

# PLIXUS GATEWAY

INSTALLATION GUIDE



## 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 © 2023 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.

## 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.

# CONTENTS

## Introduction

Getting started .....	6
About this manual .....	6
Compatibility .....	6
About Plixus Gateway .....	7
Box Contents .....	7

## Safety instructions

Safety instructions .....	10
Safety .....	10
FCC & ICES Information .....	10
Conformity and Certification Info for Japan .....	11
Important safety instructions .....	12
Power connections .....	14

## Components

Components .....	17
Plixus Gateway .....	17
Central Units .....	17
Plixus Gateway .....	19
Front view .....	19
Rear End Connectivity .....	19

## Before Installing the Plixus Gateway

Required Information .....	22
IT Considerations .....	23
Web Browser .....	23
Connectivity Towards the Internet .....	23
Connectivity between the Plixus Gateway and the Central Unit .....	25
Plixus Gateway and Central Unit Configuration .....	25
Vonage Video API network Connectivity Requirements .....	26
Whitelisting a Domain in Your Web Browser .....	28
Fixed IP Address .....	28
Email Communications .....	28

## Installation

Software Configuration .....	30
Version of the Central Unit .....	30
Confero 360 License .....	31
Audio Configuration of the Central Unit .....	32
Hardware Installation .....	33
Physical installation .....	33
Network Topology .....	34
Connection Diagram for the Audio .....	37
Connecting the Gateway To Plixus AE-R .....	37
Connecting the Gateway To Confidea WAP G4 .....	39
Communication With the Central Unit .....	41
System Testing .....	42
System Updates .....	43

## FAQS and Troubleshooting





Plixus Gateway DISPLAY AND Troubleshooting .....	46
Recovery .....	50
FAQs .....	51



# GETTING STARTED

## About This Manual

Throughout this guide we use icons to designate different types of information:

	This is a note. A note gives additional information or information that may only be applicable to some situations.
	This is a tip. A tip gives you an alternative way to do a particular step or procedure, or lets you know of an option that you may find helpful.
	This indicates that something is very important. Important information is something that you need to do in order to accomplish a certain task.
	This provides safety precaution information, that is, information that you need to be careful about to prevent potential problems when using our systems.

## Compatibility

This user manual applies to the following products:

Product	Version
Plixus Gateway	-
Plixus AE-R	≥ CRP 7.2
Confidea WAP G4	≥ CRP 1.2
Confidea WCAP G3	≥ 3.6
Plixus MME	≥ CRP 7.2
T-CAM solution	≥ 1.64

# ABOUT PLIXUS GATEWAY

Plixus Gateway is part of the Confero Cloud solution and comes in combination with your conferencing installation. It is connected to the Plixus engine on the one side, and to the Cloud on the other side, and creates secure hybrid meetings with a near face-to-face experience.

This unit acts as a secure bridge between the Confero Cloud services and the conferencing installation in the premises of the customer by allowing traffic in and out between the Internet and the local room (transfer of audio, video and conference data). It also ensures interoperability with all of the other conferencing devices (Central Unit, screen, cameras, etc.).

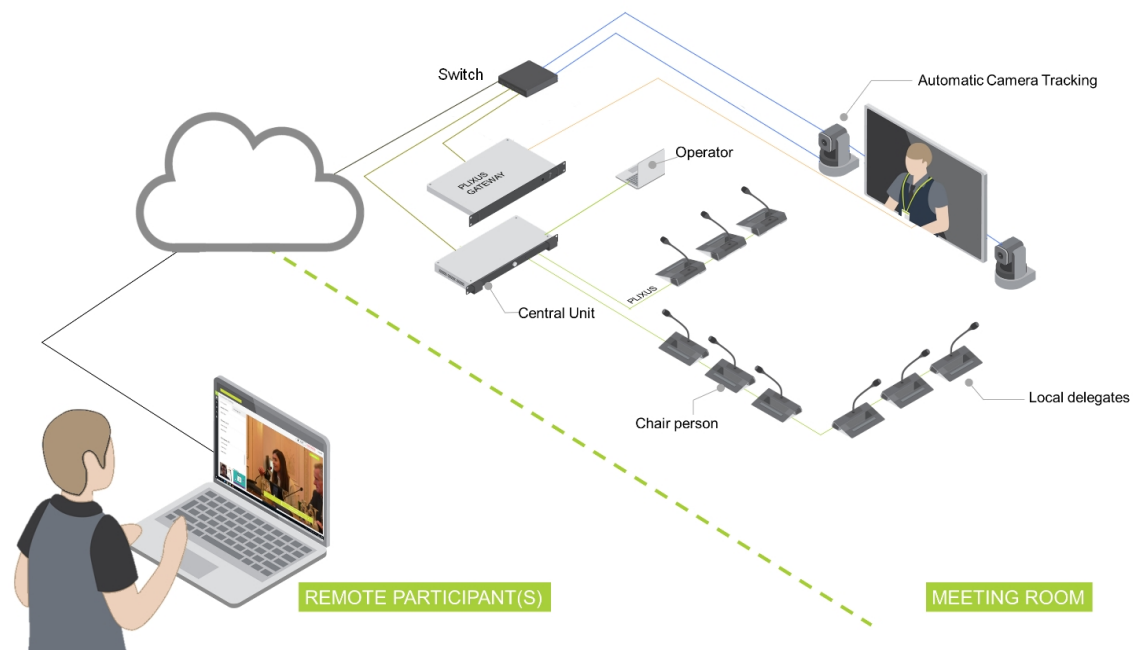


Figure 1-1 Typical Plixus Gateway setup where the gateway is connected to the Cloud, the Central Unit, the screen and the cameras

## Box Contents

If any part is missing, contact a customer service representative from Televic Conference.

- > 1 Plixus Gateway device
- > 1 power cord

- > 1 DisplayPort male-to-female HDMI adapter
- > 2 Cinch-toMiniJack cables





# SAFETY INSTRUCTIONS

The safety instructions contain general safety guidelines that integrators, installers, operators, end users, and anyone else who installs or uses Televic material is required to read and follow at all times.

## Safety

All Televic systems are state of the art devices and have been designed to meet all quality standards. Nevertheless, the individual components of the conference system can cause danger for persons and material assets if

- › the conference system is not used as intended,
- › the conference system is set up by personnel not familiar with the safety regulations,
- › the conference system is converted or altered incorrectly,
- › the safety instructions are not observed.

## FCC & ICES Information

*(U.S.A. and Canadian Models only).*

This Class B digital apparatus complies with Canadian norm ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- › Reorient or relocate the receiving antenna
- › Increase the separation between the equipment and receiver
- › Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- › Consult the dealer or an experienced radio/TV technician for help

- Consult the Federal Communications Commission’s manual “How to Identify and Resolve Radio-TV Interference Problems”

Operation is subject to the following two conditions:

1. This device may not cause harmful interference
2. This device must accept any interference received, including interference that may cause undesired operation.



Changes or modifications made to this equipment not expressly approved by Televic Conference NV may void the FCC authorization to operate this equipment.



Wireless discussion units and the Wireless Access Point comply with FCC radiation exposure limits set forth for an uncontrolled environment. These Wireless discussion units and the Wireless Access Point should be installed and operated with minimum distance of 20 cm between the radiator and your body. The RF-parts of the Wireless discussion units and the Wireless Access Point must not be co-located or operating in conjunction with any other antenna or transmitter.

## Conformity And Certification Info For Japan

This device has been granted a designation number by Ministry of Internal Affairs and Communications according to:

### **Ordinance concerning Technical Regulations Conformity Certification etc. of Specified Radio Equipment (特定無線設備の技術基準適合証明等に関する規則)**

Article 2 clause 1 item 19/3

Approval No.:

- 202WW10120791/2”
- 202XW10120791/2



This device should not be modified, otherwise the granted designation number will be invalid.

## Important Safety Instructions

1. **Read Instructions.** All the safety and operating instructions should be read before the product, device or system is operated.
2. **Retain Instructions.** The safety and operating instructions should be retained for future reference. The instructions should be kept in the vicinity of the product or system.
3. **Heed Warnings.** All warnings on the product and the operating instructions should be closely adhered to.
4. **Follow Instructions.** All instructions for installation or operating/use should be followed closely.
5. **Cleaning.** Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use only a damp cloth for cleaning. Do not use isopropanol-based detergents to clean the unit.
6. **Ventilation.** Any slots and openings in the device or equipment are provided for ventilation and to ensure reliable operation of the product and to protect it from overheating. These openings must not be blocked or covered. The openings should never be blocked by placing the product on a bed, sofa, rug, or other similar surface. This product should not be placed in a built-in installation such as a bookcase or rack unless proper ventilation is provided or the manufacturer's instructions have been adhered to.
7. **Heat.** The product should be situated away from heat sources such as radiators, heat registers, stoves, or other products (including amplifiers) that produce heat. Do not use or operate any equipment in environments that exceed the standard operating temperatures.
8. **Modifications.** Do not use any modifications, extension, or other attachments not recommended by the product manufacturer as they may cause hazards.
9. **Accessories.** Only use attachments/accessories specified by the manufacturer. Do not place this product on an unstable cart, stand, tripod, bracket, or table. The product may fall, causing serious injury to a child or adult, and serious damage to the product. Use only with a cart, stand, tripod, bracket, or table recommended by the manufacturer, or sold with the product. Any mounting of the product should follow the manufacturer's instructions, and should use a mounting accessory recommended by the manufacturer.
10. **Water and Moisture.** Do not use this product near water or in a moist environment - for example, near a bath tub, wash bowl, kitchen sink, or laundry tub; in a wet basement; or near a swimming pool, in an unprotected outdoor installation; and the like.

