Yealink

Full HD Video Conferencing System Administrator Guide

MeetingEye 600

MeetingEye 400

VC800

VC880

VC500/PVT950

VC200

Version 44.25 | October 2020

Contents

About This Guide..... 10
Related Documents..... 10
Summary of Changes..... 11
Changes for Release 44 SP1, Guide Version 44.25..... 11
Changes for Release 43, Guide Version 43.32..... 12
Changes for Release 43, Guide Version 43.31..... 12
Changes for Release 43, Guide Version 43.30..... 12
Changes for Release 43, Guide Version 43.10..... 12

Getting Started..... 13
Hardware Overview..... 13
Hardware of MeetingEye 600..... 13
Hardware of MeetingEye 400..... 15
Hardware of VC880 Codec..... 16
Hardware of PVT980 Codec..... 17
Hardware of VC800 Codec..... 18
Hardware of VC500/PVT950 Codec..... 20
Hardware of VC200 Codec..... 22
Hardware of VP59 Codec..... 24
VCR20 Remote Control..... 25
VCR11 Remote Control..... 27
VCC22 video conferencing camera..... 28
Hardware of VCH50 Video Conferencing Hub..... 30
Hardware of VCH51 Video Conferencing Hub..... 31
CP960 Conference Phone..... 32
CTP20 Touch Panel..... 34
WPP20 wireless presentation pod..... 34
Hardware of CPE90 Wired Expansion Microphones..... 35
Hardware of CPW90-BT Bluetooth Wireless Microphone..... 36
VCM38..... 36
VCM34..... 37
Hardware of MSpeaker..... 38
Hardware of MSpeaker II..... 39
CP900/CP700 Ultra-Compact Speakerphone..... 40
LED Instructions..... 41
MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/ PVT950 LED Indicator..... 41
Power Indicator LED of VP59..... 41
Camera Indicator LED of VP59..... 41
LED Instructions of VCC22 Video Conferencing Camera..... 42
LED Instructions of CTP20..... 42
Mute Indicator LED of CP960 Conference Phone..... 42
Mute Indicator LED of CPE90 Wired Expansion Microphones..... 43
LED Instructions of CPW90-BT Bluetooth Wireless Microphones..... 43
LED Instructions of WPP20 Wireless Presentation Pod..... 44
Powering on and off..... 44
Powering on MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/ PVT950..... 44

Powering off MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/PVT950 ... 45
Powering on or Powering off VP59 ... 45
Initialization Process Overview ... 45

Running the Setup Wizard ... 45

Configuration Methods ... 46
Using Web User Interface ... 46
Logging into the Web User Interface ... 46
Configuring the Web Server Type ... 47
User and Administrator Account Login ... 48
Using CTP20 Touch Panel ... 49
Using the Remote Control ... 50
Using the Virtual Remote Control ... 50
Customizing the Key Type ... 50
Disabling Remote Control Keys ... 51
Remote Controller ... 51
Use CP960 Conference Phone ... 51

Device Type Licenses and Multipoint Licenses ... 51
Licenses ... 51
Multipoint Licenses ... 52
Importing Device Type License/Multipoint License ... 52

Traditional Deployment Methods ... 53
Public IP Configuration ... 53
Intranet Deployment ... 53
NAT ... 53
STUN ... 57
H.460 ... 59
Intelligent Traversal ... 60
VPN ... 61

Cloud Deployment Method ... 63

Configuring Network Settings ... 63
Configuring IPv4 or IPv6 ... 63
Configuring IP Addressing Mode ... 64
Configuring IPv4 ... 64
Configuring IPv6 ... 66
Setting the Wireless Network ... 68
Connecting to the Wireless Network ... 68
Viewing the Wireless Network Status ... 70
Forgetting a Wi-Fi ... 70
Disabling the Wi-Fi ... 70
Wireless Access Point ... 71
Enabling the Wireless Access Point ... 71
Configuring Wireless Access Point ... 71
Viewing the Connected Devices ... 73

Adding Connected Devices to the Blocklist....74
Removing Devices from the Blocklist....74
Disabling the Wireless Access Point....75
Configuring DNS Server....75
DHCP Options....76
Supported DHCP Option of IPv4....76
DHCP Option 42, Option 2....77
DHCP Option 12....77
Configuring LLDP....77
Configuring LLDP....78
Configuring VLAN Manually....79
Configuring DHCP VLAN....80
802.1x Authentication....80
Configuring the 802.1x Authentication....81
Enabling/Disabling the PC Port....82
Network Speed and Duplex Mode....83
Supported Transmission Methods....83
Configuring Transmission Methods....83
Restricting Reserved Ports....84
Quality of Service (QoS)....85
Configuring QoS....86
Configuring MTU....87
Configuring SNMP....88

Configuring Account Settings....89
Setting SIP Account/SIP IP Call....89
Configuring SIP Accounts....89
Configuring SIP IP Call....91
Setting H. 323 Account/H.323 IP Call....93
Configuring H.323 Accounts....93
H.323 Tunneling....96
Configuring the PSTN account....97
Configuring the Video Conference Platform Account....98
Registering a Yealink Cloud Account....98
Registering a YMS Account....100
Logging into Zoom Cloud Platform....101
Registering a Pexip Account....102
Logging into the BlueJeans Cloud Platform....105
Logging into Videxio Platform....106
Registering a Custom Account....107
Configuring Quick Switch Platform....109
Logging out of the Video Conference Platform....110

Basic Settings....110
Configuring the Site Name....111
Setting the Language....112
Configuring Key Tone....112
Configure the Time and Date....112
Time Zone....113
Configuring NTP Server....115
Configuring the DST....116
Manually Configuring the Time and Date....118
Customizing the Time and Date Format....119
Setting the Time Reminder....119

Setting Screen Saver for VP59 120
Setting Wallpaper for VP59 120
Enabling/Disabling the Clock for the VP59 121
Setting the Ring Tone for the VP59 121
Configuring Automatic Sleep Time 122
Configuring the Display to Wake up the Sleeping Endpoint 122
Allowing Website Snapshot 123
Setting the Screen Saver Wait Time 123
Customizing the Local Interface for the System 123
Hide the IP Address on the Status Bar 124
Hiding the Time and the Date on the Status Bar 124
Hiding the User Interface in Idle Screen 125
Showing or Hiding Icons in a Call 125
Muting the Microphone 129
Configuring Microphone Mute Mode 129
Configuring the Keyboard Input Method 130
Configuring USB Storage 131
Configuring Local Storage 131
Configuring the Screenshot 132
Configuring to Automatically Upload Screenshots to the YMS 132
Configuring Video Recording 133
Basic Settings for CP960 Conference Phone 134
Adjusting Backlight of the CP960 Conference Phone 135
Setting the Screen Saver for CP960 Conference Phone 135
Configuring * Key for Default Input 135
Configuring Whiteboard Tools 136
Configuring the Presentation Tools 137

Configuring the Audio Settings 137

Audio Output 138
Audio Output Type 138
Specifying an Available Audio Output 139
Audio Input 140
Audio Input Type 140
Specifying an Available Audio Input 142
Media Audio Input 144
Configuring Media Audio Input 144
EQ Self Adaption 145
Configuring the EQ Self-adaption 145
Configuring the Noise Suppression 146
Tones 147
Supported Tones 147
Custom Tones Formats 147
Customizing Tones 147
Codecs 148
Audio Codec 148
Video Codecs 150
DTMF 152
DTMF Keypad 152
Transmission Ways of DTMF 152
Setting DTMF Transmission Method for SIP Protocol 153
Configuring DTMF for H.323 Protocol 154

Configuring Video Settings 154

Display Layout Settings....155
Setting the Default Layout for a Single Screen....155
Setting the Default Layout for Dual Single Screen....156
Configuring Change Layout by Content Sharing....157
Configuring Auto Zoom In Content for a Single Screen....158
Hiding Local Video Image in Equal Layout....159
Configuring Hide Local Video When PIP....159
Configuring Multi-Camera Default Layout....160
Configuring Voice Activation....161
Configuring the View Switching....161
Configuring Preview Local....163
Changing the Video Input Source....163
Configuring HDMI Extended Display by VP59....164
Specifying Content to the Secondary Screen....164
Adjusting the Monitor Display Proportion....166
Selecting Video Frame Rate and Resolution....166
Configuring the Monitor Resolution....168
Configuring VC200 Experimental Access (Auto Framing)....169
Showing the Site Name to Remote Parties....170

Configuring Content Sharing....172
Configuring Dual-Stream Protocol....172
Configuring the H.239 Protocol....172
Configuring BFCP (Binary Floor Control dual Protocol)....173
Configuring Mix-Sending....173
Configure Content Sharing....173

Configuring Camera Settings....175
Selecting and Setting Cameras....176
Viewing Camera Status....176
Specifying the Camera Control Mode for MeetingEye 600/MeetingEye 400....177
Enabling People Counting....178
Controlling the Camera....179
Adjusting the White Balance....179
Adjusting the Exposure....180
Configuring Auto Exposure Mode....181
Configuring Manual Exposure Mode....182
Configuring the Mode of Shutter Priority....183
Configuring Aperture Priority....185
Configuring the Mode of Brightness Priority....186
Configuring the Mode of WDR-Auto....187
Configuring WDR-Manual....188
Displaying Camera Name When Multi-Camera Connected....189
Adjusting the Display Image of the Camera....189
Adjusting Hangup Mode and Camera Pan Direction....191
Configuring Continuous Auto Focus....192
Setting the Camera Presets....192
Configuring Preset Synchronize With Active Camera....193
Allowing the Remote System to Control Your Camera....193
Camera Control Protocol....193
Configuring the Far Site to Control the Near Camera....195
Configuring Multi-Camera Default Layout....195
Resetting the Camera....196

Configuring Virtual Meeting Room..... 196
Setting the Endpoint as a Regular Mode Conference Room..... 197
Setting the Endpoint as VMR Mode Conference Rooms..... 197
Joining the VMR..... 199
Configuring the Third-party Virtual Meeting Room..... 200

Configuring Call Settings..... 201
Selecting a Call Protocol..... 201
Specifying the Video Call Rate..... 202
Configuring Call Rate Adaptation..... 203
Account Polling..... 203
Priority of Call Types..... 204
Configuring the Account Polling..... 204
Selecting the CTP20 Conference Call Preferences..... 204
Setting the CTP20 Contact Display Label..... 205
Configuring Additional Audio Call..... 206
Selecting the Multi-Party Resources..... 207
Configuring Call Match..... 208
Dial Plan..... 208
Adding a Dial Plan..... 209
Search Source List in Dialing..... 209
Configuring Search Source List in Dialing..... 209
Configuring SIP IP Call by Proxy..... 210
Configuring Ringback Timeout..... 210
Configuring the Auto Refuse Timeout..... 211
Auto Answer..... 211
Answering a Call Automatically When not in a Call..... 211
Answering Multiple Calls Automatically..... 212
Muting Auto-Answered Calls..... 212
Muting Auto-Dialed Calls..... 213
DND (Do Not Disturb)..... 213
Enabling DND When Not in a Call..... 213
Enabling DND during an Active Call..... 213
Enabling Fast Audio Call for CP960..... 214

Managing the Directory..... 214
Local Directory..... 214
Adding Local Contacts and Conference Contacts..... 214
Importing a Local Contact List..... 216
Exporting Local Contact List..... 217
Editing Local Contacts..... 217
Deleting Local Contacts..... 217
Yealink Cloud Contacts..... 218
Enterprise Directory..... 218
LDAP..... 219
LDAP Attributes..... 219
Configuring LDAP..... 220
Meeting Whitelist..... 222
Adding Meeting Whitelist..... 223
Deleting the Meeting Allowlist..... 223
Meeting Blacklist..... 223
Adding Meeting Blacklist..... 223

Deleting the Meeting Blacklist..... 223

Managing the Call History..... 224

Saving History Record..... 224
Adding a History Record to the Local Directory..... 224
Deleting Call Records..... 225
Deleting a Call Record..... 225
Deleting Multiple History Records..... 225
Deleting All History Records..... 225
Placing Calls from Call History..... 225

Placing a Call..... 226

Placing a Call by Entering a Number..... 226
Editing Numbers Before Placing a Call..... 227

Configuring the Security Features..... 227

Collaboration Data Security Control..... 227
Configuring the Auto Logout Time..... 228
Transport Layer Security (TLS)..... 228
Supported Cipher Suites..... 229
TLS Transport Protocol..... 230
Managing the Trusted Certificates List..... 231
Managing the Server Certificates..... 238
Secure Real-Time Transport Protocol (SRTP)..... 238
H.235 Encryption..... 240
Defending against Attacks..... 241
System Integrated with Control Systems..... 243
Connection Methods of Control Systems..... 243
Connection Settings for Control Systems..... 243

CEC Monitor Controls..... 245

Configuring CEC Monitor Controls..... 245

Accessories with Your System..... 246

Using WPP20 Wireless Presentation Pod..... 246
Using the CPN10 PSTN Box..... 246
Using the VCC22 Video Conferencing Cameras..... 246
Controlling VCC22 Camera..... 247
Adjusting the Multi-Camera Layout During a Call..... 247
Using the CPW90-BT Bluetooth Wireless Microphones with VCS..... 247
Registering CPW90-BT with VCS..... 248
Deregistering CPW90 from VCS..... 248
Viewing the Information of Bluetooth Wireless Microphones..... 249
Finding the Registered CPW90-BT..... 249
Using CTP20..... 249
Wired Connection to CTP20..... 249
Wireless Connection to CTP20..... 250
Using Multiple CTP20s for Collaboration..... 250
Using VCM34..... 250
Using VCM38..... 251
Using the Soundbar/MSpeaker II..... 251

Using CP900/CP700 Ultra-Compact Speakerphone....251

System Maintenance....251

Exporting or Importing Configuration Files....251
Exporting BIN Files from the System....251
Importing BIN Files to the System....252
Rebooting the System....252
Resetting the SD card of MeetingEye 600/MeetingEye 400/VC200/VP59....252
Resetting the System....253
Resetting the System via Configuration Methods....253
Resetting the System by using Reset Button....253
Resetting VP59 by REDIAL key....253
Exporting Log Files....254
Setting the Severity Level of the Local log....254
Setting Severity Level of the Module log....254
Exporting the Log Files to a Local PC....255
Exporting the Log Files to a USB Flash Drive....256
Exporting the Log Files to a Syslog Server....256
Capturing Packets....257
Capturing the Packets via Web User Interface....257
Capturing the Packets via Remote Control....260
Capturing the Packets via Ethernet Software....260
System Firmware....260
Upgrading the Firmware....262
Viewing Multipoint License Status....262
Viewing the Device Type....263

Troubleshooting....263

General Issues....264
Call Issues....265
Audio Issues....266
Video Issues....267
Placing a Test Call....268
System Diagnostics....268
Diagnosing the Audio....269
Diagnosing the Camera....269
Diagnosing the Network....269
System Status....270
System Status List....270
Viewing System Status....273
Viewing Call Statistics....273

About This Guide

Yealink administrator guide provides general guidance on configuring, customizing, managing, and troubleshooting video conferencing systems. This guide is not intended for an administrator who is experienced in system administration.

This guide is applicable to the following models:

- MeetingEye 600 video conferencing system
- MeetingEye 400 video conferencing system
- VC880 video conferencing system
- VC800 video conferencing system
- VC500 Pro video conferencing system
- VC500 video conferencing system
- VC200 video conferencing system
- PVT980 video conferencing system
- PVT950 video conferencing system
- VP59 video conferencing system (conference phone)

The differences between VC500 and VC500 Pro models are as follow:

Features	VC500	VC500 Pro
Work with CP960 conference phone	×	√
H.265 video codec	×	√
60 frame rate	×	√

Attention:

Notes for upgrading firmware versions:

- For VC800, VC500, VCC22, and PVT950 using new hardware, their hardware versions are 63.0.98.0.2.1.17, 71.0.50.0.2.0.16, 82.0.1.0.2.0.17, and 1137.0.2.0.2.0.16 respectively. After upgrading their firmware to version X.44.0.25, you cannot degrade them to version X.43.0.30 or earlier versions. Please upgrade with caution.
- After upgrading VP59 to version 44 (91.344.0.10), you cannot degrade it to versions earlier than 44. Please upgrade with caution.

Note:

If you purchase VC500, but you want to use the features supported by the VC500 Pro model, you can contact Yealink technical support for help.

- Related Documents
- Summary of Changes

Related Documents

The following related documents are available:

- Video Conferencing System Quick Start Guide, which describes how to assemble the system and configure the meeting room and the network.

- Video Conferencing System User Guide, which describes how to configure and use basic features available on the systems.
- Video Conferencing System Network Deployment Guide, which describes how to deploy VCS.
- Video Conferencing System Network Deployment Solution, which describes how to deploy the network for your systems.
- Yealink VCR11 Remote Control Quick Reference Guide, which describes how to use the VCR11 Remote Control.
- Yealink CP960 HD IP Conference Phone Quick Reference Guide, which describes how to use CP960 conference phone.
- Yealink CPW90-BT Bluetooth Wireless Microphones Quick Start Guide, which describes how to use CPW90-BT.
- Yealink Wi-Fi USB Dongle WF50 User Guide, which describes how to connect the wireless network to the VCS codec and provide wireless AP via WF50.
- Yealink WPP20 Wireless Presentation Pod User Guide, which describes how to use WPP20 wireless presentation pod.
- Yealink PSTN Box CPN10 Quick Start Guide, which describes how to connect VCS codec to PSTN.
- Yealink VCC22 Video Conferencing Camera Quick Start Guide, which describes how to connect the VCC22 video conferencing cameras to the VCS codec.
- Yealink CTP20 Quick Start Guide, which describes how to connect CTP20 to the VCS codec.
- Yealink VCM34 Quick Start Guide, which describes how to connect VCM34 to the VCS codec.
- Yealink VCH51 Quick Start Guide, which describes how to connect VCH51 to the VCS codec.
- Yealink Soundbar Quick Start Guide, which describes how to connect Soundbar to the VCS codec.
- Yealink MSpeaker II Quick Start Guide, which describes how to connect MSpeaker II to the VCS codec.

You can download these documentations online:

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

For support or service, please contact your Yealink reseller or go to Yealink Technical Support online:

http://support.yealink.com/.

Summary of Changes

- Changes for Release 44 SP1, Guide Version 44.25
- Changes for Release 43, Guide Version 43.32
- Changes for Release 43, Guide Version 43.31
- Changes for Release 43, Guide Version 43.30
- Changes for Release 43, Guide Version 43.10

Changes for Release 44 SP1, Guide Version 44.25

In this version, we change the design of user interface.

The following sections are new for this version:

VCM38

Using VCM38

CP900/CP700 Ultra-Compact Speakerphone

Configuring Whiteboard Tools

Configuring the Presentation Tools

Using CP900/CP700 Ultra-Compact Speakerphone

Major updates have occurred to the following sections:

Hardware of CPW90-BT Bluetooth Wireless Microphone

Selecting a Call Protocol

Specifying the Video Call Rate

Adding a Dial Plan

Using the CPW90-BT Bluetooth Wireless Microphones with VCS

Changes for Release 43, Guide Version 43.32

This guide is also available to MeetingEye 600 video conferencing system which is newly issued.

The following sections are new for this version:

- Hardware of MeetingEye 600
- Setting the Default Layout for Dual Single Screen

Changes for Release 43, Guide Version 43.31

This guide is also available to MeetingEye 400 video conferencing system which is newly issued.

The following sections are new for this version:

- Hardware of MeetingEye 400
- VCR20 Remote Control
- Specifying the Camera Control Mode for MeetingEye 600/MeetingEye 400
- Enabling People Counting

Changes for Release 43, Guide Version 43.30

The following sections are new for this version:

- Enabling/Disabling the PC Port
- Setting Screen Saver for VP59
- Setting Wallpaper for VP59
- Configuring the Display to Wake up the Sleeping Endpoint
- Configuring * Key for Default Input
- Dial Plan
- Configuring Auto Zoom In Content for a Single Screen
- Showing the Site Name to Remote Parties
- Hardware of MSpeaker II

Major updates have occurred to the following sections:

- Configuring Change Layout by Content Sharing
- Specifying Content to the Secondary Screen
- Configuring Call Rate Adaptation
- Using the Soundbar/MSpeaker II
- System Firmware

Changes for Release 43, Guide Version 43.10

The following sections are new for this version:

- Configuring Quick Switch Platform
- Configuring to Automatically Upload Screenshots to the YMS
- Configuring Call Rate Adaptation

- Displaying Camera Name When Multi-Camera Connected
- Configuring SNMP

Major updates have occurred to the following sections:

- Configuring Video Recording
- Configuring Virtual Meeting Room
- Setting the Camera Presets
- Using WPP20 Wireless Presentation Pod
- Call Issues

Getting Started

This chapter introduces the basic operation of VCS endpoints.

- Hardware Overview
- LED Instructions
- Powering on and off

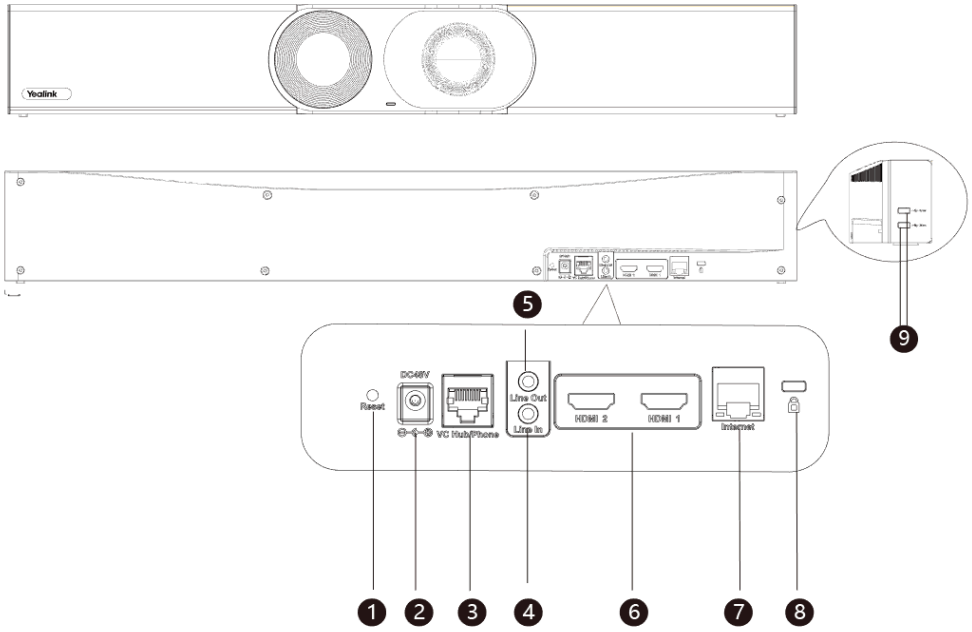
Hardware Overview

- Hardware of MeetingEye 600
- Hardware of MeetingEye 400
- Hardware of VC880 Codec
- Hardware of PVT980 Codec
- Hardware of VC800 Codec
- Hardware of VC500/PVT950 Codec
- Hardware of VC200 Codec
- Hardware of VP59 Codec
- VCR20 Remote Control
- VCR11 Remote Control
- VCC22 video conferencing camera
- Hardware of VCH50 Video Conferencing Hub
- Hardware of VCH51 Video Conferencing Hub
- CP960 Conference Phone
- CTP20 Touch Panel
- WPP20 wireless presentation pod
- Hardware of CPE90 Wired Expansion Microphones
- Hardware of CPW90-BT Bluetooth Wireless Microphone
- VCM38
- VCM34
- Hardware of MSpeaker
- Hardware of MSpeaker II
- CP900/CP700 Ultra-Compact Speakerphone

Hardware of MeetingEye 600

Yealink MeetingEye 600 is the smart video conferencing endpoint, designed for medium meeting rooms. It adopts 20MP super-wide angle lens and 10x Hybrid Zoom, providing excellent video quality with delicate

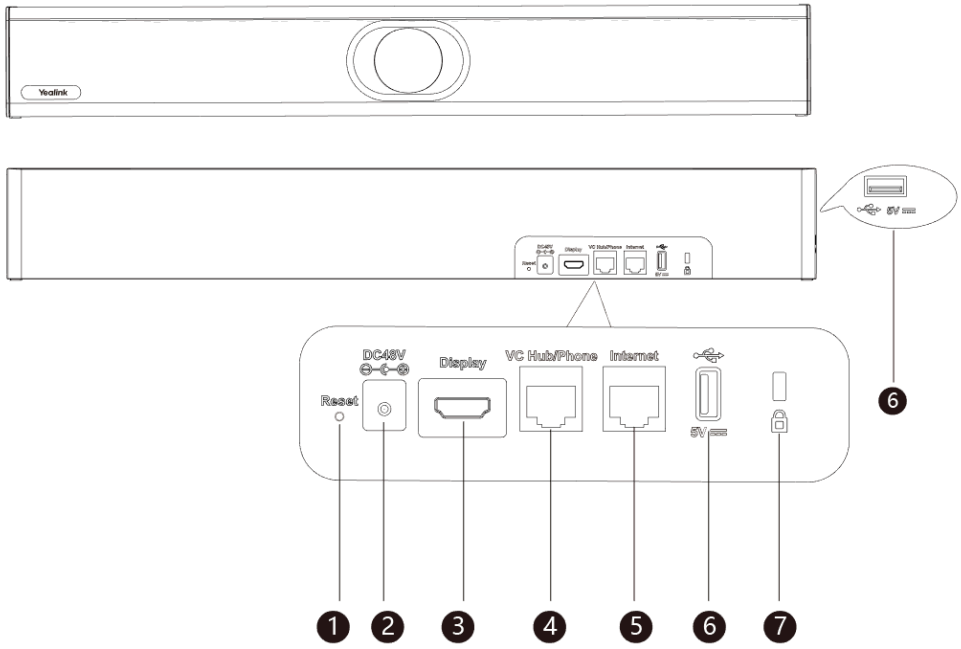
details. Its dual UHD 4K video conference, AI technologies, and the auto privacy shutter allow users to experience a smarter and safer video conference.



	Port Name	Description
1	Reset Key	Reset the VCS endpoint to factory defaults.
2	DC48V	Connect to the power source via a power adapter.
3	VC Hub/Phone	• If you want to use wired sharing to present, connect this port to the PoE port on the VCH51 video conferencing hub. • Connect to CTP20. • If you need an audio device, connect this port to the Internet port on the CP960 Conference phone. • Connect to MSpeaker II. • Connect to VCM34.
4	Line In	Connect to an audio input device via an audio cable (3.5mm).
5	Line Out	Connect to an audio output device via an audio cable (3.5mm).
6	HDMI	Connect to a monitor for displaying video images.
7	Internet	Connect to the network device.
8	Security Slot	Allow you to connect a universal security cable to the VCS endpoint, so you can lock the VCS endpoint down. The VCS endpoint cannot be removed when locked.
9	USB	• Connect to a USB flash drive for storing screenshots, recording videos or capturing packets. If you insert multiple USB flash drives to the VCS endpoint simultaneously, only the last USB flash drives you insert can be identified by the endpoint. • Insert a PSTN box CPN10 for connecting to the PSTN (Public Switched Telephone Network). • Pair with WPP20.

Hardware of MeetingEye 400

Yealink MeetingEye 400 is the smart video conferencing endpoint, designed for small meeting rooms. Supporting dual 4K video conference, 20MP camera, and 133 ° super-wide-angle lens, MeetingEye 400 delivers outstanding video quality. Its AI technologies and built-in auto privacy shutter allow users to experience a smarter and safer video conference. With 8 MEMS microphone arrays and Yealink new audio algorithms, MeetingEye 400 brings excellent audio experience in small rooms even in full-duplex mode and ensures that everyone can be heard as well as seen.



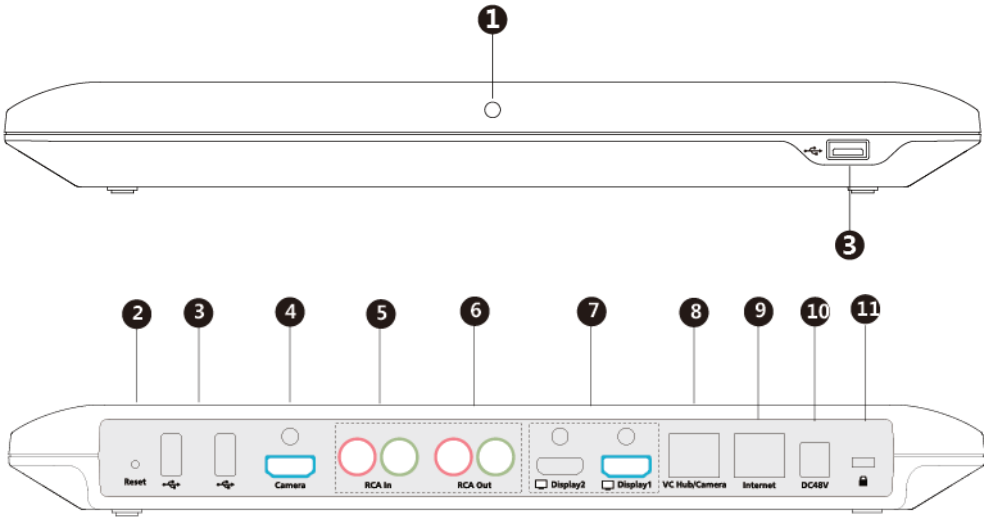
	Port Name	Description
1	Reset Key	Reset the VCS endpoint to factory defaults.
2	DC48V	Connect to the power source via a power adapter.
3	Display	Connect to a monitor for displaying video images.
4	VC Hub/Phone	• If you want to use wired sharing to present, connect this port to the PoE port on the VCH51 video conferencing hub. • Connect to CTP20. • If you need an audio device, connect this port to the Internet port on the CP960 Conference phone.
5	Internet	Connect to the network device.
6	USB	• Connect to a USB flash drive for storing screenshots, recording videos or capturing packets. If you insert multiple USB flash drives to the VCS endpoint simultaneously, only the last USB flash drives you insert can be identified by the endpoint. • Insert a PSTN box CPN10 for connecting to the PSTN (Public Switched Telephone Network). • Pair with WPP20.

	Port Name	Description
7	Security Slot	Allow you to connect a universal security cable to the VCS endpoint, so you can lock the VCS endpoint down. The VCS endpoint cannot be removed when locked.

Hardware of VC880 Codec

With rich physical interfaces for audio and video connection, VC880 can be connected to the 3rd-party camera or access to the video matrix. Possessing rich physical interfaces for audio and video connection, the system can be connected to the 3rd-party camera or access to the video matrix. In addition, it comes with the professional RCA-in/out interface that integrates the mixer with the gooseneck microphone. Its spilt-type structure can meet the deployment requirement of the control room which separates from a large conference room.

The following introduces the corresponding ports on VC880.



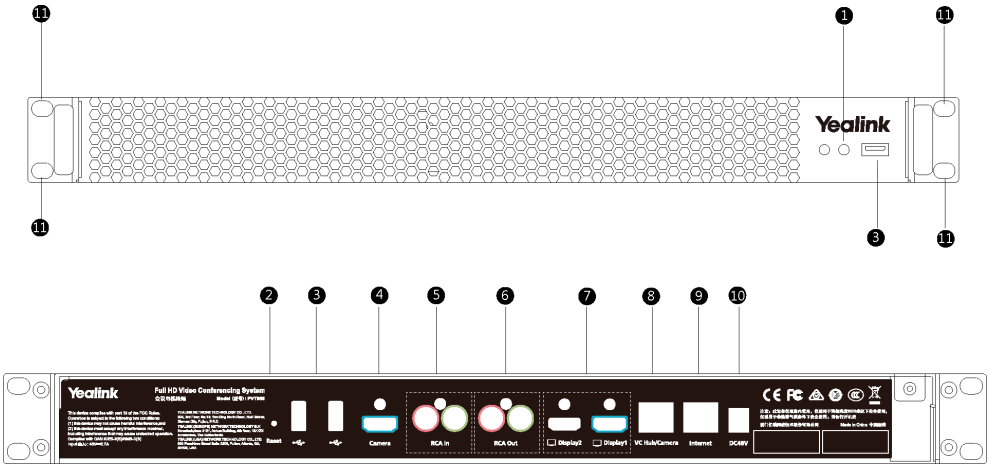
	Port Name	Description
1	LED Indicator	Indicate different status of the system.
2	Reset Key	Reset the VCS endpoint to factory defaults.
3	USB	• Insert a USB flash drive. USB flash drive can be used for storing screenshots, recorded videos or captured packets. If you insert multiple USB flash drives to the VCS endpoint simultaneously, only the last USB flash drives you insert can be identified by the endpoint. • Insert a WF50 Wi-Fi USB Dongle for connecting to Wi-Fi or providing wireless AP. • Insert a BT42 Bluetooth USB Dongle for connecting to the CPW90-BT Bluetooth wireless microphones. • Insert a PSTN box CPN10 for connecting to the PSTN (Public Switched Telephone Network).
4	Camera Port	Connect to a third-party camera.

	Port Name	Description
5	RCA In	Connect to an audio input device via an RCA cable.
6	RCA Out	Connect to an audio output device via an RCA cable.
7	Display	Connect to a monitor for displaying video images.
8	VC Hub/Camera	• If you want to use wired sharing to present, connect this port to the Codec port on the VCH50 video conferencing hub/to the PoE port on the VCH51 video conferencing hub. • Connect to CTP20. • Connect this port to the Camera port on the VCC22 video conferencing camera. • If you need an audio device, connect this port to the Internet port on the CP960 Conference phone. • Connect to VCM34.
9	Internet	Connect to the network device.
10	DC48V	Connect to the power source via a power adapter.
11	Security Slot	Allow you to connect a universal security cable to the VCS endpoint, so you can lock the VCS endpoint down. The VCS endpoint cannot be removed when locked.

Hardware of PVT980 Codec

PVT980, targeted at large meeting room, is applicable to the meeting room with a rack or the lecture hall. Possessing rich physical interfaces for audio and video connection, the system can be connected to the 3rd-party camera or access to the video matrix. In addition, it comes with the professional RCA-in/out interface that integrates the mixer with the gooseneck microphone.

The following introduces the corresponding ports on PVT980.



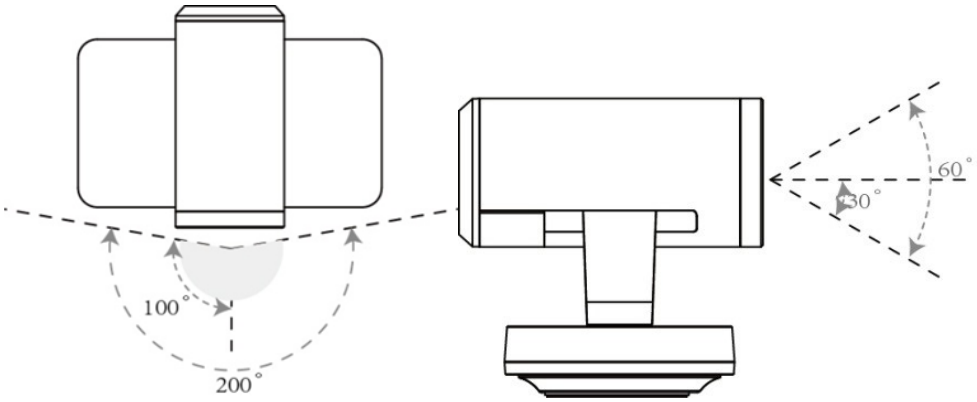
	Port Name	Description
1	LED Indicator	Indicate different status of the system.
2	Reset Key	Reset the VCS endpoint to factory defaults.

	Port Name	Description
3	USB	• Insert a USB flash drive. USB flash drive can be used for storing screenshots, recorded videos or captured packets. If you insert multiple USB flash drives to the VCS endpoint simultaneously, only the last USB flash drives you insert can be identified by the endpoint. • Insert a WF50 Wi-Fi USB Dongle for connecting to Wi-Fi or providing wireless AP. • Insert a BT42 Bluetooth USB Dongle for connecting to the CPW90-BT Bluetooth wireless microphones. • Insert a PSTN box CPN10 for connecting to the PSTN (Public Switched Telephone Network).
4	Camera Port	Connect to a third-party camera.
5	RCA In	Connect to an audio input device via an RCA cable.
6	RCA Out	Connect to an audio output device via an RCA cable.
7	Display	Connect to a monitor for displaying video images.
8	VC Hub/Camera	• If you want to use wired sharing to present, connect this port to the Codec port on the VCH50 video conferencing hub/to the PoE port on the VCH51 video conferencing hub. • Connect this port to the Camera port on the VCC22 video conferencing camera. • If you need an audio device, connect this port to the Internet port on the CP960 Conference phone. • Connect to VCM38.
9	Internet	Connect to the network device.
10	DC48V	Connect to the power source via a power adapter.
11	Slot Hole	Use the screws to lock the PVT980 system to the rack.

Hardware of VC800 Codec

VC800 codec compresses the outgoing video and audio data, transmits the data to the far site, and decompresses the incoming data.

Supporting 16:9 and 4:3 aspect ratios, it is compatible with different audio devices, and can adapt to the monitors automatically. The VC800 camera can be panned (± 100 degrees range), tilted (± 30 degrees range) and supports 12 x optical zoom, white balance, automatic gain and so on.



- Front Panel of VC800 Codec
- Rear Panel of VC800 Codec

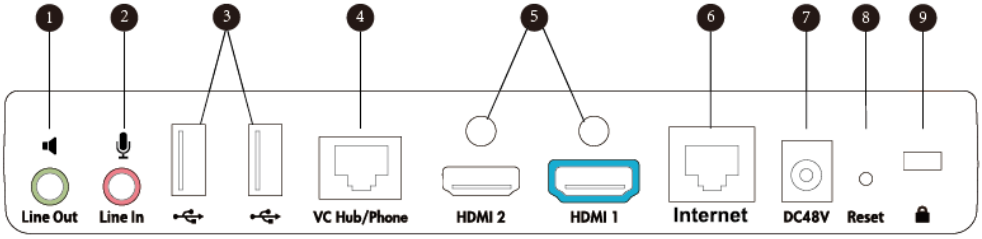
Front Panel of VC800 Codec

The LED indicator in front of the camera indicates different camera status.

Related information

MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/ PVT950 LED Indicator

Rear Panel of VC800 Codec



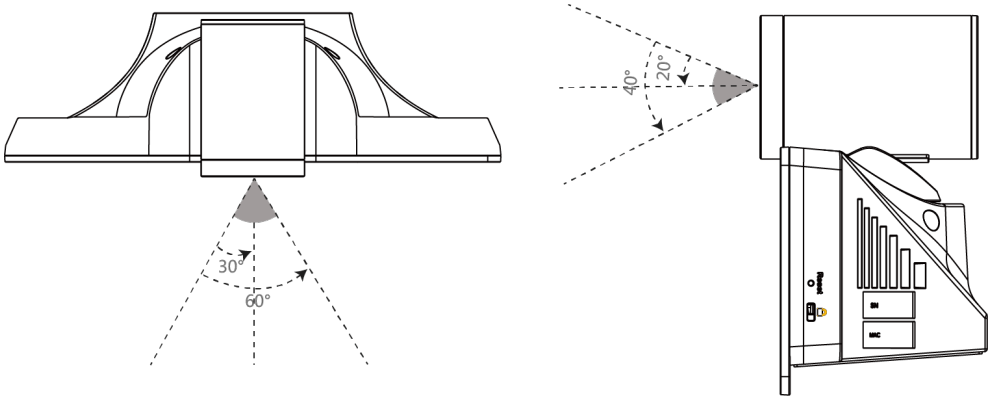
	Port Name	Description
1	Line Out	Connect to an audio output device via an audio cable (3.5mm).
2	Line In	Connect to an audio input device via an audio cable (3.5mm).
3	USB	• Insert a USB flash drive. USB flash drive can be used for storing screenshots, recorded videos or captured packets. If you insert multiple USB flash drives to the VCS endpoint simultaneously, only the last USB flash drives you insert can be identified by the endpoint. • Insert a WF50 Wi-Fi USB Dongle for connecting to Wi-Fi or providing wireless AP. • Insert a BT42 Bluetooth USB Dongle for connecting to the CPW90-BT Bluetooth wireless microphones. • Insert a PSTN box CPN10 for connecting to the PSTN (Public Switched Telephone Network).

	Port Name	Description
4	VC Hub/Phone	• If you want to use wired sharing to present, connect this port to the Codec port on the VCH50 video conferencing hub/to the PoE port on the VCH51 video conferencing hub. • Connect to CTP20. • If you need an audio device, connect this port to the Internet port on the CP960 Conference phone. • Connect to VCM38/VCM34.
5	HDMI	Connect to a monitor for displaying video images.
6	Internet	Connect to the network device.
7	DC48V	Connect to the power source via a power adapter.
8	Reset Key	Reset the VCS endpoint to factory defaults.
9	Security Slot	Allow you to connect a universal security cable to the VCS endpoint, so you can lock the VCS endpoint down. The VCS endpoint cannot be removed when locked.

Hardware of VC500/PVT950 Codec

VC500/PVT950 codec compresses outgoing video and audio data, transmits this information to the far site, and decompresses incoming data.

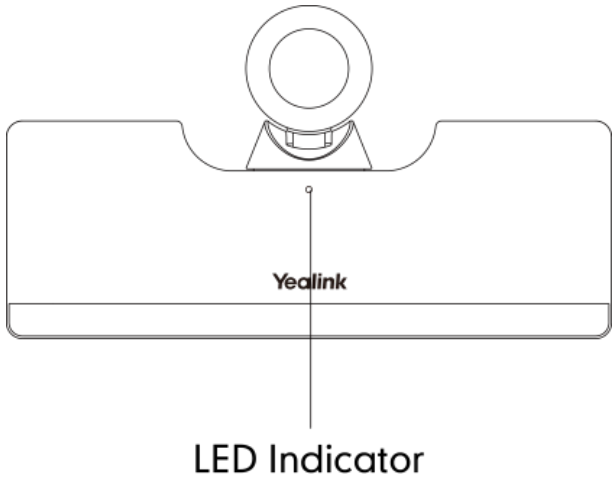
VC500/PVT950 codec, compatible with different audio devices, supports 16:9 and 4:3 aspect ratios and can adapt to the monitors automatically. The VC500/PVT950 camera can be panned (± 60 degrees range), tilted (± 40 degrees range) and support 5 x optical zoom, white balance and automatic gain.



- Front Panel of VC500/PVT950 Codec
- Rear Panel of VC500 Codec

Front Panel of VC500/PVT950 Codec

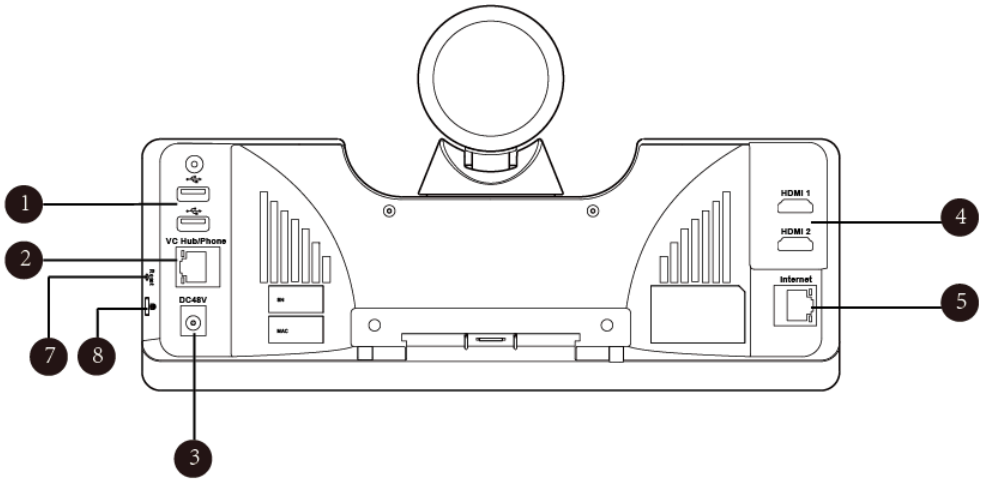
The LED indicator in front of the camera indicates different camera status.



Related information

MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/ PVT950 LED Indicator

Rear Panel of VC500 Codec



	Port Name	Description
1	USB	• Insert a USB flash drive. USB flash drive can be used for storing screenshots, recorded videos or captured packets. If you insert multiple USB flash drives to the VCS endpoint simultaneously, only the last USB flash drives you insert can be identified by the endpoint. • Connect to an audio input device via a USB to line input adapter. • Connect to an audio output device via a USB to line input adapter. • Insert a WF50 Wi-Fi USB Dongle for connecting to Wi-Fi or providing wireless AP. • Insert a BT42 Bluetooth USB Dongle for connecting to the CPW90-BT Bluetooth wireless microphones. • Insert a PSTN box CPN10 for connecting to the PSTN (Public Switched Telephone Network).

	Port Name	Description
2	VC Hub/Phone	• If you want to use wired sharing to present, connect this port to the Codec port on the VCH50 video conferencing hub/to the PoE port on the VCH51 video conferencing hub. • Connect to CTP20. • If you need an audio device, connect this port to the Internet port on the CP960 Conference phone. • Connect to VCM34. (It is not applicable to PVT950) • Connect to VCM38. (It is not applicable to VC500)
3	DC48V	Connect to the power source via a power adapter.
4	HDMI	Connect to a monitor for displaying video images.
5	Internet	Connect to the network device.
6	Reset Key	Reset the VCS endpoint to factory defaults.
7	Security Slot	Allow you to connect a universal security cable to the VCS endpoint, so you can lock the VCS endpoint down. The VCS endpoint cannot be removed when locked.

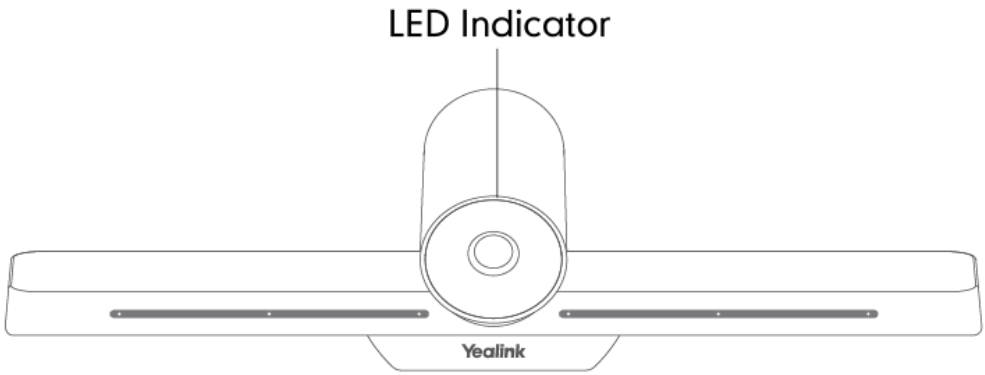
Hardware of VC200 Codec

Yealink VC200 is an entry-level smart video conferencing endpoint designed for small and huddle room. Supporting 16:9 and 4:3 aspect ratios, it is compatible with different audio devices, and can adapt to the monitors automatically. VC200 possesses many features, ultra HD 4K, 4 x digital zoom camera, 103° super-wide angle lens, white balance automatic gain and others. With 6 beamforming microphone arrays for direct voice pickup and Yealink Noise Proof Technology, VC200 brings excellent audio effect in small rooms and ensures that everyone can be heard clearly.

