



televic

confidea

Installation & User manual



***Attention:***

This manual for Wireless Confidea System 3.0 is valid only for all

WCAP+ firmware version            $\geq 1.06$

WCAP fpga version                  $\geq 1.06$

WDU+ firmware version            $\geq 1.06$

WCAP+ 71.98.0033

Cocon                                  $\geq 3.02$

## General information

|                       |   |
|-----------------------|---|
| 1 Copyright Statement | 4 |
| 2 Trademarks          | 5 |

# 1 Copyright Statement

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without the prior written permission of the publisher, except in case of brief quotations embodied in critical articles or reviews. Contents are subject to change without prior notice.

Copyright© 2008 by Televic Conference NV. All rights reserved.

The authors of this manual have made every effort in the preparation of this book to ensure the accuracy of the information. However, the information in this manual is supplied without warranty, either express or implied. Neither the authors, Televic Conference NV, nor its dealers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

## 2 Trademarks

All terms mentioned in this manual that are known to be trademarks or service marks have been appropriately capitalized. Televic NV cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

### 3 Contents

|      |   |    |
|------|---|----|
| 1    | Copyright Statement                                       | 4  |
| 2    | Trademarks  | 5  |
| 4    | How to connect  | 8  |
| 4.1  | Power up  | 8  |
| 4.2  | Accessing the web-browser                                 | 8  |
| 4.3  | Login wizard  | 8  |
| 4.4  | Introduction  | 8  |
|      | First time access   | 8  |
| 4.5  | Return to factory settings                                | 11 |
| 5    | Web server  | 12 |
| 5.1  | Compatibility   | 12 |
| 5.2  | Navigating through the webserver                          | 13 |
| 5.3  | Changing IP address                                       | 14 |
| 5.4  | Initialization  | 16 |
|      | 5.4.1 Controlled Access                                   | 16 |
| 5.5  | Unit Manager  | 17 |
|      | 5.5.1 Define groups                                       | 18 |
|      | 5.5.2 Define delegate names and assign to group           | 18 |
|      | 5.5.3 Remove delegate                                     | 19 |
|      | 5.5.4 Visualize delegate names or numbers in unit manager | 19 |
| 5.6  | Unit monitoring   | 20 |
| 5.7  | Activating microphones                                    | 21 |
| 5.8  | Conference options  | 21 |
|      | 5.8.1 Max active microphones                              | 21 |
|      | 5.8.2 Microphone modes                                    | 22 |
|      | 5.8.3 Microphone preset                                   | 23 |
| 5.9  | AUX Control   | 24 |
|      | 5.9.1 AUX In/out  | 24 |
|      | 5.9.2 General Aux settings - Audio routing                | 24 |
| 5.10 | Regional settings   | 26 |
| 5.11 | Security  | 26 |

|        |   |    |
|--------|---|----|
| 5.12   | Check firmware versions of delegate units                   | 27 |
| 5.13   | Check firmware versions of WCAP                             | 28 |
| 5.14   | Update  | 28 |
| 5.14.1 | WCAP update   | 29 |
| 5.14.2 | Update delegate units                                       | 31 |
| 6      | Frequency selection   | 32 |
| 6.1    | Check already used frequencies by other Confidea G3 systems | 32 |
| 6.2    | Selecting own frequencies                                   | 32 |
| 6.3    | The current used frequency                                  | 33 |
| 6.4    | Frequencies used by other Confidea G3 systems               | 33 |
| 6.5    | Other indications   | 33 |
| 6.5.1  | Signal quality  | 33 |
| 6.5.2  | Sorting frequencies   | 33 |
| 7      | Message screen  | 34 |
| 8      | Guidelines on optimal WCAP setup and configuration          | 35 |
| 8.1    | Positioning the Confidea Wireless Access Point              | 35 |
| 8.2    | Optimizing the position the antennas                        | 35 |
| 8.3    | Max range of WCAP   | 36 |
| 9      | Frequency Planning  | 37 |
| 9.1    | Use with WiFi base stations nearby                          | 37 |
| 9.2    | Avoiding interference b.m.o. wifi collection points         | 37 |
| 10     | Adding Cocon license to the WCAP                            | 38 |
| 10.1   | Introduction  | 38 |
| 10.2   | Get the MAC address of your central equipment               | 38 |
| 10.3   | Upload your license file                                    | 39 |
| 11     | Appendix  | 40 |
| 11.1   | Use of camera control feature                               | 40 |
| 11.1.1 | Overview  | 40 |
| 11.1.2 | Connectivity  | 40 |
| 11.1.3 | Commands for Confidea Gen III camera protocol               | 40 |

## 4 How to connect

### 4.1 Power up

After applying the 24V adapter to the power supply socket and switching the device on, the first LED blinks white. This means the system is booting.

Note: If the LED does not switch to green after some minutes or it turns red, please contact your support team.

### 4.2 Accessing the web-browser

To access the web-browser connect the LAN connector directly to your computer or to the LAN network which includes your computer.

The default IP address is **192.168.1.110**. Please make sure that your PC has an IP address and subnet mask that can access that IP address.

### 4.3 Login wizard

When you enter the web-browser for the first time you will be guided through a small wizard for initial setup of the system.

### 4.4 Introduction

The WCAP has a built-in web server that allows you to set/monitor certain parameters characterizing the wireless conference system.

The following is a step-by-step guide to give you a general idea of how to access your WCAP.

#### First time access

##### **STEP 1 – PC IP setup**



**Note:**

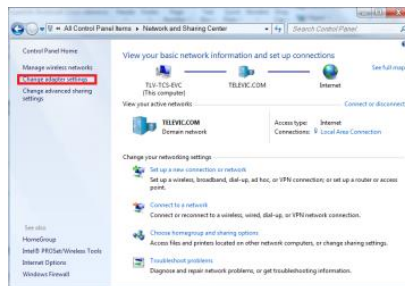
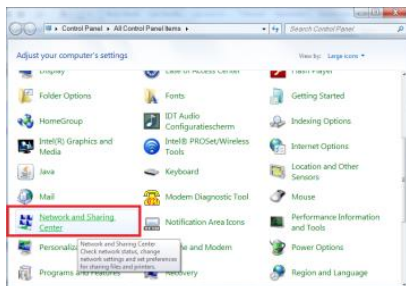
The WCAP has a default fixed IP address and subnet mask:

IP: 192.168.1.110

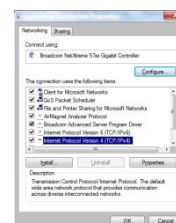
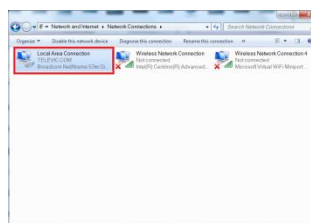
Subnet mask: 255.255.255.0

In order to access the built-in web server for the first time, the TCP IP settings from the PC or MAC must be modified. A fixed IP address has to be set. Therefore follow the instructions below.





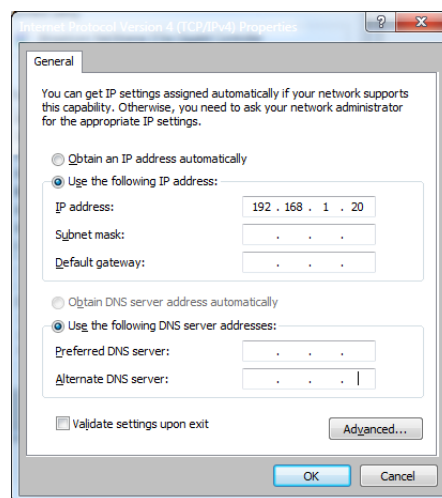
- Go to the 'Control Panel'
- Click on Network and sharing center
- Click on Change adapter settings
- Right-click on Local Area Connection
- Double on Properties
- Click on Internet Protocol (TCP/IP)
- Click Properties



## Static IP address WINDOWS 7

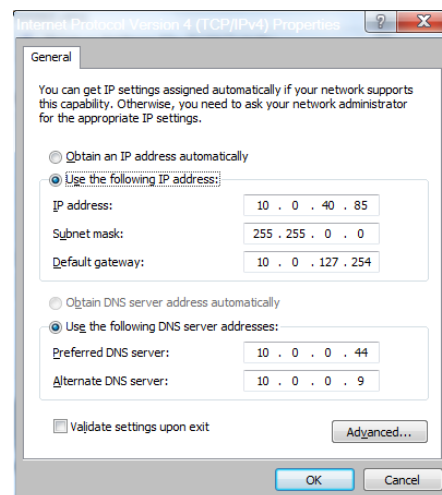
- Input your IP Address and subnet mask the IP addresses on the network must be within the same range.
- The default IP address from the WCAP is **192.168.1.110** so the computer should have an IP Address that is within the same subnet, like 192.168.1.11 and 192.168.1.20. The subnet mask must be the same for all equipment on the network: 255.255.255.0)

