Yealink

Yealink VC800&VC500 Full HD Video Conferencing System Administrator Guide

Version 31.10
Jan.2018

Copyright

Trademarks

Warranty

(1) **Warranty**

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

(2) **Disclaimer**

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

(3) **Limitation of Liability**

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

End User License Agreement

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

Patent Information

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

Customer Feedback

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

Technical Support

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

About This Guide

Thank you for choosing the Yealink VC800/VC500 full HD video conferencing system. It is an all-in-one unit that supports 1080P-full HD video conferencing and includes outstanding features such as good compatibility, easy deployment and intelligent network adaptability. VC800 is the best choice for middle-to-large enterprise, and VC500 is the best choice for SME.

The Yealink VC800/VC500 full HD video conferencing systems help enterprises organize video conferences easily and efficiently. Users can expect to enjoy the high-quality video conferencing experience very cost-effectively.

This guide is intended for administrators who need to configure, customize, manage, and troubleshoot the video conferencing system properly, rather than for end-users. It provides details on the functionality and configuration of the Yealink VC800/VC500 video conferencing system.

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

In This Guide

This administrator guide includes the following chapters:

- Chapter 1, "VC800/VC500 Video Conferencing System Introduction" describes system features, icons and Indicator LEDs.
- Chapter 2, "Getting Started" describes how to start the system.
- Chapter 3, "Configuring Network" describes how to configure network features on the system.
- Chapter 4, "VCS Deployment Method" describes how to deploy your system.
- Chapter 5, "Configuring Call Preferences" describes how to configure call preferences on the system.
- Chapter 6, "Configuring System Settings" describes how to configure basic, audio and video features on the system.
- Chapter 7, "System Management" describes how to manage system contacts and call history.
- Chapter 8, "Configuring Security Features" describes how to configure security features on the system.
- Chapter 9, "System Maintenance" describes how to upgrade system firmware and reset the system.
- Chapter 9, "Troubleshooting" describes how to troubleshoot the system and provides

some common troubleshooting solutions.

Documentations

This guide covers the VC800/VC500 video conferencing system. In addition to the administrator guide, the following related documents are available:

- Quick Start Guide, which describes how to assemble the system and configure basic network features on the system.
- User Guide, which describes how to configure and use basic features available on the systems.
- Video Conference Room Deployment Solution, which describes the conference room layout requirements and how to deploy the systems.
- Network Deployment Solution, which describes how to deploy network for your systems.
- Yealink VCR11 Remote Control Quick Reference Guide, which describes how to use the VCR11 Remote Control.
- Yealink CPW90 Quick Start Guide, which describes how to connect CPW90 wireless expansion microphones to CP960 conference phone
- Yealink CPW90 Wireless Microphones Quick Start Guide, which describes how to connect CPW90 wireless microphones to VC500 video conference phone.
- Yealink CP960 HD IP Conference Phone Quick Reference Guide, which describes how to use CP960 conference phone.
- Yealink VCC22 Video Conferencing Camera Quick Start Guide, which describes how to connect the VCC22 video conferencing cameras.

You can download the above 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://www.yealink.com/Support.aspx*.

Typographic Conventions

Yealink documentations contain a few typographic conventions.

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

Convention	Description
Bold	Highlights the web/phone user interface items such as menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (for example: Click on **Setting** ->**General**). Also used to emphasize text

Convention	Description
Blue Text	Used for cross references to other sections within this documentation (for example: refer to Troubleshooting).
Blue Text in Italics	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (for example: *Yealink VC800&VC500 Full HD Video Conferencing System User Guide.*

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

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

Firmware

Common reasons for updating firmware include fixing bugs or adding features to the device. You can download the latest firmware for your product online: *http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage*. For more information on how to upgrade the system firmware, refer to Upgrading Firmware on page 237.

Summary of Changes

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

Changes for Release 31, Guide Version 31.5

The following section is new for this version:

- VCS Deployment Method on page 43
- Video Call Rate on page 130
- Frame Rate and Resolution on page 135
- Screen Saver Waiting Time on page 149
- EQ Self Adaption on page 163
- Using VCC22 Video Conferencing Cameras on page 174
- Consumer Electronics Control (CEC) on page 187

Major updates have occurred to the following sections:

- Codecs on page 101
- VMR Mode Conference on page 109
- Restricting Reserved Ports on page 40
- Frame Rate and Resolution on page 135
- Audio Output on page 161
- Audio Input on page 164
- Configuring Camera Settings on page 177
- Video Recording on page 189
- Multipoint License on page 209

Changes for Release 30, Guide Version 30.8

Documentations of the newly released VC500 video conferencing endpoints have been added.

Major updates have occurred to the following sections:

- Intelligent Traversal on page 53
- Conference Management on page 108
- Defending against Attacks on page 231

Changes for Release 30, Guide Version 30.6

Major updates have occurred to the following sections:

- Restricting Reserved Ports on page 40
- Conference Type on page 108
- Device Type License on page 208

- Multipoint License on page 209
- Appendix B: Trusted Certificates on page 264

Table of Contents

VC800/VC500 Video Conferencing System Introduction

This chapter contains the following information about VC800/VC500 video conferencing system:

VoIP Principles

VoIP

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

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

H.323

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

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

SIP

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

to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

Physical Features of System

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

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

- A working IP network is established.
- The latest (or compatible) firmware of system is available.
- VoIP gateway is configured for SIP, or H.323 gatekeeper is configured for H.323, or Cloud server is configured for Cloud platform.

VC800 Codec

- 2 x HDMI output
- 1 x Line-in (3.5mm)
- 1 x Line-out (3.5mm)
- 1 x Yealink extension port (RJ-45) connect to VCH50/CP960 Phone
- 1 x 10/100/1000M Ethernet port
- 2 x USB 2.0
- 1 x Power port
- 1 x Security lock slot
- 1 x Reset slot

Full-HD PTZ VC800 Camera

- 1920 x 1080 video resolution
- 60 frame rate
- 12x optical zoom PTZ camera
- Horizontal field of view: 70°
- Vertical field of view: 42°
- Pan angel range: +/- 100°
- Tilt angel range: +/- 30°
- Beauty shot

VC500 Codec

- 2 x HDMI output
- 1 x Yealink extension port (RJ-45) connect to VCH50/CP960 Phone
- 1 x 10/100/1000M Ethernet port
- 2 x USB 2.0
- 1 x Power port
- 1 x Security lock slot
- 1 x Reset slot

Full-HD PTZ VC500 Camera

- 1920 x 1080 video resolution
- VC500 Pro: 60 frame rate, VC500: 30 frame rate
- 5x optical zoom PTZ camera

- Horizontal field of view: 83°
- Vertical field of view: 52°
- Pan angel range: +/- 30°
- Tilt angel range: +/- 20°
- Beauty shot

VCH50 Connections

- 1 x RJ45 port connects to VC800/VC500 codec
- 1 x RJ45 port connects to CP960
- 1 x HDMI input for content sharing (with audio)
- 1 x Mini-DP input for content sharing (with audio)
- 1x USB 2.0 for recording

Comparing VC500 Models

The difference 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	×	√

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

User Interfaces

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

- Web User Interface
- Remote Control

The following describes how to configure the VC800/VC500 video conferencing system via the two methods above.

Detailed operation steps will be introduced in the feature section.

Web User Interface

You can customize your system via web user interface. To access the web user interface, you

need to know the user name and the administrator's password. The default user name is "admin" (case-sensitive), and the default password is "0000". You can also access the web user interface with user credential, which is disabled by default. For more information on how to enable the user credential, refer to User Mode on page 213.

The system uses the HTTPS protocol to access the web user interface by default. For more information on the access protocol for web user interface access, refer to Web Server Type on page 215.

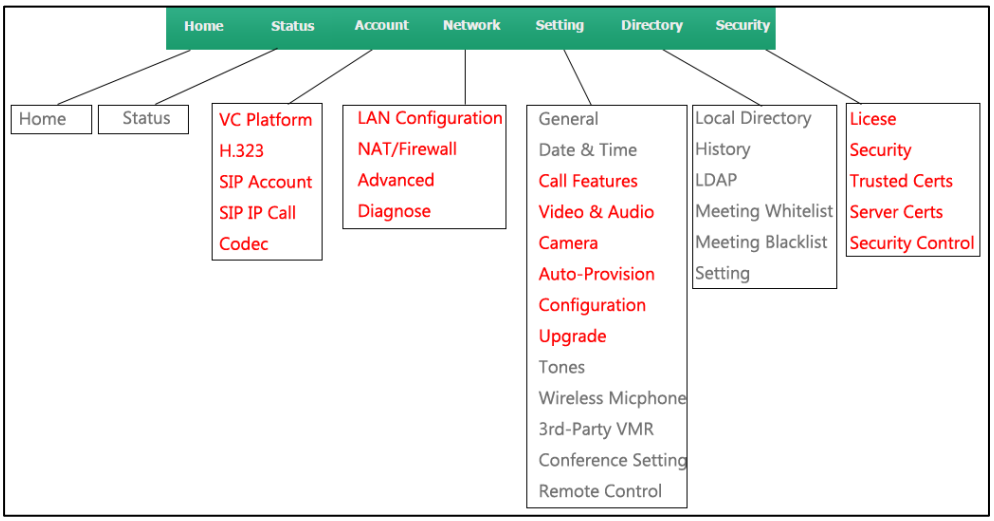
Log into the web user interface of the system:

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

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

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

The web structure tree of VC800/VC500 is shown as below, (the red highlight is hidden for users with user credentials):



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

- Placing or ending calls
- Viewing remote and nearby sites
- Enabling the mute mode or the DND mode for a call
- Changing the video input source
- Adjusting the position and focus of the camera
- Moving local camera to a preset position

- Capturing the video images
- Control the video conferencing system remotely via the virtual remote control

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

Remote Control

You can use the remote control to configure and use the VC800/VC500 video conferencing system.

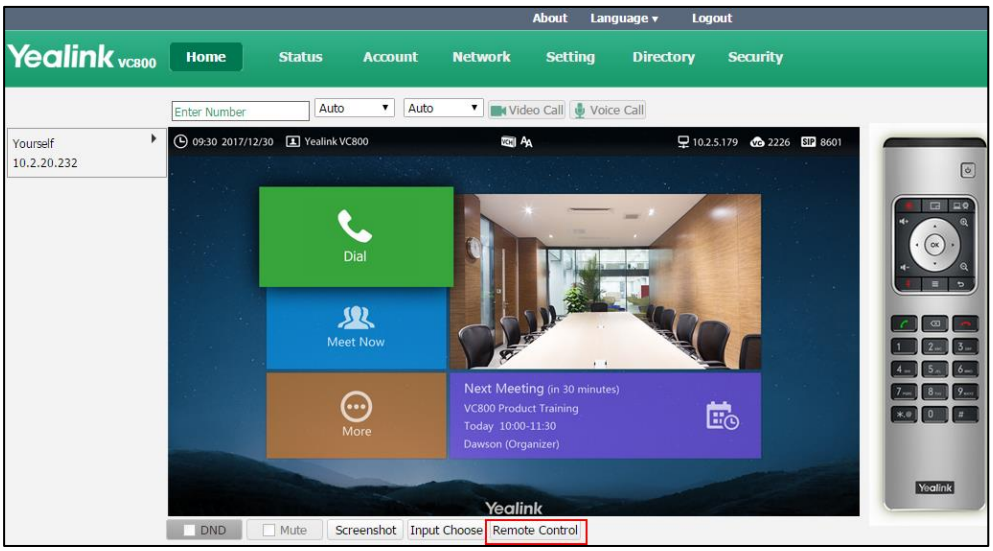
The **Advanced** option is only accessible to the user with the administrator's permission. The default administrator password is "0000".

Virtual Remote Control

In addition to using the remote control, you can also control the VC800/VC500 video conferencing system via virtual remote control.

To control VC800/VC500 video conferencing system via the virtual remote control:

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



2. Click the keys on the virtual remote control to control the VC800/VC500 video conferencing system.
3. Click **Remote Control** to hide the virtual remote control.

Configuring Remote Control

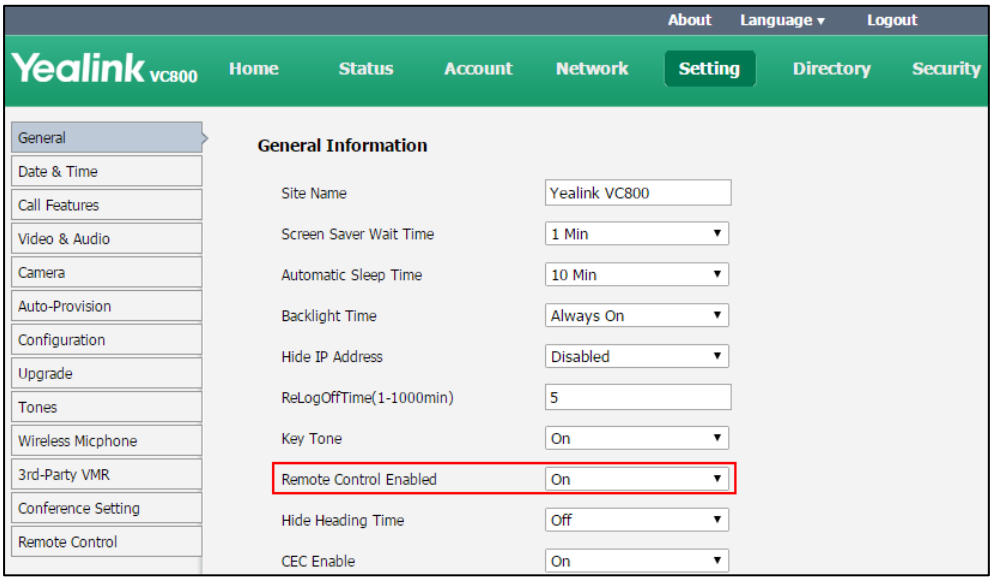
If your environment does not use remote control, you can choose to disable remote control feature.

The remote control parameter is described below:

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

To configure remote control via web user interface:

1. Click on **Setting**->**General**.
2. Select desired value from the pull-down list of **Remote Control Enabled**.



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

Getting Started

This chapter provides basic information and installation instructions for Yealink VC800/VC500 systems in the following sections:

System Initialization

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

During the initialization process, the following events take place:

Loading the ROM file

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

Configuring the VLAN

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

Querying the DHCP (Dynamic Host Configuration Protocol) Server

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

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

You need to configure the network settings of the system manually if the DHCP server does not provide them. For more information on configuring network settings manually, refer to Configuring Network Settings Manually on page 18.

Setup Wizard

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

Menu	Description
Language	Set the language displayed on the display device. The default language is English. For more information, refer to Language on page 142.
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. For more information, refer to Date & Time on page 143.
Site Name	Edit the site name. For more information, refer to on Site Name on page 140.
Password	Change the administrator password. For more information, refer to Administrator Password on page 214.
Firewall Port forwarding	Displays firewall Port forwarding information.
Network	Configure network settings. The phone will try to contact a DHCP server in your network to obtain network parameters by default. If you uncheck the DHCP checkbox, you will need to configure IPv4 or IPv6 network manually. For more information, refer to Configuring LAN Properties on page 14.
Video Conferencing Platform	(Optional) Log into the Cloud platform. Yealink video conferencing system supports Yealink VC Cloud Management Service/Yealink Meeting Server/StarLeaf/Zoom /Pexip/BlueJeans/Mind/Custom platform. For more information, refer to Cloud Deployment Method on page 58.

Enabling Communication with Remote Systems

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

Static NAT	If you choose to place your video conferencing systems in a private LAN, and you do not use Cloud platform, you can use Network Address Translation (NAT) to communicate with outside systems. This may include enabling static NAT on your system. For more information, refer to Static NAT on page 44.
Firewall	If your system communicates with other devices through a firewall, you must configure your firewall to allow incoming and outgoing traffic to the system through reserve ports. Users placing calls through a firewall to systems with IP addresses may experience one-way audio or video if the firewall is not properly configured to allow video and audio traffic. For more information, refer to Configuring the System for Use with a Firewall on page 39.
Video Conferencing Platform	If you are using Cloud server in your environment and want to place calls using Cloud account, refer to Cloud Deployment Method on page 58.
H.323	If you are using H.323 gatekeepers in your environment and want to place

	calls using a name or extension with the H.323 protocol, refer to Configuring H.323 Settings on page 64.
SIP	If you are using Session Initiation Protocol (SIP) servers in your environment to place calls using the SIP protocol, refer to Configuring SIP Settings on page 59.

Placing a Test Call

Yealink Demo rooms appear as the default entries in the local directory for a new system and a system that is reset to default settings. Use this entry to place a test call from your VC800/VC500 system.

Configuring Network

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

This chapter provides the following sections:

Preparing the Network

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

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

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

Configuring LAN Properties

DHCP

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

DHCP Option

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

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

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

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

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

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

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

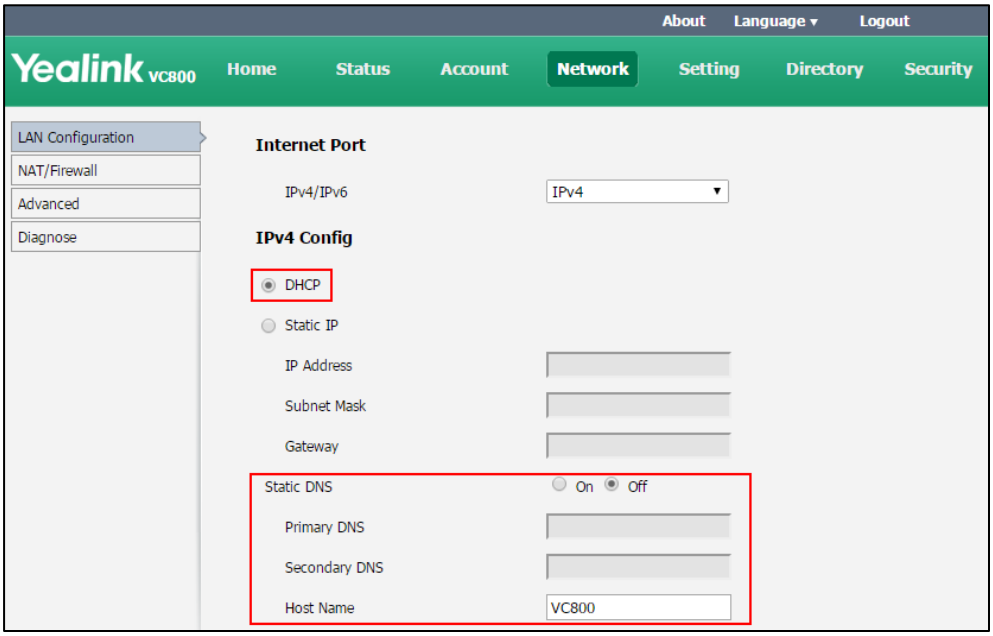
DHCP feature parameters on the system are described below:

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

To configure DHCP via web user interface:

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

3. (Optional.) Enter the host name of the system in the **Host Name** field.



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

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

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

To configure DHCP via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000)->**Internet Configuration**->**IPv4**.
2. Check the **DHCP** checkbox.
3. Select **Save** and then press OK to accept the change.

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

Static DNS

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

Parameters of static DNS on the system are described below:

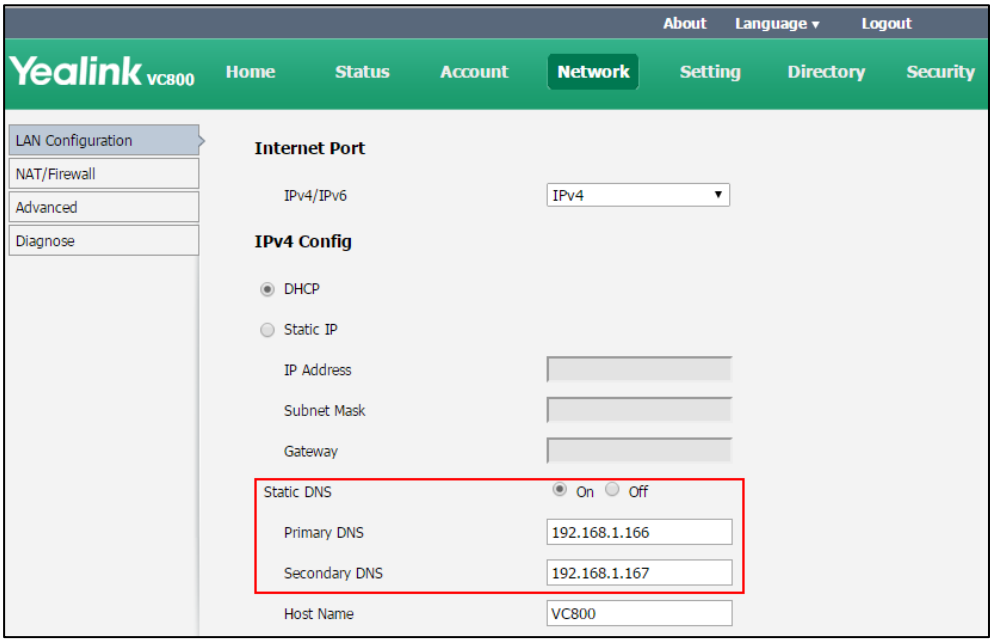
Parameter	Description	Configuration Method
Static DNS	Triggers the static DNS feature to on or off. **Default:** Off **Note**: If it is set to Off, the system will use the IPv4 DNS obtained from DHCP.	Remote Control Web User Interface

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

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

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

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



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

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

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

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

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

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

Configuring Network Settings Manually

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

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

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

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

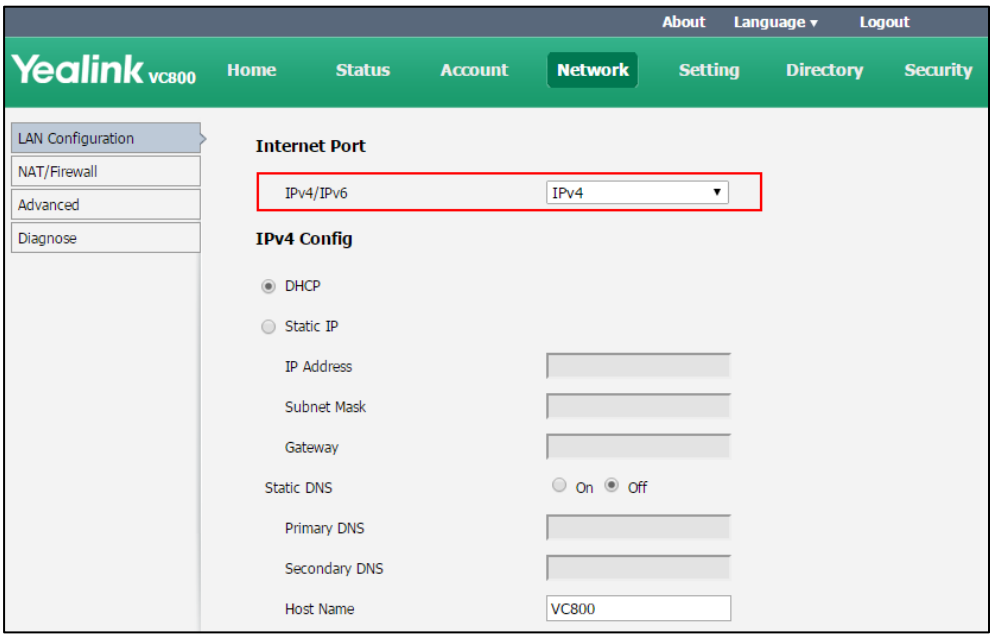
Network parameters need to be configured manually on the system are described below.

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

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

To configure the IP address mode via web user interface:

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



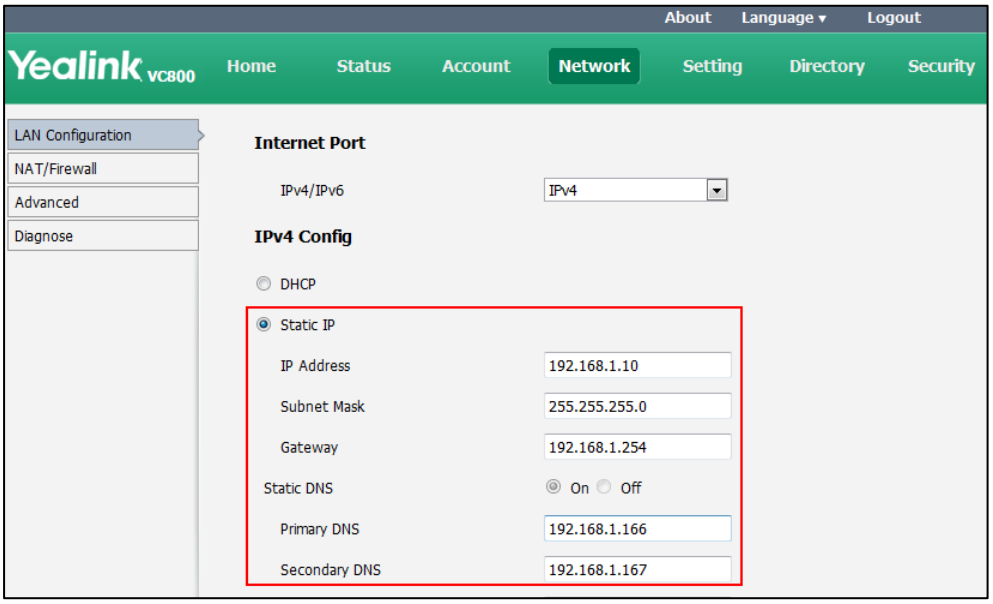
3. Click **Confirm** to accept the change.

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

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

To configure a static IPv4 address via web user interface:

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



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

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

To configure the IP address mode via phone user interface:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**Internet Configuration**.
2. Select **IPv4** or **IPv4 & IPv6** from the **IP Mode** field.
3. Select **Save**, and then press (OK) to accept the change.

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

To configure a static IPv4 address via phone user interface:

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

   The display device prompts "Reboot now?".
5. Select **OK**, and then press (OK) to reboot the system immediately.

IPv6 Support

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

Ensure that your network environment supports IPv6 and use one of the following methods to assign an IPv6 address.

- **Manual Assignment:** You can configure an IPv6 address and other configuration parameters (for example: DNS server) manually.
- **Stateful DHCPv6:** The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC 3315. DHCPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility.

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

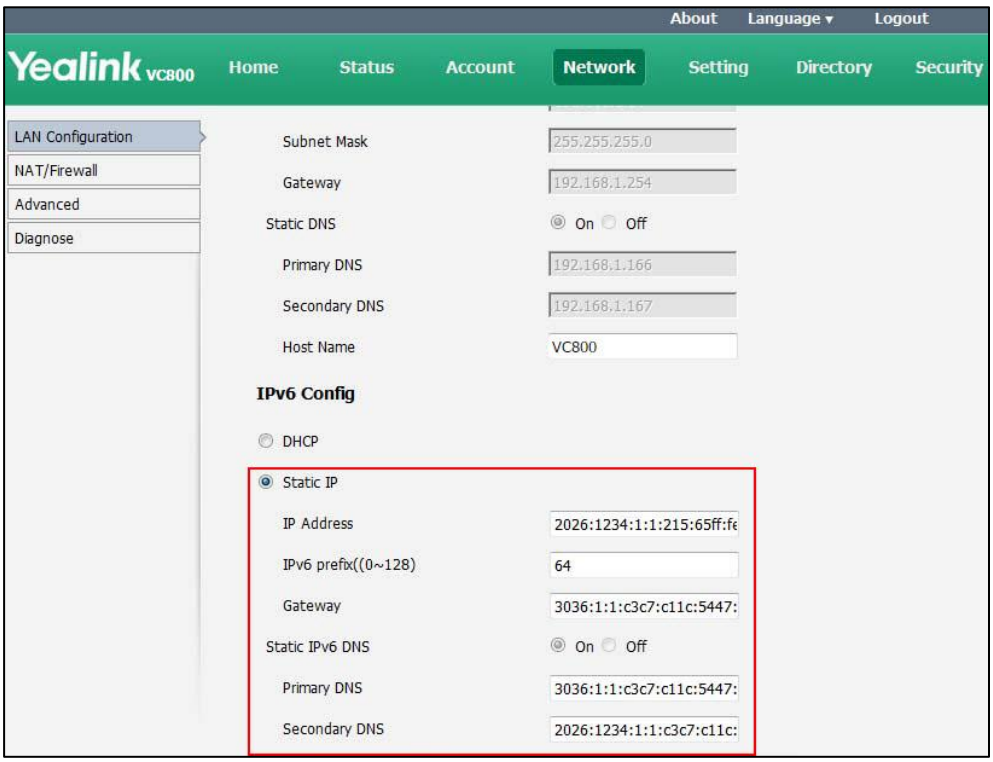
Parameter	Description	Configuration Method
IP Mode/Internet Port	Configures the IP address mode. **Default:** IPv4 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect.	Remote Control Web User Interface
Static IP	Enables or disables the system to use manually configured IPv6 network settings. **Default:** Disabled **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
IP Address	Configures the IPv6 address assigned to the system. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
IPv6 prefix((0~128)	Configures the IPv6 prefix. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the	Remote Control Web User Interface

Parameter	Description	Configuration Method
	change take effect.	
Gateway	Configures the IPv6 default gateway. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Static DNS/Static IPv6 DNS	Triggers the static IPv6 DNS feature to on or off. **Default:** Off **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
DNS Primary Server/Primary DNS	Configures the primary IPv6 DNS server. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
DNS Secondary Server/Secondary DNS	Configures the secondary IPv6 DNS server. **Default:** Blank **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

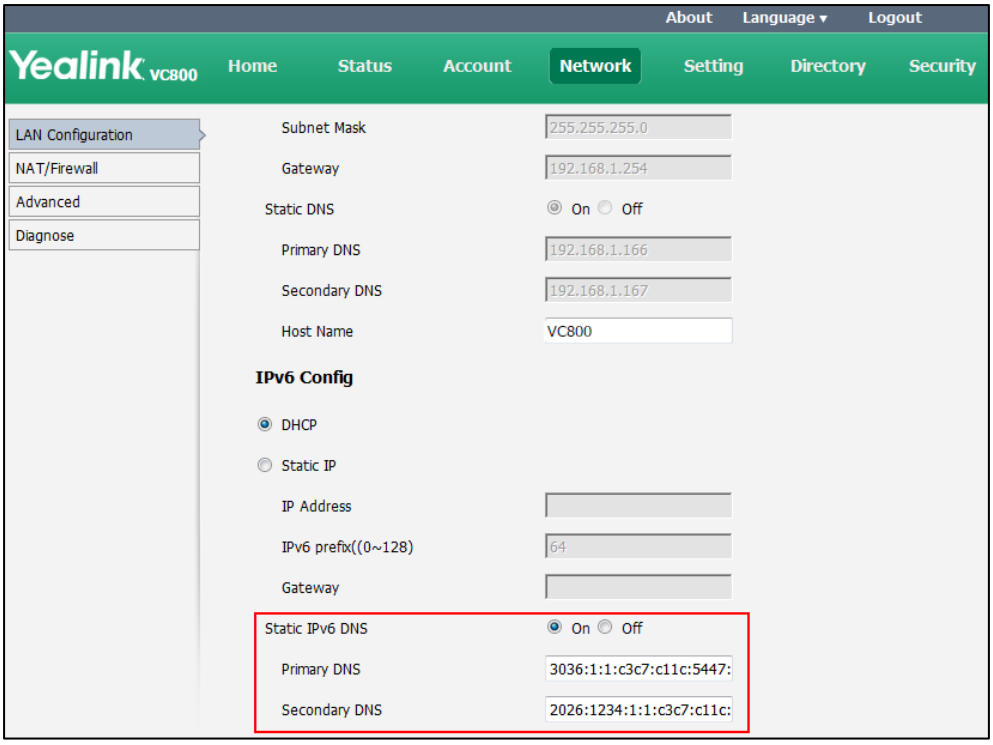
To configure IPv6 address assignment method via web user interface:

1. Click on **Network**->**LAN Configuration**.
2. Select the desired IP mode (**IPv6** or **IPv4 & IPv6**) from the pull-down list of **IPv4/IPv6**.
3. In the **IPv6 Config** block, mark the **DHCP** or the **Static IP** radio box.

- If you mark the **Static IP** radio box, configure the IPv6 address and other configuration parameters in the corresponding fields.



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



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

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

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

To configure IPv6 address assignment method via phone user interface:

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

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

7. Select **Save**, and then press OK to accept the change.

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

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

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**Internet Configuration**->**IPv6**.
2. Check the **DHCP** checkbox.
3. Check the **Static DNS** checkbox.
4. Enter the desired values in the **DNS Primary Server** and **DNS Secondary Server** fields respectively.
5. Select **Save**, and then press OK to accept the change.
6. The display device prompts "Reboot now?".
7. Select **OK**, and then press OK to reboot the system immediately.

Configuring Network Speed and Duplex Mode

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

- Auto
- 10 Mbps Full Duplex
- 100 Mbps Full Duplex
- 10 Mbps Half Duplex
- 100 Mbps Half Duplex
- 1000 Mbps Full Duplex

Auto is configured on the system by default.

Auto

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

Half-duplex

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

Full-duplex

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

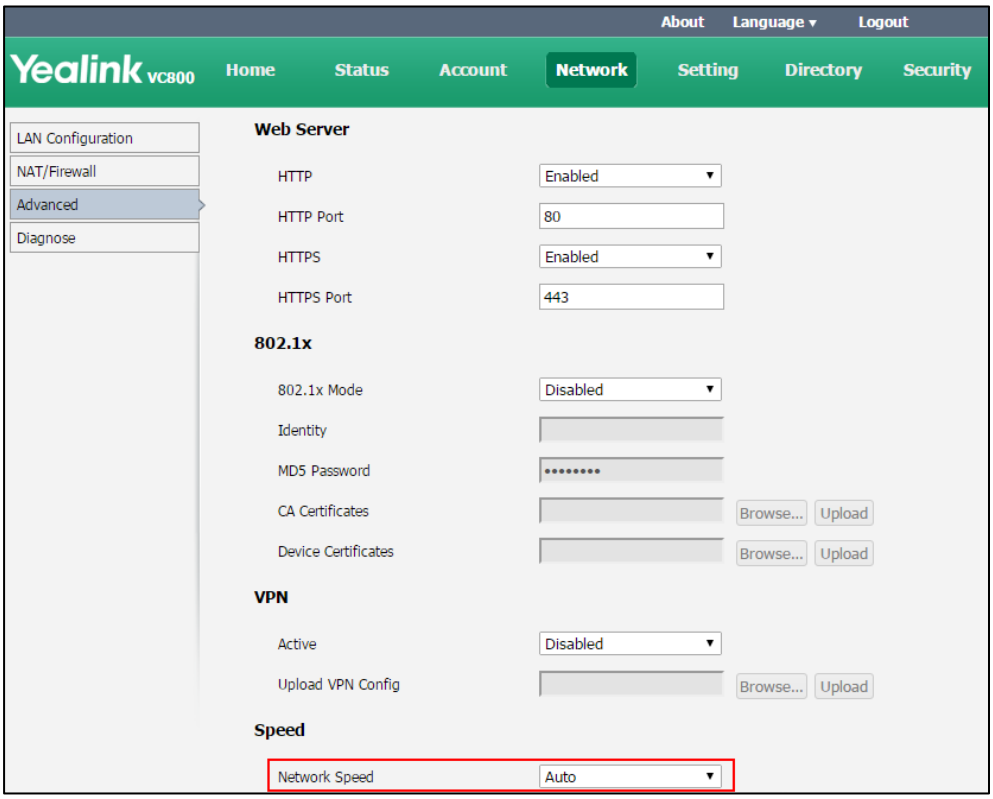
Parameter of network speed feature on the system is described below:

Parameter	Description	Configuration Method
Network Speed	Specifies the network speed and duplex mode for the system to use. **Default:** Auto **Note**: If **Auto** is selected, the network speed and duplex mode will be negotiated by the switch automatically. The network speed and duplex mode you select must be supported by the switch. If you change this parameter, the system will reboot to make the change take effect.	Web User Interface

To configure the network speed via web user interface:

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

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



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

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

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

VLAN

VLAN (Virtual Local Area Network) is used to divide a physical network logically into several broadcast domains. VLAN membership can be configured through software instead of physically relocating devices or connections. Grouping devices with a common set of requirements regardless of their physical location can greatly simplify network design. VLANs can address issues such as scalability, security, and network management.

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

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

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

LLDP

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

LLDP-MED (Media Endpoint Discovery)

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

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

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

TLV Type	TLV Name	Description
Mandatory TLVs	Chassis ID	The network address of the system.
	Port ID	The MAC address of the system.
	Time To Live	Seconds until data unit expires. The default value is 180s.
	End of LLDPDU	Marks end of LLDPDU.
Optional TLVs	System Name	Name assigned to the system. The default value is "VC800/VC500".
	System Description	Description of the system. Description includes firmware version of the system.
	System Capabilities	The supported and enabled system capabilities. The Telephone capability is supported and

TLV Type	TLV Name	Description
		enabled by default.
	Port Description	Description of port that sends data unit. The default value is "WAN PORT".
IEEE Std 802.3 Organizationally Specific TLV	MAC/PHY Configuration/Status	Duplex mode and network speed settings of the system. The Auto Negotiation is supported and enabled by default. The advertised capabilities of PMD. Auto-Negotiation is: 1000BASE-T(full duplex mode) 100BASE-TX (full duplex mode) 100BASE-TX (half duplex mode) 10BASE-T (full duplex mode) 10BASE-T (half duplex mode)
TIA Organizationally Specific TLVs	Media Capabilities	The MED device type of the system and the supported LLDP-MED TLV type can be encapsulated in LLDPDU. The supported LLDP-MED TLV types are: LLDP-MED Capabilities, Network Policy, Extended Power via MDI-PD, Inventory.
	Network Policy	Port VLAN ID, application type, L2 priority and DSCP value.
	Extended Power-via-MDI	Power type, source, priority and value.
	Inventory – Hardware Revision	Hardware revision of the system.
	Inventory – Firmware Revision	Firmware revision of the system.
	Inventory – Software Revision	Software revision of the system.
	Inventory – Serial Number	Serial number of the system.
	Inventory – Manufacturer Name	Manufacturer name of the system. The default value is "IP_Phone".
	Inventory – Model Name	Model name of the system. The default value is "VC800"/"VC500".

TLV Type	TLV Name	Description
	Asset ID	Assertion identifier of the system.

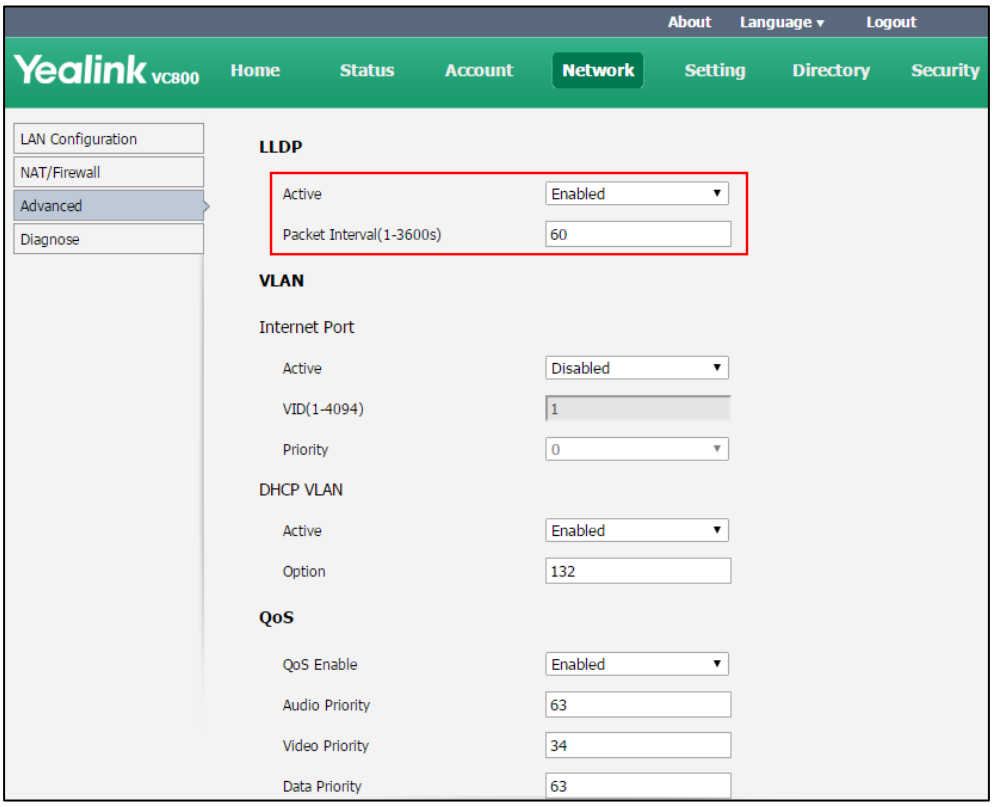
Parameters of LLDP feature on the system are described below.

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

To configure LLDP via web user interface:

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

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



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

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

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

To configure LLDP via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. In the **LLDP** block, check the **Active** checkbox.
3. Enter the desired value in the **Packet Interval (1-3600s)** field.
4. Select **Save**, and then press OK to accept the change.

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

Manual Configuration for VLAN

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

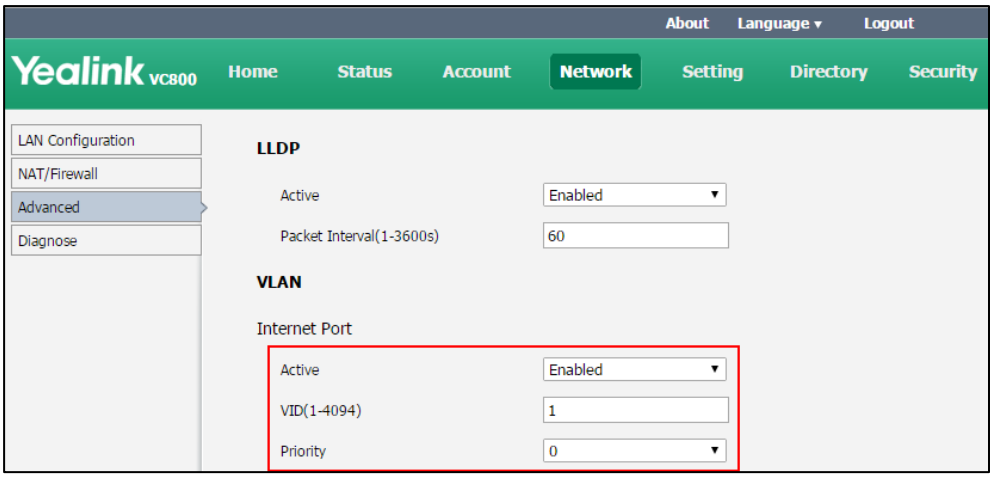
Parameters of manual VLAN on the system are described below.

Parameter	Description	Configuration Method
Internet Port->**Active**	Enables or disables VLAN for the Internet (WAN) port. **Default:** Disabled **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
VID(1-4094)	Specifies the identification of the Virtual LAN. **Default:** 1 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Priority	Configures VLAN priority for the Internet (WAN) port. **Valid values:** 0-7 7 is the highest priority, 0 is the lowest priority. **Default:** 0 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure VLAN for Internet port via web user interface:

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

4. Select the desired value (0-7) from the pull-down list of **Priority**.



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

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

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

To configure VLAN via the remote control:

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

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

DHCP VLAN

The system supports VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the system will examine the DHCP option for a valid VLAN ID. The predefined option 132 is used to supply the VLAN ID by default. You can customize the DHCP option used to request the VLAN ID.

Parameters of VLAN feature on the system are described below.

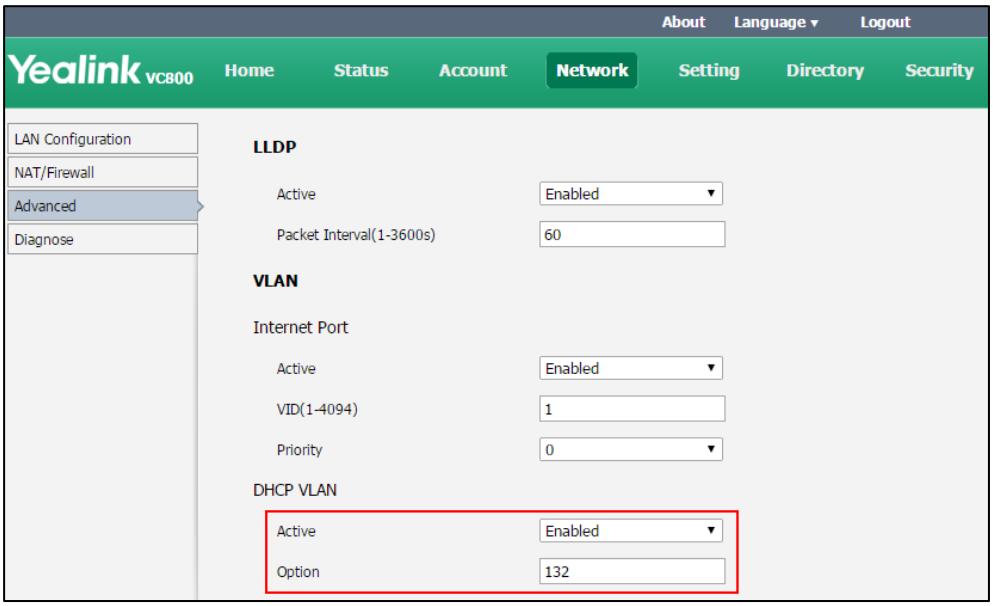
Parameter	Description	Configuration Method
DHCP VLAN->Active	Enables or disables the DHCP VLAN discovery feature on the system. **Default:** Enabled **Note**: If you change this parameter, the system will reboot to make the	Web User Interface

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

To configure DHCP VLAN discovery via web user interface:

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

   The default option is 132.



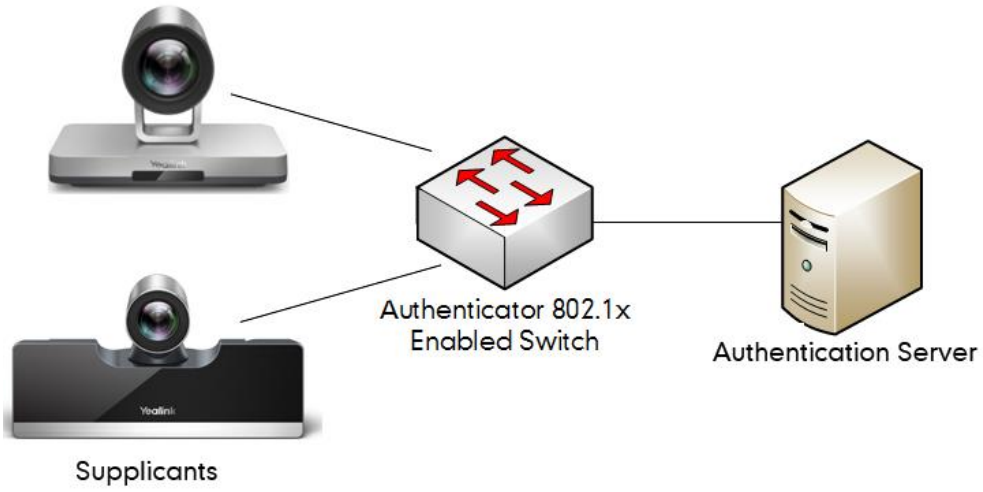
4. Click **Confirm** to accept the change.

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

802.1X Authentication

IEEE 802.1X authentication is an IEEE standard for Port-based Network Access Control (PNAC), part of the IEEE 802.1 group of networking protocols. It offers an authentication mechanism for devices to connect to a LAN or WLAN.

The 802.1X authentication involves three parties: a supplicant, an authenticator and an authentication server. The supplicant is the system that wishes to attach to the LAN or WLAN. With 802.1X port-based authentication, the system provides credentials, such as user name and default password, for the authenticator. The authenticator then forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the system is allowed to access resources located on the protected side of the network.



Yealink video conferences systems support the following protocols for 802.1X authentication:

- EAP-MD5
- EAP-TLS (requires Device and CA certificates, requires no password)
- EAP-PEAP/MSCHAPv2 (requires CA certificates)
- EAP-TTLS/EAP-MSCHAPv2 (requires CA certificates)

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

802.1X feature parameters on the system are described below:

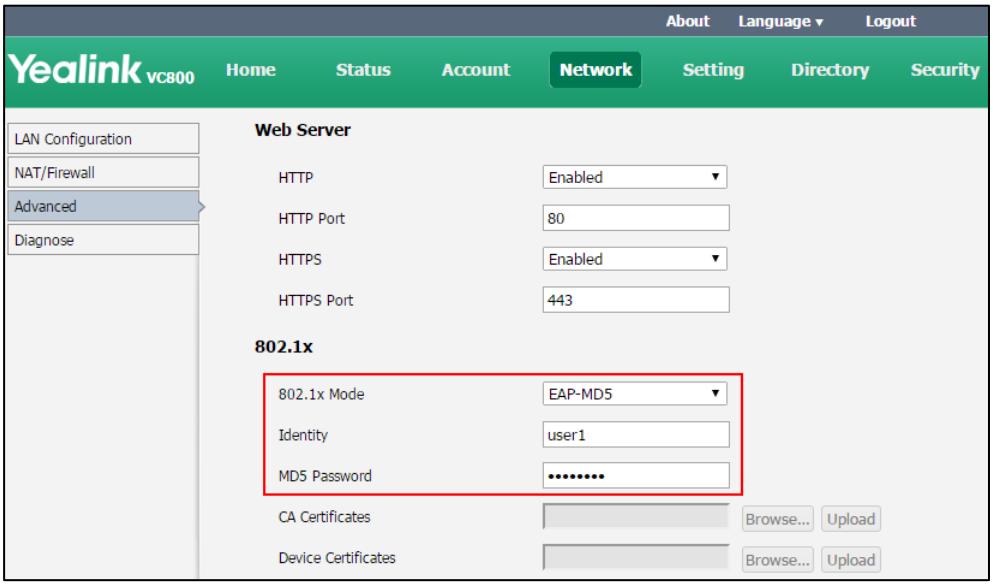
Parameter	Description	Configuration Method
802.1x Mode	Specifies the 802.1x authentication mode. • Disabled • EAP-MD5 • EAP-TLS • PEAP-MSCHAPv2	Remote Control Web User Interface

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

To configure 802.1X via web user interface:

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

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



b) If you select **EAP-TLS**:

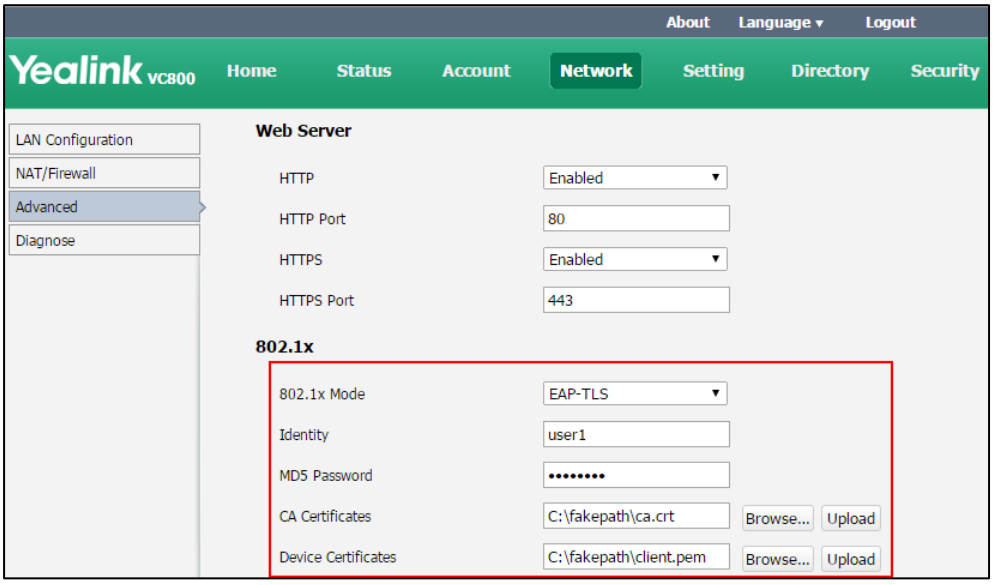
1) Enter the user name for authentication in the **Identity** field.

2) Leave the **MD5 Password** field blank.

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

4) In the **Device Certificates** field, click **Browse** to locate the desired client certificate (*.pem or *.cer) from your local system.

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



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

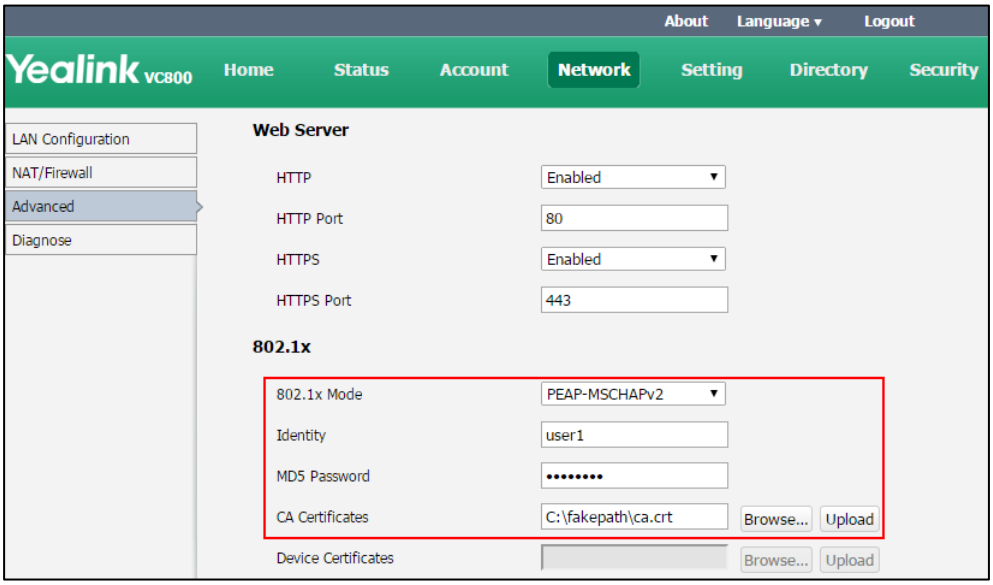
1) Enter the user name for authentication in the **Identity** field.

