Yealink

VC400 & VC120 Video Conferencing System Administrator Guide

Version 30.20
Aug.2017

Copyright

Copyright © 2017 YEALINK (XIAMEN) NETWORK TECHNOLOGY

Copyright © 2017 Yealink (Xiamen) Network Technology CO., LTD. All rights reserved. No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Yealink (Xiamen) Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

When this publication is made available on media, Yealink (Xiamen) Network Technology CO., LTD. gives its consent to downloading and printing copies of the content provided in this file only for private use but not for redistribution. No parts of this publication may be subject to alteration, modification or commercial use. Yealink (Xiamen) Network Technology CO., LTD. will not be liable for any damages arising from use of an illegally modified or altered publication.

Trademarks

Yealink®, the logo and the name and marks is trademark of Yealink (Xiamen) Network Technology CO., LTD, which are registered legally in China, the United States, EU (European Union) and other countries.

All other trademarks belong to their respective owners. Without Yealink's express written permission, recipient shall not reproduce or transmit any portion hereof in any form or by any means, with any purpose other than personal use.

Warranty

(1) **Warranty**

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS GUIDE ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS GUIDE ARE BELIEVED TO BE ACCURATE AND PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF PRODUCTS.

(2) **Disclaimer**

YEALINK (XIAMEN) NETWORK TECHNOLOGY CO., LTD. MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS GUIDE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Yealink (Xiamen) Network Technology CO., LTD. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance, or use of this guide.

(3) **Limitation of Liability**

Yealink and/or its respective suppliers are not responsible for the suitability of the information contained in this document for any reason. The information is provided "as is", and Yealink does not provide any warranty and is subject to change without notice. All risks other than risks caused by use of the information are borne by the recipient. In no event, even if Yealink has been suggested the occurrence of damages that are direct, consequential, incidental, special, punitive or whatsoever (Including but not limited to loss of business profit, business interruption or loss of business information), shall not be liable for these damages.

End User License Agreement

This End User License Agreement ("EULA") is a legal agreement between you and Yealink. By installing, copying or otherwise using the Products, you: (1) agree to be bounded by the terms of this EULA, (2) you are the owner or an authorized user of the device, and (3) you represent and warrant that you have the right, authority and capacity to enter into this agreement and to abide by all its terms and conditions, just as if you had signed it. The EULA for this product is available on the Yealink Support page for the product.

Patent Information

China, the United States, EU (European Union) and other countries are protecting one or more patents of accompanying products and/or patents being applied by Yealink.

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to *DocsFeedback@yealink.com*.

Technical Support

Visit Yealink WIKI (*http://support.yealink.com/*) for the latest firmware, guides, FAQ, Product documents, and more. For better service, we sincerely recommend you to use Yealink Ticketing system (*https://ticket.yealink.com*) to submit all your technical issues.

About This Guide

The VC400/VC120 video conferencing system represents a new generation of full high-definition video conferencing launched by Yealink. It features, in addition to a high-definition audio-visual experience, flexible compatibility, easy deployment and intelligent network adaptation. With high product standards, it is an ideal choice for SMEs. The VC400/VC120 video conferencing system allows branch offices, as well as branch and head offices, to communicate flexibly and cooperate efficiently.

The guide is intended for administrators who need to configure, customize, manage, and troubleshoot the video conferencing system properly, rather than for end-users. It provides details on the functionality and configuration of the Yealink video conferencing system.

Many of the features described in this guide involve network and account settings, which could affect the system's performance in the network. Therefore, an understanding of IP networking and a prior knowledge of VoIP telephony concepts are necessary.

See the *Yealink Products Regulatory Notices Guide* for all regulatory and safety guidance.

Documentations

This guide covers the VC400/VC120 video conferencing system. In addition to the administrator guide, the following related documentations are available:

- Quick Start Guide, which describes how to assemble the system and configure basic network features on the system.
- User Guides, which describe how to configure and use basic features available on the systems.
- Video Conference Room Deployment Solution, which describes the conference room layout requirements and how to deploy the systems.
- Network Deployment Solution, which describes how to deploy network for your systems.

You can download the above documentations from Yealink website:

http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage

For support or service, please contact your Yealink reseller or go to Yealink Technical Support online: *http://www.yealink.com/Support.aspx*.

Firmware

Common reasons for updating firmware include fixing bugs or adding features to the device. You can download the latest firmware for your product online:
http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage

For more information on how to upgrade the system firmware, refer to Upgrading System Firmware on page 269.

In This Guide

This administrator guide includes the following chapters:

- Chapter 1, "System Overview" describes system components, icons and Indicator LEDs.
- Chapter 2, "Getting Started" describes how to install and start up the system and configuration methods.
- Chapter 3, "Configuring Network" describes how to configure network features on the system.
- Chapter 4, "Configuring Call Preferences" describes how to configure call preferences on the system.
- Chapter 5, "Configuring System Settings" describes how to configure basic, audio and video features on the system.
- Chapter 6, "System Management" describes how to manage system contacts and call history.
- Chapter 7, "Configuring Security Features" describes how to configure security features on the system.
- Chapter 8, "System Maintenance" describes how to upgrade system firmware and reset the system.
- Chapter 9, "Troubleshooting" describes how to troubleshoot the system and provides some common troubleshooting solutions.

Typographic Conventions

Yealink documentations contain a few typographic conventions.

You need to know the following basic typographic conventions to distinguish types of in-text information:

Convention	Description
Bold	Highlights the web/phone user interface items such as menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (e.g., Click on **Setting** ->**General**). Also used to emphasize text
Blue Text	Used for cross references to other sections within this documentation (e.g., refer to Troubleshooting).

Convention	Description
Blue Text in Italics	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (e.g., For more information, refer to *Yealink VC400 Video Conferencing System User Guide*.

You also need to know the following writing conventions to distinguish conditional information:

Convention	Description
->	Indicates that you need to select an item from a menu. For example, **Settings**->**Basic Settings** indicates that you need to select **Basic Settings** from the **Settings** menu.

Terms

As you read this guide, you'll notice that the same terms are used repeatedly. Make sure you familiarize yourself with these terms.

Cloud platform: This term refers to Yealink VC Cloud Management Service (Yealink Cloud), Yealink Meeting Server, Zoom, BlueJeans, Pexip, Mind and Custom platform.

Cloud account: This term refers to Yealink Cloud, YMS, BlueJeans, Pexip, Mind and Custom account.

Cloud systems: This term refers to the systems that support Cloud feature, including SIP VP-T49G IP phone, VC desktop and VC110/VC120/VC400/VC500/VC800 video conferencing system.

Cloud contacts: This term refers to Yealink Cloud contacts and YMS contacts.

Summary of Changes

This section describes the changes to this guide for each release and guide version.

Changes for Release 23, Guide Version 23.20

The following section is new for this version:

- Virtual Remote Control on page 165
- Public Mode on page 162
- Hiding Menu Logo on page 178
- Multiple Preset on page 206

Major updates have occurred to the following sections:

- Configuring Video Conference Platform on page 99

- Appendix B: Trusted Certificates on page 298

Changes for Release 23, Guide Version 23.6

The following section is new for this version:

- Registering a YMS Account on page 104
- Logging out of the Cloud Platform on page 122
- Sharing Content on page 157
- Using the API with a LAN Connection on page 244
- Using the API with a Serial Connection on page 245

Major updates have occurred to the following sections:

- Intelligent Firewall Traversal on page 90
- Default Layout on page 161

Changes for Release 22, Guide Version 22.15

The following section is new for this version:

- Logging into the StarLeaf Cloud Platform on page 106

Major updates have occurred to the following sections:

- H.323 Tunneling on page 73
- Enabling H.460 Support for H.323 Calls on page 135
- Methods of Transmitting DTMF Digit on page 138
- Dual-Stream Protocol on page 196
- Camera Control Protocol on page 212
- H.235 on page 263

Changes for Release 22, Guide Version 22.5

The following sections are new for this version:

- Virtual Remote Control on page 165
- Auto Dialout Mute on page 152
- Meeting Blacklist on page 187
- USB Configuration on page 218
- Upgrading VCC20 Camera Firmware on page 270

Major updates have occurred to the following sections:

- Icon Instructions on page 25
- Configuring Video Conference Platformon page 99
- DTMF on page 137
- Dual-Stream Protocol on page 196
- Camera Control Protocol on page 212
- Secure Real-Time Transport Protocol on page 259

Changes for Release 21, Guide Version 21.20

The following sections are new for this version:

- Keyboard Input Method on page 188
- Configuring Video Conference Platform on page 99

Major updates have occurred to the following sections:

- Icon Instructions on page 25
- Setup Wizard on page 41
- Directory on page 227

Changes for Release 21, Guide Version 21.15

The following section is new for this edition:

- IPv6 Support on page 56
- Hiding Icons in a Call on page 179
- Output Resolution on page 217
- Video Recording on page 219
- Screenshot on page 221
- VCS Integrated with Control Systems on page 243

Major updates have occurred to the following sections:

- Packaging Contents on page 3
- System Component Instructions on page 10
- Configuring LAN Properties on page 48
- Search Source List in Dialing on page 239
- 8-Way MCU License on page 242

Changes for Release 20, Guide Version 20.6

The following sections are new for this version:

- Firmware on page v
- Physical Features on page 2
- VCM30 Video Conferencing Microphone Array on page 20
- Remote Control Battery Safety Information on page 39
- Static DNS on page 50
- STUN on page 84
- Rport on page 88
- DTMF on page 137
- Video Codecs on page 145
- Ringback Timeout on page 158
- Auto Refuse Timeout on page 159
- SIP IP Call by Proxy on page 159
- Meeting Password on page 184
- Meeting Whitelist on page 186
- License on page 241

Major updates have occurred to the following sections:

- Packaging Contents on page 3
- VCC18/VCC20 HD Camera on page 12
- VCR10 Remote Control on page 23
- LED Instructions on page 28
- System Installation on page 33
- VLAN on page 61
- Configuring the System for Use with a Firewall or NAT on page 77
- Enabling H.460 Support for H.323 Calls on page 135
- on page
- Audio Setting on page 189
- Dual-Stream Protocol on page 196
- Camera Control Protocol on page 212
- H.235 on page 263
- Capturing Packets on page 280

Table of Contents

About This Guide v

Documentations v
Firmware v
In This Guide vi
Typographic Conventions vi
Terms vii
Summary of Changes vii
Changes for Release 23, Guide Version 23.15 vii
Changes for Release 23, Guide Version 23.6 viii
Changes for Release 22, Guide Version 22.15 viii
Changes for Release 22, Guide Version 22.5 viii
Changes for Release 21, Guide Version 21.20 ix
Changes for Release 21, Guide Version 21.15 ix
Changes for Release 20, Guide Version 20.6 x

Table of Contents xi

System Overview 1

VoIP Principles 1
Physical Features 2
Packaging Contents 3
VC400 Packaging Contents 3
VC120 Packaging Contents 6
System Component Instructions 10
VC400/VC120 Codec 10
VCC18/VCC20 HD Camera 12
Video Conferencing Phone 14
CPE80 Expansion Microphone 19
VCM30 Video Conferencing Microphone Array 20
VCR10 Remote Control 23
Icon Instructions 25
Icons on Display Device 25
Icons on the Video Conferencing Phone 27
LED Instructions 28
User Interfaces 30
Web User Interface 30
Remote Control 31

Getting Started 33

System Installation 33
Installing the VC400 Video Conferencing System 34
Installing the VC120 Video Conferencing System 34
Installing the Camera 36
Installing Batteries in the Remote Control 38
Powering the System On and Off 39
System Initialization 39
System Startup 40
Setup Wizard 41
Enabling Communication with Other Systems 45
Placing a Test Call from VCS 46

Configuring Network 47

Preparing the Network 47
Configuring LAN Properties 48
DHCP 48
Configuring Network Settings Manually 52
IPv6 Support 56
Configuring Network Speed and Duplex Mode 60
VLAN 61
LLDP 62
Manual Configuration for VLAN 65
DHCP VLAN 67
802.1X Authentication 68
H.323 Tunneling 73
Configuring the System for Use with a Firewall or NAT 77
Call Setup and Media Ports 77
Restricting Reserved Ports 78
Network Address Translation 81
Intelligent Firewall Traversal 90
Quality of Service 91
VPN 94

Configuring Call Preferences 99

Configuring Video Conference Platform 99
Logging into the Yealink VC Cloud Management Service Platform 100
Registering a YMS Account 104
Logging into the StarLeaf Cloud Platform 106
Logging into the Zoom Cloud Platform 108
Registering a Pexip Account 111

Logging into the BlueJeans Cloud Platform 114
Logging into the Mind Platform 116
Registering a Custom Account 119
Logging out of the Cloud Platform 122
Configuring the Third-party Virtual Meeting Room 122
Configuring SIP Settings 126
SIP Account 126
SIP IP Call 128
Configuring H.323 Settings 130
Enabling H.460 Support for H.323 Calls 135
DTMF 137
Methods of Transmitting DTMF Digit 138
Codecs 143
Audio Codecs 143
Video Codecs 145
Call Protocol 146
Account Polling 148
Do Not Disturb 150
Auto Answer 151
Auto Dialout Mute 152
Call Match 153
History Record 154
Bandwidth 155
Sharing Content 157
Ringback Timeout 158
Auto Refuse Timeout 159
SIP IP Call by Proxy 159
Default Layout 161
Public Mode 162

Configuring System Settings 165

General Setting 165
Virtual Remote Control 165
Configuring Remote Control 166
Site Name 167
Backlight of the Video Conferencing Phone 168
Language 169
Date & Time 170
Automatic Sleep Time 176
Hiding IP Address 177
Hiding Menu Logo 178
Hiding Icons in a Call 179
Relog Offtime 183
Key Tone 183

Meeting Password 184
Meeting Whitelist 186
Meeting Blacklist 187
Keyboard Input Method 188
Audio Setting 189
Audio Output Device 189
Audio Input Device 191
Adjusting MTU of Video Packets 194
Dual-Stream Protocol 196
Mix Sending 200
Configuring Camera Settings 201
Multiple Preset 206
Far-end Camera Control 211
Camera Control Protocol 212
Output Resolution 217
USB Configuration 218
Video Recording 219
Screenshot 221
Tones 222

System Management 227

Directory 227
LDAP 232
Call History 237
Search Source List in Dialing 239
Dual Screen 239
Two-way Video Calls 240
Two-way Video Call with Presentation 240
Multi-way Video Calls 240
Multi-way Video Call with Presentation 241
License 241
Device Type License 241
8-Way MCU License 242
VCS Integrated with Control Systems 243
Using the API with a LAN Connection 244
Using the API with a Serial Connection 245

Configuring Security Features 247

User Mode 247
Administrator Password 248
Web Server Type 249
Transport Layer Security 251
Secure Real-Time Transport Protocol 259

H.235 263
Defending against Attacks 265
Abnormal Call Answering 265
Configuring Safe Mode Call 266

System Maintenance 269

Upgrading System Firmware 269
Upgrading VCC20 Camera Firmware 270
Importing/Exporting Configuration 270
Resetting to Factory 271
SNMP 273

Troubleshooting 277

Troubleshooting Methods 277
Viewing Log Files 277
Capturing Packets 280
Getting Information from Status Indicators 283
Analyzing Configuration Files 284
Viewing Call Statistics 284
Using Diagnostic Methods 284
Troubleshooting Solutions 286
General Issues 286
Camera Issues 288
Video & Audio Issues 289
Why does the far-site display black screen when local starts a presentation? 291
System Maintenance 292

Appendix 295

Appendix A: Time Zones 295
Appendix B: Trusted Certificates 298

Index 301

System Overview

This chapter contains the following information about VC400/VC120 video conferencing system:

- VoIP Principles
- Physical Features
- Packaging Contents
- System Component Instructions
- Icon Instructions
- LED Instructions
- User Interfaces

VoIP Principles

VoIP

VoIP (Voice over Internet Protocol) is a technology that uses the Internet Protocol instead of traditional Public Switch Telephone Network (PSTN) technology for voice communications.

It is a family of technologies, methodologies, communication protocols, and transmission techniques for the delivery of voice communications and multimedia sessions over IP networks. The H.323 and Session Initiation Protocol (SIP) are two popular VoIP protocols that are found in widespread implementation.

H.323

H.323 is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.

It is widely implemented by voice and video conference equipment manufacturers, is used within various Internet real-time applications, such as GnuGK and NetMeeting, and is widely deployed by service providers and enterprises for both voice and video services over IP networks.

SIP

SIP (Session Initiation Protocol) is the Internet Engineering Task Force's (IETF's) standard for multimedia conferencing over IP. It is an ASCII-based, application-layer control protocol (defined in RFC 3261) that can be used to establish, maintain, and terminate calls between two or more system. Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

Physical Features

Video conferencing systems are in the overall network topology, which are designed to interoperate with other compatible equipment, including application servers, media servers, Internet-working gateways, and other systems.

In order to operate systems in your network successfully, the systems must meet the following requirements:

- A working IP network is established.
- VoIP gateway is configured for SIP or H.323, and H.323 gatekeeper is configured for H.323. You can also deploy Cloud server for Cloud platform.
- The latest (or compatible) firmware of system is available.
- A call server is active and configured to receive and send SIP/H.323 messages.

The VC400 and the VC120 have same physical interfaces, camera parameters and video resolutions.

VC400/VC120 Codec Interface

- 2 x HDMI
- 1x DVI
- 1x VGA
- 1xVCS phone port(RJ-45)
- 1x10/100/1000M Ethernet
- 1 x Line-in (3.5mm)
- 1 x Line-out (3.5mm)
- 2 x USB2.0 port
- 1 x power port
- Others: 1 x power key, 1 x security lock slot, 1 x reset slot

Full-HD Camera

- 1920x1080 video resolution
- Up to 18x optical zoom PTZ camera
- Pan range: ±100°
- Tilt range: ±30°
- Beauty shot feature

Video Resolution

- Full-HD 1080P at 30fps (1920x1080), from 1Mbps
- 720P (1280x720), from 512Kbps
- W448P (768 x 448), WQVGA (400 x 240)
- 4CIF (704×576), CIF (352 x 288)

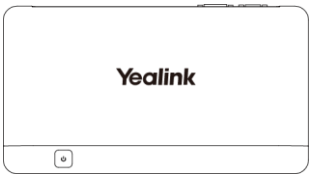
Packaging Contents

We recommend that you use the accessories provided or approved by Yealink. The use of unapproved third-party accessories may result in reduced performance

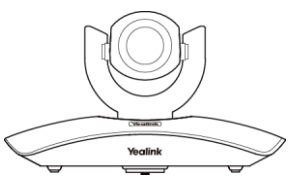
VC400 Packaging Contents

The following items are included in your package. If you find that anything is missing, contact your system administrator.

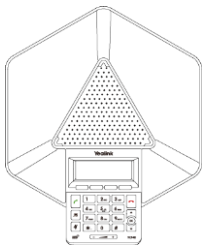
- **VC400 Codec**



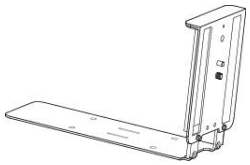
- **VCC18 HD Camera**



- **VCP40 Video Conferencing Phone**



- **L-Bracket** (for installing the camera)



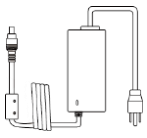
- **Camera Mounting Accessories**

Expansion bolts		× 4
Screws(Specificaiton: T4×30)		× 4
Screws(Specificaiton: M3×8)		× 2

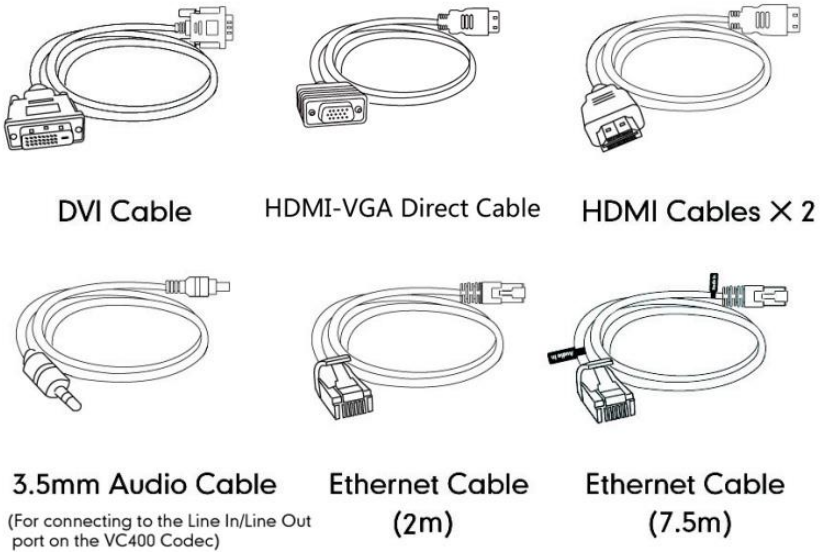
- **VCR10 Remote Control**

- **AAA Batteries×2**

- **Power Adapter**



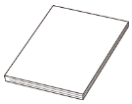
- **Cables**



- **Velcro×2**

- **Cable Ties×7**

- **Quick Start Guide**



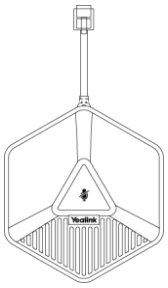
Check the list before installation. If you find that anything is missing, contact your system administrator.

Optional Accessory

The following item is optional for VC400 video conferencing system. You should purchase it separately if necessary.

The CPE80 expansion microphone is used for expanding the audio pickup range.

- **CPE80 Expansion Microphone**



VC120 Packaging Contents

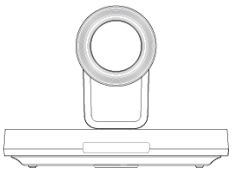
We provide the following packaging contents. You can purchase any combination according to your needs:

- VC120 Package
- VC120 Package+VCP40 Package
- VC120 Package+VCP41 Package
- VC120 Package+VCM30 Package

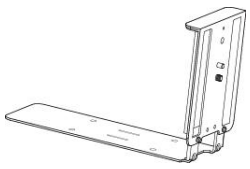
VC120 Package

- **VC120 Codec**

- **HD Camera**



- **L-Bracket** (for installing the camera)



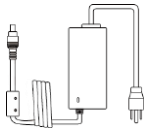
- **Camera Mounting Accessories**

Expansion bolts		× 4
Screws(Specificaiton: T4×30)		× 4
Screws(Specificaiton: M3×8)		× 2

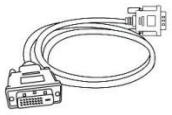
- **VCR10 Remote Control**

- **AAA Batteries×2**

- **Power Adapter**

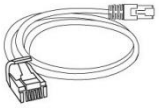


- **Cables**


DVI Cable

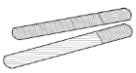
HDMI-VGA Direct Cable

HDMI Cable × 2

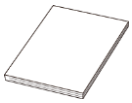

Ethernet Cable (2m)

- **Velcro×2**

- **Cable Ties×5**

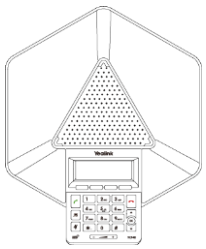


- **Quick Start Guide**

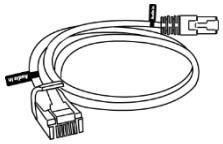


VCP40 Package

- **VCP40 Video Conferencing Phone**



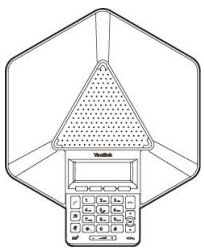
- **Ethernet Cable (7.5m)**



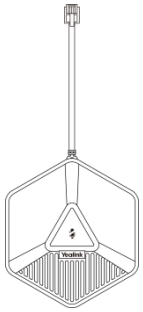
Locate the Audio In port on the VC120 Codec, and connect it to the Audio Out port of the VCP40 video conferencing phone with the 7.5m Ethernet cable.VCP40 video conferencing phone can work as an audio device for the VC120 video conferencing system. You can also place calls, answer calls or view directory and history on the VCP40 video conferencing phone.

VCP41 Package

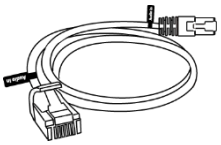
- **VCP41 Video Conferencing Phone**



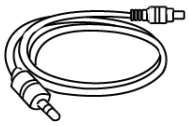
- **Expansion Microphone CPE80×2**



- **Ethernet Cable (7.5m)**



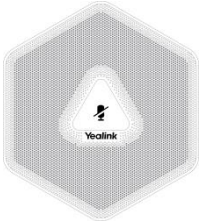
- **3.5mm Audio Cable** (for connecting a PC/Mobile device to the VCP41)



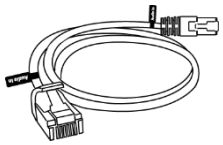
Locate the Audio In port on the VC120 Codec, and connect it to the Audio Out port of the VCP41 video conferencing phone with the 7.5m Ethernet cable. VCP41 Video conferencing phone can work as an audio device for the VC120 video conferencing system. You can also place calls, answer calls or view directory and history on the VCP41 video conferencing phone.

VCM30 Package

- **VCM30 Video Conferencing Microphone Array**



- **Ethernet Cable (7.5m)**



Locate the Audio In port of on the 120 Codec, and connect it to the Audio Out port of the VCM30 with the 7.5m Ethernet cable. VCM30 video conferencing microphone array can work as the audio input device for the VC120 video conferencing system. For more information, refer to Audio Input Device on page191.

Note Check the list before installation. If you find anything missing, contact your system administrator.

System Component Instructions

Before installing and using the VC400/VC120 video conferencing system, you need to be familiar with the following system components, including:

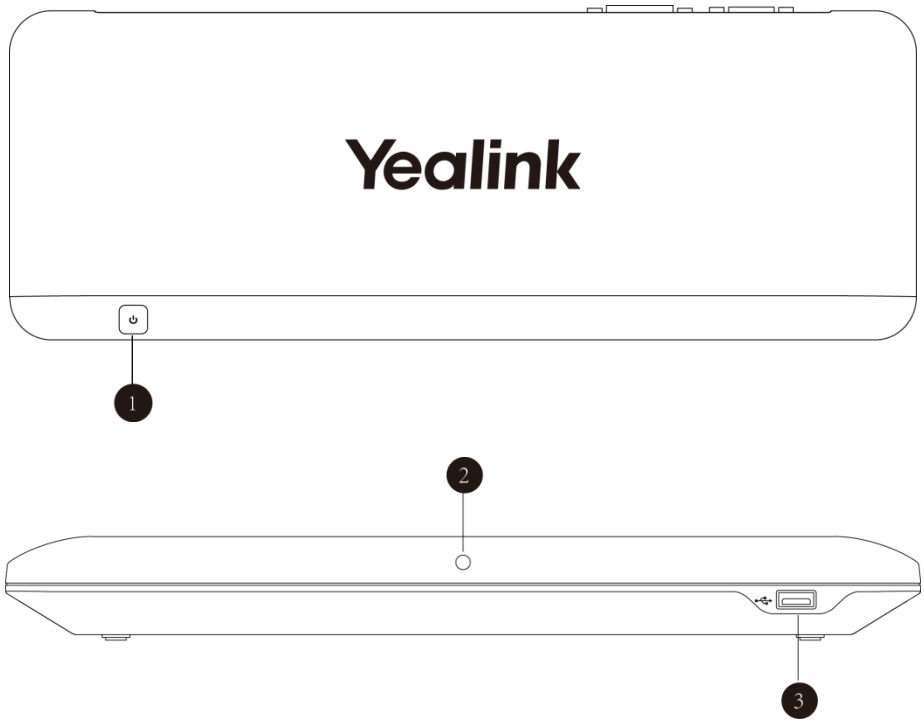
- VC400/VC120 Codec
- VCC18/VCC20 HD Camera
- Video Conferencing Phone
- CPE80 Expansion Microphone
- VCM30 Video Conferencing Microphone Array
- VCR10 Remote Control

VC400/VC120 Codec

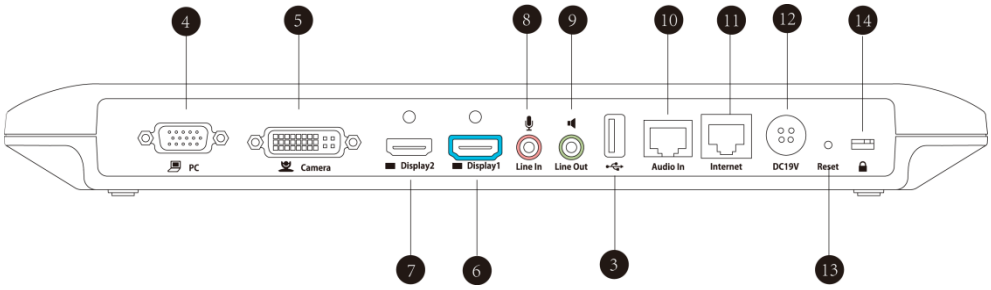
VC400/VC120 Codec supports 1080P full HD video. It supports both H. 323 and SIP protocols and can connect to a mainstream video conferencing system.

Strong audio/video processing ability, rich interfaces, compatibility with different display devices and adaptive resolution make it easy to use.

VC400/VC120 Codec front panel



VC400/VC120 Codec back panel



	Port Name	Description
①	Power Button	Powers the system on or off.
②	LED Indicator	Indicates the system statuses. For more information, refer to LED Instructions on page 28.
③	USB	Inserts a USB flash drive to one of the two USB ports for storing screenshots, recording videos or capturing packets. **Note**: If two USB flash drives are connected, only the latter one can be identified.
④	PC	Connects to a PC for sharing documents or videos during a call.
⑤	Camera	Connects to a camera. You can also connect two VCC20 cameras to the VC120 Codec using the VC Dual-camera Box VCB20.

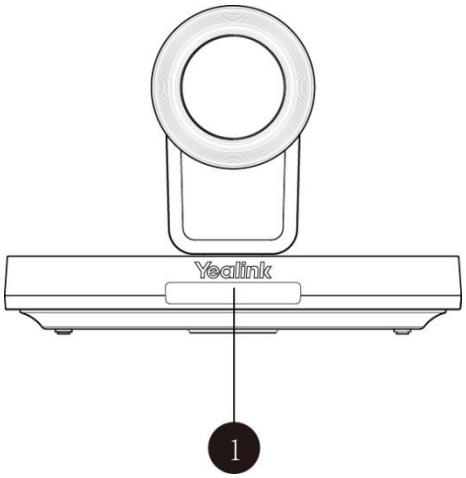
	Port Name	Description
⑥	Display1	Connects to a display device for displaying video images. When connecting only one display device, Display1 port on the VC400/VC120 Codec is the only available port.
⑦	Display2	Connects to secondary display device for displaying video images.
⑧	Line In	Connects to an audio input device using an audio cable (3.5mm).
⑨	Line Out	Connects to an audio output device using an audio cable (3.5mm).
⑩	Audio In	Connects to the video conferencing phone.
⑪	Internet	Connects to the network device.
⑫	DC19V	Connects to the power source via a power adapter.
⑬	Reset Key	Resets the system to factory defaults.
⑭	Security Slot	Allows you to connect a universal security cable to VC400/VC120 Codec, so you can lock it down. The system cannot be removed when it is locked.

VCC18/VCC20 HD Camera

The VCC18 HD camera supports 18x optical zoom, white balance and automatic gain. The VCC20 HD camera supports 12x optical zoom, white balance and automatic gain. Exceptionally clear images can bring you an immersive experience.

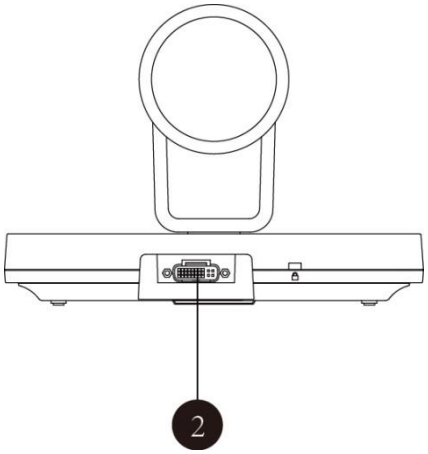
The following takes VCC20 HD camera as an example to introduce camera performance.

The front of the HD camera



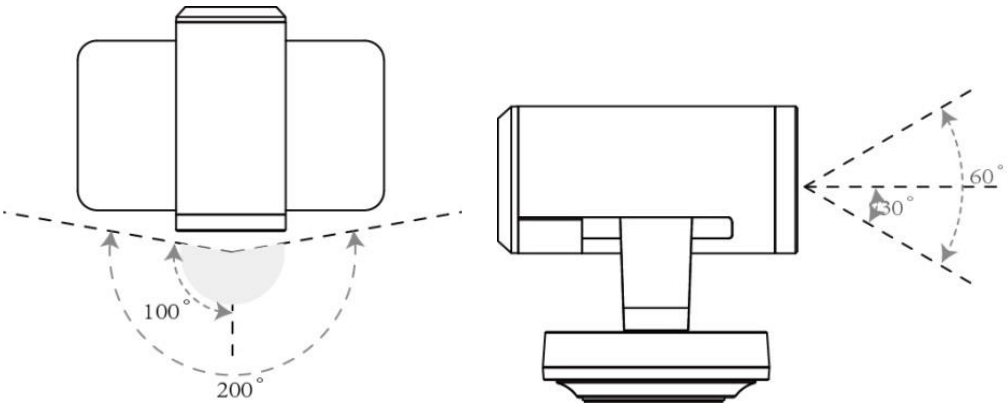
	Port Name	Description
①	LED Indicator	Indicates the system statuses. For more information, refer to LED Instructions on page 28.

The back of the HD camera



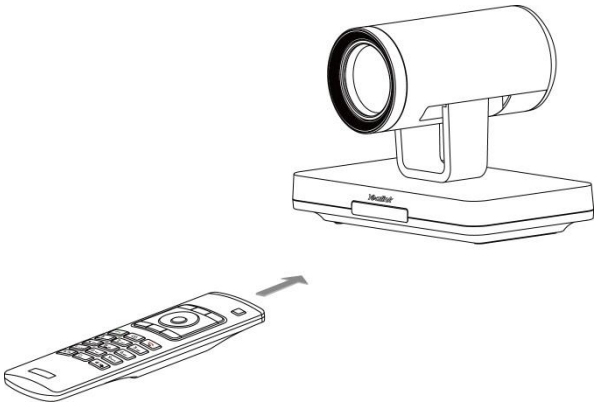
	Port Name	Description
②	Camera	Connects to the Camera port on the VC400/VC120 Codec using a DVI cable.

You can use the remote control to adjust the position or focus of the camera. The camera can be panned (± 100 degrees range), tilted (± 30 degrees range).



Infrared Sensor

The infrared sensor is located within the Yealink logo. Aim the remote control at the camera IR sensor to operate the unit.



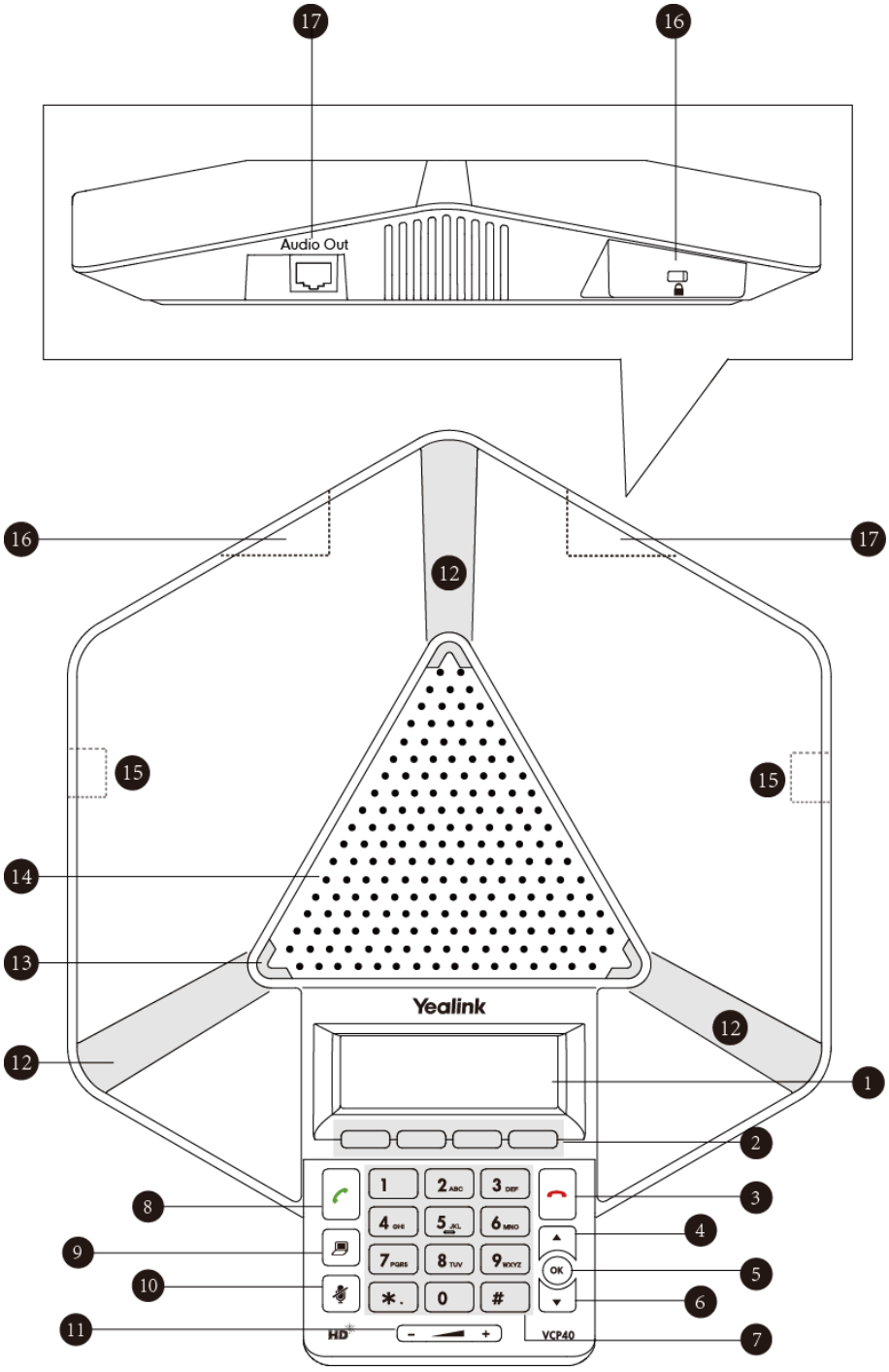
Note Avoid physically turn camera while system is powered on to prevent permanent damaging the camera. Always use the remote control to pan and tilt the camera head.

Video Conferencing Phone

VCP40 Video Conferencing Phone

The VCP40 video conferencing phone supports 360-degree audio pickup to achieve ultra-HD voice.

Connect the VCP40 phone to the VC400/VC120 Codec. It can work as an audio device for the system. You can also place calls, answer calls or view directory and history on the VCP40 phone.

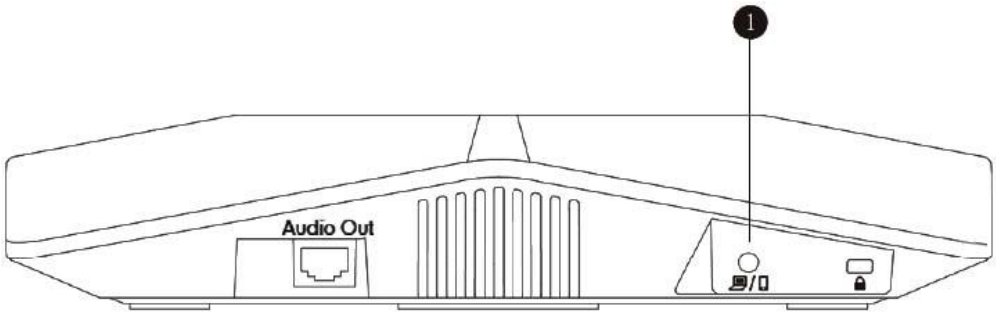


Component instructions of the VCP40 phone are:

	Item	Description
①	LCD Screen	Shows information about calls, messages, soft keys, time, date and other relevant data: • Call information−call duration • Icons (for example,) • Missed call information • Time and date
②	Soft Keys	Label automatically to identity their context-sensitive features.
③	On-hook Key	Rejects or ends a call or returns to the previous screen.
④		Scrolls upwards through the displayed information.
⑤	OK	Enters list or answers incoming calls.
⑥		Scrolls downwards through the displayed information.
⑦	Keypad	Generates the digits and special characters "." "*" "#".
⑧	Off-hook Key	Initiates a call or answers a call.
⑨	Presentation Key	Enables or disables presentation.
⑩	Mute Key	Toggles the mute feature.
⑪	Volume Key	Adjusts the volume of the speakerphone and ringer.
⑫	Microphone	Picks up voice.
⑬	LED Indicators	Indicate phone and call statuses.
⑭	Speakerphone	Provides ringer and hands-free (speakerphone) audio output.
⑮	MIC Port	Connects a CPE80 expansion microphone to one of two MIC ports.
⑯	Security Slot	Allows you to connect a universal security cable to lock down your phone. The phone cannot be removed when locked.
⑰	Audio Out Port	Connects to the video conferencing phone using the 7.5m Ethernet cable labeled Audio in. Provides the power supply for the video conferencing phone.

VCP41 Video Conferencing Phone

The features of VCP41 video conferencing phone are similar to VCP40. For more information, refer to VCP40 Video Conferencing Phone on page 14. The only difference is that the back of VCP41 has a PC/Mobile port, which allows you to connect an optional PC or Mobile Device to your phone, so that VCP41 can work as the audio input/output device of your PC or mobile device.



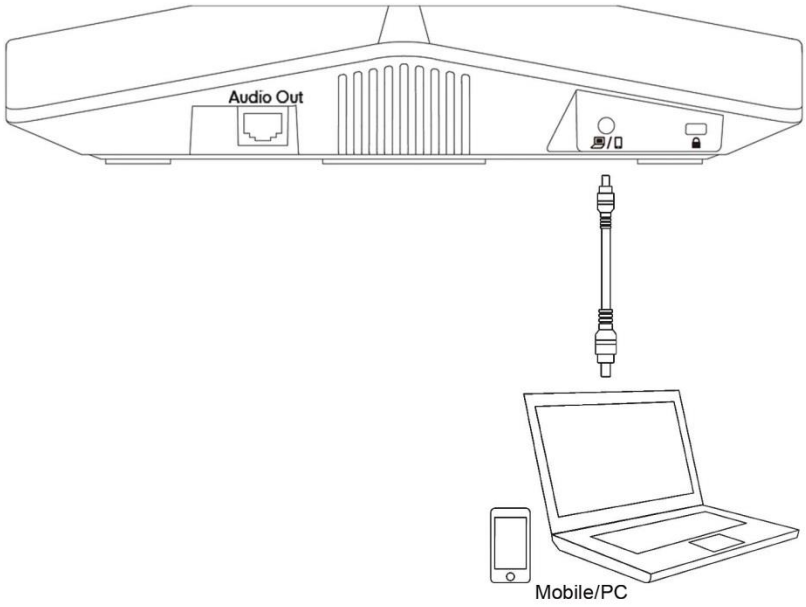
	Item	Description
①	PC/Mobile Port	Allows you to connect an optional PC or Mobile Device to your phone so that you can listen to the PC or mobile audio using your VCP41 video conferencing phone.

Connecting a PC or Mobile Device to the VCP41

You can connect a PC or mobile device to the VCP41 when your VC120 video conferencing system is idle, is placing a call or during a call.

To connect a PC or mobile device to your VCP41:

1. Connect one end of the 3.5mm audio cable to the PC/mobile port on the VCP41 phone, and connect the other end to the headset jack on the mobile device or the AUX/MIC jack on the PC.



The icon will appear on the display device, and the icon will appear on the video conferencing phone.

As a result, VCP41 will work as the audio input/output device of your PC or mobile device. For example, when the PC or mobile device is playing a video or music, you can listen to the audio on your VCP41. If your PC or mobile device receives an incoming call, you can use VCP41 to listen and speak.

Adjusting the Volume of the PC or Mobile Audio

When your PC or mobile device is during a call, you can adjust the output volume of the PC/mobile device via your VCP41.

To adjust the volume of the PC or mobile device:

1. When your PC or mobile device is during a call, press on the VCP41 to adjust the volume.

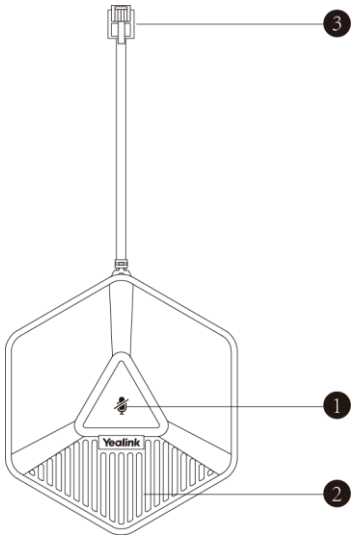
Removing the PC or Mobile Audio

To remove the PC or mobile device, disconnect the 3.5mm audio cable from the VCP41.

CPE80 Expansion Microphone

If your video conferencing room is large, you can add extra CPE80 expansion microphones to the MIC ports on the video conferencing phone to expand the audio range.

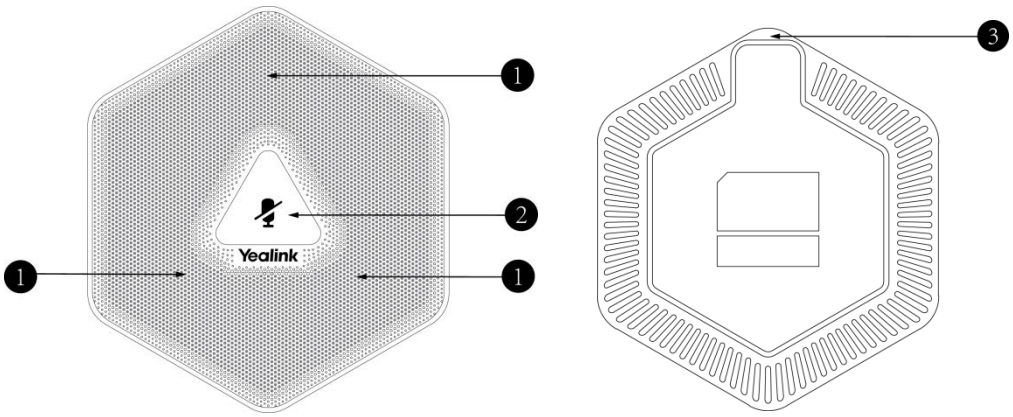
Video conferencing phone has two MIC ports. Up to two expansion microphones can be connected to a video conferencing phone. CPE80 is a directional microphone. Its coverage range is a 120 degree. Always ensure that the speaker faces the expansion microphone.



	Item	Description
①	Mute Indicator LED	Toggles and indicates mute feature.
②	Microphone	Transmits sound to other phones.
③	MIC Connector	Allows you to connect to the MIC port on the video conferencing phone.

VCM30 Video Conferencing Microphone Array

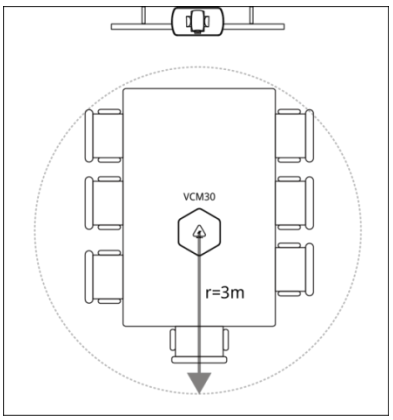
The VCM30 is a video conferencing microphone array which can work as the audio input device for VC120 video conferencing system. It has 3 built-in microphones which support 360-degree audio pickup at a radius of up to 3 meters. There is a mute button on its top. You can mute or unmute the VCM30 by tapping the mute button during a call.



	Name	Description
①	Built-in Microphones	Support 360-degree audio pickup at a radius of up to 3 meters.
②	Mute Button	Mutes or unmutes the VCM30. For more information on the mute indicator LED, refer to Icon Instructions on page 25.
③	Audio Out Port	Connects to the Audio In port of VC120 Codec using the 7.5m Ethernet cable labeled Audio In. Provides the power supply for the VCM30.

Placing the VCM30

The VCM30 has a rubber pads on its base to prevent it from sliding. You can place the VCM30 on a stable surface and keep it away from obstacles so that it can effectively pick up sounds.



Muting or Unmuting the VCM30

There is a mute button at the top of the VCM30. You can mute or unmute it in the following scenarios:

- If you do not want to have your voice broadcast during a call, you can tap the mute button to mute the VCM30.
- If you want to speak again during a call, you can tap mute button to unmute the VCM30.

To mute the VCM30 during a call:

1. Tap to mute the call.

   The mute indicator LED illuminates solid red. And the mute icon appears on the local video image.

To unmute the VCM30 during a call:

1. Tap again to unmute the call.

   The mute indicator LED illuminates solid green. And the mute icon disappears from the local video image.

Viewing VCM30 Information

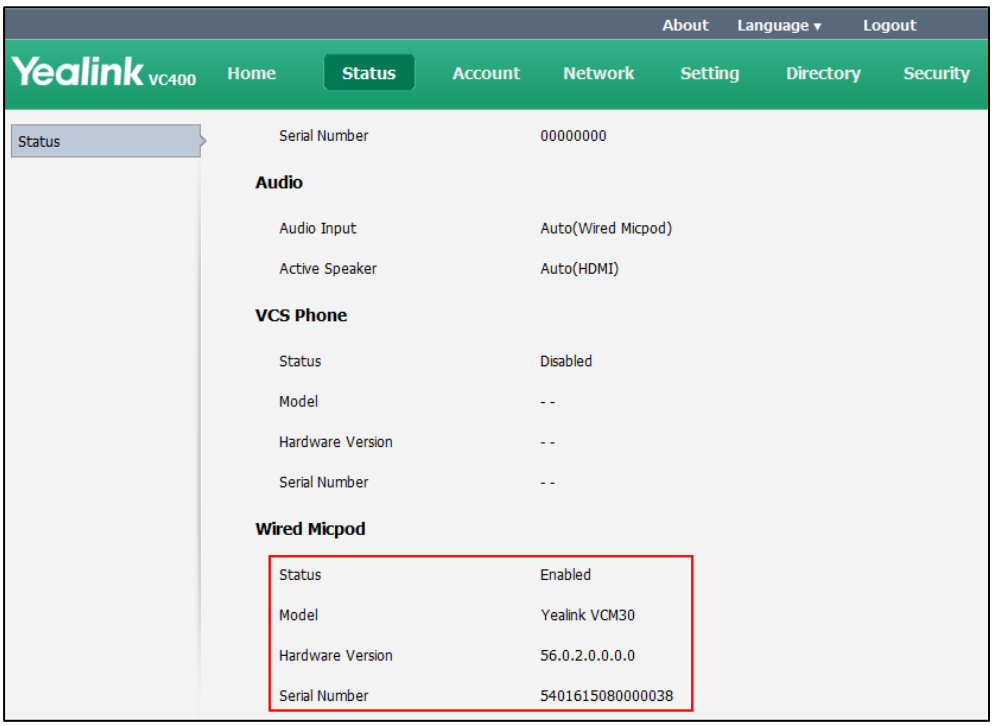
When the VCM30 is connected to the Audio In port of VC120 Codec, you can view VCM30 status via the remote control or web user interface.

Available information of VCM30 includes:

- Status
- Model
- Hardware Version
- Serial Number

To view the VCM30 information via web user interface

1. Click **Status**.

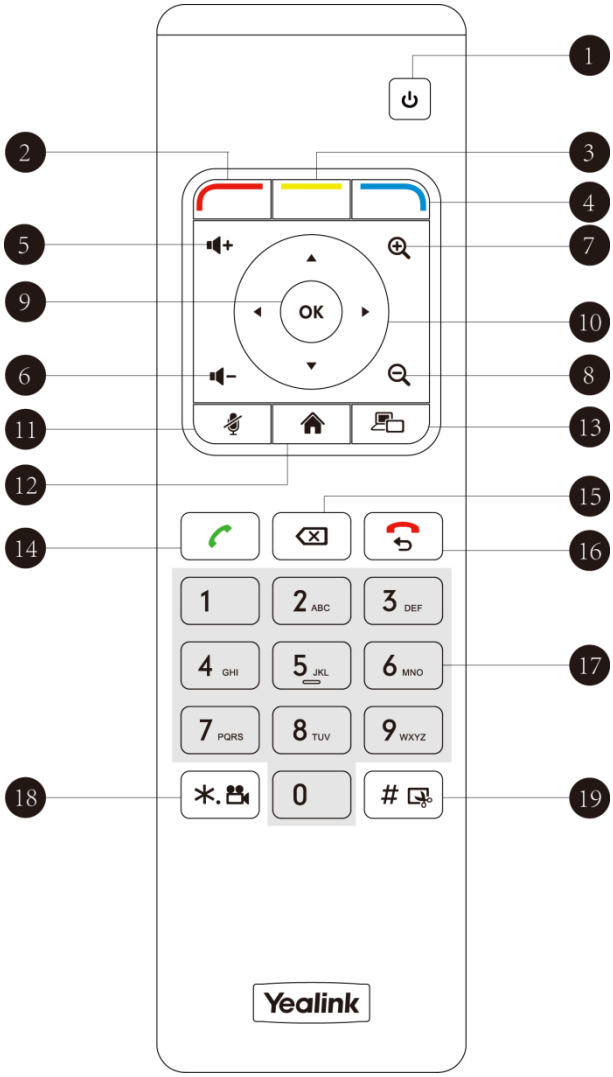


To view the VCM30 information via the remote control:

1. Select **Menu**->**Status->Wired Micpod.**

VCR10 Remote Control

VCR10 remote control is compact, and has definite function zoning. Users can organize conferences easily using infrared signals.



Hardware components of the remote control:

	Item	Description
①	Sleep Key	Puts the system to sleep or wakes the system up.
②	Red Shortcut Key	Located at the bottom left of the screen. Label automatically identifies context-sensitive features. In the idle screen, this is used to enter the main menu screen and corresponds to the Menu soft key.
③	Yellow Shortcut Key	Located at the bottom center of the screen. Label automatically identifies context-sensitive features. In the idle screen, this is used to enter the pre-dialing screen, and corresponds to the Call soft key.

	Item	Description
④	Blue Shortcut Key	Located at the bottom right of the screen. Label automatically identifies context-sensitive features. In the idle screen, this is used to save and check the camera preset position, and corresponds to the Preset soft key.
⑤	Vol+	Increases the system volume.
⑥	Vol-	Decreases the system volume.
⑦	Zoom in Key	• Increases the camera zoom or the captured image magnifications. • Behaves as page up in a multiple page list.
⑧	Zoom out Key	• Decreases the camera zoom or the captured image magnifications. • Behaves as page down in a multiple page list.
⑨	OK Key	Confirms actions or answers incoming calls.
⑩	Navigation Key	• In the menu screen, press ◀ or ▶ to switch menus, press ▲ or ▼ to select items. • In the idle screen, pan and tilt the camera to adjust the viewing angle.
⑪	Mute Key	Toggles the mute feature.
⑫	Home Key	• Returns to the idle screen when in the menu screen. • Enters the pre-dialing screen during a call.
⑬	Video Source Key	Switches the input source between Camera, Camera-PC, or PC.
⑭	Off-hook Key	• Enters the pre-dialing screen. • Places a call. • Answers a call.
⑮	Delete key	• Deletes one character at a time. • Long press to delete all characters in the input field. • On the idle screen or during a call, long press it for 2 seconds to start capturing packets and long press it for 2 seconds again to stop capturing packets.
⑯	On-hook Key	• Ends a call or exits from a conference call. • Returns to the previous screen when not in a call.

	Item	Description
⑰	Keypad	• Enters digits. • Long press 0 to generate a special character "@" in the input field. • Enters the pre-dialing screen. • Stores the preset position of the camera.
⑱	Video Recording Key	• Generates a special characters ".". • On the idle screen, press *. to start/stop recording video. • During a call, long press *. to start/stop recording video.
⑲	Snapshot Key	• Generates a pound key (#). • Captures the image from the camera. • On the idle screen, press # to capture the image from the camera. • During a call, long press # to capture the image from the camera.

Icon Instructions

Icons on Display Device

Icons appearing on the display device are described in the following table:

Icon	Description
(flashing)	Network is disconnected
	Network is available
	Packet loss
(flashing)	VCP40 video conferencing phone is not connected
(flashing)	Camera is not connected
SIP	SIP account is registered

Icon	Description
	H.323 account is registered
	Log into the Yealink VC Cloud Management Service/Yealink Meeting Server
	Log into the StarLeaf/Zoom/Pexip/BlueJeans/ Mind platform
	Auto answer
	Missed calls (this icon displays on the status bar)
	Volume is 0
	Do not disturb
	Do not disturb during a call
	Dual screen mode
	Dual video sources (when a PC is connected to the PC port on the VC400/VC120 Codec)
	A USB flash drive is inserted to the USB port on the VC400/VC120 Codec
	VPN is enabled
	Call mute
	Call encryption
	Call Hold
	Output volume is 0 during a call
	Camera that being controlled
	Indicates the content displayed on the second display device
	Camera position
	Record a video
	Dialed calls (H.323 account/SIP account/IP Call)

Icon	Description
	Dialed calls (Cloud platform)
	Received calls (H.323 account/SIP account/IP Call)
	Received calls (Cloud platform)
	Missed calls (H.323 account/SIP account/IP Call)
	Missed calls (Cloud platform)
	Local contact
	Conference contact
	Yealink Cloud contact or YMS contact
	Permanent Virtual Meeting Room

Icons on the Video Conferencing Phone

Icons appearing on the video conferencing phone LCD screen are described in the following table:

Icon	Description
(Flashing)	Network is unavailable
	SIP account is registered (the icon flashes when it is not registered successfully)
	H.323 account is registered (the icon flashes when it is not registered successfully)
	Log into the Yealink VC Cloud Management Service/Yealink Meeting Server
	Log into the StarLeaf/Zoom/Pexip/BlueJeans/ Mind platform
	Auto answer
	Do not disturb
	Call is muted

Icon	Description
	Volume is 0
	A USB flash drive is inserted to the port on the VC400 Codec
	Record a video
	Local contact
	Conference contact
	Yealink Cloud contact or YMS contact
V	Permanent Virtual Meeting Room
	Conference call
	Dialed calls (H.323 account/SIP account/IP Call)
	Dialed calls (Cloud platform)
	Received calls (H.323 account/SIP account/IP Call)
	Received calls (Cloud platform)
	Missed calls (H.323 account/SIP account/IP Call)
	Missed calls (Cloud platform)
	PC/Mobile mode (when a PC or mobile device is connected to the VCP41)

LED Instructions

Indicator LED on the VC400/VC120 Codec:

LED Status	Description
Solid green	The VC400/VC120 Codec is powered on. The VC400/VC120 Codec is upgrading firmware.
Solid red	The VC400/VC120 Codec is in sleep mode.
Solid orange	System exception (e.g., network unavailable, update failure).
Off	The VC400/VC120 Codec is powered off, is not connected to the power adapter.

Indicator LED on the camera:

LED Status	Description
Solid green	The camera is properly connected to the VC400/VC120 Codec, and the VC400/VC120 Codec is powered on.
Solid red	The VC400/VC120 Codec is in sleep mode.
Flashing green	Press the key on the remote control.
Off	The camera is not connected properly to the VC400/VC120 Codec, or the VC400/VC120 Codec is powered off.

Indicator LED on the video conferencing phone:

LED Status	Description
Solid red	The phone is initializing. The video conferencing phone is muted when the VC400 is during a call.
Flashing red	The phone is ringing.
Solid green	The phone is placing a call. There is an active call on the phone.
Off	The phone is idle. The phone is not connected to the VC400/VC120 Codec correctly.

Indicator LED of the Internet port on the VC400/VC120 Codec:

LED Status	Description
Indicator LED on the left is off.	Network is not connected.
Indicator LED on the left is solid green.	Network is connected.
Indicator LED on the right is flashing yellow.	Sending and receiving data.

Mute Indicator LED on the VCM30 video conferencing microphone array:

LED Status	Description
Solid red	The VCM30 is muted when the VC120 is during a call.
Flashing red	The VC120 is ringing.
Solid green	The VCM30 is connected to the VC120 Codec within the first 5 seconds. The VC120 is placing a call. The VCM30 is unmuted when the VC120 is during a call.
Off	The VCM30 is not connected to the VC120 Codec. The VCM30 is idle.

User Interfaces

Three are two ways to customize the configurations of your system:

- Web User Interface
- Remote Control

The following describes how to configure the VC400/VC120 video conferencing system via the two methods above.

Detailed operation steps will be introduced in the feature section.

Web User Interface

You can customize your system via web user interface. To access the web user interface, you need to know the user name and the administrator's password. The default user name is "admin" (case-sensitive), and the default password is "0000". You can also access the web user interface with user credential, which is disabled by default. For more information on how to enable the user credential, refer to User Mode on page 247.

The system uses the HTTPS protocol to access the web user interface by default. For more information on the access protocol for web user interface access, refer to Web Server Type on page 249.

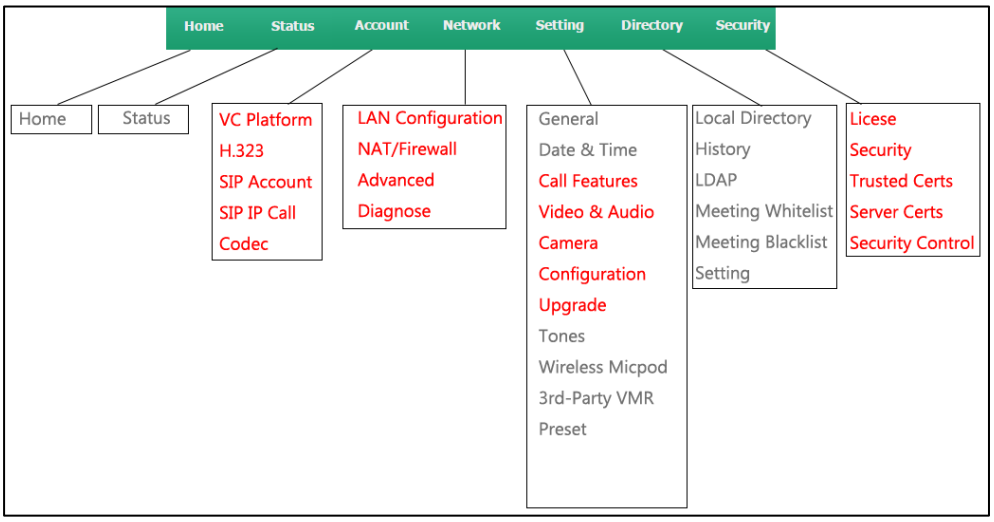
Log into the web user interface of the system:

1. Enter the IP address (e.g.,192.168.0.10) in the address bar of a web browser on your computer, and then press the **Enter** key.
2. Enter the administrator user name and password.
3. Click **Login**.

   After you log into the web user interface successfully, you can click **Logout** on the top right corner of the web interface to log out.

Administrator has full permission to access every menu in the web user interface. User can log into the web user interface with user credentials.

The web structure tree of VC400 is shown as below, (the red highlight is hidden for users with user credentials):



You can monitor or place calls via web user interface. You can do the following in the **Home** page.

- Placing or ending calls
- Viewing remote and nearby sites
- Enabling the mute mode or the DND mode for a call
- Changing the video input source
- Adjusting the position and focus of the camera
- Saving the camera preset
- Capturing the video images
- Control the video conferencing system remotely via the virtual remote control

Note Although the web user interface is used to initiate the call, it is the video conferencing system that is used for the call. It is not the PC running the web user interface.

Remote Control

You can use the remote control and display device to configure and use the VC400&VC120 video conferencing system.

For more information on the function of each key on the remote control, refer to VCR10 Remote Control on page 23. The **Advanced** option is only accessible to the user with the administrator's permission. The default administrator password is "0000".

You can also use virtual remote control on the web user interface to configure the VC400&VC120 video conferencing system. For more information, refer to Virtual Remote Control on page 165.

Getting Started

This chapter provides basic information and installation instructions for Yealink VCS systems in the following sections:

- System Installation
- Powering the System On and Off
- System Initialization
- System Startup
- Setup Wizard
- Enabling Communication with Other Systems
- Placing a Test Call from VCS

System Installation

Placing the System

Do not place the camera facing a window or other bright light. Ensure sufficient space to connect the cables. Ensure all participants are facing both the display device and the camera at the same time by putting camera and display device together.

System Components Installation

This section introduces the following:

- Installing the VC400 video conferencing system
- Installing the VC120 video conferencing system
- Installing the camera
- Installing batteries in the remote control

Note

Up to two display devices can be connected to the VC400/VC120 Codec. Because the display device is not included in the package, you need to purchase it separately if required. Ensure that the purchased display device supports HDMI input.

When connecting just one display device to the VC400/VC120 Codec, Display1 port is the only available port. If dual screen mode is required, you can connect secondary display device to the Display2 port.

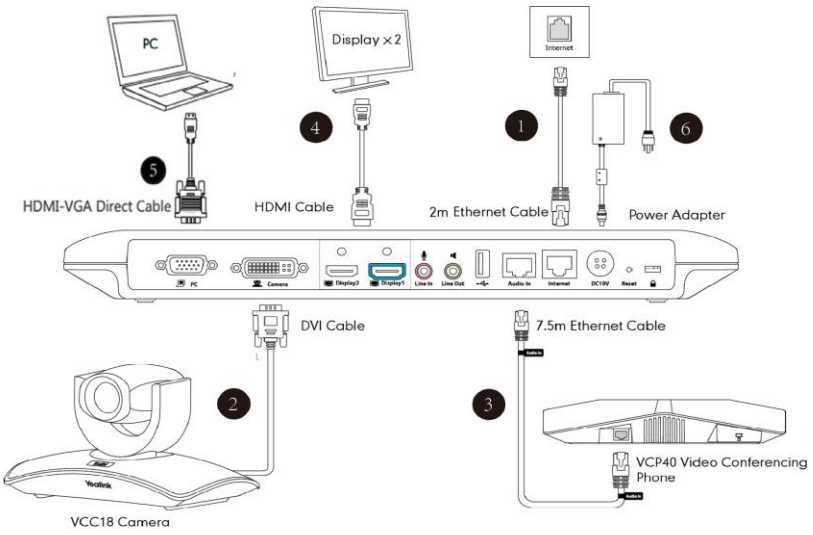
Because the DVI cable is tailor-made, please use the Yealink-supplied DVI cable.

To prevent shock damage, do not connect the power adapter and turn on the power before connecting all system components.

Installing the VC400 Video Conferencing System

Do the following:

1. Connect the **Internet** port on the VC400 Codec to a switch/hub device port with the supplied 2m Ethernet cable.
2. Locate the **Camera** port on the back of the VC400 Codec, and connect it to the **Camera** port of the camera with the supplied DVI cable.
3. Connect the **Audio In** port on the VC400 Codec to the **Audio Out** port on VCP40 video conferencing phone with the 7.5m Ethernet cable labeled Audio in.
4. Locate the **Display1** port on the VC400 Codec, and connect it to the HDMI port on the display device with the supplied HDMI cable (Make sure the display device is powered on)
5. (Optional.) Locate the **PC** port of the VC400 Codec and connect it to the **HDMI** port on the PC with the supplied HDMI-VGA direct cable for sharing content.
6. Connect the **DC19V** port on the VC400 Codec to an AC power outlet with the supplied power adapter and power cord.



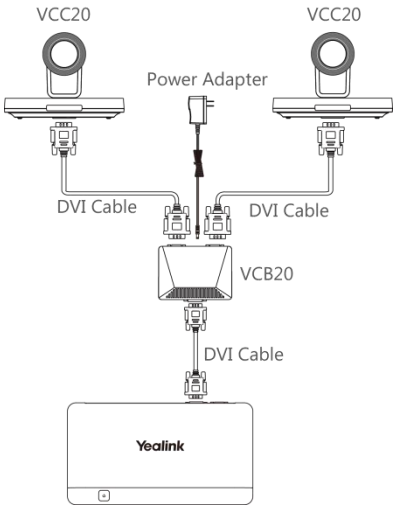
Note The VC400 video conferencing system should be used with Yealink original power adapter (19V/3.42A) only. The use of the third-party power adapter may cause the damage to the system.

Installing the VC120 Video Conferencing System

Do the following:

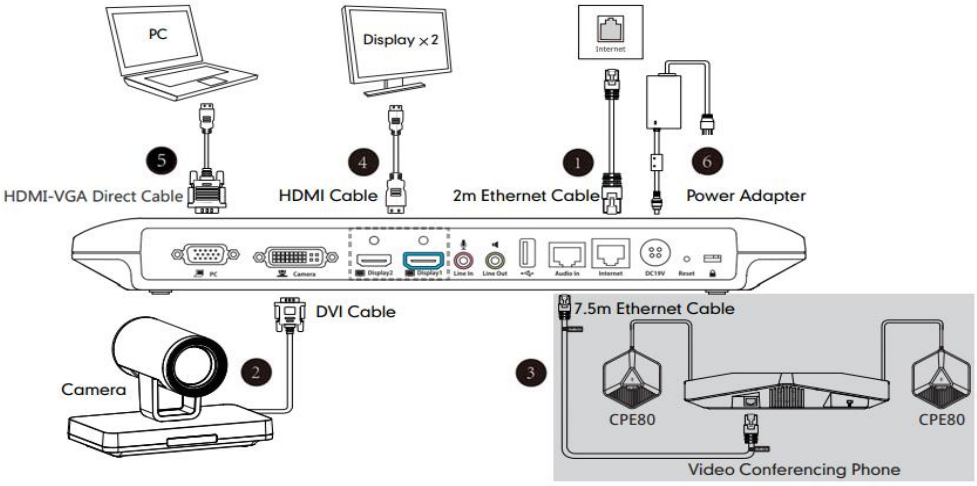
1. Connect the **Internet** port of the VC120 Codec to a switch/hub device port with the supplied 2m Ethernet cable.
2. Locate the **Camera** port on the back of the VC120 Codec, and connect it to the **Camera** port on the camera with the supplied DVI cable.

3. (Optional) If you purchase VC Dual-camera Box VCB20 separately, you can connect two VCC20 cameras to the VC120 Codec.

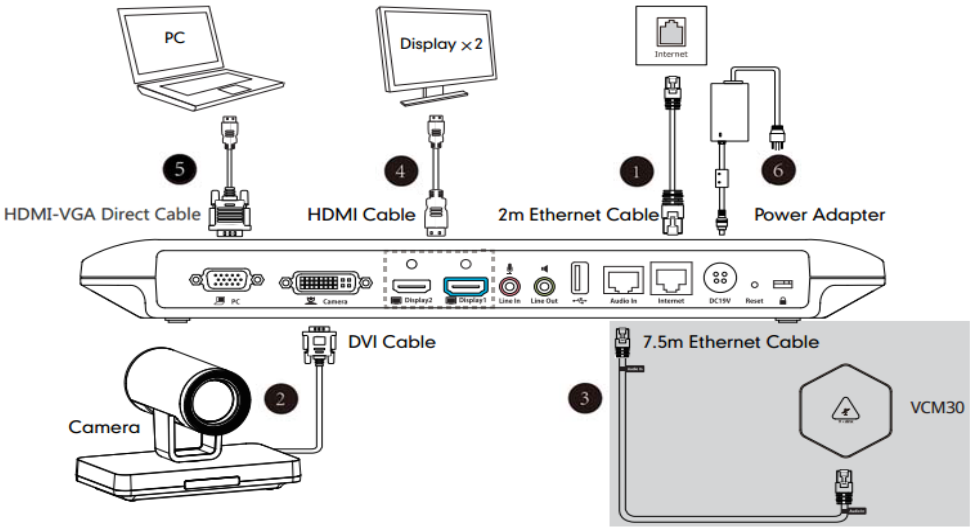


4. (Optional) Locate the **Audio In** port of the VC120 Codec, do one of the following:

- Connect it to the **Audio Out** port on the video conferencing phone with the 7.5m Ethernet cable that labeled Audio In, and then connect the free end of the expansion microphone cables to **MIC** ports on the video conferencing phone.



- Connect it to the **Audio Out** port on the VCM30 video conferencing microphone array with the 7.5m Ethernet cable that labeled Audio In.



5. Locate the **Display1** port on the VC120 Codec, and connect it to the **HDMI** port on the display device with the supplied HDMI cable (Make sure the display device is powered on)
6. (Optional.) Locate the **PC** port of the VC120 Codec and connect it to the **HDMI** port on the PC with the supplied HDMI-VGA direct cable for sharing content.
7. Connect the **DC19V** port on the VC120 Codec to an AC power outlet with the supplied power adapter and power cord.

Note The VC120 video conferencing system should be used with Yealink original power adapter (19V/3.42A) only. The use of the third-party power adapter may cause the damage to the system.

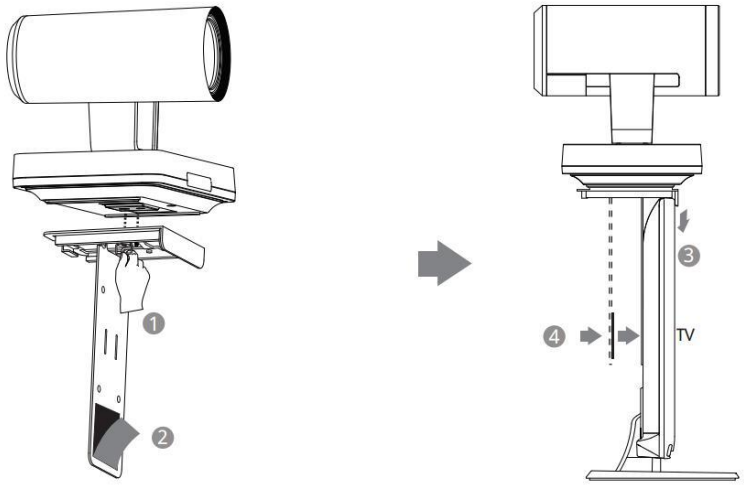
You can fasten all cables with cable ties after all devices are connected.

Installing the Camera

You can choose to mount the camera on your TV or a wall, depending on your actual needs.

a) Mounting the camera on a TV

When the thickness of your TV is between 35-120 mm, you can mount the camera on your TV.



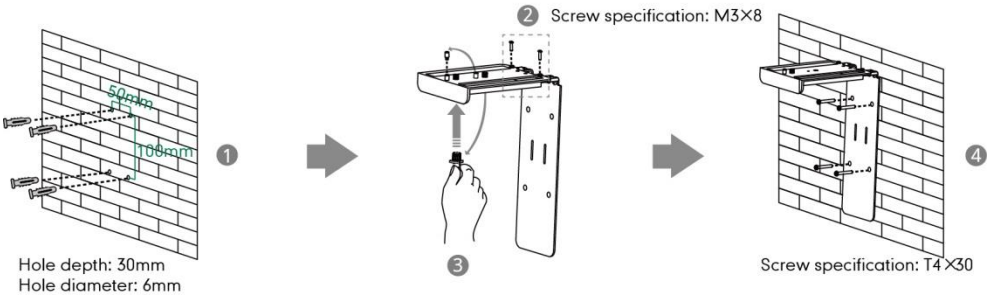
Do the following:

1. Lock the camera to the L-bracket.
2. Remove the protection of the Velcro.
3. Put the L-bracket on the top of the TV.
4. Make sure the back of the TV is clean, and then adjust the bracket to ensure close adhesion to the back of the TV with Velcro.

b) Mounting the camera on a wall

You can also decide to mount the camera on a wall. The recommended height for camera positioning is 1.5m-1.8m above the ground.

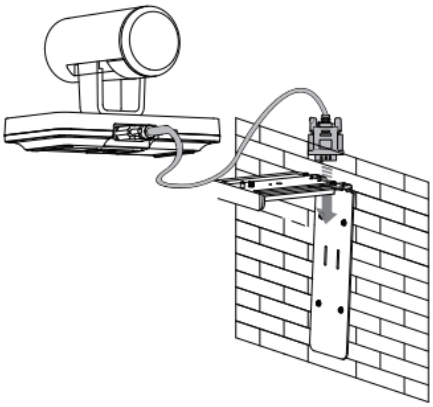
Do the following:



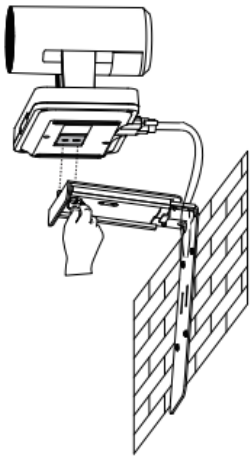
1. Punch holes into the wall and then insert the expansion bolts.

   Installation location for the expansion bolts and punching requirement are shown above.
2. Lock the L-bracket with the M3×8 screws.
3. Move the setscrews on the L-bracket to the left holes.
4. Lock the L-bracket to the wall with T4×30 screws.
5. Connect one end of the DVI cable to the camera and put the other end of the cable

through the L-bracket.



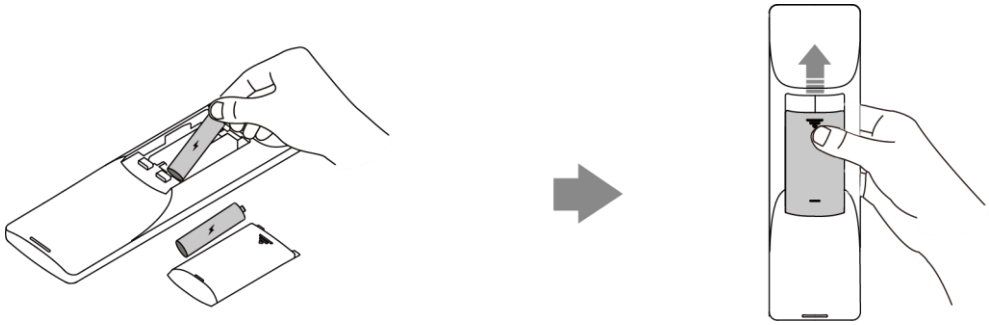
6. Lock the camera to the L-bracket, and then connect the other end of the DVI cable to the VC120 Codec.



Installing Batteries in the Remote Control

Do the following:

1. Open the battery cover on the back of the remote control.
2. Insert the batteries with the correct polarity.
3. Replace the battery cover.



Remote Control Battery Safety Information

- Never make wrong polarity connection when charging and discharging battery packs.
- Avoid crushing, puncturing, or putting a high degree of pressure on any battery, as this can cause an internal short-circuit, resulting in overheating.
- Remove the batteries if they are not in use for long period of time. Battery leakage and corrosion can damage the remote control, dispose batteries safely.
- Do not dispose used batteries in domestic waste. Dispose batteries at special collection points or return to stores if applies.
- Do not dispose batteries in a fire.

Powering the System On and Off

Note

Caution! To avoid corrupting the system, you should always power off the system using the power button on the VC400/VC120 Codec. After turning the power off in this way, wait at least 15 seconds before you unplug the power adapter from the VC400/VC120 Codec. This helps to ensure that the system powers off correctly.

To power on the system:

After all components are connected, press ⏻ on the VC400/VC120 Codec. The indicator LED on the VC400/VC120 Codec then illuminates solid green.

To power off the system:

Do one of the following:

- Long press ⏻ on the VC400/VC120 Codec.
- Short press ⏻ on the VC400/VC120 Codec, the display device will prompt "Press the power button to turn off the system. Press any button on remote control to cancel". Press ⏻ again to power off the system or press any button on the remote control to cancel.

System Initialization

Once you have power on the system, it will begin its initialization process.

During the initialization process, the following events take place:

Loading the ROM file

The ROM file sits in the flash memory of the system. Systems come from the factory with a ROM file preloaded. During initialization, systems run a bootstrap loader that loads and executes the ROM file.

Configuring the VLAN

If the system is connected to a switch, the switch will notify the system about the VLAN information defined on the switch.

Querying the DHCP (Dynamic Host Configuration Protocol) Server

The system is capable of querying a DHCP server. DHCP is enabled on the system by default. The following network settings can be obtained from the DHCP server during initialization:

- IP Address
- Subnet Mask
- Gateway
- Primary DNS (Domain Name Server)
- Secondary DNS

You need to configure the network settings of the system manually if any of them are not provided by the DHCP server. For more information on configuring network settings manually, refer to Configuring Network Settings Manually on page 52.

System Startup

After the initializing process, the system will complete startup by cycling the following steps:

1. The LED indicator on the VC400/VC120 Codec illuminates solid green.
2. The LED indicator on the camera illuminates solid green.
3. The display device displays the boot up screen.
4. The camera pans to the middle position automatically.
5. The display device displays the setup wizard (when you first start up or reset the system, the display device will display the setup wizard)

   For more information on how to complete the setup wizard, refer to Setup Wizard on page 41.
6. After completing the setup wizard, the display device displays the main screen.