11. **Moving.** A product and cart combination should be moved with care. Quick stops, excessive force, and uneven surfaces may cause the product and cart combination to overturn.

12. **Power Sources.** This product should be operated only from the type of power source indicated on the marking label. If you are not sure of the type of power supply to your home, consult your product dealer or local power company. For products intended to operate from battery power, or other sources, refer to the operating instructions.

13. **Grounding or Polarization.** Do not defeat the safety purpose of the polarized or ground-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wider blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.

14. **Power-Cord Protection.** Power-supply cords should be routed so that they are not likely to be walked on or pinched by items placed upon or against them, paying particular attention to cords at plug, convenience receptacles, and the point where they exit from the product.

15. **Lightning.** For added protection for this product during a lightning storm, or when it is left unattended and unused for long periods of time, unplug it from the wall outlet. This will prevent damage to the product due to lightning and power-line surges. (Not applicable when special functions are to be maintained, such as evacuation systems.)

16. **Overloading.** Do not overload wall outlets, extension cords or integral convenience receptacles as this can result in a risk of fire or electric shock.

17. **Object and Liquid Entry.** Never push objects of any kind into this product through openings as they may touch dangerous voltage points or short-out parts that could result in a fire or electric shock. Never spill liquid of any kind on the product.

18. **Inflammable and Explosive Substance.** Avoid using this product where there are gases, and also where there are inflammable and explosive substances in the immediate vicinity.

19. **Heavy Shock or Vibration.** When carrying this product around, do not subject the product to heavy shock or vibration.

20. **Servicing.** Do not attempt to service this product yourself as opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified service personnel.

21. **Damage Requiring Service.** Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:

- a. When the power-supply cord or plug is damaged.
- b. if liquid has been spilled, or objects have fallen into the product.
- c. If the product has been exposed to rain or water.
- d. If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions as an improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the product to its normal operation.
- e. If the product has been dropped or damaged in any way.
- f. When the product exhibits a distinct change in performance-this indicates a need for service.

22. **Replacement Parts.** When replacement parts are required, be sure the service technician has used replacement parts specified by the manufacturer or have the same characteristics as the original part. Unauthorized substitutions may result in fire, electric shock, or other hazards.

23. **Safety Check.** Upon completion of any service or repairs to this product, ask the service technician to perform safety checks to determine that the product is in proper operating condition.

24. **Coax Grounding.** If an outside cable system is connected to the apparatus, be sure the cable system is grounded. U.S.A. models only: Section 810 of the National Electrical Code, ANSI/NFPA No.70-1981, provides information with respect to proper grounding of the mount and supporting structure, grounding of the coax to a discharge apparatus, size of grounding conductors, location of discharge unit, connection to grounding electrodes, and requirements for the grounding electrode.

## Power Connections

For permanently connected equipment, a readily accessible disconnect device shall be incorporated in the fixed wiring; For pluggable equipment, the socket-outlet shall be installed near the equipment and shall be easily accessible.



This label may appear on the bottom of the apparatus due to space limitations.



The lightning flash with an arrowhead symbol, with an equilateral triangle, is intended to alert the user to the presence of un-insulated 'dangerous voltage' within the products enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.



The exclamation mark within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.



To reduce the risk of fire or electric shock, do not expose this appliance to rain or moisture. Do not open the cabinet; refer servicing to qualified personnel only.



To prevent electric shock, do not use this (polarized) plug with an extension cord receptacle or other outlet unless the blades can be fully inserted to prevent blade exposure.



Installation should be performed by qualified service personnel only in accordance with the National Electrical Code or applicable local codes.





# COMPONENTS

## Plixus Gateway



The Plixus Gateway engine is a 19" rack mountable device that can be easily integrated in the Plixus architecture. It is the central control point for traffic flowing in and out the conferencing room.

The Plixus Gateway is TLS-encrypted (versions 1.2 and 1.3 are supported), providing end-to-end security between the Gateway to the Confero Cloud platform, hosts an authentication service and also embeds a TPM2.0 module (ISO/IEC 11889), securing the transfer in and out the room of audio, video and conference data, while also ensuring interoperability with all other conferencing devices of the Plixus installation.

The Plixus Gateway must be connected to one of the following Central Units:

- > Plixus AE-R
- > Plixus MME
- > Confidea WAP G4

A Confidea WAP G3 device can be connected to the Plixus Gateway, but this needs to be established in combination with either Plixus AE-R or Plixus MME.

## Central Units

### PLIXUS AE-R



Plixus AE-R is an embedded system for meeting management that provides all the processing and signal handling required for the Plixus network. It comes with both analog and digital audio interfaces, controls the delegate units and interconnects other audio systems. A record button also allows to start and stop the audio recording of the meeting.

**CONFIDEA WAP G4**



Confidea WAP G4 controls all communication to and from the Confidea FLEX G4 Wireless units. It can be used for meeting management, and comes with both analog and digital audio interfaces, as well as recording capabilities.

**PLIXUS MME**



The Plixus Multimedia Engine provides all the processing and signal handling required for the Plixus network. It controls delegate units and interconnects to other systems, either via the external audio connections or the control ports.

# PLIXUS GATEWAY

The Plixus Gateway engine is a 19" rack mountable device that provides full security between the Confero Cloud services, the conferencing system and the users by allowing traffic in and out between the Internet and the local room (transfer of audio, video and conference data). By distributing traffic across multiple appliances, it ensures interoperability with all of the other conferencing devices (Central Unit/WAP, screen, cameras...).

## Front View

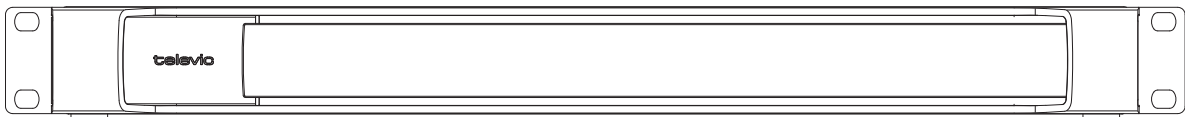


Figure 1-2 Front view of Plixus Gateway

## Rear End Connectivity

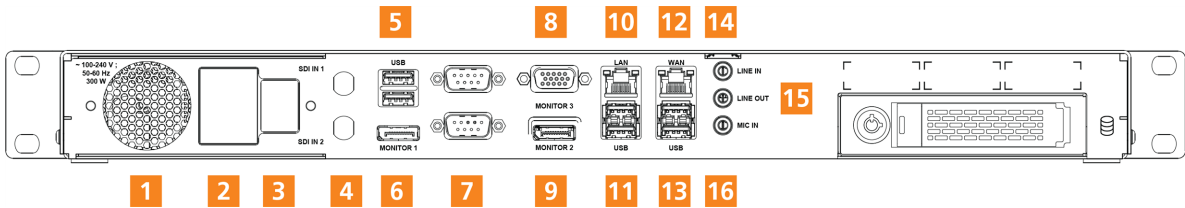


Figure 1-3 Back view of Plixus Gateway

1. Ventilation slot
2. Power connector
3. On/off switch
4. Two SDI video inputs **[Do not use SDI1]**
5. Two USB 2.0 ports
6. Display port 1 **[Mandatory to use]**
7. Two DB9 ports **[Do not use]**
8. VGA port
9. Display port 2 **[Do not use]**

10. LAN port **[Do not use]**
11. USB 2.0 port
12. WAN port
13. USB 2.0 port
14. Line in port 3.5 mm
15. Line out port 3.5 mm
16. Mic in port 3.5 mm (not functional)



The WAN port should always be used to connect the Plixus Gateway to an Internet service.

# BEFORE INSTALLING THE PLIXUS GATEWAY

This chapter describes the information that must be transferred by the customer to Televic Conference before installing the gateway . A separate document will be provided by Televic Conference for the customer to fill in.

It will also describe the basic IT requirements the customer has to meet before installing the gateway.

# REQUIRED INFORMATION

Prior to the installation of the Plixus Gateway, Televic must be provided with information from the customer in order to make sure that all the configuration parameters of the device are adjusted.

Based on the information that you will submit, Televic will create configuration files for installing the Plixus Gateway.

Visit the following page: <https://www.televic.com/en/conference/request-software-license>, select Plixus Gateway in the Product's dropdown list, and fill in the form with the requested information. You will be asked to enter the following:

- > Serial number of the Plixus Gateway
- > Full name of the Admin user (the person who will be managing other users on the Confero Cloud Platform)
- > Email of the Admin user
- > Names and email addresses of other Admin users



**Fake email addresses should not be used** as they will be treated as spam. In case fake emails are required, use "@email.com", but no other domain names.

- > Name of the organization
- > Name of the room



Make sure to enter the **right name for the organization and the room**, as they cannot be changed later on on the Confero Cloud Platform.