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

3) In the **CA Certificates** field, click **Browse** to locate the desired certificate

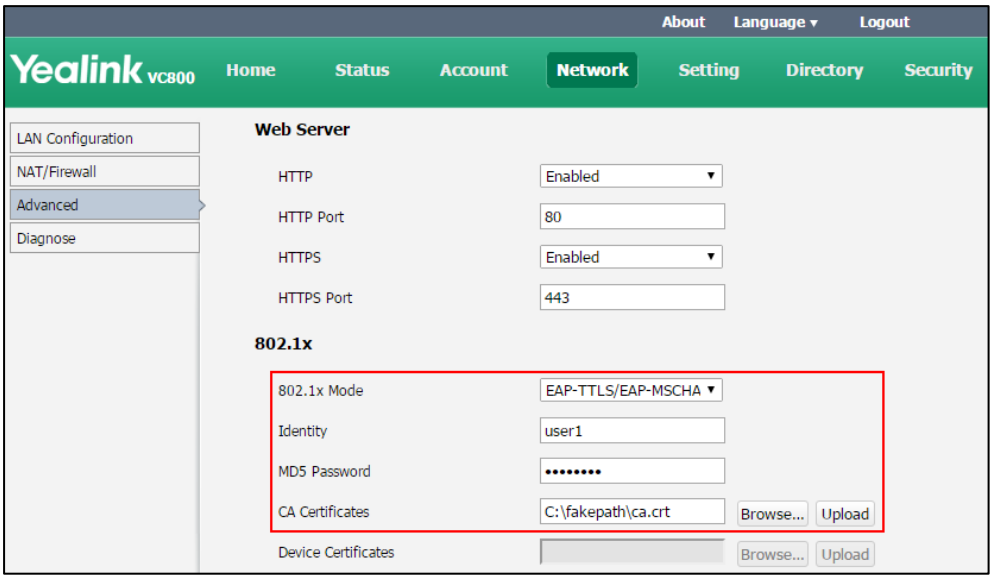
(*.pem,*.crt, *.cer or *.der) from your local system.

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



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

1) Enter the user name for authentication in the **Identity** field.
2) Enter the password for authentication in the **MD5 Password** field.
3) In the **CA Certificates** field, click **Browse** to locate the desired certificate (*.pem,*.crt, *.cer or *.der) from your local system.
4) Click **Upload** to upload the certificate.



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

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

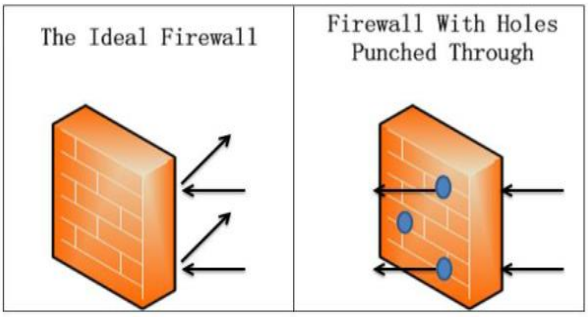
4. Click **Confirm** to reboot the system immediately.

To configure the 802.1X via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Select the desired mode from the pull-down list of **802.1x Mode**.
3. Select **Save**, and then press OK to accept the change.
   The display device prompts "Reboot now?".
4. Select **OK**, and then press OK to reboot the system immediately.

Configuring the System for Use with a Firewall

A firewall protects an organization's IP network by controlling data traffic from outside the network. Unless the firewall is designed to work with video conferencing equipment, you must configure the firewall to allow incoming and outgoing traffic to the VC800/VC500 system through the reserved ports. Users placing calls through a firewall to systems may experience one-way audio or video if the firewall is not properly configured.



Call Setup and Media Ports

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

Description	Port Range	Port Type
Gatekeeper	1719	UDP
H.323 call negotiation	1720	TCP
SIP call negotiation	5060	UDP
SIP call negotiation if TCP signaling is enabled for SIP calls.	5060	TCP
TLS signaling in SIP calls if TLS signaling is enabled.	5061	TLS
Reserved ports of the system. For more information, refer to Restricting	50000-50499 (default range)	TCP/UDP

Description	Port Range	Port Type
Reserved Ports on page 40.		
Web management port (optional)	443	TCP

Restricting Reserved Ports

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

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

The following tables identify the number of ports required per connection by protocol and the type of call. Make sure at least 200 TCP ports and 200 UDP ports are reserved for VC800/VC500 system.

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

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

Required ports for a SIP two-way call:

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

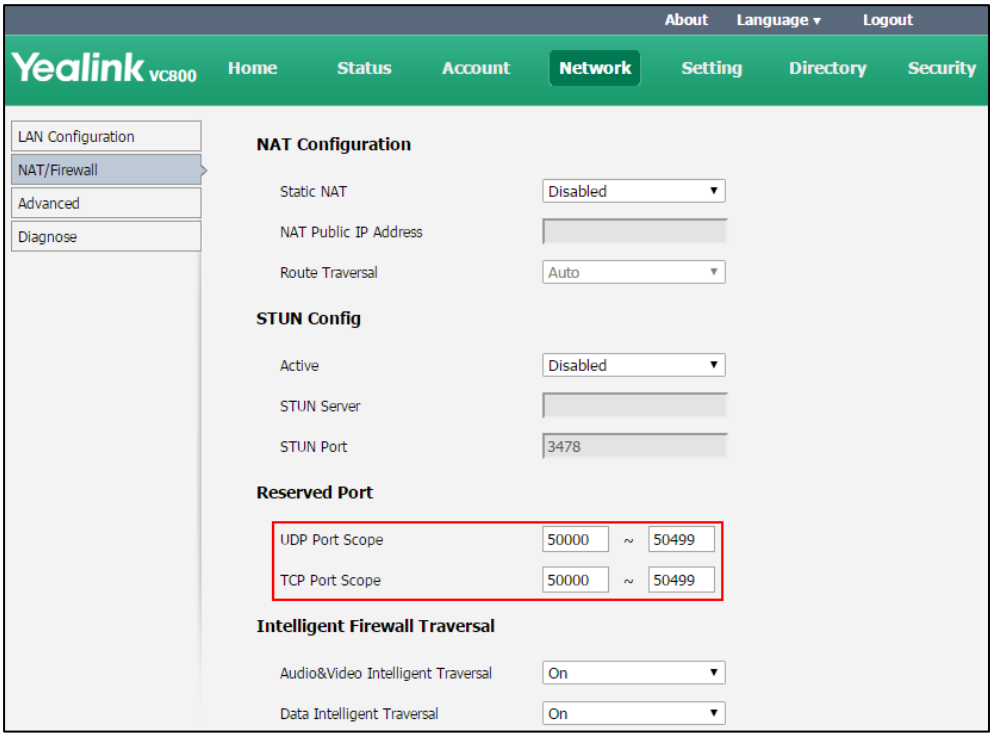
Parameters for reserved ports on the system are described below:

Parameter	Description	Configuration Method
UDP Port Scope	Configures the range of the UDP ports. **Valid values:** 1-65535 **Default range:** 50000-50499	Remote Control Web User Interface

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

To configure reserved ports via web user interface:

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



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

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

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

To configure reserved ports via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**NAT/Firewall**.
2. In the **Reserved** block, configure the range of the UDP ports and TCP ports.
3. Select **Save**, and then press OK to accept the change.
   The display device prompts "Reboot now?".
4. Select **OK**, and then press OK to reboot the system immediately.

VCS Deployment Method

This chapter provides information on how to deploy your system. This chapter provides the following sections:

Traditional Deployment Methods

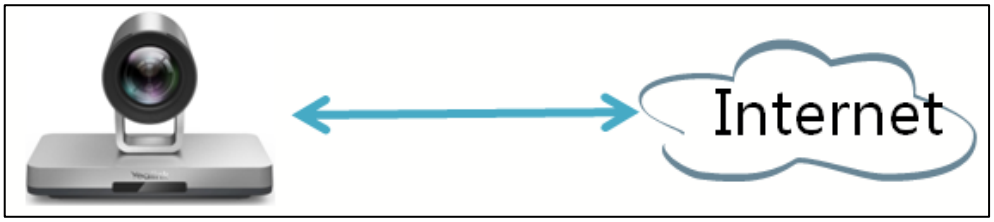
If you do not use cloud-based service, you can choose traditional deployment method to deploy your VCS, and dial IP addresses of other devices to make a call.

Use one of the following methods to deploy your VCS:

- Public IP Configuration (Outside of Firewall)
- Port forwarding with ALG feature
- Port forwarding with static NAT feature
- STUN
- H.460
- Intelligent traversal
- VPN

Public IP Configuration

Your video conferencing system is connected 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.

Port Forwarding

The most common deployment 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.

You must forward the following ports to the public network on the router or firewall.

Description	Port Range	Port Type
Gatekeeper	1719	UDP
H.323 Call setup	1720	TCP
Control and media for audio, video, content, and data/FECC	50000-50049	TCP/UDP
Web management port (optional)	443	TCP
SIP (optional)	5060-5061	TCP/UDP

Static NAT

Many application-layer protocols, such as multimedia protocols (H.323/SIP) have address or port information. The address and port information cannot be translated via the traditional NAT method, which lead to communication problems.

ALG (application layer gateway) feature on the router/firewall can help translate address and port of application-layer protocols. If your router does not support ALG (Application Level Gateway) feature, you should configure port forwarding on your router first, and then enable static NAT on your system to help H.323/SIP protocol traverse the firewall.

Note If H.460 firewall traversal is enabled on the system, the system will automatically ignore the static NAT settings for H.323 calls. For more information on H.460 firewall traversal, refer to on Enabling H.460 Support for H.323 Calls on page 52.

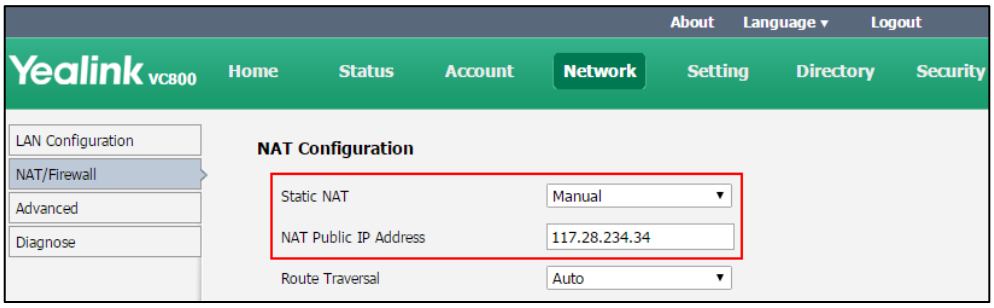
Static NAT feature parameters on the system are described below:

Parameter	Description	Configuration Method
Static NAT	Specifies the static NAT type. • **Disabled**–the system does not use the NAT feature. • **Manual**–the system uses the manually configured NAT	Remote Control Web User Interface

Parameter	Description	Configuration Method
	public address. • **Auto**—the system obtains the NAT public address from the Yealink-supplied server. **Default:** Disabled	
NAT Public IP Address	• Displays the NAT public address automatically obtained from the Yealink-supplied server if the static NAT is set to **Auto**. • Configures the NAT public address for the system if the static NAT is set to **Manual**.	Remote Control Web User Interface
NAT Traversal	Configures the NAT traversal type. You can configure it for the SIP account or SIP IP call separately. • **Disabled** • **STUN** • **StaticNat** **Default:** Disabled **Note:** Static NAT works only if this parameter is set to StaticNat.	Web User Interface

To configure static NAT via web user interface:

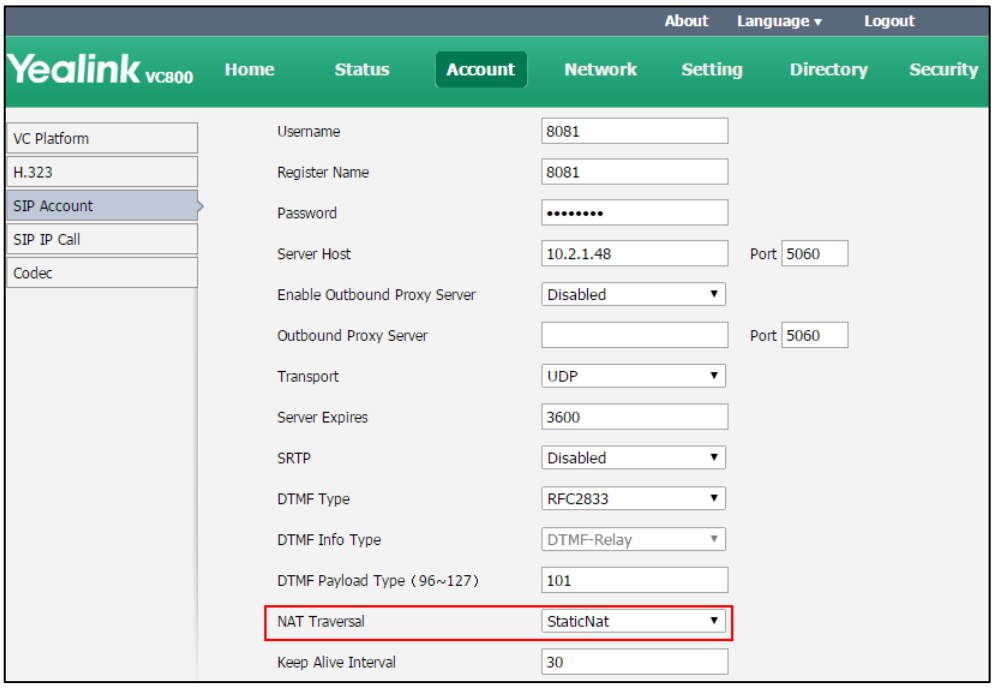
1. Click on **Network**->**NAT/Firewall**.
2. Select the desired value from the pull-down list of **Static NAT**.
3. Configure the NAT public address in the **NAT Public IP Address** field if **Manual** is selected from the pull-down list of **Static NAT**.



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

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

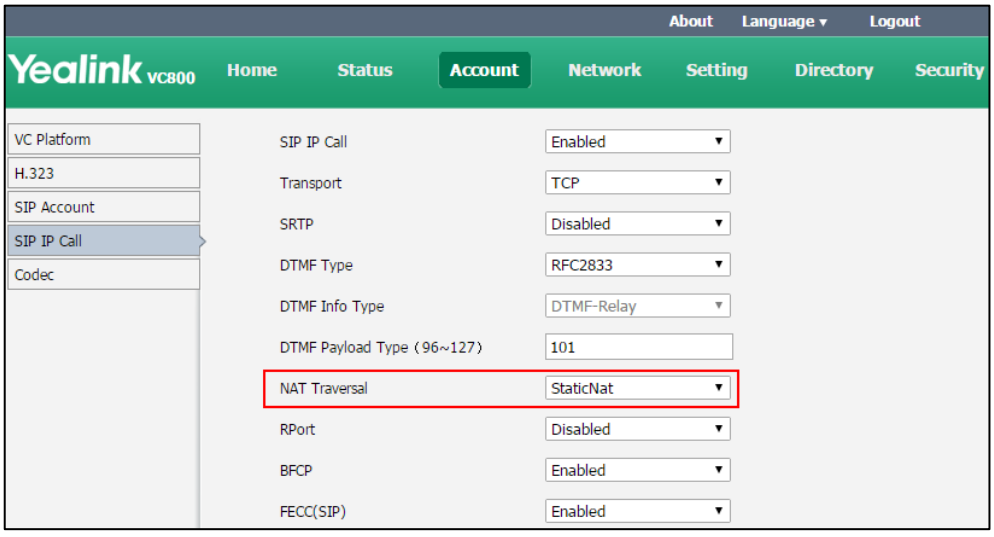
1. Click on **Account**->**SIP Account**.
2. Select **StaticNat** from the pull-down list of **NAT Traversal**.



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

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

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



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

To configure static NAT via the remote control:

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

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

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**SIP IP Call.**
2. Select **StaticNat** from the pull-down list of **NAT Traversal**.
3. Select **Save**, and then press (OK) to accept the change.

Route Traversal

If your environment has 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 route traversal feature forcibly on the VCS that is connected to the secondary router, so that the NAT works even though both devices are in the Intranet.

Note If you enable route traversal forcibly, the risk is that the VCS may fail to call the other VCS connected to the same router, because the NAT address replaces the private address.

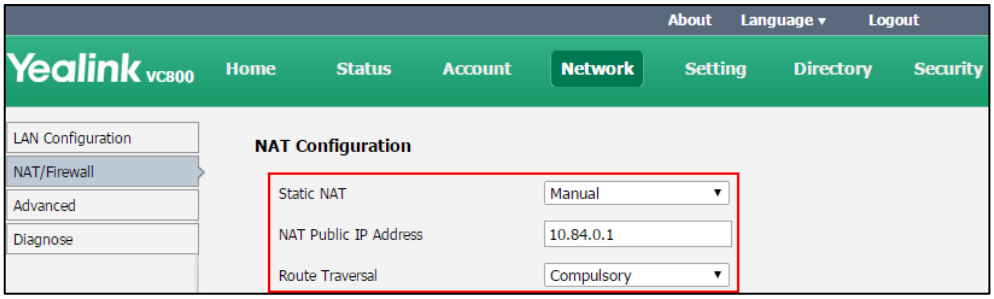
Route traversal parameters on the system are described below:

Parameter	Description	Configuration Method
Static NAT	Select **Manual**, and then configure the NAT address manually.	Remote Control Web User Interface
NAT Public IP Address	Configures the NAT address for the system manually.	Remote Control Web User Interface
Route Traversal	Configures 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. • **Compulsory**−NAT works no matter you are making a call to a public address or private address. **Default:** Auto	Web User Interface

Parameter	Description	Configuration Method
NAT Traversal	Configures the NAT traversal type. You can configure it for the SIP account or SIP IP call separately. • **Disabled** • **STUN** • **StaticNat** **Default:** Disabled **Note:** Static NAT works only if this parameter is set to **StaticNat**.	Web User Interface

To configure route traversal via web user interface:

1. Click on **Network**->**NAT/Firewall**.
2. Select **Manual** from the pull-down list of **Static NAT**.
3. Enter the NAT address in the **NAT Public IP Address** field.
4. Select **Compulsory** from the pull-down list of **Route Traversal**.



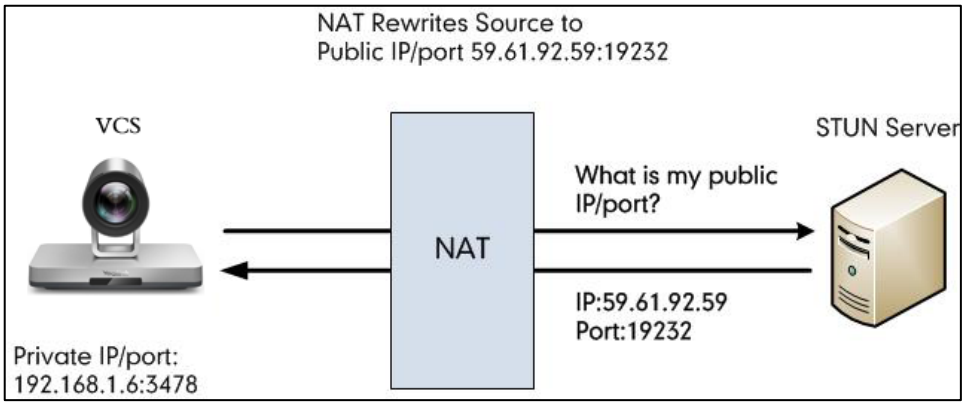
5. Click **Confirm** to accept the change.
6. Enable static NAT for SIP account or SIP IP call. For more information, refer to Static NAT on page 44.

STUN

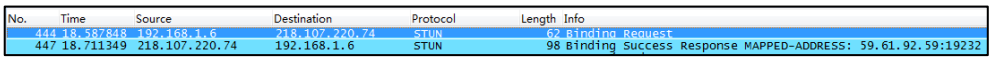
You can use the Simple Traversal of UDP through NAT (STUN) function besides ALG or static NAT. If STUN is enabled, the system can perform private-to-public network traversal using the STUN server.

STUN is a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. The STUN protocol allows the system behind a NAT to first discover the presence of a NAT and the type of NAT, and then allows the system to obtain the mapped (public) IP address and port number that the NAT has allocated for the UDP connections to remote parties. The protocol requires assistance from a third-party network server (STUN server) usually located on public Internet. The IP phone can be configured

to work as a STUN client, to send exploratory STUN messages to the STUN server. The STUN server uses those messages to determine the public IP address and port used, and then informs the client. For more information, refer to RFC3489.



Capturing packets after you enable the STUN feature, you can find that the VC800/VC500 video conferencing system sends Binding Request to the STUN server, and then mapped IP address and port is placed in the Binding Response: Binding Success Response MAPPED-ADDRESS: 59.61.92.59:19232.



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

Note STUN does not enable incoming TCP connections through NAT or incoming UDP packets through symmetric NATs.

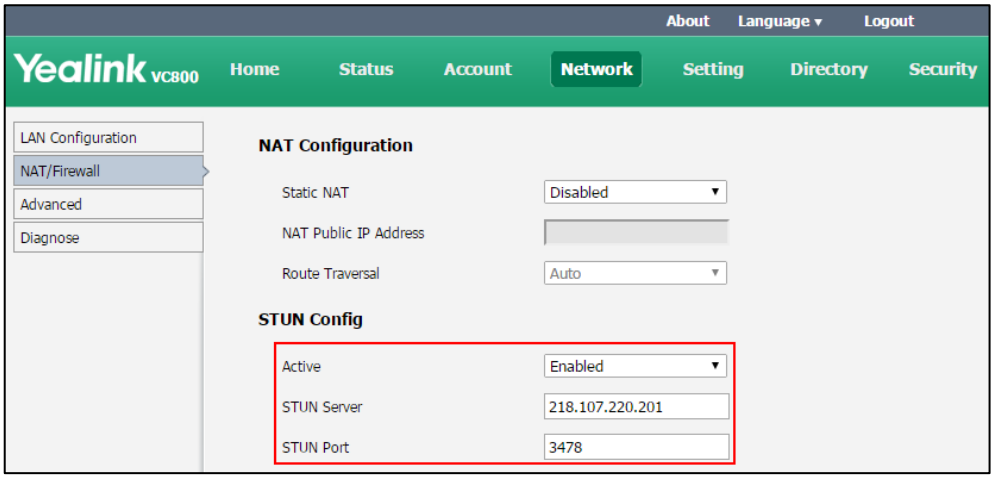
STUN feature parameters on the system are described below:

Parameter	Description	Configuration Method
Active	Enables or disables the STUN (Simple Traversal of UDP over NATs) feature on the system. **Default**: Disabled	Remote Control Web User Interface
STUN Server	Configures the IP address or the domain name of the STUN (Simple Traversal of UDP over NATs) server. **Default**: Blank	Remote Control Web User Interface
STUN Port	Configures the port of the STUN (Simple Traversal of UDP over NATs) server. **Default:** 3478	Remote Control Web User Interface

Parameter	Description	Configuration Method
NAT Traversal	Configures the NAT traversal type. You can configure it for the SIP account or SIP IP call separately. • **Disabled** • **STUN** • **StaticNat** **Default:** Disabled **Note:** Static NAT works only if this parameter is set to StaticNat.	Web User Interface

To configure STUN server via web user interface:

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

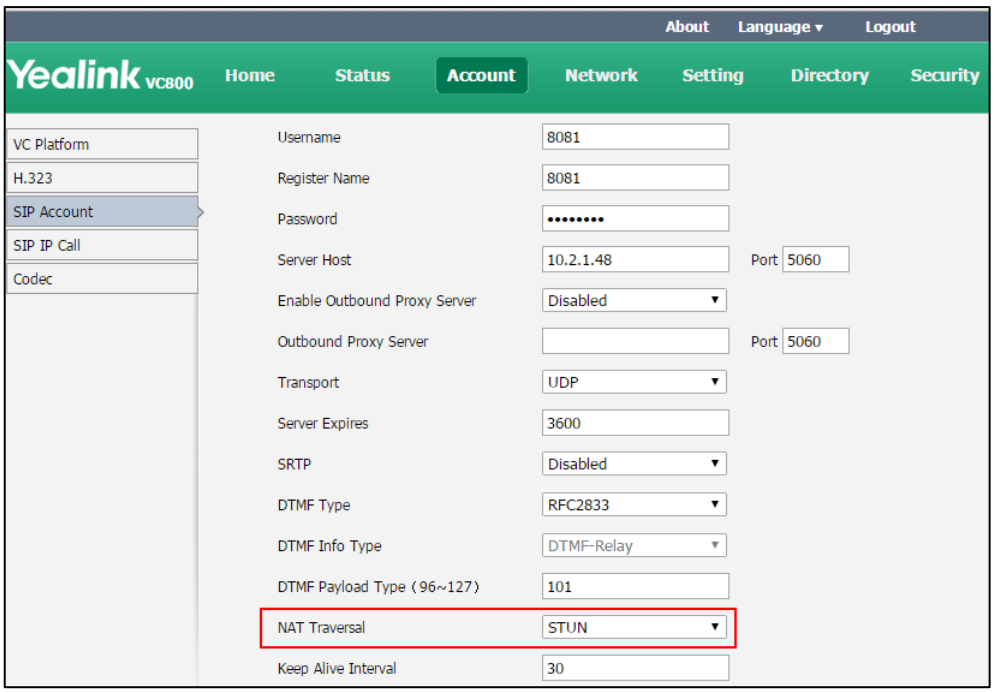


5. Click **Confirm** to accept the change.

To configure STUN for SIP account via web user interface:

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

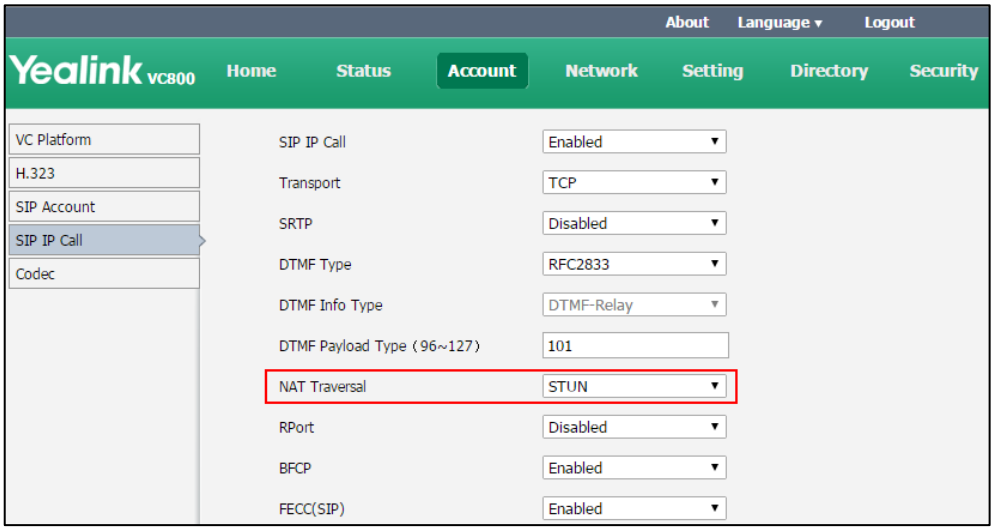
2. Select **STUN** from the pull-down list of **NAT Traversal**.



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

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

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



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

To configure STUN server via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**NAT/Firewall**.

   Mark the **ON** radio box in the **STUN Active** field.
2. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.

3. Enter the port of the STUN server in the **Port** field.
4. Select **Save**, and then press OK to accept the change.

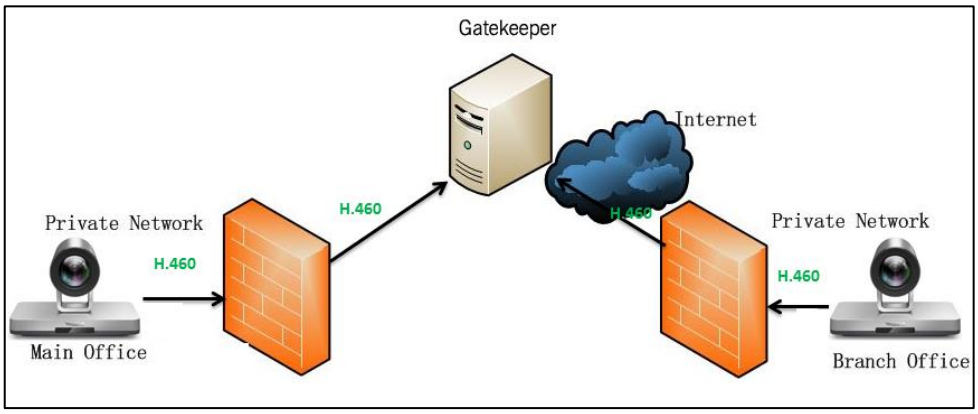
To configure STUN server for SIP IP call via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**SIP IP Call**.
2. Select **STUN** from the pull-down list of **NAT Traversal**.
3. Select **Save**, and then press OK to accept the change.

Enabling H.460 Support for H.323 Calls

Yealink video conferencing systems support firewall traversal of H.323 calls using 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 static NAT settings. For more information on static NAT, refer to Static NAT on page 44.



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

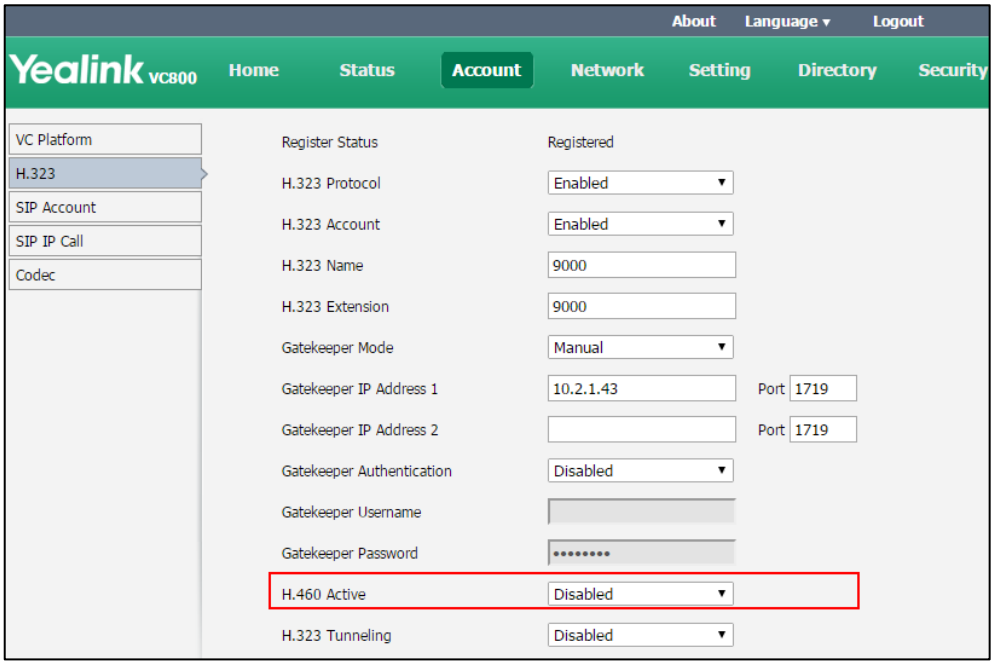
The H.460 firewall traversal parameter is described below:

Parameter	Description	Configuration Method
H.460 Active	Enables or disables firewall traversal of H.323 calls using H.460 protocols. **Default:** Disabled	Remote Control Web User Interface

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

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

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



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

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

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**H.323**.
2. Check the **H.460** checkbox.
3. Select **Save**, and then press OK to accept the change.

Intelligent Traversal

Some branch offices lack IT professionals, which means that professional network configuration (for example: port forwarding) is impossible. Yealink VCS supports intelligent traversal deployment. You can deploy the VCS in an intranet, and assign a private IP address which can access the public network. This deployment method involves a simple setup process. You can deploy the VCS without any firewall configuration. But using this method, inbound calls are unavailable, only outbound calls are available.

The principles are introduced as below:

When VCS in the Intranet calls the VCS in the public network, the VCS in the Intranet may fail to receive video & audio from the public network. The intelligent traversal feature allows the VCS in the public network to check the media source address and port of incoming RTP packets, and then send back RTP packets to the address where incoming RTP packet comes from, instead of the address provided in the Session Description Protocol (SDP).

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

The VCS A locates in the Intranet 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.

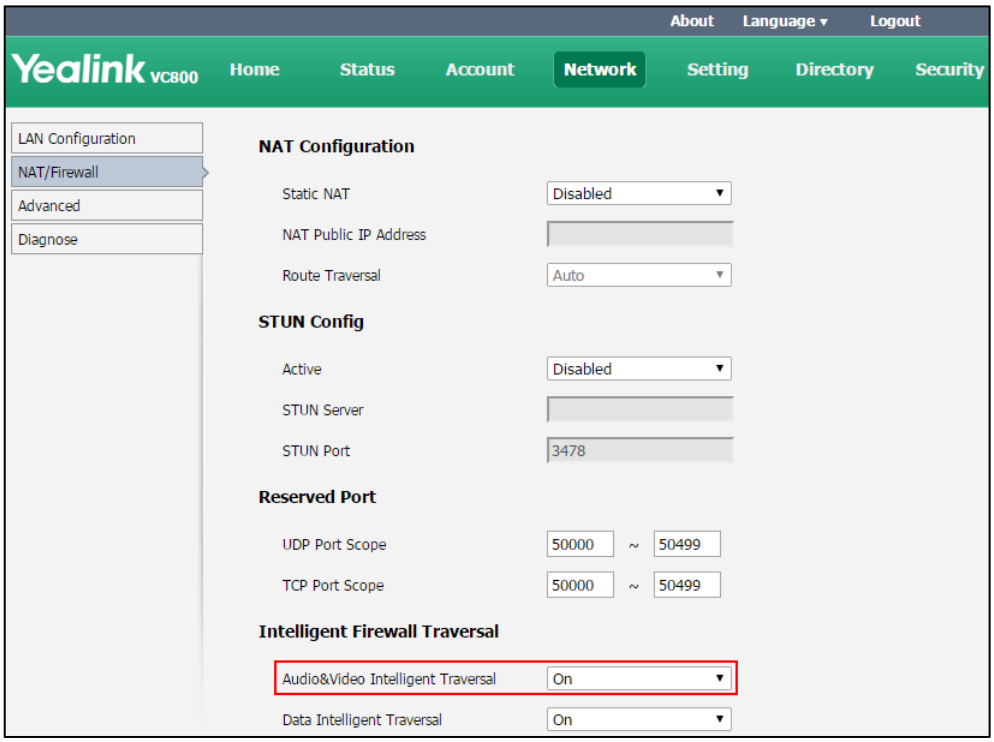
- If B disables the audio & video intelligent traversal feature, B sends RTP data to the negotiated IP address of A (private IP address provided in the Session Description Protocol), causing the device display of A appears black screen.
- If B enables the audio & video intelligent traversal feature,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

The audio & video intelligent traversal parameter is described below:

Parameter	Description	Configuration Method
Audio&Video Intelligent Traversal	Enables or disables the audio & video media stream to traverse firewall. **Default:** On	Web User Interface

To configure audio & video intelligent traversal via web user interface:

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



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

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

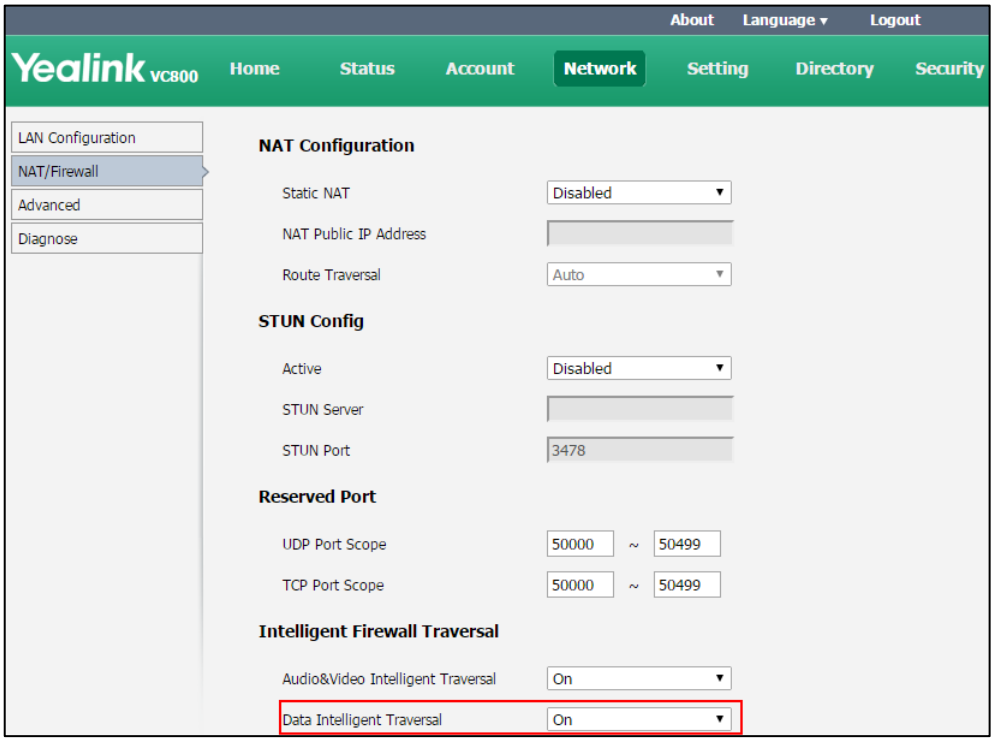
seconds by default. If the VCS B in the public network does not share content within 30 seconds, the mapped port will change, so that the VCS B may fail to share content to VCS A later. To solve this problem, enable the data intelligent traversal on VCS A, the VCS A will send keep-alive messages at regular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

The data intelligent traversal parameter is described below:

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

To configure data intelligent traversal via web user interface:

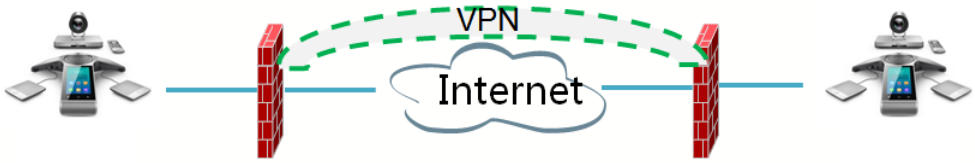
1. Click on **Network**->**NAT/Firewall**.
2. Select the desired value from the pull-down list of **Data Intelligent Traversal**.



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

VPN

VPN (Virtual Private Network) is a secured private network connection built on top of public telecommunication infrastructure, such as the Internet. It has become more prevalent due to benefits of scalability, reliability, convenience and security.



VPN Technology

VC800/VC500 systems support SSL VPN, which provides remote-access VPN capabilities through SSL. OpenVPN is a full featured SSL VPN software solution that creates secure connections in remote access facilities, designed to work with the TUN/TAP virtual network interface. TUN and TAP are virtual network kernel devices. TAP simulates a link layer device and provides a virtual point-to-point connection, while TUN simulates a network layer device and provides a virtual network segment.

VC800/VC500 systems use OpenVPN to achieve VPN feature. To prevent disclosure of private information, tunnel endpoints must authenticate each other before secure VPN tunnel is established. After VPN feature is configured properly on the IP phone, the IP phone acts as a VPN client and uses the certificates to authenticate the VPN server.

To use VPN, the compressed package of VPN-related files should be uploaded to the VC800/VC500 systems 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 unified directories of the OpenVPN certificates and key in the configuration file (vpn.cnf) for Yealink video conferencing system:

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

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

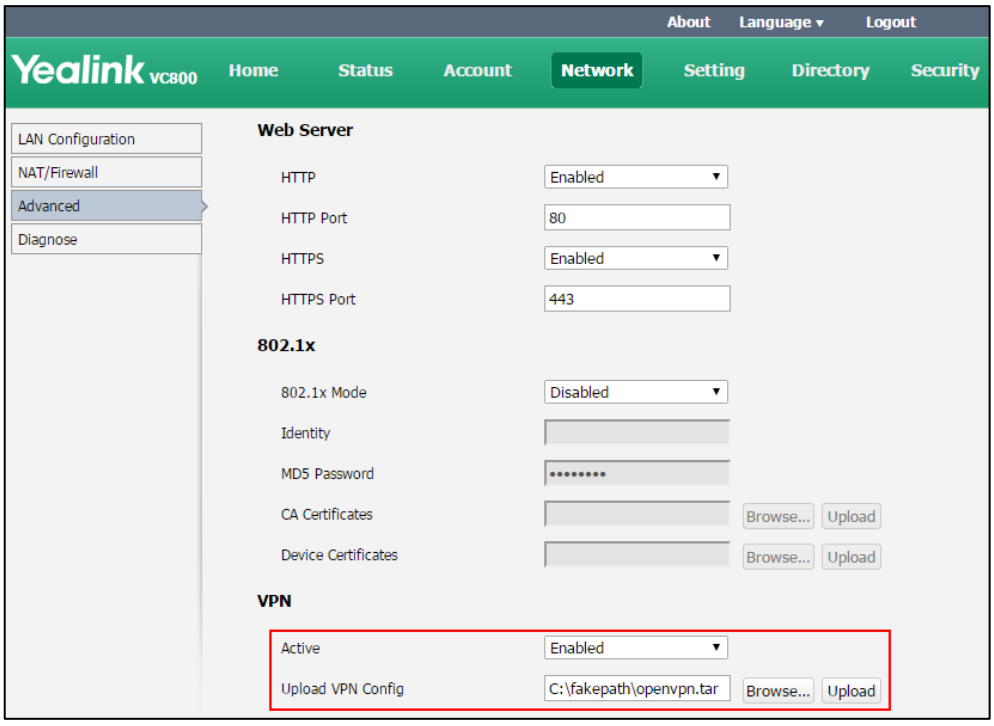
VPN feature parameters on the system are described below.

Parameter	Description	Configuration Method
VPN	Enables or disables VPN feature on the system.	Remote Control Web User Interface

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

To configure VPN via web user interface:

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



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

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

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

   If VPN is selected, you display device will display  icon.

To configure VPN via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Check the **VPN** checkbox.

   Make sure you have uploaded the compressed package of VPN-related files (*.tar) to the system via web user interface.
3. Select **Save**, and then press OK to accept the change.

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

   If VPN is selected, you display device will display  icon.

Cloud Deployment Method

When holding a video conference, customers often 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 change in the way organizations communicate. With video conference platform, organizations can communicate easily. Public IP address and complex network settings are unnecessary.

Challenges such as infrastructure costs and interoperability are eliminated. Both the head office and the branch offices can use the Cloud deployment method. Both inbound and outbound calls are available.

For more information, refer to Configuring Video Conference Platform on page 70.

Configuring Call Preferences

This chapter provides information on how to configure system's call preferences (for example: call type and network bandwidth).

This chapter provides the following sections:

Configuring SIP Settings

Yealink VC800/VC500 video conferencing system support Session Initiation Protocol (SIP). If your server supports SIP, you can use SIP to establish calls.

SIP Account

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

SIP account parameters on the system are described below:

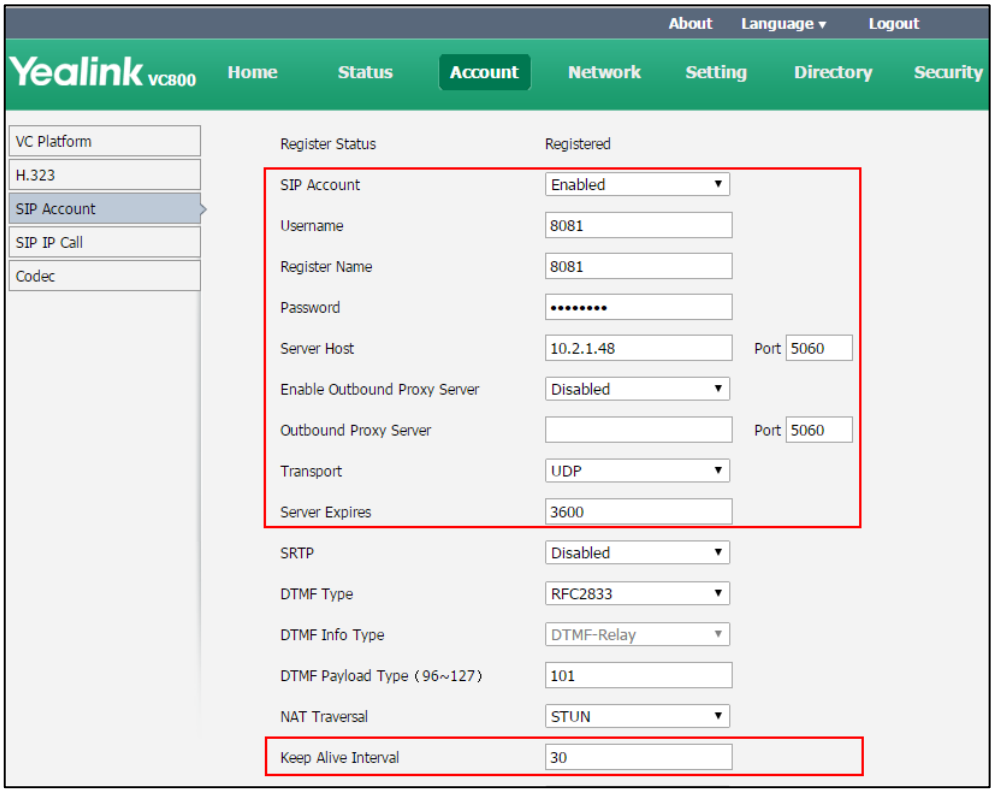
Parameter	Description	Configuration Method
SIP Account	Enables or disables the SIP account. **Default:** Enabled	Remote Control Web User Interface
User Name	Specifies the user name to use for authentication when registering with a SIP server. **Default**: Blank	Remote Control Web User Interface
Register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

Parameter	Description	Configuration Method
	65535. **Default**: 5060	
Transport	Configures the type of transport protocol for the SIP account. • **UDP**−provides best-effort transport via UDP for SIP signaling. • **TCP**−provides reliable transport via TCP for SIP signaling. • **TLS**−provides secure communication of SIP signaling. • **DNS-NAPTR**−performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** UDP **Note**: TLS is available only when the system is registered with a SIP server that supports TLS.	Remote Control Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the SIP server for SIP account. **Default:**3600	Remote Control Web User Interface
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. **Default:** 30	Web User Interface
Rport	Enables or disables the Rport feature. When the VCS locates behind a NAT device, you can enable Rport to solve the port traversal with the SIP sever. **Note:** Rport feature depends on support from a SIP server.	Web User Interface

Parameter	Description	Configuration Method
	For more information, refer to RFC 3581. **Default**: Disabled	

To configure SIP account via web user interface:

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



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

   After successful registration, the display device displays SIP.

To configure SIP account via the remote control:

1. Select **More->Setting->Advanced** (default password: 0000) ->**SIP Account**.
2. Configure the SIP account settings.
3. Select **Save**, and then press OK to accept the change.

   After successful registration, the display device displays SIP.

SIP IP Call

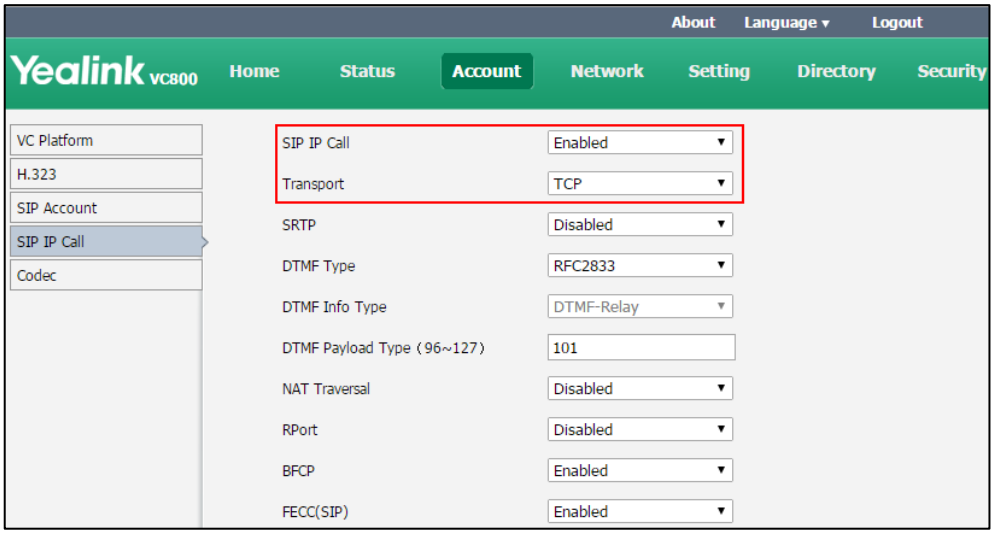
When making an IP call using the SIP protocol, the system doesn't support the TLS transport protocol. So configuration parameters of SIP IP call are divided from the SIP account. You can configure SIP IP call separately.

SIP IP call parameters on the system are described below:

Parameter	Description	Configuration Method
SIP IP Call	Enables or disables the SIP IP Call. **Default:** Enabled. **Note:** When it is set to Enabled on both sites, the VC800/VC500 can call the far site by dialing an IP address directly.	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the SIP IP call. • **UDP**–provides best-effort transport via UDP for SIP signaling. • **TCP**–provides reliable transport via TCP for SIP signaling. • **DNS-NAPTR**–performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** TCP	Remote Control Web User Interface

To configure SIP IP call via web user interface:

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



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

To configure SIP IP call via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000)->**SIP IP Call**.
2. Check the **SIP IP Call** checkbox.
3. Select **Save**, and then press OK to accept the change.

Configuring H.323 Settings

Yealink VC800/VC500 video conferencing systems support H.323 protocol. If your network uses a gatekeeper, you can register an H.323 account for the system, and specify its H.323 name and extension. This allows others to call the system by entering the H.323 name or extension instead of the IP address.

H.323 settings parameters on the system are described below:

Parameter	Description	Configuration Method
H.323 Protocol	Enables or disables the H.323 protocol. **Default:** Enabled. **Note:** Only when it is set to Enabled, can H.323 account be registered. When it is set to Enabled on both sites, the VC800/VC500 can call the far site by dialing an IP address directly.	Remote Control Web User Interface
H.323 Account	Enables or disables the H.323 account. **Default:** Enabled If it is set to disabled, the system cannot place or receive calls with the H.323 protocol.	Remote Control Web User Interface
H.323 Name	Specifies the name that gatekeepers and gateways use to identify this system. You can make point-to-point calls using H.323 names if both system are registered to a gatekeeper. **Default:** blank	Remote Control Web User Interface
H.323 Extension	Specifies the extension that gatekeepers and gateways use to identify this system. **Default:** blank **Note:** Users can place point-to-point calls using the extension if both systems are registered with a gatekeeper.	Remote Control Web User Interface

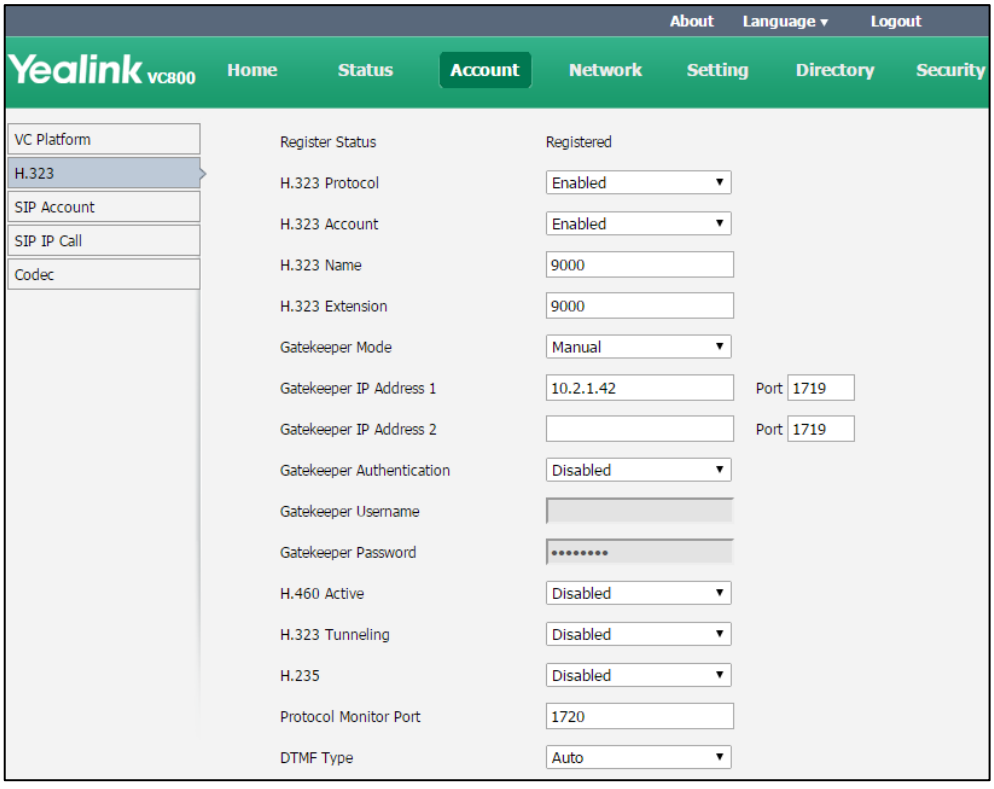
Parameter	Description	Configuration Method
Gatekeeper Type/Gatekeeper Mode	Configures the gatekeeper mode. ● **Disabled**−the system does not use a gatekeeper. ● **Auto**−the system automatically discovers a gatekeeper. ● **Manual**−specify the IP address and port for the gatekeeper manually. **Default:** Disabled	Remote Control Web User Interface
Gatekeeper Server1/Gatekeeper IP Address 1	Configures the IP address of the primary gatekeeper.	Remote Control Web User Interface
Gatekeeper Port 1/Port	Configures the port of the primary gatekeeper. **Valid values:** Integer from 0 to 65535. **Default**: 1719	Remote Control Web User Interface
Gatekeeper Server2/Gatekeeper IP Address 2	Configures the IP address of the secondary gatekeeper. **Note**: If communication with the primary gatekeeper is lost, the system registers with the alternate gatekeeper.	Remote Control Web User Interface
Gatekeeper Port 2/Port	Configures the port of the primary gatekeeper. **Valid values:** Integer from 0 to 65535. **Default**: 1719	Remote Control Web User Interface
Gatekeeper Verify /Gatekeeper Authentication	Enables or disables support for gatekeeper authentication. **Default:** Disabled **Note:** When Gatekeeper Authentication is enabled, the gatekeeper ensures that only trusted H.323 systems are allowed to access the gatekeeper.	Remote Control Web User Interface
Gatekeeper Username	Specifies the user name for authentication with gatekeeper. **Default:** blank	Remote Control Web User Interface
Gatekeeper Password	Specifies the password for authentication with gatekeeper.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Default: blank	
H.460 Active	Enables or disables firewall traversal of H.323 calls using H.460 protocols. **Default:** Disabled For more information, refer to Enabling H.460 Support for H.323 Calls on page 52.	Remote Control Web User Interface
H.323 Tunneling	(Optional) Instructs the system to send all signaling and media through the HTTP tunnel. **Default:** Disabled For more information, refer to H.323 Tunneling on page 68.	Remote Control Web User Interface
H.235	Specifies the H.235 type during an H.323 call. • **Disabled**–encrypted calls are not supported. • **Optional**–both encrypted and unencrypted calls are supported. Secure calls are supported only if the far end supports encryption. • **Compulsory**–unencrypted calls are not supported. **Default:** Disabled For more information, refer to H.235 on page 228.	Web User Interface
Protocol Monitor Port	Specifies the port for the H.323 call setup. If the ISP limits the 1720 port, you should modify the port, and dial the far site using h323:ip:port format. **Default:** 1720 **Note:** It is only applicable to IP call for H.323.	Web User Interface
Local Early Media	Enables or disables local early media feature on the system. • **Disabled**–the local system sends	Web User Interface

Parameter	Description	Configuration Method
	an Open Logical Channel (OLC) message and receives an acknowledgement message from the remote system. After receiving the acknowledgement message, the system may then transmit RTP streams to the remote system. • **Enabled**–the system sends an Open Logical Channel (OLC) message to the remote system and then transmits RTP streams to the remote system 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**: Disabled.	