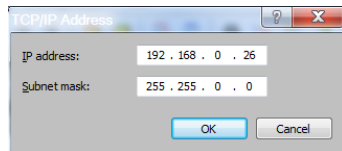
- Click **OK**



## Assigning a fixed IP Address in WINDOWS 7

- Enter the IP Settings on the PC
- In this example the PC has normally "10.0.40.85" as IP address.
- Click on Advanced and add a new IP address that is in the range of the access point, for example 192.168.0.26 and subnet mask 255.255.0.0
- Click to add

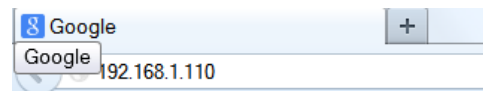




- Click OK

## **STEP 2 - Accessing WCAP**

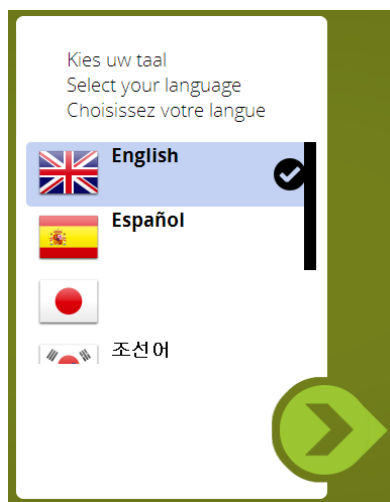
Open Internet Explorer or any other browser  
(with the computer connected to the WCAP)



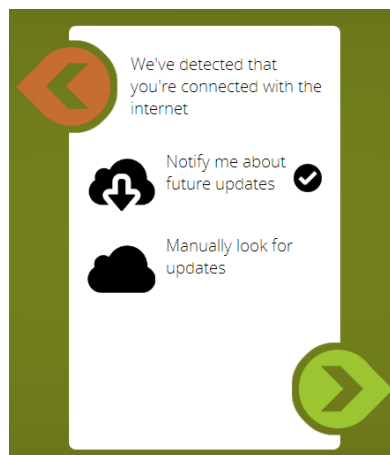
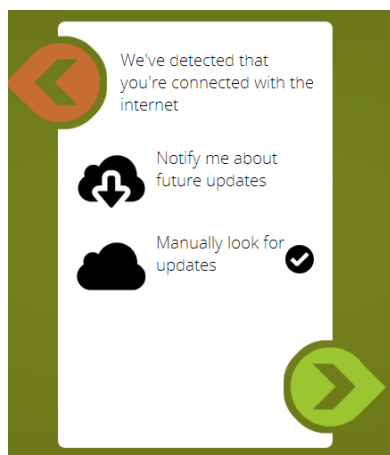
Enter **192.168.1.110** or **wcap3.local** into the Address Bar, press **Enter**

A wizard will guide you through the initial system setup:

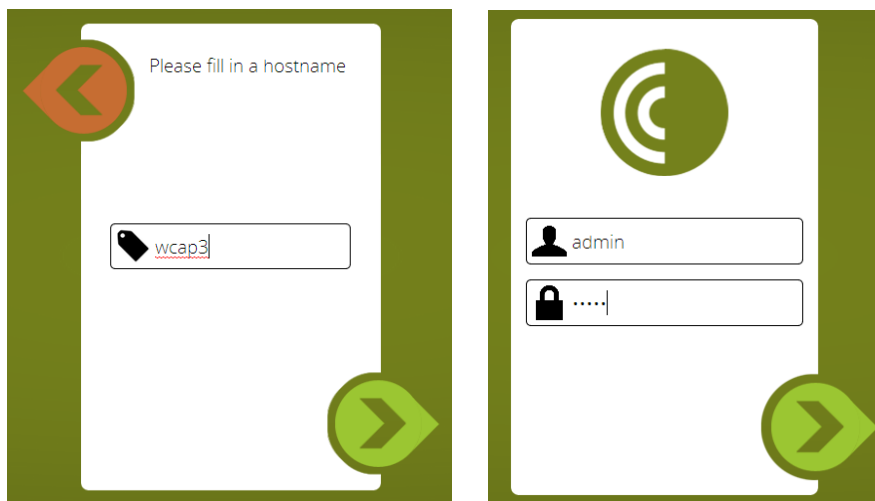
- Choose your language



- Then you can choose to be notified when updates are available. This requires that the WCAP has a connection to the internet.



- In the next item you have to fill in a hostname. This is a name which can be associated with the device for easy recognition in the system. Also when you have multiple WCAPs running simultaneously, you will be able to identify which frequencies are used by which hosts



- After you've completed the wizard you need to login. The default login and password are

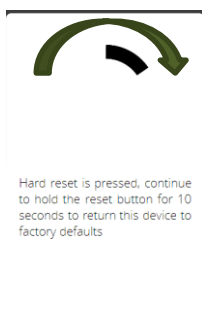
Login: **admin**

Password: **admin**

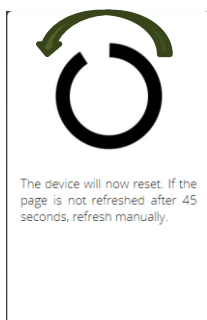
## 4.5 Return to factory settings

If the ip address is not known then a return to factory settings (default ip address) is possible by pressing the reset button next to the middle antenna , during 10 sec , and release the button .

Following screens will appear while pushing reset button and wait until the circle is completed



when releasing reset button...



# 5 Web server

## 5.1 Compatibility

The webservice is compatible with various types of mobile and desktop devices



## 5.2 Navigating through the webserver



Click on either of the available icons and navigate through the menu b.m.o. the scrollbar

After entering a submenu , use the arrow to go back to the main menu



=> home button



=> unit monitoring menu



=> settings menu



=> initialization menu



=> delegate unit manager



=> security settings



=> frequency settings



=> conference options



=> Aux control



=> regional settings



=> network settings



=> login settings



=> update screen



=> message screen




=> system information

## 5.3 Changing IP address

First we will change the IP address of the system. To do this you have to go to the settings. This can be done by clicking the settings icon.



Then scroll all the way down until you see the following icon  which indicates the network settings.

 A screenshot of the "Network settings" page. The page has a light green background. On the left side, there is a sidebar menu with several icons, including a gear icon (highlighted with a red box). The main content area is titled "Network settings" and has a sub-section "IP configuration" with a minus sign icon. The fields are:
 

- Hostname: Room1
- Address mode: Static (selected), DHCP
- IP address: 192 . 168 . 1 . 116
- Subnet mask: 255 . 255 . 0 . 0
- Gateway: 0 . 0 . 0 . 0
- API TCP port: 5011

 At the bottom of the form is a "Save settings" button.

In this menu you define:

- **Hostname**
- **Address mode (Static – DHCP)**

Static: in this mode the IP address and subnet mask is fixed and must be provided in the appropriate fields.

DHCP: DHCP stands for Dynamic Host Configuration Protocol and is a protocol used by the WCAP to obtain the parameters necessary for operation in an Internet Protocol network automatically. This protocol reduces system administration workload, allowing the WCAP to be added to the network with little or no manual configuration.

There must be a DHCP server on the network that dynamically assigns IP addresses when using the DHCP setting.

- **IP address**

Here you can enter the desired fixed IP address. Only applicable in fixed IP address mode.

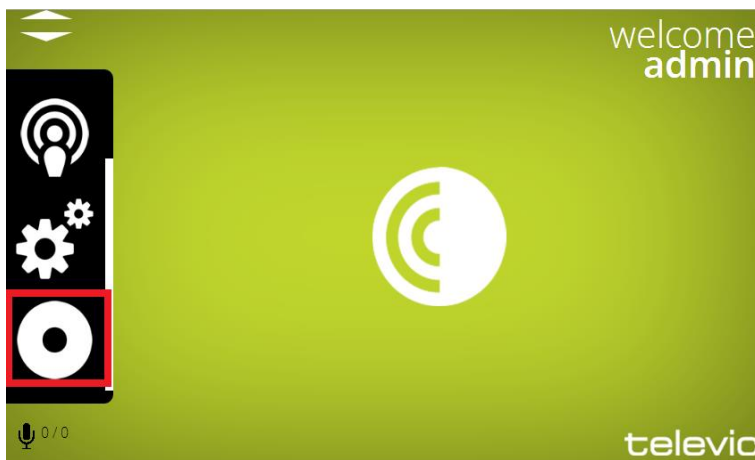
- **Subnet mask**
- **Gateway setting**

We advise to change the IP address. This will prevent conflicts when multiple access points with the same IP address are in the network.

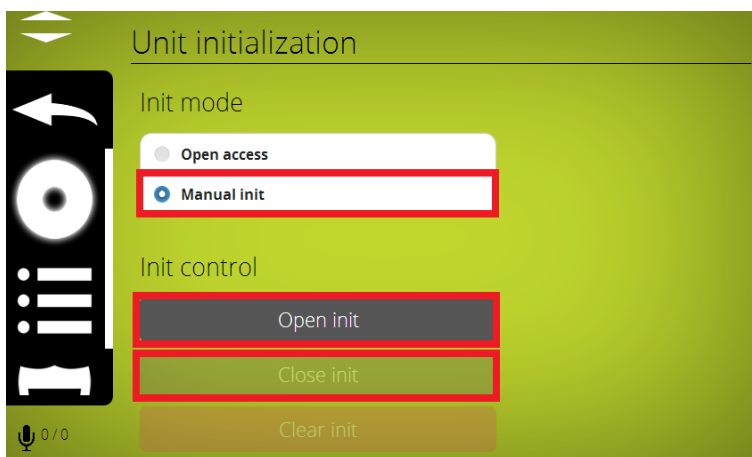
## 5.4 Initialization

In stand-alone mode, the *WCAP* supports two kinds of access: **open access** and **controlled access**.