   The main screen displays the following:

   - Time and date
   - System IP address and site name
   - Status icon
   - Soft key labels
   - Video image
7. The video conferencing phone starts up normally. The phone's LCD screen displays the site name, status icon, soft keys, time and date.

If the system has successfully passed through these steps, it starts up correctly and is ready for

use.

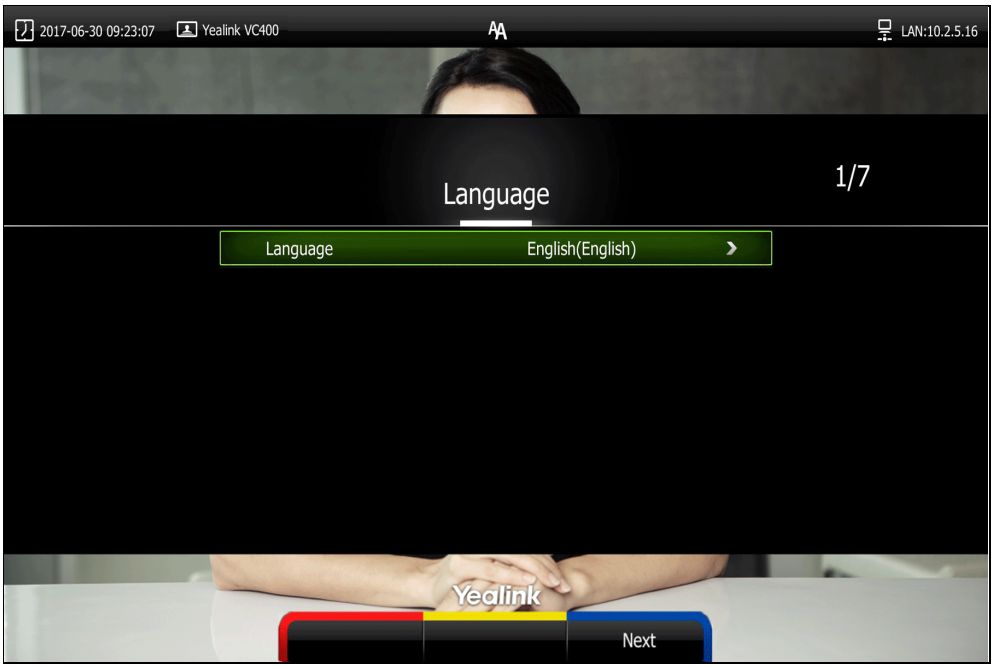
Setup Wizard

When you first start up or reset the system, the display device will display the setup wizard.

To complete the setup wizard via the remote control:

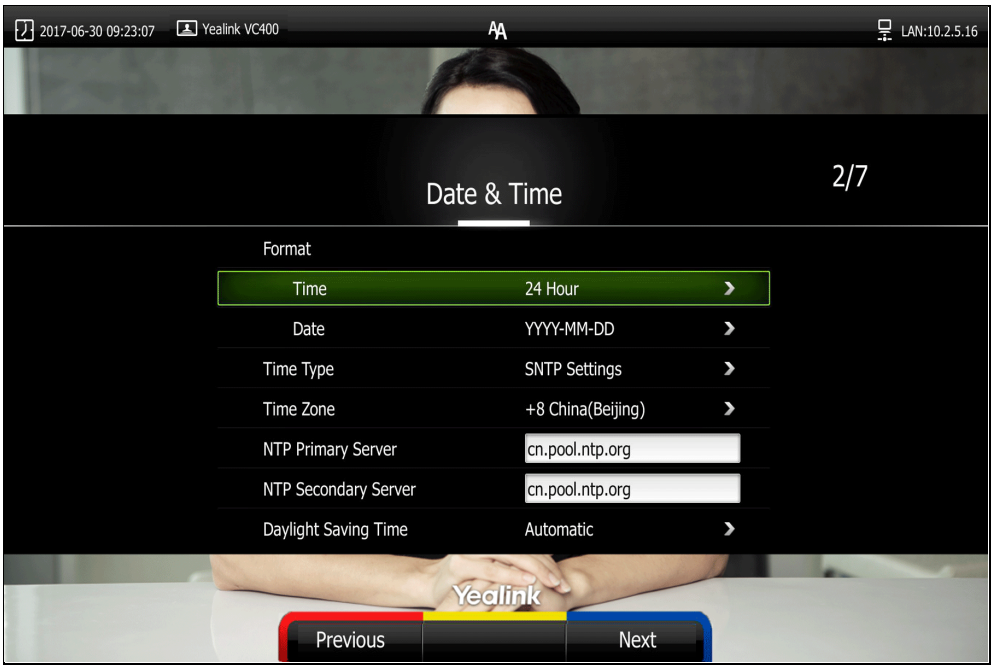
1. Set the language displayed on the display device.

   The default language is English.



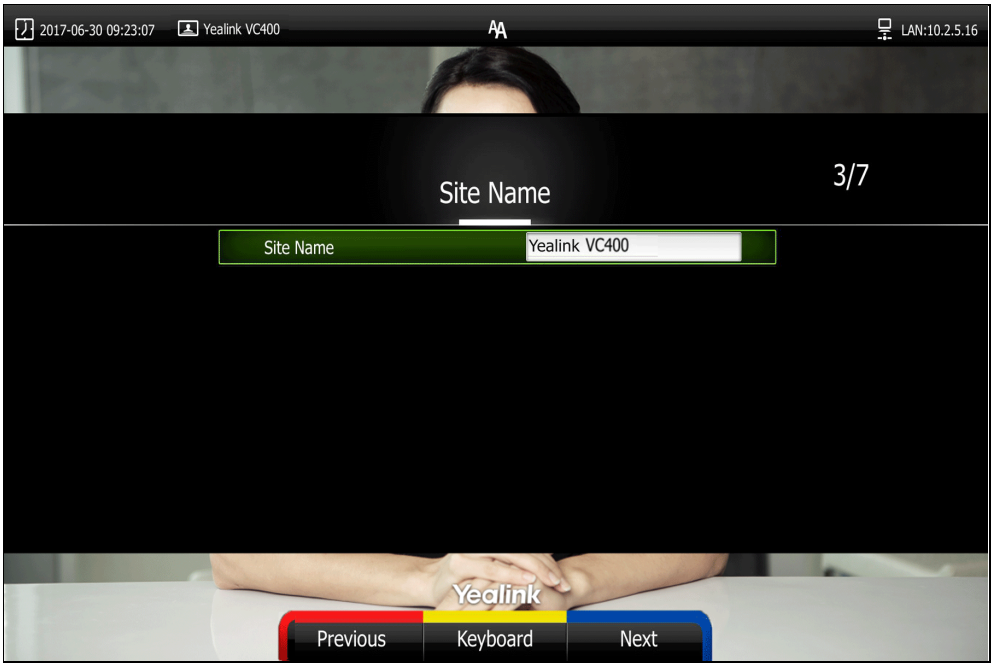
2. Press (**Next** soft key) to continue.
3. Set the date and time (e.g., set the time zone, time format, date format and the type of the daylight saving time).

The system obtains the time and date from the NTP server automatically by default. You can also configure the time and date manually. For more information, refer to on Date & Time on page 170.



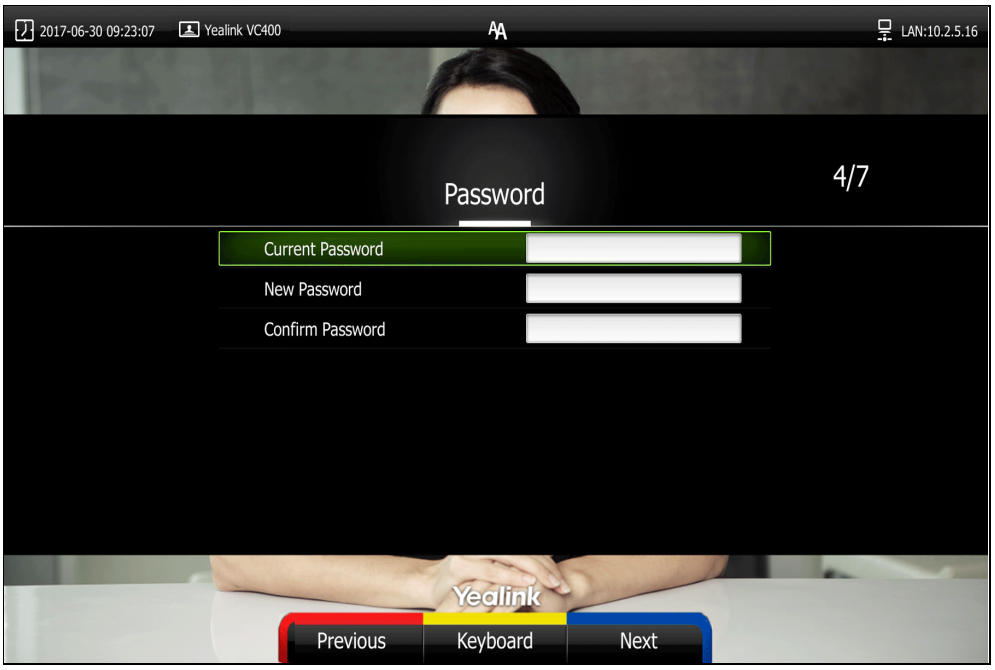
4. Press (**Next** soft key) to continue or press (**Previous** soft key) to return to the previous screen.
5. Edit the site name.

   The default site name is "Yealink VC400" or "Yealink VC120".



6. Press (**Next** soft key) to continue or press (**Previous** soft key) to return to the previous screen.
7. Change the administrator password.

The default administrator password is "0000". For security reasons, the administrator should change the default administrator password as soon as possible.



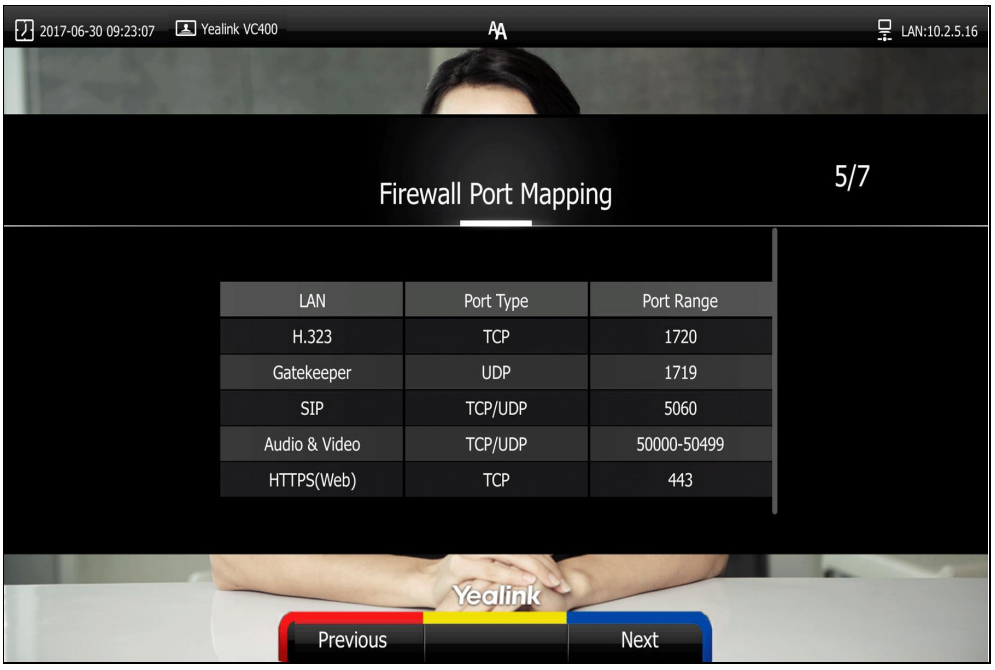
Note

Do remember the new administrator password or keep a copy of the password in a safe place. If you forget the password, you will need to reset the system to the factory settings, and then reset the password or use the default password "0000".

For more information, refer to Resetting to Factory on page 271.

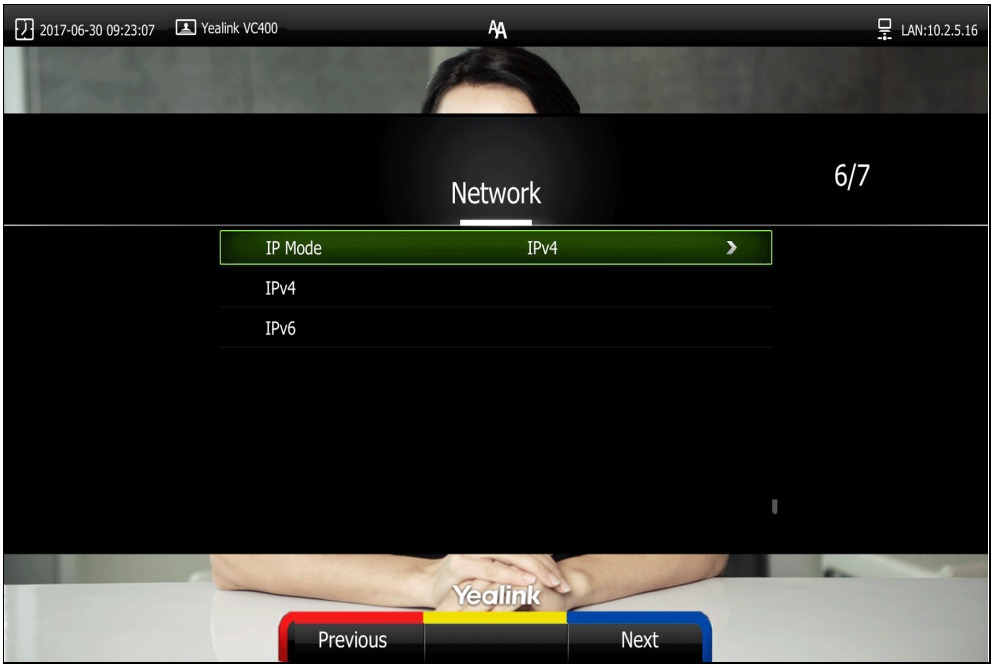
8. Press (**Next** soft key) to continue or press (**Previous** soft key) to return to the previous screen.

The display device displays firewall port mapping information.



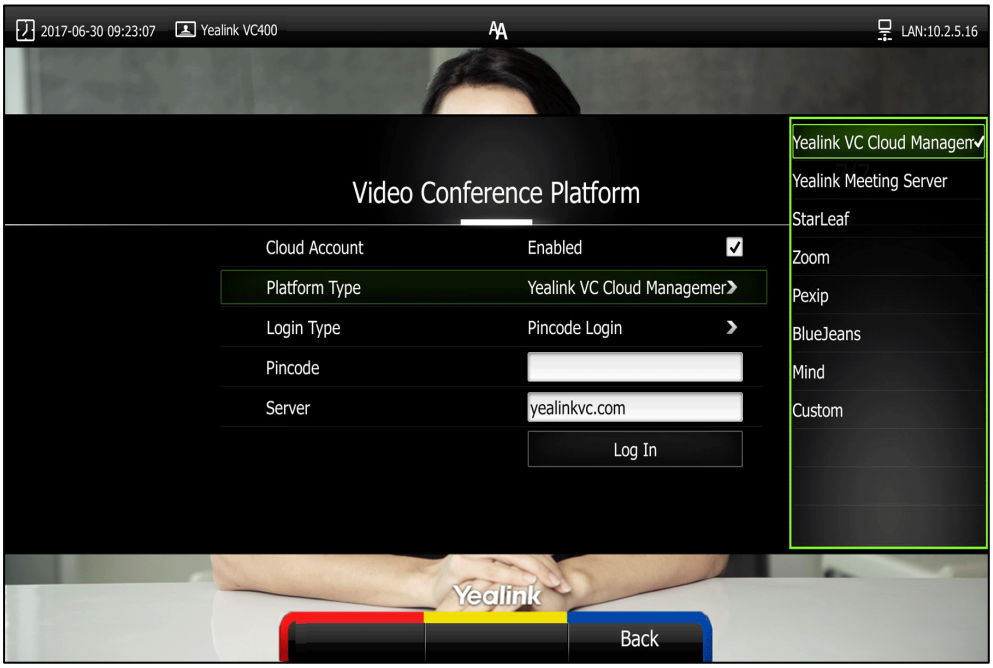
9. Press (**Next** soft key) to continue or press (**Previous** soft key) to return to the previous screen.
10. Configure network settings.

    The phone will try to contact a DHCP server in your network to obtain network parameters by default. If you uncheck the DHCP checkbox, you will need to configure IPv4 or IPv6 network manually. For more information, refer to Configuring LAN Properties on page 48.



11. Press (**Next** soft key) to continue or press (**Previous** soft key) to return to the previous screen.
12. (Optional.) Log into the Cloud platform.

Yealink video conferencing system supports Yealink VC Cloud Management Service/Yealink Meeting Server/StarLeaf/Zoom/Pexip/BlueJeans/Mind/Custom platform. For more information, refer to Configuring Video Conference Platform on page 99.



13. Press (**Complete** soft key) to complete the setup wizard.

Enabling Communication with Other Systems

Depending on your environment, you may need to make the following additional adjustments to the configuration of your video conferencing system.

Static NAT	If you choose to place your video conferencing systems in a private LAN, you must use Network Address Translation (NAT) to communicate with outside systems. This may include enabling static NAT on your system. For more information, refer to Static NAT on page 81.
Firewall	If your system communicates with other devices through a firewall, you must configure your firewall to allow incoming and outgoing traffic to the system through reserve ports. Users placing calls through a firewall to systems with IP addresses may experience one-way audio or video if the firewall is not properly configured to allow video and audio traffic. For more information, refer to Configuring the System for Use with a Firewall or NAT on page 77.
Cloud	If you are using Cloud server in your environment and want to place calls using Cloud account, refer to Configuring Video Conference Platform on page 99.
H.323	If you are using H.323 gatekeepers in your environment and want to place calls using a name or extension with the H.323 protocol, refer to Configuring H.323 Settings on page 130.
SIP	If you are using Session Initiation Protocol (SIP) servers in your environment to place calls using the SIP protocol, refer to Configuring SIP Settings on

	page 126.

Placing a Test Call from VCS

Yealink Demo1 to Yealink Demo3 are three default contacts stored in the local directory.

You can place a test call to the default contact, and the test call will be routed to the Yealink demo video conferencing system. Yealink demo contacts can help users to test quickly whether the system is normal after installation.

Configuring Network

This chapter provides information on how to configure network settings for the system. Proper network settings allow the system work efficiently in your network environment.

This chapter provides the following sections:

- Preparing the Network
- Configuring LAN Properties
- Configuring Network Speed and Duplex Mode
- VLAN
- 802.1X Authentication
- H.323 Tunneling
- Configuring the System for Use with a Firewall or NAT
- Intelligent Firewall Traversal
- Quality of Service
- VPN

Preparing the Network

Before you begin configuring the network options, you must make sure your network is ready for video conferencing.

The following table lists the network information you need to obtain from the network administrator when preparing your network.

Type	Network Information
Type of system	DHCP
	Static IP Address • IP address • Subnet mask • Gateway
DNS Server	IP address of DNS server
Call Protocol	Register information of SIP account
	Register information of H.323 account
Cloud Server	Register information of Cloud platform
802.1X	Authentication information

Configuring LAN Properties

DHCP

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to dynamically allocate network parameters to network hosts. The automatic allocation of network parameters to hosts eases the administrative burden of maintaining an IP network. The system complies with the DHCP specifications documented in RFC 2131. DHCP by default, which allows the system connected to the network to become operational by obtaining IP addresses and additional network parameters from the DHCP server.

DHCP Option

DHCP provides a framework for passing information to TCP/IP network devices. Network and other control information are carried in tagged data items that are stored in the options field of the DHCP message. The data items themselves are also called options.

DHCP can be initiated by simply connecting the system to the network. The system broadcasts DISCOVER messages to request network information carried in DHCP options. The DHCP server responds with the specific values in the corresponding options.

The following table lists the common DHCP options supported by the system.

Parameter	DHCP Option	Description
Subnet Mask	1	Specifies the client's subnet mask.
Time Offset	2	Specifies the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Router	3	Specifies a list of IP addresses for routers on the client's subnet.
Time Server	4	Specifies a list of time servers available to the client.
Domain Name Server	6	Specifies a list of domain name servers available to the client.
Log Server	7	Specifies a list of MIT-LCS UDP servers available to the client.
Host Name	12	Specifies the name of the client.
Domain Server	15	Specifies the domain name that client should use when resolving hostnames via DNS.
Broadcast Address	28	Specifies the broadcast address in use on the client's subnet.
Network Time	42	Specifies a list of the NTP servers available to the

Parameter	DHCP Option	Description
Protocol Servers		client by IP address.
Vendor-Specific Information	43	Identifies the vendor-specific information.
Vendor Class Identifier	60	Identifies the vendor type.
TFTP Server Name	66	Identifies a TFTP server when the 'name' field in the DHCP header has been used for DHCP options.
Bootfile Name	67	Identifies a bootfile when the 'file' field in the DHCP header has been used for DHCP options.

For more information on DHCP options, refer to *http://www.ietf.org/rfc/rfc2131.txt?number=2131* or *http://www.ietf.org/rfc/rfc2132.txt?number=2132*.

To make the system gather network settings via DHCP options, you need to contact your network administrator to configure the DHCP server properly.

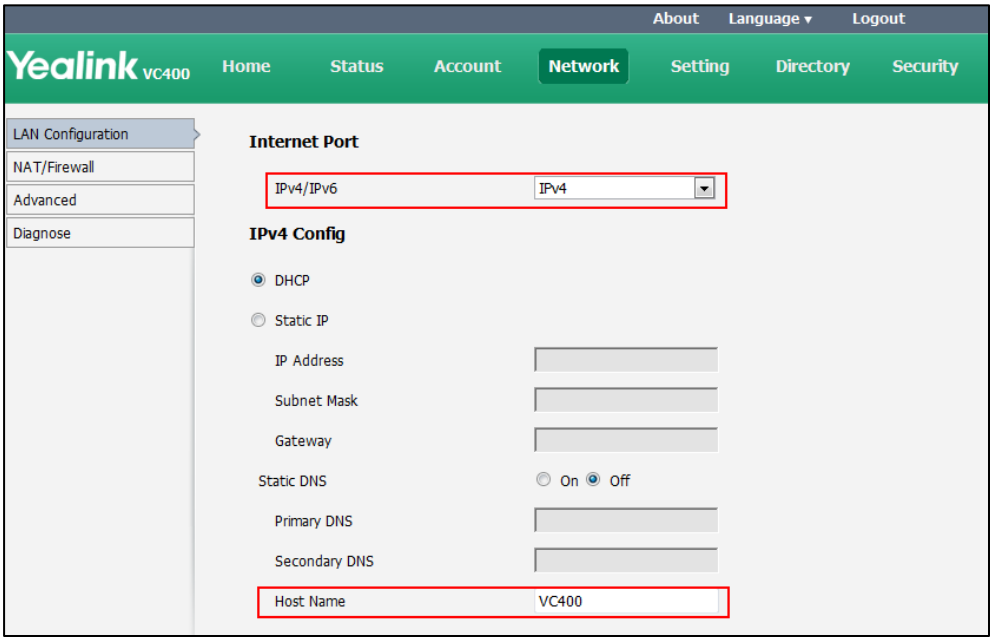
DHCP feature parameters on the system are described below:

Parameter	Description	Configuration Method
DHCP	Enables or disables the system to obtain network settings from the DHCP server. **Default:** Enabled **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Host Name	Configures the host name of the system. **Default:** Blank **Note**: When the system broadcasts DHCP DISCOVER messages, it will report the configured host name to the DHCP server via DHCP option 12. Host name is optional, so it is not a mandatory configuration item. For more information, contact your network administrator. If you change this parameter, the system will reboot to make the	Web User Interface

Parameter	Description	Configuration Method
	change take effect.	

To configure DHCP via web user interface:

1. Click on **Network**->**LAN Configuration**.
2. In the **IPv4 Config** block, mark the **DHCP** radio box.
3. (Optional.) Enter the host name of the system in the **Host Name** field.



4. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that settings will take effect after a reboot.
5. Click **Confirm** to reboot the system immediately.

To configure DHCP via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Internet Configuration**->**IPv4**.
2. Check the **DHCP** checkbox.
3. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".
4. Select **OK** to reboot the system immediately.

Static DNS

Even though DHCP is enabled, you can manually configure the static DNS address(es).

Parameters of static DNS on the system are described below:

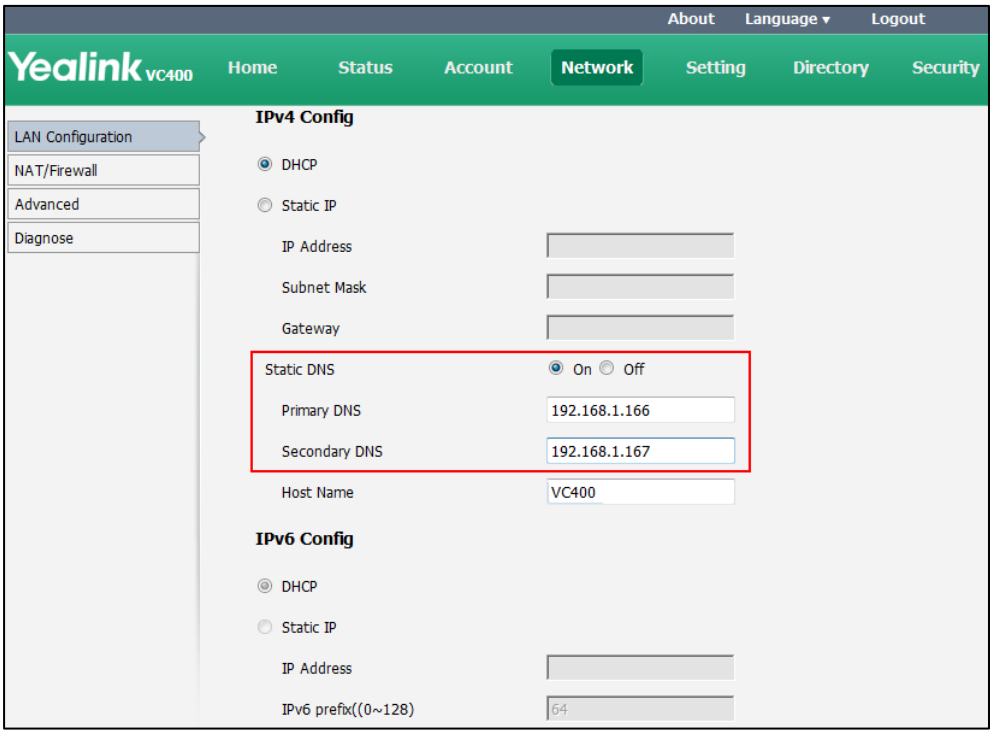
Parameter	Description	Configuration Method
Static DNS	Triggers the static DNS feature to on	Remote Control

Parameter	Description	Configuration Method
	or off. **Default:** Off **Note**: If it is set to Off, the system will use the IPv4 DNS obtained from DHCP. If it is set to On, the system will use manually configured static IPv4 DNS. It only works if the value of the "IPv4 Config" is set to DHCP. If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Primary DNS	Configures the primary IPv4 DNS server. **Default**: Blank **Note**: It only works if the value of the " Static IPv4 DNS" is set to On. If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Secondary DNS	Configures the secondary IPv4 DNS server. **Default**: Blank **Note**: It only works if the value of the " Static IPv4 DNS" is set to On. If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure static DNS address when DHCP is used via web user interface:

1. Click on **Network**->**LAN Configuration**.
2. In the **IPv4 Config** block, mark the **DHCP** radio box.
3. In the **Static DNS** block, mark the **On** radio box.

4. Enter the desired values in the **Primary DNS** and **Secondary DNS** fields.



5. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that settings will take effect after a reboot.

6. Click **Confirm** to reboot the phone.

To configure static DNS when DHCP is used via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Internet Configuration** ->**IPv4**.
2. Check the **DHCP** checkbox.
3. Check the **Static DNS** checkbox.
4. Enter the desired values in the **DNS Primary Server** and **DNS Secondary Server** fields respectively.
5. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".

Configuring Network Settings Manually

If DHCP is disabled or the system cannot obtain network settings from the DHCP server, you need to configure them manually.

The following parameters should be configured for systems to establish network connectivity:

- **IP Address**: Configure the system to use the assigned IP address.
- **Subnet Mask**: Enter the subnet mask address when the system does not automatically obtain the subnet mask.

- **Gateway**: A gateway is a network point that works as an entrance to another network.
- **Primary DNS** /**Secondary DNS**: Domain Name System (DNS) servers translates domain names (for example: www.example.com), which can be easily memorized by humans, to the numerical IP addresses (192.168.1.15) needed for the purpose of computer services and devices worldwide.

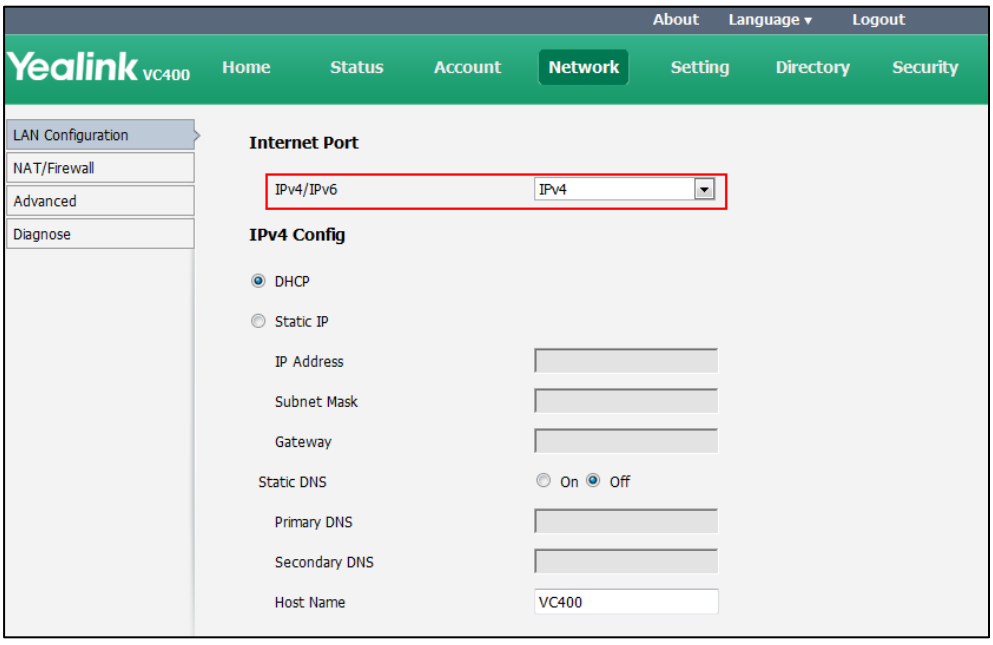
Network parameters need to be configured manually on the system are described below.

Parameter	Description	Configuration Method
Mode (IPv4/IPv6)	Configures the IP address mode. **Default:** IPv4 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.	Remote Control Web User Interface
Static IP	Enables or disables the system to use manually configured network settings. **Default:** Disabled **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
IP Address	Configures the IP address assigned to the system. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Subnet Mask	Configures the subnet mask assigned to the system. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Gateway	Configures the gateway assigned to the system. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Static DNS	Triggers the static DNS feature to on	Remote Control

Parameter	Description	Configuration Method
	or off. **Default:** Off **Note**: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Primary DNS	Configures the primary DNS server assigned to the system. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Secondary DNS	Configures the secondary DNS server assigned to the system. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure the IP address mode via web user interface:

1. Click on **Network**->**LAN Configuration**.
2. Select desired value from the pull-down list of **IPv4/IPv6**.



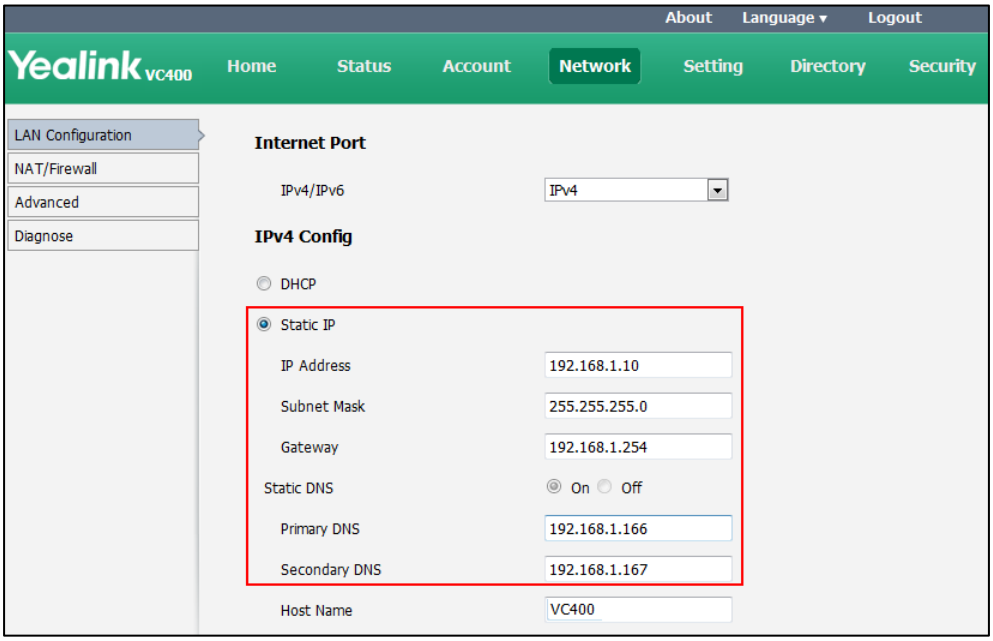
3. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that settings will take effect after a reboot.

4. Click **OK** to reboot the phone.

To configure a static IPv4 address via web user interface:

1. Click on **Network**->**LAN Configuration**.
2. In the **IPv4 Config** block, mark the **Static IP** radio box.
3. Enter the desired values in the **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS** and **Secondary DNS** fields.



4. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that settings will take effect after a reboot.

5. Click **Confirm** to reboot the system immediately.

To configure the IP address mode via phone user interface:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Internet Configuration**.
2. Select **IPv4** or **IPv4 & IPv6** from the **IP Mode** field.
3. Press the **Save** soft key to accept the change.

   The IP phone reboots automatically to make settings effective after a period of time.

To configure a static IPv4 address via phone user interface:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Internet Configuration**->**IPv4**.
2. Uncheck the **DHCP** checkbox.
3. Enter the desired values in the **IP Address**, **Subnet Mask**, **Gateway**, **DNS Primary Server** and **DNS Secondary Server** fields respectively.
4. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".

5. Select **OK** to reboot the system immediately.

IPv6 Support

Because Internet Protocol version 4 (IPv4) uses a 32-bit address, it cannot meet the increased demands for unique IP addresses for all devices that connect to the Internet. Therefore, Internet Protocol version 6 (IPv6) is the next generation network layer protocol, which designed as a replacement for the current IPv4 protocol.

IPv6 is developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. Yealink IP Phone supports IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4&IPv6 dual stack addressing mode. IPv4 uses a 32-bit address, consisting of four groups of three decimal digits separated by dots; for example, 192.168.1.100. IPv6 uses a 128-bit address, consisting of eight groups of four hexadecimal digits separated by colons; for example, 2026:1234:1:1:215:65ff:fe1f:caa.

VoIP network based on IPv6 can provide end-to-end security capabilities, enhanced Quality of Service (QoS), a set of service requirements to deliver performance guarantee while transporting traffic over the network.

If you configure the network settings on the phone for an IPv6 network, you can set up an IP address for the phone either by using DHCPv6 or by manually entering an IP address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

IPv6 Address Assignment Method

Supported IPv6 address assignment methods:

- **Manual Assignment:** An IPv6 address and other configuration parameters (e.g., DNS server) for the IP phone can be statically configured by an administrator.
- **Stateful DHCPv6:** The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC 3315. DHCPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately or concurrently with the latter to obtain configuration parameters.

How the system obtains the IPv6 address and network settings?

The following table lists where the system obtains the IPv6 address and other network settings:

DHCPv6	How the IP phone obtains the IPv6 address and network settings?
Disabled	You have to manually configure the static IPv6 address and other network settings.
Enabled	The IP phone can obtain the IPv6 address and the other network settings via DHCPv6.

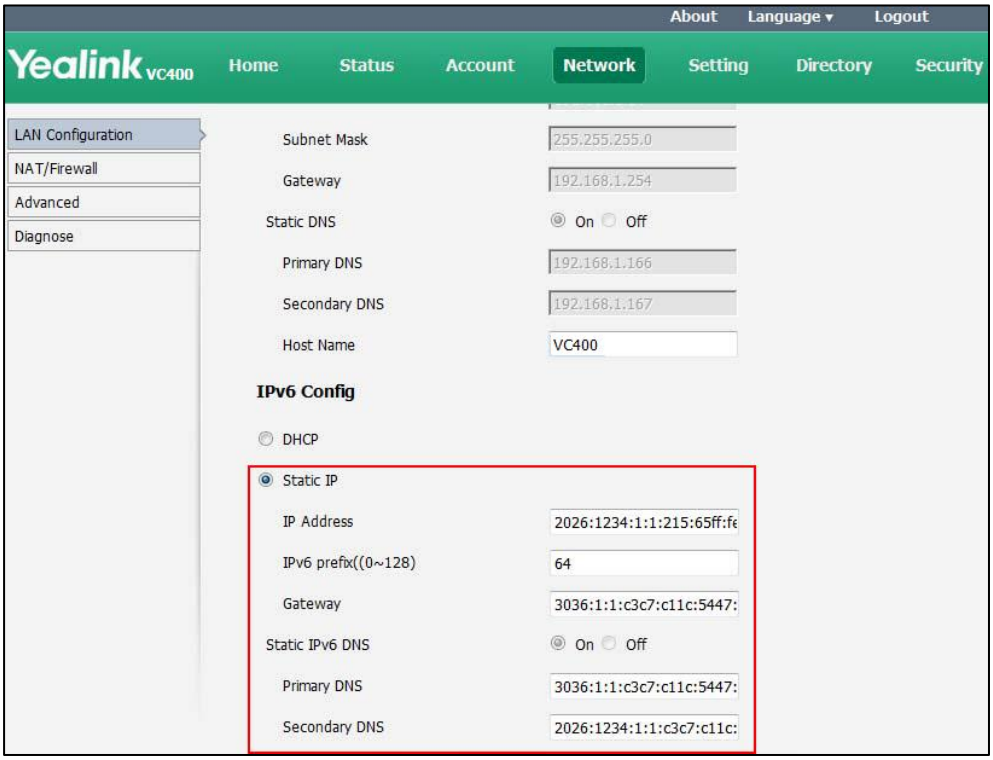
IPv6 Network parameters need to be configured manually on the system are described below.

Parameter	Description	Configuration Method
Mode (IPv4/IPv6)	Configures the IP address mode. **Default:** IPv4 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.	Remote Control Web User Interface
Static IP	Enables or disables the system to use manually configured IPv6 network settings. **Default:** Disabled **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
IP Address	Configures the IPv6 address assigned to the system. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
IPv6 prefix((0~128)	Configures the IPv6 prefix. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Gateway	Configures the IPv6 default gateway. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Static DNS/Static IPv6 DNS	Triggers the static IPv6 DNS feature to on or off. **Default:** Off **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
DNS Primary Server/Primary	Configures the primary IPv6 DNS server.	Remote Control Web User Interface

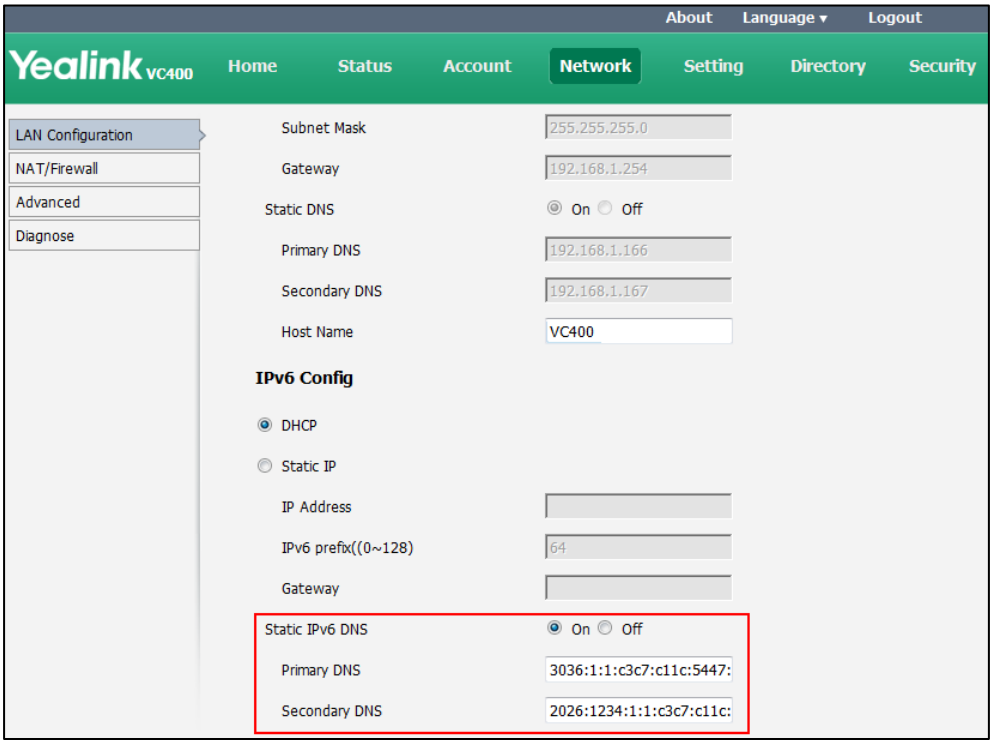
Parameter	Description	Configuration Method
DNS	**Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	
DNS Secondary Server/Secondary DNS	Configures the secondary IPv6 DNS server. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure IPv6 address assignment method via web user interface:

1. Click on **Network**->**LAN Configuration**.
2. Select the desired IP mode (**IPv6** or **IPv4 & IPv6**) from the pull-down list of **IPv4/IPv6**.
3. In the **IPv6 Config** block, mark the **DHCP** or the **Static IP** radio box.
   - If you mark the **Static IP** radio box, configure the IPv6 address and other configuration parameters in the corresponding fields.



- (Optional.) If you mark the **DHCP** radio box, you can configure the static DNS address in the corresponding fields.



4. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.

5. Click **OK** to reboot the phone.

To configure IPv6 address assignment method via phone user interface:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Internet Configuration**.
2. Select **IPv4 & IPv6** or **IPv6** from the **IP Mode** field.
3. Press ▲ or ▼ to highlight **IPv6** and press OK .
4. Select the desired IPv6 address assignment method.

   If you uncheck the **DHCP** checkbox, configure the IPv6 address and other network parameters in the corresponding fields.

5. Press the **Save** soft key to accept the change.

   The IP phone reboots automatically to make settings effective after a period of time.

To configure static DNS when DHCP is used via phone user interface:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Internet Configuration** ->**IPv6**.
2. Check the **DHCP** checkbox.
3. Check the **Static DNS** checkbox.
4. Enter the desired values in the **DNS Primary Server** and **DNS Secondary Server** fields respectively.
5. Press the **Save** soft key to accept the change.

6. The display device prompts "Reboot now?".
7. Select **OK** to reboot the system immediately.

Configuring Network Speed and Duplex Mode

You can configure the network speed and duplex mode the system uses. The network speed and duplex mode you select for the system must be supported by the switch. The network speeds and duplex modes supported by the system are:

- Auto
- 10 Mb/s Full Duplex
- 100 Mb/s Full Duplex
- 10 Mb/s Half Duplex
- 100 Mb/s Half Duplex
- 1000 Mb/s Full Duplex

Auto is configured on the system by default.

Auto

Auto means that the switch will negotiate the network speed and duplex mode for the systems to transmit voice or data over Ethernet. This process entails devices first sharing transmission capabilities and then selecting the highest performance transmission mode supported by both systems.

Half-duplex

Half-duplex transmission refers to transmitting voice or data in both directions, but in one direction at a time; this means one system can send data on the line, but not receive data simultaneously.

Full-duplex

Full-duplex transmission refers to transmitting voice or data in both directions at the same time; this means one system can send data on the line while also receiving data.

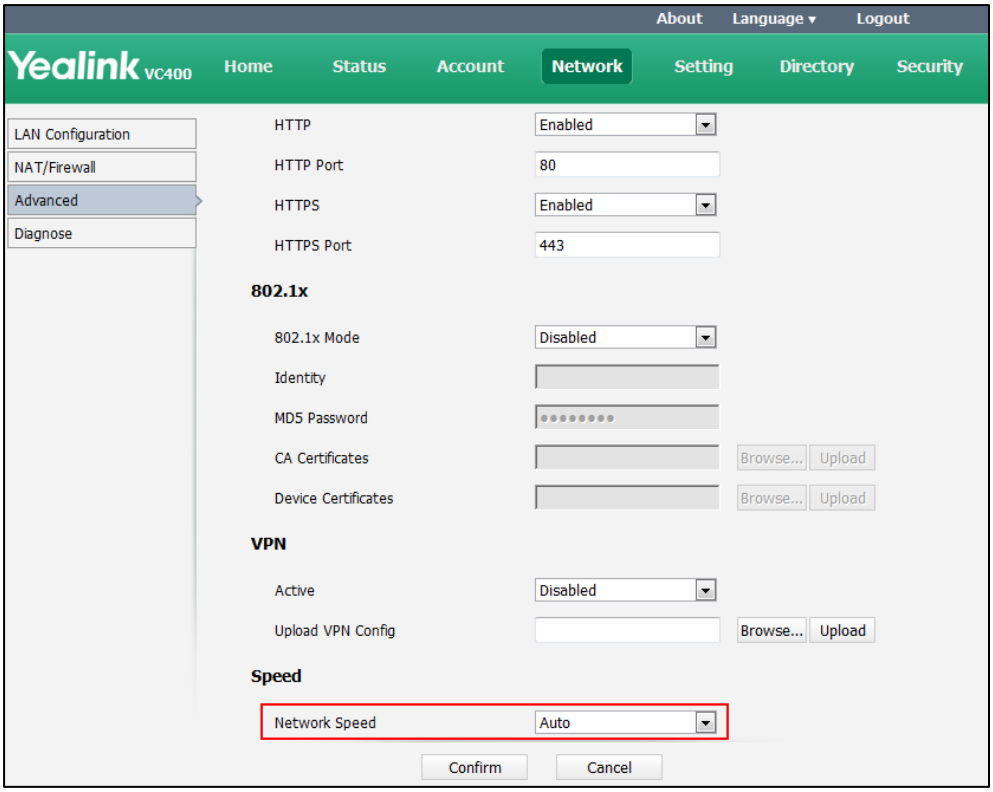
Parameter of network speed feature on the system is described below:

Parameter	Description	Configuration Method
Network Speed	Specifies the network speed and duplex mode for the system to use. **Default:** Auto **Note**: If **Auto** is selected, the network speed and duplex mode will be negotiated by the switch	Web User Interface

Parameter	Description	Configuration Method
	automatically. The network speed and duplex mode you select must be supported by the switch. If you change this parameter, the system will reboot to make the change take effect.	

To configure the network speed via web user interface:

1. Click on **Network**->**Advanced**.
2. Select the desired value from the pull-down list of **Network Speed**.



3. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that settings will take effect after a reboot.

4. Click **Confirm** to reboot the system immediately.

VLAN

VLAN (Virtual Local Area Network) is used to divide a physical network logically into several broadcast domains. VLAN membership is configurable through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements

regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security, and network management.

The purpose of VLAN configurations on the system is to insert a tag with VLAN information to the packets generated by the system. When VLAN is configured on the system properly, the system will tag all packets with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the tag's VLAN ID, as described in IEEE Std 802.3.

In addition to manual configuration, the system also supports automatic VLAN discovery via LLDP or DHCP. The assignment takes effect in the following order: assignment via LLDP, manual configuration, then assignment via DHCP.

For more information on VLAN, refer to *VLAN Feature on Yealink IP Phones*.

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows the system to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

LLDP-MED (Media Endpoint Discovery)

LLDP-MED is published by the Telecommunications Industry Association (TIA). It is an extension to LLDP that operates between endpoint devices and network connectivity devices. LLDP-MED provides the following capabilities for the system:

- Capabilities Discovery -- allows LLDP-MED system to determine the capabilities that the connected switch supports and has enabled.
- Network Policy -- provides voice VLAN configuration to notify the system which VLAN to use and QoS-related configuration for voice data. It provides a "plug and play" network environment.
- Power Management -- provides information related to how the system is powered, power priority, and how much power the system needs.
- Inventory Management -- provides a means to effectively manage the system and its attributes, such as model number, serial number and software revision.

TLVs supported by the system are summarized in the following table:

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	The network address of the system.
	Port ID	The MAC address of the system.
	Time To Live	Seconds until data unit expires.

TLV Type	TLV Name	Description
		The default value is 180s.
	End of LLDPDU	Marks end of LLDPDU.
Optional TLVs	System Name	Name assigned to the system. The default value is "VCS".
	System Description	Description of the system. Description includes firmware version of the system.
	System Capabilities	The supported and enabled system capabilities. The Telephone capability is supported and enabled by default.
	Port Description	Description of port that sends data unit. The default value is "WAN PORT".
IEEE Std 802.3 Organizationally Specific TLV	MAC/PHY Configuration/Status	Duplex mode and network speed settings of the system. The Auto Negotiation is supported and enabled by default. The advertised capabilities of PMD. Auto-Negotiation is: 1000BASE-T (full duplex mode) 100BASE-TX (full duplex mode) 100BASE-TX (half duplex mode) 10BASE-T (full duplex mode) 10BASE-T (half duplex mode)
TIA Organizationally Specific TLVs	Media Capabilities	The MED device type of the system and the supported LLDP-MED TLV type can be encapsulated in LLDPDU. The supported LLDP-MED TLV types are: LLDP-MED Capabilities, Network Policy, Extended Power via MDI-PD, Inventory.
	Network Policy	Port VLAN ID, application type, L2 priority and DSCP value.
	Extended Power-via-MDI	Power type, source, priority and value.
	Inventory – Hardware Revision	Hardware revision of the system.

TLV Type	TLV Name	Description
	Inventory - Firmware Revision	Firmware revision of the system.
	Inventory - Software Revision	Software revision of the system.
	Inventory - Serial Number	Serial number of the system.
	Inventory - Manufacturer Name	Manufacturer name of the system. The default value is "Yealink".
	Inventory - Model Name	Model name of the system. The default value is "VCS".
	Asset ID	Assertion identifier of the system.

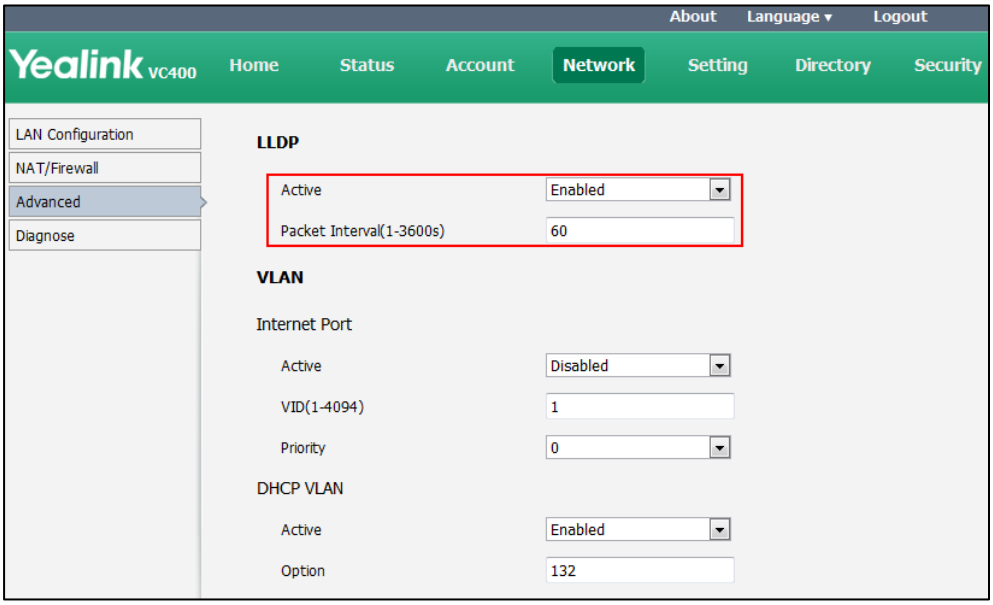
Parameters of LLDP feature on the system are described below.

Parameter	Description	Configuration Method
LLDP->**Active**	Enables or disables LLDP feature on the system. **Default:** Disabled **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Packet Interval(1-3600s)	Configures the interval (in seconds) for the system to send LLDP requests. **Default:** 60 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure LLDP via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **LLDP** block, select the desired value from the pull-down list of **Active**.

3. Enter the desired time interval in the **Packet Interval (1-3600s)** field.



4. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.

5. Click **Confirm** to reboot the system immediately.

To configure LLDP via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. In the **LLDP** block, check the **Active** checkbox.
3. Enter the desired value in the **Packet Interval (1-3600s)** field.
4. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".

5. Select **OK** to reboot the system immediately.

Manual Configuration for VLAN

VLAN is disabled on systems by default. You can configure VLAN manually. Before configuring VLAN on the systems, you need to obtain the VLAN ID from your network administrator.

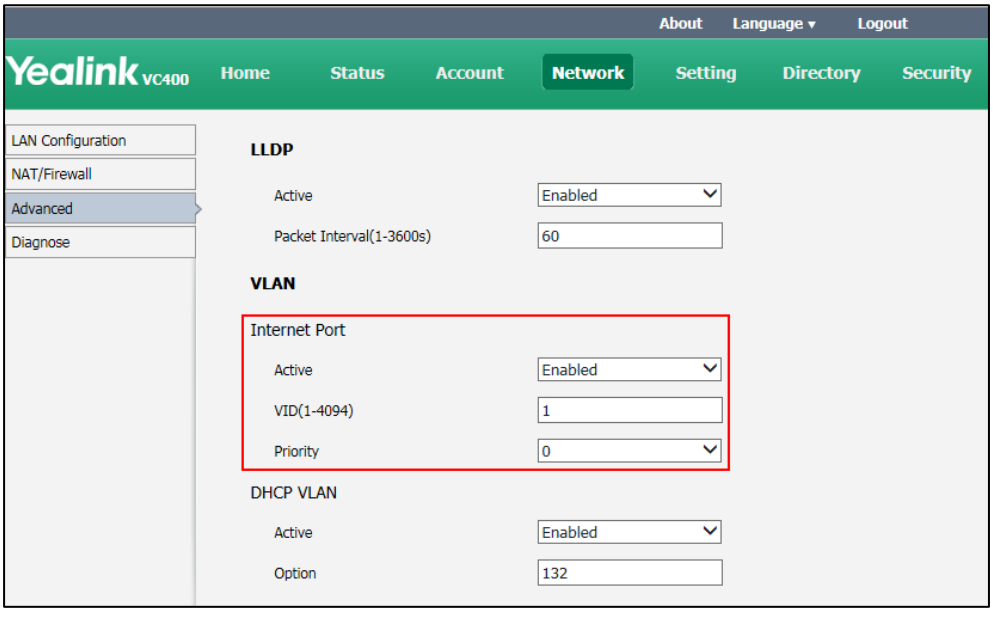
Parameters of manual VLAN on the system are described below.

Parameter	Description	Configuration Method
Internet Port->Active	Enables or disables VLAN for the Internet (WAN) port. **Default:** Disabled **Note**: If you change this parameter, the system will reboot to make the	Remote Control Web User Interface

Parameter	Description	Configuration Method
	change take effect.	
VID(1-4094)	Configures VLAN ID for the Internet (WAN) port. **Default:** 1 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Priority	Configures VLAN priority for the Internet (WAN) port. **Valid values:** 0-7 7 is the highest priority, 0 is the lowest priority. **Default:** 0 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure VLAN for Internet port via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **Internet Port Active**.
3. Enter the VLAN ID in the **VID (1-4094)** field.
4. Select the desired value (0-7) from the pull-down list of **Priority**.



5. Click **Confirm** to accept the change.

A dialog box pops up to prompt that the settings will take effect after a reboot.

6. Click **OK** to reboot the phone.

To configure VLAN via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. In the **VLAN** block, check the **Active** checkbox.
3. Enter the VLAN ID in the **VID(1-4094)** field.
4. Enter the priority value (0-7) in the **Priority** field.
5. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".
6. Select **OK** to reboot the system immediately.

DHCP VLAN

The system supports VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the system will examine the DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to request the VLAN ID. For more information on VLAN, refer to *VLAN Feature on Yealink IP Phones*.

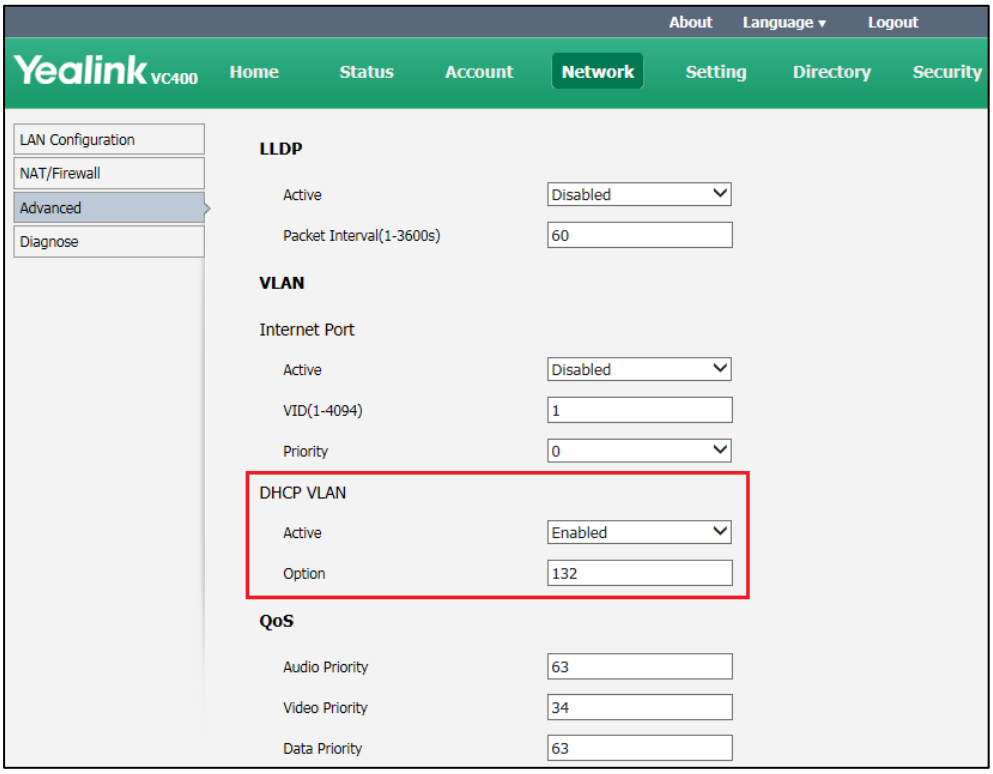
Parameters of VLAN feature on the system are described below.

Parameter	Description	Configuration Method
DHCP VLAN->Active	Enables or disables the DHCP VLAN discovery feature on the system. **Default:** Enabled **Note**: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Option	Configures the DHCP option from which the system obtains the VLAN settings. You can configure at most five DHCP options and separate them by commas. **Valid Values:** 128-254 **Default:** 132 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface

To configure DHCP VLAN discovery via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **VLAN** block, select the desired value from the pull-down list of **DHCP VLAN Active**.
3. Enter the desired option in the **Option** field.

   The default option is 132.



4. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.
5. Click **Confirm** to reboot the system immediately.

802.1X Authentication

IEEE 802.1X authentication is an IEEE standard for Port-based Network Access Control (PNAC), part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect to a LAN or WLAN. The 802.1X authentication involves three parties: a supplicant, an authenticator and an authentication server. The supplicant is the system that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the system provides credentials, such as user name and default password, for the authenticator. The authenticator then forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the system is allowed to access resources located on the protected side of the network.

The system supports the authentication protocols EAP-MD5, EAP-TLS, PEAP-MSCHAPv2 and EAP-TTLS/EAP-MSCHAPv2 for 802.1X authentication.

For more information on 802.1X authentication, refer to *Yealink 802.1X Authentication*.

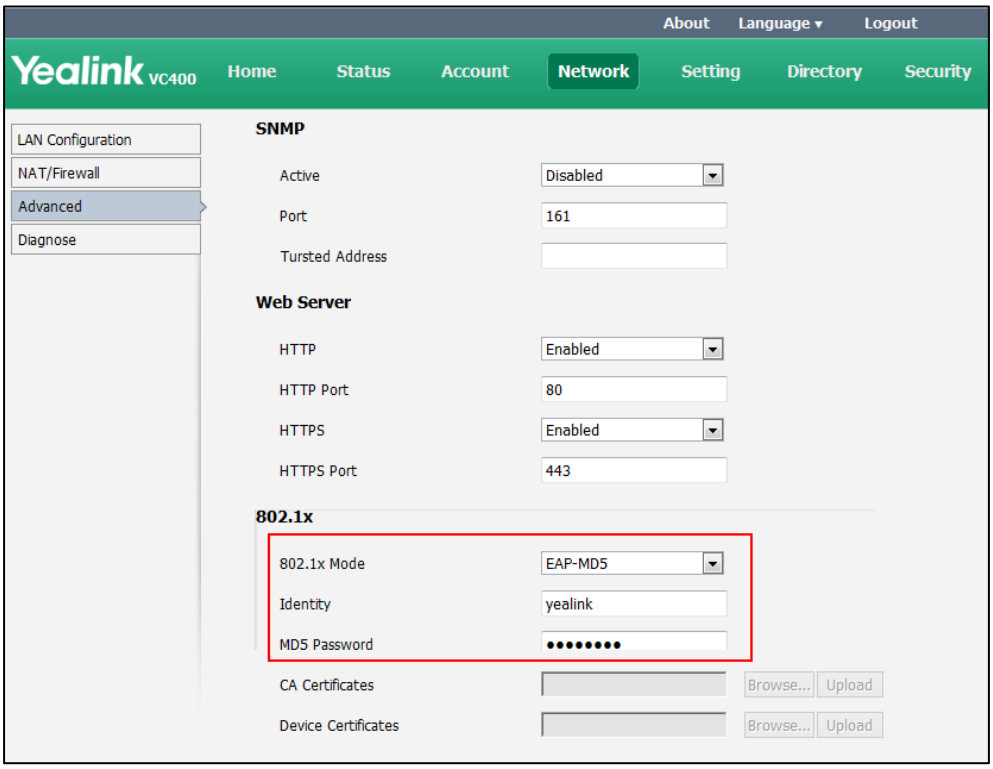
802.1X feature parameters on the system are described below:

Parameter	Description	Configuration Method
802.1x Mode	Specifies the 802.1x authentication mode. • Disabled • EAP-MD5 • EAP-TLS • PEAP-MSCHAPv2 • EAP-TTLS/EAP-MSCHAPv2 **Default:** Disabled **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Identity	Configures the user name for 802.1x authentication. **Note**: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
MD5 Password	Configures the password for 802.1x authentication. **Note**: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
CA Certificates	Configures the access URL of the CA certificate when the 802.1x authentication mode is configured as EAP-TLS, PEAP-MSCHAPV2 or EAP-TTLS/EAP-MSCHAPV2. **Note**: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Device Certificates	Configures the access URL of the device certificate when the 802.1x authentication mode is configured as EAP-TLS. **Note**: If you change this parameter, the system will reboot to make the	Web User Interface

Parameter	Description	Configuration Method
	change take effect.	

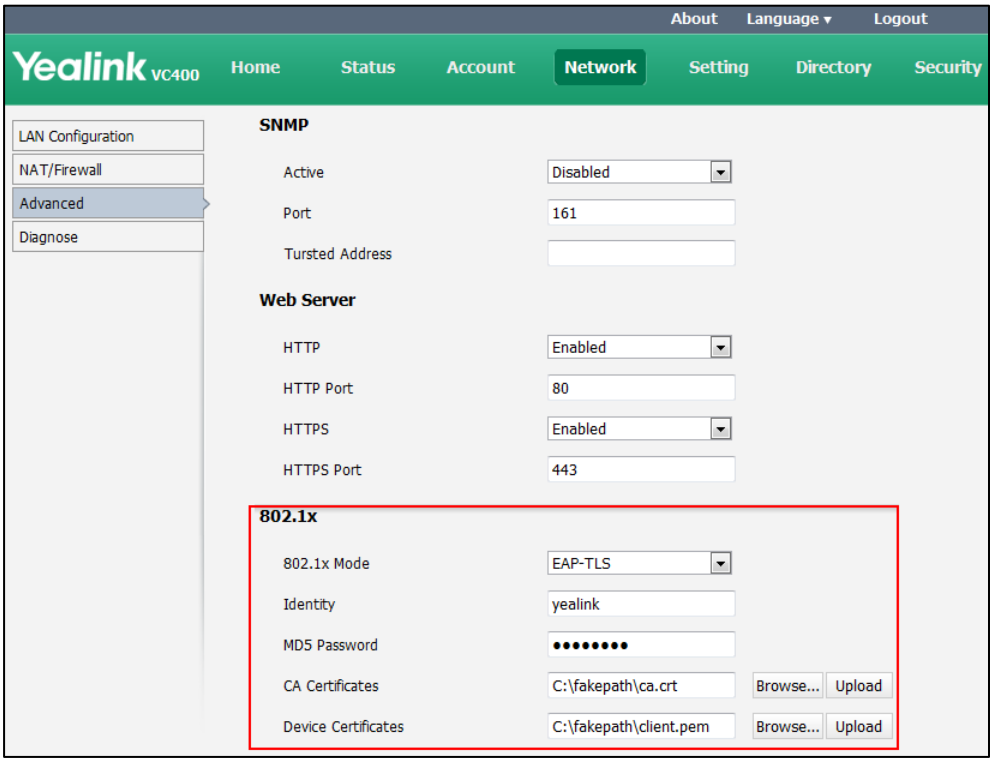
To configure 802.1X via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **802.1x** block, select the desired protocol from the pull-down list of **Mode 802.1x**.
   a) If you select **EAP-MD5**:
      1) Enter the user name for authentication in the **Identity** field.
      2) Enter the password for authentication in the **MD5 Password** field.



   b) If you select **EAP-TLS**:
      1) Enter the user name for authentication in the **Identity** field.
      2) Leave the **MD5 Password** field blank.
      3) In the **CA Certificates** field, click **Browse** to locate the desired CA certificate (*.pem,*.crt, *.cer or *.der) from your local system.
      4) In the **Device Certificates** field, click **Browse** to locate the desired client certificate (*.pem or *.cer) from your local system.

5) Click **Upload** to upload the certificates.



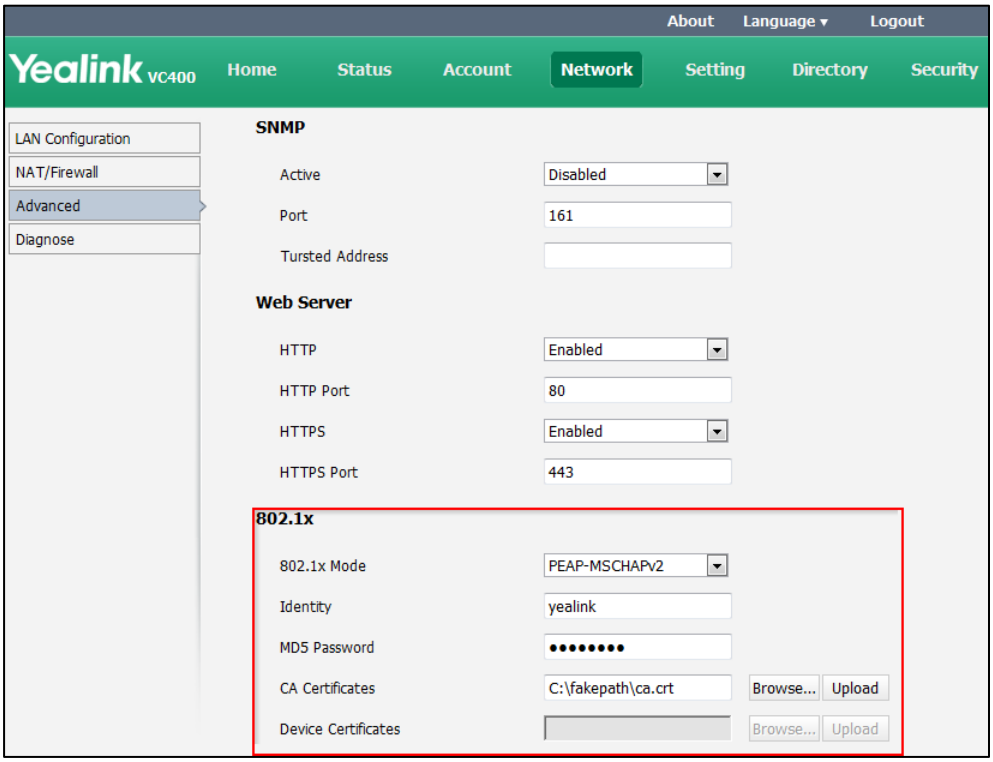
c) If you select **PEAP-MSCHAPv2**:

1) Enter the user name for authentication in the **Identity** field.

2) Enter the password for authentication in the **MD5 Password** field.

3) In the **CA Certificates** field, click **Browse** to locate the desired certificate (*.pem,*.crt, *.cer or *.der) from your local system.

4) Click **Upload** to upload the certificate.



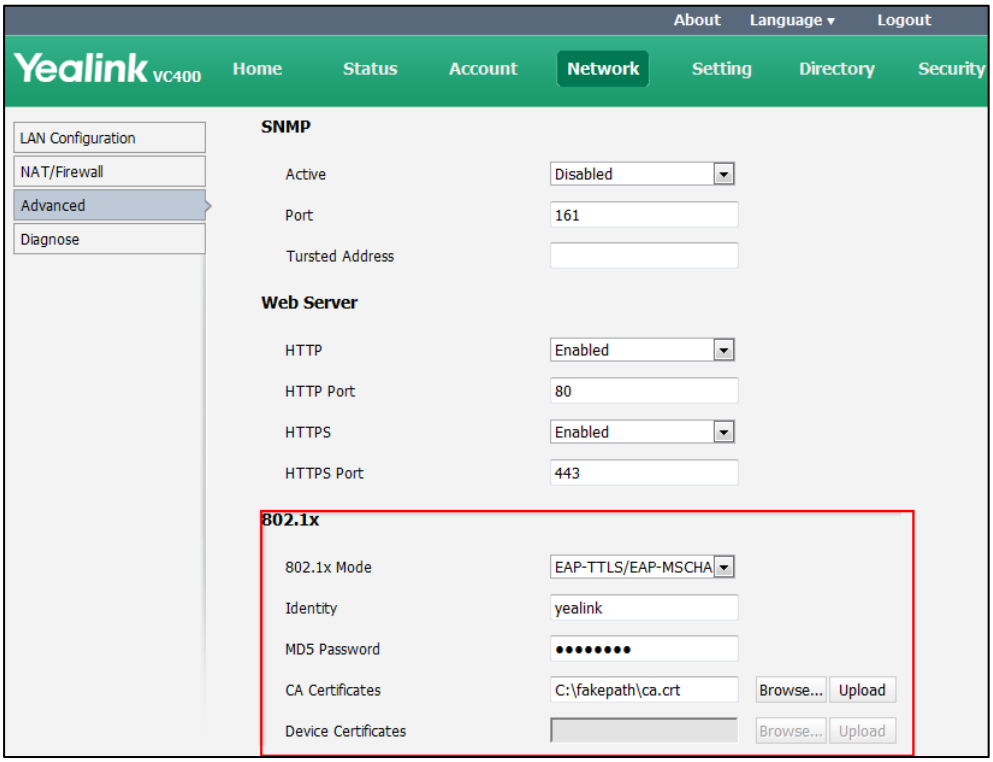
d) If you select **EAP-TTLS/EAP-MSCHAPv2**:

1) Enter the user name for authentication in the **Identity** field.

2) Enter the password for authentication in the **MD5 Password** field.

3) In the **CA Certificates** field, click **Browse** to locate the desired certificate (*.pem,*.crt, *.cer or *.der) from your local system.

4) Click **Upload** to upload the certificate.



3. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.

4. Click **Confirm** to reboot the system immediately.

To configure the 802.1X via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Select the desired mode from the pull-down list of **802.1x Mode**.
3. Press the **Save** soft key to accept the change.

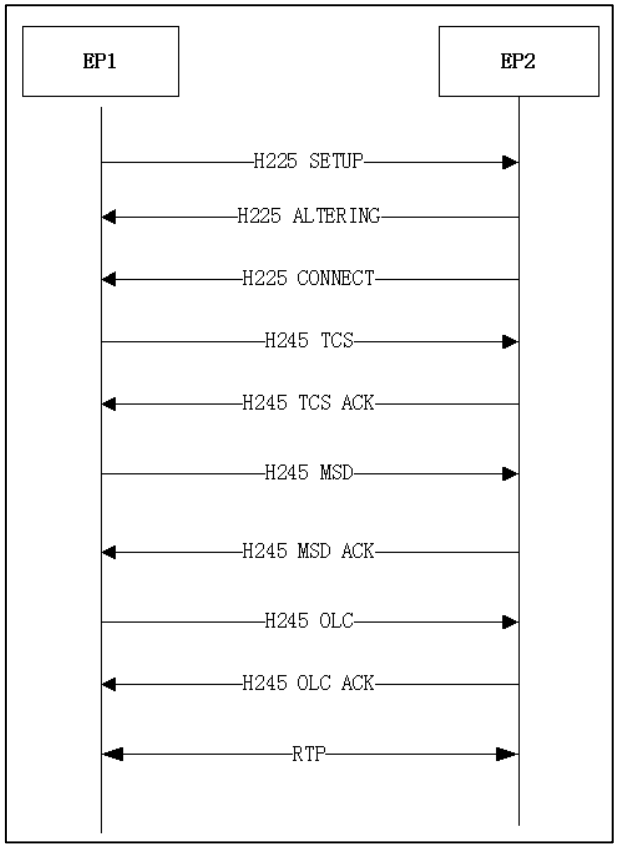
   The display device prompts "Reboot now?".

4. Select **OK** to reboot the system immediately.

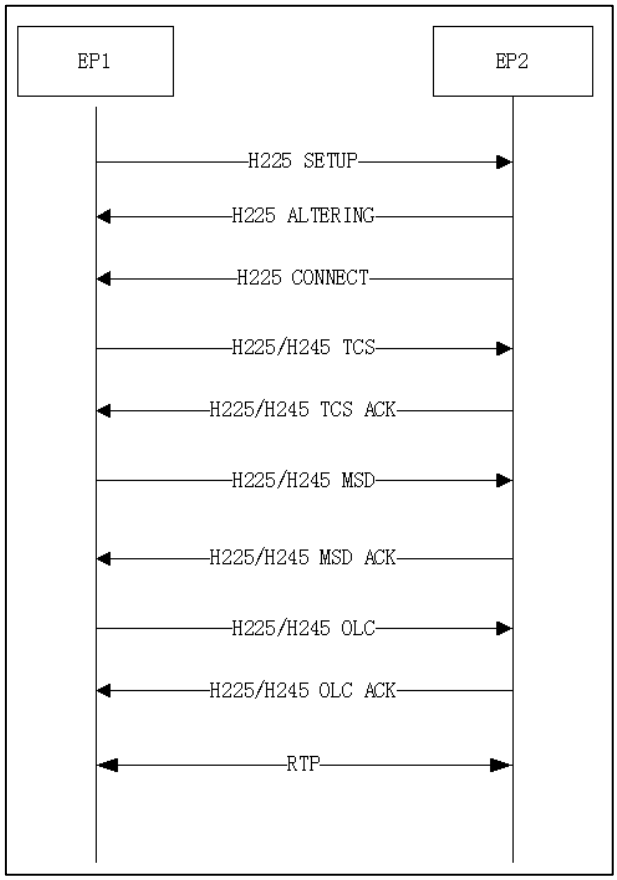
H.323 Tunneling

The H.245 protocol is a control protocol that manages the media sessions. It is a part of the H.323 protocol suite. The H.245 protocol is used primarily to negotiate the master-slave relationship between communicating systems. The H.245 messages can be encapsulated and carried between H.225 controlled system within H.225 messages. This way of "piggy-backing" an H.245 message to the H.225 message is referred to as H.323 Tunneling. The tunneling feature relies on H.225 system-to-system connectivity (via TCP) to pass H.245 messages, and uses the H.225 communication channel without creating a separate TCP socket connection (per H.323 call) for media control.

If H.323 tunneling feature is disabled, the setup processes of an H.323 call are shown below:



If H.323 tunneling feature is enabled on both sites, the setup processes of an H.323 call are shown below:



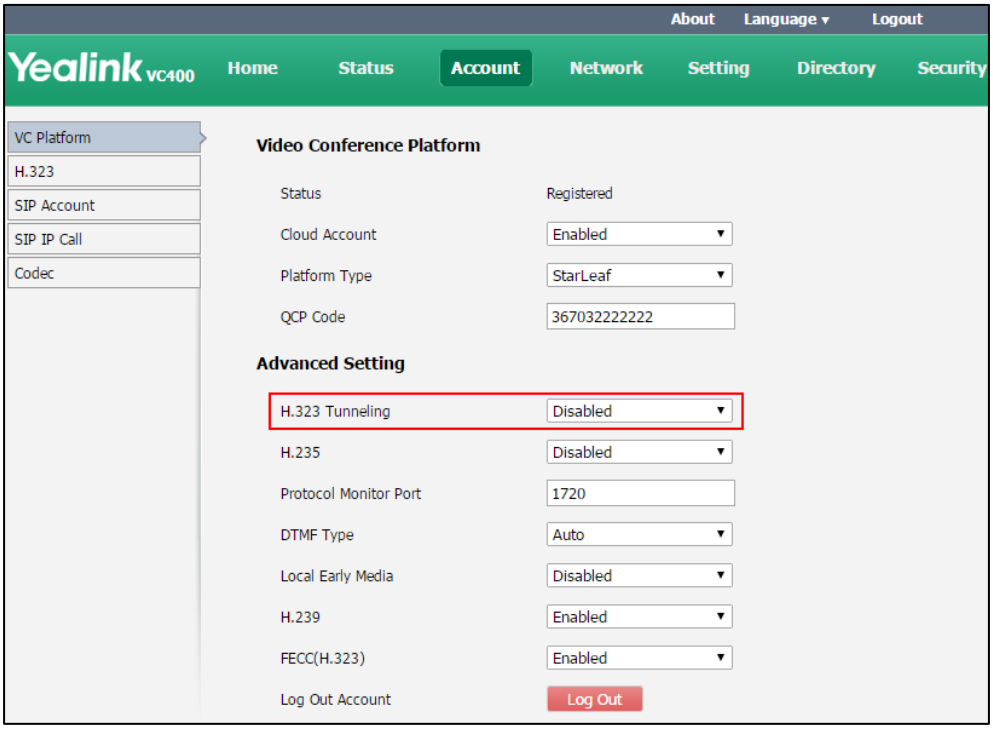
The parameter of the H.323 tunneling feature on the system is described below:

Parameter	Description	Configuration Method
H.323 Tunneling	Enables or disables the H.323 tunneling on the system. You can configure it for the StarLeaf Cloud platform or H.323 call separately. **Default:** Disabled	Remote Control Web User Interface

To configure the H.323 tunneling for StarLeaf Cloud platform via web user interface:

1. Click on **Account->VC Platform**.
2. Select **StarLeaf** from the pull-down list of **Platform Type**.

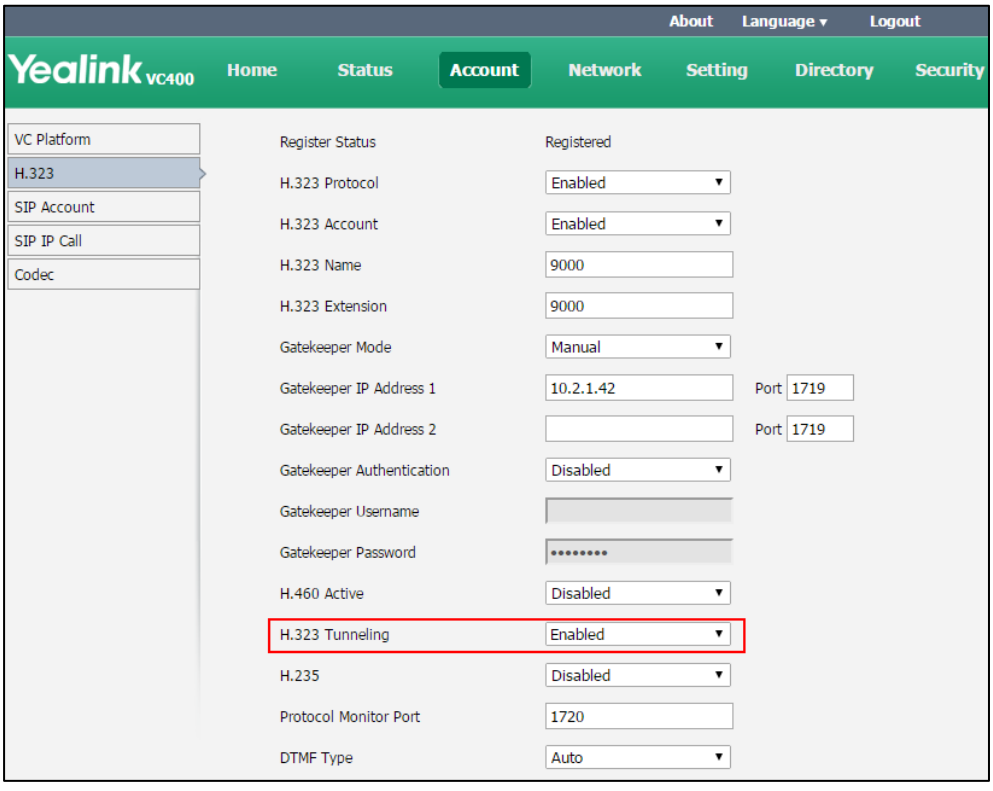
3. Select the desired value from the pull-down list of **H.323 Tunneling**.