To configure H.323 account via web user interface:

1. Click on **Account**->**H.323**.
2. Configure the H.323 account settings.



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

   After successful registration, the display device displays H323 .

To configure H.323 account via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**H.323**.
2. Configure the H.323 account settings.
3. Select **Save**, and then press OK to accept the change.

   After successful registration, the display device displays H323 .

H.323 Tunneling

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

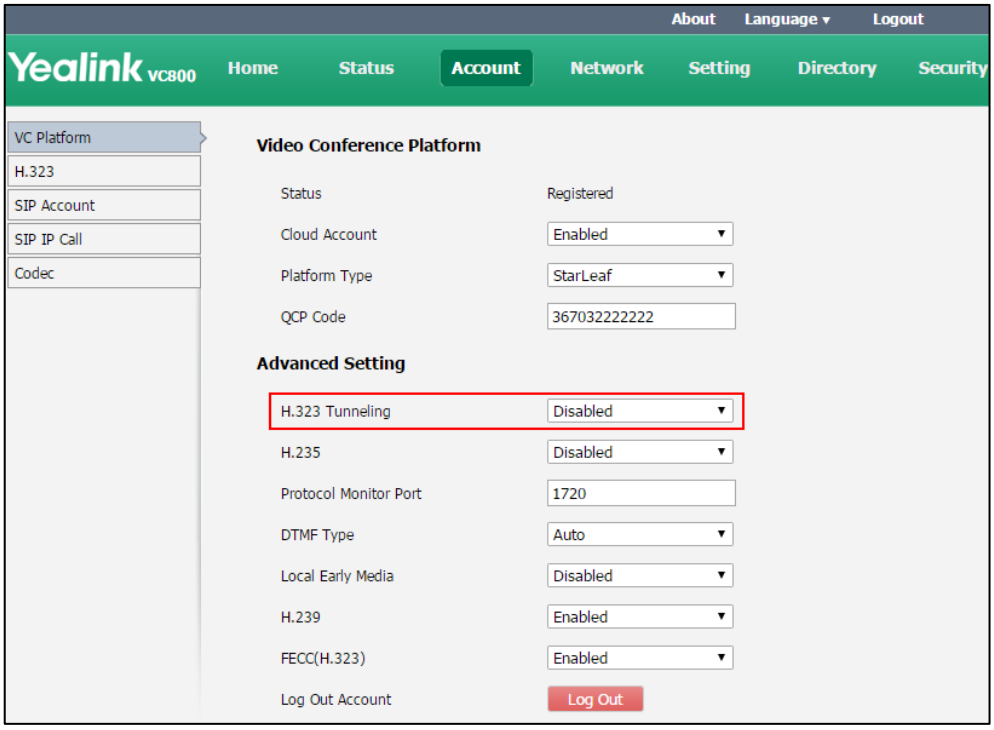
The parameter of the H.323 tunneling feature on the system is described below:

Parameter	Description	Configuration Method
H.323 Tunneling	Enables or disables the system to send all signaling and media through the HTTP tunnel. You can configure it for the StarLeaf Cloud platform or H.323 call separately. **Default:** Disabled	Remote Control Web User Interface

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

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

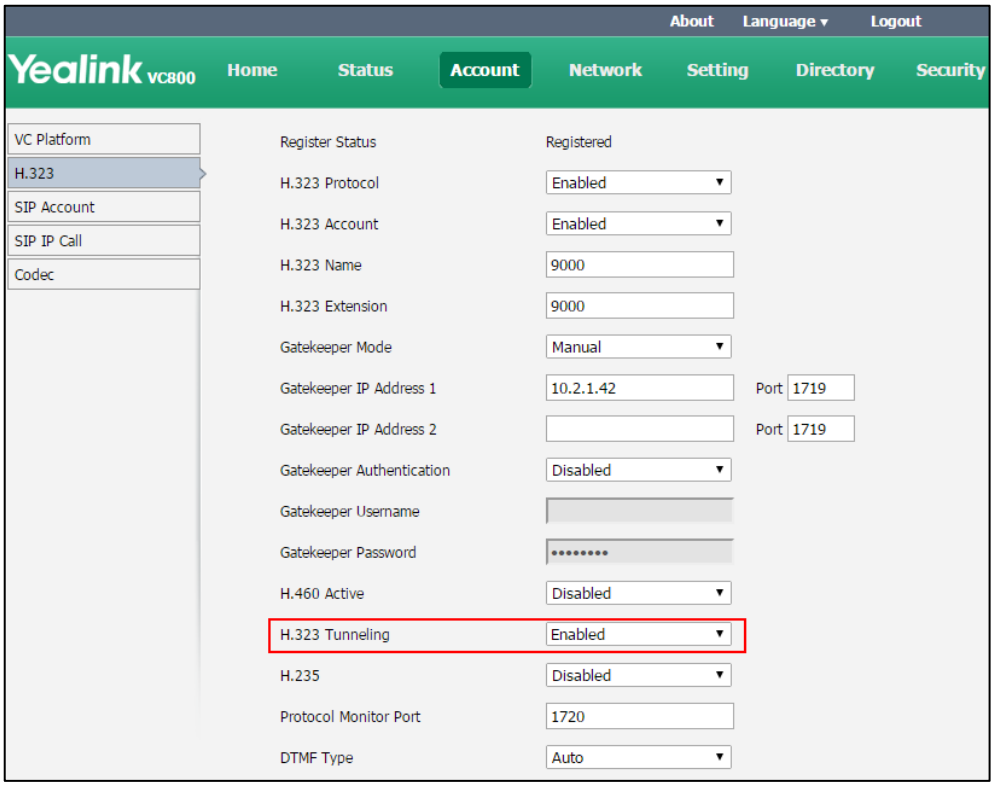
3. Select the desired value from the pull-down list of **H.323 Tunneling**.



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

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

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



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

To configure H.323 tunneling via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000)->**H.323**.
2. Check the **H.323 Tunneling** checkbox.
3. Select **Save**, and then press OK to accept the change.

Configuring Video Conference Platform

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

Logging into Yealink VC Cloud Management Service

Yealink VC800/VC500 video conferencing systems support Yealink Cloud accounts. 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*.

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

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

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

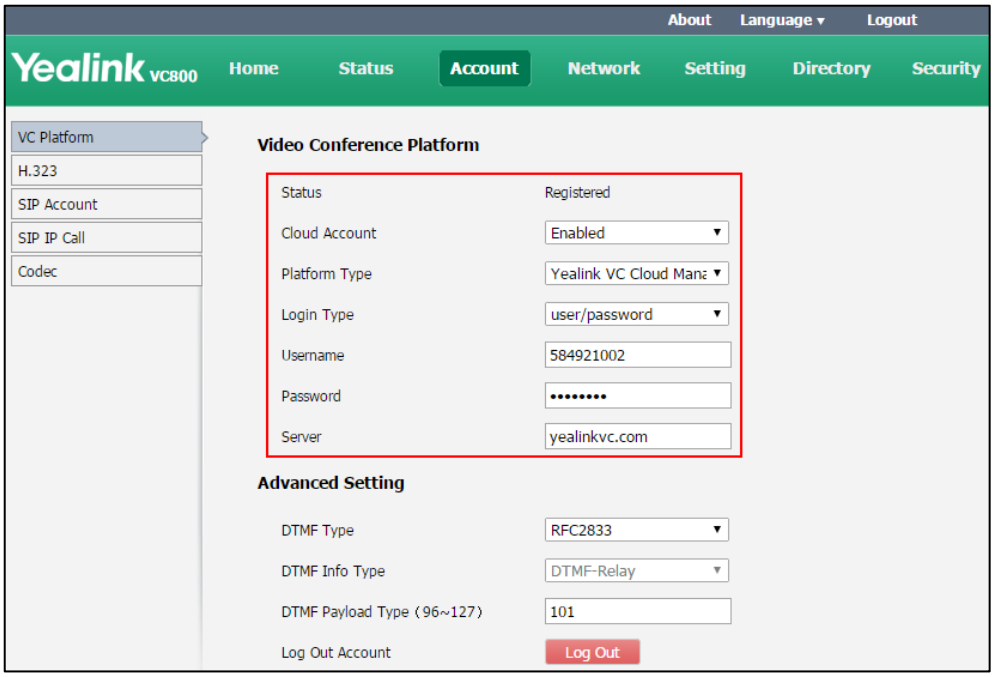
Parameter	Description	Configuration Method
	● Pexip ● BlueJeans ● Mind ● Custom **Default**: Yealink VC Cloud Management Service	
Login Type	Specifies the method for logging into the Yealink VC Cloud Management Service platform. ● **PIN Code Login**: This method uses the user's PIN code to log into the Yealink VC Cloud Management Service platform. The PIN code consists of 9 digits. You can only use the PIN code once and it will expire if unused for 7 days. Contact Cloud administrator when it expires. ● **user/password**: This method uses the user's Yealink Cloud number and password to log into the Yealink VC Cloud Management Service platform. **Default**: PIN Code Login	Remote Control Web User Interface
Pincode/Pin Code	Specifies the PIN code for logging into the Yealink VC Cloud Management Service platform. **Default**: Blank **Note:** It only works if the value of **Login Type** is set to **PIN Code Login**.	Remote Control Web User Interface
Username	Specifies the user name to log into the Yealink VC Cloud Management Service platform. **Default**: Blank **Note:** It only works if the value of **Login Type** is set to **user/password**.	Remote Control Web User Interface
Password	Specifies the password associated with the user name when signing into the	Remote Control Web User Interface

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

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

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

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



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

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

1. Select **More**->**Setting**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **Yealink VC Cloud Management Service** from the pull-down list of **Platform Type**.
4. Select the desired sign-in method from the pull-down list of **Login Type**.
   - If you select **Pincode Login:**

     Enter your PIN code in the **Pincode** field, press ▲ or ▼ to scroll to **Log In**, and then press OK.
   - If you select **Username/Password**:

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

     Press ▲or ▼to scroll to **Log In**, and then press OK.
5. Enter the IP address or domain name of the Yealink VC Cloud Management Service platform in the **Server** field.

   After successful registration, the display device displays VC.

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

Logging into Yealink Meeting Server

Yealink VC800/VC500 video conferencing systems support YMS accounts. The enterprise administrator uses the Yealink Meeting Server (YMS) to assign each user an individual YMS account. For more information on how to add YMS accounts, refer to *Yealink Meeting Server Administrator Guide*.

When you are using the YMS account, you can:

- Dial the other YMS accounts to establish a conversation.
- View and join scheduled conferences.
- Initiate and join meet now conferences.
- Join the permanent VMR.
- Manage YMS video conferences.

For detailed introduction, refer to *Yealink VC800&VC500 Full HD Video Conferencing System User Guide.*

Yealink Meeting Server parameters on the system are described below:

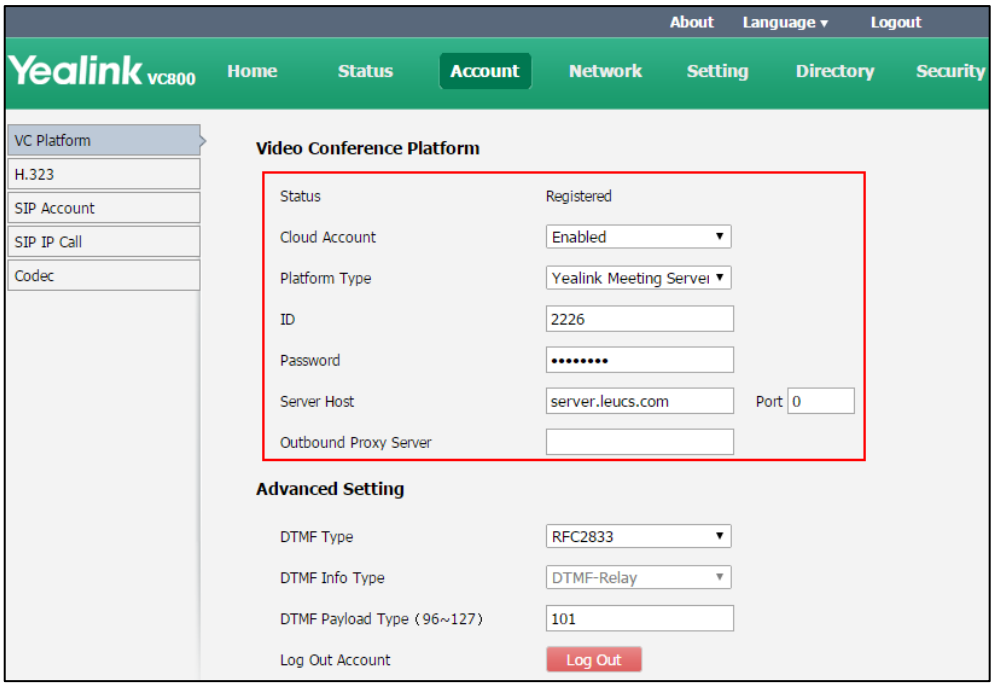
Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot register the YMS account.	Remote Control Web User Interface
Platform Type	Configures the platform type. • Yealink VC Cloud Management Service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

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

To configure Yealink Meeting Server via web user interface:

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

4. Configure the YMS account settings.



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

To configure Yealink Meeting Server via the remote control:

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

Note

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

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

Logging into Third-Party Platform

Yealink provides broad compatibility and seamless interoperability with the industry's leading Cloud-based video conferencing platforms and on-premise solutions.

Yealink video conferencing systems are compatible with StarLeaf/Zoom/BlueJeans/Pexip/Mind/Custom platform. Customers can benefit from both the

features provided by video conferencing system, such as 1080p HD video and audio, and features provided by the third-party platform, including high end customization & interoperability.

Once logging into the third-party platform, video conferencing systems can communicate with each other by entering Virtual Meeting Rooms (VMRs).

Logging into the StarLeaf Cloud Platform

You can log into the StarLeaf Cloud platform.

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

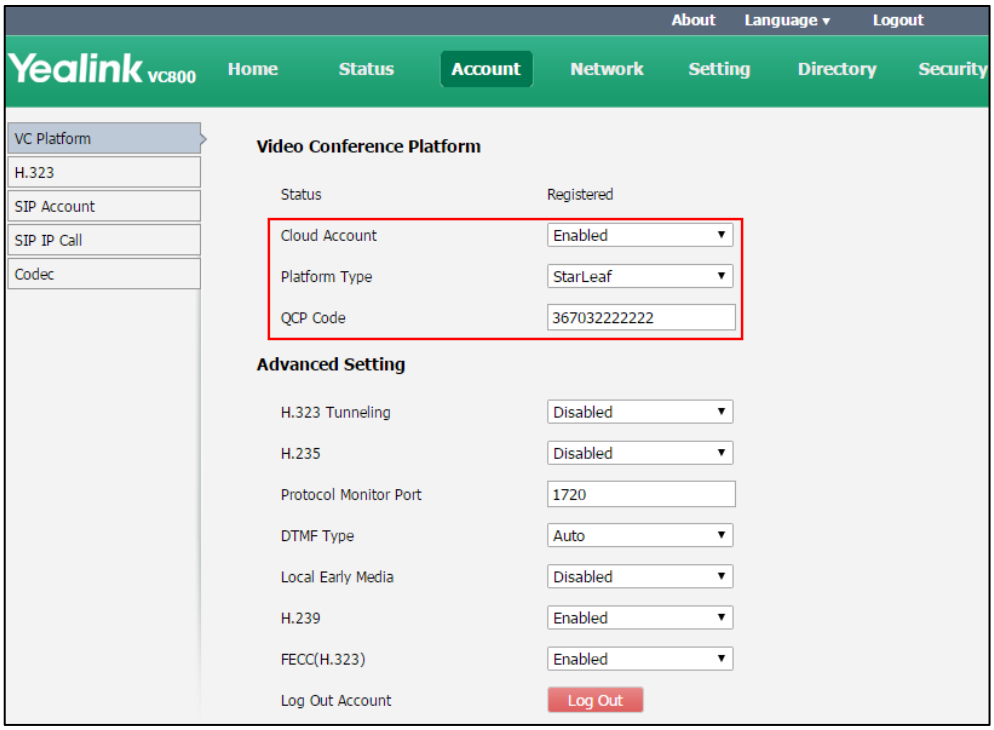
- Call the other StarLeaf Cloud account to establish a point to point call.
- Call the Meeting ID to join the Virtual Meeting Rooms.
- Call between StarLeaf Cloud account and Microsoft Skype for Business/Lync account.

StarLeaf platform parameters on the system are described below:

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

To configure StarLeaf Cloud platform via web user interface:

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



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

To configure StarLeaf Cloud platform via the remote control:

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

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

Logging into the Zoom Cloud Platform

You can log into the Zoom Cloud platform and join the virtual meeting room.

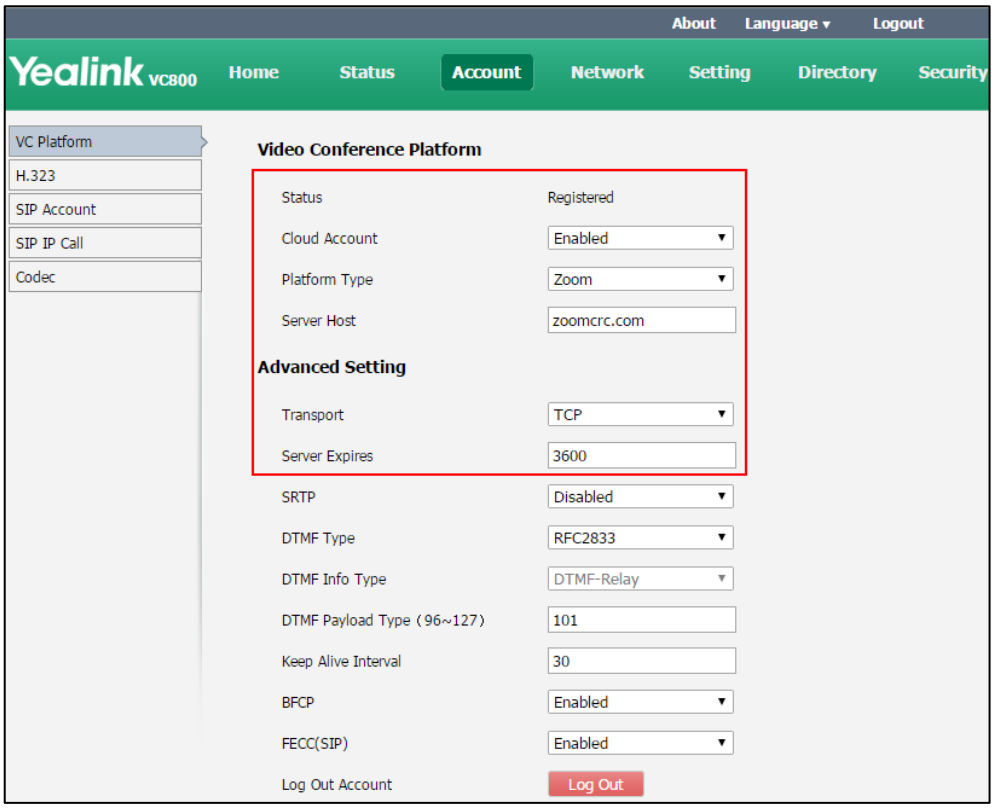
Zoom Cloud platform parameters on the system are described below:

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

Parameter	Description	Configuration Method
	port is given. **Default:** TCP	
Server Expires	Configures the registration expiration time (in seconds) of the Cloud server. **Default:**3600	Web User Interface
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. **Default:** 30	Web User Interface

To configure Zoom Cloud platform via web user interface:

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



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

To configure Zoom Cloud platform via the remote control:

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

   The default Zoom server is "zoomcrc.com".
5. Press ▲or ▼to scroll to **Log In**, and then press OK .

   After successful registration, the display device displays  .

Registering a Pexip Account

You can register the Pexip account.

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

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

Pexip platform parameters on the system are described below:

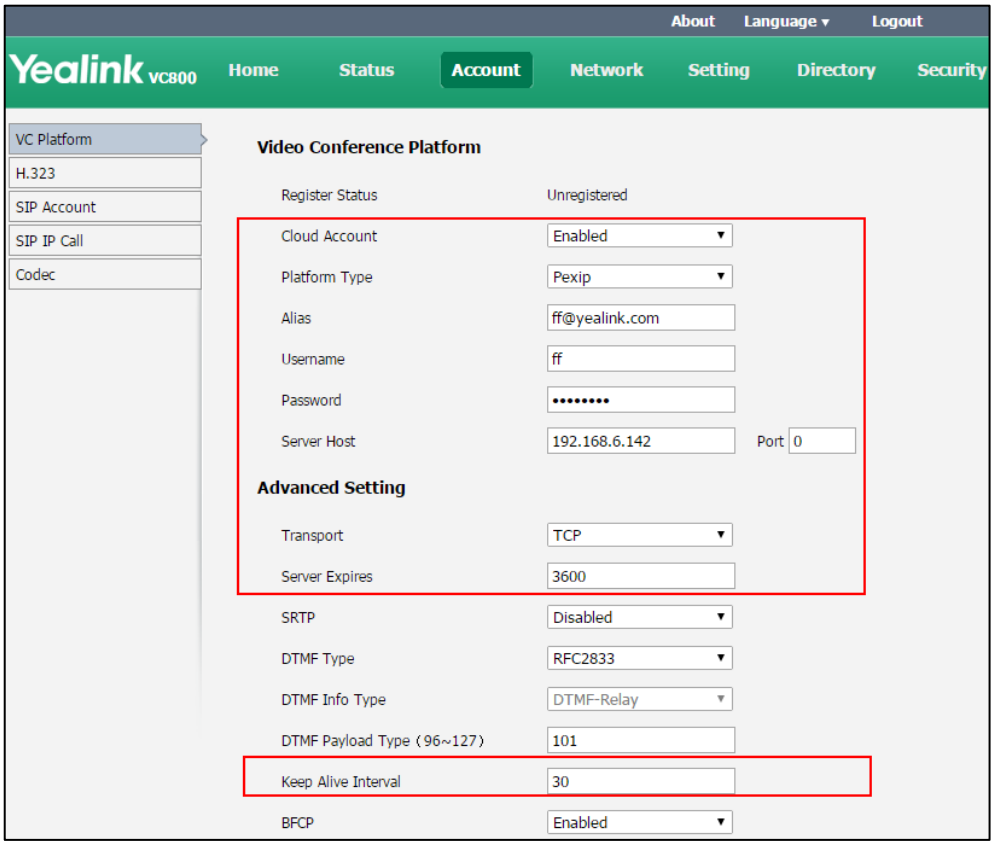
Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot register the Pexip account.	Remote Control Web User Interface
Platform Type	Configures the platform type. • Yealink VC Cloud Management Service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

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

Parameter	Description	Configuration Method
	information will be filled automatically when you enter the alias next time.	
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the connection open with the client. **Default:** 30	Web User Interface

To configure Pexip platform via web user interface:

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



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

To configure Pexip platform via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000)->**Video Conference Platform**.

2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **Pexip** from the pull-down list of **Platform Type**.
4. Configure the Pexip account settings.
5. Check the **Remember Password** checkbox to remember your registration information.
6. Press ▲ or ▼ to scroll to **Register**, and then press OK.
   After successful registration, the display device displays  .

Note You can also register the Pexip account using SIP or H.323 protocol.
For more information, refer to Configuring SIP Settings on page 59 and Configuring H.323 Settings on page 64.

Logging into the BlueJeans Cloud Platform

You can log into the BlueJeans Cloud platform and join the virtual meeting room.

BlueJeans Cloud platform parameters on the system are described below:

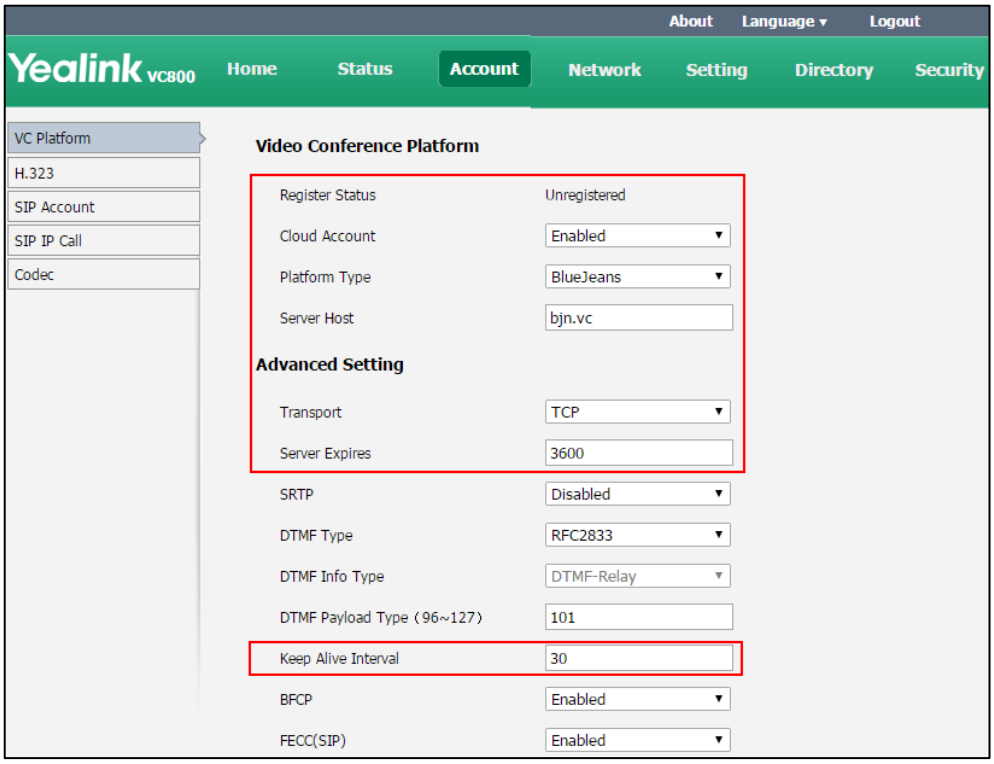
Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot log into the BlueJeans Cloud platform.	Remote Control Web User Interface
Platform Type	Configures the platform type. • Yealink VC Cloud Management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

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

To configure BlueJeans Cloud platform via web user interface:

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

4. Configure the BlueJeans Cloud platform.



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

To configure BlueJeans Cloud platform via the remote control:

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

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

   After successful registration, the display device displays  .

Logging into the Mind Platform

You can log into the Mind platform and join the virtual meeting room.

Mind platform parameters on the system are described below:

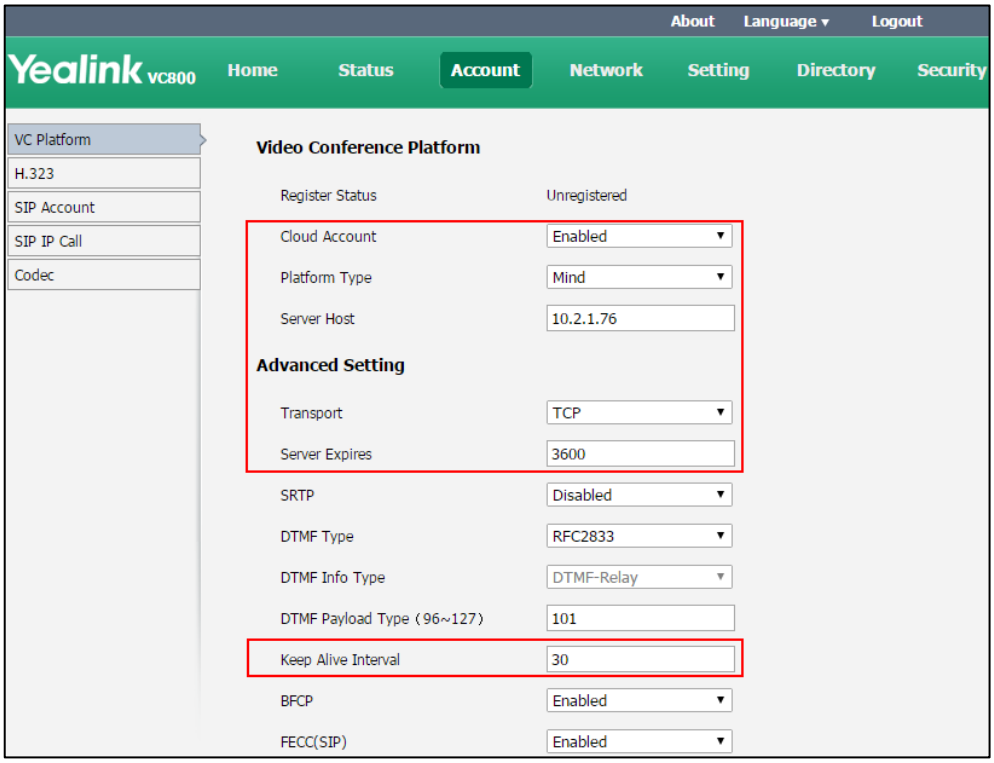
Parameter	Description	Configuration Method
Cloud Account	Enables or disables the Cloud feature. **Default:** Enabled **Note:** If it is disabled, the system cannot log into the Mind platform.	Remote Control Web User Interface

Parameter	Description	Configuration Method
Platform Type	Configures the platform type. ● Yealink VC Cloud Management Service ● Yealink Meeting Server ● StarLeaf ● Zoom ● Pexip ● BlueJeans ● Mind ● Custom **Default**: Yealink VC Cloud Management Service	Remote Control Web User Interface
Server/Server Host	Configures the IP address or domain name of the Mind server. **Default**: Blank	Remote Control Web User Interface
Transport	Configures the type of transport protocol for the Mind platform. ● **UDP**–provides best-effort transport via UDP for SIP signaling. ● **TCP**–provides reliable transport via TCP for SIP signaling. ● **TLS**–provides secure communication of SIP signaling. ● **DNS-NAPTR**–performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** TCP	Web User Interface
Server Expires	Configures the registration expiration time (in seconds) of the Cloud server. **Default:**3600	Web User Interface
Keep Alive Interval	Configures the interval (in seconds) that the system sends keep-alive messages to the registry server. So that the registry server will keep the	Web User Interface

Parameter	Description	Configuration Method
	connection open with the client. **Default:** 30	

To configure Mind platform via web user interface:

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



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

To configure Mind platform via the remote control:

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

Registering a Custom Account

You can register a custom account.

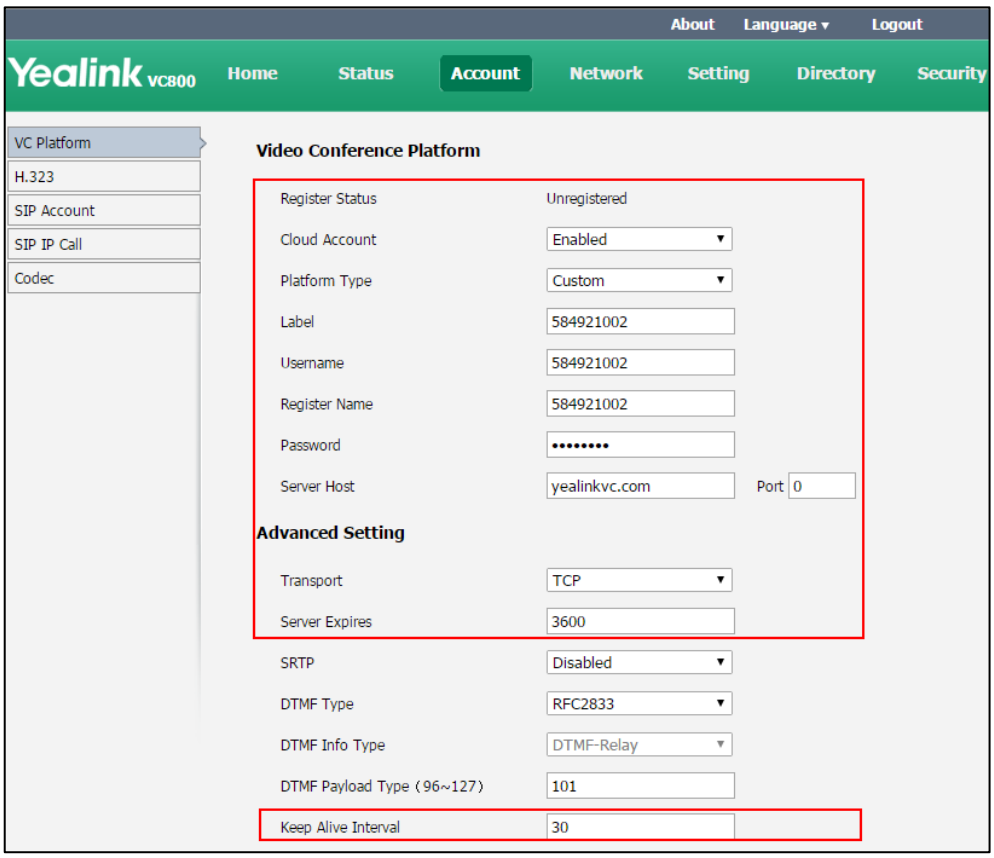
Custom account parameters on the system are described below:

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

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

To configure custom account via web user interface:

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



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

To configure custom account via the remote control:

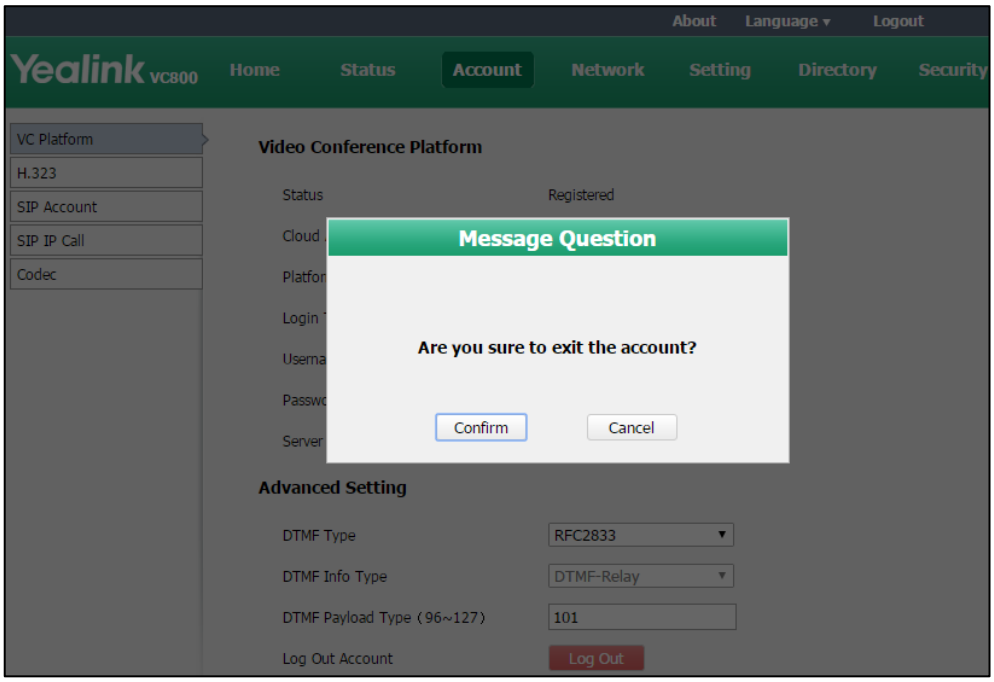
1. Select **More**->**Setting**->**Advanced** (default password: 0000)->**Video Conference Platform**.
2. In the **Cloud Account** field, check the **Enabled** checkbox.
3. Select **Custom** from the pull-down list of **Platform Type**.
4. Configure the custom account settings.
5. Check the **Remember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

Logging out of the Cloud Platform

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

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

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



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

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

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

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

Configuring the Third-party Virtual Meeting Room

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

If you do not register a Cloud account, or you have registered a Yealink Cloud account or YMS account, you can configure a third-party VMR in advance, so that you can quickly join a VMR

without registering a third-party Cloud account.

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

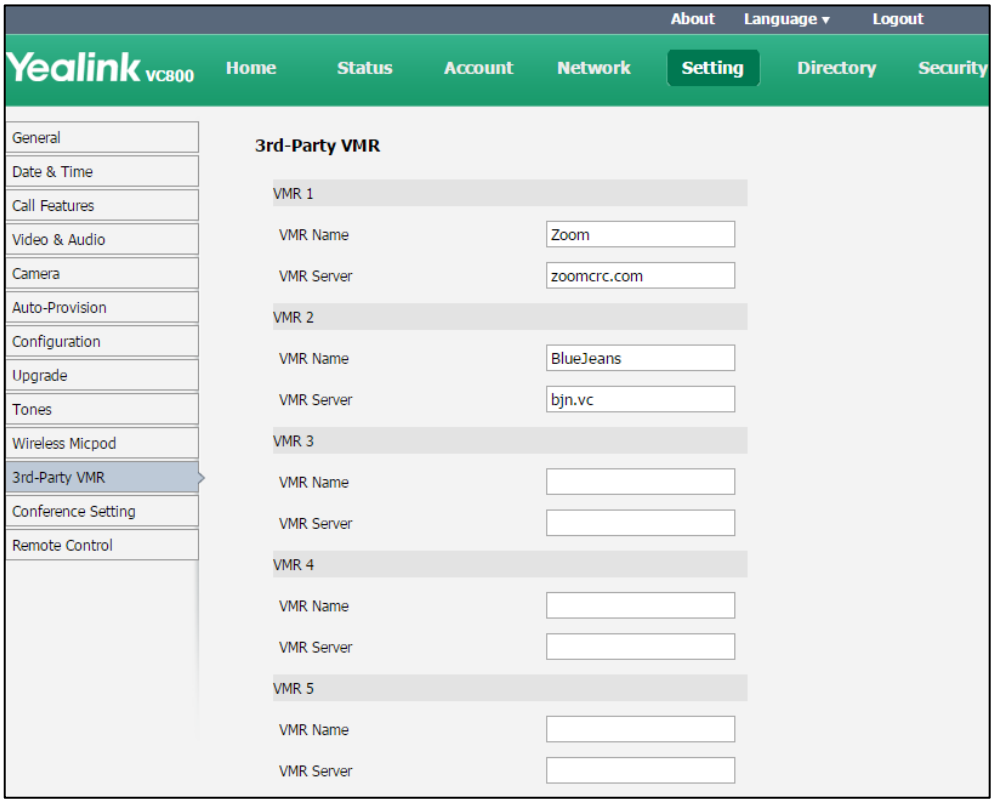
3rd-Party VMR parameters on the system are described below:

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

Parameter	Description	Configuration Method
	account/YMS account.	
VMR Server 3	Configures the virtual meeting room server address. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Name 4	Configures the virtual meeting room name. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Server 4	Configures the virtual meeting room server address. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Name 5	Configures the virtual meeting room name. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface
VMR Server 5	Configures the virtual meeting room server address. **Default**: Blank **Note:** It only works when you do not log into a Cloud platform, or you only register a Yealink Cloud account/YMS account.	Web User Interface

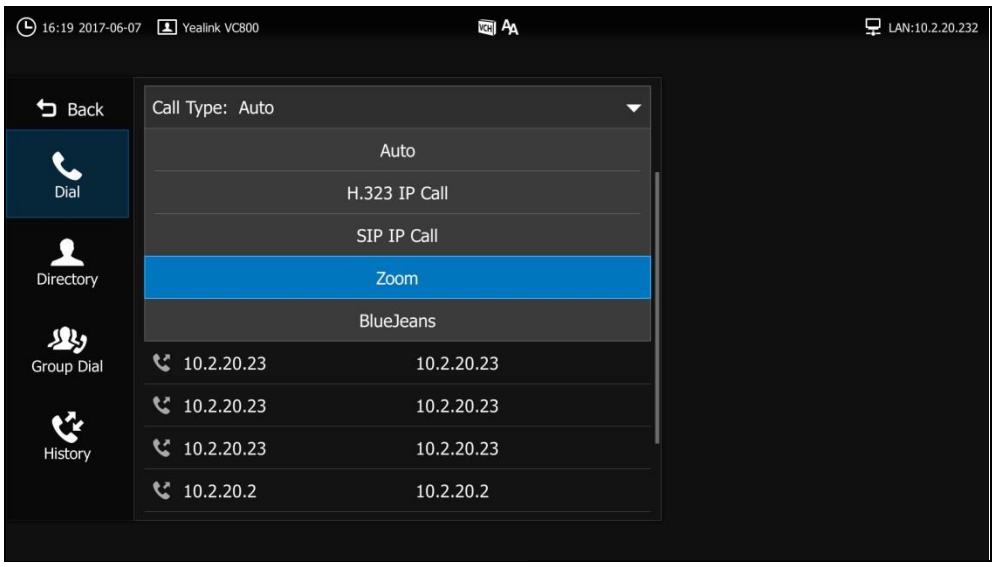
To configure the third-party virtual meeting room via web user interface:

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



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

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



For more information on how to use refer to *Yealink VC800&VC500 Full HD Video Conferencing System User Guide.*

DTMF

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

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

DTMF Keypad Frequencies:

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

Methods of Transmitting DTMF Digit

Three methods of transmitting DTMF digits on SIP calls:

- **RFC 2833** -- DTMF digits are transmitted by RTP Events compliant to RFC 2833.
- **INBAND** -- DTMF digits are transmitted in the voice band.
- **SIP INFO** -- DTMF digits are transmitted by SIP INFO messages.

The method of transmitting DTMF digits is configurable on a per-line basis.

RFC 2833

DTMF digits are transmitted using the RTP Event packets that are sent along with the voice path. These packets use RFC 2833 format and must have a payload type that matches what the other end is listening for. The default payload type for RTP Event packets is 101 and the payload type is configurable. The VC800/VC500 uses the configured value to negotiate with the other end during call establishment.

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

INBAND

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

SIP INFO

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

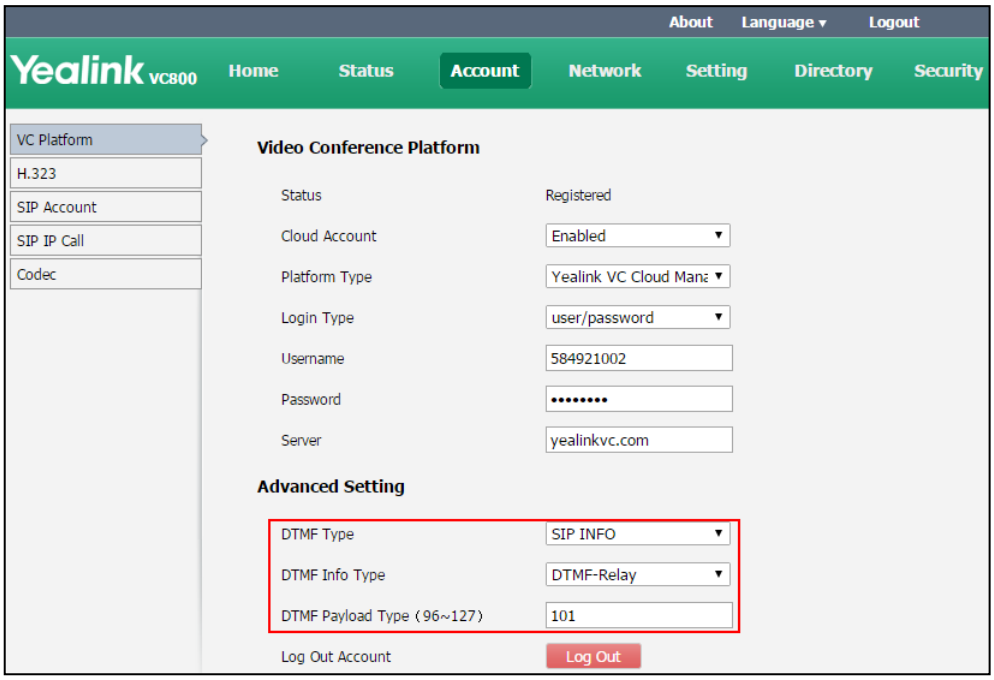
DTMF parameters on the system are described below:

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

Parameter	Description	Configuration Method
Type（96~127）	Cloud platform, SIP account or SIP IP call separately. **Default:** 101	

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

1. Click on **Account**->**VC Platform**.
2. Select the desired value from the pull-down list of **DTMF Type**.
3. If **SIP INFO** or **RFC2833+ SIP INFO** is selected, select the desired value from the pull-down list of **DTMF Info Type**.
4. Enter the desired value in the **DTMF Payload Type(96~127)** field.



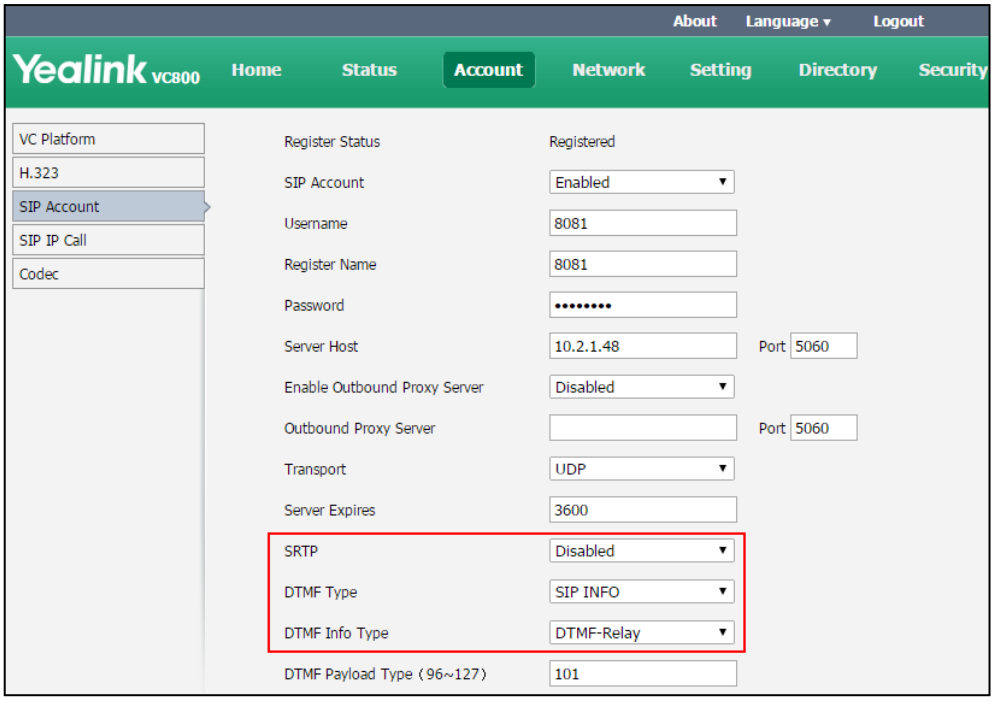
5. Click **Confirm** to accept the change.

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

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

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

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

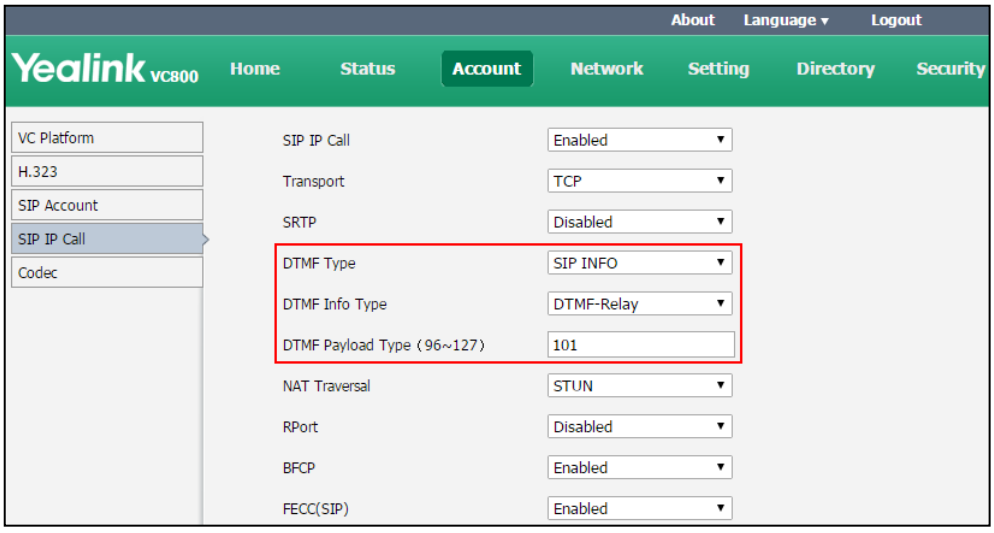


4. Click **Confirm** to accept the change.

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

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

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



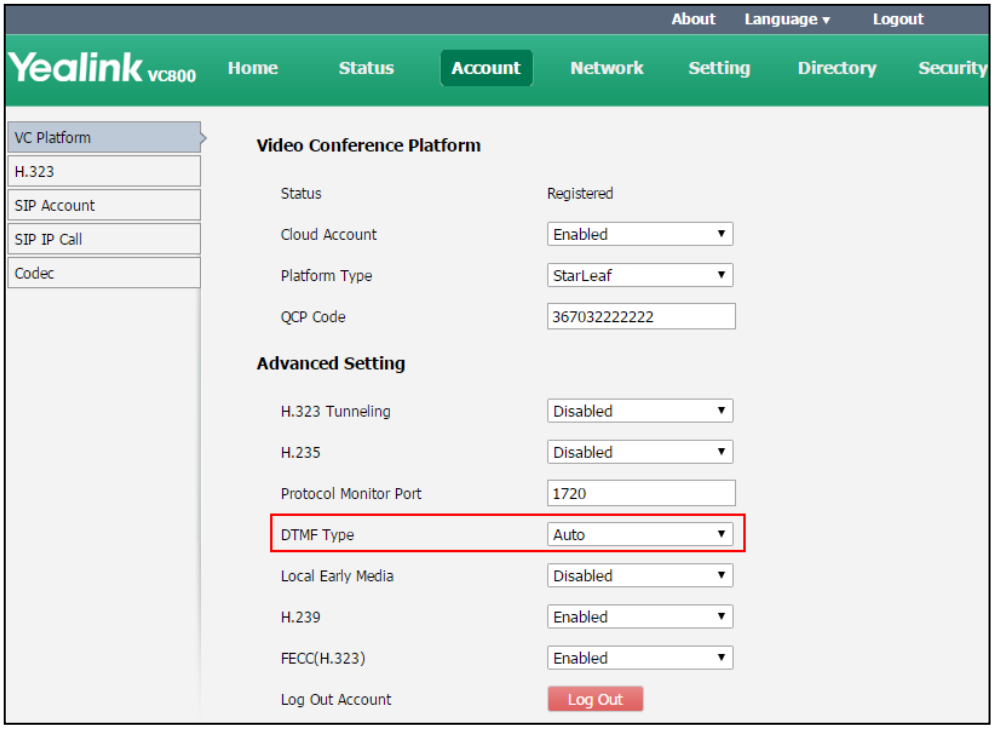
4. Click **Confirm** to accept the change.

