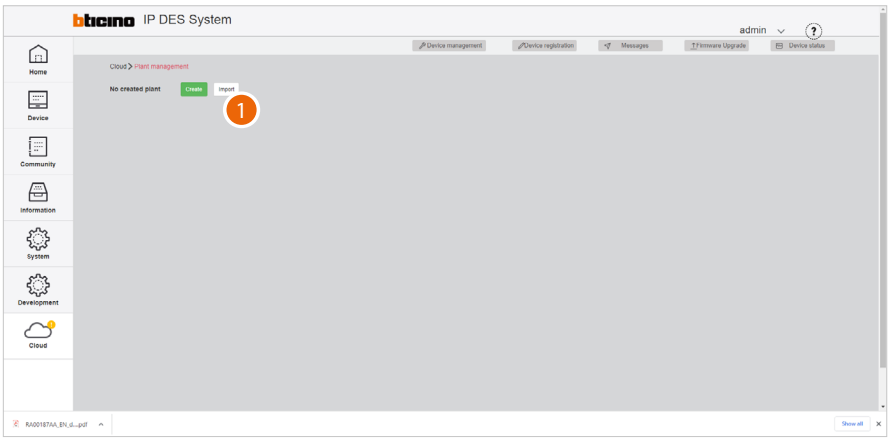
***CAUTION**: All the data will be lost*



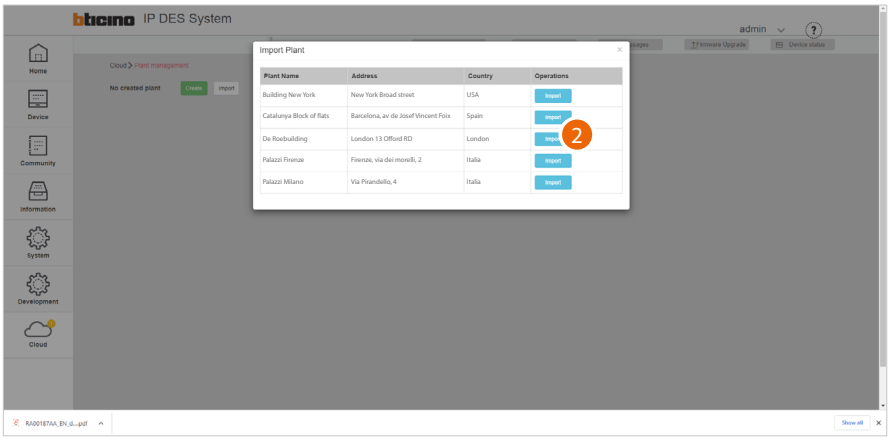
The plant was deleted from the cloud. Therefore, it is now necessary to create a new one or import another plant among those saved on the cloud.

Import a Plant

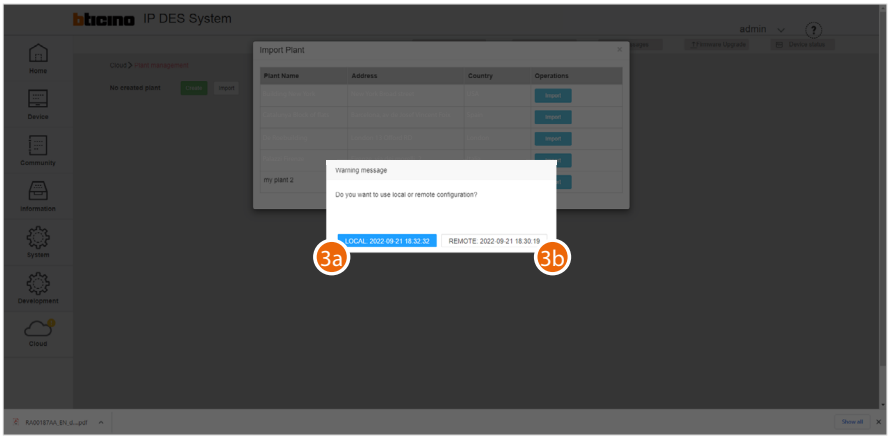
This page can be used to import a previously saved plant from the cloud



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



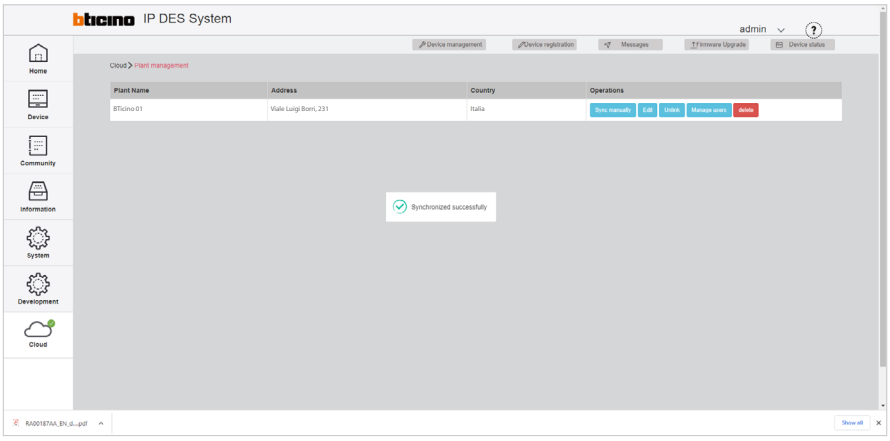
2. Click to import the plant



3a. Click to import the plant version stored on the DES Server 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



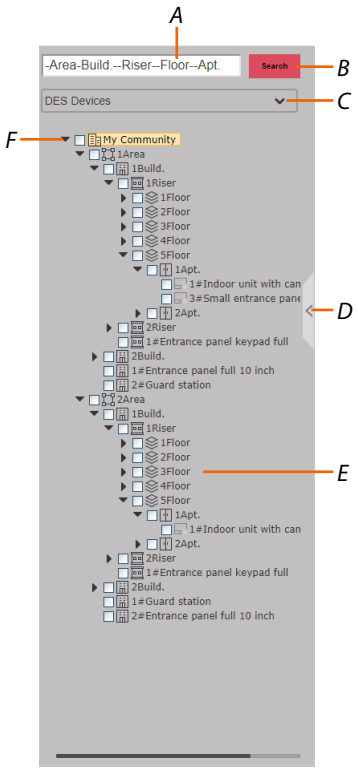
The Plant has been imported

Tree menu

The tree menu may be used for various functions, in particular:

– Create and modify the Community structure
– Populate the Community with devices and modify their parameters
– Select individual levels/devices, to view and update their parameters

The tree menu is dynamic; in some pages it opens automatically, while in others it is not available.



A When partial data are entered, the complete address is suggested

B Start the search

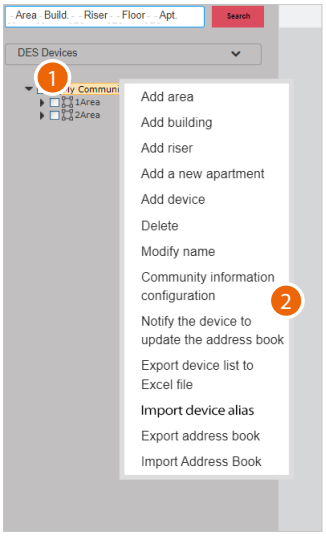
C Level type filter

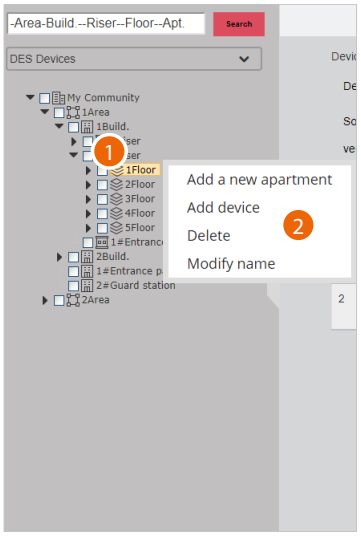
D Open/close the menu

E Community structure

F Open/close the tree menu to display sub-levels

Context sub-menu for the creation of levels/devices (device/device management)





1. Right click the level to show the context menu.
   The sub-menu will show the available functions based on the type of level.

The illustrated procedure shows the creation of a structure from scratch, starting from the Community level.

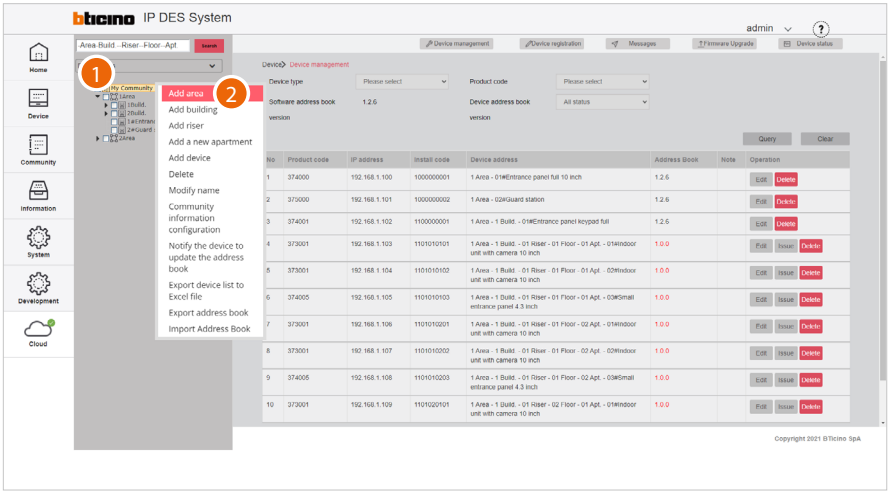
2. Click the desired command

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 apartmentt	Add an Apartment level to the community	Community, Area, Building, floor
Add device	Add a device to the community	all
Delete	Delete a level or device	all
Modify name	Modify the name of a level or device	all
Community information configuration	Define the community by setting different parameters	Community
Notify the device to update the AB	Sends the structure created and the parameters set on the levels/devices, to update the AB of the devices connected to the system	Community
Export device list to Excel® file	Export the device list to an Excel® file	Community
*Import device alias	Import a list of devices in Excel® format	Community
Export AB	Export the AB to save the structure	Community
Import AB	Import an AB previously saved	Community

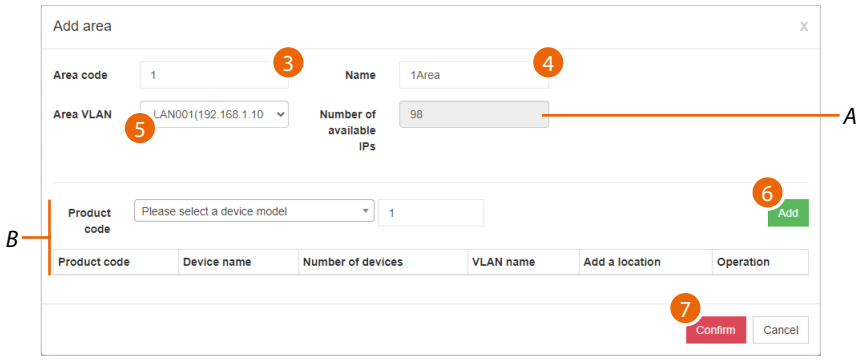
***Note**: set the call type as address book in the calling mode/0-9, A-Z, Address book page to display this item*

Add Area

This function can be used to add levels and devices to the community.
While adding a level, it is also possible to add the level devices. For example, when adding a Area (level), it is possible to also add the EP associated with that Area.



1. Right click the level to which you want to add an Area
2. Click to add the Area



A *Maximum number of addresses available (see Community Network Settings)*

B *Fields for adding the device*

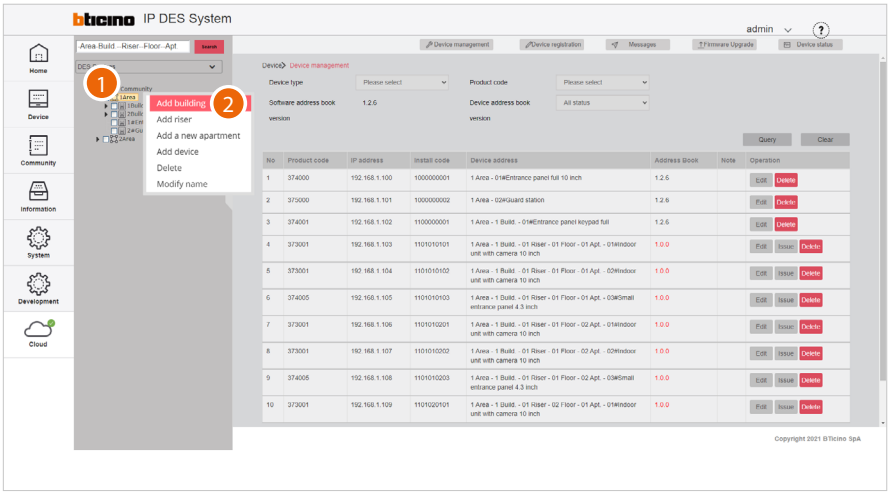
3. Select the progressive identification number

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

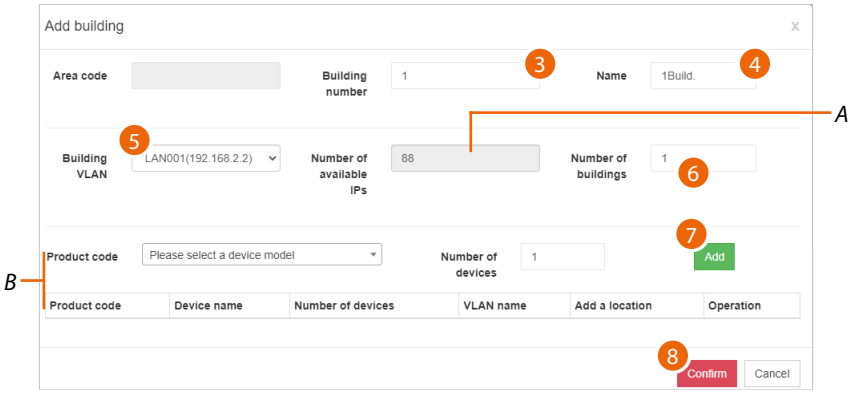
4. Enter a name for the Area
5. Select the VLAN network from those created in the Community Network Settings page
6. It is now possible to add devices to the area; see Add device
7. Click to confirm

Add 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 (level), it is possible to also add the EP associated with that Building



1. Right click the level to which you want to add a Building
2. Click to add the Building



A *Maximum number of addresses available (see Community Network Settings)*

B *Area for adding a building device*

3. Select the progressive identification number

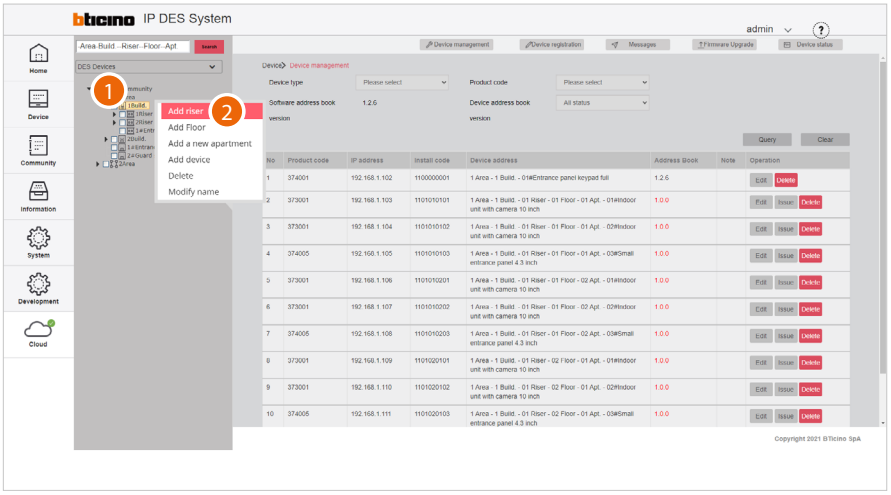
***Please note**: changing this parameter also changes the address in the community (see automatic addressing)*

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 devices to the building; see Add device
8. Click to confirm

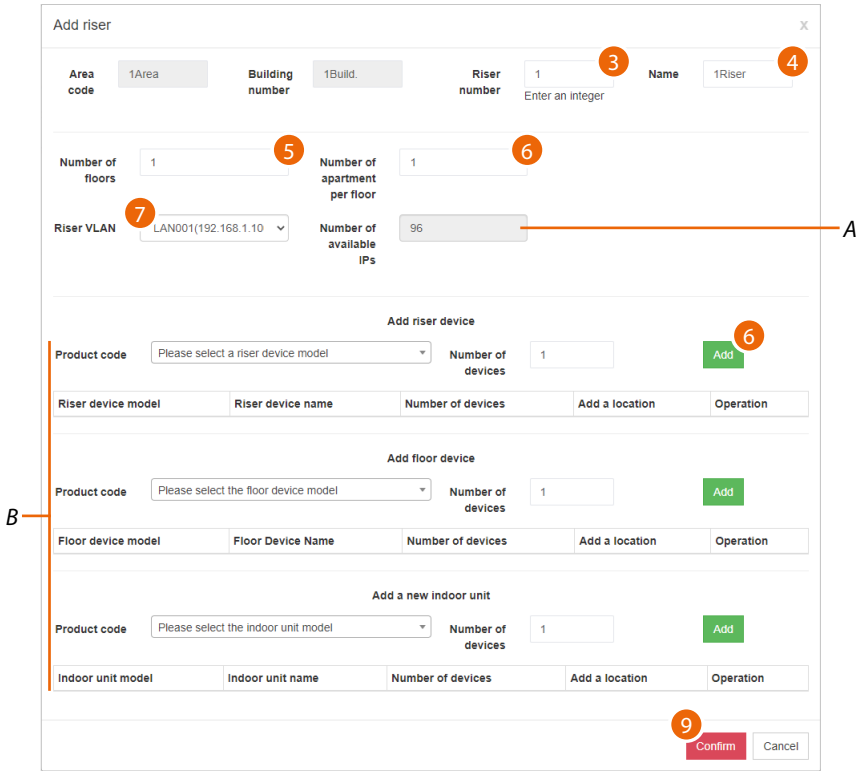
Add Riser

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 (level), 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 Floors and the number of Apartments for each Floor.



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



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

B Area for entering devices

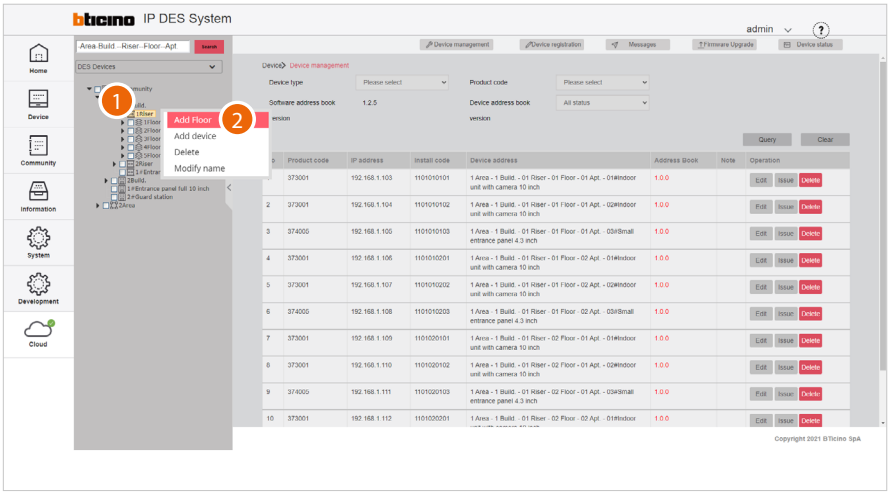
3. Select the progressive identification number

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

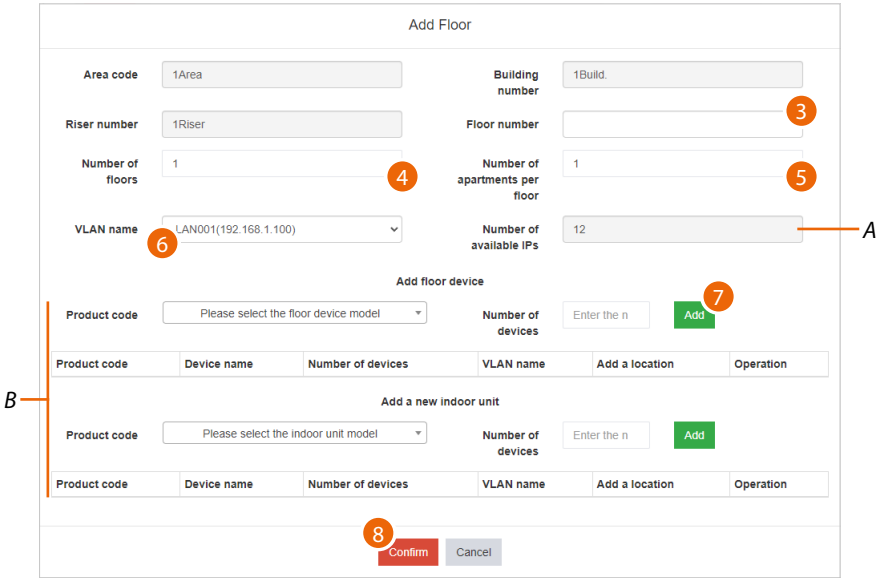
4. Enter a name for the Riser
5. Enter the number of Floors that make up the Riser
6. Enter the number of Apartment for each Floor
7. Select the VLAN network from those created in the Community Network Settings page
8. It is now possible to add Riser, Floor and Apartment devices; see Add device
9. Click to confirm

Add 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 (level), it is possible to also add the EP associated with that Floor.



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



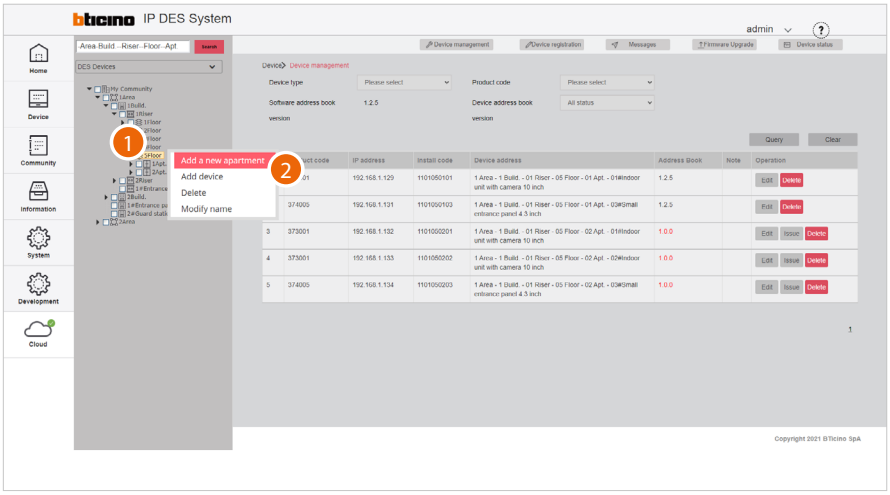
A Maximum number of addresses available (see Community Network Settings)

B Area for entering devices

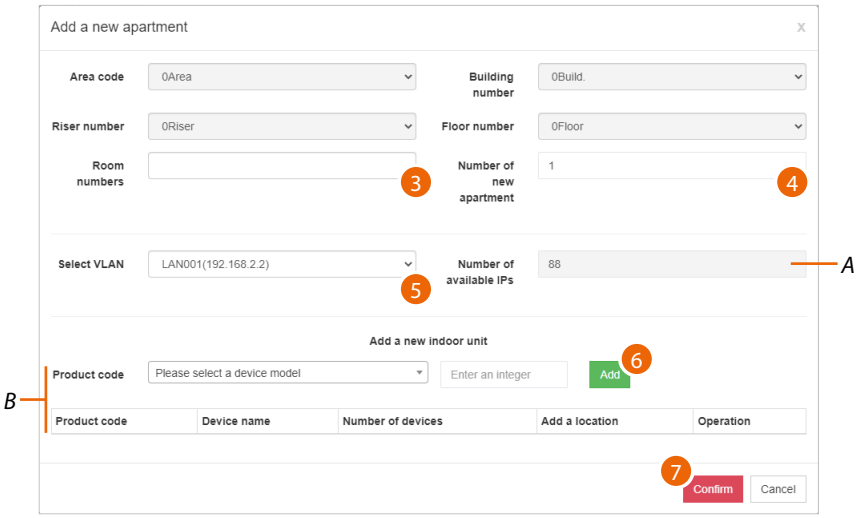
3. Enter a name for the Floor
4. Enter the number of the Floor
5. Enter the number of Apartment for each Floor
6. Select the VLAN network from those created in the Community Network Settings page
7. It is now possible to add Riser, Floor and Apartment devices; see Add device
8. Click to confirm

Add 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 (level), it is possible to also add the SEP associated with that Apartment.



1. Right 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 *Fields for adding the device*

3. Enter the apartment number
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 to the Appartment

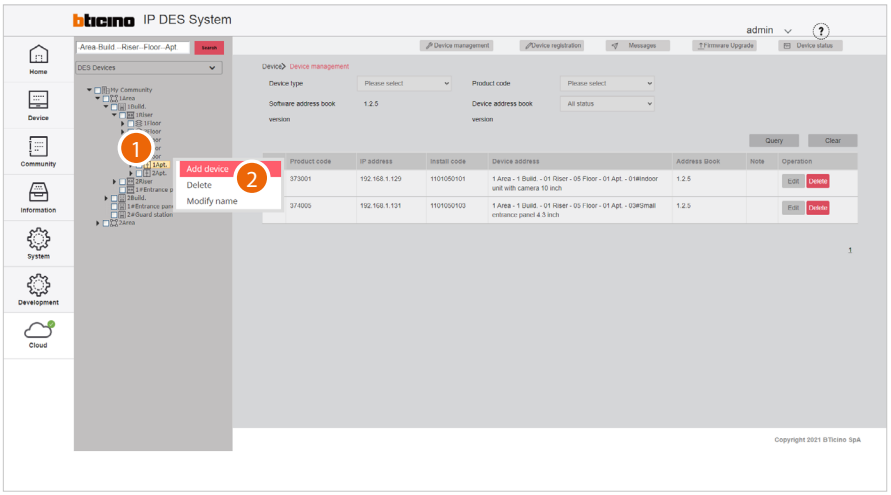
Or

7. Click to confirm and enter devices later; see Add device

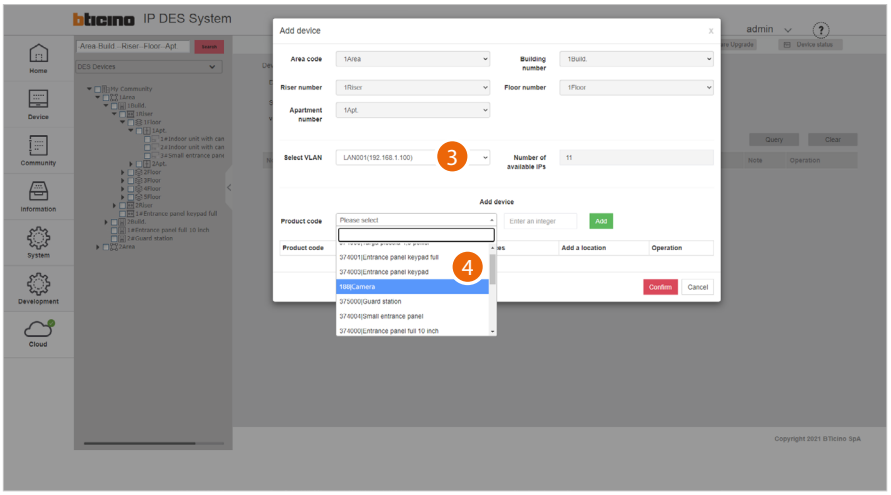
Add Device

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 template configuration)*



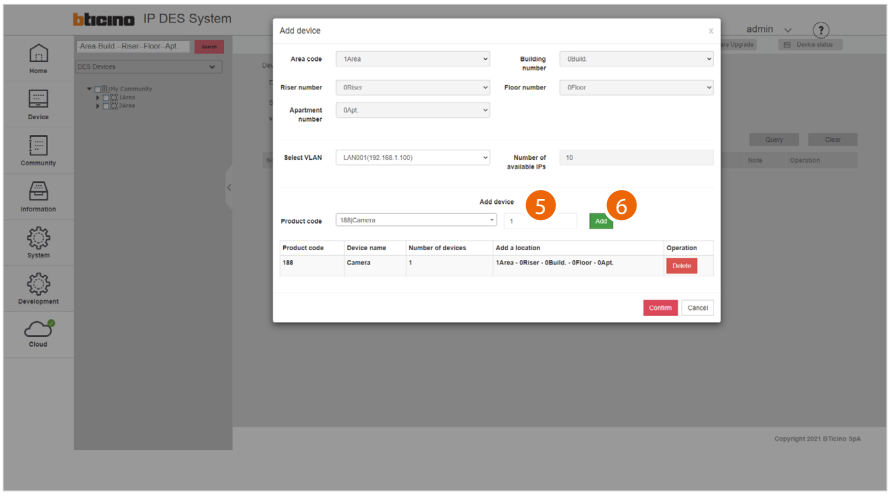
1. Right click the level to which you want to add a device
2. Click to add one or more devices



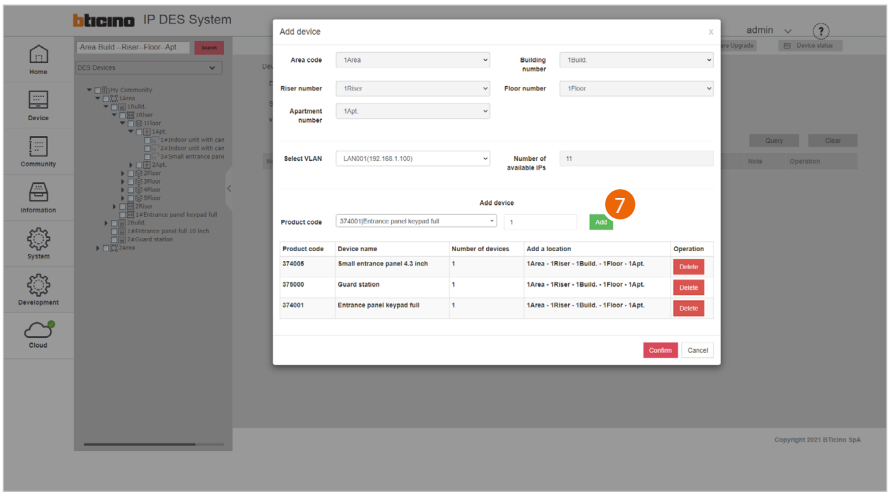
3. Select the WLAN network from those created in the Community Network Settings page
4. Select the device among those suggested, or enter the product code, if known

The available devices are:

EP	374000	EP full 10 inch
	374001	EP keypad full
	374002	Entrancepanel 10 inch
	374003	EP keypad
SEP	374004	Indoor SEP
	374005	SEP 4.3 inch
	374006	outdoor SEP
IU	373001	IU with camera 10 inch
	373002	IU with camera 7 inch
	373003	IU10 inch
	373004	IU 7 inch
	373005	Standard indoor unit
GS	375000	GS
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"*

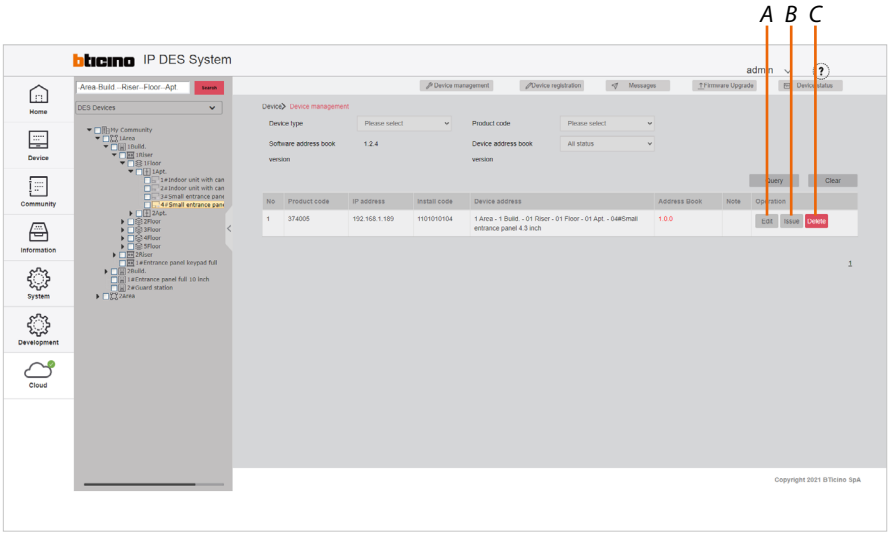


5. Enter the number of devices
6. Click to add



Several devices may be added at the same time

7. Click to confirm



The device is now available. Therefore, using the specific buttons it is now possible to:

A Change some device parameters

B Send any changes to the physical device (AB update)

C Delete the device

For these functions, see Device management

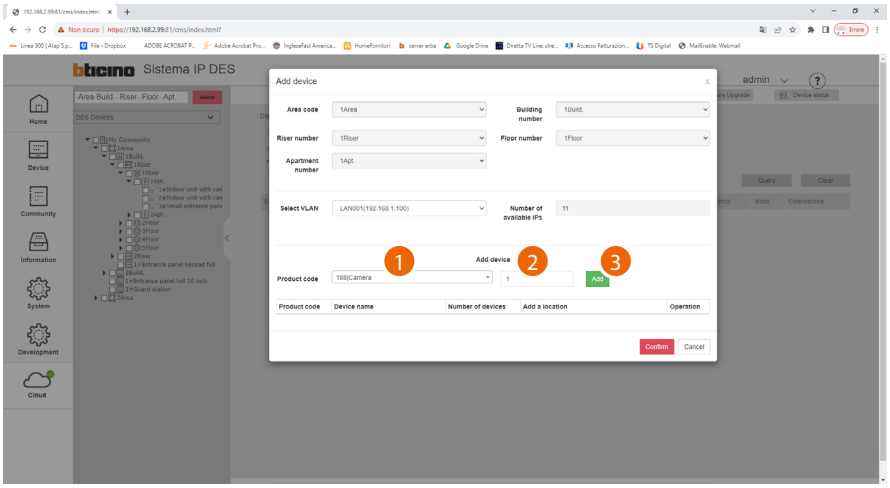
Add a OnVif IP camera

Adds a camera within the selected level in the community

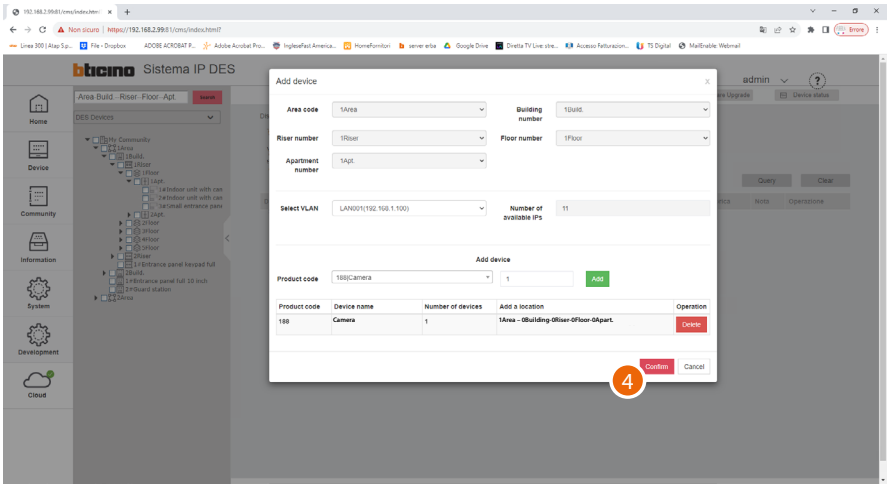
Before completing the final installation, a function test is recommended in order to be sure of compliance.
The BTicino IP video door entry system complies with the ONVIF protocol, check on the website https://www.onvif.org/conformant-products that the IP camera you want to use is also compliant.
***NOTE**: 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:

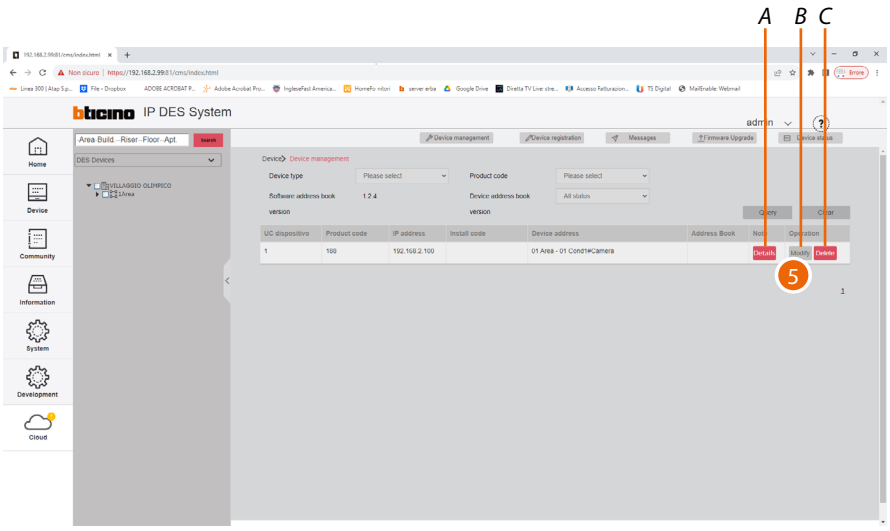
– Resolution: max 720p
– Coding: H264



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



4. Click to confirm

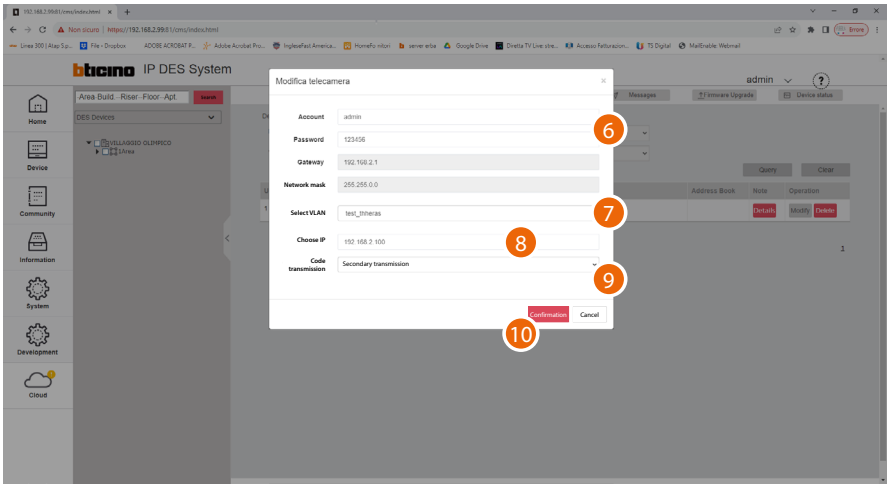


A *Display the camera details*

B *Modify the camera settings*

C *Delete the camera*

5. Select to modify the camera

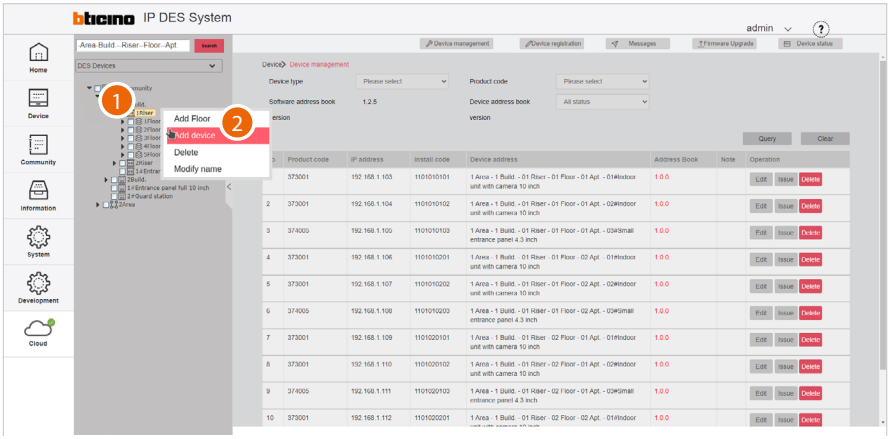


6. Enter the account (*) and password of the camera.
   For security reasons, it is recommended to change the camera password
   **NOTE: the reference account is the one from which the video stream can be taken*
7. Select the network on which the camera is installed (must be the same as the IP video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

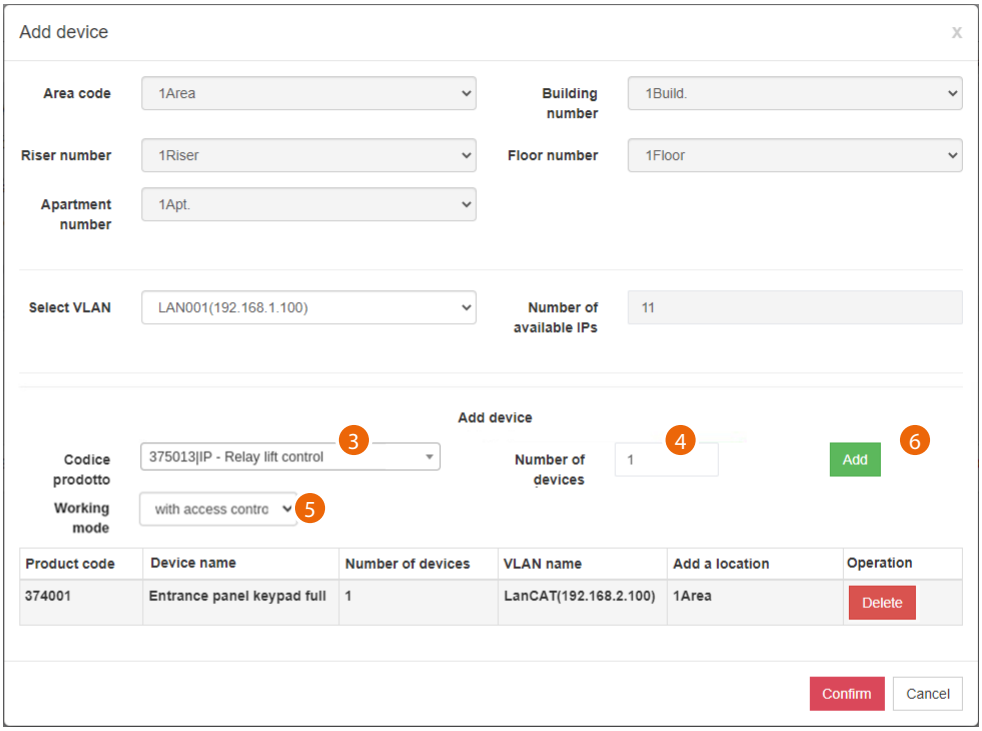
Add a lift control interface with relay 375013

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 staircase or apartment block 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

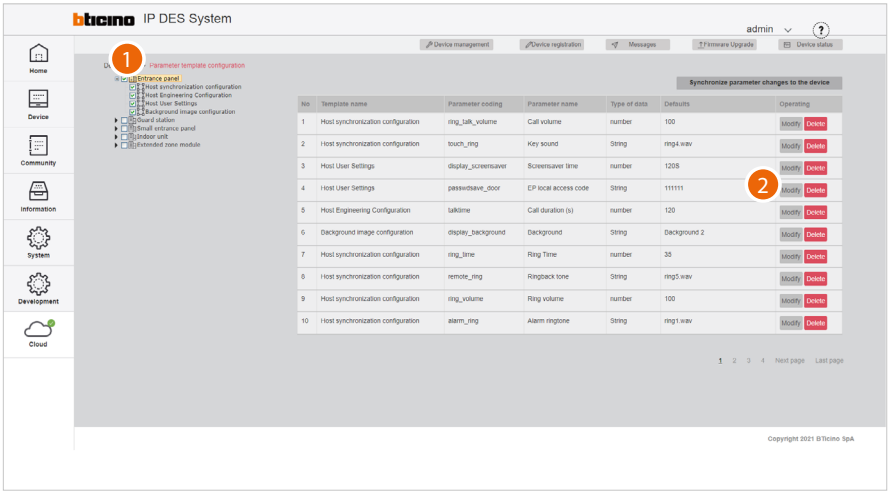


3. Select the Lift control interface with relay 375013
4. Select the quantity
5. Select the operating mode:
   - **with access control**: this mode allows to set up an exclusive call to a specific floor (e.g. only go to the third floor)
   - **ground floor call**: this mode allows to set the system so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

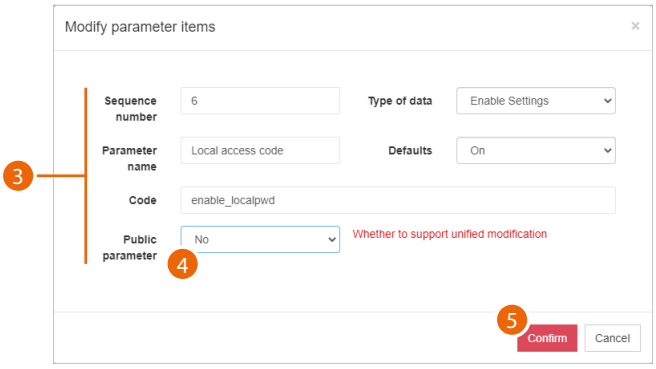
Parameter template configuration

This function defines the parameters of the devices you are going to add.
This way you will avoid having to set them individually each time.

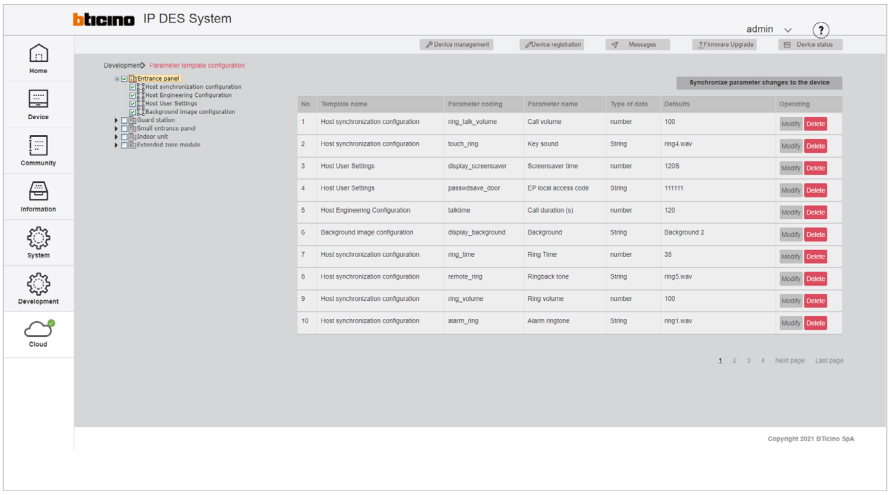
Note: *perform this operation before creating the community structure.*



1. Select the category of devices for which you want to set the default parameters
2. Click to modify the parameter



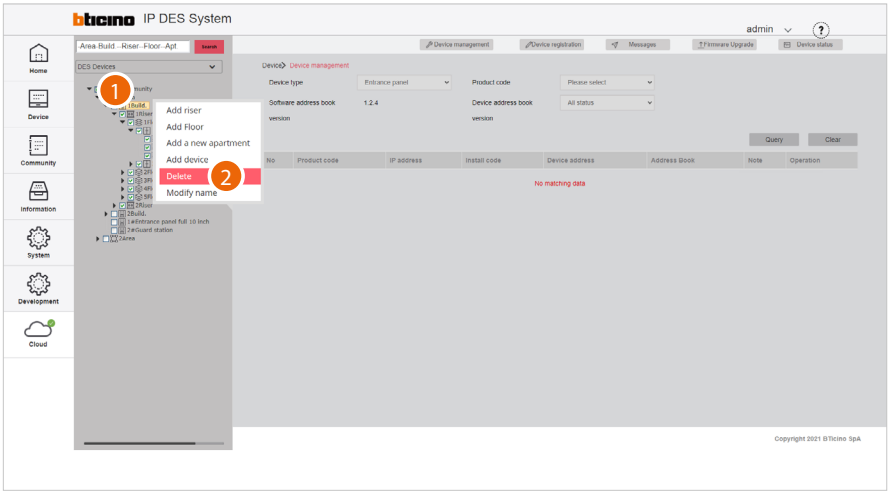
3. Edit the parameter
4. Select yes to make the parameter public.
   Public parameters will be available for editing in the Public parameter update page
5. Click to confirm



All the new devices of this category that will be added will now have the above set parameter

Delete

Delete levels and/or devices

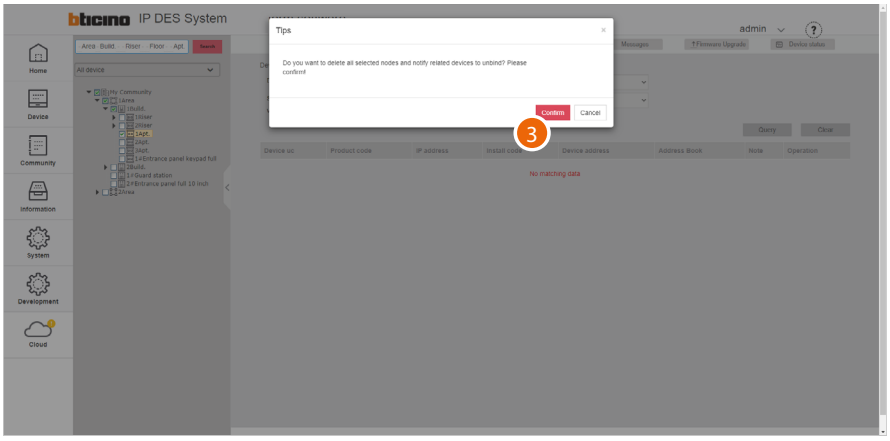


1. Tick the level or device to delete and right click

***Caution**: selecting a level will also delete its sub-levels*

***Note**: deleted levels/devices are marked with a green tick in a white box*

2. Click the command

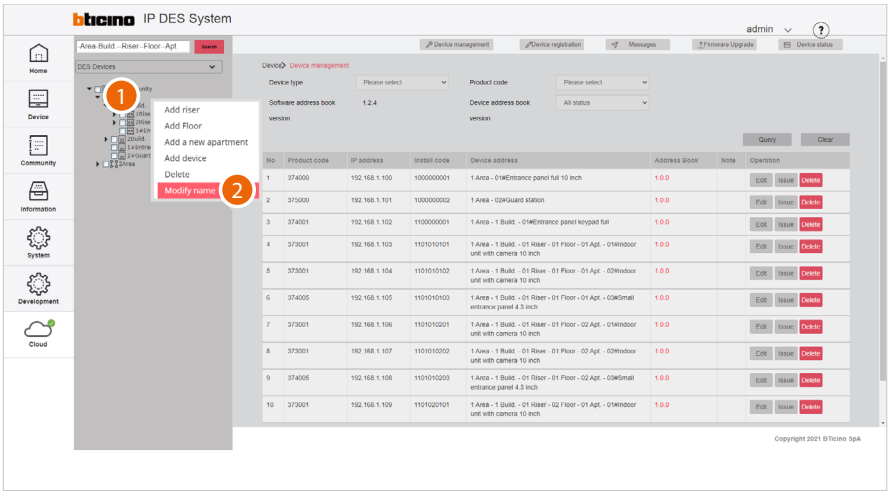


3. Click to confirm.
   Performing this operation also dissociates the physical device from the virtual one.
   The physical device is reset.

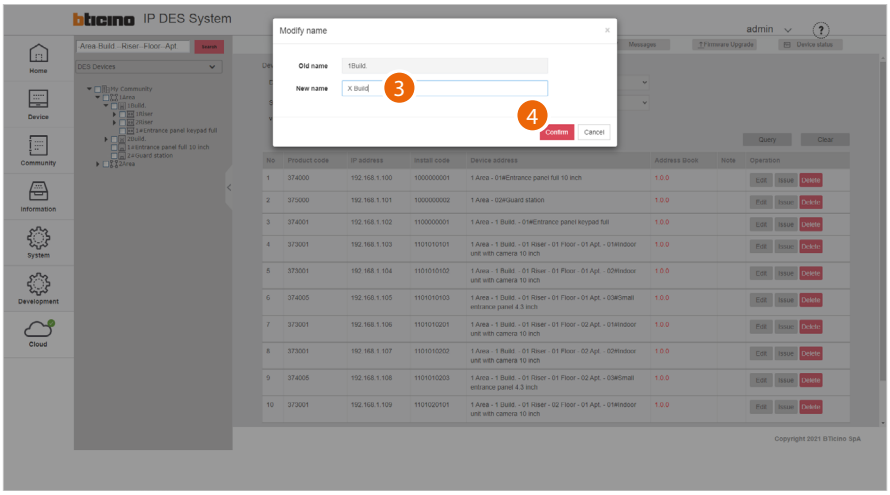
***Attention**: with this procedure, the level/device is permanently deleted. To be able to manage it again, it will be necessary to follow the adding procedures (Add Area/Building/Riser/Floor/Apartment/Device)*

Modify name

Modify the name of levels and/or devices



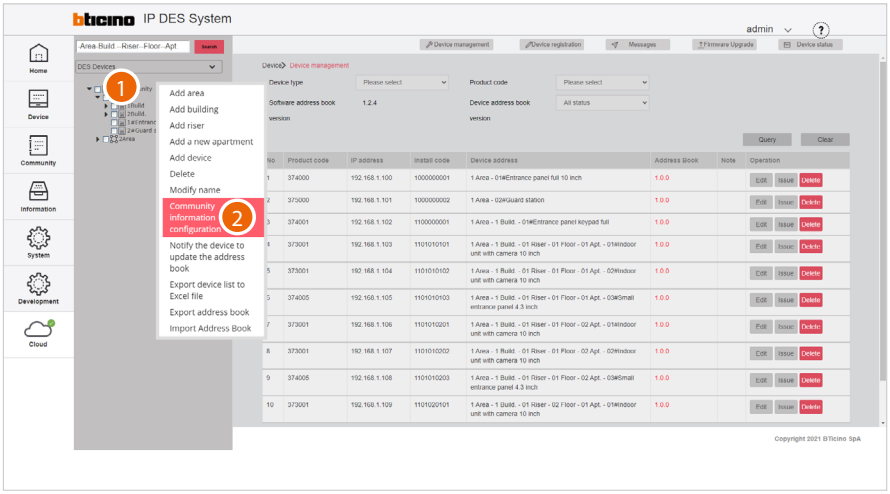
1. Right click the level or device to modify
2. Click to select the command



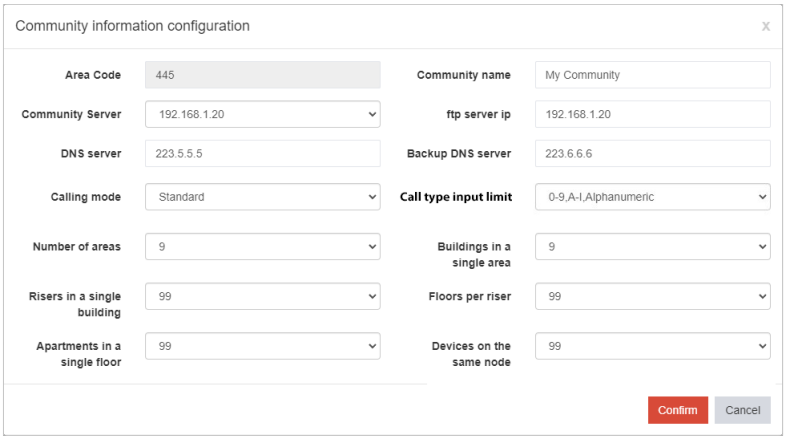
3. Enter the new name
4. Click to confirm

Community information configuration

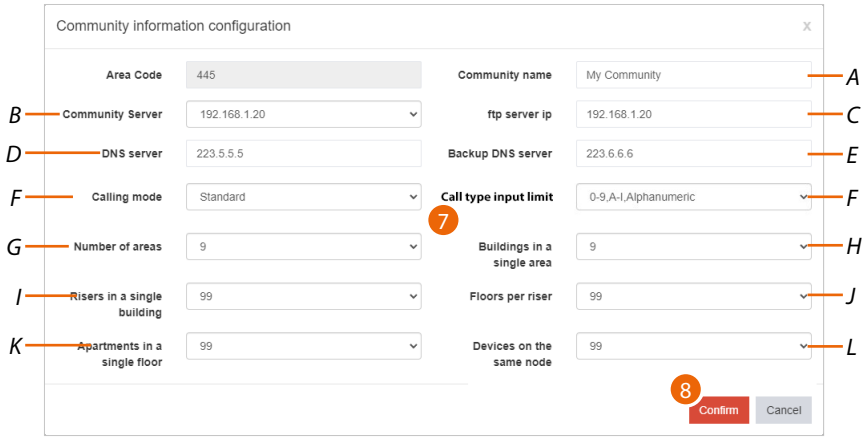
This page can be used to define parameters like number of Areas, Buildings, Risers and so on, as well as other details that will define the structure of the Community.
It is also necessary to define the type of call that will be used for all Community calls.