- > Your first name and last name
- > Name of your company
- > Your email address
- > Name of the project
- > Country

# IT CONSIDERATIONS

## Web Browser

At this moment, the Confero Cloud platform is only compatible with Google Chrome and Microsoft Edge. Confero relies on the WebRTC technology (Web Real-Time Communications), which is not supported by all browsers. Make sure you have the latest version of Chrome or Edge for a worry-free experience with the Confero Cloud platform.

## Connectivity Towards The Internet

The Plixus Gateway must have access to the Internet for both data controlling and audio/video streaming.

The same connection requirements apply to the remote delegates who will participate in the meeting.

A summary of all communication types can be found below:


IP Source	Destination	Protocol / Service	Additional information
Gateway IP address(*)	https://nexus.televic.com https://deb.debian.org https://security.debian.org	TCP port 443 (https)	Gateway update
Gatewat IP address(*)	http://http.us.debian.org http://security.debian.org	TCP port 80 (http)	

IP Source	Destination	Protocol / Service	Additional information
Gateway IP address(*)	https://tcs-confero-production.firebaseio.com https://europe-west3-tcs-confero-production.cloudfunctions.net https://tcs-confero-production.firebaseio.com/ https://confero.televic.com https://confero-proxy.televic.com logging.googleapis.com www.googleapis.com firebase.googleapis.com firestore.googleapis.com fcm.googleapis.com gcm-http.googleapis.com	TCP port 443 (https)	Google cloud (google functions and web app store)
Gateway IP address (*)	*.tokbox.com	TCP port 443 (https)	Audio/video streaming (**)
	*.opentok.com		
	<u>Optional (can cause console warnings, but will not impact the session(***)):</u> ojsp.godaddy.com crl.godaddy.com	UDP port 3478 (**)	Audio/video streaming (**), optional port for enhanced experience

(\*) Gateway IP address for WAN port (DHCP): see the [Plixus Gateway and Central Unit Configuration](#) section below for more information.

(\*\*) See the [Vonage Video API Network Connectivity Requirements](#) section below for more information.

(\*\*\*) See the [Whitelisting a Domain in your Web Browser](#) section below for more information.

 For optimal quality (720p resolution), a minimum bandwidth of 15 Mbps is assumed. Note that in case the bandwidth is (temporarily) lower, the quality of the video and audio will be impacted.



# Connectivity Between The Plixus Gateway And The Central Unit

The Plixus Gateway has to communicate with the Central Unit. The dataflows below need to be made possible:

IP Source	Destination	Protocol / Service	Additional information
Gateway IP address(*)	Central Unit (Plixus AE-R/MME or Confidea WAP G4)	TCP port 9012 (http)	REST API for meeting control

(\*) The Gateway IP address is the WAN port connection (DHCP).

## Plixus Gateway And Central Unit Configuration

The requirements regarding the configuration of the Gateway and Plixus Central Unit within the client IT network are as follows:

	Plixus Gateway	Plixus Central Unit or G4 WAP
Type of device	Linux (Debian 10 based)	Embedded Linux device
Network connection type	WAN port (DHCP)(*)	Static IP address
Additional devices that need connectivity to these devices	-	All clients who need access to the Confero 360 interface, which is required for meeting management (min. for starting a meeting).  Camera tracking solutions (for active speakers through the API).



(\*) You need a DHCP server if the WAN port is used. The Client-Identifier that is sent to the DHCP server is equal to the MAC address of the port. **The MAC address of the WAN port can be found on the label of the Plixus Gateway.**



(\*\*) The IP address of the port connected with the Central Unit must be in the same range as the Central Unit.

# Vonage Video API Network Connectivity Requirements

Televic uses Vonage (formerly TokBox), a WebRTC platform that allows to embed high-quality video, voice and messages and screen-sharing to websites.

Vonage maintains a list of IP address blocks associated with the Video API platform components. Vonage shares this information with select enterprise customers who need to know IP addresses of Vonage Video API servers in order limit exposure of their network to trusted end-points only. This list includes the following components:

- › Media servers — In routed sessions, clients send audio and video to our media server for intelligent and efficient routing.
- › TURN servers — In relayed sessions, if strict network conditions prevent direct connectivity between clients, clients use these servers to relay audio and video.
- › API server — Clients connect to this server for session initialization and signaling.
- › Logging servers — Our logging server collects anonymized data about quality and possible errors.

Vonage will support Video API enterprise customers with above-mentioned requirements by sharing the published list of IP address blocks. Vonage will also have a process in place to manage updates to the IP address blocks without disrupting service.

Vonage will provide a 90-day advance notice to customers using the published IP address blocks. But in case of an unexpected event where additional capacity needs to be added immediately to handle a surge in traffic or other business and operational decisions that result in a change in IP address blocks, Vonage will not adhere to the 90-day advance notice. In these cases, Customers would be expected to use the updated list of IP address blocks published by Vonage. Failure to stay up-to-date with the latest IP address blocks published by Vonage will lead to disruption of service.

[Sources: <https://support.tokbox.com/hc/en-us/articles/360029733631-What-are-the-TokBox-network-connectivity-requirements-> & <https://tokbox.com/developer/enterprise/content/ip-addresses/>]

## FIREWALL REQUIREMENTS

Vonage Video API services require access to specific ports. At a minimum, the following requirements must be met:

- › Open TCP port 443
- › Whitelist the following domains: *\*.tokbox.com* and *\*.opentok.com*

Along with the minimum requirements, opening UDP Port 3478 will provide a better experience. UDP is recommended over TCP for better quality audio and video. UDP favors timeliness over reliability, which is

consistent with human perceptive preferences, where we can fill in gaps but are sensitive to time-based delays.

This port only accepts inbound traffic after an outbound request is sent. The connection is bidirectional but is always initiated from the corporate network/client, so it is not possible for an external entity to send malicious traffic in the opposite direction. For the best possible experience, we recommend opening UDP ports 1025 - 65535.

Whitelist the following HTTPS verification servers for our HTTPS certificate. Not doing so may cause console warnings, but should not affect the session.

- > ocsf.godaddy.com
- > crl.godaddy.com

Alternatively, the following range of IP addresses can be whitelisted instead of the URLs:

```
{ "ipv4": [ "3.123.12.128/28", "3.127.48.224/28", "3.214.145.96/27", "3.234.232.160/27",  
"3.234.248.80/28", "3.235.255.176/28", "3.248.234.48/28", "3.248.243.144/28",  
"3.248.244.96/27", "3.25.48.192/28", "3.38.113.0/24", "3.38.114.0/24", "3.38.91.128/25",  
"3.7.161.0/26", "3.7.161.48/28", "13.251.158.0/28", "15.228.1.16/28", "18.139.118.176/28",  
"18.141.165.128/27", "18.156.18.0/27", "18.157.71.112/28", "18.179.48.208/28",  
"18.180.159.224/27", "18.202.216.0/28", "34.78.52.235", "34.218.216.144/28",  
"34.222.66.96/28", "34.223.51.192/27", "34.223.51.224/27", "35.158.127.224/28",  
"44.232.236.96/27", "44.234.90.64/28", "52.200.60.16/28", "52.213.63.176/28",  
"52.41.63.240/28", "52.51.63.16/28", "52.65.127.192/27", "52.66.255.192/27",  
"54.233.127.224/29", "54.250.250.208/28", "54.69.125.241/32", "54.89.253.64/28",  
"99.79.160.16/28", "99.80.88.240/28", "168.100.64.0/18" ] }
```



The above list of IP addresses will be subject to change. We highly recommend you to implement DNS lookup for these URLs into your firewall.



The **firewall settings for the gateway should also be set for all devices** (e.g. a laptop) **that connect to the Confero Platform** to avoid interface issues.

## PROXY REQUIREMENTS

If the only way to access the Internet from your network is through a proxy then it must be a transparent proxy or it must be configured in the browser for HTTPS connections. WebRTC does not work with proxies requiring authentication. Along with these requirements, clients may have the following rules:

## CHROME

- › Although not every option has been tested, versions 80 and higher have full support for authentication
- › We've found a forwarding proxy setup with Kerberos does not work

## Whitelisting A Domain In Your Web Browser

In case your browser is blocking the access to the Confero Cloud platform when starting the configuration of the Plixus Gateway, you can change the permission settings of the browser and whitelist the domains mentioned in the previous section.

To know how to whitelist a domain in Google Chrome, click on the following link and follow the steps: <https://support.google.com/chrome/answer/114662>.

For Microsoft Edge, go to <https://support.microsoft.com/en-us/microsoft-edge/change-site-access-permissions-for-extensions-in-microsoft-edge-7d1c889d-e267-4be0-15d4-3ed5d0c82ef5>.

## Fixed IP Address

The Plixus AE-R, Plixus MME or Confidea WAP G4 Central Unit must have a fixed IP address to be able to configure the Plixus Gateway.



The IP of the Central Unit can be achieved through DHCP. In that case, the IP should be fixed in the DHCP server. If the engine is in DHCP mode, always make sure that the IP address is always the same.

## Email Communications

To reduce the chances of sending emails that will be treated as spam, it is recommended to configure your originating email server with the following static IP address: 149.72.24.255.