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

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

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

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

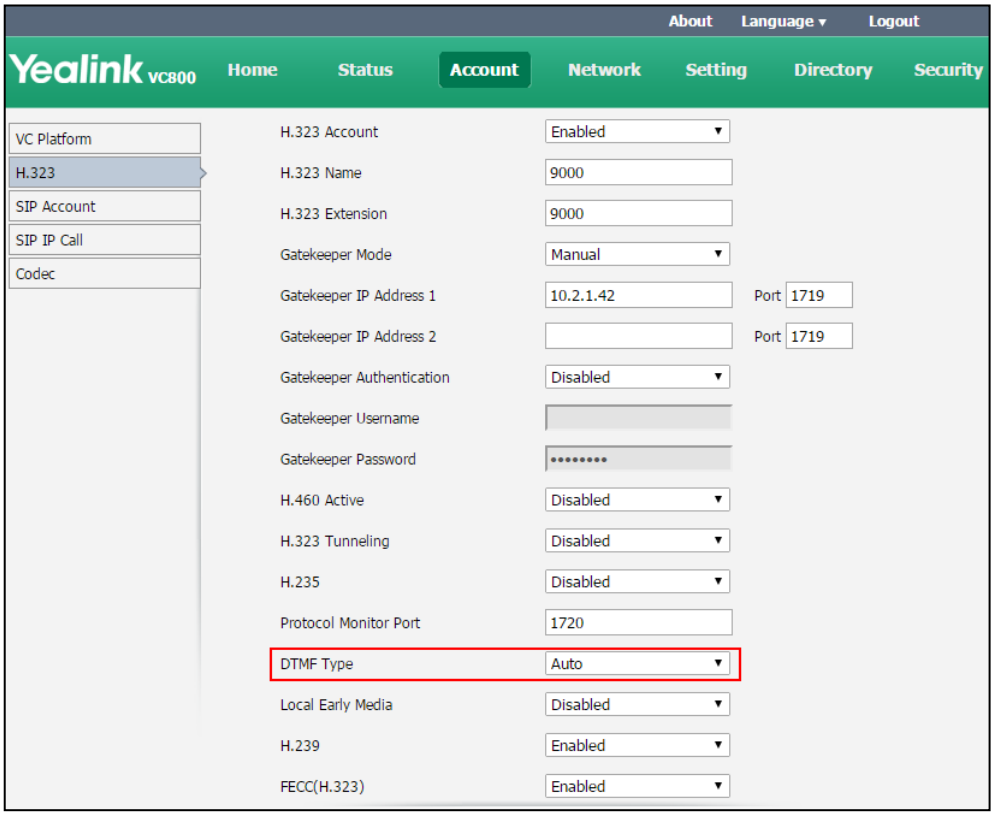


4. Click **Confirm** to accept the change.

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

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

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



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

Codecs

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

Audio Codecs

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

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

Codec	Algorithm	Bit Rate	Sample Rate	Reference
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
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	G.722.1	24 Kbps	16 or 32 Ksps	RFC 5577
G722	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

The Opus codec supports various audio bandwidths, defined as follows:

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

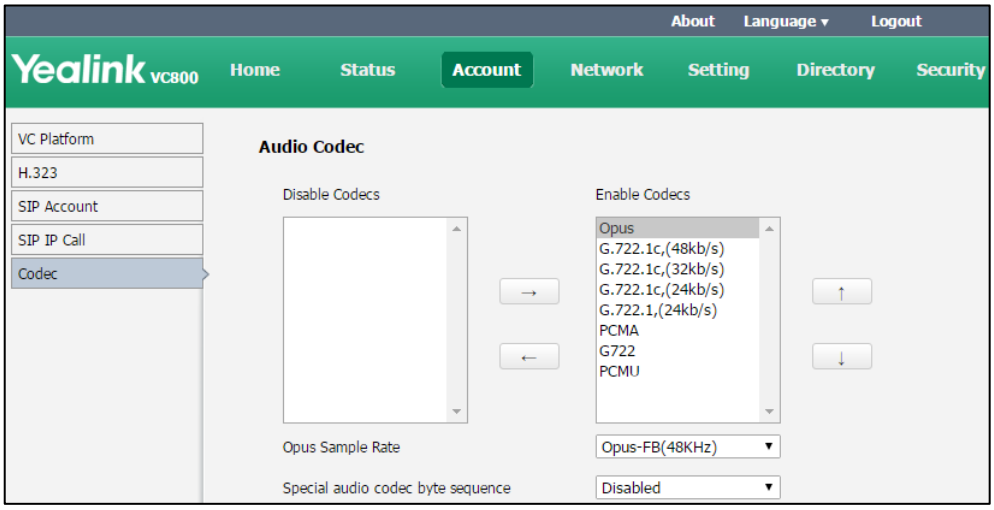
Audio codecs parameters on the system are described below:

Parameter	Description	Configuration Method
Enable Codecs	Specifies the audio codecs to be used. **Note:** All support audio codecs are enabled on the system by default.	Web User Interface
Disable Codecs	Specifies the audio codecs not to be used.	Web User Interface
Opus Sample Rate	Configures the sample rate of the opus audio codec.	Web User Interface

Parameter	Description	Configuration Method
Special audio codec byte sequence	Enables or disables the special audio codec byte sequence. • **Disabled**–the system maintains current byte sequence for audio codec. • **Enabled**–If you hear noise or you cannot hear voice during a call with a device of other vendor, it may be that your byte sequence of audio codec is contrary to another vendor, you can try to enable this feature to change the byte sequence of audio codec, so that this issue may be resolved. **Default:** Disabled	Web User Interface

To configure audio codecs via web user interface:

1. Click on **Account**->**Codec**.
2. Select the desired codec from the **Disable Codecs** or the **Enable Codecs** column.
3. Click ← or → to disable or enable the selected codec.
4. Select the desired audio codec from the **Enable Codecs** column, and click ↑ or ↓ to adjust the priority of the selected audio codecs.
5. Select the desired value from the pull-down list of **Opus Sample Rate**.
6. (Optional.)Select **Enabled** from the pull-down list of **Special audio codec byte sequence**.



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

Video Codecs

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

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

Name	MIME Type	Bit Rate	Frame Rate	Frame Size
H.264 High Profile	H264/90000	90 kbps to 2048 kbps	5 fps to 30 fps	Tx: 360P, 540P, 720P, 1080P Rx: Conventional Size Below 1080P
H.264	H264/90000			
H.263	H263/90000			Tx: CIF, 4CIF RX: QCIF, CIF, 4CIF
H265	H265/90000			Tx: 360P, 540P, 720P, 1080P Rx: Conventional Size Below 1080P

Note If you are using H.265 video codec during a two-way video calls, the system will negotiate to use H264 High profile video codec automatically when placing a new call.

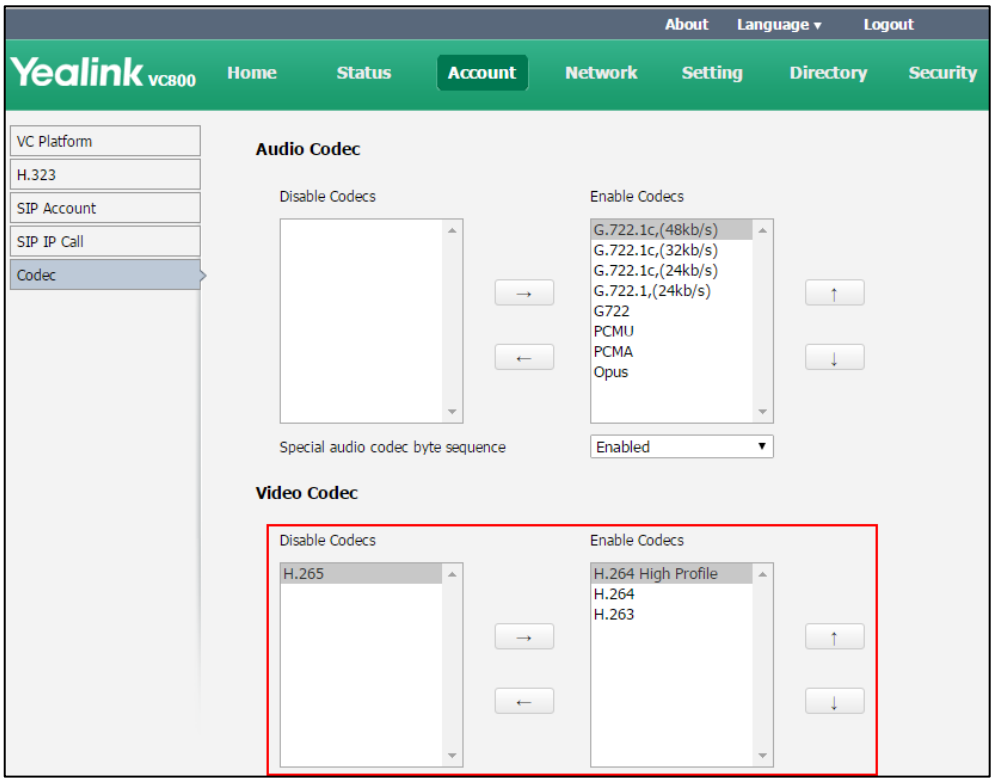
Video codecs parameters on the system are described below:

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

To configure video codecs via web user interface:

1. Click on **Account**->**Codec**.
2. Select the desired video codec from the **Disable Codecs** or the **Enable Codecs** column.
3. Click ← or → to disable or enable the selected video codec.

4. Select the desired video codec from the **Enable Codecs** column, and click ↑ or ↓ to adjust the priority of the selected video codecs.



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

Call Protocol

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

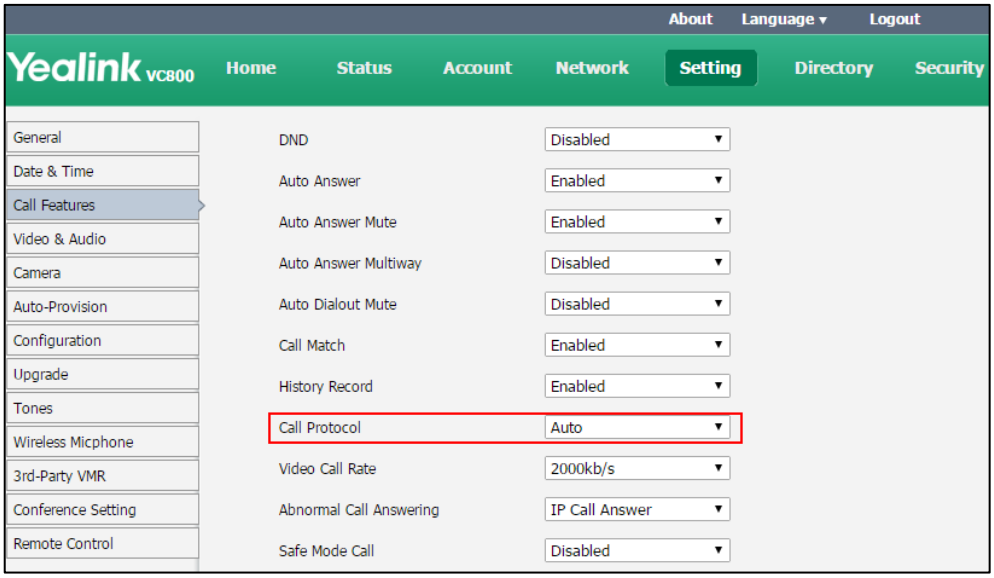
The call protocol parameter on the system is described below:

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

Parameter	Description	Configuration Method
	protocol for placing calls. **Default:** Auto	

To configure call protocol via web user interface:

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



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

To configure call protocol via the remote control:

1. Select **More**->**Setting**->**Call Features**->**Call Protocol**.
2. Select the desired value from the pull-down list of **Call Protocol**.
3. Select **Save**, and then press (OK) to accept the change.

Account Polling

The system can use different call type (**Cloud platform/H.323 account/SIP account/H.323 IP Call/SIP IP Call**) to dial a number when more than one account is registered.

The priority of call types is as follows:

- If you dial an account, the priority is: **Cloud platform>H.323 account>SIP account**.
- If you dial an IP address, the priority is: **H.323 IP Call**>**SIP IP Call**.

If account polling is disabled, the system will select the call type with the highest priority to place a call by default. In this situation, once the dialed number differs from the call type you are using, the call will fail. You can enable the account polling feature, the system can try each call type in order when dialing a number.

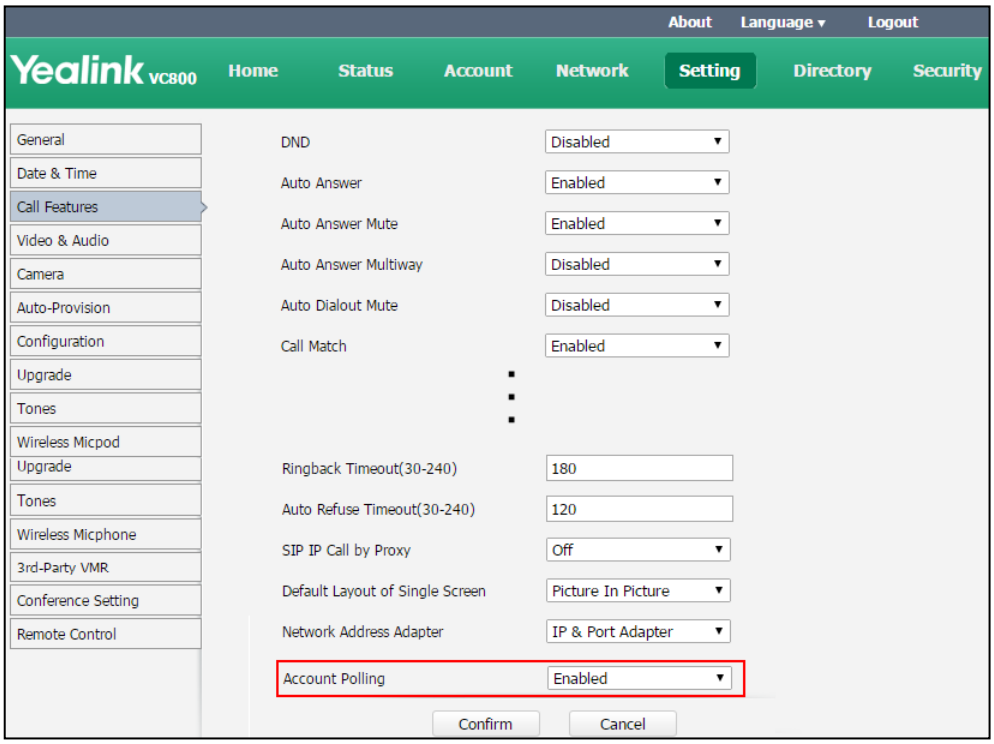
You can configure account polling feature via web user interface only.

Account polling parameter on the system is described below:

Parameter	Description	Configuration Method
Account Polling	Enables or disables the account polling on the system. • **Disabled**–the system dials a number using the call type with the highest priority. • **Enabled—**the system tries each call type in order to dial a number. **Default:** Enabled	Remote Control Web User Interface

To configure account polling via web user interface:

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



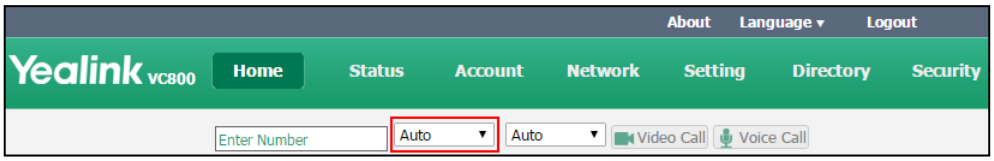
3. Click **Confirm** to accept the change.

The following example shows an example.

Scenario:

1. System A is registered with a Yealink Cloud account and a SIP account.

2. On system A, select **Auto** from the pull-down list before calling.



3. On system A, dial the number of system B.

Result:

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

Conference Management

Conference Type

VC800/VC500 video conferencing system can act as a virtual meeting room, so that other devices can dial the VC800/VC500 video conferencing system to join a meeting.

VC500 video conferencing endpoint and VC800 video conferencing system without a multipoint license can host a **Regular Mode** conference only.

VC800 video conferencing system with a multipoint license can host a **Regular Mode** conference or a **VMR Mode** conference.

Regular Mode Conference

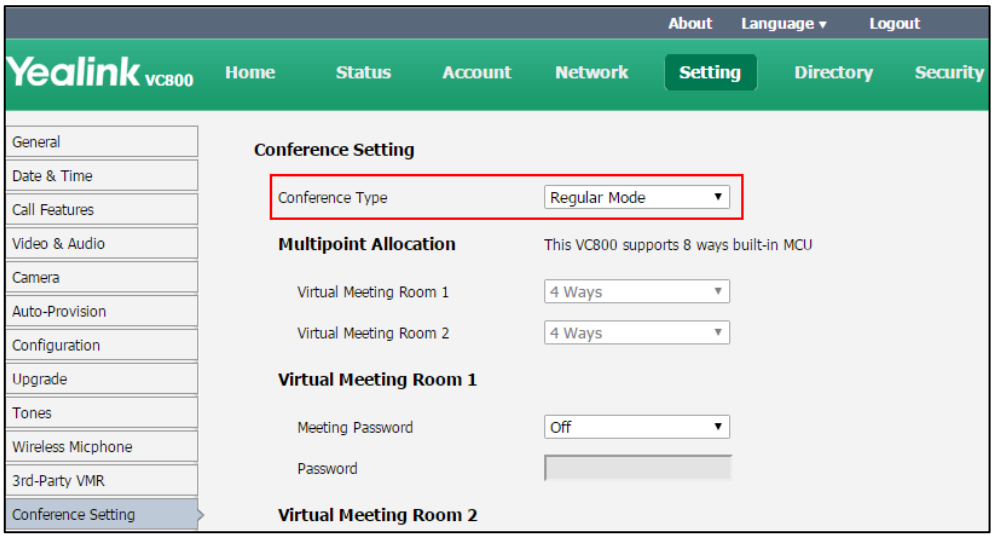
In **Regular Mode** conference, when participants call the moderator (MCU provider), the moderator will join the meeting.

The regular mode conference parameter on the system is described below:

Parameter	Description	Configuration Method
Conference Type	Specifies the conference type. • **Regular Mode** • **VMR Mode** **Default:** Regular Mode	Web User Interface

To configure regular mode conference via web user interface:

1. Click on **Setting**->**Conference Setting**.
2. Select **Regular Mode** from the pull-down list of **Conference Type**.



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

Note

For VC500 and VC800 that has no multipoint license, the regular mode conference supports up to one video call and 5 voice calls (a conference moderator and 6 participants).

For VC800 with a multipoint license, the number of participants depends on the multipoint license you imported. For more information, refer to Multipoint License on page 209.

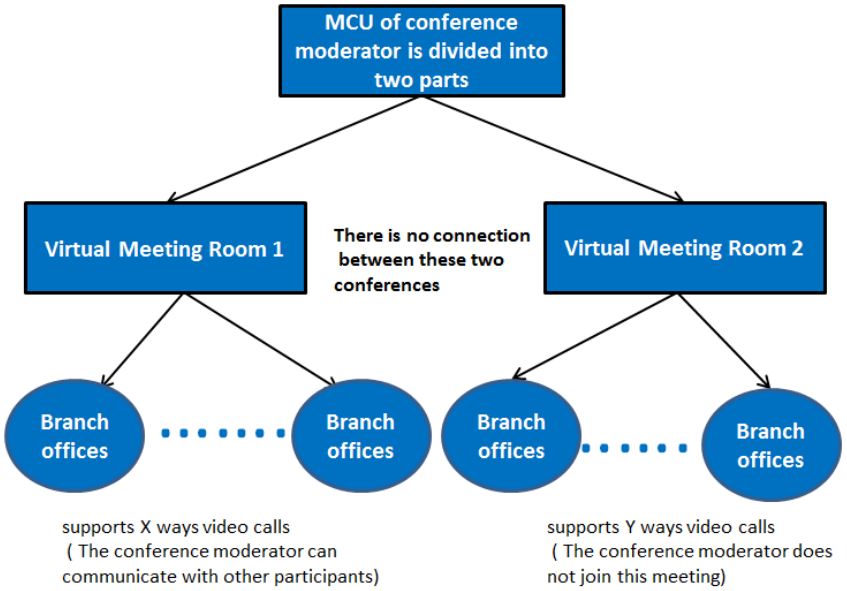
VMR Mode Conference

VMR mode conference is only applicable to VC800 video conferencing system. It is not applicable to VC500 video conferencing endpoint.

In VMR mode conference, the MCU of moderator can be used to host two independent conferences (corresponding to virtual meeting room 1 and virtual meeting room 2).

- Virtual meeting room 1: when participants call the virtual meeting room 1, the moderator will join the meeting.

- Virtual meeting room 2: when participants call the virtual meeting room 2, only participants join the meeting, the moderator does not join the meeting.



If you import a multipoint license to the VC800 system, you can allocate the MCU ways between two virtual meeting rooms.

- If you import an 8 ways multipoint license to the VC800 system, X+Y<=8. Two virtual meeting rooms supports up to 8 ways video calls.
- If you import a 16 ways multipoint license to the VC800 system, X+Y<=16. Two virtual meeting rooms supports up to 16 ways video calls.
- If you import a 24 ways multipoint license to the VC800 system, X+Y<=24. Two virtual meeting rooms supports up to 24 ways video calls.

Note When you import an 8 or 16 ways multipoint license to the VC800 system, the virtual meeting room 1 provides additional 5 voice calls.

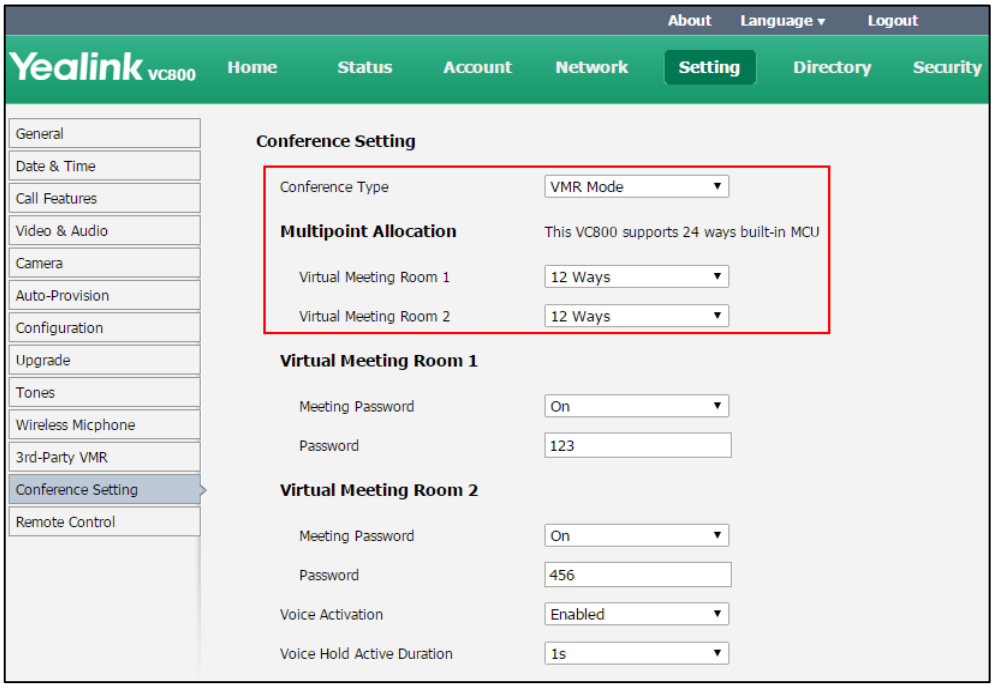
The VMR mode conference parameters on the system are described below:

Parameter	Description	Configuration Method
Conference Type	Specifies the conference type. • **Regular Mode** • **VMR Mode** **Default:** Regular Mode	Web User Interface
Multipoint Allocation ->Virtual Meeting Room 1	Allocates the maximum ways of video calls for virtual meeting room 1.	Web User Interface

Parameter	Description	Configuration Method
Multipoint Allocation ->Virtual Meeting Room 2	Allocates the maximum ways of video calls for virtual meeting room 2.	Web User Interface

To configure VMR mode conference via web user interface:

1. Click on **Setting**->**Conference Setting**.
2. Select **VMR Mode** from the pull-down list of **Conference Type**.
3. Select maximum ways of video calls from the pull-down list of **Virtual Meeting Room 1**.
4. Select maximum ways of video calls from the pull-down list of **Virtual Meeting Room 2**.



By default, the MCU are distributed equally between two virtual meeting rooms.

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

For more information on how to join a VMR mode conference, refer to Joining the Meeting on page 113.

Meeting Password

Depending on how a conference call is set up, you might be required to enter a meeting password to join the call. You can also require far-end systems to enter a meeting password to prevent unauthorized participants from joining conference calls hosted by your system.

If you host a regular mode conference, you need to configure a password for virtual meeting room 1. If you host a VMR mode conference, you need to configure passwords for virtual meeting room 1 and virtual meeting room 2 respectively.

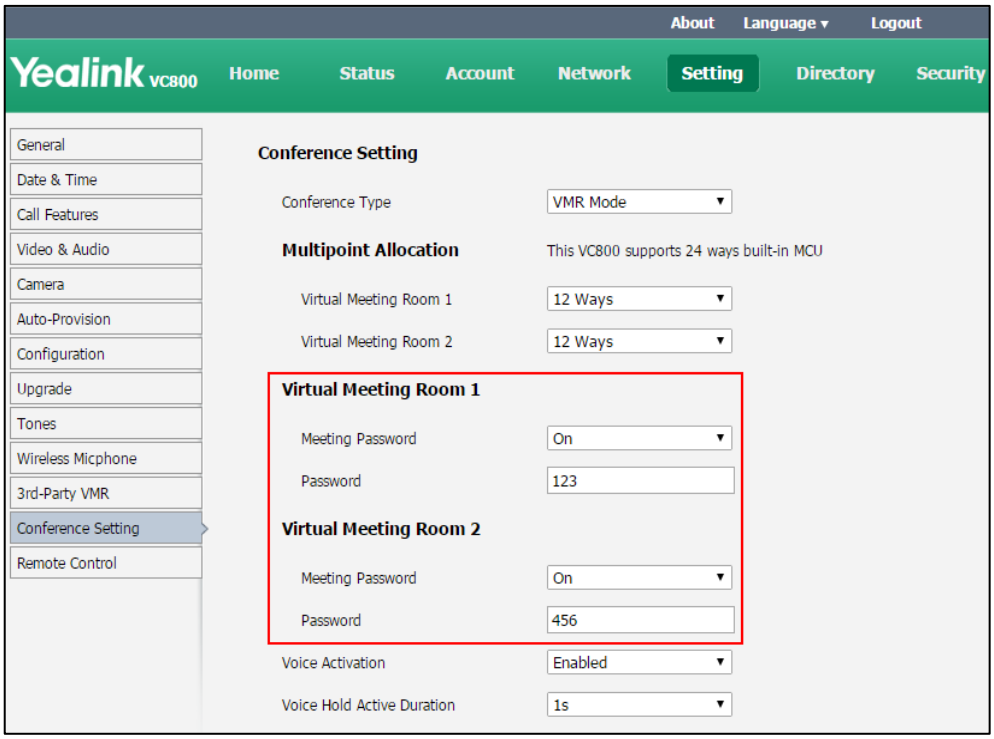
The meeting password parameter on the system is described below:

Parameter	Description	Configuration Method
Virtual Meeting Room 1->Meeting Password	Enables or disables the system to configure a password for virtual meeting room1. • **On** • **Off** **Default:** Off	Web User Interface
Virtual Meeting Room 1->Meeting Room 1Password	Configures the password for virtual meeting room 1.	Web User Interface
Virtual Meeting Room 2->Meeting Password	Enables or disables the system to configure a password for virtual meeting room 2. • **On** • **Off** **Default:** Off	Web User Interface
Virtual Meeting Room 2->Password	Configures the password for virtual meeting room 2.	Web User Interface

To set up a meeting password via web user interface:

1. Click on **Setting**->**Conference Setting**.
2. Select **On** from the pull-down list of **Meeting Password**.

3. Enter meeting password in the **Password** field.



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

Joining the Meeting

Participants can dial **IP##meeting password** or **meeting password@IP** to enter the virtual meeting room.

For example:

- The IP address of moderator is 10.3.6.201.
- 123 is meeting password for virtual meeting room 1.
- 456 is meeting password for virtual meeting room 2.

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.

Meeting Whitelist

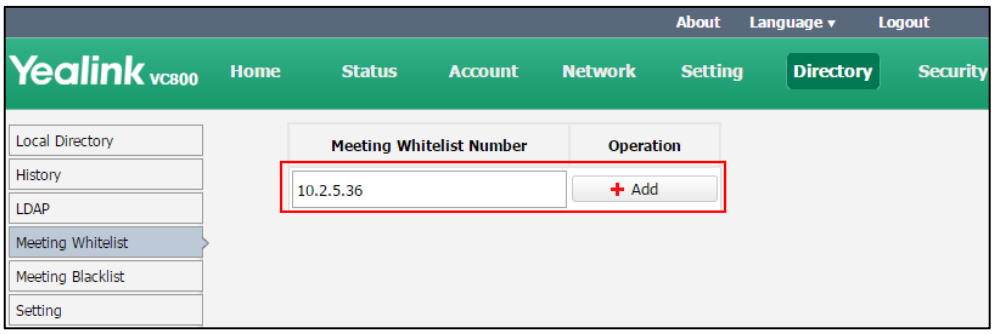
You can add the IP address, account or domain name of the remote system to the meeting whitelist. Users in the whitelist can join your conference call directly without meeting password even if you have enabled the meeting password feature. VC800/VC500 video conferencing system supports up to 100 whitelist records. Meeting whitelist is configurable via web user interface only.

The meeting whitelist parameter on the system is described below:

Parameter	Description	Configuration Method
Meeting White list Number	Add the IP address, account or domain name of the remote system to the meeting whitelist. **Default:** blank	Web User Interface

To add the meeting whitelist numbers via web user interface:

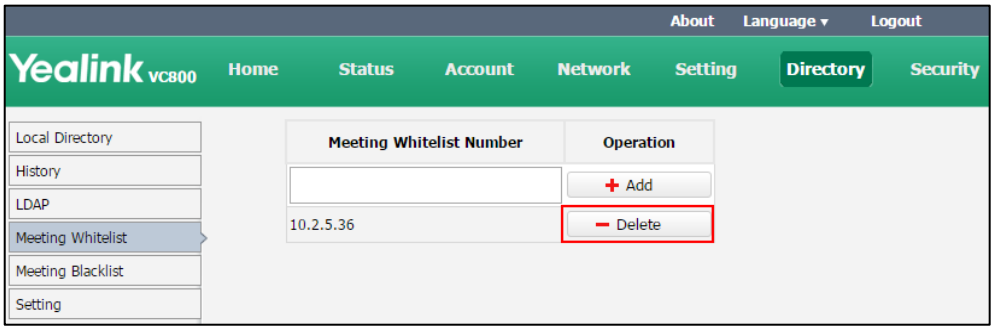
1. Click on **Directory**->**Meeting Whitelist**.
2. Enter the user's IP, account or domain name in the **Meeting Whitelist Number** field.



3. Click **Add**.
4. Repeat step 2-3 to add more numbers to the meeting whitelist.

To delete the meeting whitelist numbers via web user interface:

1. Click on **Directory**->**Meeting Whitelist.**
2. Click **Delete** beside the numbers that you want to delete.



The web user interface prompts the message "Warning: Are you sure delete the white number?".

3. Click **Confirm**.

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.

Meeting Blacklist

You can add the IP address, account or domain name of the remote system to the meeting blacklist. VC800/VC500 will refuse incoming calls from the blacklist automatically. VC800/VC500 will not remind incoming calls and save call history from blacklist.

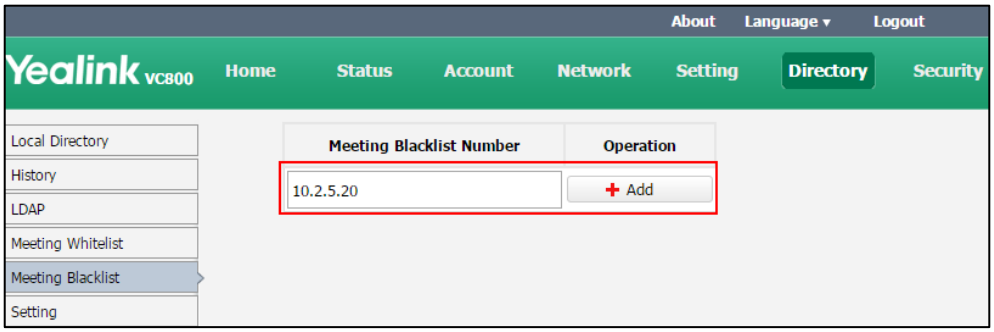
VC800/VC500 supports up to 100 blacklist records. Blacklist is configurable via web user interface only.

The meeting blacklist parameter is described below:

Parameter	Description	Configuration Method
Meeting Blacklist Number	Add the IP address, account or domain name of the remote system to the meeting blacklist. **Default:** blank	Web User Interface

To add the blacklist numbers via web user interface:

1. Click on **Directory**->**Meeting Blacklist**.
2. Enter the user's IP address, account or domain name in the **Meeting Blacklist Number** field.

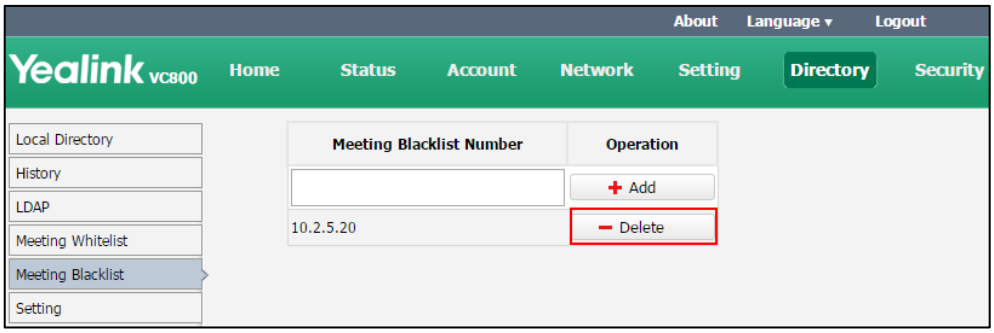


3. Click **Add**.
4. Repeat step 2-3 to add more numbers to the meeting blacklist.

To delete the blacklist numbers via web user interface:

1. Click on **Directory**->**Meeting Blacklist.**

2. Click **Delete** beside the numbers that you want to delete.



The web user interface prompts the message "Warning: Are you sure delete the black number?".

3. Click **Confirm**.

Voice Activation

Voice activation is only applicable to VC800 system with a multipoint license. It is not applicable to VC500 endpoint.

Voice activation displays the active speaker in largest pane. Other participants are displayed in a strip beside the active speaker. To minimize the changes in the layout, when a new speaker is identified, the previous speaker is replaced by the new speaker.

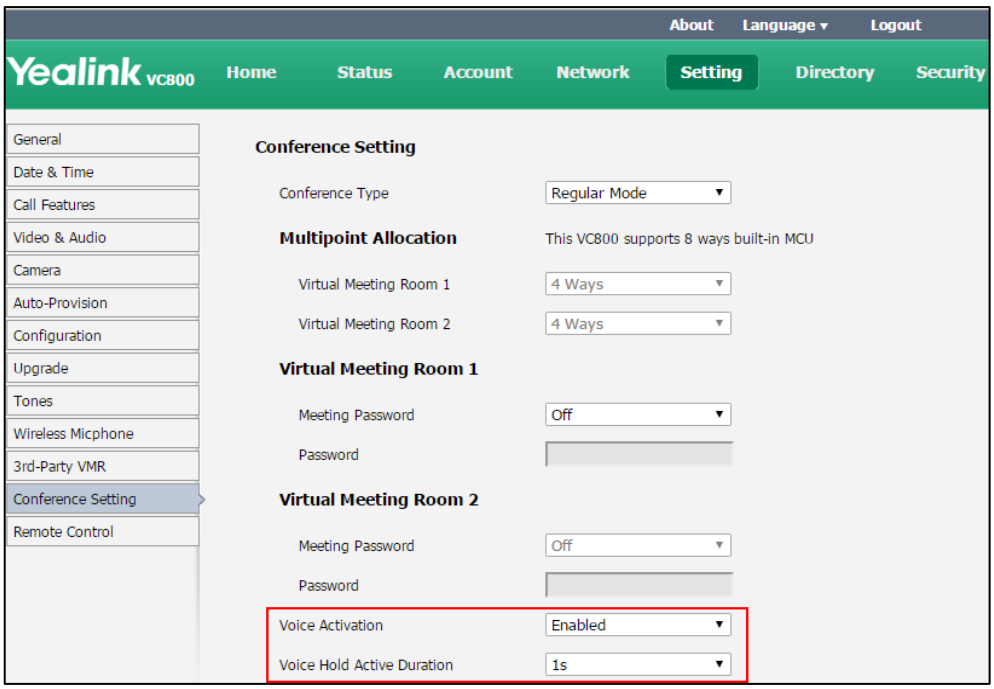
The voice activation parameter is described below:

Parameter	Description	Configuration Method
Voice Activation	Enables or disables voice activation. **Default**: Enabled	Web User Interface
Voice Hold Active Duration	Configures the voice activation interval. If voice duration of the new speaker is greater than the interval, the previous speaker is replaced by the new speaker. **Default**: 1s.	Web User Interface

To configure the voice activation via web user interface:

1. Click on **Setting**->**Conference Setting**.
2. Select the desired value from the pull-down list of **Voice Activation**.

3. Select the desired value from the pull-down list of **Video Hold Active Duration**.



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

Note Voice activation takes effect only when there are more than two participants in a conference call.

View Switching

View switching is only applicable to VC800 system with a multipoint license. It is not applicable to VC500 endpoint).

View switching enables to switch video images on the display device automatically. The switching 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 **Equal N×N** layout. When the number of participants exceeds 9, all participants' video images will be switched automatically.

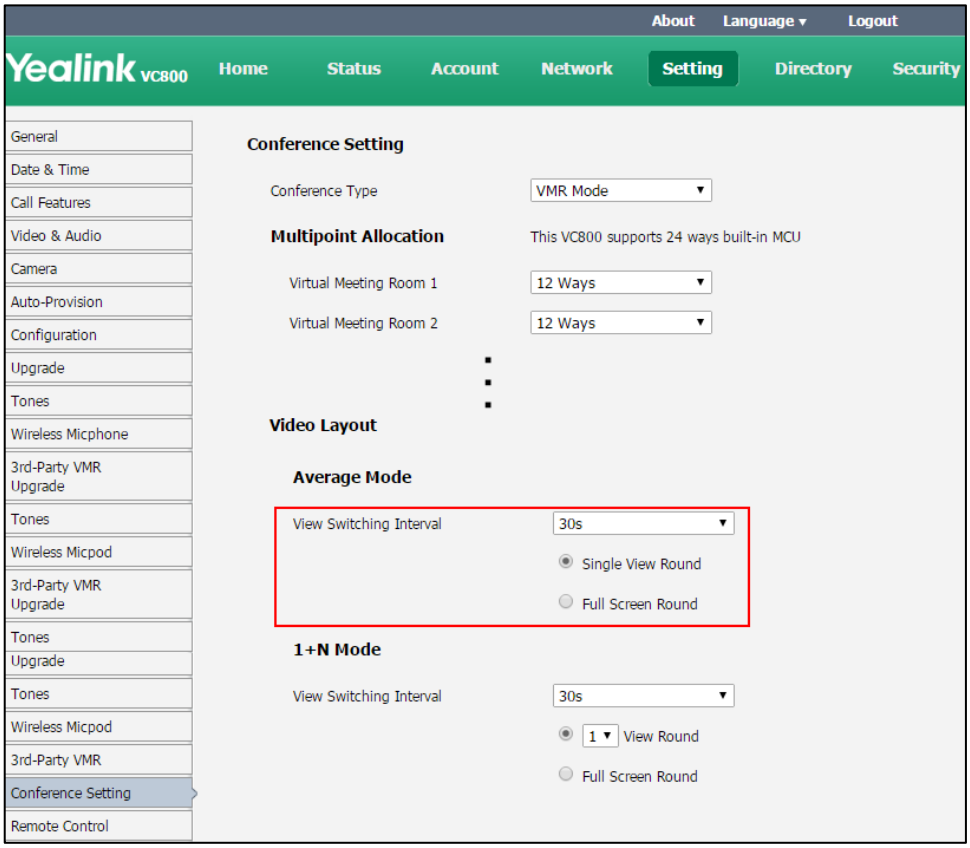
The view switching parameter is described below:

Parameter	Description	Configuration Method
View Switching Interval	Configures the view switching interval. **Default**: 30s. The video images will be switched	Web User Interface

Parameter	Description	Configuration Method
	automatically every 30 seconds.	
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

To configure view switching via web user interface:

1. Click on **Setting**->**Conference Setting**.
2. In the **Average Mode** field, select the desired value from the pull-down list of **View Switching Interval**.
3. Do one of the following:
   - Mark the **Single View Round** radio box.
   - Mark the **Full Screen Round** radio box.



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

Note

In **Equal N×N** layout, video image of the active speaker is indicated by an orange border.

If you share content in **Equal N×N** layout, 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 **Speaker View** layout and **OnePlusN** layout. When the number of participants exceeds 8, all participants' video images (except the active speaker) will be switched automatically.

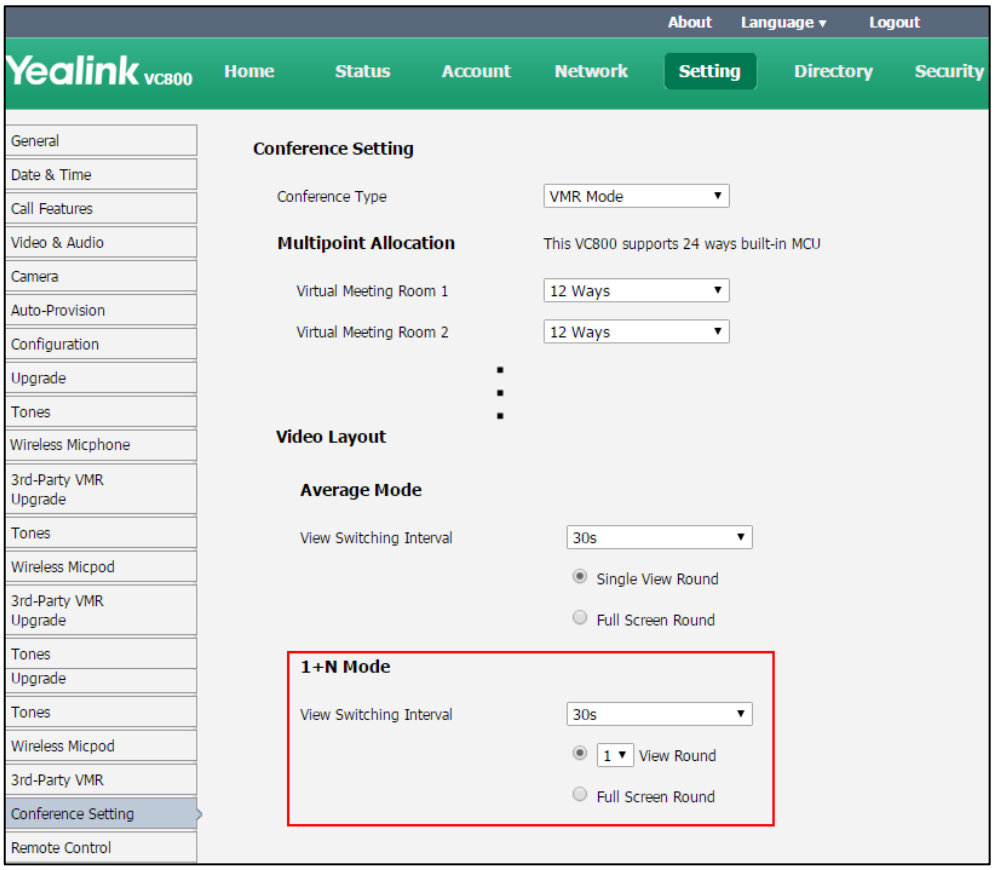
The view switching parameter is described below:

Parameter	Description	Configuration Method
View Switching Interval	Configures the view switching interval. **Default**: 30s. The video images will be switched automatically every 30 seconds.	Web User Interface
View Round	Configure how many video images to be switched at a time**.** **Valid values:** 1 to 7 **Default:** 1	Web User Interface
Full Screen Round	Switches all video images at a time.	Web User Interface

To configure view switching via web user interface:

1. Click on **Setting**->**Conference Setting**.
2. In the **1+N Mode** field, select the desired value from the pull-down list of **View Switching Interval**.
3. Do one of the following:
   - Select the desired value from the pull-down list of **View Round**.

- Mark the **Full Screen Round** radio box.



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

Note If you share content in **Speaker View** layout and **OnePlusN** layout, 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.

Default Layout of Single Screen

When only one display device is connected to the VC800/VC500 codec (single screen), you can configure the default layout when a call is established.

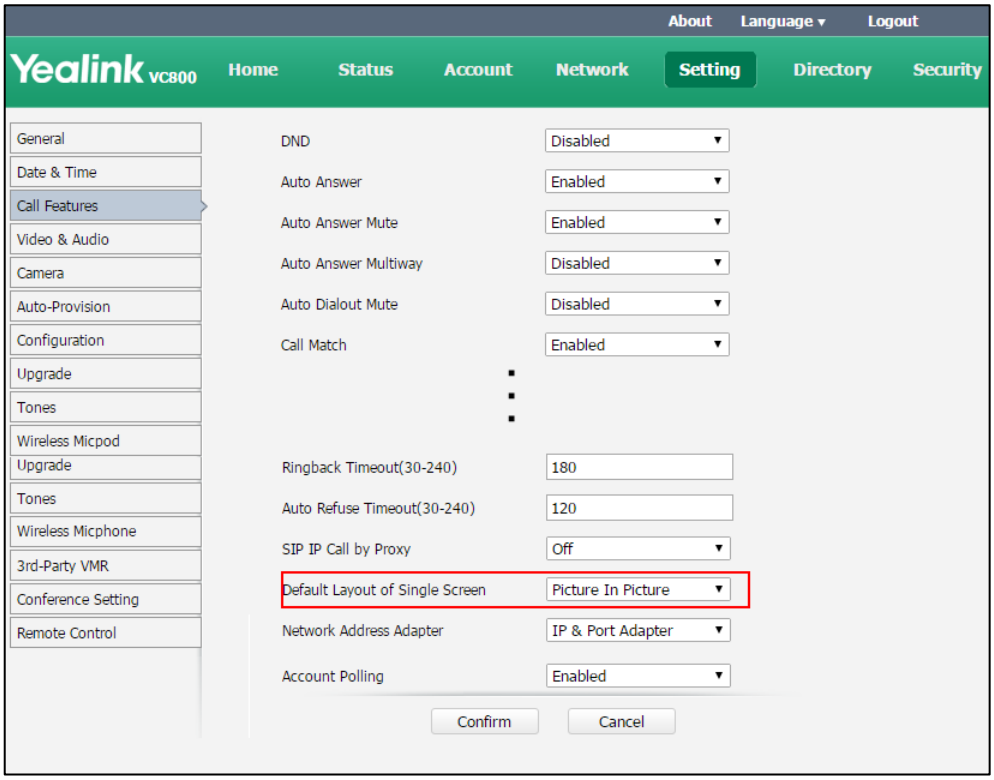
The parameters of default layout are described below:

Parameter	Description	Configuration Method
Default Layout of Single Screen	Configures the default layout of single screen when a call is established. • **Remote big Local small** • **Remote Full screen**	Web User Interface

Parameter	Description	Configuration Method
	• **Equal** • **Picture In Picture** **Default:** Picture In Picture If it is set to Remote big Local small, the remote video image is shown in big size, and the local video image below is shown in small size. If it is set to Remote Full screen, the remote video image is shown in full size. If it is set to Equal, the remote and local video images are shown in the same size. If it is set to Picture In Picture, the remote video image is shown in full screen, and local video image is shown in the PIP (Picture-in-Picture)	

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

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



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

Do Not Disturb

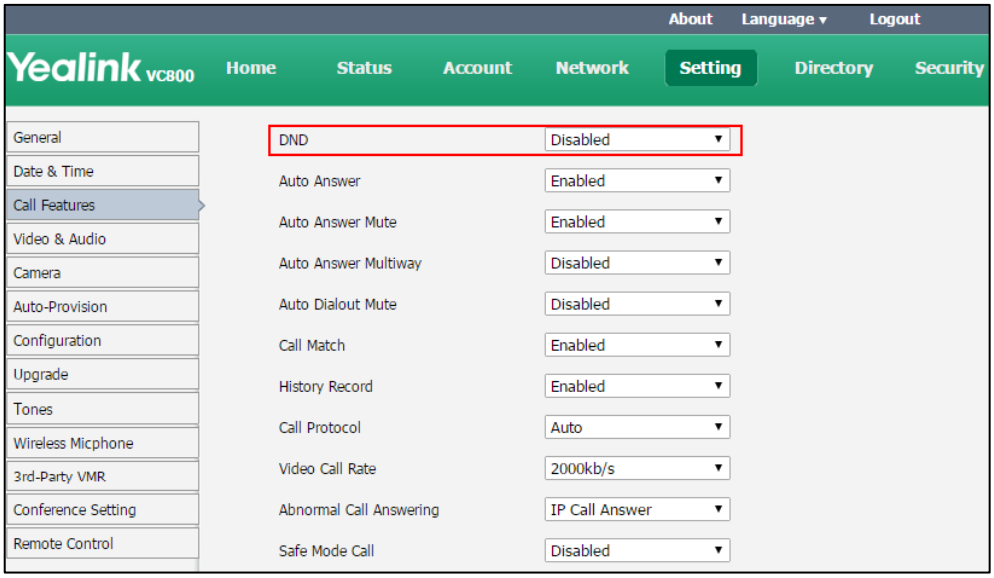
Do not Disturb allows the system to reject all incoming calls automatically. You can activate the DND mode for the system when it is idle, and the DND mode will be deactivated after the system places a call. You can also activate the DND mode for the system during a call, and the DND mode will be deactivated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

The DND parameter on the system is described below:

Parameter	Description	Configuration Method
DND	Enables or disables DND mode on the system. **Default:** Disabled	Remote Control Web User Interface CP960 conference phone

To configure DND via web user interface when the system is idle:

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



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

   If **Enabled** is selected, the display device will display  .

To configure DND via the remote control when the system is idle:

1. Select **More**->**Setting**->**Call Features**.
2. Check the **DND** checkbox.
3. Select **Save**, and then press OK to accept the change.

   The display device will display  .

To enable the DND mode via the CP960 conference phone when the system is idle:

1. Swipe down from the top of the screen.
2. Tap to enable DND.

   If the DND feature is enabled, the touch screen prompts " DND mode is enabled".

To configure DND during a call via web user interface:

1. Click **Home**.
2. Check the **DND** checkbox.

   The display device will display .

To configure DND during a call via the remote control:

1. Press or to open **Talk Menu**.
2. Press or to scroll to **DND** and then press .
3. Press to return.

   The display device will display .

To configure DND during a call via the CP960 conference phone:

1. Tap during a call to enable DND.

   The icon will appear on the status bar of touch screen.
2. Tap during a call to disable DND.

Auto Answer

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

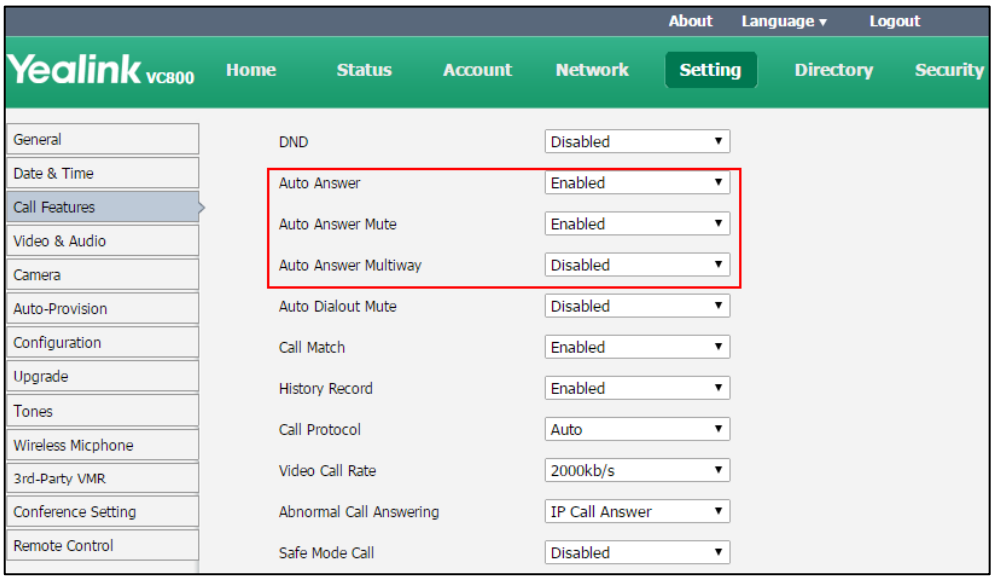
Auto answer parameters on the system are described below:

Parameter	Description	Configuration Method
Auto Answer	Enables or disables the auto answer feature on the system. **Default:** Enabled	Remote Control Web User Interface CP960 conference phone
Auto Answer Mute	Enables or disables the local microphone to be muted when an incoming call is answered automatically. **Default:** Enabled	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Auto answer mute feature is configurable only when the auto answer is enabled.	
Auto Answer Multiway	Enables or disables the system to automatically answer the incoming multipoint call. **Default:** Disabled The auto answer multiway feature is available only when the auto answer is enabled.	Remote Control Web User Interface

To configure auto answer via web user interface:

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



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

   If **Enabled** is selected, the display device will display AA .

To configure auto answer via the remote control:

1. Select **More**->**Setting**->**Call Features**.
2. Check the **Auto Answer** checkbox.
3. Check the **Auto Answer Mute** checkbox.
4. Check the **Auto Answer Multiway** checkbox.
5. Select **Save**, and then press (OK) to accept the change.

The display device will display .

To configure auto answer via the CP960 conference phone:

1. Swipe down from the top of the screen.
2. Tap to enable or disable auto answer.

   If the auto answer feature is enabled, the icon will appear on the status bar of the touch screen.

Auto Dialout Mute

The auto dialout mute feature allows the system to turn off the microphone after the other party answers your call, so that the other party cannot hear you.

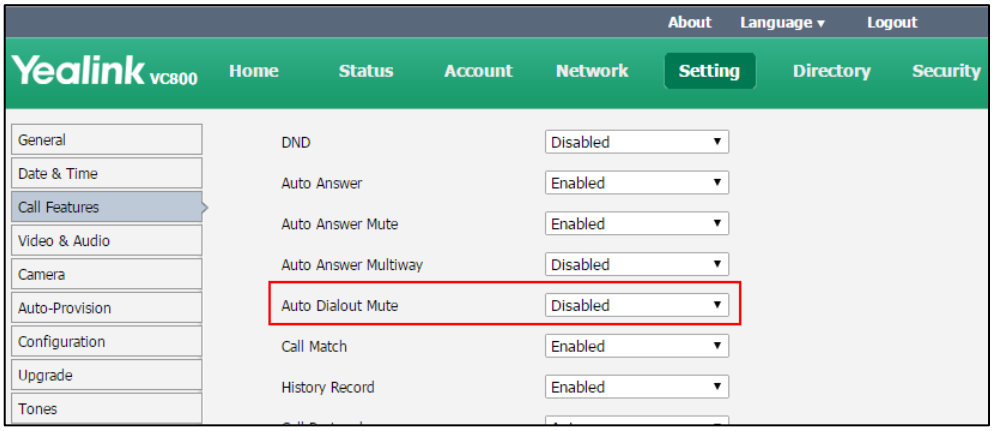
Note The system is still muted after you hang up.