1. Right click the community
2. Click to select the command



By default, the parameters cannot be changed. In order to change them, it will be necessary to enable modifications in the Development\System parameter configuration page



A Modifies the Community name

B Selects the fixed IP address of the Community SD

C Modifies the ip server ftp address of the community.

***Note**: address borrowed from the "community server" field (do not change unless in case of special requirements).*

D Modifies the address of the DNS server (unless there are special requirements, we recommend to keep the default address)

E Modifies the address of the backup DNS server (unless there are special requirements, we recommend to keep the default address)

F Select the mode and type of call depending on which address you want to use on the devices:

Call using the address of the Community
Mode = Standard
Type= do not select

Call using alphanumeric alias
Mode = Alphanumeric
Type = 0-9; A-Z, Alphanumeric
(not available for 374001/03)

Mode = Alphanumeric
Type = 0-9; A-I, Alphanumeric
(available for all devices)

Call using contact alias in the address book
Mode = Alphanumeric
Type = Address Book
(available only for devices with touch display)

G Enters the maximum number of Areas for your Community (default 9).

H Displays the maximum number of Buildings that an Area can have (default 9).

I Displays the maximum number of Risers that a Building can have (default 99).

J Displays the maximum number of Floors that a Riser can have (default 99).

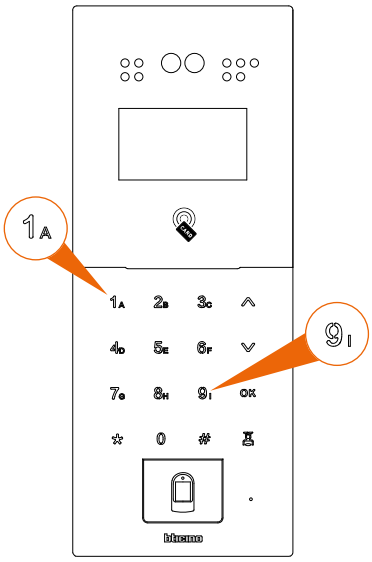
K Displays the maximum number of Apartments that a Floor can have (default 99).

L Displays the maximum number of Devices that an Apartment can have (default 99).

Note: *If even one single EP has an "0-9, AI" type keypad, select the "0-9, AI" option.*

EP with "0-9, AZ" keypad

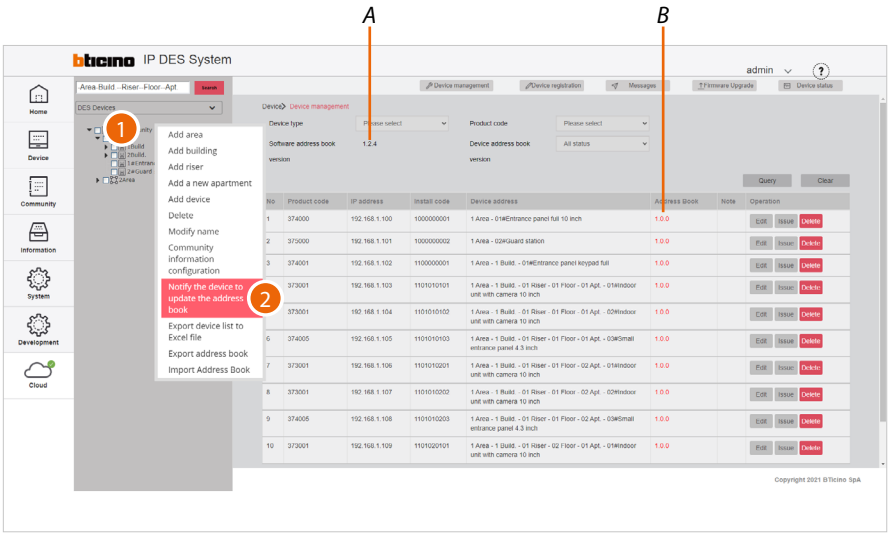
EP with "0-9, AI" keypad



7. Enter the parameters
8. Click to confirm

Notify the device to update the AB

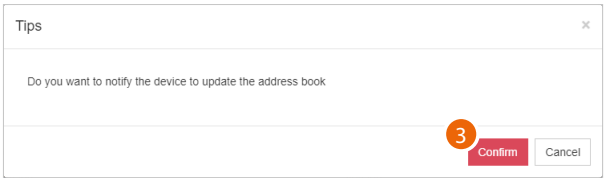
This function allows to send the AB and the parameters of the virtual devices to the physical devices in the system.
Each time this is done, the AB version will be updated.



A *AB current version*

B *Device current version*

1. Right click the community
2. Click to select the command



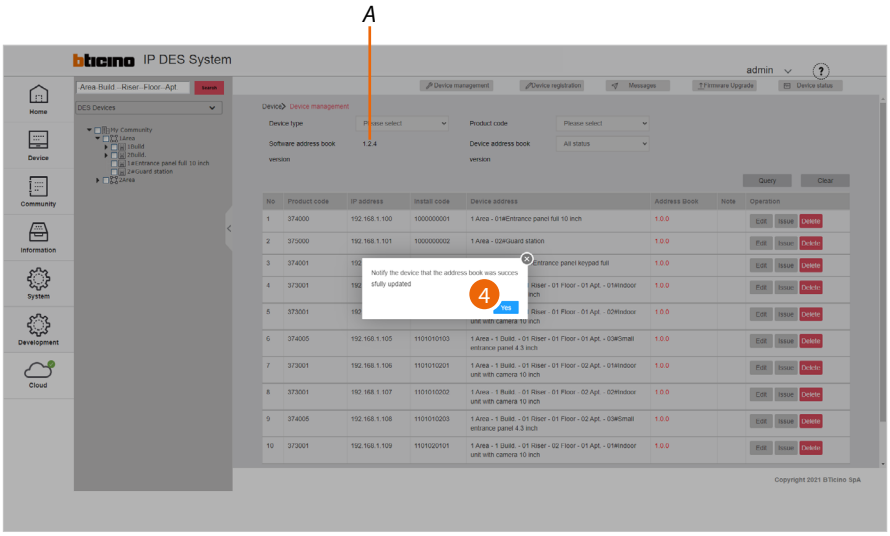
***Note**: In case of unexpected device behaviour during use, check that the AB of the SW is the same as the AB of the device*

3. Click to confirm

The configuration is completed with the devices not powered. Before switching on, the devices will automatically recover their configuration (AB)

In case of changes to the AB that do not entail a movement of the devices from the currently configured positions, the devices accept the modification without further action

A device that has been incorrectly placed in an apartment and needs to be moved must be reset (see the device manuals), so that the new AB can be loaded.



4. Click to end; the AB version has been reviewed (*A*)

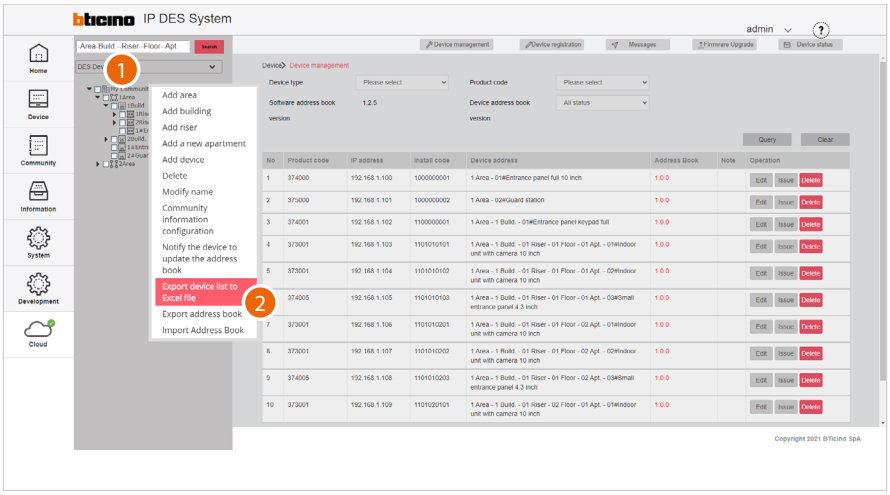
The address book is now saved in the SD. To avoid accidental loss, it is also possible to **save it in an archive file**

Export device list to Excel® file

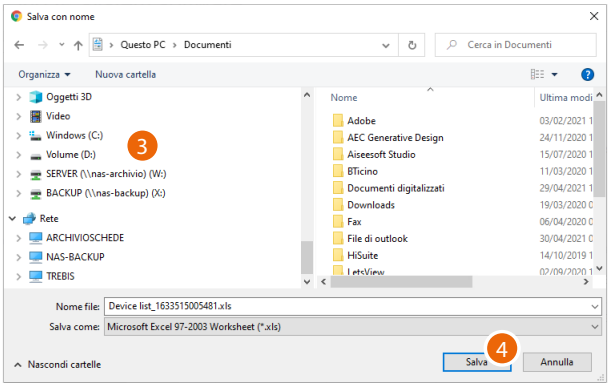
The file contains the characteristic data of each device. One of these data is the Alias.
The Alias is a customisable alphanumeric code that replaces the community address.
The alias may be of two types:

- 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.

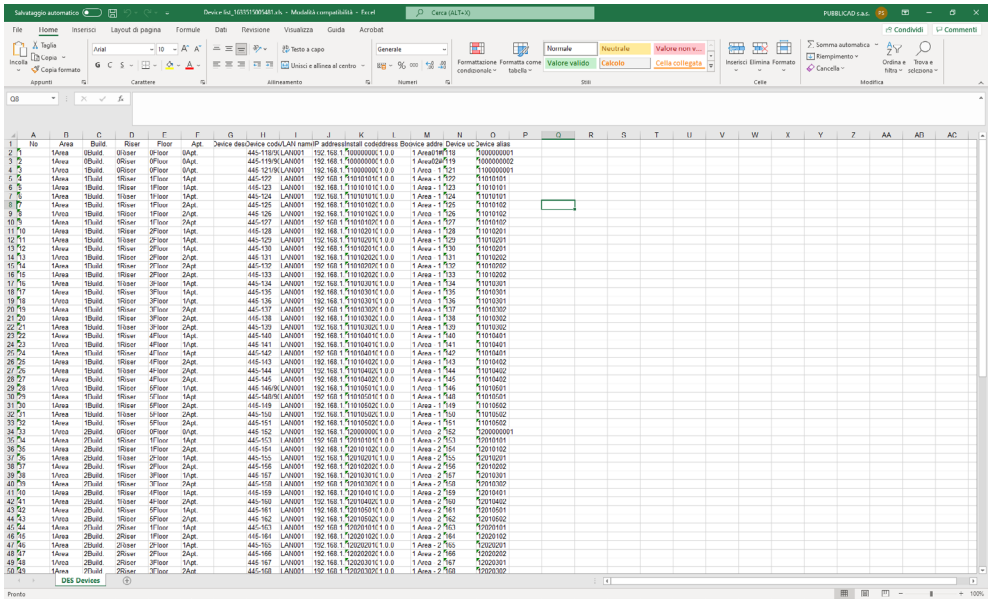
To create an alias, see creating aliases



1. Right click the community
2. Click to select the command



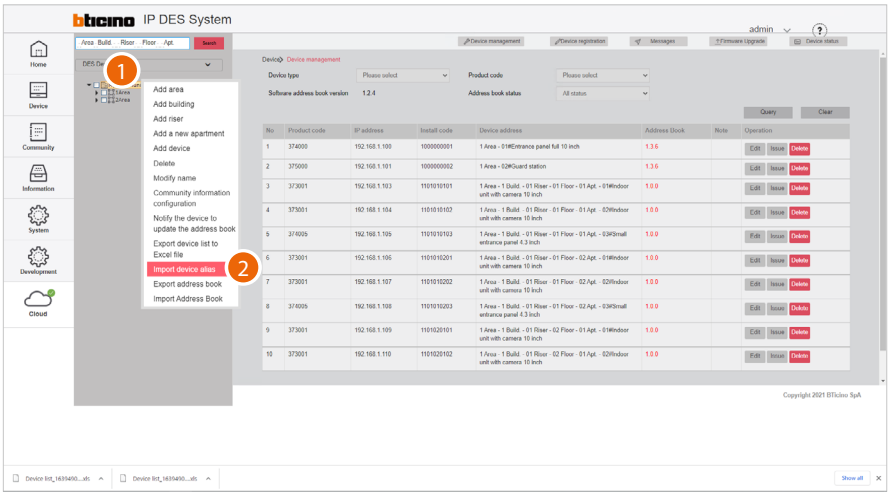
3. Select the location where to save the file
4. Click to save



The file contains the data of the devices

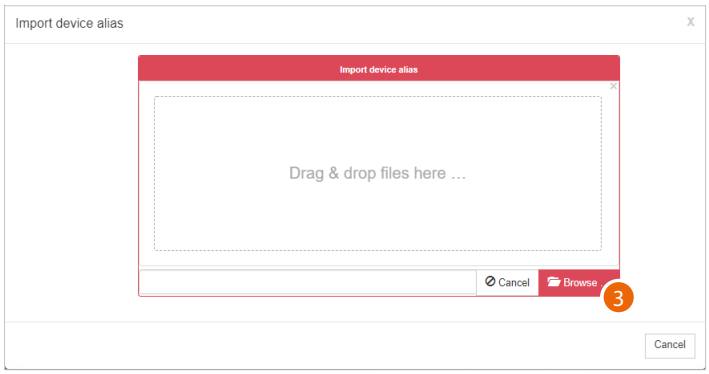
Import device alias

This function imports a device list in Excel® format, previously saved using the Export device list to Excel® file function.
This function is useful for creating aliases.

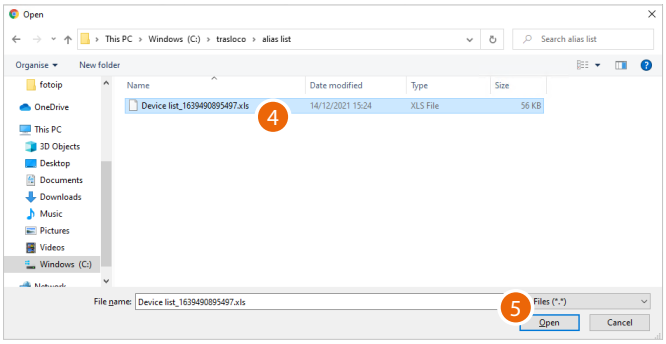


1. Right click the community
2. Click to select the command

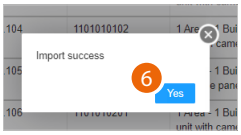
Note: *set the call type as address book in the calling mode/0-9, A-Z, Address book page to display this item*



3. Click to select the Excel® file



4. Select the file (.xlsx)
5. Click to open

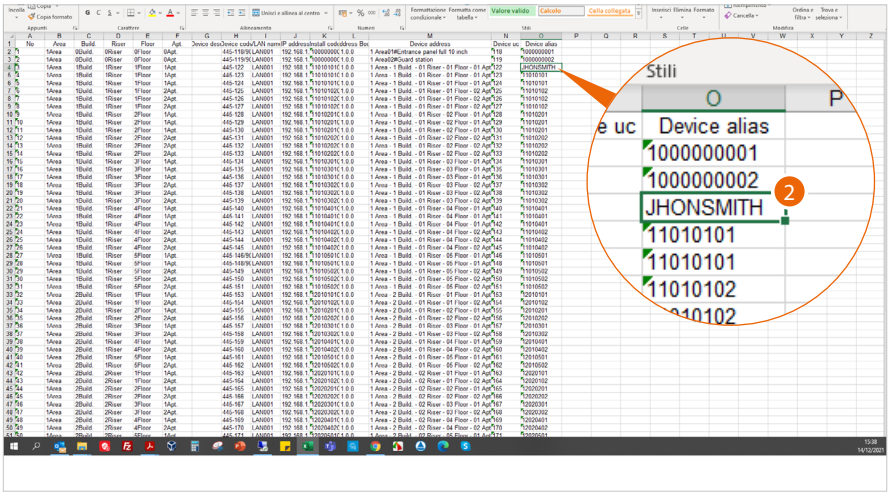


6. Click to confirm

Alias creation procedure

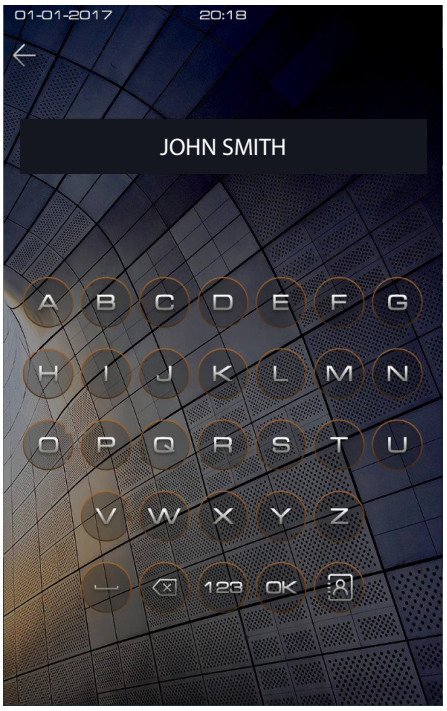
By default, to call an apartment, enter the address in the community (e.g. 11010101 from an EP). To call the apartment by entering an alias (eg JOHN SMITH):

1. open the exported excel file using the Export device list to Excel® file function



2. Locate the device in the apartment and change the address by entering an alias and save the file
3. Import the file into the project using the Import device alias function
4. Send the AB to the devices with Notify the device to update the AB

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

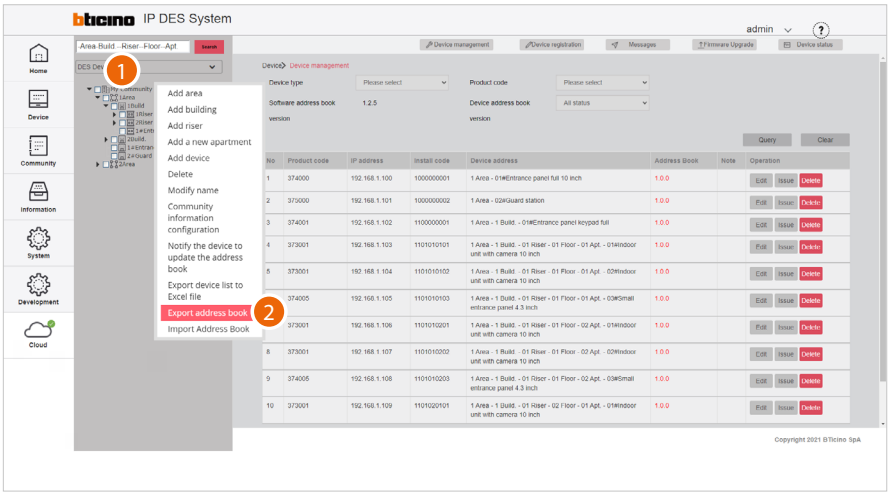


Now it is possible to use the alias JOHN SMITH to call the apartment

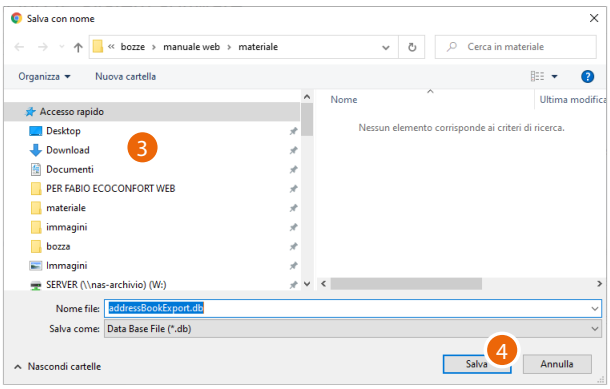
If the alias of an EP is changed, when receiving a call the alias will be displayed instead of the system address

Export Address Book

This function allows to export the AB stored in the SW.
This function can be useful in order to file a configuration for use at a later date using the **AB Import** function.



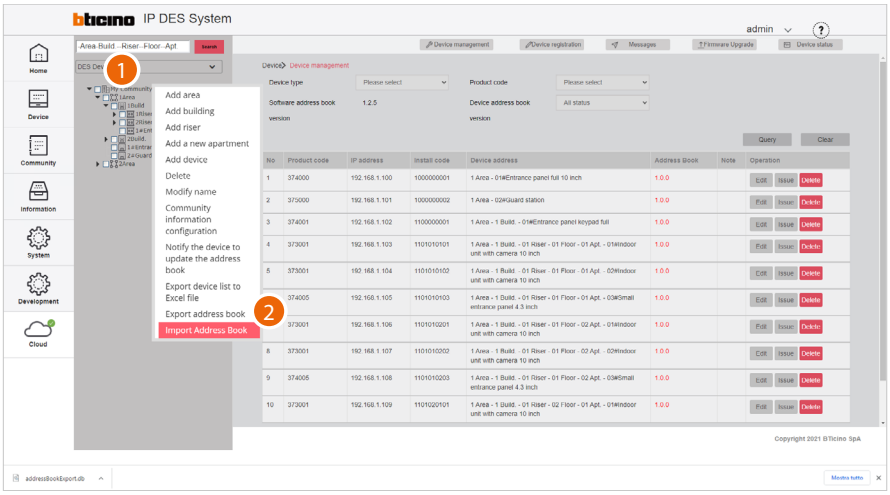
1. Right click the community
2. Click to select the command



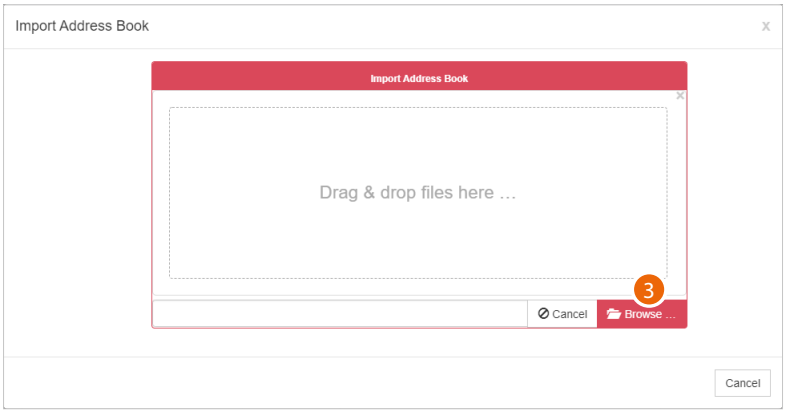
3. Select the location where to save the file (.db)
4. Click to save

Import Address Book

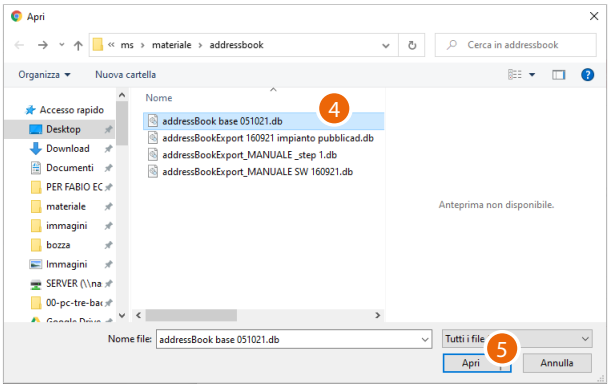
This function allows to import a previously saved AB using the Import AB function.
This function can be useful to start a new configuration from an existing one.



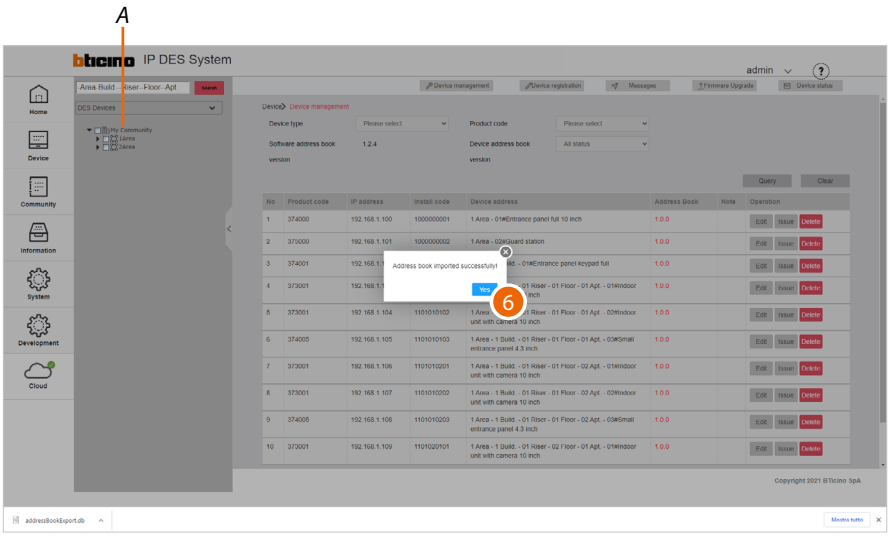
1. Right click the community
2. Click to select the command



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



4. Select the file (.db)
5. Click to open

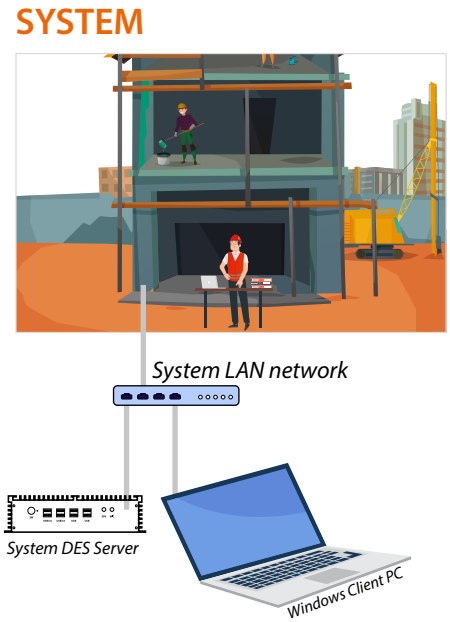


6. Click to confirm; the new structure (*A*) has been uploaded

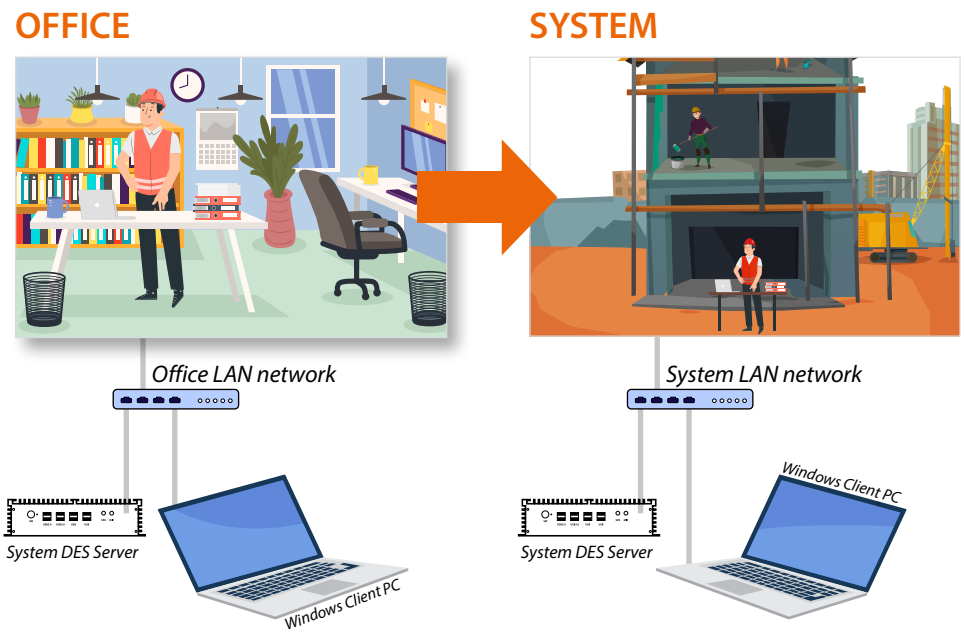
Examples of system situations

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

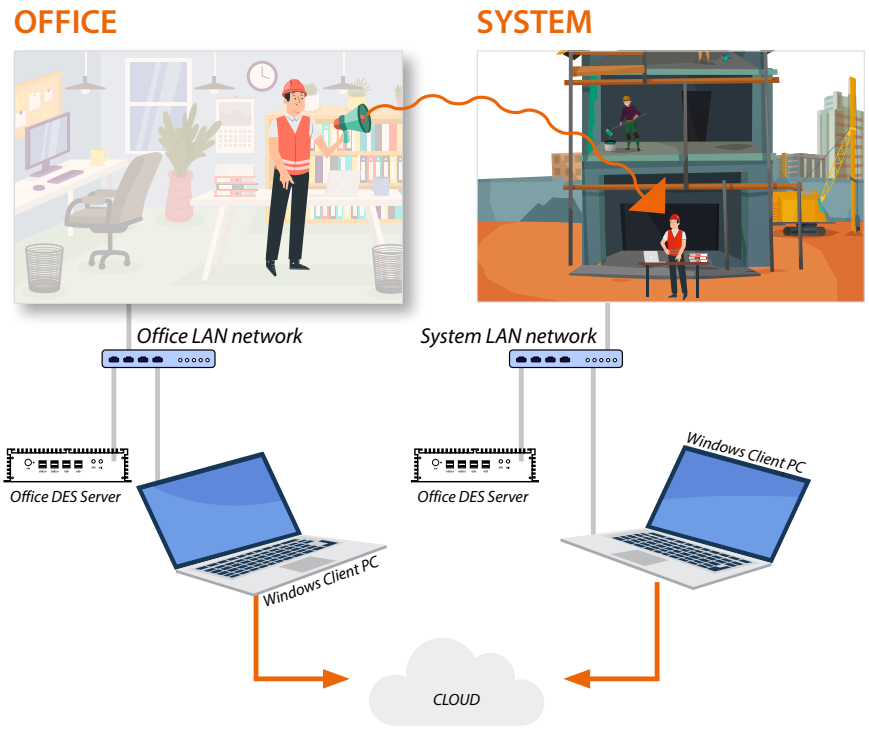


EXAMPLE 2: Pre-configuration of the server at the office and on-site system configuration
this case, the SD is configured before it is installed in the system, using a Windows Client PC and connecting it to the office LAN.
The SD is then taken on site and connected to the system LAN.
View all the steps required for the example



ESEMPIO 3: 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 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

SYSTEM

Step 01 Community VLAN network creation

Step 02 Community structure definition

Step 03 Community structure creation

Step 04 Device MAC address registration

Step 05 Community customisation

Step 06 Saving of passwords

Step 07 Registration of the Community on the installer's Cloud

Step 08 Forwarding of the address book to the DES Server

Step 09 Installation of the devices

Step 10 Activation of the devices

Step 11 System test

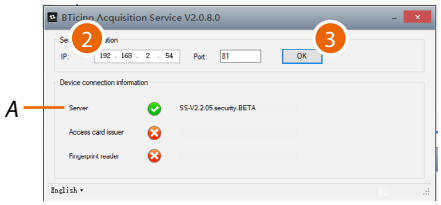
Step 12 Update of the devices

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

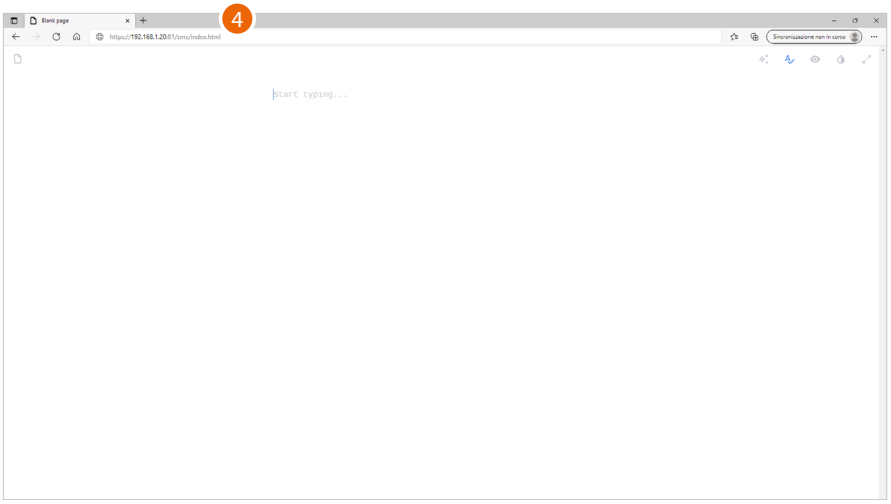
The following screen appears



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 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 MAC address identification (method 2).

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

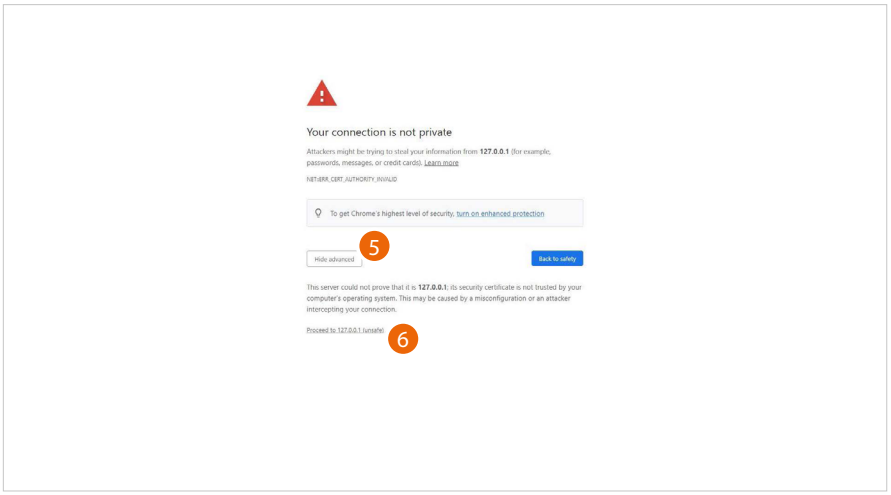


4. Open the browser and enter the http address of the DES Server:

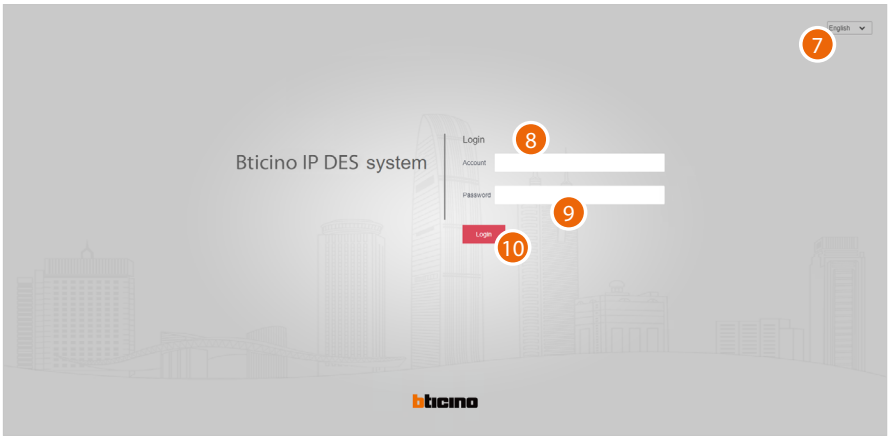
https://SD IP address:81/cms/index.html

Note: *use Crome/Edge browser and a screen with resolution 1920x1080*

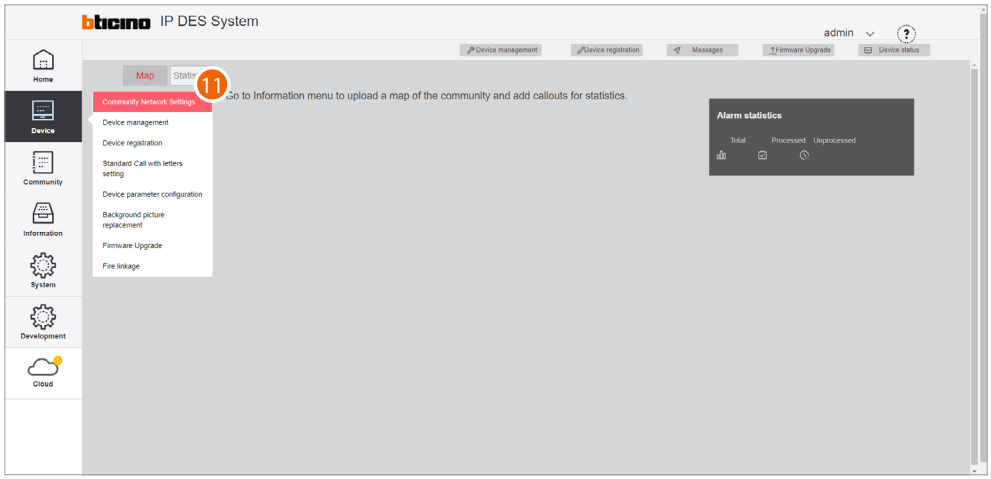
In some cases, the browser may consider the page to be unsafe.



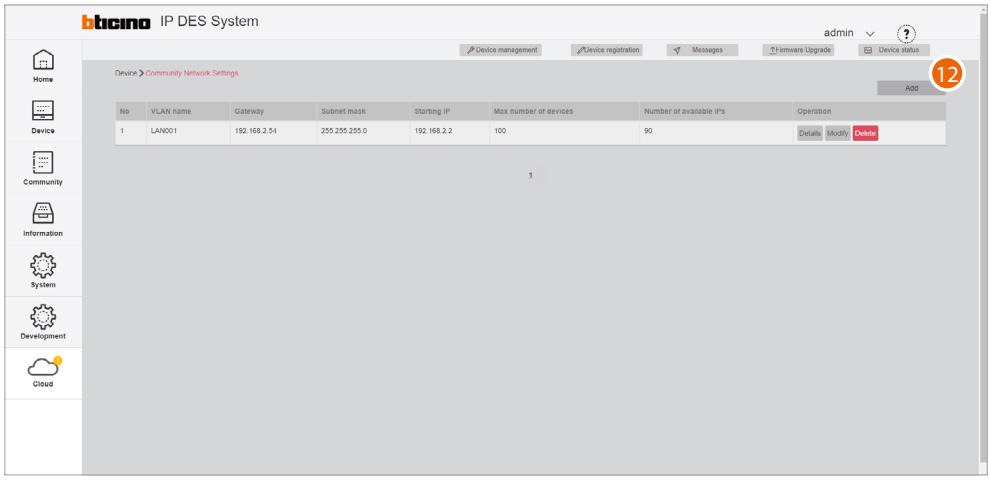
5. Click to display the advanced options
6. Click to ignore the warning and proceed



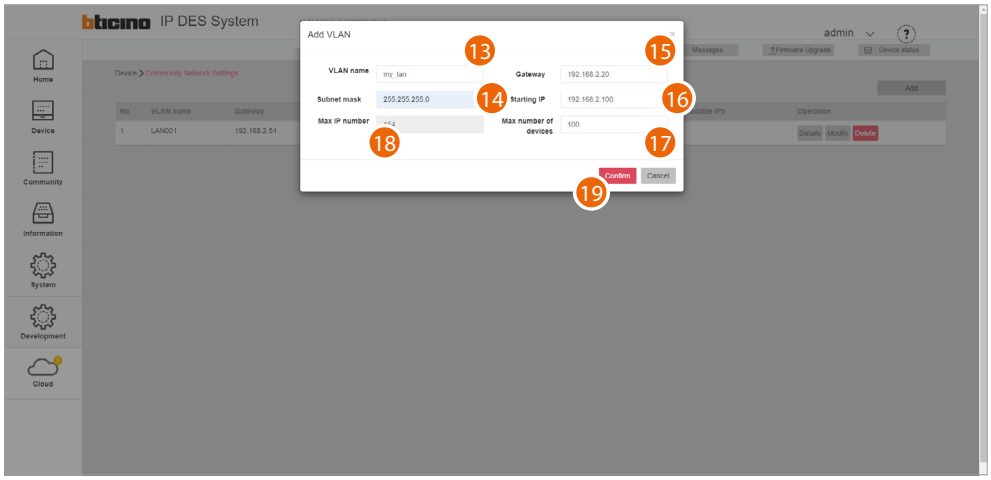
7. Select the interface language
8. Enter the login name (default admin)
9. Enter the password (default 123456)
10. Click to confirm



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

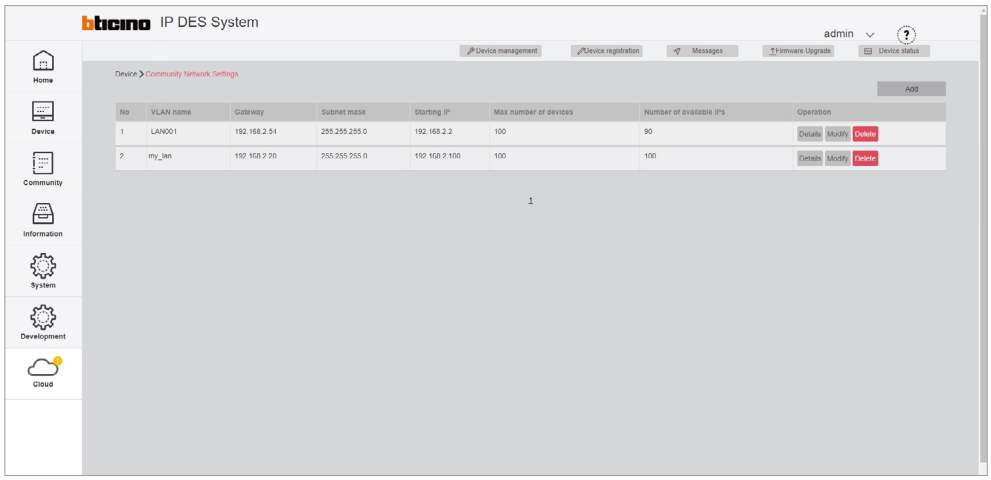


12. Click to create the community VLAN network



13. Enter the name of the community VLAN network (letters and numbers without space)
14. Enter the Subnet mask address
15. Enter the fixed IP address of the DES Server given to you by the network administrator
16. Enter the starting address from which the IP addresses of IP devices will be generated (including Onvif IP cameras and interfaces item 375013) Assignment of IP address range based on the number of video door entry devices
17. Enter the number of FULL IP devices that will be part of the Community
18. It displays the maximum number of FULL IP devices that can be installed based on the previously entered data
19. Click to confirm

***NOTE**: the parameters (13 to 1 8) must match those found on the system.*

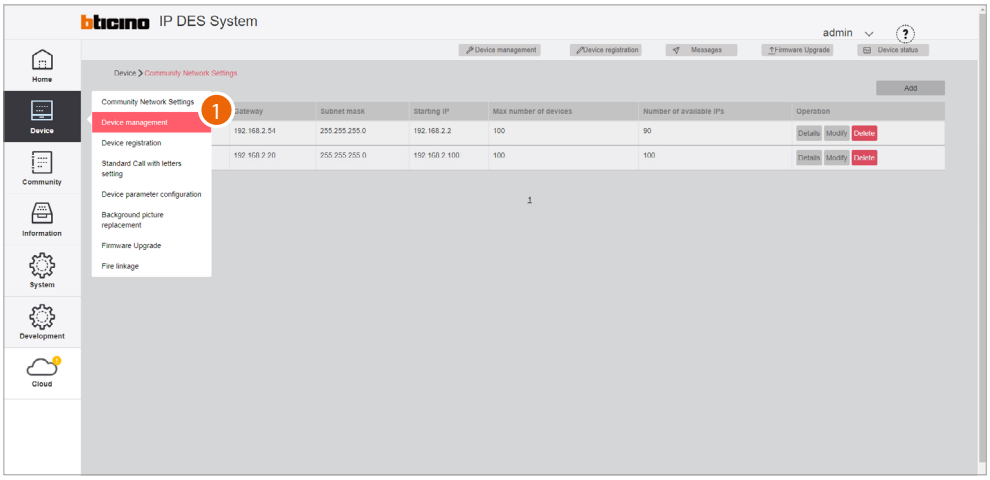


The community VLAN network has been created

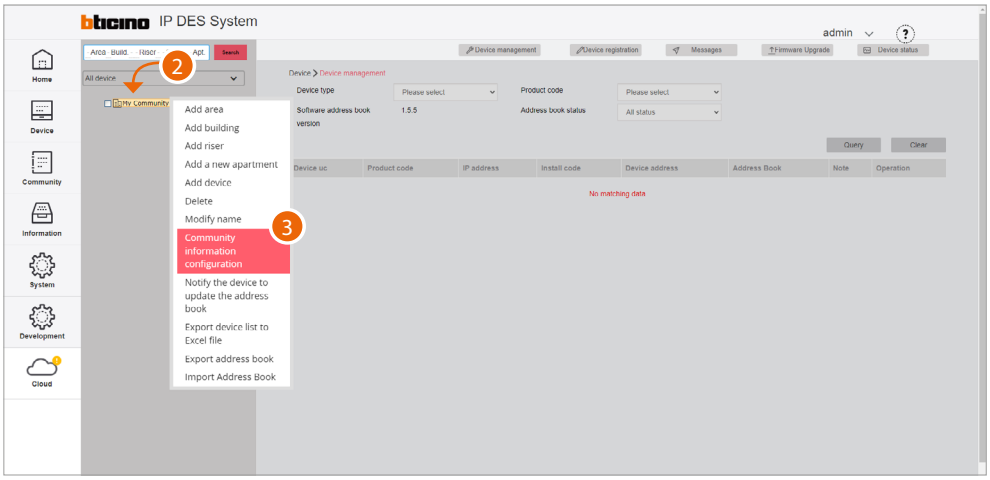
Community structure definition

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

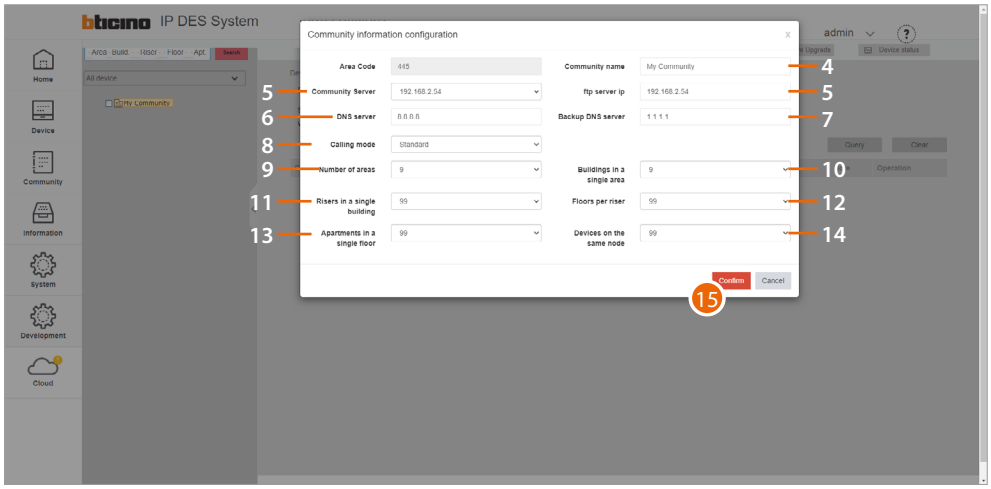
In this section, it is also necessary to define the type of call that will be used for all Community calls.



1. Click to enter the Community configuration section



2. Click the Community with the right mouse button: a drop-down menu will appear with the commands for its configuration
3. Click to open the pop-up window with the parameters that define the Community structure



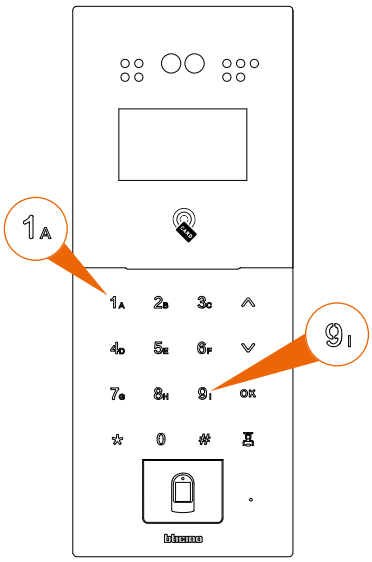
4. Change Community Name
5. Selects the fixed IP address of the Community DES Server
6. Change the address of the DNS server (unless there are special requirements, we recommend to keep the default address)
7. Change the address of the backup DNS server (unless there are special requirements, we recommend to keep the default address)
8. Selects the type of call to be used for the system: Standard or Alphanumeric.
   When selecting Alphanumeric, it will also be necessary to select a mode, "0-9, AZ" or "0-9, AI", depending on the type of EPs installed in the Community.
9. It displays the maximum number of Areas for your Community (default 9).
10. It displays the maximum number of Buildings that an Area can have (default 9).
11. It displays the maximum number of Risers that a Building can have (default 99).
12. It displays the maximum number of Floors that a Riser can have (default 99).
13. It displays the maximum number of Apartments that a Floor can have (default 99).
14. It displays the maximum number of Devices that an Apartment can have (default 99).