- Open access: This is the default mode. Any unit can connect to the WCAP without initialization procedure
- Controlled access: a unit can only connect after going through an initialization procedure.



### 5.4.1 Controlled Access



In this mode, a manual initialization is required.

The manual initialization procedure requires the use of the 3 buttons on the web server displayed above: "Open init", "Close init" and "Clear init".

Take the following steps to initialize all units:

- 1) Switch on all wireless units



- 2) As long as no WCAP was discovered , the mic leds wil flash green slowly
- 3) When the units have discovered the WCAP. This is indicated by both mic leds blinking red slowly
- 4) Select the "Clear Init", to clear any previously created initialization list.
- 5) Start the new initialization by selecting the "Open Init" button.  
After you started the new initialization, the red Microphone Status LED's on all wireless units will start to blink red .

Mic leds blinking red at a rate of 2Hz is an indication that the units are trying to connect to the Wcap

Mic leds blinking red at a rate of 1Hz is an indication that the units are waiting for the initialization

- 6) To add a unit to the initialization list, press the microphone button of the unit to add.



- 7) The LEDs will turn green indicating that the unit has been added to the initialization list.
- 8) Repeat step 5 for each unit that needs to be added.
- 9) When finished, stop and save the initialization by pressing the "Close init" button,

Only the units that have been initialized will now be able to join the conference.

The init list is stored in the *WCAP* and stays in memory even after switching the *WCAP* off.

Next time the *WCAP* and delegate units are switched on, only these units will be allowed to connect to the WCAP.

## 5.5 Unit Manager

The unit manager allows to:

- Define delegate names
- Define groups



As you can see there are two main parts, the left column is the list of delegates; the right column is the list of groups. Each delegate shows an array of information, from left to right:

- Autonomy
- Version
- Serial number
- Packet loss (if any)

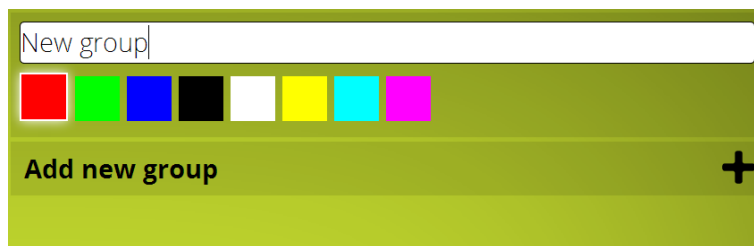
In rare cases it may appear that the delegates background is red, this means the delegate is running a golden version. Although this works, we strongly advice to reapply the update so that these units can be used to their full potential.

### 5.5.1 Define groups

A group is defined by two parameters:

- Group name
- Group color

You can make a new group by clicking on the "Add new group" button.



Add a group name and select (optionally) a group color. Press enter to save the group.



Editing the group can be done by right-clicking (or swiping) on the group entry. A small popup appears to edit or remove the group.



### 5.5.2 Define delegate names and assign to group

Right-click (or swipe) on the delegate you want to group. A small popup appears, click on edit.



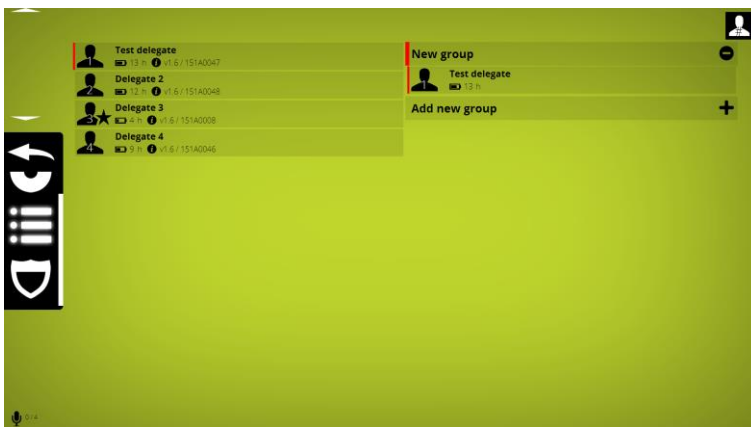
Delegate 1 |

No group

New group

Change the name; assign delegate to group. Enter to save settings.

Note: clearing the initlist will also clear the delegate names, but not the group



### 5.5.3 Remove delegate

Right – click (or swipe) on the delegate

Clicking or remove will delete the delegate unit from the initlist. This feature is only useful when manual init is used.

### 5.5.4 Visualize delegate names or numbers in unit manager



=> shows first 3 characters of the delegates name in the delegate icon , firmware version , battery status and serialnumber



=> shows first character of the delegates name in the delegate icon, firmware version , battery status and serialnumber





=> shows delegate unit nr in the delegate icon, firmware version , battery status and serialnumber





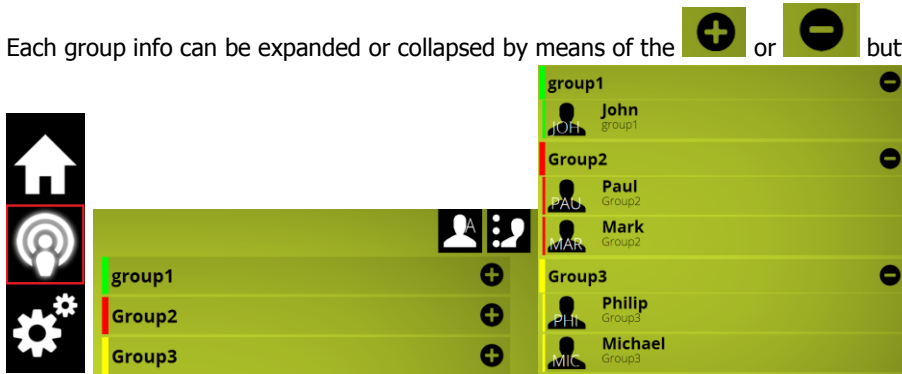
## 5.6 Unit monitoring



To monitor the delegate units activity and/or control the microphones select the icon in the main menu

A group overview now appears.

Each group info can be expanded or collapsed by means of the  or  button



=> List by delegate names



=> List by groupnames



=> List by first character of the delegates name



=> List by delegate unit number



=> show first 3 characters of the delegates name in the delegate icon , delegate name and group , when microphone is on



=> show first character of the delegates name in the delegate icon , delegate name and group , when microphone is on

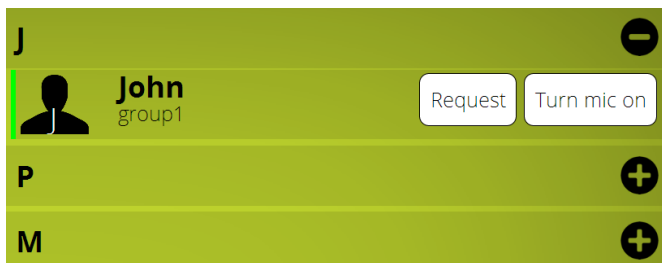


=> shows delegate unit nr in the delegate icon ,delegate name and group , when microphone is on

## 5.7 Activating microphones

Microphones can be activated by clicking on the delegate name in the monitoring screen

Microphones control button can be activated activated by right click on the delegates name



Activated microphones are indicated by following icon



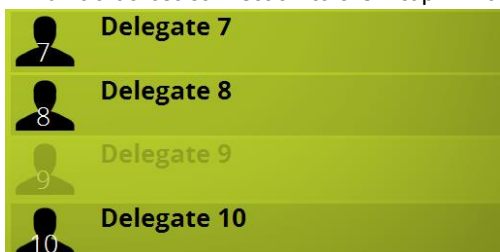
Microphones in request ar are indicated by following icon



### 5.7.1 Disconnected units

If delegate units are disconnected or lost RF link with the WCAP due to removed or depleted battery for instance, to long distance from WCAP ..they are shown as greyed out in the monitoring screen

A unit that lost connection to the wcap will be shown greyed out after +/- 30 sec



## 5.8 Conference options

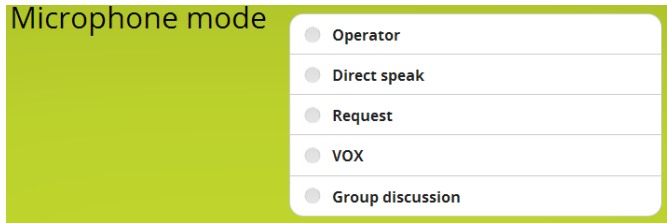
### 5.8.1 Max active microphones



Max 6 microphones can be on at the same time .

Chairman units always have priority and if max is reached , microphone of the delegate units will be deactivated to allow chairman units to switch on their microphone . In this case the microphone of the delegate unit which was switched on the longest , will be deactivated automatically .