Auto dialout mute parameter on the system is described below:

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

To configure auto dialout mute feature via web user interface:

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



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

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

Call Match

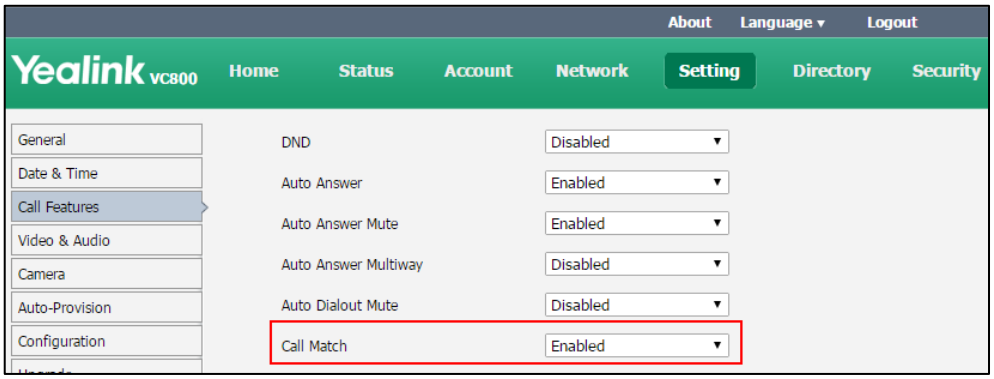
The call match feature allows the system to search for entries automatically from the search source list based on the entered string. Once matched, the results will be displayed on the screen. If no list is added to the search source list, the system will not perform a search even if call match is enabled. For more information on how to search source list in dialing, refer to Search Source List in Dialing on page 207 .

Parameter of call match on the system is described below:

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

To configure call match via web user interface:

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



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

To configure call match via the remote control:

1. Select **More**->**Setting**->**Call Features**.
2. Check the **Call Match** checkbox.
3. Press  to exit.

History Record

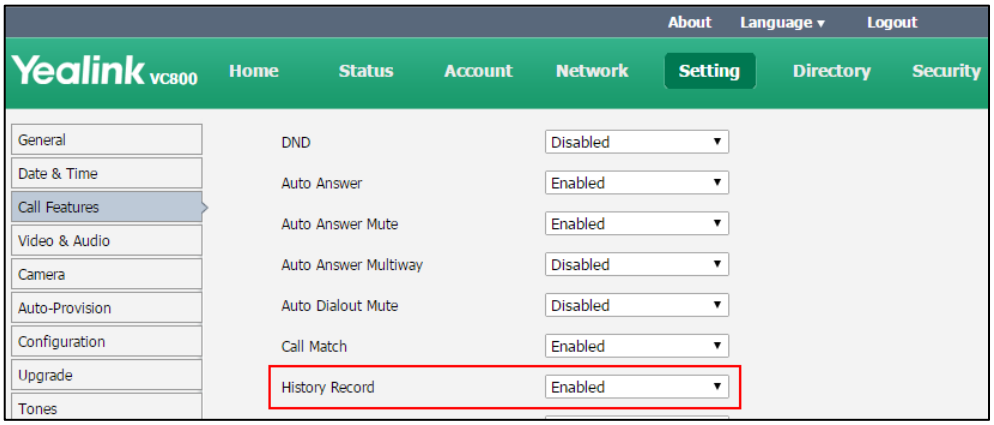
The system maintains a local call history, which contains call information such as remote party identification, time and date, and call duration. Users can manage call history list via the remote control, web user interface and CP960 conference phone. To save call history, you must enable the history record feature on the system in advance. If history record feature is disabled, the system will not save call log and prompt the missed call.

The history record parameter on the system is described below:

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

To configure history record via web user interface:

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



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

To configure history record via the remote control:

1. Select **More**->**Setting**->**Call Features**.
2. Check the **History Record** checkbox.
3. Press  to exit.

Ringback Timeout

Ringback timeout defines a specific period of time within which the VC800/VC500 video conferencing system will cancel the dialing if the call is not answered.

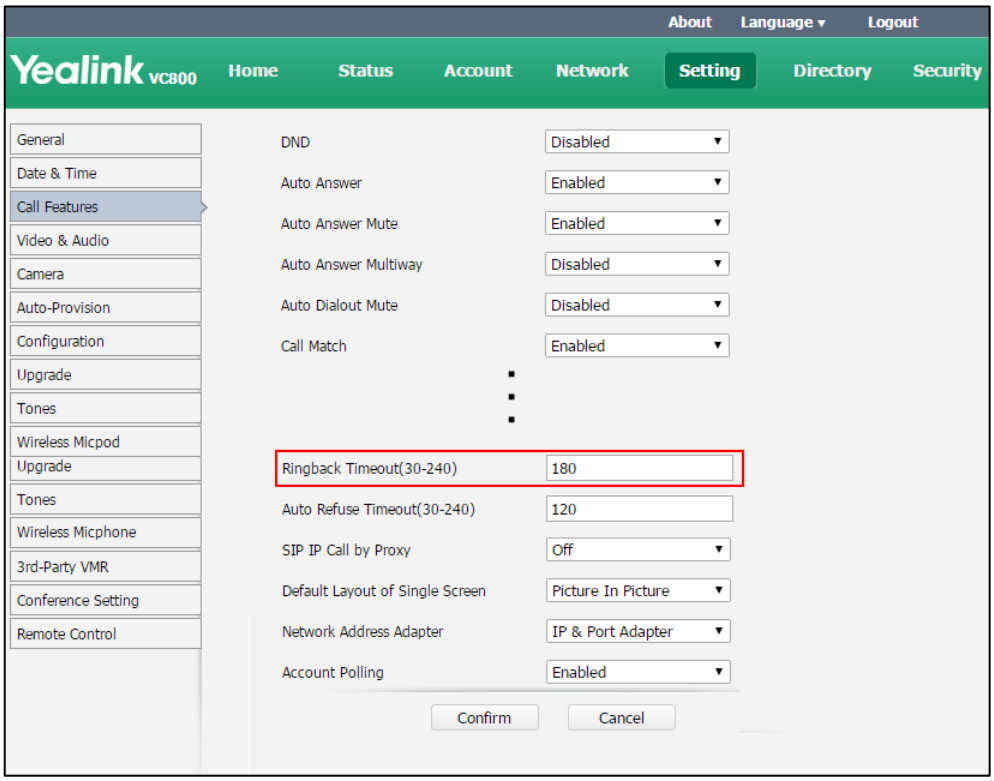
The ringback timeout parameter on the system is described below:

Parameter	Description	Configuration Method
Ringback Timeout (30-240)	Configures the duration time (in seconds) in the ringback state. **Default:** 180 If it is set to 180, the system will cancel the dialing if the call is not	Web User Interface

Parameter	Description	Configuration Method
	answered within 180s.	

To configure ringback timeout via web user interface:

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



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

Auto Refuse Timeout

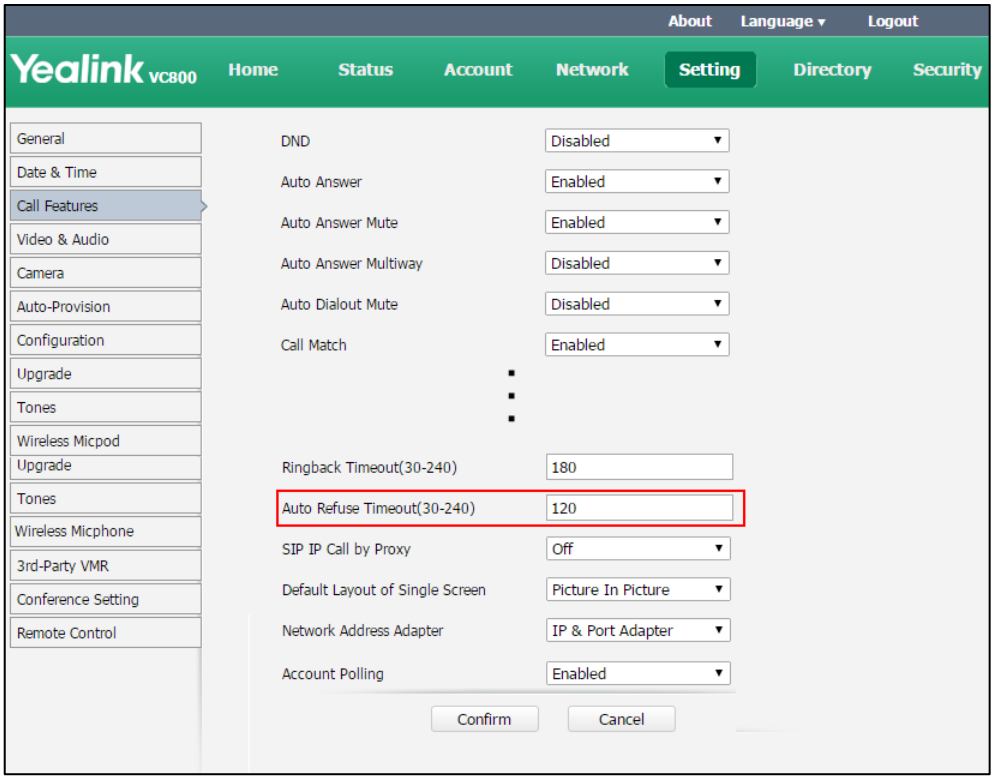
Auto refuse timeout defines a specific period of time within which the video conferencing system will stop ringing if the call is not answered.

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

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

To configure auto refuse timeout via web user interface:

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



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

SIP IP Call by Proxy

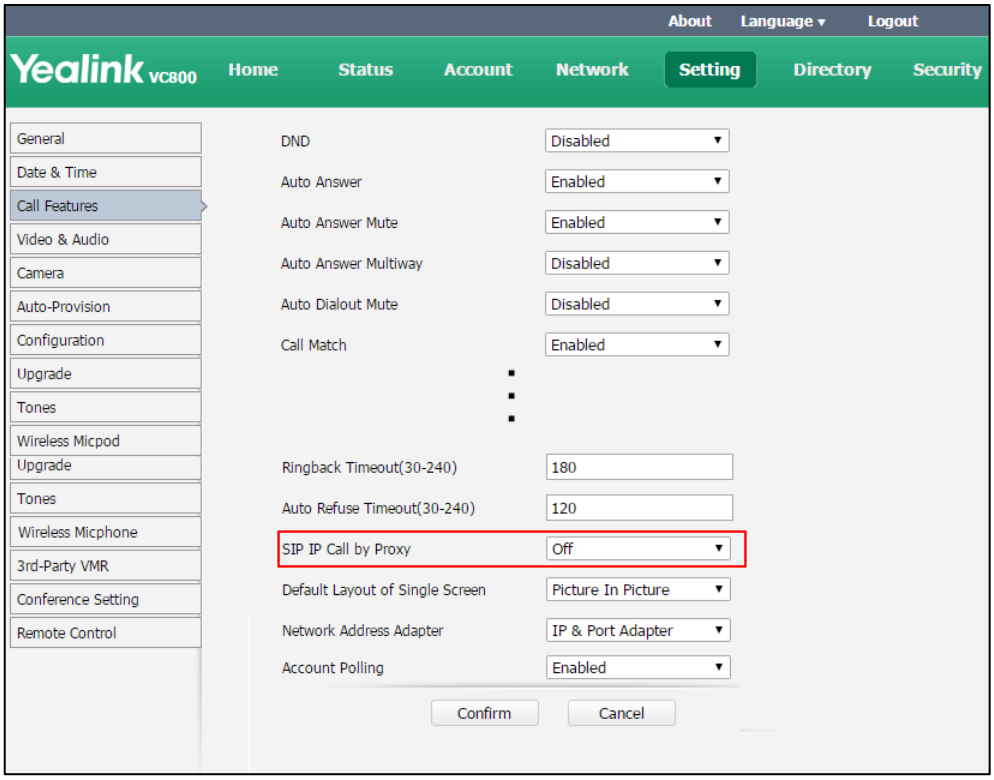
You can use SIP IP address or SIP account to dial an URI address (8000@XX.com).

The SIP IP call by proxy parameter on the system is described below:

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

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

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



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

Configure Network Quality Settings

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.

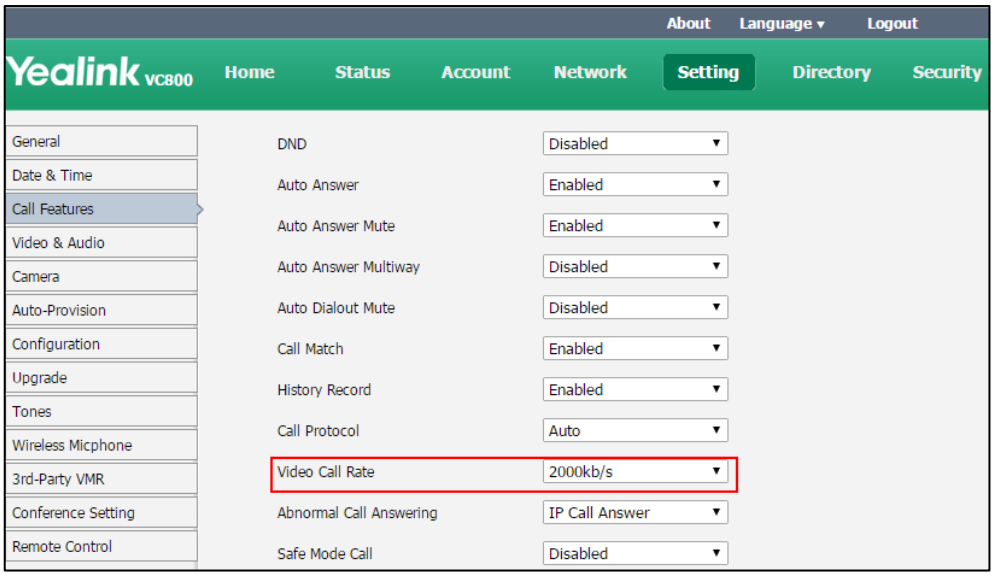
Note The call rate of audio and PC content are also affected by this configuration.

Video call rate parameters on the system are described below:

Parameter	Description	Configuration Method
Video Call Rate	Specifies the maximum video call rate. **Default:** 2000kb/s	Remote Control Web User Interface

To configure video call rate via web user interface:

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



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

To configure video call rate via the remote control:

1. Select **More**->**Setting**->**Call Features**->**Video Call Rate**.
2. Select the desired value.
3. Select **Save**, and then press OK to accept the change.

Adjusting MTU of Data Packets

Data packets that exceed the maximum transmission unit (MTU) size for any router or segment along the network path may be fragmented or dropped. This results in poor quality video at the receiving device. You can set the maximum MTU size of the data packets sent by the system. The default value is 1500 bytes. Specify the MTU size used in calls based on the network bandwidth settings. If the video becomes blocky or network errors occur, packets may be too large; decrease the MTU. If the network is burdened with unnecessary overhead; packets may be too small, increase the MTU.

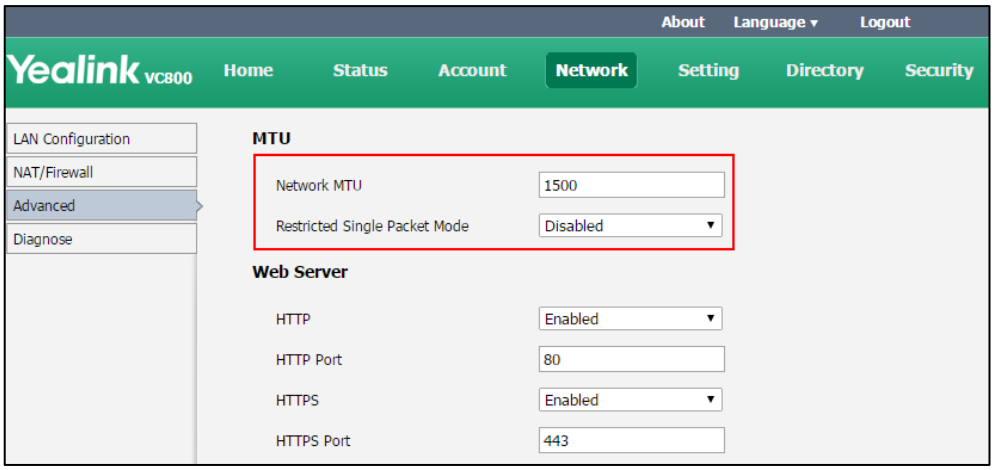
The MTU parameter on the system is described below.

Parameter	Description	Configuration Method
Network MTU	Specifies the maximum MTU size (in bytes) of data packets sent by the system. **Valid Values:** Integer from 1000 to 1500 **Default:** 1000 **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Restricted Single Packet Mode	Enables or disables the restricted single packet mode. ● **Disabled**−sends data packets using multiple packets mode. ● **Enabled**−sends data packets using single packet mode. **Default:** Disabled **Note**: Some devices of other venders only accept the data packets sent by single packet mode. If local system sends data packets using multiple packets mode, the video call may appear the mosaic phenomenon. To avoid this situation, enable this configuration. If you change this parameter, the system will reboot to make the change take effect.	Web User Interface

To configure MTU via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **MTU** block, enter the desired value in the **Network MTU** field.

3. Select the desired value from the pull-down list of **Restricted Single Packet Mode**.



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

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

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

To configure MTU via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Enter the desired value in the **Network MTU(1000-1500)** field.
3. Select **Save**, and then press OK to accept the change.

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

Quality of Service

The QoS (Quality of Service) is a method which handles the priority of audio, video and data in the network. QoS guarantees are important for applications that require a fixed bit rate and are delay sensitive when the network capacity is insufficient.

Audio QoS

To make VoIP transmissions intelligible to receivers, audio packets should not be dropped or excessively delayed. To guarantee high-quality audio transmission, audio packets should be configured with a high transmission priority.

Video QoS

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

Data QoS

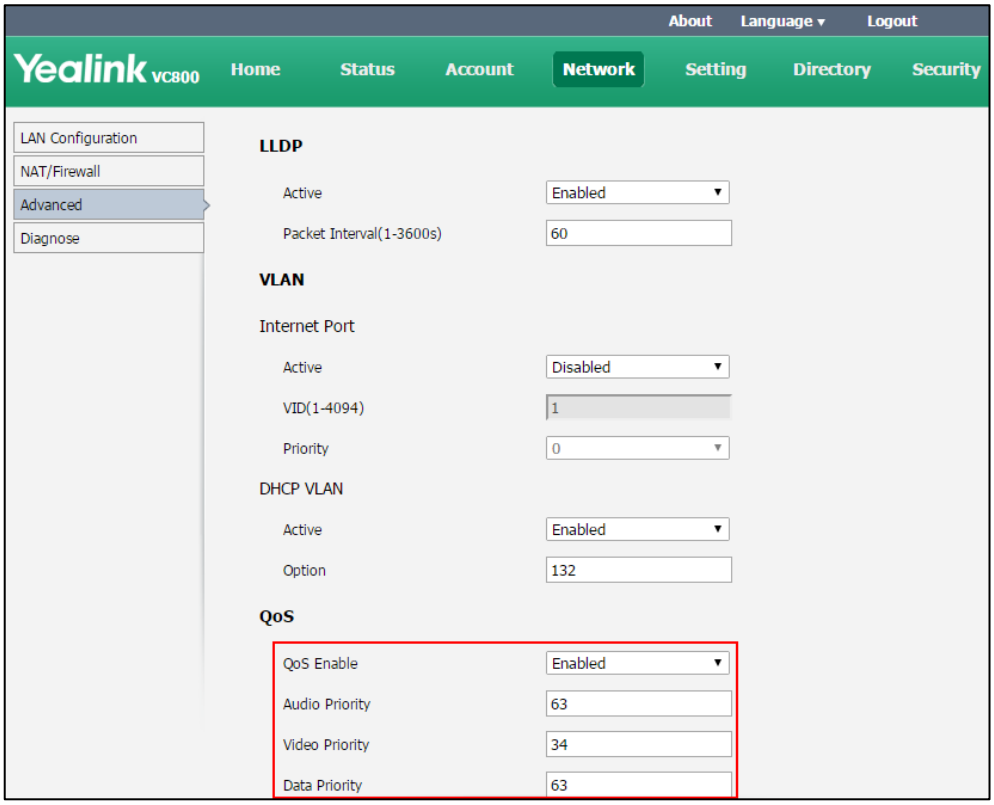
To ensure good call quality, data packets (for example: SIP signaling and H.225 call signaling) emanated from the system should be configured with a high transmission priority.

QoS feature parameters on the system are described below.

Parameter	Description	Configuration Method
QoS Enable	Enables or disables QoS feature. **Default:** Enabled **Note**: If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Audio Priority	Define which priority audio packets should have in the IP network. **Valid Values: 0-63** **Default:** 63 **Note**: The higher the number, the higher the priority. If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Video Priority	Define which priority video packets should have in the IP network. **Valid Values: 0-63** **Default:** 63 **Note**: The higher the number, the higher the priority. If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface
Data Priority	Define which priority data packets should have in the IP network. **Valid Values: 0-63** **Default:** 63 **Note**: The higher the number, the higher the priority. If you change this parameter, the system will reboot to make the change take effect.	Remote Control Web User Interface

To configure QoS via web user interface:

1. Click on **Network**->**Advanced**.
2. Select **Enabled** from the pull-down list of **QoS Enable**.
3. Enter the desired values in the corresponding fields.



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

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

To configure QoS via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Select **Enabled** from the pull-down list of **QoS Enable**.
3. Enter the desired values in the corresponding fields.
4. Select **Save**, and then press OK to accept the change.

   The display device prompts "Reboot now?".
5. Select **OK**, and then press OK to reboot the system immediately.

Frame Rate and Resolution

You can specify the maximum frame and resolution for the video and shared content.

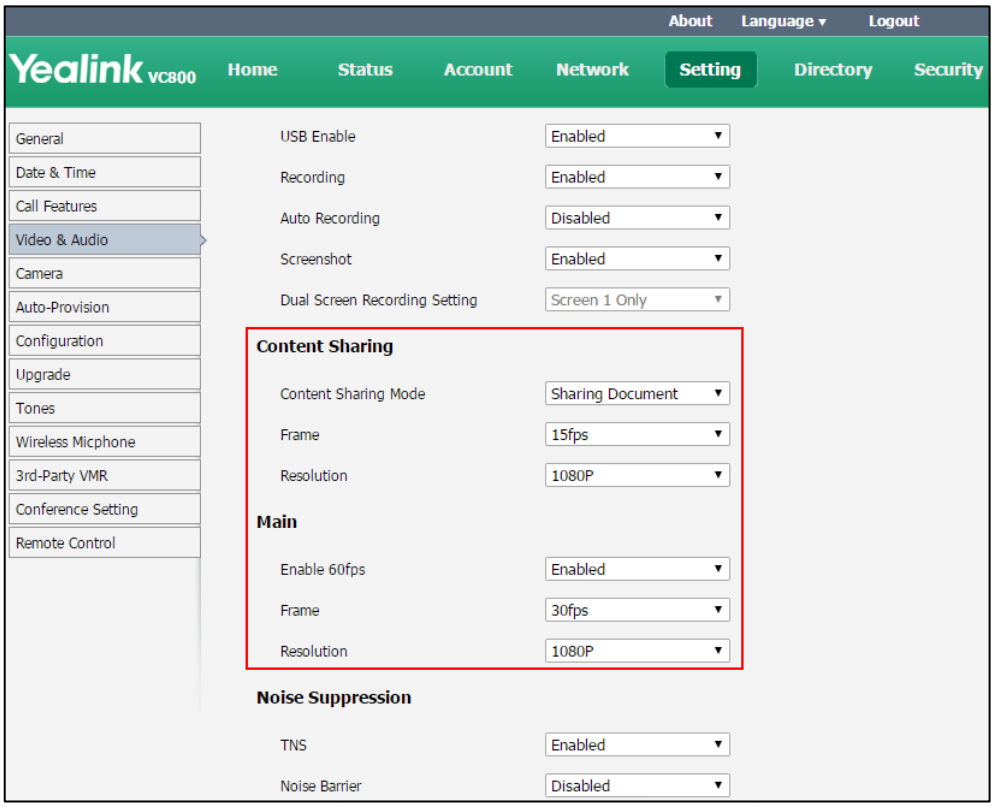
Parameters of frame rate and resolution on the system are described below:

Parameter	Description	Configuration Method

Parameter	Description	Configuration Method
Content Sharing ->Content Sharing Mode	Configures the content sharing mode. ● **Sharing Document**- select this value to save bandwidth when you are sharing a document. ● **Sharing Video**- select this value to play video fluently when you are sharing a video. **Default**: Sharing Document	Web User Interface
Content Sharing ->Frame	Specifies the maximum frame rate of the shared content. ● 30fps ● 15fps ● 5fps **Default**: 15fps	Web User Interface
Content Sharing ->Resolution	Specifies the maximum resolution of the shared content. ● 1080P ● 720P **Default**: 1080P	Web User Interface
Enable 60fps	Enables or disables 60fps for a video call. **Default:** Enabled	Web User Interface
Main->Frame	Specifies the maximum frame rate of the video. ● 60fps ● 30fps ● 15fps ● 5fps **Default**: 30fps **Note:** The 60fps appears only if **Enable 60fps** is selected to **Enabled**.	Web User Interface
Main->Resolution	Specifies the maximum resolution of the video. ● 1080P ● 720P **Default**: 1080P	Web User Interface

To configure the frame and resolution via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. In the **Content Sharing** field, select the desired value from the pull-down list of **Content Sharing Mode, Frame** and **Resolution**.
3. In the **Main** field, select the desired value from the pull-down list of **Enable 60fps, Frame** and **Resolution**.



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

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.

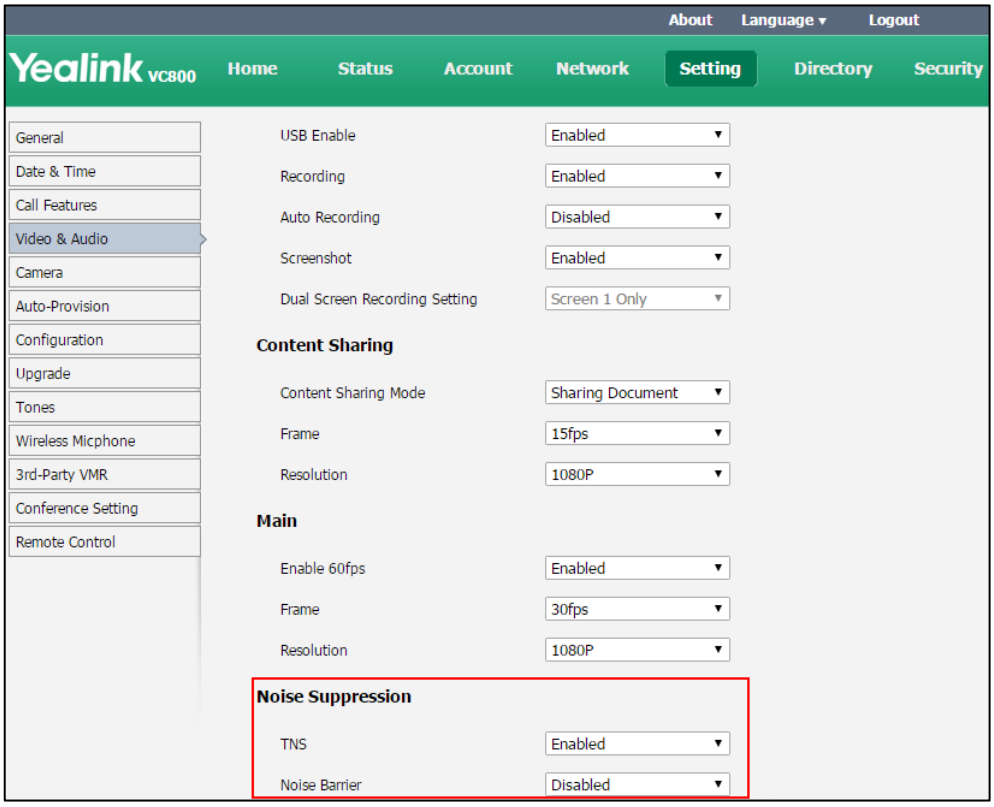
The noise suppression parameters on the system are described below:

Parameter	Description	Configuration Method
TNS	Enables or disabled the Transient Noise Suppressor (TNS). **Default:** Enabled	Web User Interface

Parameter	Description	Configuration Method
Noise Barrier	Enables or disabled the noise barrier feature. **Default:** Disabled	Web User Interface

To configure noise suppression via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Select the desired value from the pull-down list of **TNS**.
3. Select the desired value from the pull-down list of **Noise Barrier**.



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

Configuring System Settings

This chapter provides information for making configuration changes for the system, such as language, time and date, backlight of the CP960 conference phone, video&audio settings and camera settings:

Topics include:

General Settings

Custom Key Type

You can configure a custom type for the  key on the remote control.

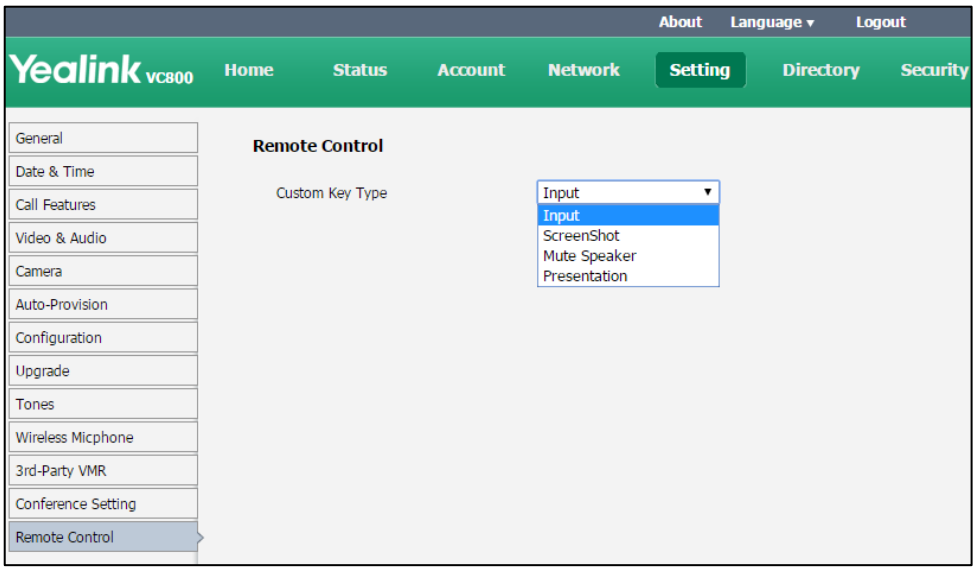
The site name parameter is described below:

Parameter	Description	Configuration Method
Custom Key Type	Configure a 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. **Default:** Presentation	Web User Interface

To configure a custom key type via web user interface:

1. Click on **Setting->Remote Control**.

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



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

Site Name

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

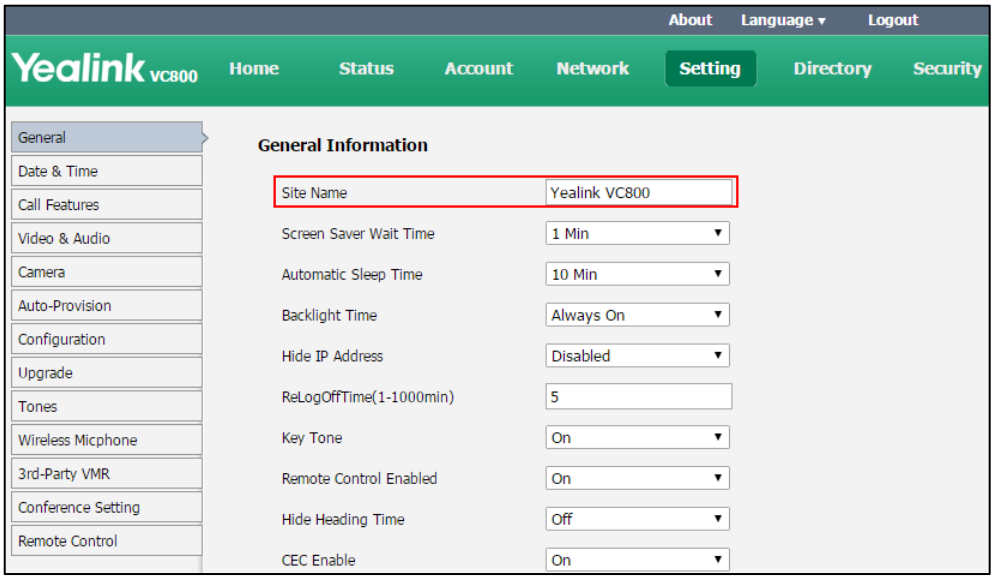
The site name parameter is described below:

Parameter	Description	Configuration Method
Site Name	Configures the site name of the system. **Valid values:** String within 64 characters **Default:** Yealink VC800/VC500	Remote Control Web User Interface

To configure the site name via web user interface:

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

2. Edit the site name in the **Site Name** field.



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

   The display device will display the changed site name.

To configure the site name via the remote control:

1. Select **More**->**Setting**->**Basic**->**Site Name**.
2. Edit the site name in the **Site Name** field.
3. Select **Save**, and then press OK to accept the change.

   The display device will display the changed site name.

Backlight of the CP960 Conference Phone

Backlight determines the brightness of the CP960 conference phone, allowing users to read easily in dark environments. Backlight time specifies the delay time to turn off the backlight when the phone is inactive.

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

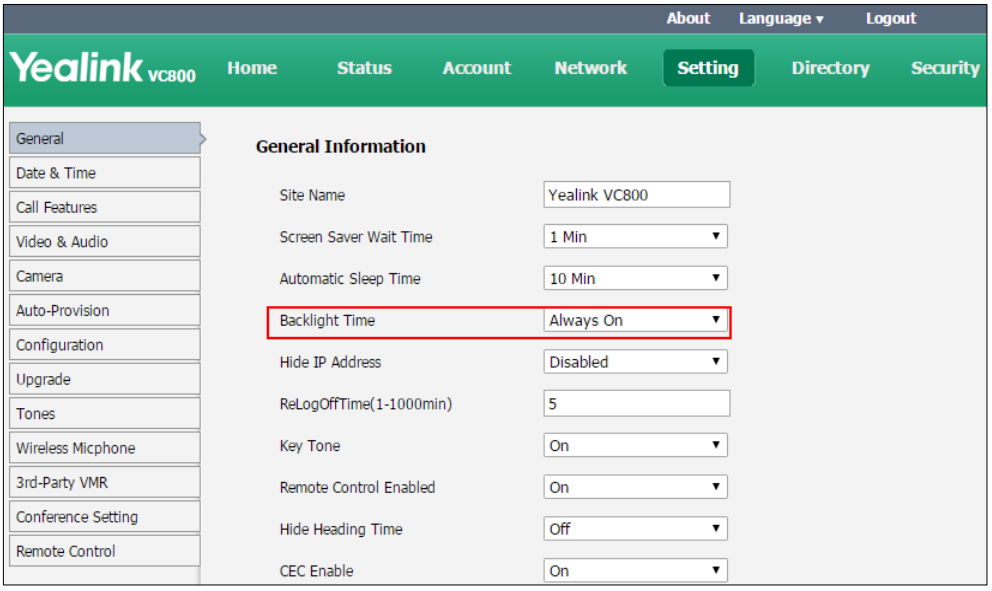
- **Always On:** Backlight is turned on permanently.
- **15s**, **3 s**, **1min**, **2min**, **5min**, **10min**, **30min:** Backlight is turned off when the phone is inactive after a preset period of time. It is automatically turned on if the status of the phone changes or any key is pressed.

The backlight parameter on CP960 conference phone is described below:

Parameter	Description	Configuration Method
Backlight Time	Configures the backlight time of the CP960 conference phone. **Default:** Always On	Web User Interface CP960 conference phone

To configure the backlight time of the CP960 conference phone via web user interface:

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



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

To configure the backlight of the CP960 conference phone:

1. Tap ->**Display**->**Backlight**.
2. Drag the **Active Level** slider to change the intensity of the touch screen.
3. Tap the **Backlight Time** field.
4. Tap the desired time in the pop-up dialog box.
5. Tap to accept the changes.

You can also drag the backlight slider on the control center to change the intensity of the touch screen.

To configure the backlight active level via the control center:

1. Swipe down from the top of the screen to enter the control center.
2. Drag the backlight slider.

Language

The default language of the display device and the CP960 conference phone is English, and you can change it via the remote control. The CP960 conference phone will detect and use the same language as the display device.

The default language of the web user interface is English. You can change the language of the web user interface via web user interface. The available languages for system are English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish,

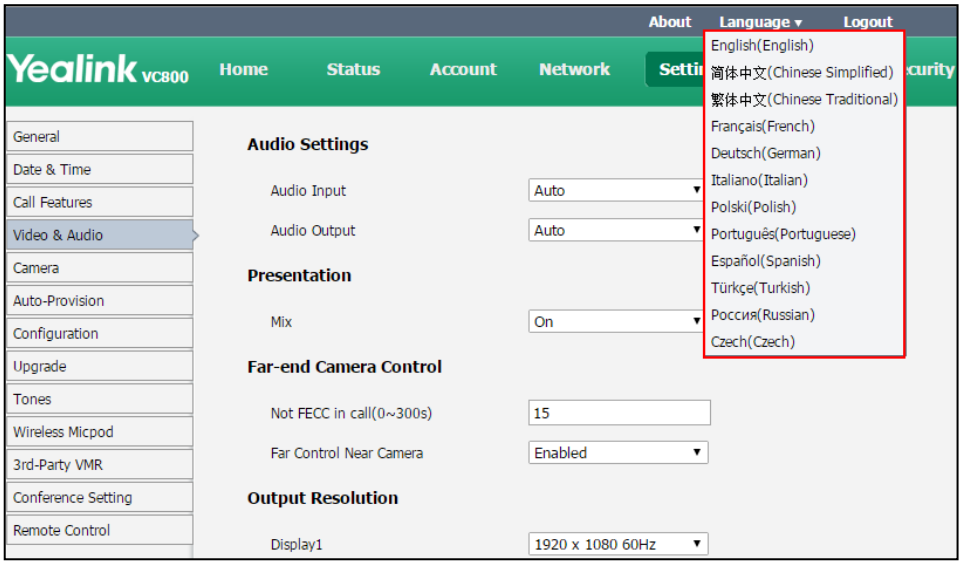
Turkish and Russian.

The language parameters on the system are described below:

Parameter	Description	Configuration Method
Language	Specifies the language for the web user interface	Web User Interface
Language	Specifies the language for the display device and the CP960 conference phone. **Default:** English	Remote Control

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

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



To specify the language for the display device and the CP960 conference phone via the remote control:

1. Select **More**->**Setting**->**Basic**->**Language**.
2. Select the desired language from the pull-down list of **Language**.
3. Select **Save**, and then press OK to accept the change.

Date & Time

Time and date are displayed on the idle screen of the display device and the CP960 conference phone. Time and date are synced automatically from the NTP server by default. The default NTP server is cn.pool.ntp.org. The NTP server is configurable manually or obtained by DHCP via DHCP Option 42. The phone will use the NTP server obtained by DHCP preferentially. If the

system cannot obtain the time and date from the NTP server, you need to manually configure them. The time and date can use one of several different formats.

Time Zone

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

Daylight Saving Time

Daylight Saving Time (DST) is the practice of temporary advancing clocks during the summertime so that evenings have more daylight and mornings have less. Typically, clocks are adjusted forward one hour at the start of spring and backward in autumn. Many countries have used DST at various times, details vary by location. DST can be adjusted automatically from the time zone configuration. Typically, there is no need to change this setting.

DST parameters are described below:

Parameter	Description	Configuration Method
DHCP Time	Enables or disables the system to update time with the offset time obtained from the DHCP server. **Default:** Disabled **Note:** it is only available to GMT 0.	Web User Interface
Time Zone	Configures the time zone. **Default:** +8 China (Beijing)	Remote Control Web User Interface
Primary Server/NTP Primary Server	Configures the primary NTP server. **Default:** cn.pool.ntp.org	Remote Control Web User Interface
Secondary Server/NTP Secondary Server	Configures the secondary NTP server. **Default:** cn.pool.ntp.org	Remote Control Web User Interface
Synchronism **(15~86400s)**	Configures the interval (in minutes) for the system to synchronize time and date with NTP server. **Default**: 1000.	Web User Interface
Daylight Saving	Configures the Daylight Saving Time (DST) type.	Remote Control Web User Interface

Parameter	Description	Configuration Method
Time	The available types for the system are: ● **Disabled**-not use DST. ● **Enabled**-use DST. You can manually configure the start time, end time and offset according to your needs. ● **Automatic-**use DST. DST will be configured automatically. You do not need to manually configure the start time, end time and offset. **Default:** Automatic	
Fixed Type	Configures the DST calculation methods. ● **By Date**- specifies the month, day and hour to be the DST start /end date. ● **By Week**- specifies the month, week, day and hour the DST start /end date. **Note:** It only works if the value of Daylight Saving Time is set to Enabled.	Web User Interface
Start Date	When the DST calculation method is set to **By Date**. Configures the time to start DST. **Note:** It only works if the value of the Daylight Saving Time is set to Enabled.	Web User Interface
End Date	When the DST calculation method is set to **By Date**. Configures the time to end DST. **Note:** It only works if the value of the Daylight Saving Time is set	Web User Interface

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

Parameter	Description	Configuration Method
	• MM/DD/YY • DD MMM YYYY • WWW DD MMM **Default:** YYYY-MM-DD	

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

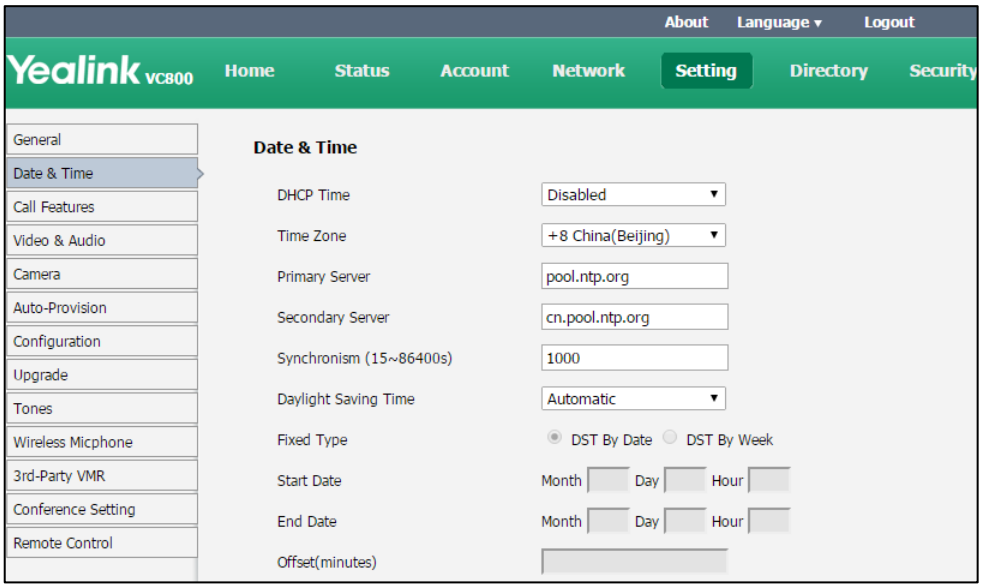
1. Click on **Setting**->**Date& Time**.
2. Select **Disabled** from the pull-down list of **Manual Time**.
3. Select the desired time zone from the pull-down list of **Time Zone**.
4. Enter the domain names or IP addresses in the **Primary Server** and **Secondary Server** fields respectively.
5. Enter the desired time interval in the **Synchronism (15~86400s)** field.
6. Select the desired value from the pull-down list of **Daylight Saving Time**.

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

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

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

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

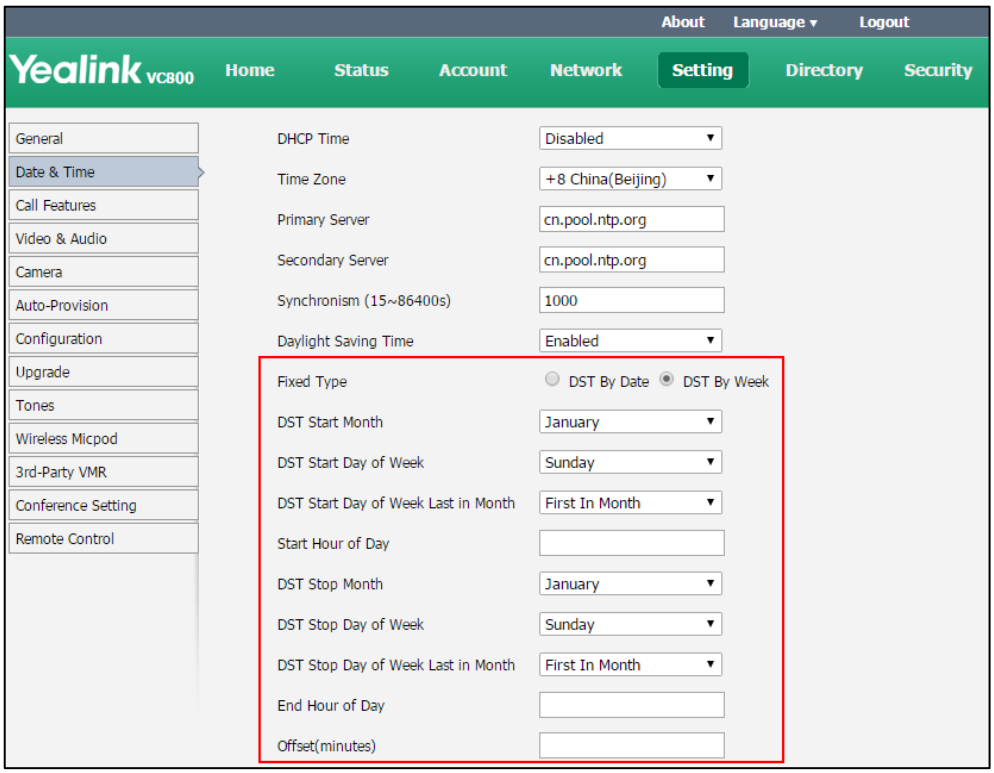


   - Mark the **DST By Week** radio box in the **Fixed Type** field.

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

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

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

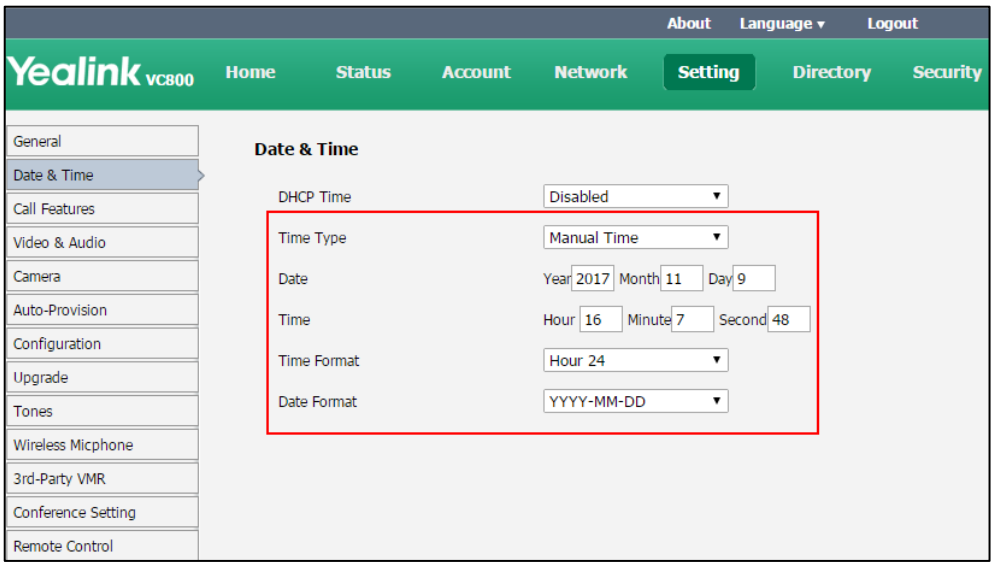


7. Enter the desired offset time in the **Offset (minutes)** field.
8. Click **Confirm** to accept the change.

To configure the time and date manually via web user interface:

1. Click on **Setting->Date& Time**.
2. Select **Manual Time** from the pull-down list of **Time Type**.
3. Enter the current date in the **Date** field.
4. Enter the current time in the **Time** field.
5. Select the desired value from the pull-down list of **Time Format**.

6. Select the desired value from the pull-down list of **Date Format**.



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

To configure the time and date format via the remote control:

1. Select **More**->**Setting**->**Basic**->**Date & Time**.
2. Configure the desired values.
3. Select **Save**, and then press OK to accept the change.

   The time and date displayed on the LCD screen of the display device and CP960 conference phone will change accordingly.

Screen Saver Waiting Time

The screen saver will automatically start each time your system has been idle for a certain amount of time (the default time is 1 minute). The screen saver is used to blank the screen or fill it with moving images.

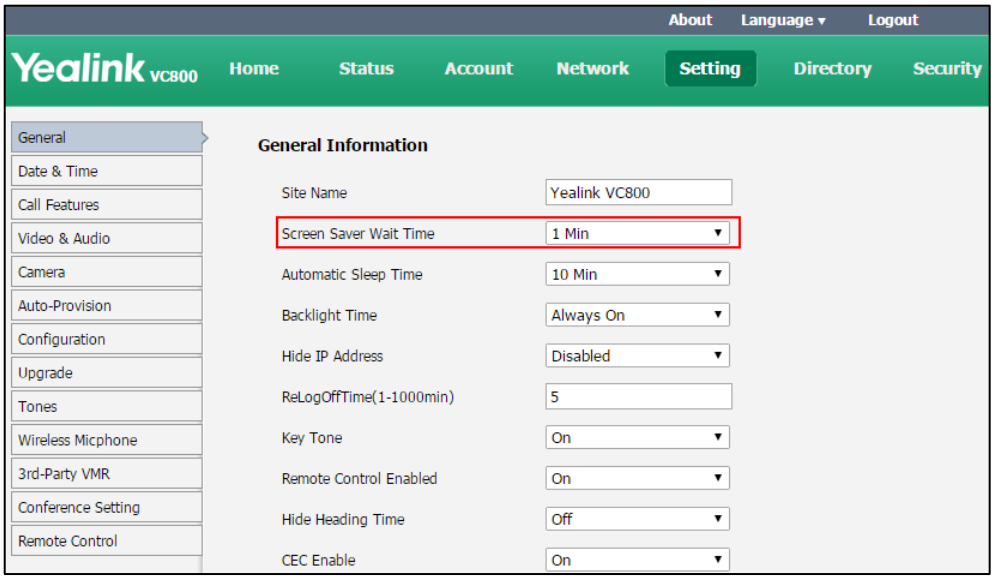
The screen saver waiting time parameter is described below:

Parameter	Description	Configuration Method
Screen Saver Wait Time	Configures the inactive time (in minutes) before the system starts screen saver. **Default:** 1 Min	Remote Control Web User Interface

To configure the screen saver waiting time via web user interface:

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

2. Select desired value from the pull-down list of **Screen Saver Wait Time**.



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

To configure the screen saver waiting time via the remote control:

1. Select **More**->**Setting**->**Basic**->**Screensaver**.
2. Select desired value.
3. Select **Save**, and then press (OK) to accept the change.

Automatic Sleep Time

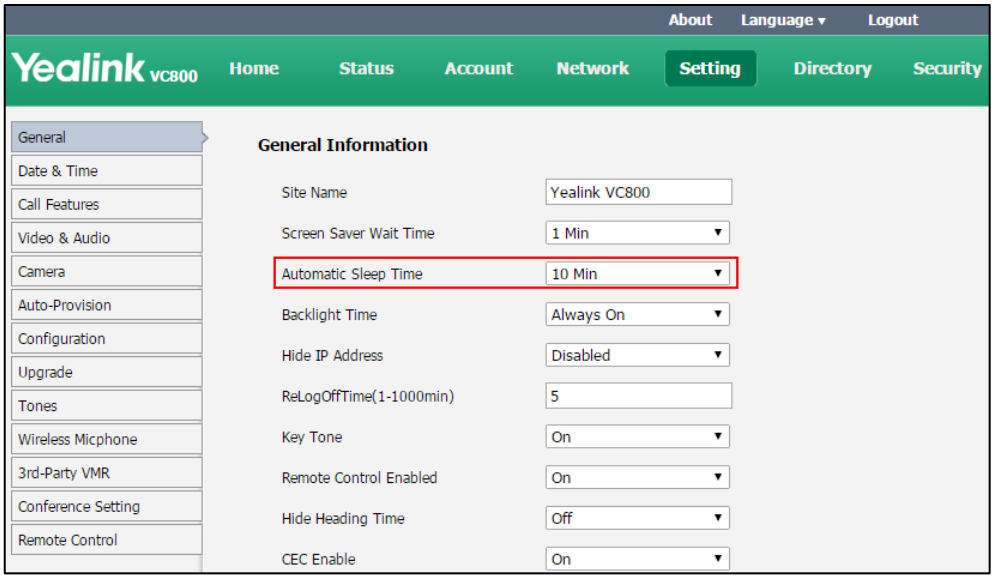
The system will enter the sleep mode automatically when it has been inactive for a period of time (the default time is 10 minutes). When the system is in sleep mode, it can still accept incoming calls. The display device will prompt "No Signal".