4. Click **Confirm** to accept the change.

To configure H.323 tunneling for H.323 via web user interface:

1. Click on **Account**->**H.323**.
2. Select the desired value from the pull-down list of **H.323 Tunneling**.



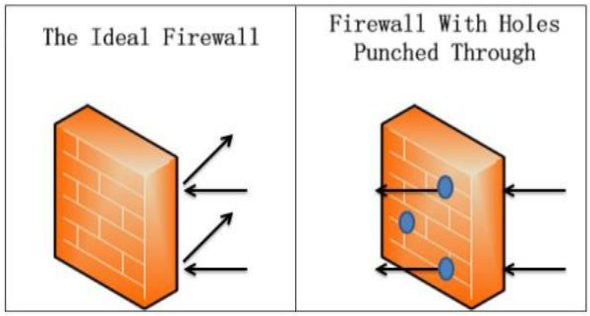
3. Click **Confirm** to accept the change.

To configure H.323 tunneling via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**H.323**.
2. Check the **H.323 Tunneling** checkbox.
3. Press the **Save** soft key to accept the change.

Configuring the System for Use with a Firewall or NAT

A firewall protects an organization's IP network by controlling data traffic from outside the network. Unless the firewall is designed to work with video conferencing equipment, you must configure the firewall to allow incoming and outgoing traffic to the VC400/VC120 system through the reserved ports. Users placing calls through a firewall to system may experience one-way audio or video if the firewall is not properly configured.



Call Setup and Media Ports

To place calls to other systems through the firewall, you must configure your firewall to allow incoming and outgoing traffic to the system through the following:

Description	Port Range	Port Type
H.323 register/call request	1719	UDP
H.323 call setup	1720	TCP
SIP (default transport protocol)	5060	UDP
SIP (when selecting the TCP transport protocol)	5060	TCP
SIP (when selecting the TLS transport protocol)	5061	TCP
Reserved ports on the system. For more information, refer to Restricting Reserved Ports on page 78.	50000-50499 (default range)	TCP/UDP

Description	Port Range	Port Type
HTTPS (Optional)	443	TCP

Restricting Reserved Ports

By default, the system communicates through TCP and UDP ports in the 50000 - 54999 range for video, voice, presentations, and camera control. The system uses only a small number of these ports during a call. The exact number depends on the number of participants in the call, the protocol used, and the number of ports required for the type of call: video or voice.

To minimize the number of UDP and TCP ports that are available for communication, you can restrict the ports range

The following tables identify the number of ports required per connection by protocol and the type of call.

Required ports for an H.323 two-way call:

Call Type	Number of Required Ports
Video	8 UDP ports (6 if presentation is disabled) 2 TCP ports
Voice	2 UDP ports 2 TCP ports
Each additional video participant requires 8 UDP ports and 2 TCP ports.	
Each additional audio participant requires 2 UDP ports and 2 TCP ports.	

Required ports for a SIP two-way call:

Call Type	Number of Required Ports
Video	8 UDP ports (5 if presentation is disabled)
Voice	2 UDP ports
Each additional video participant requires 8 UDP ports.	
Each additional audio participant requires 2 UDP ports.	

Make sure at least 200 TCP ports and 200 UDP ports are reserved for VC400&VC120. Use the following information as a guide when determining the range of port numbers.

System	Maximum Connections	Required Ports for an H.323 Call		Required Ports for a SIP Call	
VC400 without 8-way MCU	Four-way video call with a presentation and an audio call	26 UDP 8 TCP	50000-50025 50000-50007	26 UDP	50000-50025

System	Maximum Connections	Required Ports for an H.323 Call		Required Ports for a SIP Call	
VC120 without 8-way MCU	Two-way video call with a presentation and an audio call	10 UDP 4 TCP	50000-50009 50000-50003	10 UDP	50000-50009
VC400/VC120 with 8-way MCU	Eight-way video call with a presentation and an audio call	58 UDP 16 TCP	50000-50057 50000-50015	58 UDP	50000-50057

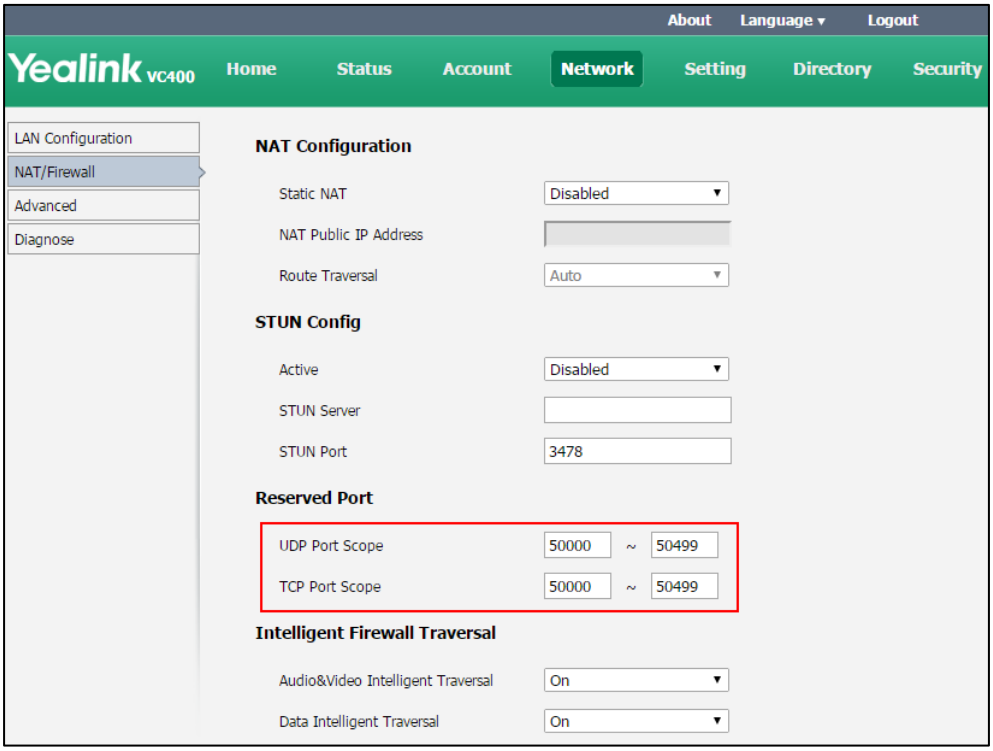
Parameters for reserved ports on the system are described below:

Parameter	Description	Configuration Method
UDP Port Scope	Configures the range of the UDP ports. **Valid values:** 1-65535 **Default range:** 50000-50499 **Note**: SIP and H.323 calls share the configured ports. If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
TCP Port Scope	Configures the range of the TCP ports. **Valid values:** 1-65535 **Default range:** 50000-50499 **Note**: SIP and H.323 calls share the configured ports. If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure reserved ports via web user interface:

1. Click on **Network**->**NAT/Firewall**.
2. In the **Reserve Port** block, configure the UDP port range in the **UDP Port Scope** field.

3. In the **Reserve Port** block, configure the TCP port range in the **TCP Port Scope** field.



4. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will be implemented after a reboot.

5. Click **Confirm** to reboot the system immediately.

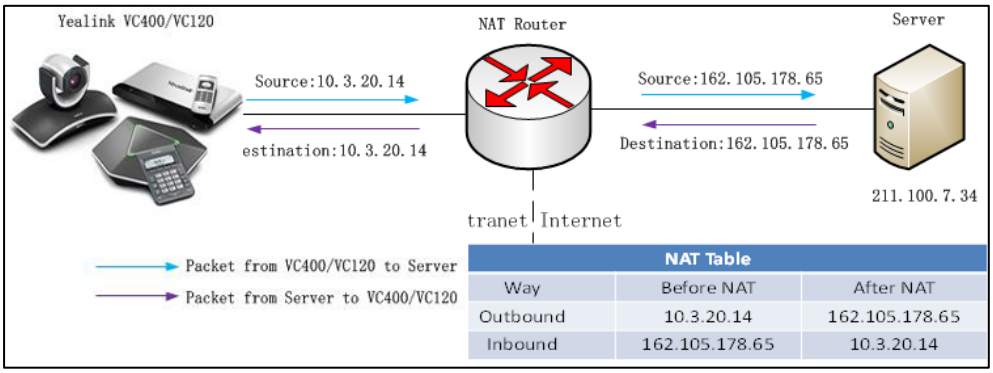
To configure reserved ports via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**NAT/Firewall**.
2. In the **Reserved** block, configure the range of the UDP ports and TCP ports.
3. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".
4. Select **OK** to reboot the system immediately.

Network Address Translation

If you choose to place your video conferencing systems in a private LAN, you must use NAT to communicate with outside systems. This may include enabling static NAT on your system.



Static NAT

NAT enables communication between devices on your LAN that have private IP addresses and devices that are accessed through a public IP network. Static NAT ensures that the same public IP address always maps to a system's private IP address so that data from the public network intended for the private system can be routed to the system reliably. If you are using static NAT to associate a public IP address with the private IP address of your system, you must configure your system to work with your static NAT server.

Note If H.460 firewall traversal is enabled on the system, the system will automatically ignore the static NAT settings for H.323 calls. For more information on H.460 firewall traversal, refer to on Enabling H.460 Support for H.323 Calls on page 135.

Static NAT feature parameters on the system are described below:

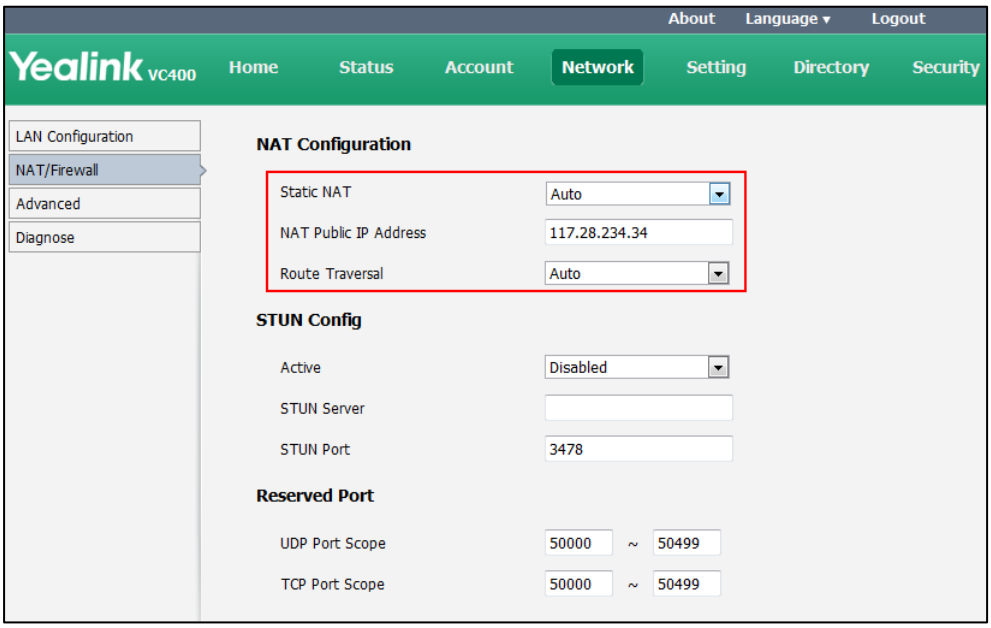
Parameter	Description	Configuration Method
Static NAT	Specifies the static NAT type. • **Disabled**–the system does not use the NAT feature. • **Manual**–the system uses the manually configured NAT public address. • **Auto**–the system obtains the NAT public address from the Yealink-supplied server. **Default:** Disabled	Remote Control Web User Interface
NAT Public IP Address	• Displays the NAT public	Remote Control

Parameter	Description	Configuration Method
	address automatically obtained from the Yealink-supplied server if the static NAT is set to **Auto**. ● Configures the NAT public address for the system if the static NAT is set to **Manual**.	Web User Interface
Route Traversal	Configures the route traversal type. ● **Auto**−NAT works only when making a call to public network or receiving a call from the public network. ● **Compulsory**−NAT works when you are in multi-level intranet network to solve the one-way audio or video problem. **Default:** Auto	Web User Interface
NAT Traversal	Configures the NAT traversal type. You can configure it for the SIP account or SIP IP call separately. ● **Disabled** ● **STUN** ● **StaticNat** **Default:** Disabled **Note:** Static NAT works only if this parameter is set to StaticNat.	Remote Control Web User Interface

To configure static NAT via web user interface:

1. Click on **Network**->**NAT/Firewall**.
2. Select the desired value from the pull-down list of **Static NAT**.
3. Configure the NAT public address in the **NAT Public IP Address** field if **Manual** is selected from the pull-down list of **Static NAT**.

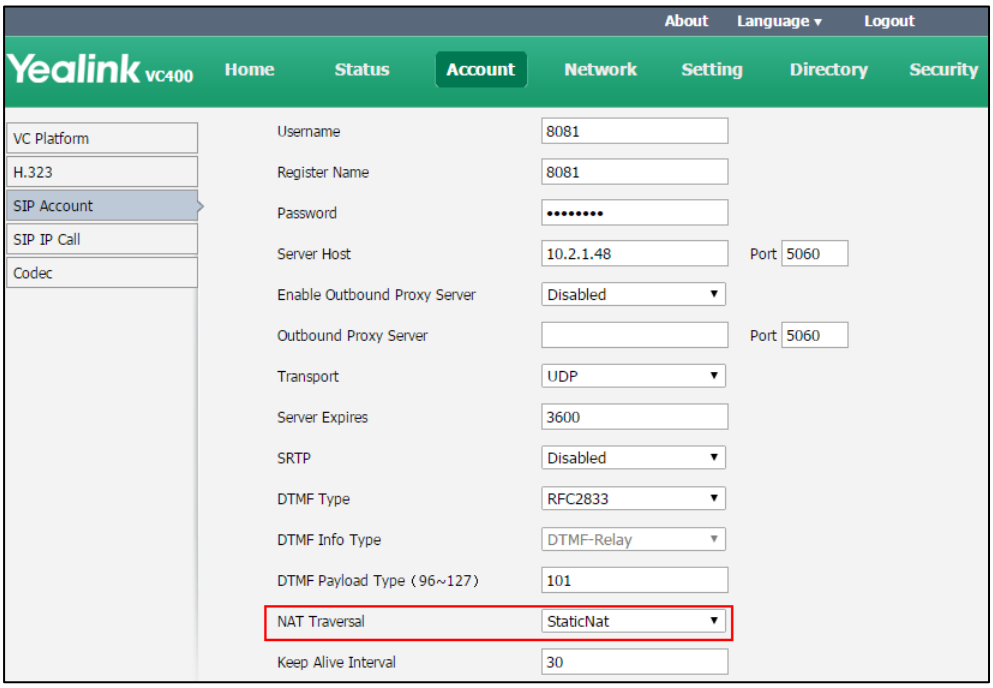
4. If multi-level intranet network has deployed in your environment, and you experience the one-way audio or video problem, select **Compulsory** from the pull-down list of **Route Traversal** to solve this problem.



5. Click **Confirm** to accept the change.

To configure Static NAT for SIP account via web user interface:

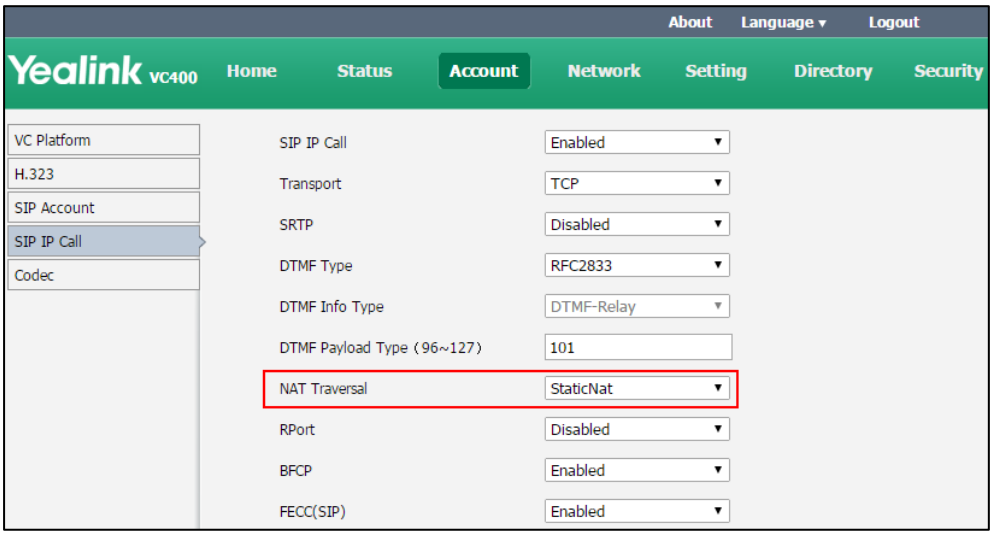
1. Click on **Account**->**SIP Account**.
2. Select **StaticNat** from the pull-down list of **NAT Traversal**.



3. Click **Confirm** to accept the change.

To configure Static NAT for SIP IP call via web user interface:

1. Click on **Account->SIP IP Call**.
2. Select **StaticNat** from the pull-down list of **NAT Traversal**.



3. Click **Confirm** to accept the change.

To configure static NAT via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**NAT/Firewall**.
2. Select the desired value from the pull-down list of **Type**.
3. Configure the NAT public address in the **Public IP Address** field if **Manual Settings** is selected from the pull-down list of **Type**.
4. Press the **Save** soft key to accept the change.

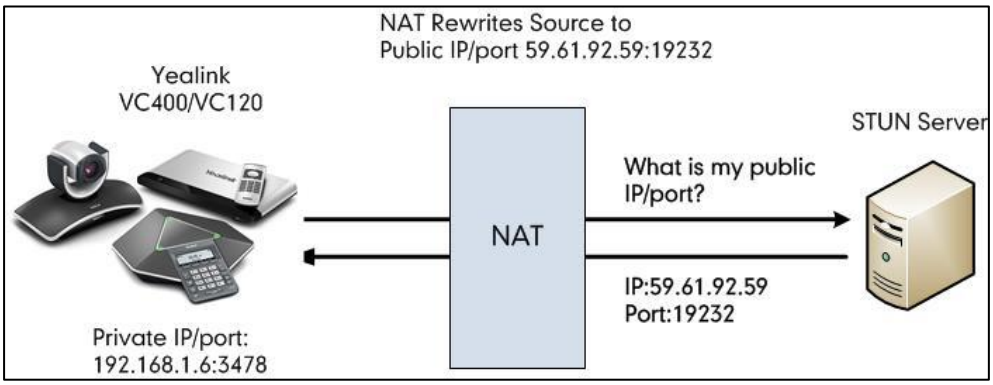
To configure static NAT for SIP IP call via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) **->SIP IP Call.**
2. Select **StaticNat** from the pull-down list of **NAT Traversal**.
3. Press the **Save** soft key to accept the change.

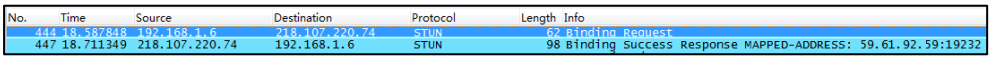
STUN

STUN is a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. The STUN protocol allows entities behind a NAT to first discover the presence of a NAT and the type of NAT (for more information on the NAT types, refer to NAT Types on page 88.) and to obtain the mapped (public) IP address and port number that the NAT has allocated for the UDP connections to remote parties. The protocol requires assistance from a third-party network server (STUN server) usually located on public Internet. The IP phone can be configured to work as a STUN client, to send exploratory STUN messages to the STUN server. The STUN server uses those messages to determine the public IP address and

port used, and then informs the client. For more information, refer to RFC3489.



Capturing packets after you enable the STUN feature, you can find that the VC400/VC120 sends Binding Request to the STUN server, and then mapped IP address and port is placed in the Binding Response: Binding Success Response MAPPED-ADDRESS: 59.61.92.59:19232.



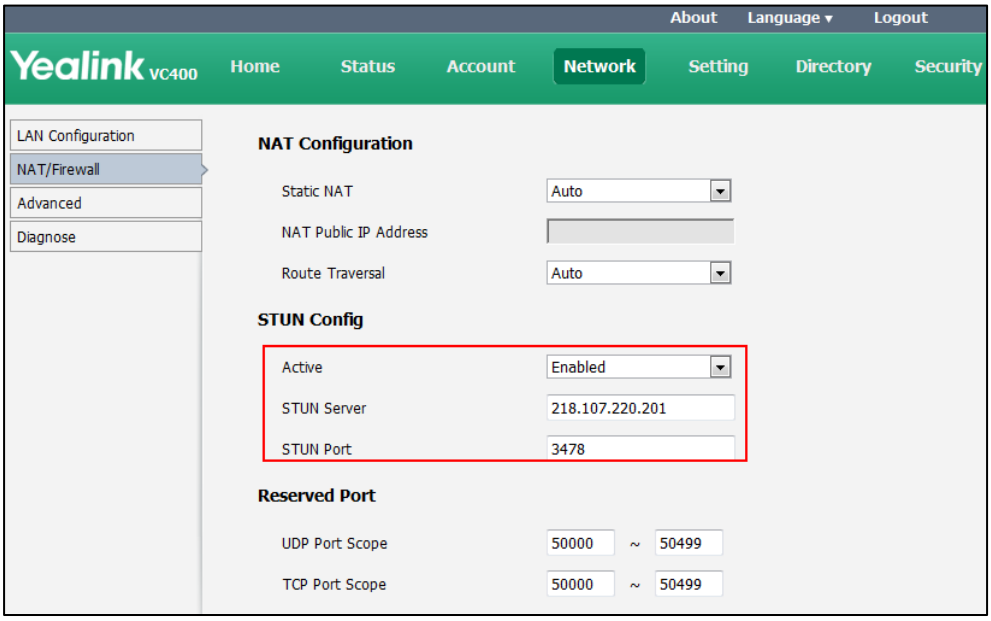
STUN feature parameters on the system are described below:

Parameter	Description	Configuration Method
Active	Enables or disables the STUN (Simple Traversal of UDP over NATs) feature on the system. **Default**: Disabled	Remote Control Web User Interface
STUN Server	Configures the IP address or the domain name of the STUN (Simple Traversal of UDP over NATs) server. **Default**: Blank	Remote Control Web User Interface
STUN Port	Configures the port of the STUN (Simple Traversal of UDP over NATs) server. **Default:** 3478	Remote Control Web User Interface
NAT Traversal	Configures the NAT traversal type. You can configure it for the SIP account or SIP IP call separately. • **Disabled** • **STUN** • **StaticNat** **Default:** Disabled	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Note: STUN works only if this parameter is set to STUN.	

To configure STUN server via web user interface:

1. Click on **Network**->**NAT/Firewall**.
2. In the **STUN Config** block, select the desired value from the pull-down list of **Active**.
3. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.
4. Enter the port of the STUN server in the **Port** field.

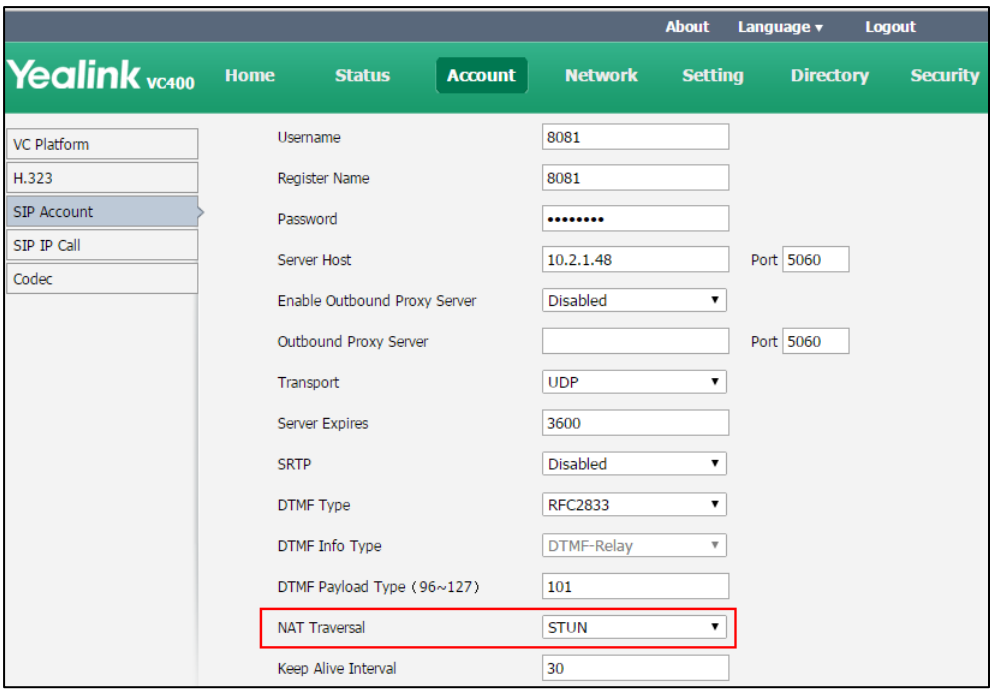


5. Click **Confirm** to accept the change.

To configure STUN for SIP account via web user interface:

1. Click on **Account**->**SIP Account**.

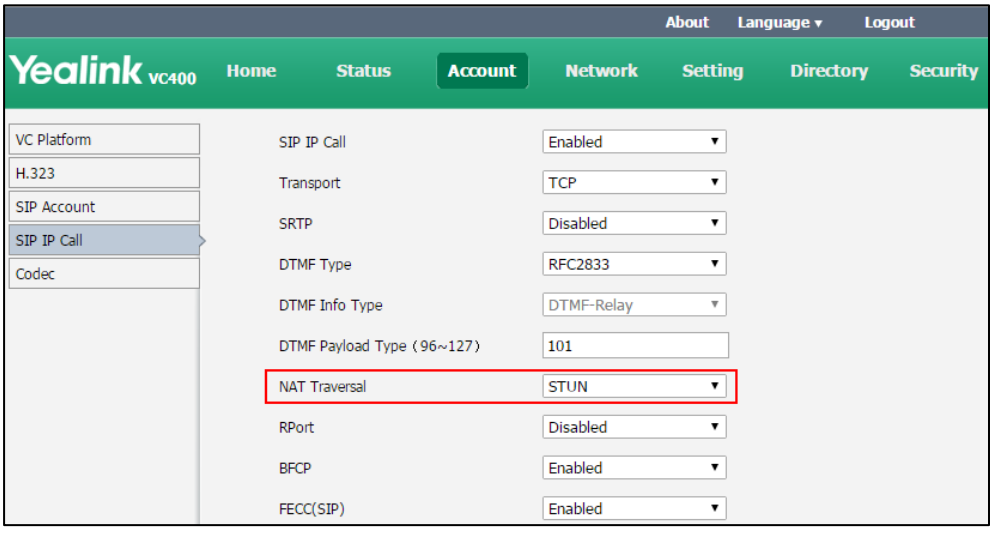
2. Select **STUN** from the pull-down list of **NAT Traversal**.



3. Click **Confirm** to accept the change.

To configure STUN for SIP IP call via web user interface:

1. Click on **Account**->**SIP IP Call**.
2. Select **STUN** from the pull-down list of **NAT Traversal**.



3. Click **Confirm** to accept the change.

To configure STUN server via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**NAT/Firewall**.
2. Check the **STUN Active** checkbox.
3. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.

4. Enter the port of the STUN server in the **Port** field.
5. Press the **Save** soft key to accept the change.

To configure STUN server for SIP IP call via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**SIP IP Call**.
2. Select **STUN** from the pull-down list of **NAT Traversal**.
3. Press the **Save** soft key to accept the change.

NAT Types

Full Cone:

A full cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Furthermore, any external host can send a packet to the internal host, by sending a packet to the mapped external address.

Restricted Cone:

A restricted cone NAT is one where all requests from the same internal IP address and port are mapped to the same external IP address and port. Unlike a full cone NAT, an external host (with IP address X) can send a packet to the internal host only if the internal host had previously sent a packet to IP address X.

Port Restricted Cone:

A port restricted cone NAT is like a restricted cone NAT, but the restriction includes port numbers. Specifically, an external host can send a packet, with source IP address X and source port P, to the internal host only if the internal host had previously sent a packet to IP address X and port P.

Symmetric:

A symmetric NAT is one where all requests from the same internal IP address and port, to a specific destination IP address and port, are mapped to the same external IP address and port. If the same host sends a packet with the same source address and port, but to a different destination, a different mapping is used. Furthermore, only the external host that receives a packet can send a UDP packet back to the internal host.

Rport

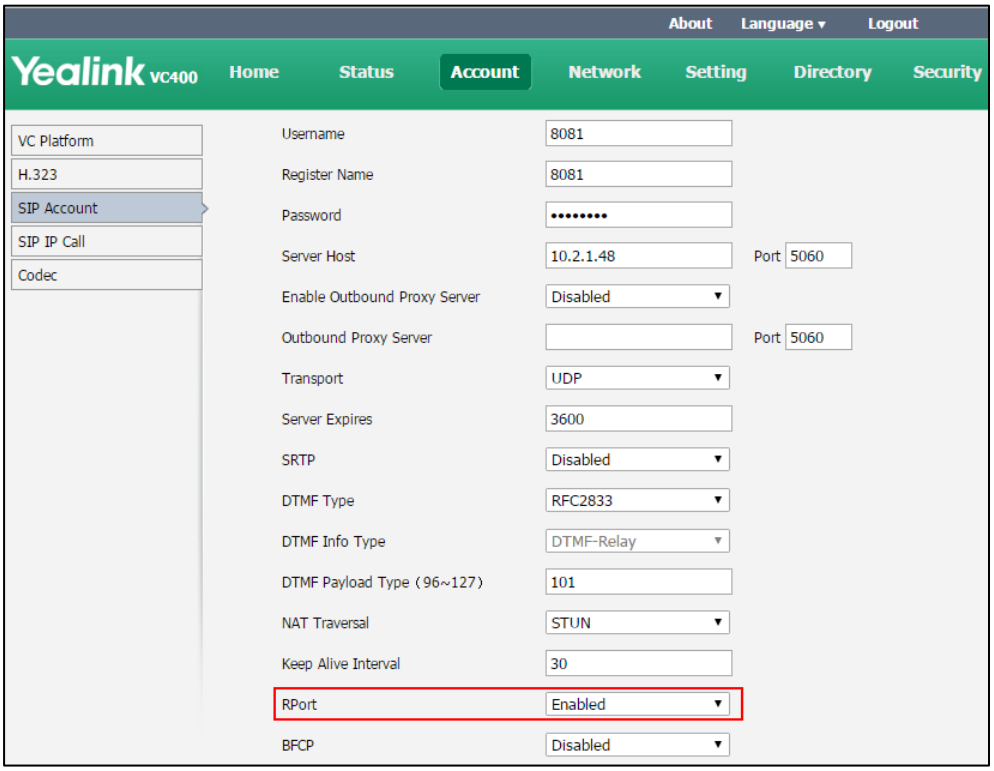
Rport in RFC 3581, allows a client to request that the server sends the response back to the source port from which the request came. Rport feature depends on support from a SIP server.

The rport parameter on the system is described below:

Parameter	Description	Configuration Method
RPort	Enables or disables NAT Rport feature. You can configure it for the SIP account or SIP IP call separately. **Default**: Enabled	Web User Interface

To configure rport feature for SIP account via web user interface:

1. Click on **Account**->**SIP Account**.
2. Select the desired value from the pull-down list of **RPort**.

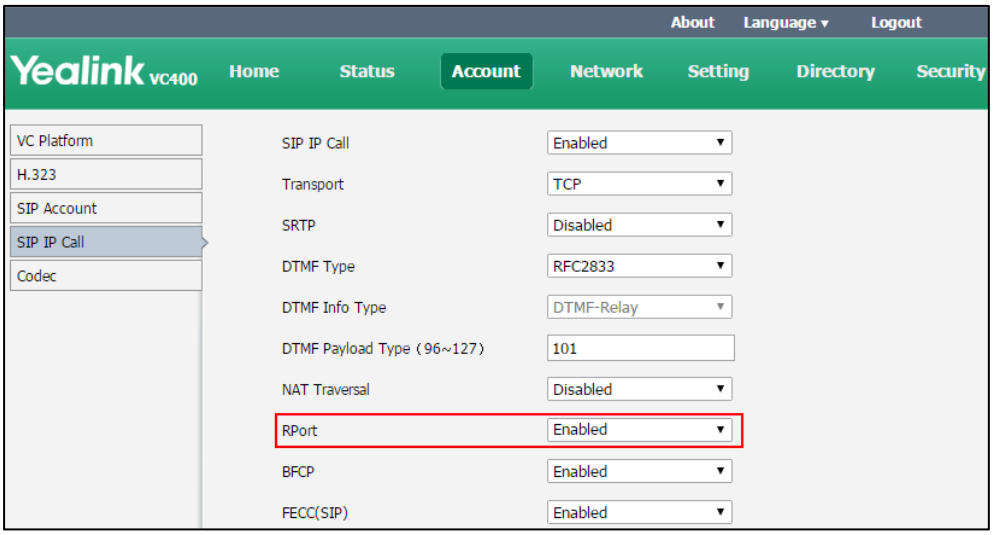


3. Click **Confirm** to accept the change.

To configure rport feature for SIP IP call via web user interface:

1. Click on **Account**->**SIP IP Call**.

2. Select the desired value from the pull-down list of **RPort**.



3. Click **Confirm** to accept the change.

Intelligent Firewall Traversal

The intelligent firewall traversal feature allows the VC400/VC120 system to check the media source address and port of incoming RTP packets, and then send back RTP packets to the address where incoming RTP packet comes from, instead of the address provided in the Session Description Protocol (SDP).

The following example illustrates a scenario for using intelligent firewall traversal:

The device A is located in the Intranet and the router does not support the ALG feature. The device B is located in the public network. A calls B, and then A sends the RTP packets to the B.

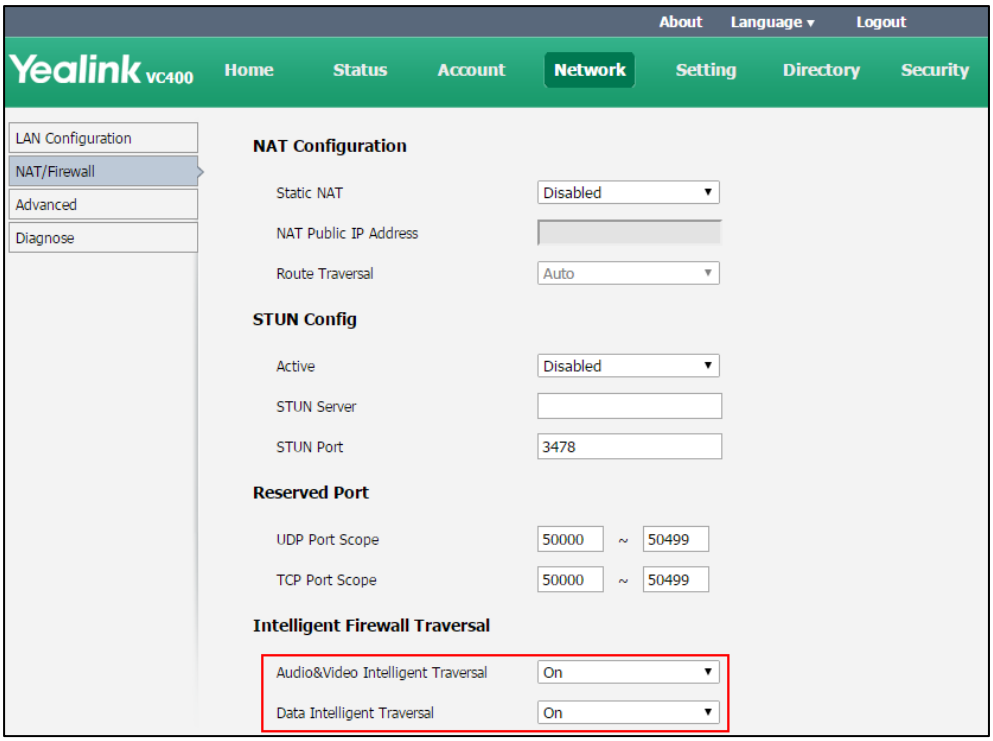
- If B enables the intelligent traversal feature, B sends back RTP packets to the address where incoming RTP packet comes from. A and B can communicate normally.
- If B disables the intelligent traversal feature, B sends RTP data to the private IP address of A, causing the device display of A appears black screen. To solve this problem, you need to enable the static NAT feature on the A device and configure the port mapping on the router.

The intelligent firewall traversal parameter is described below:

Parameter	Description	Configuration Method
Audio&Video Intelligent Traversal	Enables or disables the Audio&Video media stream to traverse firewall. **Default:** On	Web User Interface
Data Intelligent Traversal	Enables or disables the PC content and FECC protocol to traverse firewall. **Default:** On	Web User Interface

To configure intelligent firewall traversal via web user interface:

1. Click on **Network**->**NAT/Firewall**.
2. Select the desired value from the pull-down list of **Audio&Video Intelligent Traversal**.
3. Select the desired value from the pull-down list of **Data Intelligent Traversal**.



4. Click **Confirm** to accept the change.

Quality of Service

Quality of Service (QoS) is the ability to provide different priorities for different packets in the network. This allows the transport of traffic with special requirements. QoS guarantees are important for applications that require a fixed bit rate and are delay sensitive when the network capacity is insufficient. There are four major QoS factors to be considered when configuring a modern QoS implementation: bandwidth, delay, jitter and loss.

QoS provides a better network service through the following features:

- Supporting dedicated bandwidth
- Improving loss characteristics
- Avoiding and managing network congestion
- Shaping network traffic
- Setting traffic priorities across the network

The Best-Effort service is the default QoS model in the IP networks. It provides no guarantees for data delivery, which means delay, jitter, packet loss and bandwidth allocation are unpredictable. Differentiated Services (DiffServ or DS) is the most widely used QoS model. It provides a simple

and scalable mechanism for classifying and managing network traffic and providing QoS on modern IP networks. Differentiated Services Code Point (DSCP) is used to define DiffServ classes and is stored in the first six bits of the ToS (Type of Service) field. Each router on the network can provide QoS simply based on the DiffServ class. The DSCP value ranges from 0 to 63 with each DSCP specifying a particular per-hop behavior (PHB) applicable to a packet. A PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet.

Four standard PHBs available to construct a DiffServ-enabled network and achieve QoS:

- **Class Selector PHB** - backwards compatible with IP precedence. Class Selector code points are of the form "xxx000". The first three bits are the IP precedence bits. These class selector PHBs retain almost the same forwarding behavior as nodes that implement IP precedence-based classification and forwarding.
- **Expedited Forwarding PHB** - the key ingredient in DiffServ model for providing a low-loss, low-latency, low-jitter and assured bandwidth service.
- **Assured Forwarding PHB** - defines a method by which BAs (Bandwidth Allocations) can be given different forwarding assurances.
- **Default PHB** - specifies that a packet marked with a DSCP value of "000000" gets the traditional best effort service from a DS-compliant node.

VoIP is extremely bandwidth and delay-sensitive. QoS is a major issue in VoIP implementations, with regard to guaranteeing how that packet traffic is not delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee high-quality QoS only if the voice, video and data packets are given priority over other kinds of network traffic. Yealink video conferencing systems support the DiffServ model of QoS. DSCPs for voice, video and data packets that can be specified respectively.

Voice QoS

To make VoIP transmissions intelligible to receivers, voice packets should not be dropped, excessively delayed, or made to suffer varying delay. DiffServ model can guarantee high-quality voice transmission when the voice packets are configured to a higher DSCP value.

Video QoS

To ensure acceptable visual quality for video, video packets emanated from the system should be configured with a high transmission priority.

Data QoS

To ensure good call quality, data packets (e.g., SIP signaling and H.225 call signaling) emanated from the system should be configured with a high transmission priority.

QoS feature parameters on the system are described below.

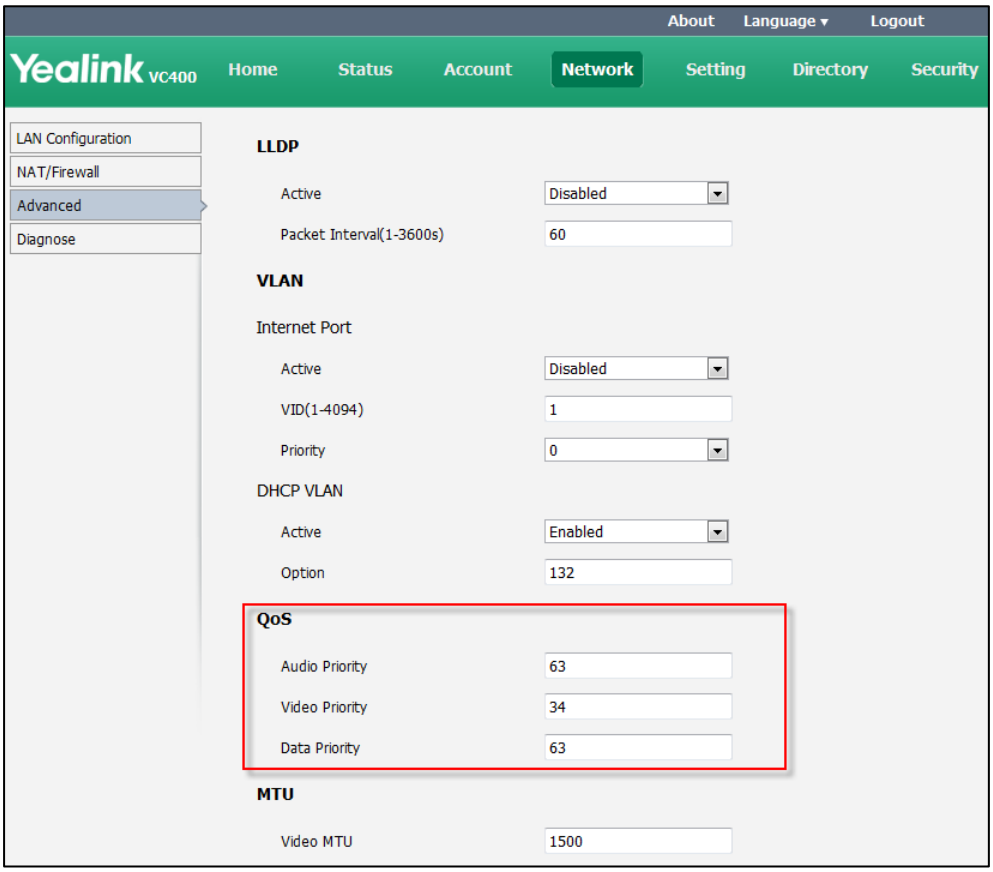
Parameter	Description	Configuration Method
Audio Priority	Specifies the DSCP value for voice	Remote Control

Parameter	Description	Configuration Method
	packets. **Valid Values: 0-63** **Default:** 63 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Video Priority	Specifies the DSCP value for video packets. **Valid Values: 0-63** **Default:** 34 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Data Priority	Specifies the DSCP value for data packets. **Valid Values: 0-63** **Default:** 63 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure QoS via web user interface:

1. Click on **Network**->**Advanced**.

2. In the **QoS** block, enter the desired values in the corresponding fields.



3. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.

4. Click **Confirm** to reboot the system immediately.

To configure QoS via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. In the **Diffserv QoS** block, enter the desired values in the corresponding fields.
3. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".

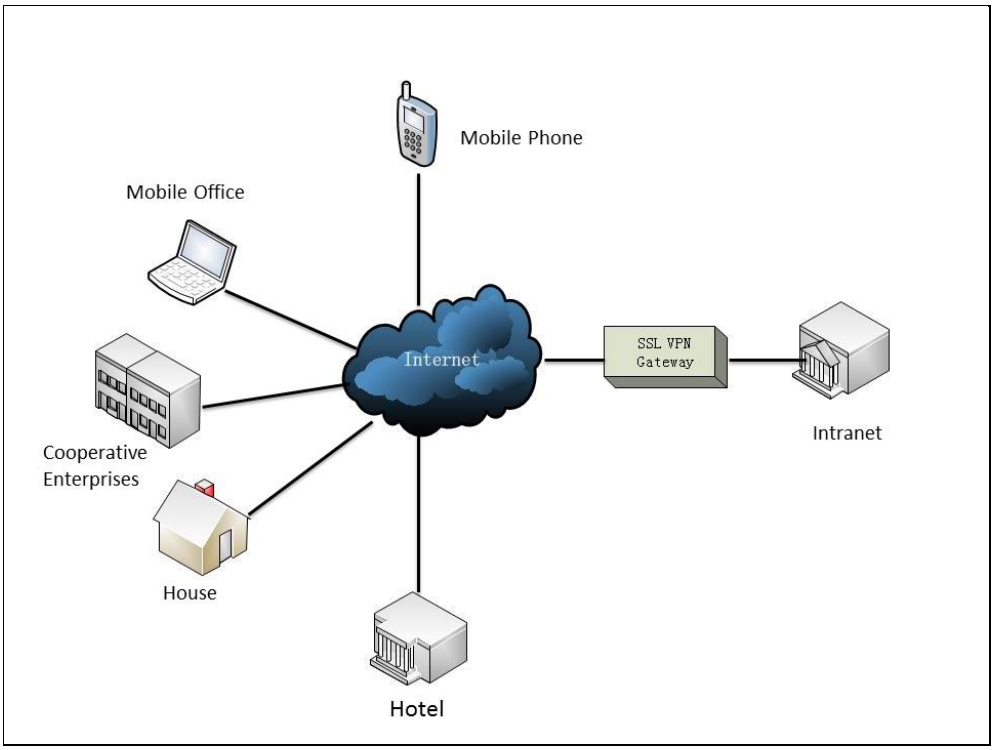
4. Select **OK** to reboot the system immediately.

VPN

VPN (Virtual Private Network) is a secured private network connection built on top of public telecommunication infrastructures, such as the Internet. VPN has become more prevalent due to the benefits of scalability, reliability, convenience and security. VPN provides remote offices or individual users with secure access to their organization's network. There are two types of VPN access: remote-access VPN (connecting an individual device to a network) and site-to-site VPN (connecting two networks together). Remote-access VPN allows employees to access their company's intranet from home or outside the office, and site-to-site VPN allows employees in

geographically separated offices to share one cohesive virtual network. VPN can also be classified by the protocols used to tunnel the traffic. It provides security through tunneling protocols: IPSec, SSL, L2TP and PPTP.

The system supports SSL VPN, which provides remote-access VPN capabilities through SSL. OpenVPN is a full featured SSL VPN software solution that creates secure connections in remote access facilities and is designed work with the TUN/TAP virtual networking interface. TUN and TAP are virtual network kernel devices. TAP simulates a link layer device and provides a virtual point-to-point connection, while TUN simulates a network layer device and provides a virtual network segment. The system uses OpenVPN to achieve the VPN feature. To prevent disclosure of private information, tunnel system must authenticate each other before secure VPN tunnel is established. After the VPN feature is configured properly on the system, the system acts as a VPN client and uses the certificates to authenticate the VPN server.



To use VPN, the compressed package of VPN-related files should be uploaded to the system in advance. The file format of the compressed package must be *.tar. The VPN-related files are: certificates (ca.crt and client.crt), key (client.key) and the configuration file (vpn.cnf) of the VPN client. For more information, refer to *OpenVPN Feature on Yealink IP Phones*.

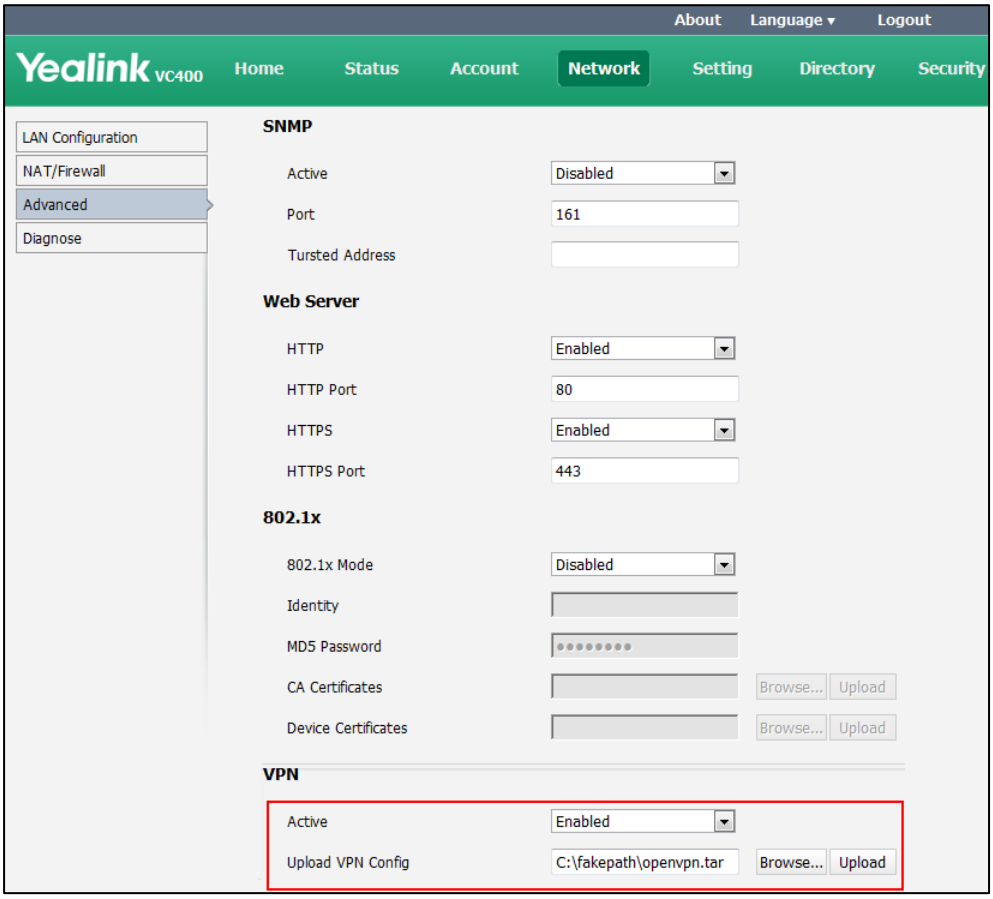
VPN feature parameters on the system are described below.

Parameter	Description	Configuration Method
VPN->Active	Enables or disables VPN feature on the system. **Default:** Disabled **Note**: You need to upload the compressed package of VPN-related	Remote Control Web User Interface

Parameter	Description	Configuration Method
	files to the system first before enabling the VPN feature. If you change this parameter, the system will reboot to make the change take effect.	
Upload VPN Config	Uploads the compressed package of VPN-related files (*.tar) to the system.	Web User Interface

To configure VPN via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **VPN** block, click **Browse** to locate the VPN file (*.tar) from your local system.
3. Click **Upload** to upload the file to the system.
4. Select the desired value from the pull-down list of **Active**.



5. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.
6. Click **Confirm** to reboot the system immediately.

To configure VPN via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Check the **VPN** checkbox.
3. Press the **Save** soft key to accept the change.

   The display device prompts “Reboot now?”.
4. Select **OK** to reboot the system immediately.

Configuring Call Preferences

This chapter provides information on how to configure system's call preferences (e.g., call protocol and network bandwidth).

This chapter provides the following sections:

- Configuring Video Conference Platform
- Configuring SIP Settings
- Configuring H.323 Settings
- DTMF
- Codecs
- Call Protocol
- Account Polling
- Do Not Disturb
- Auto Answer
- Auto Dialout Mute
- Call Match
- History Record
- Bandwidth
- Sharing Content
- Ringback Timeout
- Auto Refuse TimeoutSIP IP Call by Proxy
- Default LayoutPublic Mode

Configuring Video Conference Platform

Yealink video conferencing system can log into the Yealink VC Cloud Management Service/Yealink Meeting Server/StarLeaf/Zoom/Pexip/BlueJeans/Mind/Custom platform.

Users can access VMR using VC400&VC120 video conferencing system, whilst benefiting from both the features provided by video conferencing system, such as 1080p HD video and audio, and features provided by Yealink Meeting Server/StarLeaf/Zoom/BlueJeans/Pexip/Mind, including high end customization & interoperability.

You can obtain the account information from your administrator.

Logging into the Yealink VC Cloud Management Service Platform

Yealink VC400&VC120 video conferencing systems support Yealink Cloud accounts. The administrator uses the Yealink VC Cloud management service to assign each user an individual Yealink Cloud account. For more information, refer to *Yealink VC Cloud Management Service Administrator Guide*.

You can log into the Yealink VC Cloud Management Service platform, and dial other Yealink Cloud numbers to establish a conversation. If you want to place a call to a Yealink Cloud contact who is in the same Yealink Cloud directory as you, you can enter the 9-digit Cloud number or the extension (the last four Cloud number) to place a call. If you want to place a call to a Cloud contact who is in different Yealink Cloud directory from you, you should enter the 9-digit Cloud number to place a call.

Yealink VC Cloud Management Service platform parameters on the system are described below:

Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot log into the Yealink VC Cloud Management Service Platform.	Remote Control Web User Interface
Platform Type	Configures the platform type. • Yealink VC Cloud Management Service • Yealink Meeting Server • StarLeaf • Zoom • Pexip • BlueJeans • Mind • Custom **Default**: Yealink VC Cloud Management Service	Remote Control Web User Interface
Login Type	Specifies the method to log into the Yealink VC Cloud Management Service platform. • **PIN Code Login**: This method	Remote Control Web User Interface

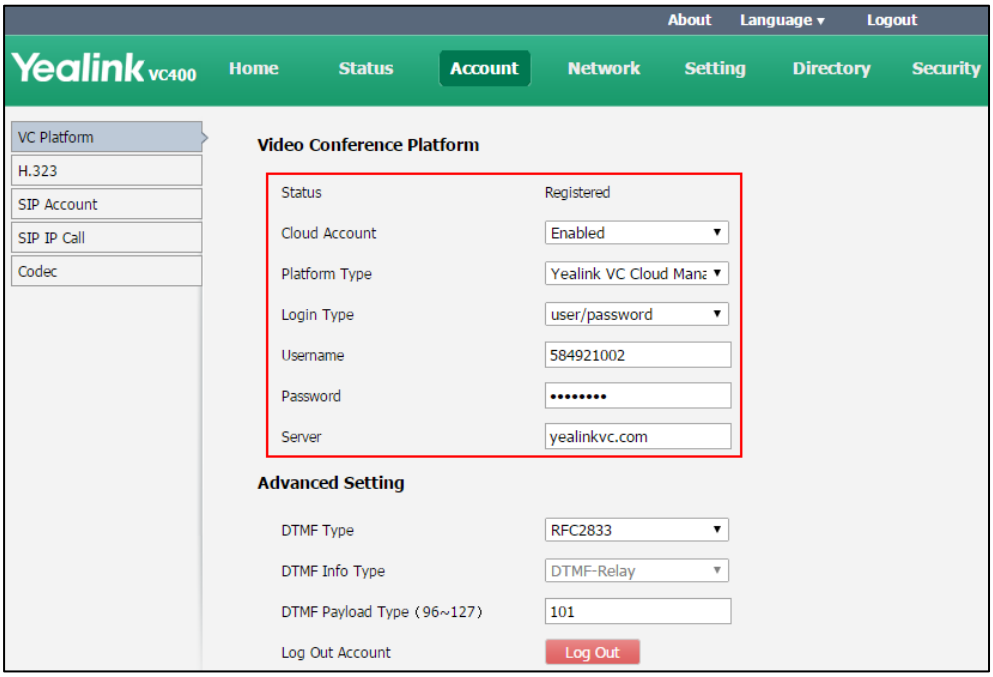
Parameter	Description	Configuration Method
	uses the user's PIN code to log into the Yealink VC Cloud Management Service platform. The PIN code consists of 9 digits. You can only use the PIN code once and it will expire if unused for 7 days. Contact Cloud administrator when it expires. • **user/password**: This method uses the user's Yealink Cloud number and password to log into the Yealink VC Cloud Management Service platform. • **Build-in Cloud Number**: This method uses build-in Cloud number to log into the Yealink VC Cloud Management Service platform. The number consists of 7 digits that are generated according to MAC address, and it never expires. **Default**: PIN Code Login	
Pincode/Pin Code	Specifies the PIN code to log into the Yealink VC Cloud Management Service platform. **Default**: Blank **Note:** It only works if the value of **Login Type** is set to **PIN Code Login**.	Remote Control Web User Interface
Username	Specifies the user name to log into the Yealink VC Cloud Management Service platform. **Default**: Blank **Note:** It only works if the value of **Login Type** is set to **user/password**.	Remote Control Web User Interface
Password	Specifies the password associated with the user name when signing into the Yealink VC Cloud Management Service platform. **Default**: Blank	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Note: It only works if the value of **Login Type** is set to **user/password**.	
Server	Configures the IP address or domain name of the Yealink VC Cloud Management Service platform. **Default**: yealinkvc.com	Remote Control Web User Interface
Remember Me	Enables or disables the system to remember the registration information. **Default:** ON **Note:** If it is on, user name and password will be filled automatically next time. It only works if the value of **Login Type** is set to **Username/Password**.	Remote Control

To configure Yealink VC Cloud Management Service platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Enabled** from the pull-down list of **Cloud Account**.
3. Select **Yealink VC Cloud Management Service** from the pull-down list of **Platform Type**.
4. Select the desired sign-in method from the pull-down list of **Login Type**.
   - Select **Build-in Cloud Number**.
   - If you select **PIN Code Login**, enter your PIN code in the **Pin Code** field.
   - If you select **user/password**, enter your Cloud number and password in the corresponding fields.

5. Enter the IP address or domain name of the Yealink VC Cloud Management Service platform in the **Server** field.



6. Click **Confirm** to accept the change.

To configure Yealink VC Cloud Management Service platform via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **Yealink VC Cloud Management Service** from the pull-down list of **Platform Type**.
4. Enter the IP address or domain name of the Yealink VC Cloud Management Service platform in the **Server** field.
5. Select the desired sign-in method from the pull-down list of **Login Type**.

   - If you select **Build-in Cloud Number**:

     Press ▲or ▼to scroll to **Onekey Login**, and then press OK.

   - If you select **Pincode Login:**

     Enter your PIN code in the **Pincode** field, press ▲ or ▼ to scroll to **Log In**, and then press OK.

   - If you select **Username/Password**:

     Enter your Cloud number and password in the corresponding fields. You can also check the **Remember Me** checkbox to remember your username and password.

     Press ▲or ▼to scroll to **Log In**, and then press OK.

After successful registration, the display device displays , and the LCD screen of the video conferencing phone displays .

Note

A Yealink Cloud account can be used to log into five Cloud systems at most simultaneously.

If you log into Yealink VC Cloud Management Service platform using the built-in Cloud number, your directory will not include the Yealink Cloud contacts, but you can dial other Yealink Cloud numbers to establish a conversation.

Registering a YMS Account

Yealink VC400/VC120 video conferencing systems support YMS accounts. The administrator uses the Yealink Meeting Server (YMS) to assign each user an individual YMS account. For more information on how to add YMS accounts, refer to *Yealink Meeting Server Administrator Guide*.

When you are using the YMS account, you can:

- Dial the other YMS accounts to establish a conversation.
- View or join the scheduled conferences.
- Enter the permanent VMR.

For detailed introduction, refer to *Video Conferencing System User Guide*.

Yealink Meeting Server parameters on the system are described below:

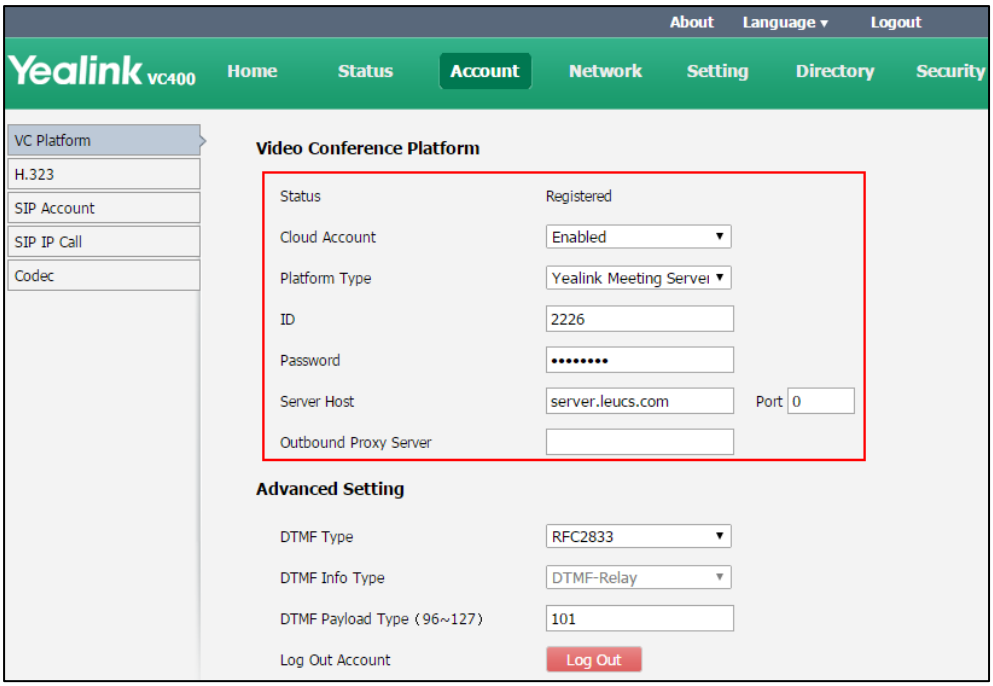
Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot register the YMS account.	Remote Control Web User Interface
Platform Type	Configures the platform type. • Yealink VC Cloud Management Service • Yealink Meeting Server • StarLeaf • Zoom • Pexip • BlueJeans • Mind • Custom **Default**: Yealink VC Cloud Management Service	Remote Control Web User Interface

Parameter	Description	Configuration Method
ID	Specifies the ID when registering a YMS account. **Default**: Blank	Remote Control Web User Interface
Password	Specifies the password associated with the ID when registering a YMS account. **Default**: Blank	Remote Control Web User Interface
Server Host	Configures the IP address or domain name of the Yealink Meeting Server. **Default**: Blank	Remote Control Web User Interface
Port	Configures the port of the Yealink Meeting Server. **Default**: 0	Web User Interface
Outbound Server/Outbound Proxy Server	Configures the IP address or domain name of the outbound proxy server. **Default:** Blank	Remote Control Web User Interface
Remember Password	Enables or disables the system to remember the registration information. **Default:** ON **Note:** If it is on, other registration information will be filled automatically when you enter the ID next time.	Remote Control

To configure Yealink Meeting Server via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Enabled** from the pull-down list of **Cloud Account**.
3. Select **Yealink Meeting Server** from the pull-down list of **Platform Type**.

4. Configure the YMS account settings.



5. Click **Confirm** to accept the change.

To configure Yealink Meeting Server via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **Yealink Meeting Server** from the pull-down list of **Platform Type**.
4. Configure the YMS account settings.
5. Check the **Remember Password** checkbox to remember your registration information.
6. Press ▲or ▼to scroll to **Register**, and then press OK.
   After successful registration, the display device displays , and the LCD screen of the video conferencing phone displays .

Note

A YMS account can be used to log into five Cloud systems at most simultaneously.

If administrator enabled the **Device upgrade** feature on Yealink Meeting Server, video conferencing systems that log into the Yealink Meeting Server will upgrade firmware automatically once the current firmware version is different from the one on Yealink Meeting Server.

Logging into the StarLeaf Cloud Platform

You can log into the StarLeaf Cloud platform.

When you place a call using the StarLeaf Cloud account, you can:

- Call the other StarLeaf Cloud account to establish a point to point call.

- Call the conference ID to join the Virtual Meeting Rooms.
- Call between StarLeaf Cloud account and Microsoft Skype for Business/Lync account.

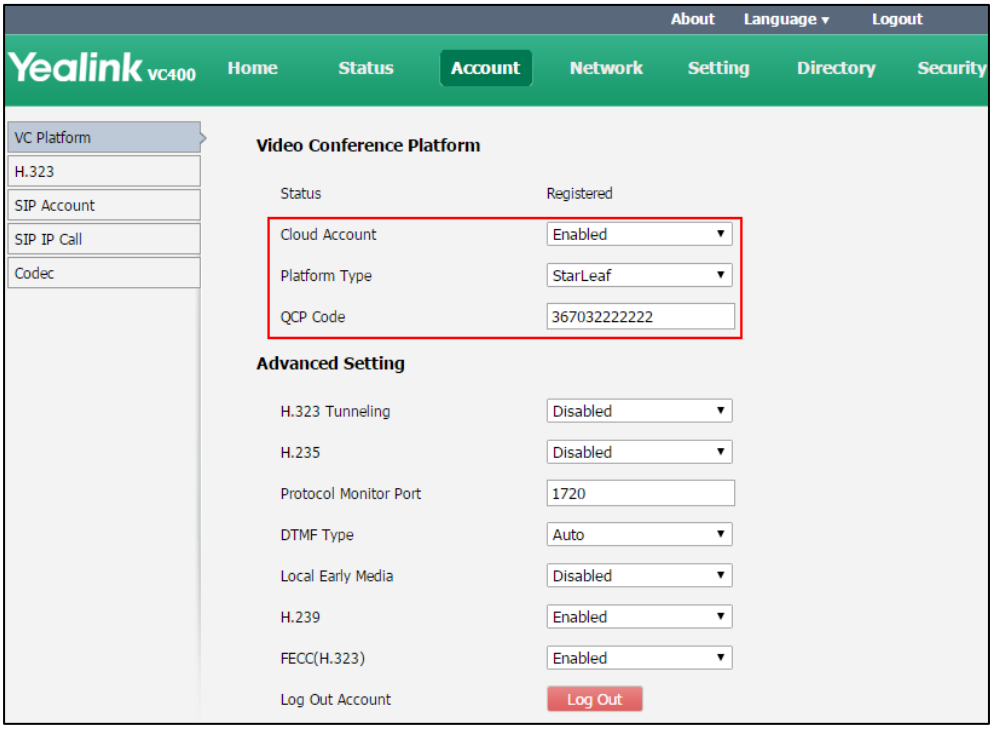
StarLeaf platform parameters on the system are described below:

Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot log into the StarLeaf Cloud platform.	Remote Control Web User Interface
Platform Type	Configures the platform type. ● Yealink VC Cloud Management Service ● Yealink Meeting Server ● StarLeaf ● Zoom ● Pexip ● BlueJeans ● Mind ● Custom **Default**: Yealink VC Cloud Management Service	Remote Control Web User Interface
QCP Code	Specifies the quick access code to log into the StarLeaf Cloud platform. **Default**: Blank	Remote Control Web User Interface

To configure StarLeaf Cloud platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Enabled** from the pull-down list of **Cloud Account**.
3. Select **StarLeaf** from the pull-down list of **Platform Type**.

4. Configure the StarLeaf Cloud platform.



5. Click **Confirm** to accept the change.

To configure StarLeaf Cloud platform via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **StarLeaf** from the pull-down list of **Platform Type**.
4. Enter the 12-digit quick access code in the **QCP Code** field.
5. Press ▲or ▼ to scroll to **Log In**, and then press OK.
   After successful registration, the display device displays , and the LCD screen of the video conferencing phone displays .

Note Systems that log into the StarLeaf Cloud platform will upgrade firmware automatically once the current firmware version is different from the one on StarLeaf Server.

Logging into the Zoom Cloud Platform

You can log into the Zoom Cloud platform and join the VMR.

Zoom Cloud platform parameters on the system are described below:

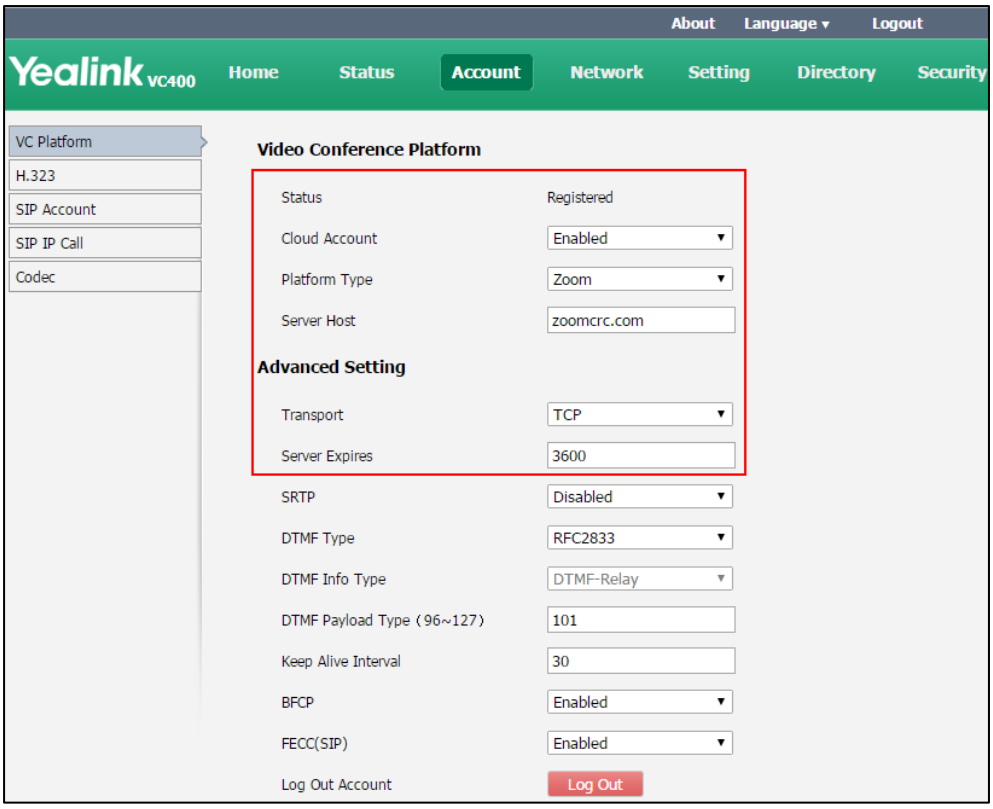
Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature.	Remote Control

Parameter	Description	Configuration Method
	Default: Enabled **Note:** If it is disabled, the system cannot log into the Zoom Cloud platform.	Web User Interface
Platform Type	Configures the platform type. ● Yealink VC Cloud Management Service ● Yealink Meeting Server ● StarLeaf ● Zoom ● Pexip ● BlueJeans ● Mind ● Custom **Default**: Yealink VC Cloud Management Service	Remote Control Web User Interface
Server/Server Host	Configures the IP address or domain name of the Zoom Cloud server. **Default**: zoomcrc.com	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the Zoom Cloud platform. ● **UDP**–provides best-effort transport via UDP for SIP signaling. ● **TCP**–provides reliable transport via TCP for SIP signaling. ● **TLS**–provides secure communication of SIP signaling. ● **DNS-NAPTR**–performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** TCP	Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the Cloud server. **Default:**3600	Web User Interface

Parameter	Description	Configuration Method
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. **Default:** 30	Web User Interface

To configure Zoom Cloud platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Enabled** from the pull-down list of **Cloud Account**.
3. Select **Zoom** from the pull-down list of **Platform Type**.
4. Configure the Zoom Cloud platform.



5. Click **Confirm** to accept the change.

To configure Zoom Cloud platform via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **Zoom** from the pull-down list of **Platform Type**.
4. Enter the domain name or IP address of Zoom server in the **Server** field.

   The default Zoom server is "zoomcrc.com".

5. Press ▲or ▼to scroll to **Log In**, and then press OK.
After successful registration, the display device displays , and the LCD screen of the video conferencing phone displays .

Registering a Pexip Account

You can register the Pexip account.

When you place a call using the Pexip account, you can:

- Call the device alias to establish a point to point call.
- Call the aliases to join the Virtual Meeting Rooms, Virtual Auditoriums or Virtual Receptions.
- Call between Pexip account and Microsoft Skype for Business/Lync account.

Pexip platform parameters on the system are described below:

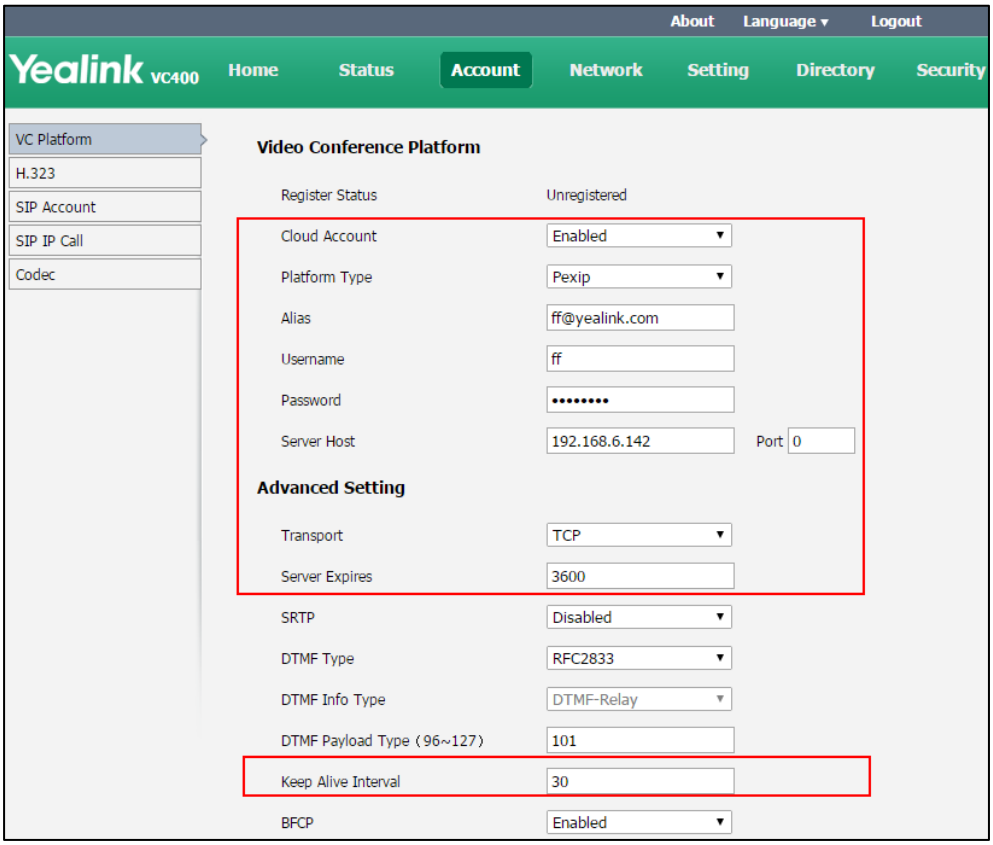
Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot register the Pexip account.	Remote Control Web User Interface
Platform Type	Configures the platform type. • Yealink VC Cloud Management Service • Yealink Meeting Server • StarLeaf • Zoom • Pexip • BlueJeans • Mind • Custom **Default**: Yealink VC Cloud Management Service	Remote Control Web User Interface
Alias	Specifies the alias when registering a Pexip account. **Default**: Blank	Remote Control Web User Interface
Username	Specifies the user name when registering a Pexip account. **Default**: Blank	Remote Control Web User Interface

Parameter	Description	Configuration Method
Password	Specifies the password associated with the user name when registering a Pexip account. **Default**: Blank	Remote Control Web User Interface
Server/Server Host	Configures the IP address or domain name of the Pexip server. **Default**: Blank	Remote Control Web User Interface
Port	Configures the port of the Pexip server. **Default**: 0	Web User Interface
Transport	Configures the type of transport protocol for the Pexip platform. ● **UDP**–provides best-effort transport via UDP for SIP signaling. ● **TCP**–provides reliable transport via TCP for SIP signaling. ● **TLS**–provides secure communication of SIP signaling. ● **DNS-NAPTR**–performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** TCP	Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the Cloud server. **Default:**3600	Web User Interface
Remember Password	Enables or disables the system to remember the registration information. **Default:** ON **Note:** If it is on, other registration information will be filled automatically when you enter the alias next time.	Remote Control
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So	Web User Interface

Parameter	Description	Configuration Method
	that the registry server will keep the connection open with the client. **Default:** 30	

To configure Pexip platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Enabled** from the pull-down list of **Cloud Account**.
3. Select **Pexip** from the pull-down list of **Platform Type**.
4. Configure the Pexip account settings.



5. Click **Confirm** to accept the change.

To configure Pexip platform via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **Pexip** from the pull-down list of **Platform Type**.
4. Configure the Pexip account settings.
5. Check the **Remember Password** checkbox to remember your registration information.
6. Press ▲ or ▼ to scroll to **Register**, and then press OK.

After successful registration, the display device displays , and the LCD screen of the video conferencing phone displays .

Note You can also register the Pexip account using SIP or H.323 protocol.
For more information, refer to Configuring SIP Settings on page 126 and Configuring H.323 Settings on page130

Logging into the BlueJeans Cloud Platform

You can log into the BlueJeans Cloud platform and join the VMR.

BlueJeans Cloud platform parameters on the system are described below:

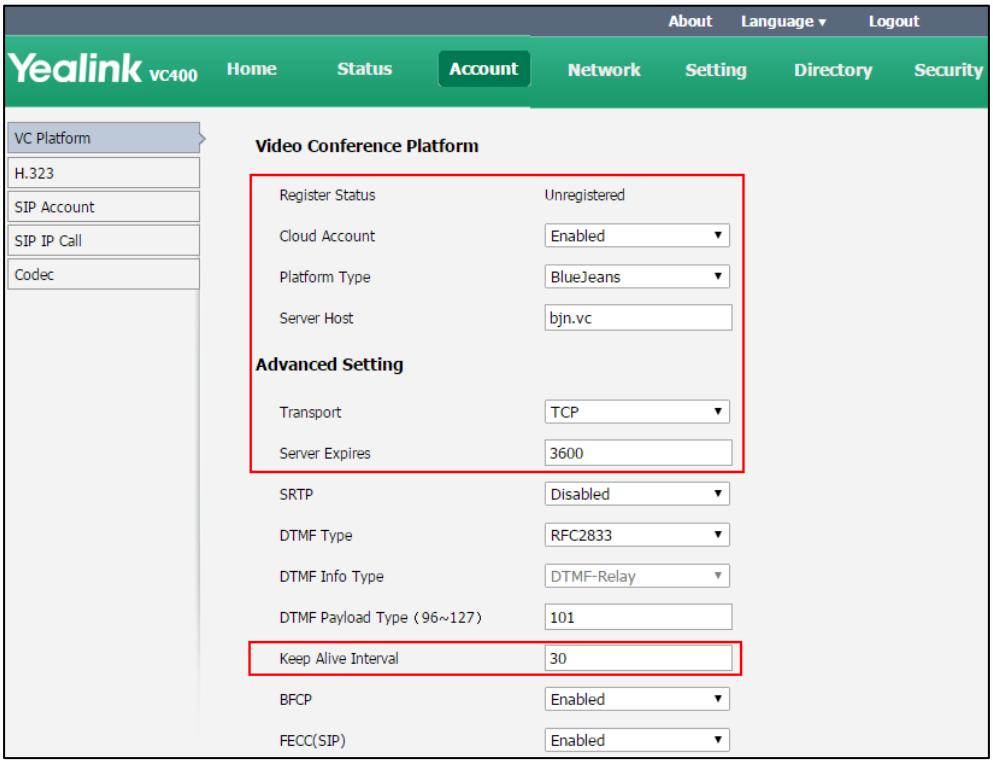
Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot log into the BlueJeans Cloud platform.	Remote Control Web User Interface
Platform Type	Configures the platform type. • Yealink VC Cloud Management Service • Yealink Meeting Server • StarLeaf • Zoom • Pexip • BlueJeans • Mind • Custom **Default**: Yealink VC Cloud Management Service	Remote Control Web User Interface
Server/Server Host	Configures the IP address or domain name of the BlueJeans server. **Default**: bjn.vc	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the BlueJeans Cloud platform. • **UDP**–provides best-effort transport via UDP for SIP	Web User Interface

Parameter	Description	Configuration Method
	signaling. • **TCP**—provides reliable transport via TCP for SIP signaling. • **TLS**—provides secure communication of SIP signaling. • **DNS-NAPTR**—performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** TCP	
Server Expires	Configures the registration expiration time (in seconds) of the Cloud server. **Default:**3600	Web User Interface
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. **Default:** 30	Web User Interface

To configure BlueJeans Cloud platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Enabled** from the pull-down list of **Cloud Account**.
3. Select **BlueJeans** from the pull-down list of **Platform Type**.