## 5.8.2 Microphone modes



### 5.8.2.1 Operator

only operator can activate microphone via webserver or Cocon software

### 5.8.2.2 Direct speak:

Enables the participant to turn on or off his microphone at any time. The only limitation here is the maximum number of microphones that may be active simultaneously.

Interrupt possible



=> When this option is on and the the maximum active microphones setting is reached, activation of an additional microphone will automatically switch off the microphone that was active for the longest time. Again, the chairmen units can always be activated.

### 5.8.2.3 Request:

Enables the participant to send a request to speak to the chairman or conference operator by pressing the microphone button (or to cancel his request by pressing the microphone button again). Once the floor is requested, the first one in the queue has blinking green mic leds , the other ones have fixed green mic leds, this means that the delegate unit is in request mode.

The chairman or conference operator grants the participant the permission to speak by using the NEXT button or by activating the microphone via Cocon software , if used.

Cancel request allowed



=> this option allows the participant to cancel his own request by pressing the microphone button again

### 5.8.2.4 Group discussion:

Any microphone can be switched until the maximum active microphones setting is reached. Other participants can switch their microphone in request mode. The first applicant who requested the floor gets the floor when one of the currently active microphones is turned off .

When a chairman pushes the NEXT button , the microphone which was active the longest time , will be switched off and the first one in the request queue will be switched on

The first one in the queue has blinking green mic leds , the other ones have fixed green mic leds

### 5.8.2.5 VOX

Is similar to direct speak + interrupt possible , but microphones are switched on by voice detection

#### Vox Treshold

Determines the sound level needed to activate the mic by VOX

VOX threshold is to be chosen in such way that a microphone is switched on directly after the person begins to speak.

A threshold setting which is too high might result in a microphone not being switched on or switched on too late.

A threshold setting which is too low might result in a microphone being switched on by ambient sound

Also the microphone preset setting will influence the choice of the Threshold level .

#### Vox Time out

The microphone will be switched off when the Vox threshold level is not reached during the amount of seconds set in the Vox time out

A Vox time out setting which is too low might result in interrupted audio when there is a pause or low passage in the audio.

#### Vox Pencil drop suppression

Avoids accidental microphone activation because of short sounds. This setting may cause a short mic activation delay

#### General remark on use of VOX :

A high microphone preset combined with strong audio input may result in the perception that the VOX activation is too slow due to the limiter release time.

#### 5.8.2.6 Last microphone remains on

When this option is set , the audio of the last delegate microphone which was switched off, still captures the sound , this way acting as an ambient microphone. In this situation the mic ringled and mic leds are not on anymore .When any other microphone is switched on again , the "ambient" microphone is then switched off.

The chairman unit is not affected by this feature

A "last mic on" status is indicated as mic active but without the mic icon

Last mic on



Mic on

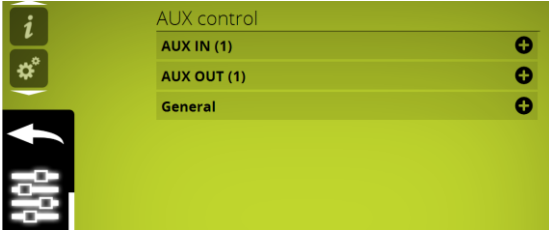


#### 5.8.3 Microphone preset

Determines the sensitivity of the microphone . This chosen setting will depend on

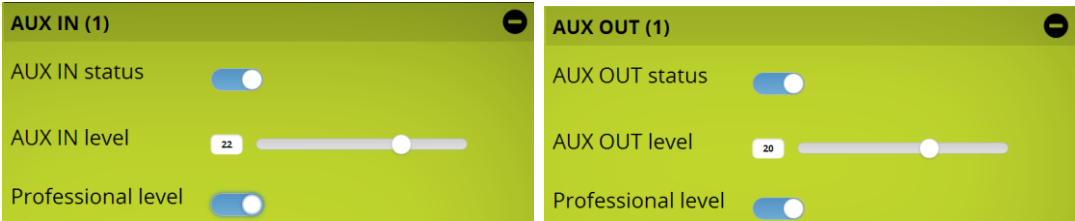
- how close or far the person is sitting from the microphone.
- Volume of external loudspeakers if present ; a *FAR* setting + high volume of external loudspeakers or external loudspeakers positioned close to the microphones may cause acoustic feedback
- External compressor limiter device : in this case *CLOSE* must be used as setting to allow maximum adjustability on the external compressor-limiter device (see also AUX control settings)

# 5.9 AUX Control



The Confidea G3 WCAP has one auxiliary input and one auxiliary output

## 5.9.1 AUX In/out



status : switches off or on the Aux input

level : volume adjustment

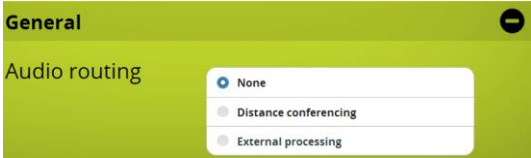
Professional level : 2 inputlevel ranges are possible :

OFF (= Consumer level) : nominal level -10DBV , max input level +10dBV

ON (= Professional level) : nominal level +4dBu , max input level +24dBu

The professional level setting should be set equal for both Aux In and Aux Out

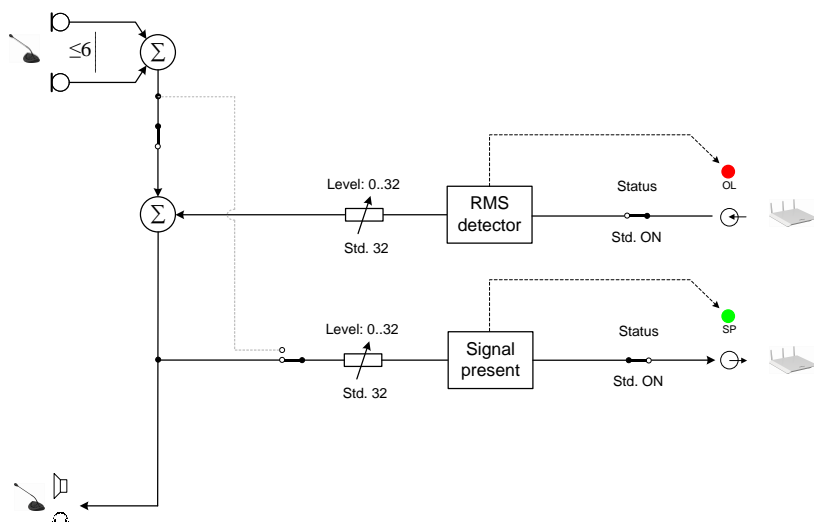
## 5.9.2 General Aux settings - Audio routing



### 5.9.2.1 None

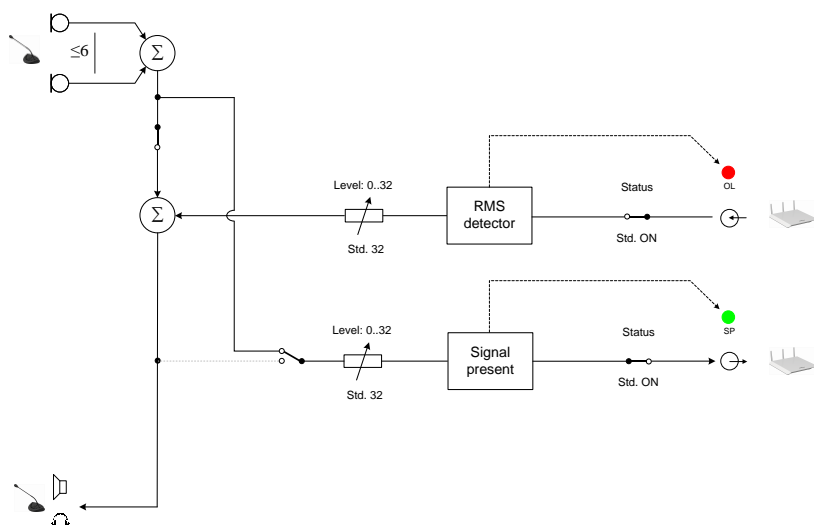
No additional audiorouting is done





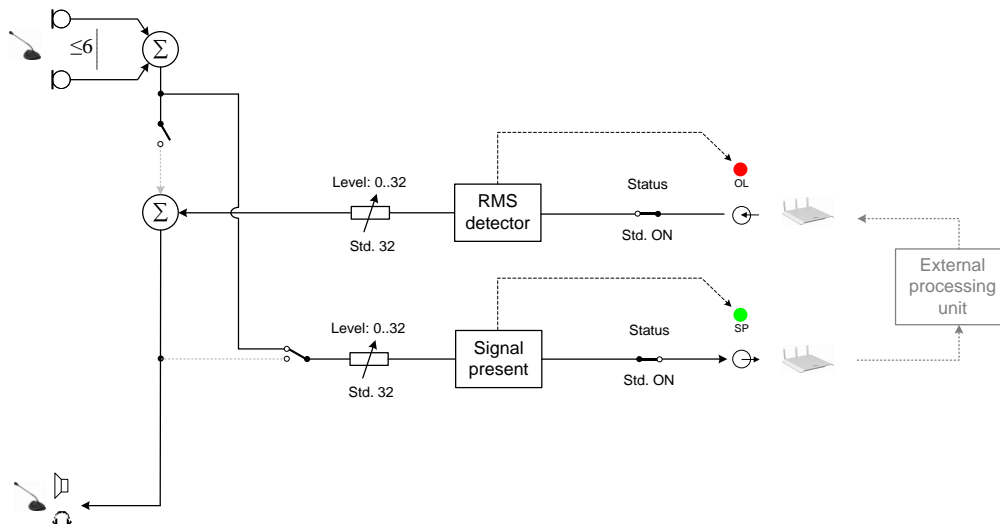
### 5.9.2.2 Distance conferencing

Distance conferencing (= N-1) option adds external signal , via aux in , to the local floor signal and sends the local floor signal , via aux out , to the remote party.