The automatic sleep time is described below:

Parameter	Description	Configuration Method
Automatic Sleep Time	Configures the inactive time (in minutes) before the system enter sleep mode. **Default:** 10 Min **Note**: During setup wizard, the automatic sleep time feature is disabled automatically. To protect the display device, you should configure the automatic sleep time immediately.	Remote Control Web User Interface

To configure the automatic sleep time via web user interface:

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



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

To configure the automatic sleep time via the remote control:

1. Select **More->Setting->Basic->Automatic Sleep Time**.
2. Select desired value.
3. Select Save, and then press OK to accept the change.

Hiding IP Address

The status bar of the display device displays IP address. You can choose to hide IP address on the status bar.

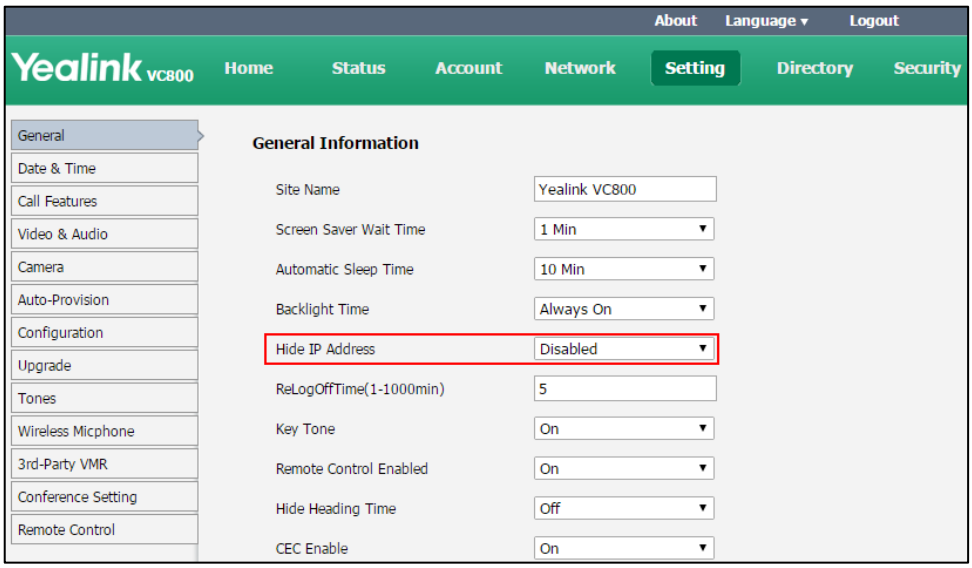
The hide IP address parameter is described below:

Parameter	Description	Configuration Method
Hide IP address	Enables or disables the system to hide IP address on the status bar. **Default:** Disabled	Web User Interface

To hide IP address via web user interface:

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

2. Select the desired value from the pull-down list of **Hide IP Address**.



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

Hiding Heading Time

The status bar of the display device displays current time and date. You can choose to hide time and date on the status bar.

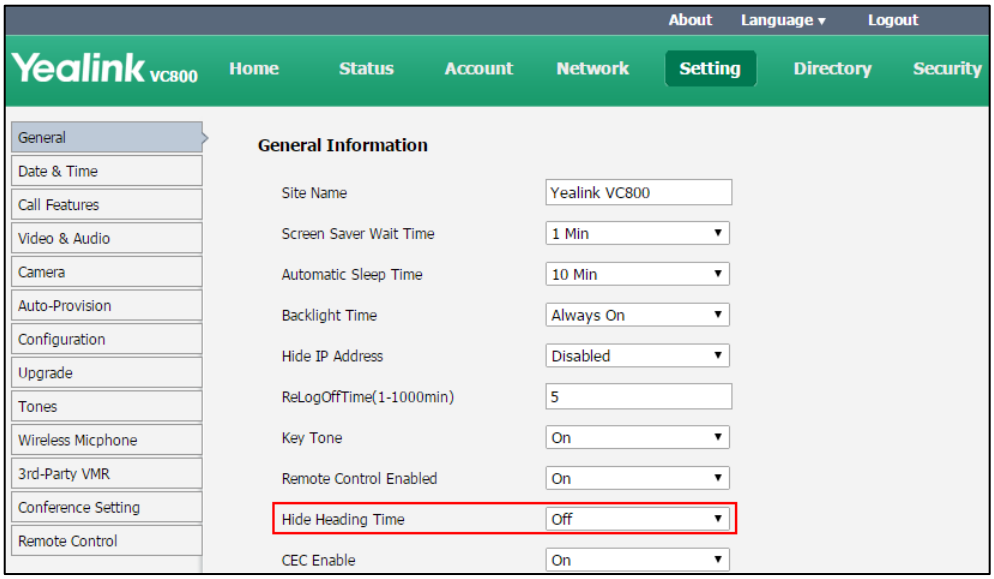
The hiding heading time parameter is described below:

Parameter	Description	Configuration Method
Hide Heading Time	Enables or disables the system to hide time and date on the status bar. **Default:** Disabled	Web User Interface

To hide heading time via web user interface:

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

2. Select the desired value from the pull-down list of **Hide Heading Time**.



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

Note This feature will not affect the time displayed on the status bar of CP960 conference phone.

Hiding Icons in a Call

During a call, the system will display some information and icons (such as call time, mute icon and recording icon) by default, you can know the call status from these information and icons. You can also hide these icons as needed to achieve the best video effects.

Parameters of hiding icons in a call feature on the system are described below:

Parameter	Description	Configuration Method
Time Icon	Enables or disables the system to hide call time during a call. • **Disabled**- the system does not display call time during a call. • **Hide with UI**- the system displays call time during a call, but the call time will disappear when the status bar is hidden. • **Enabled**- the system displays call time during a call. **Default:** Hide with UI	Web User Interface
Mute Icon	Enables or disables the system to hide mute icon ( ) during a	Web User Interface

Parameter	Description	Configuration Method
	call. • **Disabled**- the system does not display mute icon during a call. • **Hide with UI**- the system displays mute icon during a call, but the mute icon will disappear when the status bar is hidden. • **Enabled**- the system displays mute icon during a call. **Default:** Disabled	
Camera Icon	Enables or disables the system to hide camera icon () during a call. • **Disabled**- the system does not display camera icon during a call. • **Hide with UI**- the system displays camera icon during a call, but the camera icon will disappear when the status bar is hidden. • **Enabled**- the system displays camera icon during a call. **Default:** Disabled	Web User Interface
Recording Icon	Enables or disables the system to hide recording icon () during a call. • **Disabled**- the system does not display recording icon during a call. • **Hide with UI**- the system displays recording icon will disappear when the status bar is hidden. • **Enabled**- the system displays recording icon during a call. **Default:** Disabled	Web User Interface

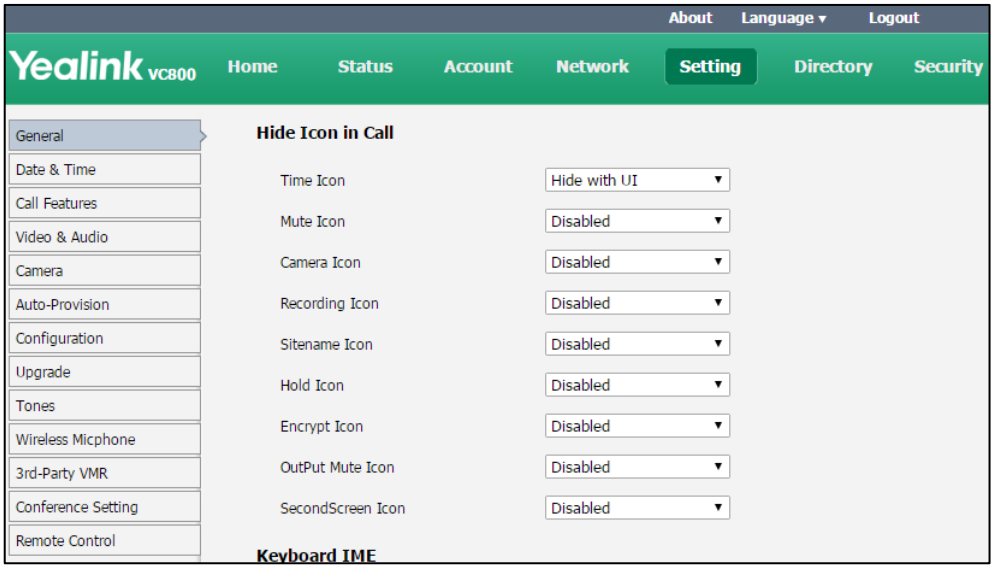
Parameter	Description	Configuration Method
Sitename Icon	Enables or disables the system to hide site name icon during a call. • **Disabled**- the system does not display site name icon during a call. • **Hide with UI**- the system displays site name icon during a call, but the site name will disappear when the status bar is hidden. • **Enabled**- the system displays site name icon during a call. **Default:** Disabled	Web User Interface
Hold Icon	Enables or disables the system to hide hold icon () during a call. • **Disabled**- the system does not display hold icon during a call. • **Hide with UI**- the system displays hold icon during a call, but the hold icon will disappear when the status bar is hidden. • **Enabled**- the system displays hold icon during a call. **Default:** Disabled	Web User Interface
Encrypt Icon	Enables or disables the system to hide encrypt icon () during a call. • **Disabled**- the system does not display encrypt icon during a call. • **Hide with UI**- the system displays encrypt icon during a call, but the encrypt icon will disappear when the status bar is hidden. • **Enabled**- the system displays encrypt icon during a call. **Default:** Disabled	Web User Interface

Parameter	Description	Configuration Method
OutPut Mute Icon	Enables or disables the system to hide output mute icon (output volume is set to 0: ) during a call. • **Disabled**- the system does not display output mute icon during a call. • **Hide with UI**- the system displays output mute icon during a call, but the output mute icon will disappear when the status bar is hidden. • **Enabled**- the system displays output mute icon during a call. **Default:** Disabled	Web User Interface
SecondScreen Icon	Enables or disables the system to hide second screen icon () during a call. • **Disabled**- the system does not display second screen icon during a call. • **Hide with UI**- the system displays second screen icon during a call, but the second screen icon will disappear when the status bar is hidden. • **Enabled**- the system displays second screen icon during a call. **Default:** Disabled	Web User Interface

To hide icons in a call via web user interface:

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

2. Select the desired values from the pull-down lists of **Time Icon**, **Mute Icon**, **Camera Icon**, **Recording Icon**, **Sitename Icon**, **Hold Icon**, **Encrypt Icon**, **OutPut Mute Icon**, and **SecondScreen Icon**.



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

Relog Offtime

The system will log out of the web user interface automatically after being inactive for a period of time (default: 5 minutes). You need to re-enter the user name and password to login. You can only configure the relog offtime via web user interface.

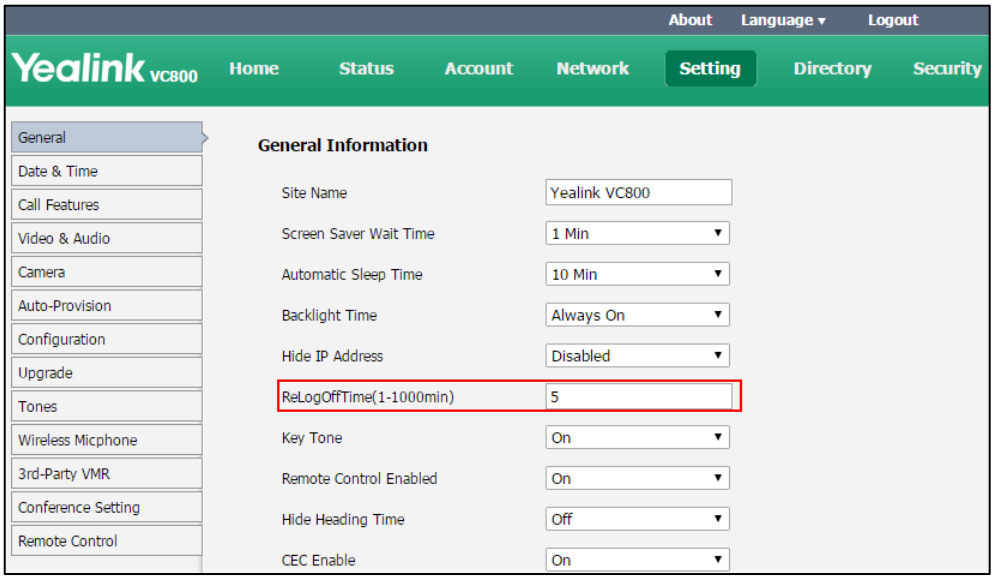
The relog offtime parameter is described below:

Parameter	Description	Configuration Method
ReLogOffTime (1-1000min)	Configures the inactive time (in minutes) before the system logs out of the web user interface automatically. **Default:** 5	Web User Interface

To configure the relog offtime via web user interface:

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

2. Enter the desired time in the **ReLogOffTime (1-1000min)** field.



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

Keyboard Input Method

On-screen keyboard on the display device supports English and Russian input methods.

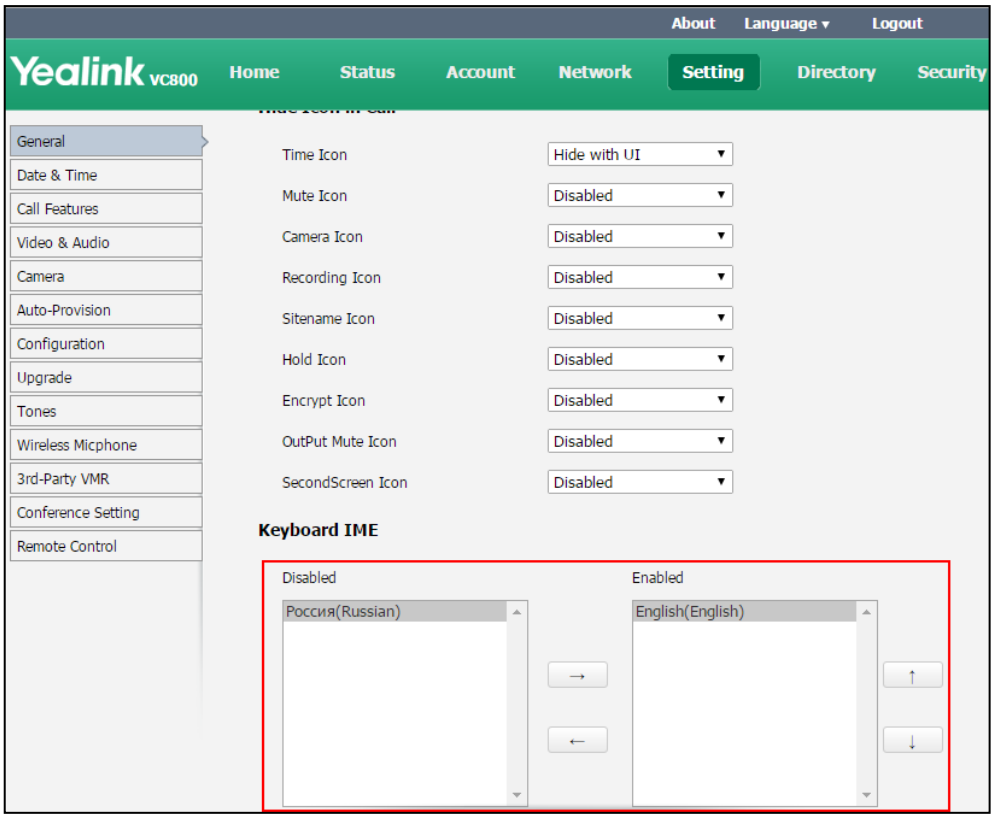
You can enter characters using the enabled input method. Changing keyboard input method is configurable via web user interface only.

To configure keyboard input method via web user interface:

1. Click on **Setting**->**General**.
2. In the **Keyboard IME** block, select the desired list from the **Disabled** column and click → .

   The selected input method appears in the **Enabled** column.
3. Repeat step 2 to add more input methods to the **Enabled** column.
4. (Optional.) To remove a list from the **Enabled** column, select the desired list and then click ← .

5. To adjust the display order of the enabled input methods, select the desired list, and click ↑ or ↓.



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

To change keyboard input method via the remote control:

1. In the editing field, select , and then press OK.
   The display device appears the on-screen keyboard.
2. Select , and then press OK to change the input method.

USB Configuration

If you have high requirement for data security, you can disable the USB feature. If you disable the USB feature, you cannot view the videos and screenshots stored in the USB flash driver via the remote control, and cannot record video or capture screenshots via the remote control.

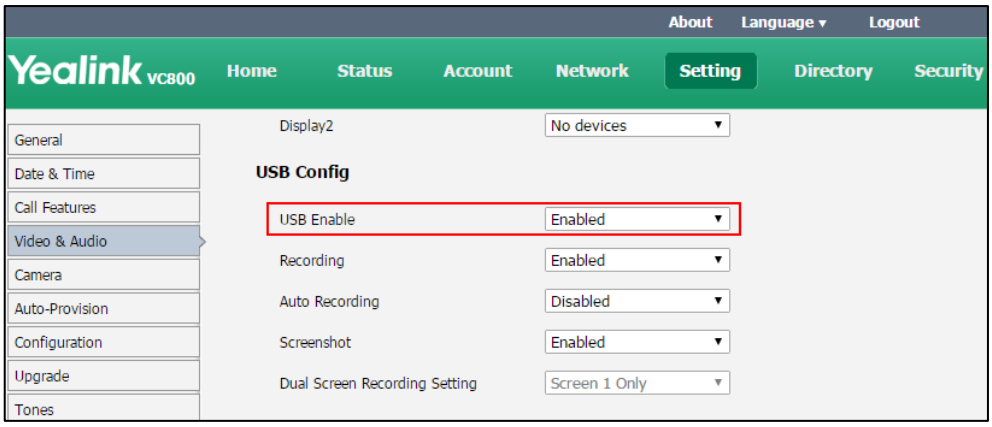
The USB configuration parameter on the system is described below.

Parameter	Description	Configuration Method
USB Enable	Enables or disables the USB feature. **Default:** Enabled **Note**: If you change this parameter, the system will reboot to make the	Web User Interface

Parameter	Description	Configuration Method
	change take effect.	

To configure USB configuration via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Select the desired value from the pull-down list of **USB Enable**.



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

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

Configuring Audio Settings

Key Tone

You can enable the key tone feature to produce a sound when you press any key on the remote control or tap the onscreen dial pad on the CP960 conference phone.

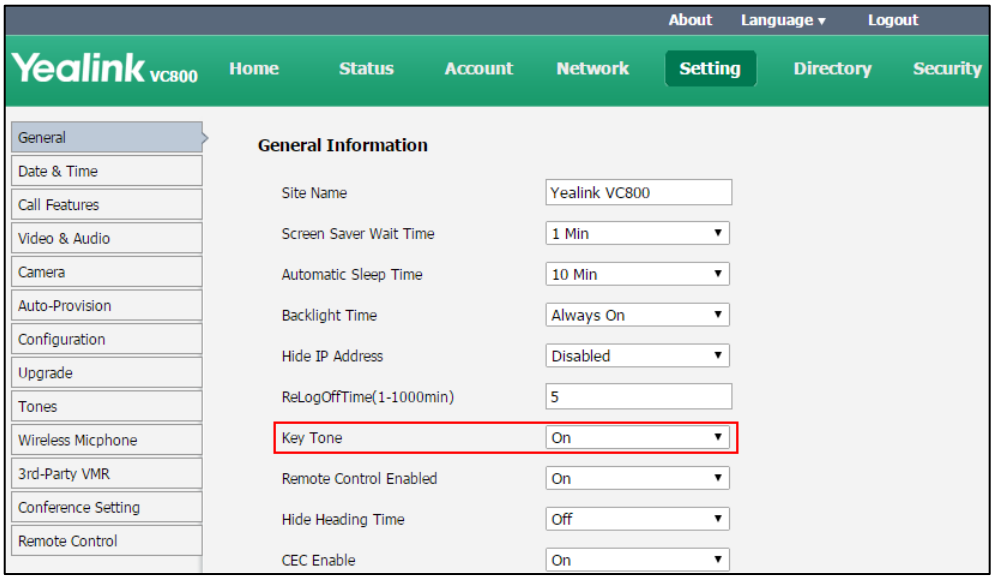
The key tone parameter is described below:

Parameter	Description	Configuration Method
Key Tone	Enables or disables the key tone. **Default:** On	Remote Control Web User Interface

To configure the key tone via web user interface:

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

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



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

To configure the key tone via the remote control:

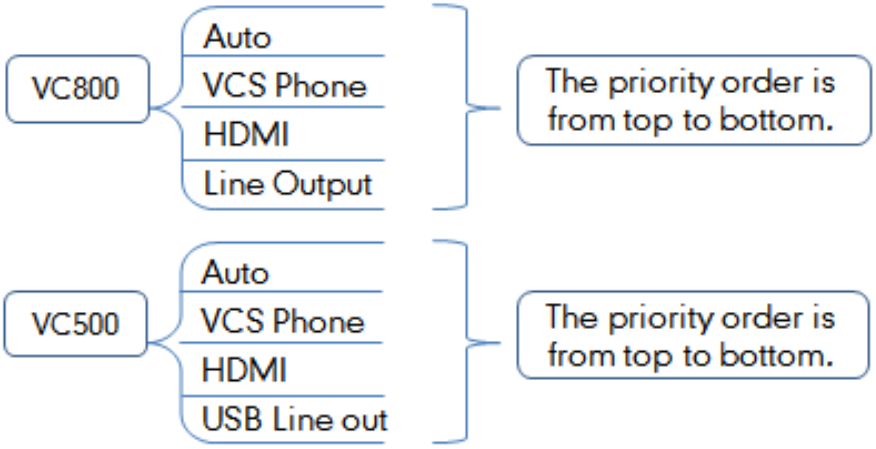
1. Select **More**->**Setting**->**Basic**.
2. Mark the radio box in the **Key Tone** field.
3. Press  to exit.

Audio Output

The system supports the following audio output:

- **Auto**
- **VCS Phone**
- **HDMI**
- **Line Output**
- **USB Line out**

By default, the system automatically selects the audio output with highest priority. The priority is: VCS Phone> HDMI>Line Output. If the audio output with highest priority is removed from the VC800/VC500, the VC800/VC500 will select the next highest priority device.



You can also specify the desired audio output via the remote control or the web user interface.

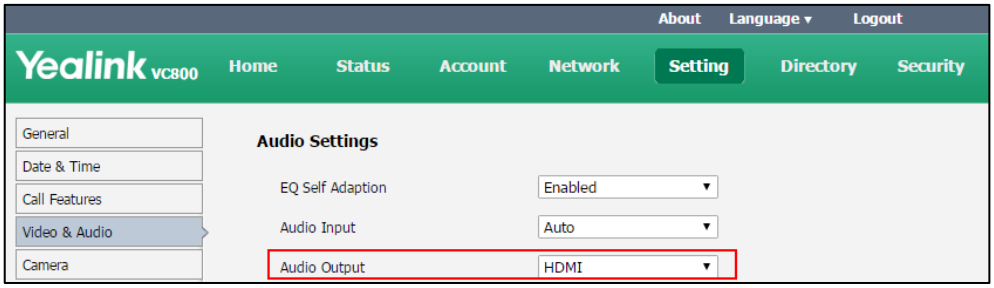
The audio output parameter is described below:

Parameter	Description	Configuration Method
Audio Output	Specifies the audio output device for the system. **Valid values:** • **Auto** - selects the audio output device with highest priority. • **VCS Phone** - selects the CP960 conference phone. • **HDMI** - selects the built-in speakerphone of the display device. • **Line Output** - speakerphone connected to the Line Out port on the VC800 codec. • **USB Line out** - Speakerphone connected to the USB port on the VC500 codec using a USB to Line-out adapter. **Default:** Auto. If **VCS Phone** is selected as the audio output device manually or automatically, the audio input	Remote Control Web User Interface

Parameter	Description	Configuration Method
	device must be **VCS Phone** or **VCS Phone+Wireless Microphone**.	

To configure the audio output via web user interface:

1. Click on **Setting->Video & Audio**.
2. Select the desired value from the pull-down list of **Audio Output**.



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

To configure the audio output via the remote control:

1. Select **More->Setting->Video & Audio->Audio Settings**.
2. Select the desired value from the pull-down list of **Audio Output**.
3. Select **Save**, and then press OK to accept the change.

EQ Self Adaption

The system supports EQ self adaption to optimize the acoustic effect.

The EQ self-adaption starts when one of the following situations occurs:

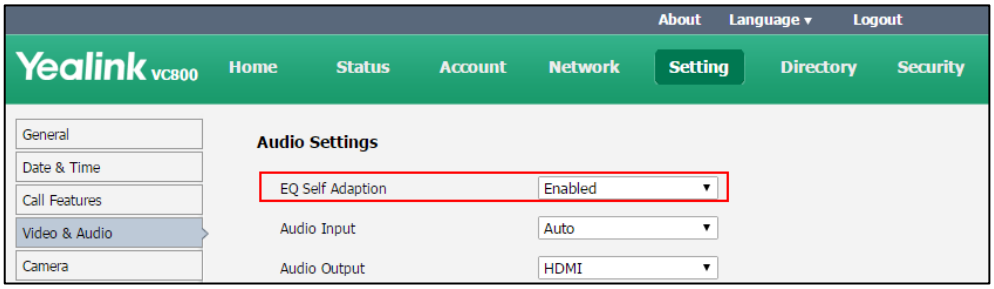
- The audio output device manually or automatically switches to **HDMI** or **Line Output/USB Line out**.
- When the system is powered on, the system finds that the **HDMI** or **Line Output/USB Line out** is current audio output device.
- The EQ self-adaption feature changes from disabled to enabled.

The EQ self adaption parameter on the system is described below.

Parameter	Description	Configuration Method
EQ Self Adaption	Enables or disables the EQ self adaption feature on the system. **Default:** Enabled	Web User Interface

To configure EQ self adaption via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Select the desired value from the pull-down list of **EQ Self Adaption**.



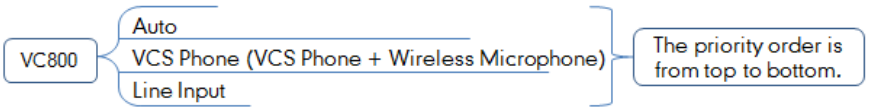
3. Click **Confirm** to accept the change.

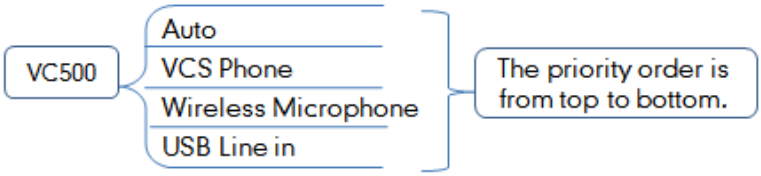
Audio Input

The system supports the following audio input audio input:

- **Auto**
- **VCS Phone**
- **Wireless Microphone**
- **Line Input**
- **USB Line in**

The priority of audio input is:





By default, the VC800/VC500 automatically selects the audio input with the highest priority. If you select "VCS Phone + Wireless Microphone" option, the VC800/VC500 will use CP960 conference phone and CPW90 expansion microphones to pick up audio at the same time.

You can also specify the desired audio input via the remote control or the web user interface.

The audio input device parameter is described below:

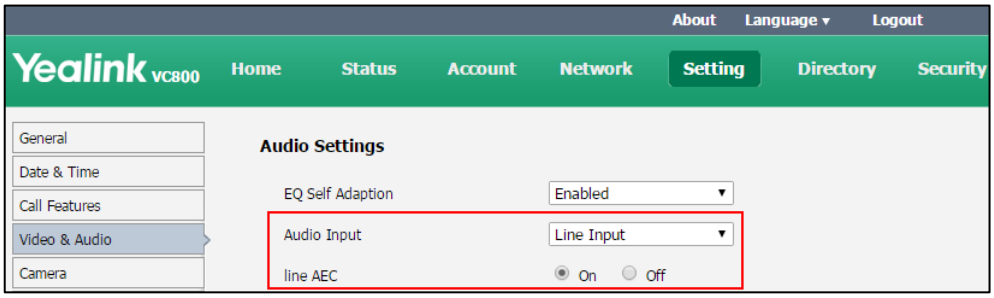
Parameter	Description	Configuration Method
Audio Input	Specifies the audio input for the system. **Valid values:** ● **Auto**- selects the audio input device with the highest priority. ● **VCS Phone**- selects the CP960 conference phone. ● **VCS Phone + Wireless Microphone**- selects the CP960 conference phone and CPW90 wireless expansion microphones ● **Wireless Microphone** - CPW90 wireless microphones ● **Line Input**- audio input device connected to the Line In port on the VC800 codec ● **USB Line in** - audio input device connected to the USB port on the VC500 codec using a USB to Line-in adapter **Default:** Auto.	Remote Control Web User Interface
line AEC	Enables or disables echo cancellation for line input device. **Valid values:** ● **On**- If you select an acoustic device (for example: a microphone) to be the line input, you can enable this configuration to eliminate echo. ● **Off**- If you select a non-acoustic device (for example: a mobile phone) to be the line input, you should disable this configuration. **Default**: Off **Note:** This configuration appears	Web User Interface

Parameter	Description	Configuration Method
	only if **Audio Input** is selected to **Line Input/USB Line in**. If you change this parameter, the system will reboot to make the change take effect.	

To configure the audio input device via web user interface:

1. Click on **Setting->Video & Audio**.
2. Select the desired value from the pull-down list of **Audio Input**.
3. In the **line AEC** block, mark the desired radio box.

   This configuration appears only if **Audio Input** is selected to **Line Input/USB Line in**.



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

To configure the audio input device via the remote control:

1. Select **More->Setting->Video & Audio->Audio Settings**.
2. Select the desired value from the pull-down list of **Audio Input**.
3. Select **Save**, and then press (OK) to accept the change.

Tones

When automatically answering an incoming call, the system will play a warning tone. You can customize tones or select specialized tone sets (vary from country to country) to indicate different conditions of the system. The default tones used on the system are the US tone sets. Available tone sets for the system:

- Australia
- Austria
- Brazil
- Belgium
- China
- Chile

- Czech
- Czech ETSI
- Denmark
- Finland
- France
- Germany
- Great Britain
- Greece
- Hungary
- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States

Configured tones can be heard on the system for the following conditions:

Condition	Description
Ring Back	Ring-back tone
Busy	When the callee is busy
Call Waiting	Call waiting tone
Auto Answer	When answering a call automatically

Tones parameters on the system are described below:

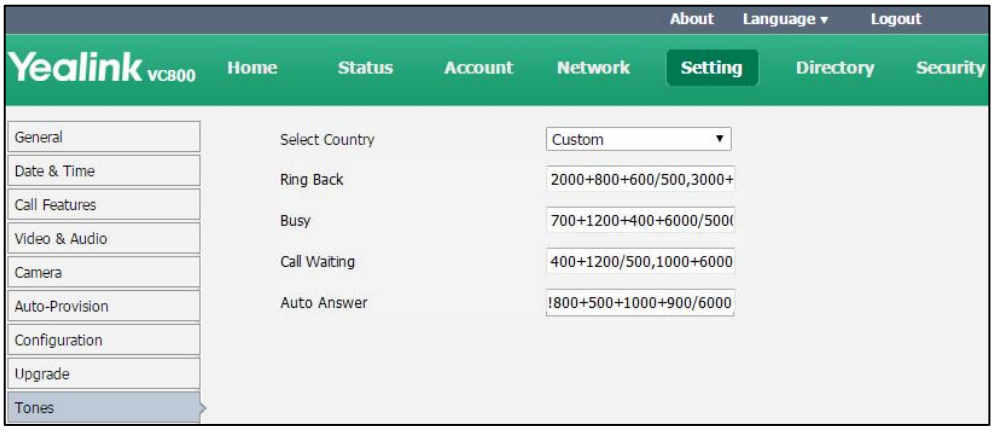
Parameter	Description	Configuration Method
Select Country	Customizes tones or selects the desired country tone set. **Default:** Custom	Web User Interface
Ring Back	Customizes the ring-back tone for the system. tone = element1[,element2] [,element3]…[,element8] Where **element** = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration **Freq**: the frequency of the tone (ranges from 200Hz to 7000 Hz). If it is set to 0Hz, it means the tone is not played. A tone consists of at most four different frequencies. **Duration**: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms. You can configure at most eight different tones for one condition, and separate them by commas. (for example: 250/200, 0/1000, 200+300/500, 600+700+800+1000/2000). If you want the system to play tones once, add an exclamation mark "!" before tones (for example: !250/200, 0/1000, 200+300/500, 600+700+800+1000/2000). **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	Web User Interface
Busy	Customizes the busy tone for the system. For more information on how to customize the tone, refer to the parameter "Ring Back".	Web User Interface

Parameter	Description	Configuration Method
	Default: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	
Call Waiting	Customizes the call waiting tone for the system. For more information on how to customize the tone, refer to the parameter "Ring Back". **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	Web User Interface
Auto Answer	Customizes the auto answer tone for the system. For more information on how to customize the tone, refer to the parameter "Ring Back". **Default**: Blank **Note**: It only works if the parameter "Select Country" is set to Custom.	Web User Interface

To configure tones via web user interface:

1. Click on **Setting**->**Tones**.
2. Select the desired value from the pull-down list of **Select Country**.

   If you select **Custom**, you can customize the tone for indicating each condition of the system.



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

Configuring Video Settings

Dual-Stream Protocol

To enhance the process of communicating with others over video, the dual-stream protocol provides the ability to share content from a computer, such as video clips or documentation. Both the video and the documentation can be transmitted to the far site simultaneously, thus meeting the requirements of different conference scenarios, such as training or medical consultation.

The Yealink video conferencing system supports the standard H.239 protocol and BFCP (Binary Floor Control Protocol). H.239 protocol is used when sharing content with the far site in H.323 calls. BFCP protocol is used when sharing content with the far site in SIP calls. Before enabling the desired protocol, ensure that the protocol is supported and enabled by the far site you wish to call. If the far site does not support the protocol for sharing content, MCU will automatically mix the content and camera video, and send them in one channel. For more information on mix sending, refer to Mix Sending on page 174.

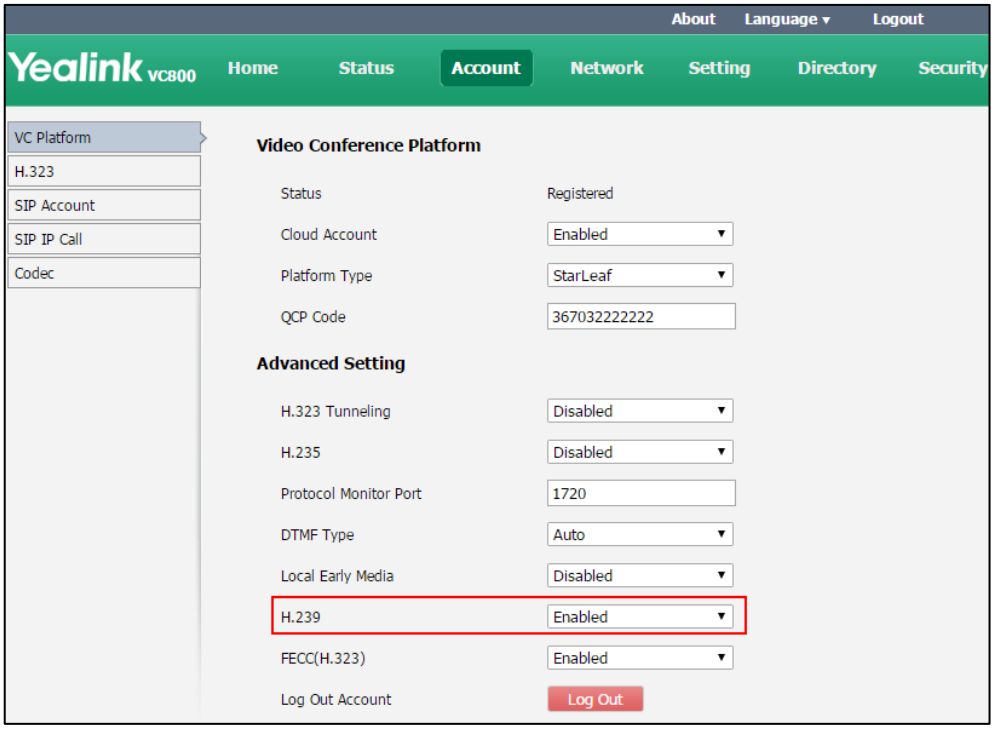
Dual-stream protocol parameters on the system are described below.

Parameter	Description	Configuration Method
H.239	Enables or disables the H.239 protocol for sharing content. You can configure it for the StarLeaf Cloud platform or H.323 call separately. **Default:** Enabled	Web User Interface
BFCP	Enables or disables the BFCP protocol for sharing content. You can configure it for Zoom/Pexip/BlueJeans/Mind/Custom platform, SIP account or SIP IP call separately. **Default:** For Zoom/Pexip/BlueJeans/Mind/Custom platform and SIP IP call, the default value is Enabled. For SIP account, the default value is Disabled. **Note:** You cannot configure it for the Yealink/StarLeaf Cloud platform.	Web User Interface

To configure H.239 dual-stream protocol for StarLeaf Cloud platform via web user interface:

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

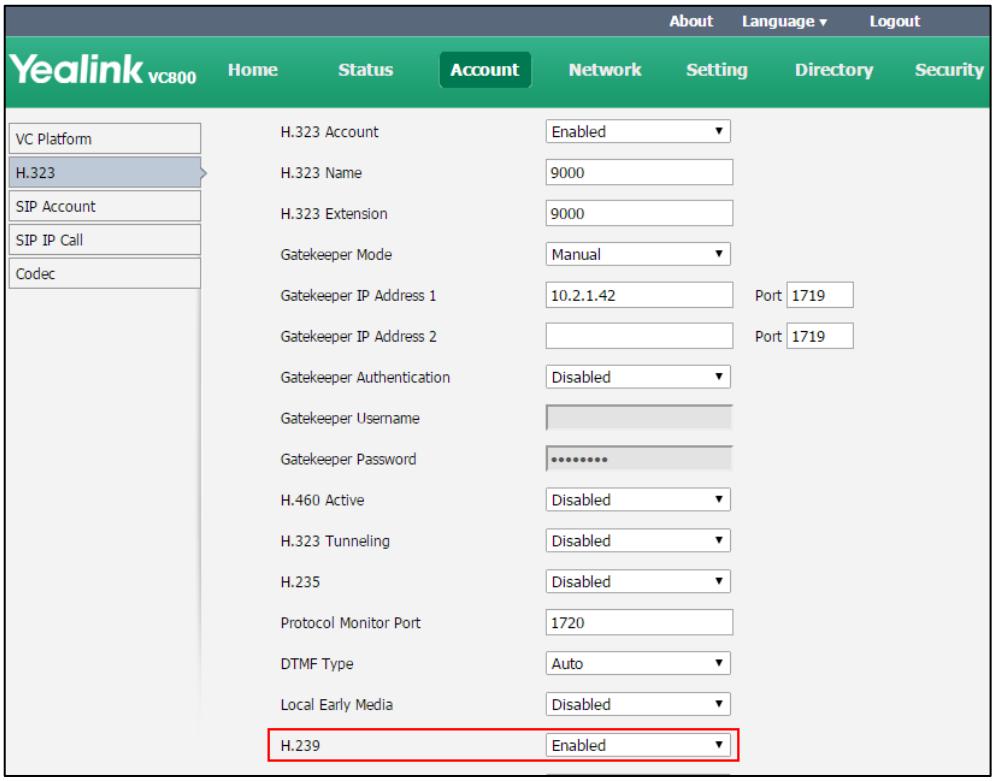
3. Select the desired value from the pull-down list of **H.239**.



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

To configure H.239 dual-stream protocol for H.323 call via web user interface:

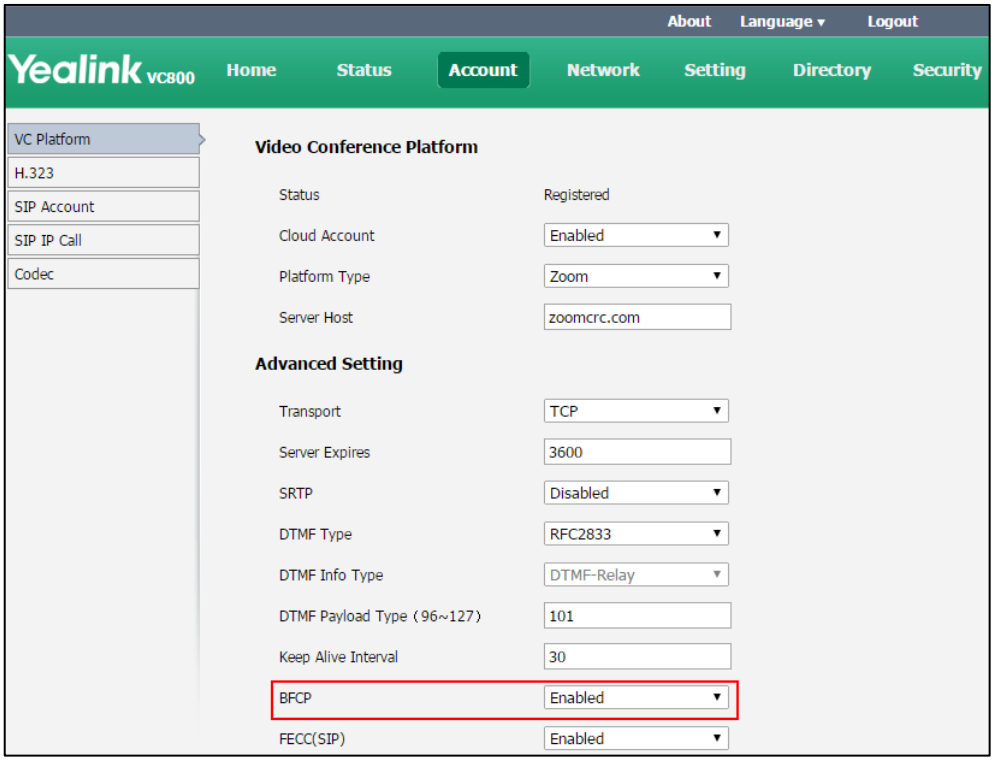
1. Click on **Account**->**H.323**.
2. Select the desired value from the pull-down list of **H.239**.



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

To configure BFCP dual-stream protocol for Zoom/Pexip/BlueJeans/Mind/Custom platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Zoom/Pexip/BlueJeans/Mind/Custom** from the pull-down list of **Platform Type**.
3. Select the desired value from the pull-down list of **BFCP**.

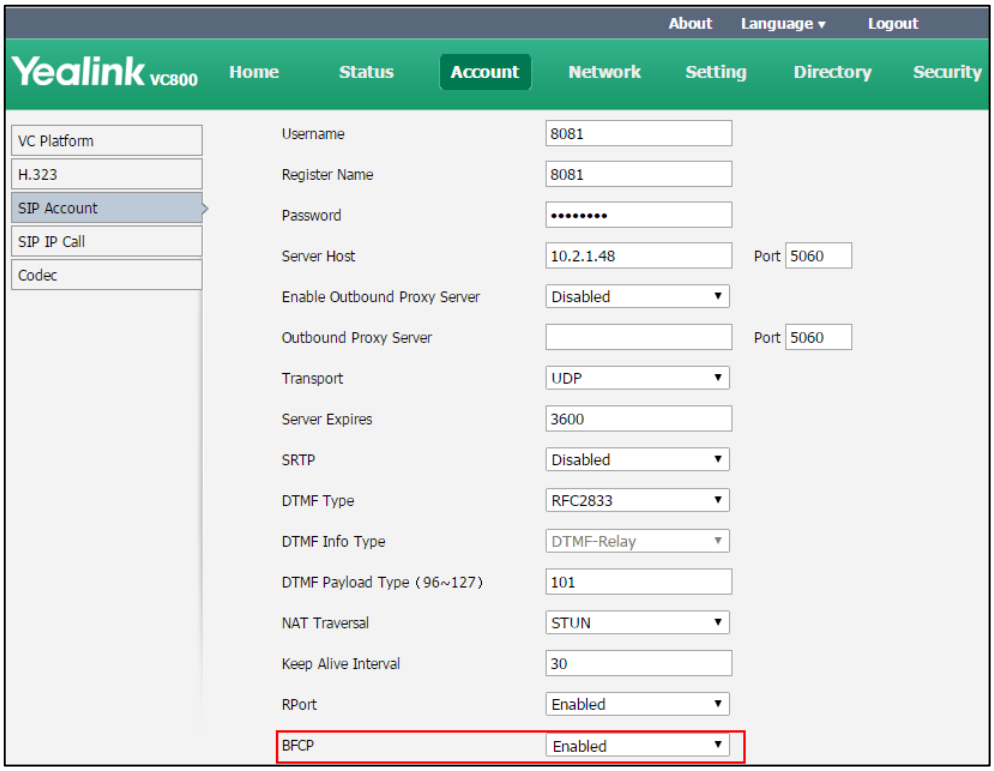


4. Click **Confirm** to accept the change.

To configure BFCP dual-stream protocol for SIP call via web user interface:

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

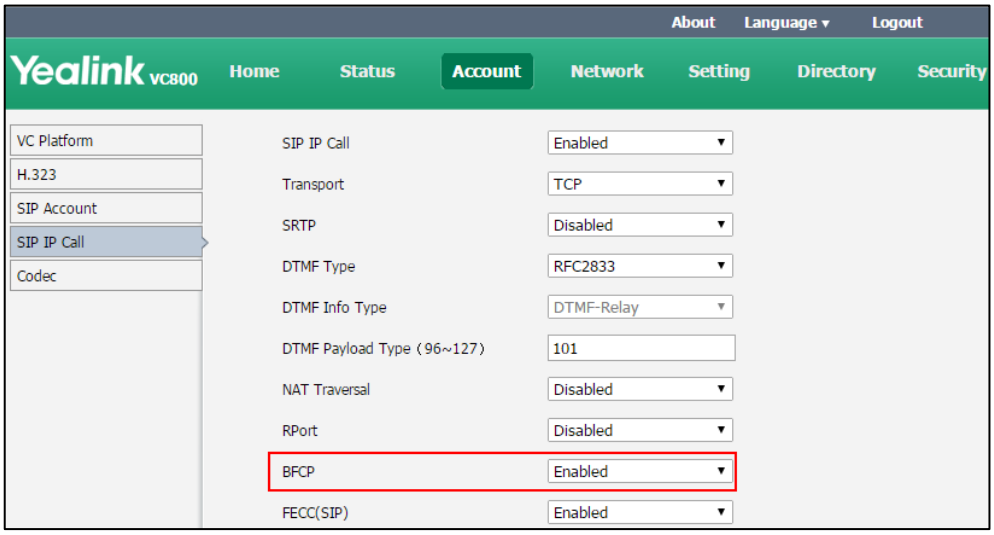
2. Select the desired value from the pull-down list of **BFCP**.



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

To configure BFCP dual-stream protocol for SIP IP call via web user interface:

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



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

Mix Sending

Content sharing allows users to share content with other conference participants during a call. When a PC is connected to the VCH50 video conferencing hub, the display device can display both the camera video and the shared content. The content sharing feature is very useful in the conference scenario in which content sharing is needed (for example: a slide or a flash).

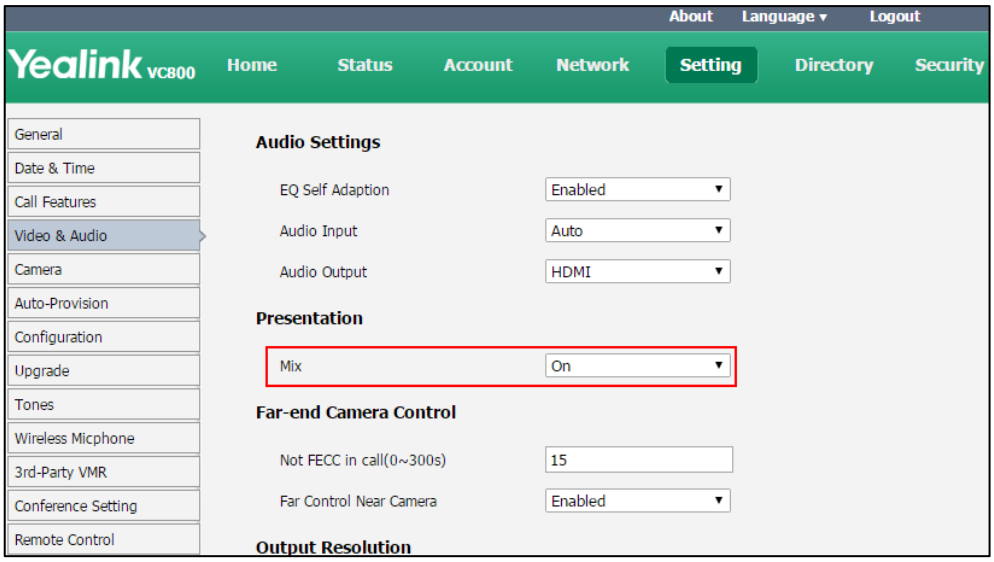
During a conference call, the far site may not support receiving shared content. In this case, you can enable mix sending feature on the system. Mix sending feature allows the sender to compound multiple video streams (local image+shared content) to one video stream, and then send it to the far site.

The mix sending parameter on the system is described below.

Parameter	Description	Configuration Method
Mix	Enables or disables the mix sending feature on the system. **Default:** On	Web User Interface

To configure mix sending via web user interface:

4. Click on **Setting**->**Video & Audio**.
5. In the **Presentation** block, select the desired value from the pull-down list of **Mix**.



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

Using VCC22 Video Conferencing Cameras

You can connect up to 8 VCC22 video conferencing cameras to the VC800 video conferencing system. For more information, refer to *Yealink VCC22 Camera Quick Start Guide*.

VCC22 video conferencing cameras are not applicable to VC500 video conferencing endpoint.

Controlling VCC22 Camera

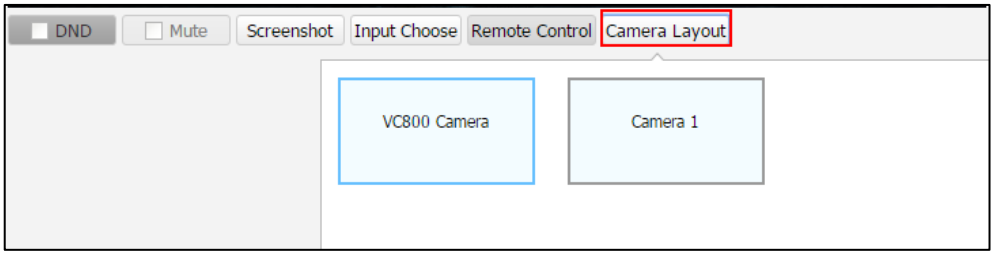
When the system is idle, you can choose the desired camera to capture video images.

Parameters of controlling VCC22 camera on the system is described below:

Parameter	Description	Configuration Method
Camera Layout	Choose the desired camera to capture video images when the system is idle. • **VC800 Camera** • **Camera 1 to 8**-the connected VCC22 conferencing cameras **Default:** VC800 Camera	Remote Control Web User Interface CP960 Conference Phone

To control VCC22 camera via web user interface:

1. Click **Home**.
2. Click **Camera Layout**.
3. Click the desired camera.



4. Hover your cursor over yourself, and then click .
5. Click the navigation key to adjust the angle of the camera.
6. Click or to adjust the focus of the camera.

To control VCC22 camera via the remote control:

1. Press to enter the cameras list.
2. Press or to scroll to the desired camera and then press OK.
3. Press the navigation key to adjust the angle of the camera.
4. Press or to adjust the focus of the camera.

To control VCC22 camera via the CP960 conference phone:

1. Tap .
2. Tap **The current control camera**.
3. Tap the desired camera.
4. Tap to return.

5. Tap the navigation key to adjust the angle of the camera.
6. Tap or to adjust the focus of the camera.

Adjusting Camera Layout

During a call, all video streams captured from the connected local cameras are synthesized to one video stream, and then sent to the far site.

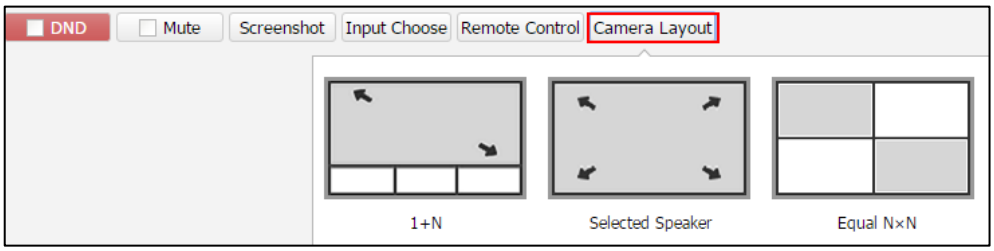
You can change the camera layout during a call.

Parameters of camera layouts on the system is described below:

Parameter	Description	Configuration Method
Camera Layout	Configures the camera layout during a video call. • **1+N**: the selected camera is given prominence in the largest pane. Other cameras are displayed in small panes. • **Selected Speaker**: the selected camera is seen in a large pane. • **Equal N×N**: every camera is given equal prominence in equal-sized panes. **Default:** 1+N	Remote Control Web User Interface CP960 Conference Phone

To adjust camera layout via web user interface:

1. Click **Home** during a call.
2. Click **Camera Layout**.



3. Click the desired camera layout.

To adjust camera layout via the remote control:

1. Press or to open **Talk Menu**.
2. Press or to scroll to **Camera Layout** and then press to enter submenu.
3. Select the desired camera layout, and then press .

To adjust camera layout via the CP960 conference phone:

1. Tap  .
2. Tap the desired layout.

Configuring Camera Settings

To display high quality video image, you can configure camera settings as required, such as white balance, exposure and sharpness.

Camera parameters are described below.