- Front Panel of VC200 Codec
- Rear Panel of VC200 Codec
- Bottom of VC200 Codec

Front Panel of VC200 Codec

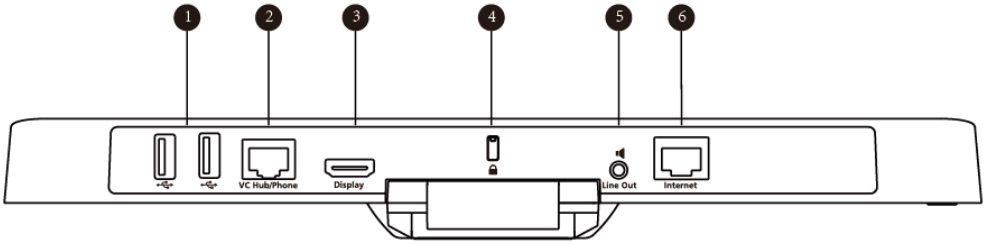
The LED indicator on the camera indicates different camera status.



Related information

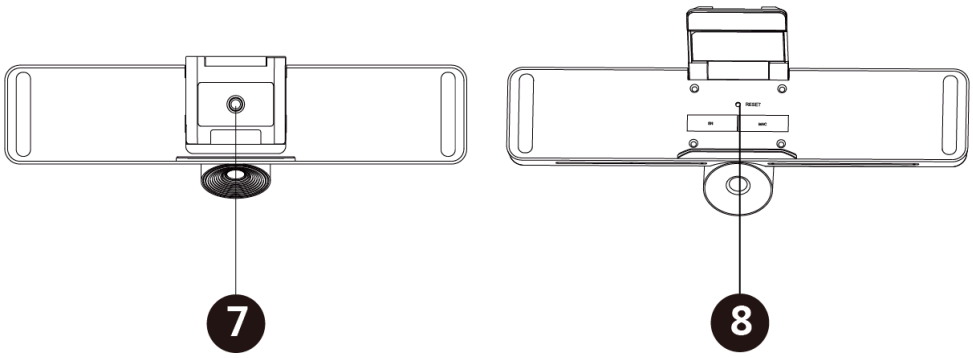
MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/ PVT950 LED Indicator

Rear Panel of VC200 Codec



	Port Name	Description
1	USB	• Connect to a USB flash drive for storing screenshots, recording videos or capturing packets. If you insert multiple USB flash drives to the VCS endpoint simultaneously, only the last USB flash drives you insert can be identified by the endpoint. • Insert a PSTN box CPN10 for connecting to the PSTN (Public Switched Telephone Network).
2	VC Hub/Phone	• If you want to use wired sharing to present, connect this port to the Codec port on the VCH50 video conferencing hub/to the PoE port on the VCH51 video conferencing hub. • If you need an audio device, connect this port to the Internet port on the CP960 Conference phone. • Connect to VCM34.
3	Display	Connect to a monitor for displaying video images.
4	Security Slot	Allow you to connect a universal security cable to the VCS endpoint, so you can lock the VCS endpoint down. The VCS endpoint cannot be removed when locked.
5	Line Out	Connect to an audio output device via an audio cable (3.5mm).
6	Internet	Connect to the PoE via the network cable.

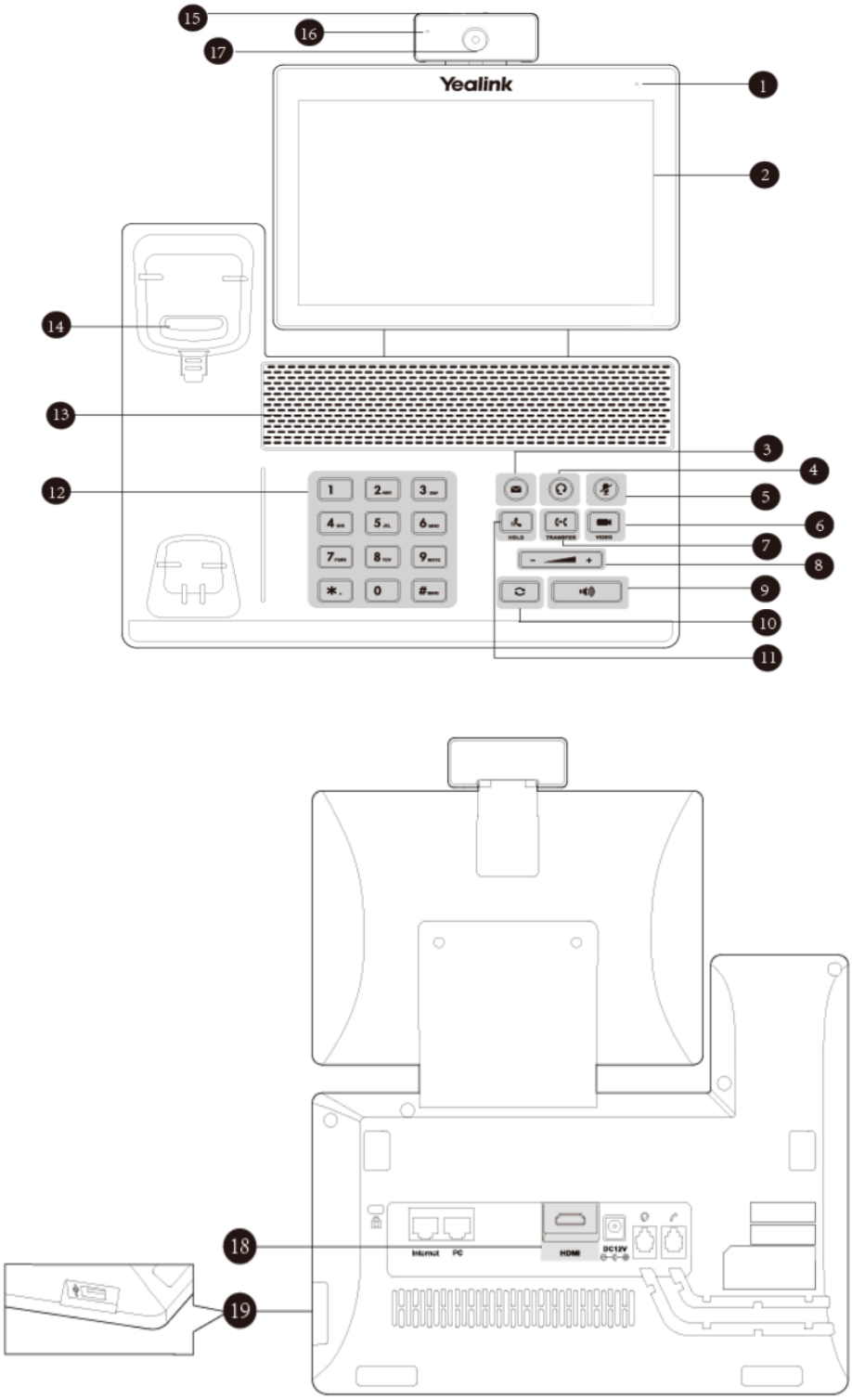
Bottom of VC200 Codec



	Port Name	Description
7	VESA	Fix VC200 to the TV stand or a tripod via a 1/4”-20 UNC screw.
8	Reset Key	Reset the VCS endpoint to factory defaults.

Hardware of VP59 Codec

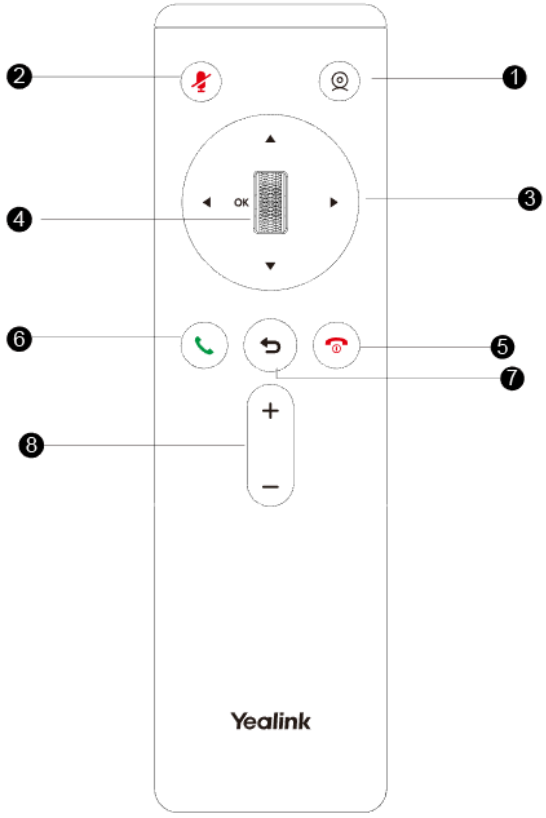
You can use VP59 as a video phone on your desktop, you can also use it as a video conferencing device in a small meeting room (20-30 square meters).



	Name	Description
1	Power Indicator LED	Indicates the call status and the system status.
2	Touch Screen	Tap the screen and select the desired menu. Displays the time, the date, the call and other related information.
3	MESSAGE Key	Not available.
4	HEADSET Key	Toggles and indicates the headset mode. The key LED glows green when headset mode is activated.
5	Mute Key	Toggles and indicates the mute feature. The key LED glows red when the call is muted.
6	VIDEO Key	• Allows you to preview local-site video when the phone is idle. • Controls the transmission of video images during calls and conferences.
7	TRANSFER Key	Not available.
8	Volume Key	Adjusts the volume of the handset, the speakerphone, the earphone, ringer or the media.
9	Speakerphone Key	Toggles and indicates the hands-free (speakerphone) mode. When the hands-free (speakerphone) mode is activated: the key LED glows green
10	REDIAL Key	Redials a previously dialed number.
11	HOLD Key	Not available.
12	Keypad	Use it to type in digits, letters and special characters.
13	Speaker	Provides hands-free (speakerphone) audio output.
14	Hookswitch	• Picking up the handset from the handset cradle, the hookswitch bounces and the phone connects to the line. • Laying down the handset on the handset cradle, the phone disconnects from the line.
15	Shutter Switch	Covers or uncovers the camera. When the camera is switched off, the video image turns to be black.
16	Camera Indicator LED	Indicates the status of video call and camera: • Receives a video call: flashing green • The camera is inserted and detected successfully on the phone: green
17	Camera Lens	Two mega-pixel camera. The optimal object distance should be from 0.35m (1 foot) to 2m (6 feet).
18	HDMI	Connect to a monitor for displaying video images.
19	USB 2.0 Port	Connect to a USB flash drive/WPP20/CPN10/USB to Line output.

VCR20 Remote Control

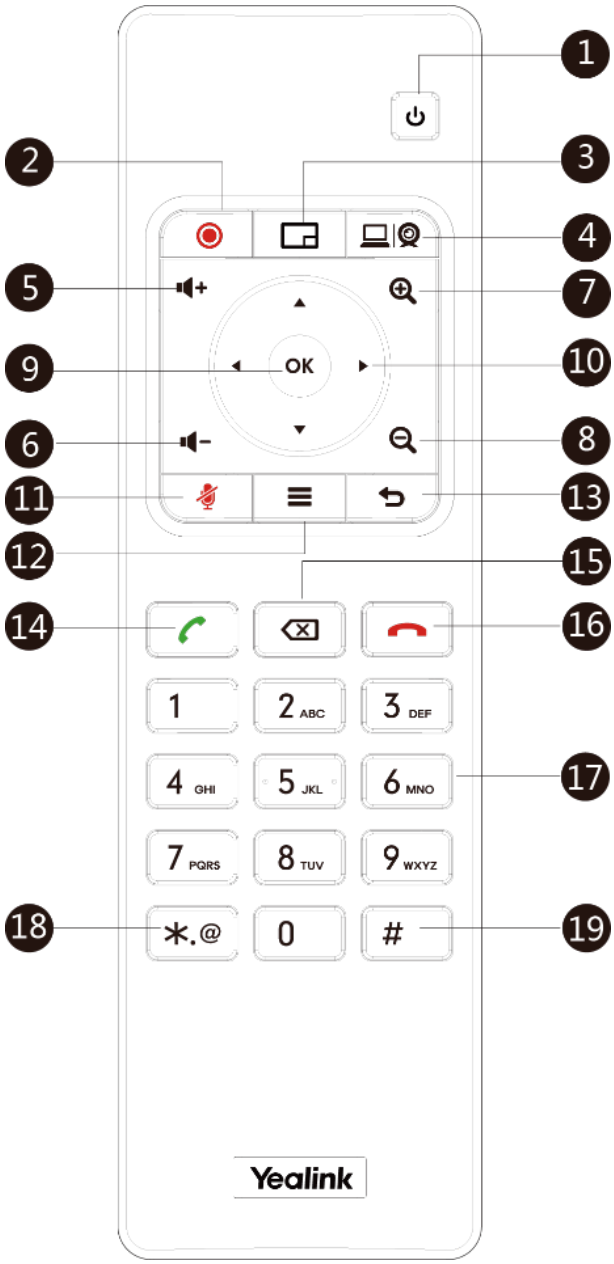
The VCR20 remote control allows you to operate a video conferencing system, including placing calls, adjusting EQ volume, controlling the camera, navigating screens, and more. The following table introduces the keys on the remote control.



	Name	Description
①	Custom Key	Customize the key function. You can configure this key as the Presentation key (default), the Tracking mode key, the ScreenShot key, the Mute Speaker key, or Cameral Control key.
②	Mute Key	Mute or unmute the microphone
③	Navigation Key	• Navigate through menu items. • Pan and tilt the camera to adjust the viewing angle.
④	Scroll Wheel (OK Key)	• Scroll up or down to the desired menu item. Press the key to go to the sub-menu or confirm actions. • Adjust the focal length of the camera: After selecting the video, scroll up or down to zoom in/out the video image.
⑤	Hang up key	• End a call or exit the current conference. • Return to the idle screen. • Long press to shut down the system or put the system to sleep. • Press it to power on the endpoint when the endpoint is shut down but not powered off.
⑥	Answer key	Go to the Pre-dialing screen, place a call or answer a call.
⑦	Back Key	Return to the previous menu.
⑧	Volume Key	Turn up/down the volume.

VCR11 Remote Control

The VCR11 remote control allows you to operate a video conferencing system, including placing calls, adjusting EQ volume, controlling the camera, navigating screens, and more. The following table introduces the keys on the remote control.



No.	Name	Description
1	Power Key	• Power on or power off the endpoint. • Put the endpoint to sleep or wake up the endpoint.
2	Video Recording Key	Start or stop recording the video and audio.
3	Layout Key	Adjust the layout during a video call.

No.	Name	Description
4	Custom Key	Customize the key function. You can configure this key as the Presentation key (default), the Input key, the ScreenShot key, Mute Speaker key, or Preset key.
5	Volume up key	Increase the speaker volume.
6	Volume down key	Turn down the speaker volume.
7	Zoom in key	• Zoom the camera in. • Zoom in the screenshot. • Turn the page up.
8	Zoom out key	• Zoom the camera out. • Zoom out the screenshot. • Turn the page down.
9	OK key	Go the sub-menu, confirm actions or answer incoming calls.
10	Navigation Key	• Navigate through menu items. • Pan and tilt the camera to adjust the viewing angle.
11	Mute Key	Mute or unmute the microphone
12	Home key	• Return to the idle screen when the endpoint is not in a call. • Open the Talk Menu during a call.
13	Back key	Return to the previous menu.
14	Off-hook Key	Go to the Pre-dialing screen, place a call or answer a call.
15	Delete Key	• Delete the text. Delete one character at a time. Long press to delete all characters in the input field. • One press to capture packets. When the device is connected to the USB flash drive, 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	• End a call or exit the current conference. • Return to the idle screen.
17	Keypad	• Enter digits. • Go to the pre-dialing screen.
18	Character Key	Enter the special characters: .@*.
19	Pound key	Enter the pound key (#).

Related information

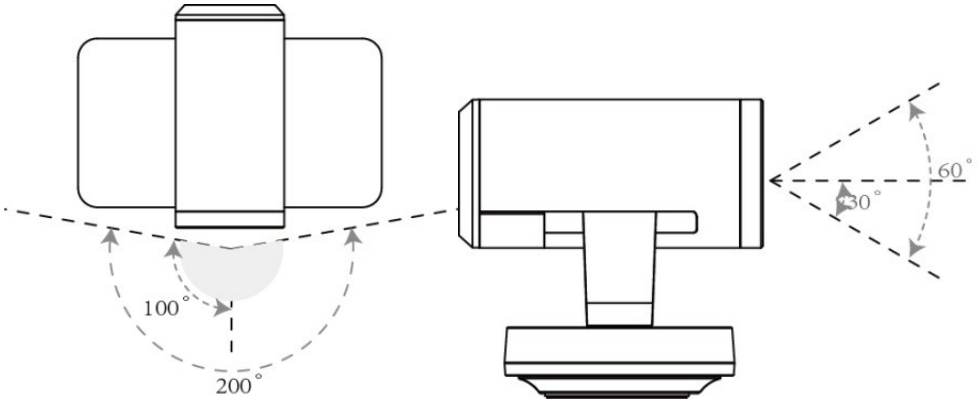
Using the Remote Control

VCC22 video conferencing camera

VCC22 is a video conferencing camera for VC880/VC800/PVT980. It adopts 12x optical zoom lens, supports 1080P/60 frame full HD video, has OSMO and PTZ function, and possesses professional video

quality and environmental adaptability. You can connect up to 9 VCC22 video conferencing cameras to the VC880/PVT980 video conferencing system, and 8 to VC800 video conferencing system.

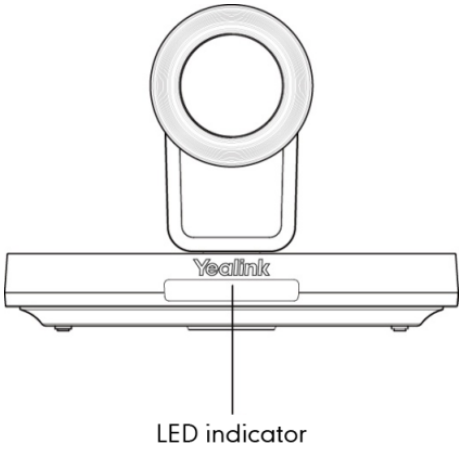
The VCC22 camera can be panned (± 100 degrees range), tilted (± 30 degrees range) and supports 12 x optical zoom, white balance and automatic gain.



- Front Panel of VCC22 Video Conferencing Camera
- Rear Panel of VCC22 Video Conferencing Camera

Front Panel of VCC22 Video Conferencing Camera

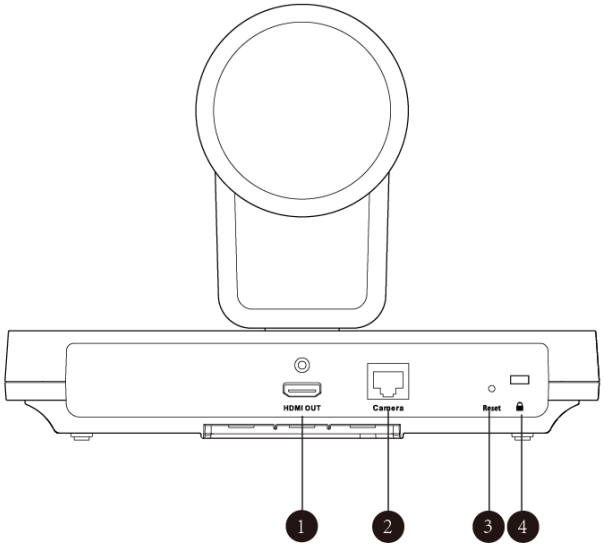
The LED indicator in front of the camera indicates different camera status.



Related information

LED Instructions of VCC22 Video Conferencing Camera

Rear Panel of VCC22 Video Conferencing Camera



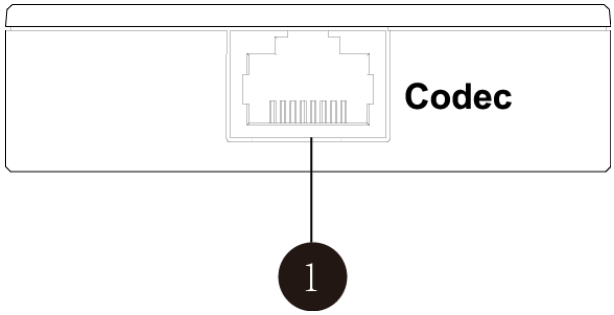
	Port Name	Description
1	HDMI Out	Connect to a monitor for displaying shared content.
2	Camera Port	Connect to a PoE switch.
3	Reset Key	Reset the camera to factory defaults.
4	Security Slot	Allow you to connect a universal security cable to VCC22, so you can lock it down. The camera cannot be removed when locked.

Hardware of VCH50 Video Conferencing Hub

You can connect VCH50 to the computer for presenting. If you want to connect a PC to your system using Ethernet cable, you need to connect the VCH50 video conferencing hub to your system. Connecting VCH50 to the computer for presenting is not applicable to VP59.

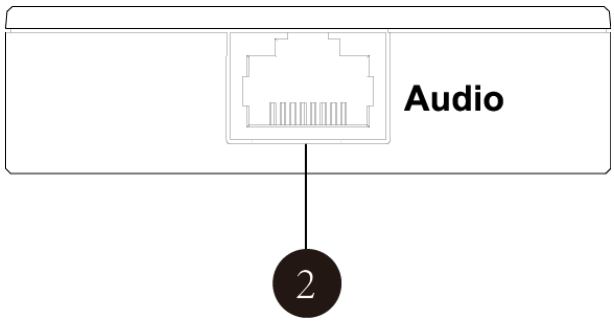
- Left Side of VCH50 Cable Hub
- Right Side of VCH50 Cable Hub
- Rear Panel of VCH50 Cable Hub

Left Side of VCH50 Cable Hub



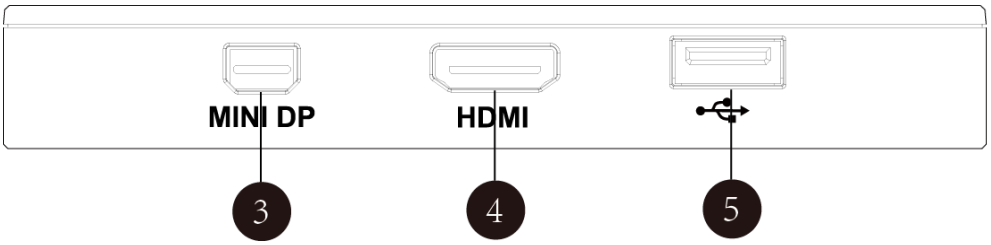
	Port Name	Description
1	Codec	Connect to the video conferencing system via the provided 7.5m network cable.

Right Side of VCH50 Cable Hub



	Port Name	Description
2	Audio	Connect to the CP960 Conference phone via the provided 0.5m network cable.

Rear Panel of VCH50 Cable Hub



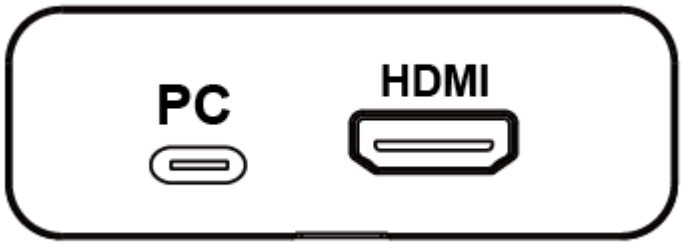
	Port Name	Description
3	MINI DP	Connect to PC via Mini-DP cable for sharing contents.
4	HDMI	Connect to PC via HDMI cable for sharing contents.
5	USB	Insert a USB flash drive. USB flash drive can be used for storing screenshots, recorded videos or captured packets.

Hardware of VCH51 Video Conferencing Hub

You can connect VCH51 to the computer for presenting. If you want to connect a PC to your system using Ethernet cable, you need to connect the VCH50 video conferencing hub to your system. Connecting VCH51 to the computer for presenting is not applicable to VP59.

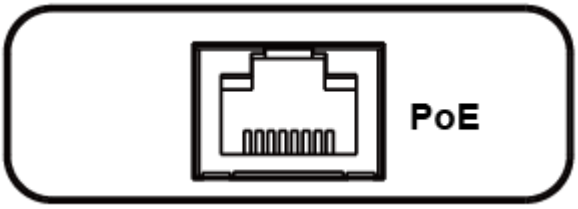
- Left Side of VCH51 Cable Hub
- Right Side of VCH51 Cable Hub

Left Side of VCH51 Cable Hub



	Port Name	Description
1	PC port	Connect to PC via Type-C cable for content sharing.
2	HDMI	Connect to PC via HDMI cable for sharing contents.

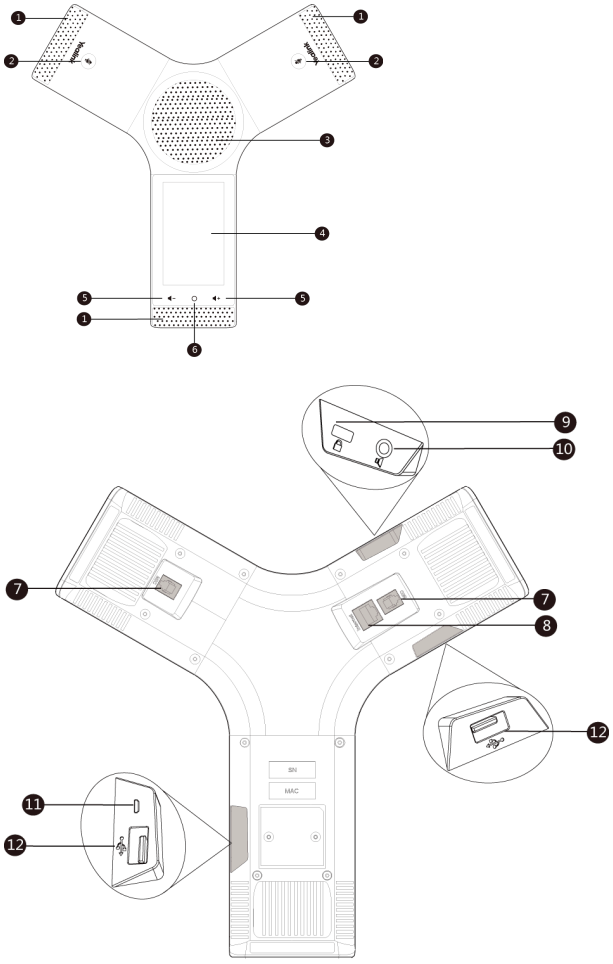
Right Side of VCH51 Cable Hub



	Port Name	Description
1	PoE	Connect to the VC Hub/Phone port on the VCS codec or to the PoE.

CP960 Conference Phone

You can use CP960 conference phone as a microphone and a speaker when you are using MeetingEye 600/MeetingEye 400/VC200/VC500/VC800/VC880/PVT980/PVT950 to place calls. You can also place calls, answer calls or view directory and history on CP960.

CP960 Conference Phone	No.	Name	Description
	1	Three Internal Microphones	Support 360-degree audio pickup at a radius of up to 6 meters.
	2	Mute Key	• Indicate the status of the device and the call. • Toggle mute feature.
	3	Speaker	Provide audio output.
	4	Touch Screen	5 inch (720 x 1280) capacitive (5-point) touch screen.
	5	Volume Touch Keys	Adjust the volume of the speaker, ringer or media.
	6	HOME Touch Key	Return to the idle screen.
	7	Wired Mic Ports	Allow you to connect CPE90 to your phone (optional).
	8	Internet	• Connect to the VC Hub/Phone port on the video conferencing system. • Connect to the Audio port on the VCH50 video conferencing hub.
	9	Security Slot	Allow you to connect a universal security cable to your phone so you can lock down your phone. The phone will not be removed after locked.
	10	3.5mm Audio-out Port	This port is unavailable when CP960 works with the video conferencing system.

CP960 Conference Phone	No.	Name	Description
	11	Micro USB Port	This port is unavailable when CP960 works with the video conferencing system.
	12	USB	• Insert a USB flash drive. USB flash drive can be used for storing screenshots, recorded videos or captured packets. If you insert multiple USB flash drives to the VCS endpoint simultaneously, only the last USB flash drives you insert can be identified by the endpoint.

Related information

Mute Indicator LED of CP960 Conference Phone

CTP20 Touch Panel

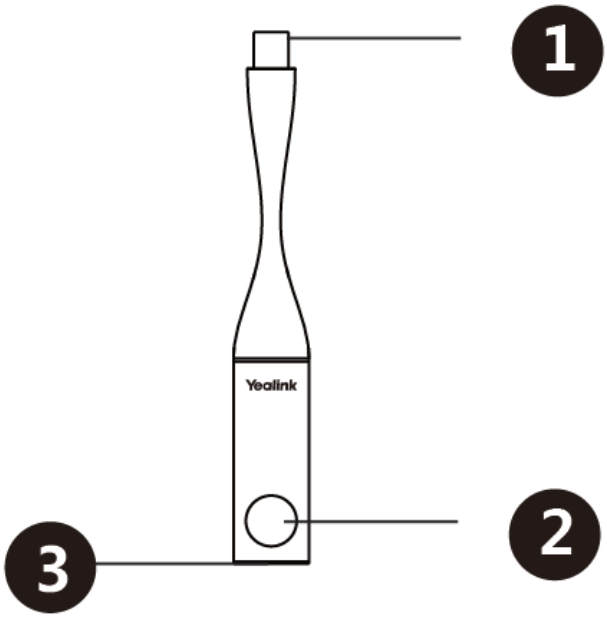
As the controller of VCS endpoints, CTP20 touch panel can help you fully control the VCS endpoints. You can use it to place calls, initiate conferences, adjust the volume, control the camera, record videos, and so on. What's more, CTP20 supports collaborative editing and the annotation, that is to say, participants can add notes to the presentation or to the whiteboard, which can improve the communication efficiency of the traditional video conferencing presentation.

Related information

Using CTP20

WPP20 wireless presentation pod

Combining a self-built 5G Wi-Fi, WPP20, the wireless presentation pod, partners up with Yealink new-generation video conferencing system to offer high-quality wireless content sharing with just one tap.



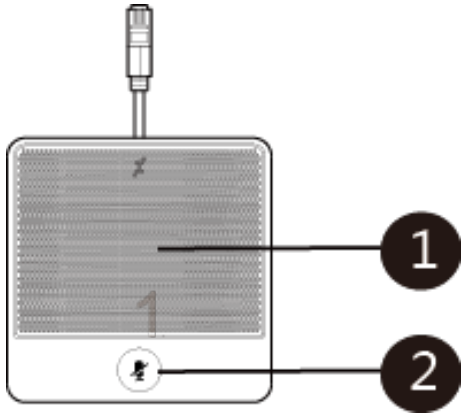
	Name	Description
1	USB	Connects to the video conferencing system to obtain Wi-Fi profile. Connects to the PC for sharing content.
2	Presentation Button	Presses it to start or to stop sharing the full screen of the PC. Long presses it for 3 seconds and release it, and then choose the window you want to share.
3	LED Indicator	Indicates the status.

Related information

LED Instructions of WPP20 Wireless Presentation Pod

Hardware of CPE90 Wired Expansion Microphones

The CPE90 can work as expansion microphones of the CP960 conference phone. It supports 360-degree audio pickup at a radius of up to 3 meters. You can connect 2 CPE90s to CP960 at most via MIC ports.



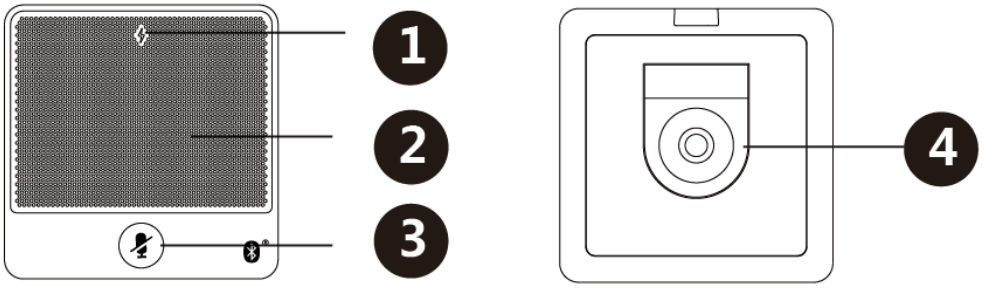
	Name	Description
1	Built-in Microphone	Supports 360-degree audio pickup at a radius of up to 3 meters.
2	Mute Key	• Indicates call status. • Toggle mute feature.

Related information

Mute Indicator LED of CPE90 Wired Expansion Microphones

Hardware of CPW90-BT Bluetooth Wireless Microphone

CPW90-BT can expand the voice pick-up range, providing an optimal audio experience. You can connect up to 2 CPW90-BTs to the VCS endpoint.



	Name	Description
1	Power Indicator LED	Indicates the battery information.
2	Built-in Microphone	Supports 360-degree audio pickup at a radius of up to 3 meters.
3	Mute Key	• Indicates call status. • Toggle mute feature.
4	Charging Slot	Put the CPW90-BT on the charging cradle to charge.

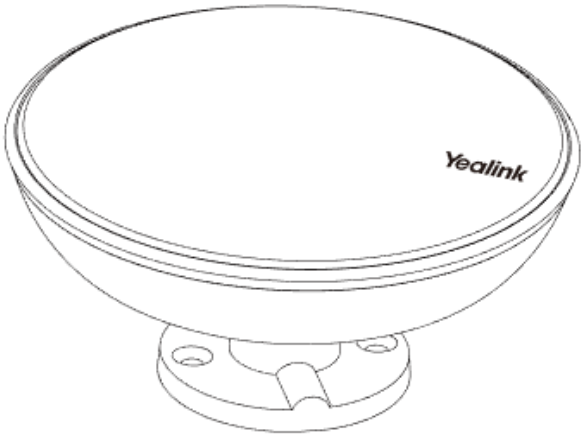
Related information

Battery Indicator LED

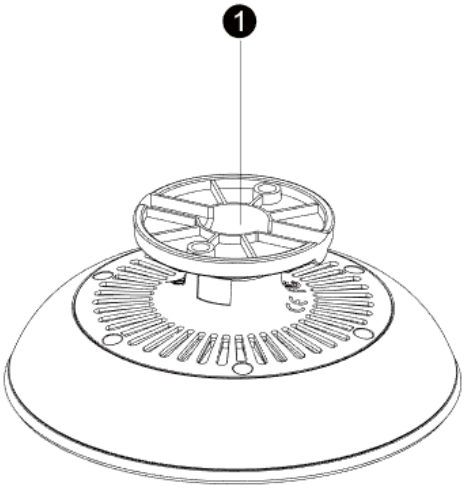
VCM38

VCM38 is a newly designed ceiling microphone with 8 built-in microphones, which can realize 360° voice pickup range. VCM38 delivers excellent voice quality with high-quality echo cancellation and Yealink noise proof technology. With Beamforming technology, VCM38 can automatically locate and optimize voice pick up for the person speaking.

Front Panel of VCM38



Rear Panel of VCM38

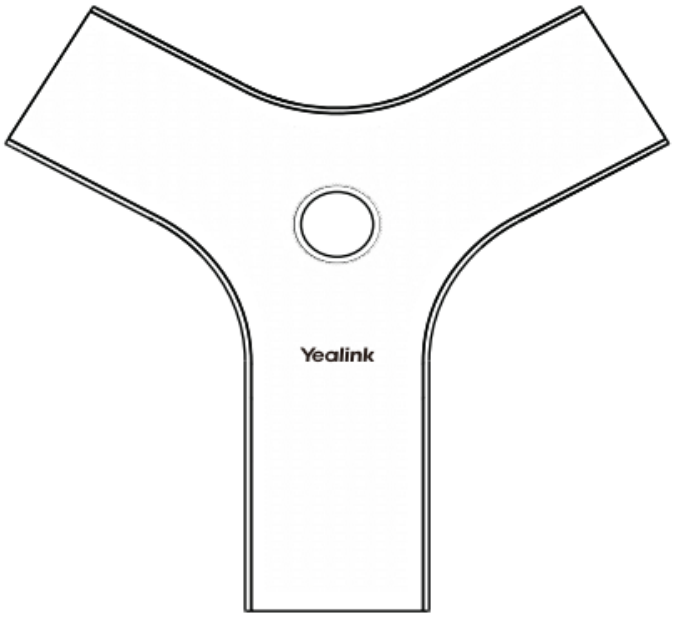


	Name	Description
1	PoE	Connect to the VC Hub/Phone port on the VCS endpoint.

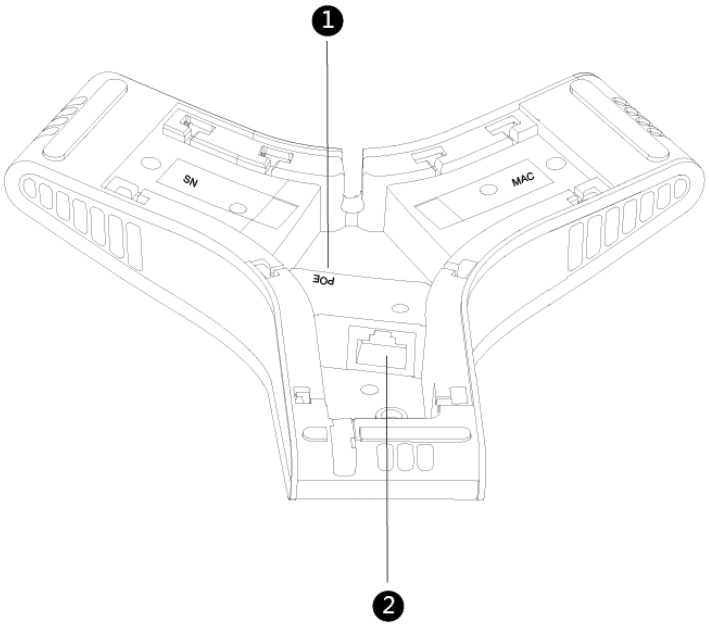
VCM34

VCM34 is a brand-new video conferencing microphone array which can work as the audio input device for Yealink Video Conferencing System. Thanks to its built-in 3-microphone array and superior audio technology, VCM34 owns a 20ft (6m) and 360° voice pickup range.

Front Panel of VCM34



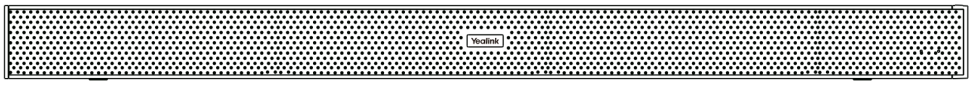
Rear Panel of VCM34



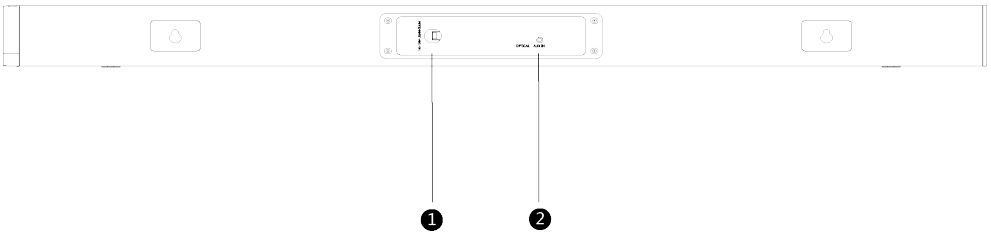
	Name	Description
1	PoE	Connect to the VC Hub/Phone port on the VCS endpoint.
2	Internet	It is used to connect VCM34.

Hardware of MSpeaker

Front Panel of MSpeaker



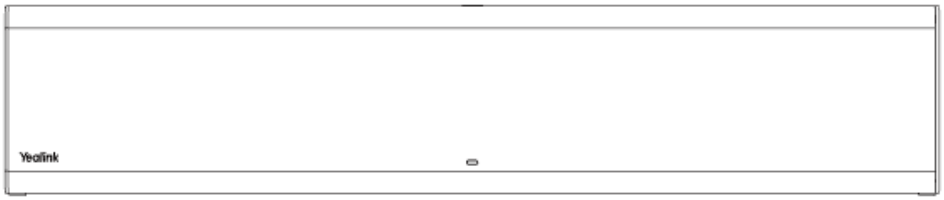
Rear Panel of MSpeaker



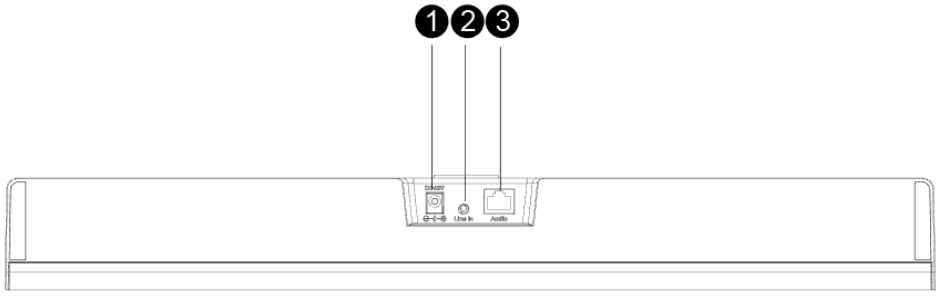
	Name	Description
1	Power Input	It is used to connect MSpeaker to the power adapter.
2	AUX In	It is used to connect MSpeaker to VC800 Line Out Port as an audio input.

Hardware of MSpeaker II

Front Panel of MSpeaker II



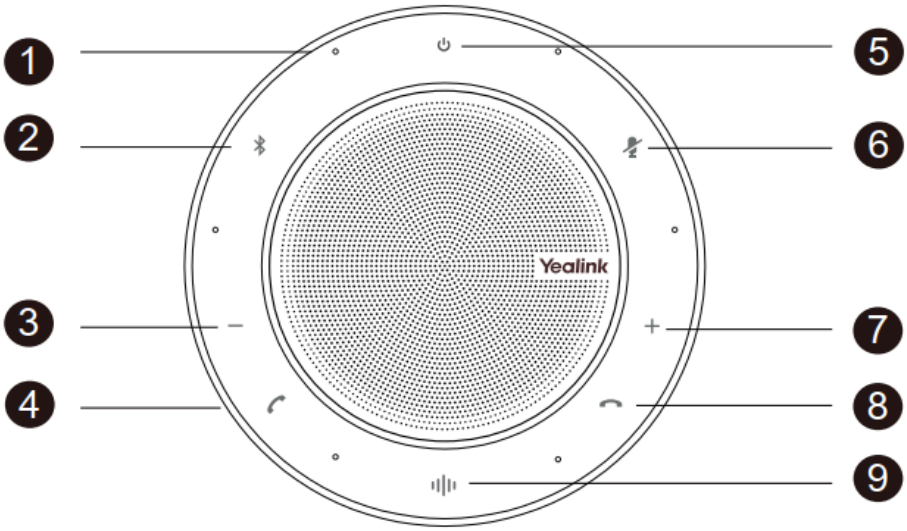
Rear Panel of MSpeaker II



	Name	Description
1	Power Input	It is used to connect MSpeaker to the power adapter.
2	Line In	It is used to connect MSpeaker II to the Line Out Port as an audio input.
3	Audio	It is used to connect MSpeaker to the VC Hub/Camera Port as an audio input.

CP900/CP700 Ultra-Compact Speakerphone

After you connect CP900/CP700 to VP59 via a USB cable, VP59 will automatically take CP900/CP700 as audio input or output device. You can use CP900/CP700 to control the call on VP59, adjust the volume, and set the mute status.



	Name	Description
1	Microphone	Provide optimal voice pickup performance.
2	Bluetooth Button	Enable/disable the Bluetooth. Tap it for 2 seconds to enable the pairing mode, then CP900/CP700 can search for and connect to a device. Double-tap to disconnect. Tap again to reconnect.
3	Volume Down	Tap to turn down the volume. **Note:** If you do not use the handset and headset, the volume of CP900/CP700 is synchronized with the one of VP59.
4	Answer Call	Answer the call; tap it for 6 seconds to reset CP900/CP700 to factory.
5	Power On/Off	Power on/off CP900/CP700.
6	Mute Key	Mute/unmute the microphone. **Note:** If you do not use the handset and headset, the mute status of CP900/CP700 is synchronized with the one of VP59.
7	Volume Up	Tap to turn up the volume. **Note:** If you do not use the handset and headset, the volume of CP900/CP700 is synchronized with the one of VP59.
8	End Call	Hand up the call or reject an incoming call; tap it for 6 seconds to reset CP900/CP700 to factory.
8	Voice Assistant Button	Enable the voice assistant.

LED Instructions

You can know the system status by viewing the LED light.

- MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/ PVT950 LED Indicator
- Power Indicator LED of VP59
- Camera Indicator LED of VP59
- LED Instructions of VCC22 Video Conferencing Camera
- LED Instructions of CTP20
- Mute Indicator LED of CP960 Conference Phone
- Mute Indicator LED of CPE90 Wired Expansion Microphones
- LED Instructions of CPW90-BT Bluetooth Wireless Microphones
- LED Instructions of WPP20 Wireless Presentation Pod

MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/ PVT950 LED Indicator

LED Status	Description
Solid green	The system is powered on.
Solid red	The system is in sleep mode.
Flashing red	The system codec is upgrading firmware.
Solid orange	System exception (for example: network unavailable, update failure).
Off	The system is powered off, or is not connected to the power adapter.

Power Indicator LED of VP59

LED Status	Description
Solid red	The phone is initializing.
Fast flashing red (0.3s)	The phone is ringing.
Slowly flashing red (1s)	The phone receives a missed call.
Solid red for 0.5s and off for 3s alternately	The phone is in power-saving mode.

Camera Indicator LED of VP59

LED Status	Description
Solid green	The phone is powered on and the camera is available. The camera is idle. The phone receives an audio-only call.
Fast flashing green	The phone receives a video call.

LED Status	Description
Solid red	There is an active video call.
Slowly flashing red	The shutter switch is open, but the local video is disabled during a video call.
Off	The phone is powered off. The camera is not properly connected to the phone. The shutter switch is closed.

LED Instructions of VCC22 Video Conferencing Camera

LED Status	Description
Solid green	The VC880/VC800/PVT980 system is powered on.
	The VC880/VC800/PVT980 is upgrading firmware.
	The VCC22 video conferencing camera is working.
Solid red	The VC880/VC800/PVT980 system is in sleep mode.
	The VCC22 video conferencing camera is disabled.
Flashing red	The VCC22 video conferencing camera is upgrading firmware.
Solid orange	The VCC22 video conferencing camera is not selected.
Off	The VCC22 video conferencing camera is not connected to the PoE switch.

LED Instructions of CTP20

LED Status	Description
Solid green	VCS codec is powered on.
Solid red	CTP20 is in sleep mode.
Solid orange	CTP20 is not connected to VCS codec.

Mute Indicator LED of CP960 Conference Phone

LED Status	Description
Solid red	The CP960 conference phone is initializing.
	The CP960 conference phone is muted.
Flashing red	The CP960 conference phone is ringing.
Solid green	The CP960 conference phone is placing a call.
	The CP960 conference phone is in a call and unmuted.
Off	The CP960 conference phone is idle.
	The CP960 conference phone is disconnected to the video conferencing system.