### 5.9.2.3 External processing

Activating the "external processing" option allows to add external signal processing equipment or a mixing board.



## 5.10 Regional settings



Language : In the regional settings the webserver language setting can be changed

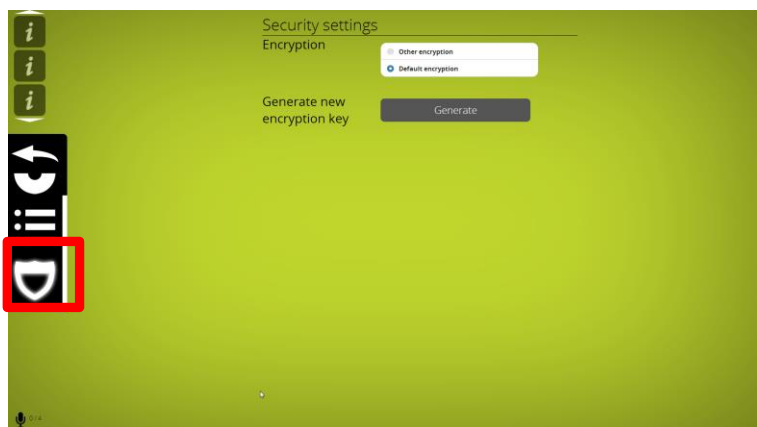
Region : the selected country or region will determine which frequencies can be used according to local regulations

## 5.11 Security

The security uses a AES 128 bit encryption.

The system has a built-in default factory encryption key. To increase the security even further, or to make sure only specific delegate units can connect to the wcap , another random encryption key can be generated and uploaded. This key will be send to all delegates connected to the system. Once other encryption option is selected only those units having the encryption will be able to log onto the system.

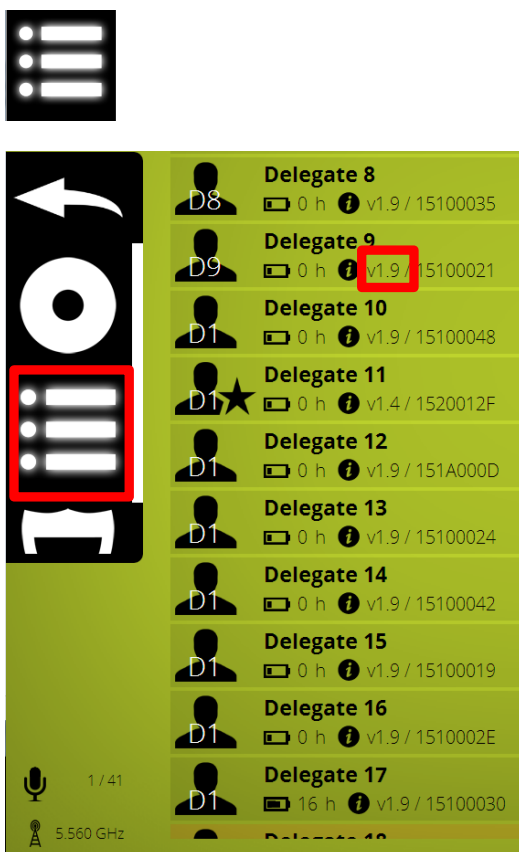
If a unit needs to be added to the system, default encryption needs to be selected first.



## 5.12 Check firmware versions of delegate units

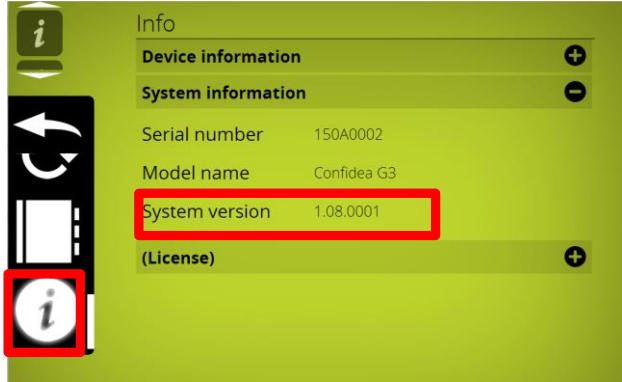
If the firmware version does not correspond with the uploaded file, for some units, the update needs to be redone to ensure all units have the same firmware version.

This can be checked via the unit monitoring list



=> shows # microphones activated and provides shortcuts to unit monitoring and frequency setting menu

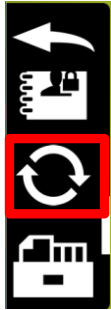
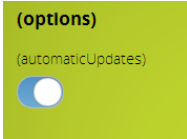
### 5.13 Check firmware versions of WCAP



### 5.14 Update

The update page can be found by going to the settings submenu and clicking on the update button (displayed as two arrows in a circular formation).

There is the choice to choose to check automatically for available updates via [www.updates.televic-conference.com](http://www.updates.televic-conference.com) or to do a manual file selection



When you get to the update page you can have one of these two situations:

- No update available: either you have the latest software and an update is not necessary or no update file has been uploaded.
- There is an update available: this could either be because you're connected to the internet and there's new version available or that you have manually uploaded a file.

**Note** that through the internet update system you'll only receive the latest updates. Older updates will still need to be installed manually. To upload a file, click on the upload button in



the right upper corner

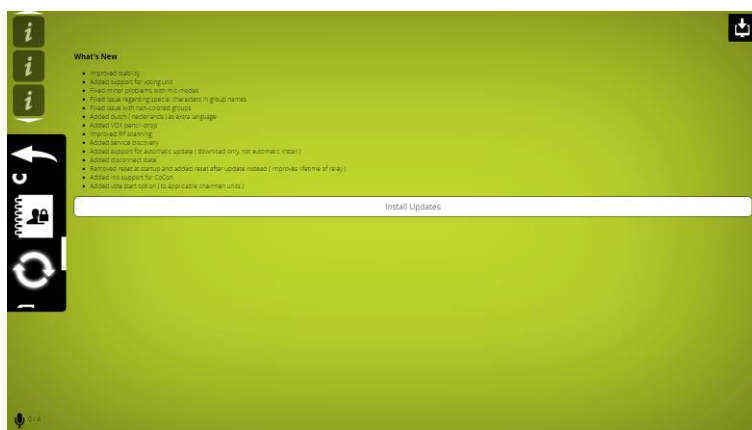
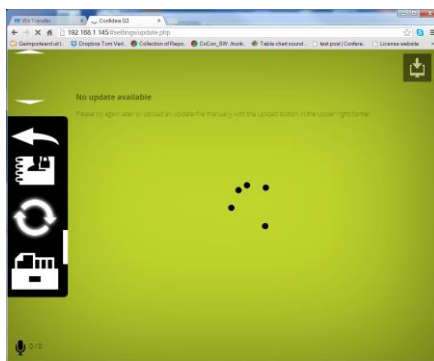
After you've selected a file, this will be uploaded automatically, however not installed automatically

The file is a compressed folder which will be automatically extracted by the system

The file for the delegate units update has following name format "WDU.x.yz.tar" or "WDU.x.yz.tuf" (both are ok)

The file for the WCAP update has following name format "AP.x.yz.tar" or "AP.x.yz.tuf" (both are ok)

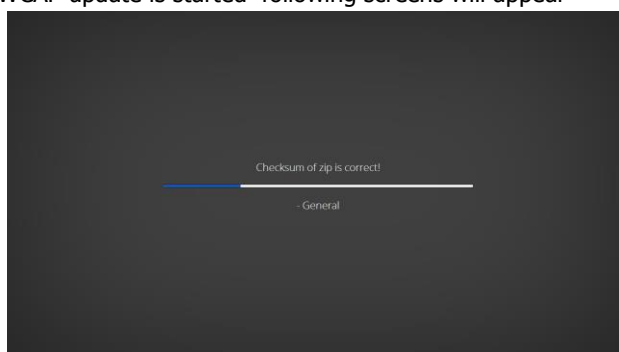
Following screen appears and after a few seconds the system is ready to start the installation of the updates and info is shown regarding the latest changes

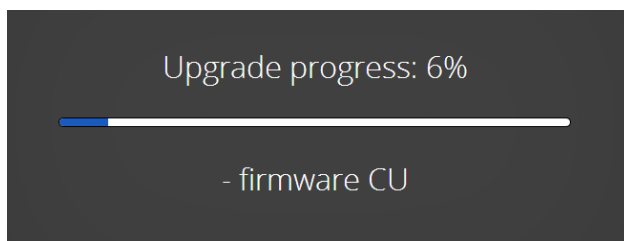
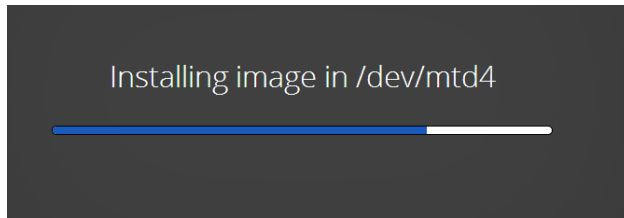
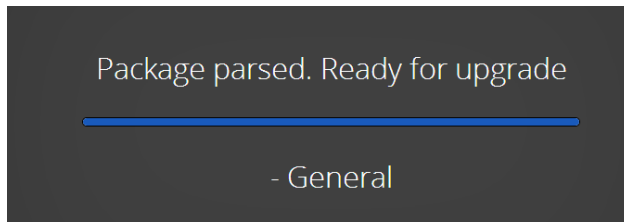


To start the update, press "install updates". (Note that when you received the update over the internet, the file will be downloaded first, so do not disconnect). Once the update has started; you'll get an overlay protecting you from making any changes to the system.