4. Configure the BlueJeans Cloud platform.



5. Click **Confirm** to accept the change.

To configure BlueJeans Cloud platform via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **BlueJeans** from the pull-down list of **Platform Type**.
4. Enter the domain name or IP address of BlueJeans server in the **Server** field.

   The default BlueJeans server is "bjn.vc".
5. Press ▲or ▼to scroll to **Log In**, and then press OK.

   After successful registration, the display device displays , and the LCD screen of the video conferencing phone displays .

Logging into the Mind Platform

You can log into the Mind platform and join the VMR.

Mind platform parameters on the system are described below:

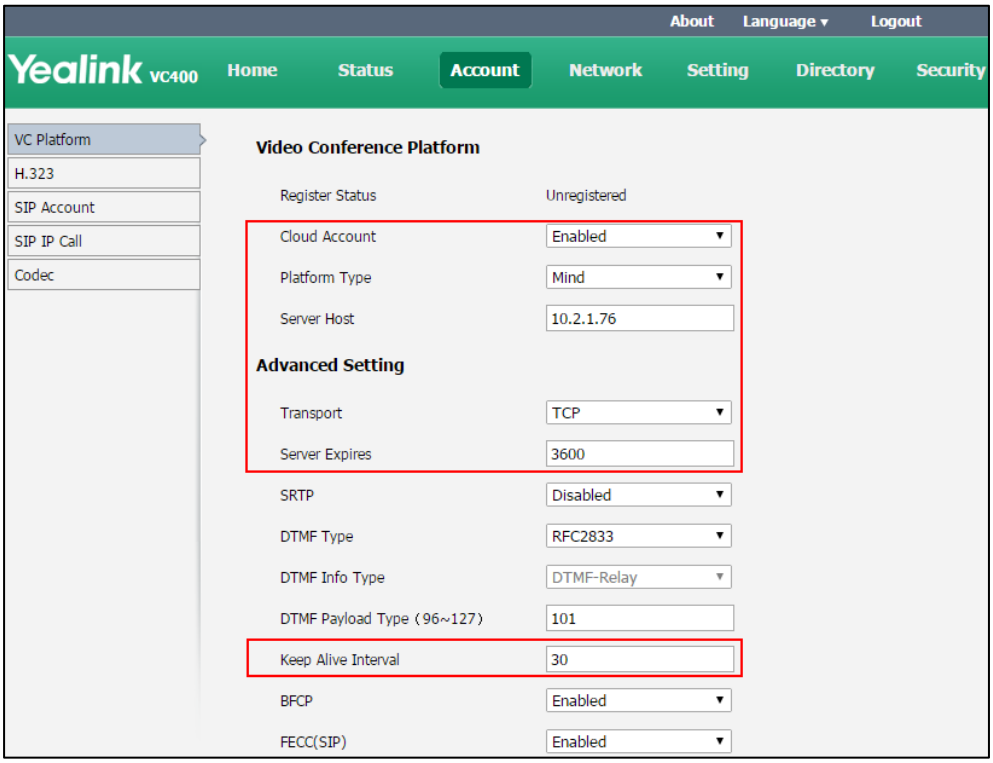
Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system	Remote Control Web User Interface

Parameter	Description	Configuration Method
	cannot log into the Mind platform.	
Platform Type	Configures the platform type. ● Yealink VC Cloud Management Service ● Yealink Meeting Server ● StarLeaf ● Zoom ● Pexip ● BlueJeans ● Mind ● Custom **Default**: Yealink VC Cloud Management Service	Remote Control Web User Interface
Server/Server Host	Configures the IP address or domain name of the Mind server. **Default**: Blank	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the Mind platform. ● **UDP**–provides best-effort transport via UDP for SIP signaling. ● **TCP**–provides reliable transport via TCP for SIP signaling. ● **TLS**–provides secure communication of SIP signaling. ● **DNS-NAPTR**–performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** TCP	Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the Cloud server. **Default:**3600	Web User Interface
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive	Web User Interface

Parameter	Description	Configuration Method
	messages to the registry server. So that the registry server will keep the connection open with the client. **Default:** 30	

To configure Mind platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Enabled** from the pull-down list of **Cloud Account**.
3. Select **Mind** from the pull-down list of **Platform Type**.
4. Configure the Mind platform.



5. Click **Confirm** to accept the change.

To configure Mind platform via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **Mind** from the pull-down list of **Platform Type**.
4. Enter the domain name or IP address of Mind server in the **Server** field.
5. Press ▲or ▼ to scroll to **Log In**, and then press OK.
   After successful registration, the display device displays , and the LCD screen of the video conferencing phone displays .

Registering a Custom Account

You can register a custom account.

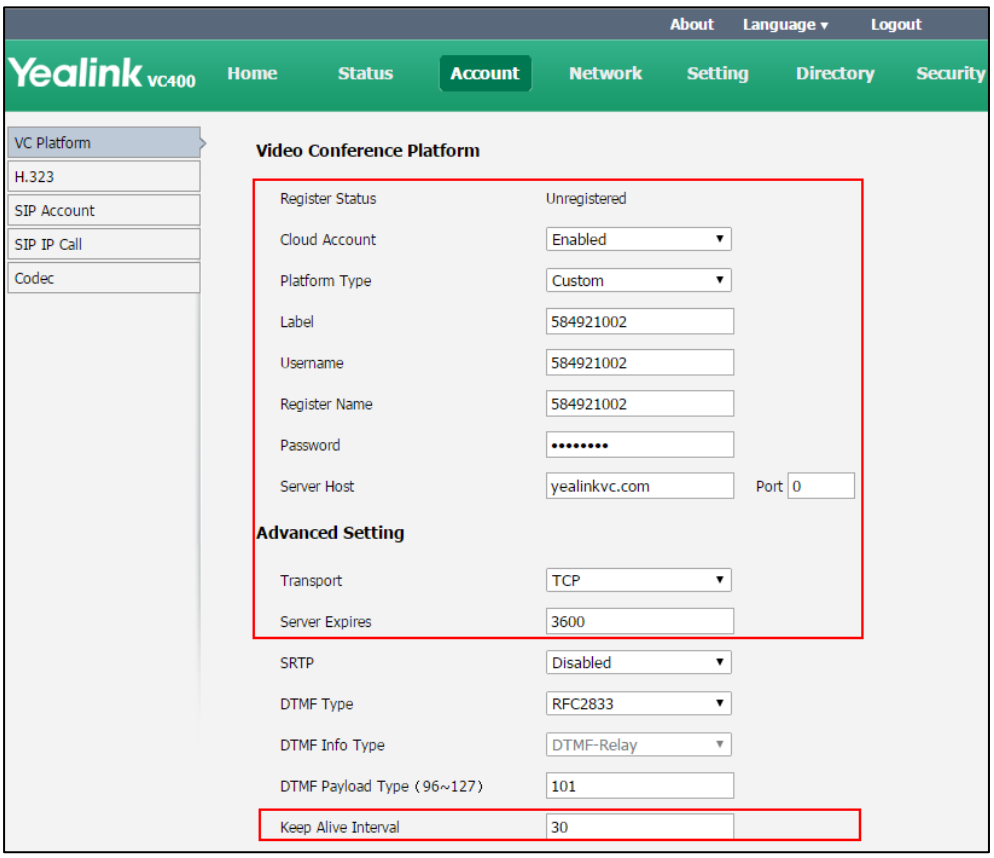
Custom account parameters on the system are described below:

Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot register the custom account.	Remote Control Web User Interface
Platform Type	Configures the platform type. • Yealink VC Cloud Management Service • Yealink Meeting Server • StarLeaf • Zoom • Pexip • BlueJeans • Mind • Custom **Default**: Yealink VC Cloud Management Service	Remote Control Web User Interface
Label	Configures the account label displayed on the display device when registering a custom account. **Default**: Blank	Remote Control Web User Interface
Username	Specifies the user name when registering a custom account. **Default**: Blank	Remote Control Web User Interface
Register Name	Configures the register name when registering a custom account. **Default**: Blank	Remote Control Web User Interface
Password	Specifies the password associated with the user name when registering a custom account. **Default**: Blank	Remote Control Web User Interface

Parameter	Description	Configuration Method
Server/Server Host	Configures the IP address or domain name of the custom server. **Default**: Blank	Remote Control Web User Interface
Port	Configures the port of the custom server. **Default**: 0	Web User Interface
Transport	Configures the type of transport protocol for the custom platform. ● **UDP**–provides best-effort transport via UDP for SIP signaling. ● **TCP**–provides reliable transport via TCP for SIP signaling. ● **TLS**–provides secure communication of SIP signaling. ● **DNS-NAPTR**–performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** TCP	Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the custom server. **Default:**3600	Web User Interface
Remember password	Enables or disables the system to remember the registration information. **Default:** ON **Note:** If it is on, other registration information will be filled automatically when you enter the user name next time.	Remote Control
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. **Default:** 30	Web User Interface

To configure custom account via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Enabled** from the pull-down list of **Cloud Account**.
3. Select **Custom** from the pull-down list of **Platform Type**.
4. Configure the custom account settings.



5. Click **Confirm** to accept the change.

To configure custom account via the remote control:

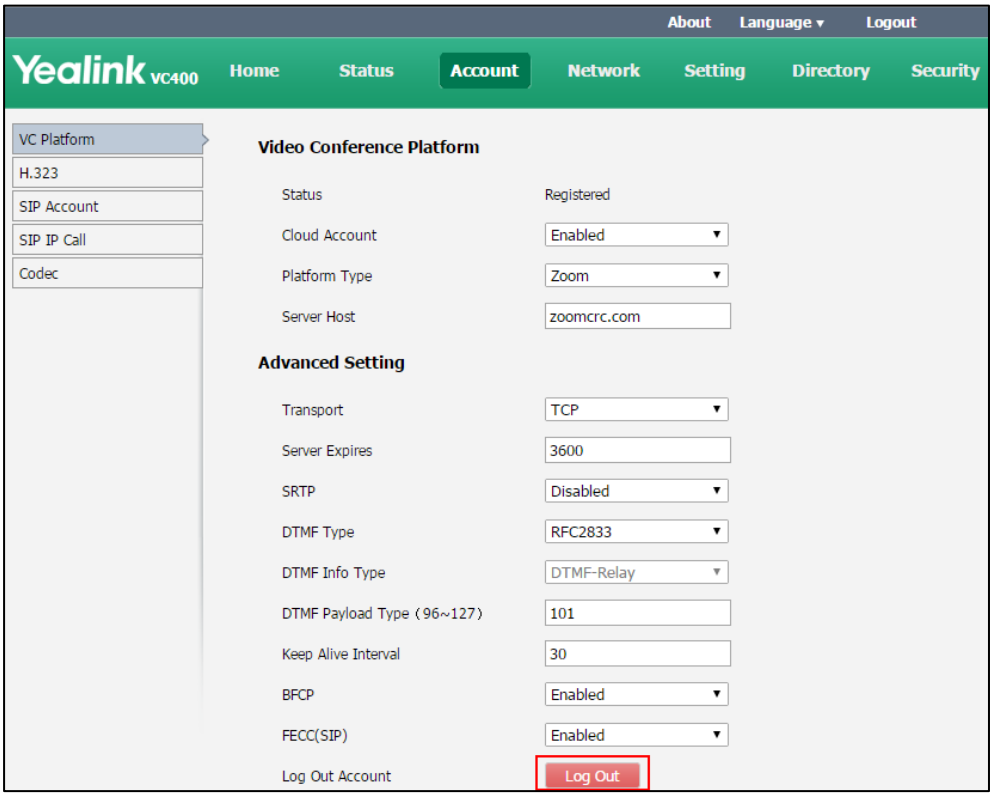
1. Select **Menu**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **Custom** from the pull-down list of **Platform Type**.
4. Configure the custom account settings.
5. Check the **Remember Password** checkbox to remember your registration information.
6. Press ▲or ▼ to scroll to **Log In**, and then press OK.

Logging out of the Cloud Platform

To log out of the Cloud platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select the desired Cloud platform from the pull-down list of **Platform Type**.
3. Click **Log Out**.

   The web user interface prompts the message "Are you sure to exit the account?".



4. Click **Confirm** to accept the change.

To log out of the Cloud platform via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. Press ▲ or ▼ to scroll to **Log Out**, and then press .

   The display device prompts "Log out the account?" OK
3. Press ▲ or ▼ to scroll to **OK**, and then press OK.

Configuring the Third-party Virtual Meeting Room

A Virtual Meeting Room (VMR) is an online space, typically hosted by a Cloud-service provider, where multiple participants can join. Participants usually join by dialing a specific number or an address with a simple name like zoomcrc.com.

If you do not register a Cloud account, or you have registered a Yealink Cloud account or YMS account, you can configure a third-party VMR in advance, so that you can quickly join a VMR without registering a third-party Cloud account.

Up to 5 third-party VMRs can be configured. Third-party VMR is configurable via web user interface only.

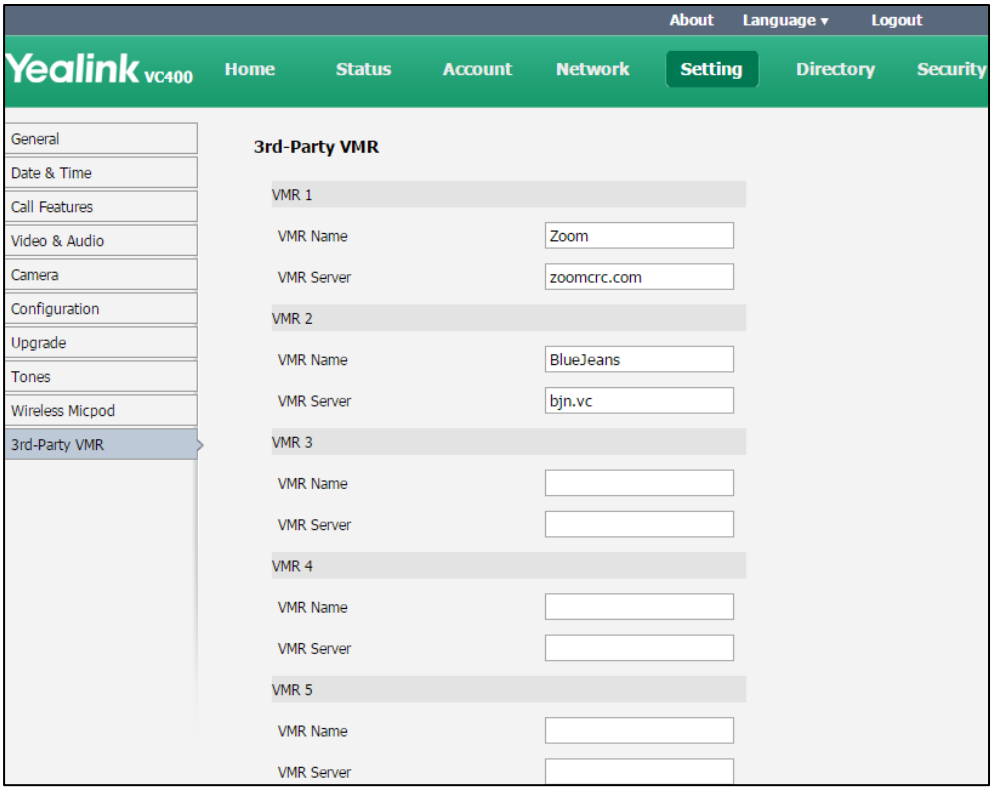
3rd-VMR parameters on the system are described below:

Parameter	Description	Configuration Method
VMR Name 1	Configures the VMR name. **Default**: Zoom **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Server1	Configures the VMR server address. **Default**: zoomcrc.com **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Name 2	Configures the VMR name. **Default**: Blue Jeans **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Server 2	Configures the VMR server address. **Default**: bjn.vc **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Name 3	Configures the VMR name. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Server 3	Configures the VMR server address.	Web User Interface

Parameter	Description	Configuration Method
	Default: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	
VMR Name 4	Configures the VMR name. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Server 4	Configures the VMR server address. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Name 5	Configures the VMR name. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Server 5	Configures the VMR server address. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface

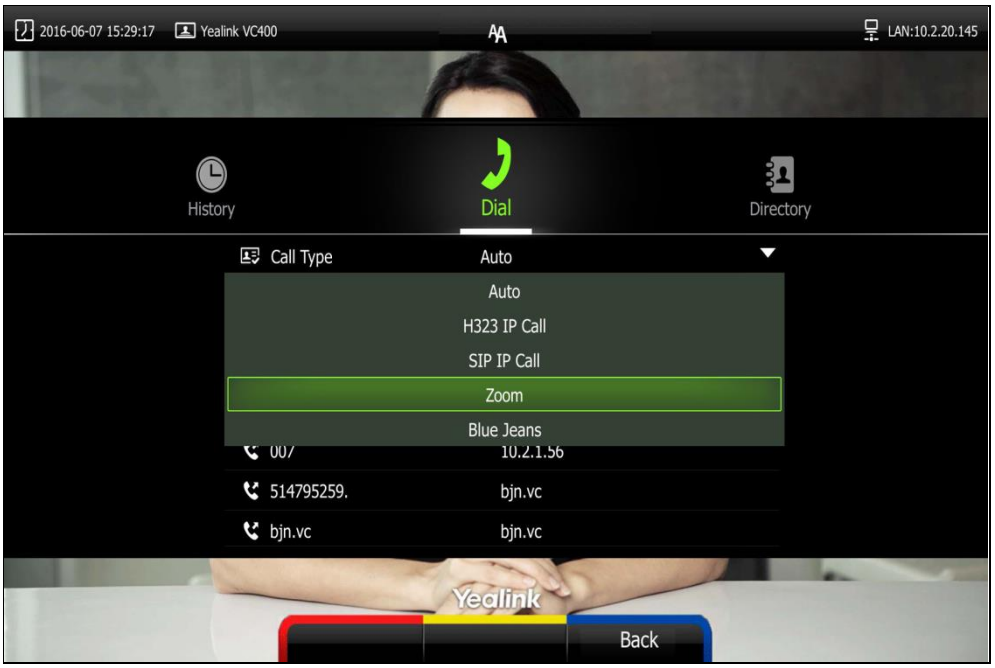
To configure the third-party VMR via web user interface:

1. Click on **Setting**->**3rd-VMR.**
2. Enter VMR name and server address in the corresponding fields respectively.



3. Click **Confirm** to accept the change.

   The VMRs will appear at the pull-down list of **Call Type** on your dialing screen. You can select the desired third-party platform to call corresponding VMRs quickly.



For more information on how to use refer to *Video Conferencing System User Guide*.

Configuring SIP Settings

Yealink VC400/VC120 video conferencing system support Session Initiation Protocol (SIP). If your server supports SIP, you can use SIP to establish calls.

SIP Account

To establish calls using SIP, you can configure a SIP account for the system.

SIP account parameters on the system are described below:

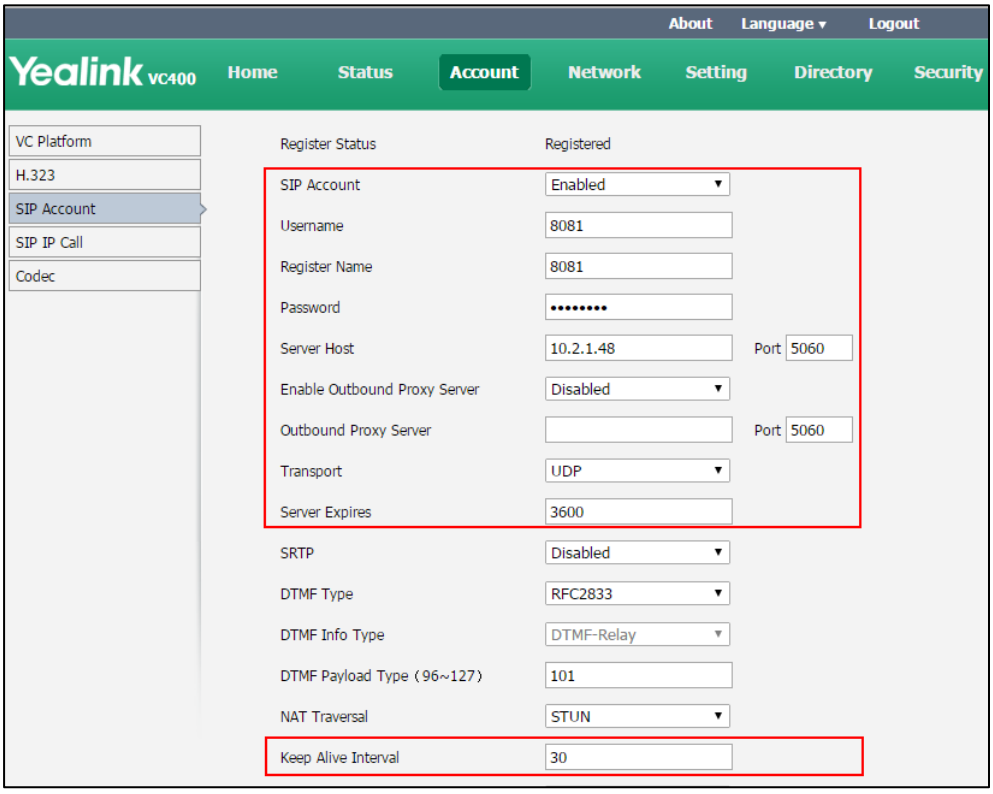
Parameter	Description	Configuration Method
SIP Account	Enables or disables the SIP account. **Default:** Enabled	Remote Control Web User Interface
Register Name	Configures the user name of the SIP account for register authentication. **Default**: Blank	Remote Control Web User Interface
User Name	Specifies the user name to use for authentication when registering with a SIP server. **Default**: Blank	Remote Control Web User Interface
Password	Specifies the password associated with the user name used to authenticate the system to the SIP server. **Default**: Blank	Remote Control Web User Interface
Server/Server Host	Configures the IP address or domain name of the SIP server for the SIP account. **Default**: Blank	Remote Control Web User Interface
SIP Server Port/Port	Configures the port of the SIP server. **Valid values:** Integer from 0 to 65535. **Default**: 5060	Remote Control Web User Interface
Outbound/Enable Outbound Proxy Server	Enables or disables the system to send requests of the SIP account to the outbound proxy server.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Default: Disabled	
Outbound Server/Outbound Proxy Server	Configures the IP address or domain name of the outbound proxy server for the SIP account. **Default:** it is configurable only when the Outbound Proxy Server is enabled.	Remote Control Web User Interface
Outbound Port/Port	Configures the port of the outbound proxy server. **Valid values:** Integer from 0 to 65535. **Default**: 5060	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the SIP account. • **UDP**−provides best-effort transport via UDP for SIP signaling. • **TCP**−provides reliable transport via TCP for SIP signaling. • **TLS**−provides secure communication of SIP signaling. • **DNS-NAPTR**−performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** UDP **Note**: TLS is available only when the system is registered with a SIP server that supports TLS.	Remote Control Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the SIP server for SIP account. **Default:**3600	Remote Control Web User Interface
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So	Web User Interface

Parameter	Description	Configuration Method
	that the registry server will keep the connection open with the client. **Default:** 30	

To configure SIP account via web user interface:

1. Click on **Account->SIP Account**.
2. Configure the SIP account settings.



3. Click **Confirm** to accept the change.

   After successful registration, the display device displays SIP, and the LCD screen of the video conferencing phone displays SIP.

To configure SIP account via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**SIP Account**.
2. Configure the SIP account settings.
3. Press the **Save** soft key to accept the change.

   After successful registration, the display device displays SIP, and the LCD screen of the video conferencing phone displays SIP.

SIP IP Call

When making an IP call using the SIP protocol, the system doesn't support the TLS transport

protocol. So configuration parameters of SIP IP call are divided from the SIP account. You can configure SIP IP call separately.

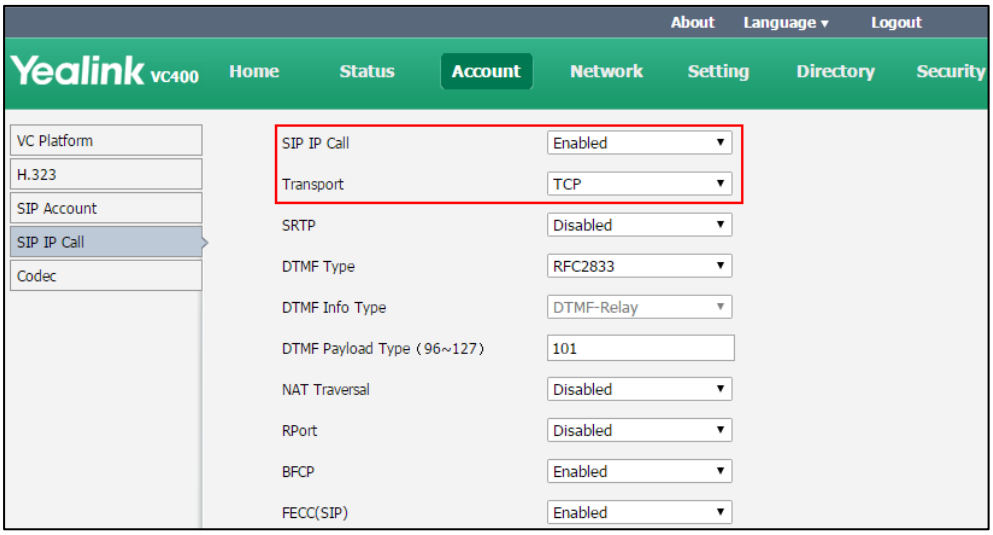
SIP IP call parameters on the system are described below:

Parameter	Description	Configuration Method
SIP IP Call	Enables or disables the SIP IP Call. **Default:** Enabled. **Note:** When it is set to Enabled on both sites, the VC400/VC120 can call the far site by dialing an IP address directly.	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the SIP IP call. ● **UDP**−provides best-effort transport via UDP for SIP signaling. ● **TCP**−provides reliable transport via TCP for SIP signaling. ● **DNS-NAPTR**−performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** TCP	Remote Control Web User Interface

To configure SIP IP call via web user interface:

1. Click on **Account->SIP IP Call**.
2. Select the desired value from the pull-down list of **SIP IP Call**.

3. Select the desired value from the pull-down list of **Transport**.



4. Click **Confirm** to accept the change.

To configure SIP IP call via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000)->**SIP IP Call**.
2. Check the **SIP IP Call** checkbox.
3. Press the **Save** soft key to accept the change.

Configuring H.323 Settings

Yealink VC400/VC120 video conferencing systems support H.323 protocol. If your network uses a gatekeeper, you can register an H.323 account for the system, and specify its H.323 name and extension. This allows others to call the system by entering the H.323 name or extension instead of the IP address.

SIP settings parameters on the system are described below:

Parameter	Description	Configuration Method
H.323 Protocol	Enables or disables the H.323 protocol. **Default:** Enabled. **Note:** Only when it is set to Enabled, can H.323 account be registered. When it is set to Enabled on both sites, the VC400/VC120 can call the far site by dialing an IP address directly.	Remote Control Web User Interface
H.323 Account	Enables or disables the H.323 account.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Default: Enabled If it is set to disabled, the system cannot place or receive calls with the H.323 protocol.	
H.323 Name	Specifies the name that gatekeepers and gateways use to identify this system. You can make point-to-point calls using H.323 names if both system are registered to a gatekeeper. **Default:** blank	Remote Control Web User Interface
H.323 Extension	Specifies the extension that gatekeepers and gateways use to identify this system. **Default:** blank **Note:** Users can place point-to-point calls using the extension if both systems are registered with a gatekeeper.	Remote Control Web User Interface
Gatekeeper Mode	Configures the gatekeeper mode. • **Disabled**−the system does not use a gatekeeper. • **Auto**−the system automatically discovers a gatekeeper. • **Manual**−specify the IP address and port for the gatekeeper manually. **Default:** Disabled	Remote Control Web User Interface
Gatekeeper IP Address 1/Gatekeeper Server 1	Configures the IP address of the primary gatekeeper.	Remote Control Web User Interface
Gatekeeper Port 1/Port	Configures the port of the primary gatekeeper. **Valid values:** Integer from 0 to 65535. **Default**: 1719	Remote Control Web User Interface

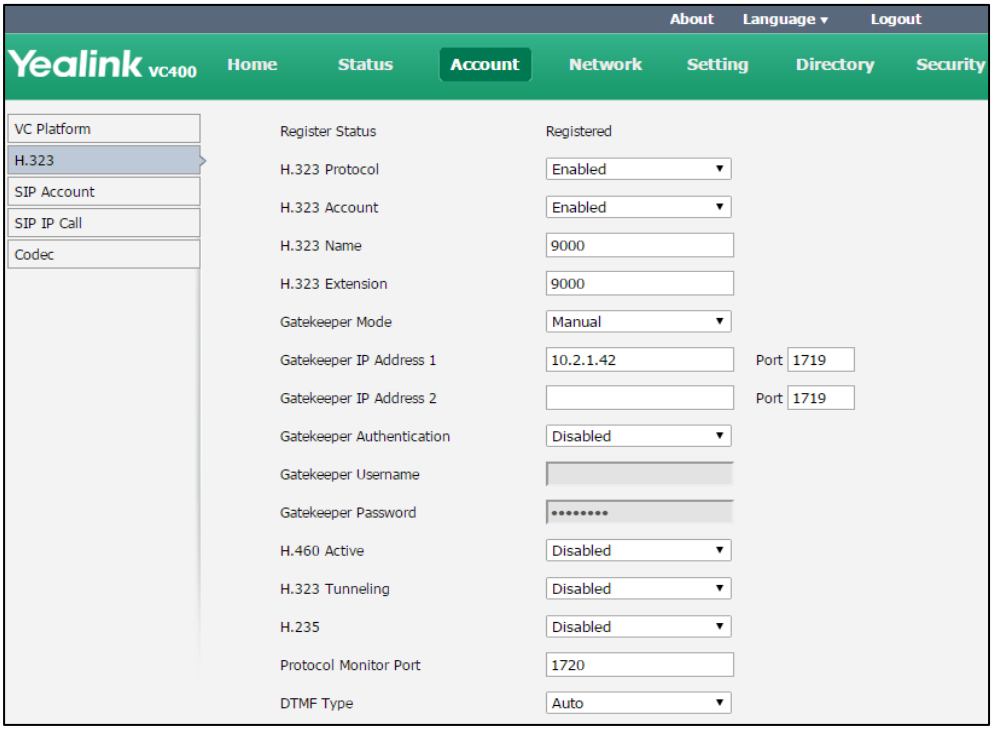
Parameter	Description	Configuration Method
Gatekeeper IP Address 2/Gatekeeper Server 2	Configures the IP address of the secondary gatekeeper.	Remote Control Web User Interface
Gatekeeper Port 2/Port	Configures the port of the primary gatekeeper. **Valid values:** Integer from 0 to 65535. **Default**: 1719	Remote Control Web User Interface
Gatekeeper Authentication	Enables or disables support for gatekeeper authentication. **Default:** Disabled **Note:** When Gatekeeper Authentication is enabled, the gatekeeper ensures that only trusted H.323 systems are allowed to access the gatekeeper.	Remote Control Web User Interface
Gatekeeper Username	Specifies the user name for authentication with gatekeeper. **Default:** blank	Remote Control Web User Interface
Gatekeeper Password	Specifies the password for authentication with gatekeeper. **Default:** blank	Remote Control Web User Interface
H.460 Active	Enables or disables firewall traversal of H.323 calls using H.460 protocols. **Default:** Disabled For more information, refer to Enabling H.460 Support for H.323 Calls on page 135.	Remote Control Web User Interface
H.323 Tunneling	(Optional) Instructs the system to send all signaling and media through the HTTP tunnel. **Default:** Disabled For more information, refer to H.323 Tunneling on page 73.	Remote Control Web User Interface
H.235	Specifies the H.235 type during an H.323 call.	Web User Interface

Parameter	Description	Configuration Method
	• **Disabled**–do not use H.235 in H.323 calls. • **Optional**–negotiate with the far site whether to use H.235 for media encryption in H.323 calls. • **Compulsory**–compulsory use H.235 for media encryption in H.323 calls. **Default:** Disabled For more information, refer to H.235 on page 263.	
Protocol Monitor Port	Specifies the port for the H.323 protocol. **Valid values:** 0-65535 **Default** 1720. **Note:** It is only applicable to H.323 IP call.	Web User Interface
Local Early Media	Enables or disables local early media feature on the system. **Default**: Disabled. If it is set to Enabled, the system will send video SDP twice during a call to solve the compatibility between Yealink device and certain devices.	Web User Interface

To configure H.323 account via web user interface:

1. Click on **Account**->**H.323**.

2. Configure the H.323 account settings.



3. Click **Confirm** to accept the change.

   After successful registration, the display device displays H323, and the LCD screen of the video conferencing phone displays H323.

To configure H.323 account via the remote control:

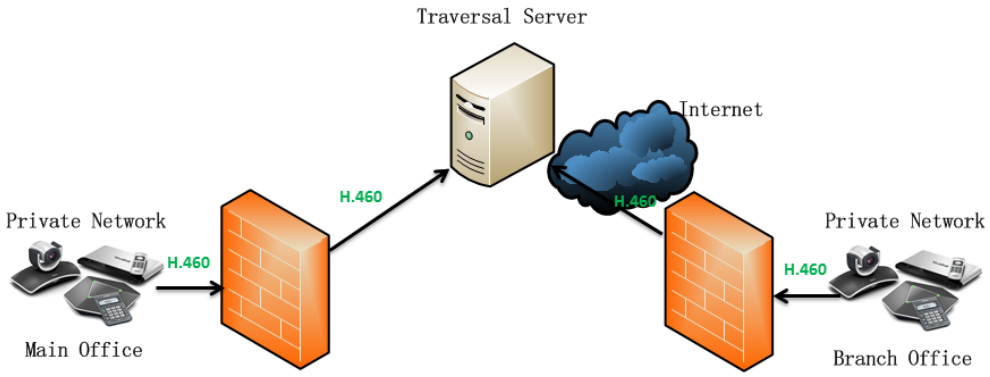
1. Select **Menu**->**Advanced** (default password: 0000) ->**H.323**.
2. Configure the H.323 account settings.
3. Press the **Save** soft key to accept the change.

   After successful registration, the display device displays H323, and the LCD screen of the video conferencing phone displays H323.

Enabling H.460 Support for H.323 Calls

Yealink video conferencing systems support firewall traversal of H.323 calls using H.460 protocols. You must have an H.460 server configured in your environment for this feature to function properly.

Note If you configure H.323 settings and enable H.460 support, the system ignores Static NAT settings. For more information on NAT, refer to Static NAT on page 81.



The H.460 firewall traversal parameter is described below:

Parameter	Description	Configuration Method
Gatekeeper Mode	Configures the gatekeeper mode. • **Disabled**–the system does not use a gatekeeper. • **Auto**–the system automatically discovers a gatekeeper. • **Manual**–specify the IP address and port for the gatekeeper manually. **Default:** Disabled	Remote Control Web User Interface
Gatekeeper IP Address 1/Gatekeeper Server 1	Configures the IP address of the primary H.460 server. **Note**: It is configurable only when the **Gatekeeper Mode** is set to Manual.	Remote Control Web User Interface
Gatekeeper Port 1/Port	Configures the port of the primary H.460 server. **Valid values:** Integer from 0 to	Remote Control Web User Interface

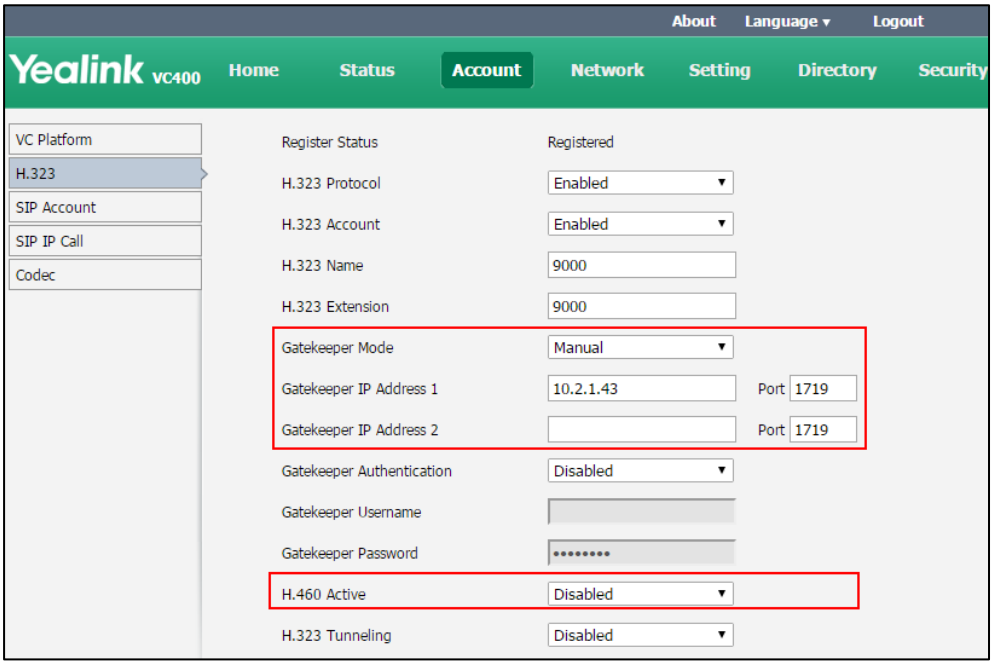
Parameter	Description	Configuration Method
	65535. **Default**: 1719	
Gatekeeper IP Address 2/Gatekeeper Server 2	Configures the IP address of the secondary H.460 server. **Note**: It is configurable only when the **Gatekeeper Mode** is set to Manual.	Remote Control Web User Interface
Gatekeeper Port 2/Port	Configures the port of the secondary H.460 server. **Valid values:** Integer from 0 to 65535. **Default**: 1719	Remote Control Web User Interface
H.460 Active	Enables or disables firewall traversal of H.323 calls using H.460 protocols. **Default:** Disabled	Remote Control Web User Interface

To enable H.460, configure the H.323 preferences first, as described in Configuring H.323 Settings chapter with the following exceptions:

To configure H.460 firewall traversal for H.323 via web user interface:

1. Click on **Account**->**H.323**.
2. Select **Manual** from the pull-down list of **Gatekeeper Mode**.
3. Enter the IP address and port number of the H.460 server in **Gatekeeper IP Address** and **Port** fields.

4. Select Enabled from the pull-down list of **H.460 Active**.



5. Click **Confirm** to accept the change.

To configure H.460 firewall traversal via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**H.323**.
2. Select **Manual Settings** from the pull-down list of **Gatekeeper Type**.
3. Enter the IP address and port number of the H.460 server in **Gatekeeper Server** and **Gatekeeper Port** fields.
4. Check the **H.460 Active** checkbox.
5. Press the **Save** soft key to accept the change.

DTMF

DTMF (Dual Tone Multi-frequency), better known as touch-tone, is used for telecommunication signaling over analog telephone lines in the voice-frequency band. DTMF is the signal sent from the IP phone to the network, which is generated when pressing the keypad during a call. Each key pressed on the IP phone generates one sinusoidal tone of two frequencies. One is generated from a high frequency group and the other from a low frequency group.

The DTMF keypad is laid out in a 4×4 matrix, with each row representing a low frequency, and each column representing a high frequency. Pressing a digit key (such as '1') will generate a sinusoidal tone for each of two frequencies (697 and 1209 hertz (Hz)).

DTMF Keypad Frequencies:

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Methods of Transmitting DTMF Digit

Three methods of transmitting DTMF digits:

- **RFC2833** -- DTMF digits are transmitted by RTP Events compliant to RFC2833.
- **INBAND** -- DTMF digits are transmitted in the voice band.
- **SIP INFO** -- DTMF digits are transmitted by SIP INFO messages.

RFC 2833

DTMF digits are transmitted using the RTP Event packets that are sent along with the voice path. These packets use RFC 2833 format and must have a payload type that matches what the other end is listening for. The default payload type for RTP Event packets is 101 and the payload type is configurable. The VCS use the configured value to negotiate with the other end during call establishment.

The RTP Event packet contains 4 bytes. The 4 bytes are distributed over several fields denoted as Event, End bit, R-bit, Volume and Duration. If the End bit is set to 1, the packet contains the end of the DTMF event. You can configure the sending times of the end RTP Event packet.

INBAND

DTMF digits are transmitted within the audio of the IP phone conversation. It uses the same codec as your voice and is audible to conversation partners.

SIP INFO

DTMF digits are transmitted by the SIP INFO messages when the voice stream is established after a successful SIP 200 OK-ACK message sequence. The SIP INFO message is sent along the signaling path of the call. The SIP INFO message can transmit DTMF digits in three ways: DTMF, DTMF-Relay and Telephone-Event.

DTMF parameters for SIP protocol on the system are described below:

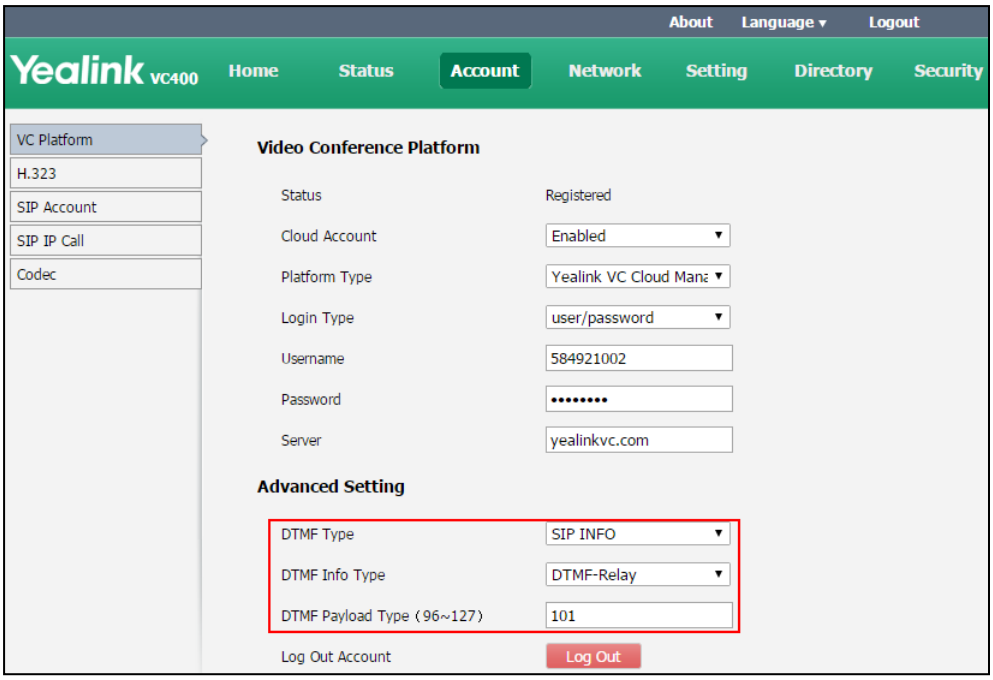
Parameter	Description	Configuration Method
DTMF Type	Configures the DTMF type. You can configure it for the Cloud platform,	Remote Control

Parameter	Description	Configuration Method
	SIP account or SIP IP call separately. ● **INBAND**−DTMF digits are transmitted in the voice band. ● **RFC2833**−DTMF digits are transmitted by RTP Events compliant to RFC2833. ● **SIP INFO**−DTMF digits are transmitted by the SIP INFO messages. ● **RFC2833+ SIP INFO**−DTMF digits are transmitted by RTP Events compliant to RFC 2833 and the SIP INFO messages. **Default**: RFC2833.	Web User Interface
DTMF Info Type	Configures the DTMF info type when DTMF type is set to SIP INFO or RFC2833+SIP INFO. You can configure it for the Cloud platform, SIP account or SIP IP call separately ● **DTMF-Relay** ● **DTMF** ● **Telephone-Event** **Default**: DTMF-Relay.	Remote Control Web User Interface
DTMF Payload Type（96~127）	Configures the value of DTMF payload. You can configure it for the Cloud platform, SIP account or SIP IP call separately. **Default:** 101	Web User Interface

To configure DTMF type for Cloud platform via web user interface:

1. Click on **Account->VC Platform**.
2. Select the desired value from the pull-down list of **DTMF Type**.
3. If **SIP INFO** or **RFC2833+ SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.

4. Enter the desired value in the **DTMF Payload Type(96~127)** field.



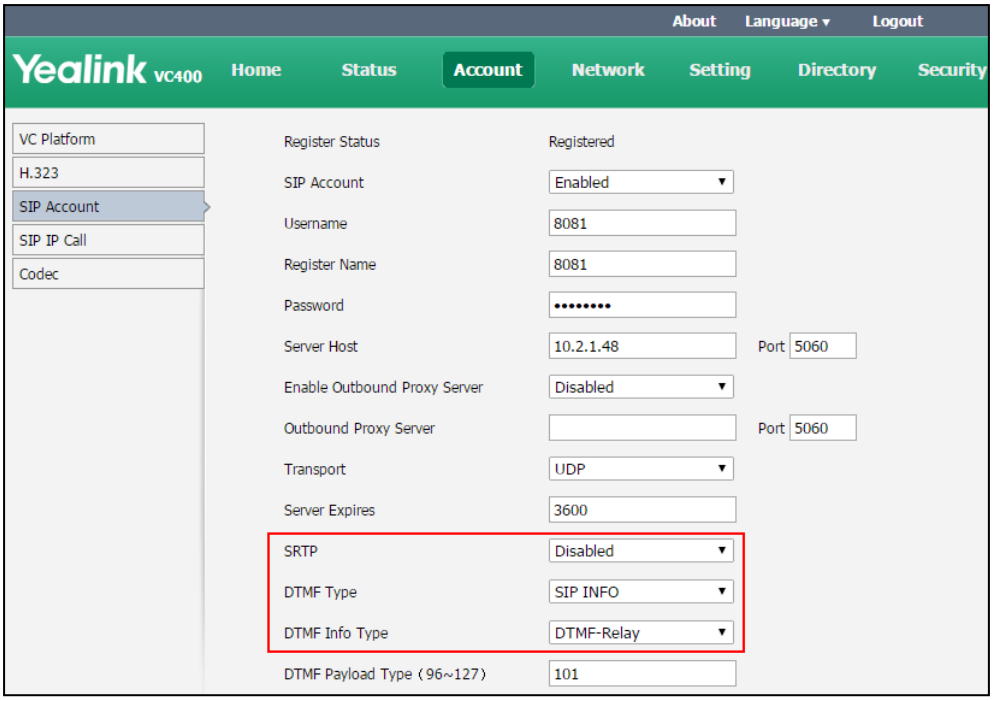
5. Click **Confirm** to accept the change.

To configure DTMF type for SIP account via web user interface:

1. Click on **Account**->**SIP Account**.
2. Select the desired value from the pull-down list of **DTMF Type**.

   If **SIP INFO** or **RFC2833+ SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.

3. Enter the desired value in the **DTMF Payload Type(96~127)** field.

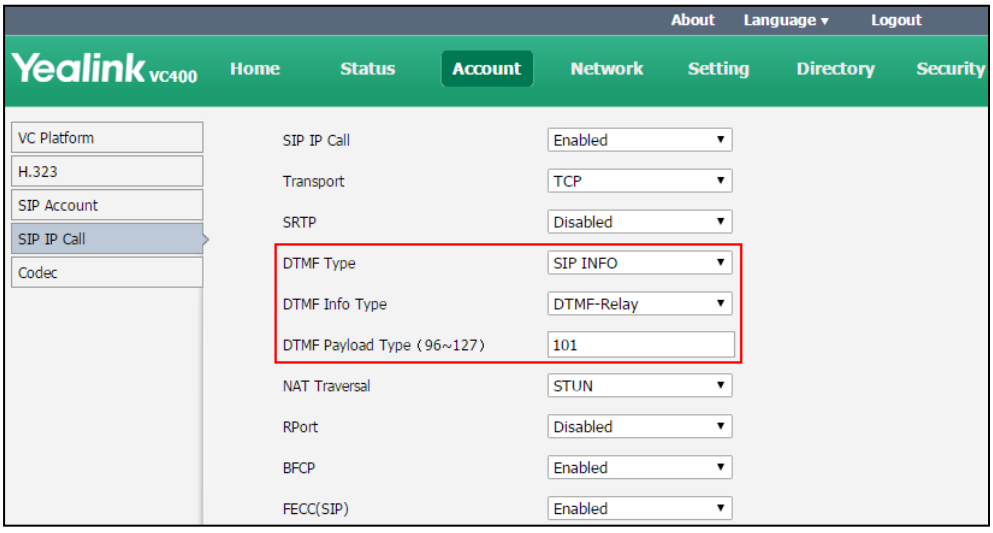


4. Click **Confirm** to accept the change.

To configure DTMF type for SIP IP call via web user interface:

1. Click on **Account**->**SIP IP Call**.
2. Select the desired value from the pull-down list of **DTMF Type**.

   If **SIP INFO** or **RFC2833+ SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.
3. Enter the desired value in the **DTMF Payload Type(96~127)** field.



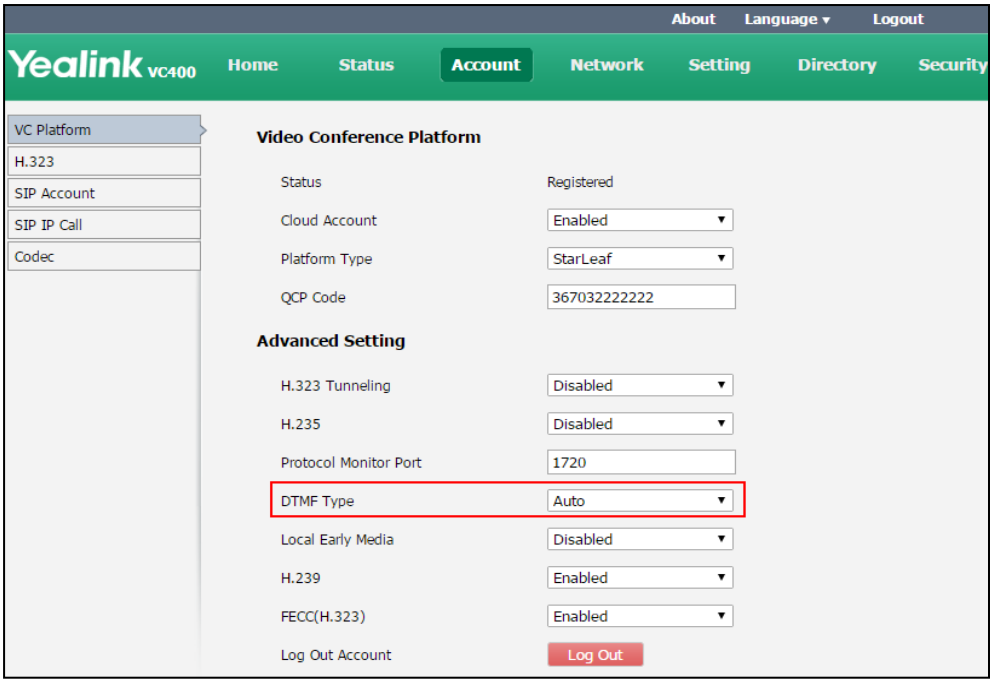
4. Click **Confirm** to accept the change.

DTMF parameters for H.323 protocol on the system are described below:

Parameter	Description	Configuration Method
DTMF Type	Configures the DTMF type. You can configure it for the StarLeaf Cloud platform or H.323 call separately. • **INBAND**–DTMF digits are transmitted in the voice band. • **Auto**–the system automatically negotiates the way (INBAND, RFC2833 or SIP INFO) to transfer DTMF digits. **Default:** Auto	Remote Control Web User Interface

To configure DTMF type for StarLeaf Cloud platform via web user interface:

1. Click on **Account->VC Platform**.
2. Select **StarLeaf** from the pull-down list of **Platform Type**.
3. Select the desired value from the pull-down list of **DTMF Type**.

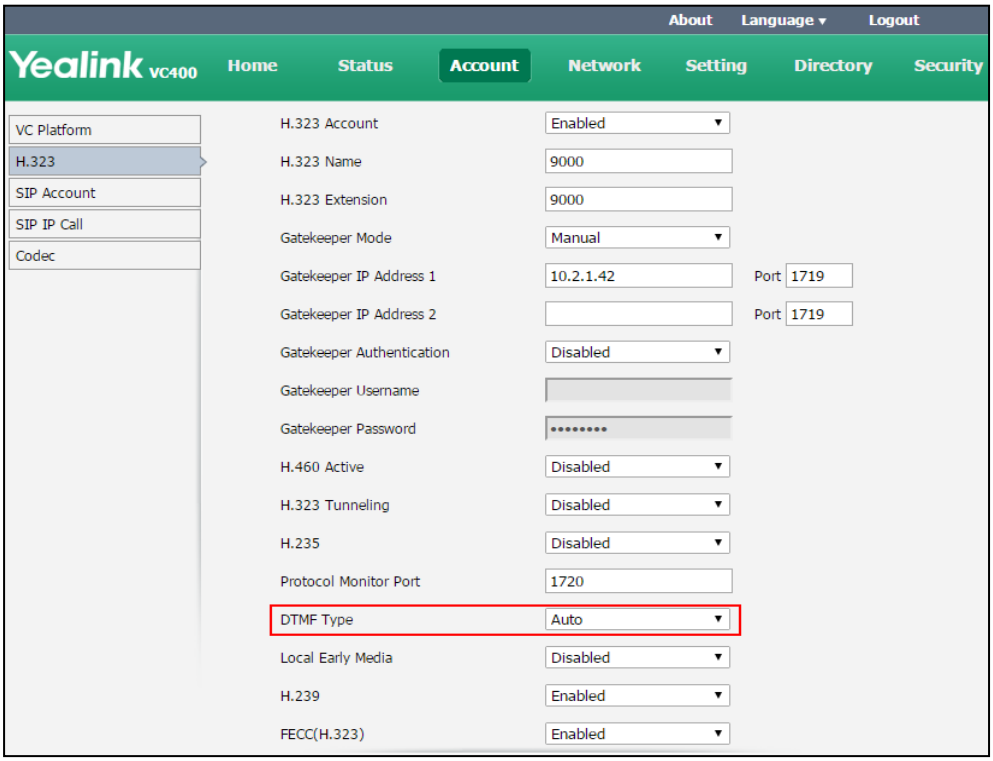


4. Click **Confirm** to accept the change.

To configure DTMF type for H.323 via web user interface:

1. Click on **Account**->**H.323**.

2. Select the desired value from the pull-down list of **DTMF Type**.



3. Click **Confirm** to accept the change.

Codecs

CODEC is an abbreviation of COmpress-DECompress, and is capable of coding or decoding a digital data stream or signal by implementing an algorithm. The object of the algorithm is to represent the high-fidelity audio/video signal with a minimum number of bits while retaining quality. This can effectively reduce the frame size and the bandwidth required for audio/video transmission.

Audio Codecs

The audio codec that the system uses to establish a call should be supported by the server. When placing a call, the system will offer the enabled audio codec list to the server and then use the audio codec negotiated with the called party according to the priority.

The following table summarizes the supported audio codecs on the system:

Codec	Algorithm	Bit Rate	Sample Rate	Reference
G.722.1c	G.722.1	48 Kbps	32 Ksps	RFC 5577
G.722.1c		32 Kbps	32 Ksps	RFC 5577
G.722.1c		24 Kbps	32 Ksps	RFC 5577

Codec	Algorithm	Bit Rate	Sample Rate	Reference
G.722.1	G.722.1	24 Kbps	16 or 32 Ksps	RFC 5577
G722	G.722	64 Kbps	16 Ksps	RFC 3551
PCMU	G.711	64 Kbps	8 Ksps	RFC 3551
PCMA	G.711	64 Kbps	8 Ksps	RFC 3551

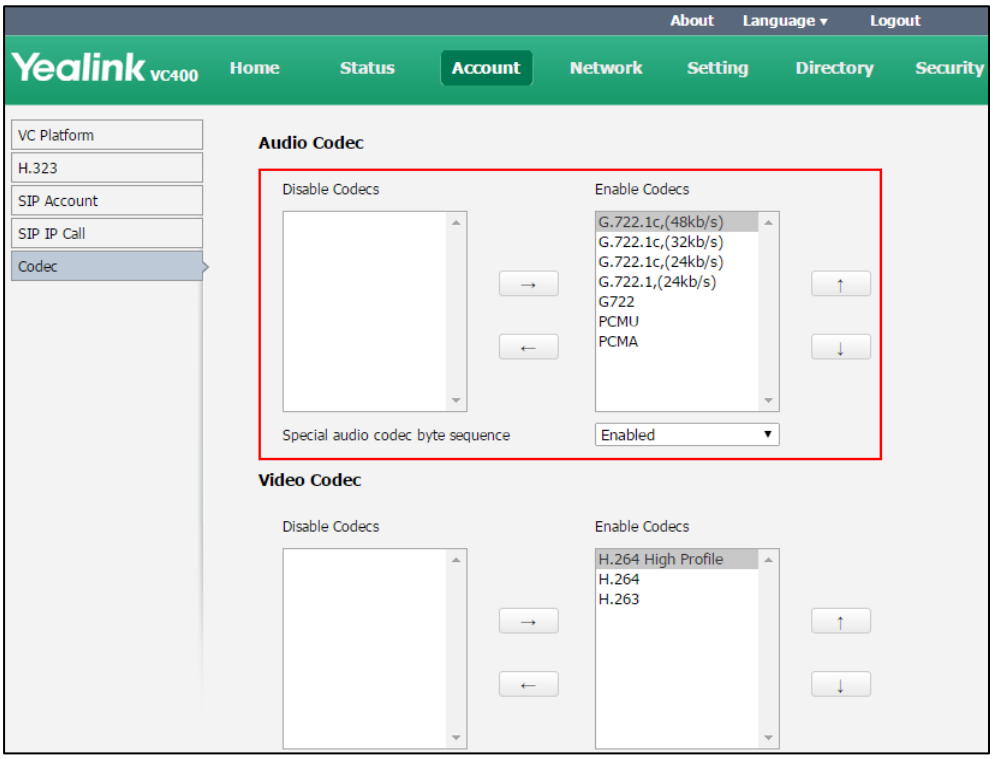
Audio codecs parameters on the system are described below:

Parameter	Description	Configuration Method
Enable Codecs	Specifies the enabled audio codecs for the system to use. **Note:** All support audio codecs are enabled on the system by default.	Web User Interface
Disable Codecs	Specifies the disabled audio codecs for the system not to use.	Web User Interface
Special audio codec byte sequence	Enables or disables the special audio codec byte sequence. **Note:** Different devices have different definition about how some Codecs are stored (Big-endian or little-endian), which may lead to the audio incompatibility problems between Yealink and certain devices. You can enable the special audio codec byte sequence feature to solve these incompatibility problems.	Web User Interface

To configure audio codecs via web user interface:

1. Click on **Account**->**Codec**.
2. Select the desired codec from the **Disable Codecs** or the **Enable Codecs** column.
3. Click ← or → to disable or enable the selected codec.
4. Select the desired audio codec from the **Enable Codecs** column, and click ↑ or ↓ to adjust the priority of the selected audio codecs.

5. (Optional) If Yealink device has audio problems with certain device, select **Enabled** from the pull-down list of **Special audio codec byte sequence**.



6. Click **Confirm** to accept the change.

Video Codecs

The video codec that the system uses to establish a call should be supported by the server. When placing a call, the system will offer the enabled video codec list to the server and then use the video codec negotiated with the called party according to the priority.

The following table summarizes the supported video codecs on the system:

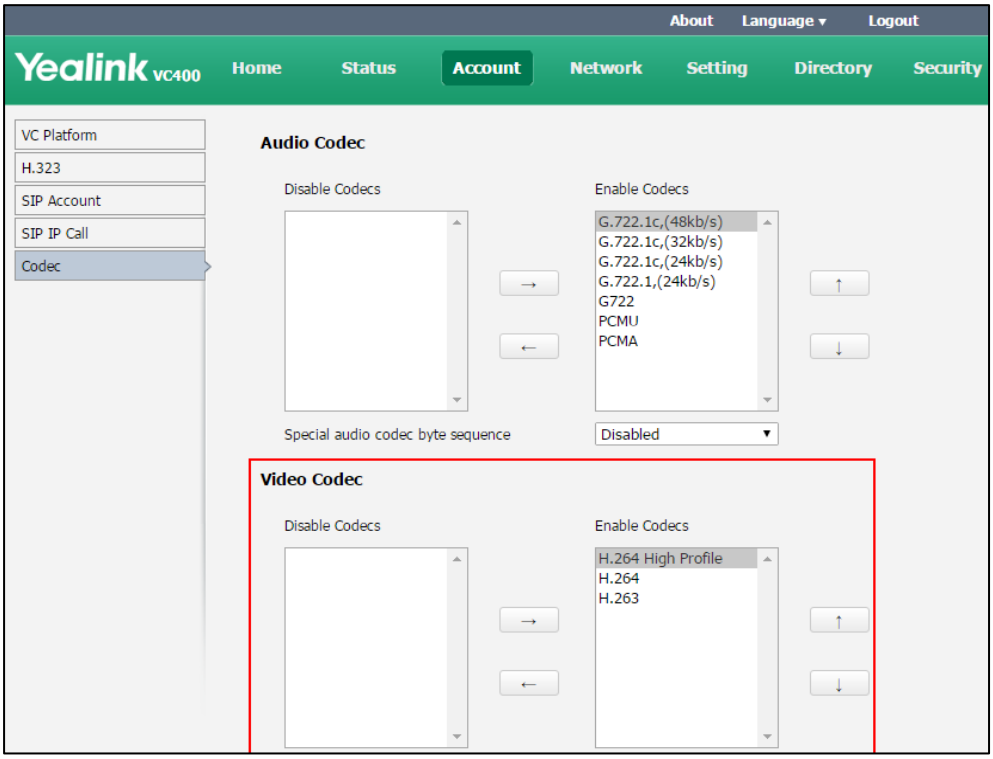
Name	MIME Type	Bit Rate	Frame Rate	Frame Size
H.264 High Profile	H264/90000	90 kbps to 2048 kbps	5 fps to 30 fps	Tx: WQVGA,360P, 448P, 540P, 720P, 1080P Rx: Conventional Size Below 1080P
H.264	H264/90000			
H.263	H263/90000			Tx: CIF, 4CIF RX: QCIF, CIF, 4CIF

Video codecs parameters on the system are described below:

Parameter	Description	Configuration Method
Enable Codecs	Specifies the enabled video codecs for the system to use. **Note:** All support video codecs are enabled on the system by default.	Web User Interface
Disable Codecs	Specifies the disabled video codecs for the system not to use.	Web User Interface

To configure video codecs via web user interface:

1. Click on **Account**->**Codec**.
2. Select the desired video codec from the **Disable Codecs** or the **Enable Codecs** column.
3. Click ← or → to disable or enable the selected video codec.
4. Select the desired video codec from the **Enable Codecs** column, and click ↑ or ↓ to adjust the priority of the selected video codecs.



5. Click **Confirm** to accept the change.

Call Protocol

The system supports SIP and H.323 protocols for incoming and outgoing calls. H.323 is commonly used to communicate to other video conferencing system. SIP is commonly used to

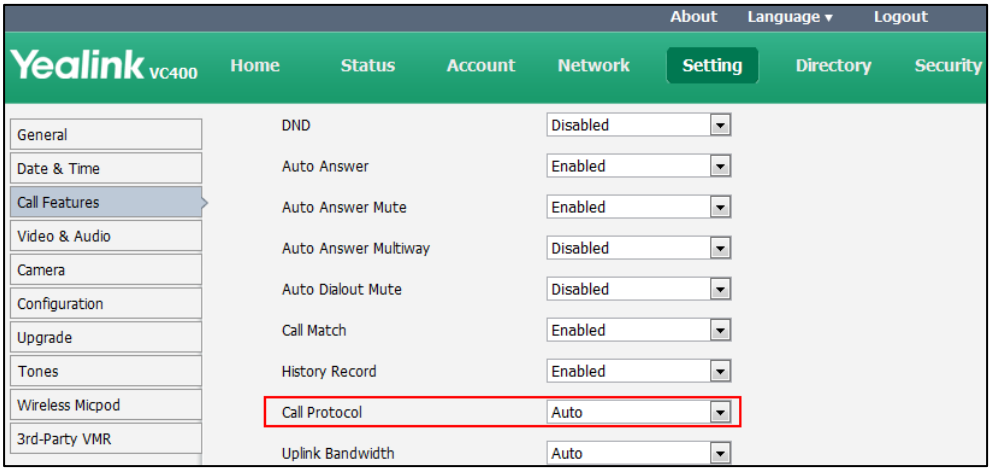
communicate with other VoIP devices. The default call protocol on the system is Auto. The system preferentially uses the H.323 protocol to place calls. If there is no available H.323 account on the system, the system will switch to the SIP protocol for placing calls. You can specify the desired protocol for the system to place calls. Ensure the remote system supports the same protocol.

The call protocol parameter on the system is described below:

Parameter	Description	Configuration Method
Call Protocol	Specifies the desired call protocol for placing calls. • **Auto**–the system automatically uses the available call protocol. • **SIP**–the system uses the SIP protocol for placing calls. • **H.323**–the system uses H.323 protocol for placing calls. **Default:** Auto	Remote Control Web User Interface

To configure call protocol via web user interface:

1. Click on **Setting**->**Call Features**.
2. Select the desired value from the pull-down list of **Call Protocol**.



3. Click **Confirm** to accept the change.

To configure call protocol via the remote control:

1. Select **Menu**->**Call Features** ->**Call Protocol**.
2. Select the desired value from the pull-down list of **Call Protocol**.
3. Press the **Save** soft key to accept the change.

Account Polling

When you dial account numbers of other system, account polling feature enables your system to use different call types according to this priority: Cloud platform>H.323 account>SIP account. If you cannot call other systems using all your registered accounts, then this call fails.

Account polling is disabled by default. When you register multiple accounts (2 or more) for your system, you can enable account polling feature. You can configure account polling feature via web user interface only.

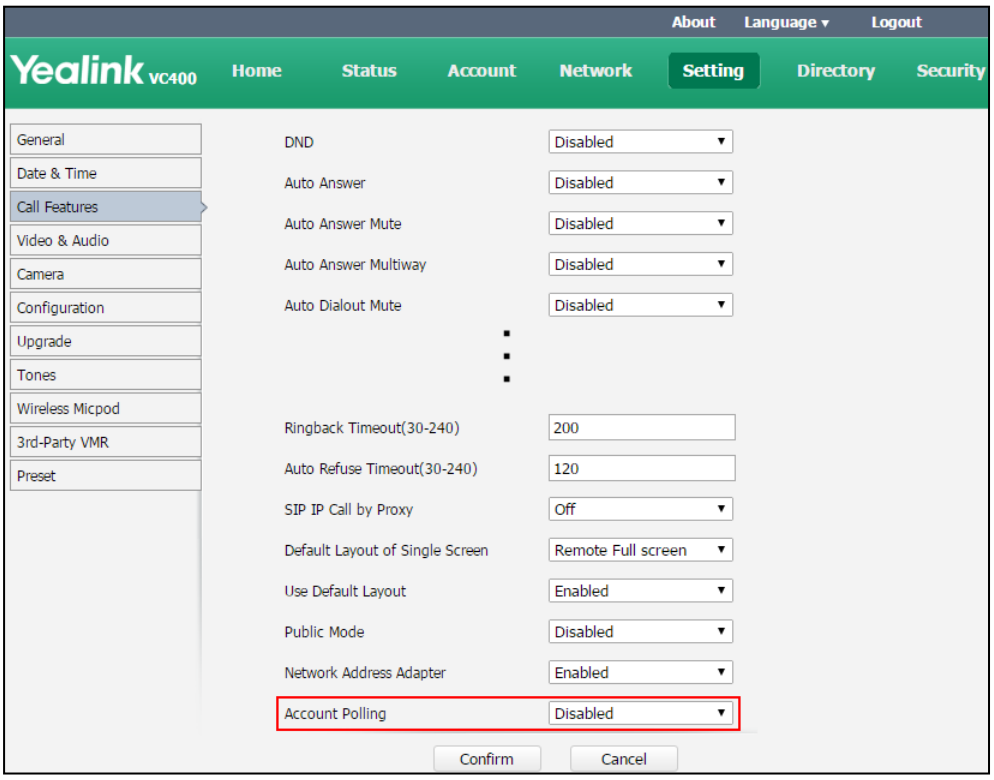
Account polling parameter on the system is described below:

Parameter	Description	Configuration Method
Account Polling	Enables or disables the account polling on the system. • **Disabled**—the system can only call other system's account using the call type with the highest priority (Cloud platform>H.323 account>SIP account). • **Enabled—**the system will attempt to call other system's account using different call types according the priority (Cloud platform>H.323 account>SIP account). **Default:** Disabled	Remote Control Web User Interface

To configure account polling via web user interface:

1. Click on **Setting**->**Call Features**.

2. Select the desired value from the pull-down list of **Account Polling**.

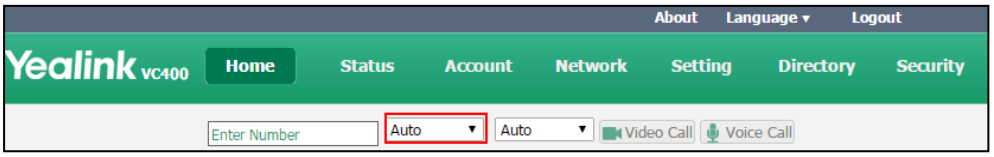


3. Click **Confirm** to accept the change.

The following example shows the way calls are placed when account polling is enabled or disabled.

Scenario:

1. System A is registered with a Yealink Cloud account and a SIP account.
2. On system A, select **Auto** from the pull-down list before calling.



3. On system A, dial the account numbers of system B.

Result:

- If account polling is disabled, system A can only use its Cloud account (highest priority) to call system B.
- If account polling is enabled, system A will use its Cloud account (highest priority) to call system B first. If this call fails, system A continues to use its SIP account (next priority) to call system B.

Do Not Disturb

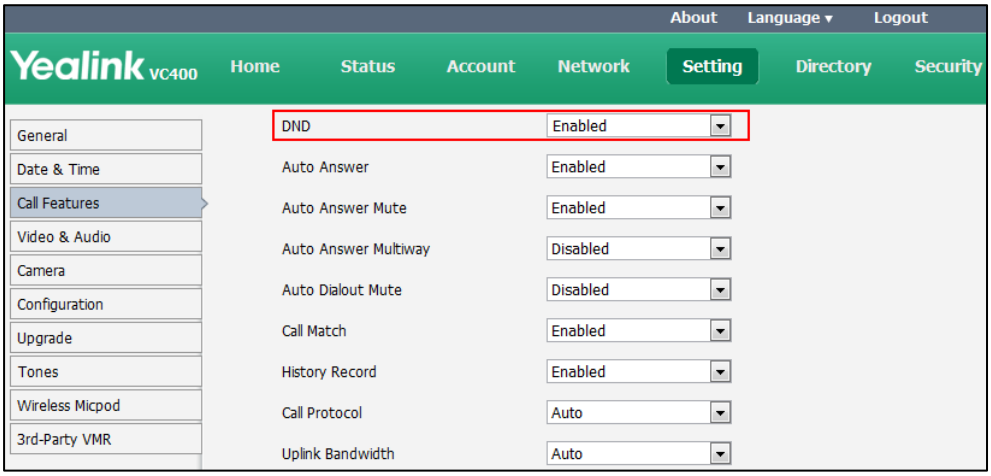
Do not Disturb allows the system to reject all incoming calls automatically. You can activate the DND mode for the system when it is idle, and the DND mode will be deactivated after the system places a call. You can also activate the DND mode for the system during a call, and the DND mode will be deactivated after the system ends the call.

The DND parameter on the system is described below:

Parameter	Description	Configuration Method
DND	Enables or disables DND mode on the system. **Default:** Disabled	Remote Control Web User Interface

To configure DND via web user interface:

1. Click on **Setting**->**Call Features**.
2. Select the desired value from the pull-down list of **DND**.



3. Click **Confirm** to accept the change.

   If **Enabled** is selected, the display device will display , and the LCD screen of the video conferencing phone will display DND.

To configure DND via the remote control:

1. Select **Menu**->**Call Features**.
2. Check the **DND** checkbox.
3. Press the **Save** soft key to accept the change.

   The display device will display , and the LCD screen of the video conferencing phone will display DND.

To configure DND during a call via web user interface:

1. Click **Home**.

2. Check the **DND** checkbox.

   The display device will display , and the LCD screen of the video conferencing phone will display DND.

To configure DND during a call via the remote control:

1. Press the **More** soft key.
2. Check the **DND** checkbox.
3. Press the **Back** soft key to exit the **More** window.

   The display device will display , and the LCD screen of the video conferencing phone will display DND.

Auto Answer

The auto answer feature allows the system to answer incoming calls automatically. The auto answer mute feature allows the system to turn off the microphone when an incoming call is answered automatically. The auto answer mute feature is available only when the auto answer feature is enabled. The auto answer multiway feature allows the system to answer new incoming calls automatically during an active call.

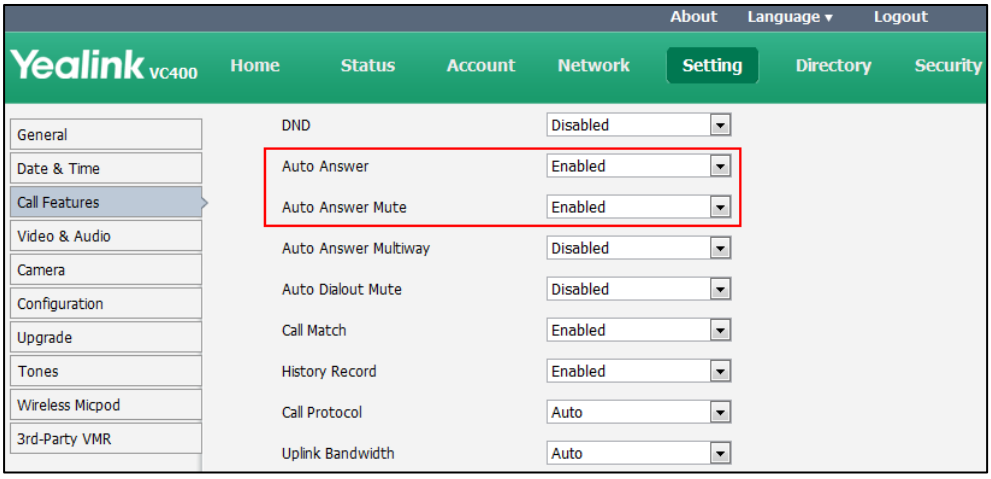
Auto answer parameters on the system are described below:

Parameter	Description	Configuration Method
Auto Answer	Enables or disables the auto answer feature on the system. **Default:** Enabled	Remote Control Web User Interface
Auto Answer Mute	Enables or disables the auto answer mute feature on the system. **Default:** Enabled Auto answer mute feature is configurable only when the auto answer is enabled.	Remote Control Web User Interface
Auto Answer Multiway	Enables or disables the auto answer multiday feature on the system. **Default:** Disabled The auto answer multiway feature is available only when the auto answer is enabled.	Remote Control Web User Interface

To configure auto answer via web user interface:

1. Click on **Setting**->**Call Features**.
2. Select the desired value from the pull-down list of **Auto Answer**.

3. Select the desired value from the pull-down list of **Auto Answer Mute**.
4. Select the desired value from the pull-down list of **Auto Answer Multiway.**



5. Click **Confirm** to accept the change.

   If **Enabled** is selected, the display device will display AA, and the LCD screen of the video conferencing phone will display [AA].

To configure auto answer via the remote control:

1. Select **Menu**->**Call Features**.
2. Check the **Auto Answer** checkbox.
3. Check the **Auto Answer Mute** checkbox.
4. Check the **Auto Answer Multiway** checkbox.
5. Press the **Save** soft key to accept the change.

   The display device will display AA, and the LCD screen of the video conferencing phone will display [AA].

Auto Dialout Mute

The auto dialout mute feature allows the system to turn off the microphone when placing a call, so that the other party cannot hear you.

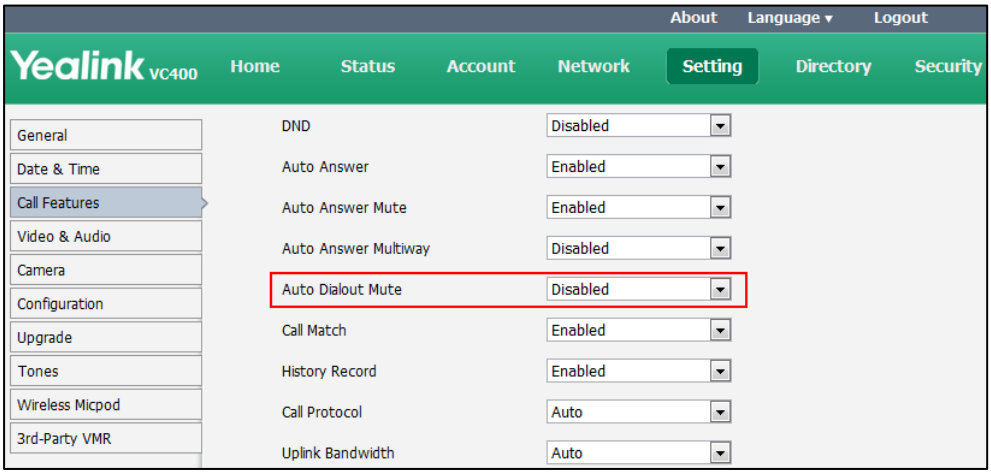
Auto dialout mute parameter on the system is described below:

Parameter	Description	Configuration Method
Auto Dialout Mute	Enables or disables the auto dialout mute feature on the system. **Default:** Disabled	Web User Interface

To configure auto dialout mute feature via web user interface:

1. Click on **Setting**->**Call Features**.

2. Select the desired value from the pull-down list of **Auto Dialout Mute**.



3. Click **Confirm** to accept the change.

   If **Enabled** is selected, your video image will display mute icon ( ) when you place a call.

Call Match

The call match feature allows the system to search for entries automatically from the search source list based on the entered string. Once matched, the results will be displayed on the screen. If no list is added to the search source list, the system will not perform a search even if call match is enabled. For more information on how to search source list in dialing, refer to Search Source List in Dialing on page 239 .

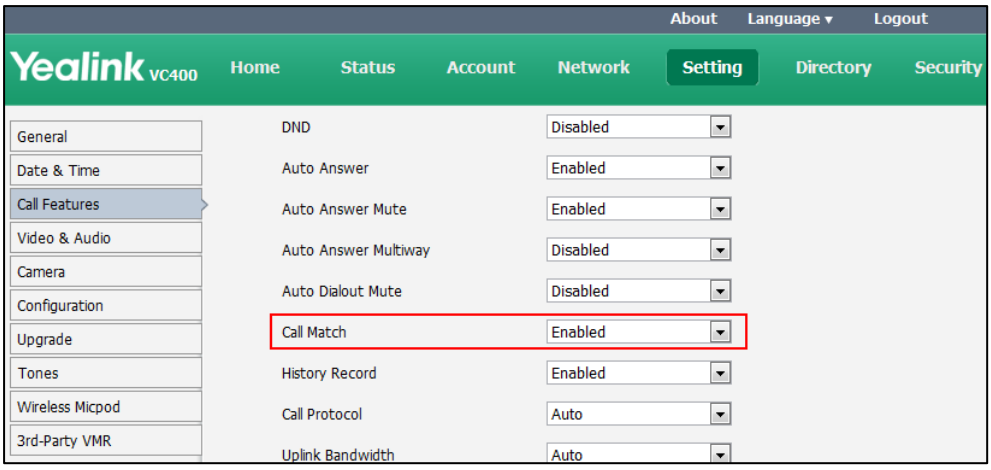
Parameter of call match on the system is described below:

Parameter	Description	Configuration Method
Call Match	Enables or disables the call match feature on the system. **Default:** Enabled	Remote Control Web User Interface

To configure call match via web user interface:

1. Click on **Setting**->**Call Features**.

2. Select the desired value from the pull-down list of **Call Match**.



3. Click **Confirm** to accept the change.

To configure call match via the remote control:

1. Select **Menu**->**Call Features**.
2. Check the **Call Match** checkbox.
3. Press the **Save** soft key to accept the change.