***Note**: The default values of item 9 through 14 are consistent with the example shown in this document, and therefore do not need to be changed.*
For other more complex structures, see ***Community information configuration****.*

***Note**: If even one single EP has an "0-9, AI" type keypad, select the "0-9, AI" option.*

EP with "0-9, AZ" keypad

EP with "0-9, AI" keypad



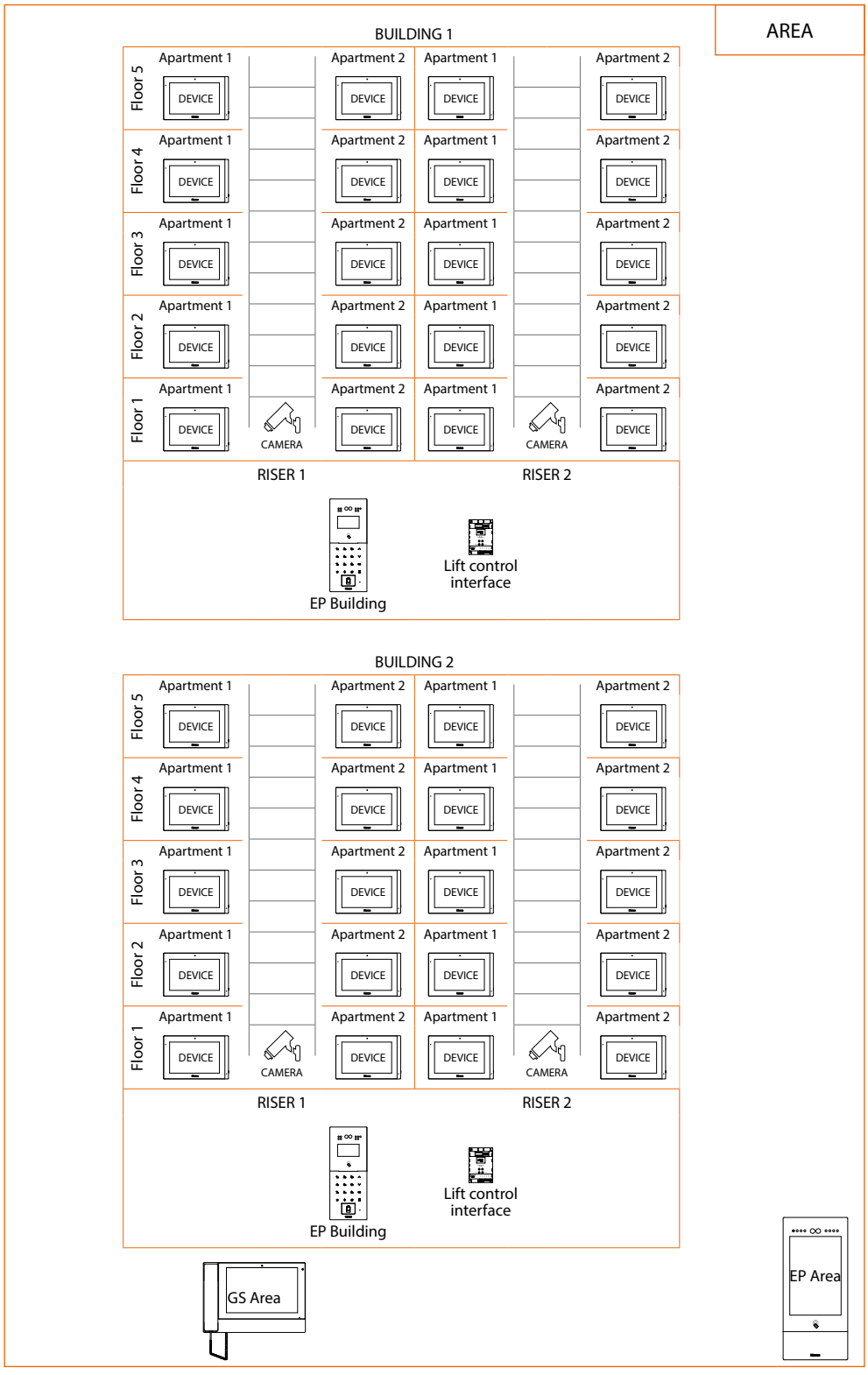
15. Click to confirm

Community structure creation

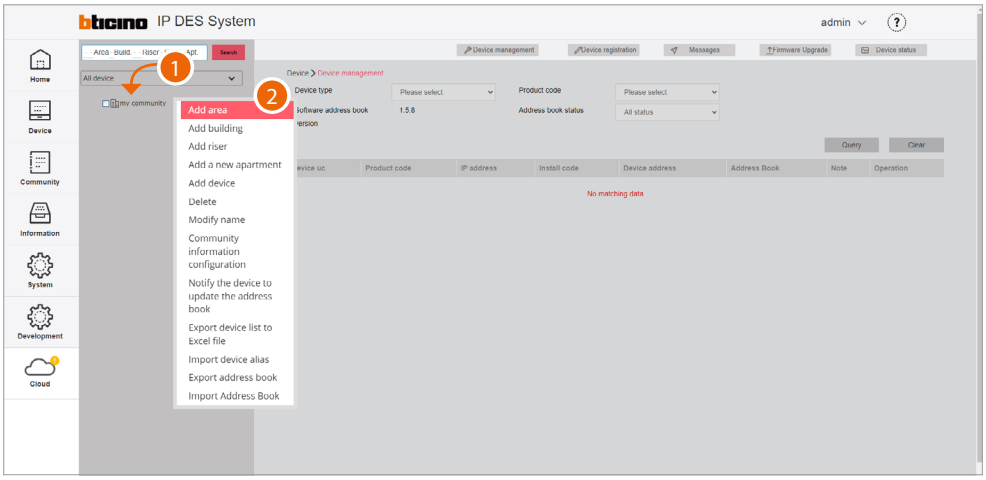
Depending on how your Community is composed, you will need to hierarchically enter:

AREA → BUILDING → RISER → FLOOR → APARTMENT → DEVICE

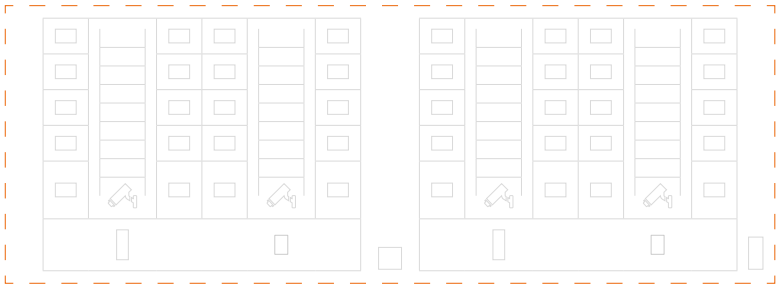
This document will show the creation of a sample structure composed as follows:

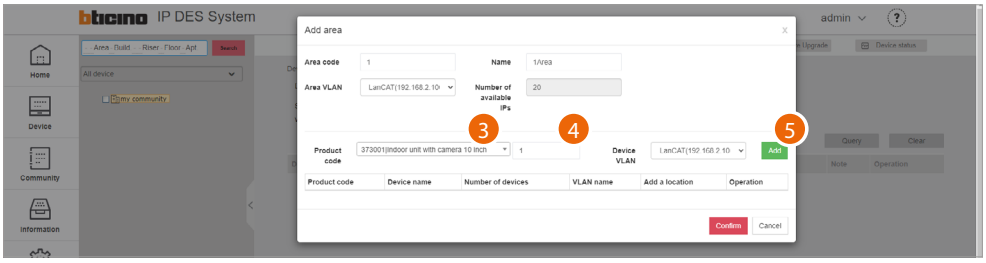


***Warning**: the configuration operations shown below are those required for creating the sample structure. See the Software Manual for all the other possible configurations.*



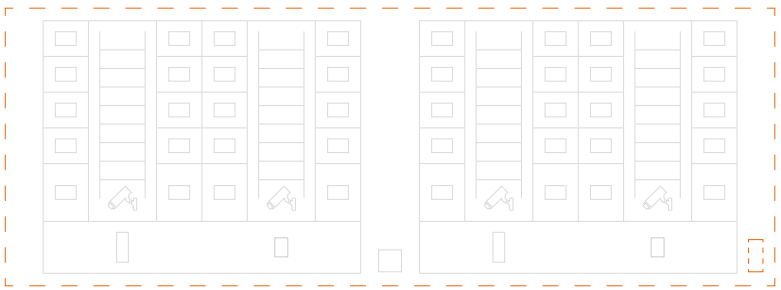
1. Click the Community with the right mouse button: a drop-down menu will appear with the commands for its configuration
2. Click to add a **new Area**

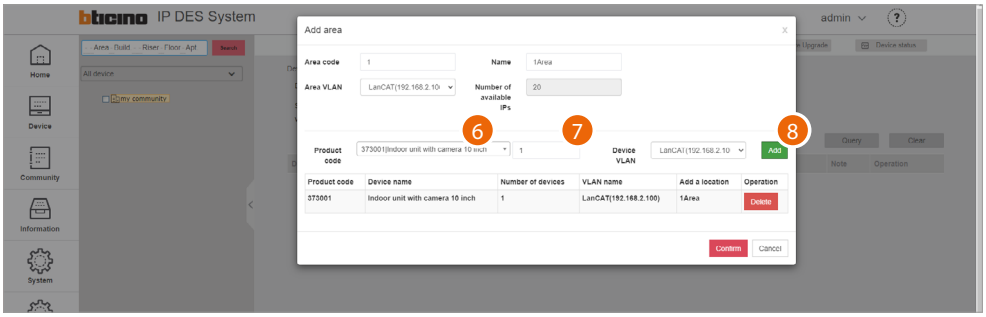




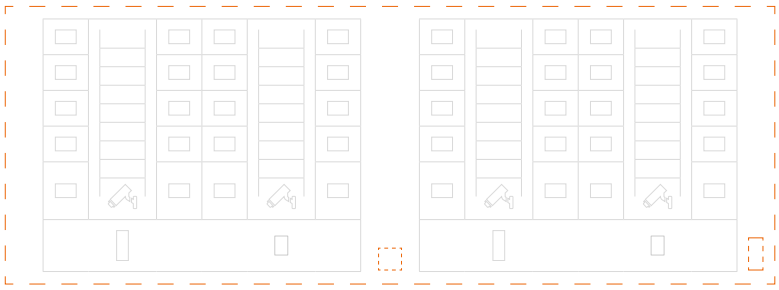
3. Select the Area device (EP Area1)*
4. Select the quantity
5. Click to add

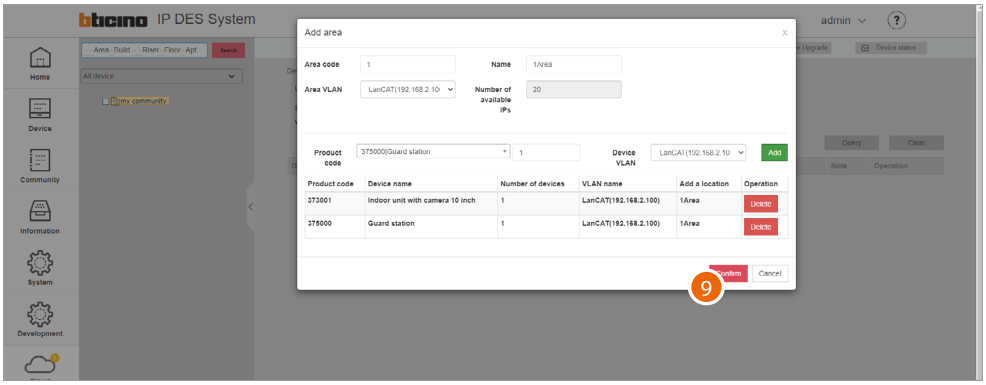
**Nota: prima di procedere con inserimento di un dispositivo ricordarsi di verificare che tutti i parametri del dispositivo rispettino le richieste, vedi Device parameter configuration*



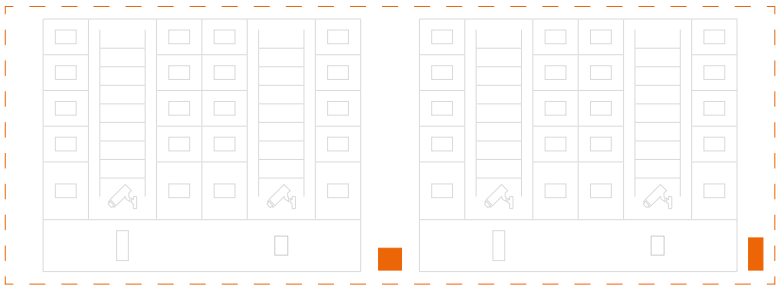


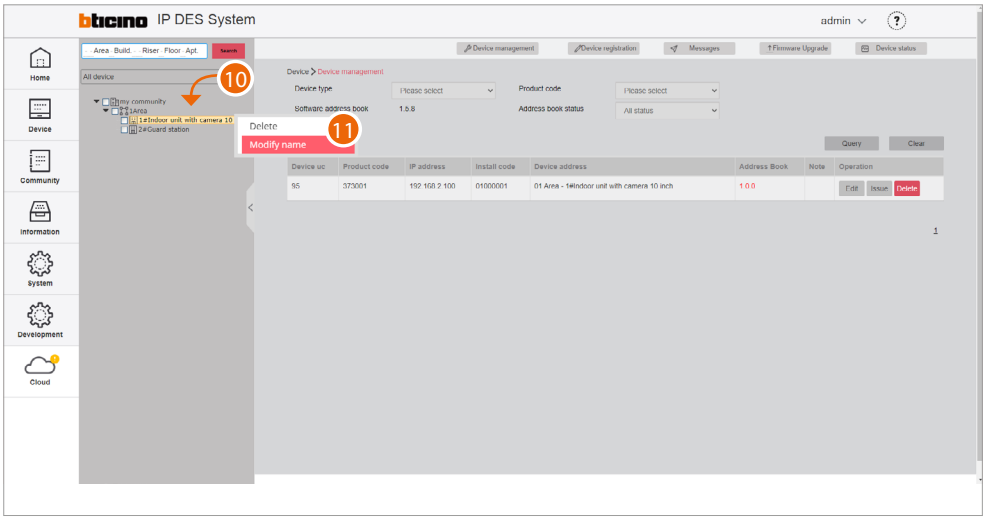
6. Select the second Area device (GS Area1)
7. Select the quantity
8. Click to add





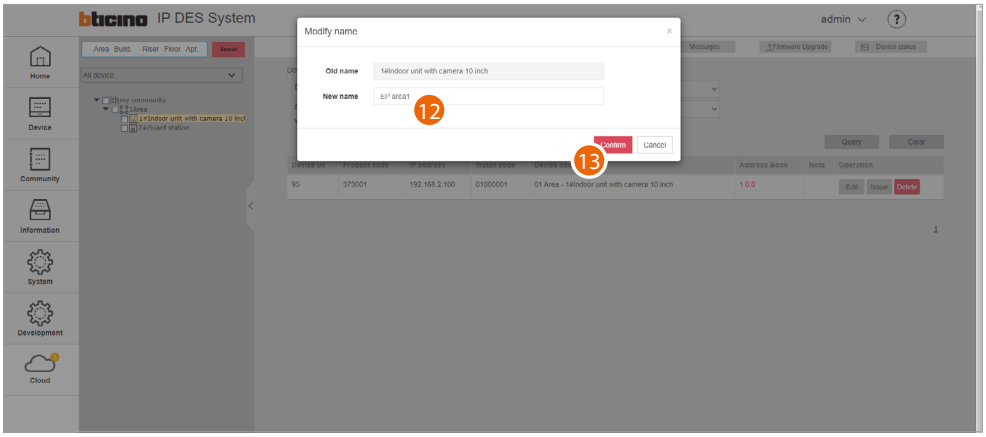
9. Click to confirm



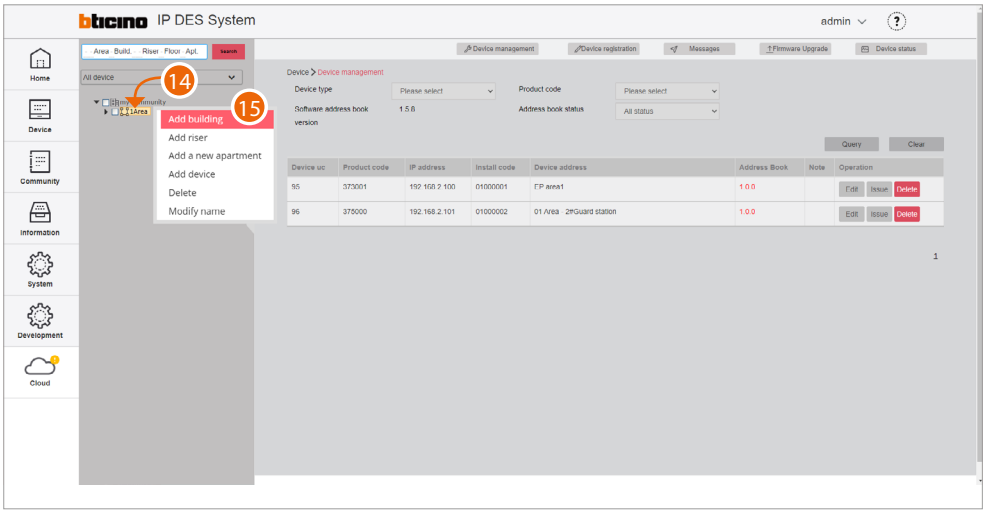


After inserting the devices, you will be able to customize their name

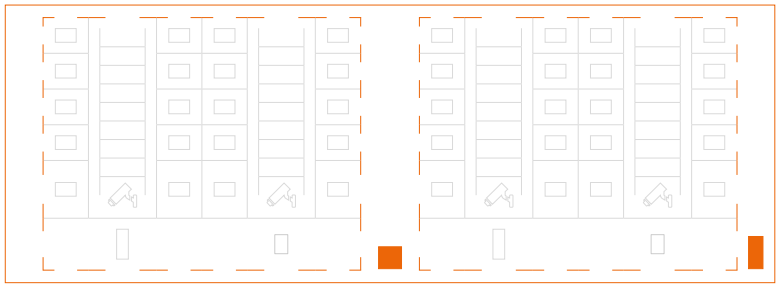
10. With the right mouse button click the device that you want to rename: a drop-down menu will appear
11. Click to open the edit window

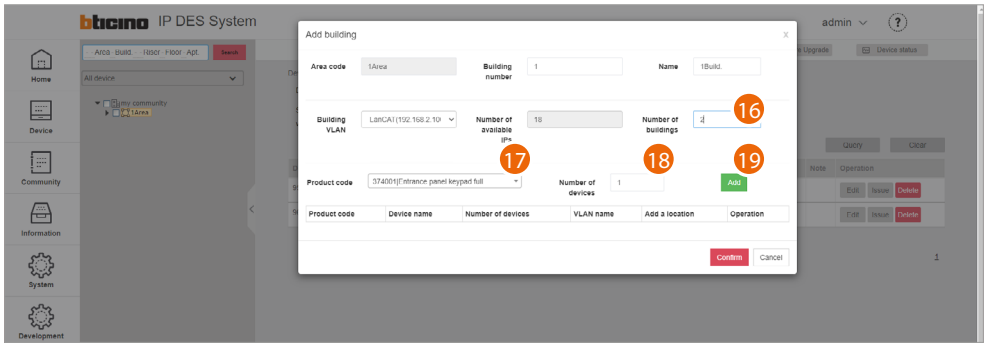


12. Enter the new name
13. Click to confirm



14. Click the Area with the right mouse button. This will open a drop-down menu
15. Click to add the **Buildings**

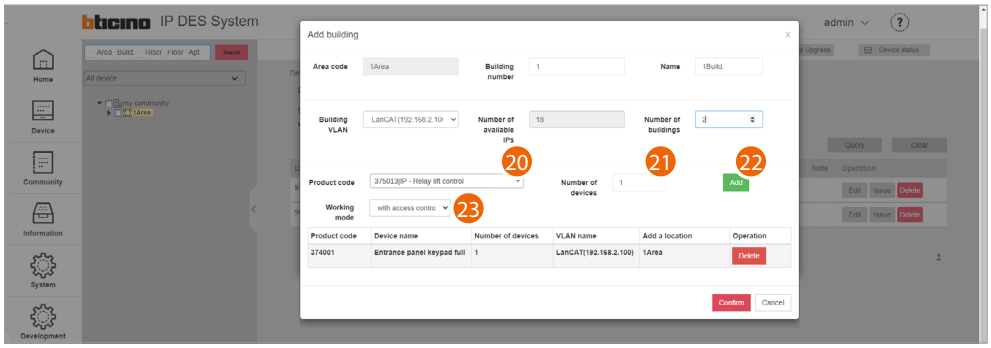




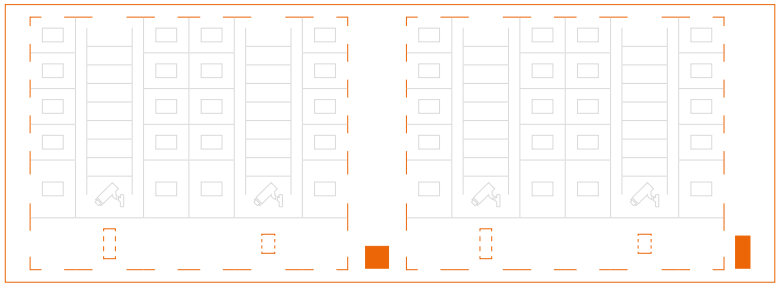
16. Select the number of buildings to add
17. Select the Building device (EP Building)

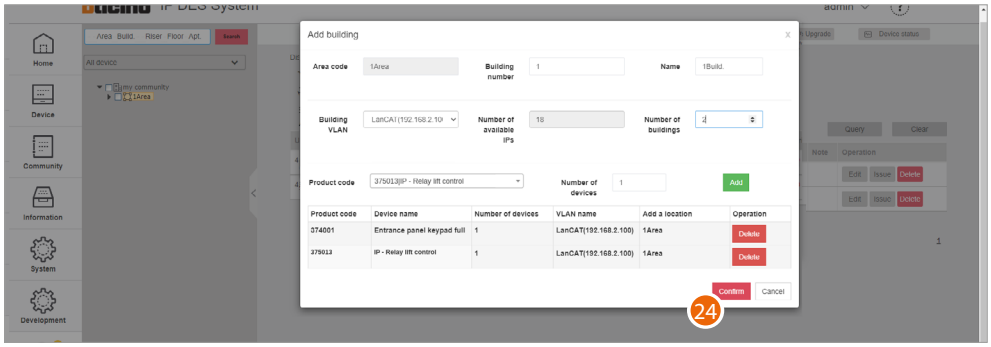
***Note**: the software automatically applies a filter to only show devices that are consistent with the component that you are adding*

18. Select the quantity
19. Click to add

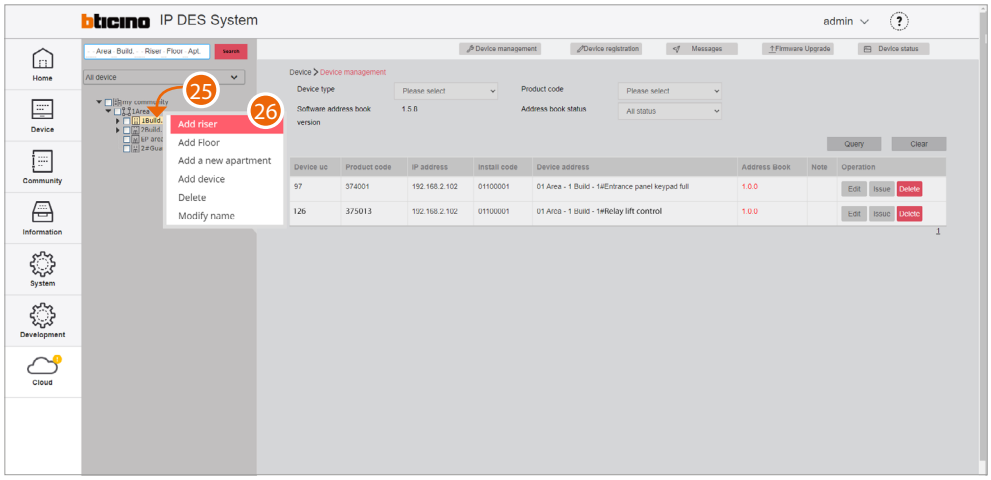


20. Select the device to add (lift control interface with relay 375013)
21. Select the quantity
22. Click to add
23. Select the operating mode:
    - **with access control**: this mode allows to set up an exclusive call to a specific floor (e.g. only go to the third floor)
    - **ground floor call**: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

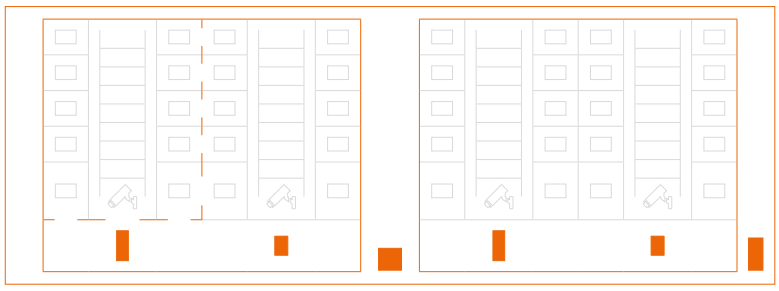


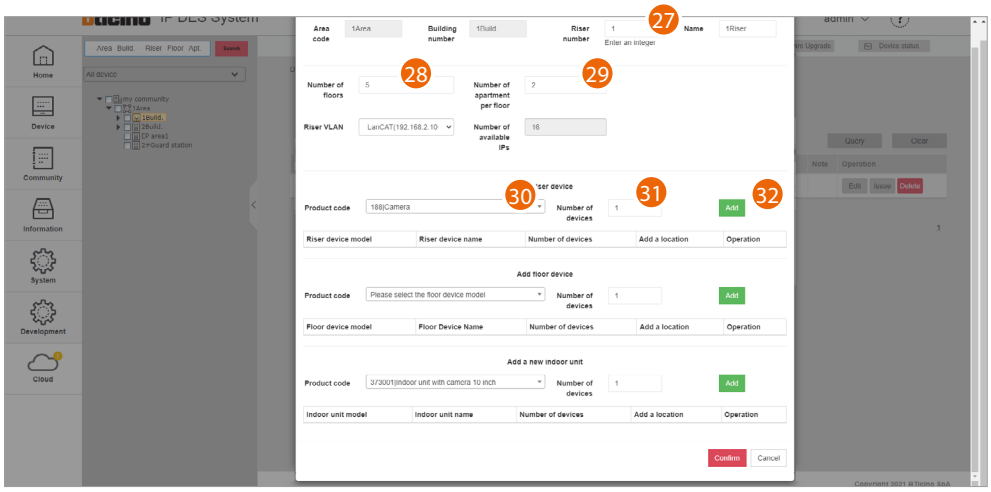


24. Click to confirm

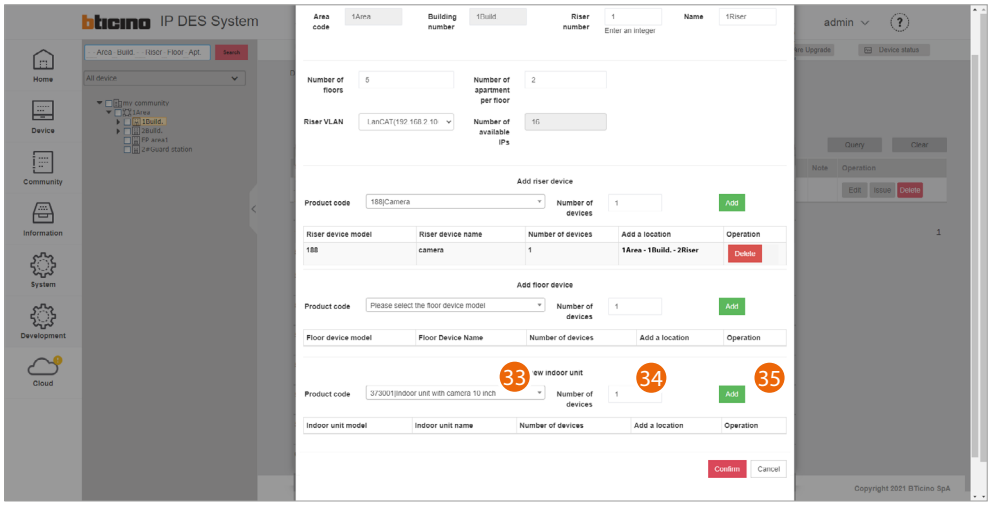


25. Click the Building with the right mouse button. This will open a drop-down menu
26. Click to add a **new Riser**

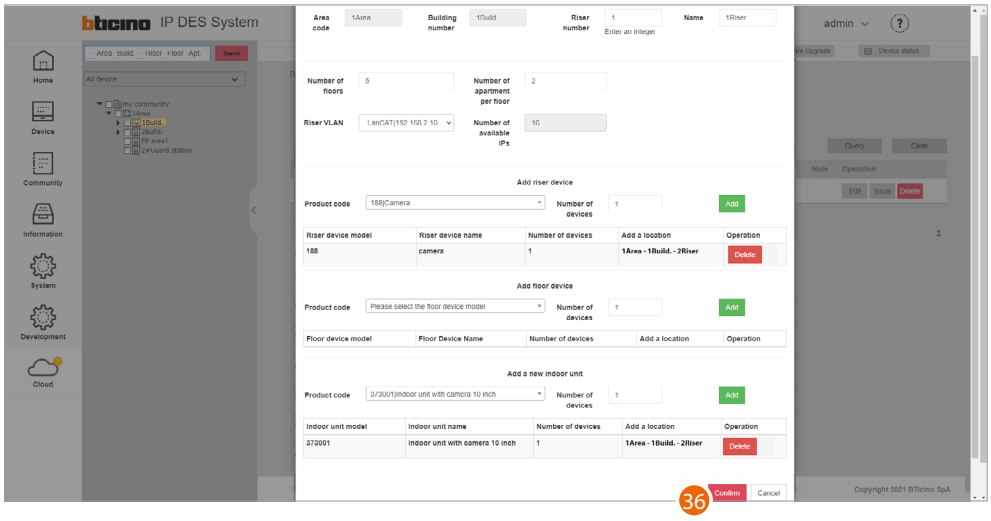




27. Enter the progressive Riser number
28. Select the number of Floors in the Building (5)
29. Select the number of Apartments for each Floor (2)
30. Select the OnVif IP camera
31. Select the quantity
32. Click to add

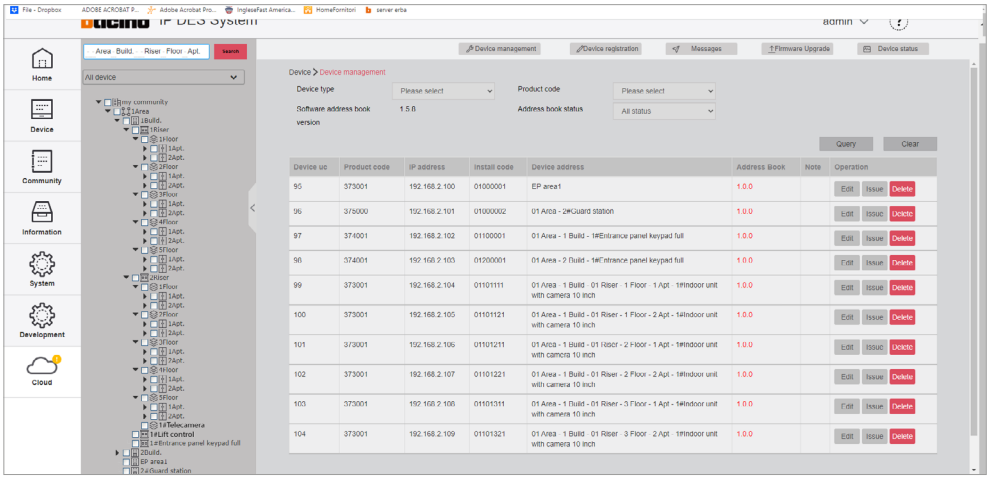


33. Select the apartment device
34. Select the quantity
35. Click to add

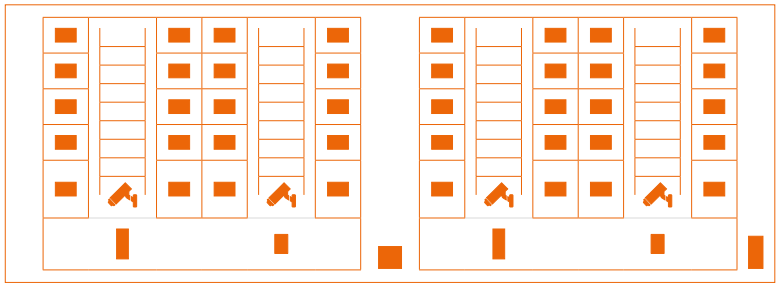


36. Click to confirm

Repeat the same steps for Riser 2

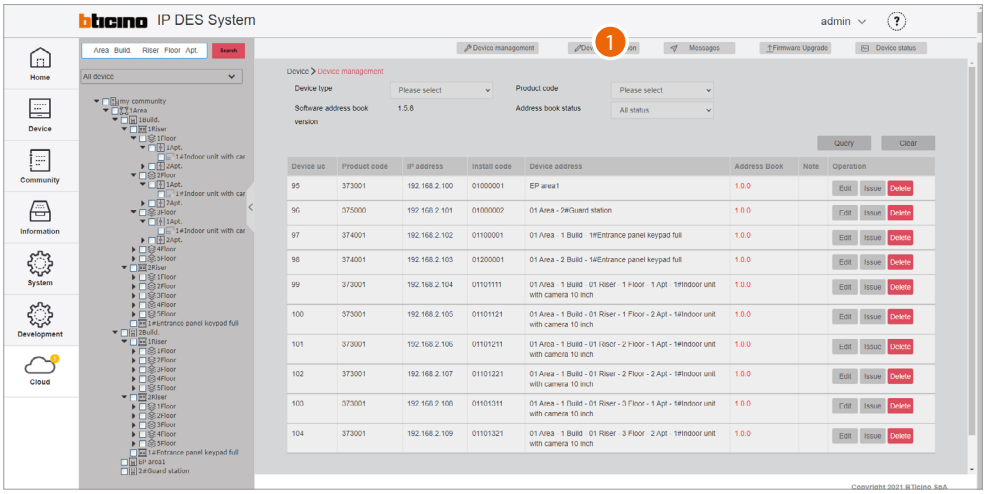


Repeat from step 21 also for building 2

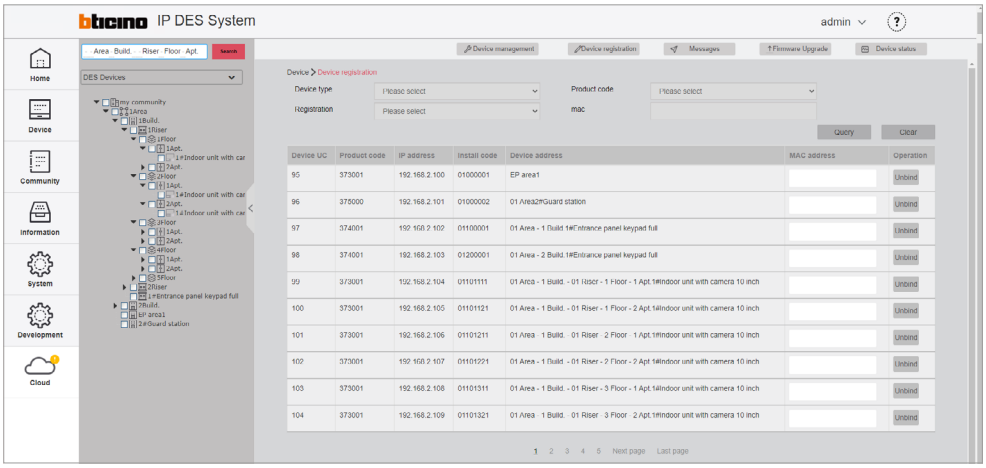


Device MAC address registration

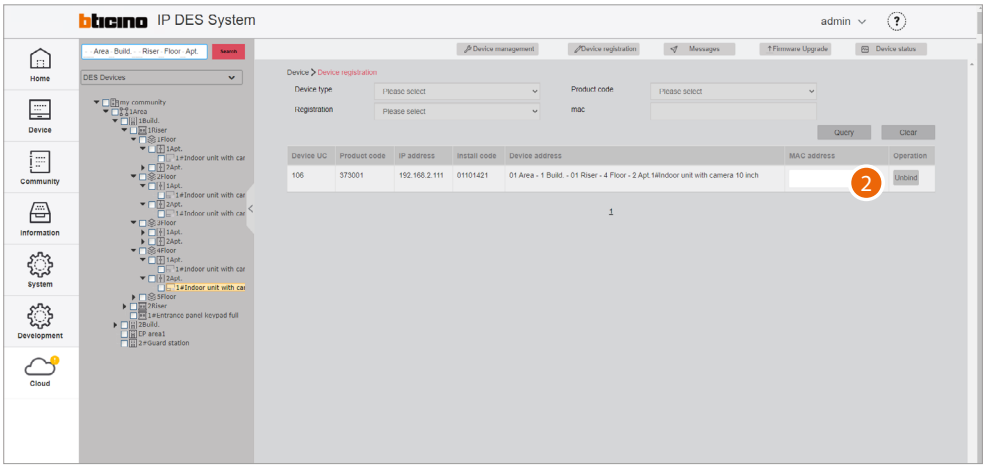
Now that the structure is complete, you will need to associate the MAC addresses of the physical devices with the virtual ones included earlier in the structure.



1. Click to enter the device registration section

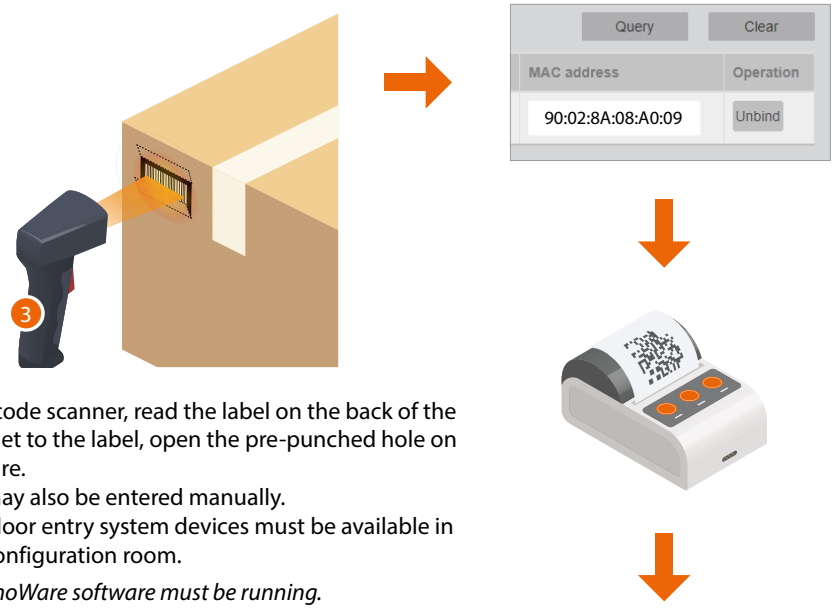


This section includes all the devices to associate. The MAC address can be entered directly from this screen



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



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.

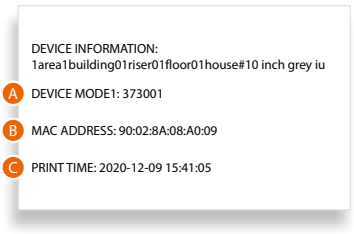
***NOTE**: the BTicinoWare software must be running.*

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



If the printer is connected to the network and ready, the label will be printed automatically.

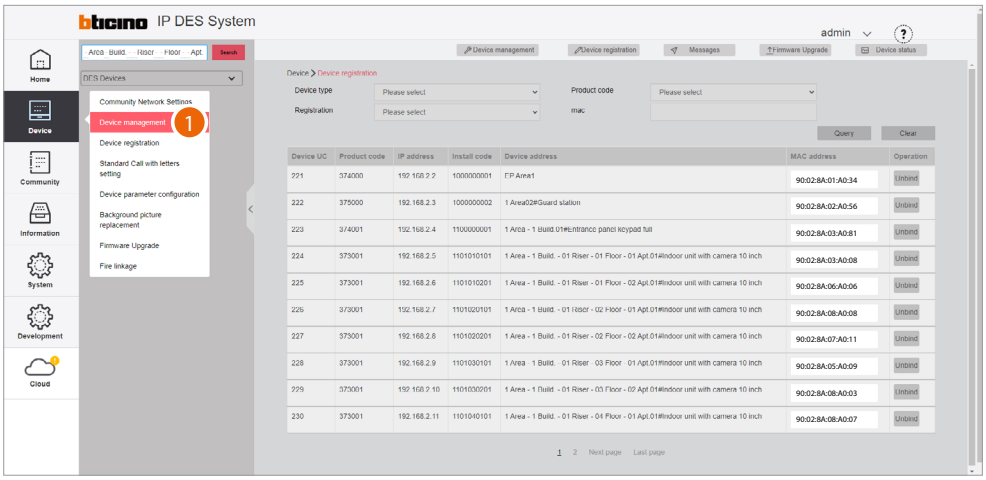
Repeat for all devices

Community customisation

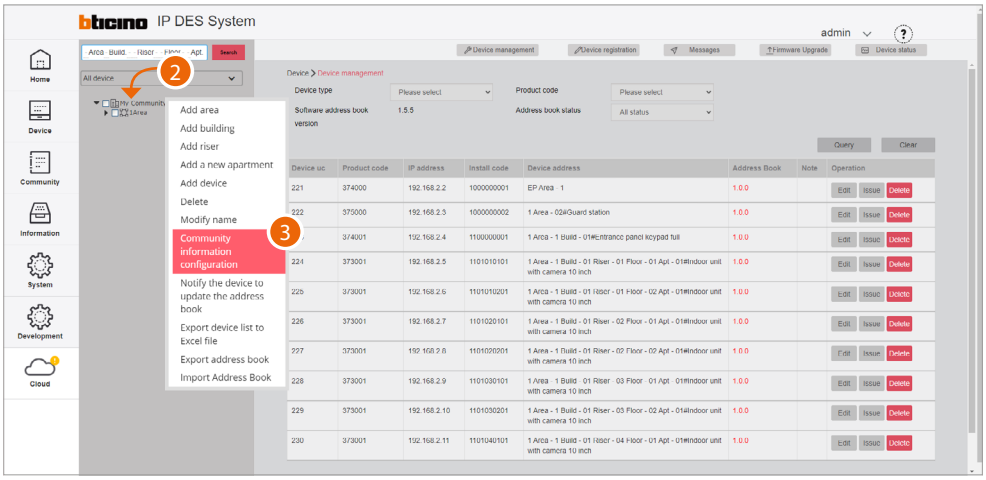
Before sending the configuration to the DES Server, we can customise the Community by e.g modifying the call mode and/or by enabling access to the Community for certain individuals.
To use a different call mode, (e.g. call mode via phonebook) to call residents, it will be necessary to:

– Change call type to alphanumeric/address book

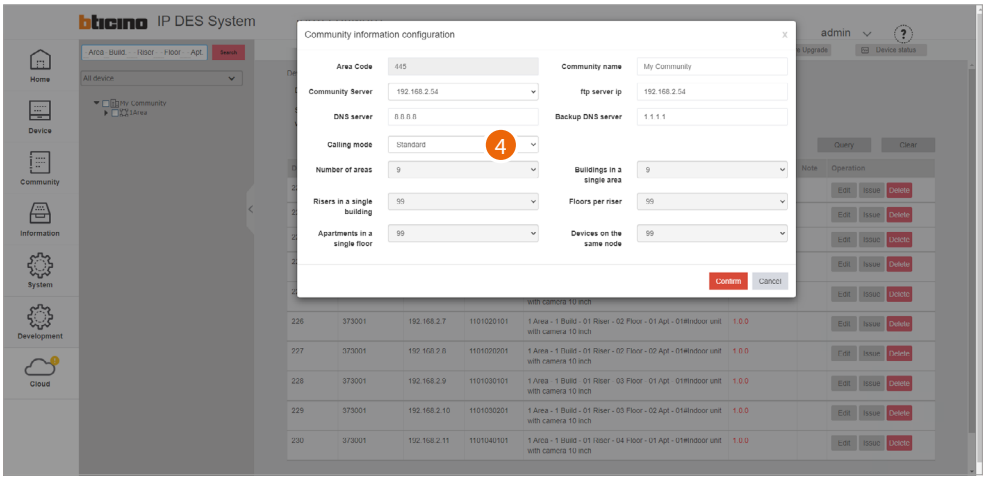
– replace the address in the community with an alias to facilitate recognition of the called party.
This function renames the apartment to a different name (alias).
The call to this apartment will be made using this new name. E.g. JOHN SMITH



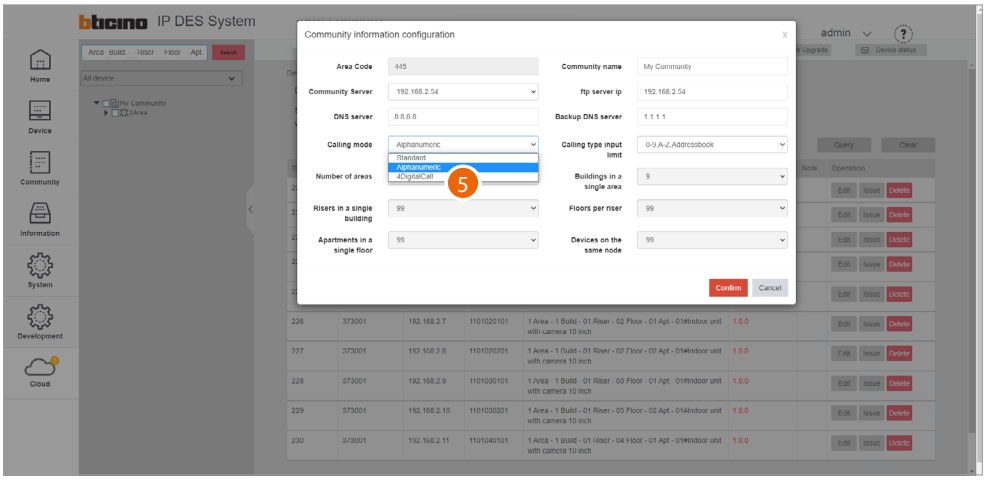
1. Select device/device management



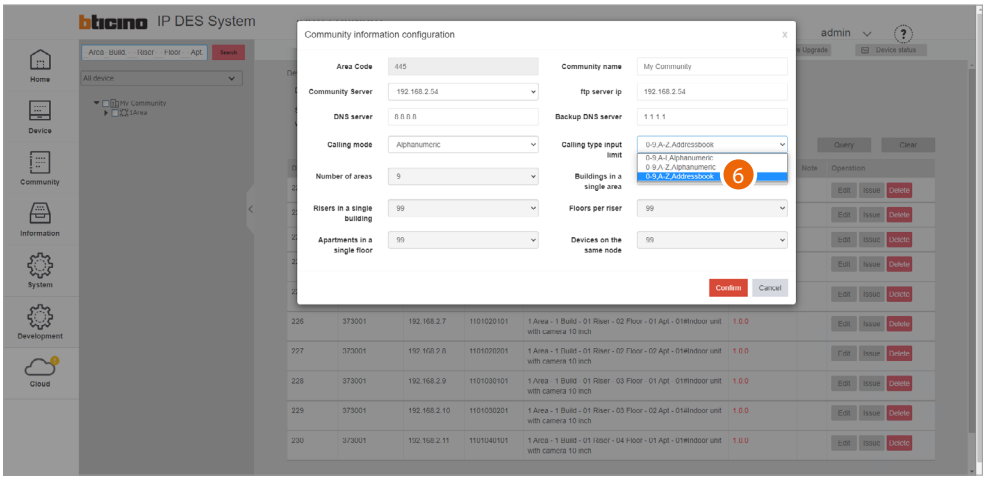
2. Right click the Community
3. Click to select the command



4 Click to modify the call mode



5. Select the alphanumeric mode

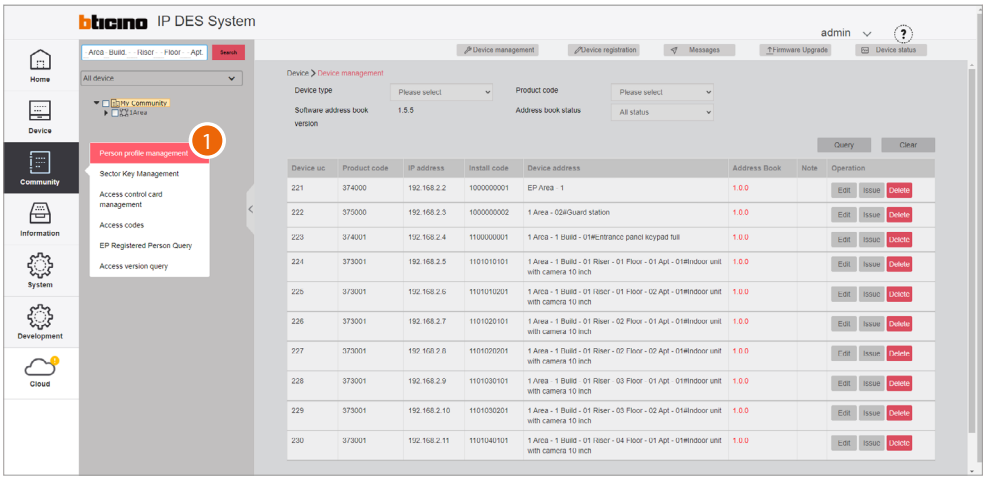


6. Select address book as entry type

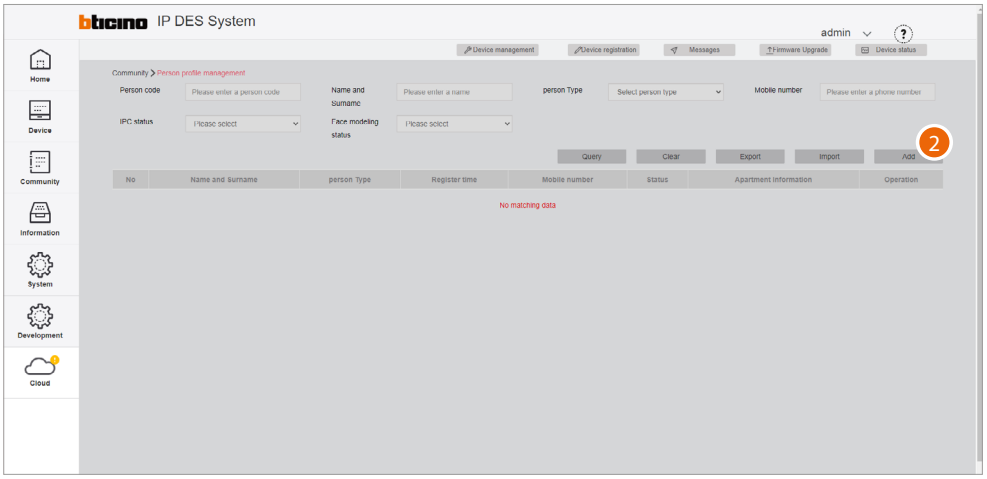
After sending the configuration to the DES server, it will be possible to call IUs using custom names (aliases). When changing the name of a GS or EP, this will be identified with this name on the receiving device when the call is made.

NOTE: *This alias format (Address Book) is not supported by entrance panels 374001/03*

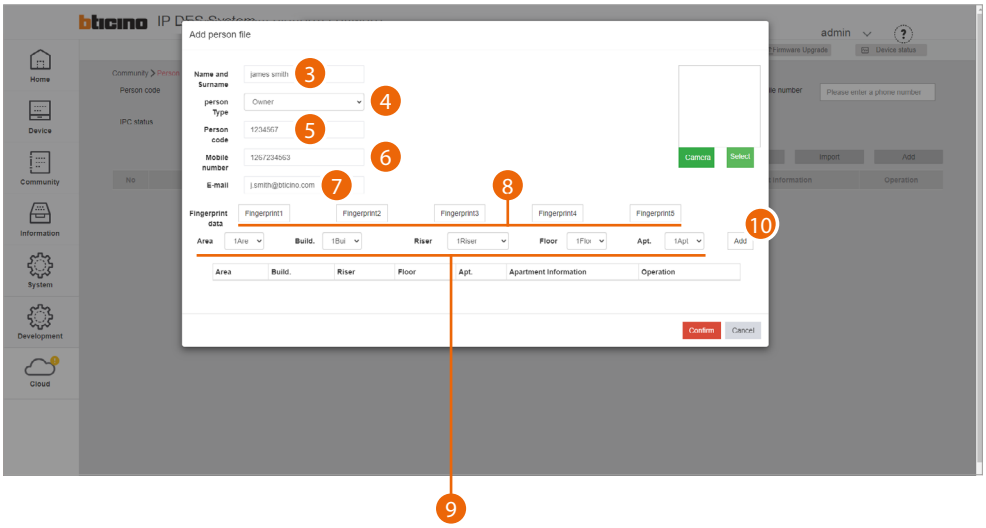
Now it is possible to add community people and give them permissions to access the structure. Depending on the type of person, different access permissions may be assigned, see Person profile management.



1. Select Community/Person profile management



2. Click to create a new person



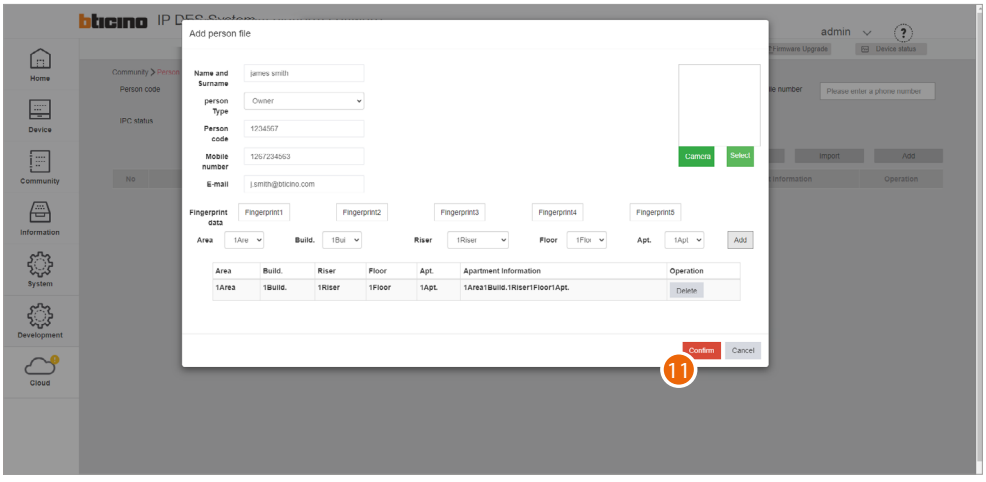
3. Enter the name and surname of the person
4. Select the type of person

Note: *some parameters may change depending on the type of person*

5. Person code
6. Enter the telephone number of the person
7. Enter the email address of the person
8. Register a fingerprint

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 to access the community, this must be registered; see Access control card management

Saving of passwords

Installer passwords are generated automatically (with random digits) and uniquely for the two types of devices:

– posti esterni (a 6 cifre)

– posti interni e centralini di portineria (a 4 cifre).

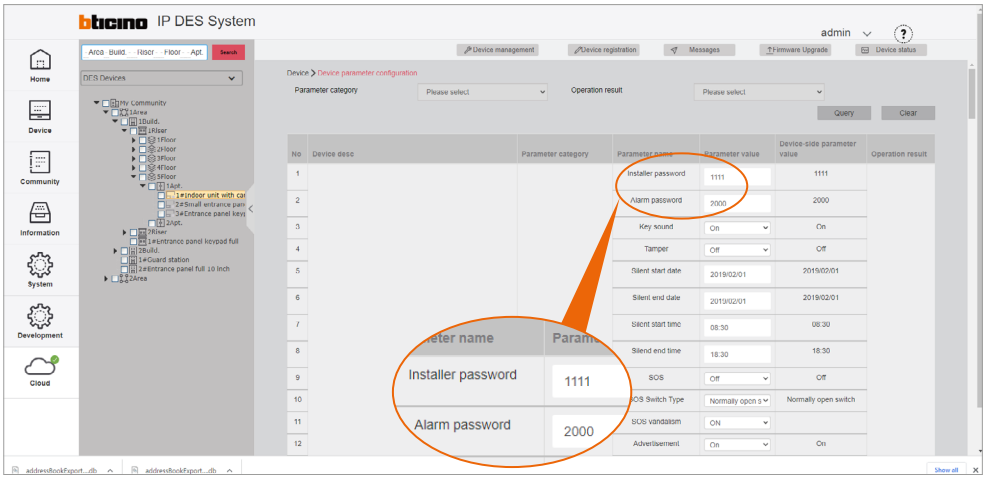
Con la stessa modalità viene generato anche il codice di accesso per apertura serratura dei posti esterni.

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

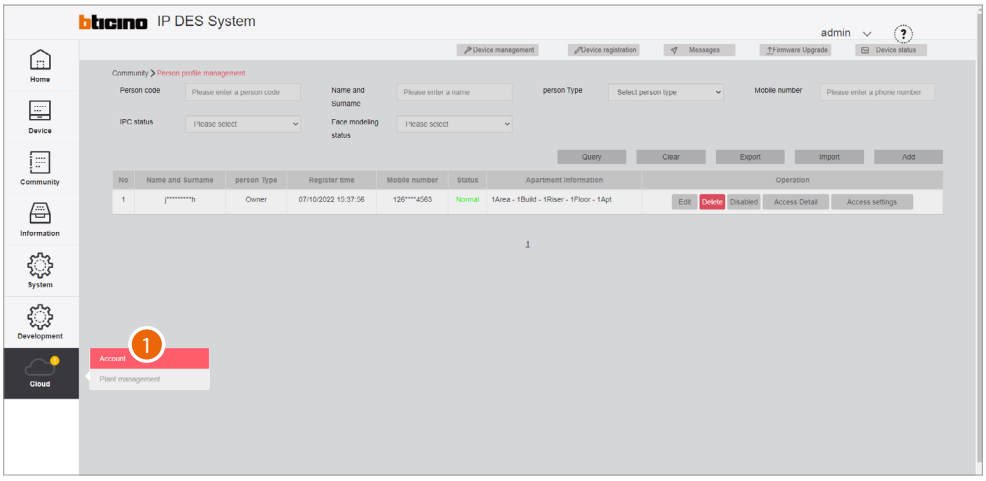
.....

1. Write down the passwords in a safe place that is always accessible.

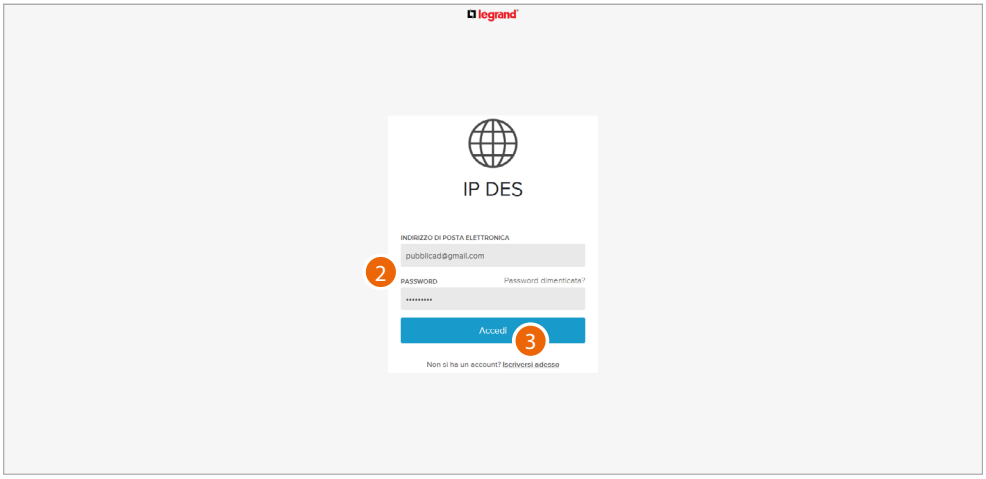
Registration of the community on the Installer's Cloud

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:

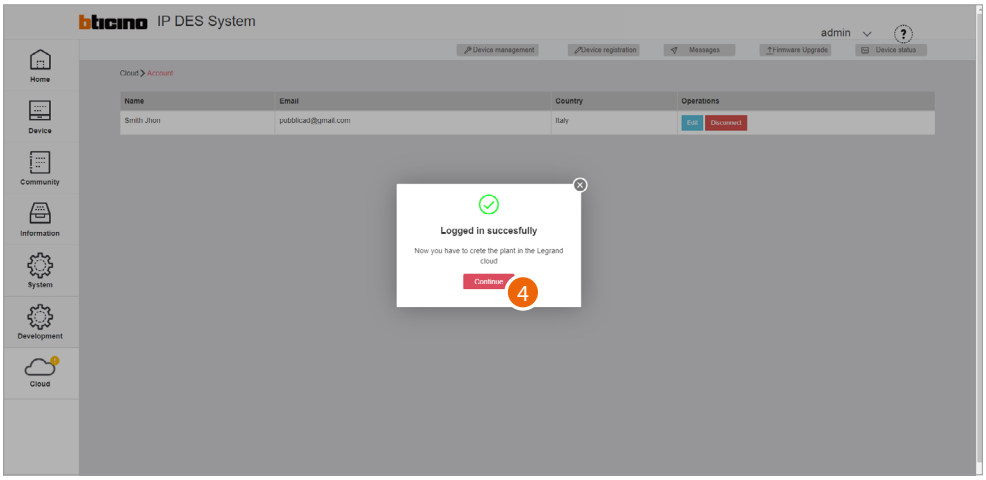
- have greater security in the event of local data loss
- associate the Home+Security app to the IU, for remote management of the video door entry system



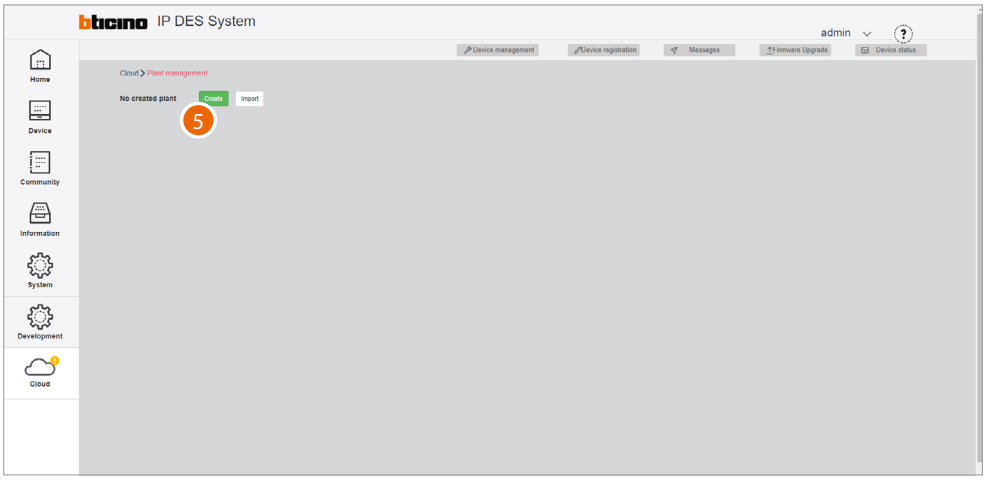
1. Click to complete the Installer's Cloud authentication process



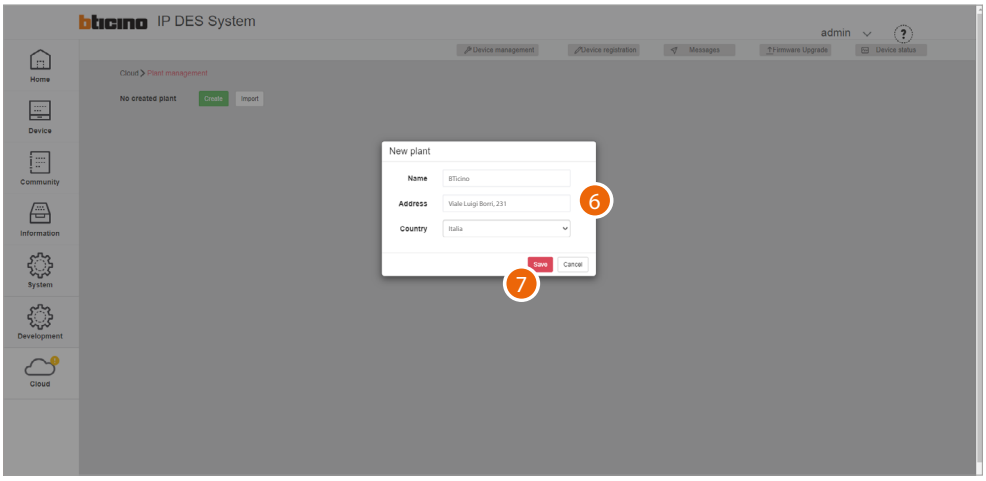
2. Enter email and password
3. Click to access



4. Click to confirm

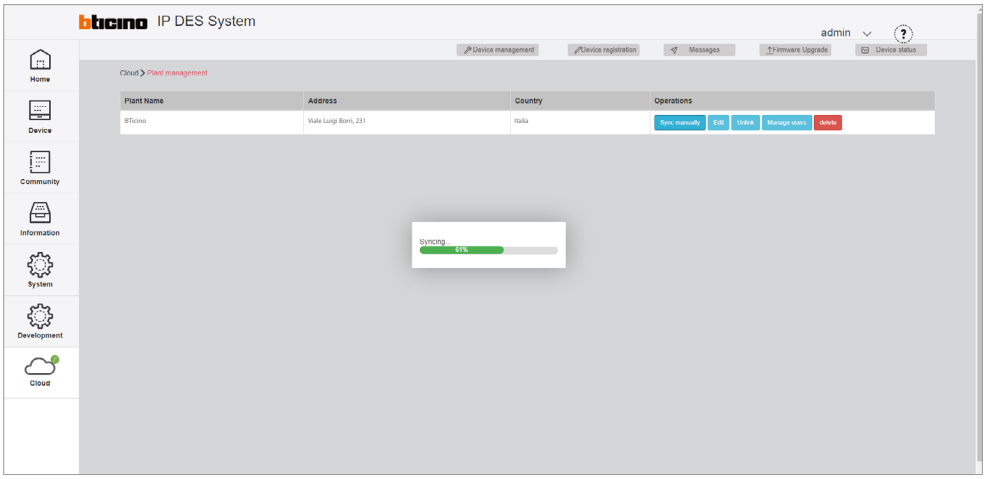


5. Click to create a new Plant



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

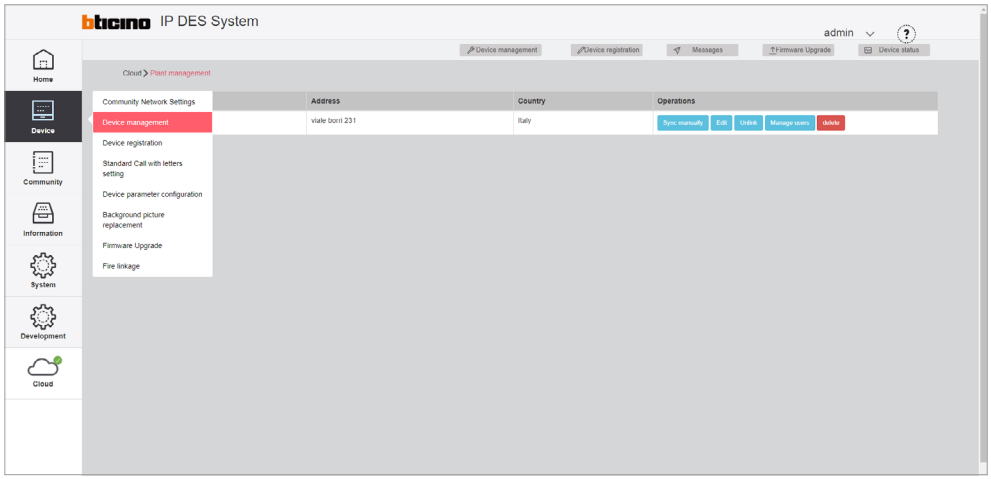
The plant is automatically synchronised



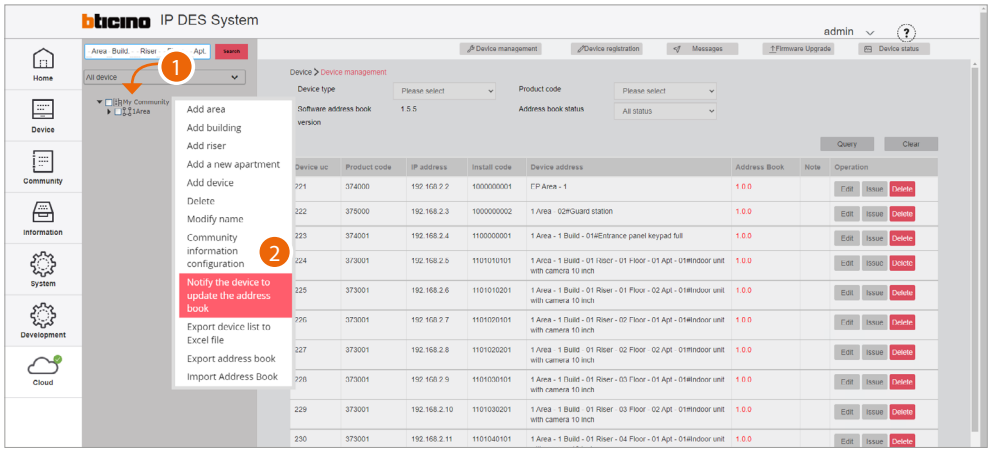
Once created, the plant remains available on the cloud.
If disconnected (unlink button), it can be retrieved from the cloud using the **Import a Plant** function.
If **deleted**, it will also be deleted from the cloud.