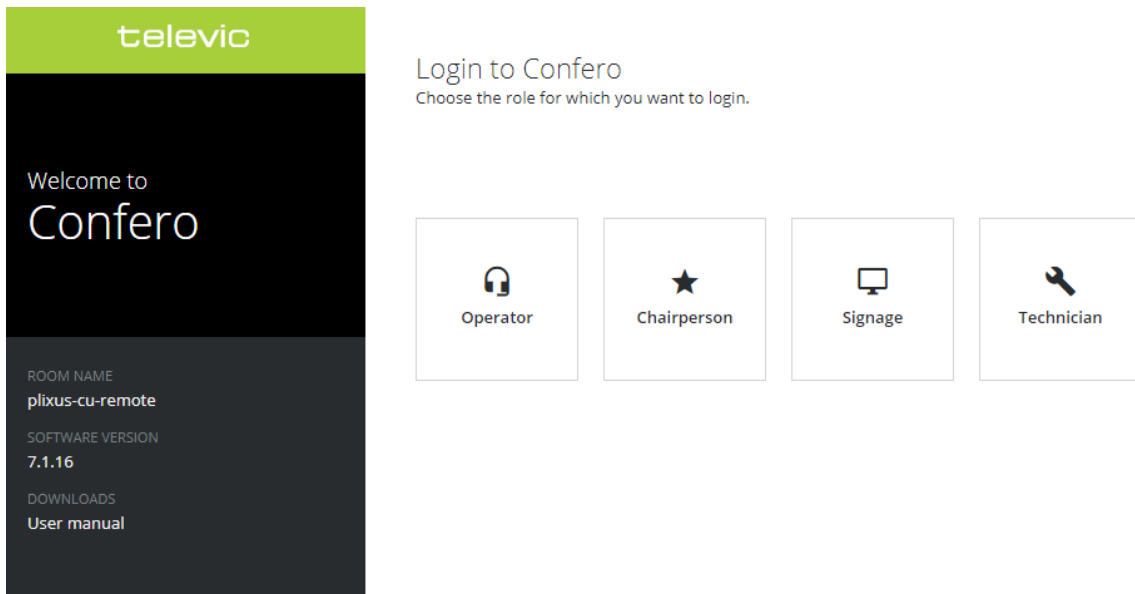
**Fake email addresses should not be used** on the Confero Cloud platform as they will be treated as spam. In case fake emails are required, use "@email.com", but no other domain names.



# SOFTWARE CONFIGURATION


Before connecting the Plixus Gateway to other devices, it is necessary to verify a few information in the software of your Central Unit.

Open your browser and enter the IP address of your Central Unit in the address bar (by default: 192.168.0.100). If you are connected to the Internet, the Confero Cloud platform opens. Log in as **Technician**.



## Version Of The Central Unit

The version of the Central Unit must be 7.2 or higher. To check the version of your Plixus AE-R, Plixus MME or Confidea WAP G4 device, process as follows:


1. Click on the **Device** icon  in the left bar menu. You will get an overview of all the devices of your installation where you can see the version of the central unit:

Device	Firmware	Software
Plixus MME SN: 14098245	6.2.2	7.1.16
Confidea T SN: 1530100C	7.1.1	
Confidea T-CV SN: 153100A6	7.1.1	
Confidea T-CI SN: 15311650	7.1.1	
Confidea T-DI SN: 15312198	7.1.1	
Confidea T-DV SN: 15320798	7.1.1	
Confidea T SN: 15382846	-	-
unICOS F/MM7 SN: 15E108A5	7.1.1	7.1.16
Confidea FLEX SN: 160107AB	7.5.1	7.1.16

2. If your Central Unit is not up-to-date, visit Televic Conference's **Software page** and look for updates: <https://www.televic-conference.com/en/plixus-software-updates>.

## Confero 360 License

The Confero 360 license must be installed. To check whether it is present in your system, process as follows:

1. Click on the **Settings** icon  in the left bar menu and then on the **License** tab. You will get an overview of all the licenses of your installation:

**Settings** | Technician

General | **License** | Camera protocol | Backup

Upload license (MAC address: 00:0e:3d:1d:a1:b7)

Upload or drop your file here (.xml)

**Your licenses**

- > Confidea FLEX | Expires on 2022-04-01 | Valid
- > Confero | Expires on 2022-04-01 | Valid

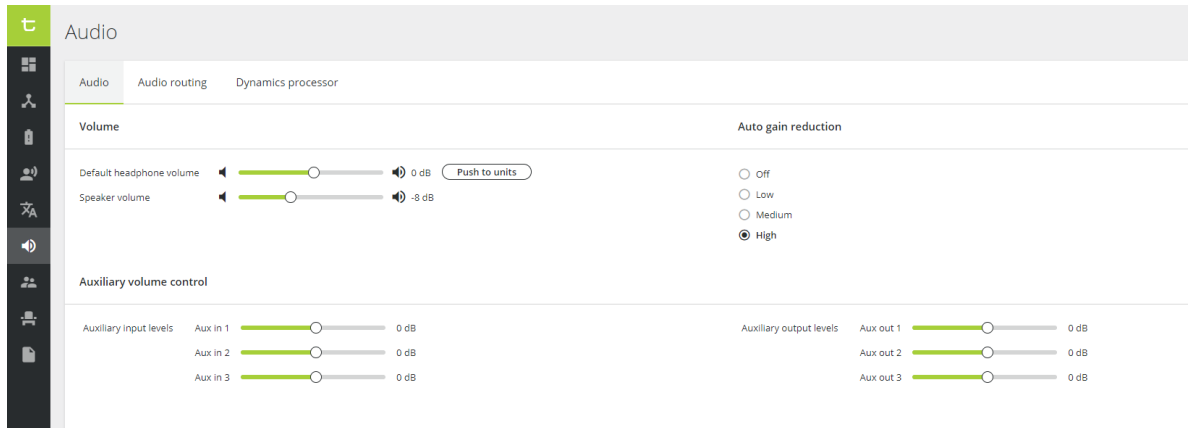
2. Verify whether or not the Confero 360 is in the list. If the Confero license does not appear in the list, you can request it to Televic Conference. Visit Televic's **Software License Request page**

here: <https://www.televic-conference.com/en/software-license-request>. After uploading the new license in your system, it will appear in the list here-above.

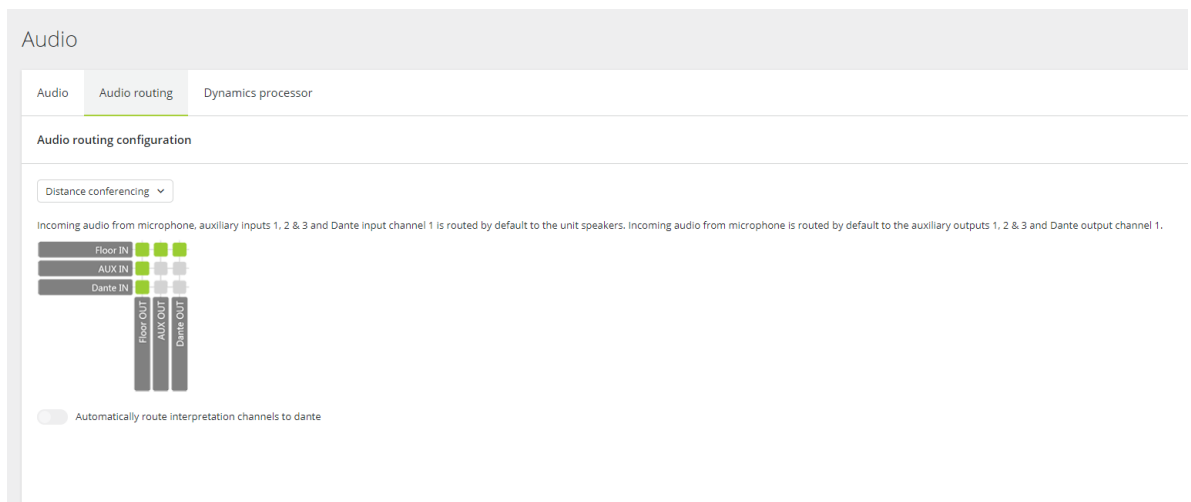
## Audio Configuration Of The Central Unit

The audio configuration must be changed in the Central Unit. Process as follows:

1. Click on the **Audio** icon . The following window opens:



2. Open the **Audio routing** tab and select **Distance conferencing** in the drop-down menu.



The software configuration is now finished. You can connect the Plexus Gateway to your other devices.



# HARDWARE INSTALLATION



Before you start, make sure to take all necessary precautions. Refer to the safety instructions and ensure that all components are installed and sufficiently powered.