Mute Indicator LED of CPE90 Wired Expansion Microphones

LED Status	Description
Solid red	The CP960 conference phone is muted.
Flashing red	The CP960 conference phone is ringing.
Solid green	The CP960 conference phone is placing a call.
	The CP960 conference phone is in a call and unmuted.
Off	The CP960 conference phone is idle.
	The CPE90 is disconnected to CP960 Conference Phone.

LED Instructions of CPW90-BT Bluetooth Wireless Microphones

- Battery Indicator LED
- Mute Indicator LED

Battery Indicator LED

LED Status	Description
Solid green for one second and then off	The CPW90-BT is powered on.
Solid green for 3 seconds and then off	The CPW90-BT is in the idle mode.
Solid green	The CPW90-BT is fully charged.
Solid red	The CPW90-BT is being charged.
Fast flashing red 3 times and then off	The battery capacity is too low to turn on the CPW90-BT.
Slowly flashing red	The battery capacity is less than 10%.
Off	If you tap the mute button and the power indicator LED on the CPW90-BT is still off, it means the CPW90-BT is powered off.

Mute Indicator LED

LED Status	Description
Slowly flashing yellow	The CPW90-BT is searching
Fast flashing yellow	The CPW90-BT is in the pairing mode.
Solid red	The system is muted.
Solid green	The system can pick voice.
Slowly flashing red	The system is receiving an incoming call.
Flashing red and green alternately	The VCS is searching for the CPW90-BT which has registered with it.
Off	The CPW90-BT is in the idle mode.

LED Instructions of WPP20 Wireless Presentation Pod

LED Status	Description
Fast flashing green	The WPP20 is starting up.
	The WPP20 is trying to pair to the video conferencing system.
	The WPP20 is plugged into the video conferencing system, and firmware update is in progress.
	The WPP20 is plugged into the video conferencing system, and the WPP20 is updating Wi-Fi profile.
Slowly flashing green	The WPP20 pairs to the video conferencing system successfully, but you are not sharing content.
Solid green	The WPP20 pairs to the video conferencing system successfully, and you are sharing content.
	Firmware update is done.
	Wi-Fi profile update is done.
Slowly flashing red	The WPP20 cannot find or connect to the video conferencing system in 10 seconds after start-up.
	The WPP20 pairs to the video conferencing system successfully, but it does not detect that the Yealink Wireless Presentation Pod software is running on your PC.
	Yealink Wireless Presentation Pod software is turned off.
	Firmware update fails.
	Wi-Fi profile update fails.

Powering on and off

- Powering on MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/PVT950
- Powering off MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/ PVT950
- Powering on or Powering off VP59
- Initialization Process Overview

Powering on MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/ PVT950

Your system starts up automatically after you connect an electrical supply. If you power off the system or the system goes to sleep mode, do the following to power it on.

Procedure

On your VCR11 remote control, press .

For VCR20 Remote Control, press .

Your system is powered on successfully, and the LED indicator glows green.

Powering off MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/PVT950

Procedure

1. On your VCR11 remote control, press .

   For VCR20 Remote Control, long press .
2. Select **Shut down**.
   The system shuts down immediately, and the LED on the system goes out.

Powering on or Powering off VP59

VP59 powers on automatically after you connect an electrical supply, and it powers off when you disconnect an electrical supply.

Initialization Process Overview

Once connected to the network and an electrical supply, the system begins initializing.

- Loading the ROM File
- Configuring the VLAN
- Querying the DHCP Server

Loading the ROM File

The ROM file, came with the system, is stored in the system flash memory. During initialization, the system runs a bootstrap loader that loads and executes the ROM file.

Configuring the VLAN

If you connect the system to a switch, the switch notifies the system of the VLAN information defined on the switch. The system can then proceed with the DHCP request for its network settings (if using DHCP).

Querying the DHCP Server

The system is capable of querying a DHCP (Dynamic Host Configuration Protocol) server. After establishing network connectivity, the system can obtain the following network parameters from the DHCP server during initialization:

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

By default, the system obtains these parameters from a DHCPv4. If the DHCP server does not supply some of the above parameters, you can configure them manually.

Running the Setup Wizard

The setup wizard appears on the monitor when you initialize the system for the first time or when you reset the system to factory. You can select the desired language via your remote control or CTP20, and configure the following features according to the setup wizard.

Menu	Description
Date & Time	The system obtains the time and date from the NTP server automatically by default. You can also configure the time and date manually.
Site Name	Edit the site name.
Password	The default administrator password is “0000”. For security reasons, you should change it as soon as possible. The new password must be at least six characters, preferably mixing with digits and letters.
Firewall Port Mapping	Displays the firewall port mapping information.
Wired Network	Your system can obtain the network settings from a Dynamic Host Configuration Protocol (DHCP) server. You can also configure network settings manually.
Wi-Fi (it only is applicable to MeetingEye 600/MeetingEye 400/VC200)	Connects to Wi-Fi.
Identity	Optional: Log into the video conferencing platform. Your system supports Yealink VC Cloud/Yealink Meeting Server/Zoom/ Pexip/BlueJeans/Videxio/Custom platform.

Configuration Methods

You can configure MeetingEye 600/MeetingEye 400/PVT980/PVT950/VC880/VC800/VC500 Pro/ VC500/ VC200 via the web user interface, the remote control, CTP20, or CP960.

For VP59, you can configure it directly or use the web user interface.

- Using Web User Interface
- Using CTP20 Touch Panel
- Using the Remote Control
- Use CP960 Conference Phone

Using Web User Interface

You can configure the VCS codec via the web user interface as an administrator or a user. For an administrator, you can configure all settings; for a user, you can only configure some basic settings and contact settings after the administrator assign the permission to you.

- Logging into the Web User Interface
- Configuring the Web Server Type
- User and Administrator Account Login

Logging into the Web User Interface

To log on to your device web user interface, you must open a web browser and enter the device IP address. Login credentials are required for accessing the web user interface. The default administrator

username is “admin” (case-sensitive) and password is “0000”. The default user name is “user” and the password is “1234”.

About this task

Note: We recommend that you use the Chrome, Internet Explorer or Firefox to access the web user interface. Some features may not work properly if you are using other or older browsers.

Table 1:

Browser	Version Requirements
Chrome	45 or later
Internet Explorer	11 or later
Firefox	52.2.9 or later

Procedure

1. Open a web browser and enter the device IP address in the address bar. For example, http(s)://10.82.24.11/, and press Enter.

   If your device is an IPv6 IP address, enter http (s): // [IP address] /.
2. Enter the administrator username and the password.
3. Click **Login**.

   Attention: The web user interface will be locked after 3 failed login attempts. Please contact your support team or try again 3 minutes later.

Related tasks

Configuring the Web Server Type

User and Administrator Account Login

Configuring the Web Server Type

The web server type determines the protocol used for accessing the web user interface of the system. Both HTTP and HTTPS are available. The HTTPS ensures that the configuration of all login information (such as user names and passwords) is transmitted using an encrypted channel. If you disable the desired protocol, you cannot access the web user interface via this protocol.

Procedure

1. Do one of the following:

   - On your web user interface, go to **Network** > **Advanced** > **Web Server**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **Web Server Type**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **Advanced Network** > **Web Server Type**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **Web Server Type**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Advanced Network** > **Web Server Type**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
HTTP	Enable or disable the user to access the web user interface via the HTTP. **Default**: On.	Web user interface Endpoint CTP20
HTTP Port	Specify the HTTP port for the user to access the web user interface. **Valid value**: Any integer from 1 to 65535. Make sure that the configured port is available. The default value is 80.	Web user interface
HTTPS	Enable or disable the user to access the web user interface by using the HTTPS. **Default**: On.	Web user interface Endpoint CTP20
HTTPS Port	Specify the HTTPs port for the user to access the web user interface. **Valid value**: Any integer from 1 to 65535. Make sure that the configured port is available. The default value is 443.	Web user interface
HTTP & HTTPS	Enable or disable the user to access the web user interface via the HTTP and HTTPS. **Default**: On.	CTP20 Endpoint (VP59)
Disabled	Disable the user to access the web user interface via the HTTP and HTTPS.	CTP20 Endpoint (VP59)

User and Administrator Account Login

- Changing the Administrator Password
- Enabling the User Type

Changing the Administrator Password

The default administrator name is “admin” and the administrator password is “0000”. Only the user with the administrator permission can change the password. For security reasons, you should change them as soon as possible. The administrator password for the system supports ASCII characters 32-126 (0x20-0x7E).

Procedure

1. Do one of the following:
   - On your web user interface, go to **Security** > **Security**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **System Settings** > **Password Reset**.

     For VP59, tap > **Settings** > **Advanced** > **System Settings** > **Password Reset**.
   - On your CTP20, tap > **Settings** > **Advanced** > **System Settings** > **Password Reset**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
User Type	Select the administrator.	Web user interface
Old Password/Current Password	Enters the old administrator password. **Default**: “0000 ”.	Web user interface Endpoint CTP20
New Password	Configure a new administrator password. **Note**: You can leave the password blank.	Web user interface Endpoint CTP20
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”.	Web user interface Endpoint CTP20

Enabling the User Type

If you enable the user type, users can access basic configurations such as contacts. The default user name is “user” and the password is “1234”.

Procedure

1. On your web user interface, go to **Security** > **Security**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
User Mode	Select User.	Web user interface
User Type	Enables the user role. **Default**: Disabled.	Web user interface
User Password (New Password and Confirm Password)	Configure a user password. **Note**: the system supports ASCII characters 32-126 (0x20-0x7E). You can also leave the password blank. **Default**: “1234 ”.	Web user interface

Using CTP20 Touch Panel

After connecting CTP20 to MeetingEye 600/MeetingEye 400/PVT980/PVT950/VC880/VC800/VC500/VC880/VC200, you can use it to configure the VCS endpoints and place calls.

Related tasks

Wired Connection to CTP20

Wireless Connection to CTP20

Using the Remote Control

You can use the real or the virtual remote control to configure the VCS endpoint and place calls. You can disable the remote control if it is not needed or not available.

Remote Control is not applicable to VP59 but you can directly do the configuration on VP59.

- Using the Virtual Remote Control
- Customizing the Key Type
- Disabling Remote Control Keys
- Remote Controller

Using the Virtual Remote Control

Except for the remote control, you can use the virtual remote control on your web user interface to control your system.

Procedure

1. On your web user interface, go to **Home** > **Remote Control**.
   The virtual remote control appears.
2. Click the corresponding keys on the remote control to control the VCS codec.
3. Click **Remote Control** to close the virtual remote control.

Customizing the Key Type

You can configure the custom key on VCR11 or on VCR20 to the desired functions as needed.

Procedure

1. On your web user interface, go to **Setting** > **Remote Control** > **Remote Control**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Custom Key Type	Specify a feature for the custom key on the remote control. • **Input**: press to select the video input source. • **ScreenShot**: press to capture screen. • **Mute Speaker**: press to mute or unmute the speaker. • **Presentation**: press to start or stop presentation. • **Tracking Mode**: press to configure the tracking mode. It is only applicable to MeetingEye 600/MeetingEye 400. **Default**: Presentation.	Web user interface

Disabling Remote Control Keys

All keys on the remote control are enabled by default. If you do not want to use some keys on the remote control, you can disable them.

Procedure

1. On your web user interface, go to **Setting** > **Remote Control**.
2. In the **Enable Remote Control Key** field, turn off the corresponding key.
3. Click **Confirm**.

Remote Controller

The remote control feature is enabled by default. If your environment does not use remote control to control the system, you can disable it.

Procedure

1. On your web user interface, go to **Setting** > **Remote Control** > **Remote Control**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Remote Controller	Disable the remote control. **Note**: the default value is On. If you select **Off**, you cannot use the real remote control or the virtual remote control to control the system.	Web user interface

Use CP960 Conference Phone

You can use the CP960 conference phone to perform calling and partial configuration tasks. For more information about how to use CP960 conference phone, refer to Yealink CP960 HD IP Conference Phone Quick Reference Guide.

Device Type Licenses and Multipoint Licenses

- Licenses
- Multipoint Licenses
- Importing Device Type License/Multipoint License

Licenses

If your system is a demo machine, namely it is used by agents to demonstrate the features to the customers. The monitor will prompt “DEMO ONLY, NOT FOR RESELL”. A demo machine supports 24-way calls (1 conference creator and 24 participants) and is valid for one year. You can change the demo machine to be a normal machine by importing a device type license, which you can get from Yealink

technical support. After changing to a normal machine, the VCS codec supports 1 video call and 5 voice calls (1 conference creator and 6 participants).

Multipoint Licenses

Only VC880/VC800/PVT980/PVT950 supports multipoint licenses. After the administrator imports the multipoint licenses to VC880/ VC800/PVT980/PVT950, you can use them to initiate multipoint video conferences.

Multipoint licenses are described as below:

Multipoint License Type	Maximum Connections	Description
MeetingEye 600/MeetingEye 400/ VC500/VC200	One-point video call with presentation and 5-point voice call (a conference organizer and 6 participants).	Multipoint video conferences are unsupported.
VC880/VC800/PVT980/PVT950 without a multipoint license		
VC880/VC800/PVT980/PVT950 with a trail multipoint license	24-point video call with presentation (a conference moderator and 24 participants)	**Period of validity**: 15-day free trial. VC880/VC800 can share this multipoint license that you can download from Yealink official website.
VC880/VC800/PVT980/PVT950 with an 8-point license	8-point video call with presentation and 5-point voice call (a conference moderator and 13 participants).	**Period of validity**: eternal. One worldwide unique license for every VC880/VC800/PVT980/ PVT950 and the license cannot be used by other devices. You can purchase the license from Yealink resellers by providing the MAC address of your VC880/ VC800/PVT980/PVT950.
VC880/VC800/PVT980/PVT950 with a 16-point license	16-point video call with presentation and 5-point voice call (a conference moderator and 21 participants).	
VC880/VC800/PVT980/PVT950 with a 24-point license	24-point video call with presentation (a conference moderator and 24 participants)	

Importing Device Type License/Multipoint License

Procedure

1. On your web user interface, go to **Security** > **License**.
2. Click the **Load License File** field.
3. Select the device type license/multipoint license from your PC.

   The file format must be *.dat.
4. Click **Upload**.

Related tasks

Viewing the Device Type

Traditional Deployment Methods

If you do not use cloud-based service, you can choose the traditional deployment method to deploy your VCS.

- Public IP Configuration
- Intranet Deployment

Public IP Configuration

For a higher demand of the audio and video, you can connect your video conferencing system to the Internet directly.

This deployment method involves a simple setup process and creates a stable network environment. However, it is more expensive due to leased line costs. This method is often used in the head office.

Intranet Deployment

- NAT
- STUN
- H.460
- Intelligent Traversal
- VPN

NAT

Many application-layer protocols, for example multimedia protocols (H.323/SIP), have the address or the port information. The address and port information included in the H.323/SIP protocol cannot be translated via the traditional NAT method and that causes some communication problems.

ALG (application layer gateway) feature on the router/firewall can help translate the address and the port of application-layer protocols, which guarantees the accuracy of the communication in the application layer.

If your router does not support ALG feature, you need to configure port forwarding on your router first, and then enable static NAT feature on your system. It can help convert the internal network address and port carried in the H.323/SIP payload to the public network address and port when communicating with the internal and external networks.

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, refer to Configuring H.460 for H.323 Protocol.

- Port Forwarding
- Configuring NAT
- Enabling Static NAT Feature for SIP Protocol

- Configuring Route Traversal

Port Forwarding

The most common scenario is deploying the VCS in an intranet (behind a firewall). You must assign a static private IP address to the VCS. In the meantime, do port forwarding on the firewall.

Port forwarding is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.

To receive a public-to-private call, you must forward the following ports to the public network on your router or firewall.

Port	Port	Static NAT/Type
H.323	1719-1720	UDP/TCP
Control and media for audio, video, content, and data/FECC	50000-51000	TCP/UDP
Web management port (optional)	443	TCP
SIP (optional)	5060-5061	TCP/UDP

Note: Forwarding the ports to the public network may cause security problems and you can prevent the endpoint from being attacked by adding a blacklist.

Related tasks

Adding Meeting Blacklist

Configuring NAT

You can use H.323 protocol to make private-to-public calls after you configure the port forwarding and enable the static NAT feature. If you want to use SIP protocol to make private-to-public calls, you also need to enable the static NAT settings for the SIP protocol.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **NAT/Firewall** > **NAT Configuration**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **NAT/Firewall** > **NAT**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **NAT/Firewall** > **NAT**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **NAT/Firewall** > **NAT**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **NAT/Firewall** > **NAT**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Static IP	Configure the static NAT type. • **Disabled**—the system does not use the NAT feature. • **Manual Control (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.	Web user interface Endpoint CTP20
NAT Public IP Address/Public IP Address	• Displays the NAT public address automatically obtained from the Yealink-supplied server if the static NAT is set to Auto. • Configure the NAT public address for the system if the static NAT is set to Manual.	Web user interface Endpoint CTP20

Related tasks

Enabling Static NAT Feature for SIP Protocol

Related information

Port Forwarding

Enabling Static NAT Feature for SIP Protocol

If you want to make private-to-public calls via SIP protocol (SIP account and SIP IP call), you need enable static NAT feature for SIP protocol.

Before you begin

Enable the static NAT feature.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call** > **NAT Traversal**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **SIP IP Call** > **NAT Traversal**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Advanced** > **Account** > **SIP IP Call** > **NAT Traversal**.

     For VP59, tap > **Settings** > **Advanced** > **Account** > **SIP IP Call** > **NAT Traversal**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **SIP IP Call** > **NAT Traversal**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
NAT Traversal	Select the static NAT.	Web user interface Endpoint CTP20

Related tasks

Configuring NAT

Related information

Port Forwarding

Configuring Route Traversal

In the Intranet, if there is a secondary router connected to the first router, the VCS connected to each router may not be able to communicate properly. In this situation, you can configure static NAT and enable the route traversal feature forcibly for the VCS connected to the secondary router, so that the NAT works even though both devices are in the Intranet.

Before you begin

Enable the static NAT feature.

About this task

⚠ **Attention:** If you enable the route traversal feature forcibly for the VCS connected to the secondary router, the VCS may fail to call other VCS connected to the same router, because the NAT address replaces the private address.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **NAT/Firewall** > **NAT Configuration**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **NAT/Firewall** > **NAT**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **NAT/Firewall** > **NAT**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **NAT/Firewall** > **NAT**.
   - On your CTP20 tap > **Settings** > **Network Setting** > **Host Network** > **NAT/Firewall** > **NAT**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Static IP	Select **Manual**/**Manual Settings**, and then configure the NAT address manually.	Web user interface Endpoint
NAT Public IP Address/Public IP Address	Configure the NAT address for the system manually.	Web user interface Endpoint
Route Traversal	Configure the route traversal type. • **Auto**—NAT works only when making a call to a public address. NAT does not work when making a call to a private address. • **Compulsion**—NAT works whatever you are making a call to a public address or private address. **Default**: Auto.	Web user interface

3. Apply the route traversal settings to the SIP protocol.

Related tasks

Enabling Static NAT Feature for SIP Protocol

Configuring NAT

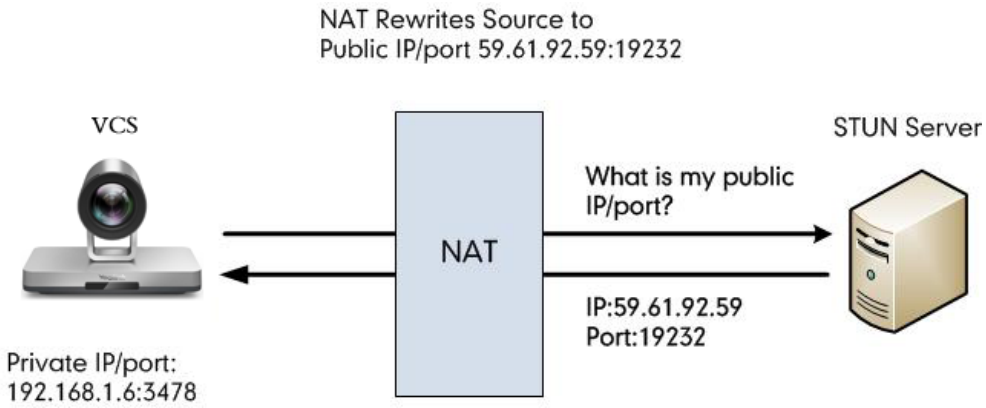
STUN

If you want to use the VCS in the intranet to place calls to the VCS in the extranet, you can use STUN server, as well as configure ALG on the router or enable static NAT on the system.

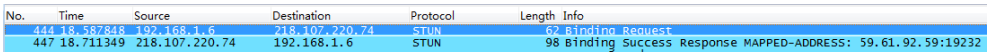
STUN is a client/server protocol, which allows the system behind a NAT to discover the NAT presence firstly, and the mapped public IP address, and then the port number that the NAT has allocated for the UDP flows to remote parties. Those information is used to establish UDP communication between two system behind the NATs.

STUN is a client/server protocol. The system works as a STUN client, sending exploratory STUN messages to the STUN server. After that, the STUN server uses those messages to determine the public IP address and the port (which is used to connect the public network to the intranet), and then informs the client. For more information, refer to RFC3489.

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



The system will send SIP message using the mapped IP address and the port.



Note:

STUN does not enable the incoming TCP connections through NAT, so H.323 is not supported. And STUN does not support the incoming UDP packets through symmetric NAT.

- Configuring STUN
- Enabling STUN Feature for SIP Protocol

Configuring STUN

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **NAT/Firewall** > **STUN Config**.
   - On your VCS: go to **More** > **Settings** > **Network** > **Wired Network** > **NAT/Firewall** > **STUN Config**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **NAT/Firewall** > **STUN Config**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **NAT/Firewall** > **STUN Config**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **NAT/Firewall** > **STUN Config**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active/STUN Active	Enable or disable the STUN (Simple Traversal of UDP over NATs) feature on the system. **Default**: Disabled.	Web user interface Endpoint CTP20
STUN Server	Configure the IP address or the domain name of the STUN (Simple Traversal of UDP over NATs) server. **Note**: the default value is blank.	Web user interface Endpoint CTP20
STUN Port	Configure the port of the STUN (Simple Traversal of UDP over NATs) server. **Default**: 3478.	Web user interface Endpoint CTP20

Enabling STUN Feature for SIP Protocol

If you want to make private-to-public calls via SIP protocol (SIP account and SIP IP call), you can enable STUN feature for SIP protocol.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call** > **NAT Traversal**.
   - On your VCS, go to **More** > **Settings** > > **Advanced** > **Account** > **SIP IP Call** > **NAT Traversal**.

     For VP59, tap > **Settings** > **Advanced** > **Account** > **SIP IP Call** > **NAT Traversal**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **SIP IP Call** > **NAT Traversal**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
NAT Traversal	Select STUN.	Web user interface Endpoint CTP20

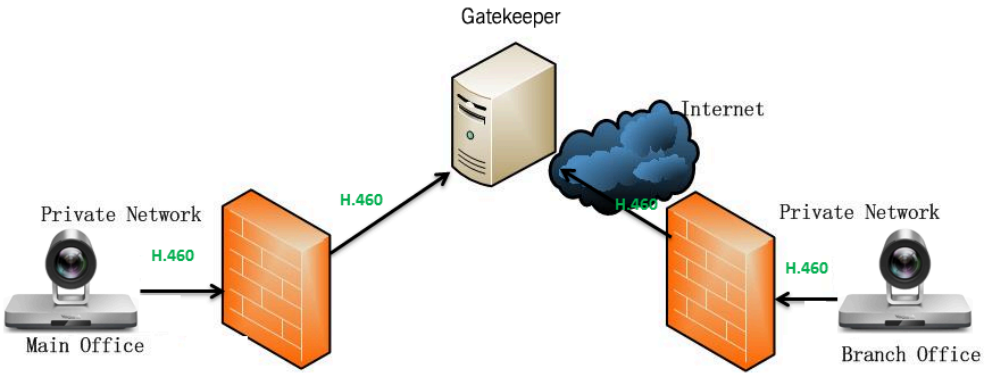
Related tasks

Setting SIP Account/SIP IP Call

Configuring NAT

H.460

VCS allows the firewall traversal of H.323 calls via H.460 protocols. To use this feature, make sure your gatekeeper supports H.460 feature.



Note:

If you configure H.323 settings and enable H.460 support, the system ignores the static NAT settings automatically.

- Configuring H.460 for H.323 Protocol

Configuring H.460 for H.323 Protocol

If you want to make private-to-public calls via H.323 protocol, you can enable H.460 feature for H.323 protocol.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **H.323** > **H.460 Active**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **H.323** > **H.460**.

     For VP59, tap > **Settings** > **Advanced** > **Account** > **H.323** > **H.460**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **H.323** > **H.460**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
H.460 Active	Enable or disable H.460 firewall traversal for H.323 calls. **Default**: Disabled.	Web user interface Endpoint CTP20

Related tasks

Setting H. 323 Account/H.323 IP Call

Intelligent Traversal

Some branch offices lack IT professionals, which means that professional network configuration (for example, the port forwarding) may be impossible. To solve this issue, Intelligent Traversal allows you to simply deploy your VCS in the intranet, and assign an IP address to VCS, which can be used to access the public network. After that you can place calls to the VCS in the public network via your intranet VCS.

This type of deployment is simple to deploy, plug and play, and does not require complex network configuration. However, this method is not applicable to the incoming calls.

- Configuring Audio & Video Intelligent Traversal
- Configuring Data Intelligent Traversal

Configuring Audio & Video Intelligent Traversal

About this task

When a VCS in the intranet calls the VCS in the public network, the audio & video streams send by the VCS in the intranet may carry the intranet IP addresses, as a result, the VCS in the public network fails to send the audio& video streams to the VCS in the intranet. Besides, the problem of one-way audio or video and no image of the VCS in the public network may occurs to the VCS in the intranet. The above problems can be solved by the feature of audio & video intelligent traversal.

This feature allows the VCS in the public network to check the media source address and the port of incoming RTP packets, and then send the RTP packets back to the address where the incoming RTP packet comes from rather than the address provided in the Session Description Protocol (SDP).

The following example illustrates a scenario about using the audio & video intelligent traversal:

The VCS A locates in the intranet with the feature of audio & video intelligent traversal enabled, and the router does not support the ALG feature. The VCS B locates in the public network. A calls B, and then A sends the RTP packets to the B.

- If B disables the audio & video intelligent traversal feature, B will send RTP data to the negotiated IP address of A (private IP address provided in the Session Description Protocol), as a result, A may see black screen.
- If B enables the audio & video intelligent traversal feature, B sends back RTP packets to the address where incoming RTP packet comes from. A and B can communicate normally.

Procedure

1. On your web user interface, go to **Network** > **NAT/Firewall** > **Audio&Video Intelligent Traversal**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Audio&Video Intelligent Traversal	Enable or disable the audio & video media stream to traverse firewall. **Default**: On.	Web user interface

Configuring Data Intelligent Traversal

About this task

When VCS in the Intranet calls the VCS in the public network, the VCS in the Intranet may fail to receive data (for example: PC content and FECC protocol) from the public network. You can use data intelligent traversal to solve these problems.

The following example illustrates a scenario about using data intelligent traversal:

The VCS A locates in the Intranet and the router supports the ALG feature. The VCS B locates in the public network.

The ALG feature on the router can temporarily map the port to a public port, which lasts 30 seconds by default. If the VCS B in the public network does not share content within 30 seconds, the mapped port will change, so that the VCS B may fail to share content with VCS A later. To solve this problem, enable the data intelligent traversal on VCS A, the VCS A will send keep-alive messages at regular intervals to keep the port open. Therefore, the VCS B can share content normally.

Procedure

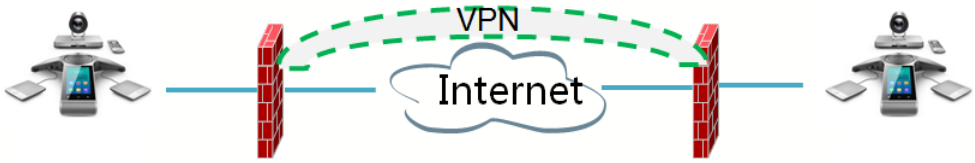
1. On your web user interface, go to **Network** > **NAT/Firewall** > **Data Intelligent Traversal**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Data Intelligent Traversal	Enable or disable the PC content and FECC protocol to traverse firewall. **Default**: On.	Web user interface

VPN

The VPN (Virtual Private Network) technology establishes a private tunnel on the public network through key exchange, encapsulation, authentication and encryption, to ensure the integrity, privacy, and validity of the transmitted data. VCS uses OpenVPN to achieve VPN feature. To prevent disclosure of private information, tunnel endpoints must authenticate each other before the secure VPN tunnel is established. After you configure VPN feature on the system, the system will act as a VPN client and uses the certificates to authenticate with the VPN server.

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



- Related VPN Files
- Configuring VPN

Related VPN Files

To use VPN, you should upload the compressed package of VPN-related files to the system in advance. The file format of the compressed package must be *.tar. The related VPN files are certificates (ca.crt and client.crt), key (client.key), and the configuration file (vpn.cnf) of the VPN client.

The following table lists the directories of the OpenVPN certificates, the key and the configuration file:

VPN files	Description	Unified Directories
ca.crt	CA certificate	/config/openvpn/keys/ca.crt
client.crt	Client certificate	/config/openvpn/keys/client.crt
client.key	Private key of the client	/config/openvpn/keys/client.key

Configuring VPN

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Advanced** > **VPN**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **VPN**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **Advanced Network** > **VPN**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **VPN**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Advanced Network** > **VPN**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active/ **VPN**	Enable or disable VPN feature on the system. **Note**: the default value is Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Upload VPN Config	Upload the compressed package of VPN-related files (*.tar) to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Cloud Deployment Method

When holding a video conference, customers may encounter several problems, such as no public IP address, weak network infrastructure, complicated firewall configuration, inefficient deployment and no traversal server.

Cloud-based technology drives positive changes in the way of organizational communication. With video conference platform, organizations can communicate easily because the public IP address and the complex network settings are unnecessary. Challenges such as infrastructure costs and interoperability are also eliminated. Both the head office and the branch offices can use the cloud deployment method. Besides, both the inbound and the outbound calls are available.

Related information

Configuring the Video Conference Platform Account

Configuring Network Settings

The following introduces how to configure network settings.

- Configuring IPv4 or IPv6
- Setting the Wireless Network
- Wireless Access Point
- Configuring DNS Server
- DHCP Options
- Configuring LLDP
- Configuring VLAN Manually
- Configuring DHCP VLAN
- 802.1x Authentication
- Enabling/Disabling the PC Port
- Network Speed and Duplex Mode
- Restricting Reserved Ports
- Quality of Service (QoS)
- Configuring MTU
- Configuring SNMP

Configuring IPv4 or IPv6

Yealink video conferencing system supports IPv4 addressing mode, IPv6 addressing mode, as well as the IPv4&IPv6 dual stack-addressing mode.

Note:

Yealink video conferencing systems comply with the DHCPv4 specifications documented in RFC 2131, and the DHCPv6 specifications documented in RFC 3315.

- Configuring IP Addressing Mode
- Configuring IPv4
- Configuring IPv6

Configuring IP Addressing Mode

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **LAN Configuration** > **Internet Port** > **IPv4/IPv6**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **IP Mode**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **IP Mode**.

     For VP59, tap > **Settings** > **Network** > **Wired Network** > **IP Mode**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wired Network** > **IP Mode**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
IP Mode/IPv6/IPv4	Configure the IP address mode. **Note**: the default mode is IPv4. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Configuring IPv4

After connected to the wired network, the system can obtain the IPv4 network settings from a Dynamic Host Configuration Protocol (DHCP) server if your network supports it. You can also configure IPv4 network settings manually.

Before you begin

Make sure that your network mode is set to IPv4 or IPv4&IPv6.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **LAN Configuration** > **IPv4 Config**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **IPv4**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **IPv4**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **IPv4** .
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wired Network** > **IPv4**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
DHCP	Enable or disable the system to obtain network settings from the DHCP server. **Note**: the default value is On. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Static IP	Enable or disable the system to use manually configured network settings. **Default**: Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
IP Address	Configure the IPv4 address assigned to the system. **Note**: It is configurable only when the network type is selected as **Static IP**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
IPV4 Subnet Mask/Subnet mask	Configure the subnet mask assigned to the system. **Note**: It is configurable only when the network type is selected as **Static IP**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Gateway/ **Default Gateway**	Configure the gateway assigned to the system. **Note**: It is configurable only when the network type is selected as **Static IP**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Static DNS	Enable or disable DNS feature. **Default**: Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Primary DNS/Pri.DNS	Configure the primary DNS server assigned to the system. **Note**: In the DHCP environment, it is configurable when the static DNS feature is enabled. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Secondary DNS/Sec.DNS	Configure the secondary DNS server assigned to the system. **Note**: In the DHCP environment, it is configurable when the static DNS feature is enabled. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Configuring IPv6

The system can automatically obtain the network parameters via DHCPv6. You can also manually configure IPv6 network. Make sure that your network environment supports IPv6.

Before you begin

Make sure that your network mode is set to IPv6 or IPv4&IPv6.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **LAN Configuration** > **IPv6 Config**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **IPv6**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **IPv6**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **IPv6** .
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wired Network** > **IPv6** .

2. Configure and save the following settings:

Parameter	Description	Configuration Method
DHCP	Enable or disable the system to obtain network settings from the DHCP server. **Note**: the default value is On. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Static IP	Enable or disable the system to manually configured IPv6 network settings. **Default**: Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
IP Address	Configure the IPv6 address assigned to the system. **Note**: It is configurable only when the network type is selected as **Static IP**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
IPv6 prefix((0~128)/ **IP prefix**	Configure the IPv6 prefix. **Note**: It is configurable only when the network type is selected as **Static IP**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Gateway	Configure the IPv6 default gateway. **Note**: It is configurable only when the network type is selected as **Static IP**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Static DNS	Enable or disable DNS feature. **Default**: Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Primary DNS/Pri.DNS	Configure the primary DNS server assigned to the system. **Note**: In the DHCP environment, it is configurable when the static DNS feature is enabled. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Secondary DNS/Sec.DNS	Configure the secondary DNS server assigned to the system. **Note**: In the DHCP environment, it is configurable when the static DNS feature is enabled. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Setting the Wireless Network

For VC880/VC800/VC500/PVT980/PVT950, you need to connect a WF50 Wi-Fi USB Dongle to the VCS endpoint for connecting to the wireless network. You can connect the MeetingEye 600/MeetingEye 400/VC200/VP59 to a wireless network directly.

- Connecting to the Wireless Network
- Viewing the Wireless Network Status
- Forgetting a Wi-Fi
- Disabling the Wi-Fi

Connecting to the Wireless Network

There are two ways to connect to the wireless network:

- Connecting to an Available Wireless Network
- Connecting to a Hidden Wireless Network

When the system connects to a wireless network, the Wi-Fi icon will display on the status bar. The Wi-Fi icon indicates the signal strength. The more arcs you see, the stronger the signal strength is.

Note: If you connect the codec to the wireless network via CTP20, make sure that CTP20 is wired to the codec.

- Connecting to the Wireless Network
- Connecting to a Hidden Wireless Network

Connecting to the Wireless Network

You can manually connect your phone to a wireless network.

Procedure

1. Do one of the following:
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wi-Fi**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wi-Fi**.

     For VP59, tap > **Settings** > **Network Setting** > **Wireless Network**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless Network**.
2. Enable **Wi-Fi**.
3. If you already enabled wireless AP, select **OK** to turn it off.
   The system will automatically search for available wireless networks in your area.
4. Select the desired wireless network (SSID) and connect to it.
   If the network is secure, enter its password in the **Password** field, and tap **Join to Network**.

Connecting to a Hidden Wireless Network

Some wireless networks do not broadcast their SSIDs, which makes them unavailable to find. In order to connect to one of those networks, you need to connect to one of them manually.

Procedure

1. Do one of the following:
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wi-Fi**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wi-Fi**.

     For VP59, tap > **Settings** > **Network Setting** > **Wireless Network**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless Network**.
2. Enable **Wi-Fi**.
3. If you already enabled wireless AP, select **OK** to turn it off.
   The system will automatically search for available wireless networks in your area.
4. Select **Other**.
5. Enter the name of the wireless network.
6. Select the desired value from the **Security Mode** drop-down menu.
7. Configure the corresponding parameters.
8. Select **Join to Network**.

Viewing the Wireless Network Status

You can view the wireless network status. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Wi-Fi** > **Wi-Fi Status**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wi-Fi** > **Wireless Status**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wi-Fi** > **Wireless Status**.
   - On your CTP20, tap > **Settings** > **System Status** > **Host System** > **Network** > **Wireless Network**.
2. View the detailed wireless network information (for example, SSID or the signal strength).

Forgetting a Wi-Fi

The device will automatically save the Wi-Fi that has been connected ever. To avoid the device connected to a saved wireless network automatically, you can configure the device not to save a Wi-Fi. Next time you need enter the Wi-Fi password to connect the Wi-Fi.

Procedure

1. Do one of the following:
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wi-Fi**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wi-Fi** > **Wi-Fi**.

     For VP59, tap > **Settings** > **Network Setting** > **Wireless Network**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless Network**.
2. Select the connected wireless network.
3. Select **Forget the Network**.

Disabling the Wi-Fi

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Wi-Fi** > **Wi-Fi Config** > **Wi-Fi**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wi-Fi**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wi-Fi** > **Wi-Fi**.

     For VP59, tap > **Settings** > **Network Setting** > **Wireless Network**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless Network**.
2. Disable the Wi-Fi.

Wireless Access Point

For VC880/VC800/VC500/PVT980/PVT950, you need to connect a WF50 Wi-Fi USB Dongle to the system for providing the wireless AP. MeetingEye 600/MeetingeEye 400/VC200/VP59 can provide wireless AP directly.

- Enabling the Wireless Access Point
- Configuring Wireless Access Point
- Viewing the Connected Devices
- Adding Connected Devices to the Blocklist
- Removing Devices from the Blocklist
- Disabling the Wireless Access Point

Enabling the Wireless Access Point

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Wireless AP**.
   - On your VCS: go to **MOre** > **Settings** > **Network Setting** > **Wireless AP** > **Wireless AP**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wireless AP** > **Wireless AP**.

     For VP59, go to > **Settings** > **Network Setting** > **Wireless AP** > **Wireless AP**.
   - If CTP20 is wired to the VCS endpoint, on your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless AP** .
2. Enable the Wireless AP.
3. If you already enabled Wi-Fi, select OK to turn it off.

Configuring Wireless Access Point

You can configure the wireless access point for the devices.

Before you begin

Make sure you enable the wireless AP.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Wireless AP** > **AP Config**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wireless AP** > **Configure AP**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wireless AP** > **Configure AP**.

     For VP59, tap > **Settings** > **Network Setting** > **Wireless AP** > **Configure AP**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless AP** > **Configure AP**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
AP Name	Configure the name of wireless AP.	Web user interface Endpoint CTP20
Security Mode	Configure the security mode of the wireless AP. • None • WPA2-PSK **Default**: WPA2-PSK.	Web user interface Endpoint CTP20
Password/AP Password	Configure the password of the wireless AP. **Note**: only when the security mode is WPA2-PSK do you need to configure this parameter.	Web user interface Endpoint CTP20
Network Sharing	Enable or disable the system to share its wired network to the connected devices. • **On**—The connected devices can use an Internet connection. • **Off**—The connected devices cannot use an Internet connection. **Default**: Disabled.	Web user interface
Frequency	Configure the frequency of the wireless AP. • 2.4G • 5G **Default**: 5G.	Web user interface Endpoint CTP20
Channel	Configure the channel of the wireless AP. **Default**: Auto.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Time (it is not applicable to MeetingEye 600/MeetingEye 400/VP59)	Configure the default time for optimizing the AP channel. • **00:00~23:00**—you can select the desired hour from 00:00 to 23:00. **Default**: Disabled. • **Optimize Wireless AP**—click this item and it will take effect automatically at the time you set.	Web user interface
AP IP Address	Configure the generation type of wireless AP address. • **Auto**—generates the wireless AP address automatically. The default network segment is 192.168.144.X. • **Manual**—If automatically generated network segment conflicts with the one you use, you can change the network segment manually. **Default**: Auto.	Web user interface
IP Address	Configure the IP address of the wireless AP. Only when the AP IP Address is manual do you need to configure this parameter.	Web user interface

Viewing the Connected Devices

Procedure

1. Do one of the following:
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wireless AP** > **AP device list**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wireless AP** > **AP device list**.

     For VP59, go to > **Settings** > **Network Setting** > **Wireless AP** > **AP device list**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless AP** > **AP device list**.
2. View the names and the MAC addresses of the connected devices.

Adding Connected Devices to the Blocklist

You can add connected devices to the blocklist, and the device is disconnected from the wireless AP.

Procedure

1. Do one of the following:
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wireless AP** > **Blacklist**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wireless AP** > **Blacklist**.

     For VP59, tap > **Settings** > **Network Setting** > **Wireless AP** > **Blacklist**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless AP** > **Blacklist**.
2. Select the desired device.

   The monitor prompts whether to move the device into blocklist.
3. Confirm the action.

   The device is disconnected from your system, and cannot be connected to the wireless AP provided by your system any more.

Removing Devices from the Blocklist

You can remove devices from the blocklist, so that the devices can connect to the wireless AP provided by the VCS endpoint.

Procedure

1. Do one of the following:
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wireless AP** > **Blacklist**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wireless AP** > **Blacklist**.
   - For VP59, tap > **Settings** > **Network Setting** > **Wireless AP** > **Blacklist**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless AP** > **Blacklist**.
2. Select the desired device.

   The monitor prompts whether to move the device into blocklist.
3. Confirm the action.

   After removed from the blocklist, the device can search and connect to the wireless AP provided by your system.

Disabling the Wireless Access Point

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Wireless AP**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wireless AP** > **Wireless AP**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wireless AP** > **Wireless AP**.

     For VP59, go to > **Settings** > **Network Setting** > **Wireless AP** > **Wireless AP**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wireless AP** .
2. Disable the wireless AP.

Configuring DNS Server

You can configure DNS server for IPv4 and IPv6 respectively. If the system obtains the network via DHCP, you can also configure the static DNS for DHCP. You can configure up to two DNS servers for the system.

About this task
If you use static IP address, static DNS is enabled by default. You can just specify the DNS server address.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **LAN Configuration** > **IPv4/IPv6**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **IPv4/IPv6**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **IPv4/IPv6**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **IPv4/IPv6** .
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Network** > **Wired Network** > **IPv4/IPv6** .
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Static DNS	Enable or disable DNS feature. **Default**: Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Primary DNS/Pri.DNS	Configure the primary DNS server assigned to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Secondary DNS/Sec.DNS	Configure the secondary DNS server assigned to the system. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Related information

Configuring IPv4 or IPv6

DHCP Options

The DHCP information with labels carries with the corresponding network and other control information. The information is called option. After connected to the network, the device will broadcast the DISCOVER request which carries the DHCP options of the network information. The DHCP server will replay the corresponding option after receiving the request.

Note:

For more information on DHCP options, refer to RFC 2131 or RFC 2132.

- Supported DHCP Option of IPv4
- DHCP Option 42, Option 2
- DHCP Option 12

Supported DHCP Option of IPv4

The following table lists the DHCP options supported by Yealink VCS in IPv4 network.

Parameter	DHCP Options	Description
Subnet Mask	1	Specify the subnet mask of the client.
Time Offset	2	Specify the offset between the client subnet and the Coordinated Universal Time (UTC).
Router	3	Specify a list of IP addresses for routers on the client's subnet.
Time Server	4	Specify a list of time servers available to the client.
Domain Name Server	6	Specify a list of domain name servers available to the client.
Host Name	12	Specify the name of the client.
Domain Server	15	Specify the domain name that client should use when resolving hostnames via DNS.
Network Time Protocol Servers	42	Specify the list of NTP server address available to the client.
Vendor-Specific Information	43	Identify the vendor-specific information.

Parameter	DHCP Options	Description
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.

DHCP Option 42, Option 2

Your system can obtain the NTP server address via DHCP.

DHCP option 42 is used to obtain the available NTP server list.

DHCP option 2 is used to specify the offset (seconds) between the system's subnet and Coordinated Universal Time (UTC).

Related tasks

Configuring NTP Server

DHCP Option 12

You can specify a hostname for the system. When the system sends the request of DHCP DISCOVER, it will report the configured host name to the DHCP server via DHCP option 12. See RFC 1035 for character restrictions.

- Configuring the Host Name

Configuring the Host Name

Procedure

1. On your web user interface, go to **Network** > **LAN Configuration** > **IPv4 Config** > **Static DNS** > **Host Name**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Host Name	Configure the host name of the system. **Note**: When the system broadcasts DHCP DISCOVER messages, it will report the configured host name to the DHCP server via DHCP option 12. For more information, contact the network administrator. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Configuring LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which allows systems 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.

When LLDP feature is enabled on systems, the systems periodically advertise their own information to the directly connected LLDP-enabled switch. The systems can also receive LLDP packets from the connected switch and obtain their VLAN IDs, and then start communications with the call control. The switch assigns a VLAN ID to the endpoint through the LLDP protocol.

- Configuring LLDP

Configuring LLDP

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Advanced** > **LLDP**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **LLDP**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **Advanced Network** > **LLDP**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **LLDP**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Advanced Network** > **LLDP**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active	Enable or disable the LLDP feature on the system. **Note**: the default value is Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Packet Interval(1-3600s)	Configure the interval (seconds) for the system to send LLDP requests. **Default**: 60 seconds. The value can be any integer from 1 to 3600. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Configuring VLAN Manually

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

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Advanced** > **VLANInternet Port**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **VLAN**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **Advanced Network** > **VLAN**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **VLAN**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Advanced Network** > **VLAN**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active	Enable or disable VLAN for the Internet port. **Note**: the default value is Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
VID(1-4094)	Configure the identification of the Virtual LAN. **Note**: the default value is 1. The value can be any integer from 1 to 4094. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Priority	Configure the VLAN priority. **Note**: the default value is 0. The value can be any integer from 0 to 7. The smaller the number is, the higher the priority is. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Configuring DHCP VLAN

Your system supports VLAN discovery via DHCP. When the VLAN discovery method is set to DHCP, the system will examine DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID (it should be predefined on the DHCP server first) by default. The administrator can customize the DHCP option used to request the VLAN ID.

Procedure

1. On your web user interface, go to **Network** > **Advanced** > **VLAN** > **DHCP VLAN**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active/STUN Active	Enable or disable the DHCP VLAN discovery feature on the system. **Note**: the default value is On. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Option	Specify the DHCP option from which the system obtains the VLAN settings. You can configure at most 5 DHCP options and separate them by commas. **Note**: the value can be any integer from 128 to 254. The default value is 132. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

802.1x Authentication

You can use 802.1x authentication to restrict the unauthorized devices to accessing the LAN. The 802.1x authentication can be used to authenticate the devices connected to the port before the system obtains all the businesses.