Notifying of the address book to the DES Server

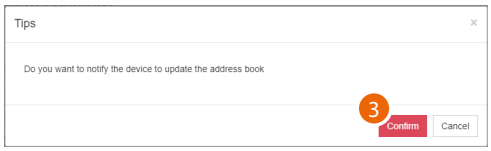
After creating the structure and configuring the virtual devices, it will be necessary to notify the address book to the system, therefore "instructing" the system to use this configuration.

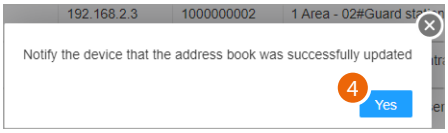


1. Select device/device management



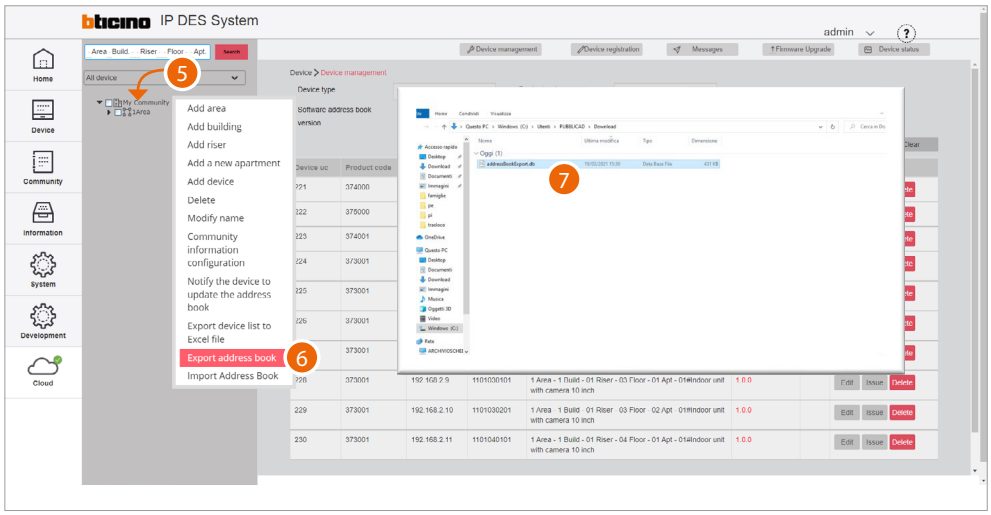
1. Click Community with the right mouse button: a drop-down menu will appear
2. Click to update the system address book





3. Click to confirm
4. Click to finish

The address book is now saved in the DES Server. To avoid accidental loss, it is also possible to save it in an archive file.

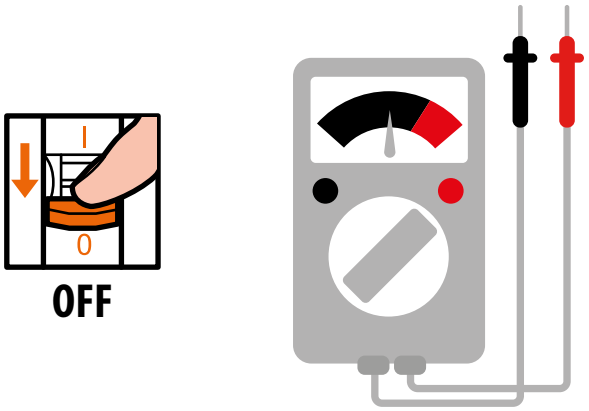


5. Click Community with the right mouse button: a drop-down menu will appear
6. Click to export the address book to a file
7. The file will be saved in the download folder of your computer

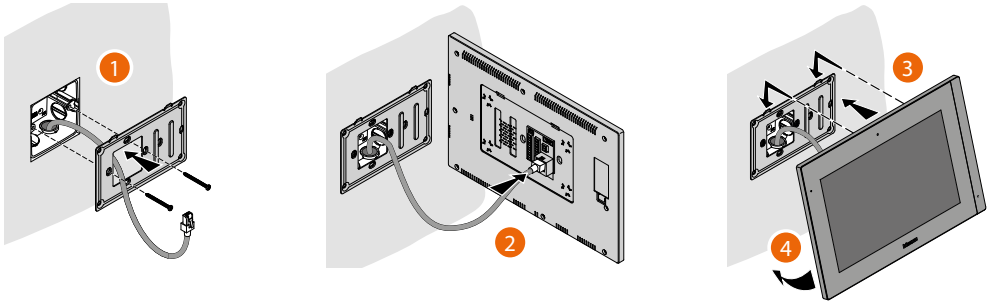
Installation of the devices

To transfer the configuration to the devices, these must be installed and powered

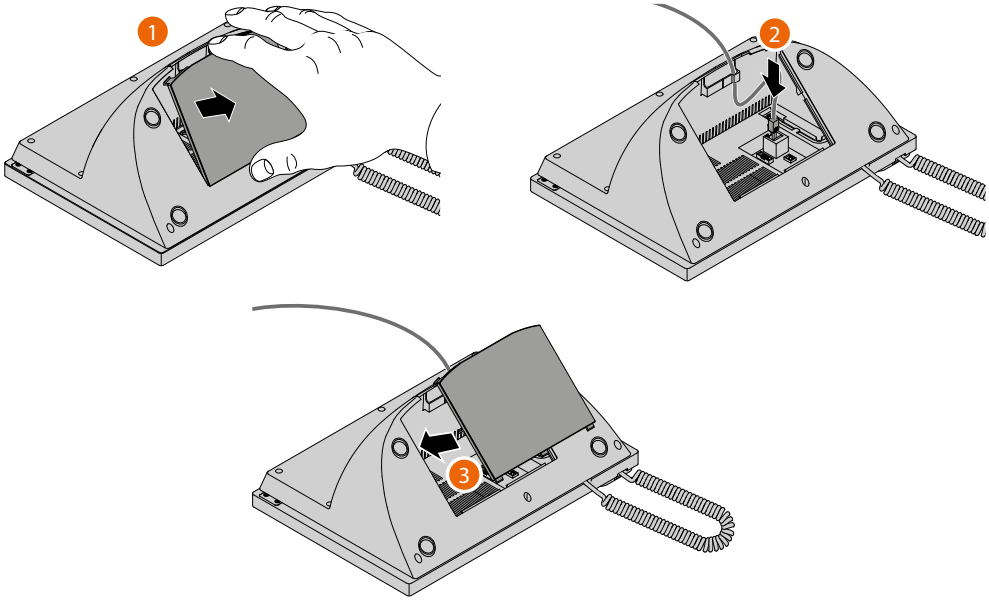
Switch off the power supply to the system and check that there is no voltage



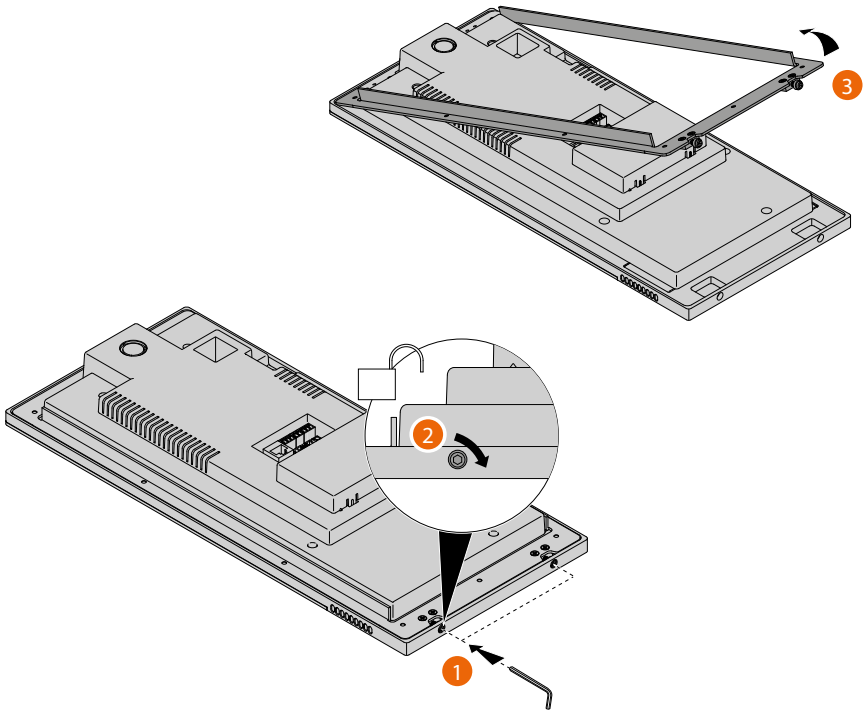
Install the devices

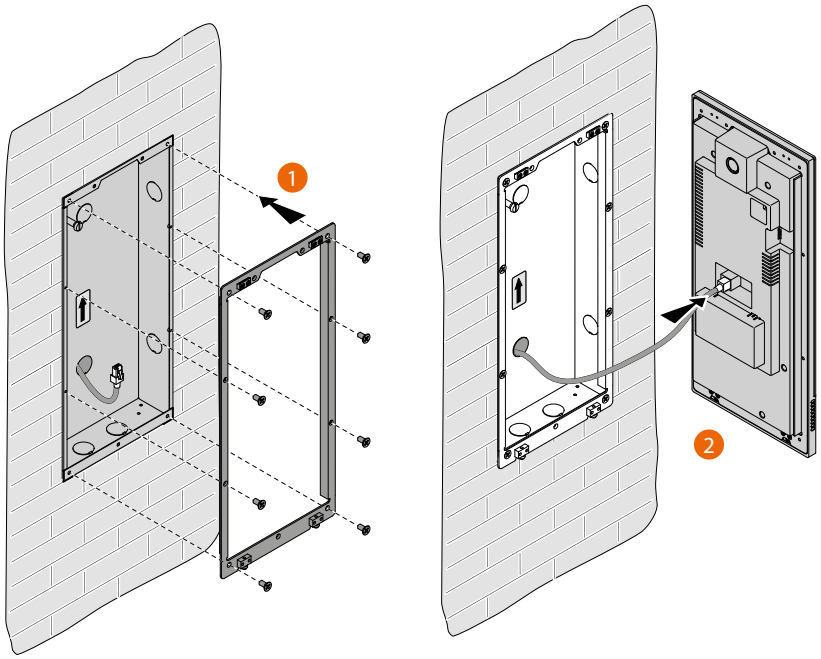


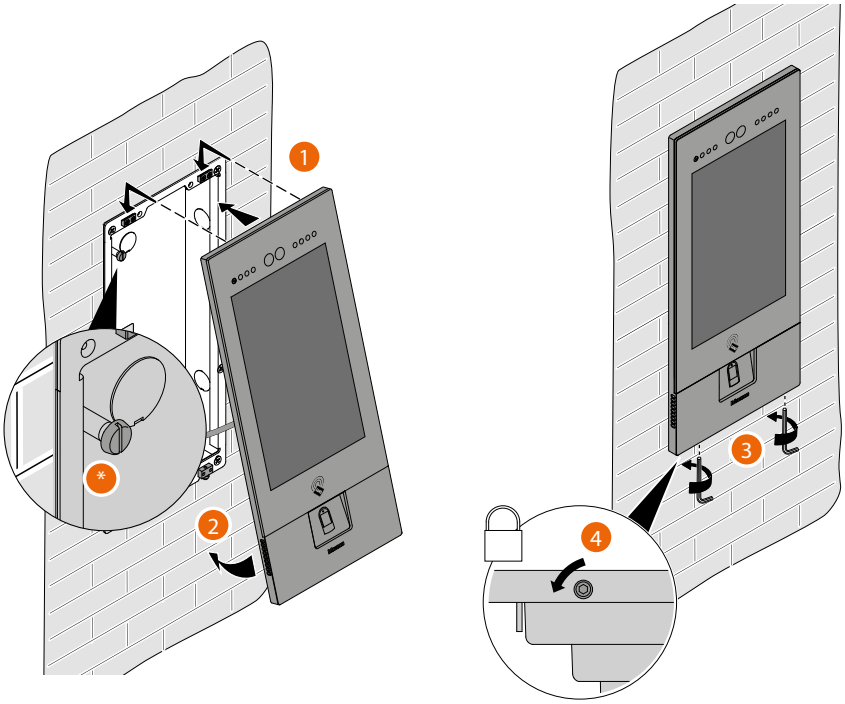
The RJ45 cable must be at least 200 mm long



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 sending an alarm to the guard station.

***Warning**: please note that the EP installation shown is representative of all EPs.*
For more details, see the specific instructions in the package

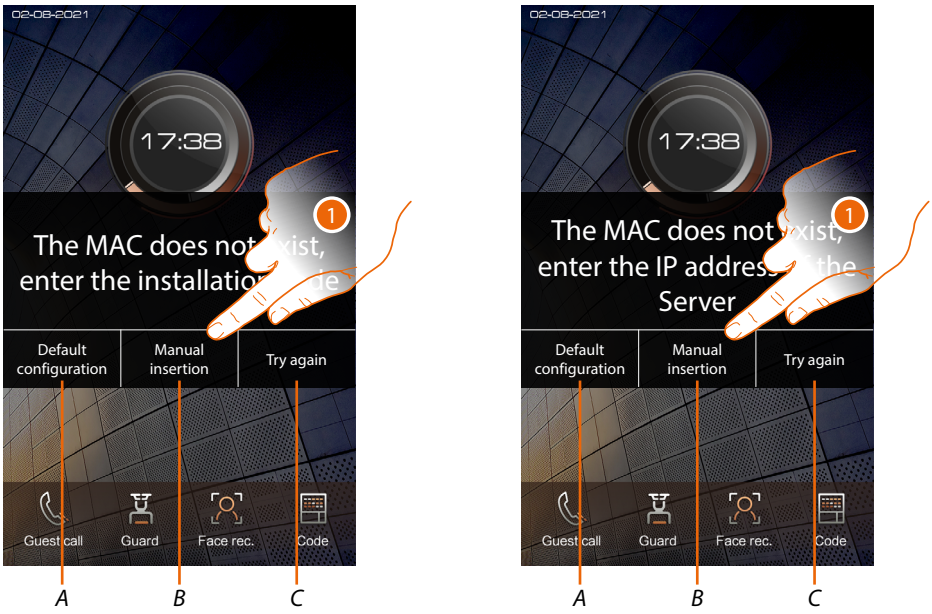
Reconnect the power supply

Activation of the devices

Thanks to the previously entered MAC address, once powered, the device checks that a configuration (address book) is available on the DES Server, and if so acquires 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.



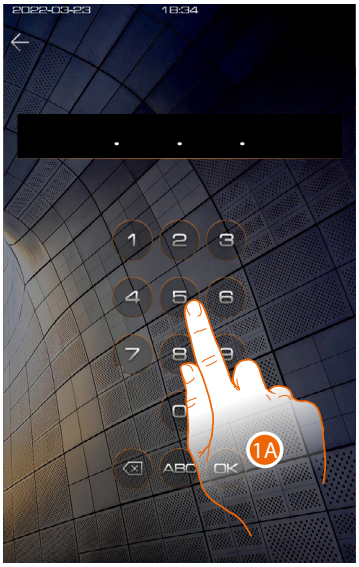
A Not to be used

B Button allowing 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 Community Network Settings, to display the installation code, see Installation code*

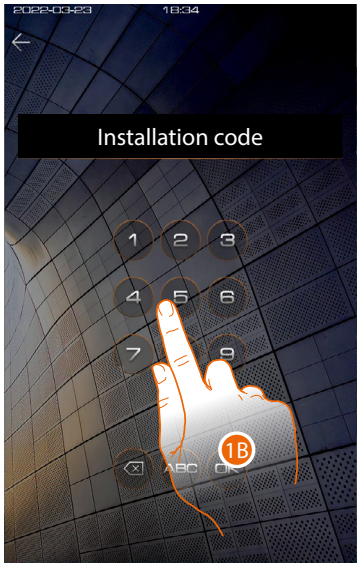
C Button to test the activation of the device

1. Click to manually enter the server IP address or the system access code

IP address



Installation code

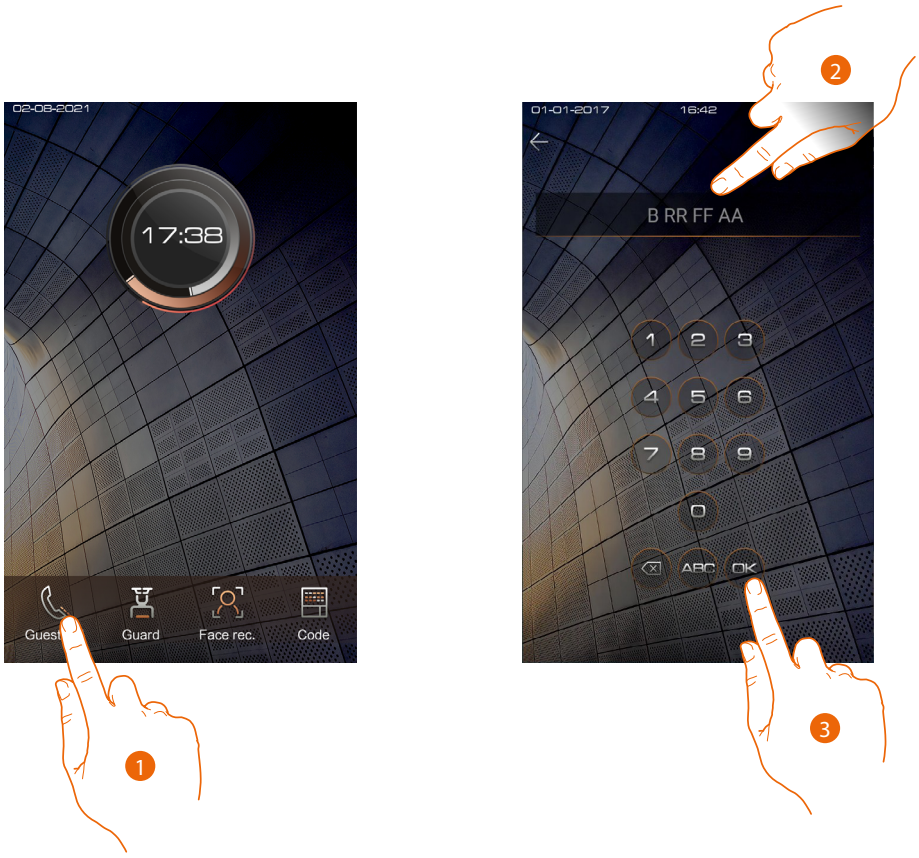


1A. Enter the IP address of the server

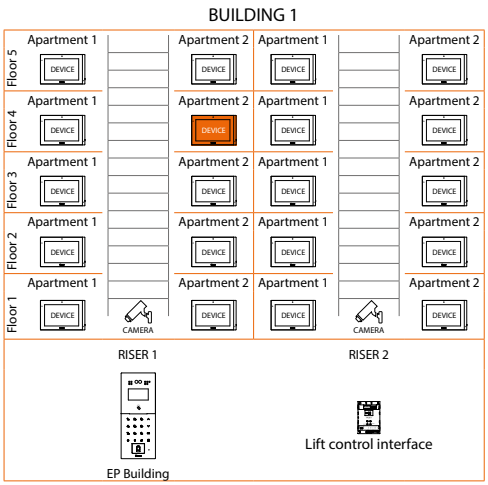
1B. Enter the installation code

System test

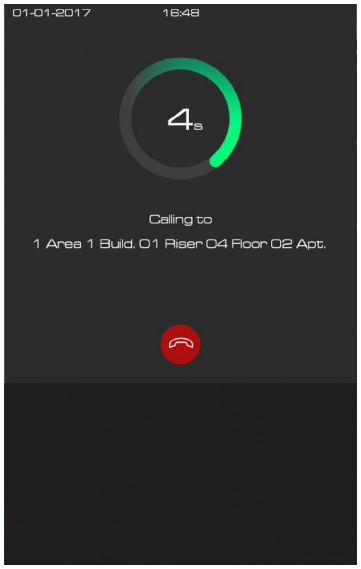
It is now possible to test the system, for example by making a call from the EP



1. Touch to make the call
2. Enter the IU address

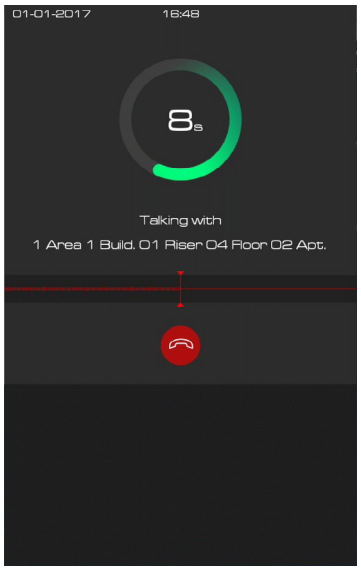


3. Touch to send the call



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. Tap to capture an image of the screen

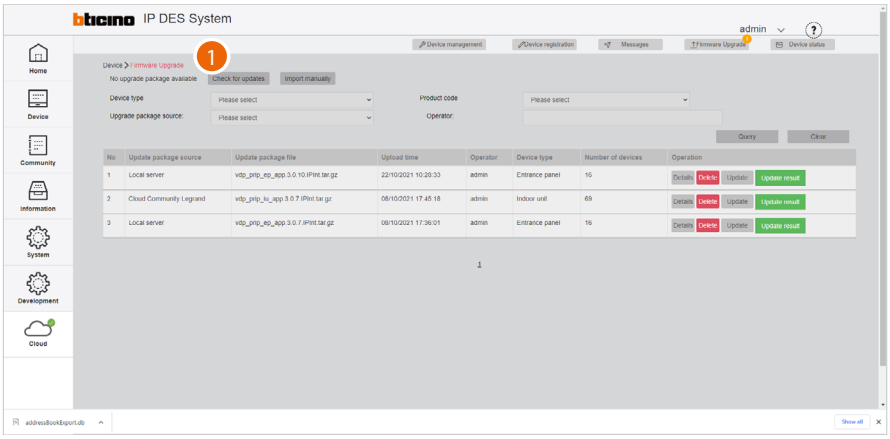
A confirmation message appears.

6. Touch to open the EP door lock

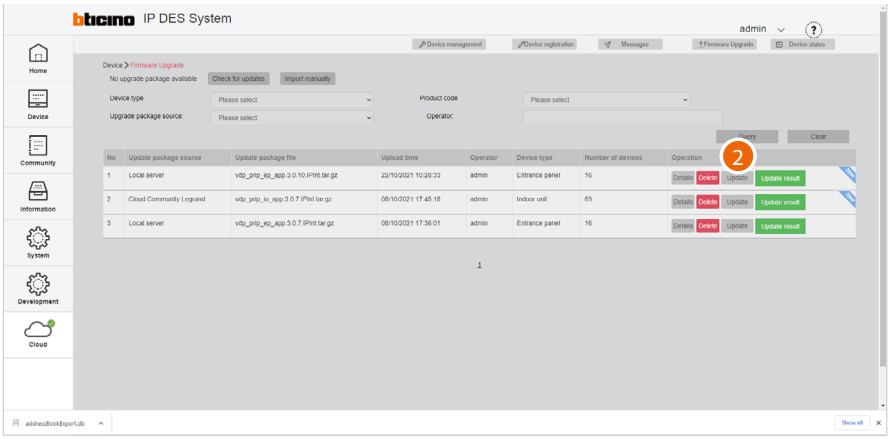
A confirmation message appears

7. Tap to adjust the volume
8. Touch to end the call

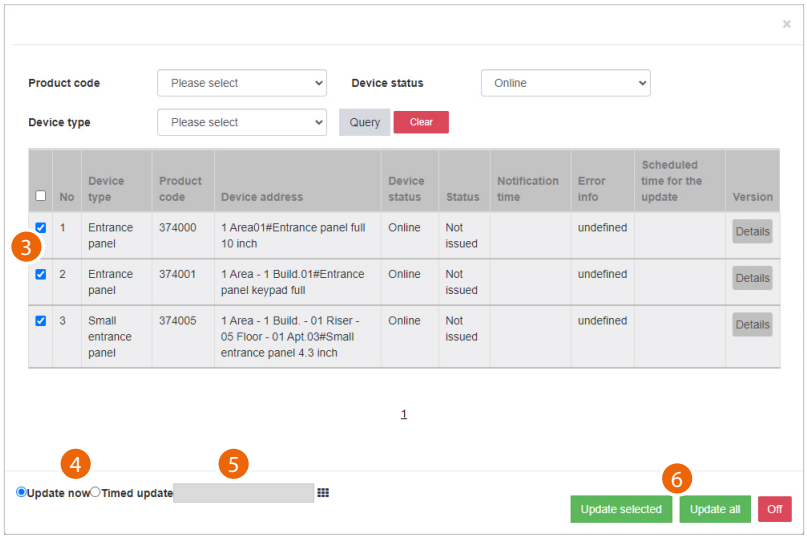
Update of the devices



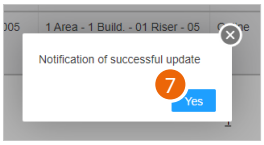
1. Click to check for updates on the cloud. If there are updates, these will be downloaded and available for installation
   NOTE: *firmware updates will only be downloaded if the last installed updates have already been deleted: the page must be empty.*



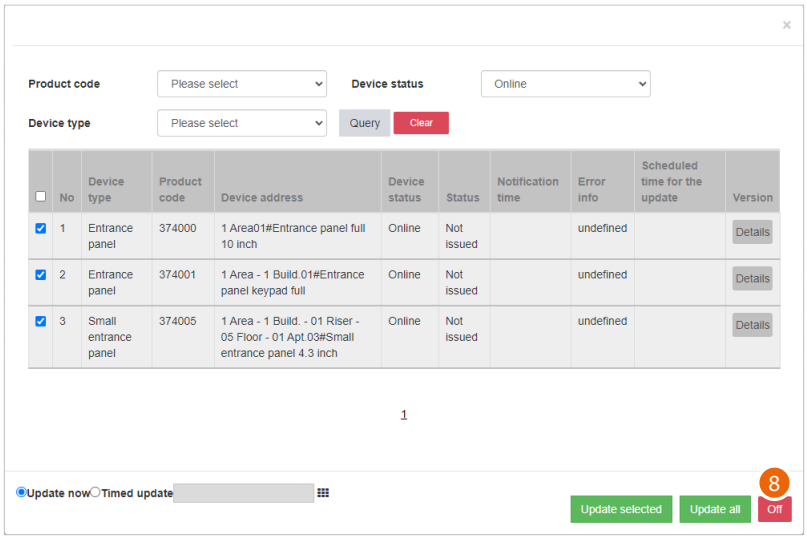
2. Click to send the update to the plant



3. After using the filters to display the relevant devices, select them
4. Decide whether to perform the update immediately or
5. Schedule an update, setting the date and time
6. Start the update for the selected devices or for all the devices



7. Click to finish



8. Click to close the panel

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

SYSTEM

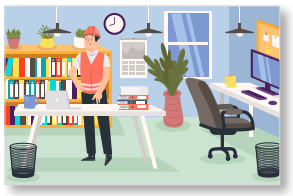
Step 01 Creation of a list of all the devices present with their corresponding item codes and MAC ADDRESSES, and recovery of the SD from the system, to take to the office

Step 02 Community VLAN network creation

Step 03 Community structure definition

Step 04 Community structure creation

OFFICE



Step 05 Device MAC address registration

Step 06 Community customisation

Step 07 Saving of passwords

Step 08 Registration of the Community on the installer's Cloud

Step 09 Forwarding of the address book to the Server DES

Step 10 Take the DES server back to the system

Step 11 Setup of the fixed DES server address on the system router

SYSTEM

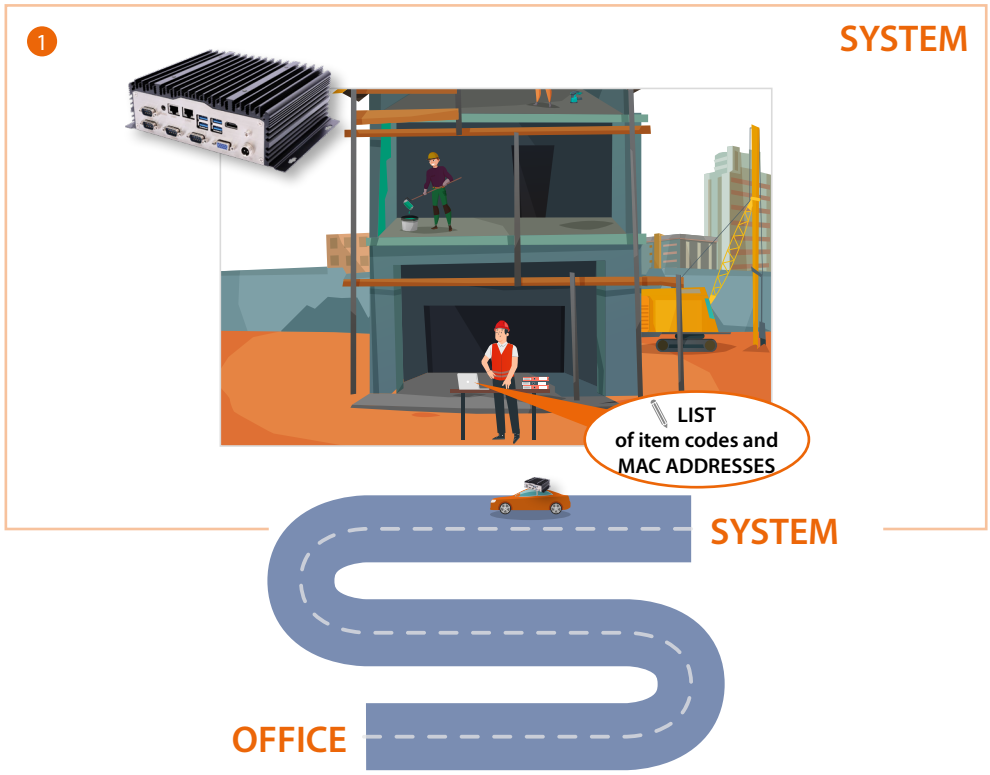
Step 12 Installation of the devices

Step 13 Activation of the devices

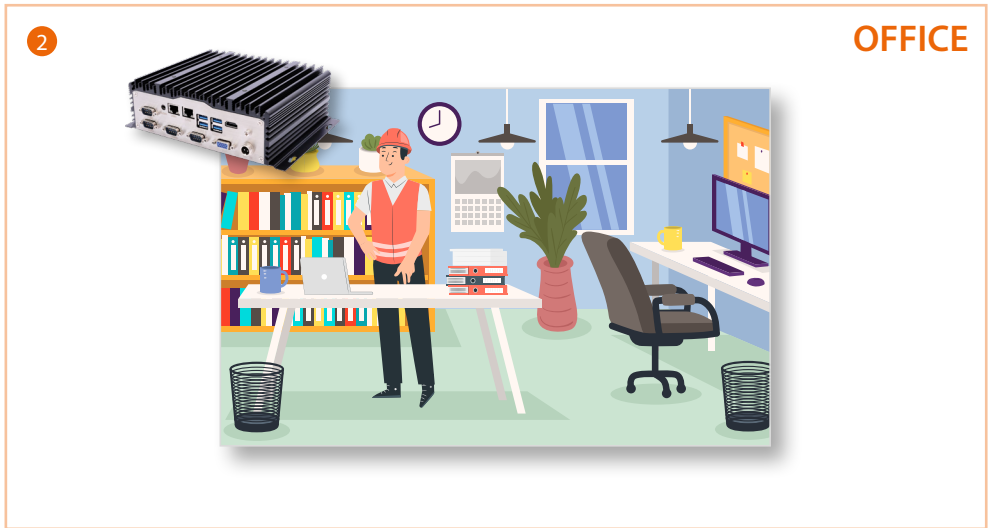
Step 14 System test

Step 15 Update of the devices

Creation of a list of all the devices present with their corresponding item codes and MAC ADDRESSES, 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.



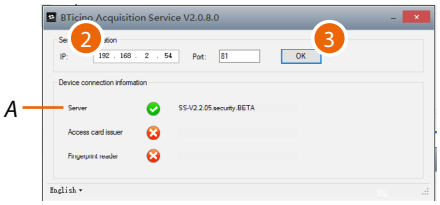
When back at the office, connect the SD to the LAN network and start the configuration.

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

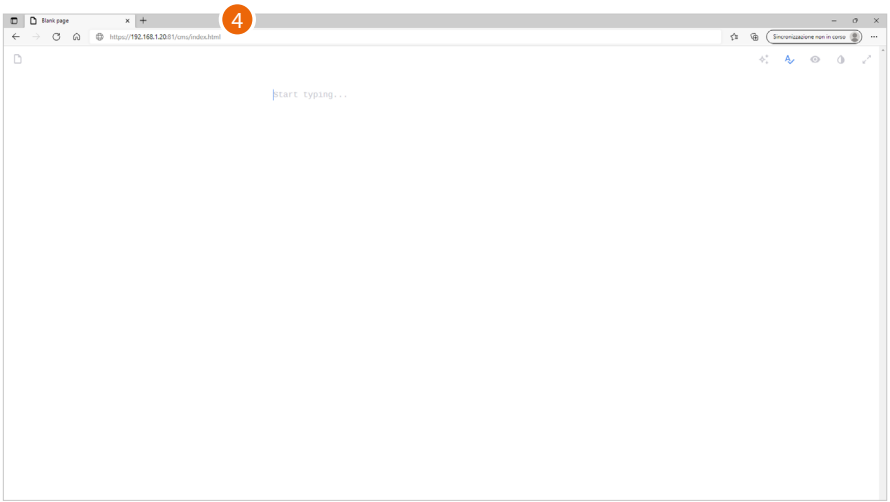
The following screen appears



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 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 MAC address identification (method 2).

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

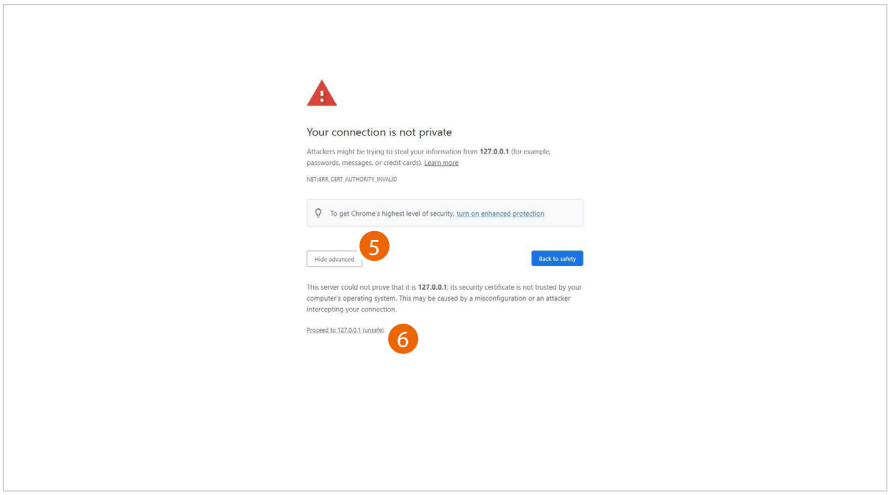


4. Open the browser and enter the http address of the DES Server:

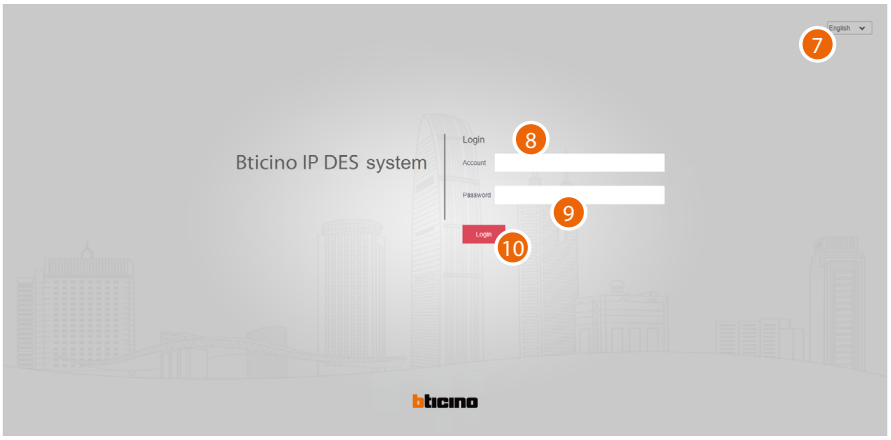
https://SD IP address:81/cms/index.html

***Note**: use Crome/Edge browser and a screen with resolution 1920x1080*

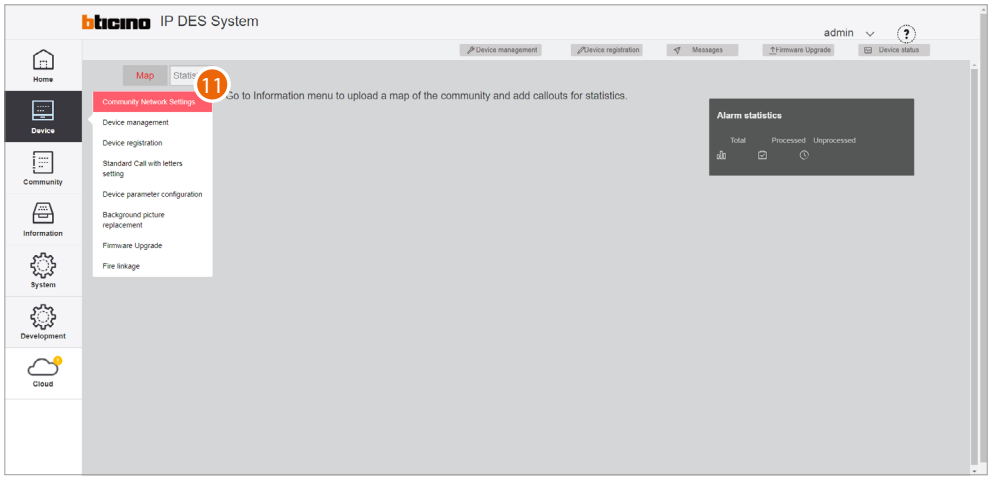
In some cases, the browser may consider the page to be unsafe.



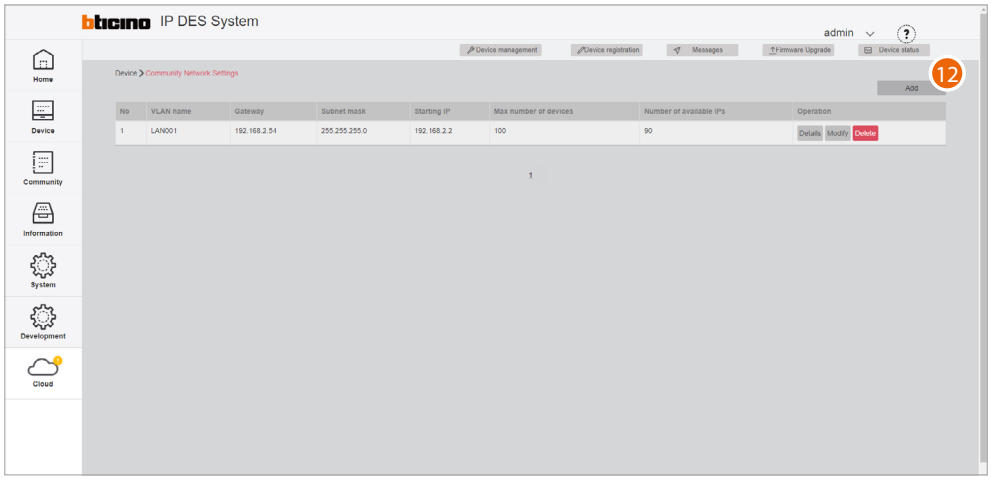
5. Click to display the advanced options
6. Click to ignore the warning and proceed



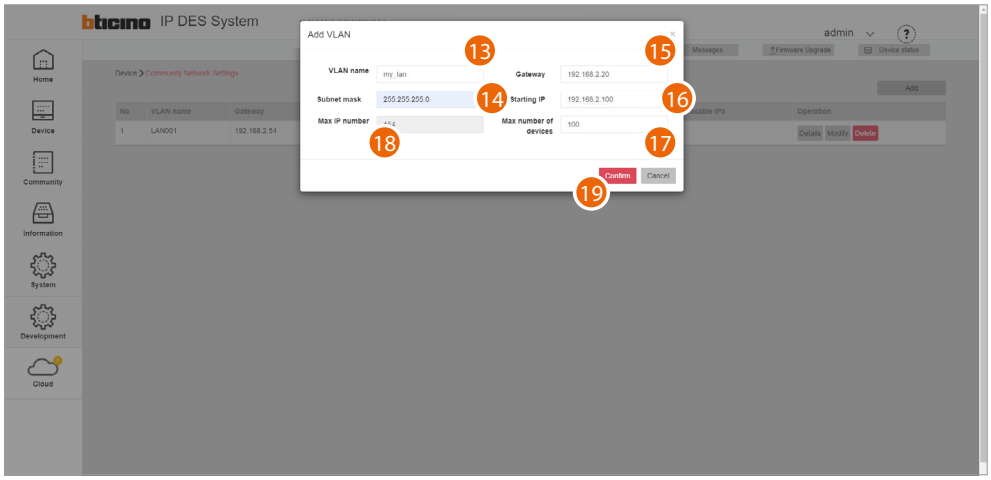
7. Select the interface language
8. Enter the login name (default admin)
9. Enter the password (default 123456)
10. Click to confirm



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

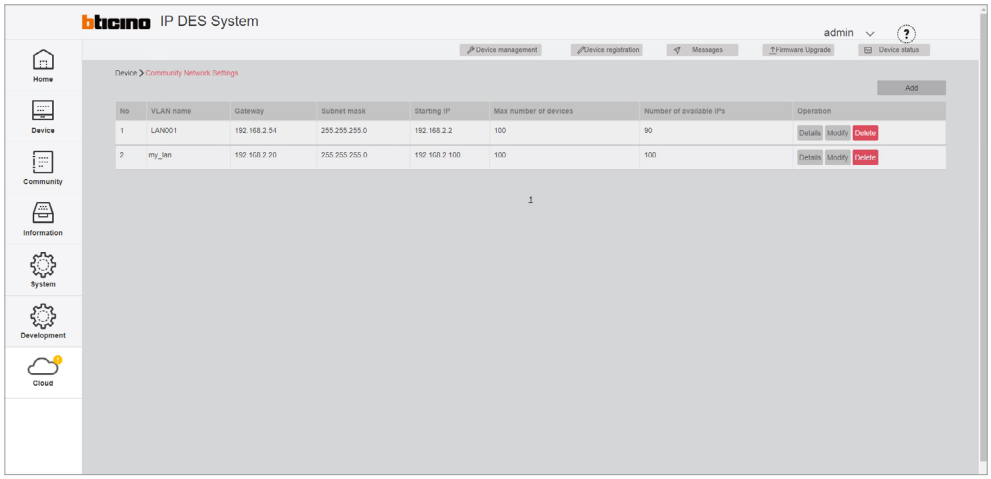


12. Click to create the community VLAN network



13. Enter the name of the community VLAN network (letters and numbers without space)
14. Enter the Subnet mask address
15. Enter the fixed IP address of the DES Server given to you by the network administrator
16. Enter the starting address from which the IP addresses of the IP devices will be generated, see Assignment of IP address range based on the number of video door entry devices
17. Enter the number of IP devices that will be part of the Community
18. It displays the maximum number of IP devices that can be installed based on the previously entered data
19. Click to confirm

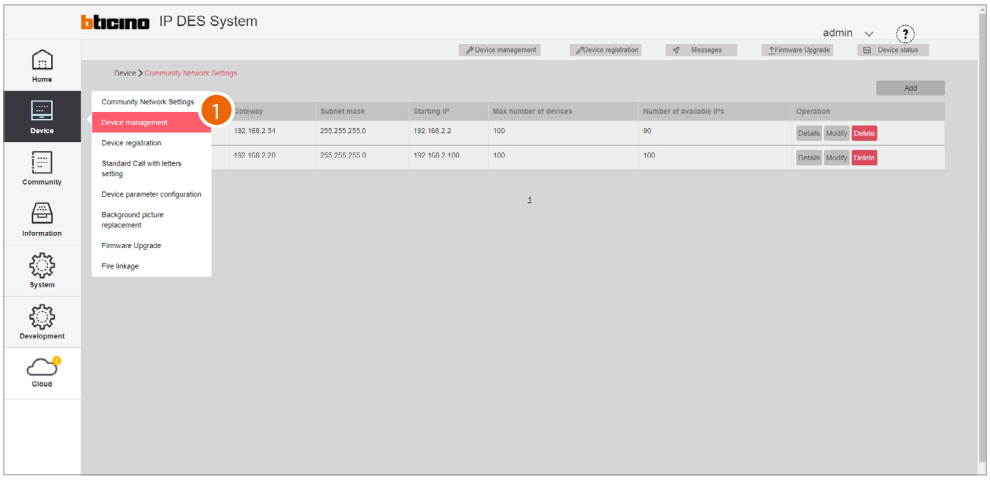
***NOTE**: the parameters (13 to 1 8) must match those found on the system.*



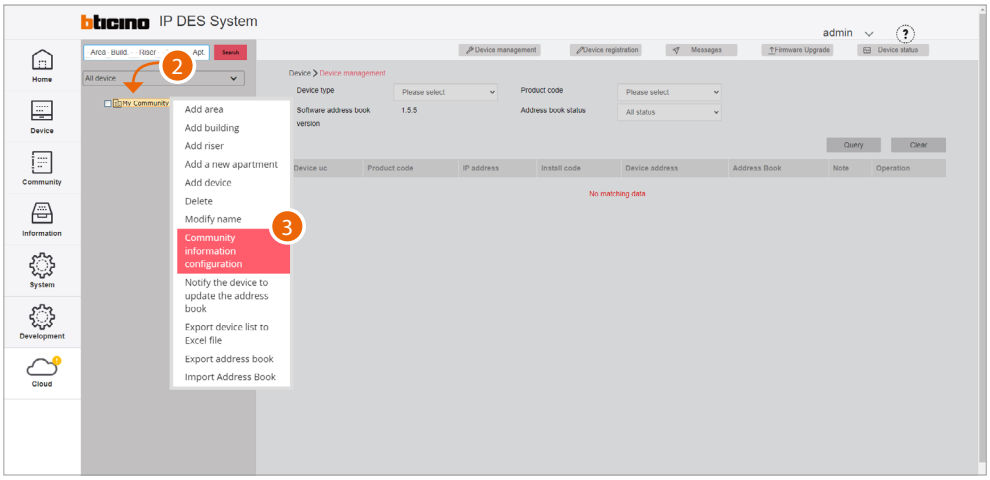
The community VLAN network has been created

Community structure definition

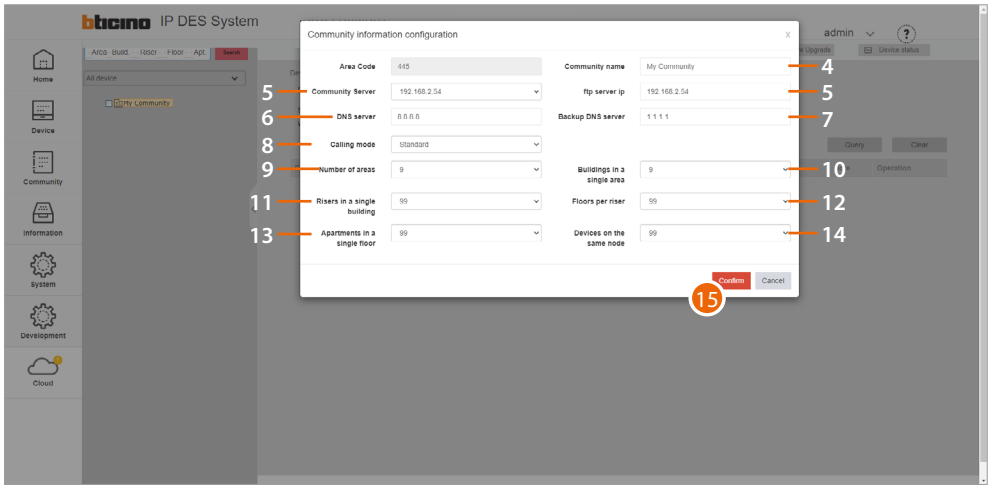
It is now necessary to define parameters like number of Areas, Buildings, Risers and so on, as well as other details that will define the structure of the Community.
In this section, it is also necessary to define the type of call that will be used for all Community calls.



1. Click to enter the Community configuration section



2. Click the Community with the right mouse button: a drop-down menu will appear with the commands for its configuration
3. Click to open the pop-up window with the parameters that define the Community structure



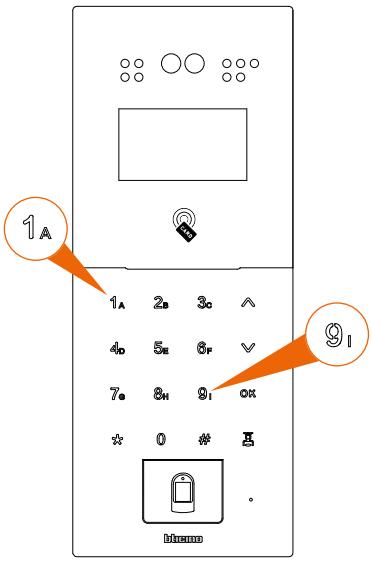
4. Change Community Name
5. Selects the fixed IP address of the Community DES Server
6. Change the address of the DNS server (unless there are special requirements, we recommend to keep the default address)
7. Change the address of the backup DNS server (unless there are special requirements, we recommend to keep the default address)
8. Selects the type of call to be used for the system: Standard or Alphanumeric.
   When selecting Alphanumeric, it will also be necessary to select a mode, "0-9, AZ" or "0-9, AI", depending on the type of EPs installed in the Community.
9. It displays the maximum number of Areas for your Community (default 9).
10. It displays the maximum number of Buildings that an Area can have (default 9).
11. It displays the maximum number of Risers that a Building can have (default 99).
12. It displays the maximum number of Floors that a Riser can have (default 99).
13. It displays the maximum number of Apartments that a Floor can have (default 99).
14. It displays the maximum number of Devices that an Apartment can have (default 99).