History Record

The system maintains a local call history, which contains call information such as remote party identification, time and date, and call duration. Users can manage call history list via the remote control, web user interface and video conferencing phone. To save call history, you must enable the history record feature on the system in advance. If history record feature is disabled, the system will not save call log and prompt the missed call.

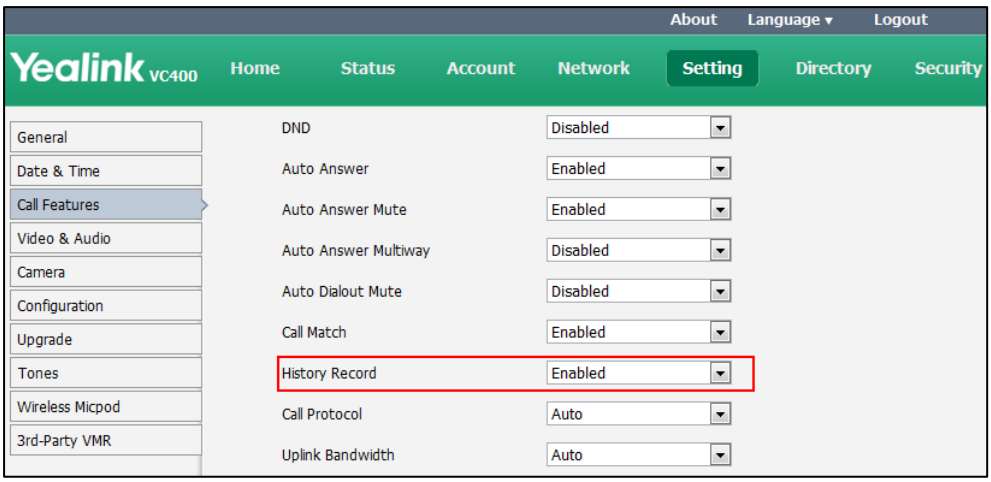
The history record parameter on the system is described below:

Parameter	Description	Configuration Method
History Record	Enables or disables the history record feature on the system. **Default:** Enabled	Remote Control Web User Interface

To configure history record via web user interface:

1. Click on **Setting**->**Call Features**.

2. Select the desired value from the pull-down list of **History Record**.



3. Click **Confirm** to accept the change.

To configure history record via the remote control:

1. Select **Menu**->**Call Features**.
2. Check the **History Record** checkbox.
3. Press the **Save** soft key to accept the change.

Bandwidth

The system automatically detects the available bandwidth for call connection by default. The VC400/VC120 supports connecting to other devices with different bandwidth. If a device with lower bandwidth joins a call, the video quality will stay the same or will not reduce a lot. You can specify the uplink and downlink bandwidths for the system to achieve the best result. Uplink bandwidth is the max bandwidth of outgoing calls, and downlink bandwidth is the max bandwidth of incoming calls. The configurable bandwidths on the system are: 256 kb/s, 384 kb/s, 512 kb/s, 640 kb/s, 768 kb/s, 1024 kb/s, 1280 kb/s, 1500 kb/s, 2000 kb/s, 3000 kb/s, 4000 kb/s, 5000 kb/s, 6000 kb/s. You can configure which bandwidth is to be used when in the dialing screen. The optional maximum bandwidth in dialing screen is the uplink bandwidth.

Note The actual bandwidth depends on the performance of the remote system, and is affected by the quality of the communication channel.

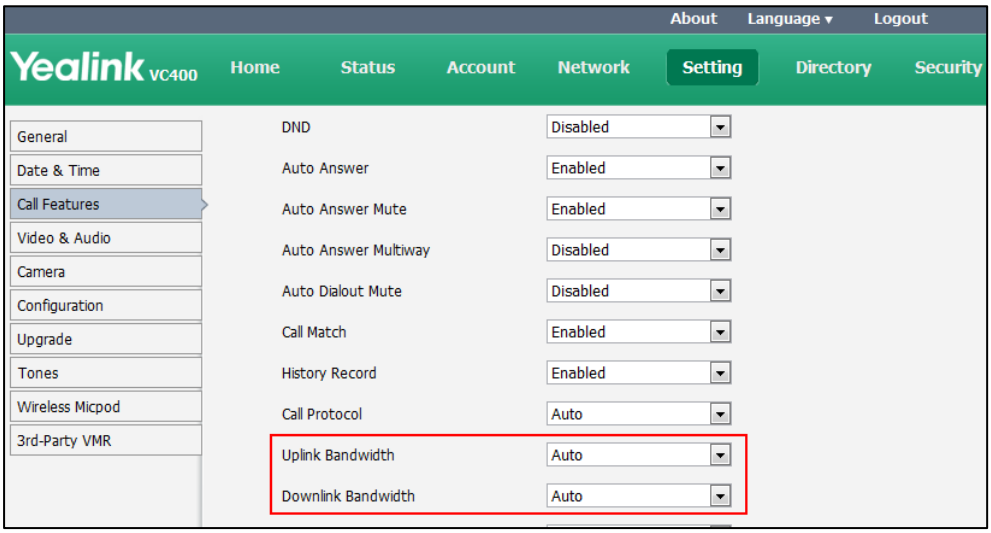
Bandwidth settings parameters on the system are described below:

Parameter	Description	Configuration Method
Uplink Bandwidth	Specifies the maximum transmitting bandwidth for the system. **Default:** Auto	Remote Control Web User Interface

Parameter	Description	Configuration Method
	If **Auto** is selected, the system will select the appropriate uplink bandwidth automatically.	
Downlink Bandwidth	Specifies the maximum receiving bandwidth for the system. **Default:** Auto If **Auto** is selected, the system will select the appropriate downlink bandwidth automatically.	Remote Control Web User Interface

To configure bandwidth settings via web user interface:

1. Click on **Setting**->**Call Features**.
2. Select the desired value from the pull-down list of **Uplink Bandwidth**.
3. Select the desired value from the pull-down list of **Downlink Bandwidth**.



4. Click **Confirm** to accept the change.

To configure bandwidth settings via the remote control:

1. Select **Menu**->**Call Features**->**Bandwidth Settings**.
2. Select the desired value from the pull-down list of **Uplink Bandwidth**.
3. Select the desired value from the pull-down list of **Downlink Bandwidth**.
4. Press the **Save** soft key to accept the change.

Note

The priority of bandwidth is as follows: System bandwidth>Contact bandwidth (refer to add local contacts).

For example: the system bandwidth is 512kbps, if contact bandwidth is set to a value greater than 512bps, than the actual contact bandwidth will be 512bps. If contact bandwidth is set to a value less than 512bps, than the actual contact bandwidth will be the value set by user.

Sharing Content

If a PC is connected to the VC400/VC120 Codec, the system will start a presentation automatically. During a call, both local and remote display devices will display the contents. You can also start/stop a presentation manually during a call. If you disconnect the PC, the presentation will stop automatically.

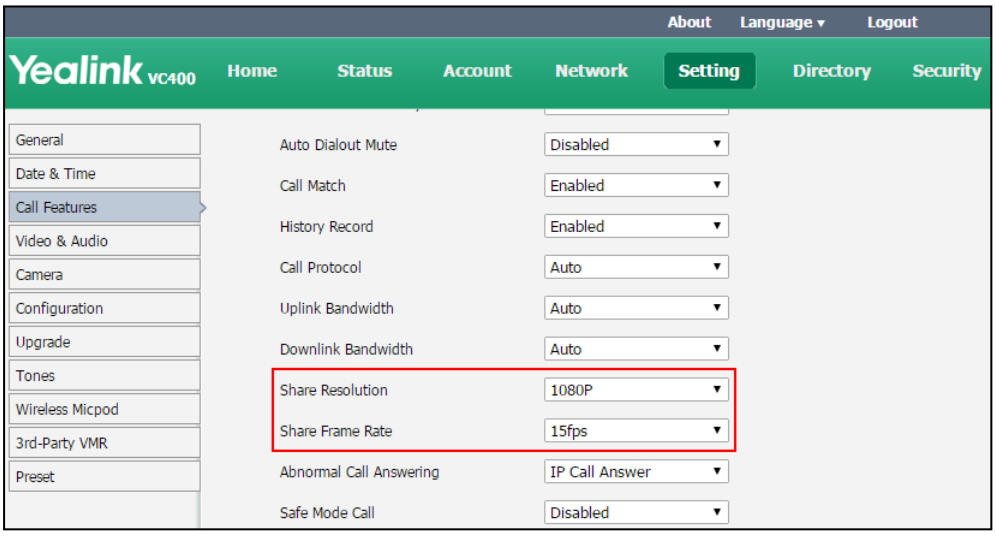
You can configure the resolution and frame rate of the presentation you are sending.

Presentation parameters on the system are described below:

Parameter	Description	Configuration Method
Share Resolution	Specifies the resolution of the presentation. • 1080P • 720P **Default**: 1080P	Web User Interface
Share Frame Rate	Specifies the frame rate of the presentation. • 30fps • 15fps • 5fps **Default**: 15fps	Web User Interface

To configure the presentation via web user interface:

1. Click on **Setting->Call Features**.
2. Select the desired value from the pull-down list of **Share Resolution**.
3. Select the desired value from the pull-down list of **Share Frame Rate**.



4. Click **Confirm** to accept the change.

Ringback Timeout

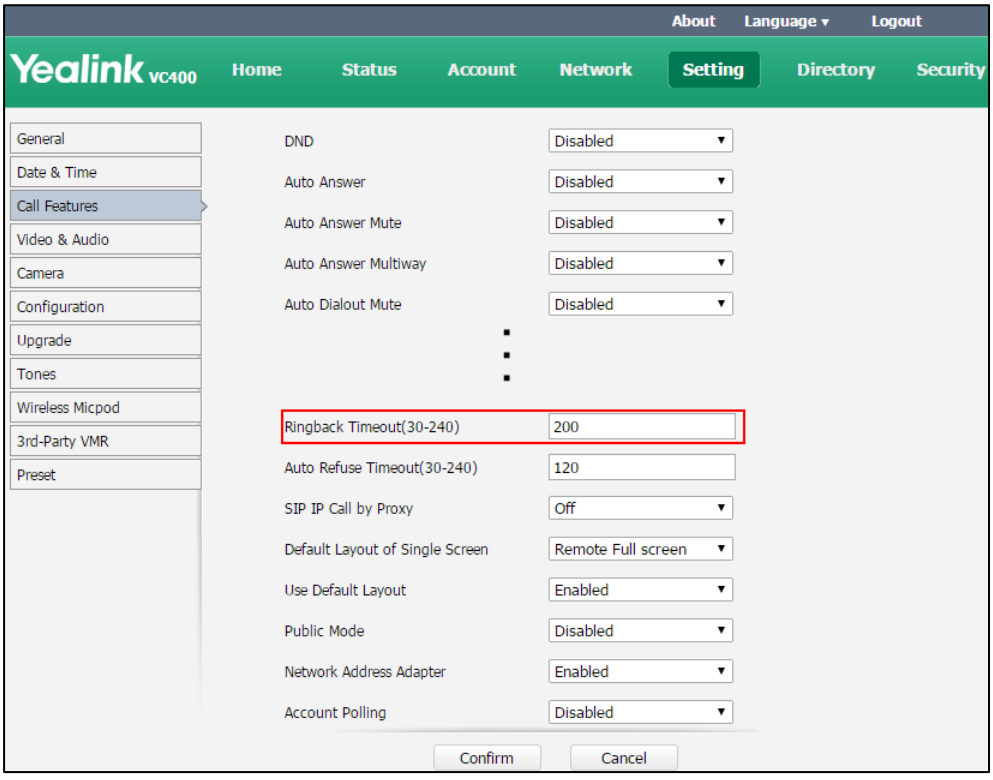
Ringback timeout defines a specific period of time within which the video conferencing system will cancel the dialing if the call is not answered.

The ringback timeout parameter on the system is described below:

Parameter	Description	Configuration Method
Ringback Timeout (30-240)	Configures the duration time (in seconds) in the ringback state. **Default:** 200 If it is set to 200, the system will cancel the dialing if the call is not answered within 200s.	Web User Interface

To configure ringback timeout via web user interface:

1. Click on **Setting**->**Call Features**.
2. Select the desired value from the pull-down list of **Ringback Timeout(30-240)**.



3. Click **Confirm** to accept the change.

Auto Refuse Timeout

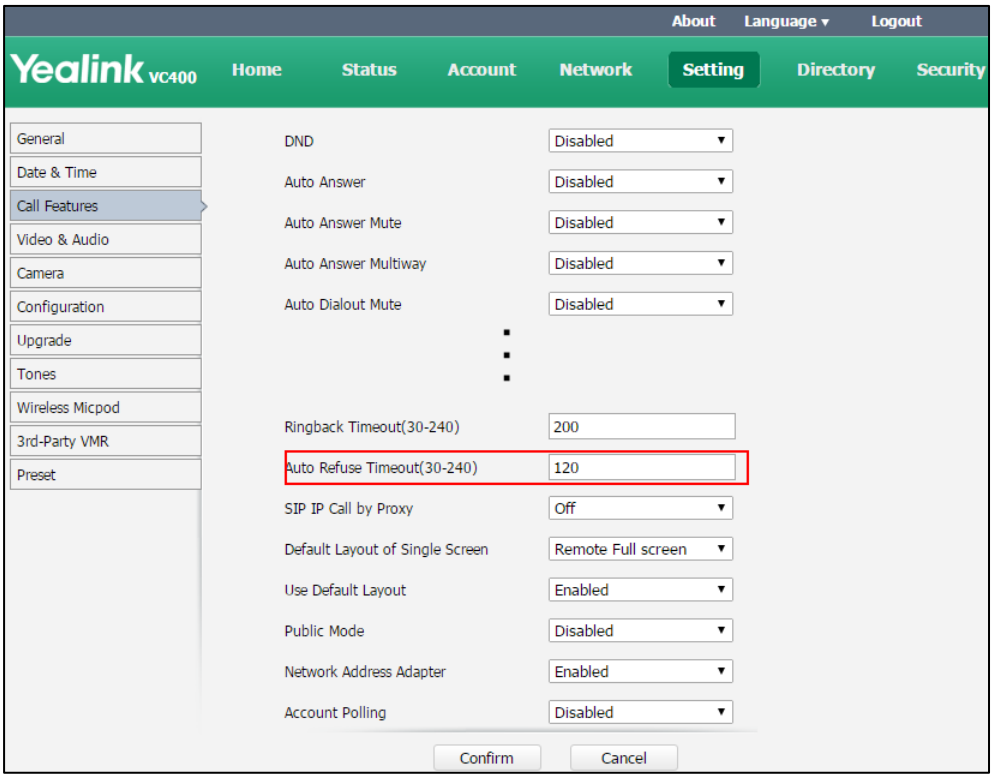
Auto refuse timeout defines a specific period of time within which the video conferencing system will stop ringing if the call is not answered.

The auto refuse timeout parameters on the system are described below:

Parameter	Description	Configuration Method
Auto Refuse Timeout (30-240)	Configures the duration time (in seconds) in the ringing state. **Default:** 120 If it is set to 120, the system will stop ringing if the call is not answered within 120s.	Web User Interface

To configure auto refuse timeout via web user interface:

1. Click on **Setting**->**Call Features**.
2. Select the desired value from the pull-down list of **Auto Refuse Timeout (30-240)**.



3. Click **Confirm** to accept the change.

SIP IP Call by Proxy

If the account of far site is an URI address (Username@Server), local site can use SIP IP call or SIP

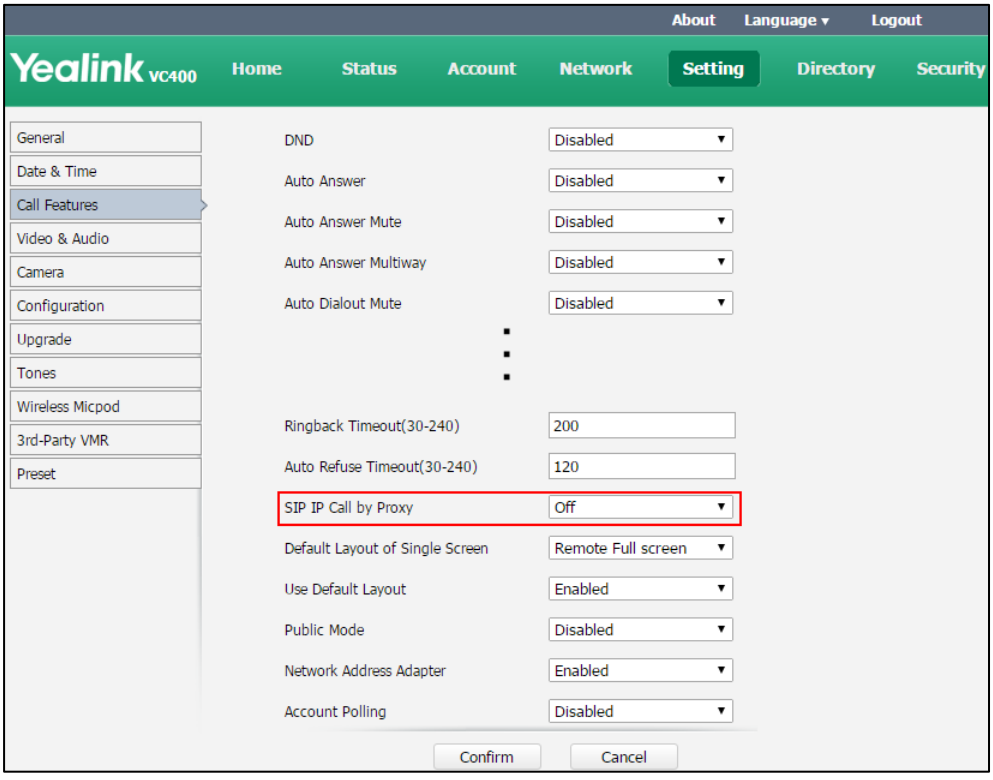
account to connect to the far site.

The SIP IP call by proxy parameters on the system are described below:

Parameter	Description	Configuration Method
SIP IP Call by Proxy	Configures the SIP IP call by proxy. • **Off**–when dialing the URI of the far site, the system actually uses SIP IP address to establish a connection. • **On**–when dialing the URI of the far site, the system uses SIP account to establish a connection. The outbound proxy server should be configured to resolve this URI address. **Default:** Off	Web User Interface

To configure the SIP IP call by proxy via web user interface:

1. Click on **Setting**->**Call Features**.
2. Select the desired value from the pull-down list of **SIP IP Call by Proxy**.



3. Click **Confirm** to accept the change.

Default Layout

When only one display device is connected to the VC400/VC120 Codec (single screen), you can configure the default layout when a call is established.

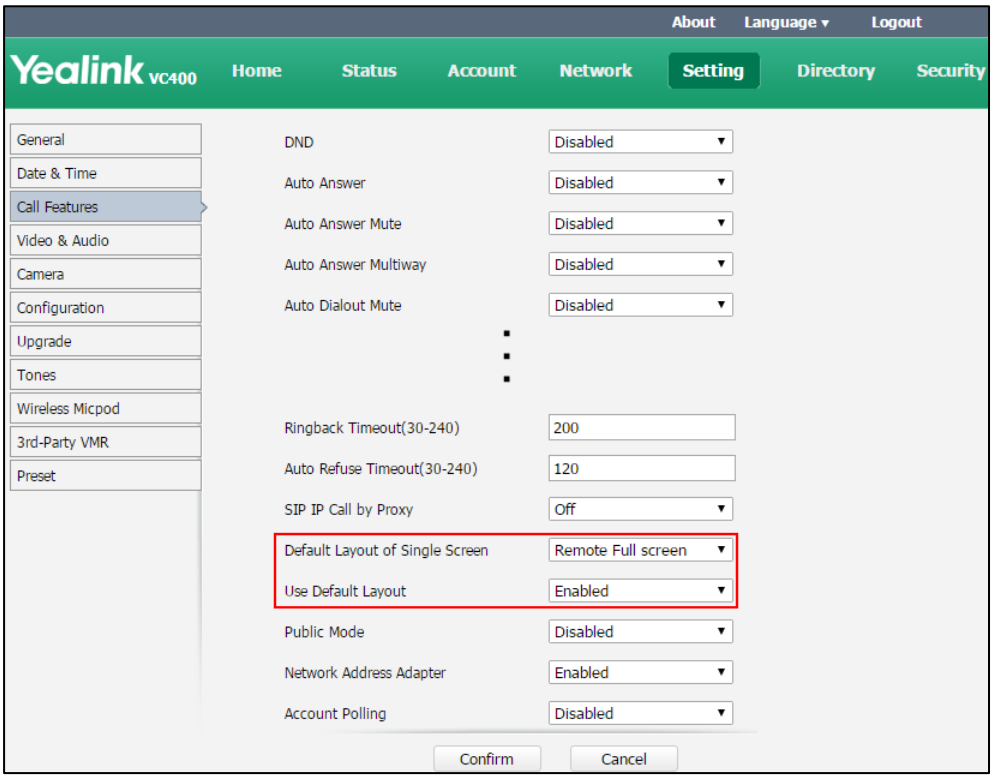
The parameters of default layout are described below:

Parameter	Description	Configuration Method
Default Layout of Single Screen	Configures the default layout of single screen when a call is established. • **Remote big Local small** • **Remote Full screen** • **Equal** **Default:** Remote Full screen If it is set to Remote big Local small, the remote video image is shown in big size, and the local video image along the right side of the screen is shown in small size when a call is established. If it is set to Remote Full screen, the remote video image is shown in full size when a call is established. If it is set to Equal, the remote and local video images are shown in the same size when a call is established.	Web User Interface
Use Default Layout	Enables or disables the system to use default layout. • **Enabled** - the system uses default layout when a call is established. • **Disabled** - the system uses the layout you specified when a call is established. **For example:** in the last call, you set the layout to be equal. The system will use the equal layout by default when a call is established.	Web User Interface

Parameter	Description	Configuration Method
	Default: Enabled	

To configure default layout of single screen via web user interface:

1. Click on **Setting**->**Call Features**.
2. Select the desired value from the pull-down list of **Default Layout of Single Screen**.
3. Select the desired value from the pull-down list of **Use Default Layout**.



4. Click **Confirm** to accept the change.

Public Mode

In your display device, public mode simplifies the idle screen by displaying only local camera and calendar schedules (if you register a YMS account and have a scheduled conference). In public mode, therefore, users can join scheduled calendar and answer calls.

Public mode is disabled by default. If it is enabled, these conditions apply:

- On the display device, status bar and three soft keys are hidden.
- On the video conferencing phone, four soft keys are hidden.
- On your remote control/virtual remote control, you can use the Zoom key, Volume key, Navigation key, OK key, On-hook Key, Mute key and Delete key (for capturing packets)
- On your video conferencing phone, you can use the Volume key, On-hook Key and Mute key.

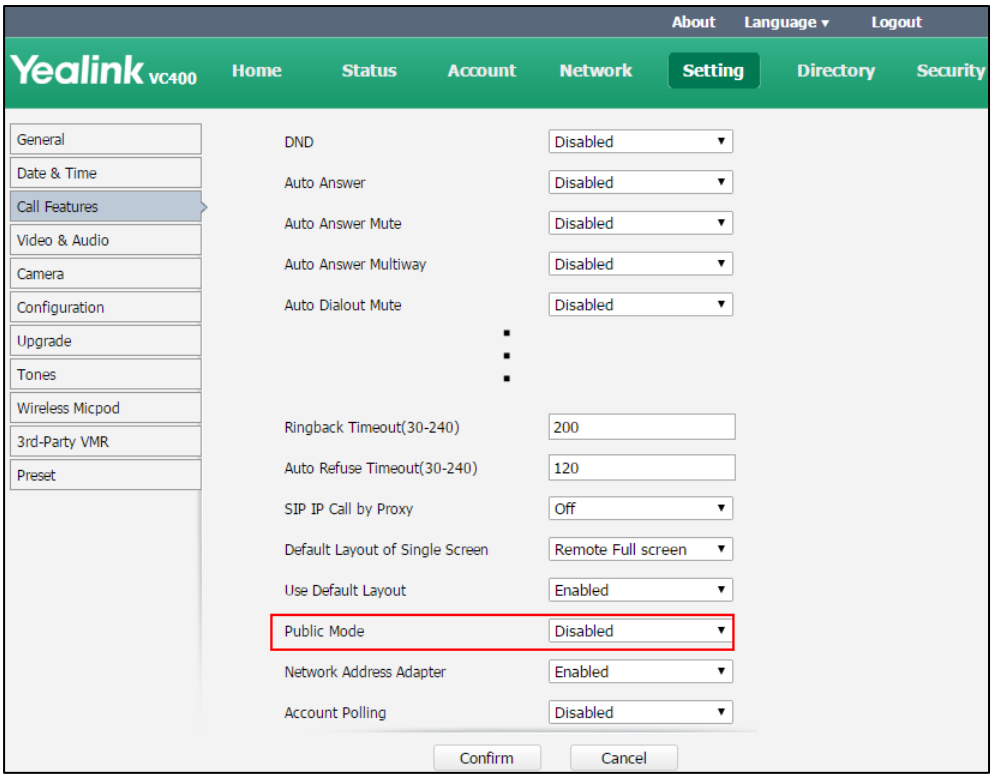
- You can use web user interface or third-party control system to configure your video conferencing system.

The parameters of public mode are described below:

Parameter	Description	Configuration Method
Public Mode	Enables or disables the public mode. **Default:** Disabled	Web User Interface

To configure public mode via web user interface:

1. Click on **Setting**->**Call Features**.
2. Select the desired value from the pull-down list of **Public Mode**.



3. Click **Confirm** to accept the change.

Configuring System Settings

This chapter provides information for making configuration changes for the system, such as language, time and date, backlight of the video conferencing phone, video & audio setting and camera setting:

Topics include:

- General Setting
- Audio Setting
- Adjusting MTU of Video Packets
- Dual-Stream Protocol
- Mix Sending
- Configuring Camera Settings
- Far-end Camera Control
- Camera Control Protocol
- Output Resolution
- USB Configuration
- Video Recording
- ScreenshotTones

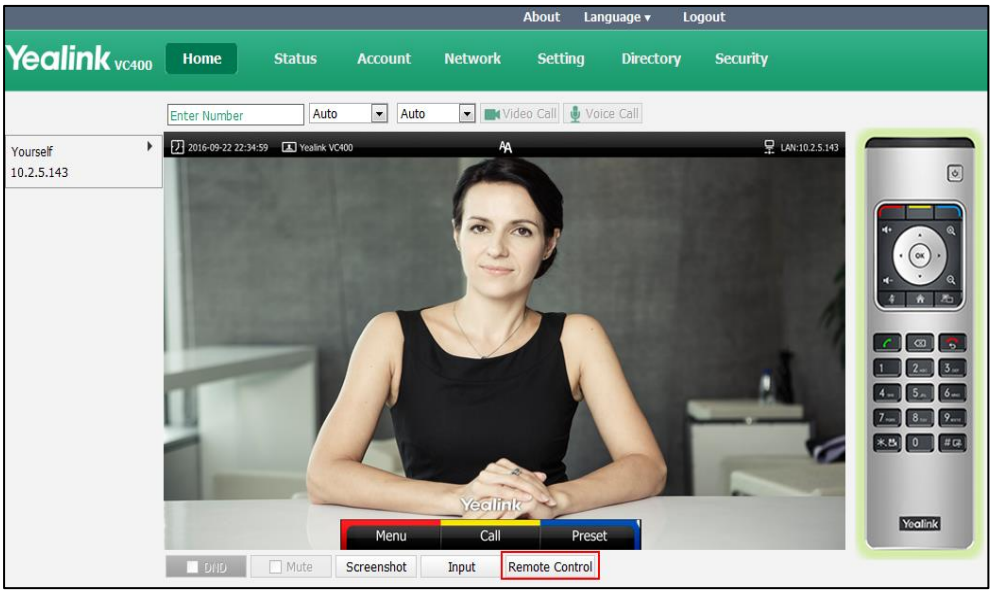
General Setting

Virtual Remote Control

In addition to using the remote control, you can also control the VC400&VC120 video conferencing system via virtual remote control.

To control video conferencing system via the virtual remote control:

1. Click **Home**->**Remote Control** when the system is idle or during a call.



2. Click the keys on the virtual remote control to control the video conferencing system.
3. Click **Remote Control** to hide the virtual remote control.

Configuring Remote Control

If your environment does not use remote control, you can choose to disable remote control feature.

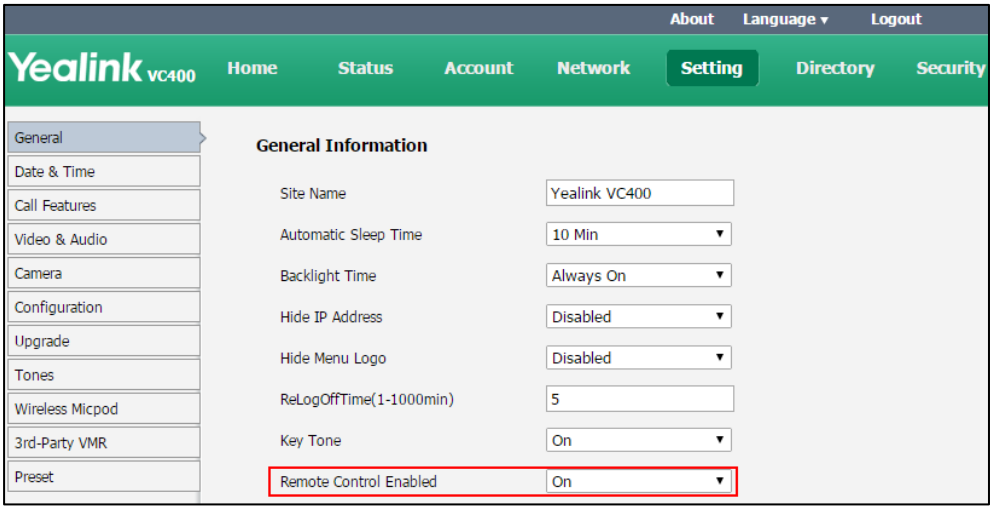
The remote control parameter is described below:

Parameter	Description	Configuration Method
Remote Control Enabled	Enables or disables the remote control feature. **Default:** On **Note**: If it is set to Off, you cannot use remote control and virtual remote control to control your video conferencing system.	Web User Interface

To configure remote control via web user interface:

1. Click **Setting**->**General**.

2. Select desired value from the pull-down list of **Remote Control Enabled**.



3. Click **Confirm** to accept the change.

Site Name

When the system is idle, the site name is displayed on the status bar of display device and video conferencing phone. You can make an IP address call to the far site, the site name will be displayed on the display device of the far site. Site name can consist of letters, numbers or special characters. You can configure the site name of the system via the remote control or web user interface.

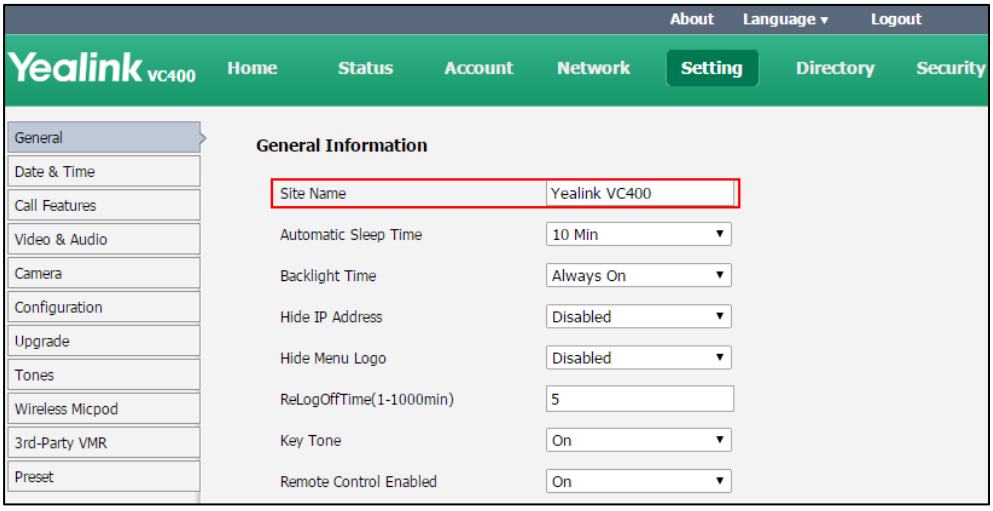
The site name parameter is described below:

Parameter	Description	Configuration Method
Site Name	Configures the site name of the system. **Valid values:** String within 64 characters **Default:** For VC400: Yealink VC400 For VC120: Yealink VC120	Remote Control Web User Interface

To configure the site name via web user interface:

1. Click on **Setting**->**General**.

dit the site name in the **Site Name** field.



2. Click **Confirm** to accept the change.

   The LCD screen of the display device and video conferencing phone will display the changed site name.

To configure the site name via the remote control:

1. Select **Menu**->**Basic**.
2. Edit the site name in the **Site Name** field.
3. Press the **Save** soft key to accept the change.

   The LCD screen of the display device and video conferencing phone will display the changed site name.

Backlight of the Video Conferencing Phone

Backlight determines the brightness of the LCD screen display, allowing users to read easily in dark environments. Backlight time specifies the delay time to turn off the backlight when the phone is inactive.

You can configure the backlight time in the following formats:

- **Always On:** Backlight is turned on permanently.
- **15 s**, **30 s**, **1 Min**, **2 Min**, **5 Min**, **10 Min**, **30 Min:** Backlight is turned off when the phone is inactive after a preset period of time. It is automatically turned on if the status of the phone changes or any key is pressed.

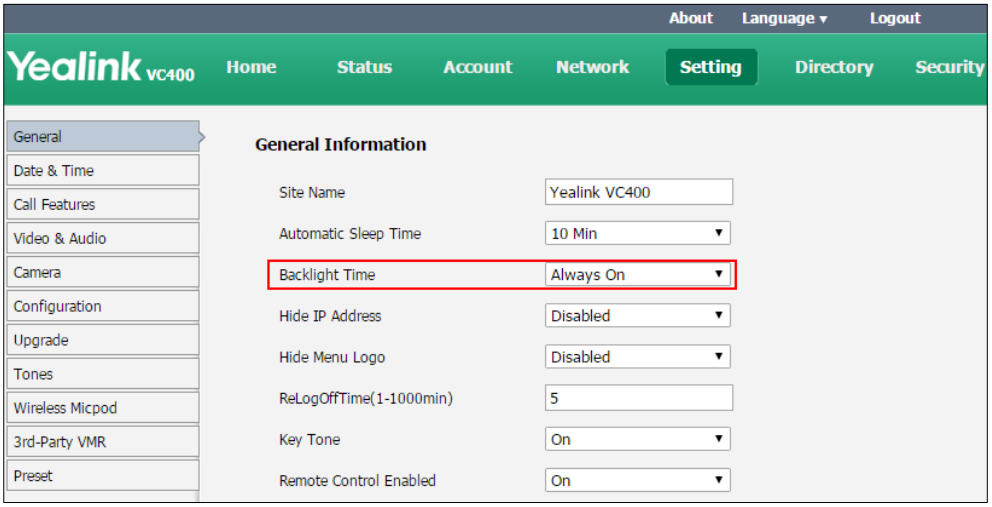
The backlight parameter on video conferencing phone is described below:

Parameter	Description	Configuration Method
Backlight Time	Configure the backlight time of the video conferencing phone.	Web User Interface

Parameter	Description	Configuration Method
	Default: Always On	

To configure the backlight time of the video conferencing phone via web user interface:

1. Click on **Setting**->**General**.
2. Select the desired value from the pull-down list of **Backlight Time**.



3. Click **Confirm** to accept the change.

Language

The default language of the LCD screen of the display device and the video conferencing phone is English, and you can change it via the remote control. The video conferencing phone will detect and use the same language as the display device.

The default language of the web user interface is English. You can change the web user interface language for web user interface.

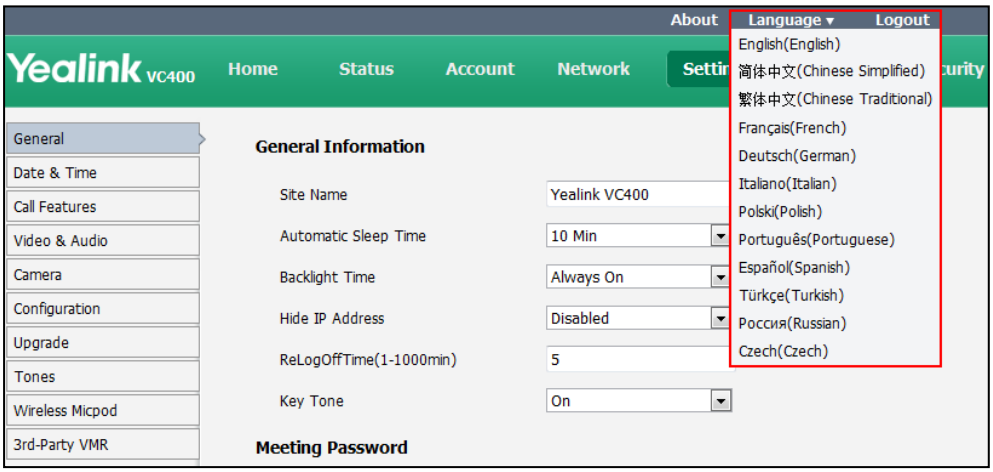
The available languages for system are English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian and Czech.

The language parameters on the system are described below:

Parameter	Description	Configuration Method
Language	Specifies the language for the web user interface	Web User Interface
Language	Specifies the language for the LCD screen of the display device and the video conferencing phone. **Default:** English	Remote Control

To specify the language for the web user interface via web user interface:

1. Click **Language** at the top of the web page.
2. Select the desired language from the pull-down list of **Language**.



To specify the language for the display device and the video conferencing phone via the remote control:

1. Select **Menu**->**Basic**.
2. Select the desired language from the pull-down list of **Language**.
3. Press the **Save** soft key to accept the change.

Date & Time

Time and date are displayed on the idle screen of the display device and the video conferencing phone. Time and date are synced automatically from the NTP server by default. The default NTP server is cn.pool.ntp.org. The NTP server is configurable manually or obtained by DHCP via DHCP Option 42. The phone will use the NTP server obtained by DHCP preferentially. If the system cannot obtain the time and date from the NTP server, you need to manually configure them. The time and date can use one of several different formats.

Time Zone

A time zone is a region on Earth that has a uniform standard time. It is convenient for areas in close commercial or other communication to keep the same time. When configuring the system to obtain the time and date from the NTP server, you must set the time zone.

Daylight Saving Time

Daylight Saving Time (DST) is the practice of temporary advancing clocks during the summertime so that evenings have more daylight and mornings have less. Typically, clocks are adjusted forward one hour at the start of spring and backward in autumn. Many countries have used DST at various times, details vary by location. DST can be adjusted automatically from the

time zone configuration. Typically, there is no need to change this setting.

DST parameters are described below:

Parameter	Description	Configuration Method
DHCP Time	Enables or disables the system to update time with the offset time obtained from the DHCP server. **Default:** Disabled **Note:** it is only available to GMT 0.	Web User Interface
Time Zone	Configures the time zone. **Default:** +8 China (Beijing)	Remote Control Web User Interface
Primary Server/NTP Primary Server	Configures the primary NTP server. **Default:** cn.pool.ntp.org	Remote Control Web User Interface
Secondary Server/NTP Secondary Server	Configures the secondary NTP server. **Default:** cn.pool.ntp.org	Remote Control Web User Interface
Synchronism **(15~86400s)**	Configures the interval (in minutes) for the system to synchronize time and date with NTP server. **Default**: 1000.	Web User Interface
Daylight Saving Time	Configures the Daylight Saving Time (DST) type. The available types for the system are: ● **Disabled**-not use DST. ● **Enabled**-use DST. You can manually configure the start time, end time and offset according to your needs. ● **Automatic**-use DST. DST will be configured automatically. You do not need to	Remote Control Web User Interface

Parameter	Description	Configuration Method
	manually configure the start time, end time and offset. **Default:** Automatic	
Fixed Type	Configures the DST calculation methods. ● **By Date**- specifies the month, day and hour to be the DST start /end date. ● **By Week**- specifies the month, week, day and hour the DST start /end date. **Note:** It only works if the value of Daylight Saving Time is set to Enabled.	Web User Interface
Start Date	When the DST calculation method is set to **By Date**. Configures the time to start DST. **Note:** It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
End Date	When the DST calculation method is set to **By Date**. Configures the time to end DST. **Note:** It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
DST Start Month **DST Start Day of Week** **DST Start Day of Week Last in Month** **Start Hour of Day**	When the DST calculation method is set to **By Week**. Configures the time to start DST. **Note**: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
DST Stop Month **DST Stop Day of Week** **DST Stop Day of Week Last**	When the DST calculation method is set to **By Week**, Configures the time to end DST.	Web User Interface

Parameter	Description	Configuration Method
in Month **End Hour of Day**	**Note**: It only works if the value of the Daylight Saving Time is set to Enabled.	
Offset(minutes)	Configures the DST offset time (in minutes). **Valid values**: -300 to +300. **Note**: It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
Time Type	Configures the DST time type. ● **SNTP:** obtain the time and date from the NTP server automatically. ● **Manual Time:** configure the time and date manually. **Default:** SNTP	Remote Control Web User Interface
Time Format/ Time	Configures the time format. ● Hour12 ● Hour24 **Default:** Hour 24	Remote Control Web User Interface
Date Format/Date	Configures the date format. ● WWW MMM DD ● DD-MMM-YY ● YYYY-MM-DD ● DD/MM/YYYY ● MM/DD/YY ● DD MMM YYYY ● WWW DD MMM **Default:** YYYY-MM-DD	Remote Control Web User Interface

To configure the NTP server, time zone and DST via web user interface:

1. Click on **Setting**->**Date &Time**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.

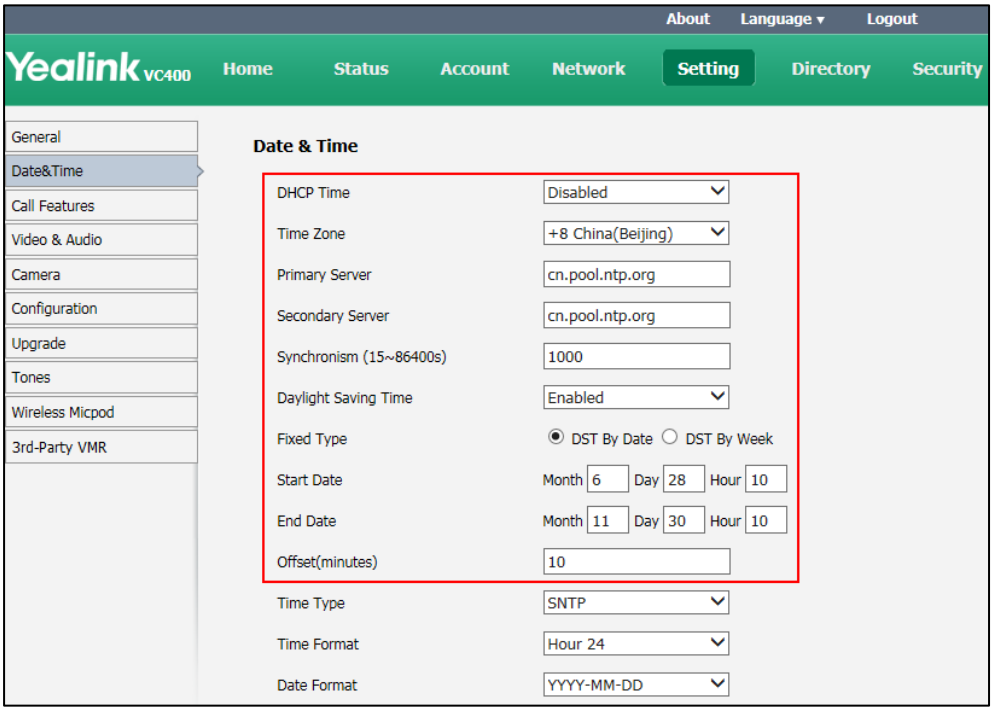
4. Enter the domain names or IP addresses in the **Primary Server** and **Secondary Server** fields respectively.
5. Enter the desired time interval in the **Synchronism (15~86400s)** field.
6. Select the desired value from the pull-down list of **Daylight Saving Time**.

   If you select **Enabled**, do one of the following:

   - Mark the **DST By Date** radio box in the **Fixed Type** field.

     Enter the start time in the **Start Date** field.

     Enter the end time in the **End Date** field.

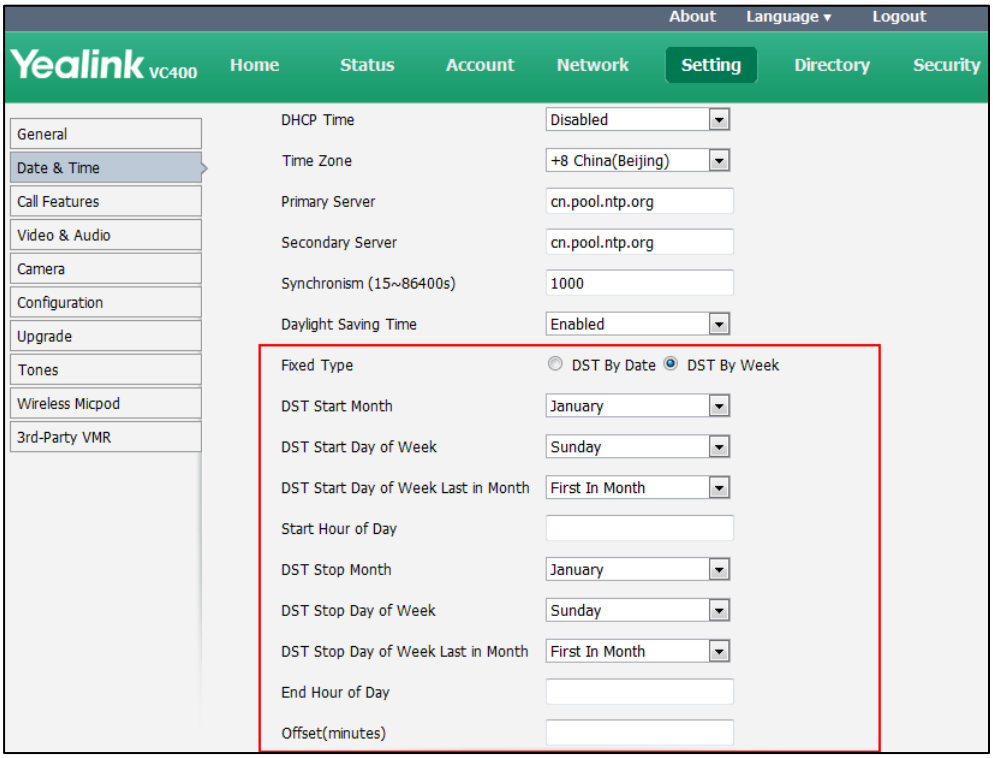


   - Mark the **DST By Week** radio box in the **Fixed Type** field.

     Select the desired values from the pull-down lists of **DST Start Month**, **DST Start Day of Week**, **DST Start Day of Week Last in Month**, **DST Stop Month**, **DST Stop Day of Week** and **DST Stop Day of Week Last in Month**.

     Enter the desired time in the **Start Hour of Day** field.

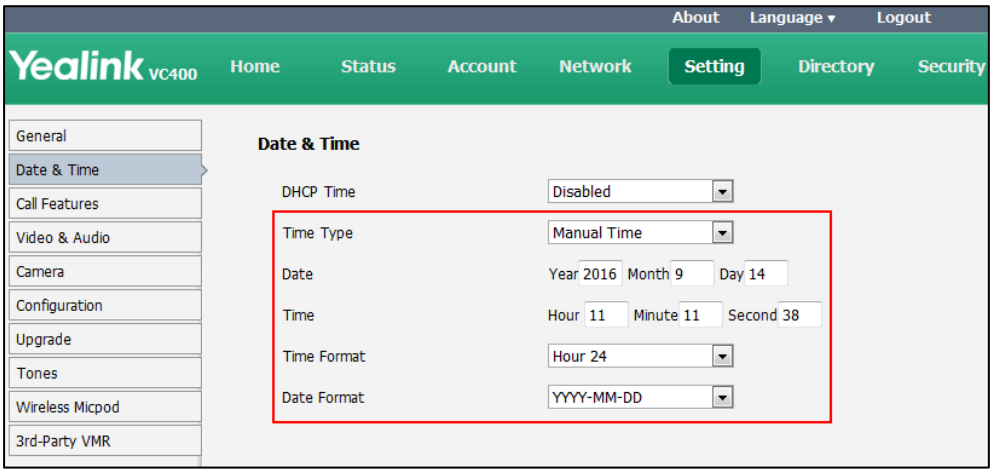
Enter the desired time in the **End Hour of Day** field.



7. Enter the desired offset time in the **Offset (minutes)** field.
8. Click **Confirm** to accept the change.

To configure the time and date manually via web user interface:

1. Click on **Setting->Date& Time**.
2. Select **Manual Time** from the pull-down list of **Time Type**.
3. Enter the current date in the **Date** field.
4. Enter the current time in the **Time** field.
5. Select the desired value from the pull-down list of **Time Format**.
6. Select the desired value from the pull-down list of **Date Format**.



7. Click **Confirm** to accept the change.

To configure the time and date format via the remote control:

1. Select **Menu**->**Basic**->**Date & Time**.
2. Configure the desired values.
3. Press the **Save** soft key to accept the change.

   The time and date displayed on the LCD screen of the display device and video conferencing phone will change accordingly.

Automatic Sleep Time

The system will enter the sleep mode automatically when it has been inactive for a period of time (the default time is 10 minutes). When the system is in sleep mode, it can still accept incoming calls. The display device will prompt "No Signal", and the LCD screen of the video conferencing phone prompts "Sleeping Press any key to resume". You can press any key on the remote control or the video conferencing phone to wake the system up. When receiving a call, the system will be woken up automatically.

You can change the automatic sleep time via the remote control or web user interface. You can also press the sleep key on the remote control to make the system sleep immediately.

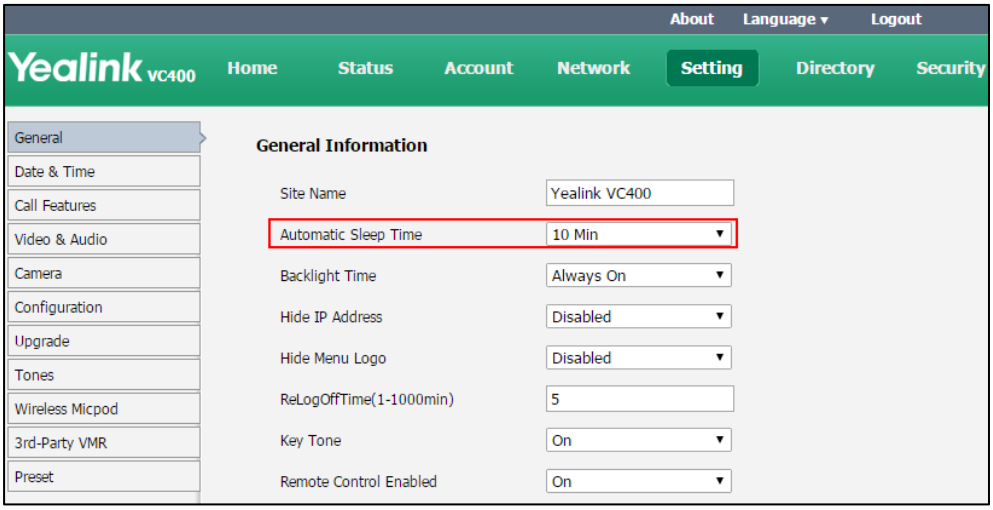
The automatic sleep time is described below:

Parameter	Description	Configuration Method
Automatic Sleep Time	Configures the inactive time (in minutes) before the system enters sleep mode. **Default:** 10 Min **Note**: During setup wizard, the automatic sleep time feature is disabled automatically. To protect the display device, you should configure the automatic sleep time immediately.	Remote Control Web User Interface

To configure the automatic sleep time via web user interface:

1. Click on **Setting**->**General**.

2. Select desired value from the pull-down list of **Automatic Sleep Time**.



3. Click **Confirm** to accept the change.

To configure the automatic sleep time via the remote control:

1. Select **Menu**->**Basic**.
2. Select desired value from the pull-down list of **Automatic Sleep Time**.
3. Press the **Save** soft key to accept the change.

Hiding IP Address

The status bar of the display device displays IP address. You can choose to hide IP address on the status bar.

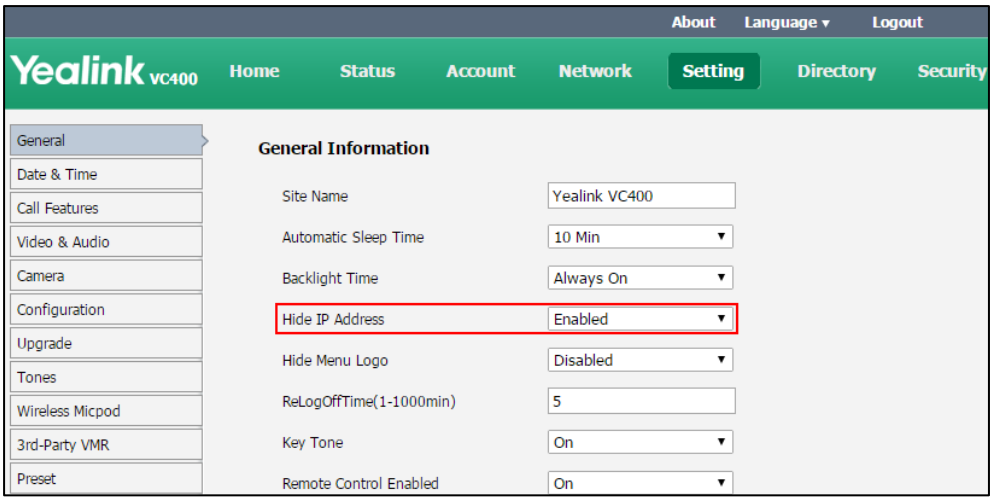
Parameter of hiding IP address on the system is described below:

Parameter	Description	Configuration Method
Hide IP address	Enables or disables the system to hide IP address on the status bar. **Default:** Disabled	Web User Interface

To hide IP address via web user interface:

1. Click on **Setting**->**General**.

2. Select **Enabled** from the pull-down list of **Hide IP Address**.



3. Click **Confirm** to accept the change.

Hiding Menu Logo

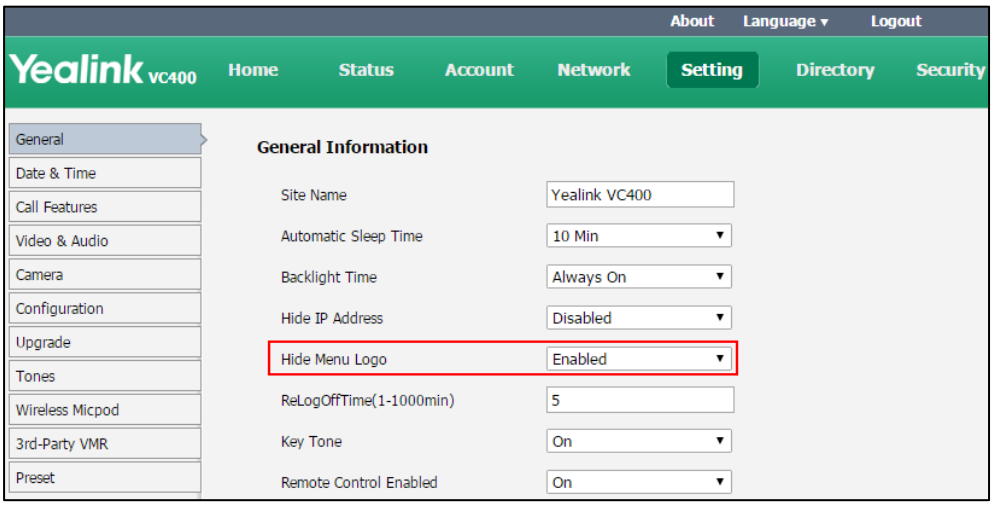
When the system is idle, a Yealink logo is shown on the display device. You can hide the Yealink logo as needed to achieve the best video effects.

Parameter of hiding menu logo on the system is described below:

Parameter	Description	Configuration Method
Hide Menu Logo	Enables or disables the system to hide Yealink logo on the idle screen. **Default:** Disabled	Web User Interface

To enable the hiding menu logo feature via web user interface:

1. Click on **Setting->General**.
2. Select the **Enabled** from the pull-down lists of **Hide Menu Logo**.



3. Click **Confirm** to accept the change.

   The Yealink logo disappears from the display device.

Hiding Icons in a Call

During a call, the system will display some information and icons (such as call time, mute icon and recording icon) by default, you can know the call status from these information and icons. You can also hide these icons as needed to achieve the best video effects.

Parameters of hiding icons in a call feature on the system are described below:

Parameter	Description	Configuration Method
Time Icon	Enables or disables the system to hide call time during a call. • **Disabled**- the system does not display call time during a call. • **Hide with operation menu** - the system displays call time during a call, but the call time will hide with operation menu. • **Enabled**- the system displays call time during a call. **Default:** Hide with operation menu	Web User Interface
Mute Icon	Enables or disables the system to hide mute icon ( ) during a call. • **Disabled**- the system does not display mute icon during a call. • **Hide with operation menu** - the system displays mute icon during a call, but the mute icon will hide with operation menu. • **Enabled**- the system displays mute icon during a call. **Default:** Disabled	Web User Interface
Camera Icon	Enables or disables the system to hide camera icon ( ) during a call. • **Disabled**- the system does not display camera icon during a	Web User Interface

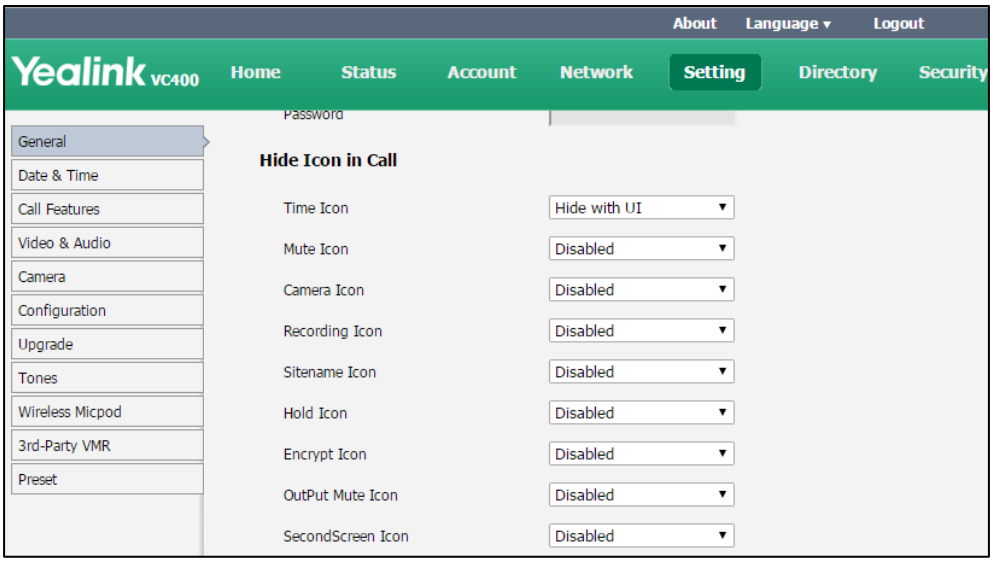
Parameter	Description	Configuration Method
	call. • **Hide with operation menu** - the system displays camera icon during a call, but the camera icon will hide with operation menu. • **Enabled**- the system displays camera icon during a call. **Default:** Disabled	
Recording Icon	Enables or disables the system to hide recording icon ( ) during a call. • **Disabled**- the system does not display recording icon during a call. • **Hide with operation menu** - the system displays recording icon during a call, but the recording icon will hide with operation menu. • **Enabled**- the system displays recording icon during a call. **Default:** Disabled	Web User Interface
Sitename Icon	Enables or disables the system to hide site name icon during a call. • **Disabled**- the system does not display site name icon during a call. • **Hide with operation menu** - the system displays site name icon during a call, but the site name icon will hide with operation menu. • **Enabled**- the system displays site name icon during a call. **Default:** Disabled	Web User Interface
Hold Icon	Enables or disables the system to hide hold icon ( ) during a call.	Web User Interface

Parameter	Description	Configuration Method
	• **Disabled**- the system does not display hold icon during a call. • **Hide with operation menu** - the system displays hold icon during a call, but the hold icon will hide with operation menu. • **Enabled**- the system displays hold icon during a call. **Default:** Disabled	
Encrypt Icon	Enables or disables the system to hide encrypt icon ( ) during a call. • **Disabled**- the system does not display encrypt icon during a call. • **Hide with operation menu** - the system displays encrypt icon during a call, but the encrypt icon will hide with operation menu. • **Enabled**- the system displays encrypt icon during a call. **Default:** Disabled	Web User Interface
OutPut Mute Icon	Enables or disables the system to hide output mute icon (output volume is set to 0:) during a call. • **Disabled**- the system does not display output mute icon during a call. • **Hide with operation menu** - the system displays output mute icon during a call, but the output mute icon will hide with operation menu. • **Enabled**- the system displays output mute icon during a call. **Default:** Disabled	Web User Interface

Parameter	Description	Configuration Method
SecondScreen Icon	Enables or disables the system to hide second screen icon ( ) during a call. • **Disabled**- the system does not display second screen icon during a call. • **Hide with operation menu** - the system displays second screen icon during a call, but the icon will hide with operation menu. • **Enabled**- the system displays second screen icon during a call. **Default:** Disabled	Web User Interface

To hide icons in a call via web user interface:

1. Click on **Setting->General**.
2. Select the desired values from the pull-down lists of **Time Icon**, **Mute Icon**, **Camera Icon**, **Recording Icon**, **Sitename Icon**, **Hold Icon**, **Encrypt Icon**, **OutPut Mute Icon**, and **SecondScreen Icon**.



3. Click **Confirm** to accept the change.

Relog Offtime

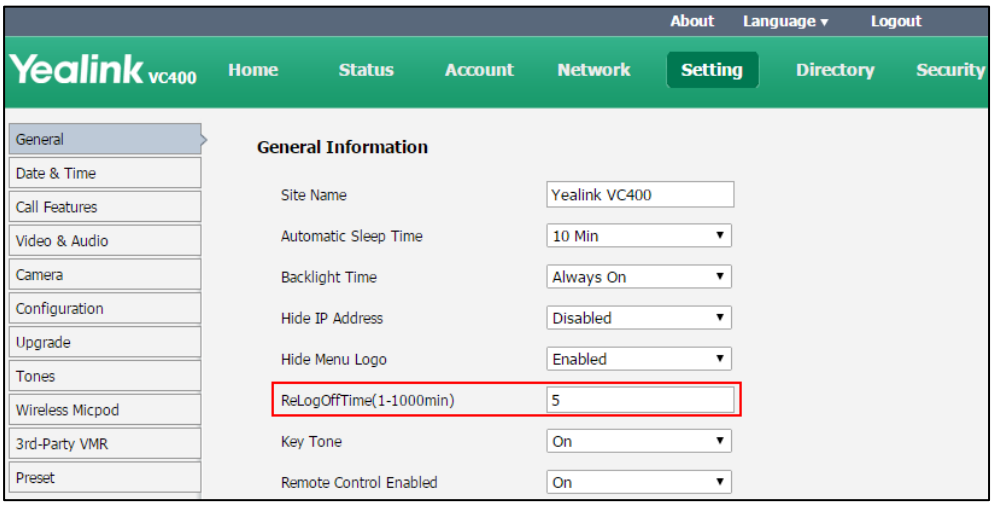
The system will log out of the web user interface automatically after being inactive for a period of time (default: 5 minutes). You need to re-enter the user name and password to login. You can only configure the relog offtime via web user interface.

The relog offtime parameter is described below:

Parameter	Description	Configuration Method
ReLogOffTime (1-1000min)	Configures the inactive time (in minutes) before the system logs out of the web user interface automatically. **Default:** 5	Web User Interface

To configure the relog offtime via web user interface:

1. Click on **Setting->General**.
2. Enter the desired time in the **ReLogOffTime (1-1000min)** field.



3. Click **Confirm** to accept the change.

Key Tone

You can enable the key tone feature for the system to make a keyboard click sound effect (key tone) when pressing any key on the remote control. If you disable this feature or system ringer volume is adjusted to 0, the system will not play a key tone when you press any key on the remote control.

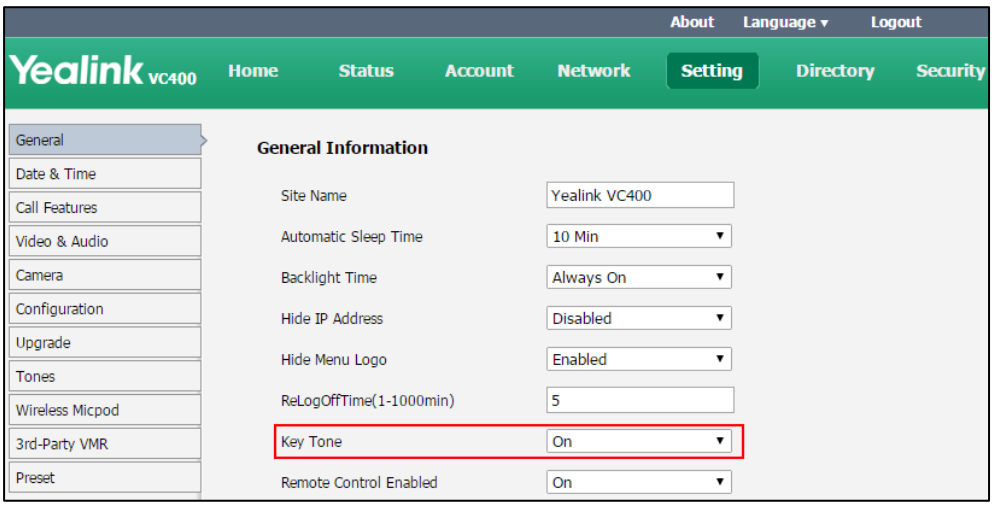
Key tone is configurable via the remote control or web user interface.

The key tone parameter is described below:

Parameter	Description	Configuration Method
Key Tone	Enables or disables the key tone. **Default:** On	Remote Control Web User Interface

To configure the key tone via web user interface:

1. Click on **Setting->General**.
2. Select the desired value from the pull-down list of **Key Tone**.



3. Click **Confirm** to accept the change.

To configure the key tone via the remote control:

1. Select **Menu->Basic**.
2. Mark the radio box in the **Key Tone** field.
3. Press the **Save** soft key to accept the change.

Meeting Password

VC400 supports meeting password feature. If an 8-way MCU is imported to your VC120, yourVC120 will support meeting password feature.

Meeting password is used to manage the incoming calls. If you enable this feature, only the people who know the meeting password can dial your system. If your system is idle, meeting password can prevent people from dialing your system. If your system is during a call or conducting a conference call, meeting password can prevent unauthorized people from joining.

Meeting password is configurable via the remote control or web user interface.

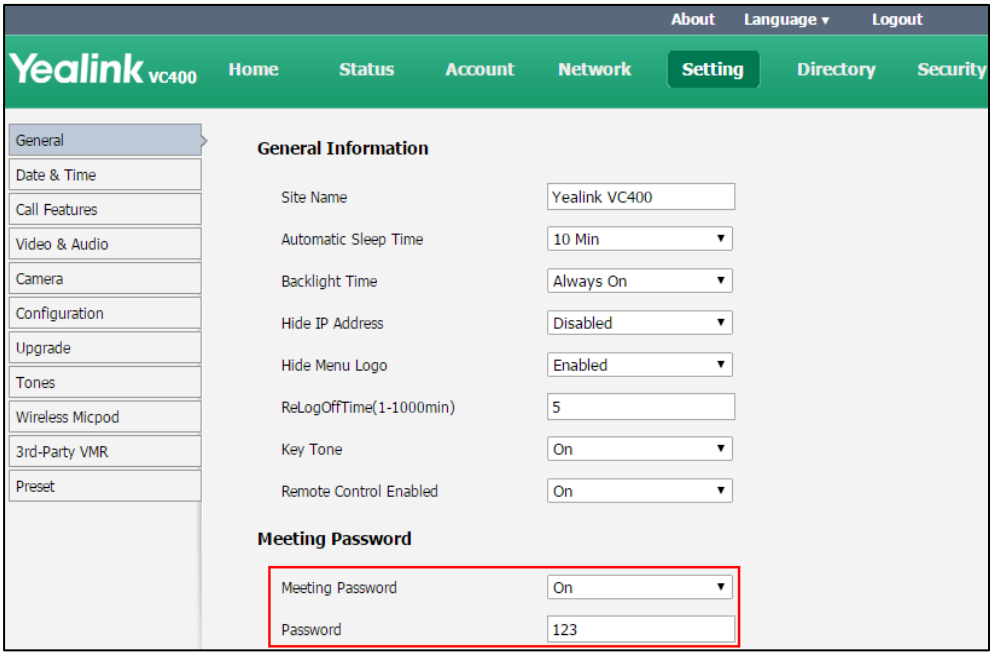
Note You can add specified users to the meeting whitelist. Users in the whitelist can dial your system without meeting password. For more information on meeting whitelist, refer to Meeting Whitelist on page 186.

The meeting password parameters are described below:

Parameter	Description	Configuration Method
Meeting Password	Enable or disable the meeting password feature. **Default:** Off	Remote Control Web User Interface
Password	Configures the meeting password. **Default:** blank	Remote Control Web User Interface

To configure the meeting password via web user interface:

1. Click on **Setting**->**General**.
2. Select the desired value from the **Meeting Password** pull-down list.
3. Enter the desired value in the **Password** field.



4. Click **Confirm** to accept the change.

To configure the meeting password via the remote control:

1. Select **Menu**->**Basic**->**Meeting Password**.
2. Check the **Meeting Password** checkbox.
3. Enter the meeting password in the **Password** field.
4. Press the **Save** soft key to accept the change.

People can press **IP##meeting password** or **meeting password@IP** to dial your system or join your conference call. For example: your IP address is 10.3.6.201 and you set 123 as your meeting password. People should press **10.3.6.201##123** or **123@10.3.6.201** to dial your system or join your conference call. If people call you without a meeting password or with a wrong meeting password, the call will fail.

Meeting Whitelist

VC400 supports meeting whitelist feature. If an 8-way MCU is imported to your VC120, your VC120 will support meeting whitelist feature.

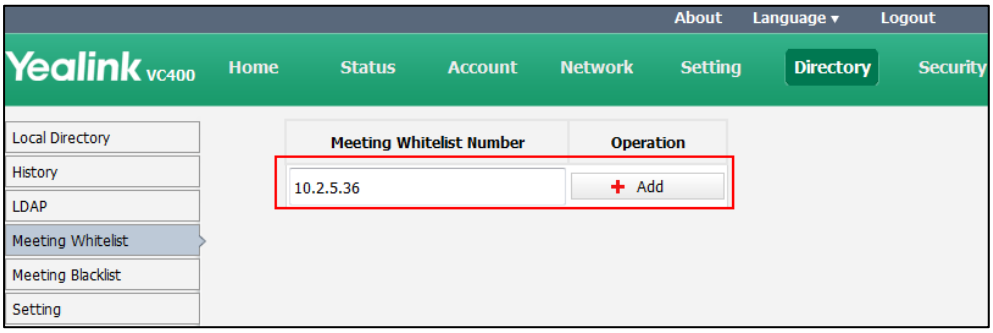
You can add the IP address, account or domain name of the remote system to the meeting whitelist. Users in the whitelist can dial your VC400/VC120 or join your conference call directly without meeting password even if you have enabled the meeting password feature. VC400 /VC120 supports up to 100 whitelist records. Meeting whitelist is configurable via web user interface only.

The meeting whitelist parameter is described below:

Parameter	Description	Configuration Method
Meeting Whitelist Number	Add the IP address, account or domain name of the remote system to the meeting whitelist. **Default:** blank	Remote Control Web User Interface

To add the meeting whitelist numbers via web user interface:

1. Click on **Directory**->**Meeting Whitelist.**
2. Enter the user's IP, account or domain name in the **Meeting Whitelist Number** field.

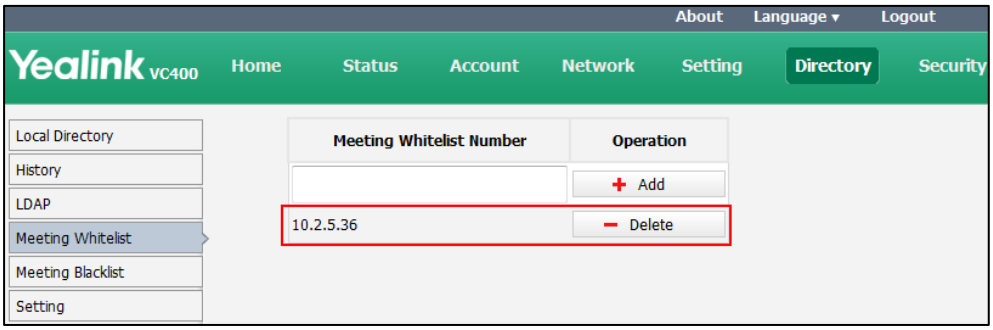


3. Click **Add**.
4. Repeat step 2-3 to add more numbers to the whitelist.

To delete the meeting whitelist numbers via web user interface:

1. Click on **Directory**->**Meeting Whitelist.**

2. Click **Delete** beside the numbers that you want to delete.



The web user interface prompts the message "Warning: Are you sure delete the white number?".

3. Click **Confirm**.

Meeting Blacklist

You can add the IP address, account or domain name of the remote system to the meeting blacklist. VC400 /VC120 will refuse incoming calls from the blacklist automatically. If the user is in both meeting whitelist and meeting blacklist, the blacklist has higher priority. VC400 /VC120 will still refuse incoming calls from this user. VC400 /VC120 will not remind incoming calls and save call history from blacklist.

VC400 /VC120 supports up to 100 blacklist records. Blacklist is configurable via web user interface only.

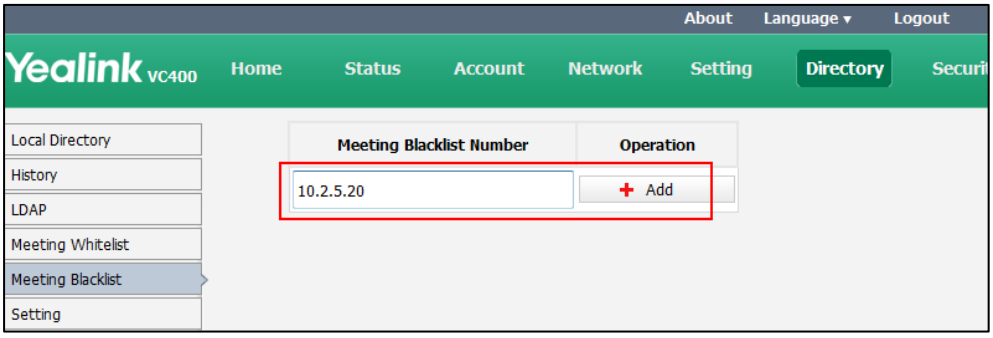
The blacklist parameter is described below:

Parameter	Description	Configuration Method
Meeting Blacklist Number	Add the IP address, account or domain name of the remote system to the meeting blacklist. **Default:** blank	Web User Interface

To add the blacklist numbers via web user interface:

1. Click on **Directory**->**Meeting Blacklist.**
2. Enter the user's IP address, account or domain name in the **Meeting Blacklist Number** field.

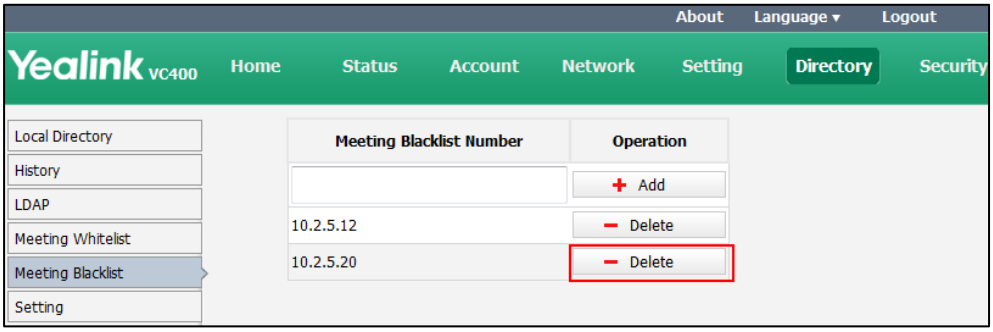
3. Click **Add**.



4. Repeat step 2-3 to add more numbers to the meeting blacklist.

To delete the blacklist numbers via web user interface:

1. Click on **Directory**->**Meeting Blacklist.**
2. Click **Delete** beside the numbers that you want to delete.



The web user interface prompts the message "Warning: Are you sure delete the black number?".

3. Click **Confirm**.

Keyboard Input Method

The on-screen keyboard supports English and Russian input methods.

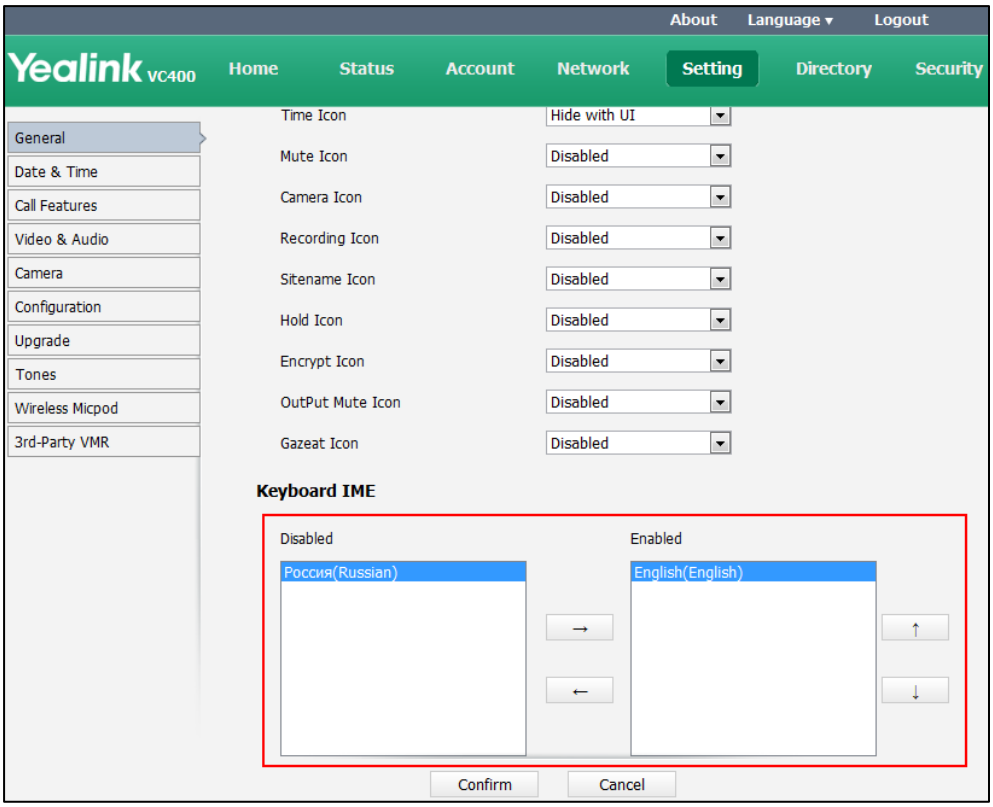
You can enter characters using the input method only when the input method is enabled. Changing keyboard input method is configurable via web user interface only.

To configure keyboard input method via web user interface:

1. Click on **Setting** ->**General**.
2. In the **Keyboard IME** block, select the desired list from the **Disabled** column and click →.

   The selected input method appears in the **Enabled** column.
3. Repeat step 2 to add more input methods to the **Enabled** column.
4. (Optional.) To remove a list from the **Enabled** column, select the desired list and then click ←.