The system supports the following protocols for 802.1X authentication:

- EAP-MD5
- EAP-TLS (Device and CA certificates are required, password is not required)
- EAP-PEAP/MSCHAPv2 (CA certificates are required)
- EAP-TTLS/EAP-MSCHAPv2 (CA certificates are required)

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

- Configuring the 802.1x Authentication

Configuring the 802.1x Authentication

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Advanced** > **802.1x**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **802.1x Mode**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **Advanced Network** > **802.1 x Mode**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **802.1 x Mode**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Advanced Network** > **802.1 x Mode**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
802.1x Mode	Specify the 802.1x authentication mode. • Disabled • EAP-MD5 • EAP-TLS • PEAP-MSCHAPv2 • EAP-TTLS/EAP-MSCHAPv2 **Note**: the default value is disabled. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Identity	Configure the user name for 802.1x authentication. **Note**: the default value is blank. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
MD5 Password	Configure the password for 802.1x authentication. **Note**: the default value is blank. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Parameter	Description	Configuration Method
CA Certificates	Upload the CA certificates. **Note**: upload the CA certificates when the 802.1x authentication mode is configured as EAP-TLS, PEAP-MSCHAPv2, or EAP-TTLS/EAP-MSCHAPv2. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Device Certificates	Upload the device certificates. **Note**: Configure the access URL of the server certificate when the 802.1x authentication mode is configured as EAP-TLS. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Enabling/Disabling the PC Port

The PC port of the VP59 is activated by default and can be used to provide computers with the network. If you do not want the VP59 to provide network to the computer, you can disable this feature.

Procedure

1. On your web user interface, go to **Network** > **PC Port** > **PC Port Active**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
PC Port Active	Enable or disable the VP59 to provide the connected computer with the network. • Disabled • Auto Negotiation **Note**: the default value is Auto Negotiation. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Related information

Network Speed and Duplex Mode

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.

VP59 allows you to configure the speed of Internet port and PC port.

- Supported Transmission Methods
- Configuring Transmission Methods

Supported Transmission Methods

The supported transmission methods for MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/PVT980/PVT950 are listed below:

- Auto
- Full Duplex (transmit in 10Mbps, 100Mbps or 1000Mbps)
- Half Duplex (transmit in 10Mbps or 100Mbps)

The supported transmission methods for VC200 are listed below:

- Auto
- Full Duplex (transmit in 10Mbps or 100Mbps)
- Half Duplex (transmit in 10Mbps or 100Mbps)

The supported transmission methods for VP59 are listed below:

- **WAN Port Link**
  - Auto Negotiation
  - Full Duplex (transmit in 10Mbps, 100Mbps or 1000Mbps)
  - Half Duplex (transmit in 10Mbps or 100Mbps)
- **PC Port Link**
  - Auto Negotiation
  - Full Duplex (transmit in 10Mbps, 100Mbps or 1000Mbps)
  - Half Duplex (transmit in 10Mbps or 100Mbps)

Configuring Transmission Methods

Procedure

1. On your web user interface, go to **Network** > **Advanced** > **Port Link**.
   For VP59, go to **Network** > **Advanced** > **Port Link**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
WAN Port Link (**WAN Port Link/PC Port Link**)	Specify the network speed and the duplex mode for the system. Note: the default value is Auto. The network speed and duplex mode you select must be supported by the switch. **PC Port Status** is only applicable to VP59. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Restricting Reserved Ports

By default, the VCS endpoint communicates through TCP and UDP ports from 50000 to 51000 for the video, the voice, the presentation, and the camera control. The VCS endpoint uses only a small number of these ports during a call. The specific number of the port 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.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **NAT/Firewall** > **Reserved Port**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **NAT/Firewall** > **Reserved Port**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **NAT/Firewall** > **Reserved Port**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **NAT/Firewall** > **Reserved Port**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **NAT/Firewall** > **Reserved Port**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
UDP Port Scope/ **UDP Lowest Port—UDP Highest Port**	Configure the range of the UDP ports. **Note**: the default UDP port range is from 50000 to 51000. The configurable port range is 1024-65000. SIP and H.323 calls share the configured ports. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
TCP Port Scope/ **TCP Lowest Port—TCP Highest Port**	Configure the range of the TCP ports. **Note**: the default TCP port range is from 50000 to 51000. The configurable port range is 1024-65000. SIP and H.323 calls share the configured ports. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Quality of Service (QoS)

Video conferencing system is subject to the bandwidth and the delay. Therefore, the QoS is very important for the network having limited bandwidth. QoS is a major issue in VoIP implementations, regarding how to guarantee that packet traffic is not delayed or dropped due to interference from other lower priority traffic. Your system supports the DiffServ model of QoS.

Audio QoS

The loss of audio packets, the delay and so on may cause poor audio quality. To solve this, you can configure DSCP priority for the audio packets.

Video QoS

Some issues, such as the video packet loss and delay may cause the video images distorted and unclear. 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 better presentation, data packets (PC content) emanated from the system should be configured with a high transmission priority. DSCPs for audio, video and data packets can be specified respectively.

- Configuring QoS

Configuring QoS

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Advanced** > **QoS**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **QoS**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **Advanced Network** > **QoS**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **QoS**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Advanced Network** > **QoS**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
QoS Enable	Enable or disable the QoS feature. **Note**: the default value is Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Audio Priority	Configure the DSCP (Differentiated Services Code Point) for audio packets. **Note**: the default value is 63. The greater the number is, the higher the priority is. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20
Video Priority/ **Video Priority (0-63)**	Configure the DSCP (Differentiated Services Code Point) for video packets. **Note**: the default value is 34. The greater the number is, the higher the priority is. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Data Priority/ **Data Priority (0-63)**	Configure the DSCP (Differentiated Services Code Point) for data packets. **Note**: the default value is 63. The greater the number is, the higher the priority is. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Configuring MTU

Data packets that exceed the maximum transmission unit (MTU) size for any router or segment along the network path may be fragmented or dropped, which may result in poor quality video at the receiving device. You can set the maximum MTU size of the data packets sent by the system.

About this task

Configure 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.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Advanced** > **MTU**.
   - On your VCS: go to **More** > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **MTU(1000-1500)**.

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Network** > **Wired Network** > **Advanced Network** > **Network MTU(1000-1500)**.

     For VP59, tap > **Settings** > **Network Setting** > **Wired Network** > **Advanced Network** > **MTU(1000-1500)**.
   - On your CTP20, tap > **Settings** > **Network Setting** > **Host Network** > **Advanced Network** > **Network MTU (1000-1500)**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Network MTU (1000-1500)	Specify the maximum MTU size (bytes) of data packets sent by the system. **Note**: the value can be any integer from 1000 to 1500. The default value is 1500. If you change this parameter, the system will reboot to make the change take effect.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Restricted Single Packet Mode	Enable or disable the restricted single packet mode. • **Off**—sends data packets by using multiple packets mode. • **On**—sends data packets by using single packet mode. **Default**: On. Some third-party devices only accept the data packets sent by single packet mode. If local system sends data packets by using multiple packets mode, the video call may appear the mosaic phenomenon. To avoid this situation, enable this **Restricted Single Packet Mode**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Configuring 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). The endpoints 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. The endpoints only support the GET request from the SNMP server. It is only applicable to MeetingEye 600/MeetingEye 400.

Procedure

1. On your web user interface, go to **Network** > **Advanced** > **SNMP**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Active/STUN Active	Enable or disable SNMP feature on the system. **Note**: the default value is Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Parameter	Description	Configuration Method
Port	Configure the SNMP port. **Note**: the value can be any integer from 1 to 65535. The default value is 161. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Trusted Address	Configure the IP address or domain name of the SNMP server. **Note**: if you change this parameter, the system will reboot to make the change take effect.	Web user interface

Configuring Account Settings

This chapter provides information on how to configure account settings.

- Setting SIP Account/SIP IP Call
- Setting H. 323 Account/H.323 IP Call
- Configuring the PSTN account
- Configuring the Video Conference Platform Account
- Configuring Quick Switch Platform
- Logging out of the Video Conference Platform

Setting SIP Account/SIP IP Call

Yealink video conferencing system supports Session Initiation Protocol (SIP). If your server supports SIP, you can make a voice/video call using the SIP account or IP address.

- Configuring SIP Accounts
- Configuring SIP IP Call

Configuring SIP Accounts

Yealink video conferencing system supports Session Initiation Protocol (SIP). If your server supports SIP, you can configure a SIP account for your device, and other users can call you by dialing your SIP account.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **SIP Account**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **SIP Account**.

     For VP59, tap > **Settings** > **Advanced** > **Account** > **SIP Account**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **SIP Account** .

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Line Active/SIP Account	Enable or disable SIP Accounts. **Note**: the default value is On. If it is set to **disabled**, the devices cannot place or receive calls via the SIP protocol.	Web user interface Endpoint CTP20
Username	The username of this SIP account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Register Name	The registration name of this SIP account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Password	The registration password of this SIP account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Server Host/Server	The IP address or domain name of the SIP server. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Port	Specify the port of the SIP server. **Note**: the default port number is 5060. The value can be any integer from 0 to 65535.	Web user interface Endpoint CTP20
Enable Outbound Proxy Server/Outbound	Enable or disable the device to send requests of the SIP account to the outbound proxy server. **Default**: Disabled.	Web user interface Endpoint CTP20
Outbound Proxy Server/ Outbound Server	Configure the IP address or domain name of the outbound proxy server for this SIP account. **Note**: only the outbound proxy server is enabled do you need to configure this parameter.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Outbound Port/Port	Configure the port of the outbound proxy server. **Note**: the default port number is 5060. The value can be any integer from 0 to 65535.	Web user interface Endpoint CTP20
Transport	Specify the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP**—it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • DNS-NAPTR—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: UDP.	Web user interface Endpoint CTP20
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the SIP server again. **Default**: 3600 seconds.	Web user interface Endpoint CTP20

Note: If you want to use SIP Account to make private-to-public calls, you also need to enable the static NAT settings or STUN feature for the SIP protocol.

Related tasks

Configuring STUN

Related information

NAT

Configuring SIP IP Call

You can use the SIP protocol for SIP IP call, which means dialing the IP address of the other party instead of the account. If you do not want the third-party or Yealink old devices (for example, VC110/VC120/VC400/T49G or VC800/VC500/VC200 running firmware version prior to V40) to make IP calls to you, you can enable the advanced security feature and set the IP call password. For MeetingEye 600/MeetingEye

400/VC880/VC800/VC500VC200/PVT980/PVT950, you can you can also disable this feature to prevent unknown public network attacks.

About this task
The SIP IP call feature on VP59 controls SIP IP call in and SIP IP call out.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **SIP IP Call**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **SIP IP Call**.

     For VP59, tap > **Settings** > **Advanced** > **Account** > **SIP IP Call**.
   - On your CTP20, tap **Settings** > **Advanced** > **Account** > **SIP IP Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
SIP IP Incoming	Enable or disable the SIP IP Incoming. If it is enabled, the system can receive an IP address call directly. **Note**: the default value is **Off**.	Web user interface
SIP IP Call Out	Enable or disable the SIP IP Call Out. If it is enabled, the system can call the far site by dialing an IP address directly. **Default**: On.	Web user interface Endpoint CTP20
Transport	Specify the type of transport protocol for the SIP IP call. The supported protocols are as follows: • **UDP**—it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. **Default**: TCP.	Web user interface Endpoint CTP20
Advanced Security	Enable or disable the advanced security. **Default**: On. If advanced security is enabled and the IP call password is configured, the third-party or Yealink old device need to use “password@IP” to call in for the SIP IP call.	Web user interface

Parameter	Description	Configuration Method
IP Call Password	Configure the password for the SIP IP call. **Note**: It can be configured only when the advanced security feature is enabled.	Web user interface
RPort	Enable or disable the RPort. **Note**: It can be configured only when the advanced security feature is enabled.	Web user interface Endpoint CTP20

Note: If you want to use SIP IP call to make private-to-public calls, you also need to enable the static NAT settings or STUN feature for the SIP IP Call.

Related tasks

Configuring NAT

Enabling Static NAT Feature for SIP Protocol

Setting H. 323 Account/H.323 IP Call

The H.323 protocol is enabled by default. You can place IP calls via the 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 you via your H.323 name or the extension instead of the IP address.

- Configuring H.323 Accounts
- H.323 Tunneling

Configuring H.323 Accounts

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **H.323**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **H.323**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **H.323**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **H.323**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
H.323 Protocol	Enable or disable the H.323 protocol. **Note**: the default value is On. Only when it is set to On can the H.323 account be registered. When it is set to On on both sites, the devices can call each other by dialing an IP address directly.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
H.323 Account	Enable or disable the H.323 account. **Note**: the default value is On. If it is set to **Off**, the devices cannot place or receive calls via the H.323 protocol.	Web user interface Endpoint CTP20
H.323 Name	Configure the device name that can be identified by the gatekeepers and gateways. **Note**: the default value is blank. If two devices are registered to the same gatekeeper, they can make point-to-point calls by dialing their H.323 names.	Web user interface Endpoint CTP20
H.323 Extension	Configure the device extension that can be identified by the gatekeepers and gateways. **Note**: the default value is blank. If two devices are registered to the same gatekeeper, they can make point-to-point calls by dialing their extensions.	Web user interface Endpoint CTP20
Gatekeeper Mode/Gatekeeper Type	Configures the gatekeeper mode. • **Off**—the system does not use a gatekeeper. • **Auto**—the system automatically discovers a gatekeeper. • **Manual**—specify the IP address and the port for the gatekeeper manually. You need manually configure the IP address and the port for the gatekeeper. **Default**: Disabled.	Web user interface Endpoint CTP20
Gatekeeper IP Address 1/ Gatekeeper Server2	Configure the IP address or the domain name for the primary gatekeeper. **Note**: the default value is blank. Only when the configuration type is manual do you need to configure this parameter.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Port/Gatekeeper Port 1	Configure the port for the primary gatekeeper. **Note**: the default port number is 1719. The value can be any integer from 0 to 65535.	Web user interface Endpoint CTP20
Gatekeeper IP Address 2/ Gatekeeper Server2	Configure the IP address or the domain name for the secondary gatekeeper. **Note**: the default value is blank. Only when the configuration type is manual do you need to configure this parameter. If the device cannot access the primary gatekeeper, the device will send the registration request to Gatekeeper Server2.	Web user interface Endpoint CTP20
Port/Gatekeeper Port 2	Configure the port for the secondary gatekeeper. **Note**: the default port number is 1719. The value can be any integer from 0 to 65535.	Web user interface Endpoint CTP20
Gatekeeper Authentication/ Gatekeeper Verify	Enable or disable support for the gatekeeper authentication. **Note**: the default value is Off. When Gatekeeper Authentication is enabled, the gatekeeper can ensure that only the trusted H.323 devices are allowed to access the gatekeeper.	Web user interface Endpoint CTP20
Gatekeeper Username	Configure the username used for the gatekeeper authentication. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Gatekeeper Password	Configure the password for the gatekeeper authentication. **Note**: the default value is blank.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Protocol Monitor Port	Configure the port of the H.323 call signaling. If you fail to place an IP call to other party via H.323 protocol, it may be caused by the ISP limiting the 1720 port, so you need modify the protocol monitor port, and call the far site by dialing h323:ip:port. **Note**: the default value is 1720. The modification on this port is only applicable for the H.323 IP call.	Web user interface
Local Early Media	Enable or disable the local early media feature on the device. • **Off**—the local system sends an Open Logical Channel (OLC) message and receives the acknowledgement message of OLC from the far site. After receiving the acknowledgement message, the system may transmit RTP streams to the far site. • **On**—the system sends an OLC message to the far site and then transmits RTP streams to the far site directly before receiving the acknowledgement message of OLC. For some gatekeepers, you need to enable this feature to avoid black screen during a call. **Default**: Off.	Web user interface

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. H.323 tunneling is supported by the video conferencing system. To use H.323 tunneling, make ensure the participants in the call enable H.323 tunneling simultaneously. When you log in to the StarLeaf platform or use an H.323 account, you can configure the H.323 tunneling feature.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **H.323** or **Account** > **VC Platform** > **Video Conference Platform** > **Platform Type** > **StarLeaf**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **H.323**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **H.323**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **H.323**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
H.323 Tunneling	Enable or disable the system to send all signaling and media through the HTTP tunnel. **Default**: Disabled.	Web user interface Endpoint CTP20

Configuring the PSTN account

PSTN box CPN10 is used to connect video conferencing system to the PSTN (Public Switched Telephone Network). It is a cost-effective solution for PSTN office. Up to 2 cascaded PSTN Boxes can be installed to video conferencing systems, which allow you to experience the conference conveniently in excellent speech quality with PSTN. For more information, refer to Yealink PSTN Box CPN10 Quick Start Guide. After PSTN is connected, you can take the PSTN as one audio and use the PSTN to join the conference mixing with the audio and video.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **PSTN Account**.
   - On your VCS endpoint, go to **More** > **Settings** > **Advanced** > **Account** > **PSTN Account**.

     For VP59, tap > **Settings** > **Advanced** > **Account** > **PSTN Account**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **PSTN Account**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Account Active/PSTN Account X	Enable or disable the PSTN account X. **Default**: On. X=1-2.	Web user interface Endpoint CTP20
Label/PSTN Account Label	Configure the PSTN account label.	Web user interface Endpoint CTP20

Configuring the Video Conference Platform Account

You can log into the following video conference platform:

- Yealink VC Cloud
- Yealink Meeting Server
- Zoom
- Pexip
- BlueJeans
- Videxio
- Custom

- Registering a Yealink Cloud Account
- Registering a YMS Account
- Logging into Zoom Cloud Platform
- Registering a Pexip Account
- Logging into the BlueJeans Cloud Platform
- Logging into Videxio Platform
- Registering a Custom Account

Registering a Yealink Cloud Account

About this task

The Yealink VC Cloud Management Service is a value-added and cloud-based service platform for Cloud systems. It offers significant convenience and cost-savings to integrators and business customers in terms of deployment, configuration and usage.

The cloud enterprise 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.

When you log into the Yealink VC Cloud Management Service, you can:

- Dial other Yealink Cloud accounts to establish a conversation.
- View and join scheduled conferences.
- Initiate and join meet now conferences.
- Join the VMR.
- Manage Yealink Cloud video conferences.
- If you purchase a collaboration service, you can use the whiteboard and content sharing features during the conference calls.

For detailed introduction, refer to Yealink Full HD Video Conferencing System User Guide.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
   - On your CTP20, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. **Note**: if it is set to **Off**, your device cannot register a Yealink Cloud account.	Web user interface Endpoint CTP20
Platform Type	Select Yealink VC Cloud Management Service.	Web user interface Endpoint CTP20
Username	Specify the username for logging into the Yealink VC Cloud Management Service platform. **Note**: the default value is blank. Only when you select to log into Yealink VC Cloud Management Service via Username/password can this feature be configured.	Web user interface Endpoint CTP20
Password	Specify the Password for logging into the Yealink VC Cloud Management Service platform. **Note**: the default value is blank. Only when you select to log into Yealink VC Cloud Management Service via Username/password can this feature be configured.	Web user interface Endpoint CTP20
Server Host/Server	The IP address or the domain name of Yealink VC Cloud Management Service platform. **Default:** onylyun.com.	Web user interface Endpoint CTP20
Remember password	Enable or disable remembering password. **Note**: the default value is On. If it is set to **On**, the password will be filled in automatically when you log in next time. Only when you select to log into Yealink VC Cloud Management Service via Username/password can this feature be configured.	Endpoint CTP20

Note:

A Yealink Cloud account can be logged into 5 devices at most simultaneously.

Registering a YMS Account

You can use Yealink YMS account to log into Yealink Meeting Server (YMS).

About this task

For more information on how to add YMS accounts, refer to Yealink Meeting Server Administrator Guide.

When you log into the Yealink Meeting Server, you can:

- Dial other YMS accounts to establish a conversation.
- View and join scheduled conferences.
- Initiate and join meet now conferences.
- Join the VMR.
- Manage YMS video conferences.
- If you purchase a collaboration service, you can use the whiteboard collaboration and content sharing collaboration (supported in V23 version or later) during the conference calls.

For detailed introduction, refer to Yealink Full HD Video Conferencing System User Guide.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
   - On your CTP20, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. **Note**: if it is set to **Off**, your device cannot log into YMS.	Web user interface Endpoint CTP20
Platform Type	Select YMS.	Web user interface Endpoint CTP20
ID	Specify the ID when registering this YMS account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Password	Specify the password when registering this YMS account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Server Host/Server	The IP address or the domain name of Yealink meeting server. **Note**: the default value is blank.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Port	Select a port of Yealink meeting server. **Note**: the default port number is 0.	Web user interface
Outbound Proxy Server/ Outbound Server	The IP address or domain name of the outbound proxy server. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Remember password	Enable or disable remembering password. **Note**: the default value is Off. If it is set to **On**, the password will be filled in automatically when you log in next time.	Endpoint CTP20

Note:

A YMS account can be logged into 5 devices at most simultaneously.

If the enterprise administrator enables the Device upgrade feature on Yealink Meeting Server, video conferencing systems with YMS accounts logged into will upgrade the firmware automatically once they receive the new firmware from Yealink Meeting Server.

Logging into Zoom Cloud Platform

You can log into Zoom cloud platform and call into the VMRs to join in the video conferences with other participants.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
   - On your CTP20, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. **Note**: if it is set to **Off**, your device cannot log into the Zoom Cloud Platform.	Web user interface Endpoint CTP20
Platform Type	Select Zoom.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Server/ **Server Host**	The IP address or the domain name of the Zoom server. **Default:** zoomcrc.com	Web user interface Endpoint CTP20
Transport	Specify the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP**—it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: TCP.	Web user interface
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the server again. **Default**: 3600 seconds.	Web user interface
Keep Alive Interval	Configure the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30 seconds.	Web user interface

Registering a Pexip Account

You can register the Pexip account.

About this task

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.
- Dial Microsoft Skype for Business/Lync account.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
   - On your CTP20, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. **Note**: if it is set to **Off**, your device cannot register a Pexip account.	Web user interface Endpoint CTP20
Platform Type	Select Pexip.	Web user interface Endpoint CTP20
Alias	Specify the alias when registering a Pexip account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Username	Specify the username for this Pexip account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Password	Specify the password for this Pexip account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Server Host/Server	The IP address or domain name of the Pexip server. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Port	The port of the Pexip server. **Default**: 0.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Remember password	Enable or disable remembering password. **Note**: the default value is Off. If it is set to **On**, the password will be filled in automatically when you enter the username next time.	Endpoint CTP20
Transport	Specify the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP**—it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: TCP.	Web user interface
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the server again. **Default**: 3600 seconds.	Web user interface
Keep Alive Interval	Configure the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30 seconds.	Web user interface

Note:

Yealink VCS also allows you to register a Pexip account via the standard H.323 or SIP protocol. For more information, refer to Setting SIP Account/SIP IP Call and Setting H. 323 Account/H.323 IP Call.

Logging into the BlueJeans Cloud Platform

You can log into the BlueJeans Cloud platform and do the followings:

About this task

You can do the following things after logging into the BlueJeans Cloud Platform:

- Call into the VMR to join the video conference with other participants.
- Receive meeting schedule from the BlueJeans Cloud platform.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
   - On your CTP20, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. **Note**: if it is set to **Off**, your device cannot log into the BlueJeans Cloud Platform.	Web user interface Endpoint CTP20
Platform Type	Select the BlueJeans Cloud Platform.	Web user interface Endpoint CTP20
Server Host/Server	The IP address or the domain name of the BlueJeans server. **Default**: bjn.vc.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Transport	Specify the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP**—it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: TCP.	Web user interface
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the server again. **Default**: 3600 seconds.	Web user interface
Keep Alive Interval	Configure the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30 seconds.	Web user interface

Logging into Videxio Platform

You can log into Videxio platform and Videxio accounts will be automatically logged into the devices.

About this task

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

- Dial Videxio accounts to establish a point-to-point call.
- Dial third-party accounts registered in the Videxio platform to establish a point-to-point call.
- Call into the VMR to join the video conference with other participants.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
   - On your CTP20, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. **Note**: if it is set to **Off**, your device cannot log into the Videxio platform.	Web user interface Endpoint CTP20
Platform Type	Select Videxio.	Web user interface Endpoint CTP20

Registering a Custom Account

You can register a custom account for communication.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
   - On your CTP20, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Cloud Account	Enables the Cloud feature. **Note**: if it is set to **Off**, your device cannot register a custom account.	Web user interface Endpoint CTP20
Platform Type	Select Custom.	Web user interface Endpoint CTP20
Label	Configure the label for this custom account. **Note**: the default value is blank.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Username	Specify the username for this custom account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Register Name	Specify the register name for this custom account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Password	Specify the password for this custom account. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Server Host/Server	The IP address or the domain name of the server. **Note**: the default value is blank.	Web user interface Endpoint CTP20
Port	Configure the port of the custom server. **Note**: the default value is 0. The value can be any integer from 0 to 65535.	Web user interface Endpoint CTP20
Remember password	Enable or disable remembering password. **Note**: the default value is Off. If it is set to **On**, the password will be filled automatically when you enter the username next time.	Endpoint CTP20

Parameter	Description	Configuration Method
Transport	Specify the transport protocol for transmitting the SIP signaling. The supported protocols are as follows: • **UDP**—it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Default**: TCP.	Web user interface
Server Expires	The registration timeout (in seconds) of the device. After the timeout, the device will send the registration request to the server again. **Default**: 3600 seconds.	Web user interface
Keep Alive Interval	Configure the interval (in seconds) that the device sends keep-alive messages to the SIP server, so that the SIP server can remain connected to the device. **Default**: 30 seconds.	Web user interface

Configuring Quick Switch Platform

If you use more than one video conference platforms to log in to the system, you may use Yealink YMS and Zoom or Yealink YMS and BlueJeans. You can log in to the accounts of different platforms in advance on

the system and enable the quickly switch platform feature. Users can quickly select the account from the account area in the top-right corner of CTP20.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **Video Conference Platform** > **Quick Switch Platform**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Switching Platform Quickly	Enable or disable the quickly switch platform feature. **Note**: the default value is **Off**. This configuration is available only when you enable Cloud account.	Web user interface CTP20

Logging out of the Video Conference Platform

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform** > **Log Out**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **Video Conference Platform** > **Log out**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **Video Conference Platform** > **Log out**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **Video Conference Platform** > **Log out**.

   It prompts whether to log out the current account.
2. Click **OK**.

Basic Settings

- Configuring the Site Name
- Setting the Language
- Configuring Key Tone
- Configure the Time and Date
- Setting Screen Saver for VP59
- Setting Wallpaper for VP59
- Enabling/Disabling the Clock for the VP59
- Setting the Ring Tone for the VP59
- Configuring Automatic Sleep Time

- Configuring the Display to Wake up the Sleeping Endpoint
- Allowing Website Snapshot
- Setting the Screen Saver Wait Time
- Customizing the Local Interface for the System
- Muting the Microphone
- Configuring Microphone Mute Mode
- Configuring the Keyboard Input Method
- Configuring USB Storage
- Configuring Local Storage
- Configuring the Screenshot
- Configuring to Automatically Upload Screenshots to the YMS
- Configuring Video Recording
- Basic Settings for CP960 Conference Phone
- Configuring * Key for Default Input
- Configuring Whiteboard Tools
- Configuring the Presentation Tools

Configuring the Site Name

You can customize the site name of the system, which displays on the status bar of the device, and displays on the far-site screen during the call.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **General** > **Basic**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **General**.

     For VP59, go to > **Settings** > **Basic** > **General**.
   - On your CTP20, tap > **Settings** > **Basic** > **General**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Site Name	Configure the site name of the system. **Note**: you can enter 64 characters at most.	Web user interface Endpoint CTP20

Setting the Language

You can specify a language displayed in the monitor and the web user interface respectively. The CP960 conference phone will detect and use the same language as the monitor.

About this task

Note: The supported languages are English, Simplified Chinese, Traditional Chinese, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian, Czech, Japanese, Vietnamese, and Korean.

Procedure

1. Do one of the following:
   - On your web user interface, click **Language** at the top of the web page.
   - On your VCS, go to **More** > **Settings** > **Basic** > **General** > **Language**.

     For VP59, tap > **Settings** > **Basic** > **Language**.
   - On your CTP20, tap > **Settings** > **Basic** > **General** > **Language**.
2. Select the desired language.
3. Save the change.

Configuring Key Tone

You can enable the key tone feature. When you press any key on the remote control or tap the onscreen dial pad on the CP960 conference phone, the system will produce a sound. For VP59, when you press any key on the phone or tap any key on the Dial page, the device will produce key tone.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Remote Control** > **Remote Control**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **General**.

     For VP59, go to > **Settings** > **Basic** > **General**.
   - On your CTP20, tap > **Settings** > **Basic** > **General**.
2. Enable/disable **Key Tone**.

Configure the Time and Date

Your system can obtain the time and date from SNTP (Simple Network Time Protocol) time server automatically. You can also manually configure the time and date.

- Time Zone
- Configuring NTP Server
- Configuring the DST
- Manually Configuring the Time and Date

- Customizing the Time and Date Format
- Setting the Time Reminder

Time Zone

You can set the time difference between GMT (Greenwich Mean Time) and your location. Therefore, different areas can keep the time consistency for the commence and communication. You can set the following time zone:

Time Zone	Time Zone Name	Time Zone	Time Zone Name
–11:00	Samoa	+01:00	Poland (Warsaw)
-10:00	United States-Hawaii-Aleutian	+02:00	Estonia (Tallinn)
-10:00	United States-Alaska-Aleutian	+02:00	Finland (Helsinki)
-09:30	French Polynesia	+02:00	Gaza Strip (Gaza)
-09:00	United States-Alaska Time	+02:00	Greece (Athens)
-08:00	Canada (Vancouver, Whitehorse)	+02:00	Israel (Tel Aviv)
-08:00	Mexico (Tijuana, Mexicali)	+02:00	Jordan (Amman)
-08:00	United States-Pacific Time	+02:00	Latvia (Riga)
-07:00	Canada (Edmonton, Calgary)	+02:00	Lebanon (Beirut)
-07:00	Mexico (Mazatlan, Chihuahua)	+02:00	Moldova (Kishinev)
-07:00	United States-Mountain Time	+02:00	Russia (Kaliningrad)
-07:00	United States-MST no DST	+02:00	Romania (Bucharest)
-06:00	Canada-Manitoba (Winnipeg)	+02:00	Syria (Damascus)
-06:00	Chile (Easter Islands)	+02:00	Turkey (Ankara)
-06:00	Mexico (Mexico City, Acapulco)	+02:00	Ukraine (Kyiv, Odessa)
-06:00	United States-Central Time	+03:00	East Africa Time
-05:00	Bahamas (Nassau)	+03:00	Iraq (Baghdad)
-05:00	Canada (Montreal, Ottawa, Quebec)	+03:00	Russia (Moscow)
-05:00	Cuba (Havana)	+03:30	Iran (Teheran)

Time Zone	Time Zone Name	Time Zone	Time Zone Name
-05:00	United States-Eastern Time	+04:00	Armenia (Yerevan)
-04:30	Venezuela (Caracas)	+04:00	Azerbaijan (Baku)
-04:00	Canada (Halifax, Saint John)	+04:00	Georgia (Tbilisi)
-04:00	Chile (Santiago)	+04:00	Kazakhstan (Aktau)
-04:00	Paraguay (Asuncion)	+04:00	Russia (Samara)
-04:00	United Kingdom-Bermuda (Bermuda)	+04:30	Afghanistan (Kabul)
-04:00	United Kingdom (Falkland Islands)	+05:00	Kazakhstan (Aqtobe)
-04:00	Trinidad&Tobago	+05:00	Kyrgyzstan (Bishkek)
-03:30	Canada-New Foundland (St.Johns)	+05:00	Pakistan (Islamabad)
-03:30	Denmark-Greenland (Nuuk)	+05:00	Russia (Chelyabinsk)
-03:00	Argentina (Buenos Aires)	+05:30	India (Calcutta)
-03:00	Brazil (no DST)	+05:45	Nepal (Katmandu)
-03:00	Brazil (DST)	+06:00	Kazakhstan (Astana, Almaty)
-02:30	Newfoundland and Labrador	+06:00	Russia (Novosibirsk, Omsk)
-02:00	Brazil (no DST)	+06:30	Myanmar (Naypyitaw)
-01:00	Portugal (Azores)	+07:00	Russia (Krasnoyarsk)
0	GMT	+07:00	Thailand (Bangkok)
0	Greenland	+08:00	China (Beijing)
0	Denmark-Faroe Islands (Torshavn)	+08:00	Singapore (Singapore)
0	Ireland (Dublin)	+08:00	Australia (Perth)
0	Portugal (Lisboa, Porto, Funchal)	+08:00	Russia (Irkutsk, Ulan-Ude)
0	Spain-Canary Islands (Las Palmas)	+08:45	Eucla
0	United Kingdom (London)	+09:00	Korea (Seoul)
0	Morocco	+09:00	Japan (Tokyo)
+01:00	Albania (Tirane)	+09:00	Russia (Yakutsk, Chita)
+01:00	Austria (Vienna)	+09:30	Australia (Adelaide)

Time Zone	Time Zone Name	Time Zone	Time Zone Name
+01:00	Belgium (Brussels)	+09:30	Australia (Darwin)
+01:00	Caicos	+10:00	Australia (Sydney, Melbourne, Canberra)
+01:00	Chad	+10:00	Australia (Brisbane)
+01:00	Spain (Madrid)	+10:00	Australia (Hobart)
+01:00	Croatia (Zagreb)	+10:00	Russia (Vladivostok)
+01:00	Czech Republic (Prague)	+10:30	Australia (Lord Howe Islands)
+01:00	Denmark (Kopenhagen)	+11:00	New Caledonia (Noumea)
+01:00	France (Paris)	+11:00	Russia (Srednekolymsk Time)
+01:00	Germany (Berlin)	+11:30	Norfolk Island
+01:00	Hungary (Budapest)	+12:00	New Zealand (Wellington, Auckland)
+01:00	Italy (Rome)	+12:00	Russia (Kamchatka Time)
+01:00	Luxembourg (Luxembourg)	+12:45	New Zealand (Chatham Islands)
+01:00	Macedonia (Skopje)	+13:00	Tonga (Nukualofa)
+01:00	Netherlands (Amsterdam)	+13:30	Chatham Islands
+01:00	Namibia (Windhoek)	+14:00	Kiribati

Configuring NTP Server

You can set a NTP time server for the desired area as required. The NTP time server address can be offered by the DHCP server or configured manually.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Date&Time**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **General** > **Date & Time**.

     For VP59, tap > **Settings** > **Basic** > **General** > **Date & Time**.
   - On your CTP20, tap > **Settings** > **Basic** > **General** > **Date & Time**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Manual Time/Time Type	Select **Off**/**SNTP Setting** to obtain the time and date from the NTP server automatically.	Web user interface Endpoint CTP20
DHCP Time	Enable or disable the system to update time with the offset time offered by the DHCP server. **Note**: the default value is Off. It is only available when the time zone is GMT 0.	Web user interface
Time Zone	Configure the time zone. For more information on available time zone, refer to Time Zone. **Note**: the default value is +8 China (Beijing).	Web user interface Endpoint CTP20
NTP Primary Server/Primary Server	Configure the NTP primary server. **Default:** pool.ntp.org.	Web user interface Endpoint CTP20
NTP Secondary Server/ Secondary Server	Configure the NTP secondary server. **Default:** pool.ntp.org.	Web user interface Endpoint CTP20
Synchronism (15~86400s)	Configure the interval (in seconds) to update time and date from the NTP server. **Default**: 1000 seconds.	Web user interface

Configuring the DST

You can set Daylight Saving Time (DST) for the system according to the location. By default, the DST is set to Automatic, so it can be adjusted automatically from the current time zone configuration.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Date&Time**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **General** > **Date & Time**.

     For VP59, tap > **Settings** > **Basic** > **General** > **Date & Time**.
   - On your CTP20, tap > **Settings** > **Basic** > **General** > **Date & Time**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Daylight Saving Time	Configure the type of DST. The available types are as below: • **Disabled**: do not use DST. • **Enabled**-use DST. You can manually configure the start time, the end time and the offset according to your needs. • **Automatic**-use DST. DST will be configured automatically. You do not need to manually configure the start time, the end time and the offset according to your needs. **Default**: Auto.	Web user interface Endpoint CTP20
Fixed Type	Specify the DST calculation methods. The available DST calculation methods are as below: • **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 when you enable Daylight Saving Time.	Web user interface
Start Date	When you select By Date as the fixed type, configure the start time of DST. **Note**: It only works when you enable Daylight Saving Time.	Web user interface
End Date	When you select By Date as the fixed type, configure the end time of DST. **Note**: It only works when you enable Daylight Saving Time.	Web user interface

Parameter	Description	Configuration Method
DST Start Month	When you select By Week as the fixed type, configures the start time of DST. **Note**: It only works when you enable Daylight Saving Time.	Web user interface
DST Start Day of Week		
DST Start Day of Week Last in Month		
Start Hour of Day		
DST Stop Month	When the DST calculation method is set to By month, configures the end month of DST. **Note**: It only works when you enable Daylight Saving Time.	Web user interface
DST Stop Day of Week		
DST Stop Day of Week Last in Month		
End Hour of Day		
Offset(minutes)	Specify the DST offset time (in minutes). Valid value: from -300 to +300. **Note**: It only works when you enable Daylight Saving Time.	Web user interface

Manually Configuring the Time and Date

You can set the time and date manually when the system cannot obtain the time and date from the NTP time server.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Date&Time**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **General** > **Date & Time**.

     For VP59, tap **Settings** > **Basic** > **Date & Time**.
   - On your CTP20, tap > **Settings** > **Basic** > **General** > **Date & Time**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Manual Time/Time Type	Select **On/Manual Setting** to obtain the time and date from the NTP server automatically.	Web user interface Endpoint CTP20

3. Configure the time and date.
4. Save the change.

Customizing the Time and Date Format

You can customize the time and date by choosing between a variety of time and date formats.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Date&Time**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Date & Time**.

     For VP59, tap > **Settings** > **Basic** > **General** > **Date & Time**.
   - On your CTP20, tap > **Settings** > **Basic** > **General** > **Date & Time**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Time Format	Configure the time format. • Hour 12 • Hour 24 **Default**: Hour 24.	Web user interface Endpoint CTP20
Date Format/Date	Configure the date format. The supported formats are as below: • 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. Note: WWW" represents the abbreviation of the week; "DD" represents a two-digit day; "MMM" represents the first three letters of the month; "YYYY" represents a four-digit year, and "YY" represents the last two digits of the year.	Web user interface Endpoint CTP20

Setting the Time Reminder

The system displays a clock on the hour during a call. You can disable it if you do not want to pay attention to time. This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Setting** > **Date&Time**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Time Reminder	Enable or disable the system to display a clock on the hour during a call. **Default**: On.	Web user interface

Setting Screen Saver for VP59

The screen saver automatically starts after the VP59 is inactive for a specified amount of time. The VP59 uses the system's built-in screen saver by default. You can set the time the phone is idle before the screen saver starts, upload the screen saver pictures and select the screen saver you want.

About this task

Either the smaller or the larger picture will be scaled proportionally to fit the screen. The screen saver picture format must meet the following:

Format	Resolution	Single File Size
.jpg/.png/*.bmp/*.jpeg	<=2.0 megapixels	<=5MB

Procedure

1. On your web user interface, go to **Setting** > **Wallpaper & Screensaver**.
2. In the **Screensaver Wait Time** field, select the desired time.

   If you do not need a screen saver, you can disable it.
3. In the **Screensaver Type** field, select a desired type of screen saver.
   - If you select **System**, when the screen saver starts, the VP59 displays the picture of the screen saver built into the system.
   - If you select **Custom**, in the **Upload Screensaver** field, click **Browse** to select a desired picture, and then click **Upload**.

     Tip: Repeat the operations to upload multiple screen savers. When the screen saver starts, all uploaded screen saver pictures will be displayed alternately.

     If you do not need a picture, you can select the corresponding picture in the **Screensaver** field and then click **Delete** to delete it.
4. Click **Confirm**.

Setting Wallpaper for VP59

VP59 uses the system's built-in wallpaper by default. You can upload the wallpapers to change the background picture displayed on the screen. If you connect an expanded display, you can also set its wallpaper.

About this task

Either the smaller or the larger picture will be scaled proportionally to fit the screen. The screen saver picture format must meet the following:

Format	Resolution	Single File Size
.jpg/.png/*.bmp/*.jpeg	<=2.0 megapixels	<=5MB

Procedure

1. On your web user interface, go to **Setting** > **Wallpaper & Screensaver**.
2. In the **Upload Wallpaper** field, select **Custom Wallpaper**, and then click + Upload Wallpaper to upload a wallpaper.

   Tip: Repeat the operations to upload multiple wallpapers. If you do not need a picture, you can hover over the current wallpaper and then click **Delete** to delete it.
3. Hover over the desired wallpaper and select **Set as system wallpaper** to customize the wallpaper for your VP59.
4. Hover over the desired wallpaper and select **Set as extend display wallpaper** to customize the wallpaper for your expanded display.
5. Click **Confirm**.

Enabling/Disabling the Clock for the VP59

After you enable the clock, the time and the date are displayed at the center of the Home page.

Procedure

1. Tap > **Settings** > **Basic** > **General**.
2. Enable/disable **Clock**.

Setting the Ring Tone for the VP59

You can set the ring tone for VP59, and the ring tone applies to all accounts registered on VP59.

Procedure

1. Tap > **Settings** > **Basic** > **General** > **RingTone**.
2. Select the desired ring tone.
3. Save the change.

Configuring Automatic Sleep Time

Static images displayed for long periods may lead to monitor burn-in, therefore, you can configure the automatic sleep time for the device. After the device goes to the sleep mode, “no signal” is displayed on the monitor. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **General** > **Basic**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **General**.
   - On your CTP20, tap > **Settings** > **Basic** > **General**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Automatic Sleep Time	Configure the inactive time (minutes) before the system enters sleep mode. **Note**: the default value is 10 minutes. When you power the system on and set the setup wizard, the automatic sleep time feature is disabled automatically. To protect the monitor, you should complete the setup wizard immediately.	Web user interface Endpoint CTP20

Configuring the Display to Wake up the Sleeping Endpoint

By default, the endpoint in sleep mode is not woken up automatically when it is connected to the display device. If you want to wake up the endpoint synchronously when you connect a display, you can enable the **Insert The Display To Wake Up** feature. This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Setting** > **Monitor** > **Display Function**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Insert The Display To Wake Up	Configure whether the endpoint in the sleep mode can be woken up when the display is connected to it. **Default**: Disabled.	Web user interface

Allowing Website Snapshot

You can choose whether to allow the web to show the same content that displayed on your monitor. If you want to prevent content on your monitor from being viewed remotely, you can disable this feature. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your VCS, go to **More** > **Settings** > **Basic** > **General**.
   - On your CTP20, tap > **Settings** > **Basic** > **General**.
2. Enable **Website Snapshot**.

Setting the Screen Saver Wait Time

The screen saver automatically starts when the system has been idle for a period of time you specified. You can configure the waiting time before the monitor starts the screen saver.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Wallpaper & Screensaver**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **General** > **Screensaver**.

     For VP59, tap > **Settings** > **Basic** > **General** > **Screensaver**.
   - On your CTP20, tap > **Settings** > **Basic** > **General** > **Screensaver**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Screen Saver Wait Time	Configure the inactive time (minutes) before the system starts the screen saver. **Default**: 1 minute.	Web user interface Endpoint CTP20

Customizing the Local Interface for the System

You can configure the time before the system starts screen saver, and customize the screen to show or hide some information.

- Hide the IP Address on the Status Bar
- Hiding the Time and the Date on the Status Bar
- Hiding the User Interface in Idle Screen
- Showing or Hiding Icons in a Call

Hide the IP Address on the Status Bar

Procedure

1. On your web user interface, go to **Setting** > **General** > **Display**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Hide IP Address	Enable or disable the IP address displayed on the status bar. • **On**—do not display the IP address. • **Off**—display the IP address. **Default**: Disabled.	Web user interface

Hiding the Time and the Date on the Status Bar

You can hide the time and the date on the status bar of your monitor. This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Setting** > **General** > **Display**.

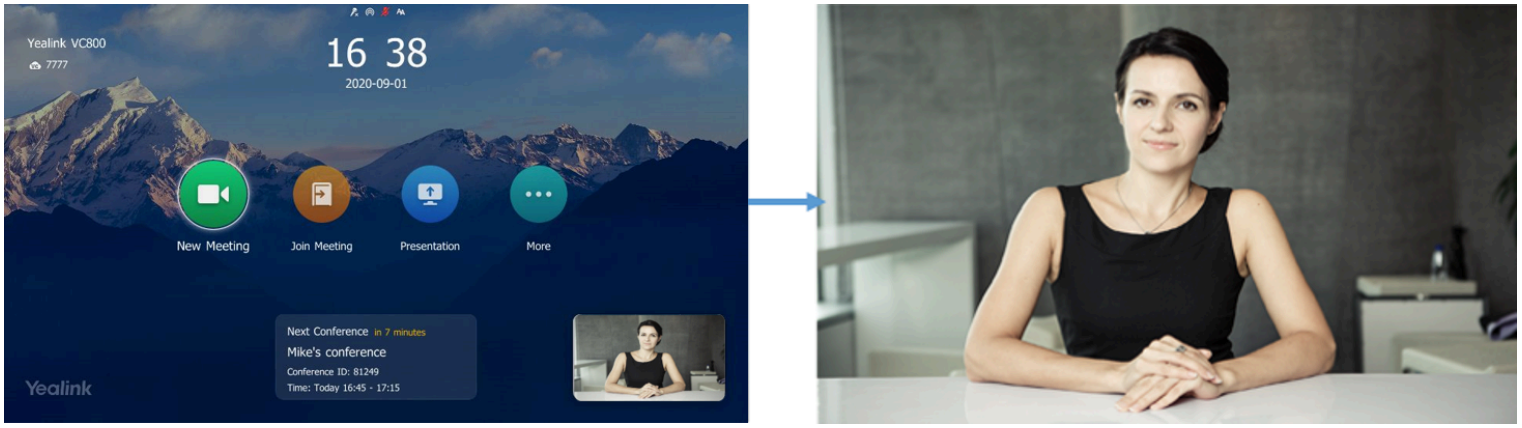
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Hide Time	Display or hide the time and the date on the status bar. • **On**—do not display the heading time. • **Off**—display the heading time. **Default**: Disabled.	Web user interface

Hiding the User Interface in Idle Screen

You can choose to hide the user interface when the system is idle. The monitor only displays the local video or the PC content. This feature is not applicable to VP59.