***Note**: The default values of item 9 through 14 are consistent with the example shown in this document, and therefore do not need to be changed.*
For other more complex structures, see ***Community information configuration****.*

***Note**: If even one single EP has an "0-9, AI" type keypad, select the "0-9, AI" option.*

EP with "0-9, AZ" keypad

EP with "0-9, AI" keypad



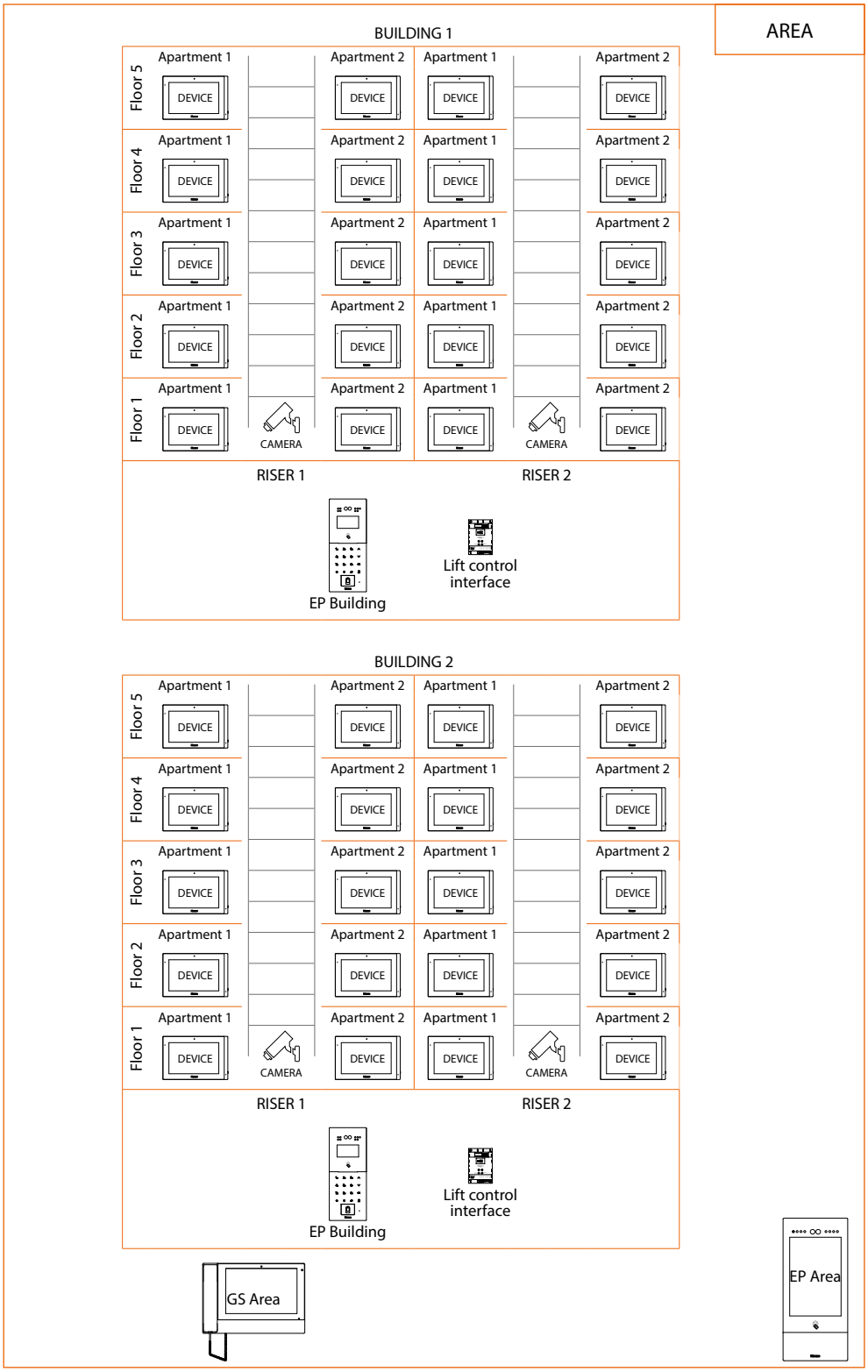
15. Click to confirm

Community structure creation

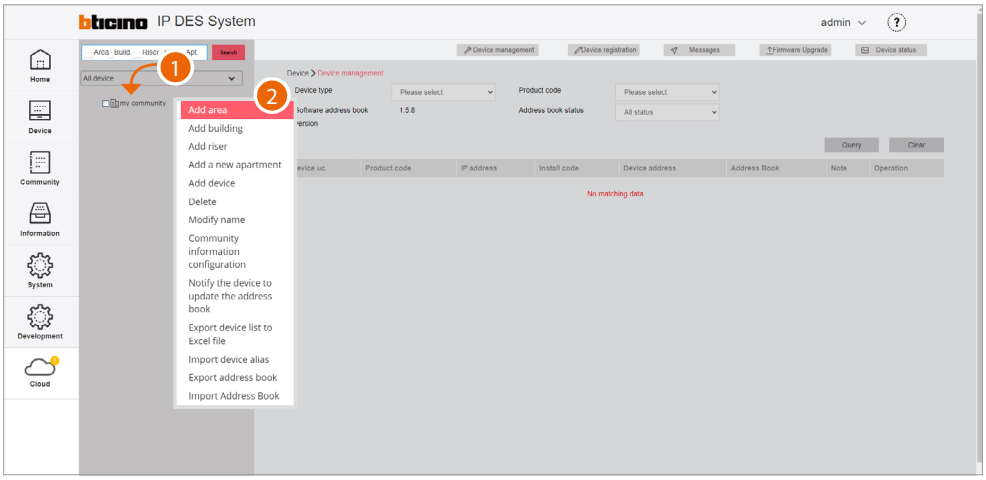
Depending on how your Community is composed, you will need to hierarchically enter:

AREA → BUILDING → RISER → FLOOR → APARTMENT → DEVICE

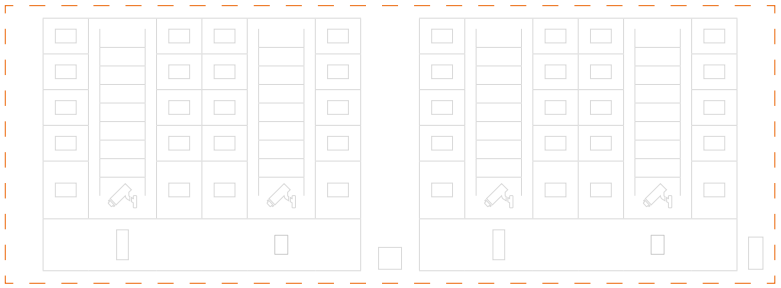
This document will show the creation of a sample structure composed as follows:

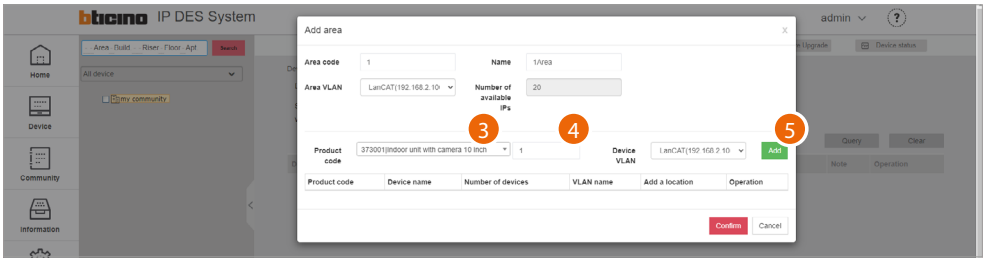


***Warning**: the configuration operations shown below are those required for creating the sample structure. See the Software Manual for all the other possible configurations.*



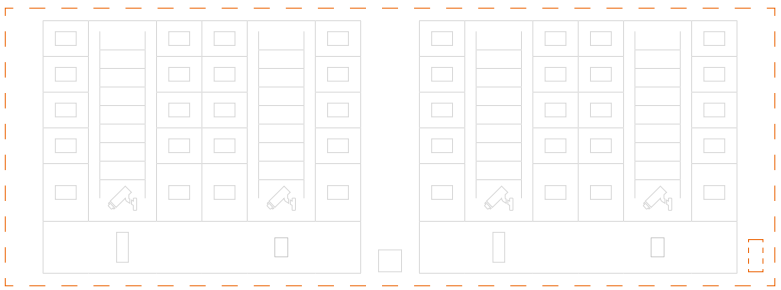
1. Click the Community with the right mouse button: a drop-down menu will appear with the commands for its configuration
2. Click to add a **new Area**

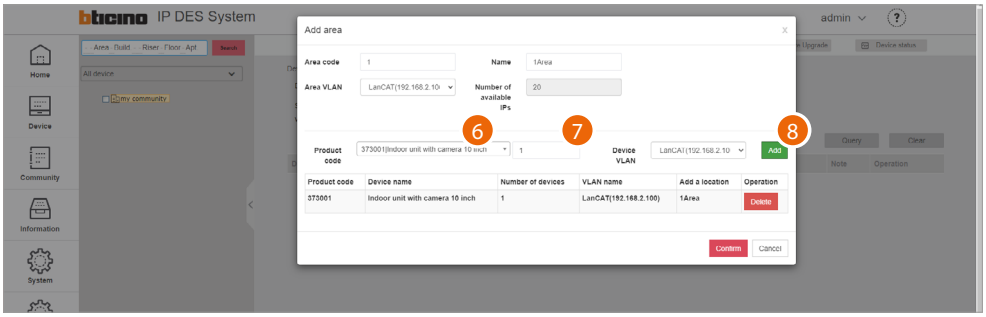




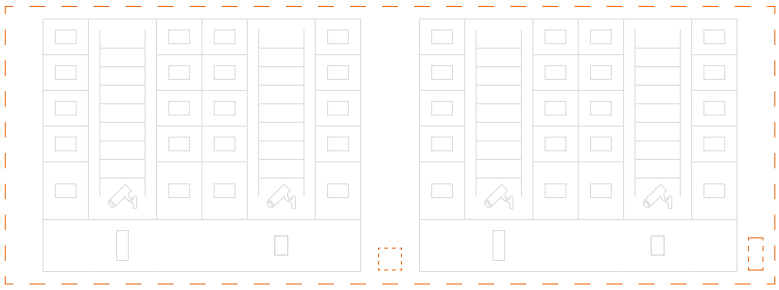
3. Select the Area device (EP Area1)*
4. Select the quantity
5. Click to add

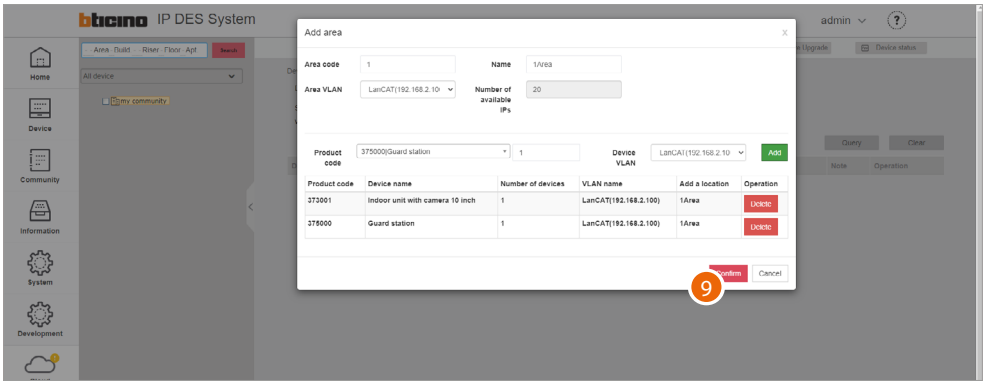
**Nota: prima di procedere con inserimento di un dispositivo ricordarsi di verificare che tutti i parametri del dispositivo rispettino le richieste, vedi Device parameter configuration*



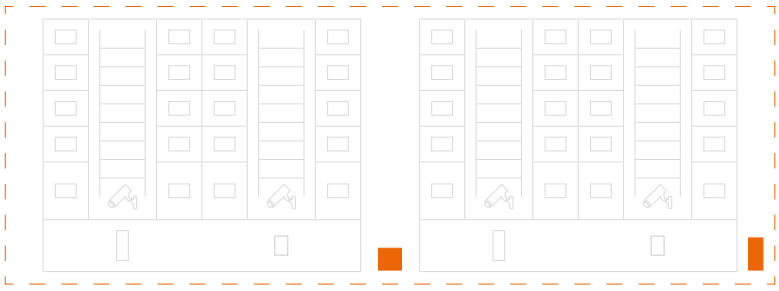


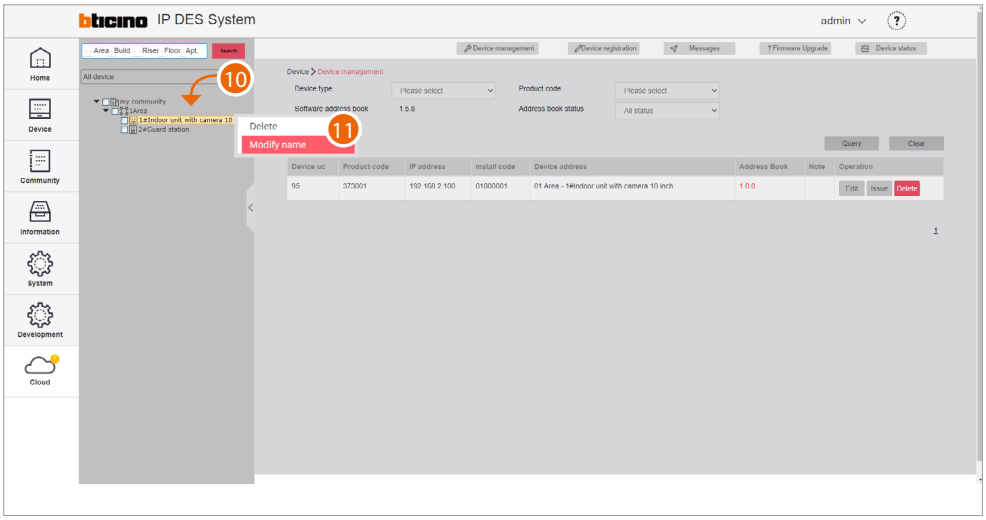
6. Select the second Area device (GS Area1)
7. Select the quantity
8. Click to add





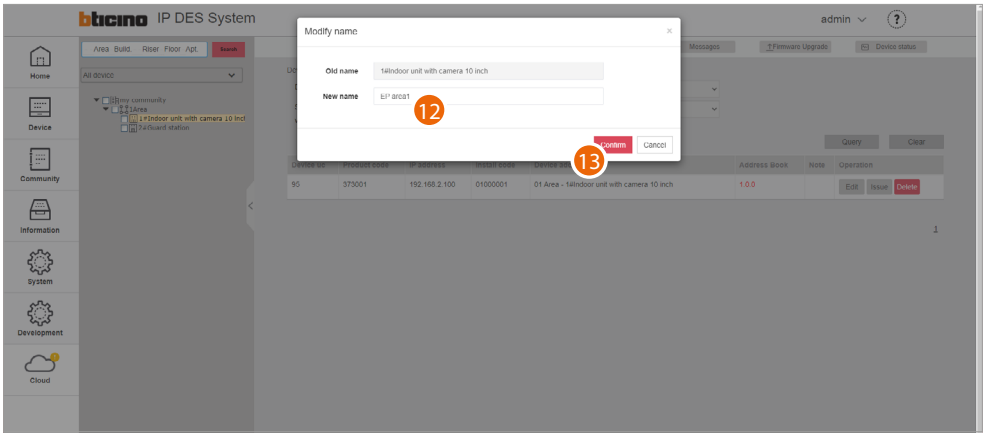
9. Click to confirm



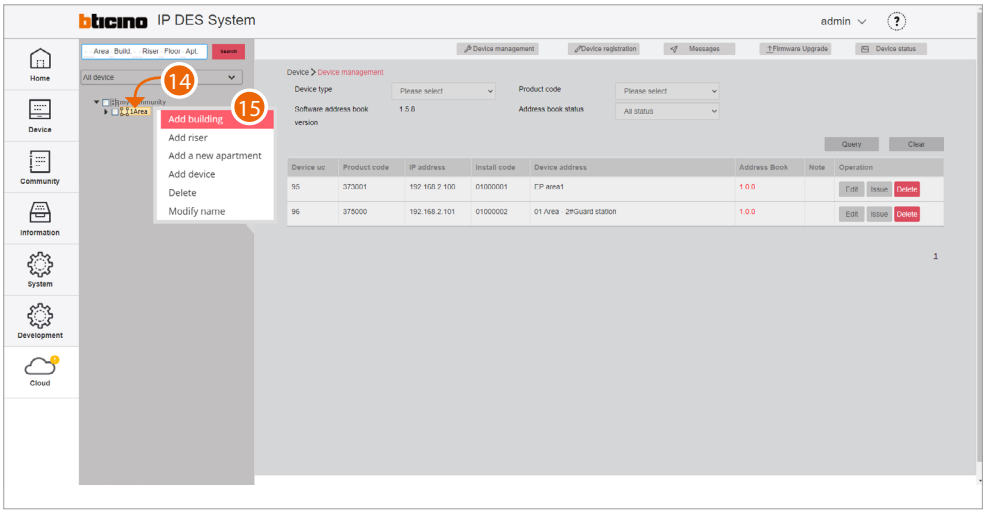


After inserting the devices, you will be able to customize their name

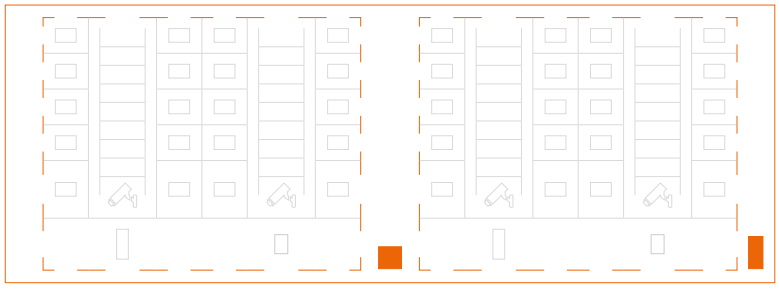
10. With the right mouse button click the device that you want to rename: a drop-down menu will appear
11. Click to open the edit window

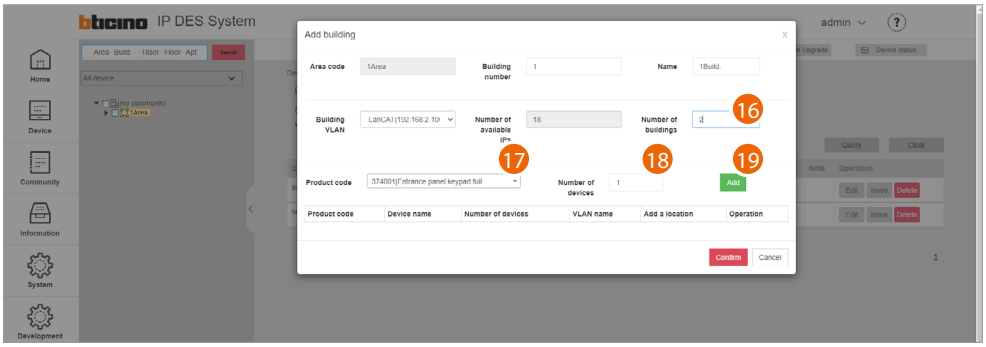


12. Enter the new name
13. Click to confirm



14. Click the Area with the right mouse button. This will open a drop-down menu
15. Click to add the **Buildings**

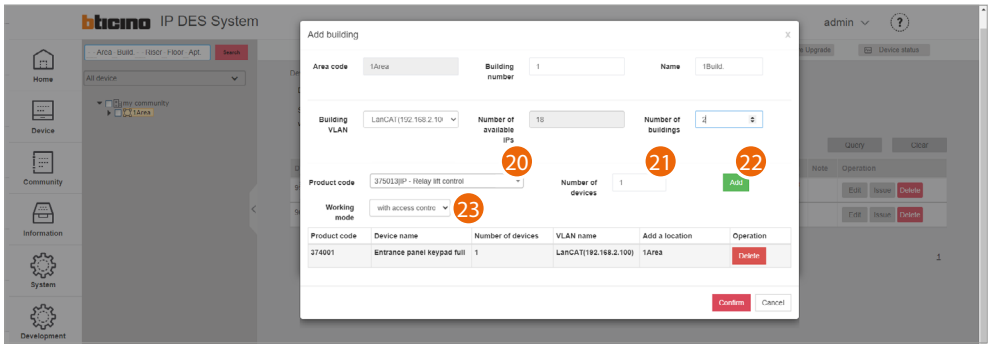




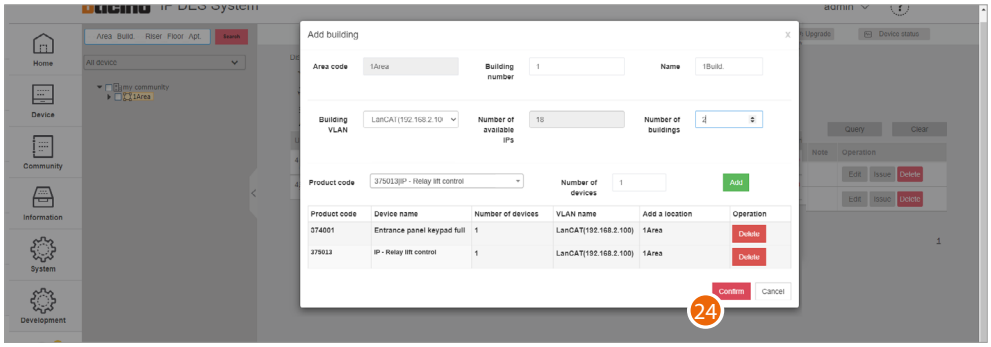
16. Select the number of buildings to add
17. Select the Building device (EP Building)

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

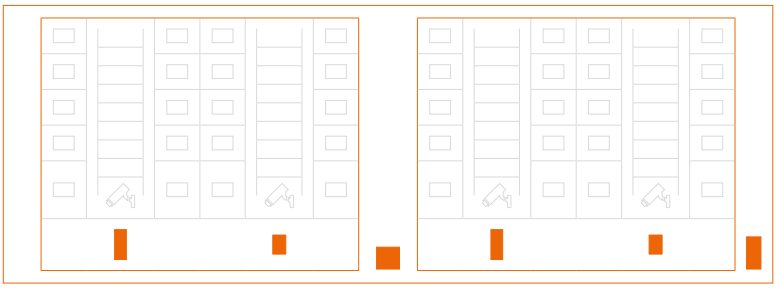
18. Select the quantity
19. Click to add

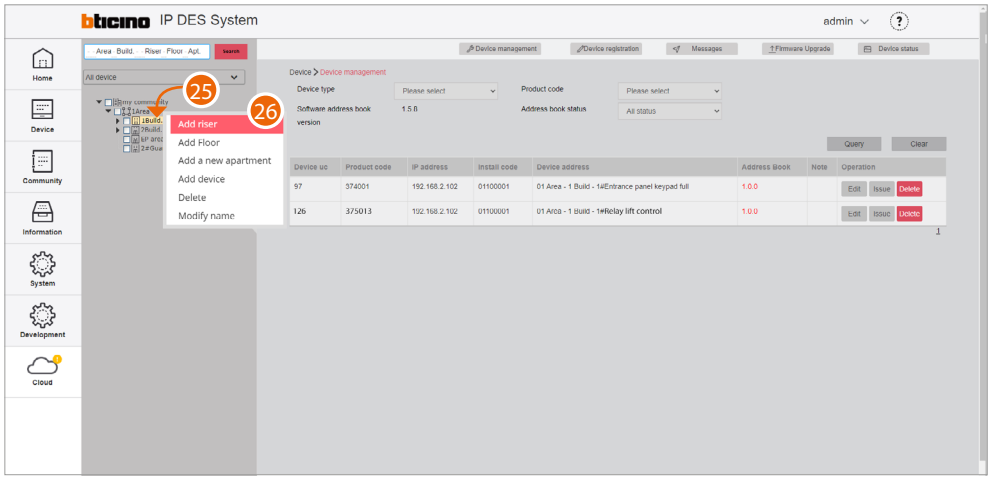


20. Select the device to add (lift control interface with relay 375013)
21. Select the quantity
22. Click to add
23. Select the operating mode:
    - **with access control**: this mode allows to set up an exclusive call to a specific floor (e.g. only go to the third floor)
    - **ground floor call**: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

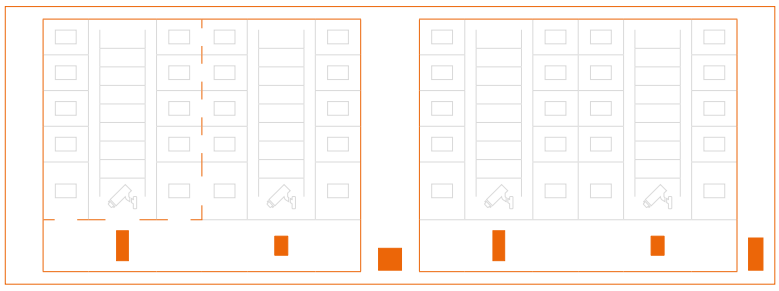


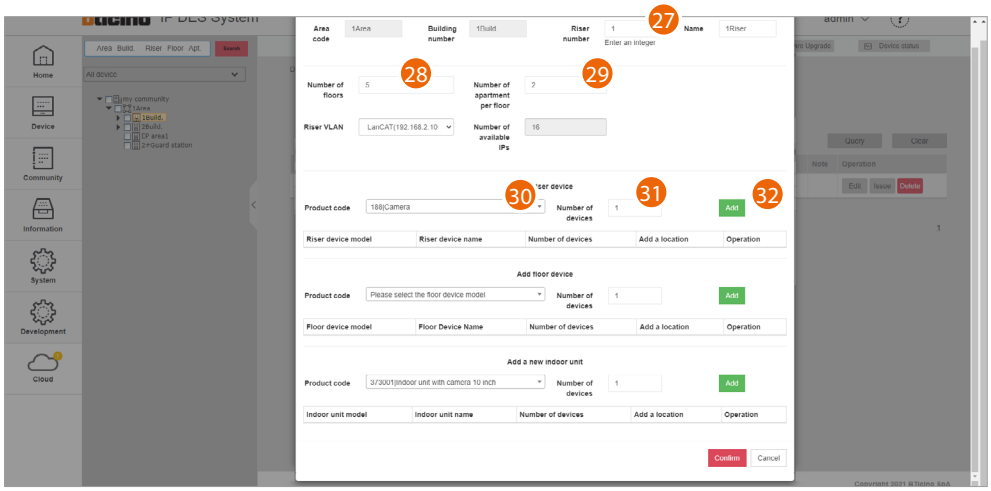
24. Click to confirm



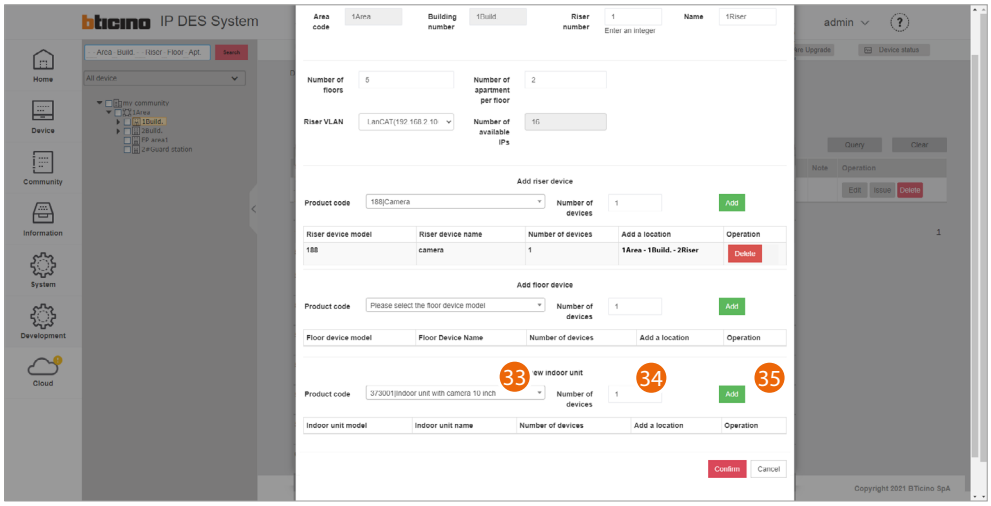


25. Click the Building with the right mouse button. This will open a drop-down menu
26. Click to add a **new Riser**

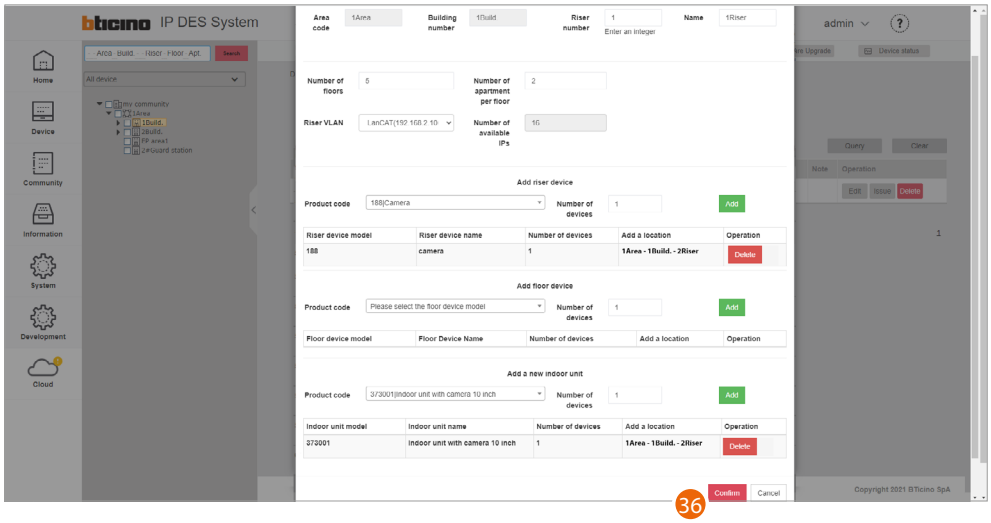




27. Enter the progressive Riser number
28. Select the number of Floors in the Building (5)
29. Select the number of Apartments for each Floor (2)
30. Select the OnVif IP camera
31. Select the quantity
32. Click to add

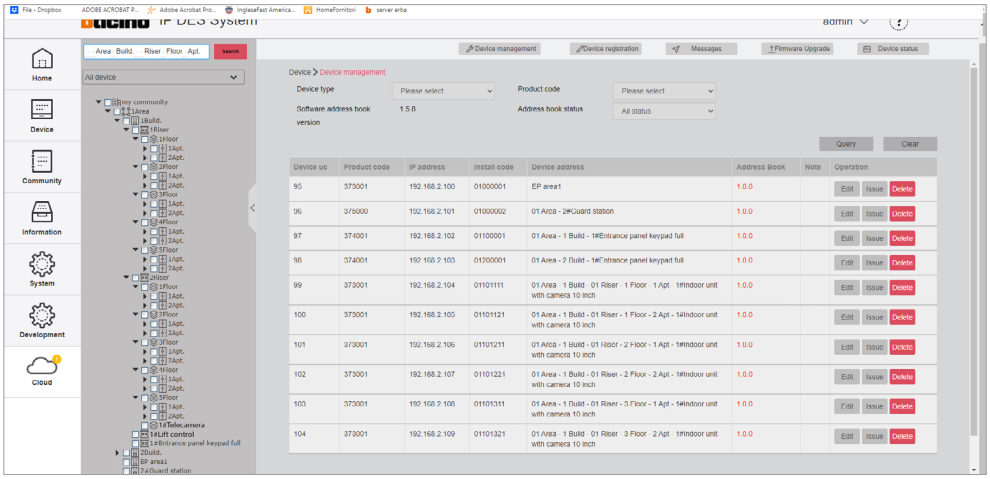


33. Select the apartment device
34. Select the quantity
35. Click to add

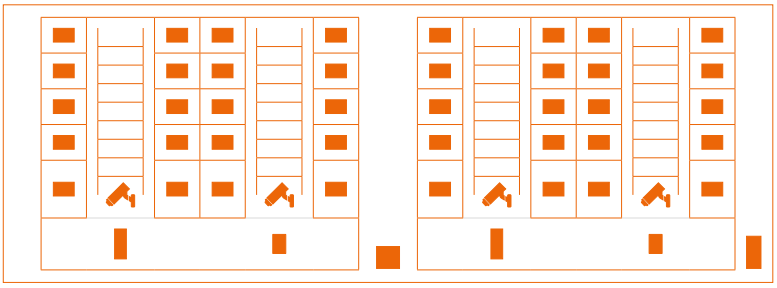


36. Click to confirm

Repeat the same steps for Riser 2

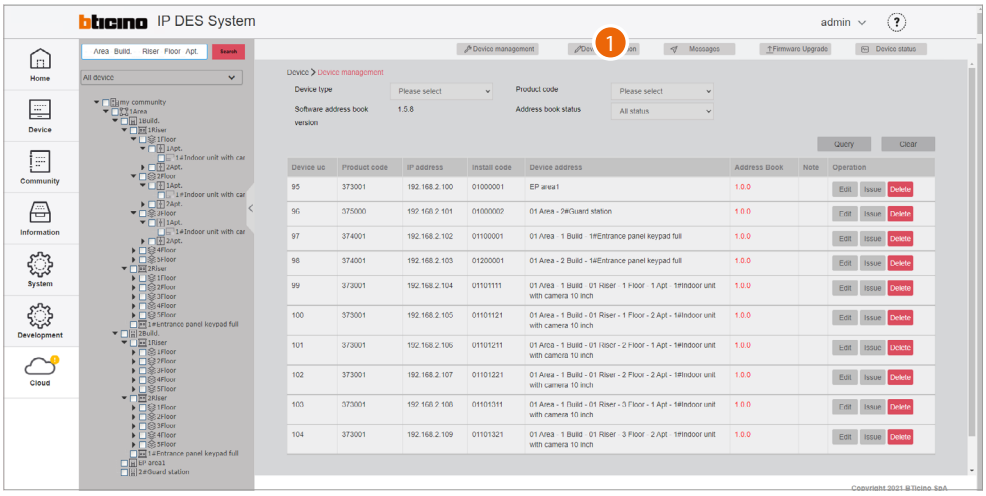


Repeat from step 21 also for building 2

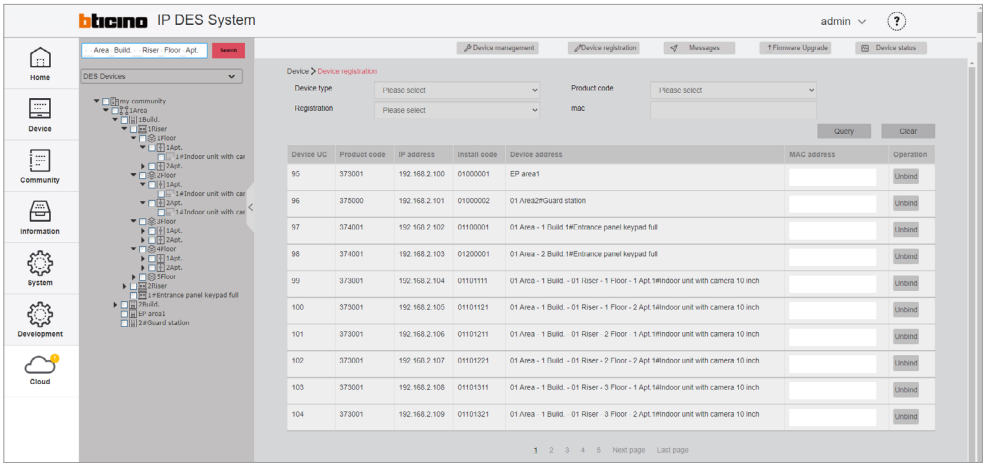


Device MAC address registration

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.

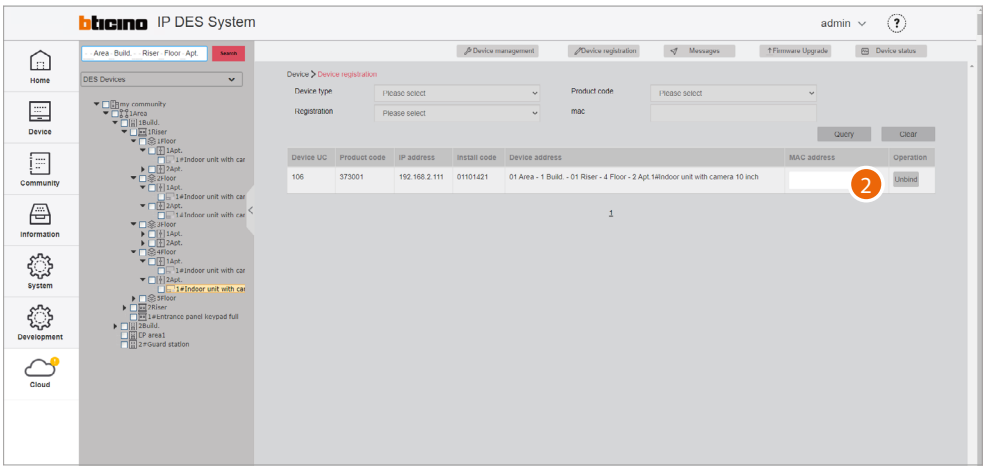


1. Click to enter the device registration section



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. Enter the MAC address

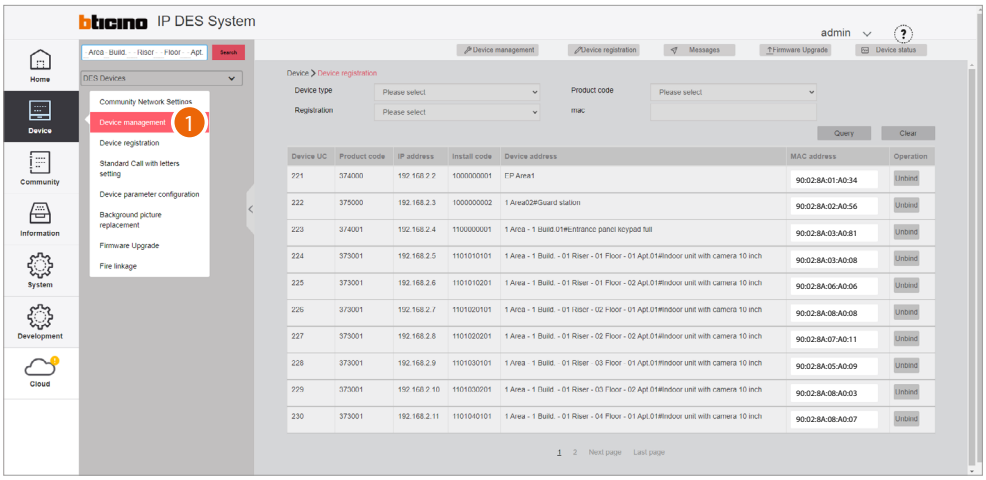
Repeat for all devices

Community customisation

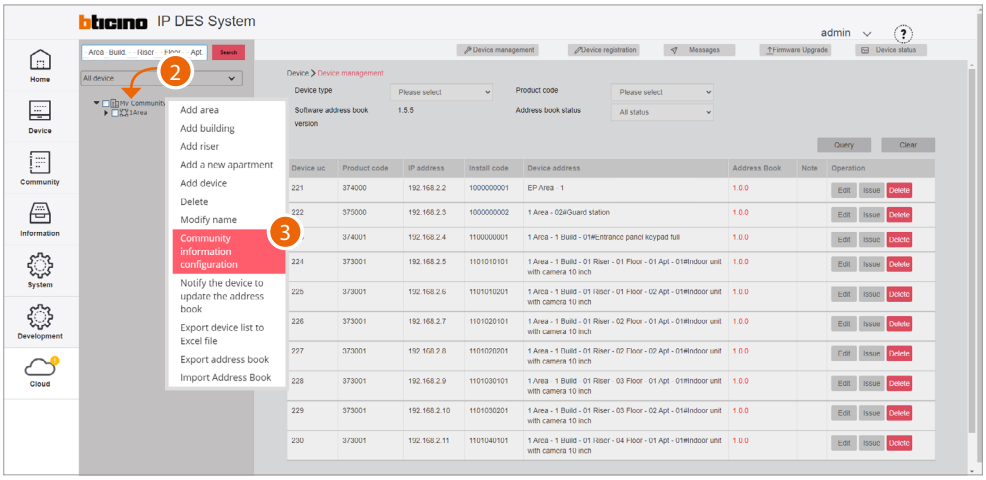
Before sending the configuration to the DES Server, we can customise the Community by e.g **modifying the call mode** and/or by **enabling access to the Community for certain individuals**.
To use a different call mode, (e.g. call mode via phonebook) to call residents, it will be necessary to:

– Change call type to alphanumeric/address book

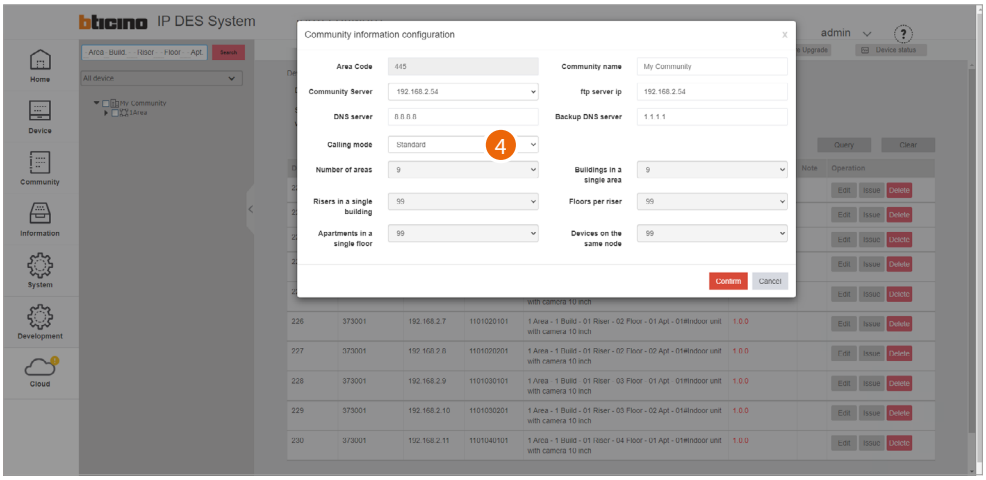
– replace **the address in the community with an alias** to facilitate recognition of the called party.
This function renames the apartment to a different name (alias).
The call to this apartment will be made using this new name.
E.g. JOHN SMITH



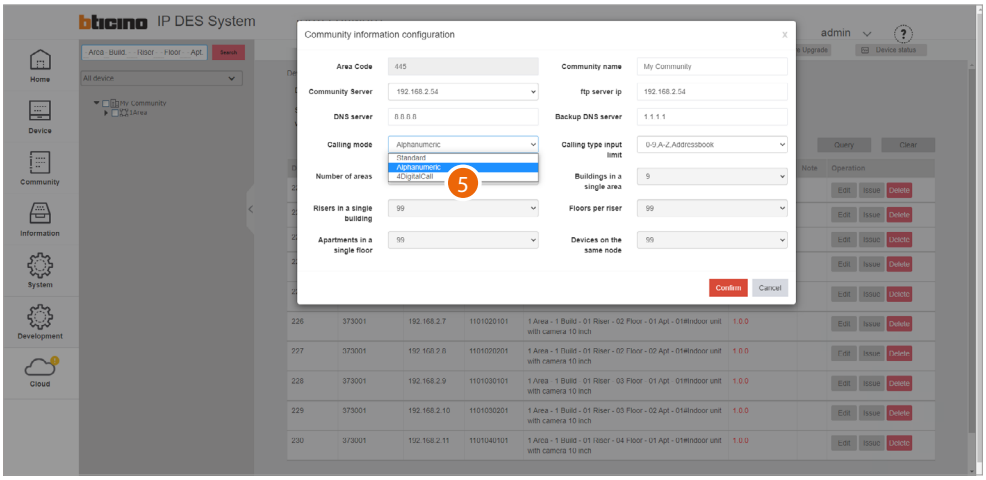
1. Select device/device management



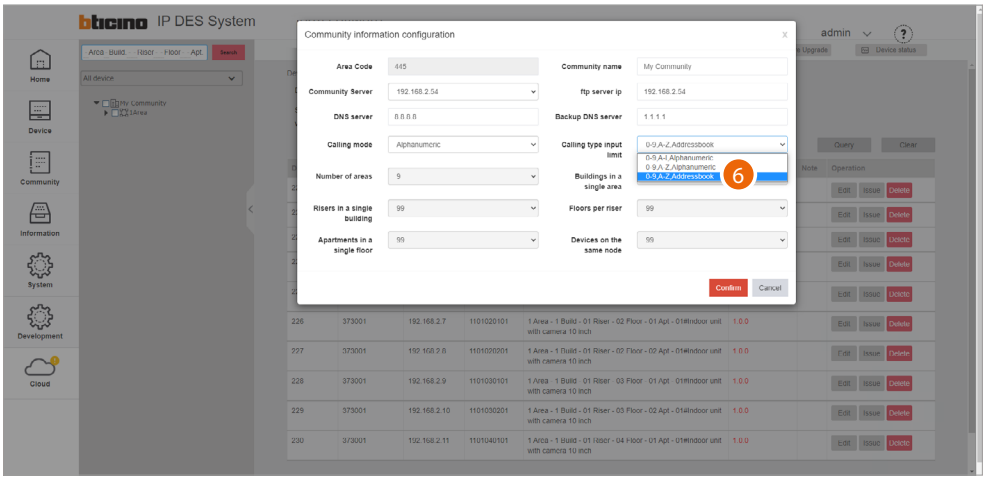
2. Right click the Community
3. Click to select the command



4 Click to modify the call mode



5. Select the alphanumeric mode

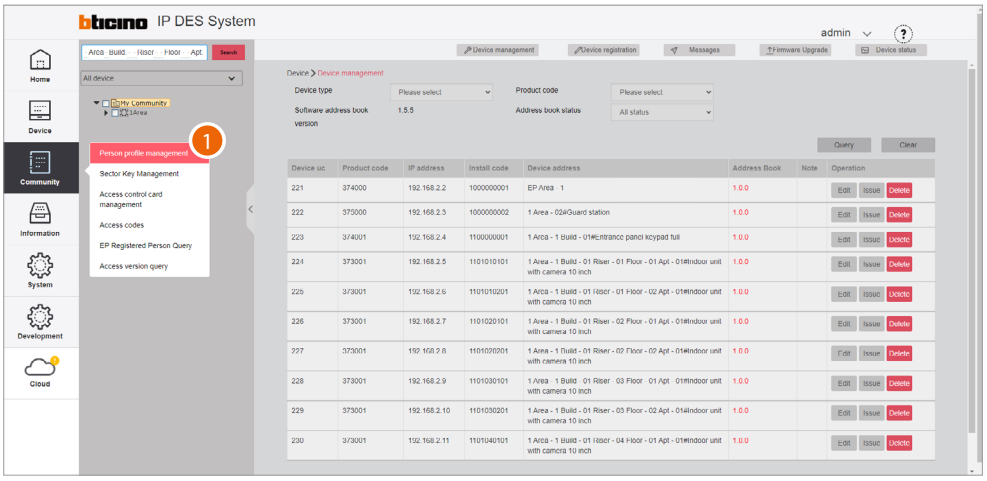


6. Select address book as entry type

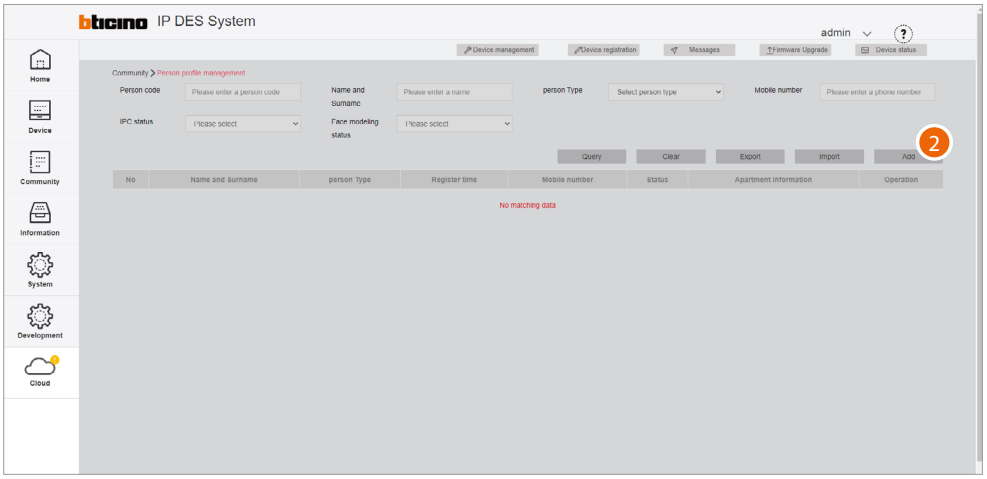
After sending the configuration to the DES server, it will be possible to call IUs using custom names (aliases). When changing the name of a GS or EP, this will be identified with this name on the receiving device when the call is made.

NOTE: *This alias format (Address Book) is not supported by entrance panels 374001/03*

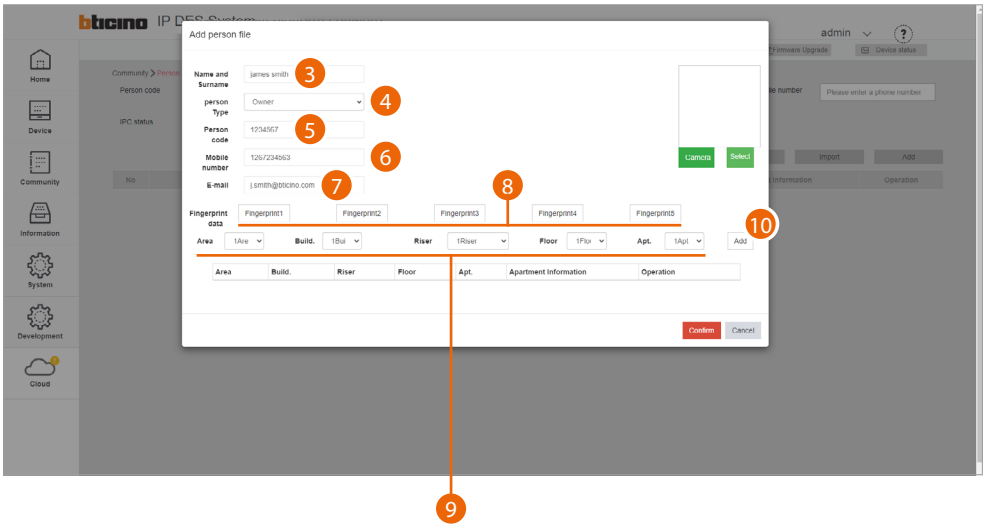
Now it is possible to add community people and give them permissions to access the structure. Depending on the type of person, different access permissions may be assigned, see **Person profile management**.



1. Select Community/Person profile management



2. Click to create a new person



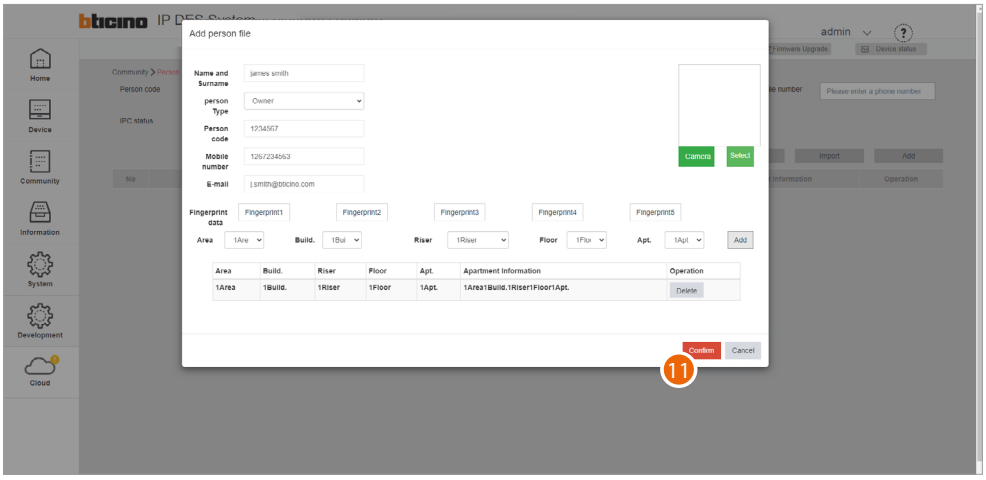
3. Enter the name and surname of the person
4. Select the type of person

Note: *some parameters may change depending on the type of person*

5. Person code
6. Enter the telephone number of the person
7. Enter the email address of the person
8. Register a fingerprint

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 to access the community, this must be registered; see Access control card management

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).

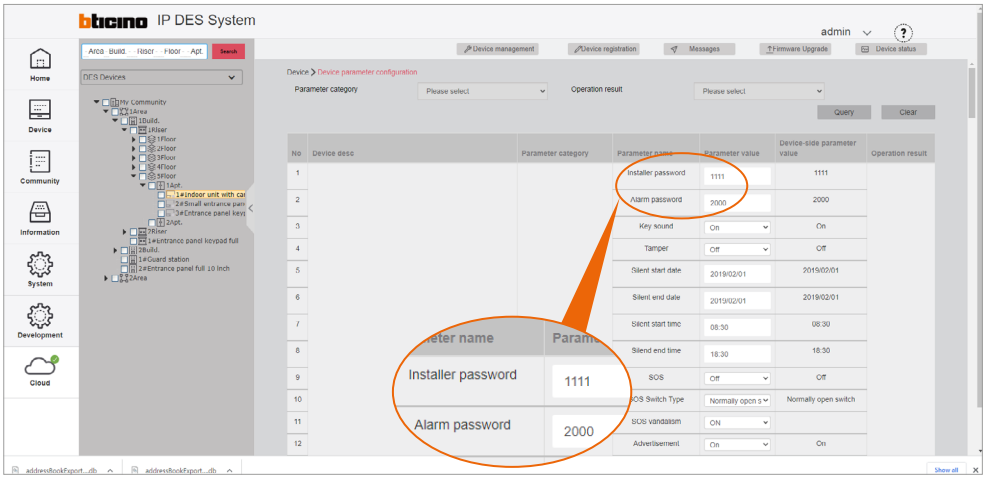
The access codes for opening the door locks of entrance panels are also generated in the same way.

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

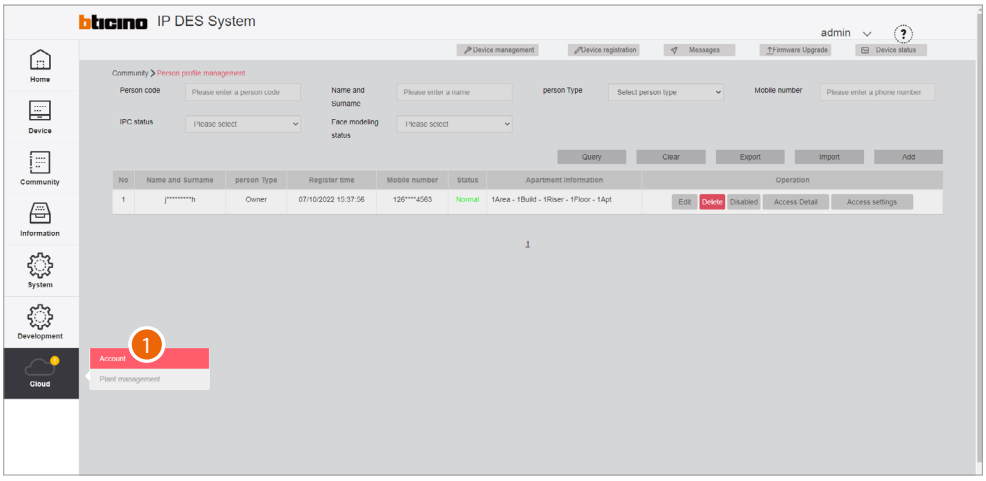
.....