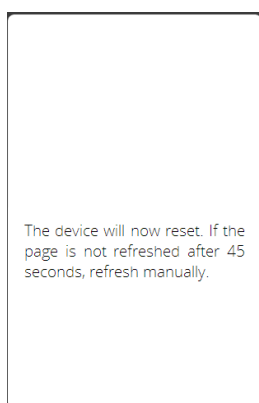
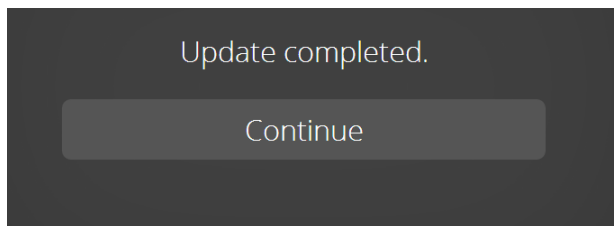
### 5.14.1 WCAP update

Once the WCAP update is started following screens will appear





During the update the WCAP led1 is green on and led2 is blinking white. When the update is finished following screen will appear

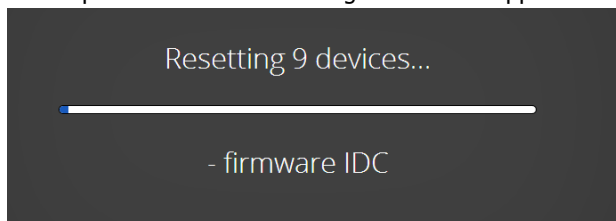


An update may take a while; do not under any circumstances turn off the device. During the system update, the device will reboot a few times, during which you cannot use the device. If the update fails, the system will boot in golden mode from which you can retry the update.

When updating delegate units, make sure they're battery is charged  $\geq 50\%$  and that you have the least amount of interference as interference will drastically increase the time to update. After a delegate update, only the devices will be reboot.

### 5.14.2 Update delegate units

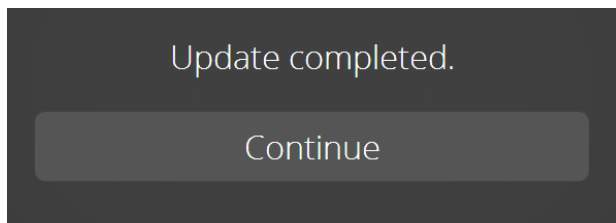
Once the WCAP update is started following screens will appear



The reset takes about 2 min



During the update the mic leds on the delegate units will light up red – left , green - right , after 10 sec, red – right , green - left , etc.....



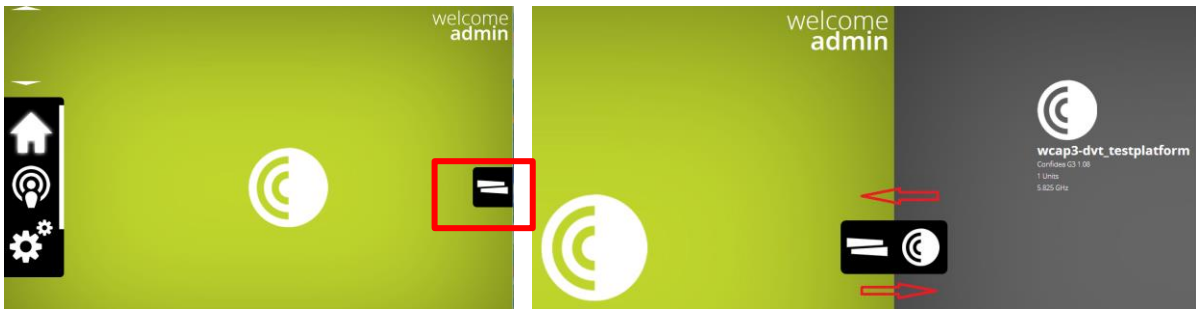
The update takes about 20 min

**Remark :** If a unit is accidentally switched off during the update (e.g; due to empty battery) , this will temporarily stop the update , but after a few minutes the update for the other units will continue

# 6 Frequency selection

## 6.1 Check already used frequencies by other Confidea G3 systems

By clicking and dragging the indicated button , from right to left and back , any other Confidea G3 system which are connected to the same LAN network will be shown by their hostname and currently active frequency.



## 6.2 Selecting own frequencies



=> enter frequency selection screen



=> add this frequency as frequency that may be used

Frequency selection can be done by means of adding the mark in the checkbox in the below screen



If more then one frequency is marked , the WCAP select automatically a frequency amongst those marked



## 6.3 The current used frequency

The current used frequency is marked with the antenna icon



## 6.4 Frequencies used by other Confidea G3 systems

Frequencies used by other Confidea G3 systems which are connected to same LAN network (see chapter 7.1) are mentioned in the below screen ; the identification of the other Confidea G3 system(s) is done by their hostnames



## 6.5 Other indications

### 6.5.1 Signal quality



=> shows the quality of the signal , based on interference detected on that frequency



=> low signal quality due to interference or low level



=> high signal quality , least or no interference



=> do not use this frequency , because signal strength to low or signal to disturbed

### 6.5.2 Sorting frequencies



=> mark/unmark all frequencies toggle button



=> sort frequencies according to signalquality



=> sort frequencies by numerical order



=> sort frequencies by numerical order per RF band

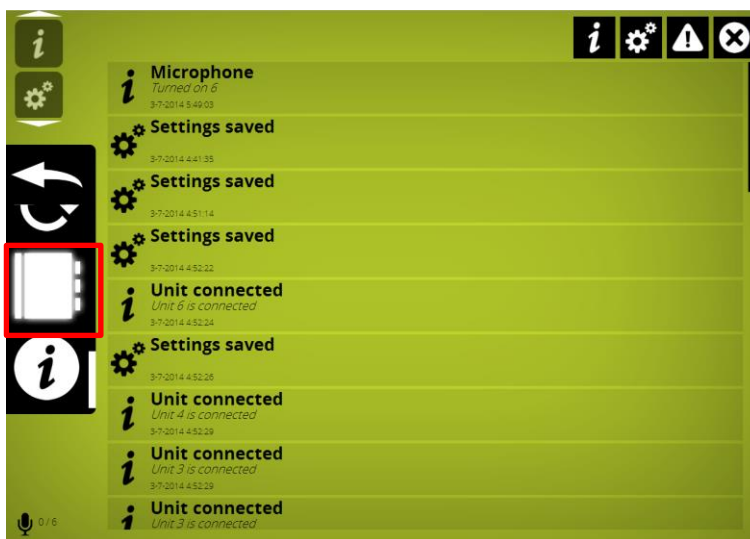


=> show all frequencies in this RF band



=> collapse all frequencies in this RF band

## 7 Message screen



The message screen can be used as monitoring or analysis tool . Every event , change of settings , warning ....is shown here (last message at the bottom).