About this task



Procedure

1. On your web user interface, go to **Setting** > **General** > **Display**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Hide UI in Idle Screen	Enables the monitor to hides the user interface when the system is idle. • **On**—hide the user interface. • **Off**—display the user interface. **Default**: Disabled.	Web user interface

Showing or Hiding Icons in a Call

During a call, the VCS endpoint will show some information and icons (such as the call time, the mute icon and recording icon) by default, so that 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. This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Call Information**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **Hide Icon in Call**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Title Bar	Enable or disable the VCS endpoint to hide the title bar during a call. • **Show**- the VCS endpoint displays the title bar. • **Hide with UI**- the VCS endpoint displays the title bar and then hide it after 5 seconds. • **Hide**- the VCS endpoint hides the title bar. **Default**: Hide with UI.	Web user interface
Time Icon	Enable or disable the VCS endpoint to hide the call time during a call. • **Show**- the VCS endpoint displays the call time. • **Hide with UI**- the VCS endpoint displays the call time and then hide it after five seconds. • **Hide**- the VCS endpoint hides the call time. **Default**: Hide with UI.	Web user interface
Mute Icon	Enable or disable the VCS endpoint to hide the mute icon ( ) during a call. • **Show**- the VCS endpoint displays the mute icon. • **Hide with UI**- the VCS endpoint displays the mute icon and then hide it after five seconds. • **Hide**- the VCS endpoint hides the mute icon. **Default**: Hide with UI.	Web user interface

Parameter	Description	Configuration Method
Camera Icon	Enable or disable the VCS endpoint to hide the camera icon ( ) during a call. • **Show**- the VCS endpoint displays the camera icon. • **Hide with UI**- the VCS endpoint displays the camera icon and then hide it after five seconds. • **Hide**- the VCS endpoint hides the camera icon. **Default**: Hide with UI.	Web user interface
Recording Icon	Enable or disable the VCS endpoint to hide the recording icon ( ) during a call. • **Show**- the VCS endpoint displays the recording icon. • **Hide with UI**- the VCS endpoint displays the recording icon and then hide it after five seconds. • **Hide**- the VCS endpoint hides the recording icon. **Default**: Show.	Web user interface
Site Name	Enable or disable the VCS endpoint to hide the site name during a call. • **Show**- the VCS endpoint displays the site name. • **Hide with UI**- the VCS endpoint displays the site name and then hide it after 5 seconds. • **Hide**- the VCS endpoint hides the site name. **Default**: Hide with UI.	Web user interface

Parameter	Description	Configuration Method
Hold Icon	Enable or disable the VCS endpoint to hide the hold icon ( ) during a call. • **Show**- the VCS endpoint displays the hold icon. • **Hide with UI**- the VCS endpoint displays the hold icon and then hide it after five seconds. • **Hide**- the VCS endpoint hides the hold icon. **Default**: Hide with UI.	Web user interface
Encrypt Icon	Enable or disable the VCS endpoint to hide the encryption icon ( ) during a call. • **Show**- the VCS endpoint displays the encryption icon. • **Hide with UI**- the VCS endpoint displays the encryption icon and then hide it after five seconds. • **Hide**- the VCS endpoint hides the encryption icon. **Default**: Hide with UI.	Web user interface
Output Mute Icon	Enable or disable the VCS endpoint to hide the output mute icon (indicates that the output volume is set to 0:) during a call. ）。 • **Show**- the VCS endpoint displays the output mute icon. • **Hide with UI**- the VCS endpoint displays the output mute icon and then hide it after five seconds. • **Hide**- the VCS endpoint hides the output mute icon. **Default**: Hide with UI.	Web user interface

Parameter	Description	Configuration Method
SecondScreen Icon	Enable or disable the VCS endpoint to hide the secondscreen icon ( ) during a call. • **Show**- the VCS endpoint displays the secondscreen icon. • **Hide with UI**- the VCS endpoint displays the secondscreen icon and then hide it after five seconds. • **Hide**- the VCS endpoint hides the secondscreen icon. **Note**: it is hide with UI by default. It is not applicable to MeetingEye 400/VC200/VP59.	Web user interface

Muting the Microphone

You can mute the local microphone during a call, so that other parties cannot hear you.

Procedure

Do one of the following during a call:

- On your web user interface, go to **Home** > **Mute**.
- On your VCS,

  For MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/PVT950, on your remote control, press the Mute Key.

  For VP59, press the MUTE key on the phone.
- On your CTP20, tap the Mute key.
- On your CP960, tap one of the Mute keys.
- On your CP960 conference phone's touch screen, tap the Mute key.
- On your CPE90 wired expansion microphones, tap the Mute key.
- On your CPW90-BT Bluetooth wireless microphones, tap the Mute key.

  If video conferencing system is muted, the icon will appear on the local video.

Configuring Microphone Mute Mode

By default, if you enable the mute mode on a single microphone (CPE90/CPW90/CPW90-BT/VCM34), other microphones will be muted synchronously. To avoid picking up unwanted sounds from other

microphones, you can choose to mute a single microphone only, and other microphones keep unmuted. This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Setting** > **Audio**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Microphone Mute Mode	Configure the microphone mute mode. • **Synchronized**- if you mute/ unmute a microphone, other microphones will be muted/ unmuted simultaneously. • **Separated**- if you can only mute/unmute one microphones, others does not respond. **Default**: Synchronized.	Web user interface

Note:

If you use the remote control or CP960 conference phone to mute/unmute a microphone, all microphone will be muted/unmuted simultaneously.

Configuring the Keyboard Input Method

You can use the full keyboard on the screen to enter or to edit the data. You can enter characters using the enabled input method. On-screen keyboard on the monitor supports English and Russian input methods. This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Setting** > **General** > **General Information** > **Keyboard IME**.
2. 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. To remove a input method from the Enabled column, select the desired input method and then click .
5. To adjust the display order of the enabled input methods, select the desired input method, and click or .
   The input method shown at the top has the highest priority.

Configuring USB Storage

If you have high requirement for data security, you can disable the USB storage. After disabling the feature, you cannot use the USB flash drive to store recorded videos, screenshots or captured packets.

Procedure

1. On your web user interface, go to **Setting** > **USB Config**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **USB Config**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
USB Enable	Enable or disable the USB feature. **Note**: the default value is On. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Configuring Local Storage

MeetingEye 600/MeetingEye 400/VC200/VP59 allows you to store the images and recorded videos to local storage as well as the USB storage.

About this task

Note: The priority of local storage is lower than USB storage. When users disable USB storage, the captured screenshot and recorded files are saved on local storage automatically.

Procedure

1. On your web user interface, go to **Setting** > **USB Config**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **USB Config**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Local Storage Enable	Enable or disable the local storage feature. **Note**: the default value is On. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Configuring the Screenshot

You can take screenshots. This feature is not applicable to VP59.

Before you begin

If you want to save the screenshot to USB flash drive, make sure a USB flash drive is available.

If you want to save the screenshot to local storage (only applicable to MeetingEye 600/MeetingEye 400/VC200), make sure the local storage is enabled.

Procedure

1. On your web user interface, go to **Setting** > **USB Config**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **USB Config**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Taking Screenshots	Enable or disable to capture the screenshot by using the remote control. • **On** • **Off** **Default**: On.	Web user interface

Related tasks

Configuring USB Storage
Configuring Local Storage

Configuring to Automatically Upload Screenshots to the YMS

If you enable this feature, the endpoint can automatically upload the screenshots you take and save on the USB flash drive or local storage (only supported by MeetingEye 600/MeetingEye 400/VC200) to the YMS, which is convenient for you to view and manage the screenshots on the YMS.

Before you begin

Make sure the Screenshot feature is enabled.

If you want to save the screenshot to USB flash drive, make sure a USB flash drive is available.

If you want to save the screenshot to local storage (only applicable to MeetingEye 600/MeetingEye 400/VC200), make sure the local storage is enabled.

About this task

This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Setting** > **USB Config**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **USB Config**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Auto Upload Screenshot	Enable or disable the auto-uploading of screenshot to YMS. • **On** • **Off** **Default**: Disabled.	Web user interface

Related tasks

Configuring Local Storage
Configuring USB Storage
Configuring the Screenshot

Configuring Video Recording

The video recording feature is enabled by default and you can configure the feature.

Before you begin

If you want to record video to USB flash drive, make sure the USB flash drive is available.

If you want to record the video to the local storage (only applicable to MeetingEye 600/MeetingEye 400/VC200/VP59), make sure you enable the local storage.

Procedure

1. On your web user interface, go to **Setting** > **USB Config**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **USB Config**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Recording	Enable or disable the video recording feature on the system. **Default**: On.	Web user interface
Auto Recording	Enable or disable the system to start recording automatically once a call is established. • **On**- the system starts recording automatically once a call is established. • **Off**- the system does not start recording automatically once a call is established. **Note**: the default value is Off. Only the Recording feature is enabled can this feature be available.	Web user interface

Parameter	Description	Configuration Method
Stop Recording When Call Established	Enable or disable the system to stop recording automatically once a call is established. • **On**- the system stops recording automatically once a call is established. • **Off**- the system does not stop recording automatically once a call is established. **Default**: Disabled. It is not applicable to VP59.	Web user interface
Stop Recording When Call Ended	Enable or disable the system to stop recording automatically once a call is ended. • **On**- the system stops recording automatically once a call is ended. • **Off**- the system does not stop recording automatically once a call is ended. **Default**: On. It is not applicable to VP59.	Web user interface
Recording Notification	Enable or disable the system to show recording icon and recording prompt. • **On**- the recording icon and the duration are displayed on the system screen. • **Off**- the recording icon and the duration are not displayed on the system screen. **Default**: On.	Web user interface
WPP20 Recording Confirm	Enable or disable the system to allow the action that you use WPP20 to record. **Default**: On.	Web user interface
Dual Screen Recording Setting	Select the desired screen. You can record the video on the selected screen when you are using dual screen. • Screen 1+2: record video on dual screen • Screen 1 Only • Screen 2 Only **Default**: Screen 1+2. It is not applicable to MeetingEye 600/ MeetingEye 400/VC200/VP59.	Web user interface

Related tasks

Configuring USB Storage

Configuring Local Storage

Basic Settings for CP960 Conference Phone

- Adjusting Backlight of the CP960 Conference Phone

- Setting the Screen Saver for CP960 Conference Phone

Adjusting Backlight of the CP960 Conference Phone

You can change the backlight brightness of the CP960 conference phone. The backlight time means the delay time to turn off the backlight when the phone has been idle for a specified time.

About this task

You can configure the backlight time as one of the following types:

- **Always On**: the backlight is turned on permanently.
- **Specific time**: the backlight is turned off when the phone has been idle for a specified time.

Procedure

Do one of the following:

- On your web user interface, go to **Setting** > **Video Conference Phone**.

  For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information** > **Backlight Time**.
- On your CP960 conference phone, tap **Setting** > **Display** > **Backlight**.
- On your CP960, swipe down from the top of the screen to enter the control center.

  Drag the backlight slider.

Setting the Screen Saver for CP960 Conference Phone

The screen saver automatically starts when CP960 conference phone has been idle for the preset waiting time. You can set screen saver for the CP960 conference phone. The CP960 conference phone supports four types of screen savers: Clock, Colors, Photo Frame and Photo Table. You can choose anyone you like, and you can configure the waiting time before the CP960 conference phone starts the screen saver.

Procedure

1. On your CP960 conference phone, go to **Setting** > **Display** > **Screen Saver**.
2. select the corresponding screen saver type.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Wait Time	Configure the inactive time (minutes) before the CP960 conference phone starts screen saver. **Default**: 10 minute.	CP960 Conference Phone

Configuring * Key for Default Input

When you tap or press the * key in the T9 keyboard, the default character is "*". You can configure the default character that is displayed first when you tap or press the * key. It not applicable to MeetingEye 600/MeetingEye 400.

About this task

When using T9 keyboard to quickly tap or press the * key, you can still switch between "*", "@" and ".".

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
*** Key Default Input**	Customize the character that is displayed first when you tap or press the * key. • * • . • @ **Note**: the default value is *.	Web user interface

Configuring Whiteboard Tools

The VCS endpoint allows you to use the whiteboard for collaboration during a conference, hence you can set the default value for whiteboard tools. It is not applicable to MeetingEye 600/ MeetingEye 400/VP59.

Procedure

1. On your web user interface, go to **Setting** > **Collaboration Tools**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Tool	Set the default tool when initiating whiteboard. • Pen • Sharpie • Marker • Laser **Note**: the default tool is laser.	Web user interface
Color	Set the default color when initiating whiteboard. • Black • Blue • Aqua • Purple • Red • Green • Orange • Yellow • White **Note**: the default color is black.	Web user interface

Parameter	Description	Configuration Method
Style	Set the default color when initiating whiteboard. • Normal • Light • Bold **Note**: the default style is regular.	Web user interface

Configuring the Presentation Tools

The VCS endpoint allows you to share the content via wired/wireless sharing, AirPlay, or Mirocast presentation. Therefore, you set the default value for presentation tools. It is not applicable to MeetingEye 600/ MeetingEye 400/VP59.

Procedure

1. On your web user interface, go to **Setting** > **Collaboration Tools**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Tool	Set the default tool when sharing content. • Sharpie • Laser **Note**: the default tool is sharpie	Web user interface
Color	Set the default color when sharing content. • Black • Blue • Aqua • Purple • Red • Green • Orange • Yellow • White **Note**: the default color red	Web user interface

Configuring the Audio Settings

- Audio Output
- Audio Input
- Media Audio Input

- EQ Self Adaption
- Configuring the Noise Suppression
- Tones
- Codecs
- DTMF

Audio Output

- Audio Output Type
- Specifying an Available Audio Output

Audio Output Type

Note: The VCS endpoint selects only one audio device as the input or output source. Besides, the selected audio device cannot picking up or playing the sound simultaneously.

Model	Audio Output
MeetingEye 600	• **Auto**- selects the audio output with the highest priority. If the audio output with the highest priority is removed, the system will select the device with the second highest priority. The priority is MSpeaker II (VCH port) > VCS Phone > Line Output > USB to Line output > HDMI > Built-in Speaker. • **MSpeaker II** • **VCS Phone** • **Built-in Speaker** • **HDMI** • **Line Output** • **USB to Line output**
MeetingEye 400	• **Auto**- selects the audio output with the highest priority. If the audio output with the highest priority is removed, the system will select the device with the second highest priority. The priority is Soudbar/MSpeaker II (VCH port) > VCS Phone > USB to Line output > HDMI > Built-in speaker. • **MSpeaker II** • **VCS Phone** • **Built-in Speaker** • **HDMI** • **USB to Line output**
VC880/VC800/VC200/PVT980	• **Auto**- selects the audio output with the highest priority. If the audio output with the highest priority is removed, the system will select the device with the second highest priority. The priority is Soudbar/MSpeaker II (VCH port) > VCS Phone > HDMI> Line Output> USB to Line output. • **Soudbar/MSpeaker II** • **VCS Phone** • **HDMI** • **Line Output** • **USB to Line output**

Model	Audio Output
VC500/PVT950	• **Auto**- selects the audio output with the highest priority. The priority is Soudbar/MSpeaker II (VCH port) > VCS Phone > HDMI> USB to Line output. • **Soudbar/MSpeaker II** • **VCS Phone** • **HDMI** • **USB to Line output**
VP59	• **Auto**- selects the audio output with the highest priority. The priority is HDMI > USB to Line output > VP59 built-in speaker. • **Built-in Speaker** • **HDMI** • **USB to Line output**

Specifying an Available Audio Output

You can specify an available audio output if you do not want to use the default audio output device.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Audio** > **Audio Settings**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **Audio Settings**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Audio**.

     For VP59, tap > **Settings** > **Basic** > **Audio**.
   - On your CTP20, tap > **Settings** > **Basic** > **Audio**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Audio Output/Extended Audio Output	Specify the audio output for the system. The supported types are as follows: • **Auto**- selects the audio output device with the highest priority. • **VCS Phone** - selects the CP960 conference phone. (it is not applicable to VP59) • **HDMI** - select the built-in speaker of the monitor. If you connect two monitors to your system, only the HDMI 1 port is available for audio output. • **Line Output** –the speaker connected to MeetingEye 600/VC880/VC800/VC200/ PVT980 codec. • **USB to Line output** - the audio output device connected to the USB port on the MeetingEye 600/ MeetingEye 400/PVT980/ PVT950/VC500/VC200/VP59 via a USB to Line output adapter. **Note**: the default value is Auto. If VCS Phone is set as the audio output device manually or automatically, the audio input device must be VCS Phone.	Web user interface Endpoint CTP20

Note:

The system will start EQ self-adaption to optimize the acoustic effect automatically when the audio output switches to **HDMI** or **Line Output/USB to Line out**.

Related information

EQ Self Adaption

Audio Input

- Audio Input Type
- Specifying an Available Audio Input

Audio Input Type

Note: The VCS endpoint selects only one audio device as the input or output source. Besides, the selected audio device cannot picking up or playing the sound simultaneously.

Model	Audio Input
MeetingEye 600	• **Auto**—the system automatically selects the audio input with the highest priority. The priority is Microphone Array VCM34 > VCS Phone > Bluetooth Microphone > Built-in Microphone > Line Input > USB to Line input. • **Microphone Array VCM34** • **VCS Phone** • **Bluetooth Microphone** • **Built-in Microphone** • **Line Input** • **USB to Line input**
MeetingEye 400	• **Auto**—the system automatically selects the audio input with the highest priority. The priority is Microphone Array VCM34 > VCS Phone > Bluetooth Microphone > Built-in Microphone > USB to Line input. • **Microphone Array VCM34** • **VCS Phone** • **Bluetooth Microphone** • **Built-in Microphone** • **USB to Line input**
VC880/VC800/PVT980	• **Auto**—the system automatically selects the audio input with the highest priority. The priority is Ceiling Microphone Array VCM38 (not applicable to VC880) > Microphone Array VCM34 > VCS Phone > Bluetooth Microphone > Line Input > USB to Line input. • **Ceiling Microphone Array VCM38** • **Microphone Array VCM34** • **VCS Phone** • **Bluetooth Microphone** • **Line Input** • **USB to Line input**
VC200	• **Auto**—the system automatically selects the audio input with the highest priority. The priority is Microphone Array VCM34 > VCS Phone > Bluetooth Microphone > Built-in Microphone > USB to Line input. • **Microphone Array VCM34** • **VCS Phone** • **Built-in Microphone** • **Bluetooth Microphone** • **USB to Line input**

Model	Audio Input
VC500/PVT950	• **Auto**—the system automatically selects the audio input with the highest priority. The priority is Ceiling Microphone Array VCM38 (not applicable to VC500) > Microphone Array VCM34 > VCS Phone > Bluetooth Microphone > USB to Line input. • **Ceiling Microphone Array VCM38** • **Microphone Array VCM34** • **VCS Phone** • **Bluetooth Microphone** • **USB to Line input**
VP59	• **Auto**—the phone automatically selects the audio input with the highest priority. The priority is Bluetooth Microphone > Built-in Microphone > USB to Line input. • **Built-in Microphone** • **USB to Line input**

Specifying an Available Audio Input

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Audio** > **Audio Settings**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **Audio Settings**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Audio**.

     For VP59, tap > **Settings** > **Basic** > **Audio**.
   - On your CTP20, tap > **Settings** > **Basic** > **Audio**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Audio Input/Extended Audio Input	Specify the audio input for the system. The supported types are as follows: • **Auto** - select the audio output with the highest priority. • **Ceiling Microphone Array VCM38** (only applicable to VC800/PVT950/PVT980) • **Microphone Array VCM34** (not applicable to VP59) • **VCS Phone** - select the CP960 conference phone. (it is not applicable to VP59) • **Built-in Microphone** - select the built-in microphone of MeetingEye 600/MeetingEye 400/VC200. • **Bluetooth Microphone** - select the CPW90-BT Bluetooth wireless microphones. (it is not applicable to VP59) • **Line Input**- the audio input device connected to the Line In port on the VC800 or to the RAC In port on the MeetingEye 600/VC880/PVT980. • **USB to Line input** - the audio input device connected to the USB port on the MeetingEye 600/MeetingEye 400/VC200/VC500/PVT950/VP59 by using a USB to Line input adapter. **Default**: Auto.	Web user interface Endpoint CTP20
Line AEC	Enable or disable echo cancellation for line input device. • **On**- eliminate the echo to the line input devices. If you select an acoustic device (for example: a microphone) to be the line input, you can enable this configuration. • **Off**- do not eliminate the echo to the line input devices. If you select a non-acoustic device (for example: a mobile phone) to be the line input, you can disable this configuration. **Note**: the default value is Off. This configuration is available only when Audio Input is set to Line Input/USB to Line input. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Parameter	Description	Configuration Method
Audio Line In	Configure the volume of line input device. **Note**: • **Valid value**: Integer from -50 to 50dB. • The default value 0 means to use the default sending volume. The value you set is based on the default value. • This configuration is available only when Audio Input is set to Line Input/USB to Line input. If you change this parameter, the system will reboot to make the change take effect. • It is not applicable to MeetingEye 400/VP59.	Web user interface

Note:

If VCS Phone is set as the audio output device manually or automatically, the audio input device must be VCS Phone or VCS Phone+Wireless Microphone.

Related information

Audio Input Type

Media Audio Input

When the Endpoint is connected to both a microphone and other media audio inputs (such as connected to a computer to play audio), you need to configure the type of media audio input, so that the mix input can be realized. The sound from the media audio input device is mixed to the local output by default and can be mixed to the remote output. This feature is not applicable to VP59.

Note: If the microphone is connected to the device via Line Input or USB to Line Input, you should not select the interface to which the microphone is connected when using the media audio input, otherwise there may be a strident sound.

- Configuring Media Audio Input

Configuring Media Audio Input

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Audio** > **Audio Settings**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **Audio Settings**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Audio**.

     For VP59, tap > **Settings** > **Basic** > **Audio**.
   - On your CTP20, tap > **Settings** > **Basic** > **Audio**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Media Audio Input	Specify the media audio input connected to the device. The supported types are as follows: • **Off**- not use any media audio input. • **Line Input (No access)**- the media audio input device connected to RCA In port on VC880 or to the Line In port on VC800. • **USB to Line input (No access)**- the media audio input device connected to the USB port on MeetingEye 600/MeetingEye 600/VC500/VC200 via a USB to line input adapter. **Default**: Disabled.	Web user interface Endpoint CTP20

EQ Self Adaption

The EQ self adaption allows the device to optimize the acoustic effect. The EQ self adaption is enabled by default. System supports manual EQ self adaption adjustment.

When your environment meets the following audio input and output, you can manually trigger the system to enter the EQ self adaption adjustment in the idle state.

For MeetingEye 600/ MeetingEye 400/VC880/VC800/VC500/PVT980/PVT950**:**

- When the audio output switches to **HDMI** or **Line Output/USB Line output** and you connect an audio input device, click **Start EQ Self Adaption** to optimize the acoustic effect.

For VP59/VC200/VC21 endpoint:

- When the audio output switches to **HDMI** or **Line Output/USB Line output**, click **Start EQ Self Adaption** to optimize the acoustic effect.
- After the factory reset, when you connect a monitor to the system for the first time.
- Configuring the EQ Self-adaption

Configuring the EQ Self-adaption

Procedure

1. On your web user interface, go to **Setting** > **Video & Audio** > **Audio Settings**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
EQ Self-Adaption	Enable or disable the EQ self-adaption feature on the system. **Default**: On.	Web user interface
Start EQ Self Adaption	Starts the EQ self-adaption feature. **Note**: This configuration appears only when the system satisfies the following conditions: • Enable the **EQ Self Adaption** feature. • The VCS phone is not selected as the audio output device. • Connect an audio input to the device (it is only applicable to MeetingEye 600/VC880/VC800/VC500/PVT980/PVT950) • The audio output is **HDMI** or **Line Output**/**USB Line out**.	Web user interface

Configuring the Noise Suppression

The impact noises in the room are picked-up, including paper rustling, coffee mugs, coughing, typing and silverware striking plates. These noises, when transmitted to remote participants, can be very distracting. You can enable the Transient Noise Suppressor (TNS) to suppress these noises. You can also enable the Noise Barrier feature to block these noises when there is no speech in a call.

Procedure

1. On your web user interface, go to **Setting** > **Audio** > **Noise Suppression**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **Noise Suppression**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Temporal Noise Shaping(TNS)	Enable or disable the Transient Noise Suppressor (TNS). • **On**—it can reduce the noise volume temporarily and block the noise in the voice. • **Disabled** **Default**: On.	Web user interface
Noise Barrier	Enables or disabled the noise barrier feature. • **On**—it can block the noise in the non-speech process. • **Off** **Default**: Disabled.	Web user interface

Tones

When receiving a message, 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.

- Supported Tones
- Custom Tones Formats
- Customizing Tones

Supported Tones

The system supports tones in the following countries. The tone set is a predefined by each country according to different device status. The tones of different countries varies.

Available tone sets for the system are described as below:

Australia	Austria	Brazil	Belgium
Chile	China	Czech	Denmark
Finland	France	Germany	Great Britain
Greece	Hungary	Lithuania	India
Italy	Japan	Mexico	New Zealand
Netherlands	Norway	Portugal	Spain
Switzerland	Sweden	Russia	United States

Custom Tones Formats

You can customize different tones for the system except for the default tone.

The custom tones formats are as below:

E1,E2,E3,E4,E5,E6,E7,E8 (you can configure up to 8 different tones which are separated by commas)

En=[!][F1][+F2][+F3][+F4] /Duration

Parameter explanation:

- 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.
- An exclamation mark “!” before tones : it means that the tone only rings once.

(for example, !250/200, 0/1000, 200+300/500, 500+1200/800，600, 600+700+800+1000/2000) means playing tones once.

Customizing Tones

Procedure

1. On your web user interface, go to **Setting** > **Tones**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Select Country	Select Custom.	Web user interface
Ring Back	Customize the ring-back tone for the VCS codec **Note**: the default value is blank. When it is blank, the American tones are enabled.	Web user interface
Busy	Customize the busy tone for the VCS codec. **Note**: the default value is blank. When it is blank, the American tones are enabled.	Web user interface
Call Waiting	Customize the call waiting tone for the VCS codec. **Note**: the default value is blank. When it is blank, the American tones are enabled.	Web user interface
Auto answer	Customize the auto answer tone for the VCS codec. **Note**: the default value is blank. When it is blank, the American tones are enabled.	Web user interface

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. The administrator can configure the codec and its priority for the devices.

- Audio Codec
- Video Codecs

Audio Codec

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.

- Supported Audio Codecs
- Configuring Audio Codecs

Supported Audio Codecs

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

Audio Codec	Algorithm	Bit Rate	Sample Rate (Effective)	Reference
Opus	opus	8-12 Kbps 16-20 Kbps 28-40 Kbps 48-64 Kbps 64-128 Kbps	8 Ksps 12 Ksps 16 Ksps 24 Ksps 48 Ksps	RFC 6716
ARES	ARES	8-64kpbs	48 Ksps	None
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
G.722.1		24 Kbps	16 or 32 Ksps	RFC 5577
G.722	G.722	64 Kbps	16 Ksps	RFC 3551
PCMU	G.711 u-law	64 Kbps	8 Ksps	RFC 3551
PCMA	G.711 a-law	64 Kbps	8 Ksps	RFC 3551
G729	G.729	16 Kbps	8 Ksps	RFC 3551

The Opus codec supports the following audio bandwidths:

Abbreviation	Audio Bandwidth	Sample Rate (Effective)
NB (narrowband)	4 kHz	8 kHz
MB (medium-band)	6 kHz	12 kHz
WB (wideband)	8 kHz	16 kHz
SWB (super-wideband)	12 kHz	24 kHz
FB (fullband)	20 kHz	48 kHz

Configuring Audio Codecs

Procedure

1. On your web user interface, go to **Account** > **Codec** > **Audio Codec**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enabled	Configure the audio codecs to be used. **Note**: You can move the disabled codec to this field.	Web user interface

Parameter	Description	Configuration Method
Disabled	Configure the audio codecs that are not used. **Note**: you can move the enabled codec to this field.	Web user interface
Opus Sample Rate	Configure the sample rate of the opus audio codec. • Opus-FB(48KHz) • Opus-SWB(24KHz) • Opus-WB(16KHz) • Opus-MB(12KHz) • Opus-NB(8KHz) **Default**: Opus-FB(48KHz).	Web user interface
Special audio codec byte sequence	Enable or disable the special audio codec byte sequence. • **Off—**keep the current codec byte sequence. • **On—**different devices have different definition about audio codec byte sequence, which may lead to the audio incompatibility problems between Yealink and certain devices. You can enable this feature to solve these incompatibility problems. **Default**: Disabled.	Web user interface

Video Codecs

The video codecs 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.

- Supported Video Codecs
- Configuring Video Codecs
- Selecting an H.265 Mode

Supported Video Codecs

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

Video Codecs	Static NAT/Type	Bit Rate	Frame Rate	Frame Size
H.264 HP	H264/90000	90—2048 kbps	5—30 fps	Tx: 360P, 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	Static NAT/Type	Bit Rate	Frame Rate	Frame Size
H.263+	H263/90000			Tx: CIF Rx: CIF
H.265 (it is not applicable to VP59)	H265/90000			Tx: 360P, 540P, 720P, 1080P Rx: Conventional Size Below 1080P

Note: H.265 video codec is only applicable to a one-way video call, and the VCS cannot be connected to a third-party camera. The VCS will negotiate with other parties to use the H264 High profile video codec automatically when more people join the call.

Tip: H.263 video codec consumes twice as much bandwidth as H.264 High profile video codec and four times as much as H.265 video codec.

Configuring Video Codecs

Procedure

1. On your web user interface, go to **Account** > **Codec** > **Video Codec**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enabled	Configure the enabled video codecs for the system to use. **Note**: You can move the disabled codec to this field.	Web user interface
Disabled	Configure the disabled video codecs. **Note**: you can move the enabled codec to this field.	Web user interface
SVC-T(it is not applicable to MeetingEye 600/MeetingEye 400/VC200/VP59)	This feature is only applicable to H.264/H.264 video codecs. **Default**: Disabled.	Web user interface

Selecting an H.265 Mode

You can select VBR or CBR for the H.265 video codec according to your network bandwidth. It is only applicable to MeetingEye 600/MeetingEye 400/VC200.

Procedure

1. On your web user interface, go to **Account** > **Codec** > **Video Codec**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
H.265 Mode	H.265 video codec. • **VBR**- the output data rate of the H.265 codec varies per time segment. You can save nearly half the bandwidth. • **CBR**- the output data rate of the H.265 codec is constant. If the latency issue appears in the call or video image is abnormal, it may result from packet loss, you can select this value to try to fix this issue. **Default**: VBR.	Web user interface

DTMF

DTMF is the signal sent from the system to the network, which is generated when pressing the keypad during a call. Each key pressed generates one sinusoidal tone of two frequencies. One is generated from a high-frequency group and the other from a low-frequency group.

- DTMF Keypad
- Transmission Ways of DTMF
- Setting DTMF Transmission Method for SIP Protocol
- Configuring DTMF for H.323 Protocol

DTMF Keypad

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)). The switch can decode the frequency group and locate the corresponding key.

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

Transmission Ways of DTMF

Three ways to transmit DTMF tones are as below: RFC2833, INBAND, SIP INFO.

RFC 2833

In-band transmission method. DTMF tones are transmitted by RTP, and the RFC 2833 packets are marked by TeleponeEvent (RTP PayloadType). One DTMF tone consists of several RTP packets with the same timestamps, which can be used to identify the same key. If the End bit of a RTP packet is 1, the packet is the last DTMF tone. The default telephoneEvent is 101, but you can change it.

INBAND

In-band transmission method. DTMF tones are transmitted together with the voice band. By analyzing the high frequency and the low frequency of the RTP packets, the device can identify the corresponding key.

SIP INFO

Out-band transmission method. DTMF tones are transmitted by SIP signaling path. The SIP INFO message can transmit DTMF tones in three ways: DTMF, DTMF-Relay and Telephone-Event.

Setting DTMF Transmission Method for SIP Protocol

You can set the DTMF transmission method for the SIP protocol when using a SIP account, placing SIP IP call, or logging in to Zoom, Pexip, BlueJeans, EasyMeet, or a custom third-party platform.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call**.
   - On your web user interface, go to **Account** > **VC Platform** > **Platform Type** > **Zoom/Pexip/ BlueJeans/Custom**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **SIP IP Call**.

     For VP59, tap > **Settings** > **Advanced** > **Account** > **SIP IP Call**.
   - On your CTP20, tap **Settings** > **Advanced** > **Account** > **SIP IP Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
DTMF Type	Configure the DTMF type. • **INBAND**—DTMF is transmitted in the voice band, together with the general RTP voice packet. • **RFC2833**—DTMF digits are transmitted by RTP packet which is compliant to RFC2833. • **SIP INFO**—DTMF digits are transmitted by SIP INFO. • **RFC2833+ SIP INFO**—DTMF digits are transmitted by RFC 2833 and the SIP INFO. **Default**: RFC2833.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
DTMF Info Type	Configure the DTMF info type when DTMF type is set to SIP INFO or RFC2833+SIP INFO. • DTMF-Relay • DTMF • Telephone-Event **Default**: DTMF-Relay.	Web user interface Endpoint CTP20
DTMF Payload Type (96~127)	Configure the value of DTMF payload. **Default**: 101.	Web user interface

Configuring DTMF for H.323 Protocol

When using an H.323 account or logging into the third-party platform, you can set the DTMF transmission method for the H.323 protocol.

Procedure

1. On your web user interface, go to **Account** > **H.323**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
DTMF Type	Configure the DTMF type. • **INBAND**—DTMF is transmitted in the voice band, together with the general RTP voice packet. • **Auto**—the system automatically negotiates the way (INBAND, RFC2833 or SIP INFO) to transfer DTMF digits. **Default**: Auto.	Web user interface Endpoint CTP20

Configuring Video Settings

- Display Layout Settings
- Changing the Video Input Source
- Configuring HDMI Extended Display by VP59
- Specifying Content to the Secondary Screen
- Adjusting the Monitor Display Proportion
- Selecting Video Frame Rate and Resolution
- Configuring the Monitor Resolution
- Configuring VC200 Experimental Access (Auto Framing)
- Showing the Site Name to Remote Parties

Display Layout Settings

- Setting the Default Layout for a Single Screen
- Setting the Default Layout for Dual Single Screen
- Configuring Change Layout by Content Sharing
- Configuring Auto Zoom In Content for a Single Screen
- Hiding Local Video Image in Equal Layout
- Configuring Hide Local Video When PIP
- Configuring Multi-Camera Default Layout
- Configuring Voice Activation
- Configuring the View Switching
- Configuring Preview Local

Setting the Default Layout for a Single Screen

When only one monitor is connected to the system, you can configure the default layout when a call is established.

About this task

For VP59, if you do not connect a monitor to it, it is a single screen by default.

Procedure

1. On your web user interface, go to **Setting** > **Monitor** > **Layout**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Display** > **Remote Session (In A Call)** > **Single Display**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Default Layout of Single Screen (it is only applicable to VC200/VC880/ VC800/VC500/ VP59)	Configure the default layout of a single screen when a call is established. • **Remote big Local small**—the remote video image is displayed in the large window and the local video image is displayed in the small window at the screen bottom. • **Remote Full screen**—the remote video image is displayed in full screen. • **Equal NxN**—the remote and the local video images are displayed in the same size. • **Picture in Picture**—the remote video image is displayed in a large window, and the local video image is reduced to a thumbnail in the bottom-right corner of the large window. (it is not applicable to VP59) **Default**: Picture-in-picture. For VP59, the default one is Remote big Local small.	Web user interface

Parameter	Description	Configuration Method
Not in Content Sharing (it is only applicable to MeetingEye 600/ MeetingEye 400)	Configure the default layout of a single screen when a call is established and has no content sharing. • **1+N—**the selected video image is displayed in the large window and other video images are displayed in small windows. • **Selected Speaker**—the selected video image is displayed in full screen. • **Equal NxN**—the remote and the local video images are displayed in the same size. • **Picture in Picture**—the remote video image is displayed in a large window, and the local video image is reduced to a thumbnail in the bottom-right corner of the large window. **Default**: Picture-in-picture.	Web user interface
While Content Sharing (it is only applicable to MeetingEye 600/ MeetingEye 400)	Configure the default layout of a single screen when a call is established and has content sharing. • **1+N—**the selected video image is displayed in the large window and other video images are displayed in small windows. • **Selected Speaker**—the selected video image is displayed in full screen. • **Equal NxN**—the remote and the local video images are displayed in the same size. **Default**: 1+N.	Web user interface

Setting the Default Layout for Dual Single Screen

When you connect two monitors to the system, you can configure the default layout for each monitor when a call is established. This feature is only applicable to MeetingEye 600.

Procedure

1. On your web user interface, go to **Setting** > **Display** > **Dual Display**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
HDMI 1	Configure the default video layout for HDMI 1 when a call is established. • **1+N**—the remote video image is displayed in the large window and the local video image is displayed in a small window at the screen bottom. • **Selected Speaker**—the remote or the local video image is displayed in full screen. • **Equal NxN**—the remote and the local video images are displayed in the same size. • **Picture in Picture**—the remote video image is displayed in a large window, and the local video image is reduced to a thumbnail in the bottom-right corner of the large window. **Note**: when no participant shares content, the remote video image is displayed in full screen; when a participant shares content, the video layout is displayed in the PiP (Picture-in-Picture) mode by default.	Web user interface
HDMI 2	Configure the default video layout for HDMI 2 when a call is established. • **Local**—the local video image is displayed in HDMI 2 when a call is established. • **Remote Full screen**—the remote video image is displayed in HDMI 2 when a call is established. • **While Content Sharing**—after the call is established with participant sharing content, the content will be displayed in HDMI2. **Note**: when no participant shares content, the local video image is displayed in HDMI 2; when a participant shares content, the content is displayed in HDMI 2 by default.	Web user interface

Configuring Change Layout by Content Sharing

The Change Layout by Content Sharing is enabled by default. During a call, when you are presenting on the endpoint with a single screen connected to, the layout mode is changed into 1+N or voice activated(except for VP59) mode automatically no matter what the current layout mode is, and the content is enlarged and displayed on the screen. If the Change Layout by Content Sharing is disabled when you are presenting during a call, the current mode is not changed in other modes, but the content is enlarged and displayed on the screen. It is not applicable to MeetingEye 600/MeetingEye 400.

About this task

If the Change Layout by Content Sharing is disabled, the display layout when you are presenting during a call is shown as below:

The current layout	Display layout after you are making a presentation
Picture-in-picture:	The display layout is changed into 1+N, and the content is enlarged and displayed in the screen.
1+N	The display layout is still 1+N, but the content is enlarged and displayed in the screen.
Selected Speaker	The display layout is still Selected Speaker, but the content is displayed in full screen.
Equal N×N	Every participant is given equal prominence in equal-sized panes.

Procedure

1. On your web user interface, go to **Setting** > **Monitor** > **Layout**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Change Layout by Content Sharing	Enable or disable **Change Layout by Content Sharing**. **Default**: On.	Web user interface

Related information

Configuring Content Sharing

Configuring Auto Zoom In Content for a Single Screen

If the endpoint is connected to a single screen, and you do not need to automatically enlarge the presentation when you are presenting, you can disable the Auto Zoom In Content feature. The screen keeps the original display layout and will not change the enlarged object. It is not applicable to MeetingEye 600/ MeetingEye 400/VP59.

Procedure

1. On your web user interface, go to **Setting** > **Monitor** > **Layout**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Display** > **Layout**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Auto Zoom In Content	Enable or disable **Auto Zoom In Content**. **Note**:This configuration can be configured only when the **Change Layout by Content Sharing** feature is disabled, and is enabled by default.	Web user interface

Related tasks

Configuring Change Layout by Content Sharing

Hiding Local Video Image in Equal Layout

If you want to focus on the far sites or the PC content in a call (its video layout is equal layout), you can choose to hide the local video image.

Procedure

1. On your web user interface, go to **Setting** > **Monitor** > **Layout**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Display** > **Layout**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Equal Display Local	Select **Off** to hide local video image when the video layout is equal. • **On**—the local video image is shown. • **Off**—the local video image is hidden. **Default**: On.	Web user interface

Configuring Hide Local Video When PIP

In the PIP (Picture-in-Picture) mode, the local video image is always shown at the bottom corner of the screen. If you enable hide local video when PIP, the local video image is automatically hidden within 5 minutes if there is no operation from the remote control/CTP20/CP960. This feature is not applicable to VP59.

About this task

PIP mode only takes effect on the local layout. In a two-way video call, the video of one end is displayed in a large window, and the video of the other end is reduced to a thumbnail in the bottom-right corner of the large window. In the YMS/Cloud conference, the large window displays the conference layout and the small window displays the local video.

Procedure

1. On your web user interface, go to **Setting** > **Monitor** > **Layout**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Display** > **Layout**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Hide Local Video When PIP	Enable or disable the local video image to hide in the PIP (Picture-in-Picture). • **On**—the local video image is hidden in the PIP. • **Off**—the local video image is shown in the PIP. **Default**: Disabled.	Web user interface

Configuring Multi-Camera Default Layout

During a call, if you connect VCC22, all the local video streams are synthesized to one video stream, and sent to the far site. You can configure the default layout when you connect multiple cameras and set the camera you want to highlight. It is not applicable to MeetingEye 600/MeetingEye 400/VC200/VC500/PVT950/VP59.

Procedure

1. On your web user interface, go to **Setting** > **Camera** > **Camera**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Multi-camera Default Layout	Configure the default camera layout when you use multiple cameras. The supported layouts are described as below: • 1+N • Selected Speaker • Average **Note**: the default value is 1+N.	Web user interface
Select a Camera	Select the camera you want to highlight. **Note**: The first connected camera. This configuration appears only if **Multi-camera Default Layout** is set to **1+N** or **Selected Speaker**.	Web user interface

Note: It is not available if you only connect one VCC22 to the system and you disable the main camera or the connected VCC22.

Configuring Voice Activation

Voice activation displays the active speaker in largest pane. Other participants are displayed in a strip beside the active speaker. When a new speaker is identified, the image of the previous speaker is replaced by the new speaker. Other video images remain unchanged.

About this task

Note:

Voice activation is only applicable to PVT980/PVT950/VC880/VC800 with a multipoint license, not applicable MeetingEye 600/MeetingEye 400/VC500/VC200/VP59.

Voice activation works only when the conference call has more than two participants.

Procedure

1. On your web user interface, go to **Setting** > **Built-in MCU Setting** > **Conference Setting**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Voice Activation	Enable or disable the voice activation feature. **Default**: On.	Web user interface
Voice Hold Active Duration	Configure the voice activation interval. **Note**: the default value is 1 second. If the voice duration of a speaker is greater than 1 second, the video image of this speaker is displayed in largest pane.	Web user interface

Configuring the View Switching

The view switching allows the video images on the monitor change automatically. It is initiated when the number of participants exceeds the number of windows in the selected video layout.

- **Average Mode**: Up to 9 video images can be displayed in the Equal N×N layout. When the number of participants exceeds 9, all participants' video images will be switched automatically. The video image of the active speaker is indicated by an orange border. If you share content, the PC content is fixed at the top-left corner and will not be switched automatically.
- **1+N Mode**: Up to 8 video images can be displayed in the Speaker View layout and the 1+N layout. When the number of participants exceeds 8, all participants' video images (except the active speaker) will be switched automatically. If you share content, the PC content is given prominence in the largest pane. The active speaker is fixed at the bottom-left corner, and other video images will be switched automatically.

Note:

The view switching is only applicable to VC880/VC800/PVT980/PVT950 system with a multipoint license. It is not applicable MeetingEye 600/MeetingEye 400/VC500/VC200/VP59.

- Configuring the Average Mode
- Configuring 1+N Mode

Configuring the Average Mode

In Equal N×N layout, when the number of participants exceeds 9, all participants' video images will be switched automatically. You can configure the switching mode.

Procedure

1. On your web user interface, go to **Setting** > **Built-in MCU Setting** > **Video Layout** > **Average Mode**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
View Switching Interval	Configure the view switching interval. **Note**: the default value is 30 seconds. The video images will be switched automatically every 30 seconds.	Web user interface
Single View Round	Switches one video image at a time.	Web user interface
Full Screen Round	Switches all video images at a time.	Web user interface

Configuring 1+N Mode

In Speaker View layout and 1+N layout, up to 8 video images can be displayed. When the number of participants exceeds 8, all participants' video images will be switched automatically. But the video images of active speaker and the content are not be switched.

Procedure

1. On your web user interface, go to **Setting** > **Built-in MCU Setting** > **Video Layout** > **1+N Mode**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
View Switching Interval	Configure the view switching interval. **Note**: the default value is 30 seconds. The video images will be switched automatically every 30 seconds.	Web user interface
View Round	Configure the number of video images to be switched at a time. **Note**: the default value is 1. **Valid value**: 1 - 7.	Web user interface
Full Screen Round	Switches all video images (except for the active speaker and the content) at a time.	Web user interface

Configuring Preview Local

If there is no local screen in the current layout (such as remote full screen or split mode does not display local), the local thumbnail image cannot be viewed when adjusting the local camera, so the camera cannot be accurately adjusted. If you enable preview local, when there is no local screen in the current layout, the local small window is superimposed in the lower right corner of the screen when you adjust the local camera. After no PTZ operation within five seconds, the local thumbnail image disappears.

Procedure

1. On your web user interface, go to **Setting** > **Monitor** > **Layout**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Display** > **Layout**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Preview Local	Enable or disable to view the local thumbnail image by adjusting camera when there is no local screen in the current layout. • **On**-You can view the local thumbnail image when you adjust the camera. • **Off**-You can not view the local thumbnail image when you adjust the camera. **Default**: On.	Web user interface

Changing the Video Input Source

The system supports the video input sources both from the camera and the PC. If you do not share the contents during the call, the video input source is camera by default; if not, switch the video input source to Camera+PC to zoom in the screen You can change the video input source and select the content to be displayed on the screen. This feature is not applicable to VP59.

Procedure

Do one of the following during a call:

- On your web user interface, go to **Home** > **Input Selection**.
- On your remote control, press the OK key to open **Talk Menu** and go to **More** > **Input Selection**.
  - If you select **PC**, the remote video image is displayed in a large window, and the PC content is displayed in a small window (Picture-in-Picture mode).
  - If you select **Camera+PC**, the PC content is displayed in a large window, and other video images are displayed in small windows.
  - If you select **Camera**, the remote video image is displayed in a large window, and the local video image is displayed in a small window (Picture-in-Picture mode).

Configuring HDMI Extended Display by VP59

After you enable the HDMI feature on VP59, if you connect a monitor to the phone during a video call, the video images of the remote party and the shared content are displayed on the monitor, and the call control page is displayed on phone screen.

Procedure

1. On VP59, tap > **Settings** > **Basic** > **General** > **HDMI**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
HDMI	Enable or disable the HDMI feature. **Default**: On.	VP59

Specifying Content to the Secondary Screen

When you connect dual display screen, you can specify the content to be displayed on the secondary monitor. It is not applicable to MeetingEye 600/MeetingEye 400/VC200/VP59. For more information about the video image displayed on two screens when you use MeetingEye 600, refer to Setting the Default Layout for Dual Single Screen.