5. To adjust the display order of the enabled input methods, select the desired list, and click ↑ or ↓ .



6. Click **Confirm** to accept the change.

To change keyboard input method via the remote control:

1. Press (**Keyboard** soft key) or (**Keyboard** soft key).
   The display device appears the on-screen keyboard.
2. Press (**abc** soft key) to change the input method.

Audio Setting

Audio Output Device

The system supports the following audio output devices:

- **Auto**
- **VCS Phone**
- **HDMI**
- **Line Output**

By default, the system automatically selects the audio output devices with highest priority. The priority is: VCS Phone>HDMI>Line Output. If the audio output device with highest priority is

removed from the Codec, the system will select the next highest priority device.

You can also specify the desired audio output device via the remote control or the web user interface.

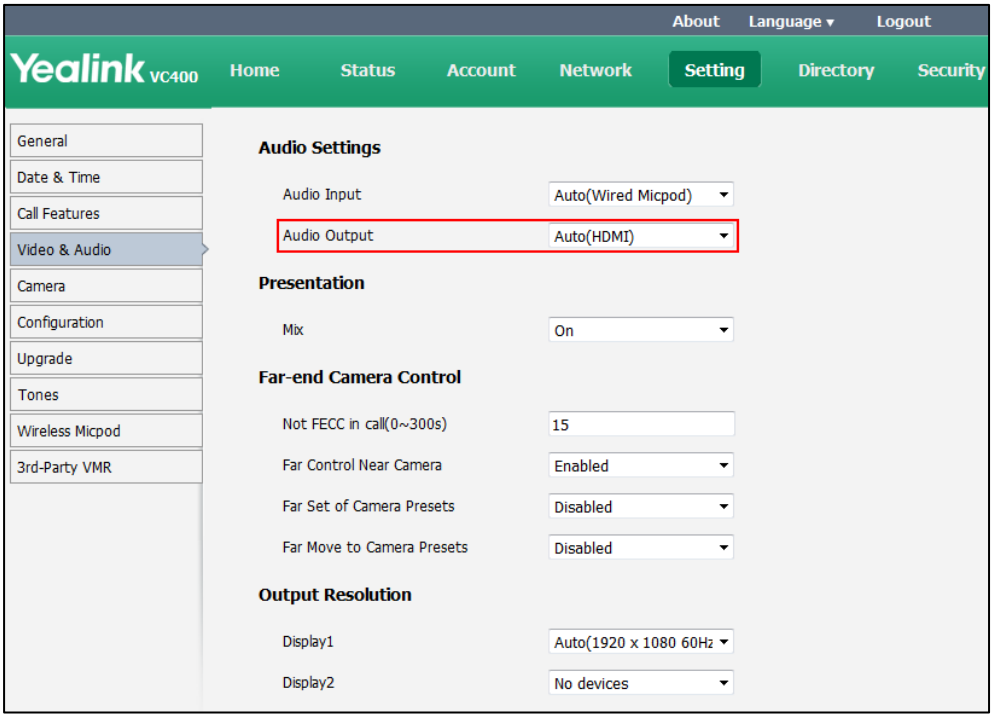
The audio output device parameter is described below:

Parameter	Description	Configuration Method
Audio Output	Specifies the audio output device for the system. **Valid values:** ● **Auto** - selects the audio output device with highest priority. ● **VCS Phone** - selects the video conferencing phone. ● **HDMI** - selects the built-in speakerphone of the display device. ● **Line Output** - selects the speakerphone connected to the Line Out port on the VC400/VC120 Codec. **Default:** Auto If **VCS Phone** is selected as the audio output device manually or automatically, the audio input device must be **VCS Phone** or **Line In+VCS Phone**.	Remote Control Web User Interface

To configure the audio output device feature via web user interface:

1. Click on **Setting->Video & Audio**.

2. Select the desired value from the pull-down list of **Audio Output**.



3. Click **Confirm** to accept the change.

To configure the automatic sleep time via the remote control:

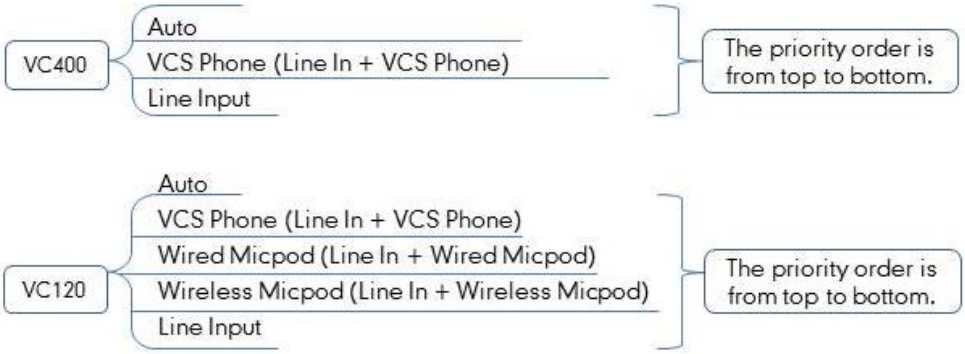
1. Select **Menu**->**Video & Audio**->**Audio Settings**.
2. Select the desired value from the pull-down list of **Audio Output**.
3. Press the **Save** soft key to accept the change.

Audio Input Device

The system supports the following audio input devices:

- **Auto** (select the audio input device with highest priority)
- **VCS Phone** (video conferencing phone)
- **Wired Micpod** (VCM30)
- **Line Input** (microphone connected to the Line In port on the VC400/VC120 Codec)
- **Line In + VCS Phone**
- **Line In + Wired Micpod**
- **Line In + Wireless Micpod**

The priority of audio input device is:



Note For more information on the wireless micpod, please contact Yealink agents.

By default, the VC400/VC120 automatically selects the audio input devices with the highest priority. If you select "Line In + device" option, the VC400/VC120 will use microphone connected to the Line In port and the device to pick up audio at the same time.

You can also specify the desired audio input device via the remote control or the web user interface.

The audio output device parameter is described below:

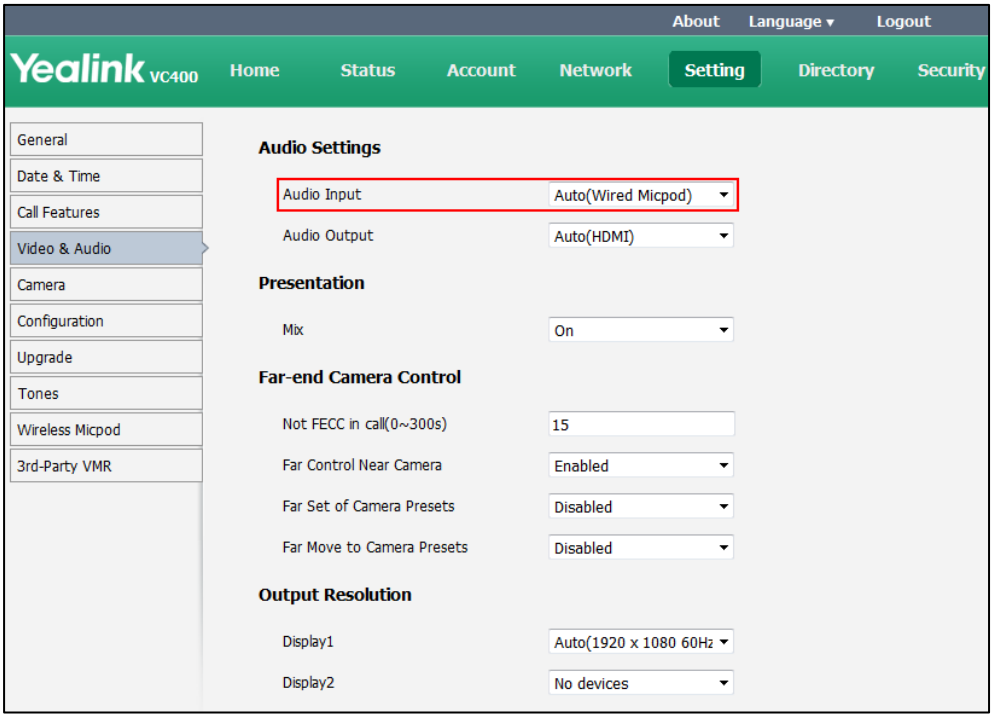
Parameter	Description	Configuration Method
Audio Input	Specifies the audio input device for the VC400/VC120. **Valid values:** • **Auto**- selects the audio input device with highest priority. • **VCS Phone**- selects the video conferencing phone. • **Wired Micpod**- selects the VCM30 video conferencing microphone array • **Line Input**- selects the microphone connected to the Line In port on the VC400/VC120 Codec. • **Line In +VCS Phone**- selects microphone connected to the Line In port on the Codec and video conferencing phone. • **Line In + Wired Micpod** - selects microphone connected	Remote Control Web User Interface

Parameter	Description	Configuration Method
	to the Line In port on the Codec and VCM30 video conferencing microphone array. **Default:** Auto. ● If **Line Input** is selected as the audio input device, the near-end audio output device will not play sound from the Line Input device. ● If "Line In + device" is selected as the audio input device, the near-end audio output device will play sound from the Line Input device. During a video training for main office and branch office, both offices need to hear the video sound, you can select this option.	

To configure the audio input device via web user interface:

1. Click on **Setting**->**Video & Audio**.

2. Select the desired value from the pull-down list of **Audio Input**.



3. Click **Confirm** to accept the change.

To configure the audio input device via the remote control:

1. Select **Menu**->**Video & Audio**->**Audio Settings**.
2. Select the desired value from the pull-down list of **Audio Input**.
3. Press the **Save** soft key to accept the change.

Adjusting MTU of Video Packets

Video packets that exceed the maximum transmission unit (MTU) size for any router or segment along the network path may be fragmented or dropped. This results in poor quality video at the receiving device. You can set the maximum MTU size of the video packets sent by the system. The default value is 1500 bytes. Specify the MTU size used in calls based on the network bandwidth settings. If the video becomes blocky or network errors occur, packets may be too large; decrease the MTU. If the network is burdened with unnecessary overhead; packets may be too small, increase the MTU.

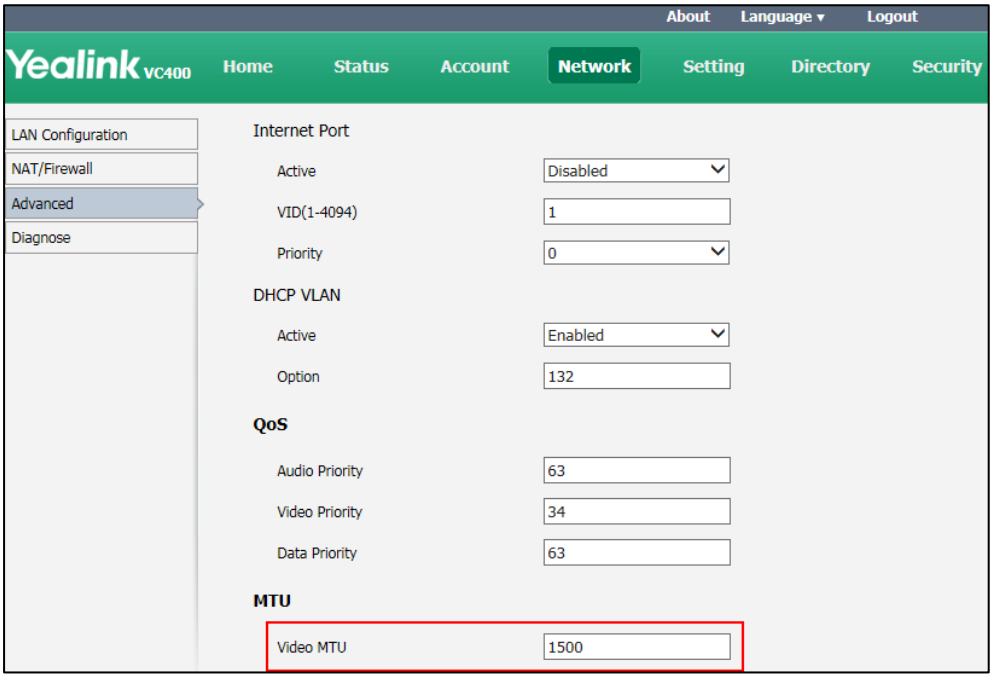
The MTU parameter on the system is described below.

Parameter	Description	Configuration Method
Video MTU	Specifies the maximum MTU size (in bytes) of video packets sent by the system. **Valid Values:** Integer from 1000 to	Remote Control Web User Interface

Parameter	Description	Configuration Method
	1500 **Default:** 1500 **Note**: If you change this parameter, the system will reboot to make the change take effect.	

To configure MTU via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **MTU** block, enter the desired value in the **Video MTU** field.



3. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.
4. Click **Confirm** to reboot the system immediately.

To configure MTU via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Enter the desired value in the **Video MTU(1000-1500)** field.
3. Press the **Save** soft key to accept the change.

   The display device prompts "Reboot now?".
4. Select **OK** to reboot the system immediately.

Dual-Stream Protocol

To enhance the process of communicating with others over video, the dual-stream protocol provides the ability to share content from a computer, such as video clips or documentation. Both the video and the documentation can be transmitted to the far site simultaneously, thus meeting the requirements of different conference scenarios, such as training or medical consultation.

The Yealink video conferencing system supports the standard H.239 protocol and BFCP (Binary Floor Control Protocol). H.239 protocol is used when sharing content with the far site in H.323 calls. BFCP protocol is used when sharing content with the far site in SIP calls. Before enabling the desired protocol, ensure that the protocol is supported and enabled by the far site you wish to call. If the far site does not support the protocol for sharing content, MCU will automatically mix the content and camera video, and send them in one channel. For more information on mix sending, refer to Mix Sending on page 200.

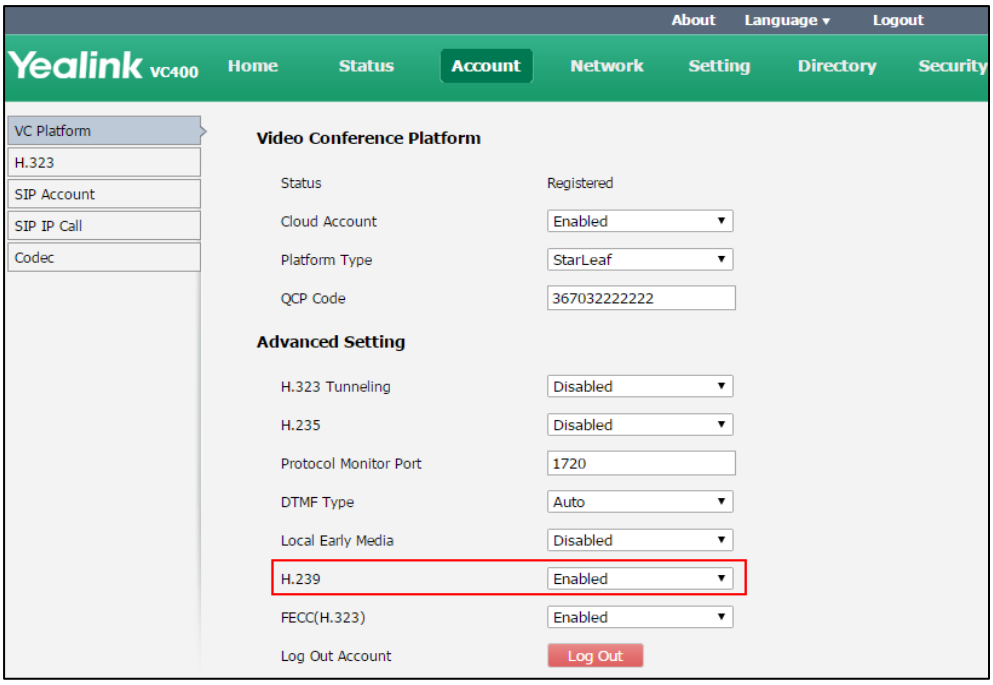
Dual-stream protocol parameters on the system are described below.

Parameter	Description	Configuration Method
H.239	Enables or disables the H.239 protocol for sharing content. You can configure it for the StarLeaf Cloud platform or H.323 call separately. **Default:** Enabled	Web User Interface
BFCP	Enables or disables the BFCP protocol for sharing content. You can configure it for Zoom/Pexip/BlueJeans/Mind/Custom platform, SIP account or SIP IP call separately. **Default:** For Zoom/Pexip/BlueJeans/Mind/Custom platform and SIP IP call, the default value is Enabled. For SIP account, the default value is Disabled. **Note:** You cannot configure it for the Yealink/StarLeaf Cloud platform.	Web User Interface

To configure H.239 dual-stream protocol for StarLeaf Cloud platform via web user interface:

1. Click on **Account->VC Platform**.
2. Select **StarLeaf f**rom the pull-down list of **Platform Type**.

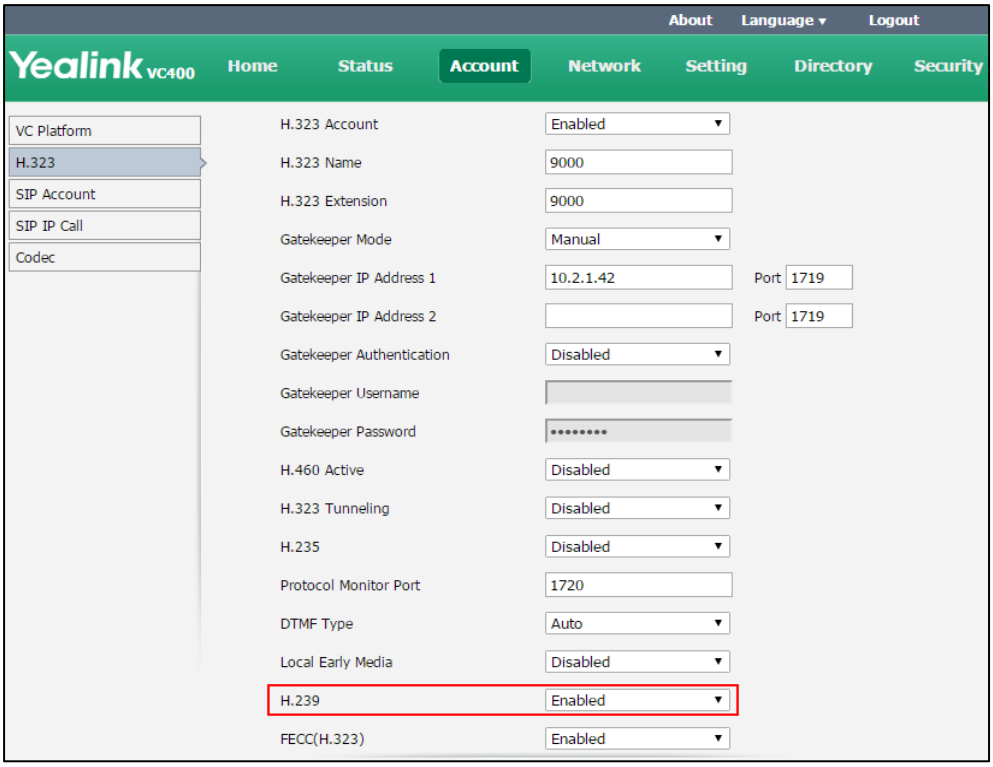
3. Select the desired value from the pull-down list of **H.239**.



4. Click **Confirm** to accept the change.

To configure H.239 dual-stream protocol for H.323 call via web user interface:

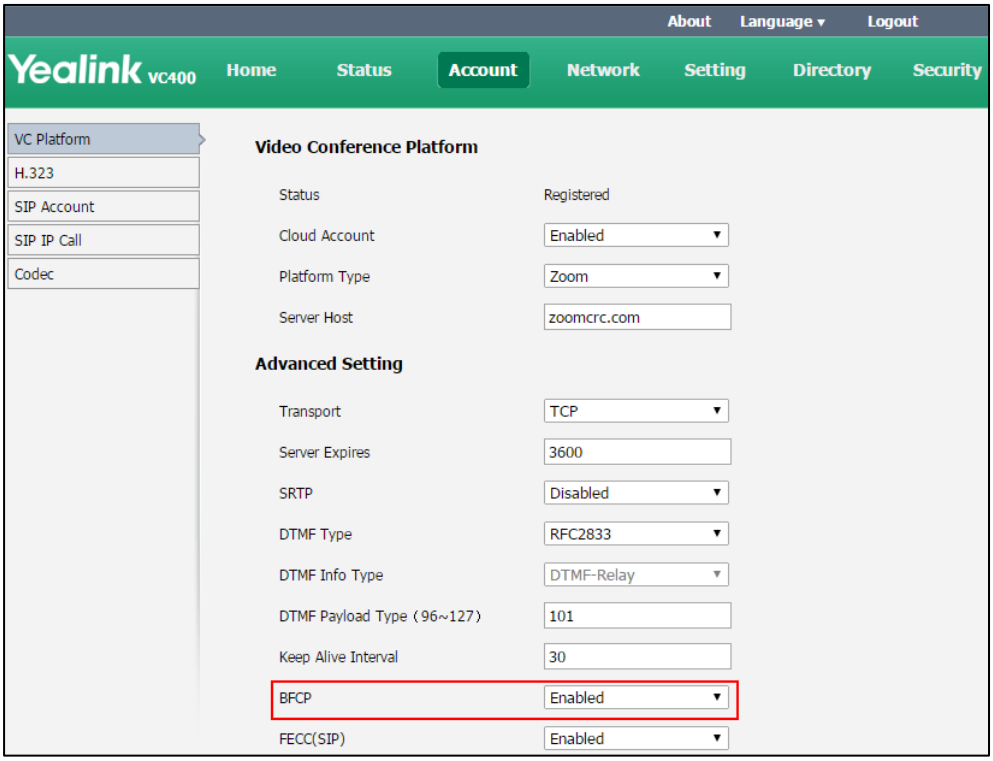
1. Click on **Account**->**H.323**.
2. Select the desired value from the pull-down list of **H.239**.



3. Click **Confirm** to accept the change.

To configure BFCP dual-stream protocol for Zoom/Pexip/BlueJeans/Mind/Custom platform via web user interface:

1. Click on **Account->VC Platform**.
2. Select **Zoom/Pexip/BlueJeans/Mind/Custom** from the pull-down list of **Platform Type**.
3. Select the desired value from the pull-down list of **BFCP**.

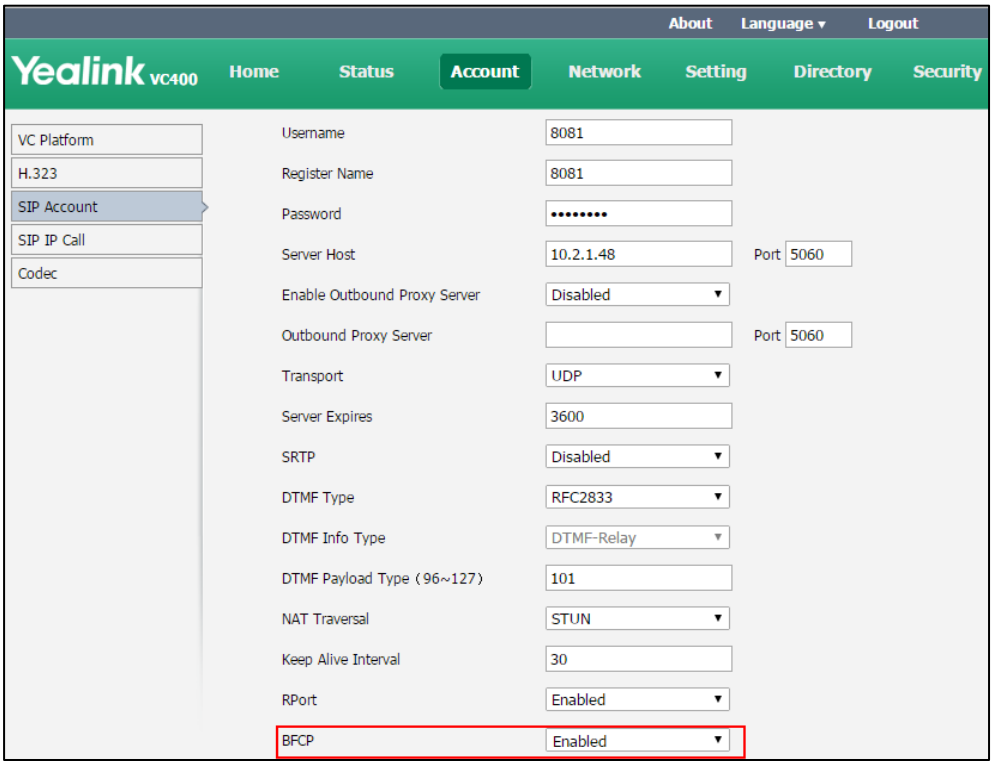


4. Click **Confirm** to accept the change.

To configure BFCP dual-stream protocol for SIP call via web user interface:

1. Click on **Account**->**SIP Account**.

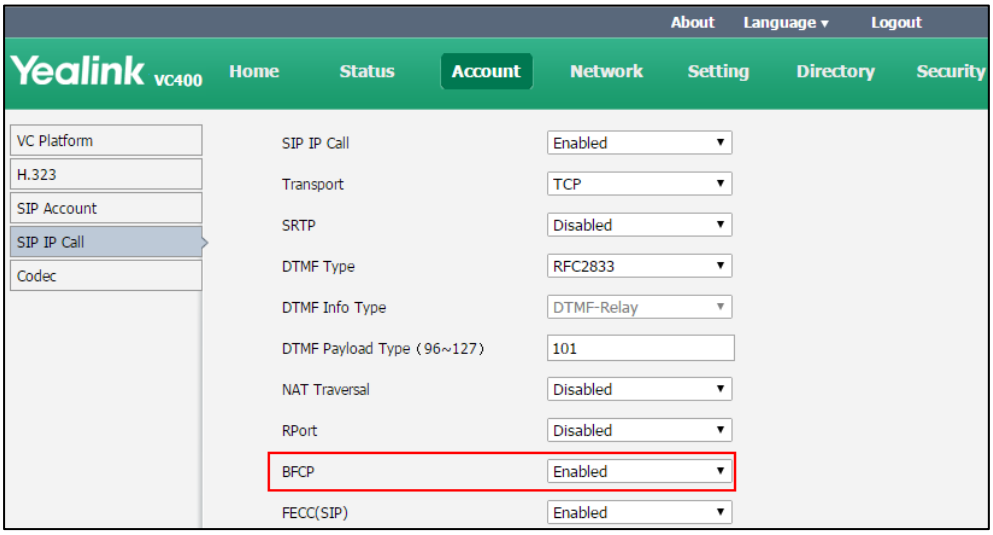
2. Select the desired value from the pull-down list of **BFCP**.



3. Click **Confirm** to accept the change.

To configure BFCP dual-stream protocol for SIP IP call via web user interface:

1. Click on **Account**->**SIP IP Call**.
2. Select the desired value from the pull-down list of **BFCP**.



3. Click **Confirm** to accept the change.

Mix Sending

Content sharing allows users to share content with other conference participants during a call. When a PC is connected to the PC port on the VC400/VC120 Codec, the display device can display both the camera video and the shared content. The content sharing feature is very useful in the conference scenario in which content sharing is needed (e.g., a slide or a flash).

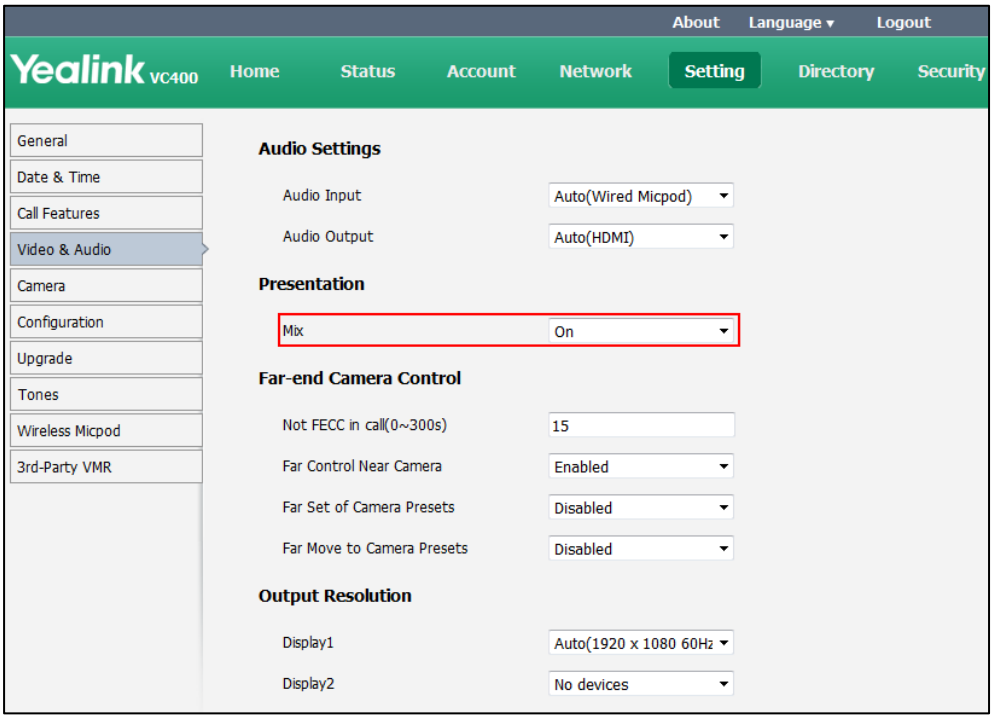
During a conference call, the far site may not support receiving shared content. In this case, you can enable mix sending feature on the system. Mix sending feature allows the sender to compound multiple video streams (local image+shared content) to one video stream, and then send it to the far site.

The mix sending parameter on the system is described below.

Parameter	Description	Configuration Method
Mix	Enables or disables the mix sending feature on the system. **Default:** Enabled	Web User Interface

To configure mix sending via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. In the **Presentation** block, select the desired value from the pull-down list of **Mix**.



3. Click **Confirm** to accept the change.

Configuring Camera Settings

To display high quality video image, you can configure camera settings as required, such as white balance, exposure and sharpness.

Camera settings parameters are described below.

Parameter	Description	Configuration Method
Exposure Compensation	Configures the value of camera exposure compensation. • Off • 1 • 2 • 3 Exposure compensation is used to compensate the camera effectively when the camera is shooting in a backlight environment. If the environment light is dark, you can increase the compensation value. **Default:** Off	Remote Control Web User Interface
Flicker	Disables or configures the value of camera flicker frequency. • 50Hz • 60Hz **Default:** 50Hz **Note**: Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source the light is powered by.	Remote Control Web User Interface
White Balance Mode	Configures the white balance mode of the VCC18 camera. • **Auto**–Yealink recommends this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	• **One push**−Use the predefined color temperature settings to provide acceptable color reproduction. • **ATW**−Automatically adjust the white balance based on the video image shoot by the camera. • **Manual**−Manually set red and blue gain. **Default:** Auto	
	Configures the white balance mode of the VCC20 camera. • **Auto**−Yealink recommends this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room. • **One push**−Use the predefined color temperature settings to provide acceptable color reproduction. • **ATW**−Automatically adjust the white balance based on the video image shoot by the camera. • **Tungsten Bulb** • **Fluorescent** • **Cool Daylight** • **Manual**−Manually set red and blue gain. **Default:** ATW	
Red Gain	Configures the red gain of the camera. **Valid Values:** 0-100 **Default:** 83 **Note**: You can set this parameter	Remote Control Web User Interface

Parameter	Description	Configuration Method
	only when the white balance mode is configured to Manual.	
Blue Gain	Configures the blue gain of the camera. **Valid Values:** 0-100 **Default:** 62 **Note**: You can set this parameter only when the white balance mode is configured to Manual.	Remote Control Web User Interface
Saturation	Configures the saturation of the camera. **Valid Values:** 0-14 **Default:** For VCC18 camera, the default value is 3. For VCC20 camera, the default value is 10.	Remote Control Web User Interface
Sharpness	Configures the sharpness of the camera. **Valid Values:** 0-14 **Default:** For VCC18 camera, the default value is 1. For VCC20 camera, the default value is 8. **Note**: The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped.	Remote Control Web User Interface
Brightness	Configures the brightness of the camera. **Valid Values:** 0-100 **Default:** For VCC18 camera, the default value is 8. For VCC20 camera, the default value is 1.	Remote Control Web User Interface

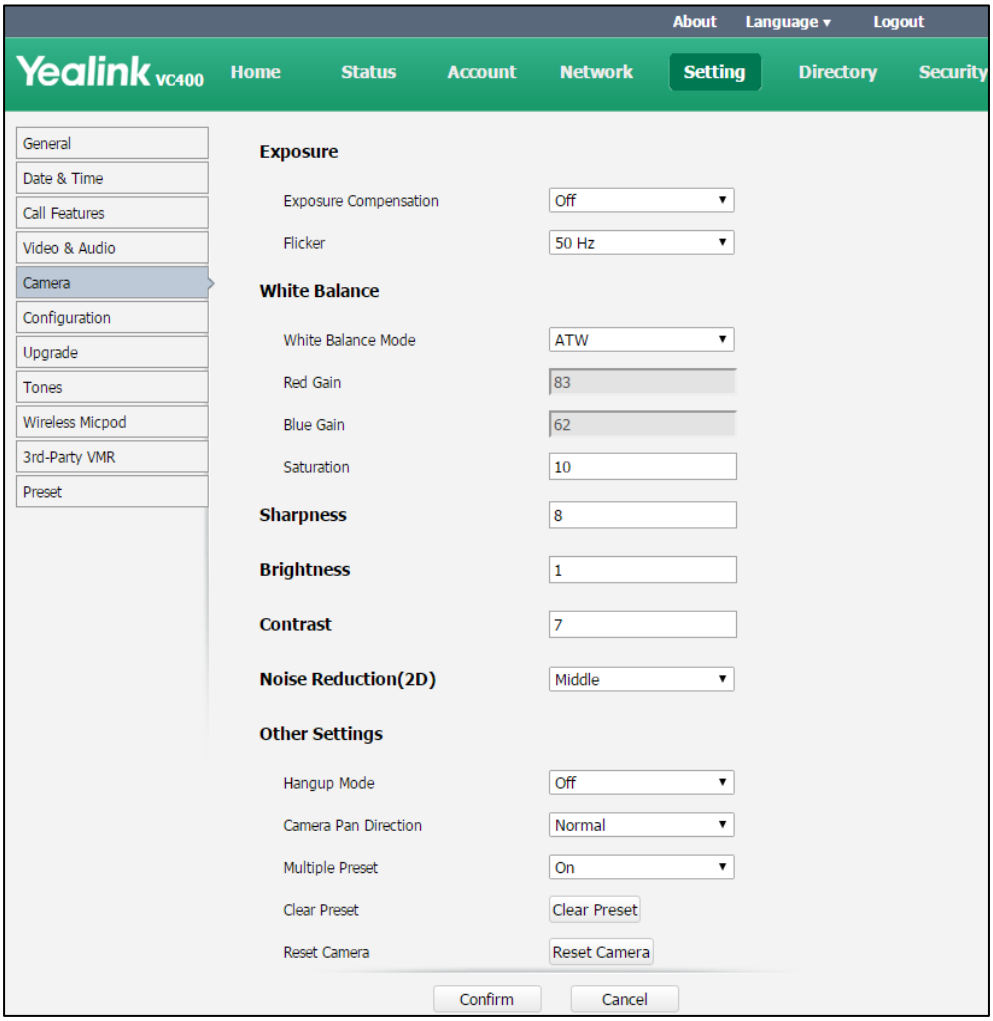
Parameter	Description	Configuration Method
Contrast	Configures the contrast of the camera. **Valid Values:** 0-100 **Default:** For VCC18 camera, the default value is 45. For VCC20 camera, the default value is 7.	Remote Control Web User Interface
Noise Reduction (2D)	Specifies the noise reduction (2D) mode. ● Off ● Low ● Middle ● High **Default:** Middle	Remote Control Web User Interface
Noise Reduction (3D)	Specifies the noise reduction (3D) mode of VCC18 camera. ● Off ● Low ● Middle ● High **Default:** Off **Note:** It is not applicable to VCC20 camera.	Remote Control Web User Interface
Hangup Mode	Enables or disables the camera to flip the image view when camera is handed at up-side-down position **Default:** Off	Remote Control Web User Interface
Camera Pan Direction	Configures the pan direction of the camera. ● Normal ● Reversed **Default:** Normal If the camera reversed mode is enabled, the camera pan direction	Remote Control Web User Interface

Parameter	Description	Configuration Method
	will be reversed when pressing the left and right navigation keys on the remote control. In this case, you can set the camera pan direction to Reversed.	
Multiple Preset	Enables or disables the multiple preset feature. **Default:** Off For more information, refer to Multiple Preset on page 206.	Web User Interface
Camera Map	Enables or disables the preview of camera presets. **Default:** On **Note**: If it is set to on, you can view the pre-saved camera presets.	Remote Control Web User Interface
Clear Preset	Clears all camera presets.	Remote Control Web User Interface
Reset Camera	Resets the camera settings to factory defaults. **Note:** The camera presets will also be cleared.	Remote Control Web User Interface

To configure camera settings via web user interface:

1. Click on **Setting**->**Camera**.

2. Configure the camera settings.



3. Click **Confirm** to accept the change.

To configure camera settings via the remote control:

1. Select **Menu**->**Video & Audio->Camera General Settings**.
2. Configure the camera settings.
3. Press the **Save** soft key to accept the change.

Multiple Preset

You can store the preset to a numeric key via the remote control or web user interface. Each camera preset stores the camera pan, tilt, and zoom settings. This means that you can point a camera at pre-defined locations by pressing stored keys.

You can store up to 10 preset camera positions using the remote control. If you want to store more than 10 preset camera positions, you can enable the multiple preset feature.

For VC400 video conferencing system, you can store up to 64 preset camera positions for VCC18 camera. For VC120 video conferencing system, if you connect two VCC20 cameras to the

VC120 Codec using the VC Dual-camera Box VCB20, you can store up to 64 preset camera positions for camera 1 and 63 preset camera positions for camera 2.

The following example illustrates a scenario where multiple preset feature is used:

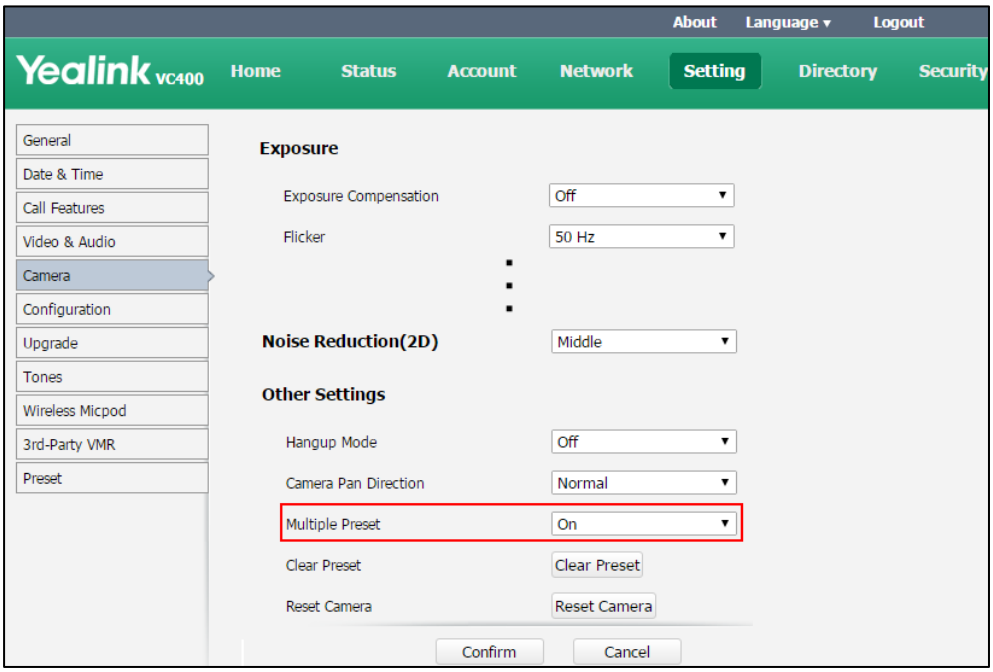
There are multiple speakers in a large meeting room. You can set multiple preset camera positions for each speaker. When someone speaks, the camera can be adjusted to the corresponding preset camera position that is associated with the current speaker.

Multiple preset parameters are described below.

Parameter	Description	Configuration Method
Multiple Preset	Enables or disables the multiple preset feature on the system. Default: **Off**	Web User Interface
Use	Points local camera at a preset position	Web User Interface
Replace Preset	Replaces the stored camera preset position with current camera preset position.	Web User Interface
Delete Preset	Deletes the selected preset position.	Web User Interface
Clear Preset	Clears all preset positions.	Remote Control Web User Interface

To configure multiple preset via web user interface:

1. Click on **Setting**->**Camera**.
2. Select the **On** from the pull-down lists of **Multiple Preset**.



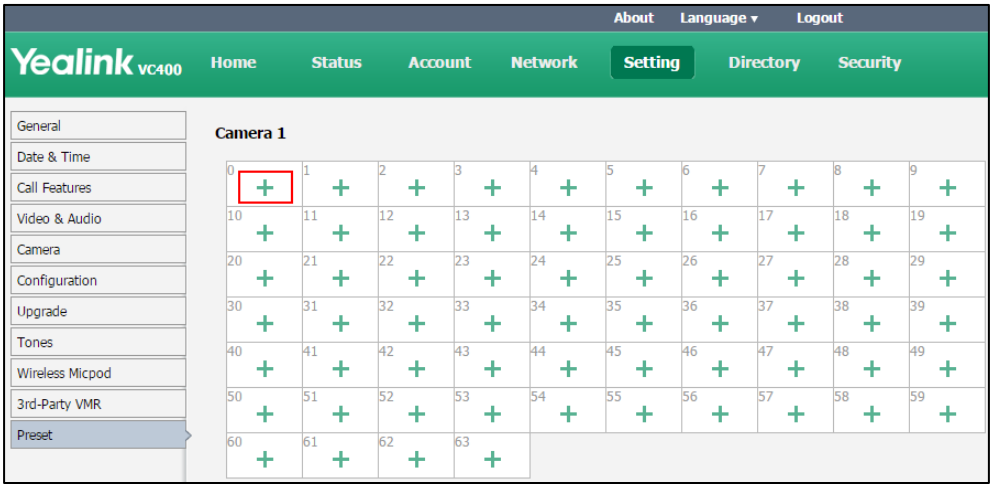
3. Click **Confirm** to accept the change.

A **Preset** menu appears.

Storing a Camera Preset

To store a camera preset position via web user interface:

1. Click on **Setting**->**Preset**.
2. Adjust the angle and focus of the camera.
3. Click + to store a camera preset to the specified number.



The web user interface prompts "Do you want to add the preset?".

4. Click **Confirm** to accept the change.

A **Preset** menu appears.

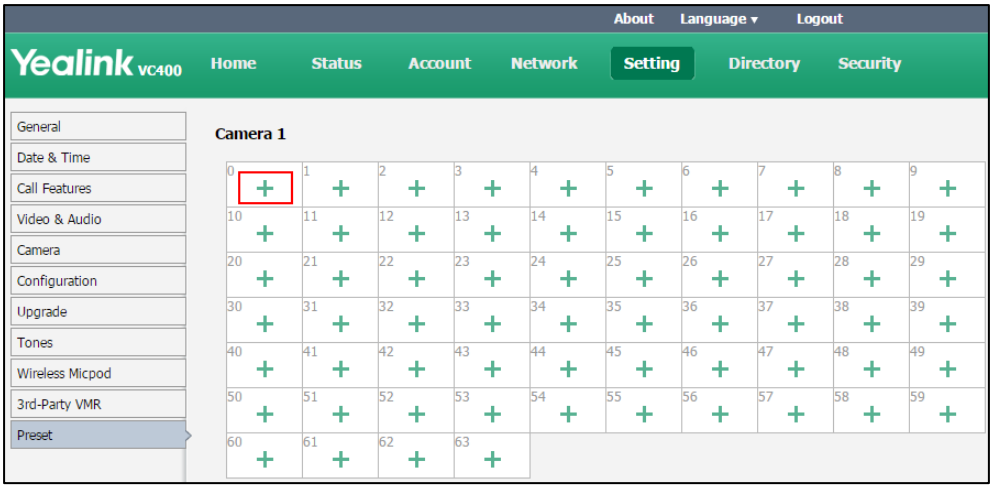
Moving Local Camera to a Preset Position

You can check whether the camera presets are correct after you set multiple camera preset positions.

To use a camera preset position via web user interface:

1. Click on **Setting**->**Preset**.

2. Click **Use** to move local camera to the corresponding preset position.

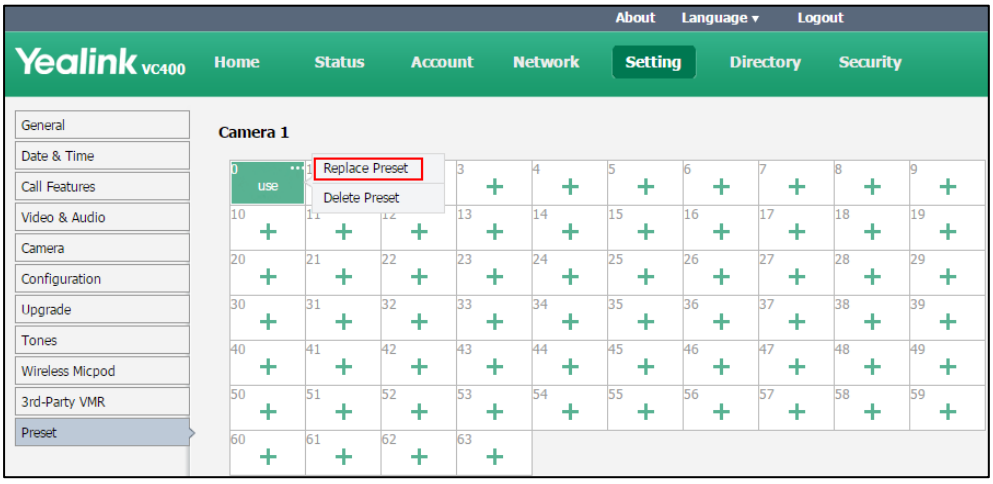


Replacing the Stored Preset

You can replace the stored camera preset position with current camera preset position.

To replace the stored camera preset position via web user interface:

1. Click on **Setting**->**Preset**.
2. Click , and then select **Replace Preset**.

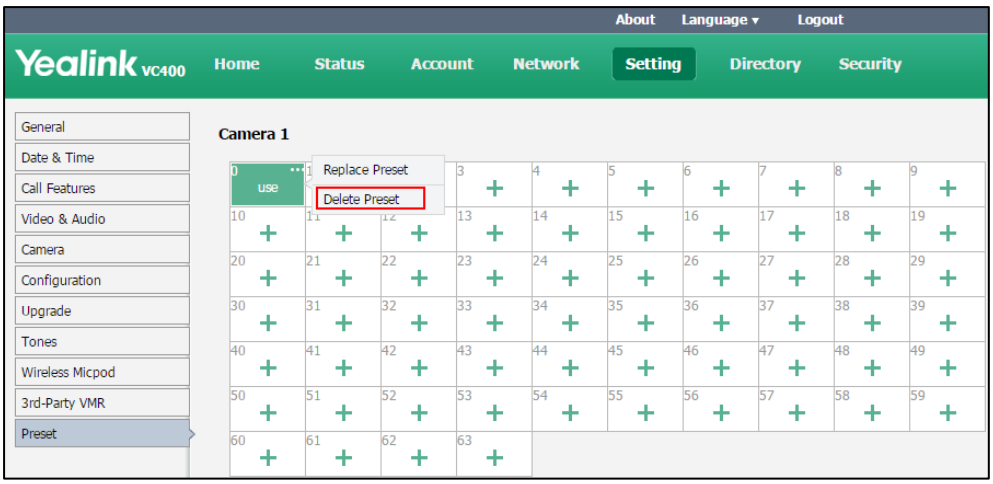


Deleting the Stored Preset

To delete the stored camera preset position via web user interface:

1. Click on **Setting**->**Preset**.

2. Click , and then select **Delete Preset**.



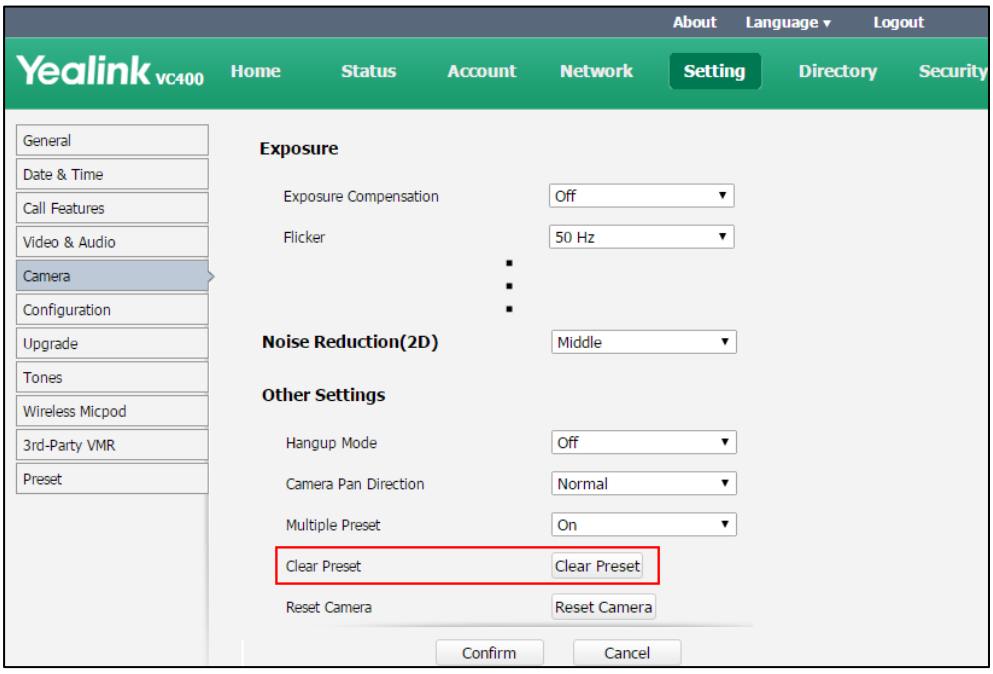
The web user interface prompts "Do you want to delete the preset?".

3. Click **Confirm** to accept the change.

Clearing the Stored Preset

To clear all camera preset positions via web user interface:

1. Click on **Setting**->**Camera**.
2. Click **Clear Preset**.



The web user interface prompts "Clear the camera data?".

3. Click **Confirm** to accept the change.

To clear all camera preset positions via the remote control:

1. Select **Menu**->**Video & Audio->Camera General Settings**.
2. Select **Clear Preset Position**.
3. Press **OK** to accept the change.

Far-end Camera Control

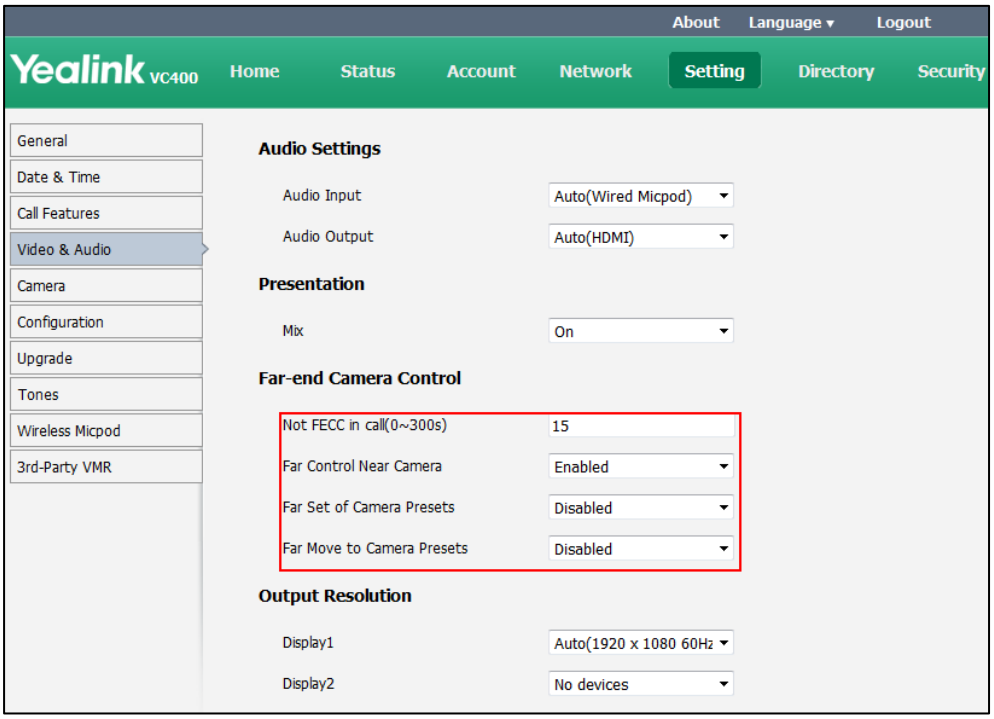
Local video is displayed on the display device of the far site during a call. For the best view, you can enable the Far Control Near Camera feature to allow the far site to control the focus and angle of the local camera. You can also specify whether the far site is allowed to store and use the local camera presets.

Far-end camera control parameters are described below.

Parameter	Description	Configuration Method
Not FECC in call(0~300s)	Configures the duration time (in seconds) when far site cannot control the local camera during a call. **Default:** 15 If it is set to 15, the far site is not allowed to control the local camera in the first 15 seconds of the call.	Web User Interface
Far Control Near Camera	Enables or disables the far site to control the local camera. **Default:** Enabled	Remote Control Web User Interface
Far Set of Camera Presets	Enables or disables the far site to create presets for the local camera. **Default:** Disabled **Note**: It only works if the value of the "Far Control Near Camera" is set to Enabled.	Remote Control Web User Interface
Far Move to Camera Presets	Enables or disables the far site to point local camera at pre-defined locations. **Default:** Disabled **Note**: It only works if the value of the "Far Control Near Camera" is set to Enabled.	Remote Control Web User Interface

To configure far-end camera control via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Enter the desired time in the **Not FECC in call(0~300s)** field.
3. Select the desired values from the pull-down lists of **Far Control Near Camera**.
4. Select the desired values from the pull-down lists of **Far Set of Camera Presets**.
5. Select the desired values from the pull-down lists of **Far Move to Camera Presets**.



6. Click **Confirm** to accept the change.

To configure far-end camera control feature via the remote control:

1. Select **Menu**->**Video & Audio->Far-end Camera Control**.
2. Make the desired changes.
3. Press the **Save** soft key to accept the change.

Camera Control Protocol

VC400/VC120 video conferencing systems support camera control protocols: FECC (Far End Camera Control). You can enable the FECC protocol for SIP call or H.323 call.

If far site wants to control the local camera, both the far site and local site should enable the camera control protocol simultaneously. If the FECC protocol is not enabled on either site, far-end camera control cannot be performed. For example, a SIP call is established between two sites, the two sites must enable FECC (SIP) protocol simultaneously to perform far-end camera control. If FECC (SIP) protocol and FECC (H.323) protocol are both enabled, the system will select the appropriate camera control protocol according to the protocol (SIP or H.323) the call uses.

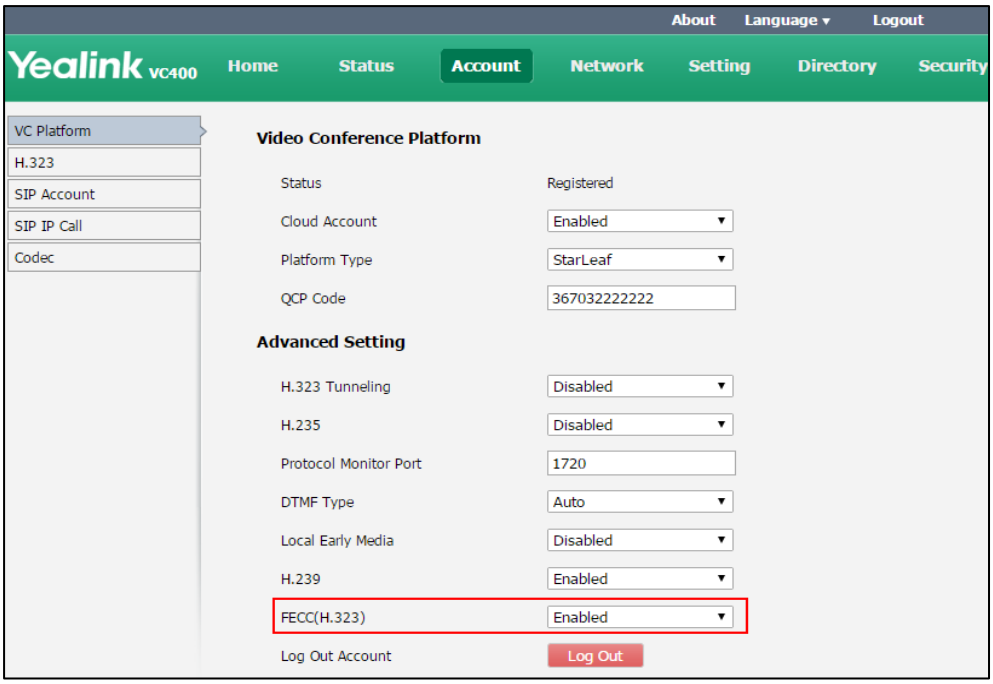
Camera control protocol parameters are described below:

Parameter	Description	Configuration Method
FECC(H.323)	Enables or disables the FECC (H.323) protocol for far site to control near camera. You can configure it for the StarLeaf Cloud platform or H.323 call separately. **Default:** Enabled	Web User Interface
FECC(SIP)	Enables or disables the FECC (SIP) protocol for far site to control near camera. You can configure it for the Zoom/Pexip/BlueJeans/Mind/Custom platform, SIP account or SIP IP call separately. **Default:** For Zoom/Pexip/BlueJeans/Mind/Custom platform and SIP IP call, the default value is Enabled. For SIP account, the default value is Disabled. **Note:** You cannot configure it for the Yealink/StarLeaf Cloud platform.	Web User Interface

To configure FECC(H.323) camera control protocol for StarLeaf Cloud platform via web user interface:

1. Click on **Account->VC Platform**.
2. Select **StarLeaf** from the pull-down list of **Platform Type**.

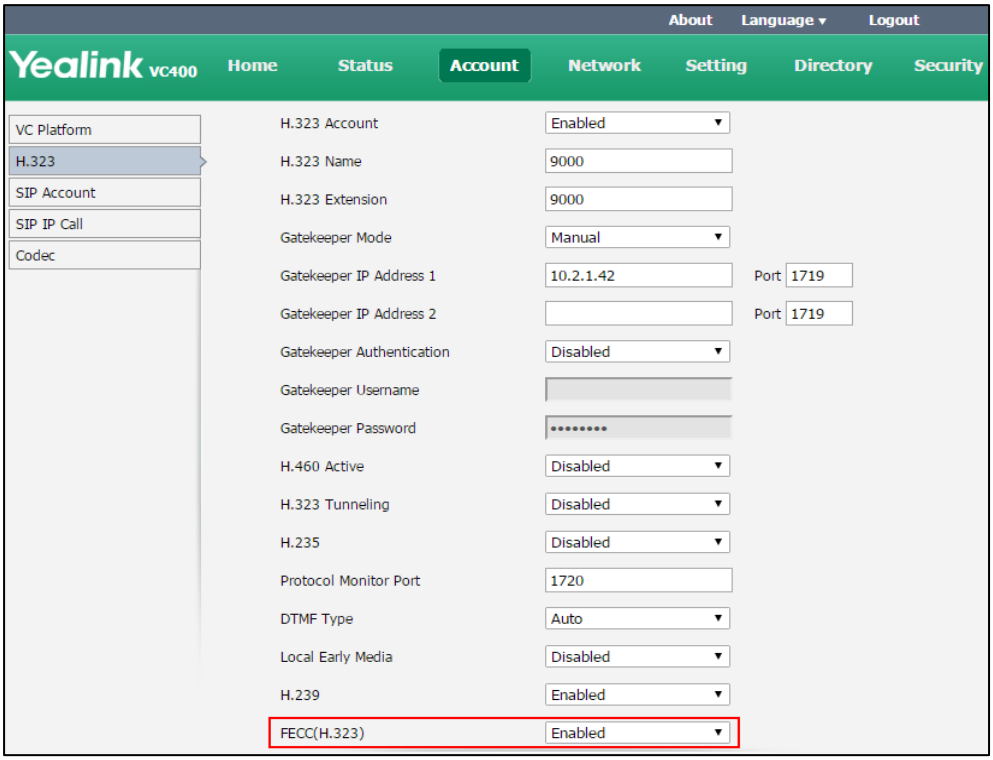
3. Select the desired value from the pull-down list of **FECC(H.323)**.



4. Click **Confirm** to accept the change.

To configure FECC(H.323) camera control protocol for H.323 calls via web user interface:

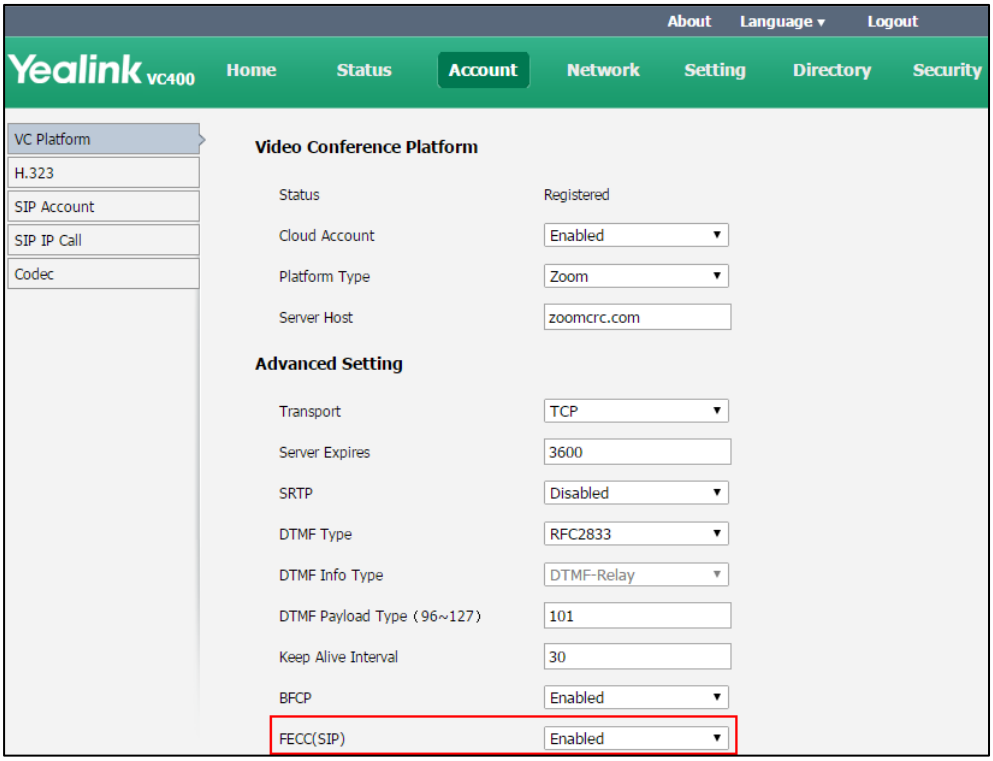
1. Click on **Account**->**H.323**.
2. Select the desired value from the pull-down list of **FECC(H.323)**.



3. Click **Confirm** to accept the change.

To configure FECC(SIP) camera control protocol for Zoom/Pexip/BlueJeans/Mind/Custom platform via web user interface:

1. Click on **Account->VC Platform**.
2. Select **Zoom/Pexip/BlueJeans/Mind/Custom** from the pull-down list of **Platform Type**.
3. Select the desired value from the pull-down list of **FECC(SIP)**.

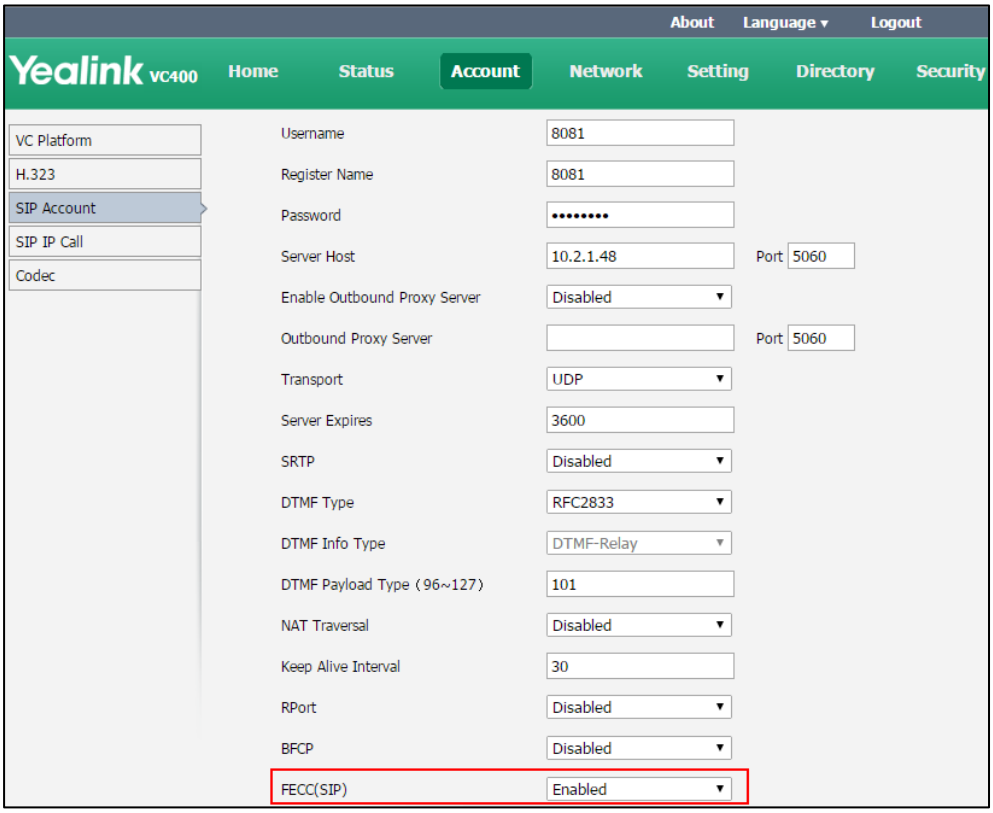


4. Click **Confirm** to accept the change.

To configure FECC(SIP) camera control protocol for SIP calls via web user interface:

1. Click on **Account**->**SIP Account**.

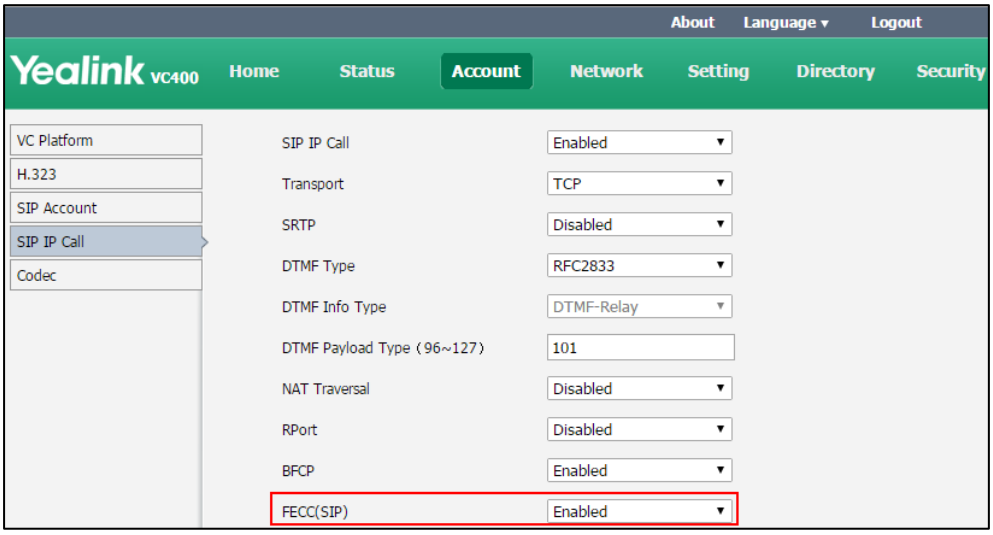
2. Select the desired value from the pull-down list of **FECC(SIP)**.



3. Click **Confirm** to accept the change.

To configure FECC(SIP) camera control protocol for SIP IP call via web user interface:

1. Click on **Account**->**SIP IP Call**.
2. Select the desired value from the pull-down list of **FECC(SIP)**.



3. Click **Confirm** to accept the change.

Output Resolution

VC400/VC120 supports output resolution adjustment. You can adjust output resolution of primary/secondary display device respectively.

Make sure the display device has connected to the VC400/VC120 Codec before configuration.

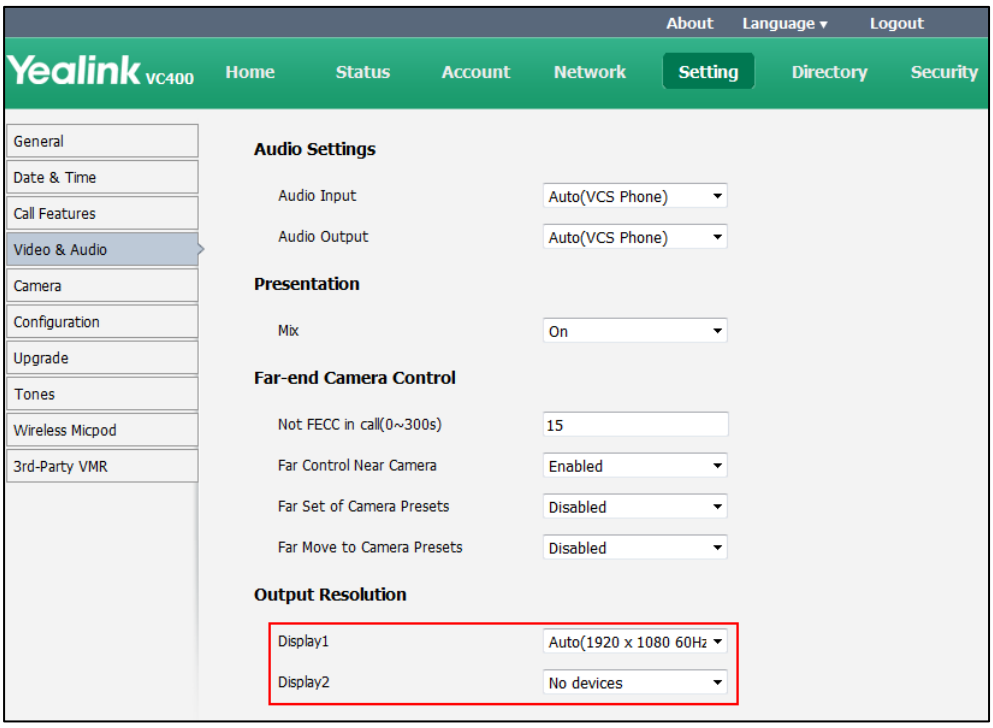
The output resolution parameters on the systems are described below.

Parameter	Description	Configuration Method
Display1	Configures the output resolution of primary display device. ● **Auto**-select the highest output resolution automatically ● Available output resolutions (The available resolutions depend on the display device you are using) **Default:** Auto	Web User Interface
Display2	Configures the output resolution of secondary display device. ● **Auto**-select the highest output resolution automatically ● Available output resolutions (The available resolutions depend on the display device you are using) **Default:** Auto	Web User Interface

To configure output resolution via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Select the desired value from the pull-down list of **Display1**.

3. Select the desired value from the pull-down list of **Display2**.



4. Click **Confirm** to accept the change.

USB Configuration

If you have high requirement for data security, you can disable the USB feature. If you disable the USB feature, you cannot view the videos and screenshots stored in the USB flash driver via the remote control, and cannot record video or capture screenshots too.

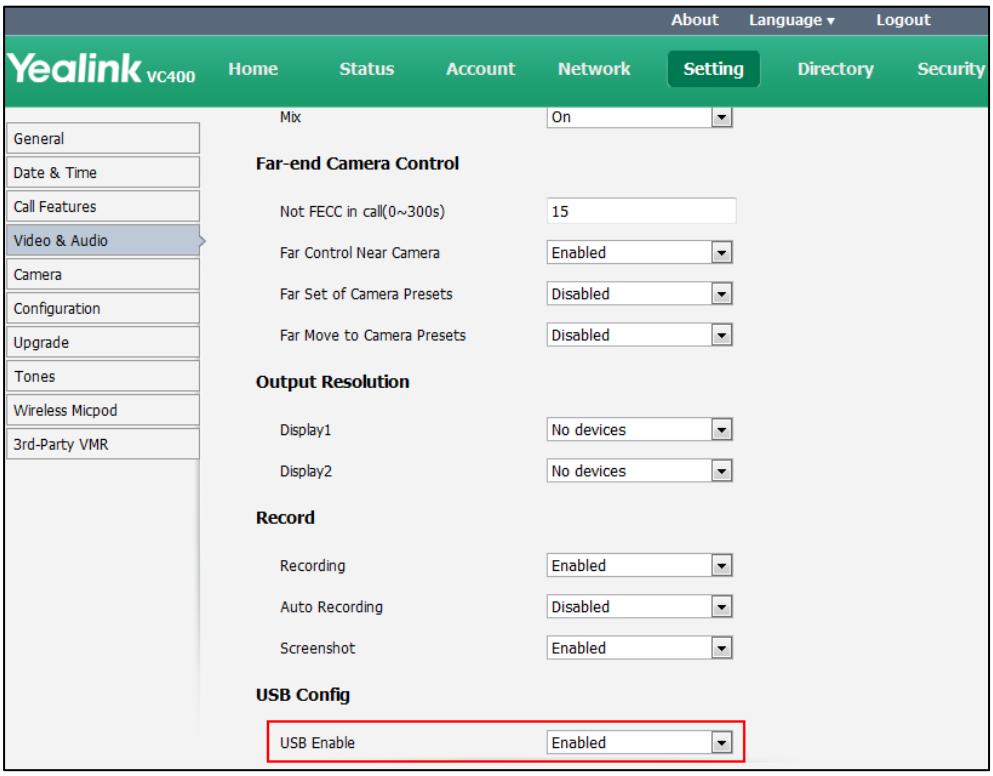
The USB configuration parameter on the system is described below.

Parameter	Description	Configuration Method
USB Enable	Enables or disables the USB feature. **Default:** Enabled	Web User Interface

To configure USB configuration via web user interface:

1. Click on **Setting**->**Video & Audio**.

2. Select the desired value from the pull-down list of **USB Enable**.



3. Click **Confirm** to accept the change.

Video Recording

When the system is idle, you can record local video via the remote control. During a call, the video and presentation which are shown on the display device can be recorded via the remote control and video conferencing phone.

Before recording video, you need to insert a USB flash drive to the USB port on the VC400/VC120 Codec to store recorded video. Make sure the USB feature is enabled.

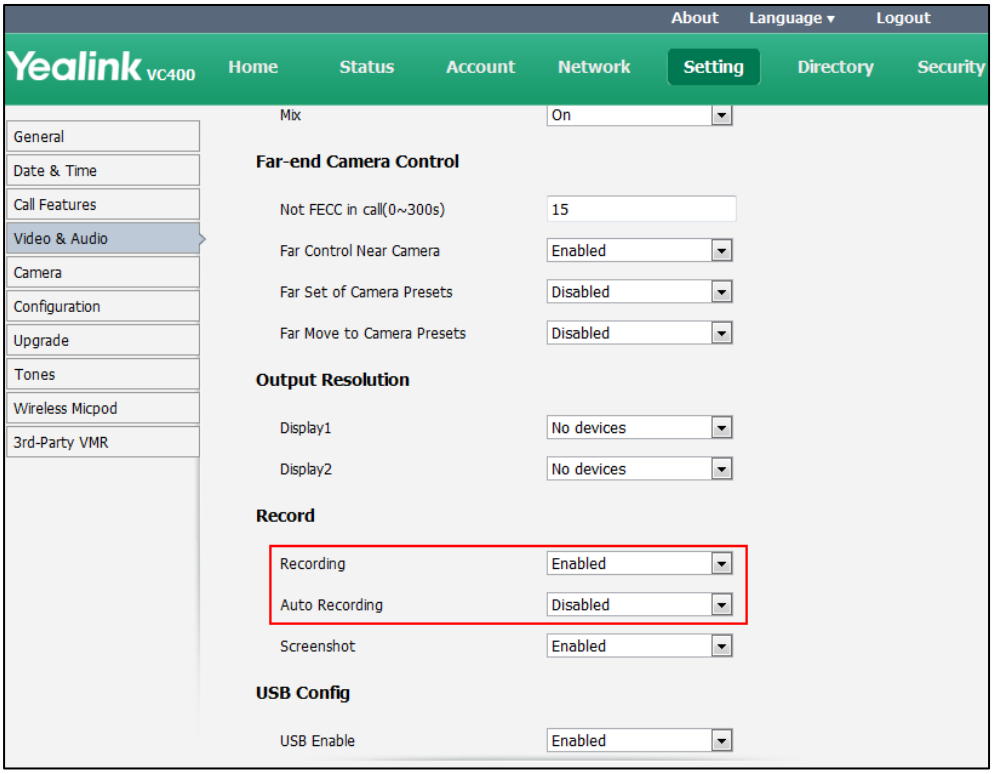
The video recording parameters on the system are described below.

Parameter	Description	Configuration Method
Recording	Enables or disables the video recording feature on the system. **Default:** Enabled If it is set to Disabled, you cannot record video.	Web User Interface
Auto Recording	Enables or disables the system to start recording automatically once a call is established. **Default:** Disabled.	Web User Interface

Parameter	Description	Configuration Method
	Note: The auto recording feature is available only when the recording feature is enabled.	

To configure video recording via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Select the desired value from the pull-down list of **Recording**.
3. Select the desired value from the pull-down list of **Auto Recording**.



4. Click **Confirm** to accept the change.

To record video when the system is idle via the remote control:

1. Press *. to start recording and press *. again to stop recording.

To record video during a call via the remote control:

1. Do one of the following:
   - Long press *. to start recording and long press *. again to stop recording.
   - Press **More** soft key to open **More** screen.
     Press ▲or ▼to scroll to **USB Recording**, and then press OK to start recording.
     Open the **More** screen, scroll to **USB Recording** again, and then press OK to stop recording.

To record video during a call via the video conferencing phone:

1. Press the **Start REC** soft key to start recording and press the **Stop REC** soft key again to stop recording.

When you start recording, the display device will show and the recording time. When you stop recording, the recording icon disappears from the screen. The display device prompts "Successfully video recording!"

Note If you start recording during a call, both your display device and remote display devices will show the icon on your video image.

Screenshot

You can capture the screenshot from the camera via the remote control or web user interface. Before capturing the screenshot, you need to insert a USB flash drive to the USB port on the VC400/VC120 Codec to store screenshots. Make sure the USB feature is enabled.

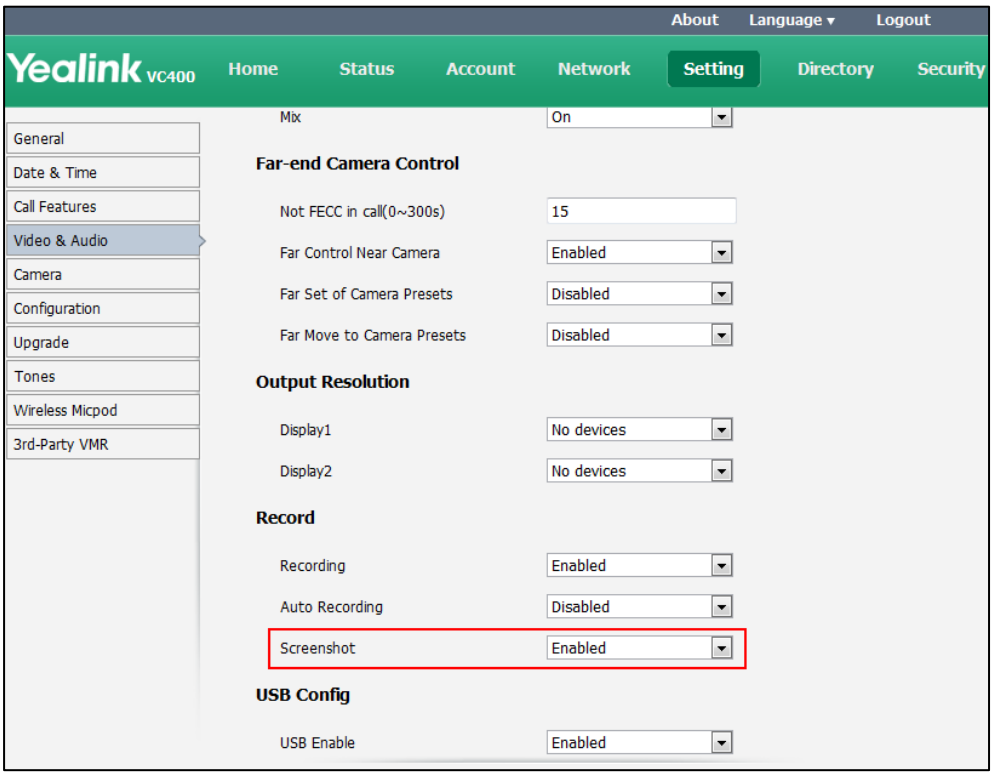
The screenshot parameter on the system is described below.