1. Write down the passwords in a safe place that is always accessible.

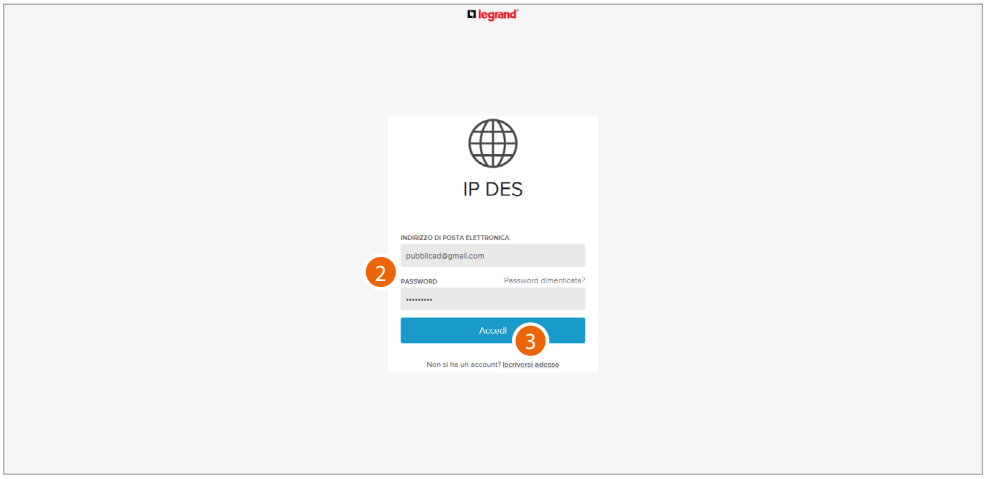
Registration of the community on the Installer's Cloud

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:

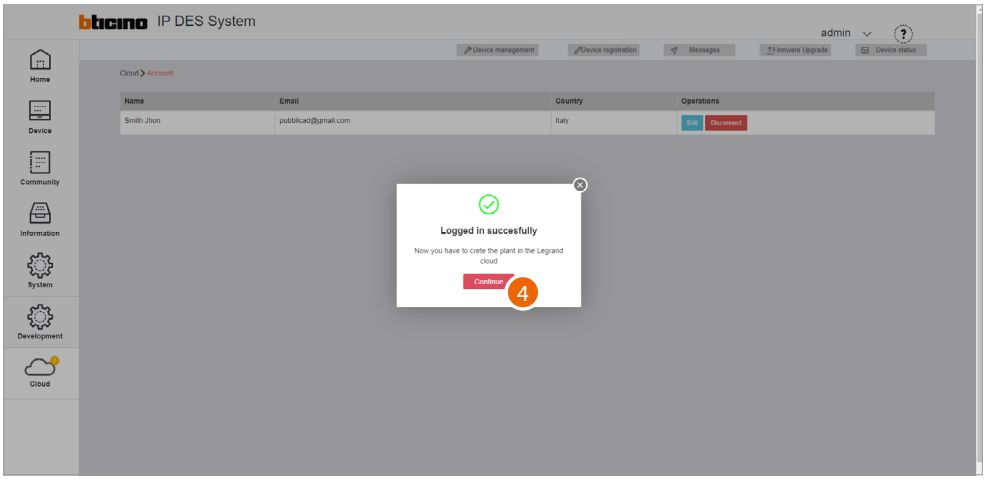
- have greater security in the event of local data loss
- associate the Home+Security app to the IU, for remote management of the video door entry system



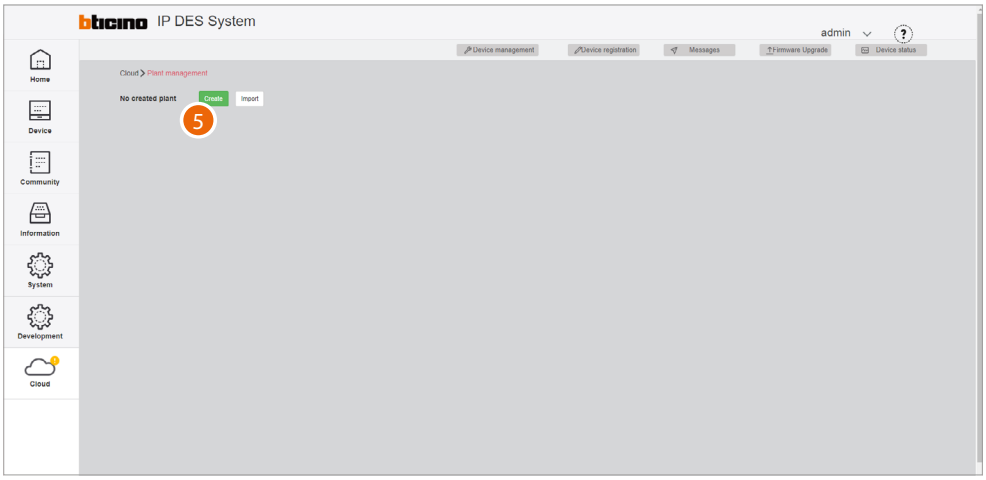
1. Click to complete the Installer's Cloud authentication process



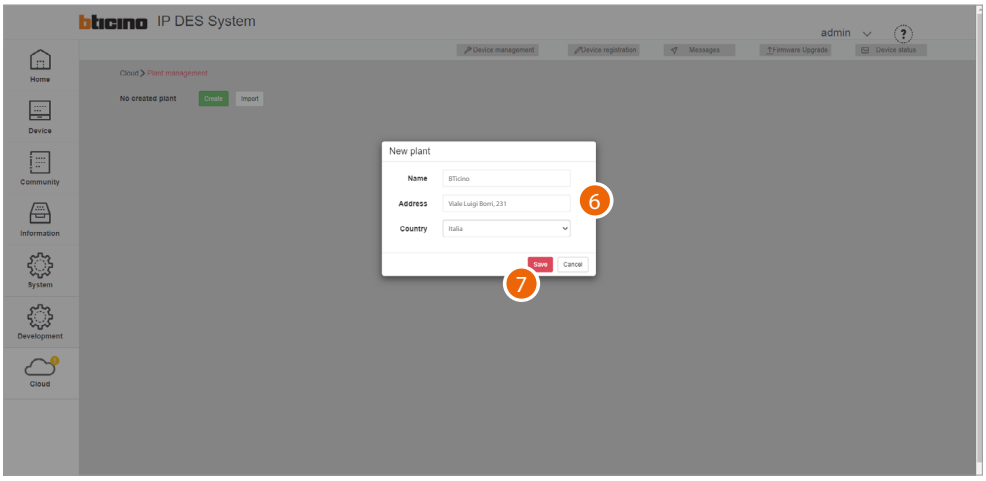
2. Enter email and password
3. Click to access



4. Click to confirm

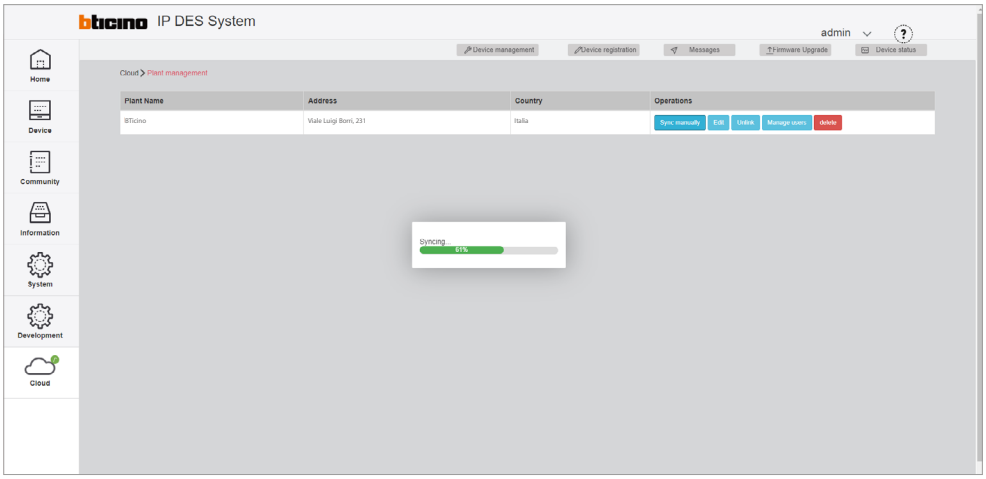


5. Click to create a new Plant



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

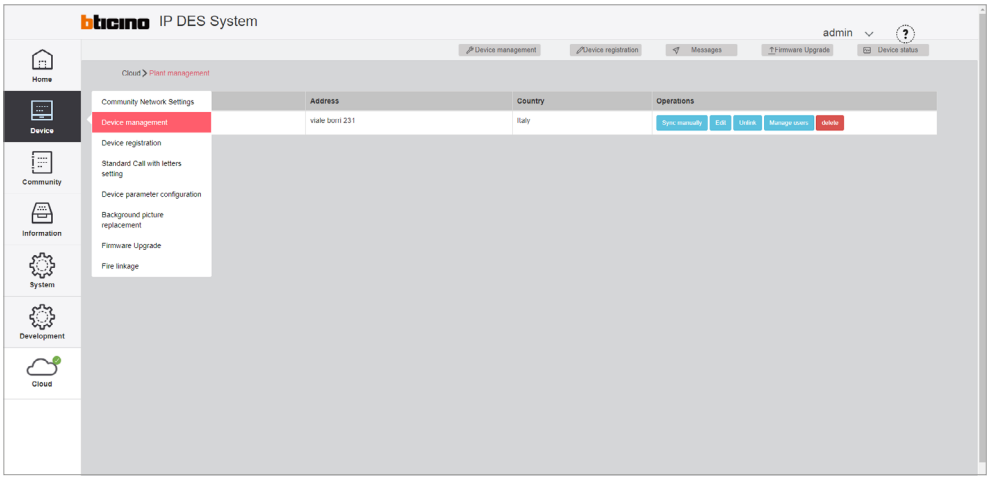
The plant is automatically synchronised



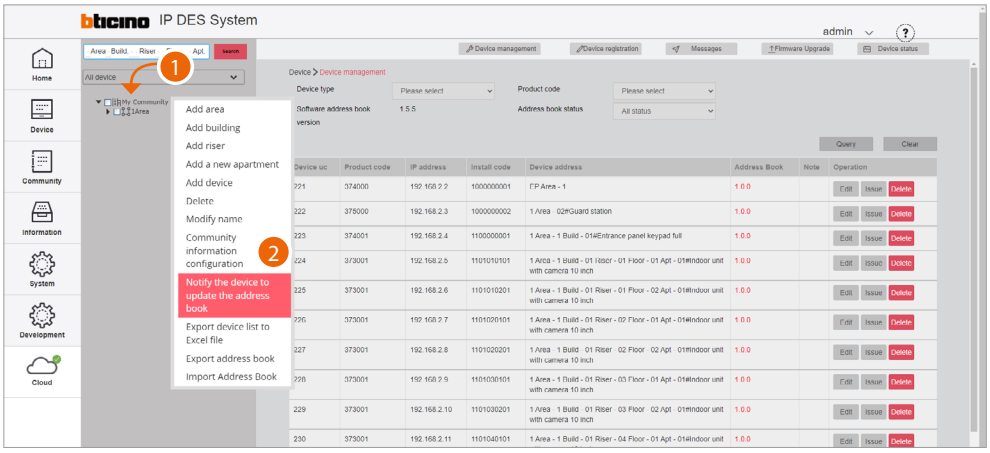
Once created, the plant remains available on the cloud.
If disconnected (unlink button), it can be retrieved from the cloud using the Import a Plant function.
If deleted, it will also be deleted from the cloud.

Notifying of the address book to the DES Server

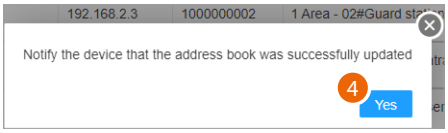
After creating the structure and configuring the virtual devices, it will be necessary to notify the address book to the system, therefore "instructing" the system to use this configuration.



1. Select device/device management

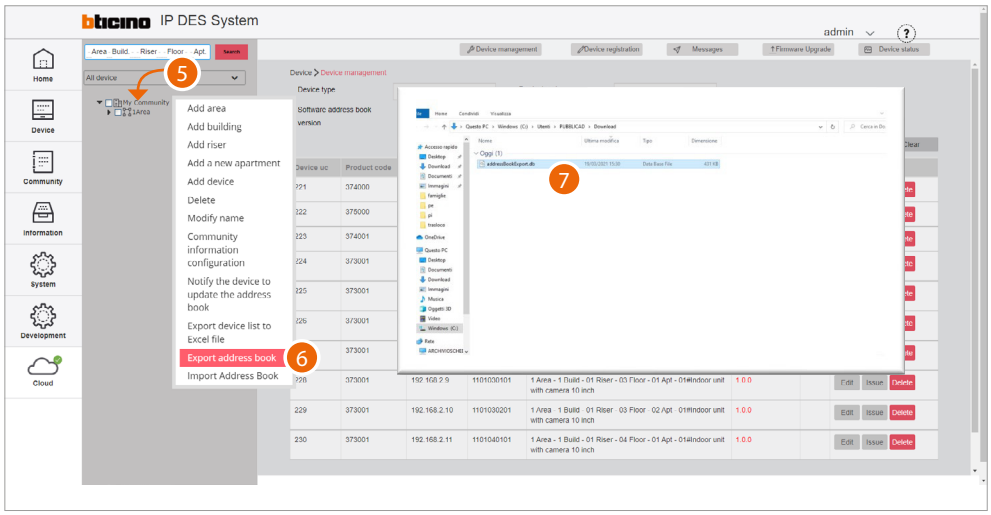


1. Click Community with the right mouse button: a drop-down menu will appear
2. Click to update the system address book



3. Click to confirm
4. Click to finish

The address book is now saved in the DES Server. To avoid accidental loss, it is also possible to save it in an archive file.



5. Click Community with the right mouse button: a drop-down menu will appear
6. Click to export the address book to a file
7. The file will be saved in the download folder of your computer

Take the DES server back to the system

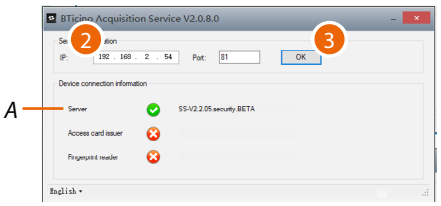
1. Disconnect the SD from the office LAN network and take it to the on-site system

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

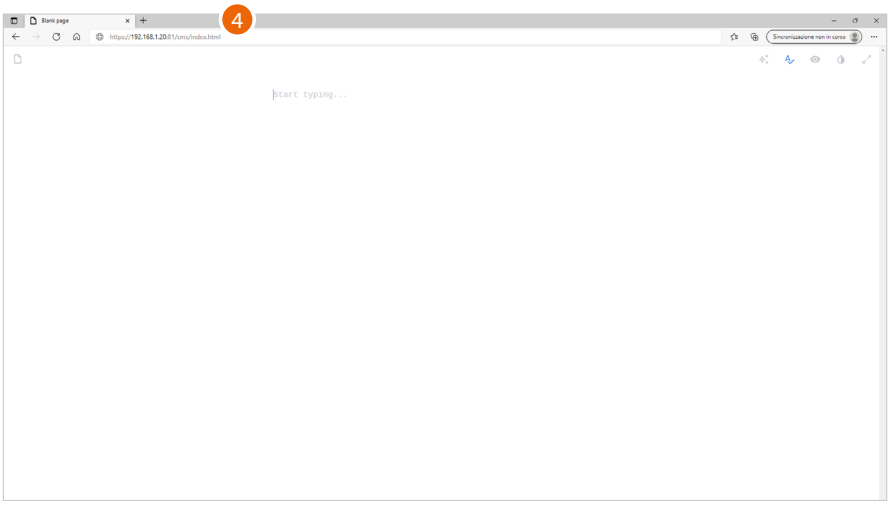
The following screen appears



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 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 MAC address identification (method 2).

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

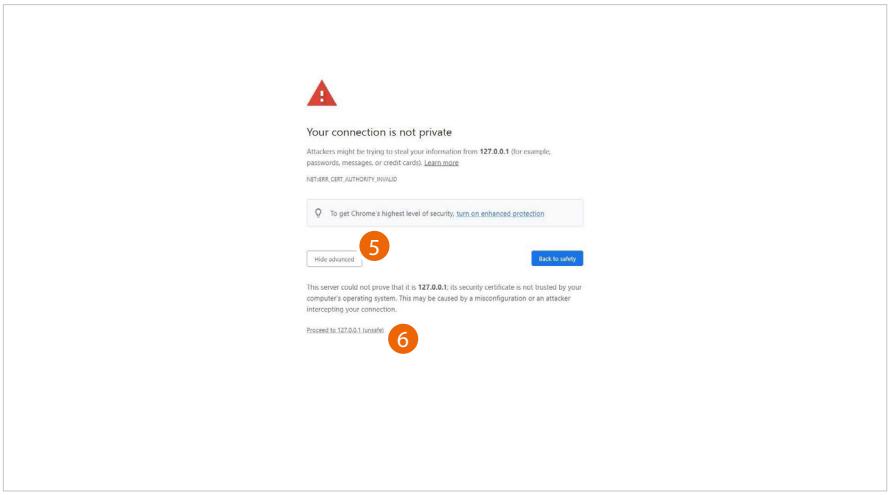


4. Open the browser and enter the http address of the DES Server:

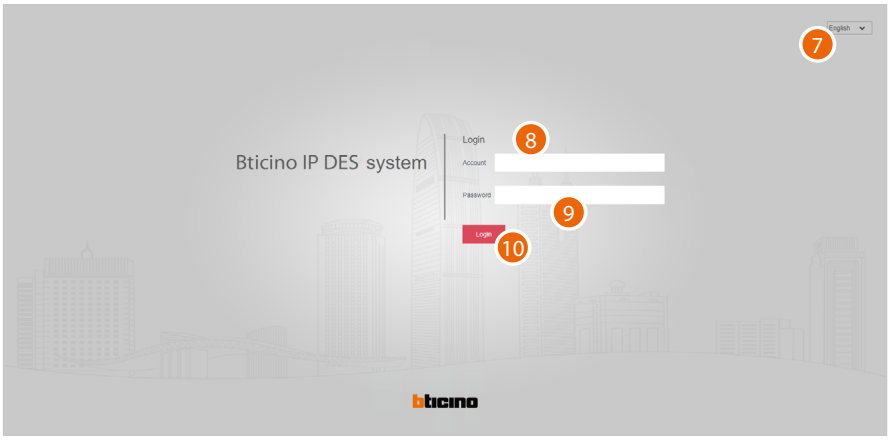
https://SD IP address:81/cms/index.html

***Note**: use Crome/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
9. Enter the password

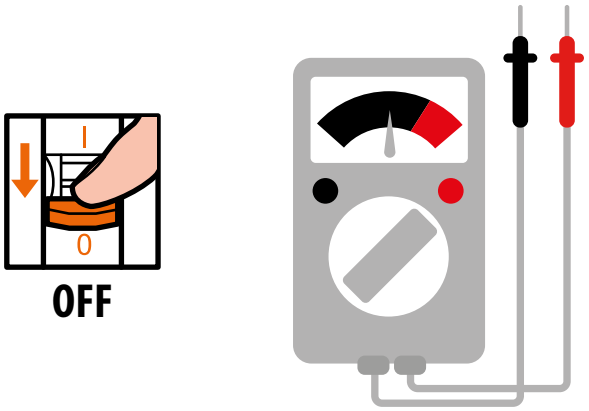
***NOTE**: login and password are those set at the office*

10. Click to confirm

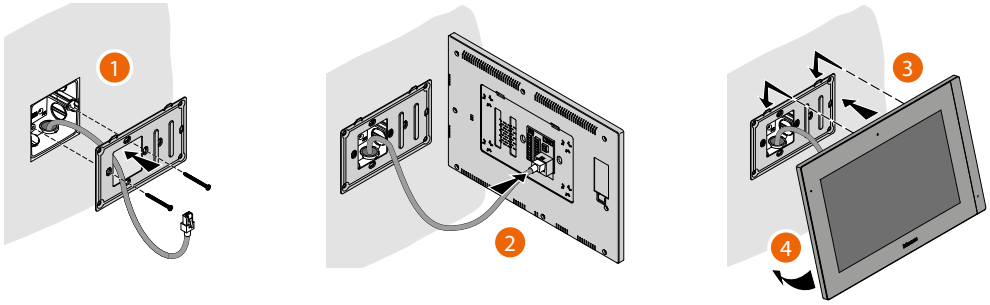
Installation of the devices

To transfer the configuration to the devices, these must be installed and powered

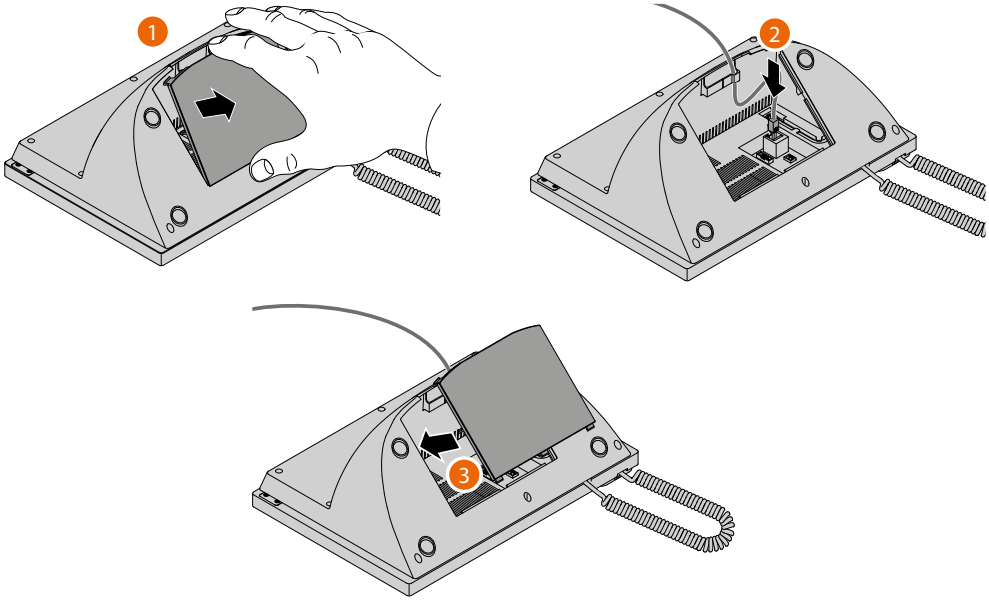
Switch off the power supply to the system and check that there is no voltage



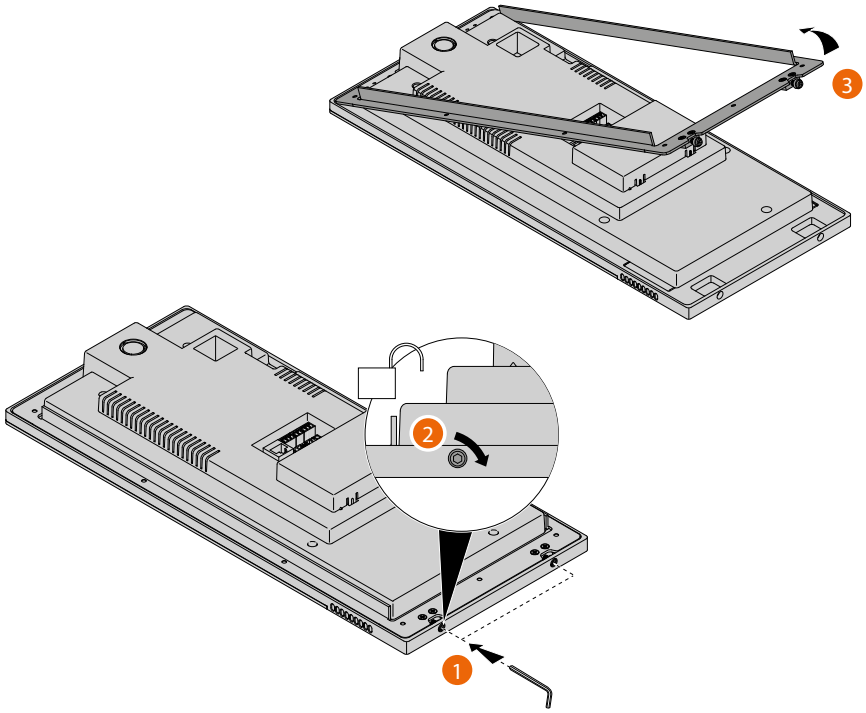
Install the devices

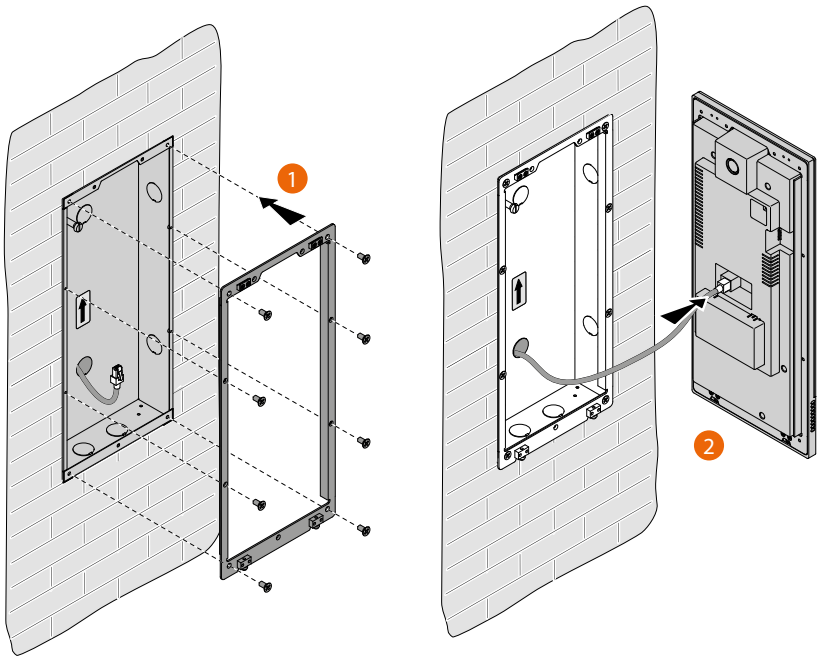


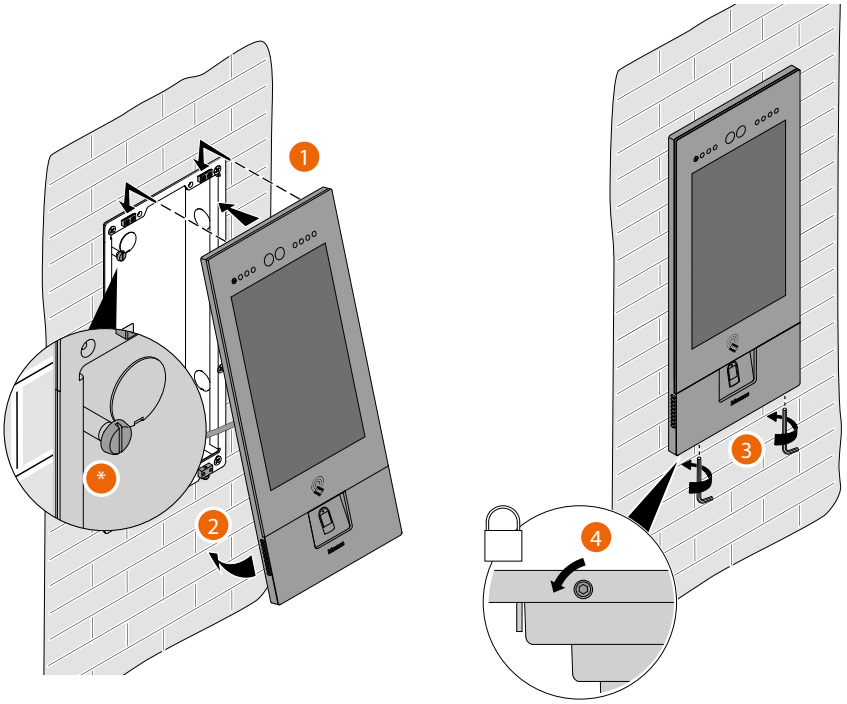
The RJ45 cable must be at least 200 mm long



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 sending an alarm to the guard station.

***Warning**: please note that the EP installation shown is representative of all EPs.*
For more details, see the specific instructions in the package

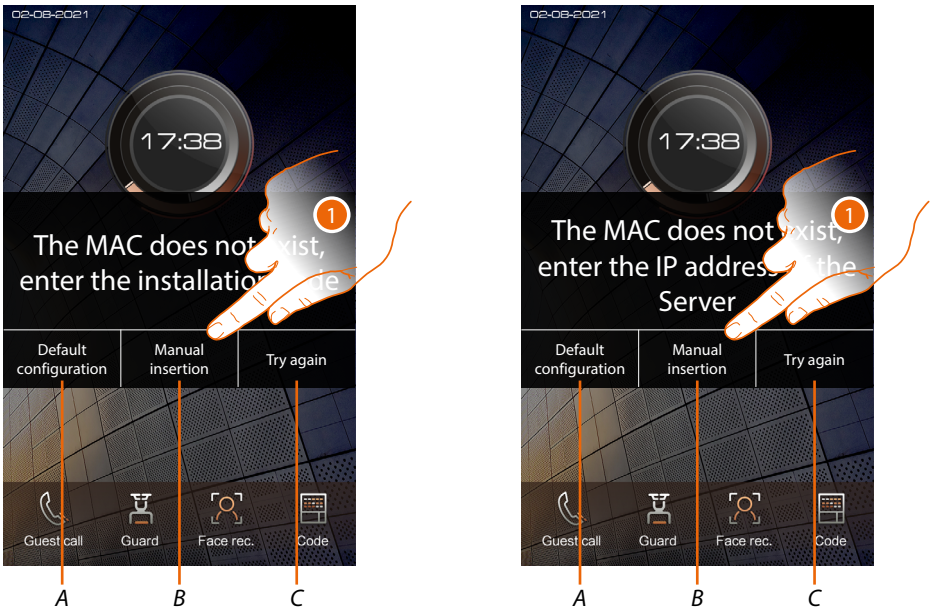
Reconnect the power supply

Activation of the devices

Thanks to the previously entered MAC address, once powered, the device checks that a configuration (address book) is available on the DES Server, and if so acquires 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.



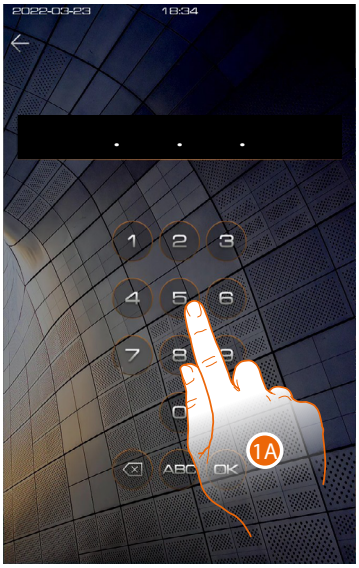
A Not to be used

B Button allowing 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 **Community Network Settings**, to display the installation code, see **Installation code

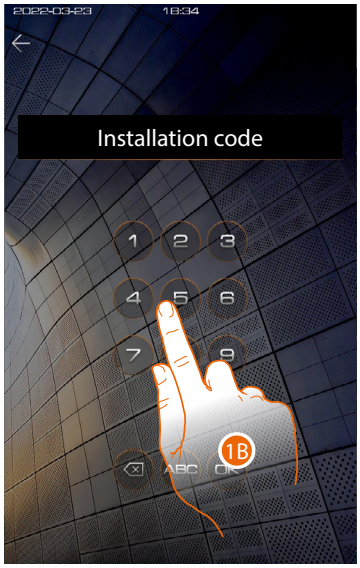
C Button to test the activation of the device

1. Click to manually enter the server IP address or the system access code

IP address



Installation code

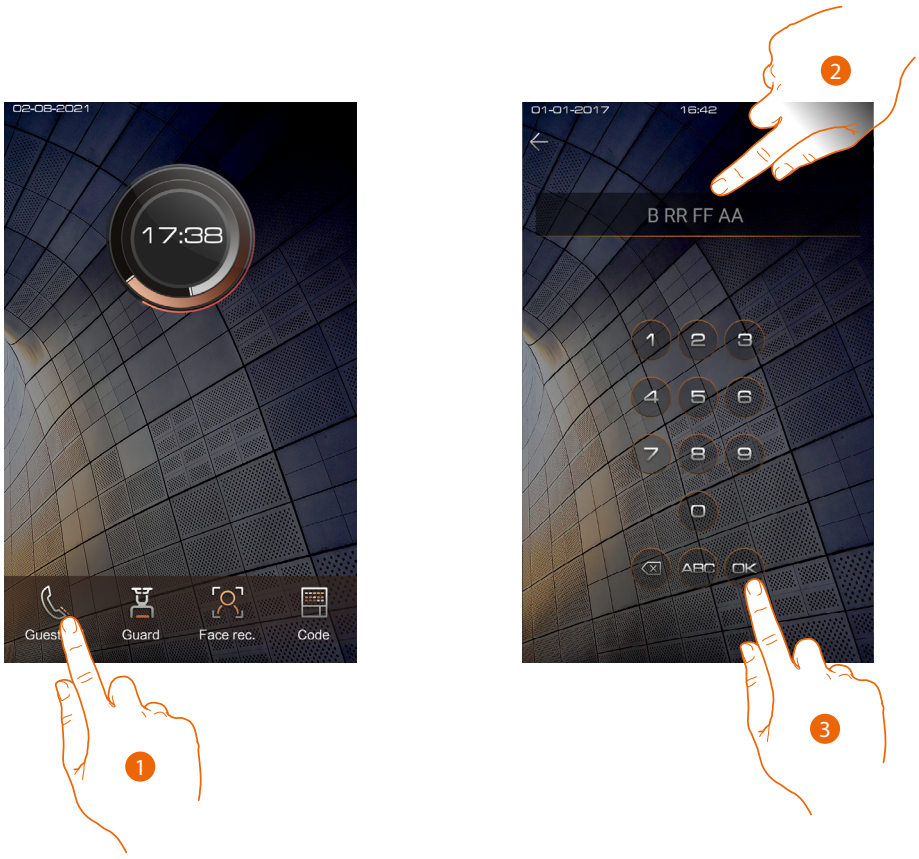


1A. Enter the IP address of the server

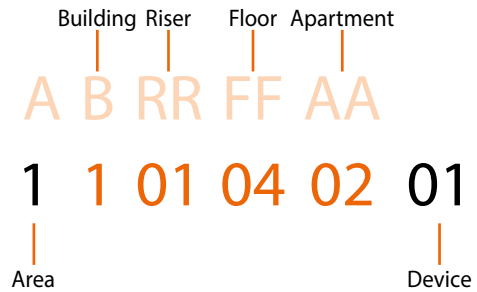
1B. Enter the installation code

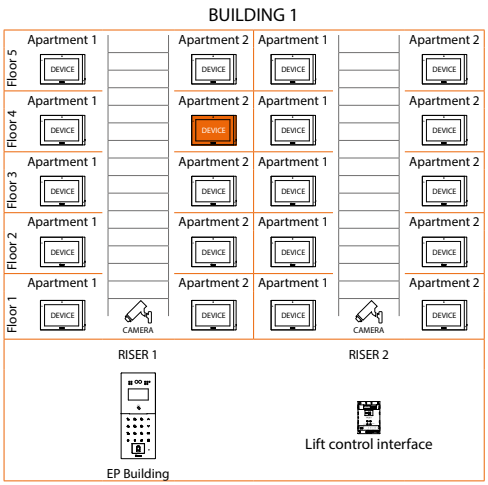
System test

It is now possible to test the system, for example by making a call from the EP

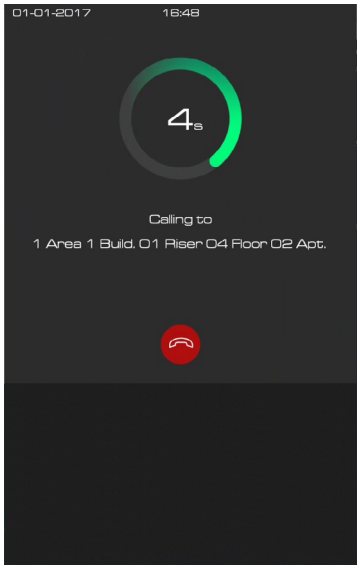


1. Touch to make the call
2. Enter the IU address



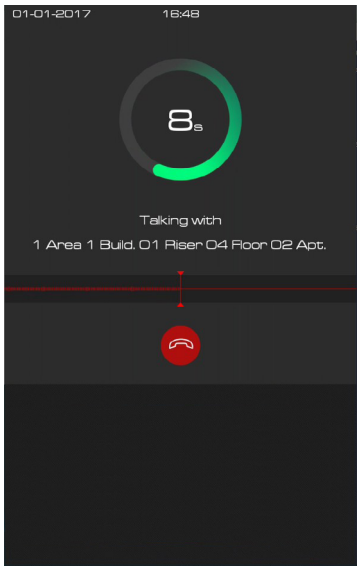


3. Touch to send the call



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. Tap to capture an image of the screen

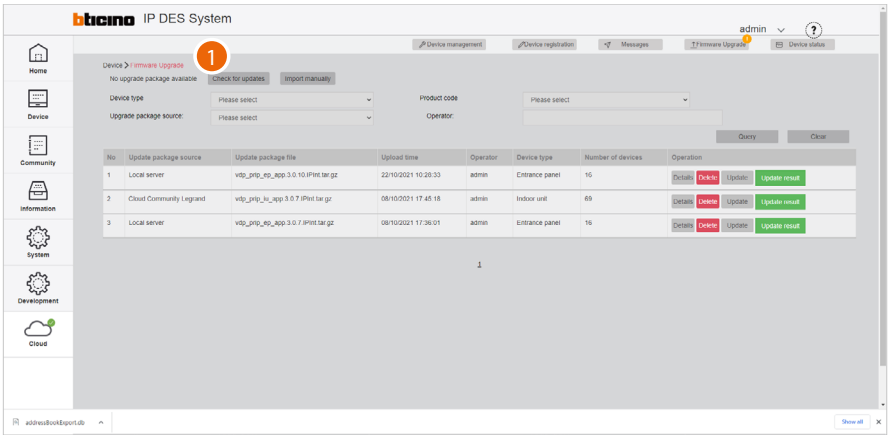
A confirmation message appears.

6. Touch to open the EP door lock

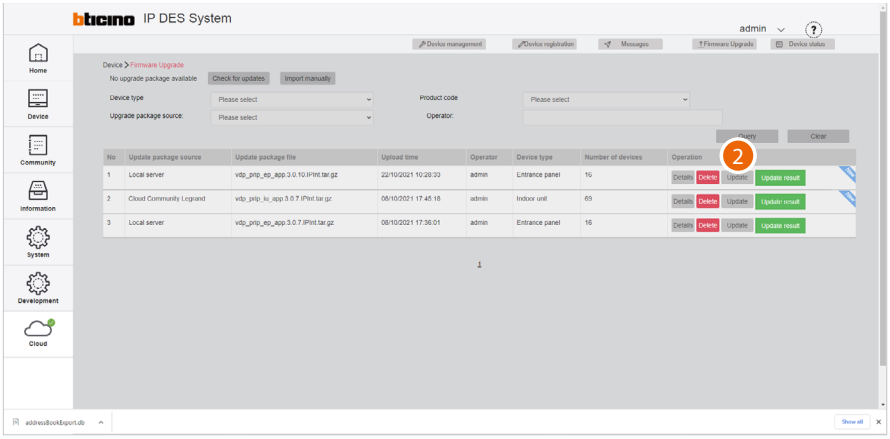
A confirmation message appears

7. Tap to adjust the volume
8. Touch to end the call

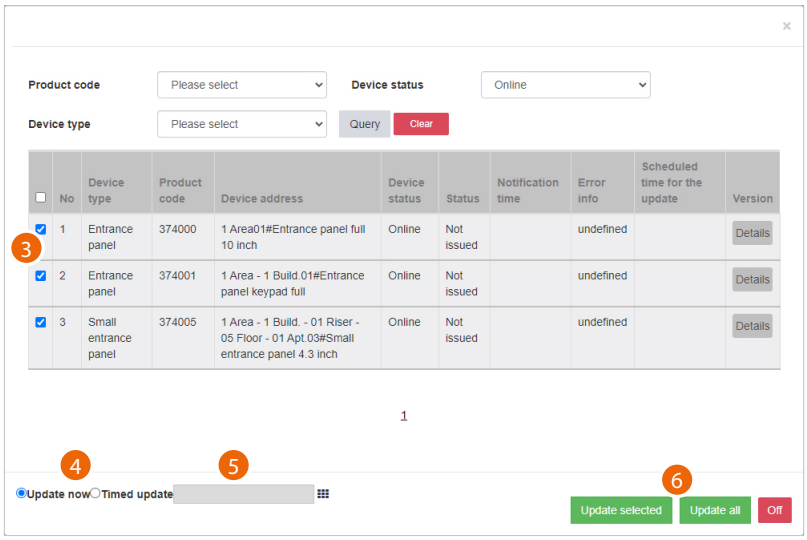
Update of the devices



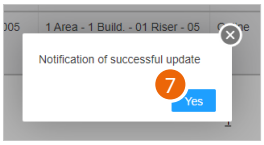
1. Click to check for updates on the cloud. If there are updates, these will be downloaded and available for installation
   ***NOTE**: firmware updates will only be downloaded if the last installed updates have already been deleted: the page must be empty.*



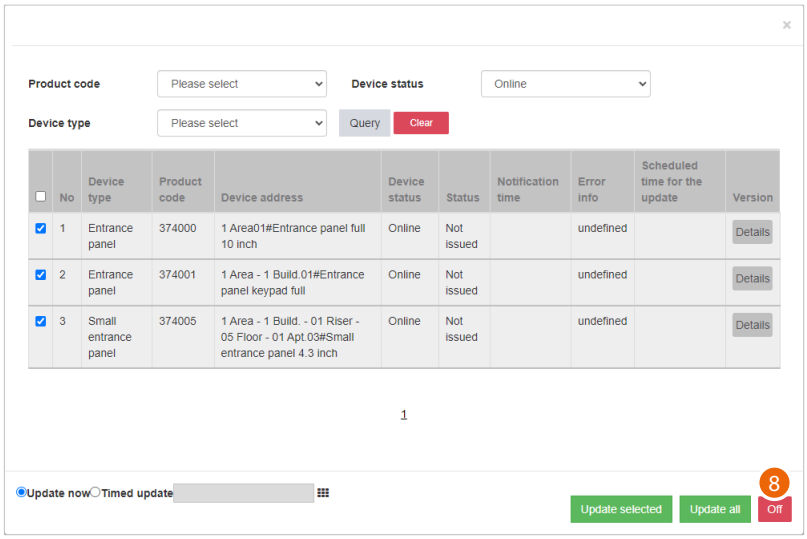
2. Click to send the update to the plant



3. After using the filters to display the relevant devices, select them
4. Decide whether to perform the update immediately or
5. Schedule an update, setting the date and time
6. Start the update for the selected devices or for all the devices



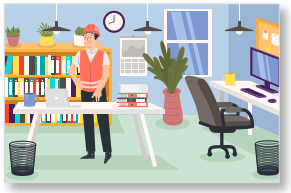
7. Click to finish



8. Click to close the panel

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

OFFICE



Step 01 Community VLAN network creation

Step 02 Community structure definition

Step 03 Community structure creation

Step 04 Device MAC address registration

Step 05 Community customisation

Step 06 Saving of passwords

Step 07 Registration of the Community on the installer's Cloud

Step 08 Forwarding of the address book to the Server DES

Step 09 Notification to the system that the Plant has been saved to the cloud

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 12 Plant authentication and synchronisation on the cloud

Step 13 Installation of the devices

Step 14 Activation of the devices

Step 15 System test

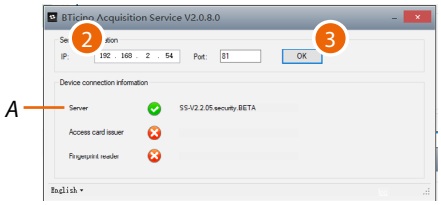
Step 16 Update of the devices

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

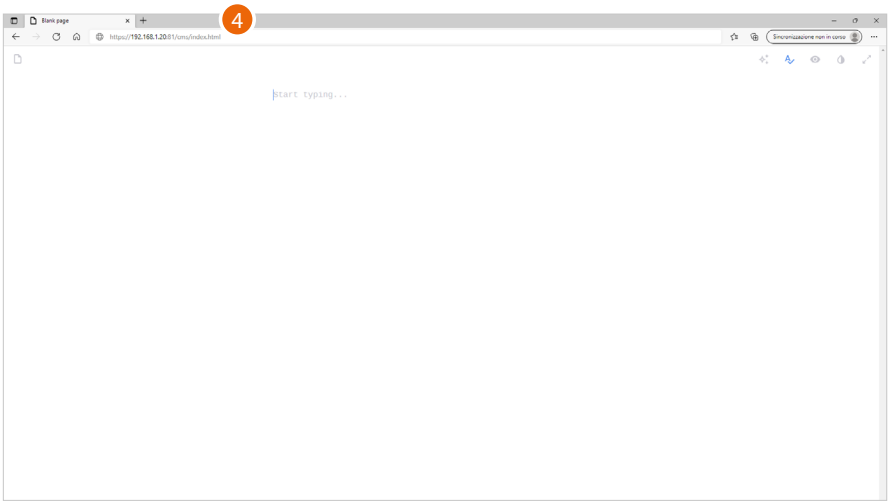
The following screen appears



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 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 MAC address identification (method 2).

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

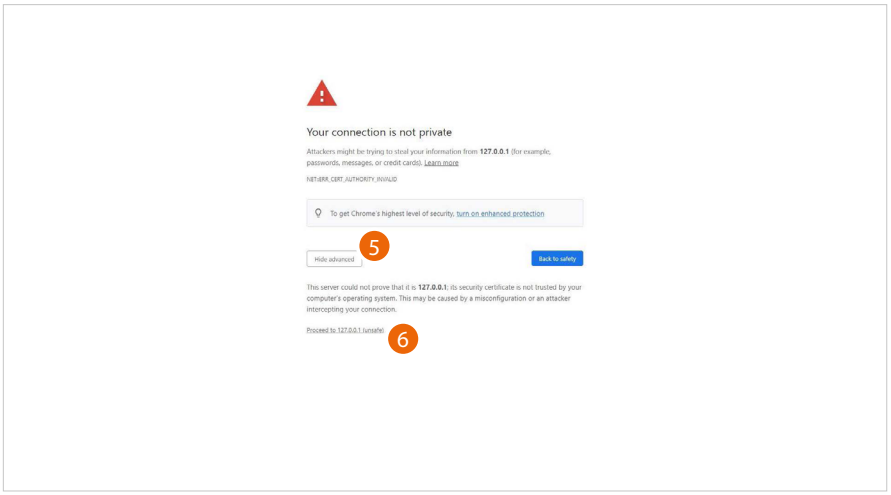


4. Open the browser and enter the http address of the DES Server:

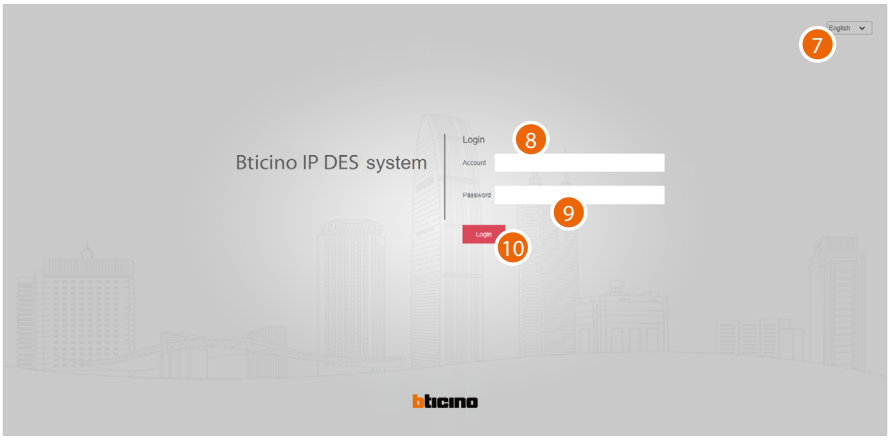
https://SD IP address:81/cms/index.html

***Note**: use Crome/Edge browser and a screen with resolution 1920x1080*

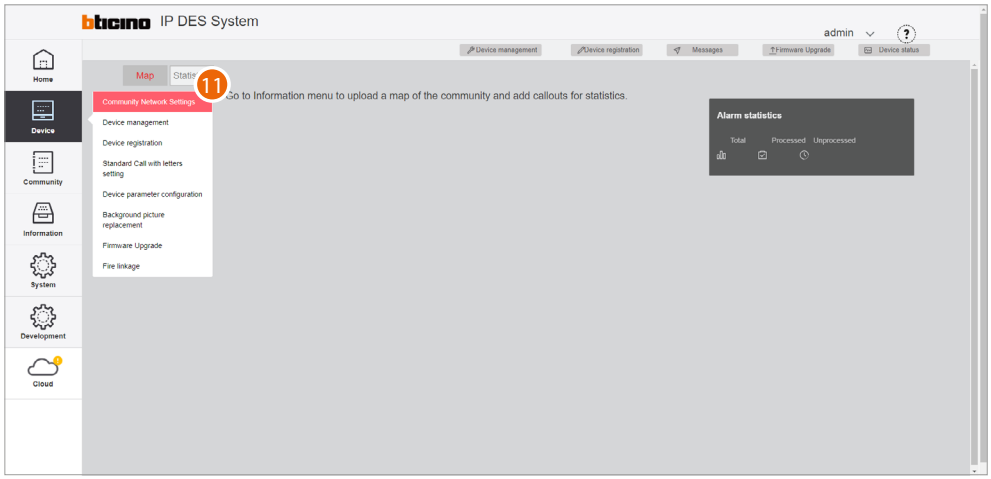
In some cases, the browser may consider the page to be unsafe.



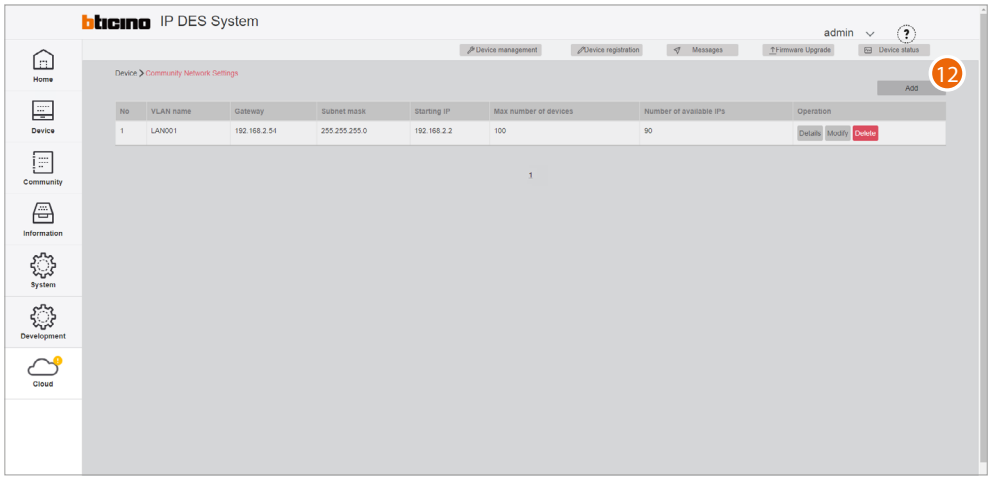
5. Click to display the advanced options
6. Click to ignore the warning and proceed



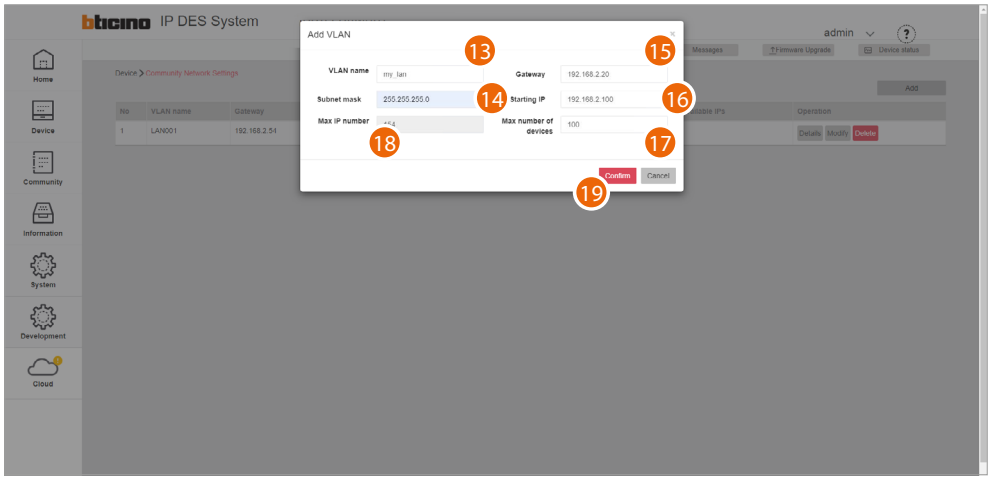
7. Select the interface language
8. Enter the login name (default admin)
9. Enter the password (default 123456)
10. Click to confirm



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

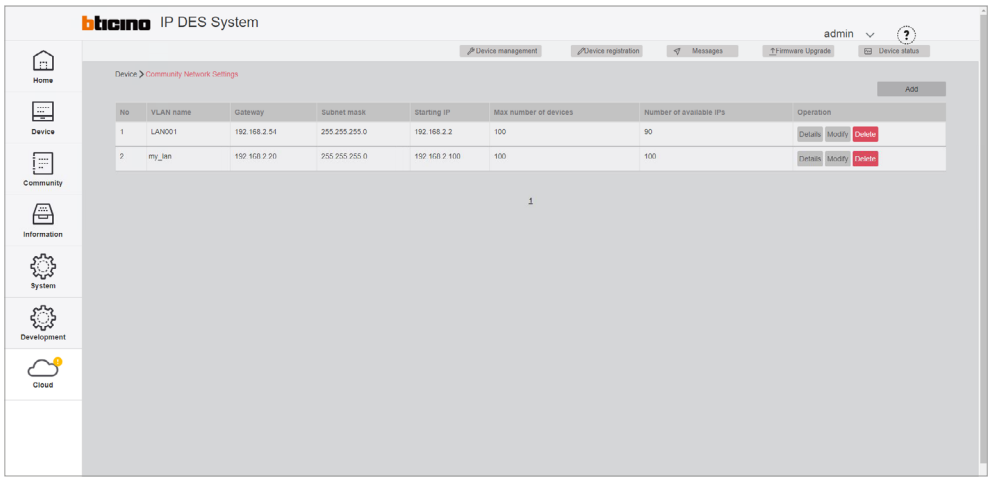


12. Click to create the community VLAN network



13. Enter the name of the community VLAN network (letters and numbers without space)
14. Enter the Subnet mask address
15. Enter the fixed IP address of the DES Server given to you by the network administrator
16. Enter the starting address from which the IP addresses of the IP devices will be generated, see Assignment of IP address range based on the number of video door entry devices
17. Enter the number of IP devices that will be part of the Community
18. It displays the maximum number of IP devices that can be installed based on the previously entered data
19. Click to confirm

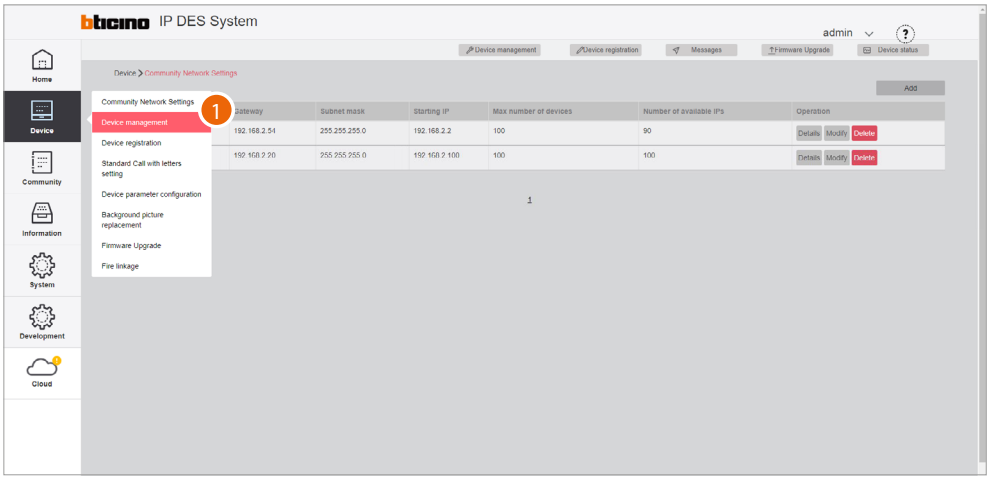
***NOTE**: the parameters (13 to 1 8) must match those found on the system.*



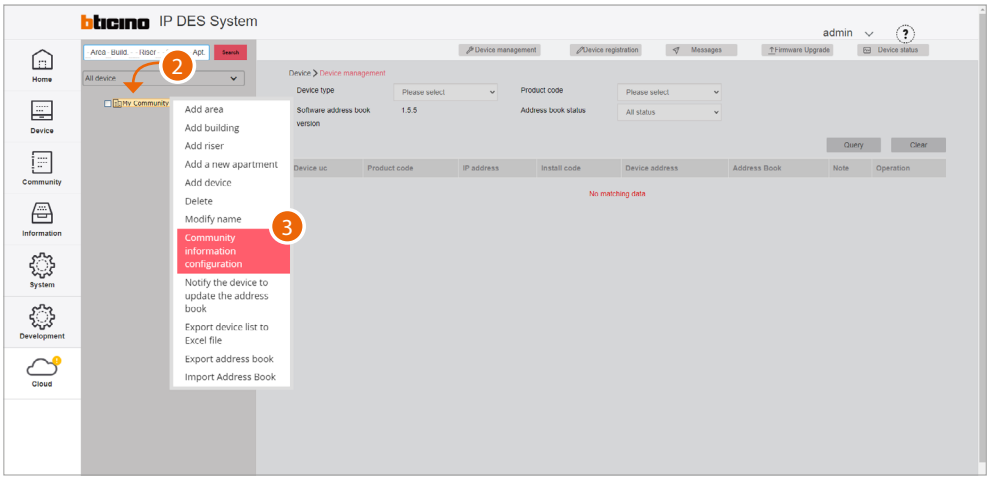
The community VLAN network has been created

Community structure definition

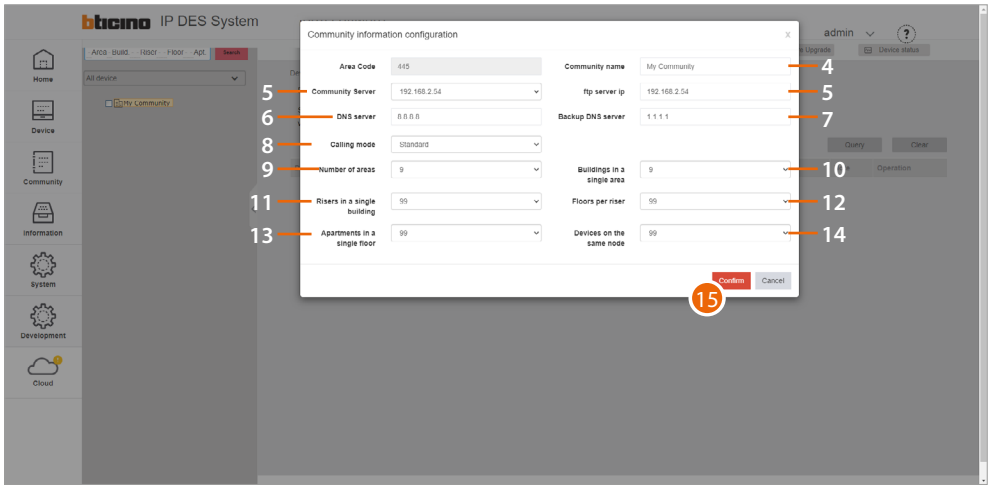
It is now necessary to define parameters like number of Areas, Buildings, Risers and so on, as well as other details that will define the structure of the Community.
In this section, it is also necessary to define the type of call that will be used for all Community calls.