=> enable messages concerning delegate units connecting , microphone activations



=> enable message concerning change of settings



=> enable warnings



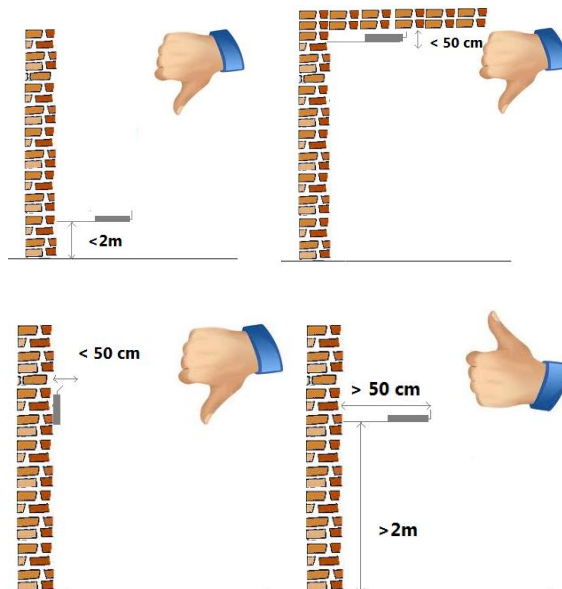
=> other messages

## 8 Guidelines on optimal WCAP setup and configuration

### 8.1 Positioning the Confidea Wireless Access Point

**Attention:** Do not place the WCAP behind obstacles like walls, cabinets, panels, projection screen, glass screens etc... , as they significantly reduce RF signal strength and quality

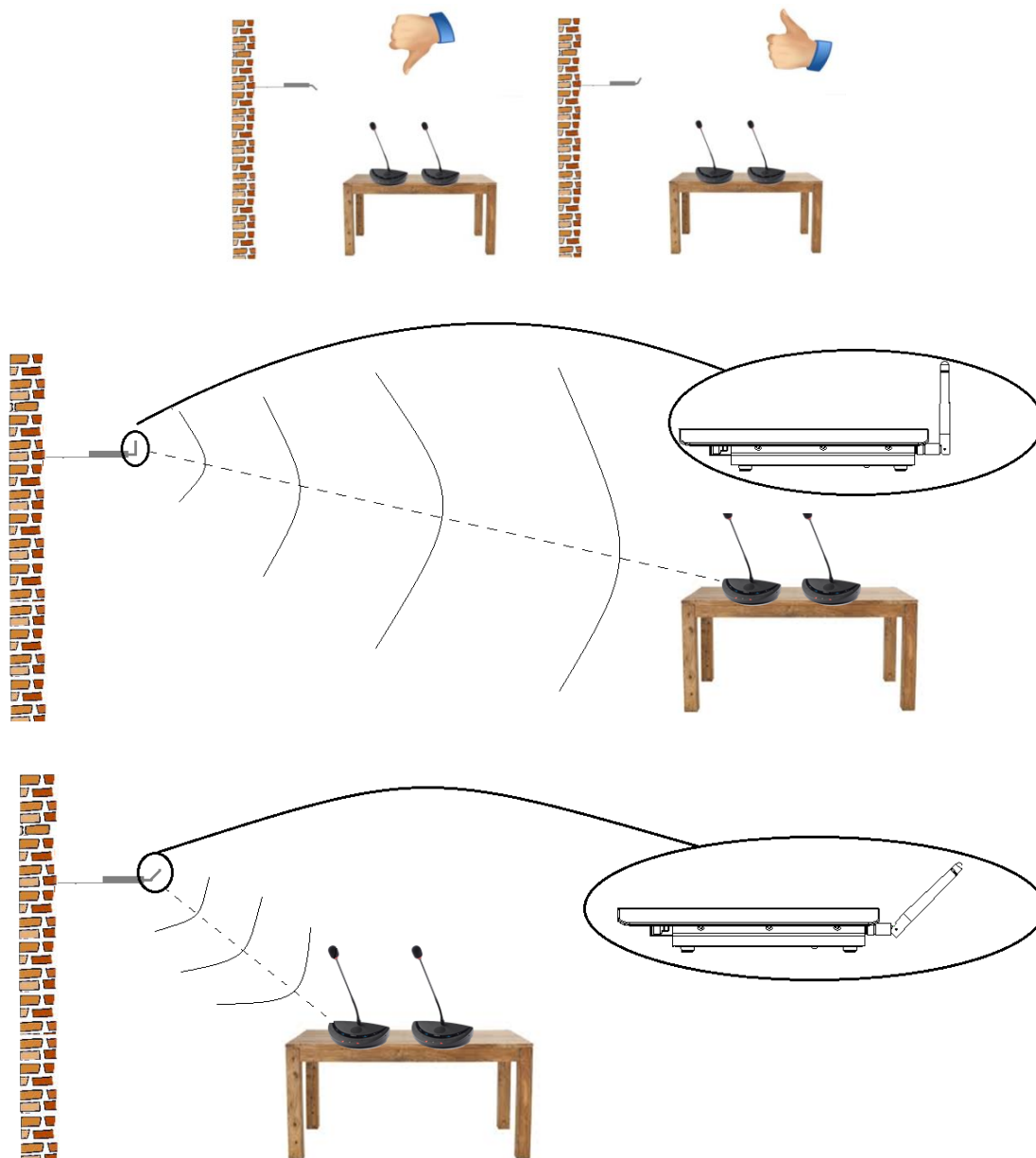
Below you can find how to select a correct positioning of the WCAP.



**Note :** When the antennas of the WCAP are positioned very close to a wall or ceiling , this may result in absorption of the RF signal , which can decrease RF signal quality.

### 8.2 Optimizing the position the antennas

**Note :** It is important not to point the antennas directly to the units  
Choosing the correct angle of the antennas in relation to the position of the delegate units is beneficial to a good overall RF link quality between WCAP and delegate units



### 8.3 Max range of WCAP

A single WCAP has a range of 30m in "open field" . However the max range can be significantly less depending on the positioning of the WCAP itself and direction of the antennas in relation to the position of the delegate units.

**Note :** Certain buildingmaterials like concrete , or metal may absorb part of the RF signalradiation, resulting in a reduction of the max distance between the access point and units

# 9 Frequency Planning

## 9.1 Use with WiFi base stations nearby

If more than one WCAP or Wifi accesspoints are in the same room or within 30m. range , it is strongly advised that not more than one of them uses automatic frequency selection , to avoid that the frequencyscanning is disturbed by the other accesspoint(s) . If multiple accesspoints are used within each other's reach, manual frequency selection based on frequency planning is strongly recommended to avoid that wifi access points and Confidea WCAP would use the same frequencies

When the Confidea wireless system is set to manually selected the wireless carrier frequency, then you must make sure the Confidea wireless carrier does not overlap the already occupied WiFi wireless carrier channels.

When using manual frequency selection in 5GHz band , ideally the frequency selection is done in such way that between 2 used frequencies , there is a 40Mhz "distance" to avoid interference by RF sidebands.

## 9.2 Avoiding interference b.m.o. wifi collection points

The transmission mode between WDU's and WCAP is specially designed to be used in very challenging environments where a high density of wifi signals is present due to wifi access points as well as so called smart devices , which may cause RF interferences

Wifi devices such as smartphones , I-Pads..... may send regular probing signals over the entire wifi band to search for a wifi connection. This probing can cause temporary interference and will continue until a wifi connection was established. When a large number of wifi devices is present in the room , these probing signals may cause WDU connection loss due to saturation of the used frequency .

Therefore it is strongly recommended that a wifi collection point is set up, so wifi devices can lock on to them and this way reduce further the risk of interference.

**Note : The wifi access points must have sufficient capacity to ensure wifi connection for all present wifi devices .**

**If there is not a sufficient wifi connection capacity for the present mobile wifi devices , unstable functionality of the Confidea wireless system due to interference can not be excluded !**

# 10 Adding Cocon license to the WCAP

## 10.1 Introduction

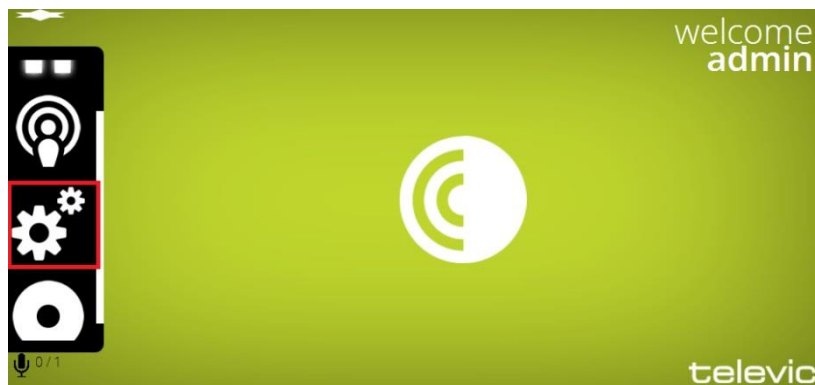
With the release of Confidea Gen 3 we've changed the CoCon license file location from the PC where the Room Server is installed, to the device to which CoCon will be connecting. This means that now you do not need to send us the MAC address of your PC but the MAC address of your Confidea Gen 3 Access Point. This way the license is independent of the computer onto which the CoCon Room Server is running, the license will allow only 1 concurrent connection and the software will adapt automatically to the license modules which are active in the license file.

To obtain the MAC address of the Confidea Gen 3 WCAP please follow the procedure underneath.