Parameter	Description	Configuration Method
Screenshot	Enables or disables the screenshot feature on the system. **Default:** Enabled If it is set to Disabled, you cannot capture screenshot.	Web User Interface

To configure screenshot via web user interface:

1. Click on **Setting**->**Video & Audio**.

2. Select the desired value from the pull-down list of **Screenshot**.



3. Click **Confirm** to accept the change.

To capture screenshots via web user interface:

1. Click **Home**->**Screenshot** when the system is idle or during a call.

To capture screenshots when the system is idle via the remote control:

1. Press #.

To capture screenshots during a call via the remote control:

1. Do one of the following:

   - Long press #.
   - Press **More** soft key to open **More** screen.

     Press ▲or ▼to scroll to **Screenshot**, and then press OK to capture screenshot.

Tones

When automatically answering an incoming call, the system will play a warning tone. You can customize tones or select specialized tone sets (vary from country to country) to indicate different conditions of the system. The default tones used on the system are the US tone sets. Available tone sets for the system:

- Australia

- Austria
- Brazil
- Belgium
- China
- Chile
- Czech
- Czech ETSI
- Denmark
- Finland
- France
- Germany
- Great Britain
- Greece
- Hungary
- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States

Configured tones can be heard on the system for the following conditions:

Condition	Description
Ring Back	Ring-back tone
Busy	When the callee is busy
Call Waiting	Call waiting tone

Condition	Description
Auto Answer	When answering a call automatically

Tones parameters on the system are described below:

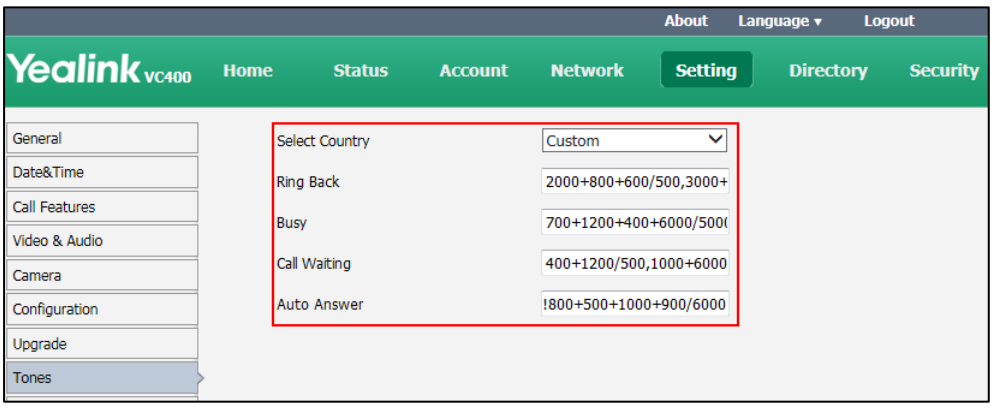
Parameter	Description	Configuration Method
Select Country	Customizes tones or selects the desired country tone set. **Default:** Custom	Web User Interface
Ring Back	Customizes the ring-back tone for the system. tone = element1[,element2][,element3]…[,element8] Where **element** = [!]Freq1[+Freq2][+Freq3][+Freq4]/Duration **Freq**: the frequency of the tone (ranges from 200Hz to 7000 Hz). If it is set to 0Hz, it means the tone is not played. A tone consists of at most four different frequencies. **Duration**: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms. You can configure at most eight different tones for one condition, and separate them by commas. (e.g., 250/200, 0/1000, 200+300/500, 600+700+800+1000/2000). If you want the system to play tones once, add an exclamation mark "!" before tones (e.g., !250/200, 0/1000, 200+300/500, 600+700+800+1000/2000). **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	Web User Interface
Busy	Customizes the busy tone for the system. For more information on how to	Web User Interface

Parameter	Description	Configuration Method
	customize the tone, refer to the parameter "Ring Back". **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	
Call Waiting	Customizes the call waiting tone for the system. For more information on how to customize the tone, refer to the parameter "Ring Back". **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	Web User Interface
Auto Answer	Customizes the auto answer tone for the system. For more information on how to customize the tone, refer to the parameter "Ring Back". **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	Web User Interface

To configure tones via web user interface:

1. Click on **Setting**->**Tones**.
2. Select the desired value from the pull-down list of **Select Country**.

   If you select **Custom**, you can customize the tone for indicating each condition of the system.



3. Click **Confirm** to accept the change.

System Management

This chapter provides operating instructions, such as managing directory, call history and dual screen. Topics include:

- Directory
- LDAP
- Call History
- Search Source List in Dialing
- Dual Screen
- License
- VCS Integrated with Control Systems

Directory

VC400/VC120 system can display: local contacts, Yealink Cloud contacts and YMS contacts.

- **Local contacts:** The VC400 system can store up to 500 local contacts and 100 conference contacts. The VC120 system can store up to 500 local contacts, and does not support conference contacts.

  You can add multiple numbers for a local contact (at most 3). A conference contact consists of one or more local contacts (at least 1, at most 3). You can establish a conference call quickly by calling conference contacts.

  You can import or export local contact list to different systems to share the local directory. The system only supports the XML and CSV format contact lists. You can view local directory via web user interface, remote control and the video conferencing phone. But you can edit or delete the local directory via web user interface and remote control.
- **Yealink Cloud contacts**: If you log into the Yealink VC Cloud Management Service platform, Yealink Cloud contacts which are created by your administrator, appear in your directory. Note that only the administrator can add, edit and delete Yealink Cloud contacts on the Yealink VC Cloud management service. On your VC400&VC120, you can only search for and place calls to the Yealink Cloud contacts. For more information on Yealink VC Cloud management service, refer to *Yealink VC Cloud Management Service Administrator Guide*.
- **YMS contacts:** If you log into the Yealink Meeting Server, enterprise directory which is created by your administrator, appears in your directory. Note that only the administrator can add, edit and delete the YMS contacts and permanent VMR on the Yealink Meeting Server (YMS). The administrator can also determine whether synchronize the permanent VMR to the VC400&VC120. On your VC400&VC120, you can only search for and place calls

to the YMS contacts and permanent VMR. For more information on Yealink Meeting Server, refer to *Yealink Meeting Server Administrator Guide*.

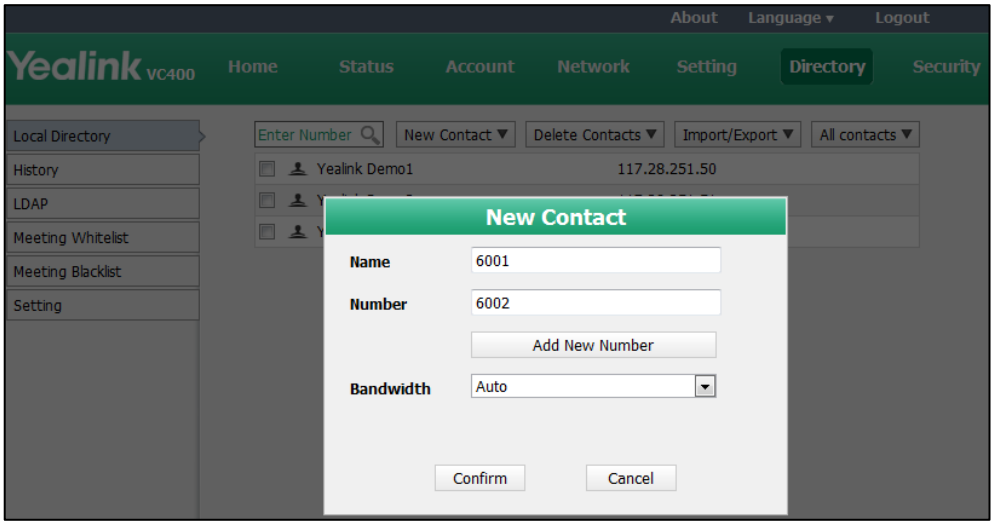
Note Starleaf/Zoom/Pexip/BlueJeans/Mind platform does not provide Cloud contacts for video conferencing system.

The following sections give you detailed steps on how to manage the local directory.

To add local contacts via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Select **Local** from the pull-down list of **New Contact**.
3. Enter the desired name in the **Name** field.
4. Enter the desired number in the **Number** field.
5. Click **Add New Number**, enter other number of the contact.
6. Select the desired contact bandwidth from the pull-down list of **Bandwidth**.

   The default contact bandwidth is **Auto**. The system will select the appropriate bandwidth automatically

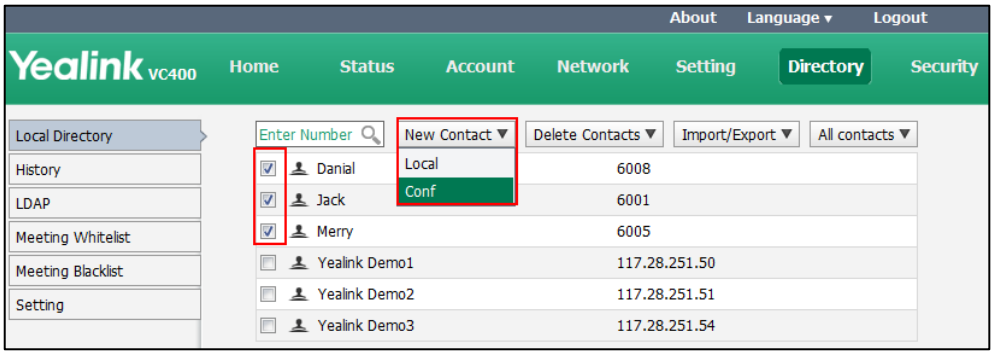


7. Click **Confirm** to accept the change.

To add conference contacts via web user interface:

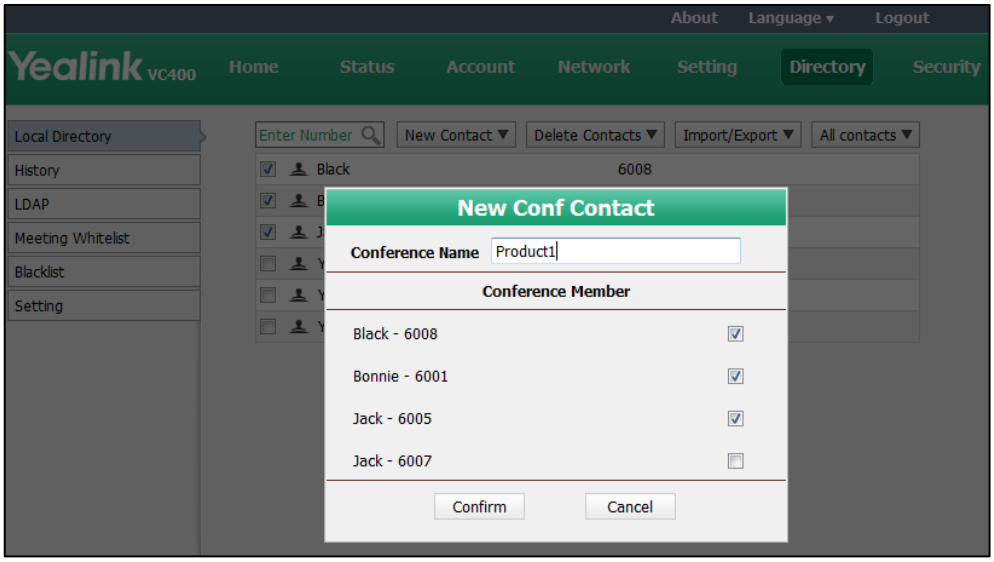
1. Click on **Directory**->**Local Directory**.
2. Check the checkboxes of the desired contacts.
3. Select **Conf** from the pull-down list of **New Contact**.

4. Click **New Contact**, and select **Conf**.



5. Enter the desired name in the **Conference Name** field.

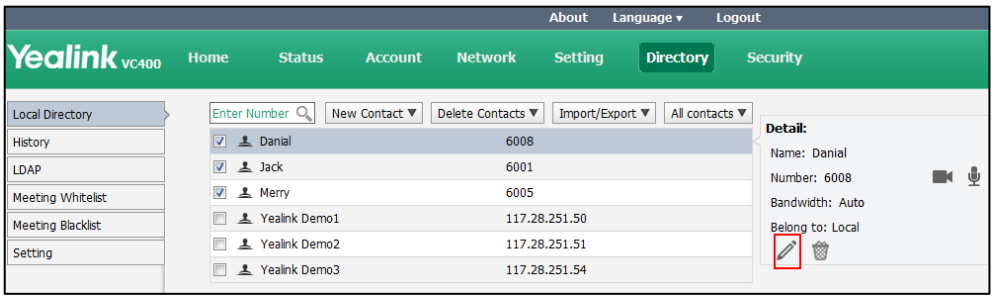
   If multiple numbers are stored for the selected contacts, the system will select number 1 by default.



6. Click **Confirm** to accept the change.

To edit contacts from the local directory via web user interface:

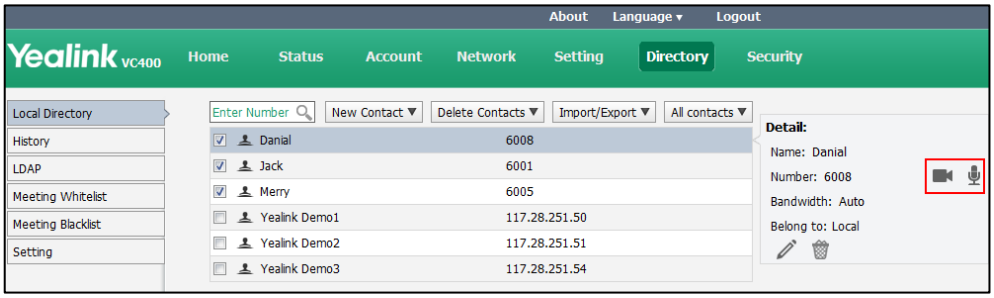
1. Click on **Directory**->**Local Directory**.
2. Hover your cursor over the local contact you want to edit.
3. Click in the pop-up detail box.



4. Edit the contact information.
5. Click **Confirm** to accept the change.

To place calls to contacts from the local directory via web user interface:

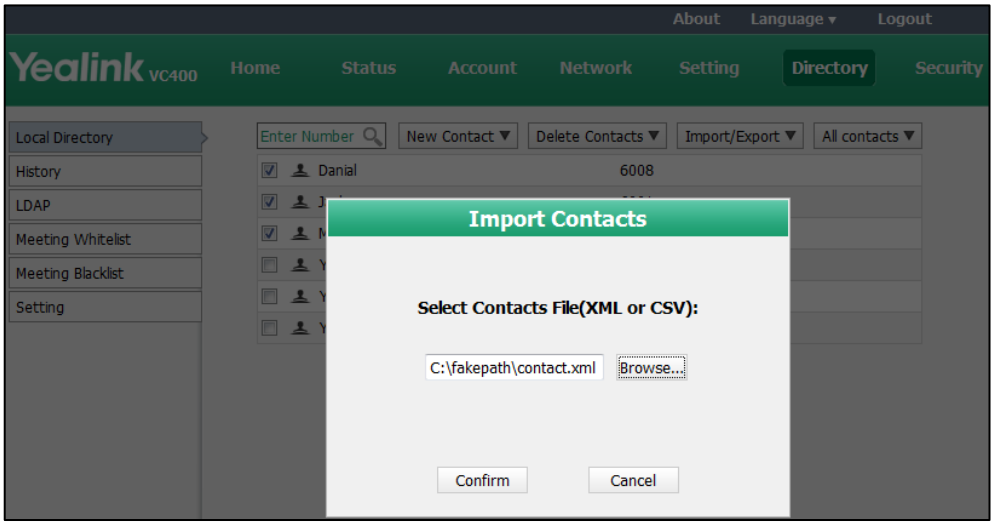
1. Click on **Directory**->**Local Directory**.
2. Hover your cursor over the desired contact.
3. Click or in the pop-up detail box to place a video or voice call.



The web user interface prompts "Connecting, please wait!" and jumps automatically to the **Home** screen.

To import an XML file of the local contact list via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Select **Import**. from the pull-down list of **Import/Export**.
3. Click **Browse** to locate a local contact list file (file format must be *.xml) from your local system.



4. Click **Confirm** to import the local contact list.

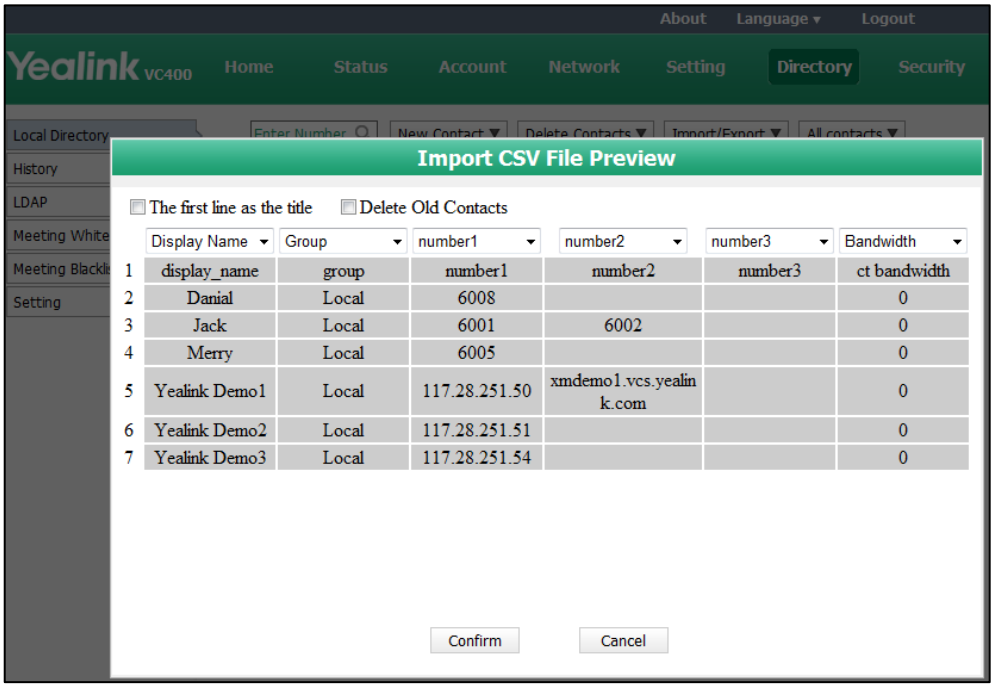
   The web user interface prompts "Contacts imported successfully!".

To import a CSV file of local contact list via web user interface:

1. Click on **Directory**->**Local Directory**.

2. Select **Import**. from the pull-down list of **Import/Export**.
3. Click **Browse** to locate a local contact list file (file format must be *.csv) from your local system.
4. Click **Confirm**.

   The web user interface is shown below:



5. (Optional.) Check the **The first line as the title** checkbox.

   It will prevent importing the title of the local contact information which is located in the first line of the CSV file.

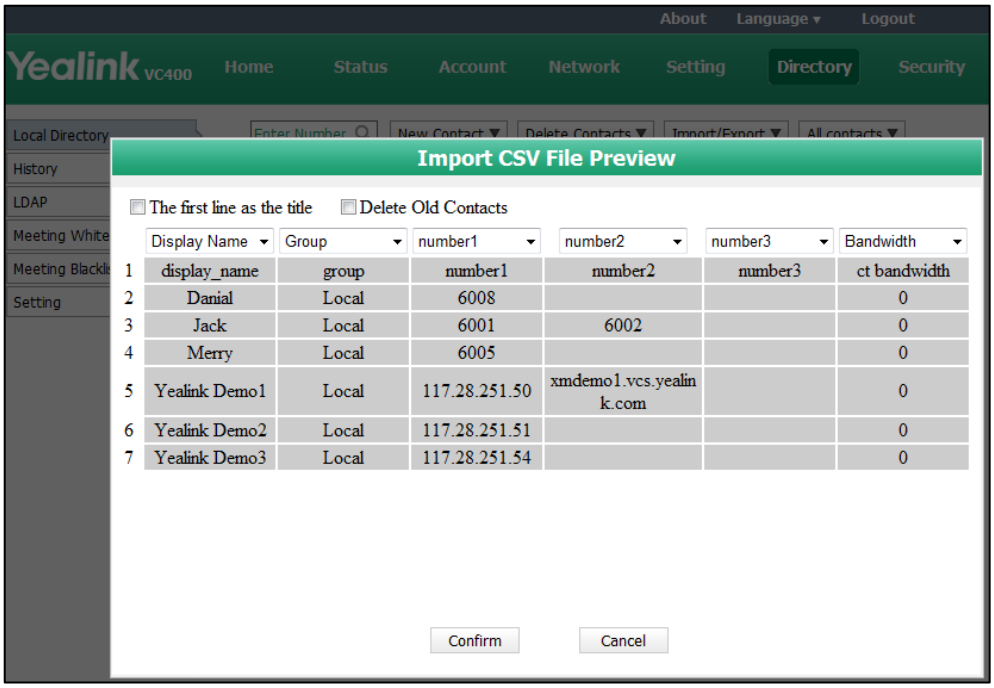
6. (Optional.) Check the **Delete Old Contacts** checkbox.

   It will delete all existing local contacts while importing the local contact list.

7. Select the desired value from the pull-down list.

   - If **Ignore** is selected, this column will not be imported to the system.
   - If **Display Name** is selected, this column will be imported to the system as the contacts' name.
   - If **number1/2/3** is selected, this column will be imported to the system as the contacts' number.

- If **Bandwidth** is selected, this column will be imported to the system as the contact's bandwidth.



8. Click **Confirm** to complete importing the local contact list.

   The web user interface prompts "Contacts imported successfully!".

To export a XML/CSV file of the local contact list via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Select **Export XML** or **Export CSV** from the pull-down list of **Import/Export**.

   The local contact list is saved to your local system.

LDAP

LDAP (Lightweight Directory Access Protocol) is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. Yealink VCS systems are configurable to interface with a enterprise directory server that supports LDAP version 2 or 3. The following LDAP servers are supported:

- Microsoft Active Directory
- Sun ONE Directory Server
- Open LDAP Directory Server
- Microsoft Active Directory Application Mode (ADAM)

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using the system. Therefore they do not have to maintain the local directory. Users can search and dial out from the LDAP directory and save LDAP entries to the local directory. LDAP entries displayed on the display device screen are read only. They cannot be added to, edited or

deleted by users. When an LDAP server is configured properly, the system can look up entries from the LDAP server in a wide variety of ways. The LDAP server indexes all the data in its entries, and "filters" may be used to select the desired entry or group, and retrieve the desired information.

Configurations on the system limit the amount of displayed entries when querying from the LDAP server, and decide how the attributes are displayed and sorted.

Performing a LDAP search on the system:

- Enter search content in the dialing screen. (Ensure that the LADP is in the enabled search source lists)
- In the **Directory** screen, select **Company** to enter the LDAP search screen, and then enter a few characters which you want to search.

The system will send the search request to the LDAP server, the LDAP server then performs a search based on the entered content and configured filter condition, and returns results to the system.

LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on the system:

Abbreviation	Name	Description
gn	givenName	First name
cn	commonName	LDAP attribute is made up from given name joined to surname.
sn	surname	Last name or family name
dn	distinguishedName	Unique identifier for each entry
dc	dc	Domain component
-	company	Company or organization name
-	telephoneNumber	Office phone number
mobile	mobilephoneNumber	Mobile or cellular phone number
ipPhone	IPphoneNumber	Home phone number

LADP parameters are described below:

Parameter	Description	Configuration Method
LDAP Enable	Enables or disables the LDAP feature on the system. **Default:** Disabled	Web User Interface
LDAP Name Filter	Configures the name attribute for LDAP searching.	Web User Interface

Parameter	Description	Configuration Method
	Example: (|(cn=%)(sn=%))	
LDAP Number Filter	Configures the number attribute for LDAP searching. **Example:** (|(telephoneNumber=%)(mobile=%))	Web User Interface
LDAP TLS Mode	Configures the connection mode between the LDAP server and video conferencing system. ● **LDAP**–Unencrypted connection between LDAP server and the system (port 389 is used by default). ● **LDAP TLS Start**–TLS/SSL connection between LDAP server and the system (port 389 is used by default). ● **LDAPs**–TLS/SSL connection between LDAP server and the system (port 636 is used by default). **Default:** LDAP	Web User Interface
LDAP Server Address	Configures the domain name or IP address of the LDAP server.	Web User Interface
Port	Configures the LDAP server port. **Default:** 389	Web User Interface
LDAP User Name	Configures the user name used to login the LDAP server. **Note:** The user name is provided by the server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user name to access the LDAP server.	Web User Interface
LDAP Password	Configures the password to login the LDAP server. **Note:** The password is provided by	Web User Interface

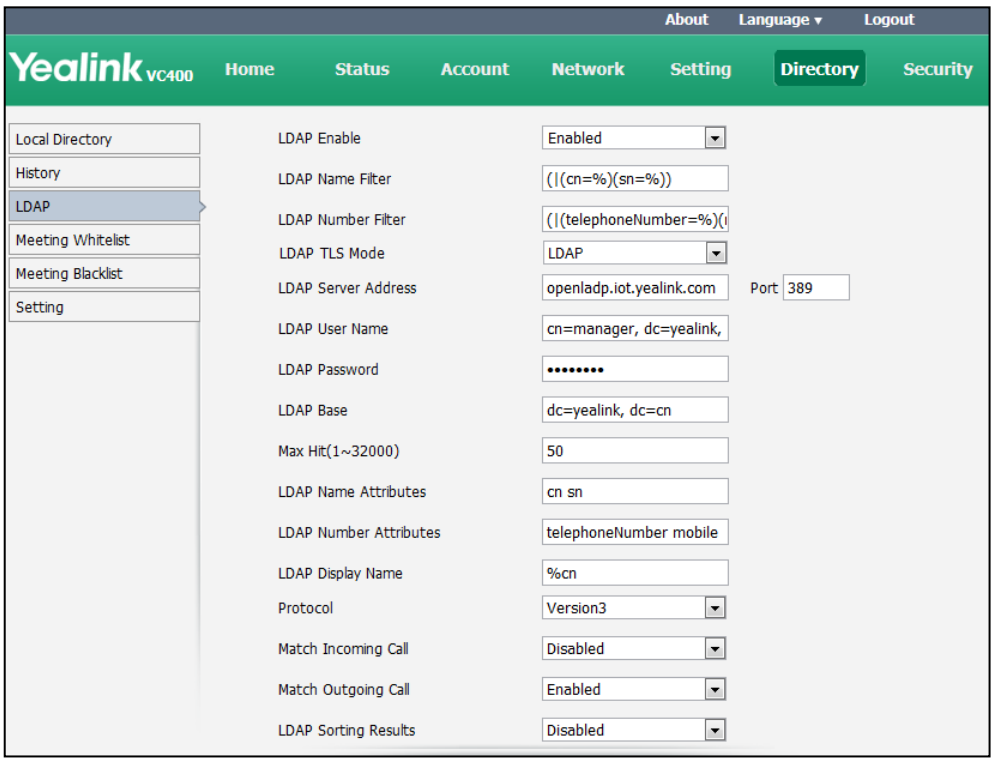
Parameter	Description	Configuration Method
	the server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user password to access the LDAP server.	
LDAP Base	Configures the root path of the LDAP search base. **Example:** cn=manager,dc=yealink,dc=cn	Web User Interface
Max Hit(1~32000)	Configures the maximum number of search results to be returned by the LDAP server.	Web User Interface
LDAP Name Attributes	Configures the name attributes of each record to be returned by the LDAP server. **Note:** multiple name attributes should be separated by spaces. **Example**: cn sn	Web User Interface
LDAP Number Attributes	Configures the number attributes of each record to be returned by the LDAP server. **Note:** multiple numbers attributes should be separated by spaces. **Example**: telephoneNumber mobile	Web User Interface
LDAP Display Name	Configures the display name of the contact record displayed on the LCD screen. **Note:** multiple numbers attributes should be separated by spaces. **Example**: %cn	Web User Interface
Protocol	Configures the protocol for the LDAP server. **Note:** Make sure the protocol value corresponds with the version assigned on the LDAP server.	Web User Interface
Match Incoming Call	Enables or disables the system to match caller numbers with LDAP contacts. **Default**: Disabled	Web User Interface

Parameter	Description	Configuration Method
	Note: If the match is successful, the system will display the caller name when receives an incoming call.	
Match Outgoing Call	Enables or disables the system to match outgoing call numbers with LDAP contacts. **Default**: Enabled **Note:** If the match is successful, the system will display the contact name when places a call.	Web User Interface
LDAP Sorting Results	Enables or disables the system to sort the search results in alphabetical order or numerical order. **Default**: Disabled	Web User Interface

For more information on string representations of LADP query filters, refer to RFC2254.

To configure LDAP via web user interface:

1. Click on **Directory**->**LDAP**.
2. Enter the desired values in the corresponding fields.
3. Select the desired values from the corresponding pull-down lists.



4. Click **Confirm** to accept the change.

Call History

The VC400/VC120 video conferencing system maintains call history lists of All Calls, Missed Calls, Placed Calls and Received Calls. The system supports up to 100 history entries, including local history entries and Cloud history entries.

You can view the call history, place a call or delete an entry from the call history list. You can view the call history and place a call from the call history list via web user interface or the remote control, but you can delete call history only via web user interface.

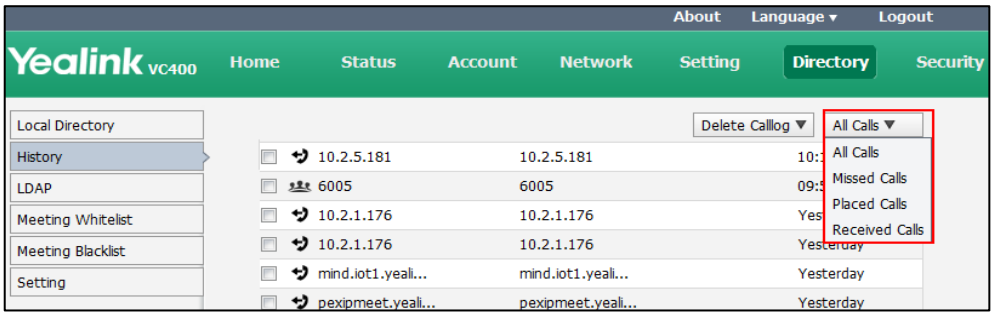
History record feature is enabled by default. If it is disabled, the call history won't be saved. For more information, refer to History Record on page 154.

Note VC120 video conferencing system only supports local call history. It does not support conference call history.

To view call history via web user interface:

1. Click on **Directory**->**History**.

   The web user interface displays all call history.



2. Click **All Calls**, select the desired call history list.

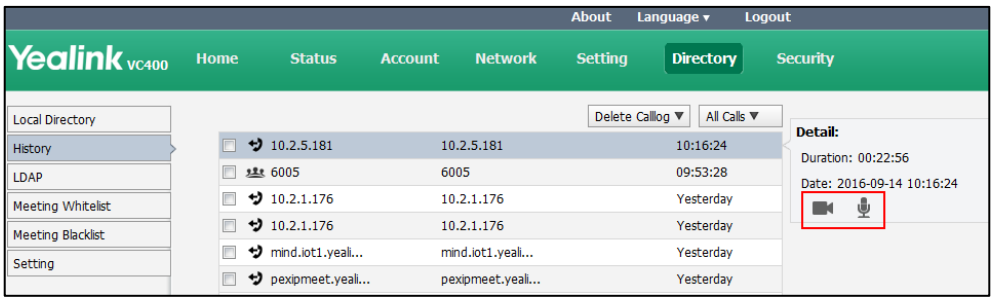
To place a call from the call history list via web user interface:

1. Click on **Directory**->**History**.

   The web user interface displays all call history.

2. Hover your cursor over the entry you want to call.

3. Click or in the pop-up detail box to place a video or voice call.



The web user interface prompts "Connecting, please wait!" and jumps automatically to the **Home** screen.

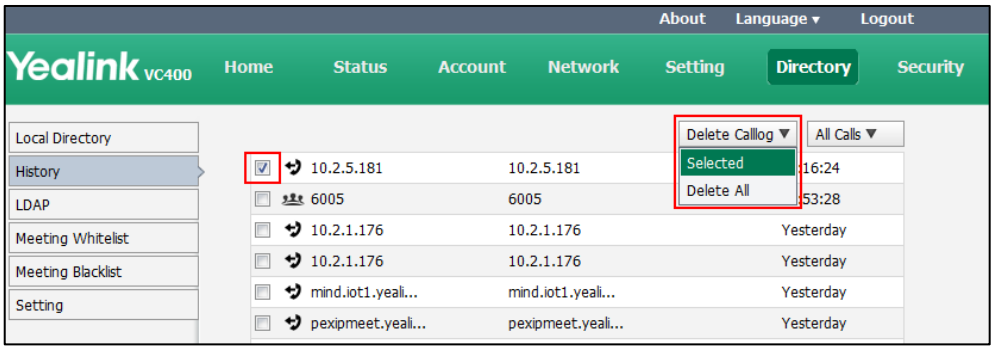
To delete an entry from the call history list via web user interface:

1. Click on **Directory**->**History**.

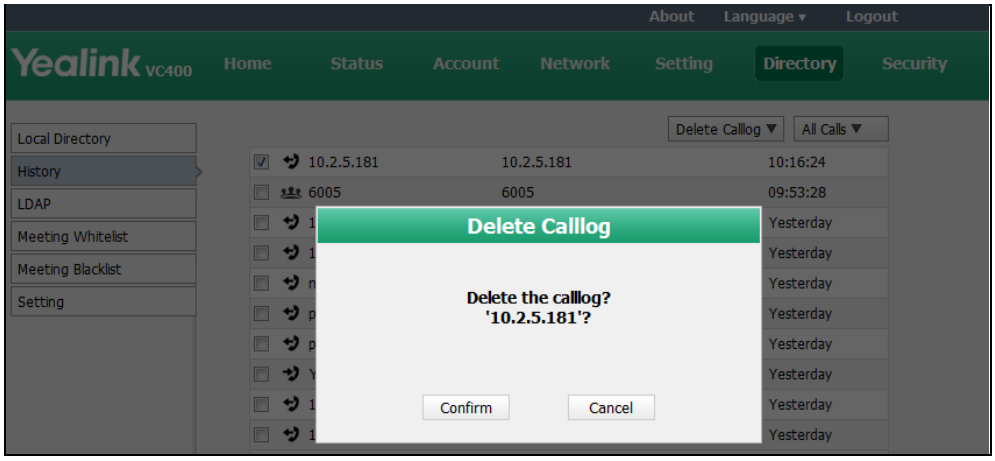
   The web user interface displays all call history.

2. Mark the checkbox for the entry you want to delete.

3. Click **Delete Callog**, and select **Selected**.



The web user interface prompts "Delete the callog?"



5. Click **Confirm** to delete the callog.

You can also select **Delete All** from the from the pull-down list of **Delete Callog** to delete all call log.

Search Source List in Dialing

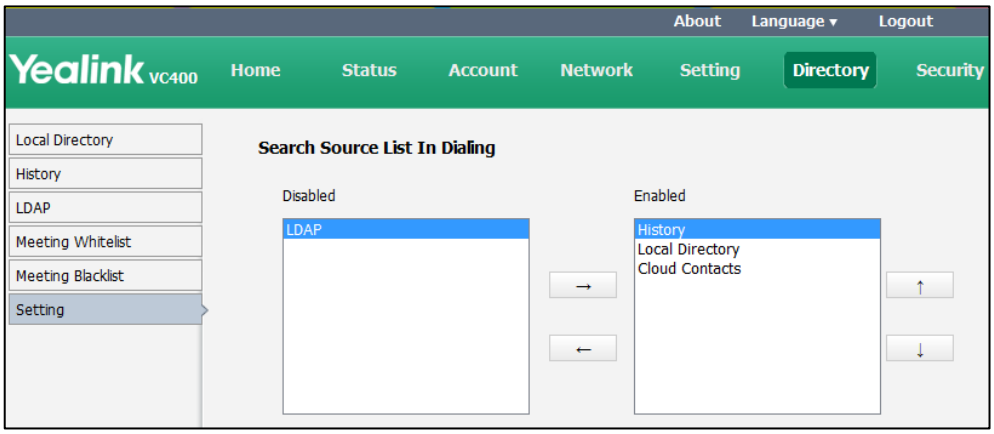
When you enter a few characters in the dialing screen, the system will search for contacts from the enabled search source lists, and display the result in the dialing screen. The lists can be History, Local Directory, Cloud Contact (including your Yealink Cloud contacts and YMS contacts) and LDAP.

To match the desired list, you need to enable the search source list first. If you want to match the LADP list, make sure LDAP is already configured. For more information on how to configure LDAP, refer to LDAP on page 232.

To configure search source list in dialing via web user interface:

1. Click on **Directory**->**Setting**.
2. In the **Search Source List In Dialing** block, select the desired list from the **Disabled** column and click →.

   The selected list appears in the **Enabled** column.
3. Repeat step 2 to add more lists to the **Enabled** column.
4. (Optional.) To remove a list from the **Enabled** column, select the desired list and then click ←.
5. To adjust the display order of the enabled list, select the desired list, and click ↑ or ↓.



6. Click **Confirm** to accept the change.

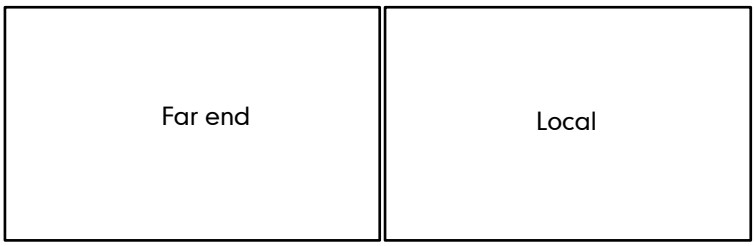
Dual Screen

The VC400/VC120 has two display ports. When connecting only one display device to the VC400/VC120 Codec, Display1 port is the only available port. To make it easier for users to view video images, users can connect two display devices to Display1 and Display2 ports respectively. When two display devices are connected to the VC400/VC120 Codec, the status bar of the primary display device will display icon.

Two-way Video Calls

In the primary display device, the remote video image is shown in full size.

In the secondary display device, the local video image is shown in full size.

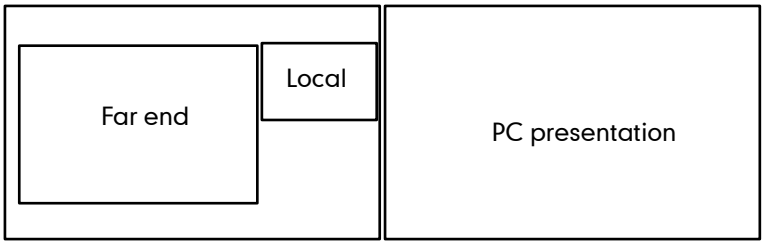


Primary display device Secondary display device

Two-way Video Call with Presentation

In the primary display device, the remote video image is shown in big size, and the local video image along the right side of the screen is shown in small size.

In the secondary display device, the presentation is shown in full size.



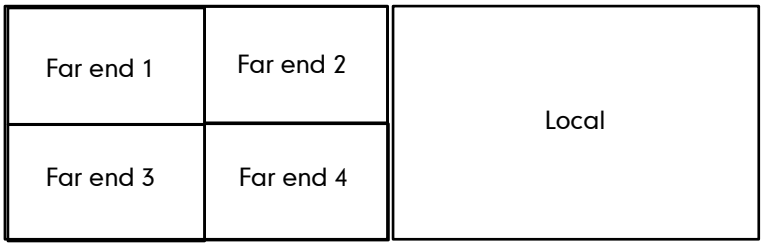
Primary display device Secondary display device

Multi-way Video Calls

Take four-way conference as an example.

In the primary display device, all video images are shown in the same size.

In the secondary display device, the local video image is shown in full size.



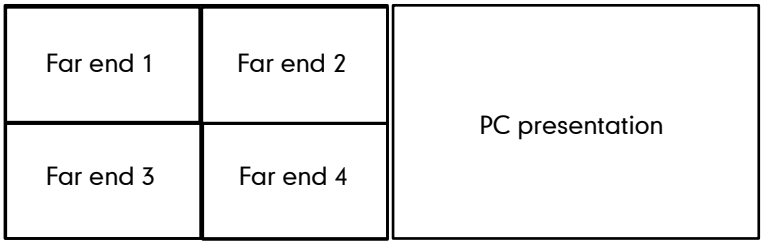
Primary display device Secondary display device

Multi-way Video Call with Presentation

Take four-way conference as an example.

In the primary display device, all video images are shown in the same size.

In the secondary display device, the presentation is shown in full size.



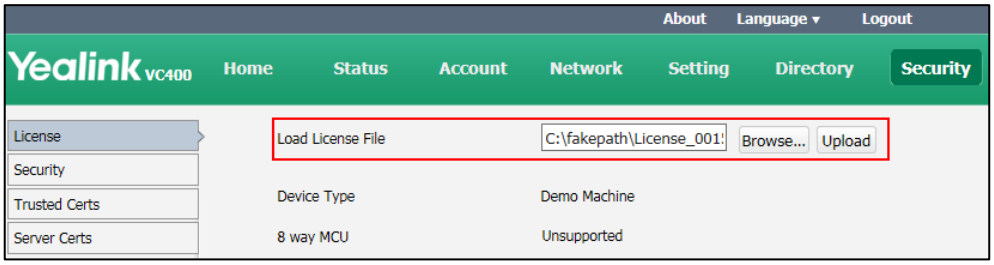
License

Device Type License

If the VC400/VC120 is a demo machine, namely it is used by agents to demonstrate system functions to the customers. The LCD screen of the system will prompt "DEMO ONLY, NOT FOR RESELL". You can change the VC400/VC120 from a demo machine to be a normal machine by importing a device type license. The device type license is configurable via web user interface only.

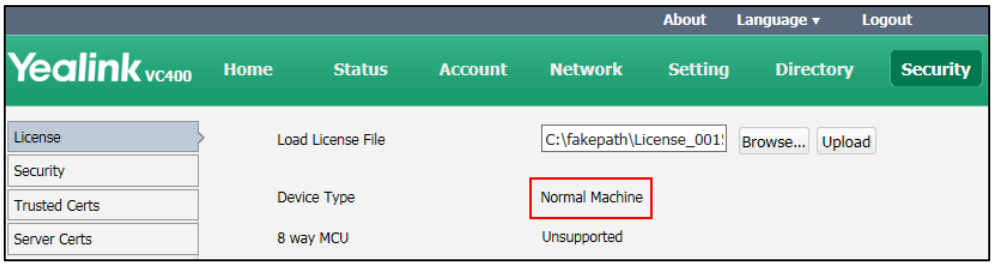
To import the device type license via web user interface:

1. Click on **Security** ->**License**.
2. Click **Browse** to locate the device type license (the file format must be *.dat) from your local system.



3. Click **Upload** to complete importing the device type license.

The device type will change from "Demo Machine" to "Normal Machine".



8-Way MCU License

To initiate a multipoint conference, you must use an MCU.

Without 8-way MCU, the VC400 video conferencing system supports 4-way video calls and an additional voice call (an original caller and four other sites). You can import an 8-way MCU to extend the VC400 to support 8-way video calls and an additional voice call (an original caller and eight other sites).

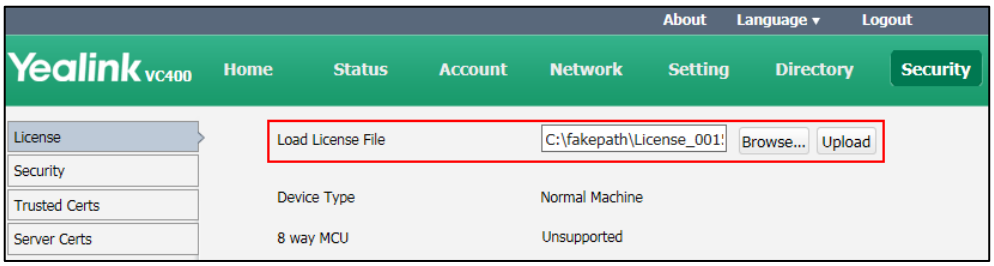
Without 8-way MCU, the VC120 video conferencing system supports one video call and one voice call. You can import an 8-way MCU to extend the VC120 to support 8-way video calls and an additional voice call (an original caller and eight other sites). 8-way MCU is configurable via web user interface only.

8-way MCU is configurable via web user interface only. VC400/VC120 video conferencing system supports a permanent version of the 8-way MCU and a trial version of the 8-way MCU. They have the same feature.

- **Permanent version of the 8-way MCU**: each VC400/VC120 has a unique MCU license. The MCU license cannot be used for other systems. You need to contact Yealink resellers to purchase it, please provide the MAC address of your VC400/VC120 when purchasing.
- **Trial version of the 8-way MCU**: VCS can share a MCU license. You can download a 30-day trial from Yealink website.

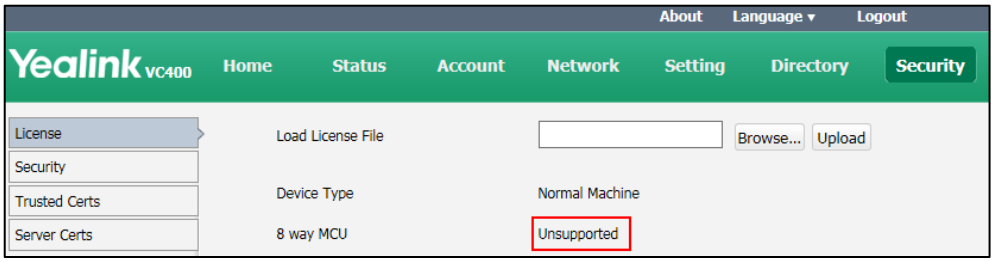
To import the 8-way MCU via web user interface:

1. Click on **Security** ->**License**.
2. Click **Browse** to locate the 8-way MCU (the file format must be *.dat) from your local system.

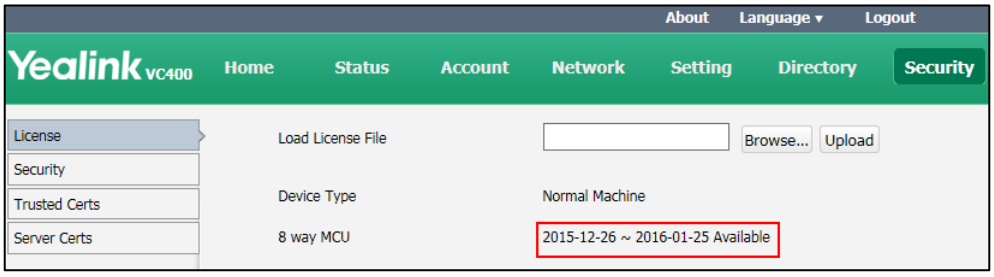


3. Click **Upload** to complete importing the 8-way MCU.

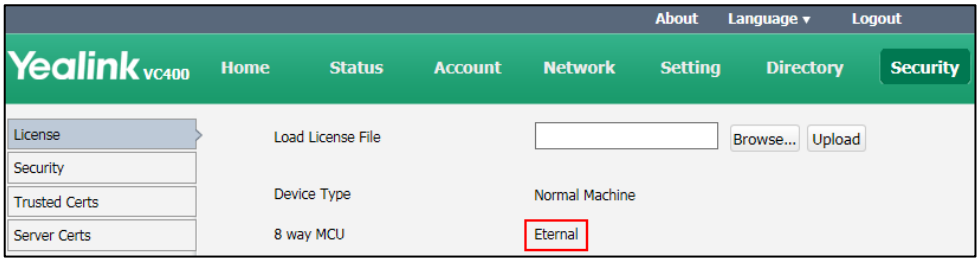
- If the 8 way MCU displays **Unsupported**, it means you have not imported an 8-way MCU.



- If the 8 way MCU displays **X~Y Available**, it means you have imported a trail version of 8-way MCU. So the VC400/VC120 supports up to 8-way video calls and an additional voice call (an original caller and eight other sites) in X~Y period.



- If the 8 way MCU displays **Eternal**, it means you have imported a permanent version of the 8-way MCU. So the VC400/VC120 supports up to 8-way video calls and an additional voice call (an original caller and eight other sites) permanently.



Note

Upgrading the system or performing a factory reset will not affect the imported 8-way license.

If the system has been imported a trial version of the 8-way license and the license has not expired, and you import a permanent version to the system, the permanent version will overwrite the trial version.

If the system has been imported a permanent version of the 8-way license, and you import a trial version to the system, the permanent version will not be overwritten.

VCS Integrated with Control Systems

The Yealink video conferencing systems provide an API interface for the third-party control system. The API commands can be sent to Yealink video conferencing systems over LAN or

serial port, to realize controlling the Yealink video conferencing systems.

Using the API with a LAN Connection

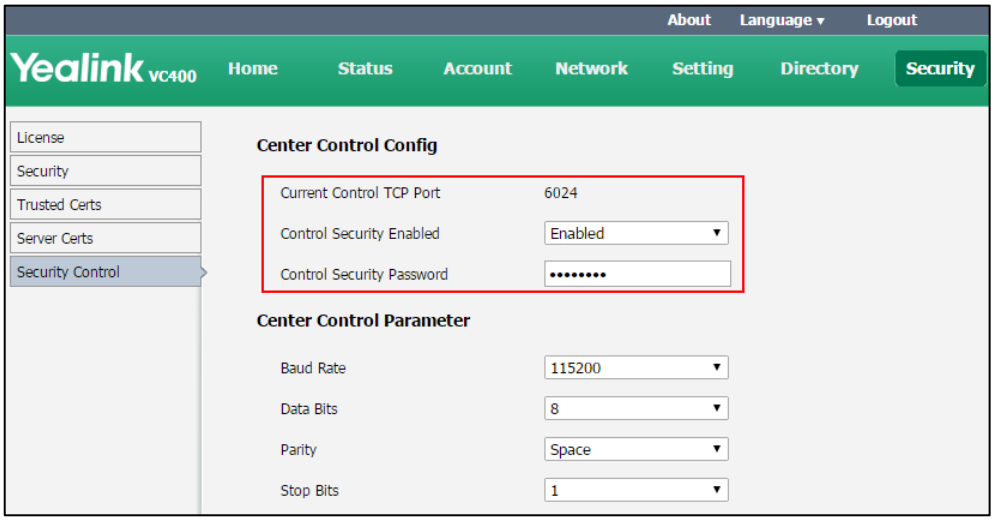
API commands can be sent to video conferencing system through TCP protocol. The control system needs to know the IP address and port of the Yealink video conferencing system. For security, you can configure an authentication password for TCP connection.

LAN Connection parameters are described below.

Parameter	Description	Configuration Method
Current Control TCP Port	Control TCP port (read-only). **Default:** 6024	Web User Interface
Control Security Enabled	Enables or disables an authentication password for TCP connection **Default:** Enabled	Web User Interface
Control Security Password	Configures the authentication password for TCP connection.	Web User Interface

To configure LAN Connection parameters via web user interface:

1. Click on **Security**->**Security Control**.
2. Select the desired value from the pull-down lists of **Control Security Enabled**.
3. Enter the desired password in the **Control Security Password** field.



4. Click **Confirm** to accept the change.

Using the API with a Serial Connection

You can use the API with a serial connection to control Yealink video conferencing system. The USB port on the Yealink video conferencing system can be connected to the serial port on the control system through a USB to RS-232 cable.

You must connect and configure the control system and the video conferencing system for serial communication.

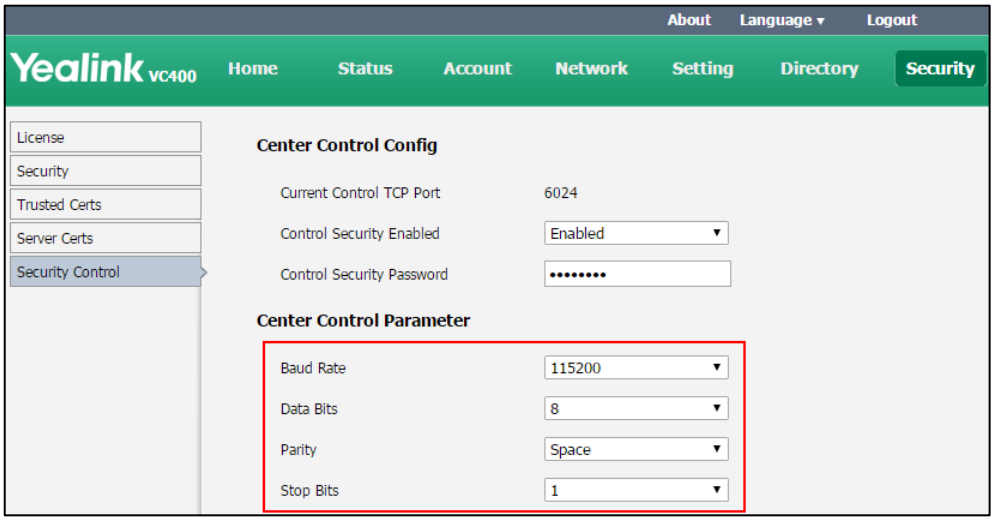
Serial Connection parameters are described below.

Parameter	Description	Configuration Method
Baud Rate	Configures the baud rate. Available baud rates are: • **2400** • **4800** • **9600** • **19200** • **38400** • **115200** **Default:** 115200 **Note**: It must be the same rate for both devices.	Web User Interface
Data Bits	Configures the data bits. Available data bits are: • **7** • **8** **Default:** 8 **Note**: It must be the same data bits for both devices.	Web User Interface
Parity	Configures the parity. Available parity are: • **None** • **Odd** • **Even** • **Space** **Default:** Space **Note**: It must be the same parity for	Web User Interface

Parameter	Description	Configuration Method
	both devices.	
Stop Bits	Configures the stop bits. Available stop bits are: • **1** • **2** **Default:** 1 **Note**: It must be the same stop bits for both devices.	Web User Interface

To configure serial connection parameters via web user interface:

1. Click on **Security**->**Security Control**.
2. Select the desired value from the pull-down lists of **Baud Rate**.
3. Select the desired value from the pull-down lists of **Data Bits**.
4. Select the desired value from the pull-down lists of **Parity**.
5. Select the desired value from the pull-down lists of **Stop Bits**.



6. Click **Confirm** to accept the change.

When you successfully deploy environment and configure the third-party control system, the Yealink video conferencing systems and the control devices, you can remotely manage certain features of your video conferencing system via the control device.

For more information, refer to *Yealink VC Deployment and User Manual for Control Systems*.

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- User Mode
- Administrator Password
- Web Server Type
- Transport Layer Security
- Secure Real-Time Transport Protocol
- H.235
- Defending against Attacks

User Mode

Users can access the system menus directly (except the “Advanced” menu) on the display device. The “Advanced” menu requires administrator credentials. You can enable the user mode to provide two levels of access for the menus. You need to configure a password for the user when the user mode is enabled. Users are prompted to enter the password when accessing the menus (except the “Status” menu). After the user mode is enabled, the user can log into the web user interface of the system with user credentials. The default user name is “user”.

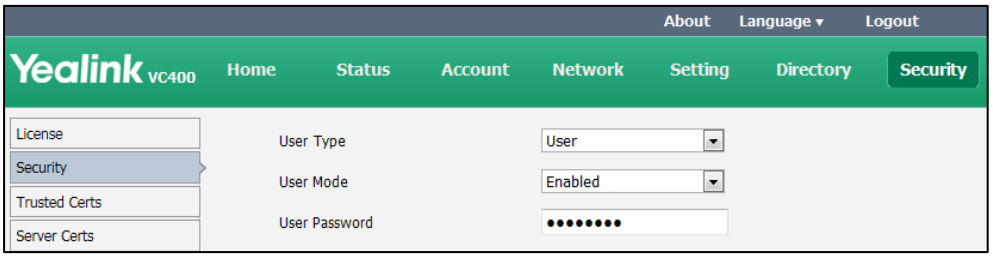
User mode parameters on the system are described below:

Parameter	Description	Configuration Method
User Type	Specifies the user type. **Default:** Administrator **Note:** To enable the user mode, you need to select User for this parameter.	Web User Interface
User Mode	Enables or disables the user mode. **Default:** Disabled **Note:** It is only applicable to the user mode. The administrator mode is enabled by default.	Web User Interface
User Password	Configures a password for the user to access the menu options or log into the web user interface. **Note:** It can only be configured	Web User Interface

Parameter	Description	Configuration Method
	when the user mode is enabled. The system supports ASCII characters 32-126(0x20-0x7E) in passwords. You can leave the password blank.	

To configure user mode via web user interface:

1. Click on **Security**->**Security**.
2. Select **User** from the pull-down list of **User Type**.
3. Select **Enabled** from the pull-down list of **User Mode**.
4. Configure a password or leave it blank in the **User Password** field.



5. Click **Confirm** to accept the change.

Administrator Password

The default enabled user type is administrator. Users can log into the web user interface and access the "Advanced" menu option with administrator privilege by default. The default administrator password is "0000" and can be only changed by an administrator. For security reasons, the administrator should change the default administrator password as soon as possible. The system supports ASCII characters 32-126(0x20-0x7E) in passwords.

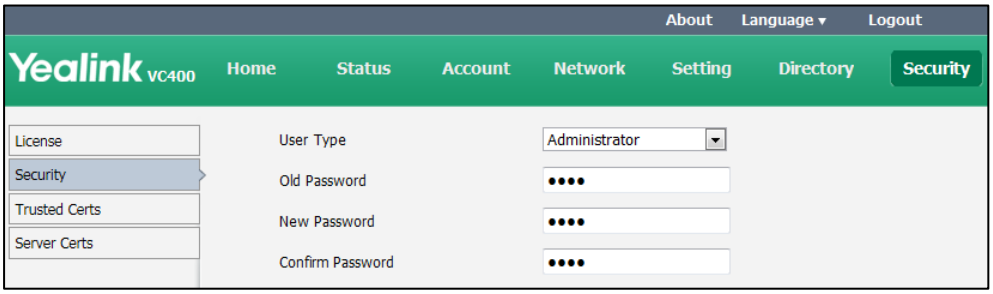
Administrator password parameters on the system are described below:

Parameter	Description	Configuration Method
User Type	Specifies the user type. **Default:** Administrator **Note:** To configure a new administrator password, you need to select Administrator for this parameter.	Web User Interface
Old Password	Enters the old administrator password. **Note:** The default administrator password is "0000".	Remote Control Web User Interface

Parameter	Description	Configuration Method
New Password	Configures a new administrator password. **Note:** You can leave the password blank.	Remote Control Web User Interface
Confirm Password	Enters the new configured administrator password. **Note:** The entered password must be the same as the one configured by the parameter "New Password".	Remote Control Web User Interface

To configure administrator password via web user interface:

1. Click on **Security**->**Security**.
2. Select **Administrator** from the pull-down list of **User Type**.
3. Enter the old administrator password in the **Old Password** field.
4. Enter a new password in the **New Password** field.
5. Enter the new password or leave it blank in the **User Password** field.



6. Click **Confirm** to accept the change.

To configure administrator password via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Password Reset**.
2. Enter the old password in the **Current Password** field.
3. Configure a new password in the **New Password** and **Confirm Password** fields.
4. Press the **Save** soft key to accept the change.

Web Server Type

Web server type determines the access protocol of the system's web user interface. The system supports both HTTP and HTTPS protocols for accessing the web user interface. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. HTTPS is a web protocol that encrypts and decrypts user page requests as well as the pages returned by the web server. Both the HTTP and HTTPS port numbers are configurable.

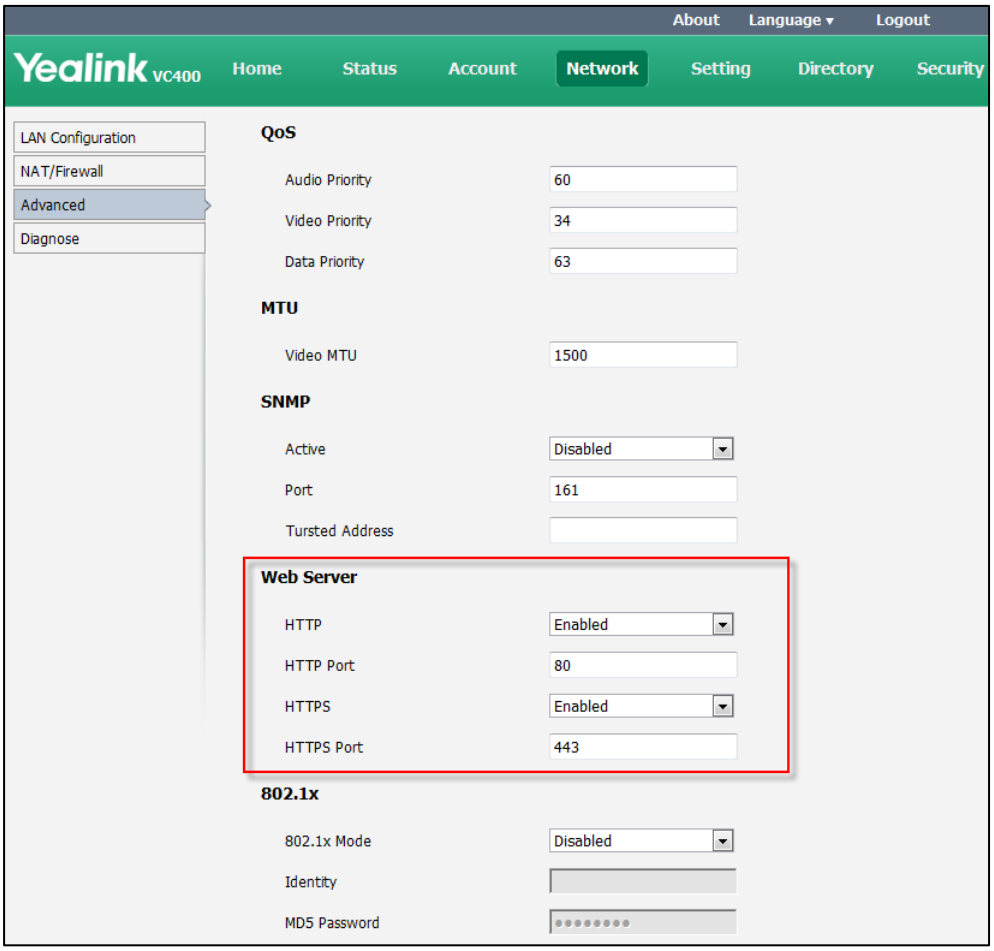
Web server type parameters on the system are described below:

Parameter	Description	Configuration Method
HTTP	Enables or disables the user to access the web user interface of the system using the HTTP protocol. **Default:** Enabled	Remote Control Web User Interface
HTTP Port	Specifies the HTTP port for the user to access the web user interface of the system. **Valid Values:** 1-65535 **Default:** 80 **Note:** Ensure that the configured port is not used.	Web User Interface
HTTPS	Enables or disables the user to access the web user interface of the system using the HTTPS protocol. **Default:** Enabled	Remote Control Web User Interface
HTTPS Port	Specifies the HTTPS port for the user to access the web user interface of the system. **Valid Values:** 1-65535 **Default:** 443 **Note:** Ensure that the configured port is not used.	Web User Interface

To configure web server type via web user interface:

1. Click on **Network**->**Advanced**.
2. Select the desired value from the pull-down list of **HTTP**.
3. Enter the desired HTTP port in the **HTTP Port** field.
4. Select the desired value from the pull-down list of **HTTPS**.

5. Enter the desired HTTPS port in the **HTTPS Port** field.



6. Click **Confirm** to accept the change.

To configure web server type via the remote control:

1. Select **Menu**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Select the desired value from the pull-down list of **Web Server Type**.
3. Press the **Save** soft key to accept the change.

Transport Layer Security

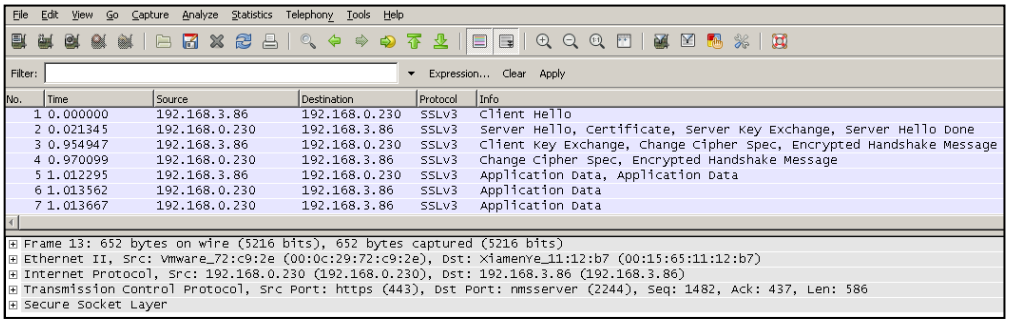
TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing the system to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

TLS protocol is composed of two layers: TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The system supports TLS 1.0. A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the TLS/SSL network protocol. The system supports the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the system and TLS server to establish an encrypted communication channel:



Step1: The system sends "Client Hello" message proposing SSL options.

Step2: Server responds with "Server Hello" message selecting the SSL options, sends its public key information in "Server Key Exchange" message and concludes its part of the negotiation with "Server Hello Done" message.

Step3: The system sends key session information (encrypted by server's public key) in the "Client Key Exchange" message.

Step4: Server sends "Change Cipher Spec" message to activate the negotiated options for all future messages it will send.

The system can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for the SIP account, the message of the SIP account will be encrypted after the successful TLS negotiation.

Certificates

The system can serve as a TLS client or a TLS server. The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate**: When the system requests a TLS connection with a server, the system should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The system has 36 built-in trusted certificates. You can upload up to 10 custom certificates to the system. The format of the certificates must be *.pem, *.cer, *.crt and *.der. For more information on 36 trusted certificates, refer to Appendix B: Trusted Certificates on page 298.
- **Server Certificate**: When clients request a TLS connection with the system, the system sends the server certificate to the clients for authentication. The system has two types of built-in server certificates: a unique server certificate and a generic server certificate. You can only upload one server certificate to the system. The old server certificate will be overridden by the new one. The format of the server certificate files must be *.pem and *.cer.
  - **A unique server certificate**: It is installed by default and is unique to a system (based on the MAC address) and issued by the Yealink Certificate Authority (CA).
  - **A generic server certificate**: It is installed by default and is issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the system may send a

generic certificate for authentication.

The system can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates. You can specify the type of certificates the system accepts: default certificates, custom certificates, or all certificates.

Common Name Validation feature enables the system to mandatorily validate the common name of the certificate sent by the connecting server. And Security verification rules are compliant with RFC 2818.

TLS parameters on the system are described below:

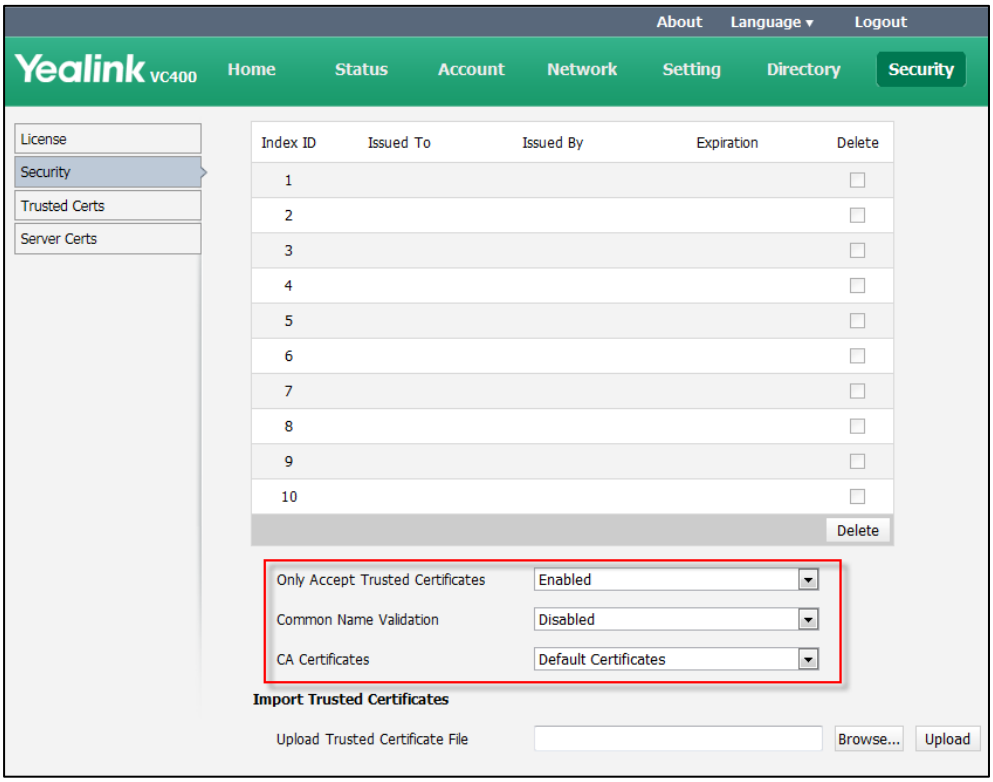
Parameter	Description	Configuration Method
Transport	Configures the type of transport protocol. You can configure it for the Zoom/Pexip/BlueJeans/Mind/Custom platform, or SIP account separately. ● **UDP**−provides best-effort transport via UDP for the SIP signaling. ● **TCP**−provides reliable transport via TCP for SIP signaling. ● **TLS**−provides secure communication for SIP signaling. ● **DNS-NAPTR**−performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** For Zoom/Pexip/BlueJeans/Mind/Custom platform, the default value is TCP. For SIP account, the default value is UDP. **Note:** You cannot configure it for the Yealink/StarLeaf Cloud platform.	Remote Control Web User Interface
Only Accept Trusted Certificates	Enables or disables the system to only trust the server certificates in the Trusted Certificates list. **Default:** Enabled **Note:** If it is enabled, the system will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, will the system trust the server.	Web User Interface

Parameter	Description	Configuration Method
	If you change this parameter, the system will reboot to make the change take effect.	
Common Name Validation	Enables or disables the system to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server. **Default:** Disabled **Note:** If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
CA Certificates	Configures the type of certificates in the Trusted Certificates list for the system to authenticate for the TLS connection. • **Default Certificates** • **Custom Certificates** • **All Certificates** **Default:** Default Certificates **Note:** If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Upload Trusted Certificate File	Upload the custom CA certificate to the system. **Note:** A maximum of 10 CA certificates can be uploaded to the system. The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.	Web User Interface
Device Certificates	Upload the customized CA certificate to the system. • **Default Certificates** • **Custom Certificates** **Default:** Default Certificates **Note:** If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Upload Server Certificate File	Upload the custom device certificate to the system. **Note:** Only one device certificate can be	Web User Interface

Parameter	Description	Configuration Method
	uploaded to the system. The device certificate you want to upload must be in *.pem or *.cer format.	

To configure the trusted certificate feature via web user interface:

1. Click on **Security**->**Trusted Certs**.
2. Select the desired value from the pull-down list of **Only Accept Trusted Certificates**.
3. Select the desired value from the pull-down list of **Common Name Validation**.
4. Select the desired value from the pull-down list of **CA Certificates**.



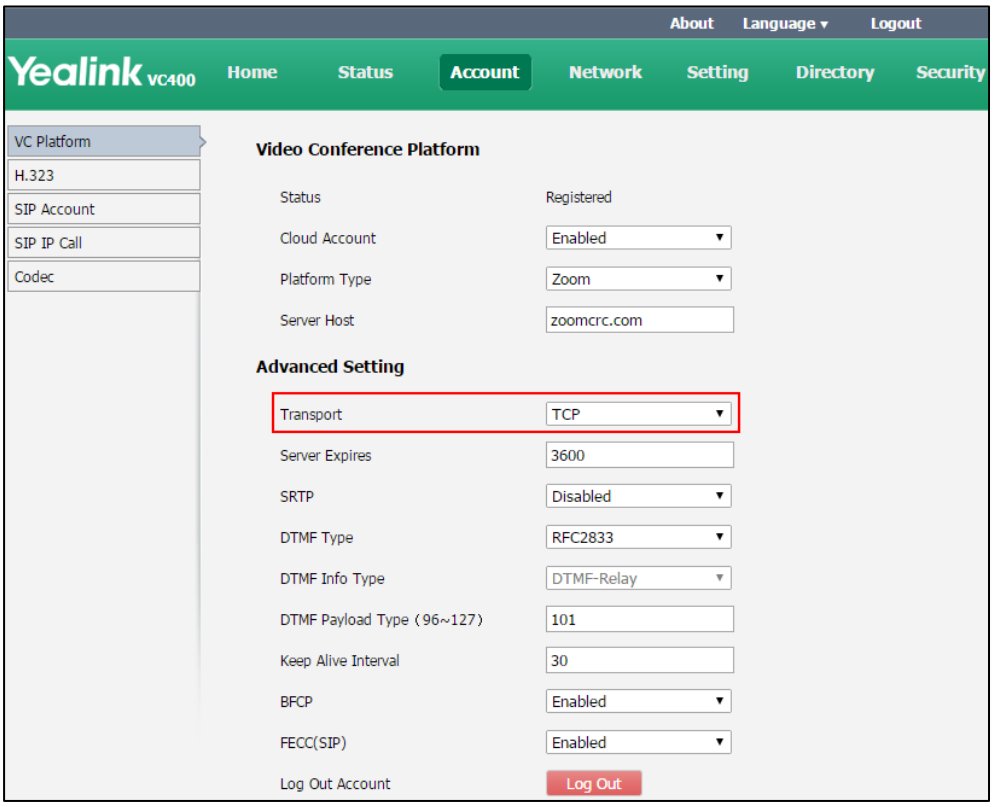
5. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.
6. Click **Confirm** to reboot the system immediately.

To configure TLS for the Zoom/Pexip/BlueJeans/Mind/Custom platform via web user interface:

1. Click on **Account->VC Platform**
2. Select **Zoom/Pexip/BlueJeans/Mind/Custom** from the pull-down list of **Platform Type**.

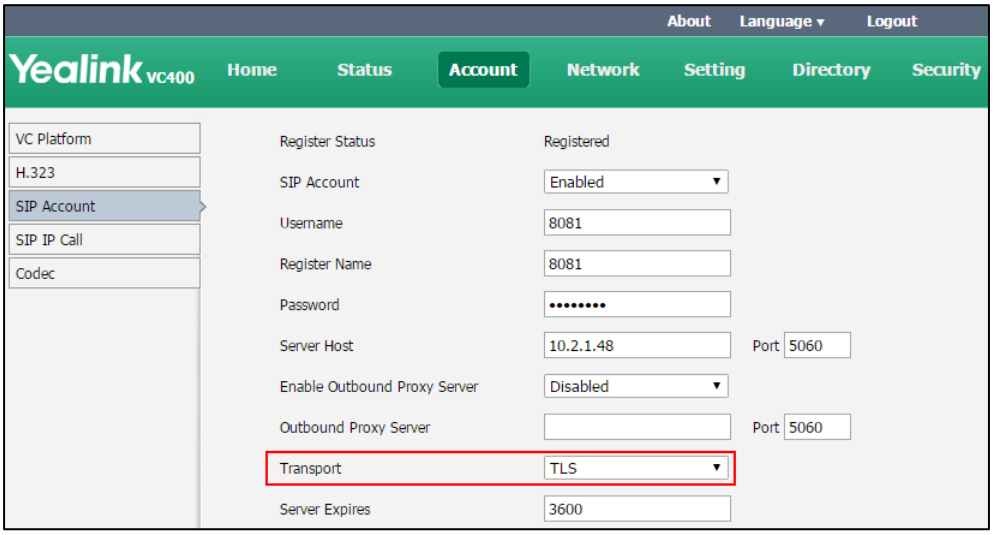
3. Select **TLS** from the pull-down list of the **Transport**.



4. Click **Confirm** to accept the change.

To configure TLS for the SIP account via web user interface:

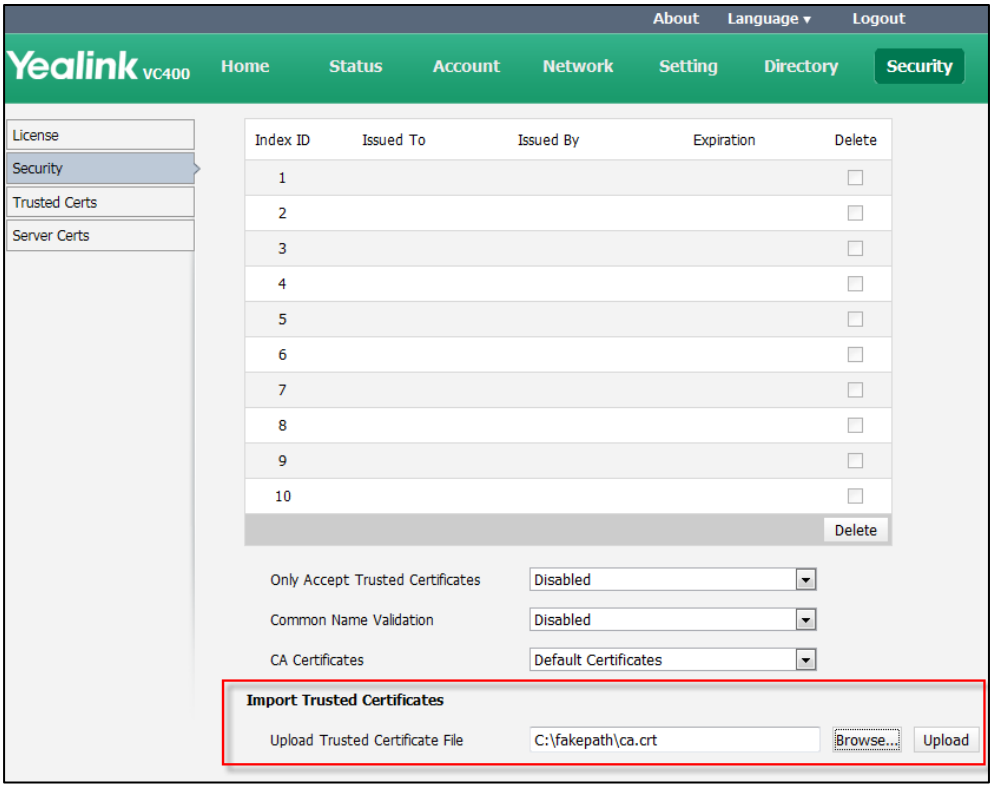
1. Click on **Account**->**SIP Account**.
2. Select **TLS** from the pull-down list of the **Transport**.



3. Click **Confirm** to accept the change.

To upload a CA certificate via web user interface:

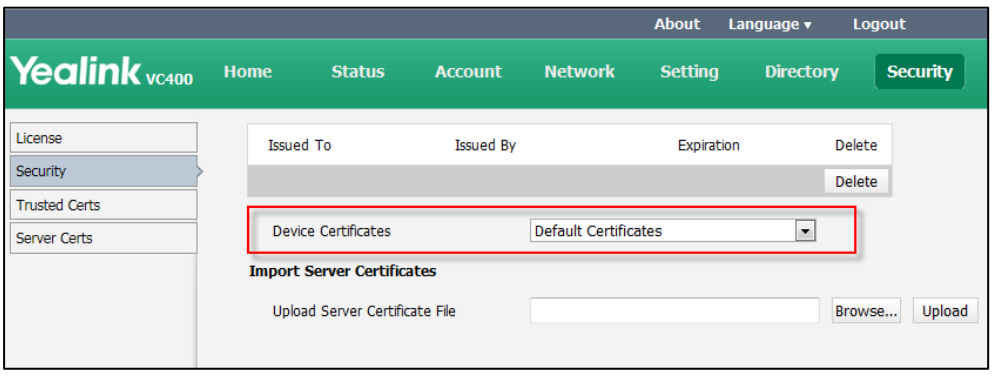
1. Click on **Security**->**Trusted Certs**.
2. Click **Browse** to locate the certificate (*.pem,*.crt, *.cer or *.der) from your local system.



3. Click **Upload** to upload the certificate.

To configure the device certificate via web user interface:

1. Click on **Security**->**Server Certs**.
2. Select the desired value from the pull-down list of **Device Certificates**.