Parameter	Description	Configuration Method
Camera	Configures the desired camera. • **VC800 Camera/VC500 Camera** • **Camera 1 to 8**–select the desired VCC22 camera (it is configurable when VCC22 camera is connected). • **All Camera**–select all cameras. **Default:** VC800 Camera/VC500 Camera	Web User Interface
Status	Enables or disables the VCC22 video conferencing camera. It is configurable when VCC22 video conferencing camera is connected. **Default:** Enabled	Web User Interface
Camera Name	Configures a name for the VCC22 video conferencing camera. It is configurable when VCC22 video conferencing camera is connected. **Default:** Camera 1 to 8	Web User Interface
Exposure Compensation	Configures the value of camera exposure compensation. • Off • 1 to 12 Exposure compensation is used to compensate the camera effectively when the camera is shooting in a	Remote Control Web User Interface

Parameter	Description	Configuration Method
	backlight environment. If the environment light is dark, you can increase the compensation value. **Default:** 1	
Flicker	Configures the value of camera flicker frequency. ● 50Hz ● 60Hz **Default:** 50Hz **Note**: Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source the light is powered by.	Remote Control Web User Interface
White Balance Mode	Configures the white balance mode of the camera. ● **Auto**−Yealink recommends this setting for most situations. It calculates the best white balance setting based on lighting conditions in the room. ● **InDoor** ● **OutDoor** ● **OnePush** ● **ATW** ● **Manual**−Manually set red and blue gain. **Default:** ATW	Remote Control Web User Interface
Red Gain	Configures the red gain of the camera. **Valid Values:** 0-100 **Default:** 50 **Note**: You can set this parameter only when the white balance mode	Remote Control Web User Interface

Parameter	Description	Configuration Method
	is configured to Manual.	
Blue Gain	Configures the blue gain of the camera. **Valid Values:** 0-100 **Default:** 50 **Note**: You can set this parameter only when the white balance mode is configured to Manual.	Remote Control Web User Interface
Display Mode	Configures the display mode of the camera. • **High Definition** • **Standard** • **Mild** • **Custom Definition** **Default:** Standard	Remote Control Web User Interface
Saturation	Configures the saturation of the camera. **Valid Values:** 0-100 **Default:** 50	Remote Control Web User Interface
Sharpness	Configures the sharpness of the camera. **Valid Values:** 0-100 **Default:** 15 **Note**: The picture will be sharp and clear, but moderate to heavy motion at low call rates can cause some frames to be dropped.	Remote Control Web User Interface
Brightness	Configures the brightness of the camera. **Valid Values:** 0-100 **Default:** 50	Remote Control Web User Interface
Contrast	Configures the contrast of the camera. **Valid Values:** 0-100 **Default:** 49	Remote Control Web User Interface

Parameter	Description	Configuration Method
Noise Reduction (2D)	Specifies the noise reduction (2D) mode. ● Off ● Low ● Middle ● High **Default:** Middle	Remote Control Web User Interface
Noise Reduction (3D)	Specifies the noise reduction (3D) mode. **Valid Values:** 0-22 **Default:** 3	Remote Control Web User Interface
WDR	Specifies the wide dynamic range. ● Off-do not use WDR ● 1-5 **Default:** 2	Remote Control Web User Interface
Hangup Mode	Enables or disables the camera to flip the image view when camera is handed at up-side-down position **Default:** Off	Web User Interface
Camera Pan Direction	Configures the pan direction of the camera. ● Normal ● Reversed **Default:** Normal If the camera reversed mode is enabled, the camera pan direction 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.	Web User Interface
Reset Camera	Reset the camera settings to factory defaults. **Note:** The camera presets will also be cleared.	Web User Interface

To configure camera settings via web user interface:

1. Click on **Setting**->**Camera**.
2. Configure the camera settings.
3. Click **Confirm** to accept the change.

To configure camera settings via the remote control:

1. Select **More**->**Setting** ->**Camera Setting**.
2. Configure the camera settings.
3. Select **Save**, and then press OK to accept the change.

Far-end Camera Control

Local video is displayed on the display device of the far site during a call. For the best view, you can enable the **Far Control of Near Camera** feature to allow the far site to control the focus and angle of the local camera.

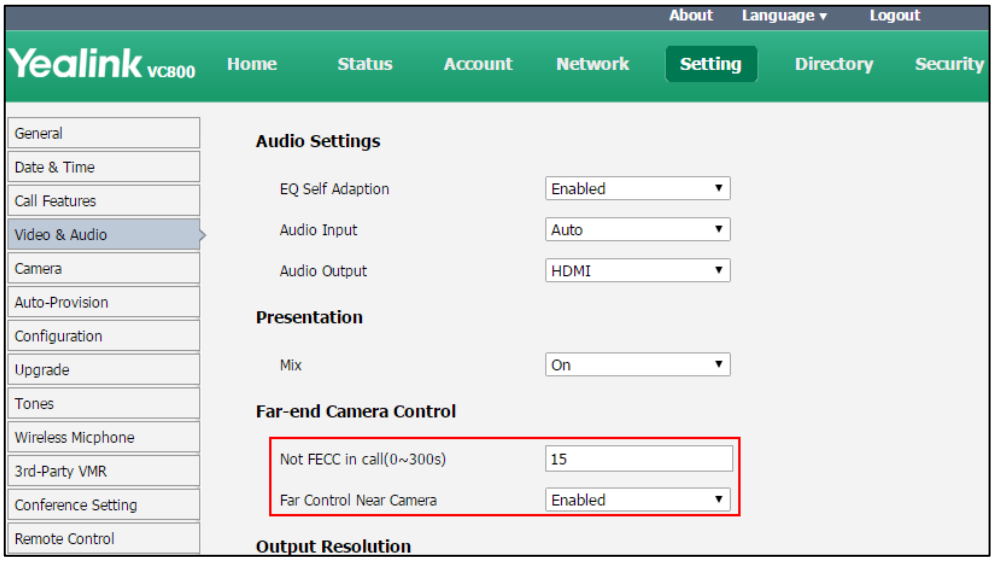
Far-end camera control parameters are described below.

Parameter	Description	Configuration Method
Not FECC in call(0~300s)	Configures the duration time (in seconds) when far site cannot control the local camera during a call. **Default:** 15 If it is set to 15, the far site is not allowed to control the local camera in the first 15 seconds of the call.	Web User Interface
Far Control Near Camera	Enables or disables the far site to control the local camera. **Default:** Enabled	Remote Control Web User Interface

To configure far-end camera control via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Enter the desired time in the **Not FECC in call(0~300s)** field.

3. Select the desired values from the pull-down lists of **Far Control Near Camera**.



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

To configure far control near Camera feature via the remote control:

1. Select More->**Setting**->**Video & Audio**.
2. Check the **Far Control Near Camera** checkbox
3. Press  to exit.

Camera Control Protocol

VC800/VC500 video conferencing system supports camera control protocols: FECC (Far End Camera Control). You can enable the FECC protocol for SIP call or H.323 call.

If far site wants to control the local camera, both the far site and near site should enable the camera control protocol simultaneously. If the FECC protocol is not enabled on either site, far-end camera control cannot be performed. For example, a SIP call is established between two sites, the two sites must enable FECC (SIP) protocol simultaneously to perform far-end camera control. If FECC (SIP) protocol and FECC (H.323) protocol are both enabled, the system will select the appropriate camera control protocol according to the protocol (SIP or H.323) the call uses.

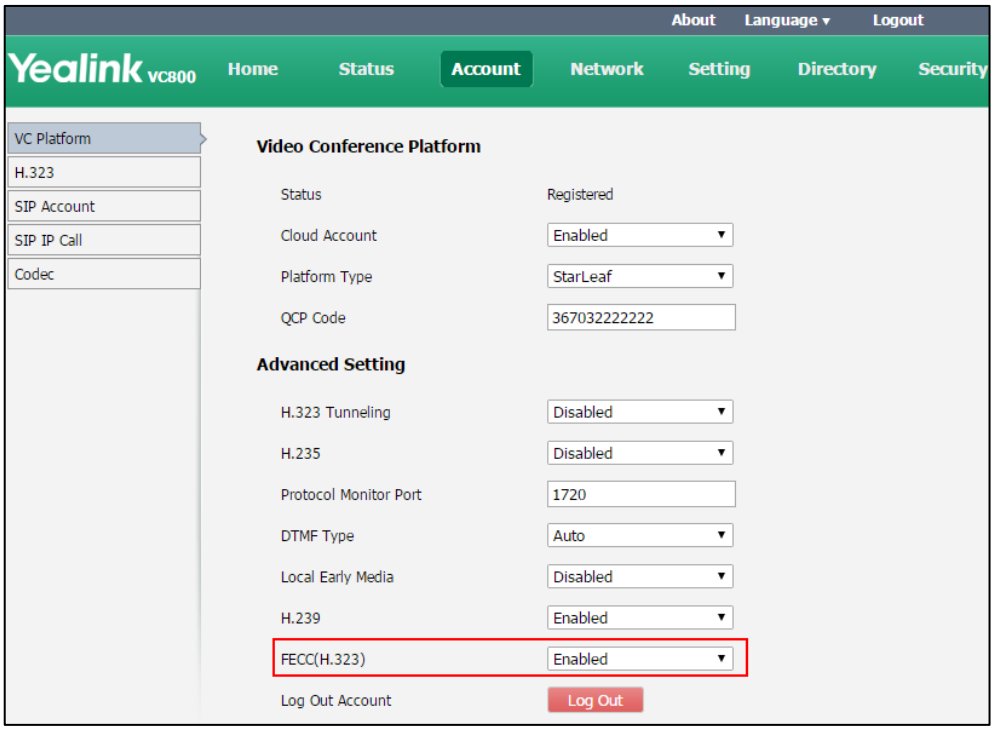
Camera control protocol parameters are described below:

Parameter	Description	Configuration Method
FECC(H.323)	Enables or disables the FECC (H.323) protocol for far site to control near camera. You can configure it for the StarLeaf Cloud platform or H.323 call separately. **Default:** Enabled	Web User Interface

Parameter	Description	Configuration Method
FECC(SIP)	Enables or disables the FECC (SIP) protocol for far site to control near camera. You can configure it for the Zoom/Pexip/BlueJeans/Mind/Custom platform, SIP account or SIP IP call separately. **Default:** For Zoom/Pexip/BlueJeans/Mind/Custom platform and SIP IP call, the default value is Enabled. For SIP account, the default value is Disabled. **Note:** You cannot configure it for the Yealink/StarLeaf Cloud platform.	Web User Interface

To configure FECC(H.323) camera control protocol for StarLeaf Cloud platform via web user interface:

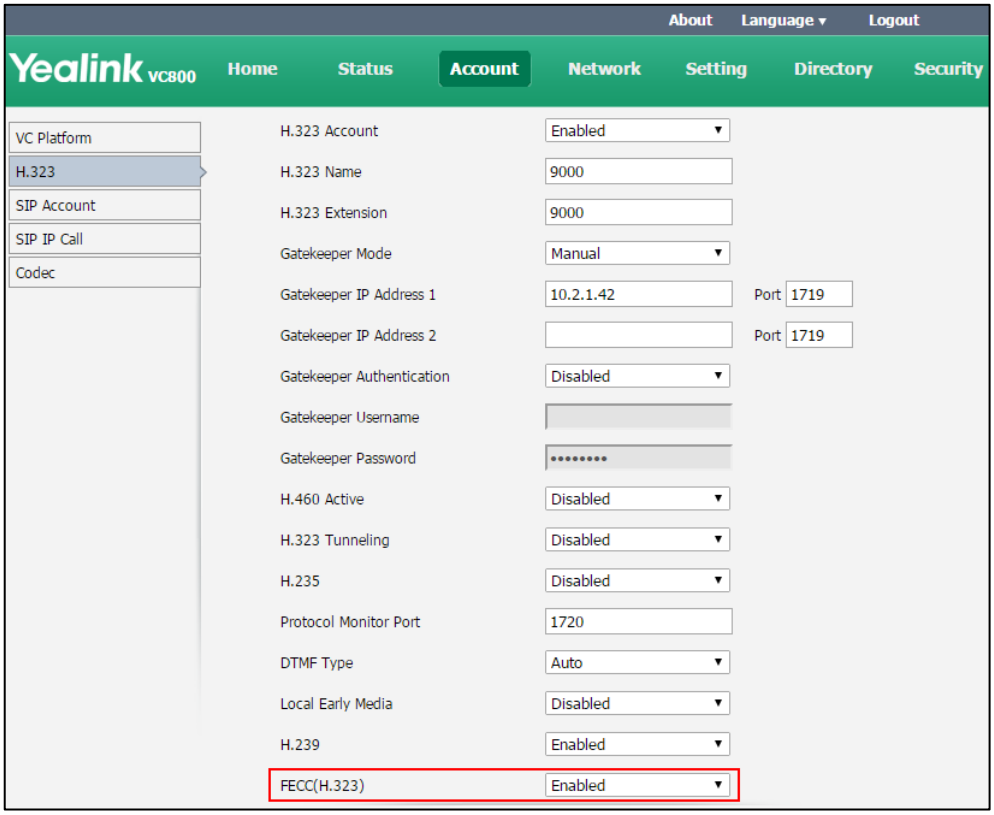
1. Click on **Account**->**VC Platform**.
2. Select **StarLeaf** from the pull-down list of **Platform Type**.
3. Select the desired value from the pull-down list of **FECC(H.323)**.



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

To configure FECC(H.323) camera control protocol for H.323 calls via web user interface:

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

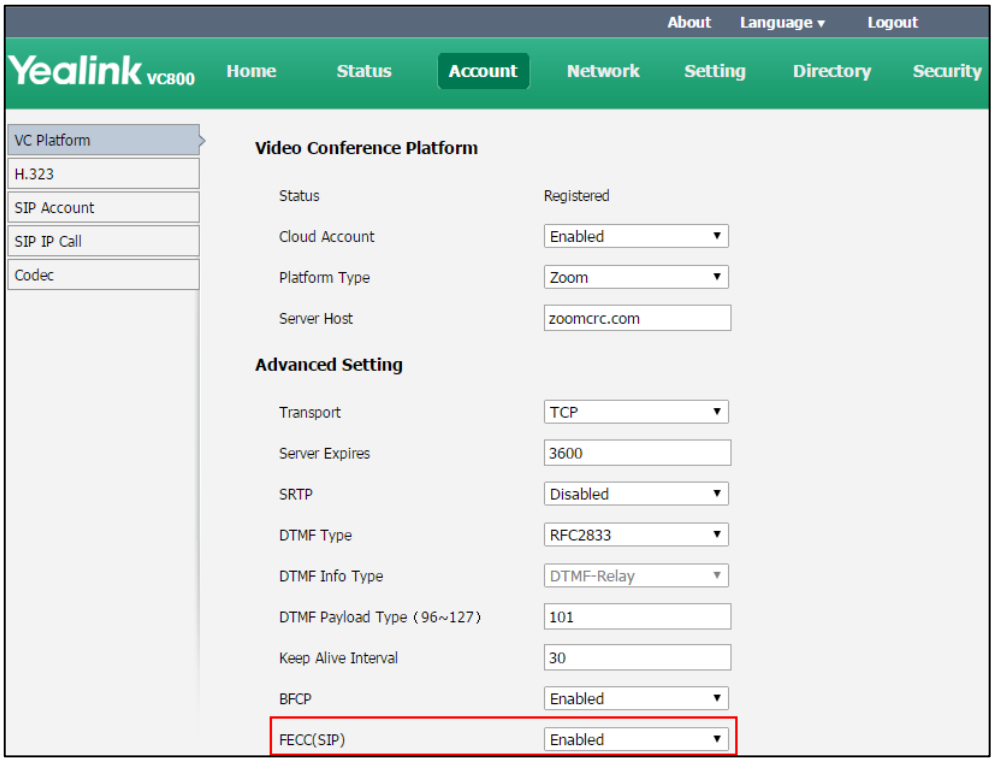


3. Click **Confirm** to accept the change.

To configure FECC(SIP) camera control protocol for Zoom/Pexip/BlueJeans/Mind/Custom platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Zoom/Pexip/BlueJeans/Mind/Custom** from the pull-down list of **Platform Type**.

3. Select the desired value from the pull-down list of **FECC(SIP)**.

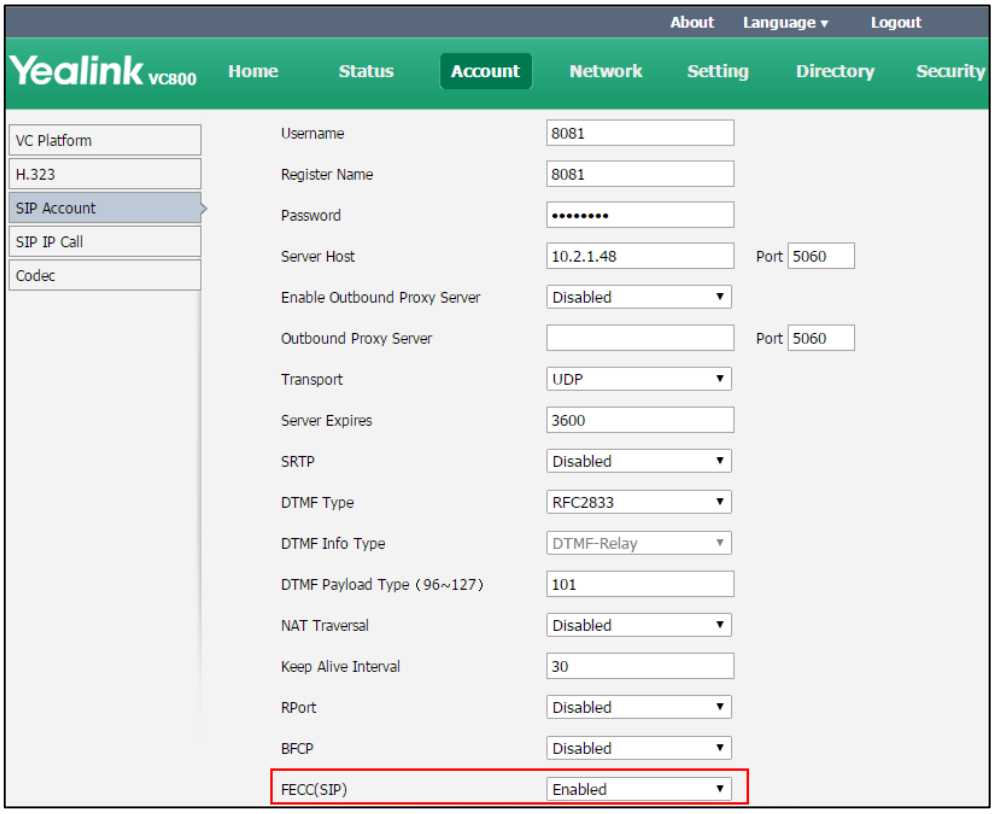


4. Click **Confirm** to accept the change.

To configure FECC(SIP) camera control protocol for SIP calls via web user interface:

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

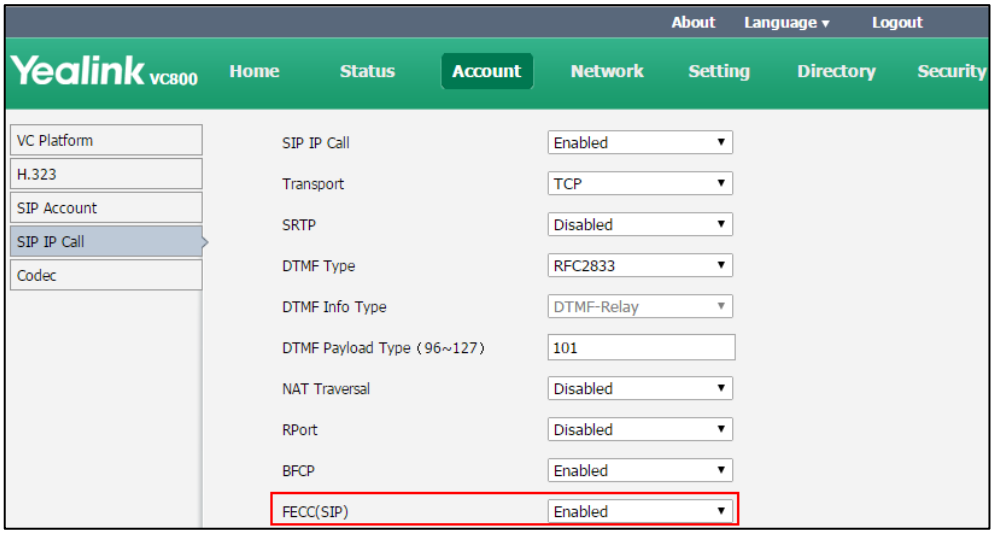
2. Select the desired value from the pull-down list of **FECC(SIP)**.



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

To configure FECC(SIP) c camera control protocol for SIP IP call via web user interface:

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



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

Consumer Electronics Control (CEC)

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.

CEC feature is enabled by default on Yealink video conferencing system. Ensure that all display devices connected to the system supports and enables CEC feature.

The following CEC features are available:

- **One Touch Play**-Use the system remote control to wake up the display devices. All connected CEC-capable display devices are powered on, and their displays are switched to VCS input.
- **System Standby**-When the VCS enters sleep mode, all connected CEC-capable display devices are switched to standby mode for power saving.

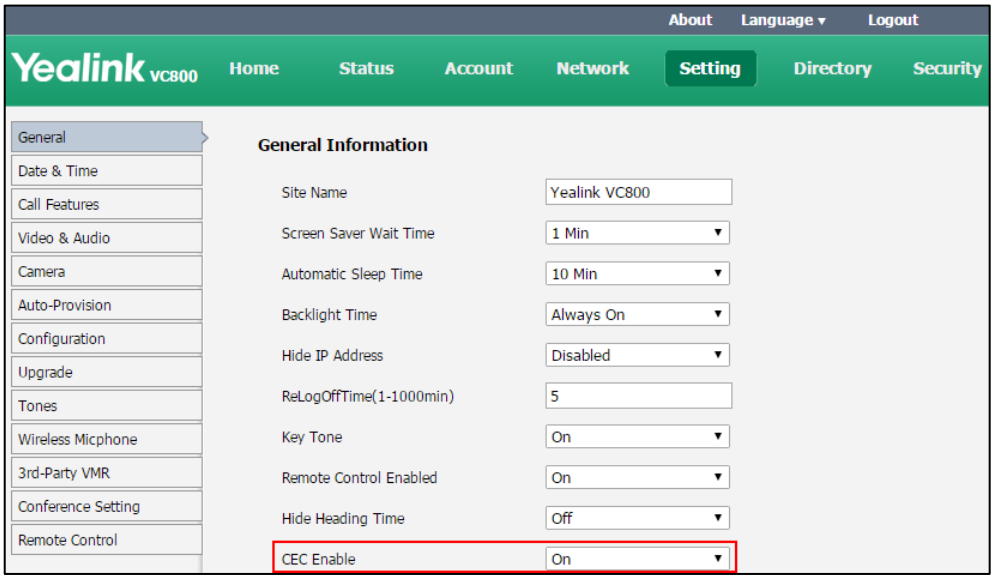
Note The VCS does not respond to CEC commands issued by a television remote control.

The CEC parameter on the system is described below.

Parameter	Description	Configuration Method
CEC Enable	Enables or disables the CEC feature. **Default:** Enabled	Web User Interface

To configure CEC feature via the web user interface:

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



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

Output Resolution

VC800/VC500 video conferencing system supports output resolution adjustment. You can adjust output resolution of primary/secondary display device respectively.

Make sure the display device has connected to the VC800/VC500 codec before configuration.

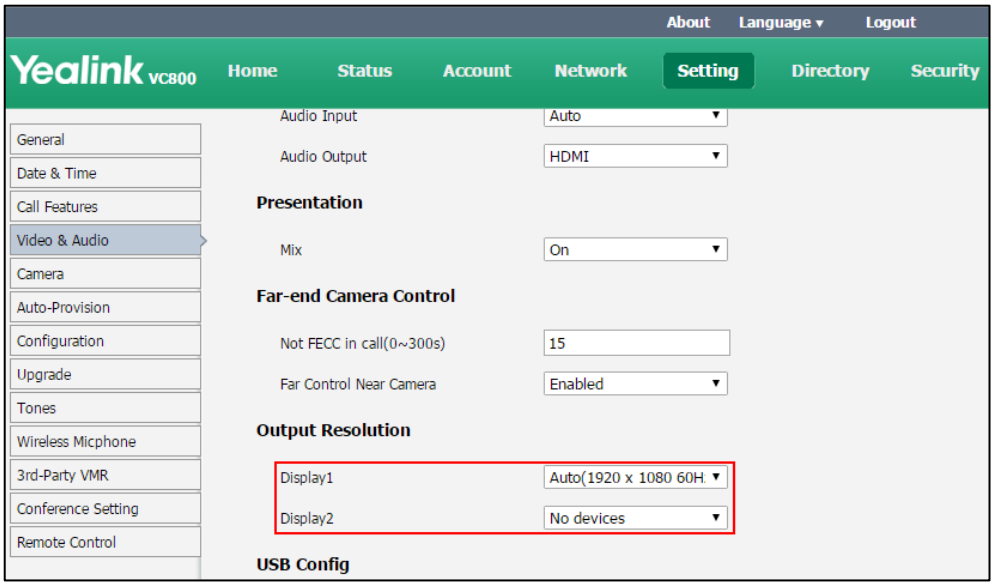
The output resolution parameters on the system are described below.

Parameter	Description	Configuration Method
Display1	Configures the output resolution of primary display device. ● **Auto**-select the highest output resolution automatically ● Available output resolutions (The available resolutions depend on the display device you are using) **Default:** Auto	Web User Interface CP960 conference phone
Display2	Configures the output resolution of secondary display device. ● **Auto**-select the highest output resolution automatically ● Available output resolutions (The available resolutions depend on the display device you are using) **Default:** Auto	Web User Interface CP960 conference phone

To configure output resolution via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Select the desired value from the pull-down list of **Display1**.

3. Select the desired value from the pull-down list of **Display2**.



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

To configure output resolution via the CP960 conference phone:

1. Tap -> **Display** -> **Output Resolution**.
2. Tap the **Diaplay1**/**Display2** field.
3. Tap the desired output resolution in the pop-up dialog box.
4. Tap to accept the change.

Video Recording

Before recording video, make sure a USB flash driver is connected to VC800/VC500 codec, VCH50 video conferencing hub or CP960 conference phone and the USB feature is enabled. For more information, please refer to USB Configuration on page 159.

The recorded video will be saved in .mkv format and named as the recorded time and date. Video can be played on either the system itself or on a computer using an application capable of playing .wav files.

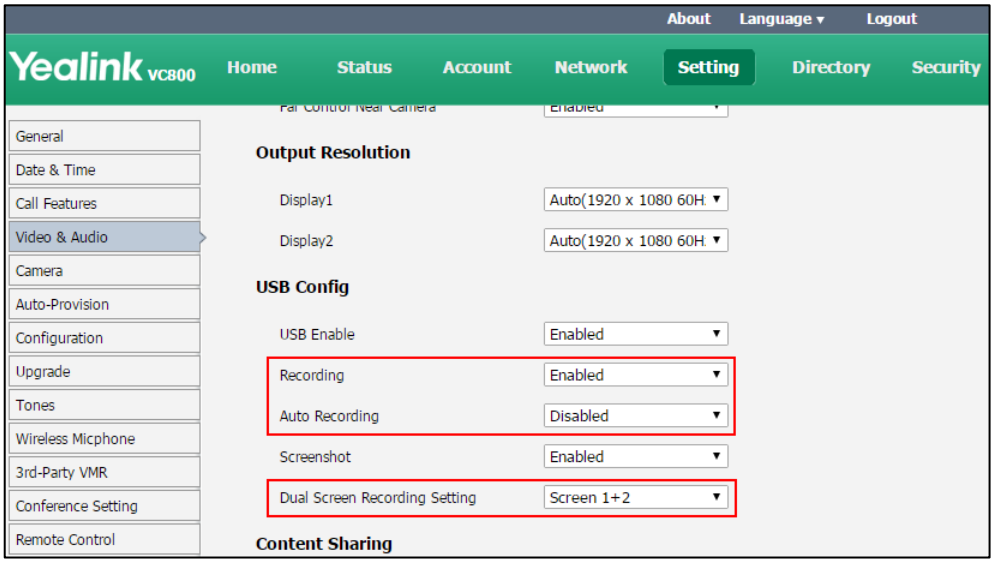
The video recording parameters on the system are described below.

Parameter	Description	Configuration Method
Recording	Enables or disables the video recording feature on the system. **Default:** Enabled If it is set to Disabled, you cannot record video.	Web User Interface
Auto Recording	Enables or disables the system to start recording automatically once a call is established. **Default:** Disabled. **Note**: The auto recording feature is available only when the recording feature is enabled.	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	Web User Interface

To configure video recording via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Select the desired value from the pull-down list of **Recording**.
3. Select the desired value from the pull-down list of **Auto Recording**.

4. If you connect dual screen, select the desired value from the pull-down list of **Dual Screen Recording Setting**.



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

To record video via the remote control via the remote control:

1. Press to start recording and then press again to stop recording.
   When you start recording, the display device will show and the recording time. When you stop recording, the recording icon disappears from the screen. The display device prompts "USB record succeed".

To record video via the CP960 conference phone via the CP960 conference phone:

1. Tap to start recording and then tap to stop recording.
   When you start recording, the status bar of touch screen will prompt "Recording". When you stop recording, the display device prompts "USB record succeed".

Screenshot

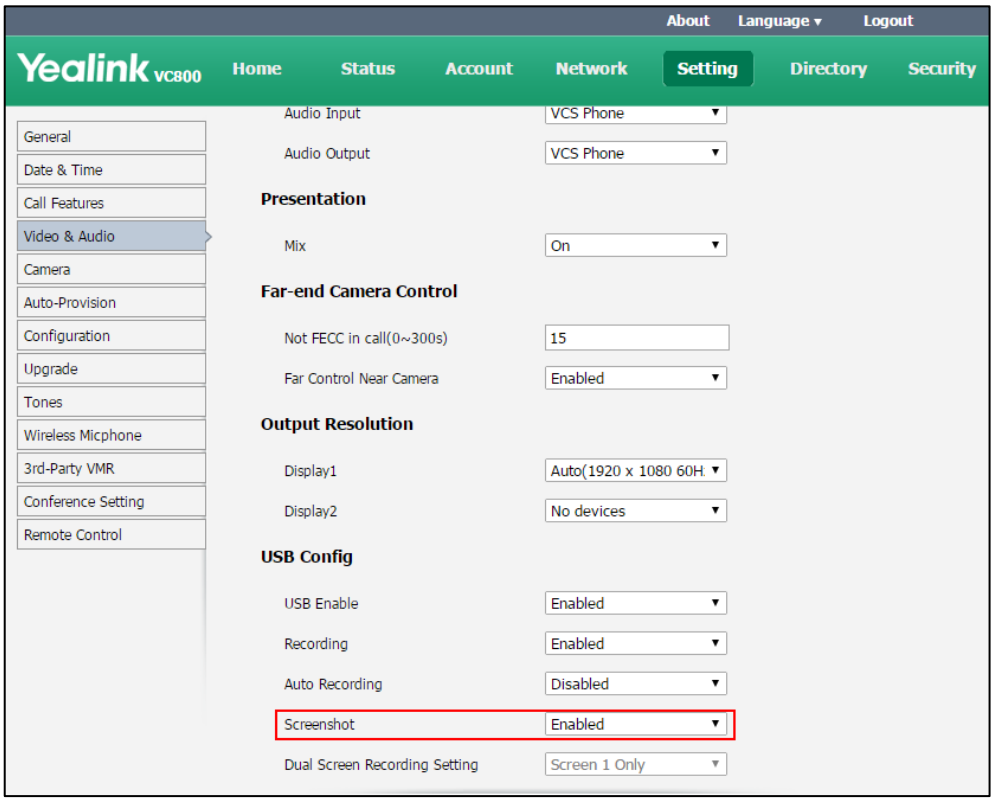
You can capture the screenshot from the camera via the remote control, CP960 conference phone or web user interface. Make sure a USB flash driver is connected to VC800/VC500 codec, VCH50 video conferencing hub or CP960 conference phone and the USB feature is enabled. For more information, please refer to USB Configuration on page 159.

The screenshot parameter on the system is described below.

Parameter	Description	Configuration Method
Screenshot	Enables or disables the screenshot feature on the system. **Default:** Enabled If it is set to Disabled, you cannot capture screenshot.	Web User Interface

To configure screenshot via web user interface:

1. Click on **Setting**->**Video & Audio**.
2. Select the desired value from the pull-down list of **Screenshot**.



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

To capture screenshots via the web user interface when the system is idle or during a call:

1. Click **Home**
2. Click **Screenshot**.

To capture screenshots via the remote control when the system is idle or during a call:

1. If  is set to **Screenshot** key, press  to capture screenshot.

   For more information on how to customize the key, refer to Custom Key on page 139.

To capture screenshots via the CP960 conference phone when the system is during a call:

1. Tap  ->  .

System Management

This chapter provides operating instructions, such as managing directory, call history and dual screen. Topics include:

Directory

VC800/VC500 system can display: local contacts, Yealink Cloud contacts and YMS contacts.

- **Local contacts:** The VC800 system can store up to 500 local contacts and 100 conference contacts (conference contacts are available only when a multipoint license is imported to the VC800 system. The VC500 endpoint can store up to 500 local contacts, and does not support conference contacts).

  A conference contact consists of one or more local contacts. You can establish a conference call quickly by calling conference contacts.

  You can import or export local contact list to different systems to share the local directory. The system only supports the XML and CSV format contact lists. You can manage local directory via web user interface, remote control and the CP960 conference phone.

- **Yealink Cloud contacts**: If you log into the Yealink VC Cloud Management Service platform, Yealink Cloud contacts which are created by your cloud enterprise administrator, appear in your directory. Note that only the cloud enterprise administrator can add, edit and delete Yealink Cloud contacts on the Yealink VC Cloud management service. On your VC800/VC500, you can only search for and place calls to the Yealink Cloud contacts. For more information on Yealink VC Cloud management service, refer to *Yealink VC Cloud Management Service Administrator Guide*.

- **YMS contacts**: If you log into the Yealink Meeting Server, enterprise directory which is created by your enterprise administrator, appears in your directory. Note that only the enterprise administrator can add, edit and delete YMS contacts on Yealink Meeting Server (YMS). For more information on Yealink Meeting Server, please refer to *Yealink Meeting Server Administrator Guide*. On VC800/VC500, you can only place calls to or search for YMS contacts.

- There are four types of YMS contact:

  - **User**：The users have YMS accounts. The enterprise administrator can create

departments for users.

- **Room system**: The devices registered YMS accounts in the video meeting room.
- **Third party device**: The devices without YMS accounts.
- **VMR**: It is also called the Permanent VMR. The enterprise administrator can determine whether to synchronize the permanent VMR to the VC800/VC500.

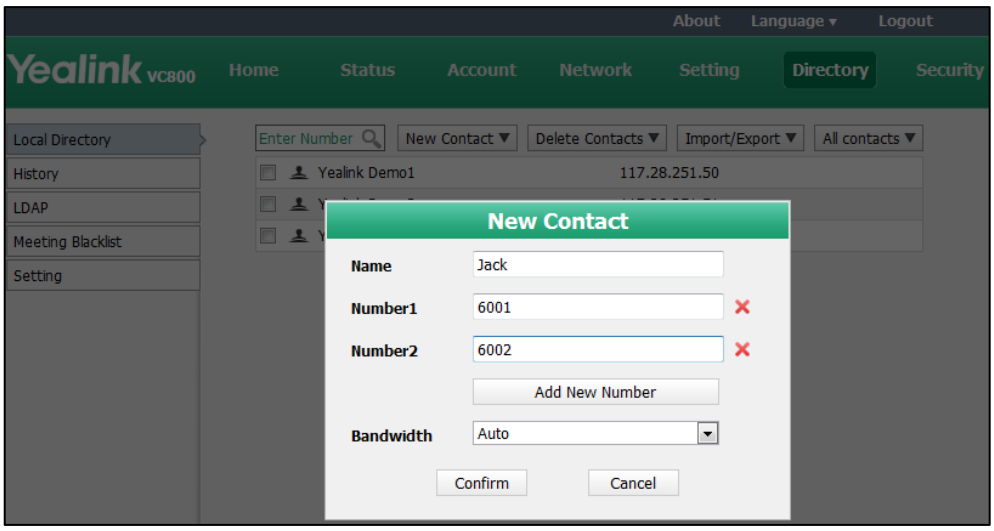
Note StarLeaf/Zoom/Pexip/BlueJeans/Mind platform does not provide Cloud contacts for video conferencing system.

The following sections give you detailed steps on how to manage the local directory.

To add local contacts via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Select **Local** from the pull-down list of **New Contact**.
3. Enter the desired name in the **Name** field.
4. Enter the desired number in the **Number** field.
5. Click **Add Number,** enter other number of the contact.
6. Select the desired contact bandwidth from the pull-down list of **Bandwidth**.

   The default contact bandwidth is **Auto**. The system will select the appropriate bandwidth automatically

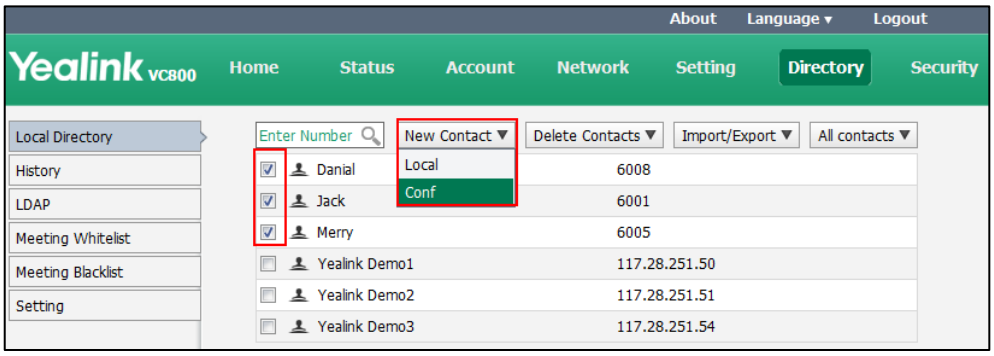


7. Click **Confirm** to accept the change.

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 Video Call Rate on page 130.

To add conference contacts (only applicable to VC800 with a multipoint license) via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Check the checkboxes of the desired contacts.
3. Select **Conf** from the pull-down list of **New Contact**.
4. Click **New Contact**, and select **Conf**.

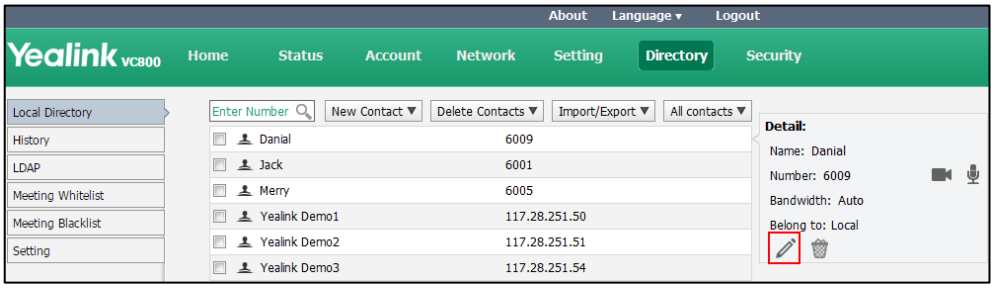


5. Enter the desired name in the **Conference Name** field.

   If multiple numbers are stored for the selected contacts, the system will select number 1 by default.
6. Click **Confirm** to accept the change.

To edit contacts via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Hover your cursor over the local contact you want to edit.
3. Click  in the pop-up detail box.

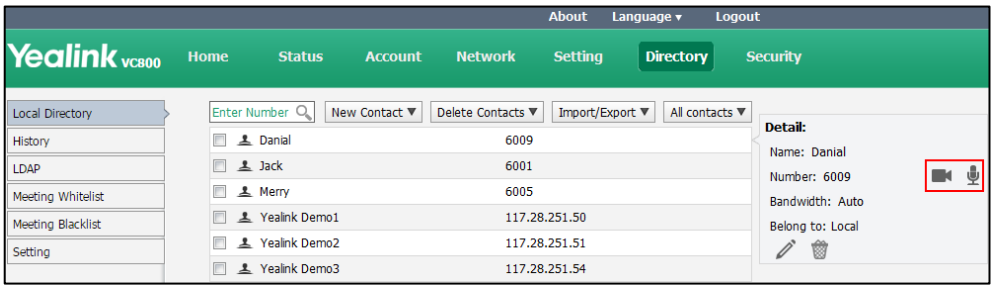


4. Edit the contact information.
5. Click **Confirm** to accept the change.

To place calls to local contacts from the local directory via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Hover your cursor over the desired local contact.

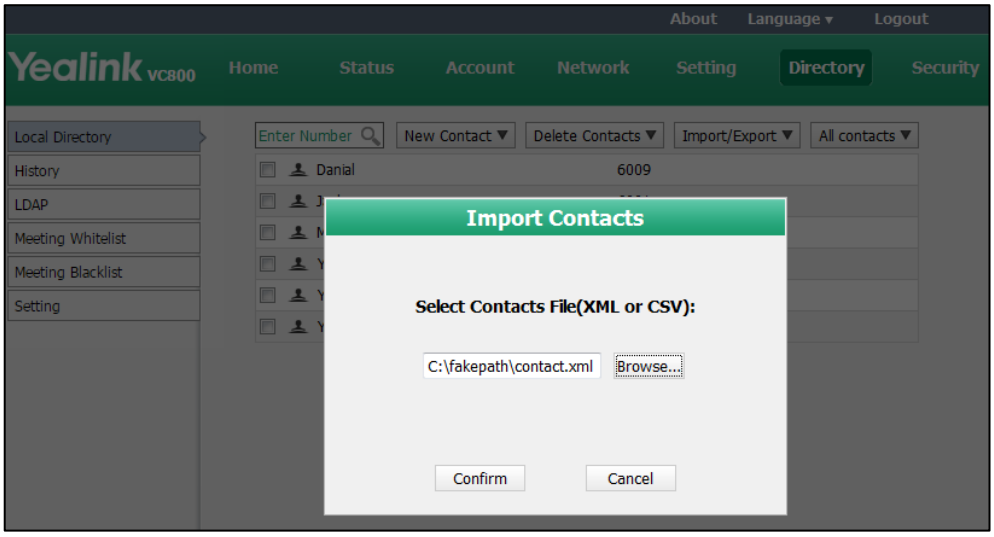
3. Click or in the pop-up detail box to place a video or voice call.



The web user interface prompts" Connecting, please wait!" and jumps automatically to the **Home** screen.

To import an XML file of the local contact list via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Select **Import** from the pull-down list of **Import/Export**.
3. Click **Browse** to locate a local contact list file (file format must be *.xml) from your local system.



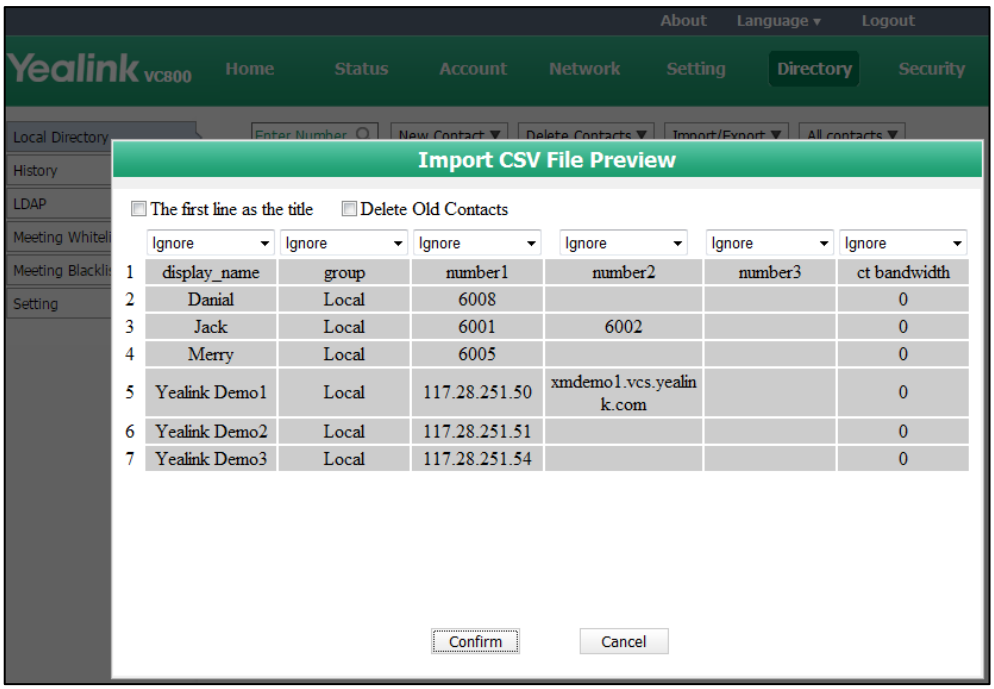
4. Click **Confirm** to import the local contact list.

   The web user interface prompts "Contacts imported successfully!".

To import a CSV file of local contact list via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Select **Import** from the pull-down list of **Import/Export**.
3. Click **Browse** to locate a local contact list file (file format must be *.csv) from your local system.
4. Click **Confirm**.

The web user interface is shown below:



5. (Optional.) Check the **The first line as the title** checkbox.

   It will prevent importing the title of the local contact information which is located in the first line of the CSV file.

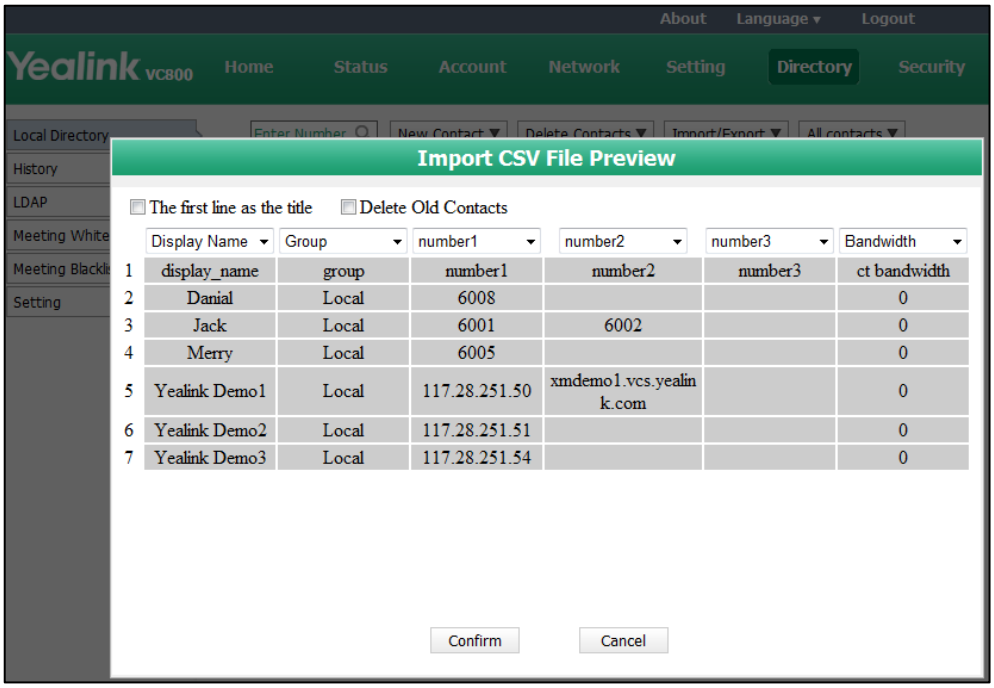
6. (Optional.) Check the **Delete Old Contacts** checkbox.

   It will delete all existing local contacts while importing the contact list.

7. Select the desired value from the pull-down list.

   - If **Ignore** is selected, this column will not be imported to the system.
   - If **Display Name** is selected, this column will be imported to the system as the local contact's name.
   - If **number** is selected, this column will be imported to the system as the local contact's number.

- If **Bandwidth** is selected, this column will be imported to the system as the local contact's bandwidth.

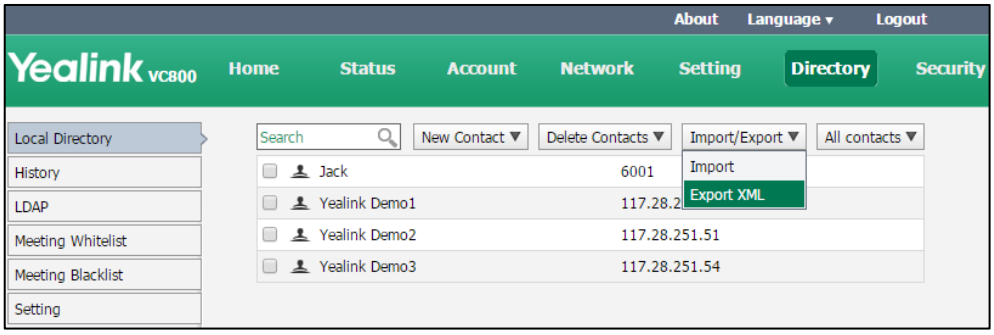


8. Click **Confirm** to complete importing the local contact list.

   The web user interface prompts "Contacts imported successfully!".

To export a XML file of the local contact list via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Select **Export XML** from the pull-down list of **Import/Export**.



The local contact list is saved to your local system.

LDAP

LDAP (Lightweight Directory Access Protocol) is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. Yealink VC800/VC500 system is configurable to interface with a enterprise directory server that supports LDAP version 2 or 3.

The following LDAP servers are supported:

- Microsoft Active Directory
- Sun ONE Directory Server
- Open LDAP Directory Server
- Microsoft Active Directory Application Mode (ADAM)

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using the system. Therefore they do not have to maintain the local directory. Users can search for and dial out from the LDAP directory and save LDAP entries to the local directory. LDAP entries displayed on the display device screen are read only. They cannot be added to, edited or deleted by users. When an LDAP server is configured properly, the system can look up entries from the LDAP server in a wide variety of ways. The LDAP server indexes all the data in its entries, and "filters" may be used to select the desired entry or group, and retrieve the desired information.

Configurations on the system limit the amount of displayed entries when querying from the LDAP server, and decide how the attributes are displayed and sorted.

Performing a LDAP search on the system:

- Enter search content in the dialing screen. (Ensure that the LADP is in the enabled search source lists)
- In the **Directory** screen, select **Company** to enter the LDAP search screen, and then enter a few characters which you want to search.

The system will send the search request to the LDAP server, the LDAP server then performs a search based on the entered content and configured filter condition, and returns results to the system.

LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on the system:

Abbreviation	Name	Description
gn	givenName	First name
cn	commonName	LDAP attribute is made up from given name joined to surname.
sn	surname	Last name or family name
dn	distinguishedName	Unique identifier for each entry
dc	dc	Domain component
-	company	Company or organization name
-	telephoneNumber	Office phone number
mobile	mobilephoneNumber	Mobile or cellular phone number

Abbreviation	Name	Description
ipPhone	IPphoneNumber	Home phone number

LADP parameters are described below:

Parameter	Description	Configuration Method
LDAP Enable	Enables or disables the LDAP feature on the system. **Default:** Disabled	Web User Interface
LDAP Name Filter	Configures the name attribute for LDAP searching. **Example:** (|(cn=%)(sn=%))	Web User Interface
LDAP Number Filter	Configures the number attribute for LDAP searching. **Example:** (|(telephoneNumber=%)(mobile=%))	Web User Interface
LDAP TLS Mode	Configures the connection mode between the LDAP server and video conferencing system. ● **LDAP**−Unencrypted connection between LDAP server and the system (port 389 is used by default). ● **LDAP TLS Start**−TLS/SSL connection between LDAP server and the system (port 389 is used by default). ● **LDAPs**−TLS/SSL connection between LDAP server and the system (port 636 is used by default). **Default:** LDAP	Web User Interface
LDAP Server Address	Configures the domain name or IP address of the LDAP server.	Web User Interface
Port	Configures the LDAP server port. **Default:** 389	Web User Interface

Parameter	Description	Configuration Method
LDAP User Name	Configures the user name used to log into the LDAP server. **Note:** The user name is provided by the server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user name to access the LDAP server.	Web User Interface
LDAP Password	Configures the password to log into the LDAP server. **Note:** The password is provided by the server administrator. If the LDAP server allows 'anonymous' to login, you don't need to provide the user password to access the LDAP server.	Web User Interface
LDAP Base	Configures the root path of the LDAP search base. **Example:** cn=manager,dc=yealink,dc=cn	Web User Interface
Max Hit(1~32000)	Configures the maximum number of search results to be returned by the LDAP server.	Web User Interface
LDAP Name Attributes	Configures the name attributes of each record to be returned by the LDAP server. **Note:** multiple name attributes should be separated by spaces. **Example**: cn sn	Web User Interface
LDAP Number Attributes	Configures the number attributes of each record to be returned by the LDAP server. **Note:** multiple numbers attributes should be separated by spaces. **Example**: telephoneNumber mobile	Web User Interface
LDAP Display Name	Configures the display name of the contact record displayed on the LCD screen. **Note:** multiple numbers attributes should be separated by spaces.	Web User Interface

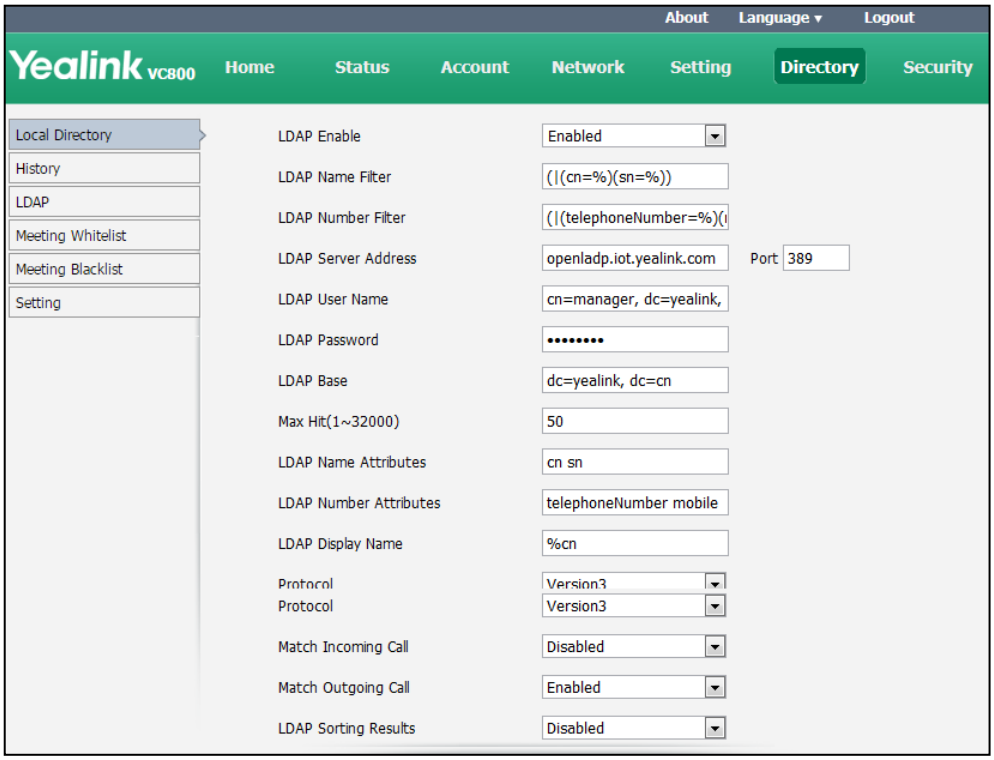
Parameter	Description	Configuration Method
	Example: %cn	
Protocol	Configures the protocol for the LDAP server. **Note:** Make sure the protocol value corresponds with the version assigned on the LDAP server.	Web User Interface
Match Incoming Call	Enables or disables the system to match caller numbers with LDAP contacts. **Default**: Disabled **Note:** If the match is successful, the system will display the caller name when receives an incoming call.	Web User Interface
Match Outgoing Call	Enables or disables the system to match outgoing call numbers with LDAP contacts. **Default**: Enabled **Note:** If the match is successful, the system will display the contact name when places a call.	Web User Interface
LDAP Sorting Results	Enables or disables the system to sort the search results in alphabetical order or numerical order. **Default**: Disabled	Web User Interface

For more information on string representations of LDAP query filters, refer to RFC 2254.