## Physical Installation

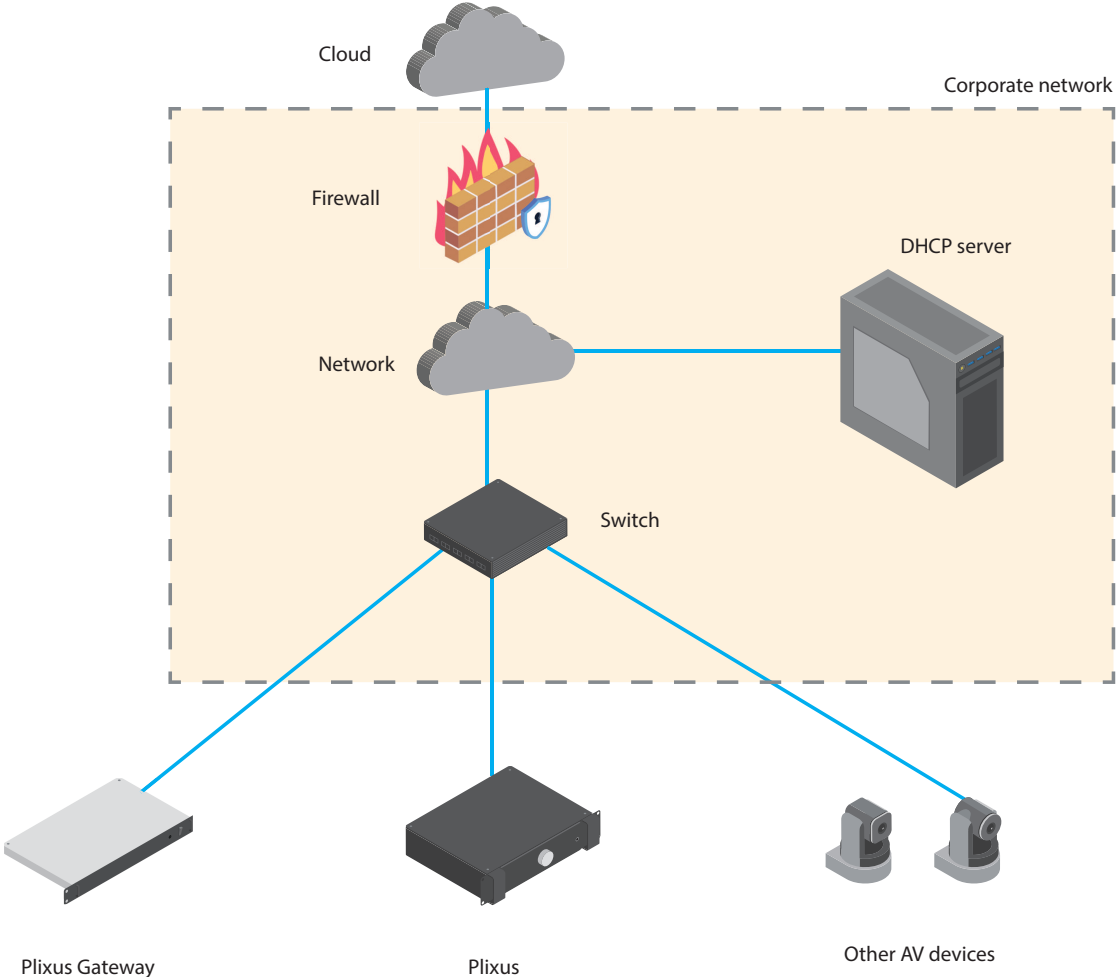
Before connecting the Plixus Gateway to the other devices of your conferencing system, it has to be physically installed in the room. You can install the Gateway on a desktop, on a wall, or in a rack. Follow the procedure below:

1. Connect the power cord to the power port of the Plixus Gateway.
2. Mount the Plixus Gateway horizontally (e.g. in a rack, on a desktop) or vertically:
  - > **If mounted on a rack**, attach the Gateway to the rack using the mounting screws.
  - > **If placed on a desktop**, make sure the Gateway is in its permanent location with adequate space for airflow maintenance.
  - > **If mounted vertically**, use an adequate mounting kit (not included).
3. Plug the other end of the power cord to a power outlet.
4. Turn on the power switch.
5. Connect the Gateway to the PeO switch, the Central Unit and a monitor (if applicable). Depending on the type of Central Unit of your installation, refer to one of the connecting diagrams below.

# Network Topology

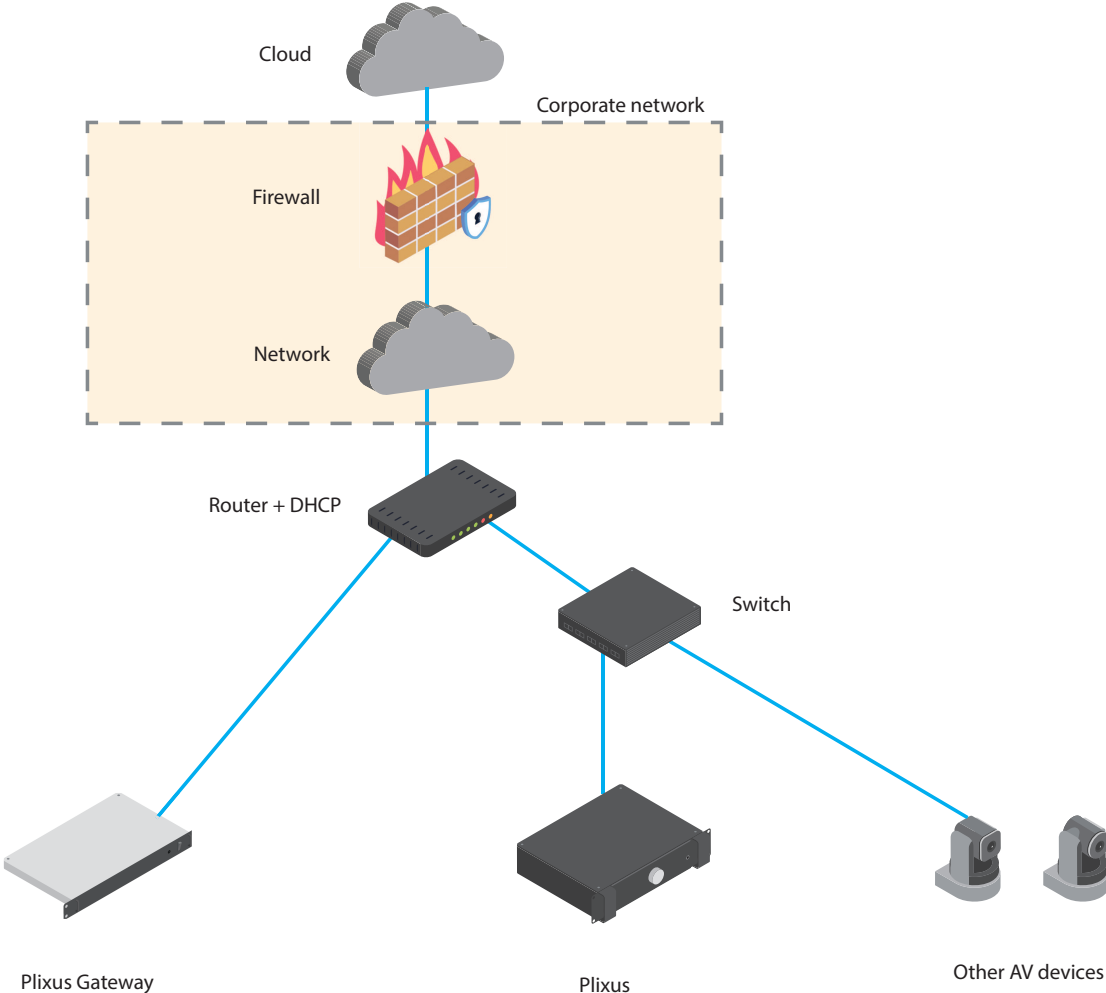
## BASIC SETUPS

The Plixus Gateway and other network devices are connected to the switch. The firewall, the switch and the DHCP server all belong to the corporate network. Any device can be blocked from accessing the Internet via the firewall.



The DHCP server is included in the router. DHCP is required for the Gateway and, optionally, the Plixus Central Unit. Blocking the Plixus Central Unit and other AV devices from accessing the Internet can be done via the router or the firewall.

Because the DHCP server is inside the router, it is possible to set it so that it is not exposed to the corporate network.