Procedure

1. On your web user interface, go to **Setting** > **Video** > **Output For Display 2**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Output in IDLE	Specify the content to be displayed on the secondary monitor when the system is idle. • **Auto**—The secondary monitor displays the content in this priority: PC>Active Camera>VCS Camera>Camera N. • **PC**—The secondary monitor displays the PC content. • **Active Camera**—The secondary monitor displays the video images from the currently active camera. If you change the active camera, the video image on the secondary monitors also changes. For example, if you use the VC880/ VC800/PVT980 camera as the active camera first, and then you select the preset of camera 1 (The **Preset Synchronize With Active Camera** feature is enabled, and the active camera becomes camera 1 at this time), the secondary monitor displays the image of camera 1. • **VCS Camera** (it is not applicable to VC880)—The secondary monitor displays the video images from the camera built-in VCS. • **Camera N**—The secondary monitor displays the video images from the connected camera N. **Note**: the default value is Auto.	Web user interface

Parameter	Description	Configuration Method
Default Output in Call	Specify the content to be displayed on the secondary monitor during a call. • **Auto**—The secondary monitor displays the content in this priority: PC> Local camera. • **PC**—The secondary monitor displays the PC content. • **Local**—The secondary monitor displays the video images from the local camera. **Note**: the default value is Auto. After you specify “Output for Display 2”, you can still modify the content to be displayed on the secondary monitor temporarily during a call via CTP20 or remote control. But the next time you establish a call, the content to be displayed on the secondary monitor is controlled by the “Output For Display 2” .	

Related tasks

Configuring Preset Synchronize With Active Camera

Adjusting the Monitor Display Proportion

If you use the TV as the display device, the TV might not display the entire video image. To solve this problem, you can adjust the display proportion to display the entire video image as you need. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your VCS, go to **More** > **Settings** > **Basic** > **General** > **Display**.
   - On your CTP20, tap > **Settings** > **Basic** > **General** > **Display**.
2. Adjust the monitor display.
3. Save the change.

Selecting Video Frame Rate and Resolution

To transfer a clear and smooth video, you can specify the maximum frame and resolution for local video according to the network environment.

About this task

Note: High video frame rate or high resolution requires large bandwidth. For the optimal video display, we recommend that you select the corresponding frame rate, resolution, and the content video mode according to your occupied bandwidth (the bandwidth ration between the video and the content is 1 to 2). For MeetingEye 600/ MeetingEye 400, up to 4K30fps can be supported.

Procedure

1. On your web user interface, go to **Setting** > **Video** > **People Video**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **People Video**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enable 4K (it is only applicable to MeetingEye 600/MeetingEye 400)	Enable or disable 4K for the local video when you are in a point-to-point video call or on the idle screen. **Default**: Disabled.	Web user interface
Content Video Mode (it is only applicable to MeetingEye 600/ MeetingEye 400)	Enable or disable the content video mode for the local video when you are in a point-to-point video call or on the idle screen. • Fluency First: when the bandwidth is insufficient, the system will display the people video with decreasing the resolution first. • Definition First: when the bandwidth is insufficient, the system will display the people video with decreasing the frame rate first. When the frame rate is less than 15fps, the system will decrease the resolution. **Default**: Fluency First.	Web user interface
Enable 60fps	Enable or disable 60fps for a video call. **Note**: the default value is enabled. It is not applicable to VC200/PVT950.	Web user interface
Frame	Configure the maximum frame rate of the video. • 5 frame rate • 15 frame rate • 30 frame rate • 60fps—this option appears only when you enable 60fps. **Default**: 30 fps.	Web user interface

Parameter	Description	Configuration Method
Resolution	Configure the maximum resolution of the video. • 1080P • 720P • 360P • 4K—this option appears only when you **Enable 4K**. It is only applicable to MeetingEye 600/MeetingEye 400. **Default**: 1080P.	Web user interface

Note:

If both parties do not use H.265 codec, and choose to use WDR exposure mode and 60fps, the call will switch to auto exposure mode automatically. For more information, refer to Adjusting the Exposure.

Configuring the Monitor Resolution

You can specify the resolution for the monitor.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Display/Monitor** > **Output Resolution**.
   - On your CP960 conference phone, go to **Settings** > **Display** > **Output Resolution**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
HDMI 1	Set the output resolution of the HDMI 1 display device. • **Auto**-select the highest output resolution automatically. • The available output resolutions (The available resolutions depend on the monitor you are using). **Default**: Auto.	Web user interface CP960 Conference Phone
HDMI 2 (it is not applicable to MeetingEye 600/MeetingEye 400/VC200/VP59)	Enable or disable the HDMI 2 display. **Default**: On.	Web user interface

Parameter	Description	Configuration Method
HDMI 2 (it is not applicable to MeetingEye 400/VC200/VP59)	Set the output resolution of the HDMI 2 display device. • **Auto**-select the highest output resolution automatically. • The available output resolutions (The available resolutions depend on the monitor you are using). **Default**: Auto. It is configurable only when HDMI 2 display is enabled.	Web user interface CP960 Conference Phone

Configuring VC200 Experimental Access (Auto Framing)

The experimental access feature currently includes the auto framing, which is mainly based on face detection. Real-time detection and position tracking are performed on all faces in the conference room. The camera can be automatically adjusted according to the number of participants and position changes. All participants are covered in the output screen.

About this task

⚠ **Attention:** Note the following points when using the VC200 experimental access feature:

- After the auto framing is enabled, other devices cannot perform PTZ control on the VCS camera, and the camera preset function does not take effect.
- The number of face detections on the VC200 can support up to 8 faces simultaneously in a range of 5 meters.
- The experimental access is a new feature that Yealink is exploring. It is available to users for trial use in advance, and may have unstable problems. It is not recommended as a daily function.

Procedure

1. On your web user interface, go to **Security** > **Experimental Access**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Experimental Access	It is configurable only after the experimental access is enabled. **Note**: the default value is Off. It takes 5 consecutive confirmations to activate the experimental access feature.	Web user interface

Parameter	Description	Configuration Method
Auto Framing	After enabled, the VC200 can automatically adjust the camera according to the number of participants and position changes, and output all participants' screens. The panorama is output when no person is detected in the initial state or in the camera angle. **Note**: the default value is Off. It is configurable only when the experimental access feature is enabled.	Web user interface

Showing the Site Name to Remote Parties

Showing the local site name to the remote parties allows remote parties to better identify the site when making multi-way video calls. You can also customize the site name position, the text size, the color, and set the background color and background transparency of the text. It is not applicable to MeetingEye 600/ MeetingEye 400/VP59.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Show Site Name On Video**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Show Site Name	Configure whether to show the site name to the remote parties during a call. **Default**: Disabled.	Web user interface
Location	Configure the position where the local site name is displayed on the screens of the remote parties during a call. • Upper Left • Lower Left • Upper Right • Lower Right **Default**: Lower Right.	Web user interface
Text Size	Configure the text size of the local site name to be displayed on the screens of the remote parties during a call. • Large • Middle • Small **Default**: Middle.	Web user interface

Parameter	Description	Configuration Method
Test Color	Configure the text color of the local site name to be displayed on the screens of the remote parties during a call. • White • Black • Gray • Red • Orange • Yellow • Green • Aqua • Blue • Purple **Default**: White.	Web user interface
Background Color	Configure the text background color of the local site name to be displayed on the screens of the remote parties during a call. • White • Black • Gray **Default**: Gray.	Web user interface
Background Transparency	Configure the text background transparency of the local site name to be displayed on the screens of the remote parties during a call. • Opaque • Semitransparent • Transparent **Default**:	Web user interface

Note: The site name is not displayed in the following cases:

- PVT980/PVT950/VC880/VC800/VC500 uses the H265 video codec to establish a call

  VC200 uses the H263 protocol to establish a call
- PVT980/VC880/VC800 uses built-in MCU to establish a local conference

Tip: In a cloud/YMS conference call, the site name set by Yealink Meeting Management Platform/Yealink Meeting Server is displayed in the top-left corner by default. To avoid name superposition, you can disable this feature on the Yealink Meeting Management Platform/Yealink Meeting Server or the endpoint.

Related tasks

Configuring the Site Name

Configuring Content Sharing

Content sharing is to send a secondary stream through a dual-stream protocol or a mix sending method, so that the remote party can share your local content presentation. If the far site does not support the dual-stream protocol, you can select the Mix Sending feature to mix the video and content, and then send them to the far site in one stream.

By default, the PC presentation is enabled on the system when the content is sharing. If you do not want the system to automatically start a PC presentation, you can disable it. You can configure the mode, the frame rate and the resolution for the shared content.

For more information, refer to Yealink Meeting Server User Guide.

- Configuring Dual-Stream Protocol
- Configuring Mix-Sending
- Configure Content Sharing

Configuring Dual-Stream Protocol

The dual-stream protocol allows the video and PC content to be transmitted to the far site simultaneously, thus meeting the requirements of different conference scenarios, such as training or medical consultation. Based on this protocol, the participants can share contents while having a video call.

The Yealink video conferencing system supports the standard H.239 protocol and BFCP (Binary Floor Control Protocol). The Yealink Cloud account and YMS account support dual-stream protocol by default. If you want to share contents during the call using the SIP protocol and H.323 protocol, you need to enable the H.239 protocol and BFCP in advance.

- Configuring the H.239 Protocol
- Configuring BFCP (Binary Floor Control dual Protocol)

Configuring the H.239 Protocol

H.239 protocol is used when sharing content with the far site in H.323 calls. You can configure the H.239 protocol for the H.323 account.

Procedure

1. On your web user interface, go to **Account** > **H.323**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
H.239	Enable or disable the H.239 protocol. **Default**: On.	Web user interface

Configuring BFCP (Binary Floor Control dual Protocol)

BFCP is used when sharing content with the remote in SIP calls. You can configure the BFCP protocol for Zoom, Pexip, BlueJeans, or a custom third-party platform, SIP account, and SIP IP call.

Procedure

1. On your web user interface, go to **Account** > **VC Platform** > **Platform Type** > **Zoom/Pexip/ BlueJeans /Videxio/Custom** or go to **Account** > **SIP Account/SIP IP Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
BFCP	Enable or disable the BFCP. **Default**: On. This feature is not applicable to Yealink StarLeaf Cloud platform.	Web user interface

Related tasks

Configuring Mix-Sending

Configuring Mix-Sending

During a call, the remote party may not support dual-stream protocol or fail to negotiate with the dual-stream protocol. Therefore, you need enable this feature, so that multiple video streams (the local video + the local content) can be synthesized to one video stream and sent to the remote.

Procedure

1. On your web user interface, go to **Setting** > **Video** > **Content Video**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **Presentation**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Mix	Enable or disable the mix-sending feature on the system. **Note**: the default value is On.	Web user interface

Note: If the call parties enable the dual-stream protocol, the dual-stream protocol will be used to send multiple video streams.

Configure Content Sharing

You can configure whether to enable PC presentation on the system when the content is sharing. You can also specify the mode, the maximum frame and the resolution for the shared content. Make sure that the definition of the presentation is good. You can not configure the content sharing mode for VP59, but you can configure frame and resolution for VP59.

Procedure

1. On your web user interface, go to **Setting** > **Video** > **Content Video**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **Content Sharing**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enable 4K (it is only applicable to MeetingEye 600/MeetingEye 400)	Enable or disable 4K for content sharing. **Default**: Disabled.	Web user interface
Enable 60fps (it is only applicable to MeetingEye 600/MeetingEye 400)	Enable or disable 60fps for content sharing. **Default**: Disabled.	Web user interface
Content Sharing Mode (it is not applicable to VP59)	Configure the content sharing mode. • **Sharing Document**- select this value to save bandwidth when you are sharing a document. By default, the maximum frame rate is 15fps and the maximum resolution is 1080P. • **Sharing Video**: select this value to play video fluently when you are sharing a video. By default, the maximum frame rate is 30fps and the maximum resolution is 720P. **Default**: sharing document.	Web user interface
Frame	Configure the maximum frame rate when the content is sharing. • 5 frame rate • 15 frame rate • 30 frame rate • 60fps—this option appears only when you enable **Enable 60fps**. It is only applicable to MeetingEye 600/MeetingEye 400. **Default**: 15 fps.	Web user interface

Parameter	Description	Configuration Method
Resolution	Configure the maximum resolution when the content is sharing. • 1080P • 720P • 4K—this option appears only when you enable **Enable 4K**. It is only applicable to MeetingEye 600/MeetingEye 400. **Default**: 1080P.	Web user interface
Automatic Content Sharing (it is not applicable to VP59)	Configure whether to enable PC presentation on the system when the content is sharing. **Default**: On.	Web user interface
Miracast PIN (it is only applicable to MeetingEye 600/MeetingEye 400)	Configure the PIN code for authentication when using Miracast presentation. **Note**: when using Miracast presentation, the PIN code will display in the top-right corner of the screen. It is enable by default.	Web user interface
Miracast PIN Validity(30-120s) (it is only applicable to MeetingEye 600/MeetingEye 400)	Configure the valid time for entering PIN code when using Miracast presentation. **Note**: its value is from 30 to 120s and it defaults to 60s. This parameter is only available when you enable **Miracast PIN**.	Web user interface

Configuring Camera Settings

You can configure the following settings on MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/PVT950.

- Selecting and Setting Cameras
- Viewing Camera Status
- Specifying the Camera Control Mode for MeetingEye 600/MeetingEye 400
- Enabling People Counting
- Controlling the Camera
- Adjusting the White Balance
- Adjusting the Exposure
- Displaying Camera Name When Multi-Camera Connected
- Adjusting the Display Image of the Camera

- Adjusting Hangup Mode and Camera Pan Direction
- Configuring Continuous Auto Focus
- Setting the Camera Presets
- Configuring Preset Synchronize With Active Camera
- Allowing the Remote System to Control Your Camera
- Configuring Multi-Camera Default Layout
- Resetting the Camera

Selecting and Setting Cameras

You can select a camera, enable or disable the selected camera, or customize the camera name. This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Setting** > **Camera**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Camera	Configure the desired camera.	Web user interface
Status	Enable or disable the selected camera. **Default**: On. It is not applicable to MeetingEye 600/ MeetingEye 400/VC200/VC500/PVT950.	Web user interface
Camera Name	Customize a name for the camera.	Web user interface

Viewing Camera Status

About this task

This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Camera Info**.
   - On your VCS, go to **More** > **Settings** > **System Status** > **Camera**.
   - On your CTP20, tap > **Settings** > **System Status** > **Camera**.
2. You can view the following camera status:

Parameter	Description	Configuration Method
Camera Name	Customize a name for the camera.	Web user interface
Model	The VCS codec model.	Endpoint

Parameter	Description	Configuration Method
IP	The IP address of the selected camera.	Web user interface
Firmware Version	The firmware version of the selected camera.	Web user interface
Hardware Version	The hardware version of the selected camera.	Web user interface
SPEC	The specification of the selected camera.	Web user interface Endpoint CTP20
MAC	The MAC address of the selected camera.	Web user interface
Camera Hardware	The hardware version of the camera lens.	Web user interface Endpoint CTP20

Specifying the Camera Control Mode for MeetingEye 600/MeetingEye 400

You can specify the camera control mode of MeetingEye 600/MeetingEye 400 as manual control, auto framing, or speaker tracking mode. When you set it as manual control mode, you can manually adjust the angle and the focal length of your camera. With the real-time face detection, the auto framing feature can automatically adjust the camera according to the number and the position of the participants, covering every participant in the conference. Moreover, the speaker tracking feature, based on the auto framing feature, can automatically detect the speaking participant and zoom in his video image, providing an optimal closeup of the speaker.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Camera Mode**.
   - On your MeetingEye 600/MeetingEye 400, go to **More** > **Camera Control**.

     Press the scroll key to display more menu items.
   - On your CTP20, tap .

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Intelligent Tracking/Tracking Mode	Specify the camera control mode. • **Manual Control** • **Auto Framing**: if you enable this mode, the camera will be adjusted automatically and you cannot control the camera. • **Speaker Tracking**(only applicable to MeetingEye 600/MeetingEye 400): if you enable this mode, the camera will be adjusted automatically and you cannot control the camera. **Default**: Manual Control	Web user interface Endpoint CTP20

Enabling People Counting

Through face detection, MeetingEye 600/MeetingEye 400 can count up to 30 participants. When the conference ends, you can view the maximum number of participants, the conference type, the conference start and end time on the web user interface. You can export the conference record to your PC.

Procedure

1. On your web user interface, go to **Setting** > **Advanced Features** > **People Counting**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enable People Counting	Enable or disable the people counting feature. • On • Off **Default**: Disabled.	Web user interface

Parameter	Description	Configuration Method
Save Quantity(strip)	Configure the number of conference records displayed on the web user interface. When you reach the limit you set, the newly added conference record will cover the oldest record. • 50 • 100 • 200 • 500 • 1000 **Note**: this configuration appears only when you enable People Counting. The default value is 50.	Web user interface

Tip: When the call ends, click Data Output in the **Conference Record** field to export the conference record to your PC.

Controlling the Camera

You can pan, tilt and zoom your own camera. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Home** > **Yourself** > .
   - On your VCS, go to **More** > **Camera Control**.
   - On your CP960 conference phone, tap **Camera**.
   - On your CTP20, tap .
2. Use the navigation keys to adjust the camera angle.
3. Click ( ) or ( ) to adjust the focal length.
   If you use VCR20 Remote Control, scroll up or down to adjust the focal length.

Adjusting the White Balance

To display high-quality video image, you can adjust camera white balance. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **White Balance**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera** > **White Balance**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **White Balance**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
White Balance Mode	Configure the white balance mode of the camera. • **Auto**—Yealink recommends that you use this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room. • **InDoor** • **OutDoor** • **OnePush** • **ATW**—automatically adjust the white balance according to the picture took by the camera. • **Manually/ Manual**—manually adjust the color temperature. **Default**: ATW.	Web user interface Endpoint CTP20
Color Temperature	Configure the value of the color temperature. **Note**: the value is from 2800K to 6800K. The default value is the color temperature tested in the your current environment. You can set this parameter only when the white balance mode is configured to Manual.	Web user interface Endpoint

Adjusting the Exposure

To display the high-quality video image, you can adjust the camera Exposure. This feature is not applicable to VP59.

- Configuring Auto Exposure Mode
- Configuring Manual Exposure Mode
- Configuring the Mode of Shutter Priority
- Configuring Aperture Priority
- Configuring the Mode of Brightness Priority
- Configuring the Mode of WDR-Auto
- Configuring WDR-Manual

Configuring Auto Exposure Mode

The auto-exposure feature can achieve the desired brightness level (or so-called target brightness level) in different lighting conditions and scenes, so that the videos or images captured are neither too dark nor too bright.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera** > **Exposure**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Exposure**.
2. Select **Auto/Auto Exposure** from the **Exposure/Exposure mode** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Exposure Compensation	Configure the value of exposure compensation. The exposure compensation is used to compensate the camera effectively when the camera is shooting in a backlit environment. If the environment light is dark, you can increase the compensation value. **Note**: the valid value is -6 to 6. The default value is 0.	Web user interface Endpoint CTP20
Flicker	Configure the value of camera flicker frequency. The supported types are as follows: • 50 Hz • 60 Hz • Off The indoor lights powered by a 50Hz or 60Hz power source may produce a flicker. You can adjust the camera flicker frequency according to the power source that the light is powered by. **Default**: 50 Hz.	Web user interface Endpoint CTP20
Gain Limit	Specify the value. **Note**: the valid value is 1 to 15. For VC880/VC800/VC500/ VC200/PVT980/PVT950, the default value is 4; for MeetingEye 600/ MeetingEye 400, the default value is 15.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Wide Dynamic Range	Off or Specify the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Note**: For MeetingEye 600/ VC880/VC800/VC500/VC200/ PVT980/PVT950, the default value is 2; for MeetingEye 400, the default value is off.	Web user interface Endpoint CTP20
Photometry	Configure the value of metering. • Average • Central • Bottom • Top **Default**: Average.	Web user interface Endpoint CTP20

Configuring Manual Exposure Mode

Manual exposure mode allows you to achieve a combined exposure of the camera aperture size and the shutter speed.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera** > **Exposure**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Exposure**.
2. Select **Manual/Manual Exposure** from the **Exposure** mode drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Aperture (it is not applicable to MeetingEye 400/ VC200)	Configure the value of aperture. • Off • F1.6, F2.0, F2.4, F2.8, F3.4, F4, F4.8, F5.6, F6.8, F8, F9.6, F11, F14 **Note**: For VC880/VC800/VC500/PVT980/ PVT950, the default value is F3.4; for MeetingEye 600, the default value is F1.6.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Shutter	Configure the value of the shutter. **Value**: 1/60, 1/90, 1/100, 1/125, 1/180, 1/250, 1/350, 1/500, 1/725 1/1000, 1/1500, 1/2000, 1/3000, 1/4000, 1/6000, 1/10000 **Default**: 1/100.	Web user interface Endpoint CTP20
Gain/Gain Limit	Specify the value. **Note**: the valid value is 1 to 15. For MeetingEye 400/VC880/VC800/VC500/ VC200/PVT980/PVT950, the default value is 2; for MeetingEye 600, the default value is 6.	Web user interface Endpoint CTP20
Wide Dynamic Range	Off or Specify the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Note**: For MeetingEye 600/VC880/VC800/ VC500/VC200/PVT980/PVT950, the default value is 2; for MeetingEye 400, the default value is off.	Web user interface Endpoint CTP20

Configuring the Mode of Shutter Priority

Shutter priority allows you to choose a specific shutter speed while the camera adjusts the aperture to ensure adequate exposure.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera** > **Exposure**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Exposure**.
2. Select **Shutter Priority** from the **Exposure Mode** drop-down menu.

3. Configure and save the following settings:

Parameter	Description	Configuration Method
Shutter	Configure the value of the shutter. **Valid Value**: 1/60, 1/90, 1/100, 1/125, 1/180, 1/250, 1/350, 1/500, 1/725, 1/1000, 1/1500, 1/2000, 1/3000, 1/4000, 1/6000, 1/10000 **Default**: 1/100.	Web user interface Endpoint CTP20
Exposure Compensation	Configure the value of exposure compensation. The exposure compensation is used to compensate the camera effectively when the camera is shooting in a backlit environment. If the environment light is dark, you can increase the compensation value. **Note**: the valid value is -6 to 6. The default value is 0.	Web user interface Endpoint CTP20
Gain Limit	Specify the value. **Note**: the valid value is 1 to 15. For VC880/VC800/VC500/VC200/PVT980/PVT950, the default value is 4; for MeetingEye 600/MeetingEye 400, the default value is 15.	Web user interface Endpoint CTP20
Wide Dynamic Range	Off or Specify the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Note**: For MeetingEye 600/VC880/VC800/VC500/VC200/PVT980/PVT950, the default value is 2; for MeetingEye 400, the default value is off.	Web user interface Endpoint CTP20
Photometry	Configure the value of metering. • Average • Central • Bottom • Top **Default**: Average.	Web user interface Endpoint CTP20

Configuring Aperture Priority

Aperture priority allows you to set a specific aperture value, and then the camera can automatically select a appropriate shutter speed to match the aperture value via the exposure value measured by the camera metering system.

About this task

This feature is not applicable to MeetingEye 400/VC200.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera** > **Exposure**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Exposure**.
2. Select **Aperture Priority** from the **Exposure Mode** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Aperture	Disable aperture or set the desired value. **Value**: F1.6, F2.0, F2.4, F2.8, F3.4, F4.0, F4.8, F5.6, F6.8, F8, F9.6, F11, F14 and off For VC880/VC800/VC500/PVT980/PVT950, the default value is F3.4; for MeetingEye 600, the default value is F1.6.	Web user interface Endpoint CTP20
Exposure Compensation	Configure the value of exposure compensation. The exposure compensation is used to compensate the camera effectively when the camera is shooting in a backlit environment. If the environment light is dark, you can increase the compensation value. **Note**: the valid value is -6 to 6. The default value is 0.	Web user interface Endpoint CTP20
Flicker	Configure the value of camera flicker frequency. **Frequency**: • 50 Hz • 60 Hz The indoor lights powered by a 50Hz or 60Hz power source may produce a flicker. You can adjust the camera flicker frequency according to the power source that the light is powered by. **Default**: 50 Hz.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Gain/Gain Limit	Specify the value. **Note**: the valid value is 1 to 15. For MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/PVT950, the default value is 6; for MeetingEye 600, the default value is 6.	Web user interface Endpoint CTP20
Wide Dynamic Range	Off or Specify the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Default**: 2.	Web user interface Endpoint CTP20
Photometry	Configure the value of metering. • Average • Central • Bottom • Top **Default**: Average.	Web user interface Endpoint CTP20

Configuring the Mode of Brightness Priority

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera** > **Exposure**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Exposure**.
2. Select **Brightness Priority** from the **Exposure** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Brightness	Configure the value of brightness. **Note**: the value is from 0 to 14. For MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/PVT950, the default value is 6; for MeetingEye 600, the default value is 9.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Flicker	Configure the value of camera flicker frequency. The supported types are as follows: • 50 Hz • 60 Hz The indoor lights powered by a 50Hz or 60Hz power source may produce a flicker. You can adjust the camera flicker frequency according to the power source that the light is powered by. **Default**: 50 Hz.	Web user interface Endpoint CTP20
Wide Dynamic Range	Off or Specify the WDR. The value represents the compression degree of the dynamic range Cameras with WDR technology can work perfectly both in the bright and the dark conditions and present clear images that balances different lighting, so that you can identify the details. • **Off**-do not use WDR. • 1~5 **Note**: For MeetingEye 600/VC880/VC800/ VC500/VC200/PVT980/PVT950, the default value is 2; for MeetingEye 400, the default value is off.	Web user interface Endpoint CTP20
Photometry	Configure the value of metering. • Average • Central • Bottom • Top **Default**: Average.	Web user interface Endpoint CTP20

Configuring the Mode of WDR-Auto

WDR-auto mode is not applicable to MeetingEye 600/MeetingEye 400/VC200.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - go to **More** > **Setting** > **Camera** > **Exposure**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Exposure**.
2. Select **WDR-Auto** from the **Exposure/Exposure mode** drop-down menu.

3. Configure and save the following settings:

Parameter	Description	Configuration Method
Exposure Compensation	Configure the value of exposure compensation. The exposure compensation is used to compensate the camera effectively when the camera is shooting in a backlit environment. If the environment light is dark, you can increase the compensation value. **Note**: the valid value is -6 to 6. The default value is 0.	Web user interface Endpoint CTP20

Configuring WDR-Manual

WDR-Manual mode is not applicable to MeetingEye 600/MeetingEye 400/VC200.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Exposure**.
   - go to **More** > **Setting** > **Camera** > **Exposure**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Exposure**.
2. Select **WDR-Manual** from the **Exposure/Exposure mode** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Exposure Compensation	Configure the value of exposure compensation. The exposure compensation is used to compensate the camera effectively when the camera is shooting in a backlit environment. If the environment light is dark, you can increase the compensation value. **Note**: the valid value is -6 to 6. The default value is 0.	Web user interface Endpoint CTP20
Exposure Ratio	Configure the value of exposure ratio. **Note**: the valid value is 1 to 16. The default value is 1. The exposure ratio represents the ratio of long exposure to short exposure. In a backlit environment, the bright part uses a short exposure and the dark part uses a long exposure.	Web user interface Endpoint CTP20

Displaying Camera Name When Multi-Camera Connected

If multiple cameras are connected to the VC880/VC800/PVT980, you can configure the device to display the camera names to distinguish the installation position or shooting position of each camera.

Before you begin

Customize the name of your cameras.

Procedure

1. On your web user interface, go to **Setting** > **Camera** > **Other Settings**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Display Camera Name When Multicamera	Enable or disable to display the camera names of the multiple cameras. **Default**: Disabled.	Web user interface

Related tasks

Selecting and Setting Cameras

Adjusting the Display Image of the Camera

To display high-quality video image, you can adjust display mode of the camera or customize the image display. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Graphics**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera** > **Graphics**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Graphics**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Display Mode	Configure the display mode of the camera. • High Definition • Standard • Mild • Custom **Default**: Standard.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Saturation	Configure the saturation of the camera's image. The saturation means the maximum intensity of color in the image. **Note**: the value is from 0 to 100. The default value is 50.	Web user interface Endpoint CTP20
Sharpness	Configure the sharpness of the camera's image. The sharpness is an indicator that reflects the definition of the image plane and the sharpness of image edge. Increasing the sharpness will improve the definition of the image. However, if the sharpness is set too high, the image will look distorted and glaring. **Note**: the value is from 0 to 100. The default value is 15.	Web user interface Endpoint CTP20
Brightness	Configure the brightness of the camera's image. **Note**: the value is from 0 to 100. The default value is 50.	Web user interface Endpoint CTP20
Contrast	Configure the contrast of the camera's image. **Note**: the value is from 0 to 100. For VC880/VC800/VC500/ VC200/PVT980/PVT950, the default value is 49; for MeetingEye 600/ MeetingEye 400, the default value is 50.	Web user interface Endpoint CTP20
Noise Reduction (2D)	Specify the noise reduction (2D) mode. The available modes are described as below: • Off • Low • Middle • High **Default**: Middle.	Web user interface Endpoint CTP20

Parameter	Description	Configuration Method
Noise Reduction (3D)	Specify the noise reduction (3D) mode. It indicates the coefficient of the reduced noise in the image. The higher the coefficient is, the smaller the noise is. **Valid value**: 0 - 22. The default value is 3.	Web user interface Endpoint CTP20

Adjusting Hangup Mode and Camera Pan Direction

To display high-quality video image, you can adjust camera settings as required, such as white balance, exposure and sharpness. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Other Settings**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera** > **Other**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Other**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Hangup Mode	Enable or disable the camera to flip the image view when camera is handed at up-side-down position. If this mode is enabled, the picture took by the camera is upside down. This mode is applicable to install the camera on the meeting room ceiling. **Default**: Disabled.	Web user interface Endpoint CTP20
Camera Pan Direction	Configure the pan direction of the camera. • Normal • Reversed If you set the **Camera Pan Direction** as reversed, the camera pan direction 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. **Default**: Normal.	Web user interface Endpoint CTP20

Configuring Continuous Auto Focus

If you want to make the camera focus on the moving object automatically, you can enable this feature. If you want a fixed focal length for presentation, for example, the class, you can disable this feature. It is not available to MeetingEye 400/VC200/VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Focus**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera**.
2. Configure and save the following settings:

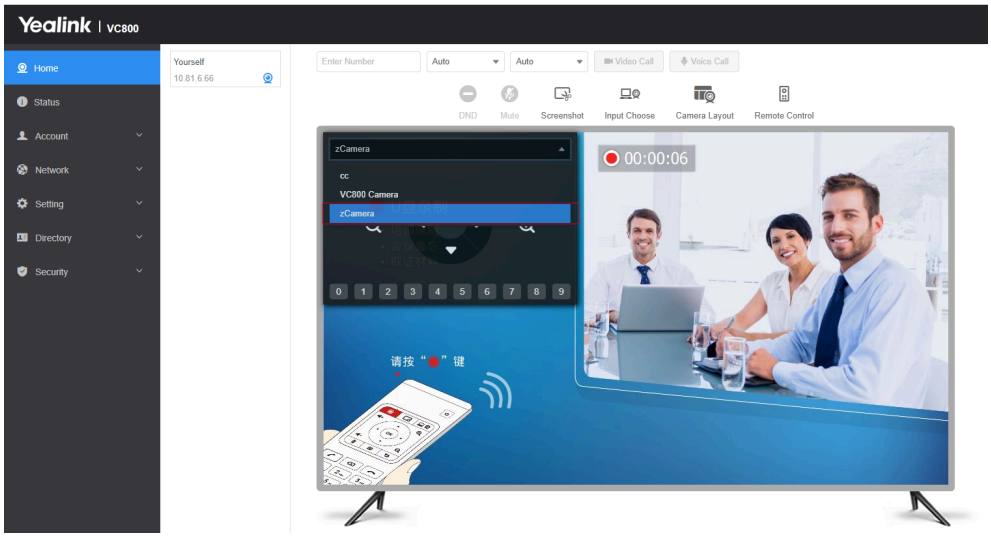
Parameter	Description	Configuration Method
Continuous Auto Focus	Enable or disable this feature. **Default**: On.	Web user interface Endpoint CTP20

Setting the Camera Presets

Presets are the pre-saved settings of both the angle and the focal length for the camera. The camera presets can help you quickly point a camera at pre-defined locations. The camera presets can remain in effect until you change them.

Procedure

1. On your web user interface, go to **Home** > **Yourself** > .
2. If there are multiple cameras connected, click the camera name area in the top-left corner and select the desired camera from the drop-down menu.



3. Click any number to configure the camera presets.
   You can add, modify, and delete the preset.

   Note: For more information about configuring presets via CP960 conference phone or CTP20, refer to the Yealink Full HD Video Conferencing System User Guide.

Configuring Preset Synchronize With Active Camera

The preset synchronize with active camera feature is applicable to VC880/VC800/PVT980 connected to the multi-camera VCC22 Be default, if multiple camera presets are set for the endpoint, after selecting the preset, the corresponding camera adjusts to the preset position and is selected as the currently active camera. If preset synchronize with active camera feature is disabled, after switching the preset, the corresponding camera is adjusted to this preset position, but the current active camera is not switched, and the active camera is still the camera selected by the current endpoint.

Procedure

1. On your web user interface, go to **Setting** > **Camera** > **Other Settings**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Preset Synchronize With Active Camera	Enable or disable the **Preset Synchronize With Active Camera**. **Default**: On.	Web user interface

Related tasks

Setting the Camera Presets

Allowing the Remote System to Control Your Camera

You can allow the far-end to control your camera, so that the far-end can meet their watching need.

To allow the far-end system to control your camera, meet the following conditions:

- Enable the protocol of camera control.
- Enable the feature of far control near camera (it is not applicable to VP59).

Note: Note that during a call, you can use your VP59 to control the far-end camera, but the far-end cannot control the camera of your VP59.

- Camera Control Protocol
- Configuring the Far Site to Control the Near Camera

Camera Control Protocol

If far site wants to control your camera, both the far site and you should enable the camera control protocol simultaneously. Your system supports FECC (Far End Camera Control) protocol. You can enable the FECC(H.323) protocol for the H.323 call and enable FECC(SIP) protocol for the SIP call.

- Configuring FECC (H.323) Protocol
- Configuring FECC (SIP) Protocol

Configuring FECC (H.323) Protocol

When logging in to the StarLeaf platform or using an H.323 account, you can enable the FECC (H.323) protocol for H.323 calls. To control the far-site camera, the call parties should enable this protocol simultaneously.

Procedure

1. On your web user interface, go to **Account** > **H.323**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
FECC (H.323)	Enable or disable FECC(H.323). If you enable FECC (H.323) protocol, the remote can control the near camera. **Default**: On.	Web user interface

Configuring FECC (SIP) Protocol

When using SIP account, SIP IP call, or logging in to Zoom, Pexip, BlueJeans, Videxio, or a custom third-party platform, you can enable FECC (SIP) control for SIP calls. To control the far-site camera, the call parties should enable this protocol simultaneously.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **Video Conference Platform** > **Platform Type** > **Zoom/Pexip/BlueJeans/Videxio/Custom**.
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
FECC (SIP)	Enable or disable the FECC (SIP) protocol for the far site to control the near camera. **Note:** For Zoom/Pexip/BlueJeans/ EasyMeet/Videxio/Custom and SIP IP call, BFCP is enabled by default. For SIP account, BFCP is disabled by default.	Web user interface

Configuring the Far Site to Control the Near Camera

You can enable this feature to allow the remote to control your local camera, so that the image captured by the local camera can be displayed properly on the remote monitor. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Call Features** > **In-Call Settings**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **Far Control Near Camera**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Camera**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Far Control Near Camera	Enable or disable the far site to control the near-site camera. **Default**: On.	Web user interface Endpoint CTP20

Configuring Multi-Camera Default Layout

During a call, if you connect VCC22, all the local video streams are synthesized to one video stream, and sent to the far site. You can configure the default layout when you connect multiple cameras.

Procedure

1. On your web user interface, go to **Setting** > **Camera** > **Camera**.
2. Select the desired camera.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Multi-camera Default Layout	Configure the camera layout during a video call. • **1+N**: the video image of the selected camera is displayed in large window, and the video images of other cameras are displayed in thumbnails. • **Selected Speaker**: the video image of the selected camera is in full-screen. • **Equal N×N**: the video images of all cameras have equal size. **Default**: 1+N.	Web user interface

Resetting the Camera

You can reset the camera to factory defaults. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Camera** > **Other Settings**.
   - On your VCS: go to **More** > **Settings** > **Basic** > **Camera** > **Other**.
   - On your CTP20, tap > **Settings** > **Basic** > **Camera** > **Other**.
2. Select **Reset Camera.**
   The page prompts whether or not you are sure to reset.
3. Confirm the action.

Configuring Virtual Meeting Room

Yealink video conferencing system can act as a virtual meeting room, so that other devices can dial the system to join a meeting. Your system supports the following two conference types: regular mode conference room and virtual meeting room. You can configure the conference type and set the meeting password for the conference. This feature is not applicable to VP59.

The differences between regular mode meeting room and virtual meeting room are as below:

Meeting Room Type	Supported Model	Difference	Multipoint Allocation
Regular Mode	MeetingEye 600/MeetingEye 400/ VC880/VC800/VC500/C200/PVT980/ PVT950	Virtual meeting room 1: when participants call the virtual meeting room 1, the moderator also joins the meeting.	Up to 1 video call and 5 voice calls.
VMR Mode	VC800/VC880/PVT980 with a multipoint license	Virtual meeting room 1: when participants call the virtual meeting room 1, the moderator also joins the meeting.	The total MCU ways of the two virtual meeting rooms are depended on the multipoint license you imported. You can allocate the MCU ways between two virtual meeting rooms respectively.
		Virtual meeting room 2: when participants call the virtual meeting room 2, only participants join the meeting, the moderator does not join the meeting.	

You can also configure the third-party virtual meeting room to make multi-party video calls.

Note:

If you log into the Yealink VC Cloud Management Service, the conference may be managed via the Yealink VC Cloud Management Service only, you cannot configure it on your system.

- Setting the Endpoint as a Regular Mode Conference Room
- Setting the Endpoint as VMR Mode Conference Rooms
- Joining the VMR
- Configuring the Third-party Virtual Meeting Room

Related concepts

Multipoint Licenses

Setting the Endpoint as a Regular Mode Conference Room

For regular mode conference, virtual meeting room 1 is available. You can configure the password for virtual meeting room 1 to prevent unauthorized participants from joining the virtual conference room.

Procedure

1. On your web user interface, go to **Setting** > **Built-in MCU Setting** > **Conference Setting**.
2. Select **Regular Mode** from the **Conference Type** drop-down menu.
3. If you need to configure a conference room password for virtual conference room 1, configure and save the following settings:

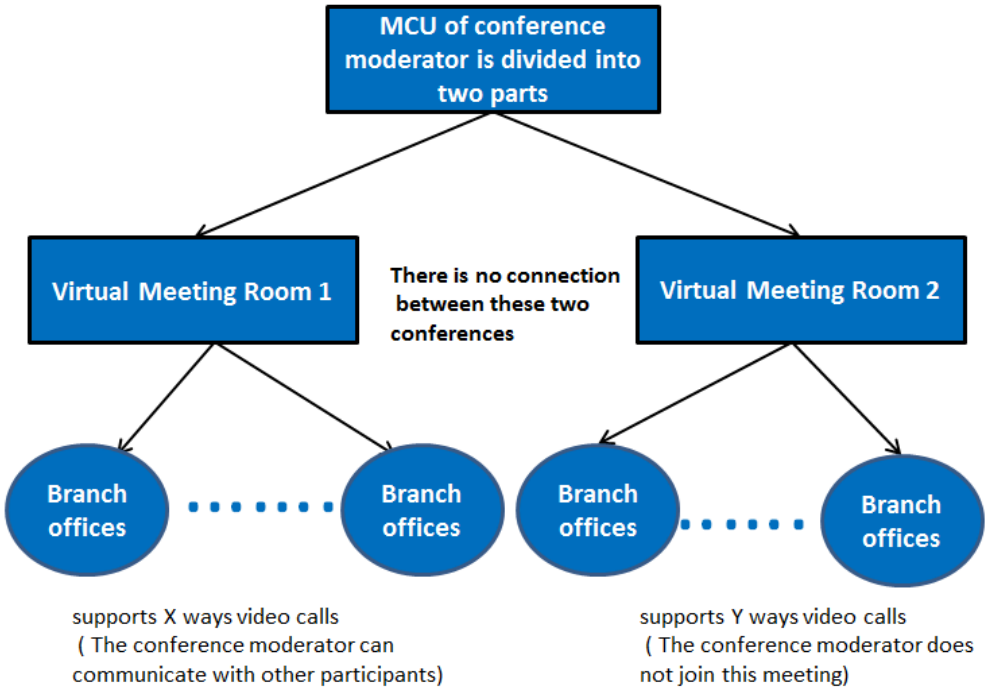
Parameter	Description	Configuration Method
Virtual Meeting Room 1 > **Meeting Password**	Enable or disable the system to configure a password for virtual meeting room1. **Default**: Disabled.	Web user interface
Virtual Meeting Room 1 > **Password**	Configure the password for virtual meeting room 1. **Valid Value**: 1 to 10, default value: 6.	Web user interface

Setting the Endpoint as VMR Mode Conference Rooms

In VMR mode conference, MCU can be used to host two independent conferences, corresponding to virtual meeting room 1 and virtual meeting room 2. You can configure the password for virtual meeting room 1 and virtual meeting room 2 to prevent unauthorized participants from joining the virtual conference room, and allocate the total MCU ways between two virtual meeting rooms at random.

About this task

This feature is only applicable to VC800/VC880/PVT980. For VC880 / PVT980, VMR mode conferences are not supported when two or more cameras are connected.



- If you import an 8 ways multipoint license to the VC800/VC880/PVT980, X+Y<=8. Virtual meeting room 1 and virtual meeting room 2 support up to 8 ways video calls.
- If you import an 16 ways multipoint license to the VC800/VC880/PVT980, X+Y<=16. Virtual meeting room 1 and virtual meeting room 2 support up to 16 ways video calls.
- If you import an 24 ways multipoint license to the VC800/VC880/PVT980, X+Y<=24. Virtual meeting room 1 and virtual meeting room 2 support up to 24 ways video calls.

Note: When you import an 8 or 16-way multipoint license to the VC800/VC880/PVT980, virtual meeting room 1 provides additional 5 voice calls.

Procedure

1. On your web user interface, go to **Setting** > **Built-in MCU Setting** > **Conference Setting**.
2. Select **VMR Mode** from the **Conference Type** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Multipoint Allocation > **Virtual Meeting Room 1**	Allocates the maximum ways of video calls for virtual meeting room 1.	Web user interface
Multipoint AllocationVirtual Meeting Room 2	Allocates the maximum ways of video calls for virtual meeting room 2.	Web user interface
Virtual Meeting Room 1 > **Meeting Password**	Enable or disable the system to configure a password for virtual meeting room1. **Default**: Disabled.	Web user interface

Parameter	Description	Configuration Method
Virtual Meeting Room 1 > **Password**	Configure the password for virtual meeting room 1. **Valid Value**: 1 to 10, default value: 6.	Web user interface
Virtual Meeting Room 2 > **Meeting Password**	Enable or disable the system to configure a password for virtual meeting room 2. **Note**: the default value is Off. Only when the meeting room type is VMR mode can this parameter be configured.	Web user interface
Virtual Meeting Room 2Password	Configure the password for virtual meeting room 2. **Valid Value**: 1 to 10, default value: blank. Only when the meeting room type is VMR mode can this parameter be configured.	Web user interface

Note: If you set a password for the virtual conference room, the remote party can not call in when using other account.

Joining the VMR

If the virtual meeting room requires no password, dial IP address or account to enter the VMR.

If the virtual meeting room requires a password, only dial **IP##meeting password** or **meeting password@IP** to enter the VMR.

Example:

- The IP address of the moderator is 10.3.6.201.
- The meeting password for virtual meeting room 1 is 123.
- The meeting password for virtual meeting room 2 is 456.

Participants can dial 10.3.6.201##123 or 123@10.3.6.201 to enter the virtual meeting room 1.

Participants can dial 10.3.6.201##456 or 456@10.3.6.201 to enter the virtual meeting room 2.

Without a meeting password or with a wrong meeting password, the call will fail.

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.

About this task

If you do not register a Cloud account, or you only register a Yealink Cloud account or YMS account, you can configure a third-party VMR (Zoom/BlueJeans/Pexip/Videxio Platform) 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.

Procedure

1. On your web user interface, go to **Setting** > **3rd Party VMR**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
VMR Name 1 to 5	Specify the name of the virtual meeting room . **Note**: • The VMR name 1 is Zoom by default. • The VMR name 1 is BlueJeans by default. • The VMR name 3 to 5 is empty by default. 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 1 to 5	The IP address or the domain name of the VMR server. **Note**: • The VMR server 1 is zoomcrc.com by default. • The VMR server 2 is bjn.vc by default. • The VMR server 3 to 5 is empty by default. 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

You can see the configured third-party VMR from the drop-down menu of **Call type** on the Home page of the web user interface or the **Dial** screen on the monitor. You can select the desired VMR from the pull-down menu, and then enter the conference ID to call the corresponding VMR.

Configuring Call Settings

- Selecting a Call Protocol
- Specifying the Video Call Rate
- Configuring Call Rate Adaptation
- Account Polling
- Selecting the CTP20 Conference Call Preferences
- Setting the CTP20 Contact Display Label
- Configuring Additional Audio Call
- Selecting the Multi-Party Resources
- Configuring Call Match
- Dial Plan
- Search Source List in Dialing
- Configuring SIP IP Call by Proxy
- Configuring Ringback Timeout
- Configuring the Auto Refuse Timeout
- Auto Answer
- Muting Auto-Answered Calls
- Muting Auto-Dialed Calls
- DND (Do Not Disturb)
- Enabling Fast Audio Call for CP960

Selecting a Call Protocol

The system supports SIP and H.323 protocols for the incoming and the outgoing calls.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Call Features**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Call Features**.

     For VP59, tap > **Settings** > **Basic** > **Call Features**.

     On your CTP20, tap > **Settings** > **Basic** > **Cal Features**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Call Protocol/Call Type	Specify the desired call protocol for placing calls. The supported types are as follows: • **Auto**—the system automatically uses the available call protocol. The system preferentially uses the H.323 protocol to place calls. • **SIP**—the system only uses the SIP protocol for placing calls. • **H.323**—the system only uses H.323 protocol for placing calls. **Default**: Auto.	Web user interface Endpoint CTP20

Specifying the Video Call Rate

You can specify the maximum video call rate. The configurable video call rates on the system are: 64kb/s, 128kb/s, 256kb/s, 384kb/s, 512kb/s, 768kb/s, 1024kb/s, 1280kb/s, 1500kb/s, 2000kb/s, 3000kb/s, 4000kb/s, 5000kb/s, 6000kb/s.

About this task

Note: The call rate of audio and PC content are also affected by this configuration.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Call Features**.

     For VP59, tap > **Settings** > **Basic** > **Call Features**.