1. Click to enter the Community configuration section



2. Click the Community with the right mouse button: a drop-down menu will appear with the commands for its configuration
3. Click to open the pop-up window with the parameters that define the Community structure



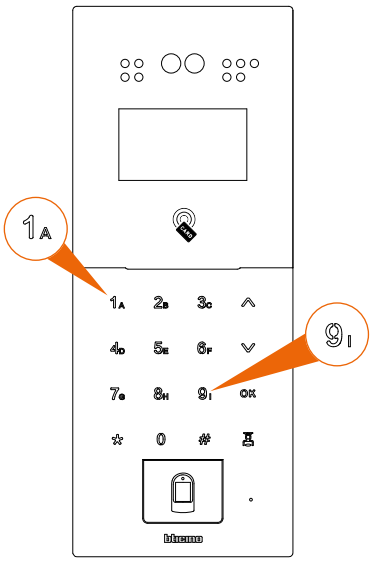
4. Change Community Name
5. Selects the fixed IP address of the Community DES Server
6. Change the address of the DNS server (unless there are special requirements, we recommend to keep the default address)
7. Change the address of the backup DNS server (unless there are special requirements, we recommend to keep the default address)
8. Selects the type of call to be used for the system: Standard or Alphanumeric.
   When selecting Alphanumeric, it will also be necessary to select a mode, "0-9, AZ" or "0-9, AI", depending on the type of EPs installed in the Community.
9. It displays the maximum number of Areas for your Community (default 9).
10. It displays the maximum number of Buildings that an Area can have (default 9).
11. It displays the maximum number of Risers that a Building can have (default 99).
12. It displays the maximum number of Floors that a Riser can have (default 99).
13. It displays the maximum number of Apartments that a Floor can have (default 99).
14. It displays the maximum number of Devices that an Apartment can have (default 99).

***Note**: The default values of item 9 through 14 are consistent with the example shown in this document, and therefore do not need to be changed.*
For other more complex structures, see ***Community information configuration****.*

***Note**: If even one single EP has an "0-9, AI" type keypad, select the "0-9, AI" option.*

EP with "0-9, AZ" keypad

EP with "0-9, AI" keypad



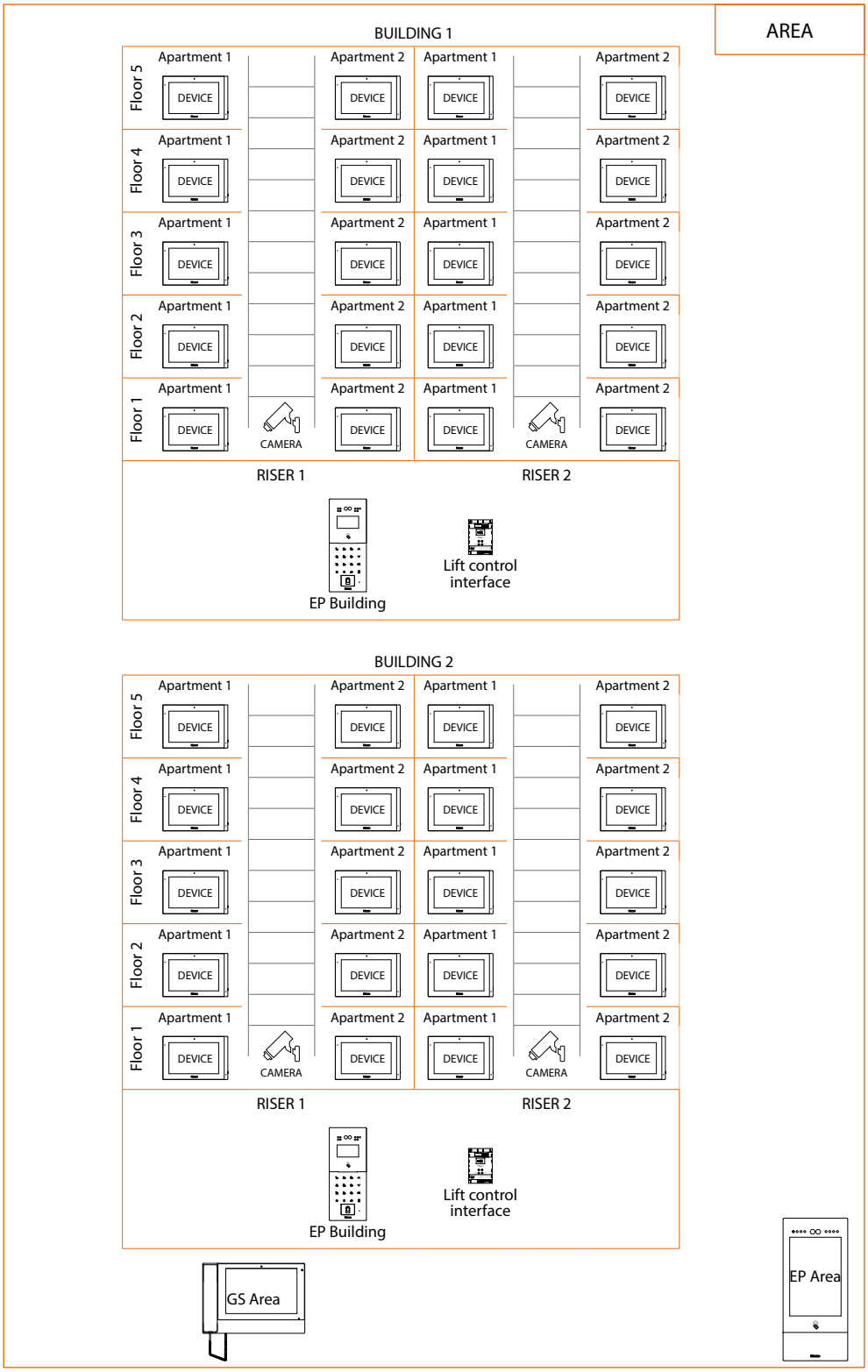
15. Click to confirm

Community structure creation

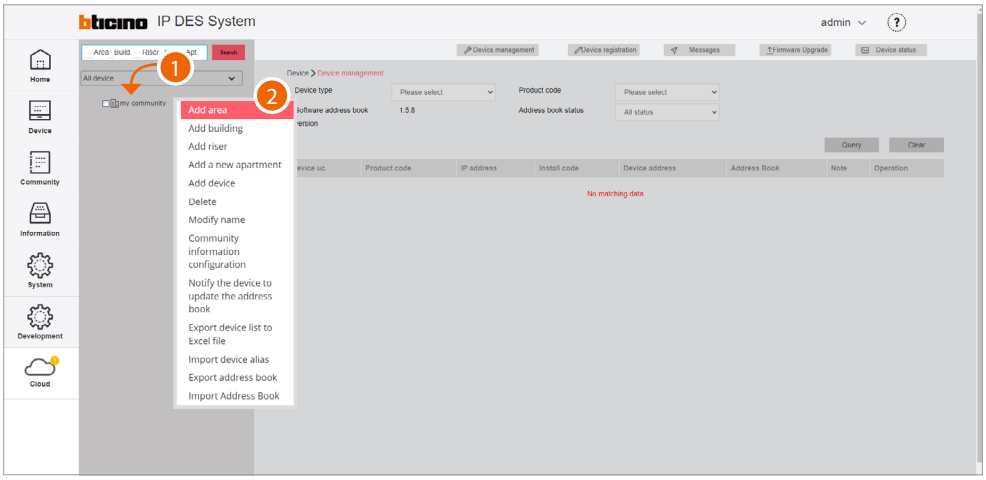
Depending on how your Community is composed, you will need to hierarchically enter:

AREA → BUILDING → RISER → FLOOR → APARTMENT → DEVICE

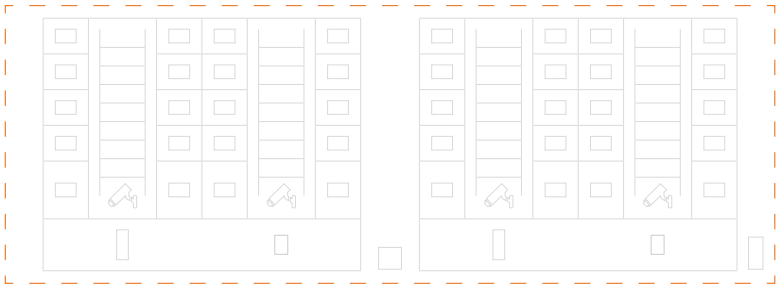
This document will show the creation of a sample structure composed as follows:

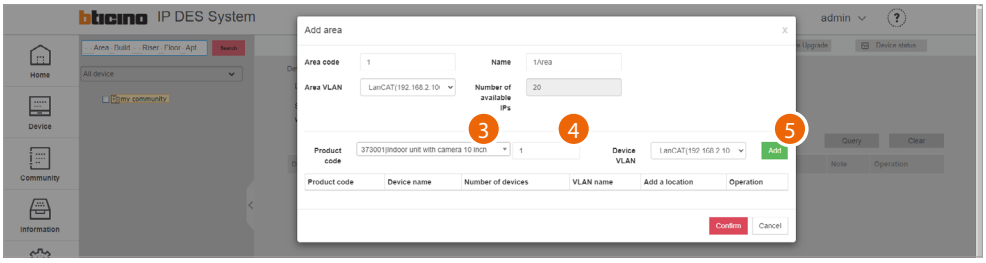


***Warning**: the configuration operations shown below are those required for creating the sample structure. See the Software Manual for all the other possible configurations.*



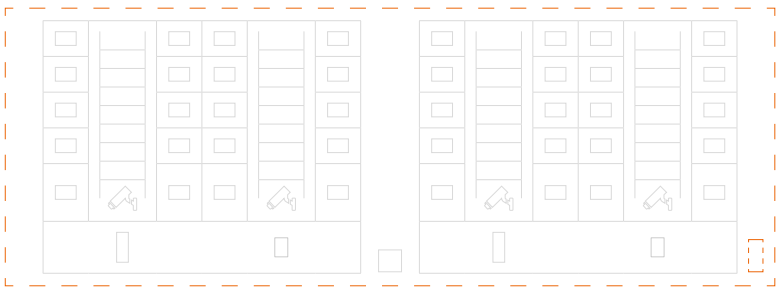
1. Click the Community with the right mouse button: a drop-down menu will appear with the commands for its configuration
2. Click to add a **new Area**

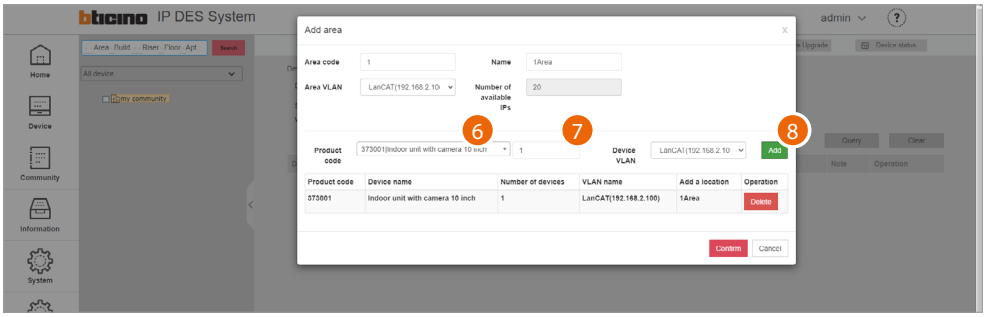




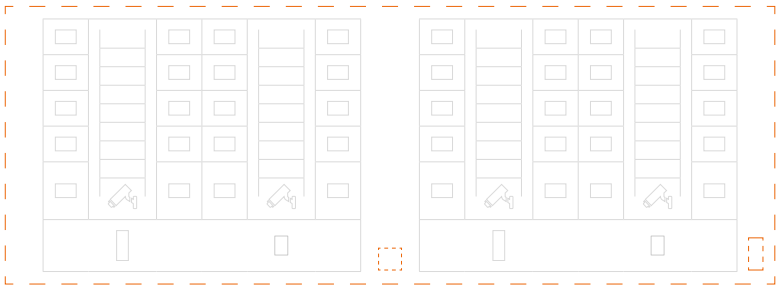
3. Select the Area device (EP Area1)*
4. Select the quantity
5. Click to add

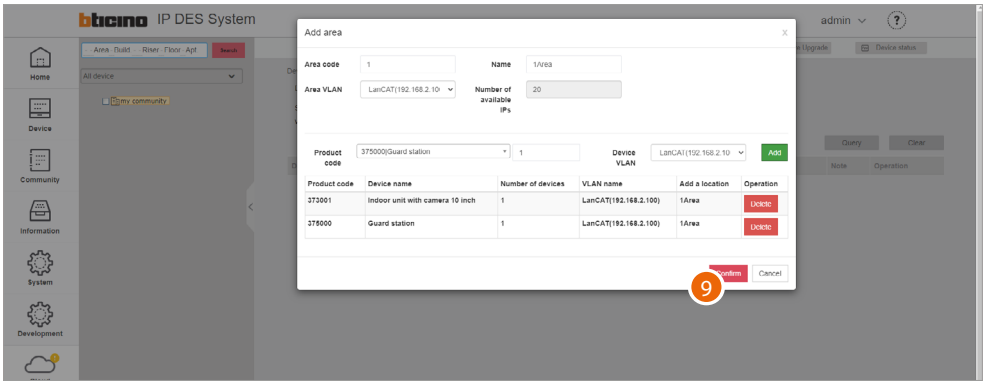
**Nota: prima di procedere con inserimento di un dispositivo ricordarsi di verificare che tutti i parametri del dispositivo rispettino le richieste, vedi* *Device parameter configuration*



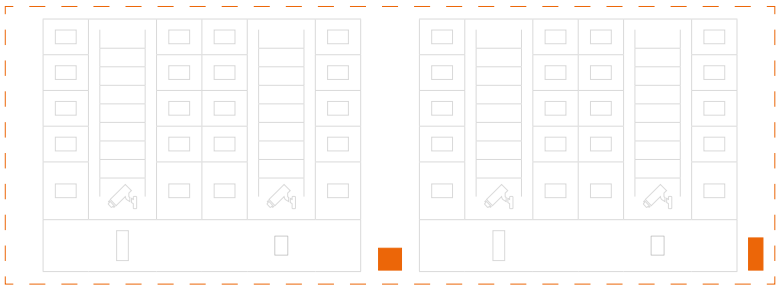


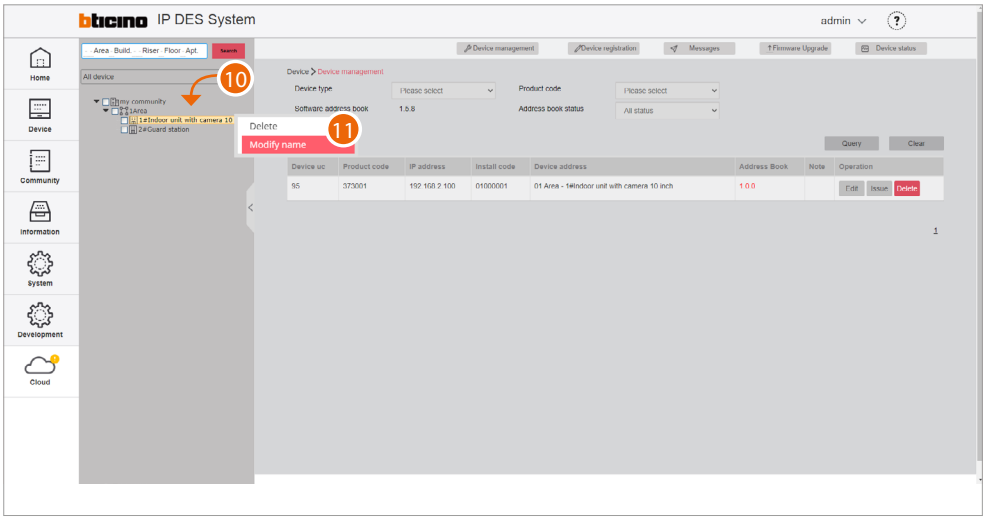
6. Select the second Area device (GS Area1)
7. Select the quantity
8. Click to add





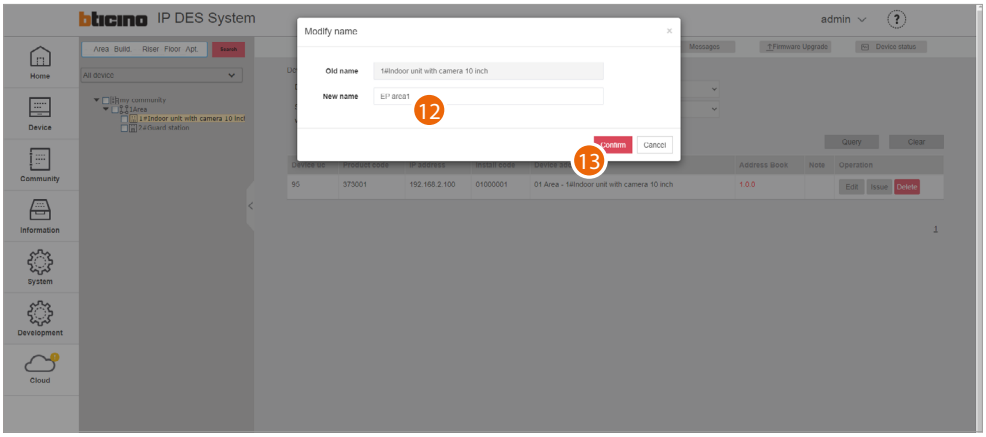
9. Click to confirm



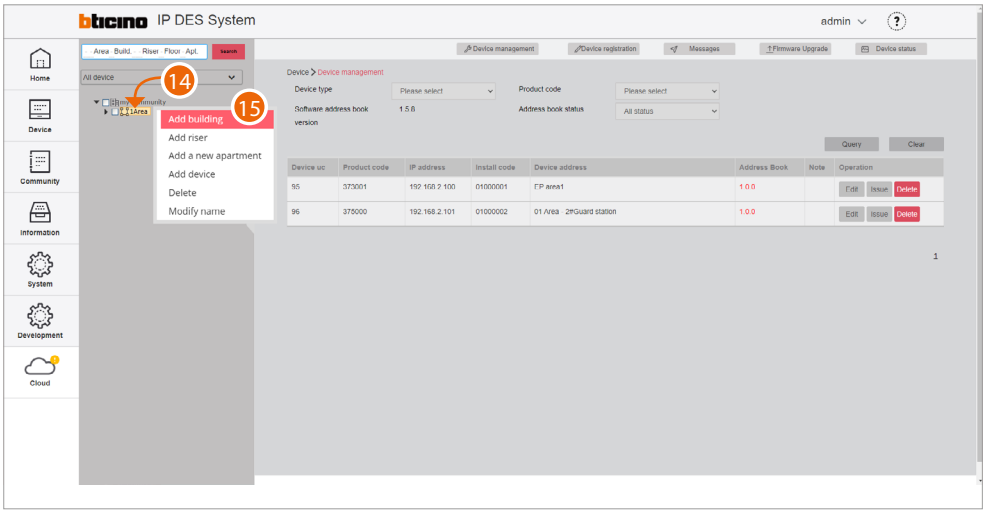


After inserting the devices, you will be able to customize their name

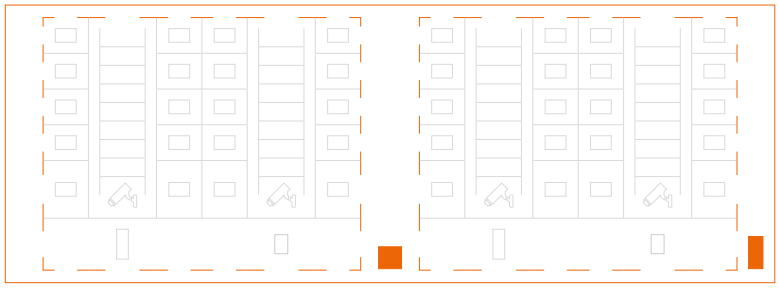
10. With the right mouse button click the device that you want to rename: a drop-down menu will appear
11. Click to open the edit window

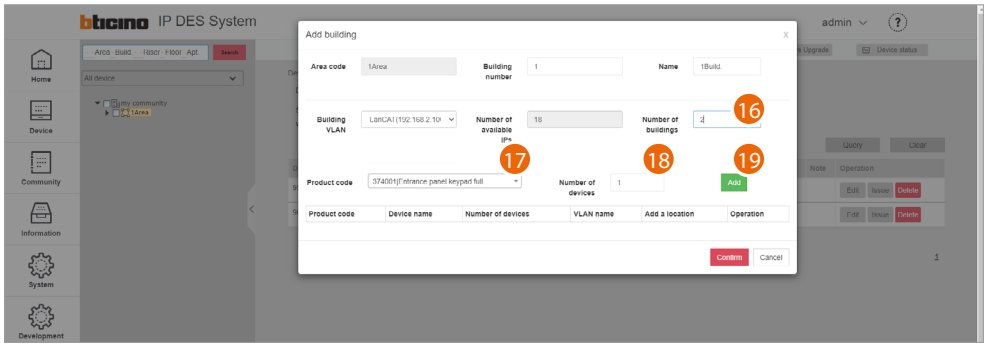


12. Enter the new name
13. Click to confirm



14. Click the Area with the right mouse button. This will open a drop-down menu
15. Click to add the **Buildings**

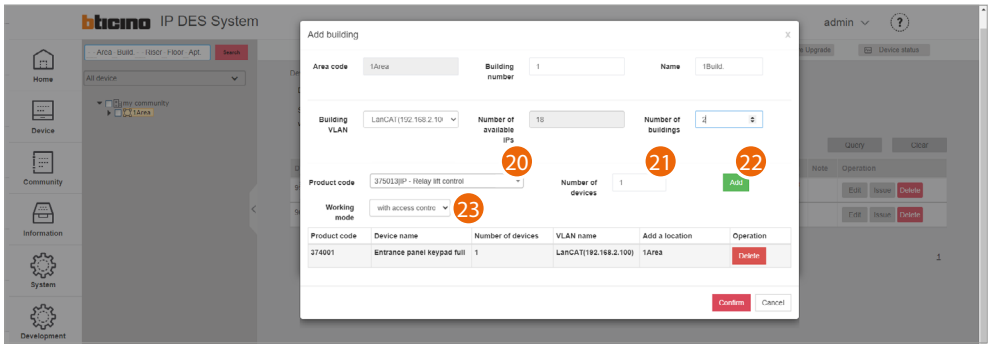




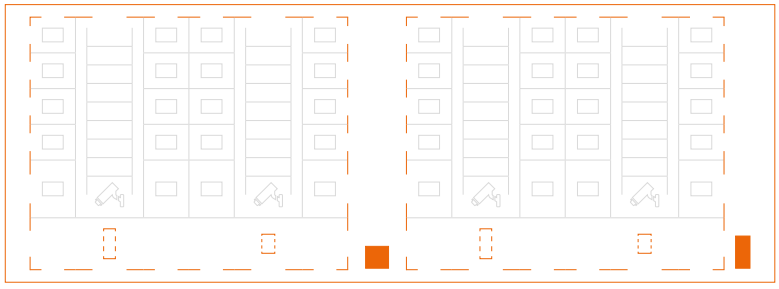
16. Select the number of buildings to add
17. Select the Building device (EP Building)

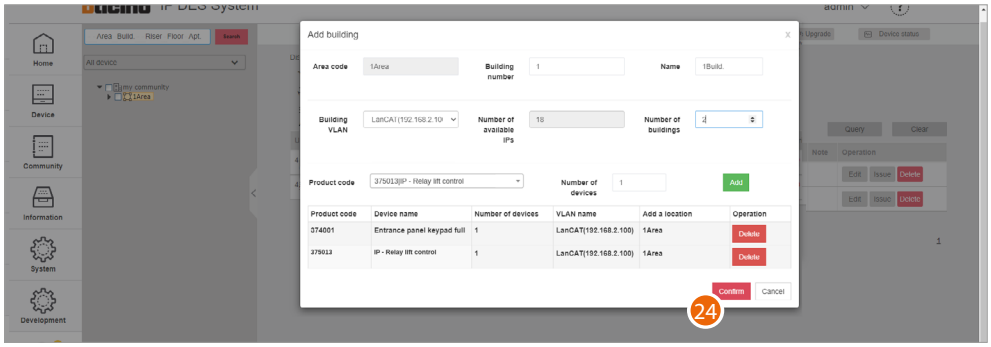
***Note**: the software automatically applies a filter to only show devices that are consistent with the component that you are adding*

18. Select the quantity
19. Click to add

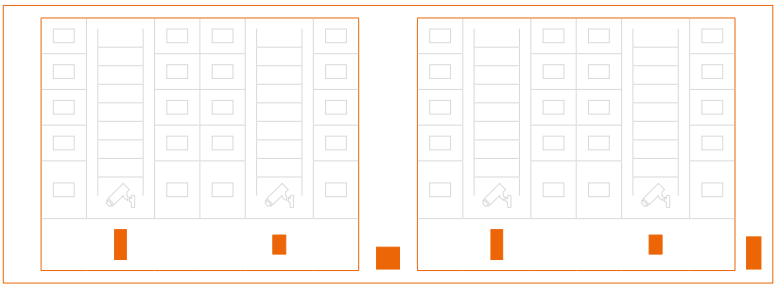


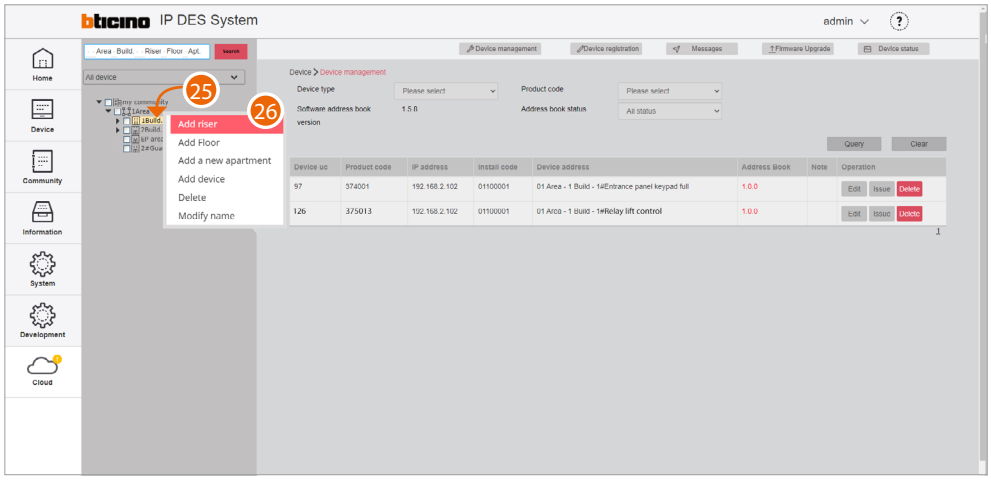
20. Select the device to add (lift control interface with relay 375013)
21. Select the quantity
22. Click to add
23. Select the operating mode:
    - **with access control**: this mode allows to set up an exclusive call to a specific floor (e.g. only go to the third floor)
    - **ground floor call**: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



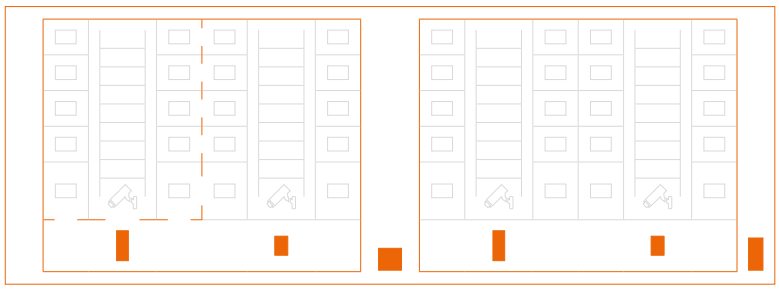


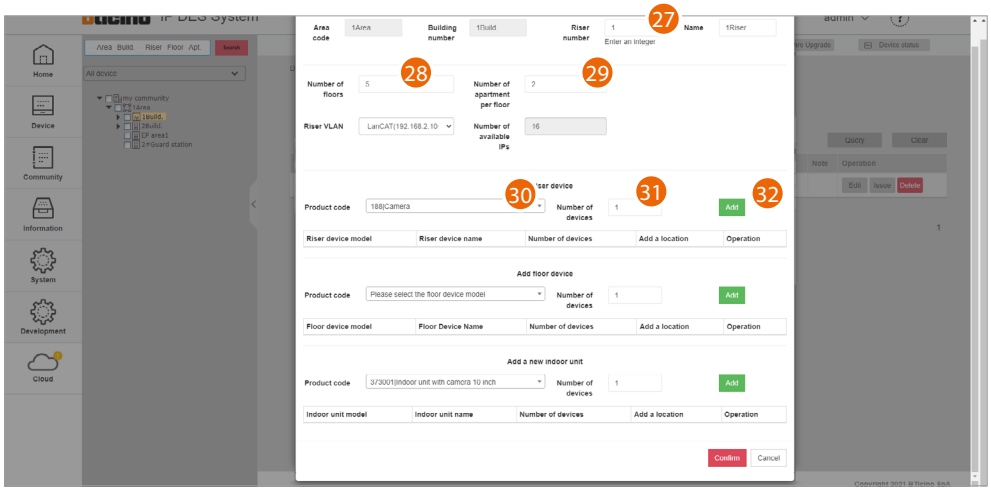
24. Click to confirm



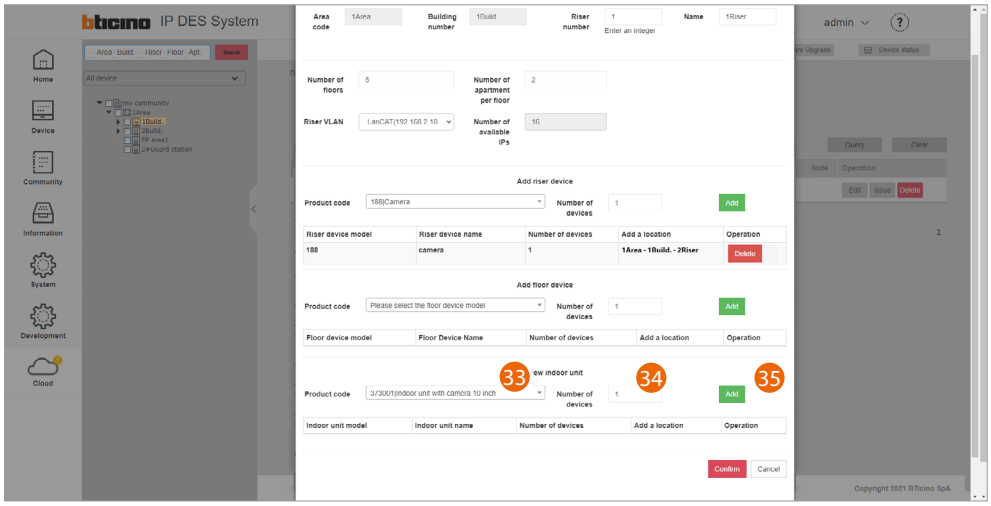


25. Click the Building with the right mouse button. This will open a drop-down menu
26. Click to add a **new Riser**

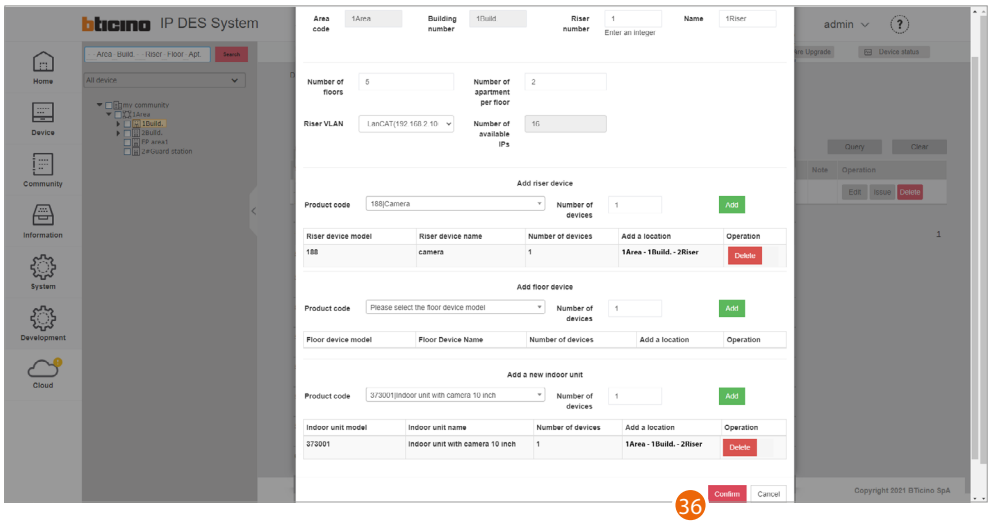




27. Enter the progressive Riser number
28. Select the number of Floors in the Building (5)
29. Select the number of Apartments for each Floor (2)
30. Select the OnVif IP camera
31. Select the quantity
32. Click to add

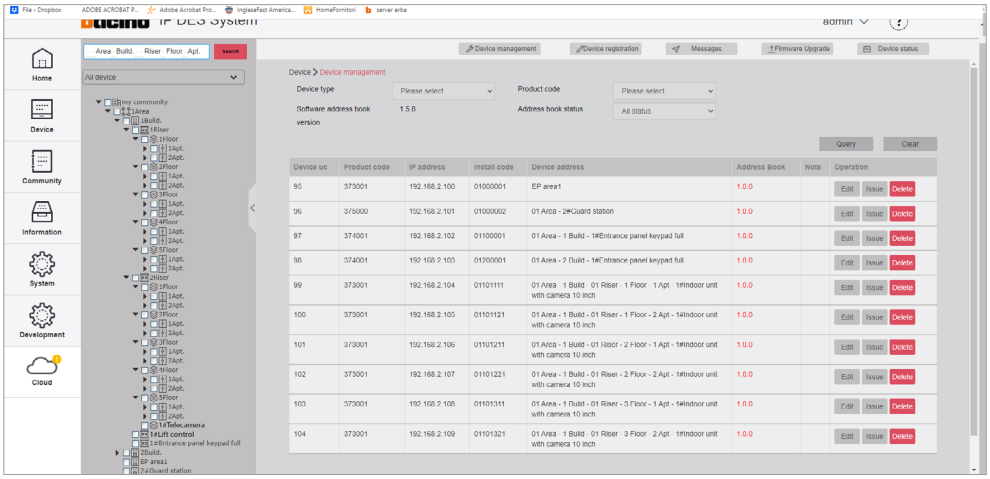


33. Select the apartment device
34. Select the quantity
35. Click to add

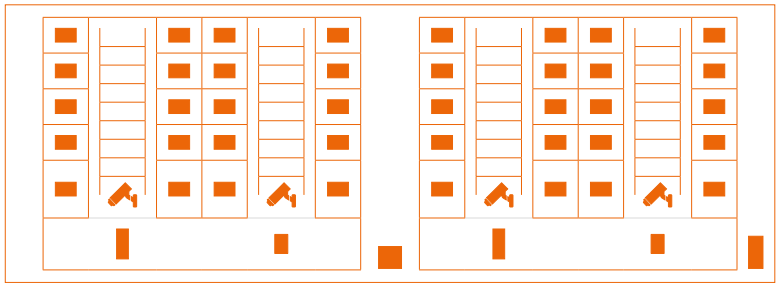


36. Click to confirm

Repeat the same steps for Riser 2

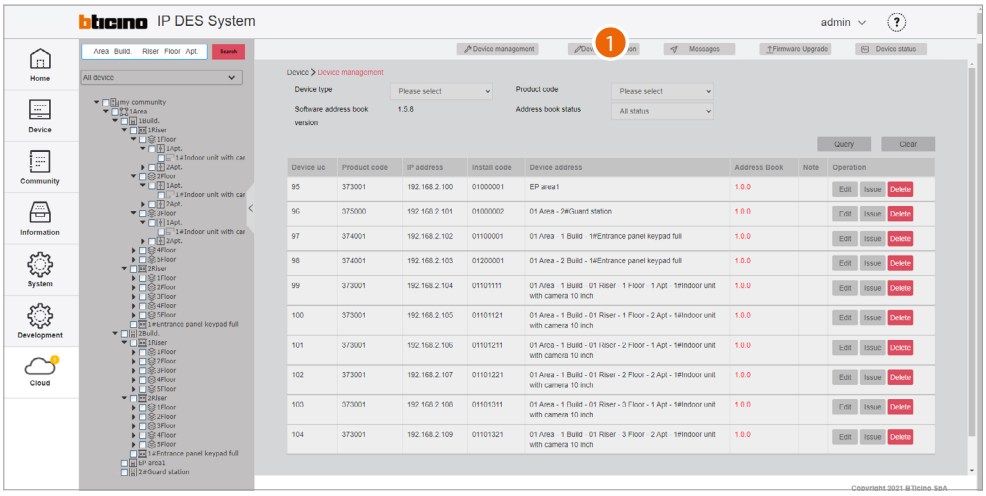


Repeat from step 21 also for building 2

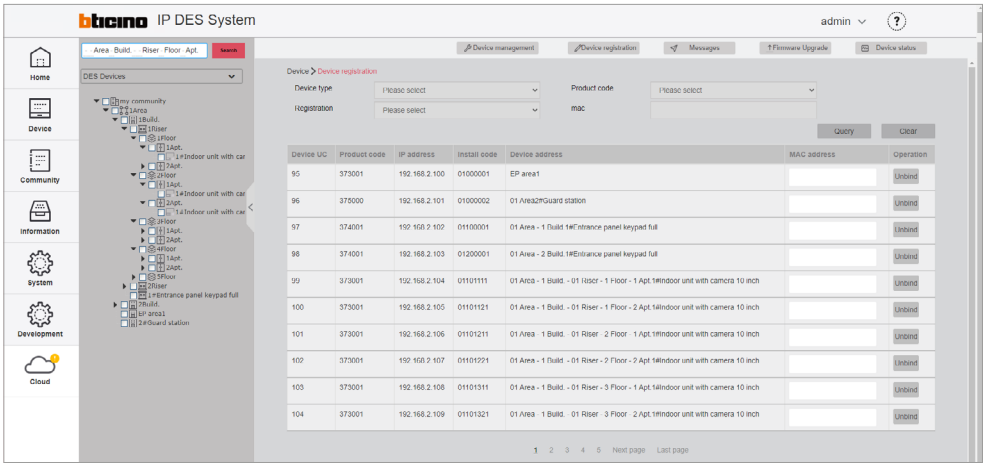


Device MAC address registration

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.

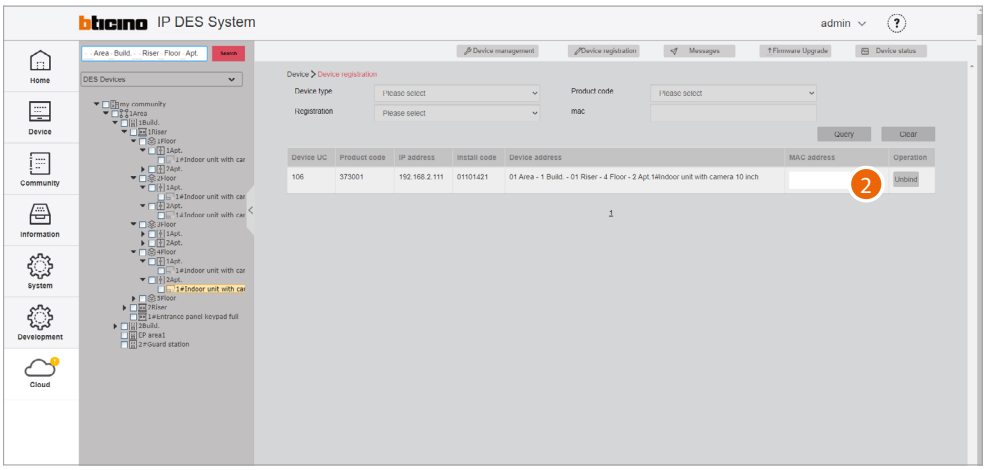


1. Click to enter the device registration section



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. Enter the MAC address

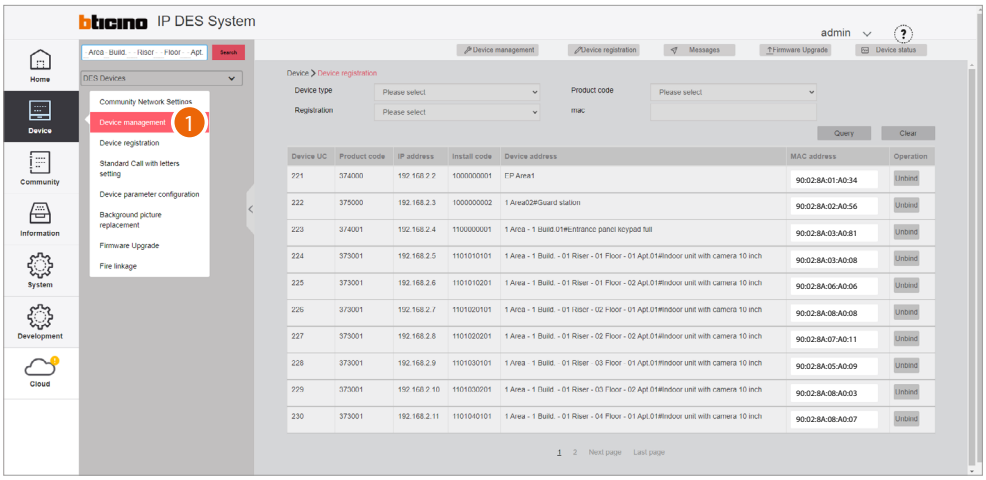
Repeat for all devices

Community customisation

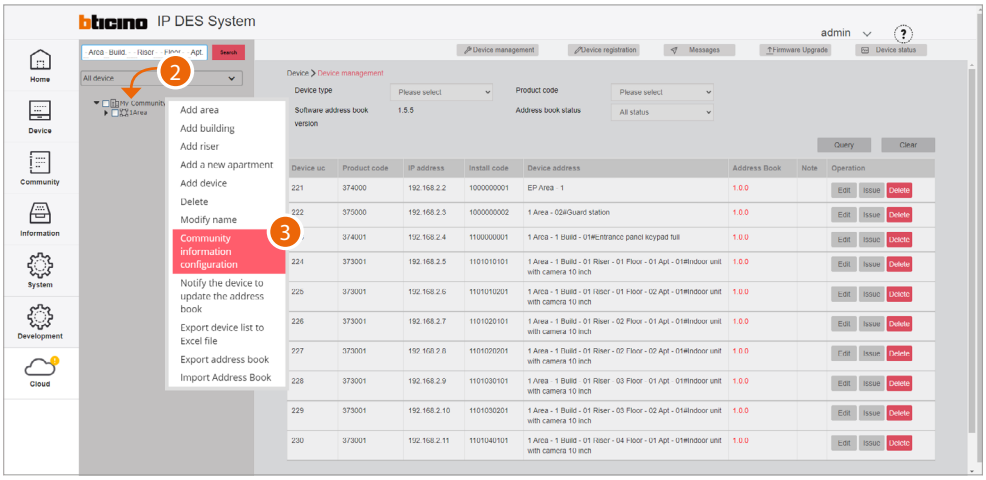
Before sending the configuration to the DES Server, we can customise the Community by e.g modifying the call mode and/or by enabling access to the Community for certain individuals.
To use a different call mode, (e.g. call mode via phonebook) to call residents, it will be necessary to:

– Change call type to alphanumeric/address book

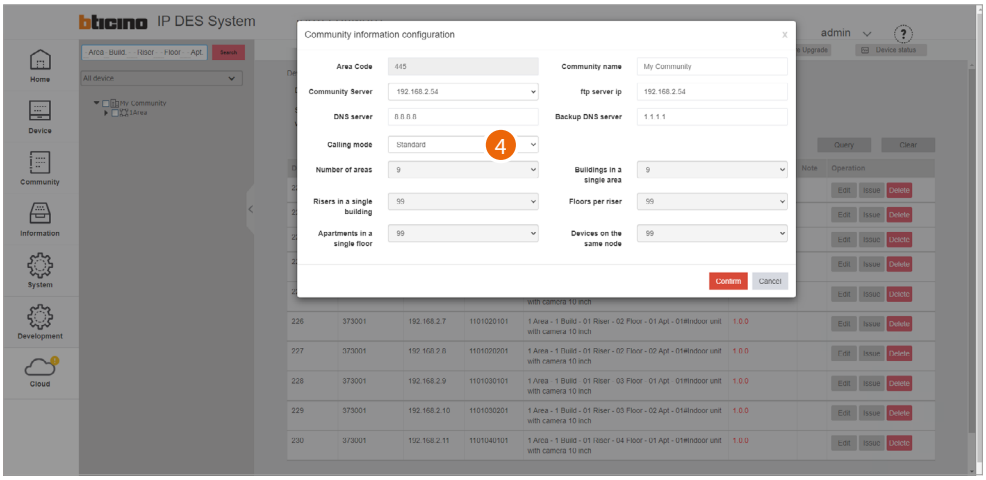
– replace the address in the community with an alias to facilitate recognition of the called party.
This function renames the apartment to a different name (alias).
The call to this apartment will be made using this new name.
E.g. JOHN SMITH



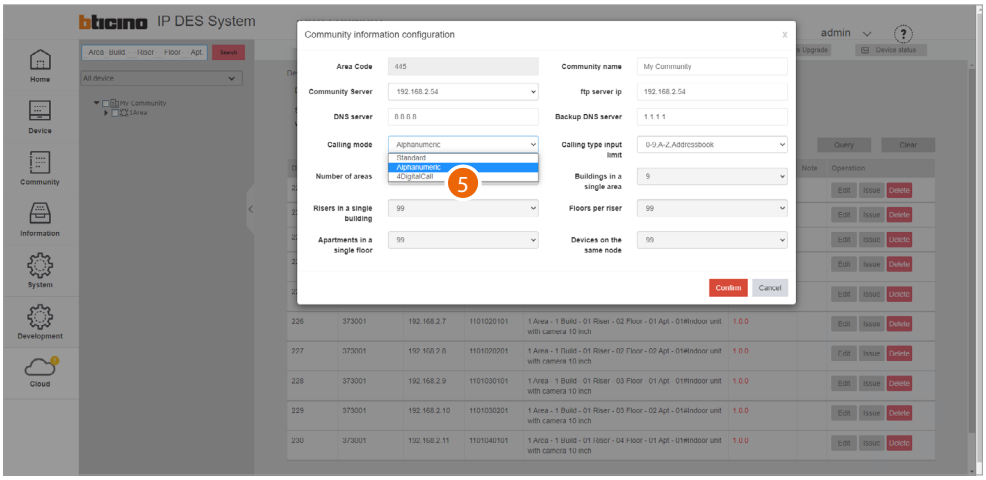
1. Select device/device management



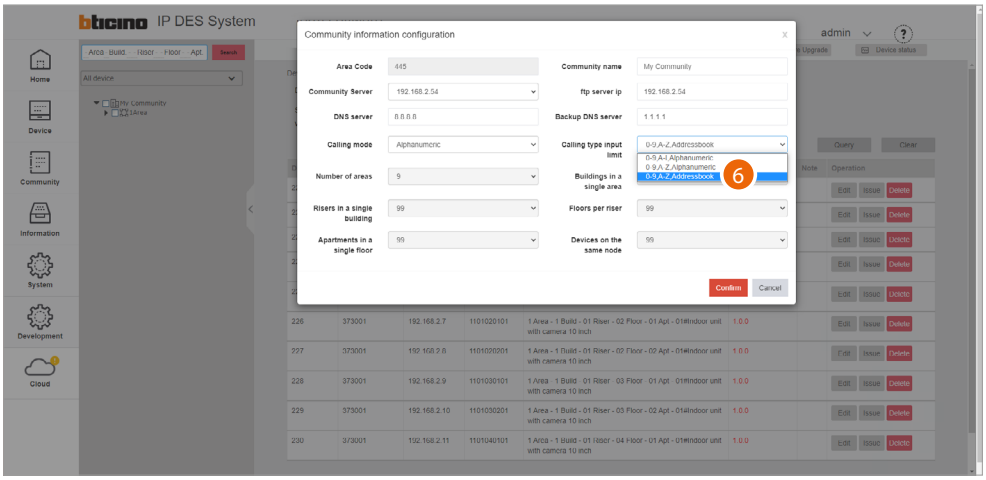
2. Right click the Community
3. Click to select the command



4 Click to modify the call mode



5. Select the alphanumeric mode

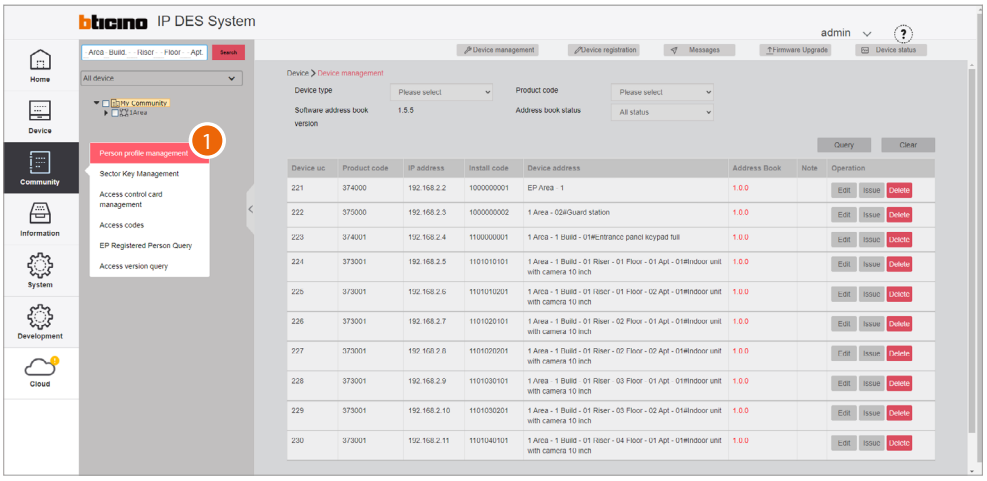


6. Select address book as entry type

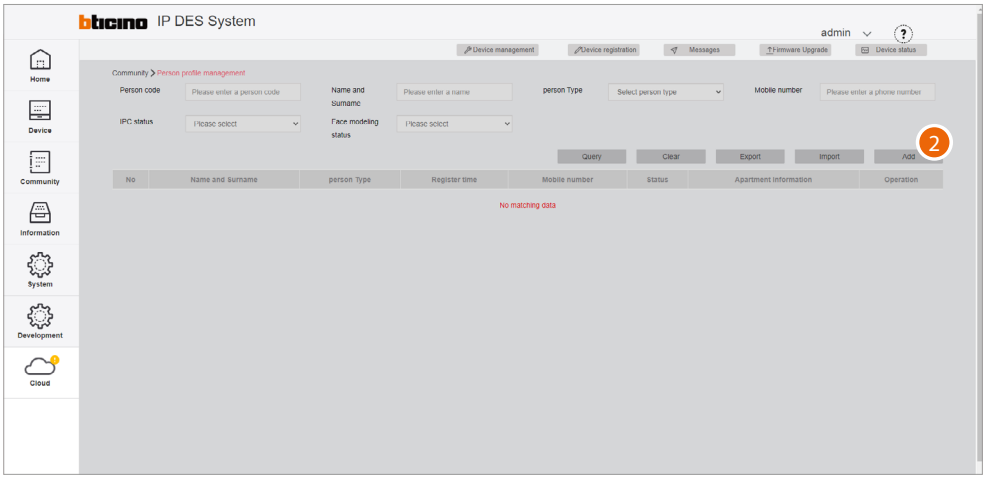
After sending the configuration to the DES server, it will be possible to call IUs using custom names (aliases). When changing the name of a GS or EP, this will be identified with this name on the receiving device when the call is made.

NOTE: *This alias format (Address Book) is not supported by entrance panels 374001/03*

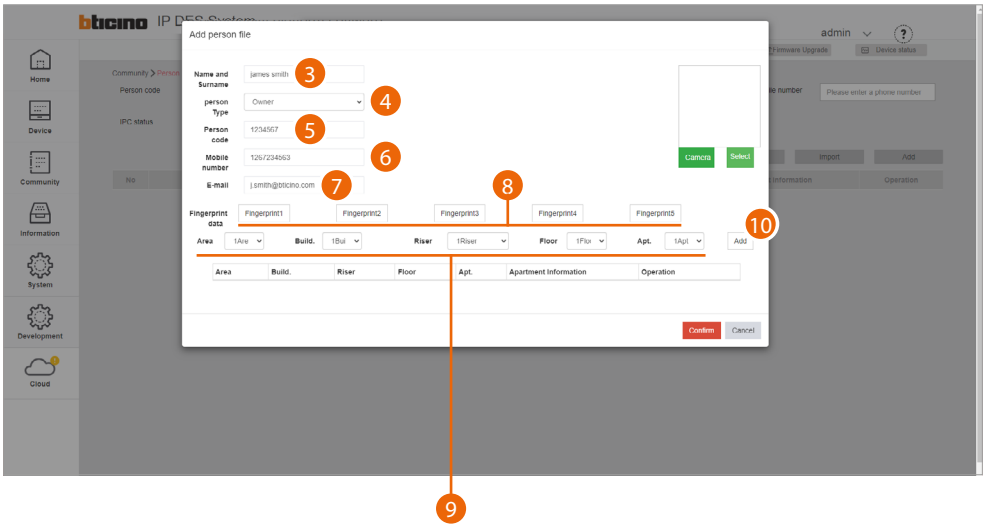
Now it is possible to add community people and give them permissions to access the structure. Depending on the type of person, different access permissions may be assigned, see Person profile management.



1. Select Community/Person profile management



2. Click to create a new person



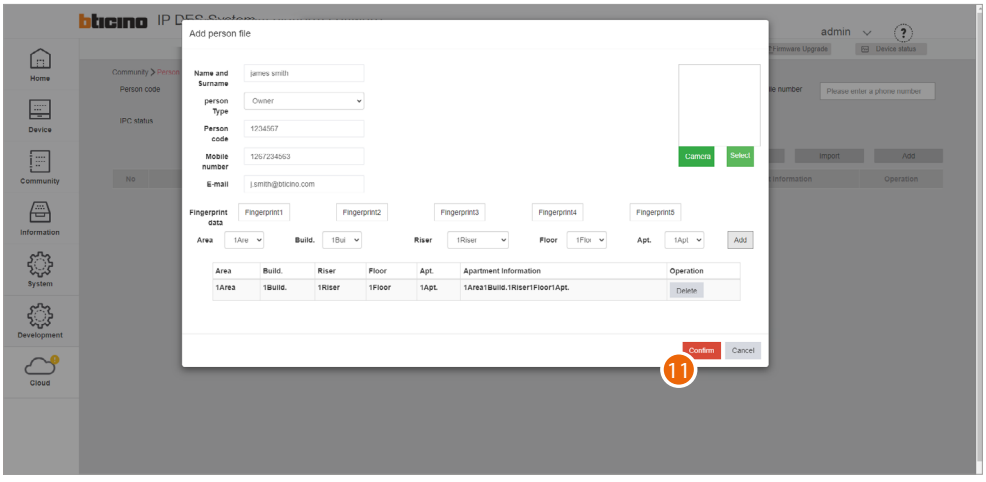
3. Enter the name and surname of the person
4. Select the type of person

Note: *some parameters may change depending on the type of person*

5. Person code
6. Enter the telephone number of the person
7. Enter the email address of the person
8. Register a fingerprint

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 to access the community, this must be registered; see Access control card management

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).