## ADVANCED SETUP

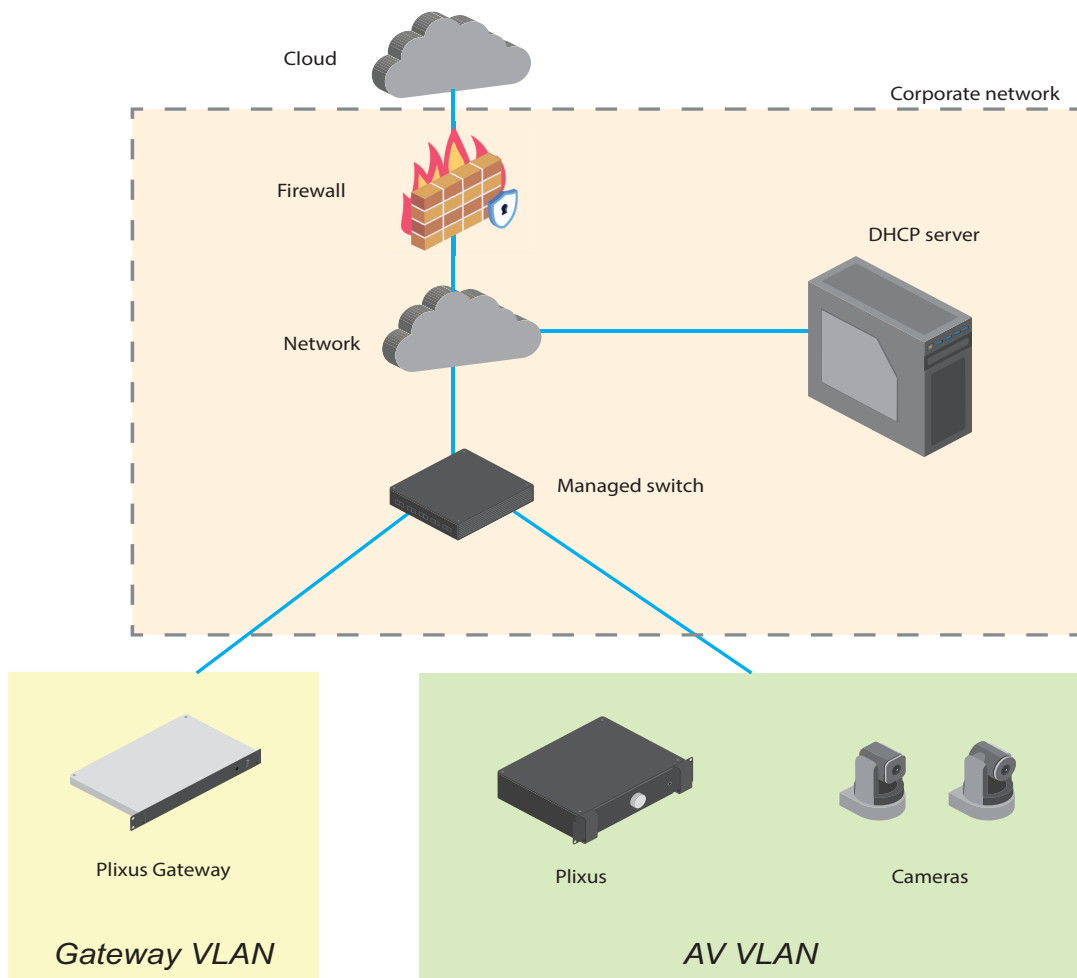
The Plexus Gateway, Plexus engine and AV devices are separate VLAN networks and are connected to a switch.

To be more secure, it is possible to set network restrictions on the VLAN level.

- Regarding the Gateway VLAN, the Gateway needs access to all the domains mentioned in the [IT Considerations chapter](#) of this manual. Access to the Plexus Central Unit and the cameras is also needed.
- Regarding the AV VLAN, the Plexus Central Unit needs access to the Gateway, and the cameras need access to the Gateway

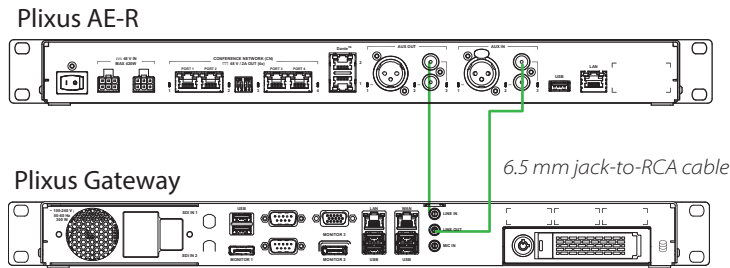


In case VLAN are involved, a **managed switch** is required to configure and control the network.



# Connection Diagram For The Audio

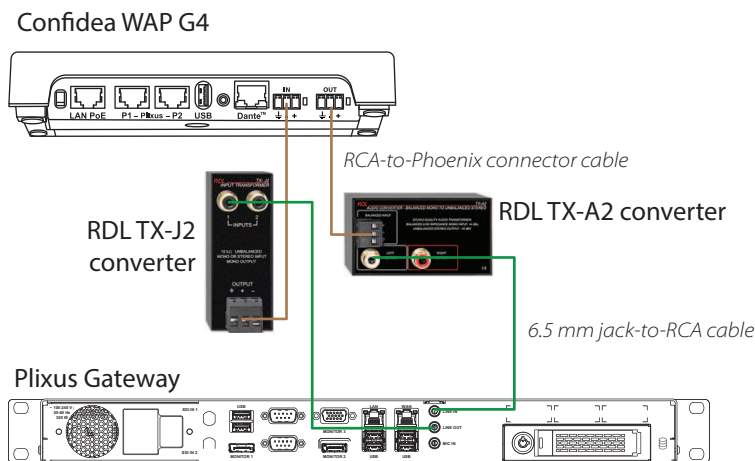
## WITH PLIXUS AE-R



The LINE IN port of the Plexus Gateway must be connected to the AUX OUT 3 port of Plexus AE-R.

The LINE OUT port of the Plexus Gateway must be connected to the AUX IN 3 port of Plexus AE-R.

## WITH CONFIDEA WAP G4



To connect the LINE OUT (green female Jack port on the Plexus Gateway) to the AUX IN of the Confidea WAP G4, use an unbalanced-to-balance converter to convert the signals. In the diagram, we use a RDL TX-J2 converter.

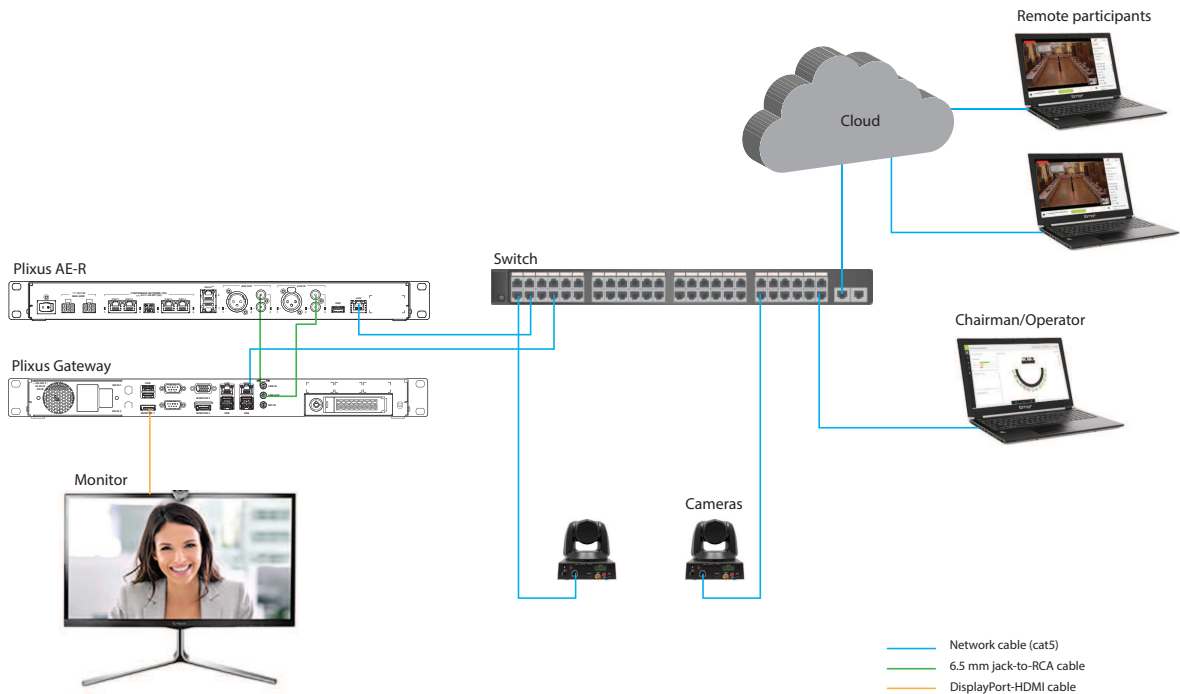
To connect the LINE IN (green female Jack port on the Plexus Gateway) to the AUX OUT of the Confidea WAP G4, use an unbalanced-to-balanced converter to convert the signals. In the diagram, we use a RDL TX-A2 converter.

# Connecting The Gateway To Plexus AE-R

If your Central Unit is a Plexus AE-R device, refer to the diagram below to connect the Plexus Gateway.




It is highly recommended to install the Plixus Gateway as close as possible to the Central Unit in order to make sure that the audio cables are not too long.




- › The Plixus Gateway should be connected to the WAN port.
- › In case SDI cameras are used, they should be connected to the SDI input 2 of the Plixus Gateway.
- › In case you are using the **T-CAM** solution, a PC with the installed **T-CAM software** will need to be connected to the system. Please refer to the T-CAM manual for more information.
- › The Chairman of the room needs to see the other participants during a meeting. A monitor can be connected to the Plixus Gateway via the Display port HDMI adapter.
- › The LINE IN port of the Plixus Gateway must be connected to the AUX OUT 3 port of Plixus AE-R.
- › The LINE OUT port of the Plixus Gateway must be connected to the AUX IN 3 port of Plixus AE-R.