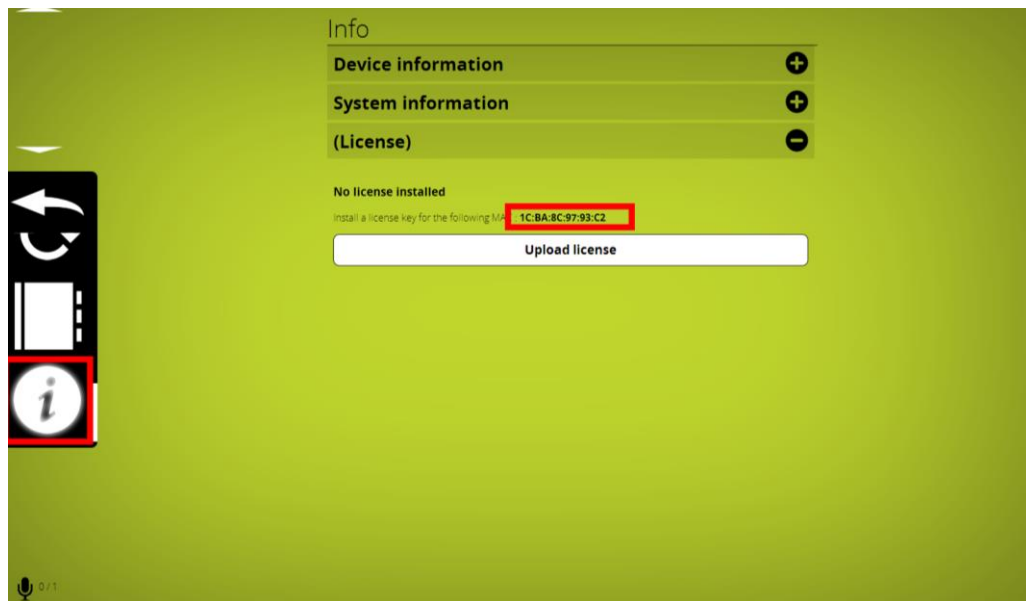
## 10.2 Get the MAC address of your central equipment

The default IP address Confidea Gen 3 WCAP is 192.168.1.100. Please use a recent web browser to browse to the addresses indicated. If it's the first time you set up your device a small wizard will appear to set your language and etc.

You can login using username "admin" and password "admin". (Yes, we've been very creative this time...). Then go to the settings page:



Then click on the license file icon:



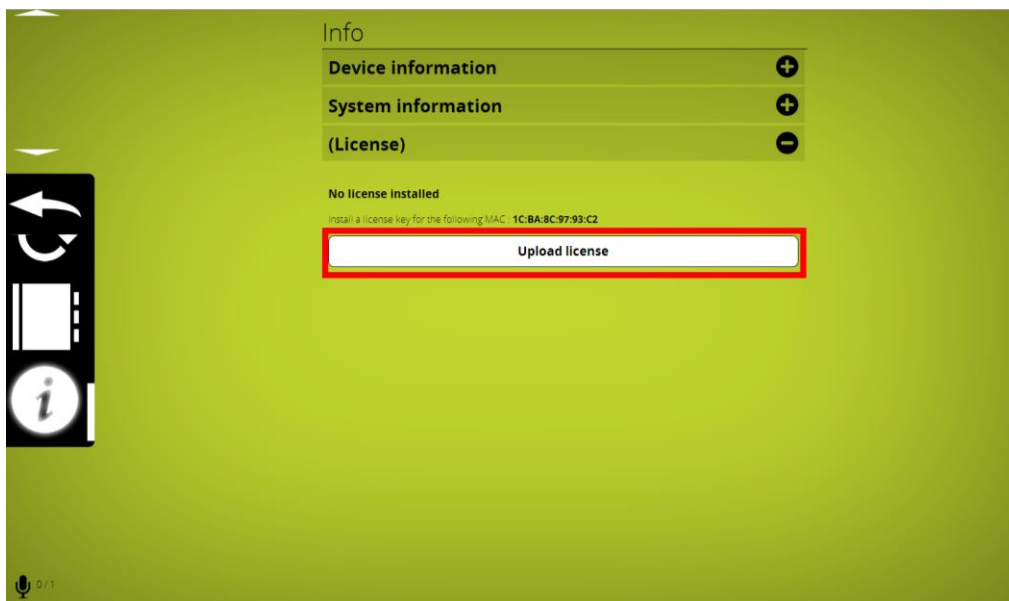
Please copy this MAC address and send it along with your P-number (can be found on the CoCon box) to the following email address:

[Cocon-license@televic.com](mailto:Cocon-license@televic.com)

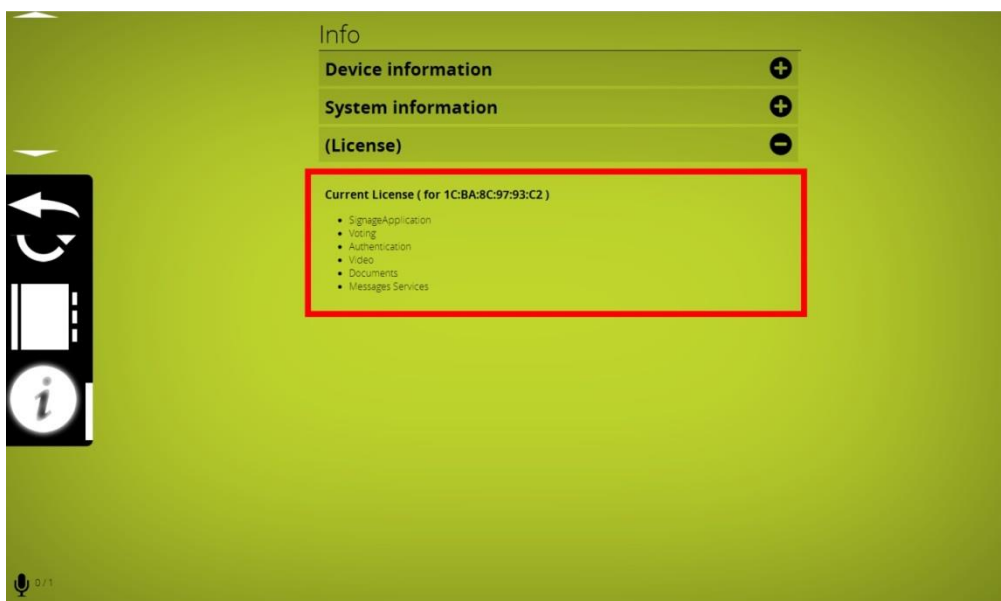
### 10.3 Upload your license file

Then you will receive an email containing your requested license file. This is an xml file which you can open with notepad or something similar to verify if the correct modules have been activated. The name of the file contains the MAC address of your device.

To upload your file onto your central equipment, click on the upload button below the mac-address:



Then a popup will appear. Please select the received license file. It will load onto the device and its content will appear.



Now you can connect CoCon with the central equipment.

# 11 Appendix

## 11.1 Use of camera control feature

### 11.1.1 Overview

The Confidea Gen III Conference System supports a camera control. The commands, which the camera control should understand, will be described shortly.

Confidea Gen III WCAP sends out data via UDP to the camera system  
The camera control function can be enabled via the Confidea Gen III webserver

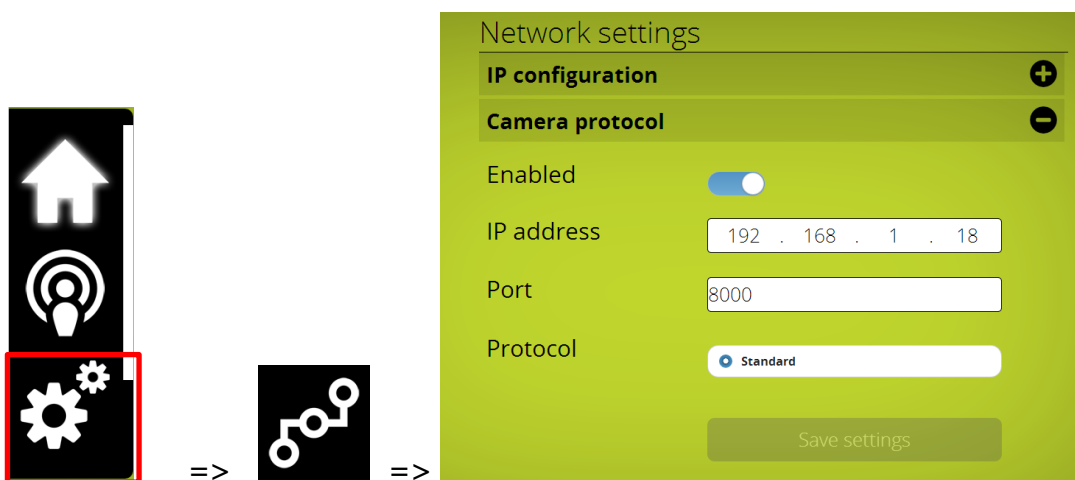
### 11.1.2 Connectivity

The Confidea Gen III WCAP sends the camera commands via UDP to a destination ip-address , which can be defined in the Confidea Gen III webserver .

The default UDP communication port is 8000. When selecting a port nr manually via the Confidea Gen III webserver, a portnr > **3000** should be chosen.

### 11.1.3 Commands for Confidea Gen III camera protocol

Available settings via Confidea Gen III webserver



**Enabled** : 0 = off , 1=on

**Ip address** = destination ip address (udp) of camera system

**Port** = destination port (udp)

The data which is send by the Confidea Gen III WCAP after a microphone button event , is in JSON format, **{“UID”: micnr,“status”: x}**

**Micnr** : micronumber , one or more digits



**Status** : 0 = off, 1 = on, 2 = request , 3 = prior

e.g. of data send when microphone 7 is in request :

```
{"UID": 7,"status": 2}
```