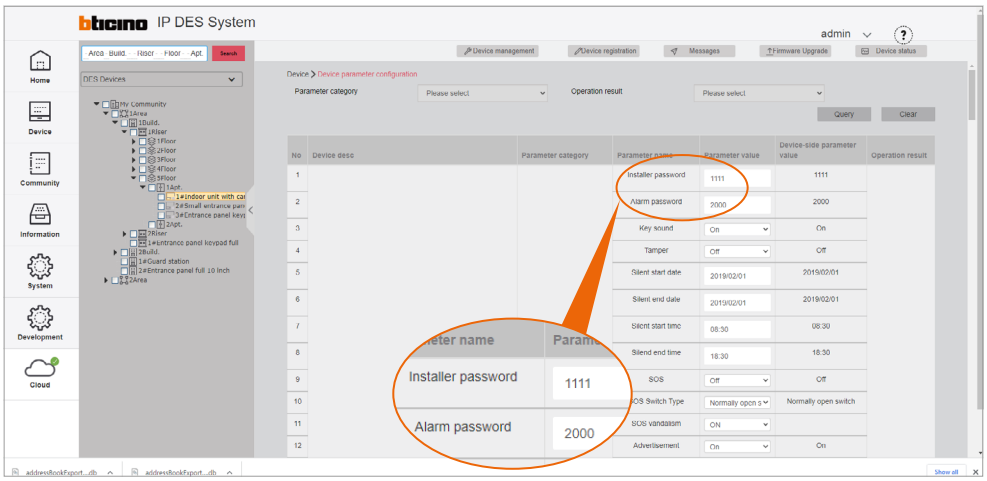
The access codes for opening the door locks of entrance panels are also generated in the same way.

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

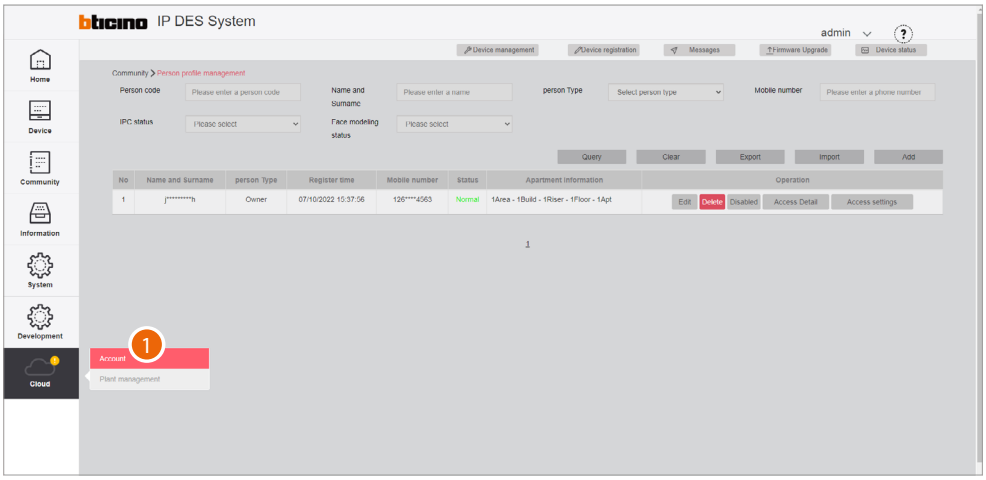
.....

1. Write down the passwords in a safe place that is always accessible.

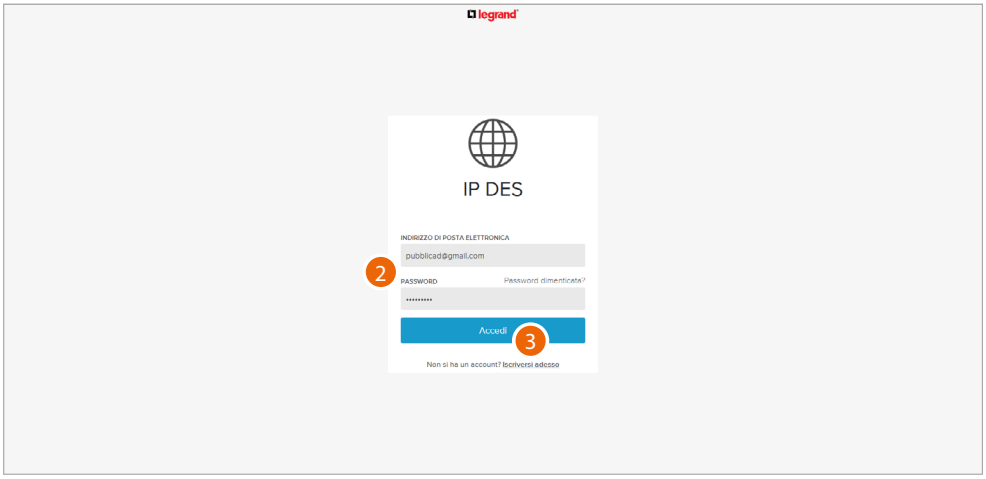
Registration of the community on the Installer's Cloud

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:

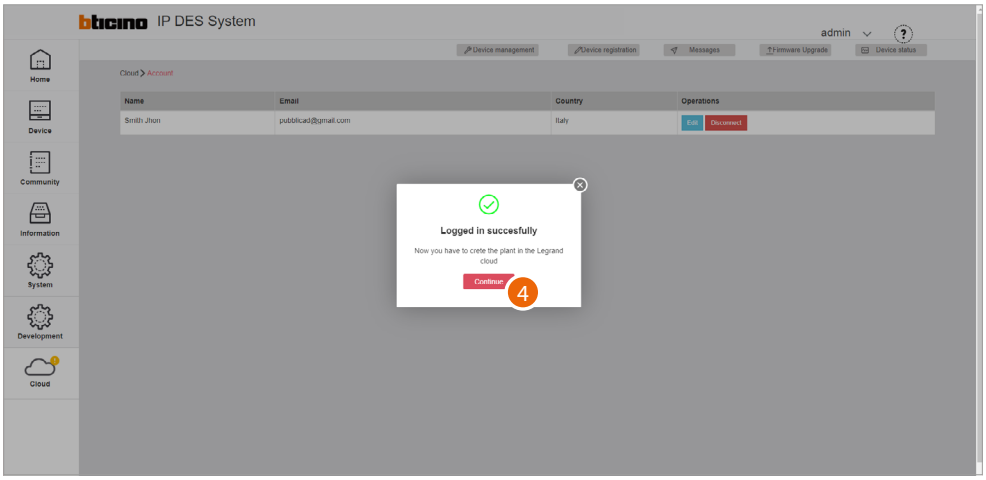
- have greater security in the event of local data loss
- associate the Home+Security app to the IU, for remote management of the video door entry system



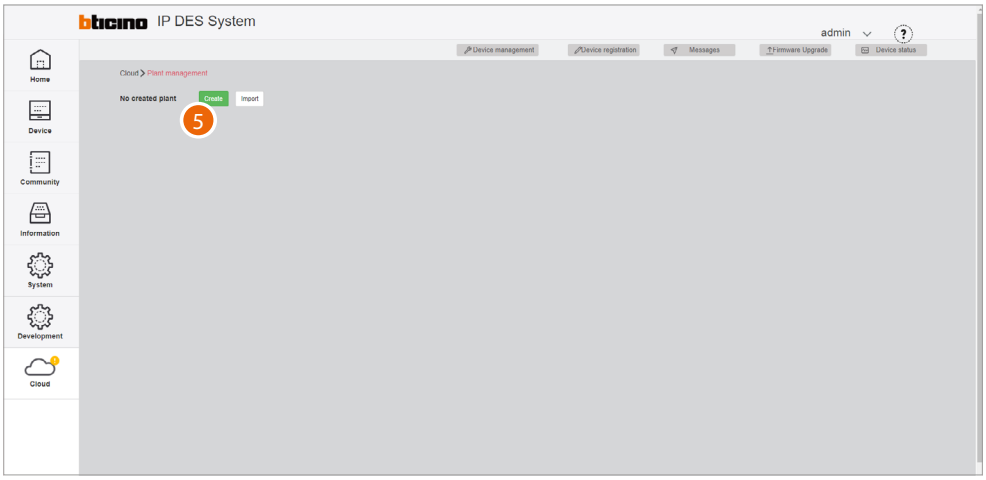
1. Click to complete the Installer's Cloud authentication process



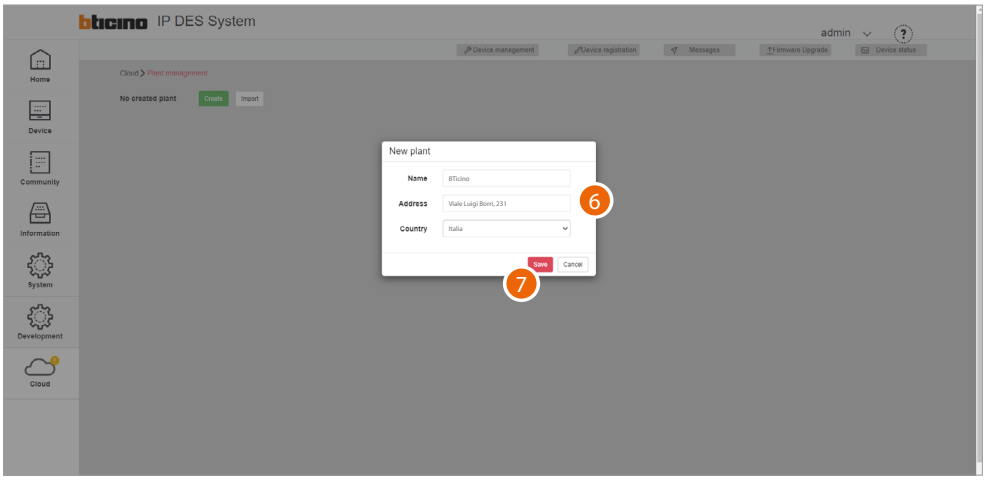
2. Enter email and password
3. Click to access



4. Click to confirm

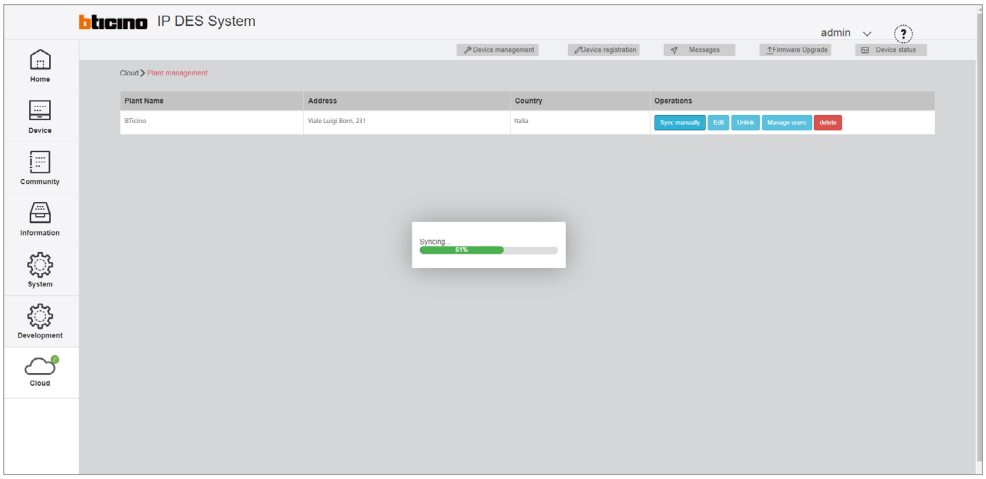


5. Click to create a new Plant



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

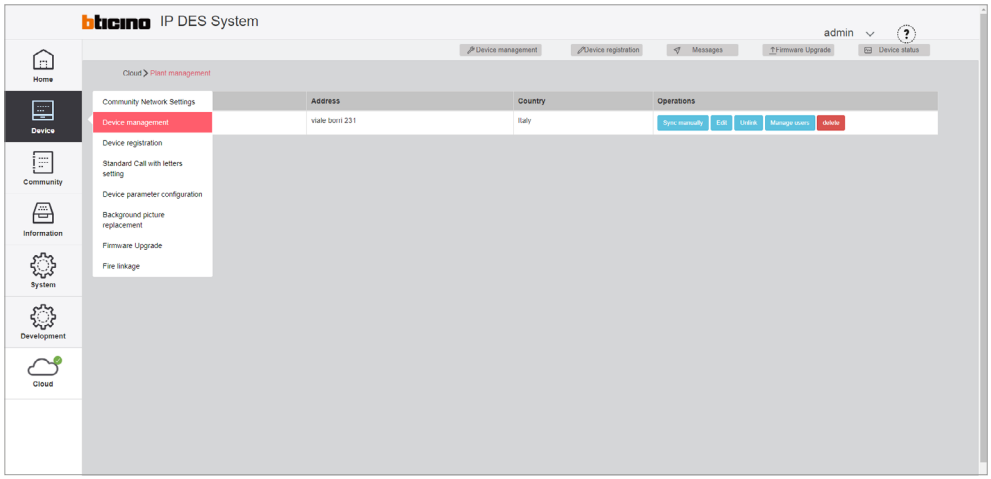
The plant is automatically synchronised



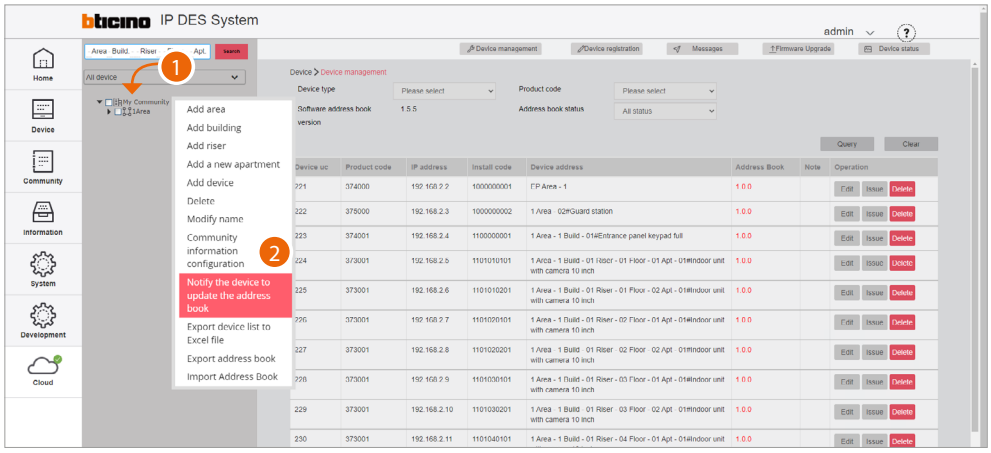
Once created, the plant remains available on the cloud.
If disconnected (unlink button), it can be retrieved from the cloud using the **Import a Plant** function.
If **deleted**, it will also be deleted from the cloud.

Notifying of the address book to the DES Server

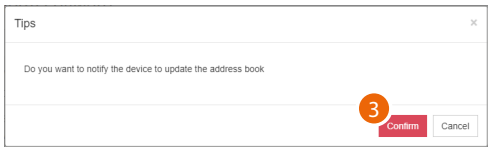
After creating the structure and configuring the virtual devices, it will be necessary to notify the address book to the system, therefore "instructing" the system to use this configuration.

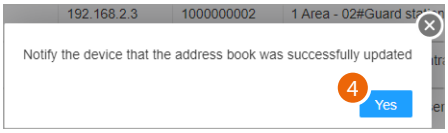


1. Select device/device management



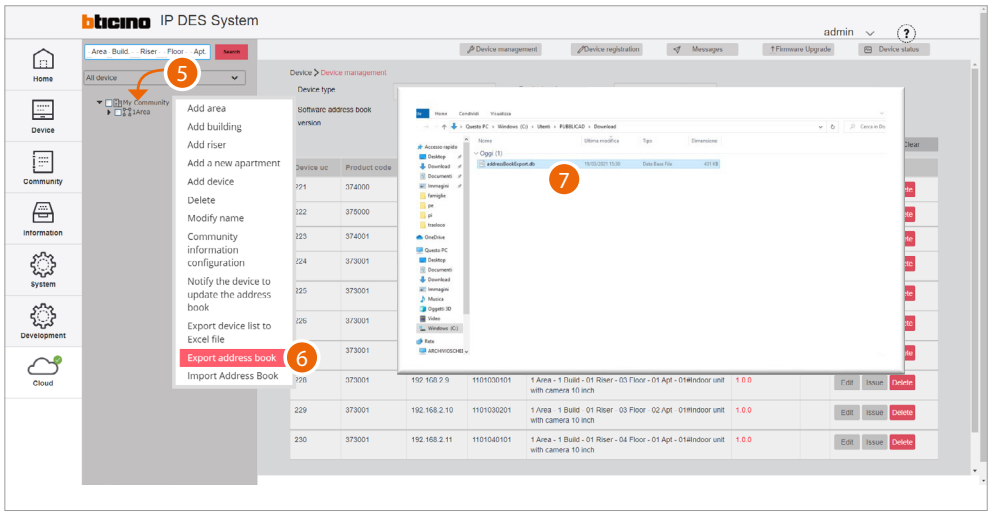
1. Click Community with the right mouse button: a drop-down menu will appear
2. Click to update the system address book





3. Click to confirm
4. Click to finish

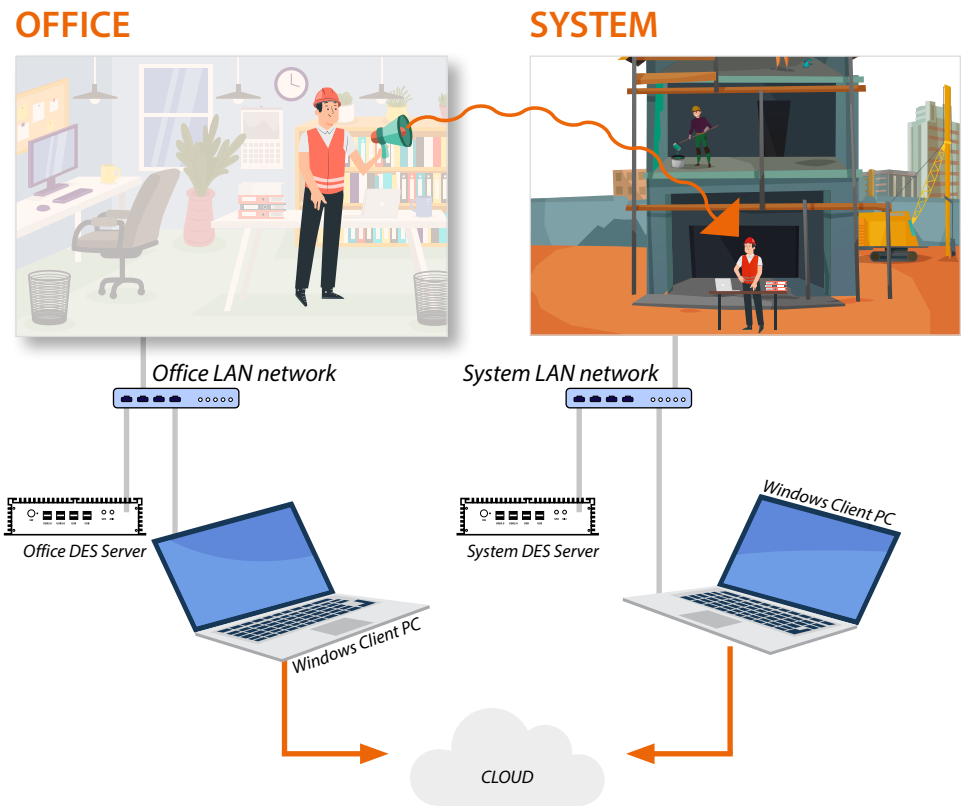
The address book is now saved in the DES Server. To avoid accidental loss, it is also possible to save it in an archive file.



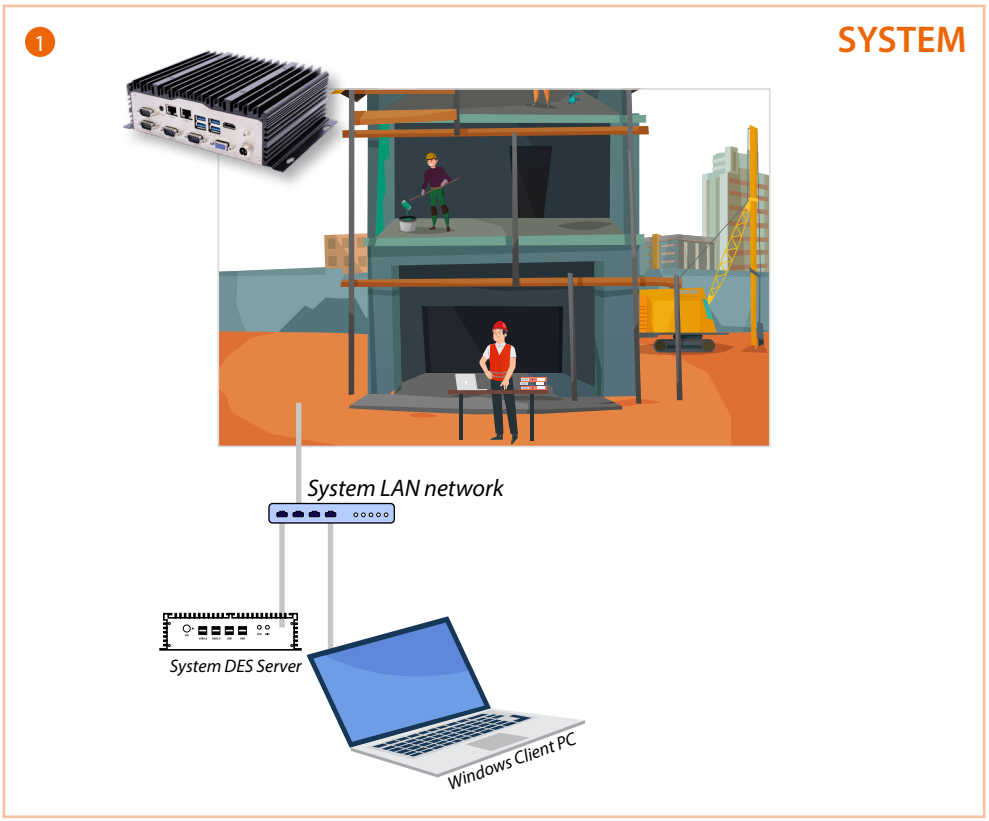
5. Click Community with the right mouse button: a drop-down menu will appear
6. Click to export the address book to a file
7. The file will be saved in the download folder of your computer

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



Connection of the DES Server on the system

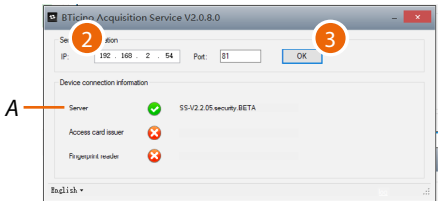


1. Connect the SD to the system LAN network

Setup of the fixed DES server address on the system router

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

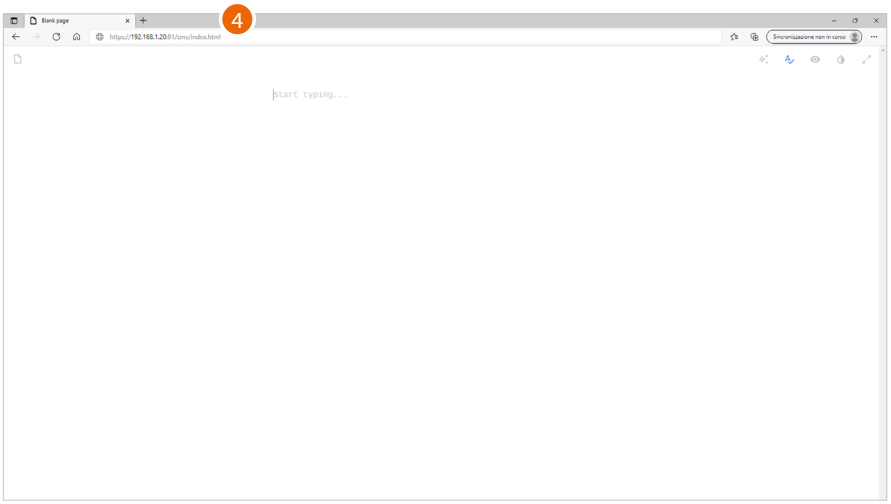
The following screen appears



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 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 MAC address identification (method 2).

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

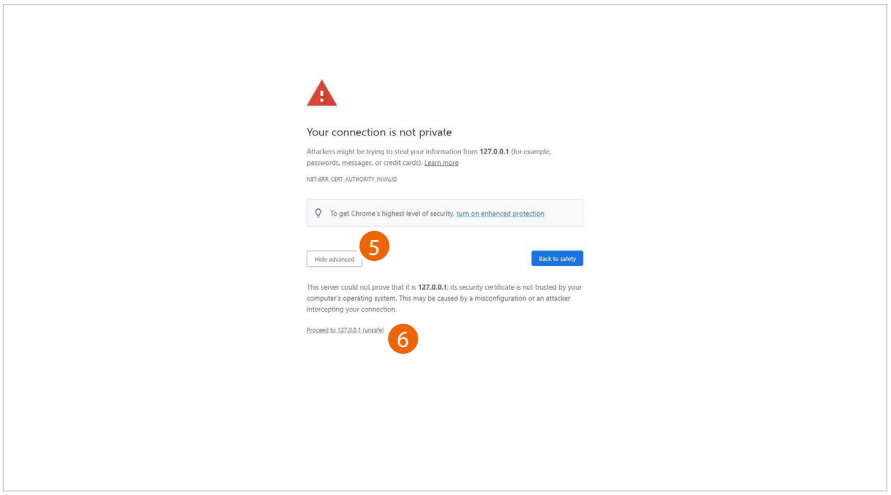


4. Open the browser and enter the http address of the DES Server:

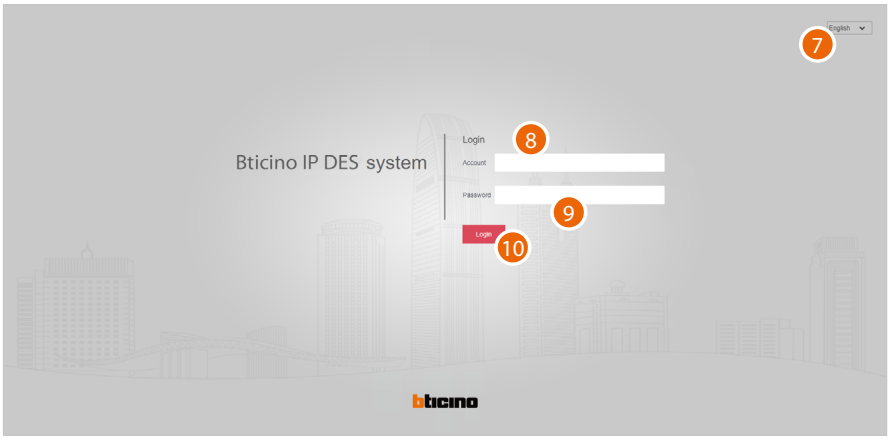
https://SD IP address:81/cms/index.html

Note: *use Crome/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. Click to confirm

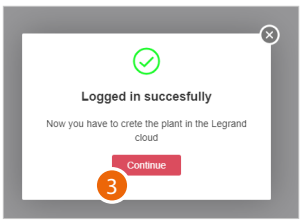
Plant authentication and synchronisation on the cloud

After logging in with the credentials provided by the office, it is possible to synchronise the Plant on the cloud

***NOTE**: alternatively, it is possible to import the configuration file provided by the office*

Authentication

1. Enter email and password
2. Click to access

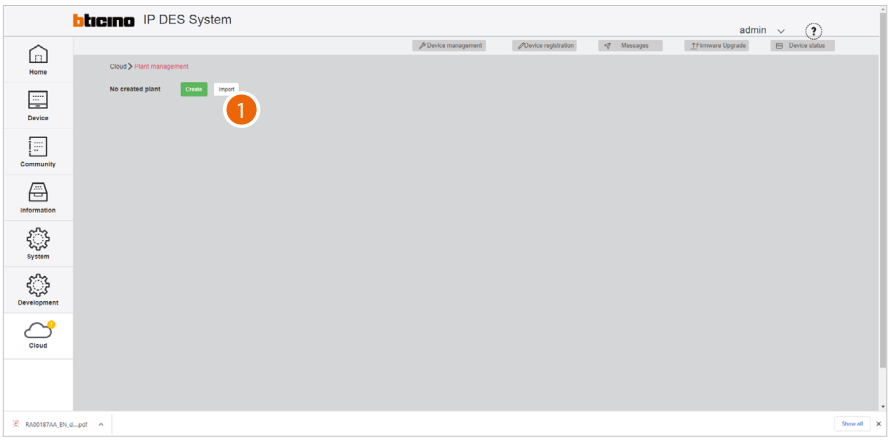


3. Click to confirm.

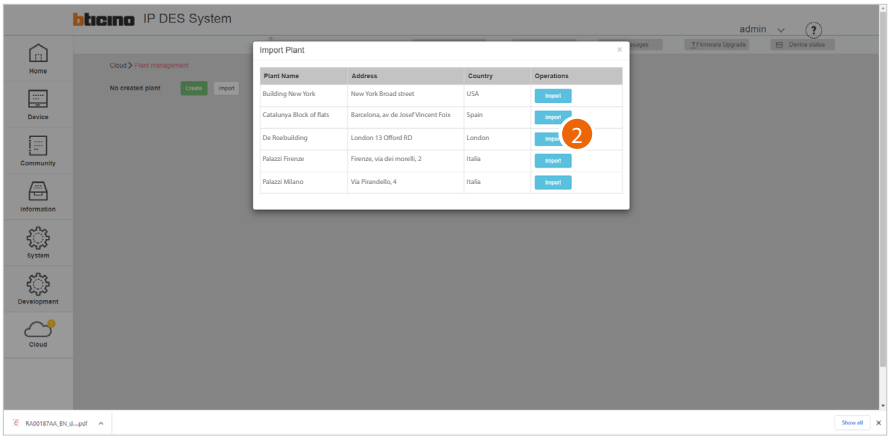
Import the Plant from the cloud

Now it is possible to import the Plant saved on the cloud from the office

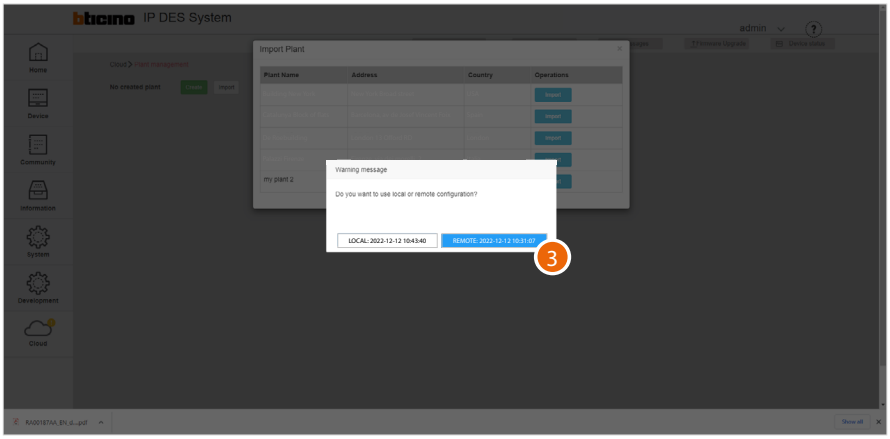
To access the Cloud see First access



1. Click to import the Plant from those saved.

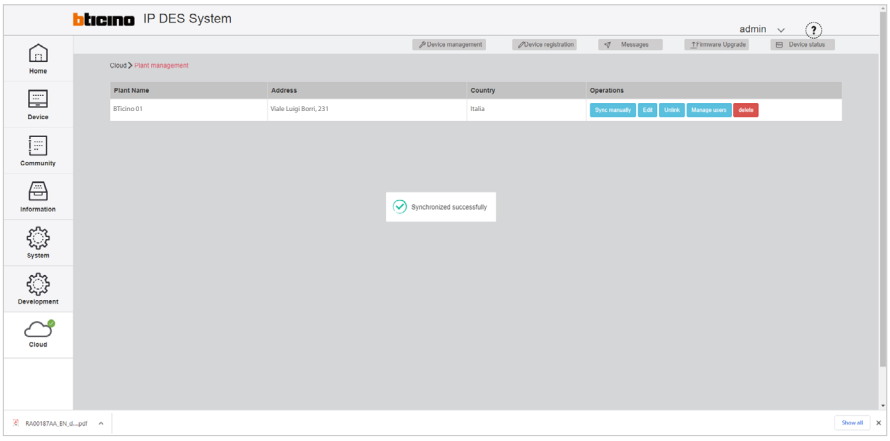


2. Click to import the plant



3. Click to import the plant version stored on the cloud

***Attention**: it is important to select the remote version created at the office.*

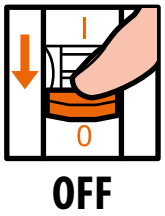


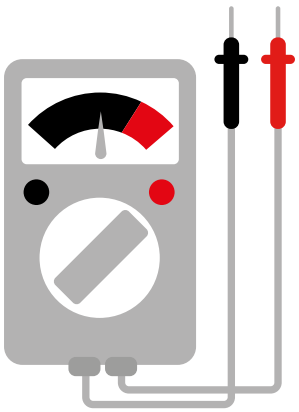
The Plant has been imported

Installation of the devices

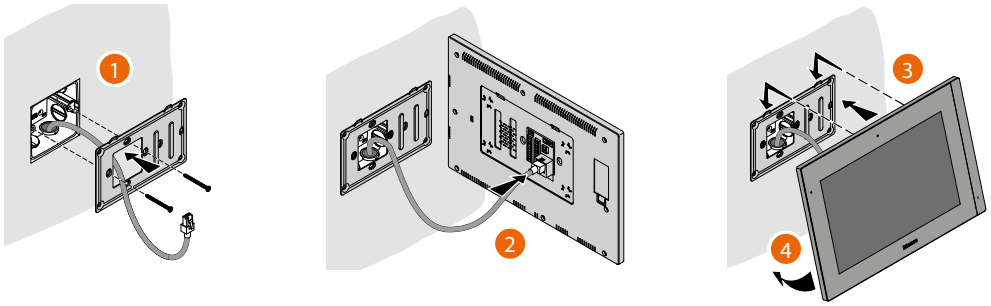
To transfer the configuration to the devices, these must be installed and powered

Switch off the power supply to the system and check that there is no voltage

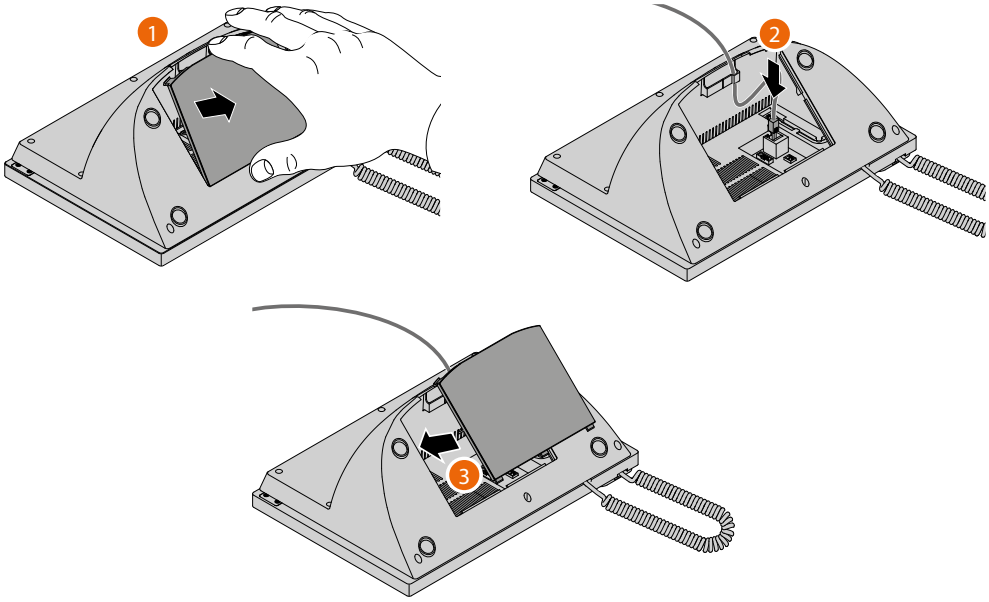




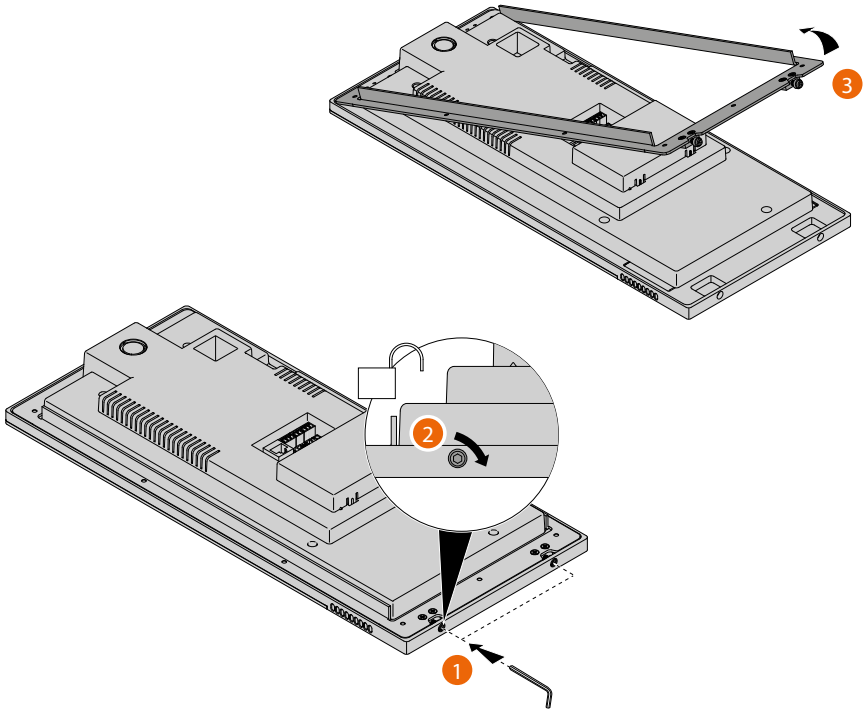
Install the devices

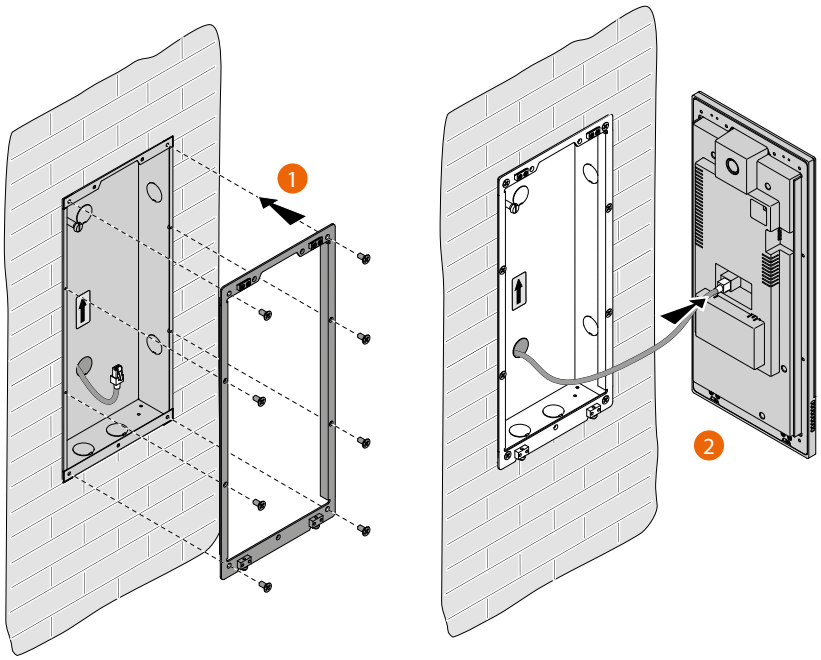


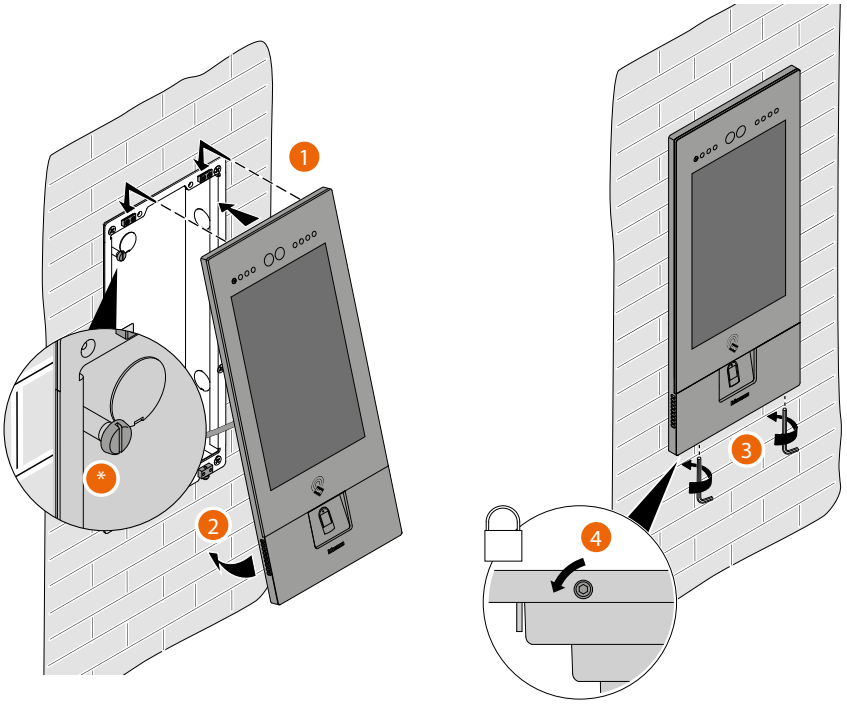
The RJ45 cable must be at least 200 mm long



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 sending an alarm to the guard station.

***Warning**: please note that the EP installation shown is representative of all EPs.*
For more details, see the specific instructions in the package

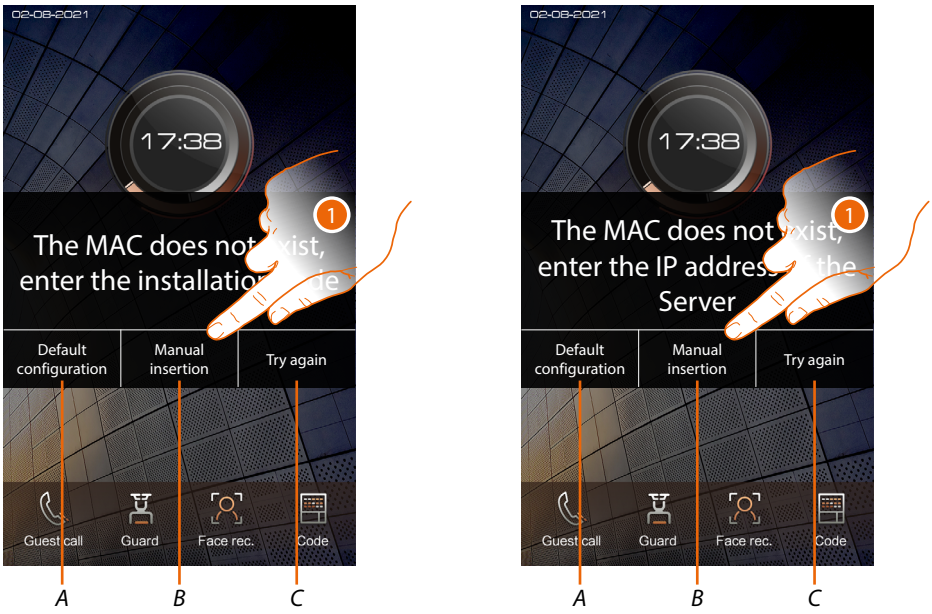
Reconnect the power supply

Activation of the devices

Thanks to the previously entered MAC address, once powered, the device checks that a configuration (address book) is available on the DES Server, and if so acquires 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.



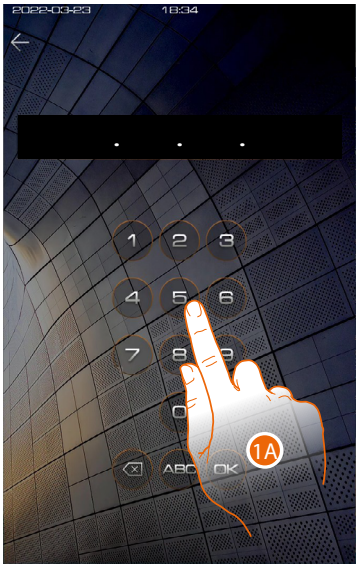
A Not to be used

B Button allowing 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 Community Network Settings, to display the installation code, see Installation code*

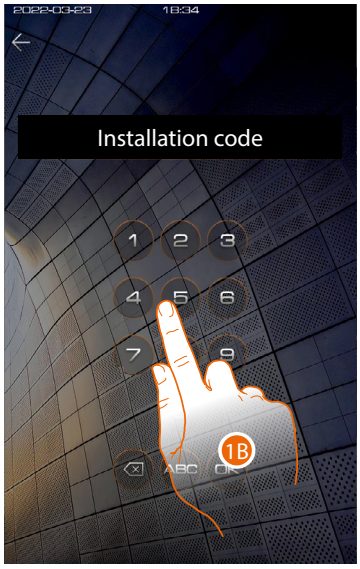
C Button to test the activation of the device

1. Click to manually enter the server IP address or the system access code

IP address



Installation code

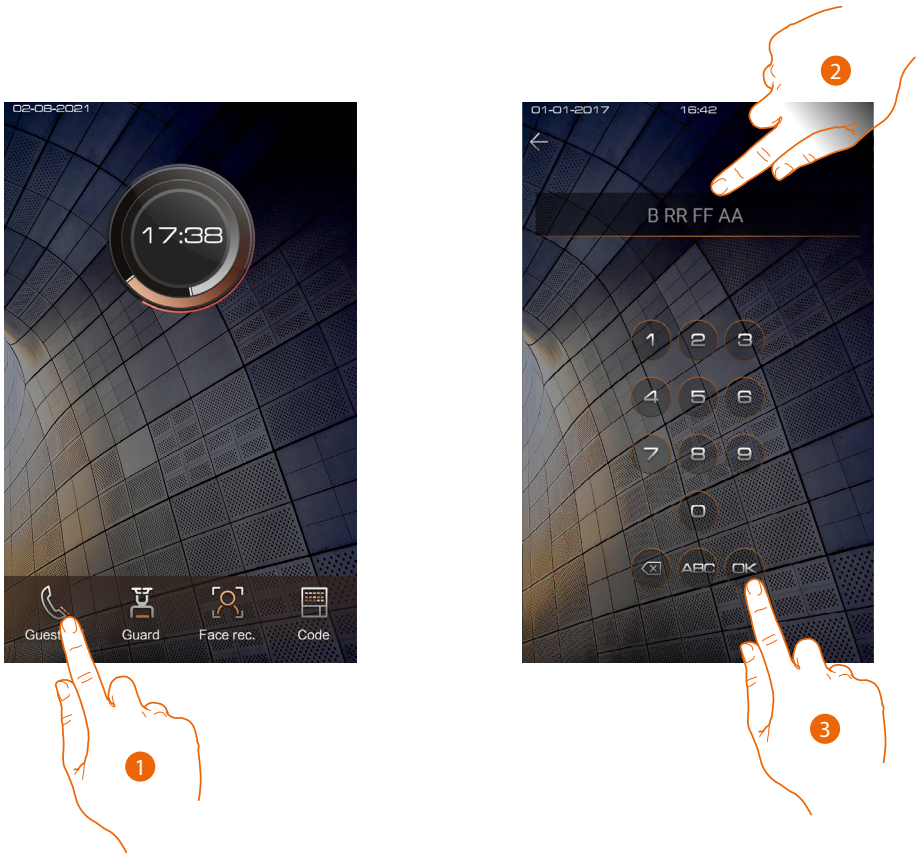


1A. Enter the IP address of the server

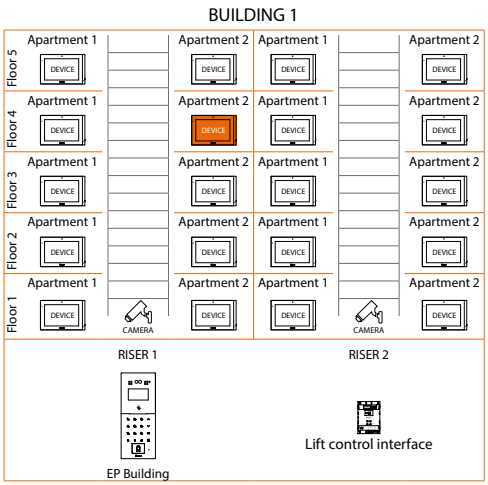
1B. Enter the installation code

System test

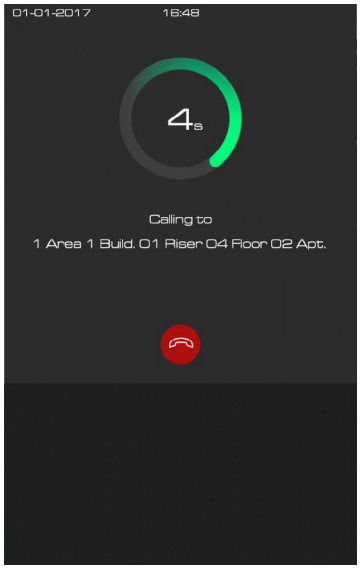
It is now possible to test the system, for example by making a call from the EP



1. Touch to make the call
2. Enter the IU address

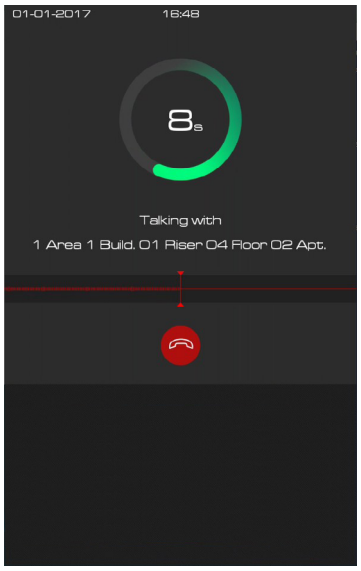


3. Touch to send the call



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. Tap to capture an image of the screen

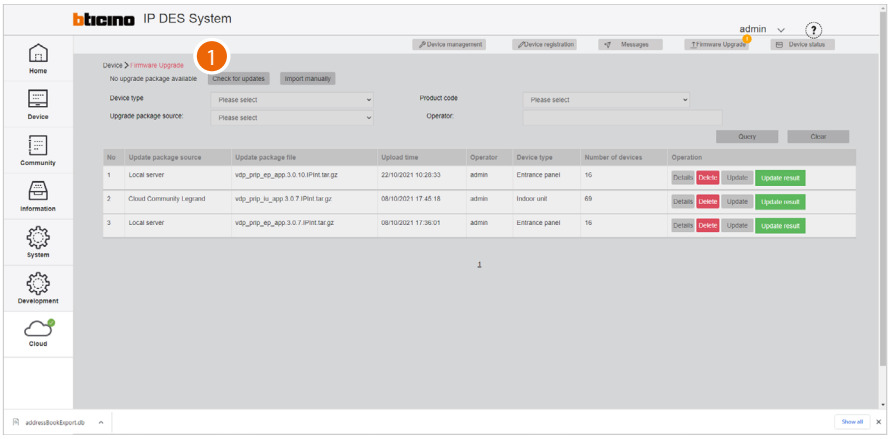
A confirmation message appears.

6. Touch to open the EP door lock

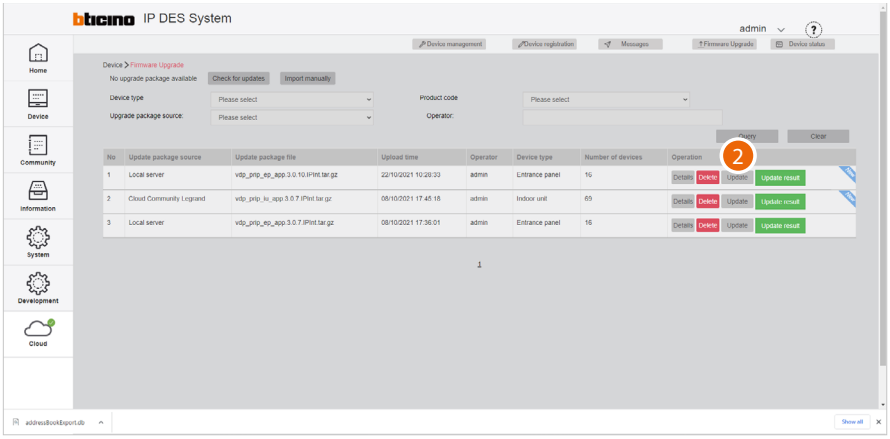
A confirmation message appears

7. Tap to adjust the volume
8. Touch to end the call

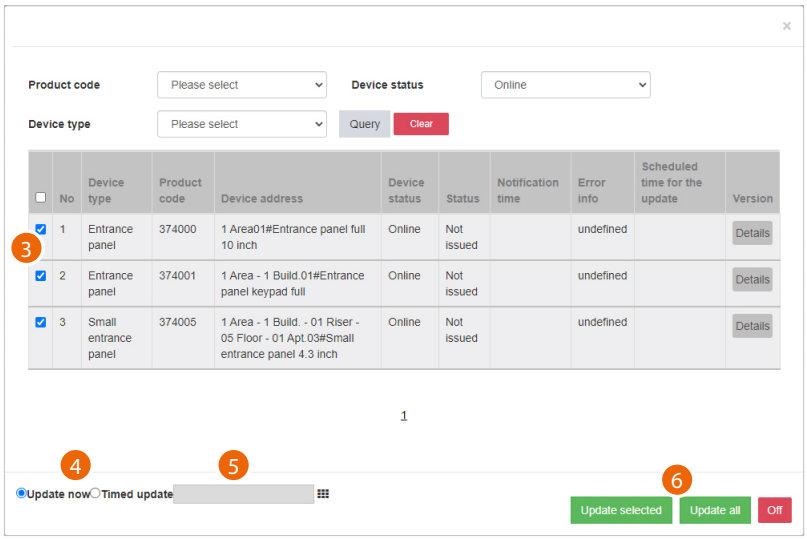
Update of the devices



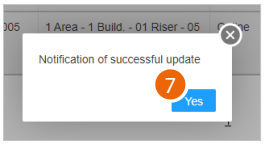
1. Click to check for updates on the cloud. If there are updates, these will be downloaded and available for installation
   ***NOTE**: firmware updates will only be downloaded if the last installed updates have already been deleted: the page must be empty.*



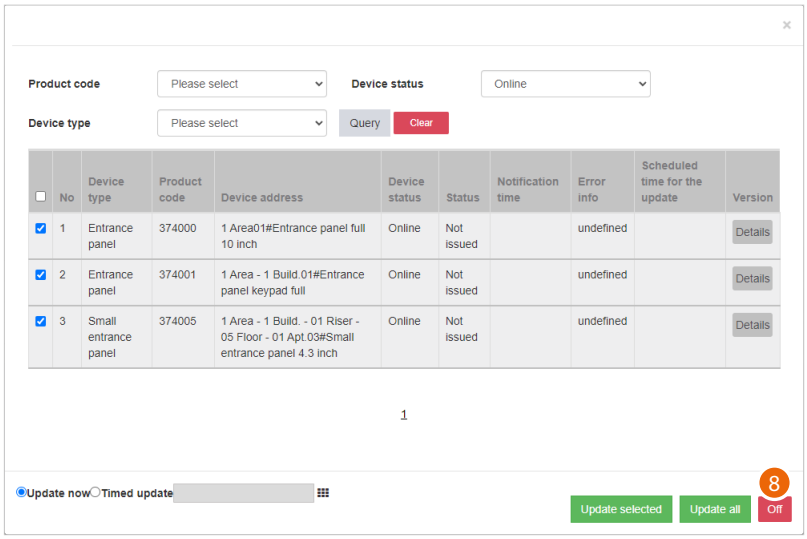
2. Click to send the update to the plant



3. After using the filters to display the relevant devices, select them
4. Decide whether to perform the update immediately or
5. Schedule an update, setting the date and time
6. Start the update for the selected devices or for all the devices



7. Click to finish



8. Click to close the panel

BTicino SpA
Viale Borri, 231
21100 Varese
www.bticino.com