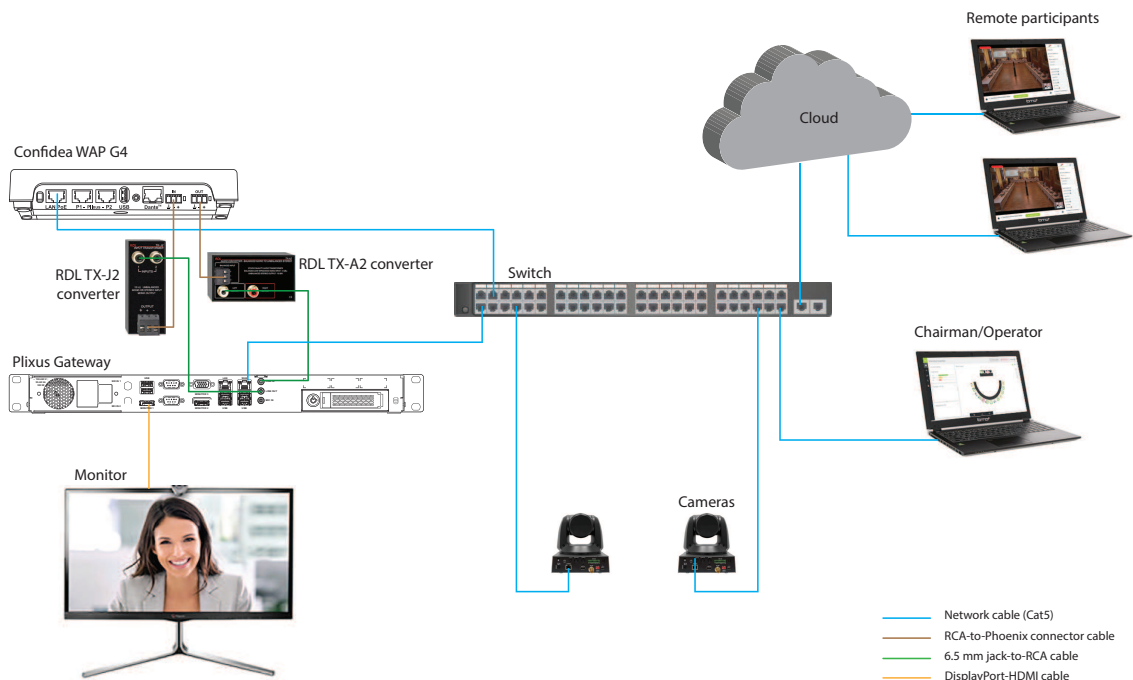
- If you need to connect a monitor to the Gateway, you must use the Monitor1 port.
- The Plixus Gateway must receive an IP address from the DHCP server installed on the customer's network.
- The IP address of Plixus AE-R must be in the same range as the IP address of the Plixus Gateway.

 If you want to combine inputs (e.g. a wireless microphone) and/or outputs (e.g. external speakers) with the Plixus Gateway, make sure that the Plixus Gateway is directly connected to Plixus AE-R, and that the **inputs/outputs are handled by Plixus AE-R**.

## Connecting The Gateway To Confidea WAP G4

If your Central Unit is a Confidea WAP G4 device, refer to the diagram below to connect the Plixus Gateway.

 The Confidea WAP G4 is using balanced audio signals while the Plixus Gateway is using unbalanced audio signals. To solve this problem, we highly recommend to use audio converters.



- › The Plixus Gateway should be connected to the WAN port.
- › To connect the LINE OUT (green female Jack port on the Plixus Gateway) to the AUX IN of the Confidea WAP G4, use an unbalanced-to-balance converter to convert the signals. In the diagram, we use a RDL TX-J2 converter.
- › To connect the LINE IN (green female Jack port on the Plixus Gateway) to the AUX OUT of the Confidea WAP G4, use an unbalanced-to-balanced converter to convert the signals. In the diagram, we use a RDL TX-A2 converter.
- › In case SDI cameras are used, they should be connected to the SDI input 2 of the Plixus Gateway.
- › In case you are using the **T-CAM** solution, a PC with the installed **T-CAM software** will need to be connected to the system. Please refer to the T-CAM manual for more information.
- › The Chairman of the room needs to see the other participants during a meeting. A monitor can be connected to the Plixus Gateway via the Display port HDMI adapter.
- › If you need to connect a monitor to the Gateway, you must use the Monitor1 port.
- › The Plixus Gateway must receive an IP address from the DHCP server installed on the customer network.
- › The IP address of the Confidea WAP G4 must be in the same range as the IP address of the Plixus Gateway.





# SYSTEM TESTING

The test plan is an official document that ensures that the entire setup has been tested. It has to be filled in and signed by the customer and is not included in this manual.



It is recommended to organize a "real use" test case meeting in order to complete the test plan.

The test plan is a separate document and is not included in the manual.

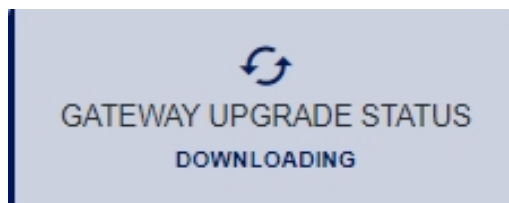
# SYSTEM UPDATES

The system updates are automatic and periodic. They start one minute after switching on the Plixus Gateway. Afterwards, they run on an hourly basis.

When the system is checking for software updates, the following message appears:



When the system is downloading software updates, the following message appears:

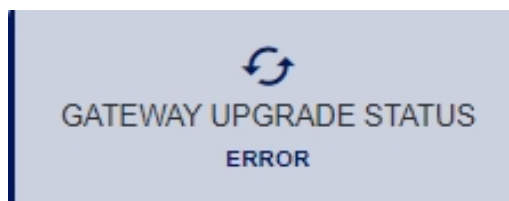


During the update, the following message appears:



The system will reboot automatically after every update.

In case the update fails, the following message appears. Contact Televic Conference's Support Service.



Do not turn off the Plixus Gateway when an upgrade is in progress!



To avoid any troubleshooting, the system is not allowed to update when a meeting is in progress on the Central Unit.



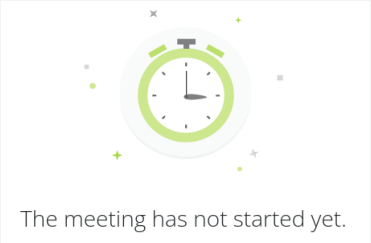
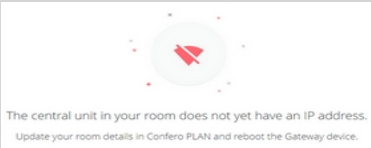

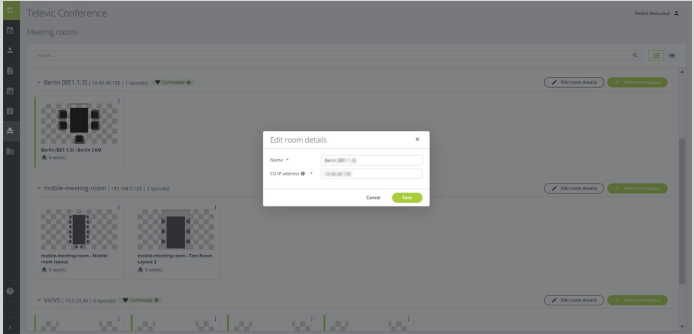
In order to ensure the correct functionality of the system, the Central Unit and other devices of your conferencing system must be up-to-date. The updates must be done manually. Refer to the [Software Configuration](#) section or to the corresponding manuals for more information.

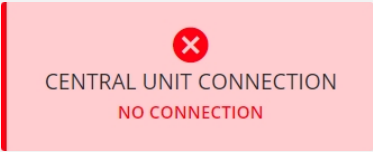
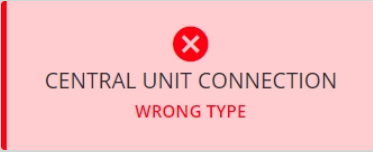
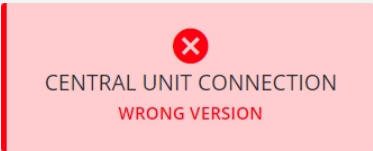
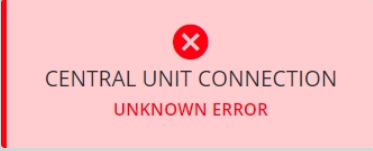
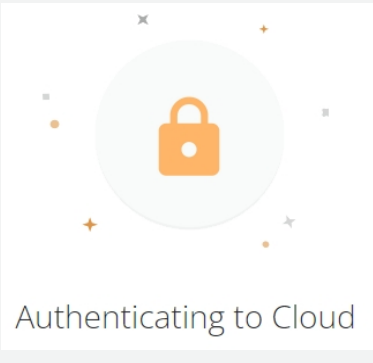
# FAQS AND TROUBLESHOOTING

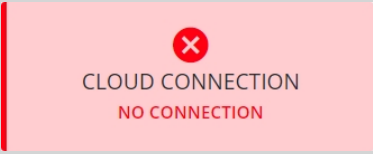
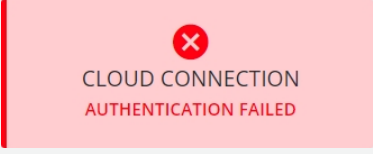
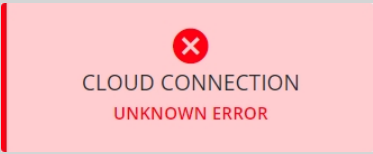

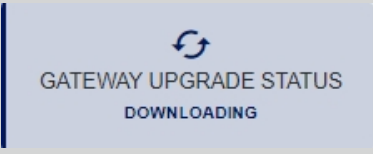

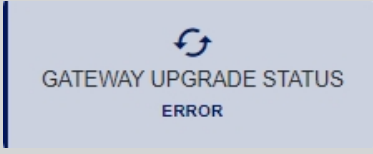
This chapter lists the information and error messages that can show on the screen of the Plixus Gateway, as well as the questions the customer may have when installing the device.