     On your CTP20, tap > **Settings** > **Basic** > **Cal Features**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Video Call Rate	Configure the maximum video call rate. **Note**: for VC880/VC800/VC500/VC200/PVT980/PVT950, the default value is 2000kb/s; for MeetingEye 600/MeetingEye 400, the default value is 4000kb/s.	Web user interface Endpoint CTP20

Configuring Call Rate Adaptation

The call rate adaptation feature is enabled by default. When the network bandwidth is less than the specified call rate, the endpoint will adaptively modify the sending resolution and frame rate to lower the sending rate during a call. In some network environments, if the sending rate is lowered, the sending resolution and frame rate cannot be restored due to call rate adaptation. You need to disable the call rate adaptation feature to place calls at a specified rate. Disabling the call rate adaptation feature can avoid the situation that the bandwidth cannot be recovered after packet loss.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Call Rate Adaptive	Enable or disable the call rate feature. **Default**: On.	Web user interface

Account Polling

Account polling feature allows the system to use different call types (Cloud platform/H.323 account/SIP account/PSTN account/H.323 IP Call/SIP IP Call) to dial a number when more than one account is registered. If account polling is disabled, the system can only dials a number by using the call type with the highest priority. That is, once the dialed number differs from the call type with the highest priority you are using, you cannot place a call.

Example

1. System A is registered with a Yealink Cloud account and a SIP account.
2. Select the call type automatically. Dial the number.
   - 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 (the second highest priority) to call system B.
   - If account polling is disabled, system A can only use its Cloud account (highest priority) to call system B. SIP account can not be used to call out.

- Priority of Call Types

- Configuring the Account Polling

Priority of Call Types

In the dialing screen, if you select the call type automatically, the system will select a call type according to the following priority:

- If you dial an account, the priority is: **Cloud platform**>**H.323 account**>**SIP account**>**PSTN account**.
- If you dial an IP address, the priority is: **H.323 IP Call**>**SIP IP Call**.

Configuring the Account Polling

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Account Polling	Enable or disable the account polling on the system. • **Off**—the system dials a number by using the call type with the highest priority. If you disable this feature, once the dialed number differs from the call type you are using, you cannot place the call. • **On**—the system tries each call type in order to dial a number. **Default**: On.	Web user interface

Related tasks

Placing a Call by Entering a Number

Selecting the CTP20 Conference Call Preferences

The CTP20 conference call options include **Start Conference**, **Dial, Directory**, and **History**, and you can initiate a conference from any call option. The meeting call preferences determines the call interface that is first entered when the meeting is initiated.

Procedure

1. On your web user interface, go to **Setting** > **Touch Panel** > **First Conference Call**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features** > **First Conference Call**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
First Conference Call	Configure the conference call preferences. • Auto • Dial • Directory • History • Start Conference **Default**: Auto. If you have logged in to a YMS or a Yealink cloud account, the default value is **Start Conference**. Otherwise, the default value is **Dial**.	Web user interface

Setting the CTP20 Contact Display Label

The contact interface displays all contact groups by default, including all Cloud contacts/YMS contacts (if you log in to a YMS or Yealink Cloud accounts), local contacts, and LDAP contacts. If the contact is not commonly used, you can choose to hide the contact list. You can also set the default contact tab based on frequently used contacts so that when you select a contact, you can locate the corresponding contact list to find the desired contact quickly.

Procedure

1. On your web user interface, go to **Setting** > **Touch Panel** > **Directory**.
   For MeetingEye 600/MeetingEye 400, go to **Directory** > **Setting** > **Directory**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enterprise	Enable or disable to display the list of Yealink Cloud /YMS contacts. **Note**: It is enabled by default. It can be configured only when logging in to a YMS or Yealink Cloud account.	Web user interface
Device	Enable or disable to display the devices account list. **Note**: It is enabled by default. It can be configured only when logging in to a YMS or Yealink Cloud account.	Web user interface
VMR	Enable or disable to display the VMR list. **Note**: It is enabled by default. It can be configured only when logging in to a YMS or Yealink Cloud account.	Web user interface

Parameter	Description	Configuration Method
External	Enable or disable to display the external contact list. **Note**: It is enabled by default. It can be configured only when logging in to a YMS or Yealink Cloud account.	Web user interface
Local directory	Enable or disable to display the local contact list. **Default**: On.	Web user interface
Conference Contacts	Enable or disable to display the conference contact list. **Default**: On.	Web user interface
LDAP	Enable or disable to display the LDAP list. **Note**: It is enabled by default.	Web user interface
Tab Default	Configure the list of contacts that is displayed by default when you enter the contact interface. **Note**: If you have logged in to a YMS or a Yealink Cloud account, the default value is **Enterprise**. Otherwise, the default value is **Local**.	Web user interface

Configuring Additional Audio Call

If you enable this feature, when the number of video calls reaches the limit (except for 24-way video calls) in the call, additional 5 users can still place audio calls to join the call. Otherwise, additional 5 users cannot place audio calls to join the call. This feature is disabled by default.

About this task

For example, for VC800 with 16-way license, if you disable additional audio call, when you create a call, only 16 participants can place video calls to join your call, the 17th participant cannot join the call.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **In-Call Settings**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Additional Audio Call	Enable or disable the additional audio call. **Default**: Disabled.	Web user interface

Selecting the Multi-Party Resources

If you are during a P2P call, you can invite a third party using its own capacity (built-in MCU) or the server VMR to initiate a conference. It is not applicable to MeetingEye 600/MeetingEye 400.

About this task

The systems can select multi-party resources by the following:

Prerequisites	Types of multiparty resources	Multiparty resources used when inviting the third party
VC500/VC200/ VP59 uses Cloud account or YMS account with priority to make a P2P call.	**Auto**	Upgrade to be a server VMR conference first, if so, use the Endpoint own capacity to initiate a conference call
VC880/VC800 system (without an imported multipoint license) uses Cloud account or YMS account to make a P2P call.		
VC880/VC800 system (with an imported multipoint license) uses any call type (Cloud/YMS/SIP/ H.323/IP) to make a P2P call.		Uses the capacity to initiate a conference call
PVT980/PVT950 system uses any call type (Cloud/YMS/SIP/ H.323/IP) to make a P2P call.		Uses the capacity to initiate a conference call
Any call type (Cloud/YMS/SIP/ H.323/IP) is used to make a P2P call	**Endpoint Built-in MCU**	Uses the capacity to initiate a conference call
Cloud account or YMS account is used to make a P2P call.	**Server VMR**	Uses server VMR to initiate a conference call

Note: The system uses its own capacity to initiate a conference call in following situations: one is dialing a group to initiate a conference call when the system is idle, the other one is receiving a call when the system is during a P2P call.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **In-Call Settings**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Multiparty Resources	Configure the multiparty resources that the system uses to initiate a conference call. • **Auto**—the available multi-party resources are used automatically. • **Endpoint Built-in MCU** • **Server VMR** **Default**: Auto.	Web user interface

Configuring Call Match

The call match feature allows the dialing screen to display the search result after you enter the search criteria.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
   - On your VCS endpoint, go to **More** > **Settings** > **Basic** > **Call Features**.

     For VP59, tap > **Settings** > **Basic** > **Call Features**.

     On your CTP20, tap > **Settings** > **Basic** > **Cal Features**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Call Match	Enable or disable the call match feature. **Default**: On.	Web user interface Endpoint CTP20

Dial Plan

Dial plan is a string of characters that governs the way how the endpoints process the inputs received from the keypads. You can use the regular expression to define the dial plan. Dial plan is only applicable to VP59.

The replace rule is an alternative string that replaces the numbers you entered. You need to know the following basic replace rule:

Regular expression	Description
.	It can be used as a placeholder or multiple placeholders for any string. Example: “12.” would match “123”, “1234”, “12345”, “12abc”, and so on.
x	It can be used as a placeholder for any character. Example: “12x” would match “121”, “122”, “123”, “12a”, and so on.
-	It can be used to match a range of characters within the brackets. Example: “[5-7]” would match the number “5”, ”6” or ”7”.
,	It can be used as a separator within the bracket. Example: “[2,5,8]” would match the number ”2”, “5” or “8”.
[]	The square bracket "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: "91[5-7]1234"would match “9151234”, “9161234”, “9171234”.
()	The parenthesis "( )" can be used to group together patterns, for instance, to logically combine two or more patterns. Example: "([1-9])([2-7])3" would match “923”, “153”, “673”, and so on.

Regular expression	Description
$	The “$ number” followed by the sequence number of a parenthesis means the characters placed in the parenthesis. The sequence number stands for the corresponding parenthesis. Example: A replace rule configuration, Prefix: "001(xxx)45(xx)", Replace: "9001$145$2". When you dial out "0012354599" on your phone, the phone will replace the number with "90012354599". “$1” matches 3 digits in the first parenthesis, that is, “235”. “$2” means 2 digits in the second parenthesis, that is, “99”.

- Adding a Dial Plan

Adding a Dial Plan

Procedure

1. On your web user interface, go to **Setting** > **Dial Plan**.
2. In the **Prefix** field, enter the the number you want to replace.
3. In the **Replace** field, enter the alternate string instead of what the user enters.
4. Click **Add**.

Note: For example: Prefix: (xxxx) , Replace: 9069$1.

When you dial out 1234, the phone will replace the number with 90691234.

Search Source List in Dialing

The search source list in dialing allows you to search entries from the source list when the system is in the dialing screen.

The source list includes History, Local Directory, Cloud Contacts, Enterprise Directory and LDAP. To make the system search a specific list, you need configure the list first.

Note:

Cloud Contacts and Enterprise Directory appear in the search source list only when you log into the corresponding platform.

If you want to match the LDAP list, make sure LDAP is already configured, refer to LDAP.

- Configuring Search Source List in Dialing

Related tasks

Configuring Call Match

Configuring Search Source List in Dialing

Procedure

1. On your web user interface, go to **Directory** > **Setting** > **Search Source List In Dialing**.
2. Select the desired list from the **Disabled** column and click .
3. The selected search source list appears in the Enabled column.
4. Repeat step 2 to add more search source lists to the Enabled column.
5. To remove a list from the Enabled column, select the desired list and then click .

6. To adjust the search priority of the enabled search source lists, select the desired list, and click or .
7. The list shown on the top has the highest priority.
   The system will search the list with higher priority preferentially.

Configuring SIP IP Call by Proxy

If the account of far site is an URI address (for example, 8000@XX.com), you can use SIP IP address or SIP account to call the far site. By default, the SIP IP call by proxy feature is disabled. When dialing the URI of the far site, the system uses the SIP IP address to establish a connection. If the SIP IP call by proxy feature is enabled, the system uses the SIP account to establish a connection when dialing the URI of the far site.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
SIP Call by Proxy	Enable or disable the SIP call by proxy. **Default**: Disabled.	Web user interface

Configuring Ringback Timeout

The ringback timeout defines that if the remote party does not answer your call within specific time, the call will be hung up automatically.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Ringback Timeout(30-240)	Configure the ringback time (seconds). **Note**: the valid value is from 30 to 240 and the default value is 180. If it is set to 180, the call will be hung up automatically if the remote party does not answer the call within 180s.	Web user interface

Configuring the Auto Refuse Timeout

The auto refuse timeout defines a specific period of time after which the system will stop ringing if the call is not answered.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Auto Refuse Timeout (30-240)	Configure the duration time (seconds) in the ringing state. **Note**: the value is from 30 to 240. The default value is 120. If it is set to 120, the system will stop ringing if the call is not answered within 120s.	Web user interface

Auto Answer

You can allow the system to answer incoming calls automatically in the idle mode or during the call.

- Answering a Call Automatically When not in a Call
- Answering Multiple Calls Automatically

Answering a Call Automatically When not in a Call

You can specify whether to answer a call automatically when the system is not in a call.

About this task

⚠ **Attention:** Auto answer feature may create security issues. For example, an unexpected caller can view your video conference room randomly.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Call Features** > **Call Features** > **Inbound Call Settings**.
   - On your VCS, go to **More**.

     For VP59, tap > **Settings** > **Basic** > **Call Features**.
   - On your CP960 conference phone, swipe down from the top of the screen to enter the control center.
   - On your CTP20, tap > **Settings** > **Basic** > **Cal Features**.
2. Enable or disable **Auto Answer**.
3. Save the change.

Related tasks

Muting Auto-Answered Calls

Answering Multiple Calls Automatically

You can specify whether to answer a call automatically when the system is already in a call.

Before you begin

Make sure the auto answer is enabled.

About this task

⚠ **Attention:** Auto answer feature may create security issues. For example, an unexpected caller can view your video conference room randomly.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Call Features** > **Call Features** > **Inbound Call Settings**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Call Features**.

     For VP59, tap > **Settings** > **Basic** > **Call Features**.
   - On your CP960 conference phone, swipe down from the top of the screen to enter the control center.
   - On your CTP20, tap > **Settings** > **Basic** > **Cal Features**.
2. Enable or disable **Auto Answer Multiway**.
3. Save the change.

Muting Auto-Answered Calls

The Auto Answer Mute feature avoids the caller hearing the local conversation freely when an incoming call is answered automatically. Enable the local microphone to be muted when an incoming call is answered automatically.

About this task

Only the Auto Answer Mute feature is enabled can this feature be available.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Call Features** > **Call Features** > **Inbound Call Settings**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Call Features**.

     For VP59, tap > **Settings** > **Basic** > **Call Features**.
   - On your CTP20, tap > **Settings** > **Basic** > **Cal Features**.
2. Enable or disable **Auto Answer Mute.**
3. Save the change.

Related information

Auto Answer

Muting Auto-Dialed Calls

The Auto Dialout Mute feature allows the endpoint to turn off the microphone after the other party answers your call. Therefore, other party cannot hear you.

About this task

Note: The system is still muted after you hang up.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
2. Enable or disable **Auto Dialout Mute**.
3. Save the change.

DND (Do Not Disturb)

You can enable do not disturb feature to reject incoming calls automatically. All the rejected calls will be recorded to the missed call list.

- Enabling DND When Not in a Call
- Enabling DND during an Active Call

Enabling DND When Not in a Call

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Call Features**.
   - On your VCS, go to **More**.

     For VP59, tap > **DND**.
   - On your CP960 conference phone, swipe down from the top of the screen to enter the control center.
   - On your CTP20, tap .
2. Enable **DND**.
3. Save the change.

Enabling DND during an Active Call

To prevent callers from interrupting the active call, you can enable DND during an active call. The DND feature will be disabled automatically after the call ends.

Procedure

Do one of the following during a call:

- On your web user interface, go to **Home** > **DND**.
- On your VCS: on your remote control, press OK key to open the **Talk Menu** and go to **More** > **DND**.

  For VP59, tap > **DND**.
- On your CP960 conference phone, go to **More** > **DND**.

- On your CTP20, tap > **DND**.

Enabling Fast Audio Call for CP960

If you enable this feature and users register SIP accounts or H.323 accounts in VCS endpoints, you can view the interface of **Audio Call** on CP960 conference phone. You can tap **Audio Call** to place an audio call, and the call is placed via SIP account or H.323 account by default. This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
2. Enable **Fast Audio Call**.

Managing the Directory

This chapter describes how to manage and configure directory settings. Your system provides local directory, Yealink cloud directory, Yealink enterprise directory and LDAP directory.

- Local Directory
- Yealink Cloud Contacts
- Enterprise Directory
- LDAP
- Meeting Whitelist
- Meeting Blacklist

Local Directory

You can add, edit, delete, search or simply dial a contact from the local directory.

- Adding Local Contacts and Conference Contacts
- Importing a Local Contact List
- Exporting Local Contact List
- Editing Local Contacts
- Deleting Local Contacts

Adding Local Contacts and Conference Contacts

A conference contact consists of one or more local contacts. You can establish a conference quickly by calling the conference contact. It is not applicable to MeetingEye 600/MeetingEye 400/VC500/VC200/VP59.

- Adding a Local Contact
- Adding Conference Contacts

Adding a Local Contact

You can add 500 local contacts to your system at most.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Directory** > **Local** > **New Contact**.
   - For VP59, tap **Dial/New Meeting** > **Directory** > **Add** > **Add Local Contact**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Name	Configure the contact name.	Web user interface Endpoint CTP20
Number	Configure the contact number.	Web user interface Endpoint CTP20
Add New Number	You can add up to 3 numbers for the local contact.	Endpoint CTP20
Bandwidth	Select the desired bandwidth. The default value is Auto, which means the system will select the appropriate bandwidth automatically. **Note**: When you call a local contact, the call rate that applies (video call rate or bandwidth) is the rate with the lower value. For more information, refer to Specifying the Video Call Rate.	Web user interface Endpoint CTP20

Adding Conference Contacts

You can add 100 conference contacts at most.

About this task

Note: Adding conference contact is only applicable to VC880/VC800/PVT980/PVT950 with a multipoint license.

Procedure

1. Do one of the following:
   - If you import the multipoint license to the device, on your web user interface, go to **Directory** > **Local**.

     Select the check boxes of desired local contacts and click **New Contact** > **Conf**.
2. Enter the conference name.

3. Save the change.

Note:

The number of local contacts that you can add to a conference contact depends on the imported multipoint license.

For example, if you import a 24-way license to your VC880/ VC800/PVT980/PVT950, you can add up to 24 local contacts to the conference contact. For more information the MCU certificate, contact the system administrator.

Related tasks

Viewing Multipoint License Status

Importing a Local Contact List

You can upload a local contact list to your system to add multiple contacts at a time. The system supports the XML and CSV format contact lists.

Procedure

1. On your web user interface, go to **Directory** > **Local Directory**.
2. Click **Import**.
3. Click the import box, and upload the contact file from your computer.
4. Click **Import**.
5. If you import a CSV format contact list, configure and save the following settings:

Parameter	Description	Configuration Method
The first line as the title	It will prevent importing the title of the local contact information which is located in the first line of the CSV file. • Check—do not import the first line of the CSV file. • Uncheck—import the first line of the CSV file.	Web user interface
Delete Old Contacts	It will delete all existing local contacts while importing the contact list. • Check—delete the old contacts. • Uncheck—do not delete the old contacts.	Web user interface
Ignore	This column will not be imported to the system.	Web user interface
Display name	This column will be imported to the system as the local contact's name. **Note**: This column must be imported to the system, or you cannot import the local contact list.	Web user interface

Parameter	Description	Configuration Method
Group	This column will be imported to the system as the group.	Web user interface
Number	This column will be imported to the system as the local contact's number.	Web user interface
Bandwidth	This column will be imported to the system as the local contact's bandwidth.	Web user interface

Exporting Local Contact List

You can export a local contact list in XML format from your system. Therefore, you can share it with other systems.

Procedure

1. On your web user interface, go to **Directory** > **Local Directory**.
2. Click **Export** > **XML/CSV**.

Editing Local Contacts

Procedure

1. Do one of the following:
   - On your web user interface, go to **Directory** > **Local Directory**.

     Hover your cursor over the desired local contact, and click .
   - For VP59, go to **Dial/New Meeting** > **Directory**.

     Select the desired local contact and tap **Edit Phone Contact**.
   - On your CP960 conference phone, tap **Directory**.

     Tap beside the desired contact.
2. Edit the contact information.

Deleting Local Contacts

You can delete a contact, multiple contacts or all contacts in your local directory.

- Deleting Multiple Local Contacts
- Deleting All Local Contacts
- Deleting a Local Contact

Deleting Multiple Local Contacts

Procedure

1. On your web user interface, go to **Directory** > **Local Directory**.
2. Select the checkboxes of desired local contacts.
3. Click **Delete Contacts**, and select **Selected**.

   The page prompts whether or not you are sure to delete.
4. Confirm the action.

Deleting All Local Contacts

Procedure

1. On your web user interface, go to **Directory** > **Local Directory**.
2. Select **Delete Contacts** > **Delete All**.
   The page prompts whether or not you are sure to delete.
3. Confirm the action.

Deleting a Local Contact

Procedure

1. Do one of the following:
   - On your web user interface, go to **Directory** > **Local Directory**.

     Hover your cursor over the desired local contact, and click .
   - For VP59, go to **Dial** > **Directory**.

     Select the desired local contact and tap **Delete Phone Contact**.
   - On your CP960 conference phone, tap **Directory**.

     Tap after the desired contact, and then tap **Delete**.
2. Confirm the action.

Yealink Cloud Contacts

Cloud directory appears only when you log into the Yealink VC Cloud Management Service. Contact your system administrator for more information. Cloud directory includes all Yealink cloud contacts which are created and managed by the enterprise administrator. Only the Yealink Cloud enterprise administrator can add, edit and delete Yealink Cloud contacts on the Yealink VC Cloud Management Service platform.

On your system, you can only search for and place calls to the Yealink cloud contacts.

Related tasks

Registering a Yealink Cloud Account

Enterprise Directory

The enterprise directory appears only when you log into the Yealink Meeting Server. The enterprise directory includes all YMS contacts which are created and managed by your enterprise administrator. Note that only the enterprise administrator can add, edit and delete YMS contacts on the Yealink Meeting Server.

On your system, you can only search for and place calls to the YMS contacts.

Related tasks

Registering a YMS Account

LDAP

LDAP is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. You can configure the systems to interface with a corporate directory server that supports LDAP version 2 or 3. The following LDAP servers are supported: 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 advantage of LDAP is that users can quickly find contacts from the LDAP server without having to maintain the phone book locally. The contact information returned by the LDAP server is read-only, and the user can call an LDAP contact, but cannot add, edit, or delete an LDAP contact. The administrator can configure the filtering conditions of the LDAP request on the devices, such as the number of displayed contacts, the returned information, and how to sort contacts.

The method about how the devices search for contacts on LDAP is described as below:

- Enter the content you want to search in the Dialing interface (ensure that the callee has enabled the LDAP in the matching list).
- In the Contact interface, select the “Colleague” group to go to the LDAP search interface and enter the desired content.

The device sends a search request to the LDAP server, and the LDAP server will search all contacts according to the input content and the filtering condition, and then return the matched result to the device.

- LDAP Attributes
- Configuring LDAP

LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on systems.

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	The unique identifier for each entry
dc	dc	The domain component
-	company	The company or the organization name
-	telephoneNumber	The office phone number
mobile	mobilephoneNumber	The mobile or cellular phone number
ipPhone	IPphoneNumber	The home phone number

Configuring LDAP

Procedure

1. On your web user interface, go to **Directory** > **LDAP**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
LDAP Enable	Enable or disable the LDAP feature on the system. **Default**: Disabled.	Web user interface
LDAP Name Filter	Configure the name attribute for LDAP searching. **Example**: (|(cn=%)(sn=%))	Web user interface
LDAP Number Filter	Configure the number attribute for LDAP searching. **Example**: (|(telephoneNumber=%)(mobile=%))	Web user interface
LDAP TLS Mode	Configure the connection mode between the LDAP server and the 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	Configure the domain name or the IP address of the LDAP server.	Web user interface
Port	Configure the LDAP server port. **Default**: 389.	Web user interface

Parameter	Description	Configuration Method
LDAP User Name	Configure the user name used to log into the LDAP server. **Note**: The user name is provided by the LDAP 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	Configure the password to log into the LDAP server. **Note**: The password is provided by the LDAP server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the password to access the LDAP server.	Web user interface
LDAP Base	Configure the root path of the LDAP search base. **Example**: cn=manager,dc=yealink,dc=cn	Web user interface
Max.Hits	Configure the maximum number of search results returned by the LDAP server. **Valid Value**: 1 to 32000, default value: 50.	Web user interface
LDAP Name Attributes	Configure the name attributes of each record returned by the LDAP server. **Note**: multiple name attributes should be separated by spaces. **Example**: cn sn	Web user interface
LDAP Number Attributes	Configure the number attributes of each record returned by the LDAP server. **Note**: multiple number attributes should be separated by spaces. **Example**: telephoneNumber mobile	Web user interface

Parameter	Description	Configuration Method
LDAP Display Name	Configure the contact attributes displayed on the LCD screen. **Note**: multiple contact attributes should be separated by spaces. **Example**: %cn	Web user interface
Protocol	Specify 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	Enable or disable the system to match caller numbers with LDAP contacts. If the match is successful, the system will display the caller name when receiving an incoming call. **Default**: Disabled.	Web user interface
Call Match	Enable or disable the system to match outgoing call numbers with LDAP contacts. If the match is successful, the system will display the contact name when placing a call. **Default**: Disabled.	Web user interface
LDAP Sorting Results	Enable or disable the system to sort the search results in alphabetical order or numerical order. **Default**: Disabled.	Web user interface

For more information about the string display method of the LDAP search filter, refer to *http://www.ietf.org/rfc/rfc2254*.

Meeting Whitelist

You can add meeting whitelist. The users in the whitelist can join your conference call directly without meeting password even if you have enabled the meeting password feature. Your system supports up to 100 whitelist records. This feature is not applicable to VP59.

- Adding Meeting Whitelist
- Deleting the Meeting Allowlist

Adding Meeting Whitelist

The users in the whitelist can call you without the password.

Procedure

1. On your web user interface, go to **Directory** > **Meeting Whitelist**.
2. Enter the desired number.
   The value can be the IP address, the account number, or the domain name.
3. Click **Add**.

Note:

Users in the whitelist can join virtual meeting room 1 of conference moderator without a password. If conference moderator hosts a VMR mode conference, users in the whitelist still need password to join virtual meeting room 2.

Deleting the Meeting Allowlist

Procedure

1. On your web user interface, go to **Directory** > **Meeting Whitelist**.
2. Click beside the desired allowlist.
   It prompts whether you are sure to delete the whitelist.
3. Confirm the action.

Meeting Blacklist

You can add meeting blacklist. Your system will refuse incoming calls from the blacklist automatically. Your system will not remind incoming calls or save call history from blacklist.

Your system supports up to 100 blacklist records.

- Adding Meeting Blacklist
- Deleting the Meeting Blacklist

Adding Meeting Blacklist

You can add the desired number to the meeting blacklist and the VCS endpoint will refuse incoming calls from the blacklist automatically.

Procedure

1. On your web user interface, go to **Directory** > **Meeting Blacklist**.
2. Enter the desired number.
   The value can be the IP address, the account number, or the domain name.
3. Click **Add**.

Deleting the Meeting Blacklist

Procedure

1. On your web user interface, go to **Directory** > **Meeting Blacklist**.

2. Click beside the desired blacklist.
   It prompts whether you are sure to delete the blacklist.
3. Confirm the action.

Managing the Call History

The call history contains the list of all calls, the missed calls, the placed calls and the received calls. You can view up to 100 pieces of the call records. The call log contains call information such as remote party identification and time and date of the call.

- Saving History Record
- Adding a History Record to the Local Directory
- Deleting Call Records
- Placing Calls from Call History

Saving History Record

You can configure the system to save the history records or not.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **General** > **Basic**.
     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Call Features**.
     For VP59, tap > **Settings** > **Basic** > **Call Features**.
   - On your CTP20, tap > **Settings** > **Basic** > **Cal Features**.
2. Enable/disable **History Record**.

Adding a History Record to the Local Directory

Procedure

1. Do one of the following:
   - For VP59, go to **New Meeting/ Dial** > **History**.
     Select **All Calls** or **Missed Call**.
     Select the desired call record.
     Tap **Add to Contact** on the right side of the screen.
   - On your CP960 conference phone, tap **History**.
     Tap beside the desired history record, and then tap **Add to Contact**.
2. Edit the corresponding information and save the information.

Deleting Call Records

You can delete a single call record, multiple call records or all call records.

- Deleting a Call Record
- Deleting Multiple History Records
- Deleting All History Records

Deleting a Call Record

Procedure

1. Do one of the following:
   - For VP59, select the desired call type and tap **Delete Call**.
   - On your CP960 conference phone, tap **History**.

     Tap ⓘ after the desired call record, and then tap **Delete**.
2. Confirm the action.

Deleting Multiple History Records

Procedure

1. On your web user interface, go to **Directory** > **History**.
2. Select the checkboxes of desired history records.
3. Click **Delete Calllog**, and select **Selected**.

Deleting All History Records

Procedure

Do one of the following:

- On your web user interface, go to **Directory** > **History**.

  Go to **Delete Calllog** > **Delete All**.

Placing Calls from Call History

Procedure

Do one of the following:

- On your web user interface, go to **Directory** > **History**.

  Click or beside the desired call record to place a video or audio call.
- On your VCS, go to **Dial** > **History**.

  If you register a Yealink Cloud account or YMS account, go to **New Meeting** > **History**.

  Select the desired call record and dial it out.

  For VP59, select the desired call type and tap the desired call record to dial it out.

- On your CP960 conference phone, tap **History**.

  Tap ⓘ beside the desired call record and then tap **Video Call** or **Voice Call**.
- On your CTP20, tap **Dial** > **History**.

  If you register a Yealink Cloud account or YMS account, go to **New Meeting** > **History**.

  Select the desired call type and the call record,then dial it out.

Placing a Call

You can use your system just like a regular phone to place calls in numerous ways.

- Placing a Call by Entering a Number
- Editing Numbers Before Placing a Call

Placing a Call by Entering a Number

You can place a call by using the web user interface, the remote control or the CP960 conference phone.

About this task

You can place a call to following account types:

- IP address (for example: 192.168.1.15)
- H. 323 account
- SIP account
- Cloud account
- PSTN account
- SIP URI (for example: 2210@sip.com)

Procedure

Do one of the following:

- On your web user interface, go to **Home**.

  Enter the number in the **Enter Number** field.

  Select the desired call type and video call rate.

  Click **Video Call** or **Voice Call** to place a video or voice call.
- On your VCS, go to **Dial** > **Dial**.

  If you register a Yealink Cloud account or YMS account, go to **New Meeting** > **Dial**.

  Go to **Auto** at the screen bottom and select the desired call type from the drop-down menu.

  Enter the number and dial.

  For VP59, Enter the number and dial.
- On your CP960 conference phone, tap **Dial**.

  Tap **Auto**, and select the desired call type from the drop-down menu.

  Enter the number and dial.

- On your CTP20, tap **Dial** > **Dial**.

  If you register a Yealink Cloud account or YMS account, go to **New Meeting** > **Dial**.

  Tap **Auto** and select the desired call type from the drop-down menu.

  Enter the number and dial.

Related tasks
Specifying the Video Call Rate
Related information
Account Polling

Editing Numbers Before Placing a Call

In the Dial or History screen, you can edit the contact numbers or history records and then dial out.

Procedure

1. Do one of the following:
   - For VP59, go to **Dial/New Meeting** > **History** > **All Calls/Missed Call**.

     Select the desired call record and tap **Edit before calling**.
   - On your CP960 conference phone, tap **History**.

     Tap ⓘ beside the desired record.
2. Edit the number and dial out.

Configuring the Security Features

The following introduces how to configure the security features.

- Collaboration Data Security Control
- Configuring the Auto Logout Time
- Transport Layer Security (TLS)
- System Integrated with Control Systems

Collaboration Data Security Control

By default, WPP20 and CTP20 connection via wireless need to authenticate first when receiving shared content or initiating receiving whiteboard. It can prevent other people from using WPP20 or CTP20 outside the conference room to obtain shared content or whiteboard annotations via wireless connection. Only one authentication is required during the call. After each collaboration in the non-call, the host will cache the authentication status of the accessory within a certain period of time. If timeout, the accessory needs to be re-authenticated. You can configure whether the accessory needs to confirm the collaborative data security control before joining the collaboration. This feature is not applicable to VP59.

About this task
Pay attention to the following two situations:

- The process of receiving the shared content or initiating receiving whiteboard only needs to be authenticated once. That is, if the authentication is performed when the shared content is received, the whiteboard can be initiated within the configured authentication state time without re-authentication.

- When the same PC is replaced with a different WPP20 or the WPP20 is removed and reconnected or the PC is restarted, re-authentication is not required. When the same WPP20 is replaced with a different PC, authentication is required if the PC has not been authenticated.

Procedure

1. On web user interface, go to **Setting** > **Collaboration Tools** > **Collaboration Data**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Video & Audio** > **Collaboration Data**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Accessories Join Collaboration Confirmation	Enable or disable the WPP20/CTP20 accessory for wireless connection to be authenticated first when receiving collaboration data. **Note**: the default value is On. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Configuring the Auto Logout Time

The system will log out of the web user interface automatically after being inactive for a period of time. You need to re-enter the login credentials to login. You can change the auto logo time.

Procedure

1. On your web user interface, go to **Setting** > **General** > **Basic** > **ReLogOffTime(1-1000min)**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information** > **ReLogOffTime(1-1000min)**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
ReLogOffTime (1-1000min)	Specify the inactive time (minutes) before the system logs out of the web user interface automatically. **Default**: 5 minute.	Web user interface

Transport Layer Security (TLS)

Transport Layer Protocol (TLS) is a commonly used protocol for ensuring communications privacy and managing the security of the message transmission. When secured by the TLS protocol, the device can transmit the data and communicate safely.

The TLS protocol includes two protocol groups: the TLS handshake protocol and the TLS record protocol. The TLS handshake protocol allows the server and the client to authenticate with each other before negotiating about the data, the encryption algorithms and the encrypted keys. The TLS Record Protocol completes the actual data transmission and ensures the data integrity and confidentiality. The TLS protocol

uses an asymmetric encryption algorithm to exchange keys, a symmetric encryption algorithm to ensure data confidentiality, and the MAC algorithms to ensure data integrity.

- Supported Cipher Suites
- TLS Transport Protocol
- Managing the Trusted Certificates List
- Managing the Server Certificates
- Secure Real-Time Transport Protocol (SRTP)
- H.235 Encryption
- Defending against Attacks

Supported Cipher Suites

The system supports TLS version 1.0, 1.1 and 1.2. 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 by 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
- DES-CBC3-MD5
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- RC2-CBC-MD5
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- RC4-64-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
- 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-RC2-CBC-MD5
- EXP-RC4-MD5

TLS Transport Protocol

When using SIP account, SIP IP call, or logging in to Zoom, Pexip, BlueJeans or a custom third-party platform, you can choose the TLS transport method for the SIP protocol to ensure the confidentiality of the communication and the security of the information transmission.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **Video Conference Platform** > **Platform Type** > **Zoom/Pexip/BlueJeans/Videxio/Custom**.
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Account** > **SIP Account/ SIP IP Call**.

     For VP59, go to > **Settings** > **Advanced** > **Account** > **SIP Account/SIP IP Call**.
   - On your CTP20, tap > **Settings** > **Advanced** > **Account** > **SIP Account/ SIP IP Call**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Transport	Specify the transport protocol for SIP signaling. The supported protocols are as follows: • **UDP**—it provides the best transmission for SIP signaling. • **TCP**—it provides a reliable transmission for SIP signaling. • **TLS**—it provides a safe transmission for SIP signaling. TLS is available only when the device is registered on a SIP server that supports TLS. • **DNS-NAPTR**—the device performs the DNS NAPTR and SRV request to find the service type and the port if no server port is given. **Note**: • Yealink Cloud Platform and StarLeaf Cloud platform cannot be configured. • The default value of the Zoom/Pexip/BlueJeans/ Videxio/Custom Cloud platform/SIP IP call is TCP. • The default value of EasyMeet Cloud platform is TLS. • The default value of the SIP account is UDP. • If you use TLS, you need to upload the CA certificate to the server for the devices.	Web user interface Endpoint CTP20

Managing the Trusted Certificates List

When the system serves as a TLS client and requests a TLS connection with a server, the system should verify the server certificate sent by the server to decide whether it is trusted based on the trusted certificates list.

About this task

The trusted certificates list contains the default and the custom certificates.

- **Default Certificates**: The system has 36 built-in trusted certificates.

- **Custom Certificates**: You can upload up to 10 trusted certificates with the size no more than 5M to the system. The CA certificates supported by the system must be in .pem, .cer, .crt, or .der file format.

Procedure

1. On your web user interface, go to **Security** > **Trusted Certs**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Only Accept Trusted Certificates	Enable or disable the system only trusting the server certificates in the trusted certificates list. **Note**: the default value is On. If it is disabled, the system can connect to the server no matter whether the certificate send by the system is valid or not. 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. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Common Name Validation	Enable or disable the system to mandatorily validate the CommonName or SubjectAltName of the server certificate sent by the server. This security verification rules are compliant with RFC 2818. **Note**: the default value is Off. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Parameter	Description	Configuration Method
CA Certificates	Specify the certificate type in the Trusted Certificates list for the system to authenticate for the TLS connection. • **Default Certificates**—the device authenticates whether the server is reliable via the built-in CA certificates. • **Custom Certificates**—the device authenticates whether the server is reliable via the uploaded CA certificates. • **All Certificates**—the device authenticates whether the server is reliable via both the built-in and the uploaded CA certificates. **Note**: the default value is **Default Certificates**. 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 for the device. **Note**: the certificate must be in .pem, .der, .crt, or .cer file format. You can upload up to 10 CA certificates.	Web user interface

- Default Certificates List

Default Certificates List

The following introduces 204 most common used CA Certificates built in Yealink video conferencing system.

- Baltimore CyberTrust Root
- ISRG Root X1
- GlobalSign
- Cybertrust Global Root
- Wells Fargo Root Certificate Authority
- Thawte Personal Freemail CA
- Thawte Server CA
- Thawte Premium Server CA
- QuoVadis Root Certification Authority
- Baltimore CyberTrust Root
- TDC Internet Root CA
- Sonera Class2 CA
- Root CA Generalitat Valenciana
- DST Root CA X3

- WellsSecure Public Root Certificate Authority
- GeoTrust Global CA
- Visa eCommerce Root
- QuoVadis Root CA 2
- E-Tugra Certification Authority
- Hongkong Post Root CA 1
- Security Communication RootCA1
- Trustis FPS Root CA
- Yealink Server CA
- Baltimore CyberTrust Root
- Swisscom Root CA 1
- KISA RootCA 1
- Entrust Root Certification Authority
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA II
- TC TrustCenter Universal CA I
- TC TrustCenter Class 4 CA II
- RSA Security 2048 V3
- CNNIC ROOT
- Certum CA
- Certigna
- NetLock Arany (Class Gold) Főtanúsítvány
- GlobalSign Root CA
- ACEDICOM Root
- Class 1 Public Primary Certification Authority
- Class 3 Public Primary Certification Authority - G2
- Class 1 Public Primary Certification Authority - G2
- Class 2 Public Primary Certification Authority - G2
- Class 4 Public Primary Certification Authority - G2
- Class 3 Public Primary Certification Authority
- Certinomis - Autorité Racine
- D-TRUST Root Class 3 CA 2 2009
- D-TRUST Root Class 3 CA 2 EV 2009
- Microsec e-Szigno Root CA 2009
- Certum Trusted Network CA
- Secure Certificate Services
- Trusted Certificate Services
- AAA Certificate Services
- COMODO RSA Certification Authority
- ComSign Secured CA
- GlobalSign Root CA - R3
- GeoTrust Universal CA 2
- GeoTrust Universal CA
- SecureSign RootCA11
- Security Communication RootCA2
- Entrust.net Certification Authority (2048)
- EE Certification Centre Root CA
- Autoridad de Certificacion Firmaprofesional CIF A62634068
- ES
- AffirmTrust Commercial

- AffirmTrust Networking
- TWCA Root Certification Authority
- TWCA Global Root CA
- Entrust Root Certification Authority - G2
- SecureTrust CA
- Secure Global CA
- TC TrustCenter Universal CA III
- Network Solutions Certificate Authority
- COMODO Certification Authority
- AC Raíz Certicámara S.A.
- China Internet Network Information Center EV
- Actalis Authentication Root CA
- DigiCert High Assurance EV Root CA
- DigiCert Global Root CA
- DigiCert Assured ID Root CA
- QuoVadis Root CA 2
- QuoVadis Root CA 3
- Hellenic Academic and Research Institutions RootCA 2011
- Atos TrustedRoot 2011
- EC-ACC
- Swisscom Root CA 2
- Swisscom Root EV CA 2
- certSIGN ROOT CA
- TeliaSonera Root CA v1
- Government Root Certification Authority
- T-TeleSec GlobalRoot Class 2
- T-TeleSec GlobalRoot Class 3
- Yealink Equipment Issuing CA
- Yealink Root CA
- ePKI Root Certification Authority
- Go Daddy Class 2 Certification Authority
- Starfield Class 2 Certification Authority
- XRamp Global Certification Authority
- ISRG Root X1
- SwissSign Gold CA - G2
- SwissSign Silver CA - G2
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 1 Public Primary Certification Authority - G3
- thawte Primary Root CA
- GeoTrust Primary Certification Authority
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G5
- StartCom Certification Authority
- Chambers of Commerce Root
- Global Chambersign Root
- America Online Root Certification Authority 1
- OISTE WISeKey Global Root GA CA
- Izenpe.com
- Entrust Root Certification Authority - EC1

- VeriSign Universal Root Certification Authority
- thawte Primary Root CA - G3
- GeoTrust Primary Certification Authority - G3
- Thawte Universal CA Root
- Security Communication EV RootCA1
- America Online Root Certification Authority 2
- DigiCert Assured ID Root G2
- DigiCert Trusted Root G4
- DigiCert Global Root G2
- DigiCert Assured ID Root G3
- DigiCert Global Root G3
- Amazon Root CA 1
- VeriSign Class 3 Public Primary Certification Authority - G4
- GeoTrust Primary Certification Authority - G2
- USERTrust RSA Certification Authority
- thawte Primary Root CA - G2
- COMODO ECC Certification Authority
- Starfield Root Certificate Authority - G2
- Starfield Services Root Certificate Authority - G2
- Go Daddy Root Certificate Authority - G2
- Chambers of Commerce Root - 2008
- Global Chambersign Root - 2008
- Buypass Class 3 Root CA
- Buypass Class 2 Root CA
- AffirmTrust Premium
- AffirmTrust Premium ECC
- StartCom Certification Authority G2
- Amazon Root CA 3
- Amazon Root CA 4
- Amazon Root CA 2
- GENBAND
- CA Disig Root R1
- CA Disig Root R2
- Yealink Root CA
- Yealink Root CA
- Yealink Root CA
- Yealink Root CA 2
- Yealink Root CA 2
- Yealink Root CA 2
- Symantec Class 3 Secure Server CA - G4
- yealinkvc.com
- quickconnect.starleaf.com
- Go Daddy Root Certificate Authority - G2
- Videxio AS Root CA
- StarLeaf CA
- MarketWare Server CA 2
- QuoVadis Root CA 2 G3
- DigiCert SHA2 High Assurance Server CA
- Sectigo RSA Organization Validation Secure Server CA
- QuoVadis Global SSL ICA G3

- *.okta.com
- GTS CA 1O1
- Sectigo RSA Domain Validation Secure Server CA
- Trusted Secure Certificate Authority DV
- Swiss Government Root CA III
- Certplus Root CA G1
- USERTrust ECC Certification Authority
- TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı H5
- GlobalSign
- TUBITAK Kamu SM SSL Kok Sertifikasi - Surum 1
- SSL.com Root Certification Authority RSA
- OpenTrust Root CA G2
- Staat der Nederlanden EV Root CA
- IdenTrust Public Sector Root CA 1
- QuoVadis Root CA 1 G3
- OpenTrust Root CA G3
- SSL.com EV Root Certification Authority RSA R2
- Staat der Nederlanden Root CA - G3
- SSL.com EV Root Certification Authority ECC
- TrustCor RootCert CA-1
- SSL.com Root Certification Authority ECC
- CFCA EV ROOT
- Hellenic Academic and Research Institutions ECC RootCA 2015
- OpenTrust Root CA G1
- SZAFIR ROOT CA2
- GDCA TrustAUTH R5 ROOT
- AC RAIZ FNMT-RCM
- TrustCor ECA-1
- LuxTrust Global Root 2
- Certum Trusted Network CA 2
- TrustCor RootCert CA-2
- IdenTrust Commercial Root CA 1
- Certinomis - Root CA
- Certplus Root CA G2
- Hellenic Academic and Research Institutions RootCA 2015
- OISTE WISeKey Global Root GB CA
- QuoVadis Root CA 3 G3
- Hotspot 2.0 Trust Root CA - 01
- Hotspot 2.0 Trust Root CA - 02
- Hotspot 2.0 Trust Root CA - 03

Note:

The most common used CA Certificates are built in Yealink phones. Due to memory constraints, we cannot ensure a complete set of certificates. If there is no the desired certificate in the above list, contact your distributor for the desired one. After that, you can upload the certificate into your phone. For more information on uploading custom CA certificate, refer to Transport Layer Security (TLS).

Managing the Server Certificates

The system can serve as a TLS server. When clients request a TLS connection with the system, the system sends the server X.509 (V3) certificate (device certificate) to the clients for authentication.

About this task

The server X.509 (V3) certificate contains the default and the custom certificates, and you can specify the certificate type sent by the endpoint to the client for authentication.

- **Default Certificates**: a unique server certificate and a generic server certificate.

  Only if no unique certificate exists, the system may send a generic certificate for authentication.
- **Custom Certificates**: You can only upload one server certificate to the endpoint. The old server certificate will be overridden by the new one. The server certificate must be in .pem or .cer file format with the size less than 5M.

Procedure

1. On your web user interface, go to **Security** > **Server Certs**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Device Certificates	Specify the type of the server certificates for the system to send for TLS authentication. • **Default Certificates** • **Custom Certificates** **Note**: the default value is Default Certificates. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Upload Server Certificate File	Upload the server certificate. **Note**: the certificate must be in .pem or .cer file format. Only one server certificate can be uploaded to the system.	Web user interface

Secure Real-Time Transport Protocol (SRTP)

Secure Real-Time Transport Protocol (SRTP) encrypts the RTP during SIP calls to avoid interception and eavesdropping. The RTP and the RTP stream in a call are encrypted by AES algorithm which is compliant with RFC3711. The data in the RTP stream cannot be understood even though it is captured or intercepted. Only the receiver has the key to restore the data. To use SRTP, the parties participating in the call must enable SRTP feature simultaneously. When this feature is enabled on both sites, the encryption type used in the session is negotiated by the systems. This negotiation process is compliant with RFC 4568.

When you place a call that enables SRTP, the system sends an INVITE message with the RTP encryption algorithm to the destination system.