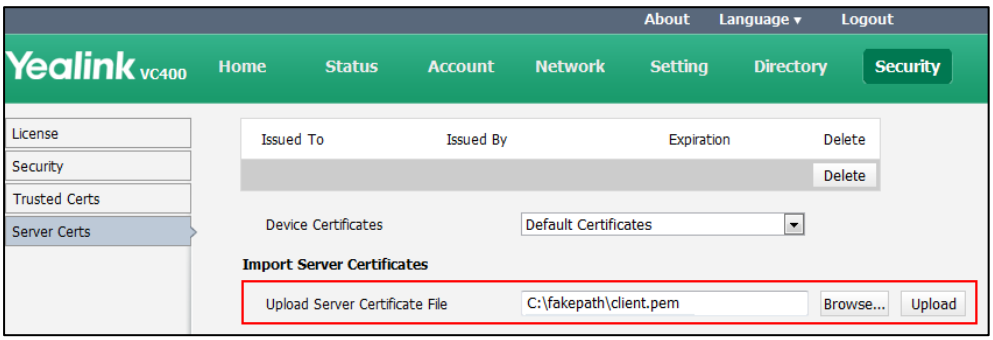
3. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.

4. Click **Confirm** to reboot the system immediately.

To upload a device certificate via web user interface:

1. Click on **Security**->**Server Certs**.
2. Click **Browse** to locate the certificate (*.pem or *.cer) from your local system.



3. Click **Upload** to upload the certificate.

Secure Real-Time Transport Protocol

During a confidential call, you can configure Secure Real-Time Transport Protocol (SRTP) to encrypt RTP streams to avoid interception and eavesdropping. Both RTP and RTCP signaling may be encrypted using an AES algorithm as described in RFC3711. Encryption modifies the data in the RTP streams so that, if the data is captured or intercepted, it cannot be understood—it sounds like noise. Only the receiver knows the key to restore the data. To use SRTP encryption for SIP calls, the participants in the call must enable SRTP simultaneously. When this feature is enabled on both systems, the encryption algorithm utilized for the session is negotiated between the systems. This negotiation process is compliant with RFC 4568.

When a site places a call on the SRTP enabled system, the system sends an INVITE message with the RTP encryption algorithm to the destination system.

The following is an example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NzFlNTUwZDk2OGVlOTc3YzNkYTkwZWVkMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
```

```
a=ptime:20
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm, and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.

The following is an example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

The SRTP parameter on the system is described below:

Parameter	Description	Configuration Method
SRTP	Specifies the SRTP type. You can configure it for the Zoom/Pexip/BlueJeans/Mind/Custom platform, SIP account or SIP IP call separately. ● **Disabled—**do not use SRTP in SIP calls. ● **Optional**−negotiate with the far site whether to use SRTP for media encryption in SIP calls. ● **Compulsory**−compulsory use SRTP for media encryption in SIP calls. **Default:** Disabled **Note:** You cannot configure it for the Yealink/StarLeaf Cloud platform.	Web User Interface

Rules of SRTP for media encryption in SIP calls:

Far \ Near	Compulsory	Optional	Disabled
Compulsory	SRTP Call	SRTP Call	Fail to establish call
Optional	SRTP Call	SRTP Call	RTP Call
Disabled	Fail to establish call	RTP Call	RTP Call

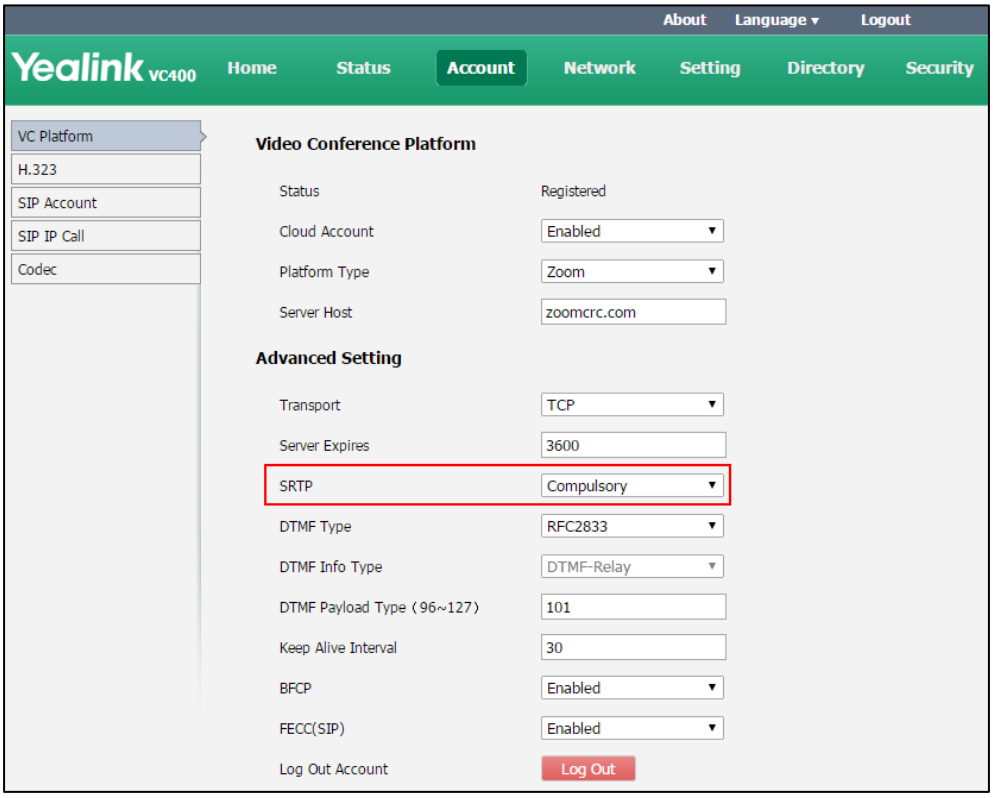
When SRTP is enabled on both systems, RTP streams will be encrypted, and the lock icon appears on the display device of each system after successful negotiation.

Note

If SRTP is enabled for the Cloud platform or SIP account, you should also configure the transport type to TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to Transport Layer Security on page 251.

To configure SRTP for Zoom/Pexip/BlueJeans/Mind/Custom platform via web user interface:

1. Click on **Account->VC Platform**.
2. Select **Zoom/Pexip/BlueJeans/Mind/Custom** from the pull-down list of **Platform Type**.
3. Select the desired value from the pull-down list of **SRTP**.

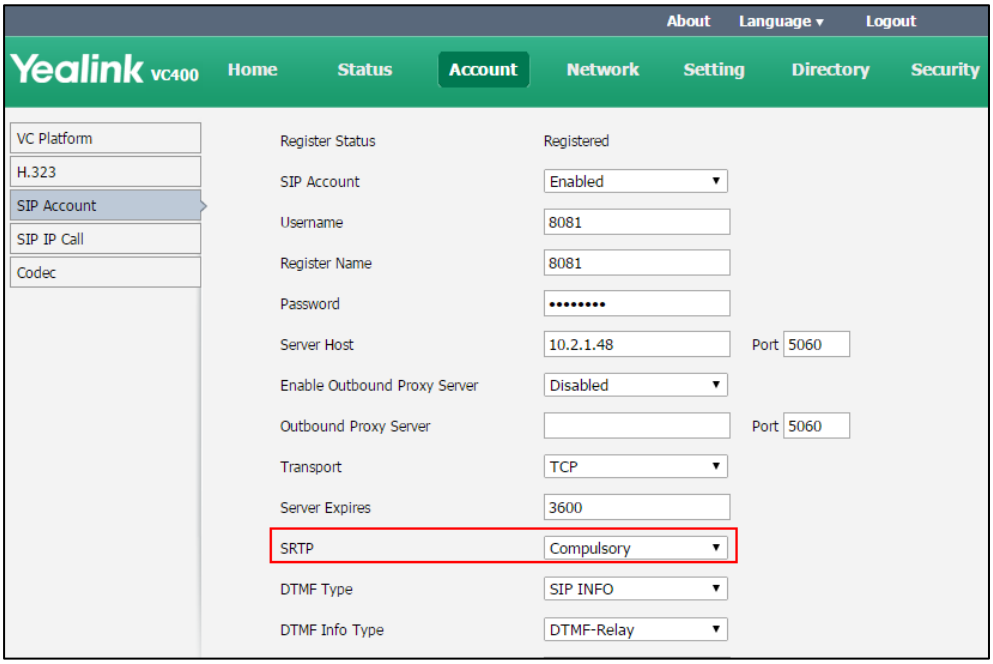


4. Click **Confirm** to accept the change.

To configure SRTP for SIP account via web user interface:

1. Click on **Account->SIP Account**.

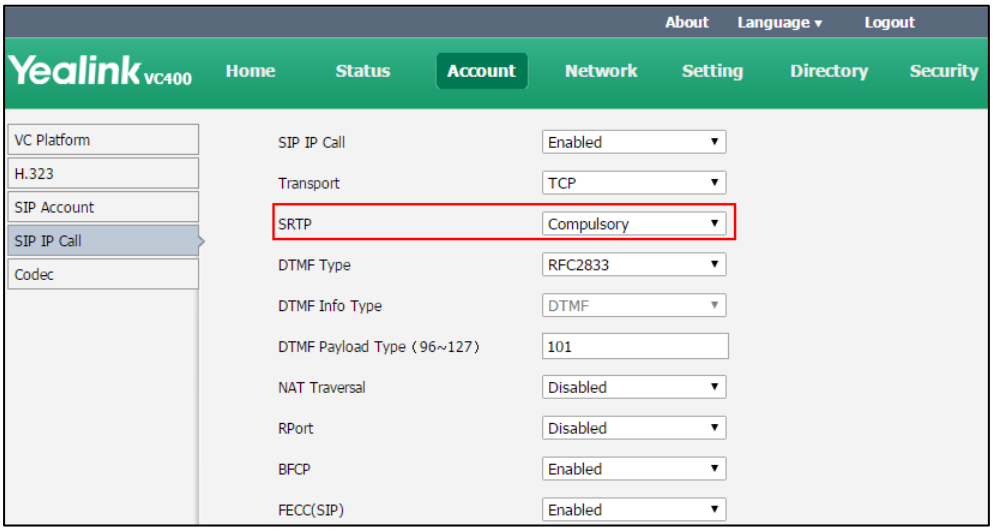
2. Select the desired value from the pull-down list of **SRTP**.



3. Click **Confirm** to accept the change.

To configure SRTP for SIP IP call via web user interface:

1. Click on **Account->SIP IP Call**.
2. Select the desired value from the pull-down list of **SRTP**.



3. Click **Confirm** to accept the change.

H.235

Yealink video conferencing systems support H.235 128-bit AES algorithm using the Diffie-Hellman key exchange protocol in H.323 calls. To use H.235 feature for H.323 calls, the participants in the call must enable the H.235 feature simultaneously. When a site places a call on the H.235 feature enabled system, the system negotiates the encryption algorithm with the destination system.

The H.235 parameter on the system is described below:

Parameter	Description	Configuration Method
H.235	Specifies the H.235 type. You can configure it for the StarLeaf Cloud platform or H.323 call separately. • **Disabled**–do not use H.235 in H.323 calls. • **Optional**–negotiate with the far site whether to use H.235 in H.323 calls. • **Compulsory**–compulsively use H.235 in H.323 calls. **Default:** Disabled	Web User Interface

Rules of H.235 security in H.323 calls:

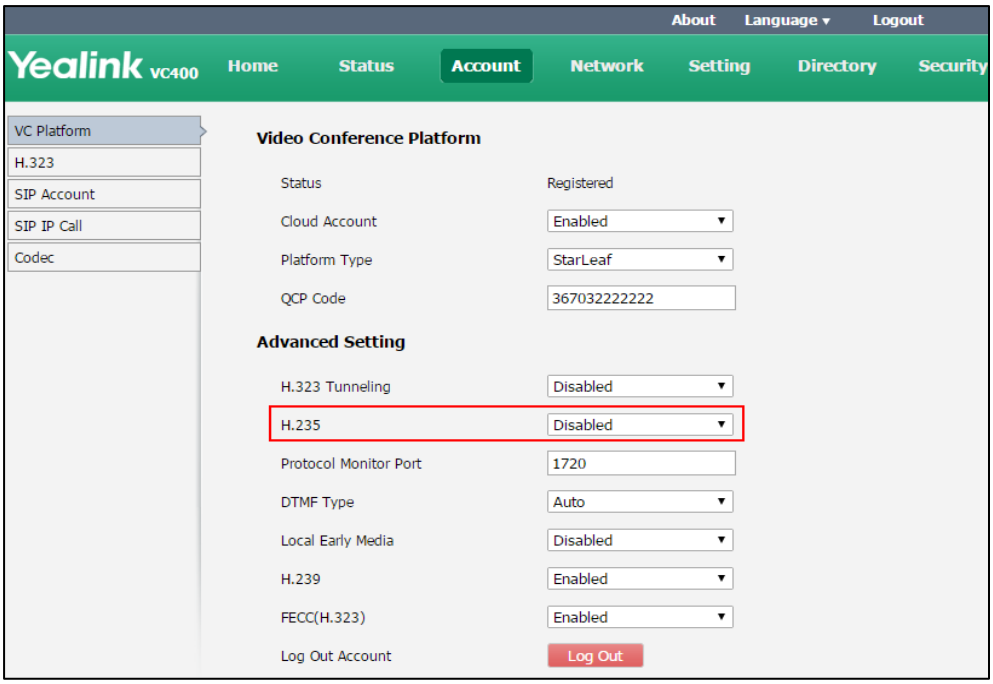
Far / Near	Compulsory	Optional	Disabled
Compulsory	H.235 Call	H.235 Call	Fail to establish call
Optional	H.235 Call	H.235 Call	RTP Call
Disabled	Fail to establish a call	RTP Call	RTP Call

When H.235 is enabled on both systems, calls will be encrypted, and the lock icon appears on the display device of each system during a call.

To configure H.235 for StarLeaf Cloud platform via web user interface:

1. Click on **Account->VC Platform**.
2. Select **StarLeaf** from the pull-down list of **Platform Type**.

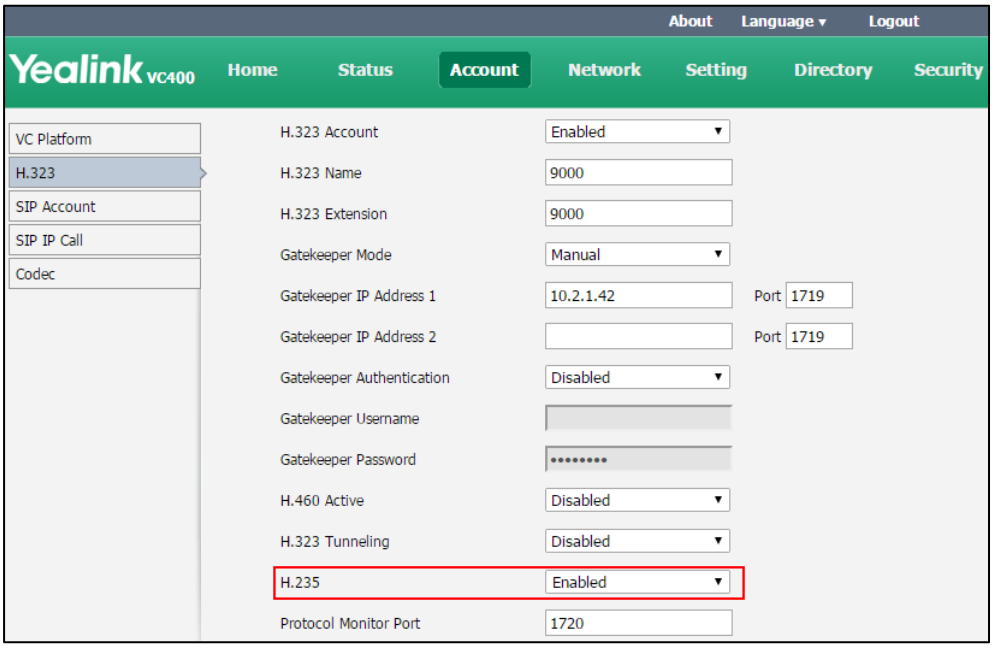
3. Select the desired value from the pull-down list of **H.235**.



4. Click **Confirm** to accept the change.

To configure H.235 for H.323 via web user interface:

1. Click on **Account**->**H.323**.
2. Select the desired value from the pull-down list of **H.235**.



3. Click **Confirm** to accept the change.

Defending against Attacks

VCS sometimes receives calls from unknown caller, and the calls may be unable to answer. To ensure the communications security of the VCS, you can configure abnormal call answering feature for handling abnormal SIP incoming calls. For incoming H.323 calls, you can configure Safe Mode Call feature.

Abnormal Call Answering

When destination address of the incoming SIP call does not match local address, the call is considered to be an abnormal call. You can reject the abnormal SIP incoming call, or answer it using IP address or SIP account randomly.

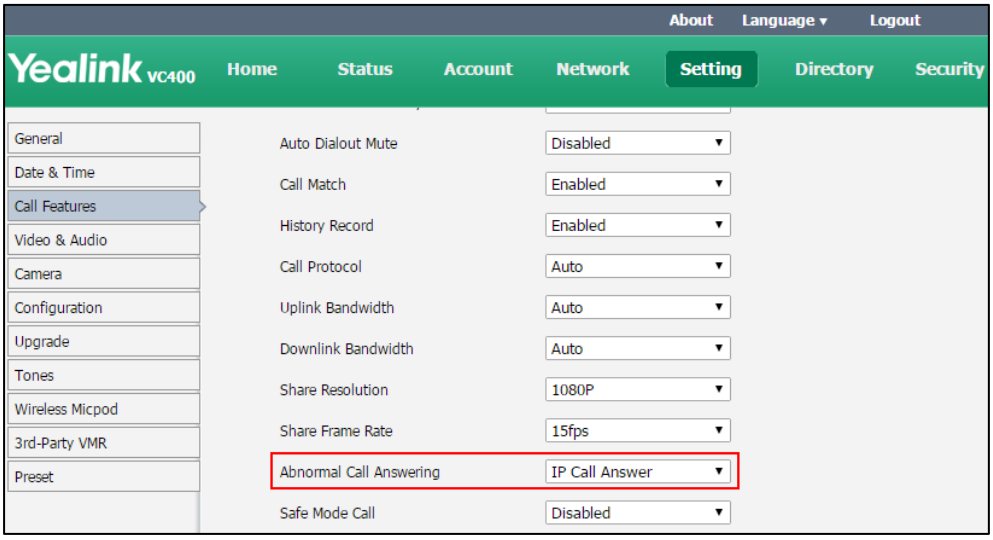
The abnormal call answering parameter on the system is described below:

Parameter	Description	Configuration Method
Abnormal Call Answering	Specifies the account type for answering abnormal SIP incoming calls. • **Disabled**–reject the abnormal SIP incoming calls. • **Account Answer**–use the SIP account to answer the abnormal SIP incoming calls. • **IP Call Answer—**use IP address to answer the abnormal SIP incoming calls. **Default:** IP Call Answer	Web User Interface

To configure abnormal call answering via web user interface:

1. Click on **Setting**->**Call Features.**

2. Select the desired value from the pull-down list of **Abnormal Call Answering**.



3. Click **Confirm** to accept the change.

Configuring Safe Mode Call

Safe Mode Call feature is used to verify whether the incoming H.323 call is coming from a video conferencing system.

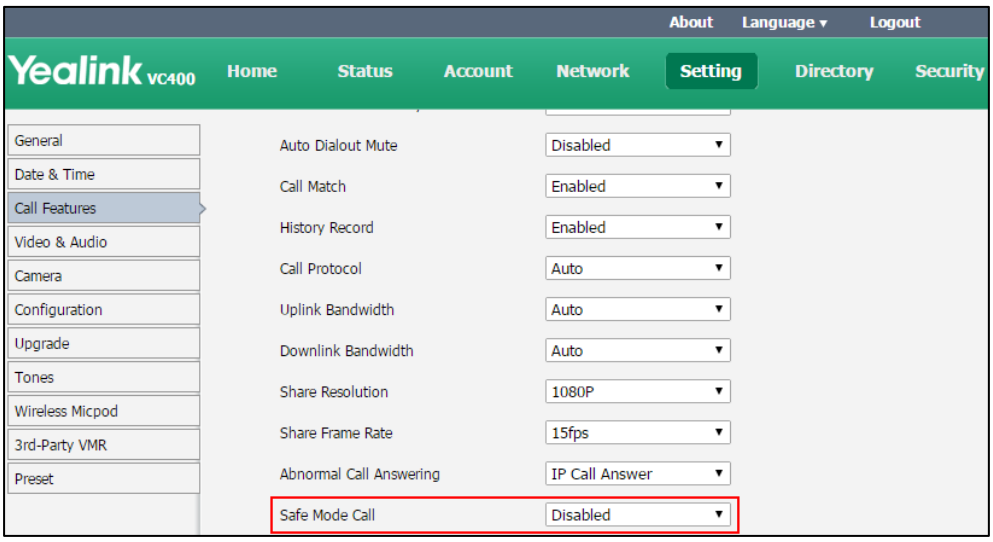
The Safe Mode Call parameter on the system is described below:

Parameter	Description	Configuration Method
Safe Mode Call	Enables or disables the Safe Mode Call feature • **Disabled**–Answer incoming H.323 calls directly without validation. • **Enabled—**Verify whether the incoming H.323 call is coming from a video conferencing system. If it is, the VC400&VC120 video conferencing system will answer it. If not, the incoming call will be rejected. **Default:** Enabled	Web User Interface

To configure Safe Mode Call via web user interface:

1. Click on **Setting**->**Call Features.**

2. Select the desired value from the pull-down list of **Safe Mode Call**.



3. Click **Confirm** to accept the change.

System Maintenance

This chapter provides basic system maintenance, including upgrading firmware, managing configurations, resetting systems and how to monitor network via SNMP. Topics include:

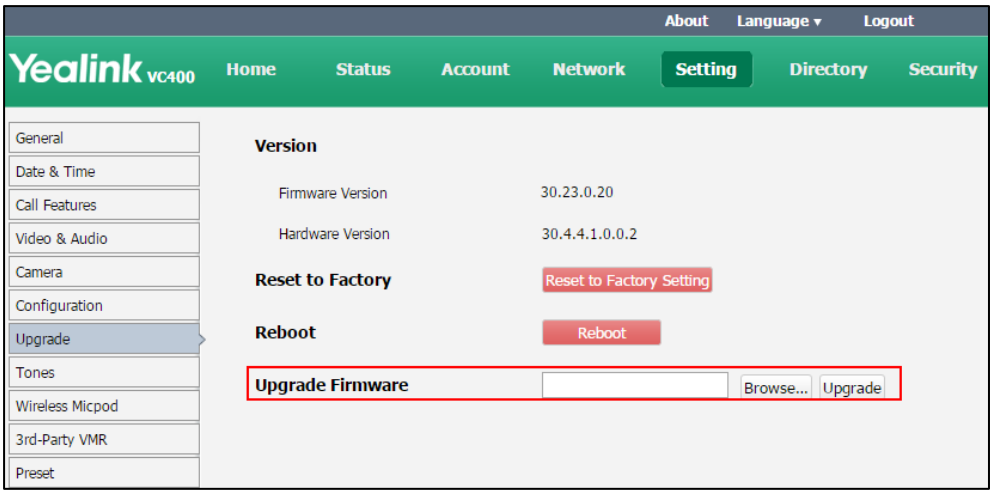
- Upgrading System Firmware
- Upgrading VCC20 Camera Firmware
- Importing/Exporting Configuration
- Resetting to Factory
- SNMP

Upgrading System Firmware

The newly released firmware version may add new features. Because of this, Yealink recommends you to update the latest firmware. You can upgrade the system firmware via web user interface. The firmware name of the VC400 video conferencing system is: 30.x.x.x.rom (x is the actual firmware version), the firmware name of the VC120 video conferencing system is: 40.x.x.x.rom (x is the actual firmware version). You can download the latest firmware version from the Yealink website.

To upgrade firmware via web user interface:

1. Click on **Setting**->**Upgrade**.
2. Click **Browse** to locate the firmware from your local system.



3. Click **Upgrade** to upgrade the firmware.

   The browser pops up the dialog box "Firmware of the video conference system will be updated. It will take 5 minutes to complete. Please don't power off!".

4. Click **Confirm** to confirm upgrading.

Note

Caution! Don't remove the Ethernet cable and power cord during the upgrade process. Don't close or refresh the web page when upgrading the firmware via web user interface.

Upgrading VCC20 Camera Firmware

Camera firmware is included in the system firmware. The VCC20 camera will upgrade automatically in one the following situations:

- The VCC20 camera has been connected to the VC120 Codec. When you upgrade the VC120 video conferencing system, the VCC20 camera will upgrade automatically.
- After you upgrade the VC120 video conferencing system, and then you connect the VCC20 camera to the VC120 Codec with the supplied DVI cable. The VCC20 will detect the new firmware, and upgrade automatically.

When the VCC20 is updating, the display device prompts "The camera is updating, do not plug out the camera, please waiting..."

Note

If you connect two VCC20 cameras to the VC120 Codec using the VC Dual-camera Box VCB20 (You should purchase it separately if necessary), the firmware of Camera 1 will be upgraded automatically by default. Only when you change video input resource to Camera 2, will the Camera 2 be upgraded.

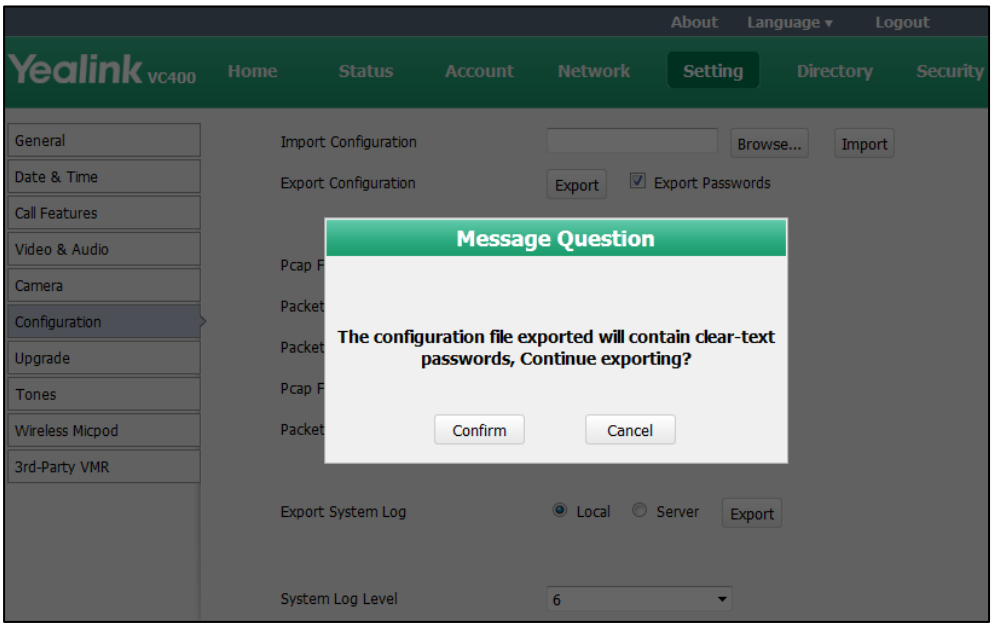
Importing/Exporting Configuration

We may need you to provide the system configurations for the Yealink field application engineers to help analyze problems. You can import configurations to your system to configure your system quickly. The file format of configuration file must be *.bin.

To export the system configurations via web user interface:

1. Click on **Setting**->**Configuration**.
2. Check or uncheck the **Export Passwords** checkbox according to actual demand.
3. Click **Export.**

If you check the **Export Passwords** checkbox, the web user interface is shown below:



4. Click **Confirm** to export the configurations.

To import the phone configurations via web user interface:

1. Click on **Setting**->**Configuration**.
2. Click **Browse** to locate a configuration file from your local system.
3. Click **Import** to import the configuration file.

Resetting to Factory

Reset the system to factory configurations after you have tried all appropriate troubleshooting suggestions but still have not solved your problems.

When factory resetting the video system, the following happens:

- The call logs will be deleted.
- Passwords will be reset to default.
- All system parameters will be reset to default values.
- All custom files will be deleted. Such as, certificates, local contacts and registered accounts.

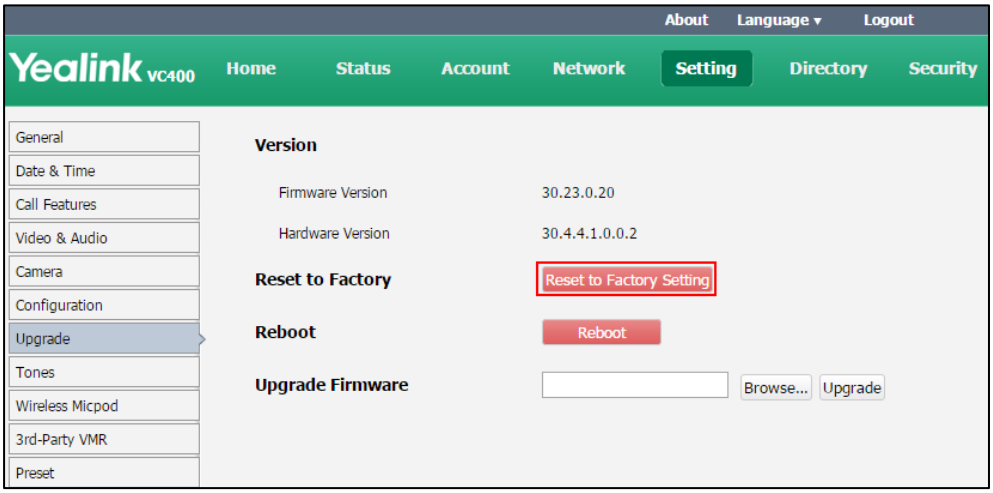
It is not possible to undo a factory reset. But you can export the configuration first, and then you can re-import the configuration to recovery the system after the reset.

You can reset the system via the reset key on the VC400/VC120 Codec, remote control or web user interface.

Note Reset of the system may take a few minutes. Do not power off until the phone starts up successfully.

To reset the system via web user interface:

1. Click on **Setting**->**Upgrade**.
2. Click **Reset to Factory Setting** in the **Reset to Factory** field.



The web user interface prompts the message "Reset the system?".

3. Click **Confirm** to confirm the resetting.

To reset the system via the remote control:

1. Select **Menu** ->**Advanced** (default password: 0000)->**Reboot & Reset**
2. Select **Reset**, and then press OK .

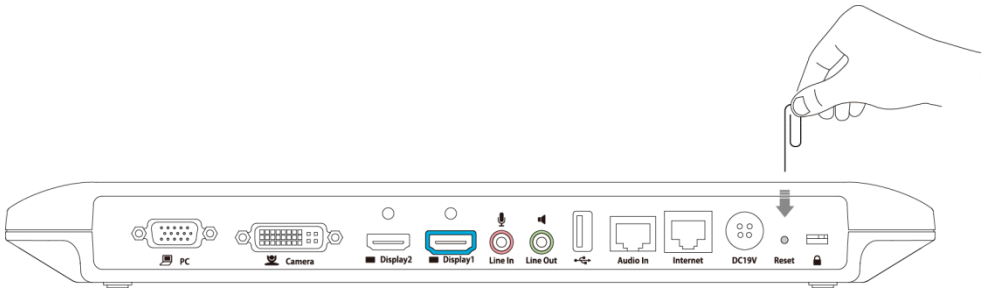
   The display device prompts "Reset to Factory?".
3. Select **OK**, and then press OK .

   The system reboots automatically. The system will reset to factory sucessfully after startup.

To reset the system via the rest key on the VC400/VC120 Codec:

Using tiny objects (for example, the paper clip) to press and hold the reset button for 15 seconds until the screen turns black.

Do not power off the system during the factory restore process. The system reverts to the default factory settings and restarts automatically. This will take a few minutes.



SNMP

SNMP (Simple Network Management Protocol) is an Internet-standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications. The variables accessible via SNMP are organized in hierarchies, which are described by Management Information Bases (MIBs).

Yealink systems support SNMPv1 and SNMPv2. They act as SNMP clients, receiving requests from the SNMP server. The SNMP server may send requests from any available source port to the configured port on the client, while the client responds to the source port on the SNMP server. Yealink systems only support the GET request from the SNMP server.

You can download SNMP application to monitor and manage information on a network entity.

The following table lists the basic object identifiers (OIDs) supported by the system.

MIB	OID	Description
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.1.0	The textual identification of the contact person for the system, together with the contact information. For example, Sysadmin (root@localhost)
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.2.0	An administratively-assigned name for the system. If the name is unknown, the value is a zero-length string. For example, Yealink VC400.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.3.0	The physical location of the system. For example, Server Room
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.4.0	The time (in milliseconds) since the network management portion of the system was last re-initialized.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.5.0	The firmware version of the system.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.6.0	The hardware version of the system.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.7.0	The system's model.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.8.0	The MAC address of the system.
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.9.	The IP address of the system.

MIB	OID	Description
	0	
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.10.0	The target version to which the current version is updated automatically. Format: MacVersion[*]ComVersion[*] For example, MacVersion[0.0.0.1]ComVersion[0.0.0.1]
YEALINK-MIB	1.3.6.1.2.1.37459.2.1.11.0	The command of the system reboot. Format: snmpset -v 2c XXXX public 37459.2.1.11.0 s reboot XXXX refers to the IP address of the system.

SNMP parameters on the system are described below:

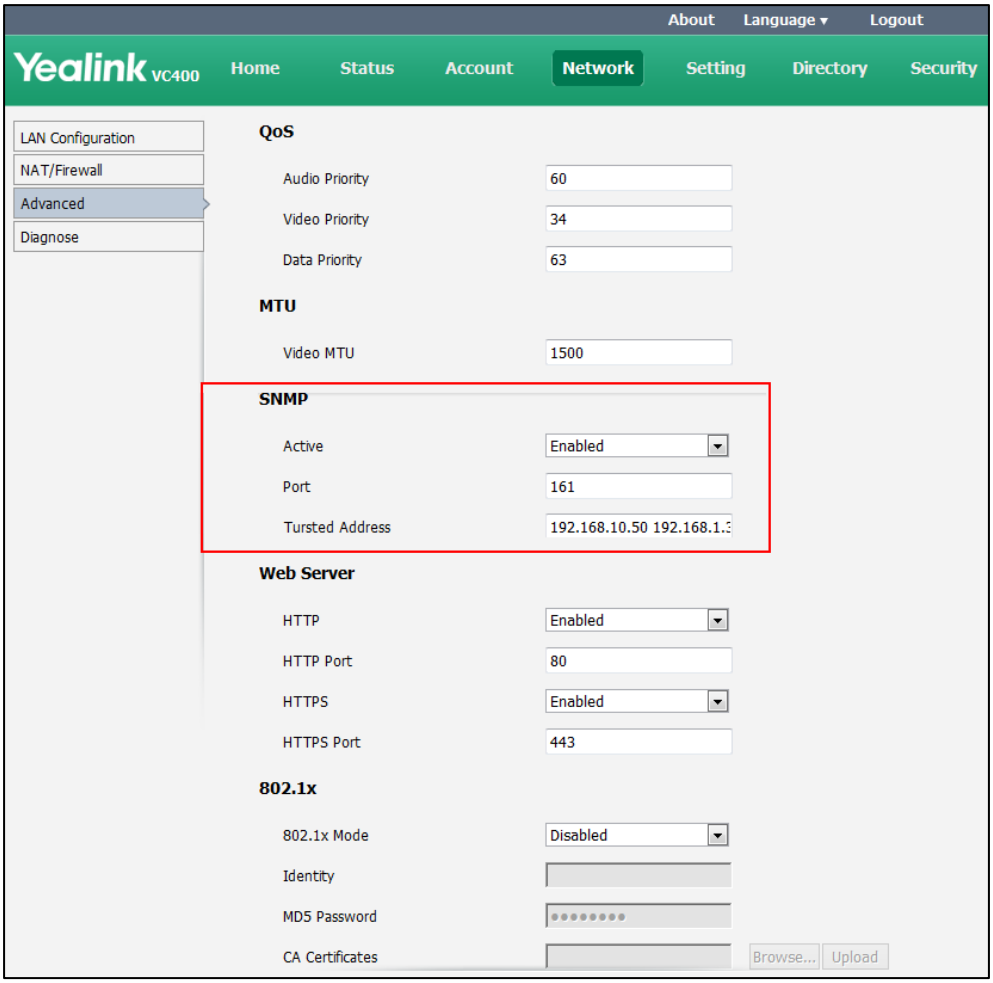
Parameter	Description	Configuration Method
SNMP->**Active**	Enables or disables SNMP feature on the system. **Default:** Disabled **Note:** If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Port	Specifies the SNMP port. **Valid Values:** 1-65535 **Default:** 161 **Note:** If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Trusted Address	Configures IP address(es) or domain name of the trusted SNMP server. Multiple IP addresses or domain names should be separated by spaces. **Note:** If it is left blank, the system accepts and handles GET requests from any SNMP server. If you change this parameter, the system will reboot to make the	Web User Interface

Parameter	Description	Configuration Method
	change take effect.	

To configure SNMP via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **SNMP** block, select **Enabled** from the pull-down list of **Active**.
3. Enter the SNMP port in the **Port** field.
4. Enter the IP address or domain name of the SNMP server in the **Trusted Address** field.

   Multiple IP addresses or domain names should be separated by spaces.



5. Click **Confirm** to accept the change.

   A dialog box pops up to prompt that the settings will take effect after a reboot.
6. Click **Confirm** to reboot the system immediately.

Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using the VC400/VC120 video conferencing system.

Troubleshooting Methods

The system can provide feedback in a variety of forms, such as log files, packets, status indicators and so on, which can help an administrator to find the system problem more easily and resolve it.

The following sections will help you to better understand and resolve the working status of the system.

- Viewing Log Files
- Capturing Packets
- Getting Information from Status Indicators
- Analyzing Configuration Files
- Viewing Call Statistics
- Using Diagnostic Methods

Viewing Log Files

The log files are Yealink specific debug files which may be requested by the Yealink support organization if you need technical support. The current log files are time stamped event log files. You can export the log files to a syslog server or the local system. The administrator can specify the location where the log will be exported to and the severity level of the log.

System Log Level specifies the log level to be recorded. The default system log level is 6.

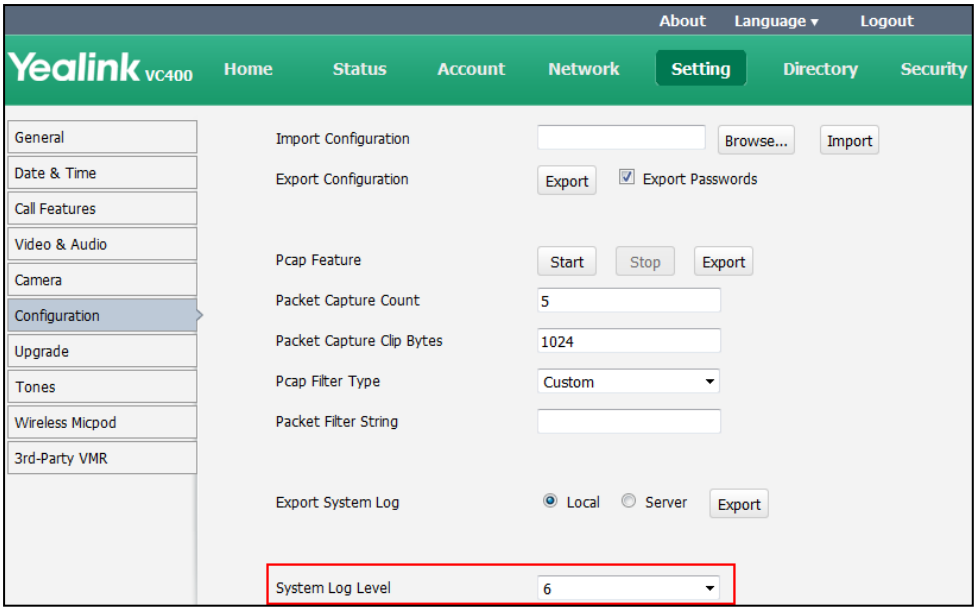
System log level parameters are described below:

Parameter	Description	Configuration Method
Export System Log	Specify where the system log will be exported. **Valid values:** • **Local**-export the system log to the local computer. • **Server-**export the system log	Web User Interface

Parameter	Description	Configuration Method
	to the specified server. **Default:** Local	
Server Name	Specify the server address where the log will be exported. **Note**: It only works if the parameter "Export System Log" is set to Server.	Web User Interface
System Log Level	Specify the system log level. **Note**: The supported level is 0-9. Higher value indicates more detailed content. **Default**: 6	Web User Interface

To configure the system log level via web user interface:

1. Click on **Setting**->**Configuration**.
2. Select the desired level from the pull-down list of **System Log Level**.

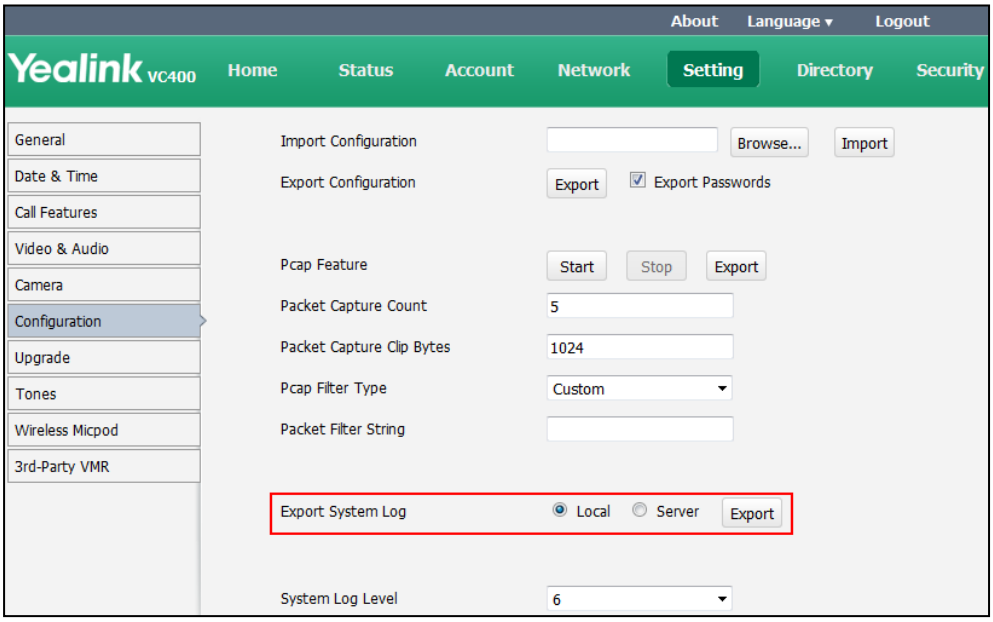


3. Click **Confirm** to accept the change.

To export a log file to the local system via web user interface:

1. Click on **Setting**->**Configuration**.

2. Mark the **Local** radio box In the **Export System Log** field.



3. Click **Export** to open the file download window, and then save the file to your local system.

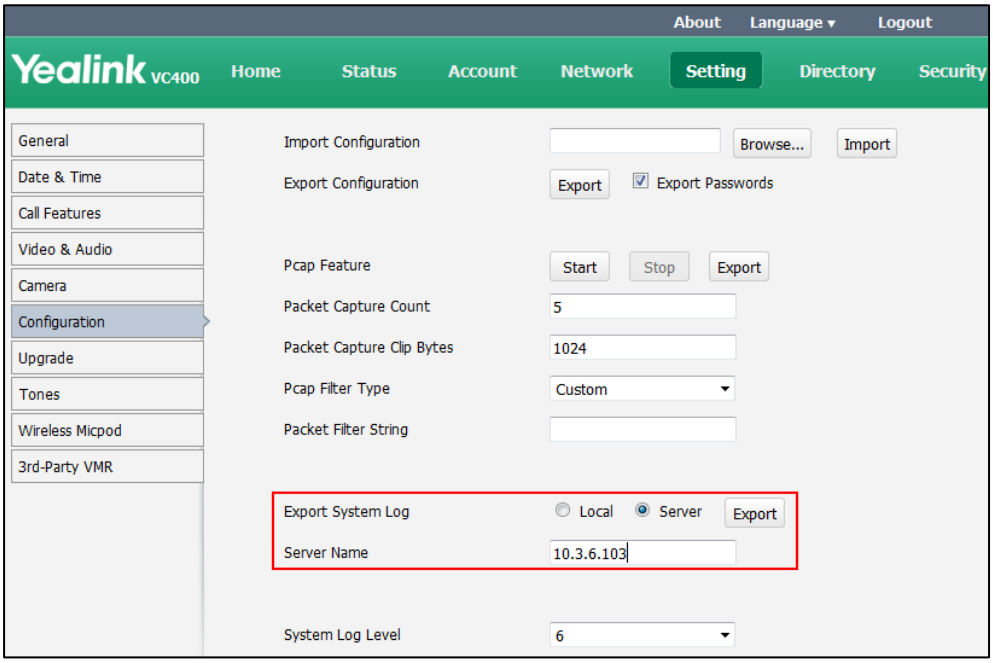
The following figure shows a portion of a log file:

```
  496 root       8876 SW  /yealink/bin/ggsvca_ipp
  497 root       8876 SW  /yealink/bin/ggsvca_ipp
  498 root       8876 SW  /yealink/bin/ggsvca_ipp
  499 root       8876 SW  /yealink/bin/ggsvca_ipp
  500 root       8876 SW  /yealink/bin/ggsvca_ipp
  501 root       8876 SW  /yealink/bin/ggsvca_ipp
  507 root      16424 SW  /yealink/bin/Screen.exe
  508 root      10344 SW  /yealink/bin/sipServer.exx
  509 root      10344 SW  /yealink/bin/sipServer.exx
  515 root      16424 SW  /yealink/bin/Screen.exe
  517 root      16424 SW  /yealink/bin/Screen.exe
  519 root      10344 SW  /yealink/bin/sipServer.exx
  521 root      16424 SW  /yealink/bin/Screen.exe
  522 root      16424 SW  /yealink/bin/Screen.exe
  523 root      16424 SW  /yealink/bin/Screen.exe
  524 root      10344 SW  /yealink/bin/sipServer.exx
  525 root            SW< [IRQ 45]
  526 root      10344 SW  /yealink/bin/sipServer.exx
  527 root      16424 SW  /yealink/bin/Screen.exe
  528 root      16424 SW  /yealink/bin/Screen.exe
  529 root      16424 SW  /yealink/bin/Screen.exe
 1147 root       1788 SWN sleep 1000
 1227 root      10120 SWN ConfigManApp.com
 1228 root       4624 SW  /yealink/bin/mini_httpd -p 80 -d /yealink/html -c cgi
 1229 root       2812 SWN sh -c cd /tmp;ifconfig >> Messages;ps >> Messages;tar
 1230 root       2812 RWN ps
Feb 29 06:01:09 mini_httpd[388]: mini_httpd.c(1510):child process 1227 exit!
Feb 29 06:01:12 mini_httpd[1232]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com,query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1232 exit!
Feb 29 06:01:12 mini_httpd[1233]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com,query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1233 exit!
Feb 29 06:01:12 mini_httpd[1234]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com,query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1234 exit!
```

To export a log file to a syslog server via web user interface:

1. Click on **Setting**->**Configuration**.
2. Mark the **Server** radio box in the **Export System Log** field.

3. Enter the IP address or domain name of the syslog server in the **Server Name** field.



A dialog box pops up to prompt that settings will take effect after a reboot.

4. Click **Confirm** to reboot the system immediately.

Capturing Packets

The administrator can capture packets in three ways: capturing the packets via web user interface, remote control or using the Ethernet software. Engineers can analyze the packets to troubleshoot problems.

Packets parameters are described below:

Parameter	Description	Configuration Method
Pcap Feature	Start and stop capturing packets or export the captured packets.	Web User Interface
Packet Capture Count	Configures the count of the number of packets to capture. **Default:** 5	Web User Interface
Packet Capture Clip Bytes	Configures the maximum size (in KB) of every packet to capture. **Default:** 1024	Web User Interface
Pcap Filter Type	Configures the filter type of the packet to capture. **Valid Values:** • **Custom**–Customize the packet	Web User Interface

Parameter	Description	Configuration Method
	filter string. • **SIP or H245 or H225**−Capture SIP, H245 and H225 packets. It depends on the supportive protocol of the system. • **RTP**−Capture RTP packets. **Default:** Custom	
Packet Filter String	Customizes the packet filter string. **Syntax:** Protocol+Direction+Host(s)+ Value +Logical Operations+Other Expression **Protocol**: Values: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp. Application-level protocol, such as http, dns and sip are not supported. If no protocol is specified, all the protocols are used. **Direction**: Values: src, dst, src and dst, src or dst If no source or destination is specified, the "src or dst" keywords are applied. For example: "host 10.2.2.2" is equivalent to "src or dst host 10.2.2.2". **Host(s)**: Values: net, port, host, portrange. If no host(s) is specified, the "host" keyword is used. For example: "src 10.1.1.1" is equivalent to "src host 10.1.1.1". **Logical Operations**: Values: not, and, or. Negation ("not") has highest precedence. Alternation ("or") and concatenation ("and") have equal precedence and associate left to right. For example: "not tcp port 3128 and tcp port 23" is	Web User Interface

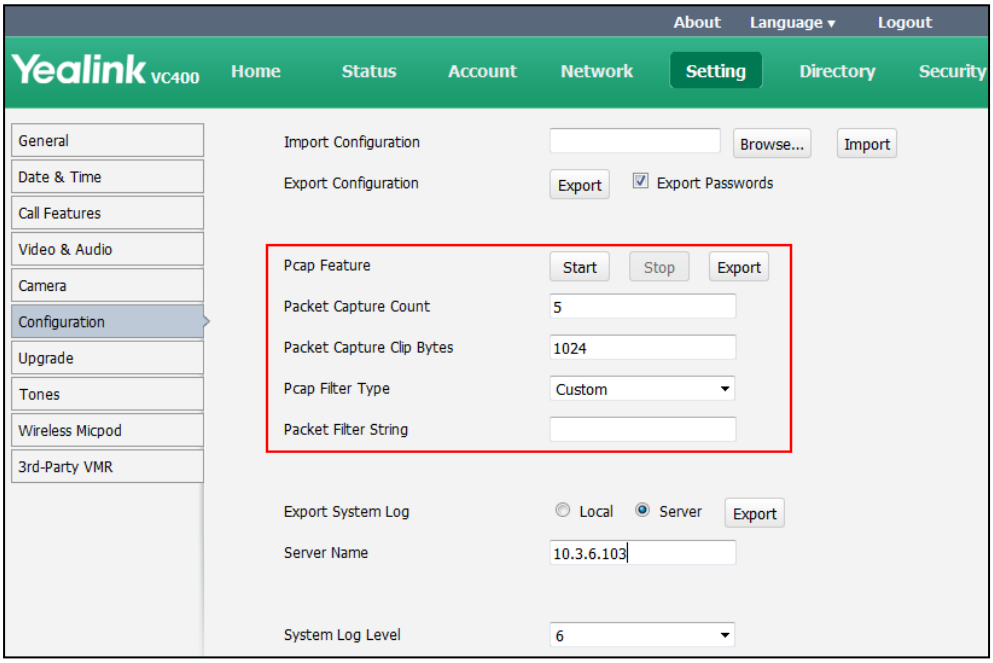
Parameter	Description	Configuration Method
	equivalent to "(not tcp port 3128) and tcp port 23". "not tcp port 3128 and tcp port 23" is NOT equivalent to "not (tcp port 3128 and tcp port 23)". **Example**: (src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst port range 200-10000 and dst net 10.0.0.0/8 Displays packets with source IP address 10.4.1.12 or source network 10.6.0.0/16, the result is then concatenated with packets having destination TCP port range from 200 to 10000 and destination IP network 10.0.0.0/8. **Default**: Blank **Note**: It only works if the parameter "Pcap Filter Type" is set to Custom.	

To capture packets via web user interface:

1. Click on **Setting**->**Configuration**.
2. Enter the desired value in the **Packet Capture Count** field.
3. Enter the desired value in the **Packet Capture Clip Bytes** field.
4. Select the desired value from the pull-down list of **Pcap Filter Type**.

   If **Custom** is selected, enter the desired packet filter string in the **Packet Filter String** field.
5. Click **Start** to start capturing signal traffic.
6. Reproduce the issue to get stack traces.
7. Click **Stop** to stop capturing.

8. Click **Export** to open the file download window, and then save the file to your local system.



To capture packets via the remote control:

Before capturing packets, you need to insert a USB flash drive to the USB port on the VC400/VC120 Codec to store packets. Make sure the USB feature is enabled.

1. Long press ⌫ when the system is idle or during a call.

   The display device prompts "Onekey-capture is running, press the Backspace key for 2s to turn off it".

2. Long press ⌫ for 2 seconds to stop capturing packets.

   The packets are saved in the yealink.debug folder on your USB flash driver.

To capture packets using the Ethernet software:

Connect the Internet ports of the system and the PC to the same hub, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic. You can also set mirror port on a switch to monitor the port connected to the system.

Getting Information from Status Indicators

In some instances, status indicators are helpful for finding system troubles. Status indicators may consist of the power LED, icons on the status bar of the display device or prompt messages.

The following shows two examples of obtaining the system information from status indicators:

- If a LINK failure of the system is detected, the icon will appear on the status bar of the display device, indicating the current network is not available.
- If the power LED does not light, it indicates the system is not powered on.

For more information on the icons, refer to Icon Instructions on page 25.

Analyzing Configuration Files

Wrong configurations may have an impact on your system use. You can export configuration file to check the current configuration of the system and troubleshoot if necessary. For more information on how to export system configuration, refer to Importing/Exporting Configuration on page 270.

Viewing Call Statistics

You can enter the view call statistics screen during an active call. Information includes:

- **Total Bandwidth:** Uplink Bandwidth and Downlink Bandwidth.
- **Video**: Resolution, Codec, Bandwidth, Frame Rate, Jitter, Total Packet Lost, Packet Lost(%)
- Protocol used during a call.
- Device information of the far site.
- **Audio:** Codec, Bandwidth, Sample Rate, Jitter, Total Packet Lost, Packet Lost(%)
- **Share:** Resolution, Codec, Bandwidth, Frame Rate.

Use the remote control to select **More**->**Call Statistics** during an active call to view call statistics.

Using Diagnostic Methods

The system supports the following diagnostic methods:

- **Audio Diagnose**: Check whether the audio input device and audio output device are working properly.
- **Camera Diagnose**: Check whether the camera can pan and change focus normally.
- **Ping**: Check whether the system can establish contact with the IP address that you specify.
- **Trace Route**: Display the route (path) and measure transit delays of packets across an Internet Protocol (IP) network.

Above diagnostic methods can be configured using remote control. Ping and Trance Route can also be configured via web user interface.

To diagnose audio via the remote control:

1. Select **Menu**->**Diagnose** menu.
2. Select **Audio Diagnose**, and then press OK.
3. Speak into the microphone.
4. Check whether the microphone can pick up audio and play back the audio properly.

   If the system plays back the audio normally, it means that audio works well.

5. Press OK to stop audio diagnostics.

To diagnose the camera via the remote control:

1. Select **Menu**->**Diagnose** menu.
2. Select **Camera Diagnose**, and then press OK .
3. Press navigation keys to adjust the camera position.
4. Press or to adjust the focus.

   If the camera can move and zoom normally, it means that the camera works properly.
5. Press the **Back** soft key to stop camera diagnose.

To diagnose network via the remote control:

1. Select **Menu**->**Diagnose**->**Ping**.
2. Select **Start**, and then press OK .
3. The system will Ping **yealinkvc.com** address by default. This will check whether the system can establish contact with the public IP address.
4. You can also enter any IP address (for example, the IP address of the remote system) in the **Ping** field.

   It measures the round-trip time from transmission to reception and reports errors and packet loss. The results of the test include a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times.
5. Press the **Back** soft key to return to the Diagnose menu.

Trace Route:

1. Select **Menu**->**Diagnose**->**Trace Route**.
2. Select **Start**, and then press OK .
3. The system will trace **8.8.8.8** address by default.
4. You can also enter any IP address (for example, the IP address of the remote system) in the **Trace Route** field.

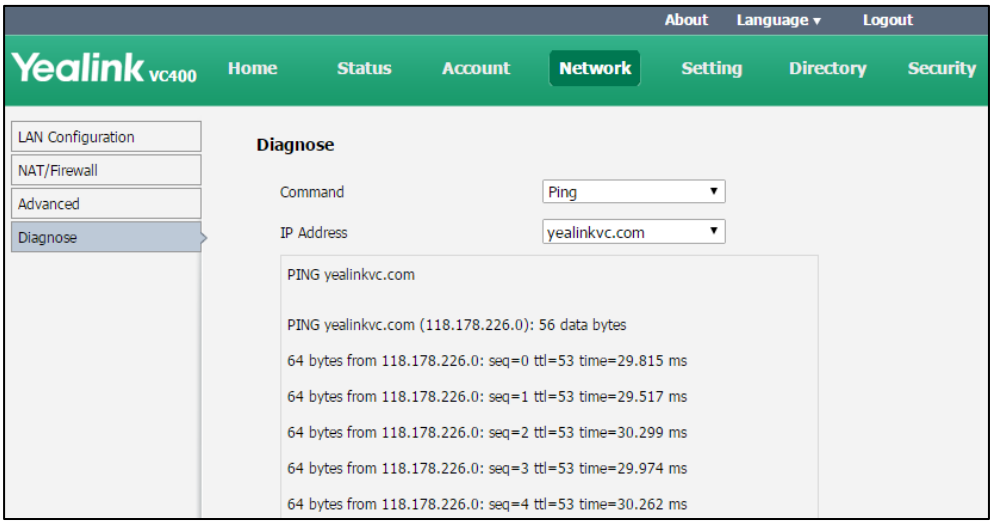
   If the test is successful, the VC400/VC120 system lists the hops between the system and the IP address you entered. You can check whether congestion happens via the time cost between hops.
5. Press the **Back** soft key to return to the Diagnose menu.

To diagnose network via web user interface:

1. Click on **Network** ->**Diagnose**.
2. Select the desired diagnostic method from the pull-down list of **Command**.
3. Click **Start** to start diagnosing.

   You can also enter any IP address in the **IP Address** field.

The web page displays the diagnosis:



4. Click **Stop** to complete diagnosing.

   You can click **Copy** to copy the content to the clipboard.

Troubleshooting Solutions

This chapter provides general troubleshooting solutions to help you solve the problems you might encounter when using your system.

Ensure the system has not been physically damaged when experiencing a problem. Check whether the cables are loose and the connections are correct and secure. These are common causes of problems.

If problems you encounter are not mentioned in this chapter, you can contact your distributor or Yealink FAE.

General Issues

Why is the display device black?

- Check whether the display device is connected properly to the VC400/VC120 Codec.
- Check whether the system is in sleep mode. Press any key on the video conferencing phone or remote control to resume system operation.
- Check whether the display device is in sleep mode or is turned off. Press the power button on the remote control or on the display device.
- Check whether you have selected the correct video input source. You can try to switch video input source.

Why doesn't the display device display time and date correctly?

- If you have configured the system to obtain the time and date from the NTP server automatically, ensure that SNTP server and time zone are configured correctly in the system and whether the connection between the system and NTP server is working properly.
- If you have configured the system to obtain the time and date manually, ensure that you have configured the time and date correctly.

Why doesn't the remote control work?

- Check whether the system is powered on.
- Check whether the positive and negative charges of the battery are connected correctly.
- Check whether the battery has sufficient power left.
- Check whether no special fluorescent or neon signs nearby.

Why does the system fail to call the far site?

- Check whether the network of the local site is available.
- Check whether the network of the far site is available.
- Check whether the far site enables the DND feature.
- Check whether the accounts have been registered correctly, and the system uses the appropriate account to call the far site.
- Ensure that the number you are calling is correct.
- Check whether the far site rejects your call.
- Check whether the firewall blocks the inbound traffics from the other site.
- Check whether the far site has already up to maximum call-in limitation.
- If the local site is forced to use encryption, ensure that the far site enables encryption too. For more information on call encryption, refer to Secure Real-Time Transport Protocol on page 259 and H.235 on page 263.
- Ensure the far site supports the same call protocol as the local site.

Why does the system fail to call the far site via IP address?

- Ensure that at least one call protocol is enabled on both sites. For more information, refer to Configuring SIP Settings on page 126 and Configuring H.323 Settings on page 130.
- Ensure that the network is connected correctly.
- Ensure that the network is configured correctly. For more information, refer to Configuring LAN Properties on page 48.
- Ping the IP address of the far site. Contact your system administrator if it fails. For more information, refer to Using Diagnostic Methods on page 284.

Why doesn't the status bar of the display device display IP address?

- Check whether the network is available.
- Check whether the LAN property is configured correctly. For more information on LAN property configuration, refer to Configuring LAN Properties on page 48.
- Check whether the system has enabled the hide IP address feature. For more information on disabling the hide IP address feature, refer to Hiding IP Address on page 177.
- Check whether the system has configured firewall and NAT correctly. For more information on, refer to Configuring the System for Use with a Firewall or NAT on page 77.

Why does the network keep losing packets?

- Check whether the network is available and the LED indicator on the left of the Internet port illuminates green.
- Try to use the low speed connection to check whether packets are lost. Deficient bandwidth is an important reason for packet loss.
- Check the configuration of the network speed and duplex mode on the system, switch and router.

Camera Issues

Why can't I adjust the camera angle and focus?

- You can adjust the camera when the system is idle or during a call. The camera cannot be adjusted when the system is in the menu screen.
- Ensure that the batteries in the remote control are in good working condition, and installed correctly.
- Aim the remote control at the sensor when operating the unit.
- Ensure that no objects are obstructing the sensor on the front of the camera.
- Ensure that the LED on the front of the camera flashes green when you use the remote control to operate the unit.
- Ensure that what you are controlling is the local camera.
- Reboot the system.
- If the above suggestions cannot solve your problem, perhaps the remote control is broken. You can contact your system administrator for help.

Why can't adjust the remote camera during an active call?

- Use the remote control to control the local camera to check whether the remote control can be used normally.
- Ensure that the far site has enabled the Far Control Near Camera feature. For more

information, refer to Far-end Camera Control on page 211.

- Ensure that what you are controlling is the remote camera. Select **More**->**Near/Far Camera** during an active call and then select the remote video image.
- Ensure the far site supports the same call protocol as the local site. For more information, refer to Camera Control Protocol on page 212.

Why is the video quality bad?

- Ensure that the display device has suitable resolution.
- Check whether the packet has been lost. For more information on packet loss, refer to Viewing Call Statistics on page 284.
- Ensure that camera settings are configured correctly, such as brightness and white balance.
- Avoid high-intensity indoor light or direct sunlight on the camera.

Video & Audio Issues

Why can't I hear the audio during a call?

- Ensure that the local audio output device is connected correctly.
- Use audio diagnose to check whether the audio device is working normally.
- Ensure that the ringer volume is not set to the minimum.
- Check whether the far site is muted.

Why can't the far site hear the local audio?

- Ensure that the local audio input device is connected correctly.
- Check whether the local site is muted.
- Check whether the system has enabled the auto answer mute feature.
- Check whether the system has enabled the auto dialout mute feature.

Why can't I hear the other site clearly during a call?

- Ensure that the speaker volume of the far site is not set too low.
- Muffled audio reception from the far side may be caused by highly reverberant rooms. Speak in close proximity to the phone.
- Adjust the priority order for your audio codec if you have chosen a low-bandwidth audio codec to be first. For more information, refer to Audio Codecs on page 143.
- For best results, ensure that the caller is using a Yealink video conferencing system. Audio quality from your video conferencing system will vary when calling a non-Yealink system.
- Dust and debris may cause audio quality. . Do not use any kind of liquid or aerosol cleaner on the phone. A soft, slightly damp cloth should be sufficient to clean the top surface of

the phone if necessary.

Why is the voice quality poor?

Users may receive poor voice quality during a call, such as intermittent voice, low volume, echo or other noise. It is difficulty to diagnosis the root causes of the voice anomalies. The possible reasons are:

- Users sit too far from or near to the microphone.
- The audio pickup device is moved frequently.
- Intermittent voice is probably caused by voice packet loss or jitter. Voice packet loss may occur due to network congestion. Jitter may occur due to information reorganization of the transmission or receiving equipment, such as, delay processing, retransmission mechanism or buffer overflow.
- Noise devices, such as computers or fans, may make it difficult to hear each other's voices clearly.
- Wires may also cause this problem. Replace the old with the new cables, and then reconnect to check whether the new cables provide better connectivity.

Why can't I view the local video image?

- Check whether the local site camera is connected to the VC400/VC120 Codec correctly.
- Check whether camera is powered on, and the LED indicator illuminates green.
- Check whether the camera is selected for the current video input source.
- Check the screen layout to see whether the remote video image is shown in full size.

Why can't I view the menu?

- Check whether the Display1 port of VC400/VC120 Codec is connected to the HDMI port on the display device.

Why can't I start a presentation?

- Check whether a PC is connected to the VC400/VC120 Codec.
- Check whether the PC is sending a signal.
- Check the call statistics to see whether the system is sharing content.
- Ensure that dual-stream is configured correctly. For more information, refer to Dual-Stream Protocol on page 196.

Why does the far-site display black screen when local starts a presentation?

This situation may due to the difference between Signaling Server address and the Media Server address.

The actual address is different from the negotiated address, so that start a presentation in this situation will result in the failure of sending packets to the correct address. You can disable the network adaptive feature, so that the system will send packets to the negotiated address other than the actual address.

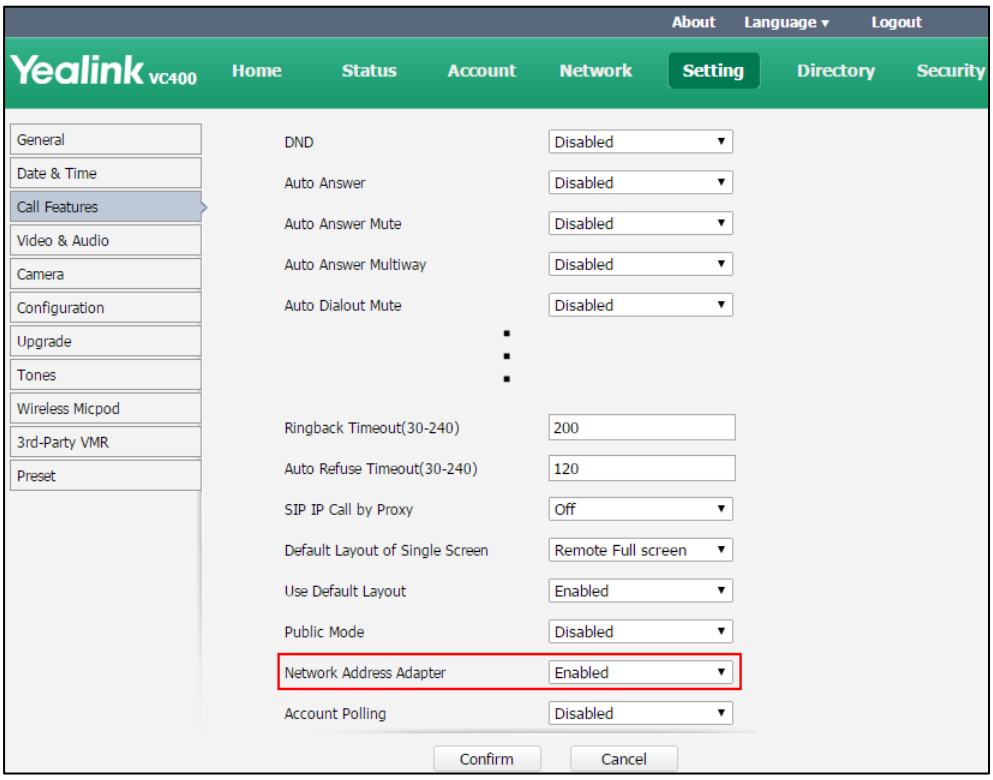
Network address adapter parameter is described below:

Parameter	Description	Configuration Method
Network Address Adapter	Enable or disable the network address adapter feature. **Valid values:** • **Enabled**-send packets to the actual address. • **Disabled-** send packets to the negotiated address other than the actual address. **Default:** Enabled	Web User Interface

To configure the network address adapter via web user interface:

1. Click on **Setting**->**Call Features**.

2. Select the desired level from the pull-down list of **Network Address Adapter**.



3. Click **Confirm** to accept the change.

System Maintenance

How to prevent monitor burn-in?

Refer to your monitor's documentation for specific recommendations and instructions. The following guidelines help prevent image burn-in:

- Ensure that static images are not displayed for long periods.
- Be aware that meetings that last more than an hour without much movement can have the same effect as a static image.
- Configure the automatic sleep time to be 1 hours or less.
- Consider decreasing the monitor's sharpness, brightness, and contrast settings if they are set to their maximum values.

How to reboot the system?

When you do one of the following, the system will reboot:

- Reboot system
- Reset system
- Upgrade firmware

- Configure some features need to take effect after a reboot

You can reboot the system in the following ways:

- Long press the power button on the VC400/VC120 Codec.
- Select **Menu**->**Advanced** (default password: 0000) ->**Reboot & Reset**->**Reboot**, and then press OK .
- Login web user interface and click on **Setting**->**Upgrade**->**Reboot,** and then click **Confirm**.

To avoid corrupting the system, you should not unplug the power adapter from the system to power off the system.

Why does the system fail to upgrade?

- Ensure that the firmware is different from the firmware currently in use.
- Ensure that the downloaded firmware applies to the system.
- Ensure that the system is powered on normally, and the network is available during the upgrade process.
- When upgrading firmware via web user interface, ensure that the web user interface is not refreshed or closed during the upgrade process.

Appendix

Appendix A: Time Zones

Time Zone	Time Zone Name
−11:00	Samoa
−10:00	United States-Hawaii-Aleutian
−10:00	United States-Alaska-Aleutian
−09:30	French Polynesia
−09:00	United States-Alaska Time
−08:00	Canada(Vancouver, Whitehorse)
−08:00	Mexico(Tijuana, Mexicali)
−08:00	United States-Pacific Time
−07:00	Canada(Edmonton, Calgary)
−07:00	Mexico(Mazatlan, Chihuahua)
−07:00	United States-Mountain Time
−07:00	United States-MST no DST
−06:00	Canada-Manitoba(Winnipeg)
−06:00	Chile(Easter Islands)
−06:00	Mexico(Mexico City, Acapulco)
−06:00	United States-Central Time
−05:00	Bahamas(Nassau)
−05:00	Canada(Montreal, Ottawa, Quebec)
−05:00	Cuba(Havana)
−05:00	United States-Eastern Time
−04:30	Venezuela(Caracas)
−04:00	Canada(Halifax, Saint John)
−04:00	Chile(Santiago)
−04:00	Paraguay(Asuncion)
−04:00	United Kingdom-Bermuda(Bermuda)
−04:00	United Kingdom(Falkland Islands)
−04:00	Trinidad&Tobago
−03:30	Canada-New Foundland(St.Johns)
−03:00	Denmark-Greenland(Nuuk)
−03:00	Argentina(Buenos Aires)
−03:00	Brazil(no DST)
−03:00	Brazil(DST)
−02:30	Newfoundland and Labrador
−02:00	Brazil(no DST)
−01:00	Portugal(Azores)

Time Zone	Time Zone Name
0	GMT
0	Greenland
0	Denmark-Faroe Islands(Torshavn)
0	Ireland(Dublin)
0	Portugal(Lisboa, Porto, Funchal)
0	Spain-Canary Islands(Las Palmas)
0	United Kingdom(London)
0	Morocco
+01:00	Albania(Tirane)
+01:00	Austria(Vienna)
+01:00	Belgium(Brussels)
+01:00	Caicos
+01:00	Chad
+01:00	Spain(Madrid)
+01:00	Croatia(Zagreb)
+01:00	Czech Republic(Prague)
+01:00	Denmark(Kopenhagen)
+01:00	France(Paris)
+01:00	Germany(Berlin)
+01:00	Hungary(Budapest)
+01:00	Italy(Rome)
+01:00	Luxembourg(Luxembourg)
+01:00	Macedonia(Skopje)
+01:00	Netherlands(Amsterdam)
+01:00	Namibia(Windhoek)
+01:00	Poland (Warsaw)
+02:00	Estonia(Tallinn)
+02:00	Finland(Helsinki)
+02:00	Gaza Strip(Gaza)
+02:00	Greece(Athens)
+02:00	Israel(Tel Aviv)
+02:00	Jordan(Amman)
+02:00	Latvia(Riga)
+02:00	Lebanon(Beirut)
+02:00	Moldova(Kishinev)
+02:00	Russia(Kaliningrad)
+02:00	Romania(Bucharest)
+02:00	Syria(Damascus)
+02:00	Turkey(Ankara)
+02:00	Ukraine(Kyiv, Odessa)
+03:00	East Africa Time

Time Zone	Time Zone Name
+03:00	Iraq(Baghdad)
+03:00	Russia(Moscow)
+03:30	Iran(Teheran)
+04:00	Armenia(Yerevan)
+04:00	Azerbaijan(Baku)
+04:00	Georgia(Tbilisi)
+04:00	Kazakhstan(Aktau)
+04:00	Russia(Samara)
+04:30	Afghanistan(Kabul)
+05:00	Kazakhstan(Aqtobe)
+05:00	Kyrgyzstan(Bishkek)
+05:00	Pakistan(Islamabad)
+05:00	Russia(Chelyabinsk)
+05:30	India(Calcutta)
+05:45	Nepal(Katmandu)
+06:00	Kazakhstan(Astana, Almaty)
+06:00	Russia(Novosibirsk, Omsk)
+06:30	Myanmar(Naypyitaw)
+07:00	Russia(Krasnoyarsk)
+07:00	Thailand(Bangkok)
+08:00	China(Beijing)
+08:00	Singapore(Singapore)
+08:00	Australia(Perth)
+08:00	Russia(Irkutsk, Ulan-Ude)
+08:45	Eucla
+09:00	Korea(Seoul)
+09:00	Japan(Tokyo)
+09:00	Russia(Yakutsk, Chita)
+09:30	Australia(Adelaide)
+09:30	Australia(Darwin)
+10:00	Australia(Sydney, Melbourne, Canberra)
+10:00	Australia(Brisbane)
+10:00	Australia(Hobart)
+10:00	Russia(Vladivostok)
+10:30	Australia(Lord Howe Islands)
+11:00	New Caledonia(Noumea)
+11:00	Russia(Srednekolymsk Time)
+11:30	Norfolk Island
+12:00	New Zealand(Wellington, Auckland)
+12:00	Russia(Kamchatka Time)
+12:45	New Zealand(Chatham Islands)

Time Zone	Time Zone Name
+13:00	Tonga(Nukualofa)
+13:30	Chatham Islands
+14:00	Kiribati

Appendix B: Trusted Certificates

Yealink video conferencing system trusts the following CAs by default:

- Symantec Class 3 Secure Server CA
- Class 1 Public Primary Certification Authority
- Deutsche Telekom AG Root CA 2
- VeriSign Class 1 Public Primary Certification Authority - G5
- VeriSign Class 3 Public Primary Certification Authority - G4
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 1 Public Primary Certification Authority - G3
- GeoTrust Primary Certification Authority - G2
- Yealink.com
- Yealinkvc.com
- Class 3 Public Primary Certification Authority - G2
- Equifax Secure Global eBusiness CA-1
- DigiCert High Assurance EV Root CA
- VeriSign Universal Root Certification Authority
- Equifax Secure Certificate Authority
- Thawte Primary Root CA
- Thawte Personal Freemail CA
- Class 3 Public Primary Certification Authority
- GeoTrust Global CA
- Quickconnect.starleaf.com
- GeoTrust Primary Certification Authority
- GeoTrust Universal CA 2
- GeoTrust Global CA 2
- thawte Primary Root CA - G3
- thawte Primary Root CA - G2
- Class 1 Public Primary Certification Authority - G2
- Thawte Premium Server CA
- VeriSign Class 4 Public Primary Certification Authority - G3
- StarLeaf CA

- VeriSign Class 2 Public Primary Certification Authority - G3
- Thawte Server CA
- Equifax Secure eBusiness CA-1
- GeoTrust Inc.
- Class 2 Public Primary Certification Authority - G2
- Class 4 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G5

Note Yealink endeavors to maintain a built-in list of most common used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, you can send a request to your local distributor. At this point, you can upload your particular CA certificate into your phone. For more information on uploading custom CA certificate, refer to Transport Layer Security on page 251.

Index

Numeric

802.1x Authentication 68

A

Abnormal Call Answering 265
About This Guide v
Adjusting MTU of Video Packets 194
Administrator Password 248
Analyzing Configuration Files 284
Appendix A: Time Zones 295
Appendix B: Trusted Certificates 298
Audio Input Device 191
Audio Output Device 189
Auto Answer 151
Auto Dialout Mute 152
Automatic Sleep Time 176
Auto Refuse Timeout 159

B

Backlight of the Video Conferencing Phone 168
Bandwidth 155

C

Call History 237
Call Match 153
Call Protocol 146
Camera Control Protocol 212
Camera Issues 288
Codecs 143
Configuring Call Preferences 99
Configuring Camera Settings 201
Configuring Video Conference Platform 99
Configuring H.323 Setting 130
Configuring LAN Properties 48
Configuring Network 47
Configuring Network Settings Manually 52
Configuring Network Speed and Duplex Mode 60
Configuring Packets 280
Configuring Safe Mode Call 266
Configuring SIP Settings 126
Configuring System Settings 165
Configuring the System for Use with a Firewall or NAT 77
Configuring the Third-party Virtual Meeting Room 122

D

Date and Time 170
Default Layout 161
Defending against Attacks 265
DHCP 48
Directory 227
Documentations v
Do Not Disturb 150
DTMF 137
Dual-Stream Protocol 196

E

Enabling Communication with Other Systems 45
Enabling H.460 Support for H.323 Calls 135

F

Far-end Camera Control 211
Firmware v

G

General Issues 286
Getting Information from Status Indicators 283
Getting Started 33

H

H.235 263

H.323 Tunneling 73
Hiding IP Address 177
Hiding Icons in a Call 179
Hiding Menu Logo 178
History Record 154

I

Icons on Display Device 25
Icons on the Video Conferencing Phone 27
Importing/Exporting Configuration 270
Index 301
Intelligent Firewall Traversal 90
In This Guide vi
IPv6 Support 56

K

Keyboard Input Method 188
Key Tone 183

L

Language 169
LDAP 232
LED Instructions 25
License 241
LLDP 62
Logging into the BlueJeans Cloud Platform 114
Logging into the Mind Platform 116
Logging into the StarLeaf Cloud Platform 106
Logging into the Yealink VC Cloud Management Service 100
Logging into the Zoom Cloud Platform 108

M

Manual Configuration for VLAN 65
Meeting Blacklist 187
Meeting Password 184
Meeting Whitelist 186
Methods of Transmitting DTMF Digit 138
Mix Sending 200
Multiple Preset 206

N

Network Address Translation 81

O

Output Resolution 217

P

Packaging Contents 3
Physical Features 2
Placing a Test Call from VCS 46
Powering the System On and Off 39
Preparing the Network 47
Public Mode 162

Q

Quality of Service 91

R

Relog Offtime 183
Remote Control 31
Registering a Custom Account 119
Registering a Pexip Account 111
Registering a YMS Account 104
Resetting to Factory 271
Restricting Reserved Ports 78
Ringback Timeout 158
Rport 88

S

Screenshot 221
Search Source List in Dialing 239
Secure Real-Time Transport Protocol 259
Setup Wizard 41
SIP IP Call by Proxy 159
Site Name 167
SNMP 273
Static DNS 50
STUN 84
Summary of Changes vii
System Component Instructions 10
System Installation 39

System Maintenance 292
System Startup 40
Web User Interface 30

T

Table of Contents xi
Terms vii
Tones 222
Transport Layer Security 251
Troubleshooting 277
Troubleshooting Methods 277
Troubleshooting Solutions 286
Typographic Conventions vi

U

Upgrading System Firmware 269
Upgrading VCC20 Camera Firmware 270
USB Configuration 218
User Interfaces 30
User Mode 247
Using the API with a LAN Connection 244
Using the API with a Serial Connection 245
Using Diagnostic Methods 284

V

VC400/VC120 Codec 10
VCC18/VCC20 HD Camera 12
VCM30 Video Conferencing Microphone Array 20
VCR10 Remote Control 23
VCS Integrated with Control Systems 243
Video & Audio Issues 289
Video Codecs 145
Video Conferencing Phone 14
Video Recording 219
Viewing Call Statistics 284
Viewing Log Files 277
Virtual Remote Control 165
VLAN 61
VoIP Principles 1
VPN 94

W

Web Server Type 249