# PLIXUS GATEWAY DISPLAY AND TROUBLESHOOTING



Here-above are the messages that can be displayed on the screen of the Plixus Gateway:

Displayed message	Meaning
 <p>The meeting has not started yet.</p>	<p><b>The connection between the Plixus Gateway and the Central Unit is functional.</b></p> <p>When the connection with the Central Unit is functional, extra information is also displayed on the screen (state of the connection, information about the WAN and the Central Unit):</p> <pre data-bbox="646 741 823 965"> CLOUD CONNECTION: OK WAN IP: 10.40.204.159 WAN SUBNET: 255.255.254.0 WAN GATEWAY: 10.40.205.254 CU CONNECTION: Ok CU TYPE: AUDIO_ENGINE CU VERSION: 7.2.16-682 CU IP: 10.40.204.37 CU SUBNET: 255.255.254.0 CU GATEWAY: 10.40.205.254                     </pre>
 <p>The central unit in your room does not yet have an IP address. Update your room details in Confero PLAN and reboot the Gateway device.</p>	<p><b>The Central Unit in your room does not yet have an IP address.</b></p> <p>The Room Details in Confero Cloud are not correct and need to be edited. Open Confero Cloud, click on the Meeting Rooms icon  in the menu, and click on "Edit room details". Enter the right IP address of the Central Unit and click on "Save".</p> 

Displayed message	Meaning
 <p>CENTRAL UNIT CONNECTION NO CONNECTION</p>	<p><b>The Plixus Gateway cannot connect to the Central Unit.</b></p> <p>Refer to the <a href="#">Before Installing Plixus Gateway</a> chapter to make sure the Gateway has been configured based on the information you sent to Televic Conference. Verify that Central Unit has the correct IP address (same as the one used to onboard the Gateway)</p> <p>Refer to the <a href="#">Installation</a> chapter and verify that all devices are properly connected and that the network configuration is correct: the Gateway should be able to reach the Central Unit.</p>
 <p>CENTRAL UNIT CONNECTION WRONG TYPE</p>	<p><b>The Central Unit is not compatible with the Plixus Gateway.</b></p> <p>The gateway can be connected to either Plixus AE-R, Confidea WAP G4 or Plixus MME.</p>
 <p>CENTRAL UNIT CONNECTION WRONG VERSION</p>	<p><b>The Central Unit is not up-to-date.</b></p> <p>The Central Unit requires a mandatory update to keep working with the Confero Platform. The meetings will not be synced anymore from the Cloud to the Central Unit.</p> <p>Keep in mind that the Plixus Gateway is automatically updated but that the Central Unit needs to be updated <b>manually</b>.</p> <p>Refer to the <a href="#">Software Configuration</a> section or to the manual of your Central Unit, and update the Central Unit.</p>
 <p>CENTRAL UNIT CONNECTION UNKNOWN ERROR</p>	<p><b>Unidentified error.</b></p> <p>Refer to the <a href="#">Installation</a> chapter and verify that all devices are properly connected.</p> <p>Contact Televic Conference's Support Service if the problem persists.</p>
 <p>Authenticating to Cloud</p>	<p><b>Authenticating to Cloud.</b></p> <p>This message is shown at startup when the gateway is trying to authenticate itself to the Confero Cloud services.</p>

Displayed message	Meaning
 <p>CLOUD CONNECTION NO CONNECTION</p>	<p><b>The system cannot connect to the Internet.</b></p> <p>Verify that the connection of the Plixus Gateway is properly connected to the Central Unit and the PoE switch.</p> <p>Verify that the Central Unit is properly connected to the PoE switch.</p> <p>Verify that the firewall settings are correctly configured.</p> <p>Verify that the PoE switch is properly connected to the Internet.</p> <p>Verify the state of the network.</p>
 <p>CLOUD CONNECTION AUTHENTICATION FAILED</p>	<p><b>The authentication to the cloud failed.</b></p> <p>Verify that the firewall settings are correctly configured.</p> <p>Verify that you have sent all the required information to Televic Conference before installing the gateway, in particular the serial number and the IP address of the Central Unit. Refer to the <a href="#">Required Information</a> section of the manual, as well as to the information sheet you had to fill in and send to Televic Conference.</p> <p>Contact Televic Conference to make sure the Plixus Gateway has been configured properly.</p>
 <p>CLOUD CONNECTION UNKNOWN ERROR</p>	<p><b>Unidentified error.</b></p> <p>Refer to the <a href="#">Installation</a> chapter and verify that all devices are properly connected.</p> <p>Contact Televic Conference's Support Service if the problem persists*.</p>
 <p>GATEWAY STATUS UPDATE INFORMATION</p>	<p><b>Checking for updates.</b></p> <p>The system is checking if new software updates are available.</p>
 <p>GATEWAY UPGRADE STATUS DOWNLOADING</p>	<p><b>Upgrade downloading.</b></p> <p>The gateway is downloading the latest upgrade files. The upgrade will start soon.</p>
 <p>GATEWAY STATUS UPGRADE IN PROGRESS</p>	<p><b>Update in progress.</b></p> <p>The system is being updated. The Plixus Gateway will reboot when the updating process is finished. Do not turn off the Plixus Gateway while an update is in progress.</p>
 <p>GATEWAY UPGRADE STATUS ERROR</p>	<p><b>Upgrade error.</b></p> <p>The Gateway failed to upgrade itself. Contact Televic Conference's Support Service if the problem persists*.</p>



Displayed message	Meaning
 <p>A screenshot of a gateway status message. It features a blue circular refresh icon at the top. Below the icon, the text reads "GATEWAY STATUS" followed by "RECOVERY IN PROGRESS" on the next line. The background is a light blue-grey color.</p>	<p><b>A recovery USB stick has been inserted in the Plixus Gateway</b> The gateway will install the recovery software.</p>
 <p>A screenshot of a gateway status message. It features a blue circular refresh icon at the top. Below the icon, the text reads "GATEWAY STATUS" followed by "UNKNOWN" on the next line. The background is a light blue-grey color.</p>	<p><b>Unidentified error.</b> Contact Televic Conference's Support Service if the problem persists*.</p>

**\* Televic Conference's Support Service:**

Open a support ticket online: <https://www.televic-conference.com/en/support-home>

or

Get support via phone: +32 51332004 (international rates may apply)

# RECOVERY

In case the Plixus Gateway encounters issues that cannot be solved because it cannot update by itself anymore (e.g. the update server was changed while the Gateway was offline for a long period of time and could not be notified about that change), it is possible to restore the configuration using a recovery USB stick.

If necessary, contact Televic Conference (or your installer or integrator) to ask for recovery content and get the procedure to install it via a USB stick.

# FAQS

## **Can I use one gateway for two different rooms?**

No, it is not possible to use one gateway for two different rooms. Each room needs one gateway.

## **Can I configure the gateway with a fixed IP address?**

No, the gateway never has a fixed IP address. DHCP is always activated on the gateway.

## **Which of the SDI ports can be used on the gateway?**

Only the SDI2 port can be used. The SDI1 port is not connected for now.

## **I only see a white screen with Televic in the left corner of the gateway. What does it mean?**

It means the gateway has not been configured with the IP address of the Central Unit. There is no connection between the devices. Verify that the installation has been done properly.

## **Is the Confero Cloud platform compatible with all browsers?**

No. At this moment, the Confero Cloud platform is only compatible with Google Chrome and Microsoft Edge. Confero relies on the WebRTC technology (Web Real-Time Communications) that is not supported by all browsers. For a worry-free access to the platform, you need the latest version of Google Chrome or Microsoft Edge.

## **How do I access the Confero Cloud platform through a firewall?**

The following domains need to be whitelisted:

- > \*.televic.com
- > \*.tokbox.com
- > \*.opentok.com

See the [Whitelisting a Domain in Your Web Browser](#) section for more information.



The **firewall settings for the gateway should also be set for all devices** (e.g. a laptop) **that connect to the Confero Platform** to avoid interface issues.

## **Does the Gateway provide a USB audio/video stream into the laptop or is a converter needed?**

It's possible to take the video and audio out of the Gateway, but you will need an AV bridge.

## **Why do I have no audio coming in and out when using the Confero Cloud Platform?**

Have you selected **Distance conferencing** in the **Audio** settings? See the [Audio Configuration of the Central Unit](#) section for more information

**[Confero CAM] The Gateway cannot access the cameras and/or the cam composer freezes?**

The cameras have been powered on at the same time or after the Gateway. To avoid detection issues, the cameras need to be powered on first. Process as follows:

- › Power on the cameras and leave them on for a few seconds.
- › Power on the Gateway

**TELEVIC CONFERENCE**

Leo Bekaertlaan 1

8870 Izegem

Belgium

+32 51 30 30 45

**GET IN TOUCH**