The rules of SRTP for media encryption in SIP calls are described as below:

Remote\Local	Compulsory	Optional	Disabled
Compulsory	SRTP Call	SRTP Call	Fail to establish a call
Optional	SRTP Call	SRTP Call	RTP Call
Disabled	Fail to establish a call	RTP Call	RTP Call

Example of the INVITE message carried with the RTP encryption algorithm in the SDP is described as below:

```
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 replying the 200 OK message which carries the negotiated RTP encryption algorithm.

Example of the 200 message carried with the RTP encryption algorithm in the SDP is described as below:

```
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
```

Note:

If you enable SRTP and you can also enable TLS, which can ensure the security of SRTP encryption. For more information about TLS, refer to TLS Transport Protocol.

- Configuring SRTP

Configuring SRTP

You can set SRTP for the SIP protocol when using a SIP account, SIP IP call, or logging in to Zoom, Pexip, BlueJeans, or a custom third-party platform.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Account** > **VC Platform** > **Platform Type** > **Zoom/Pexip/BlueJeans/Custom**.
   - On your web user interface, go to **Account** > **SIP Account/SIP IP Call**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
SRTP	Specify the SRTP type. The supported types are as follows: • **Disabled**—the SRTP feature is disabled in the SIP call. • **Optional**—the call parties in a SIP call will negotiate whether to use the SRTP feature or not. • **Compulsory**—the SRTP feature is enabled compulsorily in the SIP call. **Default**: Disabled.	Web user interface

During the SIP call, call parties can see the encrypted icon displayed in their screens.

H.235 Encryption

H.235 system provides the identity authentication, the data encryption, and the integration. H.235 encrypts the RTP during H.323 calls to avoid interception and eavesdropping.

The H.235 is supported by the systems. The parties participating in the call must enable H.235 feature simultaneously. When this feature is enabled on both sites, the encryption type used in the session is negotiated between the systems. The StarLeaf platform also supports H.235 encryption. After logging in to the StarLeaf platform, you can use H.235 encryption.

Rules of H.235 security in H.323 calls are described as below:

Remote\Local	Compulsory	Optional	Disabled
Compulsory	H.235 Call	H.235 Call	Fail to establish a call
Optional	H.235 Call	H.235 Call	RTP Call
Disabled	Fail to establish a call	RTP Call	RTP Call

- Configuring H.235 Encryption

Configuring H.235 Encryption

When you log in to the StarLeaf platform or use an H.323 account, you can configure the H.235 encryption feature for the H.323 protocol.

Procedure

1. On your web user interface, go to **Account** > **H.323**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
H.235 Encryption	Configure the H.235 encryption. The supported types are as follows: • **Disabled**—the H.235 encryption feature is disabled in the H.323 call. • **Optional**—the call parties in an H.323 call will negotiate whether to use the H.235 encryption feature or not. • **Compulsory**—the H.235 encryption feature is enabled compulsorily in the H.323 call. **Default**: Disabled.	Web user interface

During the H.323 call, call parties can see the encrypted icon displayed in their screens.

Defending against Attacks

VCS sometimes may receive calls from unknown caller, and the calls may be unable to answer. For the communication security, VCS supports the features of defending against attacks. You can configure the abnormal call answering feature to handle the abnormal SIP incoming call or configure the safe mode call feature to verify the H.323 incoming call.

- Configuring Abnormal Call Answering
- Configuring the Safe Mode Call

Configuring Abnormal Call Answering

When the destination address of the incoming SIP call does not match the local address, the call is considered to be an abnormal call. You can deal with them by setting them as the abnormal SIP incoming call. You can reject the abnormal SIP incoming call, or answer it by using IP address or SIP account randomly. This feature is not applicable to VP59.

Procedure

1. On your web user interface, go to **Call Features** > **Call Features** > **Inbound Call Settings**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Abnormal Call Answering	Specify the account type for answering abnormal SIP incoming calls. The supported types are as follows: • **Disabled**—reject the abnormal SIP incoming calls. • **Account Answer**—use the registered 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

Configuring the Safe Mode Call

The safe mode call feature is used to verify whether the incoming H.323 call is coming from an H.323 endpoint.

Procedure

1. On your web user interface, go to **Setting** > **Inbound Call Settings**.

   For MeetingEye 600/MeetingEye 400, go to **Setting** > **Call Features**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Safe Mode Call	Enable or disable the safe mode call feature. The supported types are as follows: • **Off**—answer incoming H.323 calls directly without validation. • **On**—verify whether the incoming H.323 call is coming from an H.323 endpoint. If it is, the system will answer it. If not, the incoming call will be rejected. **Default**: Disabled.	Web user interface

System Integrated with Control Systems

Yealink video conferencing system provides API for third-party control system to integrate with. Therefore, third-party control system can control Yealink video conferencing system via API. This feature is not applicable to VP59.

- Connection Methods of Control Systems
- Connection Settings for Control Systems

Connection Methods of Control Systems

You can connect Yealink video conferencing system to the control system via LAN connection or Serial connection. Select one of the following:

- **LAN Connection**: Make sure the Yealink video conferencing system and the control system are in the same network segment. If you use this mode to control the system, TCP protocol is recommended. To establish a connection, the control system needs to know the IP address and TCP port of the Yealink video conferencing system.
- **Serial Connection**: 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.

For more information, refer to Yealink VC Deployment and User Manual for Control Systems and API Commands Introduction for Yealink Video Conferencing System.

Connection Settings for Control Systems

You need to finish following settings before you connect the video conferencing system to the control system. This feature is not available to VP59.

Procedure

1. On your web user interface, go to **Security** > **Security Control**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Current Control TCP Port	Control TCP port (read-only). **Default**: 6024.	Web user interface
Control Security Enabled	Enable or disable an authentication password when the control system tries to connect to the video conferencing system. **Default**: On. If you change this parameter, the system will reboot to make the change take effect.	Web user interface

Parameter	Description	Configuration Method
Control Security Password	The authentication password required when the control system tries to connect to the video conferencing system. **Default**: blank. **Note**: this parameter is only available for **Control Security Enabled**. If you change this parameter, the system will reboot to make the change take effect.	Web user interface
Baud Rate	Configure the baud rate. • **2400** • **4800** • **9600** • **19200** • **38400** • **115200** **Note**: The default value is 115200. It must be the same rate for the control system and Yealink video conferencing system.	Web user interface
Data Bits	Configure the data bits. • **7** • **8** **Note**: The default value is 8. It must be the same rate for the control system and Yealink video conferencing system.	Web user interface
Parity	Configure the parity. • **None** • **Odd** • **Even** • **Space** **Note**: **Default**: blank. It must be the same rate for the control system and Yealink video conferencing system.	Web user interface

Parameter	Description	Configuration Method
Stop Bits	Configure the stop bits. • **1** • **2** **Note**: The default value is 1. It must be the same rate for the control system and Yealink video conferencing system.	Web user interface

CEC Monitor Controls

Consumer Electronics Control (CEC) is a feature of HDMI designed to allow users to command and control devices connected through HDMI by using only one remote control. The users can use a remote control to control all the devices connected by HDMI.

MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/PVT980/PVT950 supports the CEC feature by default. Make sure that you connect a monitor CEC supported to the system and enable the CEC feature on the monitor. This feature is not applicable to VC200/VP59.

The following CEC features are available:

- One Touch Play-Use the system remote control to wake up the monitors. All connected CEC-capable monitors are powered on, and their displays are switched to VCS input.
- **System Standby**-When the VCS enters sleep mode, all connected CEC-capable monitors are switched to standby mode for power saving.

Note:

The VCS does not respond to CEC commands issued by a television remote control.

- Configuring CEC Monitor Controls

Configuring CEC Monitor Controls

Procedure

1. On your web user interface, go to **Setting** > **Monitor** > **Display Function**.
   For MeetingEye 600/MeetingEye 400, go to **Setting** > **General** > **General information**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
CEC Enable	Enable or disable the CEC feature. **Default**: Disabled.	Web user interface

Accessories with Your System

This section describes the how to use the accessories. For more information on other accessories, refer to related guide.

- Using WPP20 Wireless Presentation Pod
- Using the CPN10 PSTN Box
- Using the VCC22 Video Conferencing Cameras
- Using the CPW90-BT Bluetooth Wireless Microphones with VCS
- Using CTP20
- Using VCM34
- Using VCM38
- Using the Soundbar/MSpeaker II
- Using CP900/CP700 Ultra-Compact Speakerphone

Using WPP20 Wireless Presentation Pod

For VC880/VC800/VC500/PVT980/PVT950, you can pair with up to 5 WPP20s for content sharing at the same time. However, for MeetingEye 600/MeetingEye 400/VC200/VP59, only 1 WPP20 can be supported.

For more information, refer to Yealink WPP20 Wireless Presentation Pod Quick Start Guide.

Note: We do not recommend using WPP20 across walls, otherwise the signal energy may be consumed.

Using the CPN10 PSTN Box

It is a cost-effective solution for PSTN office. Up to 2 cascaded PSTN Boxes can be installed to video conferencing systems, which allow you to experience the conference conveniently in excellent speech quality with PSTN. For more information, refer to Yealink PSTN Box CPN10 Quick Start Guide. Up to two PSTN accounts can be registered on the system, with one-way audio call for one account. You can call PSTN users, receive the call from PSTN users, or create a conference with the PSTN user.

Using the VCC22 Video Conferencing Cameras

You can connect up to 9 VCC22 video conferencing cameras to the VC880/PVT980 video conferencing system. For VC800 video conferencing system, you can connect up to 8 VCC22 video conferencing cameras. For more information, refer to Yealink VCC22 Camera Quick Start Guide. VCC22 video conferencing cameras are not applicable to MeetingEye 600/MeetingEye 400/VC500/VP59/VC200/ VC500/ PVT950.

- Controlling VCC22 Camera
- Adjusting the Multi-Camera Layout During a Call

Controlling VCC22 Camera

When the VCS endpoint is idle, you can select the desired camera to display its video images on the display device, adjust focal length, or pan and tilt the camera.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Home** > **Camera Layout**.
   - On your CP960 conference phone, tap **Camera** > **The current control camera**.
   - On your CTP20, tap .
2. Select the desired camera and then adjust the angle and the focus.

Adjusting the Multi-Camera Layout During a Call

During a call, all video streams captured from the connected cameras are synthesized to one video stream, and then sent to the far site. You can change the camera layout during a call.

Procedure

1. Do one of the following when the system is during a call:
   - On your web user interface, go to **Home** > **Camera Layout**.
   - On your CP960 conference phone, go to **Camera** > **Layout**.
   - On your CTP20, tap > **Multi-camera Layout Switching**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Camera Layout	Configure the camera layout during a video call. • **1+N**: the video image of the selected camera is displayed in large window, and the video images of other cameras are displayed in thumbnails. • **Selected Speaker**: the video image of the selected camera is in full-screen. • **Equal N×N**: the video images of all cameras have equal size. **Default**: 1+N.	Web user interface Endpoint CP960 Conference Phone CTP20

3. If you select **1+N** or **Selected Speaker** as the camera layout, you should choose a camera you want to focus on.

Using the CPW90-BT Bluetooth Wireless Microphones with VCS

CPW90-BT Bluetooth wireless microphones can work as the audio input devices of your video conferencing system. You can connect up to 2 CPW90-BT Bluetooth wireless microphones to the video

conferencing system. For more information, refer to CPW90-BT Bluetooth Wireless Microphones Quick Start Guide.

- Registering CPW90-BT with VCS
- Deregistering CPW90 from VCS
- Viewing the Information of Bluetooth Wireless Microphones
- Finding the Registered CPW90-BT

Registering CPW90-BT with VCS

If you purchase the VCS endpoint and the Bluetooth wireless microphones together, they are already paired. Just turn the Bluetooth wireless microphones on to use them. If the model of your VCS endpoint is VC500/VC800/VC880/PVT980/PVT950, make sure a BT42 Bluetooth USB Dongle is connected before you use the Bluetooth wireless microphones. If you purchase Bluetooth wireless microphones separately, you need to pair them with the VCS endpoint manually.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Microphone** > **Search Mic**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Wireless Microphone** > **Search Mic**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Audio** > **Wireless Microphone** > **Add Wireless Microphone**.

     For VP59, tap > **Settings** > **Basic** > **Audio** > **Wireless Microphone** > **Add Wireless Microphone**.
   - On your CTP20, tap > **Settings** > **Basic** > **Audio** > **Wireless Microphone** > **Add Wireless Microphone**.
2. Place the Bluetooth wireless microphones on the charger and long press the mute button for 5 seconds until the mute LED indicator fast flashes yellow.

   The Bluetooth wireless microphones are paired with the VCS endpoint.

   Note: Up to 2 Bluetooth wireless microphones can be connected to one VCS endpoint.

Deregistering CPW90 from VCS

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Microphone** > **Log Out**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Wireless Microphone** > **Deregistration**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Audio** > **Wireless Microphone**.

     Select a wireless microphone and then select **Unbind**.

     For VP59, tap > **Settings** > **Basic** > **Audio** > **Wireless Microphone** > **Add Wireless Microphone**.

     Select a wireless microphone and then select **Unbind**.
   - On your CTP20, tap > **Settings** > **Basic** > **Audio** > **Wireless Microphone**.

     Select a wireless microphone and then select **Unbind**.

   The page prompts whether or not you are sure to unbind.

2. Click **OK**.

Viewing the Information of Bluetooth Wireless Microphones

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Microphone**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Wireless Microphone**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Audio** > **Wireless Microphone**.

     For VP59, tap > **Settings** > **Basic** > **Audio** > **Wireless Microphone**.
   - On your CTP20, tap > **Settings** > **Basic** > **Audio** > **Wireless Microphone** and select the desired wireless microphone.
2. Select a desired microphone to view the information.

Finding the Registered CPW90-BT

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Microphone**.

     For MeetingEye 600/MeetingEye 400, go to **Setting** > **Wireless Microphone**.
   - On your VCS, go to **More** > **Settings** > **Basic** > **Audio** > **Wireless Microphone**.

     For VP59, tap > **Settings** > **Basic** > **Audio** > **Wireless Microphone**.
   - On your CTP20, tap > **Settings** > **Basic** > **Audio** > **Wireless Microphone** > **Add Wireless Microphone**.
2. Select a wireless microphone and then select **Find**.

   The mute indicator LED on the CPW90-BT flashes red and green alternately.

Using CTP20

CTP20 supports wired and wireless connections. MeetingEye 600/MeetingEye 400/PVT980/PVT950/VC880/VC800/VC500 can connect up to 4 CTP20s and the VC200 can connect only one CTP20. VP59 cannot be used with a CTP20.

- Wired Connection to CTP20
- Wireless Connection to CTP20
- Using Multiple CTP20s for Collaboration

Wired Connection to CTP20

After connected to the VC Hub/Phone port via the network cable, CTP20 will be connected to the VCS endpoint automatically. For more information about the connection between CTP20 and VCS endpoints, refer to Yealink CTP20 Quick Start Guide.

Wireless Connection to CTP20

If the VC Hub/Phone port of the VCS endpoint is occupied, you can connect CTP20 to the PoE switch for power supply and to the wireless AP provided by the VCS endpoint.

Before you begin

Make sure you enable Wireless AP on VCS endpoints. For VC880/VC800/VC500/PVT980/PVT950, you also need to connect WF50 to them.

About this task

Note: If the codec connects to the wireless network and the Wireless AP is disabled, the CTP20 cannot use the wireless connection.

Procedure

1. Enable **Wi-Fi**.
2. Connect to the wireless AP provided by the VCS endpoint.
3. Enter the password and tap **OK**.
   After the wireless AP is connected, you can use CTP20 to work with the VCS endpoint.

Related tasks

Enabling the Wireless Access Point
Configuring Wireless Access Point

Using Multiple CTP20s for Collaboration

In a meeting room, you can use multiple CTP20s for whiteboard collaboration or presentation. Up to 4 CTP20s can be connected to MeetingEye 600/MeetingEye 400/PVT980/PVT950/VC880/VC800/VC500 simultaneously, and only 1 CTP20 can be connected to VC200.

The collaboration methods are as below:

- **Status Synchronizing**: The status of the VCS endpoint can be synchronized to all connected CTP20s.
- **Configuration Synchronizing**: in idle state, you can configure the VCS endpoint via each CTP20, and the new configuration will cover the old configuration and take effect immediately.
- **Whiteboard Collaboration**: you can use each CTP20 to initiate the whiteboard collaboration which can be received by other CTP20s simultaneously, but the editing and noting on each CTP20 are independent. If you close the whiteboard of one CTP20 connected to a VCS endpoint, the whiteboards of other connected CTP20s are closed simultaneously.
- **Presentation Collaboration**: if you enable the feature of auto-presentation on the VCS endpoint, after you start presenting on the local computer/Apple devices, the presentation will be synchronized to all CTP20s, but the editing and noting on each CTP20 are independent. If you do not enable the feature of auto-presentation, you can initiate the presentation on any CTP20 and the presentation will be synchronized to all the CTP20s, but the editing and noting on each CTP20 are independent. If you close the presentation on one CTP20 connected to a VCS codec, the presentation on other connected CTP20s are closed simultaneously.

Note: If multiple CTP20s are wired to a VCS endpoint, you need a multi-port switch.

Using VCM34

To further improve the sound quality, you can connect a VCM34 to the VCS endpoint. If you need to expand the pickup range, you can connect multiple VCM34s in cascade (up to 4 VCM34s). VP59 cannot be used with a VCM34. For more information, refer to Yealink VCM34 Quick Start Guide.

Using VCM38

After connecting VCM38 to VC800/PVT980/PVT950, you can use it directly. If you want to expand the pickup range, you can use a switch for connecting up to 8 VCM38s. For more information the connection between the VCS endpoint and VCM38, refer Yealink VCM38 Quick Start Guide (EN,CN).

Using the Soundbar/MSpeaker II

The Soundbar/MSpeaker II can be used as the audio output device. It can be used directly after connected to the system. VP59 cannot be used with a Soundbar/MSpeaker II. For more information about how to use the Soundbar, refer to Yealink Soundbar Quick Start Guide/Yealink MSpeaker II Quick Start Guide.

Using CP900/CP700 Ultra-Compact Speakerphone

After you connect CP900/CP700 to VP59 via a USB cable, VP59 will automatically take CP900/CP700 as the audio input or output device and charge CP900/CP700. You can use CP900/CP700 to control the call on VP59, adjust the volume, and set the mute status. For more information about connecting and using CO900/CP700, refer to Yealink CP900 Quick Start Guide or Yealink CP700 Quick Start Guide.

System Maintenance

The following topics describe system maintenance, such as how to set up a system profile, perform a factory restore, and upgrade the system firmware.

- Exporting or Importing Configuration Files
- Rebooting the System
- Resetting the SD card of MeetingEye 600/MeetingEye 400/VC200/VP59
- Resetting the System
- Exporting Log Files
- Capturing Packets
- System Firmware
- Viewing Multipoint License Status
- Viewing the Device Type

Exporting or Importing Configuration Files

You can export the configuration files to check the current configuration of the system and to troubleshoot if necessary. You can also import configuration files for a quick and easy configuration. The format of the imported configuration file must be "*.bin".

- Exporting BIN Files from the System
- Importing BIN Files to the System

Exporting BIN Files from the System

Procedure

1. On your web user interface, go to **Setting** > **Configurations** > **Configuration** > **Export Configuration**.

2. Click **Export**.

Importing BIN Files to the System

Procedure

1. On your web user interface, go to **Setting** > **Configuration** > **Configuration** > **Import Configuration**.
2. Click Browse and select a BIN configuration file from your computer.
3. Click **Import**.

Rebooting the System

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Upgrade** > **Reboot**.
   - On your VCS,

     For MeetingEye 600/MeetingEye 400, go to **More** > **Settings** > **Advanced** > **System Settings** > **Reboot & Reset** > **Reboot**.

     For VP59, tap > **Settings** > **Advanced** > **System Settings** > **Reboot & Reset** > **Reboot**.
   - On your CTP20, tap > **Settings** > **Advanced** > **System Settings** > **Reboot & Reset** > **Reboot**.

   It prompts whether you are sure reboot.
2. Confirm the action.

Resetting the SD card of MeetingEye 600/MeetingEye 400/VC200/VP59

You can reset SD card (local storage) of MeetingEye 600/MeetingEye 400/VC200/VP59 to clear all captured screenshots or recorded videos.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Upgrade** > **Reset Built-in SD Card**.
   - On your VCS,

     For MeetingEye 600/MeetingEye 400, go to **More** > **Setting** > **Advanced** > **System Settings** > **Reboot & Reset** > **Reset Built-in Setting Card**.

     For VP59, tap > **Settings** > **Advanced** > **System Settings** > **Reboot & Reset** > **Reset Built-in Setting Card**.

   The page prompt whether or not you are sure to reset.
2. Confirm the action.

Resetting the System

Generally, some common issues may occur while using the system. You can reset your system and camera to factory configurations after you have tried all troubleshooting suggestions.

- Resetting the System via Configuration Methods
- Resetting the System by using Reset Button
- Resetting VP59 by REDIAL key

Resetting the System via Configuration Methods

Procedure

1. Do one of the following:
   - On your web user interface, go to **Setting** > **Upgrade** > **Reset to Factory Setting**.
   - On your VCS, go to **More** > **Settings** > **Advanced** > **Reboot & Reset** > **Reset**.

     For VP59, tap > **Settings** > **Advanced** > **System Settings** > **Reboot & Reset** > **Reset**.
   - On your CTP20, go to > **Settings** > **Advanced** > **System Settings** > **Reboot & Reset** > **Reset**.

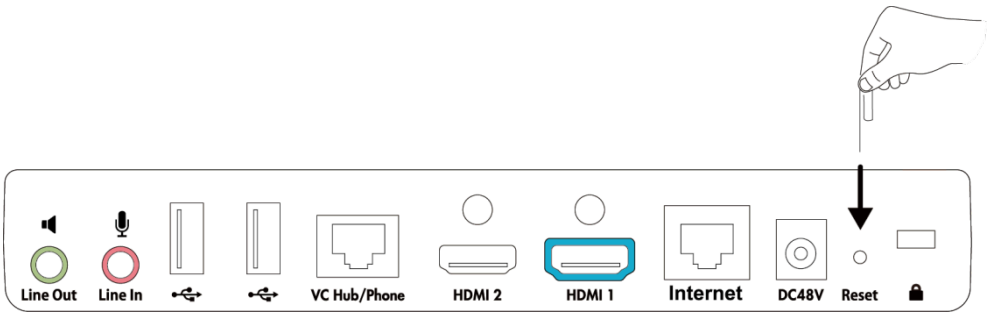
   It prompts whether or not you are sure to reset.
2. Confirm the action.

Resetting the System by using Reset Button

You can use the Reset button to reset the system. No Reset Key on VP59.

Procedure

On your video conferencing system or the VCC22 video conferencing camera, using tiny object (for example, the paper clip) to press and hold the reset button for 15 seconds until the monitor turns black.



Attention:

Do not power off the system during the system reset.

Resetting VP59 by REDIAL key

You can use the REDIAL key to reset VP59 to factory.

Procedure

1. On the Home page, long press the REDIAL key.

   It prompts whether or not you are sure to reset.
2. Confirm the action.

Exporting Log Files

Log files are essential when troubleshooting the phone issues. Log files contain information about phone activities and the phone configuration profile. You can also export the log to the local PC or to a specific syslog server.

- Setting the Severity Level of the Local log
- Setting Severity Level of the Module log
- Exporting the Log Files to a Local PC
- Exporting the Log Files to a USB Flash Drive
- Exporting the Log Files to a Syslog Server

Setting the Severity Level of the Local log

Procedure

1. On your web user interface, go to **Setting** > **Configuration** > **Local Log**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Local Log	Specify the local log level. **0**-system is unusable **1**-action must be taken immediately **2**-critical condition **3**-error conditions **4**-warning conditions **5**-normal but significant condition **6**-informational **Note**: the default value is 6. The smaller the number is, the higher the priority is. Higher value indicates more detailed content.	Web user interface
Max Log File Size	Limit the maximum size (kb) of local log files. **Default**: 20480.	Web user interface

Setting Severity Level of the Module log

You can configure severity level of each module of the system.

Procedure

1. On your web user interface, go to **Setting** > **Configuration** > **Module Log**.

2. Configure and save the following settings:

Parameter	Description	Configuration Method
Module Log Level	Specify the module log level. • All—all modules • Driver • System • Service • Connectivity • Video & Audio • Protocol • Deploy • Web • App • Talk The available levels are as below: • 0 • 1 • 2 • 3 • 4 • 5 • 6 **Default**: all, 6. If you set the log level for a specified module and then set the log level for all modules, the log level of a specified module will be overwritten by the log level of all modules.	Web user interface

Exporting the Log Files to a Local PC

Procedure

1. On your web user interface, go to **Setting** > **Configuration** > **Local Log**.
2. In the **Enable Local Log** field, select **On**.
3. Reproduce the issue.
4. Click **Export**.

Note:

The severity level of the exported Module Log will not be greater than the local Log Level. For example: If you set Local Log Level to 3 and set Talk log Level to 6, the exported Talk log Level will still be 3 in your exported local log. If you set Local Log Level to 5 and set Talk log Level to 4, the exported Talk log Level will be 4 in your exported local log.

Exporting the Log Files to a USB Flash Drive

Procedure

1. On your web user interface, go to **Setting** > **Configuration** > **Local Log**.
2. In the **Enable Local Log** field, select **On**.
3. In the **USB Auto Exporting Syslog** field, select **On**.
4. Click **Confirm**.

   A folder named yealink.debug appears in your USB flash drive, which includes the log files.

   Note:

   The severity level of the exported Module Log will not be greater than the local Log Level. For example: If you set Local Log Level to 3 and set Talk log Level to 6, the exported Talk log Level will still be 3 in your exported local log. If you set Local Log Level to 5 and set Talk log Level to 4, the exported Talk log Level will be 4 in your exported local log.

Exporting the Log Files to a Syslog Server

Procedure

1. On your web user interface, go to **Setting** > **Configuration** > **Syslog**.
2. Configure and save the following settings:

Parameter	Description	Configuration Method
Enable Syslog	Select **On** to enable the system to upload log messages to the syslog server. **Default**: On.	Web user interface
Syslog Server	Configure the IP address or the domain name of the syslog server.	Web user interface
Port	Configure the port of the syslog server.	Web user interface
Syslog Transport Type	Configure the transport protocol that the device uses when exporting log messages to the syslog server. • UDP • TCP • TLS **Default**: UDP.	Web user interface

Parameter	Description	Configuration Method
Syslog Level	Specify the level of syslog information that displayed in the syslog. **0**-system is unusable **1**-action must be taken immediately **2**-critical condition **3**-error conditions **4**-warning conditions **5**-normal but significant condition **6**-informational **Note**: the default value is 6. Higher value indicates more detailed content.	Web user interface
Syslog Facility	Configure the facility that generates the log messages. **Default**: Local Use 0.	Web user interface
Syslog Prepend Mac	Enable or disable syslog prepend Mac. **Default**: Disabled.	Web user interface

Note:

The severity level of the exported Module Log will not be greater than the Syslog Level. For example, if you set Syslog Level as 3 and set Talk log Level as 6, the exported Talk log Level will still be 3. If you set Local Log Level as 5 and set Talk log Level as 4, the exported Talk log Level will be 4.

Capturing Packets

You can capture packets in three ways: capturing the packets via web user interface, on the remote control or using the Ethernet software. You can analyze the packet captured for troubleshooting.

- Capturing the Packets via Web User Interface
- Capturing the Packets via Remote Control
- Capturing the Packets via Ethernet Software

Capturing the Packets via Web User Interface

You can capture the packets via the web user interface. You can also download the captured packets to your computer. The video conferencing system supports the following two modes for capturing packets:

- **Enhanced**: directly exporting the packets file to local PC while capturing.
- **Normal**: manually exporting the packets file to local PC after stopping capturing.

- Capturing the Packets in Enhanced Way

- Capturing the Packets in Normal Way

Capturing the Packets in Enhanced Way
You can capture more packets in enhanced way than normal mode.

Procedure

1. On your web user interface, go to **Setting** > **Configuration**.
2. Select **Enhanced** from the **Pcap Type** drop-down menu.
3. In the **Pcap Feature** field, click **Star**t to start capturing enhanced packets.
4. Reproduce the issue.
5. Click **Stop** to stop capturing.

Capturing the Packets in Normal Way

Procedure

1. On your web user interface, go to **Setting** > **Configuration**.
2. Select **Normal** from the **Pcap Type** drop-down menu.
3. Configure and save the following settings:

Parameter	Description	Configuration Method
Packet Capture Device	Configure the port where you want to capture packets: • **WAN**—capture packets of the wired network. • **Ext0**—capture packets of the CP960 conference phone • **Wlan0**—capture packets of the wireless network. **Default**: WAN.	Web user interface
Packet Capture Count	Configure the count of the number of packets to capture. **Default**: 5.	Web user interface
Packet Capture Clip KB	Configure the number of bytes (in kb) of the packet to capture. **Default**: 1024.	Web user interface

Parameter	Description	Configuration Method
Pcap Filter Type	Configure the filter type of the packet to capture. The supported types are as follows: • **Custom**—Customize the packet filter string. • **SIP or H245 or H225**—Capture SIP, H245 and H225 packets. • **RTP**—Capture RTP packets **Default**: Custom.	Web user interface
Packet Filter String	Customizes the packet filter string. For more information, refer to Packet Filter String. **Note:** the default value id blank. It works only when you set the Pcap Filter Type to Custom.	Web user interface

4. Click **Confirm**.
5. In the **Pcap Feature** field, click **Star**t to start capturing enhanced packets.
6. Reproduce the issue.
7. Click **Stop** to stop capturing.
8. Click **Export** to open the file download window, and then save the file to your local system.

- Packet Filter String

Packet Filter String

You can customize the packet filter string to capture the desired packets.

Syntax:

Protocol+Direction+Host(s)+ Value +Logical Operations+Other Expression

The following table introduces the syntax.

Syntax	Description
Protocol	Values: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp If no protocol is specified, all the protocols are used. Note that the application-level protocol, such as http, dns and sip are not supported.
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".

Syntax	Description
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 the highest priority. Alternation ("or") and concatenation ("and") have equal priority and associate from left to right. For example, "not tcp port 3128 and tcp port 23" is 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

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.

Capturing the Packets via Remote Control

You can capture packets via your remote control, and store the packets to the USB flash drive. This feature is not applicable to VP59.

Before you begin

If you want to save packets to the USB flash drive, make sure a USB flash drive is connected, and the USB feature is enabled.

Procedure

1. On the idle screen or during a call, long press ⌫ on VCR11 or the Mute Key on VCR20.

   The monitor prompts “Onekey-capture has been turned on, press the Backspace key for 2s to turn off it”.
2. Long press ⌫ on VCR11 or the Mute Key on VCR20 for 5 seconds to stop capturing packets.

   The packets are saved in the yealink.debug folder on your USB flash drive.

Related tasks

Configuring USB Storage

Capturing the Packets via Ethernet Software

Connect the Internet ports of your system and your computer to the same HUB, and then use Ethernet software to capture the signal traffic.

System Firmware

The newly released firmware version may add new features. Therefore, Yealink recommends you to update the latest firmware.

Attention:

Notes for upgrading firmware versions:

- For VC800, VC500, VCC22, and PVT950 using new hardware, their hardware versions are 63.0.98.0.2.1.17, 71.0.50.0.2.0.16, 82.0.1.0.2.0.17, and 1137.0.2.0.2.0.16 respectively. After upgrading their firmware to version X.44.0.25, you cannot degrade them to version X.43.0.30 or earlier versions. Please upgrade with caution.
- The firmware versions of all released devices need to match each other. If you want to upgrade the VCS endpoint running in version 40 or earlier versions (for example, X.32.0.40, X.32.10.40, or X.32.0.35) to X.44.0.25 or later versions, you need to upgrade it to any version between X.40.0.1 to X.43.0.30 first, and upgrade it to X.44.0.25 or later versions.
- After upgrading VP59 to version 44 (91.344.0.10), you cannot degrade it to versions earlier than 44. Please upgrade with caution.

The following table lists the latest firmware name for each system model.

Device model	System Firmware
MeetingEye 400 video conferencing system	120.43.0.25.rom
MeetingEye 600 video conferencing system	120.43.0.25.rom
VP59 video conferencing system	91.344.0.20.rom
VC200 video conferencing system	80.44.0.25.rom
VC880 video conferencing system	63.44.0.25.rom
VC800 video conferencing system	
VC500 video conferencing system	
VCC22 video conferencing camera	
PVT980 video conferencing system	1345.44.0.25.rom
PVT950 video conferencing system	
CP960 Conference Phone	73.344.0.20.rom
WPP20 wireless presentation pod	81.44.0.20.rom
CTP20 Touch Panel	85.44.0.25.rom
MSpeaker II	98.44.0.20.rom
CP900 Ultra-Compact Speakerphone	100.420.0.20.rom
CP700 Ultra-Compact Speakerphone	100.420.0.20.rom

You can download the latest firmware online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

- Upgrading the Firmware

Upgrading the Firmware

You can upgrade firmware for the system and accessories at the same time. Accessories that have not uploaded firmware will not be upgraded.

About this task

Note: Do not close and refresh the browser when the system is upgrading firmware via web user interface. Do not unplug the network cables and power cables when the system is upgrading firmware.

Procedure

1. On your web user interface, go to **Setting** > **Upgrade**.
2. Click the white box beside the desired firmware.
3. Upgrading the firmware.

   Note: If you connect multiple CTP20s to the VCS, all the firmware of CTP20s will be updated simultaneously.

Viewing Multipoint License Status

Procedure

1. Do one of the following:
   - On your web user interface, go to **Security** > **License**.
   - On your VCS, go to **More** > **Settings** > **System Status** > **License**.
   - On your CP960 conference phone, go to **Settings** > **License**.
   - On your CTP20, tap > **Settings** > **System Status** > **Host System** > **Device**.
2. The multipoint licenses status is described as below:

Parameter	Description	Configuration Method
Multipoint Status	Indicates whether or not a multipoint license has been imported to the system. • Active/STUN Active • Inactive (without a multipoint license or the imported multipoint license has expired)	Web user interface Endpoint CP960 Conference Phone CTP20
Multipoint Ways	Indicates that the multipoint license is imported to the system. • Unsupported • 8 points • 16 points • 24 points	Web user interface Endpoint CP960 Conference Phone CTP20

Parameter	Description	Configuration Method
Period of validity/Period	Indicates the validity period of the imported multipoint license. • Unsupported • X~Y Available • Eternal	Web user interface Endpoint CP960 Conference Phone CTP20

Note:

Upgrading the system or performing a factory reset will not affect the imported multipoint license.

If you import a trial multipoint license to the system and the license has not expired, and then you import a permanent multipoint license to the system, the trial multipoint license will be overwritten. On the contrary, the permanent multipoint license will not be overwritten by the trial multipoint license.

If you import a new permanent multipoint license to the system, the previous permanent multipoint license will be overwritten.

Viewing the Device Type

You can view the device type, including the demo machine and normal machine. For VP59, there is not different device type.

Procedure

Do one of the following:

- On your web user interface, go to **Security** > **License**.
- On your VCS, go to **More** > **Settings** > **System Status** > **License**.
- On your CP960 conference phone, go to **Settings** > **License**.
- On your CTP20, tap > **Settings** > **System Status** > **Host System** > **Device**.

Parameter	Description	Configuration Method
Device Type	Indicate the device type. • Demo machine • Normal Machine	Web user interface Endpoint CP960 Conference Phone CTP20

Troubleshooting

When your system is unable to operate properly, you need to troubleshoot issues.

Make sure that the system is not physically damaged when experiencing a problem, and the cables are loose and the connections are correct or not. All these are common issues.

- General Issues
- Call Issues
- Audio Issues

- Video Issues
- Placing a Test Call
- System Diagnostics
- System Status
- Viewing Call Statistics

General Issues

Symptom	Reason	Solution
Your system does not respond to the remote control.	The remote control battery is dead.	Replace batteries.
	The remote control battery is installed incorrectly.	Installed batteries correctly.
	Aim the remote control at the wrong direction.	Aim the remote control at the sensor when you perform a task.
	You may control the far-site camera during a call.	Ensure that you are controlling the near-site camera.
	There are some objects obstructing the sensor on the front of the camera.	Ensure that no objects are obstructing the sensor on the front of the camera.
	The remote control is broken.	Replace remote control.Remote control
You forget the administrator password for the system	You cannot access the advanced settings.	Reset your system.
Time and date are wrong	The system fails to obtain the time and date from the SNTP server automatically.	Contact the network administrator.
		Manually configure the time and date.
You cannot adjust the camera angle and the focus	The local image is not selected.	Select local image using your remote control before adjusting camera.
	The system is in the operation menu.	Adjust the camera when the system is idle or during a call.
	The remote control is not working.	Check the remote control.
How to prevent monitor 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 or the screen saver.
	Unsuitable monitor parameters.	You can decrease the monitor's sharpness, brightness, and contrast settings if they are set to their maximum values.

Call Issues

Symptom	Reason	Solution
You cannot receive calls.	The network is unavailable.	Contact the network administrator.
	Your system cannot receive calls when the far site dials your account.	Check whether your account is registered.
	DND (Do Not Disturb) mode is enabled.	Disable DND.
You fail to call far site.	The far site enables DND (Do Not Disturb) mode.	Contact the far site to disable DND.
	The account is not registered	Check whether the call parties register the accounts.
	Fail to dial the IP address of the far site.	At least one call protocol(SIP/H.323) is enabled.
		Ping the IP address of the far site. If it fails, contact the network administrator. Connect the network administrator.
	The far site system is powered off.	Contact the far site to power on the system.
	The call protocol(SIP/H.323) that far site uses is different from yours.	Both sites use the same call protocol (SIP/H.323).
	Encryption negotiation (SRTP/H.235) fails.	If one site uses encryption, ensure that the other site enables the encryption too.
	The firewall blocks the traffics.	Open necessary ports on the firewall.
	The password of the built-in MCU Virtual Meeting Room is enabled.	Disable the password of the built-in MCU Virtual Meeting Room.
	Your monitor prompts: Call Fail Busy Here. • Far site rejects your SIP call. • Far site does not answer your SIP call. • Far site has reached maximum sessions when you place a SIP call.	Contact the far site.

Symptom	Reason	Solution
	Your monitor prompts: Call Fail Remote endpoint refused call. Far site rejects your H.323 call • Far site rejects your H.323 call. • Far site does not answer your H.323 call. • Far site has reached maximum sessions when you place an H.323 call.	Contact the far site.
	Your monitor prompts: Network disconnected	Check the network connection.
	Your monitor prompts: Maximum number of sessions reached.	The maximum sessions is depend on the multipoint license imported to the system.

Audio Issues

Symptom	Reason	Solution
You cannot hear the audio during a call.	The volume is set to 0.	Adjust the volume.
	The far site mutes the microphone.	Contact the far site to check whether the microphone is unmuted.
You cannot hear the audio clearly during a call.	The speaker volume is too low.	Adjust the volume.
	The muffled audio reception from the far site may be caused by highly reverberant rooms.	Contact the far site to speak in close proximity to the phone.
	You choose a low-bandwidth audio codec.	Adjust the priority order of your audio codec.
	Noise devices, such as computers or fans.	Enable noise suppression.
	Dust and debris may cause the 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.
Far site cannot hear your audio during a call.	No audio input device.	Audio input device is connected correctly.
	The speaker of the far site is obscured or damaged.	Ensure that speaker is not obscured or damaged. Do not stack items on top of the CP960 conference phone.

Symptom	Reason	Solution
	Your microphone is muted	Unmute the microphone.
	The volume of the far site is set to 0.	Contact the far site to adjust the volume.
You may experience poor voice quality during a call, such as intermittent voice, echo or other noise.	The users sit too far from or near to the microphone.	Adjust the distance.
	The audio pickup device is moved frequently.	Put the audio pickup device in the fixed location.
	Network congestion.	Contact the network administrator.
	Cable gets old.	Replace the old cables with the new cables, and then check whether the new cables provide better connectivity.
You cannot hear the ring tone when receiving a call.	The volume is set to 0.	Adjust the volume.

Video Issues

Symptom	Reason	Solution
Picture is blank on the monitor.	The system is in sleep mode.	Press any key on the remote control to wake the system.
	The system is powered off.	The system is powered on.
	The HDMI cable is not connected to the system.	Make sure that the monitor is connected to the system and powered on.
The video quality is poor.	Unsuitable monitor resolution.	Adjust the monitor resolution.
	The packet is lost.	View the call statistics to check whether the packet is lost and contact the network administrator.
	Unsuitable camera parameters.	Adjust the camera parameters, such as the brightness and the white balance.
	High-intensity indoor light or direct sunlight on the camera.	Avoid those situations.
You cannot share content.	PC is not connected.	Connect a PC to your system.
	The PC is turned off.	Turn on the PC.
	The VCH50/VCH51 video conferencing hub or WPP20 wireless presentation pod is broken.	Replace it.

Symptom	Reason	Solution
	The WPP20 wireless presentation pod cannot connect to the video conferencing system.	• Connect the WPP20 to the video conferencing system to obtain Wi-Fi profile. • Make sure the wireless AP feature of video conferencing system is enabled.

The far site displays black screen when you share contents.	The reason may be that the remote device is placed in the private LAN and its negotiated media address in the signaling is different from its actual public IP address. If you share contents in this situation, the contents will be sent to the negotiated media address other than the actual public IP address. This may lead to failure.	You can configure network address adapter to let the content send to the actual public IP address.
		Procedure:
		• On your web user interface, go to **Setting** > **Call Features** > **Outbound Call Settings**.
		• Select the desired value from the drop-down menu of **Network Address Adapter**:
		  • **Disabled**- send contents to the negotiated media address.
		  • **IP Adapter**-send contents to the actual public IP address.
		  • **Port Adapter**- send contents to the actual public port.
		  • **IP & Port Adapter**- send contents to the actual public IP address and port.

Placing a Test Call

When you finish installing and deploying the video conferencing system, you can call the Yealink Demo site (117.28.251.50 or 117.28.234.45) to test your setup. If you fail to establish a call with Yealink Demo site, contact your network administrator to check whether or not the intranet works.

System Diagnostics

You can diagnose the audio, camera and network.

- Diagnosing the Audio
- Diagnosing the Camera
- Diagnosing the Network

Diagnosing the Audio

You can check whether the speaker connected to your system can pick up voice and play audio normally.

Procedure

1. Do one of the following:
   - On your VCS: go to **More** > **Settings** > **Diagnose** > **Audio Diagnose**.

     For VP59, tap > **Settings** > **Diagnose** > **Audio Diagnose** > **Start**.
   - On your CTP20, tap > **Settings** > **Diagnose** > **Audio Diagnose** > **Start**.
2. Speak to the microphone.
3. Check whether or not the microphone can pick up the sound properly.
4. If the microphone can pick up the sound properly and play it, the audio can work.
5. Stop diagnosing.

Diagnosing the Camera

You can check whether the camera can pan and change the focus normally. This feature is not applicable to VP59.

Procedure

1. Do one of the following:
   - On your VCS, go to **More** > **Settings** > **Diagnostics** > **Camera Diagnostics**.
   - On your CTP20, tap > **Settings** > **Diagnose** > **Camera Diagnose**.
2. Adjust the camera angle.
3. Select or or to zoom out or zoom in.
4. If the camera can move and zoom normally, it means that the camera is working well.
5. On your remote control, press to stop diagnosing.

Diagnosing the Network

The wrong network settings may result in inaccessibility of your system and poor network performance. You can use the ping or trace route to troubleshoot network connectivity problems.

- Checking the Network Using “Ping” Method
- Checking the Network Using “Trace Route” Method

Checking the Network Using “Ping” Method

The Ping method can help you check whether the system can be connected to the IP address of the remote device.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Diagnose**, and select **Ping** from the drop-down menu of **Command**.
   - On your VCS: go to **More** > **Settings** > **Diagnostics** > **Ping**.

     For VP59, tap > **Settings** > **Diagnostics** > **Ping**.
   - On your CTP20, tap > **Settings** > **Diagnose** > **Ping**.
2. Select **Start**.
3. Optional: You can also ping other IP addresses.
4. Select **Stop**.

Checking the Network Using “Trace Route” Method

You can use the trace route method to diagnose the network. If the test is successful, the system lists the hops between the system and the IP address you entered. You can check whether the congestion happens by viewing the time cost among the hops.

Procedure

1. Do one of the following:
   - On your web user interface, go to **Network** > **Diagnostics**, and select **Trace Route** from the drop-down menu of **Command**.
   - On your VCS: go to **More** > **Settings** > **Diagnostics** > **Trace Route**.

     For VP59, tap > **Settings** > **Diagnostics** > **Trace Route**.
   - On your CTP20, tap > **Settings** > **Diagnose** > **Trace Route**.
2. Select **Start**.
3. Optional: You can also track other IP addresses.
4. Select **Stop**.

System Status

You might need to provide system information, such as network settings and firmware for technical support.

- System Status List
- Viewing System Status

System Status List

The available status is listed below:

Parameter		Description	Method
System		• System Model • Firmware Version • Hardware Version • Product ID • The product ID (it is only applicable to MeetingEye400)	Web user interface Endpoint CP960 Conference Phone
		• Uptime	Web user interface
Collaboration Touch Panel (it is not applicable to VP59)		• System Model • Firmware Version • Hardware Version	Web user interface Endpoint CTP20 Touch Panel
VCP960 Status (it is not applicable to VP59)		• Status	Endpoint (Remote Control)
		• Firmware Version • Hardware Version • Serial number • IP • MAC	Web user interface Endpoint (Remote Control) CTP20
WPP20 Status (WPP20 is connected to the codec)		• Firmware Version	Web user interface
Mainframe Network	**Network**	• Network type • Internet Port/IP Mode	Web user interface Endpoint CTP20 Touch Panel
	IPv4	• Internet Port Type • IP • Subnet Mask • **Gateway** • DNS server	Web user interface Remote control CP960 Conference Phone CTP20 Touch Panel

Parameter		Description	Method
	Network Common	• NAT Public IP Address/Public IP Address • MAC • Wi-Fi Mac Address • Machine ID (it is only applicable to VP59) • WAN Port Status (it is only applicable to VP59) • PC Port Status (it is only applicable to VP59)	Web user interface Endpoint CTP20 Touch Panel
	AP Status (wireless AP is enabled)	• AP • AP Name • Security Mode • Password • Network Sharing • Band • Channel	Web user interface Endpoint CTP20
Account		• Cloud Platform • Cloud Account • SIP Protocol • SIP Account • H.323 Protocol • H. 323 Account	Web user interface Endpoint CP960 Conference Phone CTP20 (view cloud platform and account only)
Camera (it is not applicable to VP59)		• Status • Device model • SPEC • Camera Hardware	Web user interface Endpoint CP960 Conference Phone CTP20
Audio		• Active microphone • Active speaker • Media Audio Input	Web user interface (cannot view the media audio input) Endpoint CP960 Conference Phone (cannot view the media audio input)

Parameter	Description	Method
License	• Device Type • Multipoint Status • Multipoint Ways • Period of validity/ Period	Web user interface Endpoint CP960 Conference Phone CTP20
Storage (it is only applicable to VC200/VP59)	View the local storage	Web user interface

Viewing System Status

Procedure

1. Do one of the following:
   - On your web user interface, go to **Status**.
   - On your VCS, go to **More** > **Settings** > **System Status**.
   - On your CP960 conference phone, go to **Settings**.
   - On your CTP20, tap > **Settings** > **System Status**.
2. Select the desired list to view the status.

Viewing Call Statistics

About this task

If voice quality is poor during a call, you can view call statistics to find out the reason. The call statistics includes:

- **Bandwidth**: the received and the sent bandwidth.
- **Video**: the definition, the codec, the bandwidth, the frame rate, the jitter, the packet and its loss rate.
- The protocol used to placing calls.
- The device information.
- **Audio**: the codec, the bandwidth, the sample rate, the frame rate, the jitter, the packet and its loss rate.
- **Content**: the codec, the bandwidth, the definition and the frame rate.

Procedure

In a call

- For MeetingEye 600/MeetingEye 400/VC880/VC800/VC500/VC200/PVT980/PVT950, select **Home**.

  Position your mouse pointer over the desired far site, and click .
- On your VCS: , on your remote control, press the OK key to open **Talk Menu**, go to **More** > **Call Statistics**, and press the navigation keys to select the desired participant.

  For VP59, tap **More** > **Call Statistics**.
- On your CP960 conference phone, go to **More** > **Statistics**.

  Tap the desired participant to view the call statistics.

- On your CTP20, tap **Participants**.

  Tap ••• > **Call Statistics** beside the desired participant.