To configure LDAP via web user interface:

1. Click on **Directory**->**LDAP**.
2. Enter the desired values in the corresponding fields.

3. Select the desired values from the corresponding pull-down lists.



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

Call History

The VC800/VC500 video conferencing system maintains call history lists of All Calls, Missed Calls, Placed Calls and Received Calls. The system supports up to 100 history entries, including local history entries and Cloud history entries.

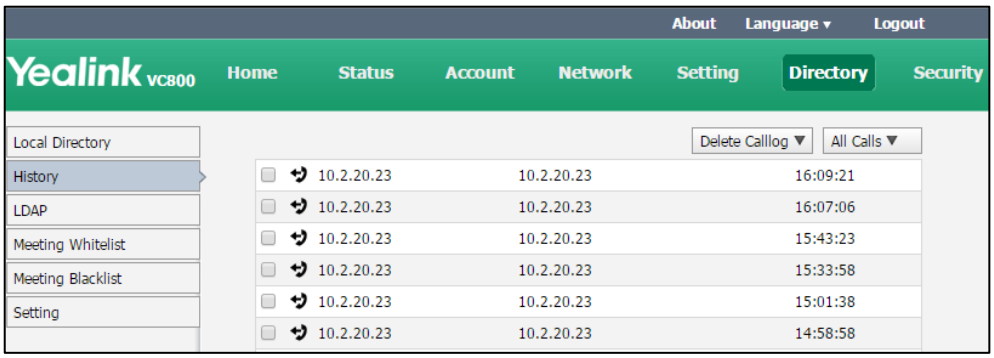
You can view the call history, place a call or delete an entry from the call history list. You can view the call history and place a call from the call history list via web user interface or the remote control, but you can delete call history only via web user interface.

History record feature is enabled by default. If it is disabled, the call history won't be saved. For more information, refer to History Record on page 126.

To view call history via web user interface:

1. Click on **Directory**->**History**.

The web user interface displays all call history.



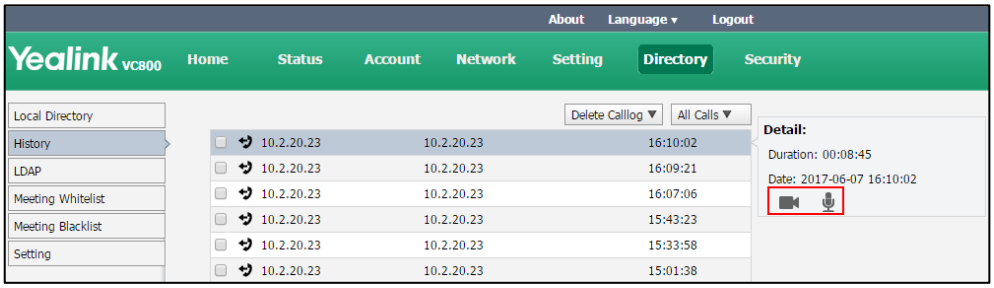
2. Click **All Calls**, select the desired call history list.

To place a call from the call history list via web user interface:

1. Click on **Directory**->**History**.

   The web user interface displays all call history.

2. Hover your cursor over the entry you want to call.
3. Click or in the pop-up detail box to place a video or voice call.



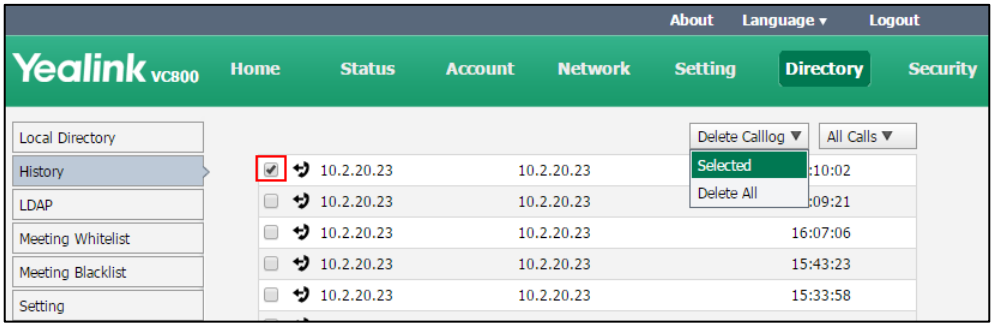
The web user interface prompts" Connecting, please wait!" and jumps automatically to the **Home** screen.

To delete an entry from the call history list via web user interface:

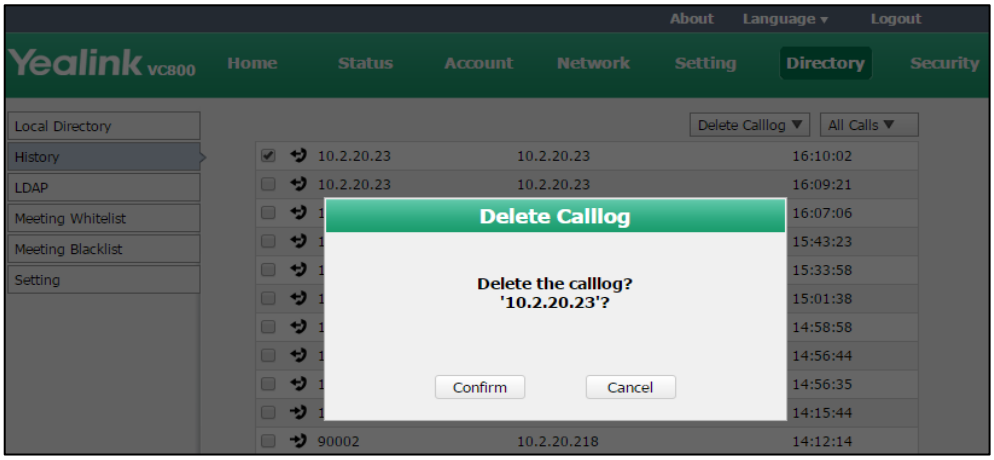
1. Click on **Directory**->**History**.

   The web user interface displays all call history.

2. Check the checkbox for the entry you want to delete.
3. Click **Delete Calllog**, and select **Selected**.



The web user interface prompts "Delete the calllog 'xxx'? "



5. Click **Confirm** to delete the call log.

You can also select **Delete All** from the from the pull-down list of **Delete Calllog** to delete all call log.

Search Source List in Dialing

When you enter a few characters in the dialing screen, the system will search for contacts from the enabled search source lists, and display the result in the dialing screen. The lists can be History, Local Directory, Cloud Contacts, YMS contacts and LDAP.

Note Cloud contacts and YMS contacts appear in the search source list only when you log into the Yealink VC Cloud Management Service or register a YMS account.

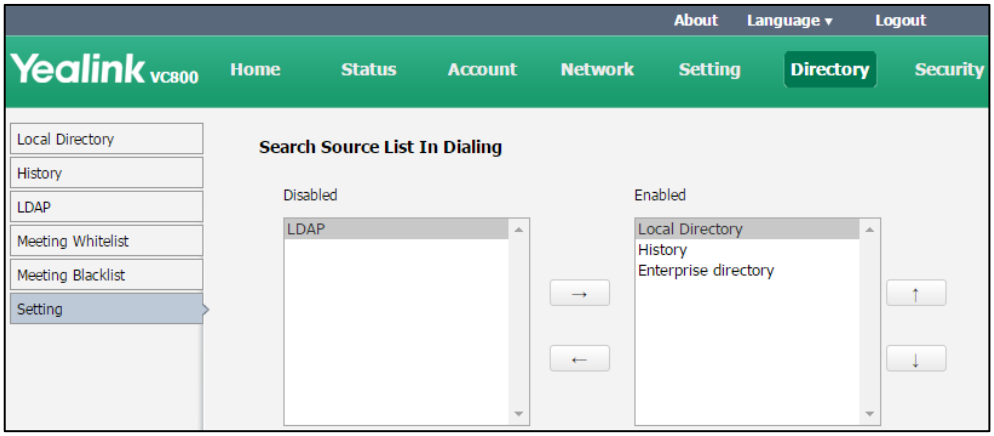
To match the desired list, you need to enable the search source list first. If you want to match the LADP list, make sure LDAP is already configured. For more information on how to configure LDAP, refer to LDAP on page 200.

To configure search source list in dialing via web user interface:

1. Click on **Directory**->**Setting**.
2. In the **Search Source List In Dialing** block, select the desired list from the **Disabled** column and click →.

   The selected list appears in the **Enabled** column.
3. Repeat step 2 to add more lists to the **Enabled** column.
4. (Optional.) To remove a list from the **Enabled** column, select the desired list and then click ←.

5. To adjust the display order of the enabled list, select the desired list, and click ↑ or ↓.



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

License

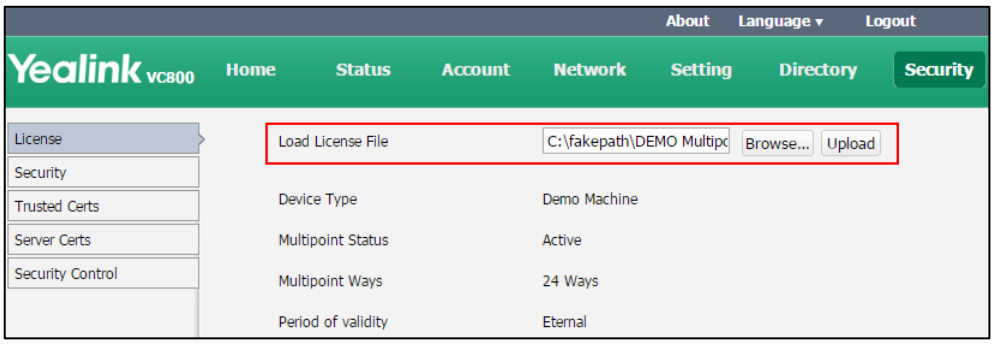
Device Type License

If the VC800/VC500 is a demo machine, namely it is used by agents to demonstrate system functions to the customers. The display device will prompt "DEMO ONLY, NOT FOR RESELL".

A DEMO machine supports 24 ways multipoint calls (an original caller and 24 other sites). You can change the VC800/VC500 from a demo machine to be a normal machine by importing a device type license. After changing to a normal machine, the VC800/VC500 supports one video call and a voice call (an original caller and two other sites). The device type license is configurable via web user interface only.

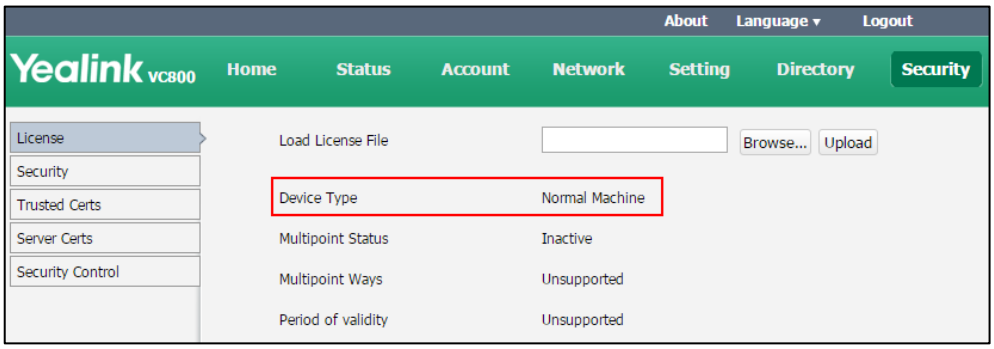
To import the device type license via web user interface:

1. Click on **Security**->**License**.
2. Click **Browse** to locate the device type license (the file format must be *.dat) from your local system.



3. Click **Upload** to complete importing the device type license.

   The device type will change from "Demo Machine" to "Normal Machine".



Multipoint License

You can use your VC800 system to participate in multipoint conferences. Multipoint conferences require a multipoint license. Multipoint license is configurable via web user interface only. Multipoint license is not applicable to VC500 endpoint.

Maximum connections of the multipoint licenses are described as below.

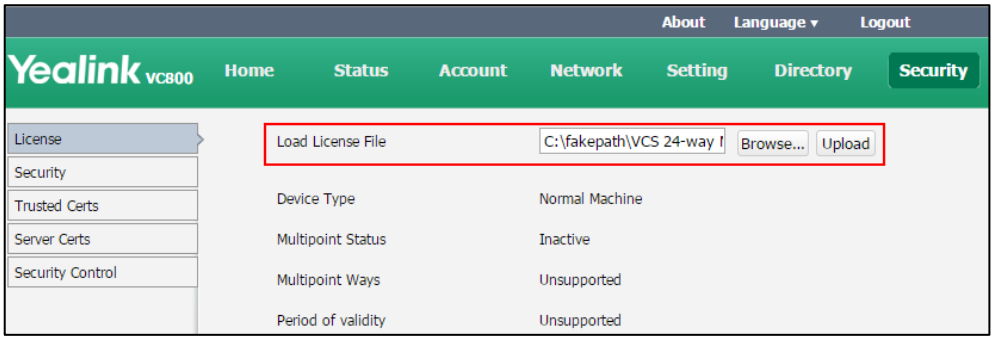
Multipoint License Type	Maximum Connections	Description
VC800 without a multipoint license	One video call with a presentation and 5 voice calls (a conference moderator and 6 participants).	Multipoint conferences are unsupported.
VC500		
VC800 with a trial multipoint license	24 ways video call with a presentation (a conference moderator and 24 participants)	**Period of validity**: 15-day free trial VC800 models can use this trial multipoint license. You can download it from Yealink website.
VC800 with an 8 ways multipoint license	8 ways video call with a presentation and 5 voice calls (a conference moderator and 13 participants).	**Period of validity**: Eternal You need to contact Yealink resellers to purchase it, please provide the MAC address of your VC800 when purchasing.
VC800 with a 16 ways multipoint license	16 ways video call with a presentation and 5 voice calls (a conference moderator and 21 participants).	
VC800 with a 24 ways multipoint license	24 ways video call with a presentation (a conference moderator and 24 participants)	

The multipoint license parameters on the system are described below.

Parameter	Description	Configuration Method
Load License File	Import a multipoint license.	Web User Interface
Multipoint Status	Indicates whether a multipoint license has been imported to the VC800 system or not. • Active • Inactive (without a multipoint license or the imported multipoint license has expired)	Web User Interface
Multipoint Ways	Indicates the multipoint license imported to the VC800 system. • Unsupported • 8 Ways • 16 Ways • 24 Ways	Web User Interface
Period of validity	Indicates the validity period of the imported multipoint license. • Unsupported • X~Y Available • Eternal	Web User Interface

To import the multipoint license via web user interface:

1. Click on **Security**->**License**.
2. Click **Browse** to locate the multipoint license (the file format must be *.dat) from your local system.



3. Click **Upload** to complete importing the multipoint license.

To view multipoint license status via web user interface:

1. Click **Status**.

To view multipoint license status via the remote control:

1. Select **More**->**Status**->**License**.

To view multipoint license status via the CP960 conference phone:

1. Tap  ->**License**.

Note

Upgrading the system or performing a factory reset will not affect the imported multipoint license.

If the system has been imported a trial multipoint license and the license has not expired, and you import a permanent multipoint license to the system, the permanent multipoint license will overwrite the trial multipoint license.

If the system has been imported a permanent multipoint license, and you import a trial multipoint license to the system, the permanent multipoint license will not be overwritten.

If you import a new permanent multipoint license to the system, the previous permanent multipoint license will be overwritten.

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

User Mode

Two roles are supported for accessing the system, an admin role and a user role. Admins can perform administrator activities such as changing configuration. Users can perform only user-type activities. You need to configure a password for the user when the user mode is enabled.

After the user mode is enabled, the user can log into the web user interface of the system with user credentials. The default user name is "user".

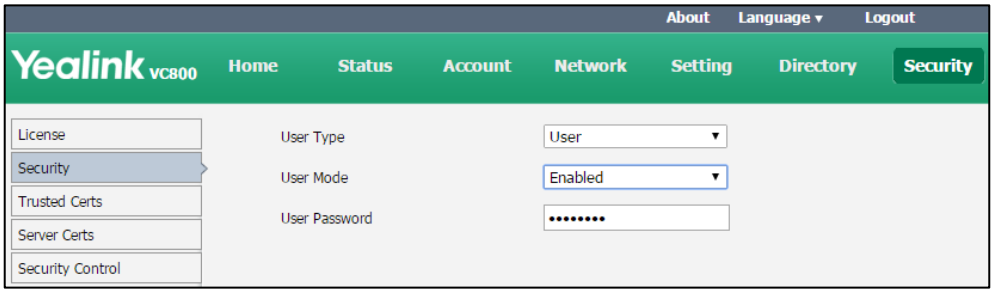
User mode parameters on the system are described below:

Parameter	Description	Configuration Method
User Type	Specifies the user type. **Default:** Administrator **Note:** To enable the user type, you need to select User for this parameter.	Web User Interface
User Mode	Enables or disables the user mode. **Default:** Disabled **Note:** It is only applicable to the user. The administrator mode is enabled by default.	Web User Interface
User Password	Configures a password for the user to access the menus or log into the	Web User Interface

Parameter	Description	Configuration Method
	web user interface. **Note:** It can only be configured when the user mode is enabled. The system supports ASCII characters 32-126(0x20-0x7E) in passwords. You can leave the password blank.	

To configure user mode via web user interface:

1. Click on **Security**->**Security**.
2. Select **User** from the pull-down list of **User Type**.
3. Select **Enabled** from the pull-down list of **User Mode**.
4. Configure a password or leave it blank in the **User Password** field.



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

Administrator Password

The default enabled user type is administrator. Users can log into the web user interface and access the "Advanced" menu with administrator privilege by default. The default administrator password is "0000" and can be only changed by an administrator. For security reasons, the administrator should change the default administrator password as soon as possible. The system supports ASCII characters 32-126(0x20-0x7E) in passwords.

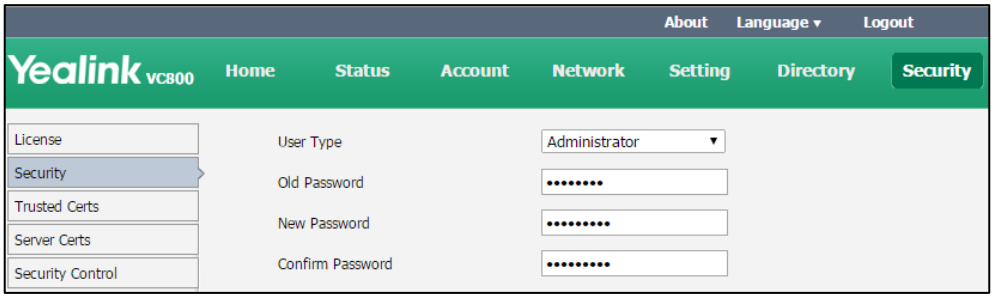
Administrator password parameters on the system are described below:

Parameter	Description	Configuration Method
User Type	Specifies the user type. **Default:** Administrator **Note:** To configure a new administrator password, you need to select Administrator for this parameter.	Web User Interface
Old Password	Enters the old administrator password.	Remote Control Web User Interface

Parameter	Description	Configuration Method
	Note: The default administrator password is "0000".	
New Password	Configures a new administrator password. **Note:** You can leave the password blank.	Remote Control Web User Interface
Confirm Password	Enters the new configured administrator password. **Note:** The entered password must be the same as the one configured by the parameter "New Password".	Remote Control Web User Interface

To configure administrator password via web user interface:

1. Click on **Security**->**Security**.
2. Select **Administrator** from the pull-down list of **User Type**.
3. Enter the old administrator password in the **Old Password** field.
4. Enter a new password in the **New Password** field.
5. Enter the new password or leave it blank in the **User Password** field.



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

To configure administrator password via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000)->**Password Reset**.
2. Enter the old password in the **Current Password** field.
3. Configure a new password in the **New Password** and **Confirm Password** fields.
4. Select **Save**, and then press OK to accept the change.

Web Server Type

Web server type determines the access protocol of the system's web user interface. The system supports both HTTP and HTTPS protocols for accessing the web user interface. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols. HTTPS is a web protocol

that encrypts and decrypts user page requests as well as the pages returned by the web server. Both the HTTP and HTTPS port numbers are configurable.

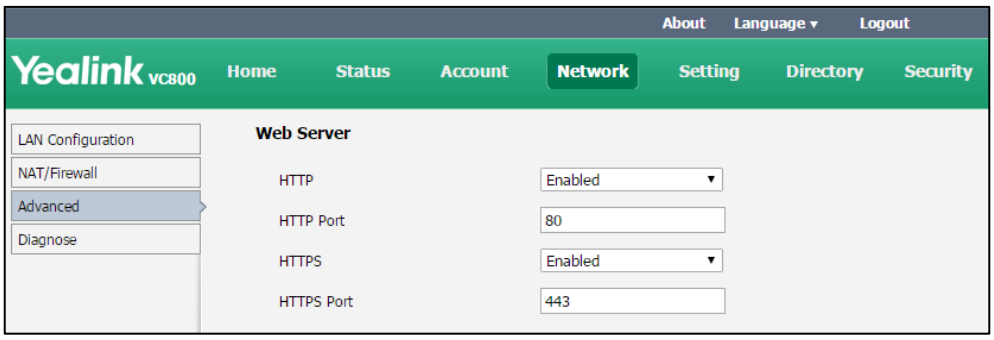
Web server type parameters on the system are described below:

Parameter	Description	Configuration Method
HTTP	Enables or disables the user to access the web user interface of the system using the HTTP protocol. **Default:** Enabled	Remote Control Web User Interface
HTTP Port	Specifies the HTTP port for the user to access the web user interface of the system. **Valid Values:** 1-65535 **Default:** 80 **Note:** Ensure that the configured port is not used.	Web User Interface
HTTPS	Enables or disables the user to access the web user interface of the system using the HTTPS protocol. **Default:** Enabled	Remote Control Web User Interface
HTTPS Port	Specifies the HTTPS port for the user to access the web user interface of the system. **Valid Values:** 1-65535 **Default:** 443 **Note:** Ensure that the configured port is not used.	Web User Interface

To configure web server type via web user interface:

1. Click on **Network**->**Advanced**.
2. Select the desired value from the pull-down list of **HTTP**.
3. Enter the desired HTTP port in the **HTTP Port** field.
4. Select the desired value from the pull-down list of **HTTPS**.

5. Enter the desired HTTPS port in the **HTTPS Port** field.



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

To configure web server type via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000) ->**Advanced Network**.
2. Select the desired value from the pull-down list of **Web Server Type**.
3. Select **Save**, and then press OK to accept the change.

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

Transport Layer Security

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing the system to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

TLS protocol is composed of two layers: TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

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 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

You can provide secure communication for SIP signaling using TLS transport protocol.

TLS parameter on the system is described below:

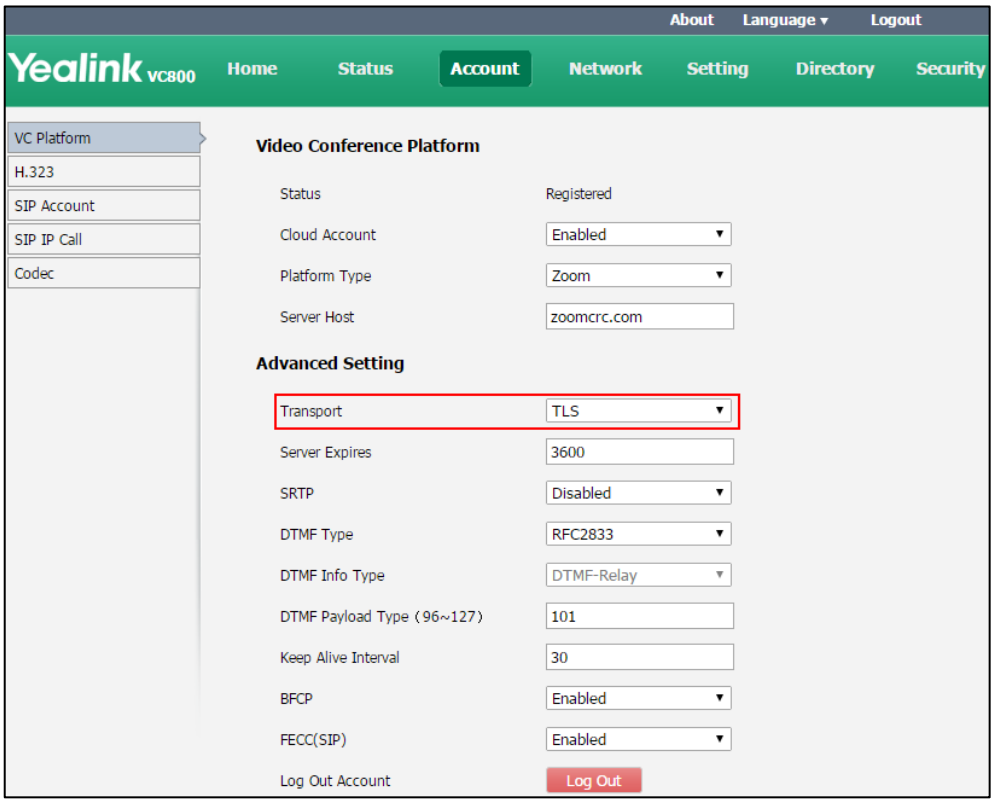
Parameter	Description	Configuration Method
Transport	Configures the transport protocol for SIP signaling. You can configure it for the Zoom/Pexip/BlueJeans/Mind/Custom	Remote Control Web User Interface

Parameter	Description	Configuration Method
	platform, or SIP account separately. ● **UDP**–provides best-effort transport via UDP for the SIP signaling. ● **TCP**–provides reliable transport via TCP for SIP signaling. ● **TLS**–provides secure communication for SIP signaling. ● **DNS-NAPTR**–performs the DNS NAPTR and SRV queries for the service type and port if no server port is given. **Default:** For Zoom/Pexip/BlueJeans/Mind/Custom platform, the default value is TCP. For SIP account, the default value is UDP. **Note:** You cannot configure it for the Yealink/StarLeaf Cloud platform.	

To configure TLS for the Zoom/Pexip/BlueJeans/Mind/Custom platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Zoom/Pexip/BlueJeans/Mind/Custom** from the pull-down list of **Platform Type**.

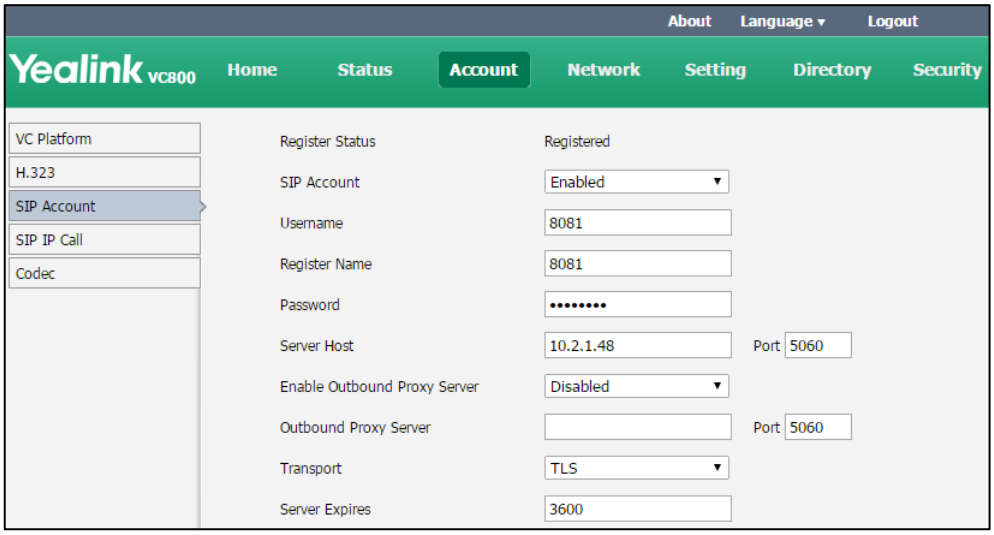
3. Select **TLS** from the pull-down list of the **Transport**.



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

To configure TLS for the SIP account via web user interface:

1. Click on **Account->SIP Account**.
2. Select **TLS** from the pull-down list of the **Transport**.



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

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.

The trusted certificates list contains the default and custom certificates.

- **Default Certificates**: The system has 36 built-in trusted certificates. For more information refer to Appendix B: Trusted Certificates on page 264.
- **Custom Certificates**: You can upload up to 10 trusted certificates to the system. The format of the certificates must be *.pem, *.cer, *.crt and *.der.

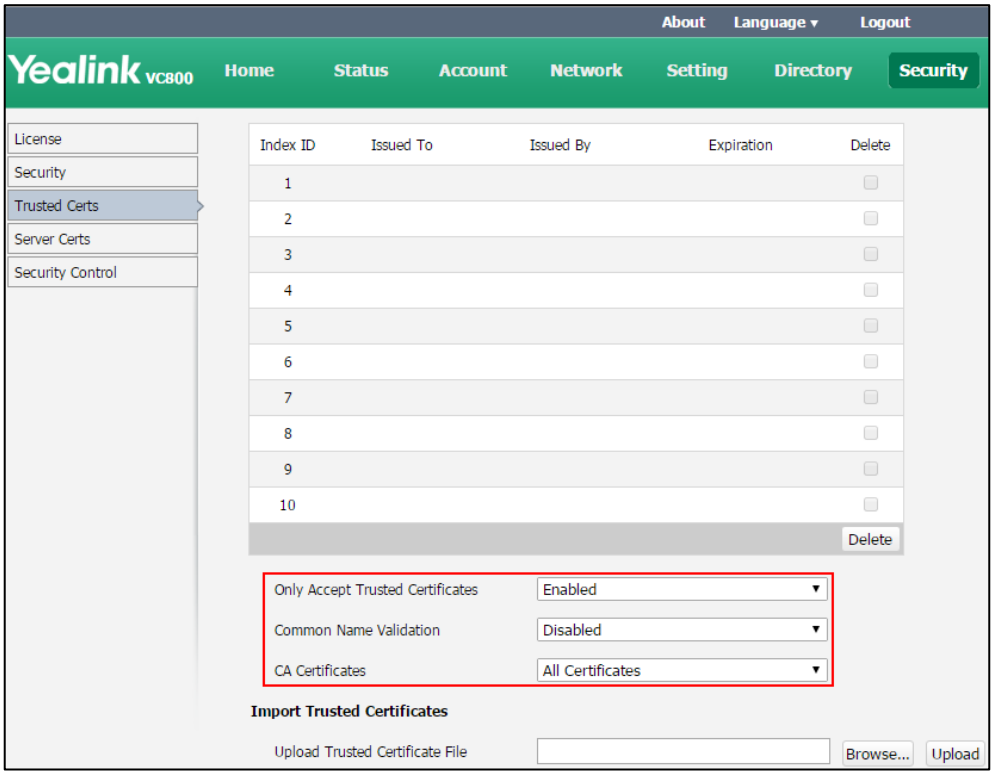
Trusted certificates parameters on the system are described below:

Parameter	Description	Configuration Method
Only Accept Trusted Certificates	Enables or disables the system to only trust the server certificates in the trusted certificates list. **Default:** Enabled **Note:** If it is enabled, the system will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, will the system trust the server. If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Common Name Validation	Enables or disables 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. **Default:** Disabled **Note:** If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
CA Certificates	Configures the type of certificates in the Trusted Certificates list for the system to authenticate for the TLS connection. • **Default Certificates** • **Custom Certificates** • **All Certificates**	Web User Interface

Parameter	Description	Configuration Method
	Default: Default Certificates **Note:** If you change this parameter, the system will reboot to make the change take effect.	
Upload Trusted Certificate File	Configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Note:** A maximum of 10 CA certificates can be uploaded to the system. The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.	Web User Interface

To configure the trusted certificate feature via web user interface:

1. Click on **Security**->**Trusted Certs**.
2. Select the desired value from the pull-down list of **Only Accept Trusted Certificates**.
3. Select the desired value from the pull-down list of **Common Name Validation**.
4. Select the desired value from the pull-down list of **CA Certificates**.

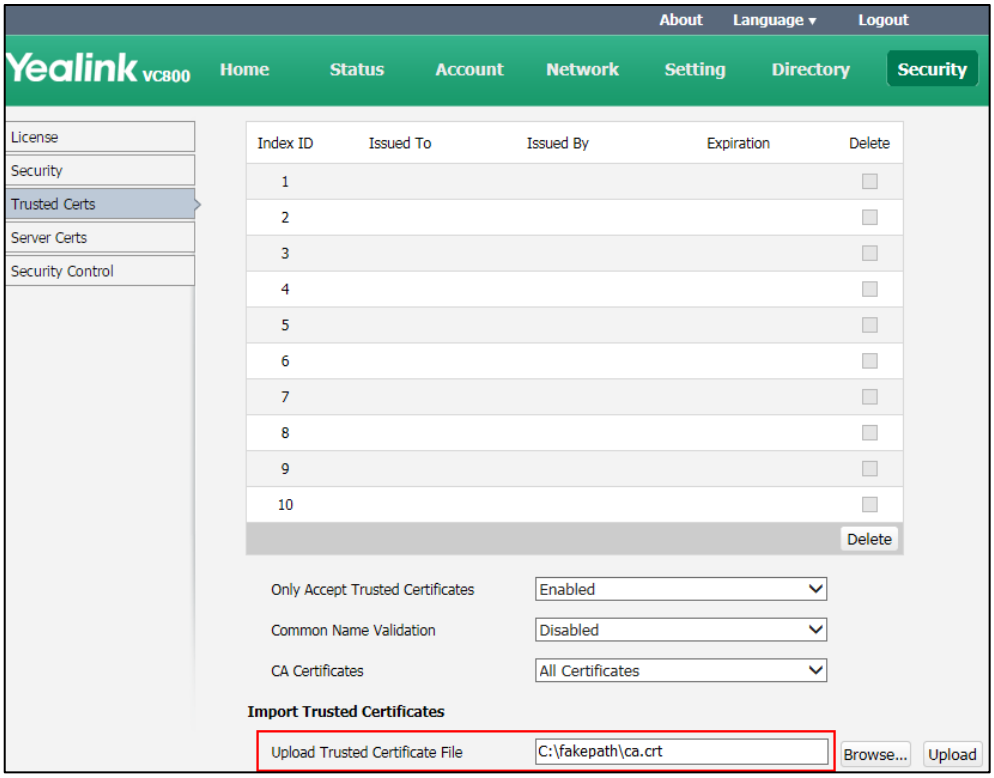


5. Click **Confirm** to accept the change.

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

To upload a CA certificate via web user interface:

1. Click on **Security**->**Trusted Certs**.
2. Click **Browse** to locate the certificate (*.pem,*.crt, *.cer or *.der) from your local system.



3. Click **Upload** to upload the certificate.

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 certificate (device certificate) to the clients for authentication.

The server certificate contains the default and custom certificates.

- **Default Certificates**: a unique server certificate and a generic server certificate.

  A unique server certificate: It is installed by default and is unique to a system (based on the MAC address) and issued by the Yealink Certificate Authority (CA).

  A generic server certificate: It is installed by default and is issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the system may send a generic certificate for authentication.

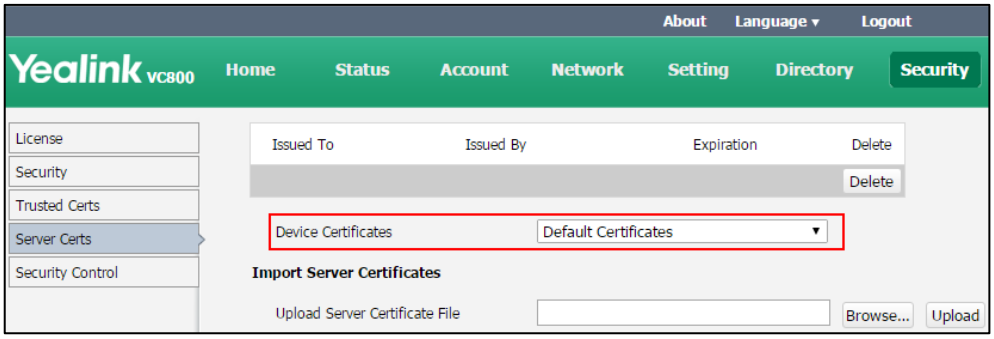
- **Custom Certificates**: You can only upload one server certificate to the system. The old server certificate will be overridden by the new one. The format of the server certificate files must be *.pem and *.cer.

Server certificates parameters on the system are described below:

Parameter	Description	Configuration Method
Device Certificates	Configures the type of the server certificates for the system to send for TLS authentication. • **Default Certificates** • **Custom Certificates** **Default:** Default Certificates **Note:** If you change this parameter, the system will reboot to make the change take effect.	Web User Interface
Upload Server Certificate File	Configures the access URL of the server certificate the system sends for authentication. **Note:** Only one server certificate can be uploaded to the system. The server certificate you want to upload must be in *.pem or *.cer format.	Web User Interface

To configure the server certificate via web user interface:

1. Click on **Security**->**Server Certs**.
2. Select the desired value from the pull-down list of **Device Certificates**.



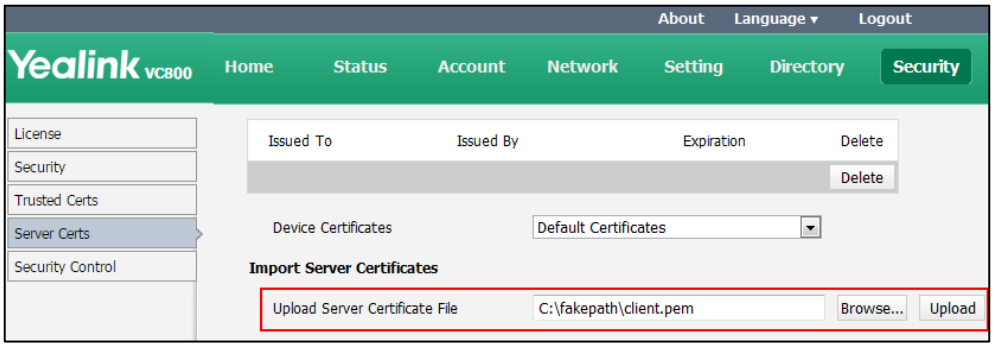
3. Click **Confirm** to accept the change.

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

To upload a server certificate via web user interface:

1. Click on **Security**->**Server Certs**.

2. Click **Browse** to locate the certificate (*.pem or *.cer) from your local system.



3. Click **Upload** to upload the certificate.

Secure Real-Time Transport Protocol

During a confidential call, you can configure Secure Real-Time Transport Protocol (SRTP) to encrypt RTP streams to avoid interception and eavesdropping. Both RTP and RTCP signaling may be encrypted using an AES algorithm as described in RFC3711. Encryption modifies the data in the RTP streams so that, if the data is captured or intercepted, it cannot be understood—it sounds like noise. Only the receiver knows the key to restore the data. To use SRTP encryption for SIP calls, the participants in the call must enable SRTP simultaneously. When this feature is enabled on both systems, the encryption algorithm utilized for the session is negotiated between the systems. This negotiation process is compliant with RFC 4568.

When a site places a call on the SRTP enabled system, the system sends an INVITE message with the RTP encryption algorithm to the destination system.

The following is an example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NzFlNTUwZDk2OGVlOTc3YzNkYTkwZWVkMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
```

```
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm, and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.

The following is an example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

The SRTP parameter on the system is described below:

Parameter	Description	Configuration Method
SRTP	Specifies the SRTP type. You can configure it for the Zoom/Pexip/BlueJeans/Mind/Custom platform, SIP account or SIP IP call separately. ● **Disabled**−encrypted calls are not supported. ● **Optional**−both encrypted and unencrypted calls are supported. Secure calls are supported only if the far end supports encryption. ● **Compulsory**−unencrypted calls are not supported. **Default:** Disabled **Note:** You cannot configure it for the Yealink/StarLeaf Cloud platform.	Web User Interface

Rules of SRTP for media encryption in SIP calls:

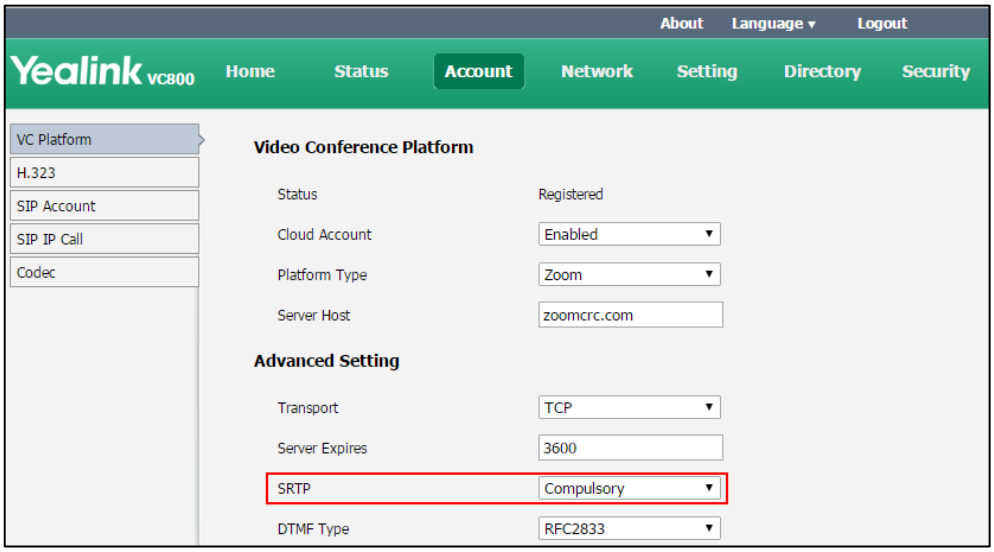
Far \ Near	Compulsory	Optional	Disabled
Compulsory	SRTP Call	SRTP Call	Fail to establish call
Optional	SRTP Call	SRTP Call	RTP Call
Disabled	Fail to establish call	RTP Call	RTP Call

When SRTP is enabled on both systems, RTP streams will be encrypted, and the lock icon appears on the display device of each system after successful negotiation.

Note If SRTP is enabled for the Cloud platform or SIP account, you should also configure the transport type to TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to Transport Layer Security on page 217.

To configure SRTP for Zoom/Pexip/BlueJeans/Mind/Custom platform via web user interface:

1. Click on **Account**->**VC Platform**.
2. Select **Zoom**/**Pexip**/**BlueJeans**/**Mind**/**Custom** from the pull-down list of **Platform Type**.
3. Select the desired value from the pull-down list of **SRTP**.

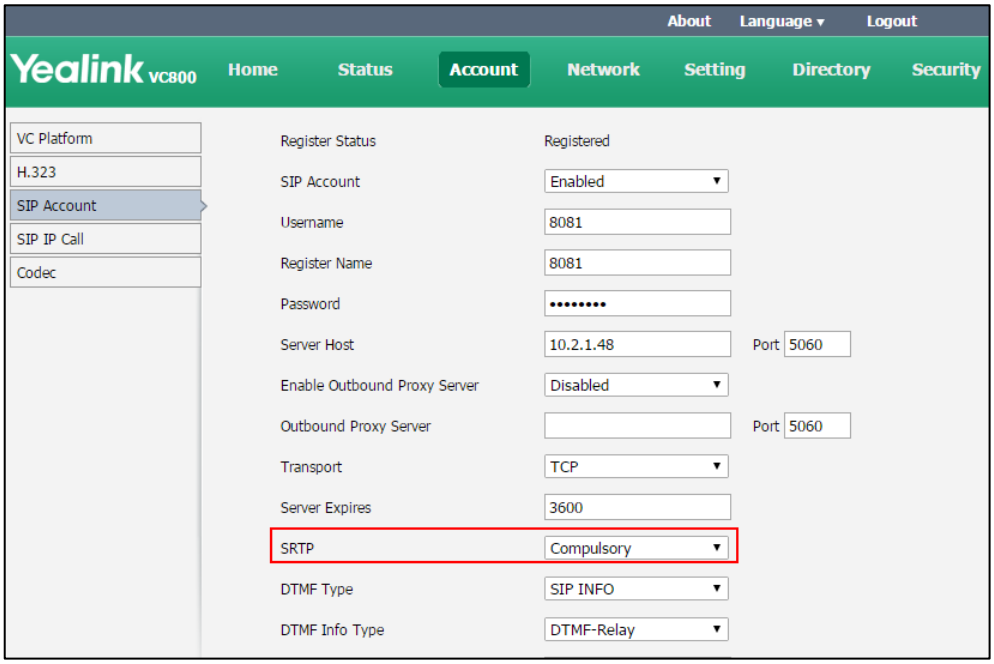


4. Click **Confirm** to accept the change.

To configure SRTP for SIP account via web user interface:

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

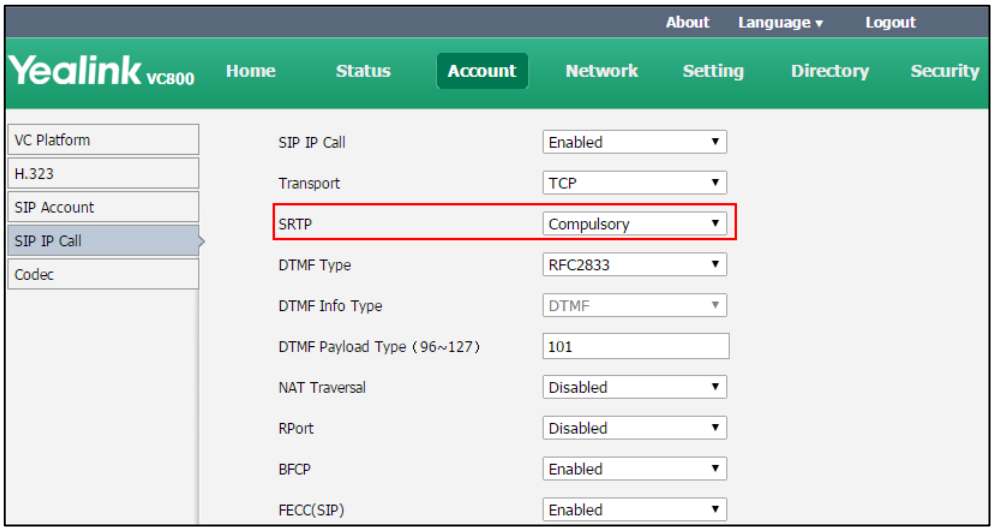
2. Select the desired value from the pull-down list of **SRTP**.



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

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

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



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

H.235

Yealink VC800/VC500 video conferencing systems support H.235 128-bit AES algorithm using the Diffie-Hellman key exchange protocol in H.323 calls. To use H.235 feature for H.323 calls, the participants in the call must enable the H.235 feature simultaneously. When a site places a call

on the H.235 feature enabled system, the system negotiates the encryption algorithm with the destination system.

The H.235 parameter on the system is described below:

Parameter	Description	Configuration Method
H.235	Specifies the H.235 type. You can configure it for the StarLeaf Cloud platform or H.323 call separately. • **Disabled**–encrypted calls are not supported. • **Optional**–both encrypted and unencrypted calls are supported. Secure calls are supported only if the far end supports encryption. • **Compulsory**–unencrypted calls are not supported. **Default:** Disabled	Web User Interface

Rules of H.235 security in H.323 calls:

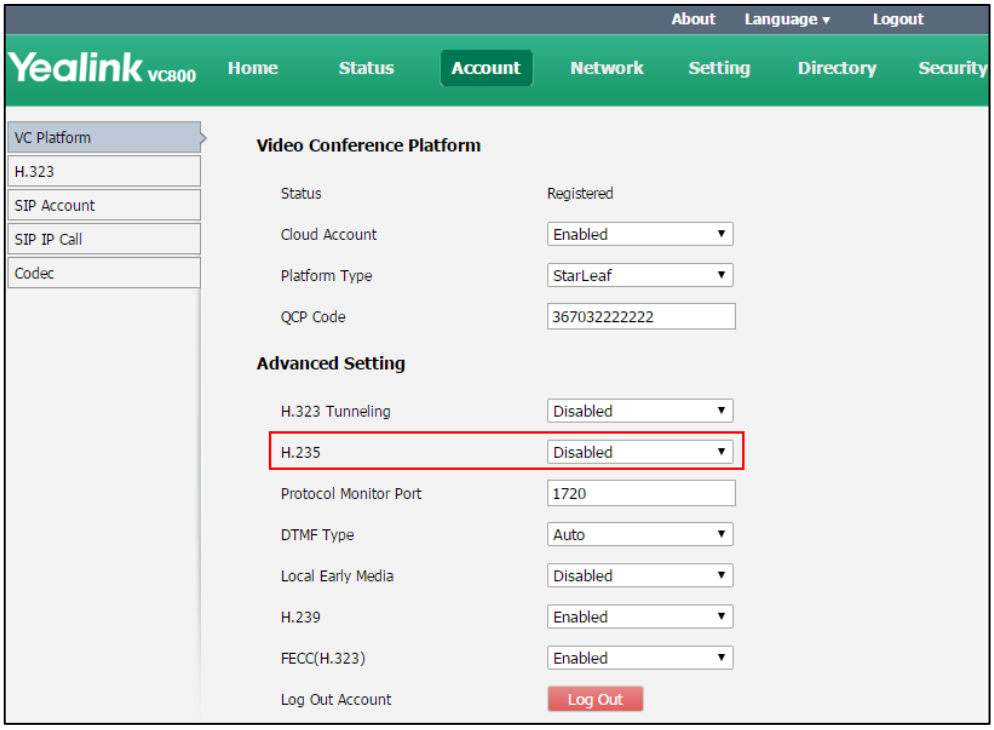
Far \ Near	Compulsory	Optional	Disabled
Compulsory	H.235 Call	H.235 Call	Fail to establish call
Optional	H.235 Call	H.235 Call	RTP Call
Disabled	Fail to establish a call	RTP Call	RTP Call

When H.235 is enabled on both systems, calls will be encrypted, and the lock icon  appears on the display device of each system during a call.

To configure H.235 for StarLeaf Cloud platform via web user interface:

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

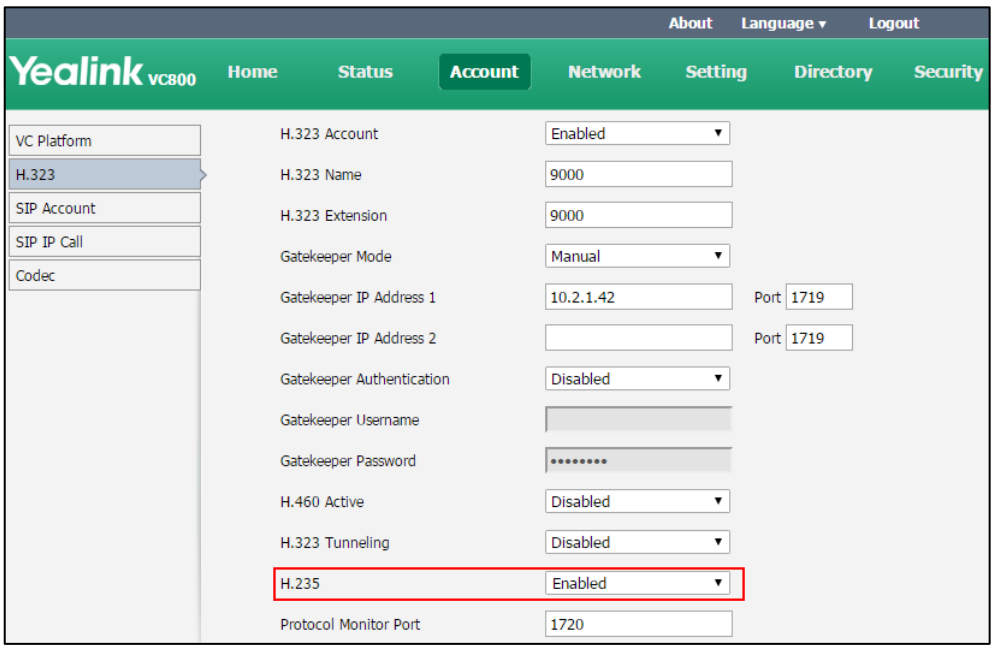
3. Select the desired value from the pull-down list of **H.235**.



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

To configure H.235 for H.323 calls via web user interface:

1. Click on **Account**->**H.323**
2. Select the desired value from the pull-down list of **H.235**.



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

Defending against Attacks

VCS sometimes receives calls from unknown caller, and the calls may be unable to answer. To ensure the communications security of the VCS, you can configure abnormal call answering feature for handling abnormal SIP incoming calls. For incoming H.323 calls, you can configure Safe Mode Call feature.

Abnormal Call Answering

When destination address of the incoming SIP call does not match local address, the call is considered to be an abnormal call. You can reject the abnormal SIP incoming call, or answer it using IP address or SIP account randomly.

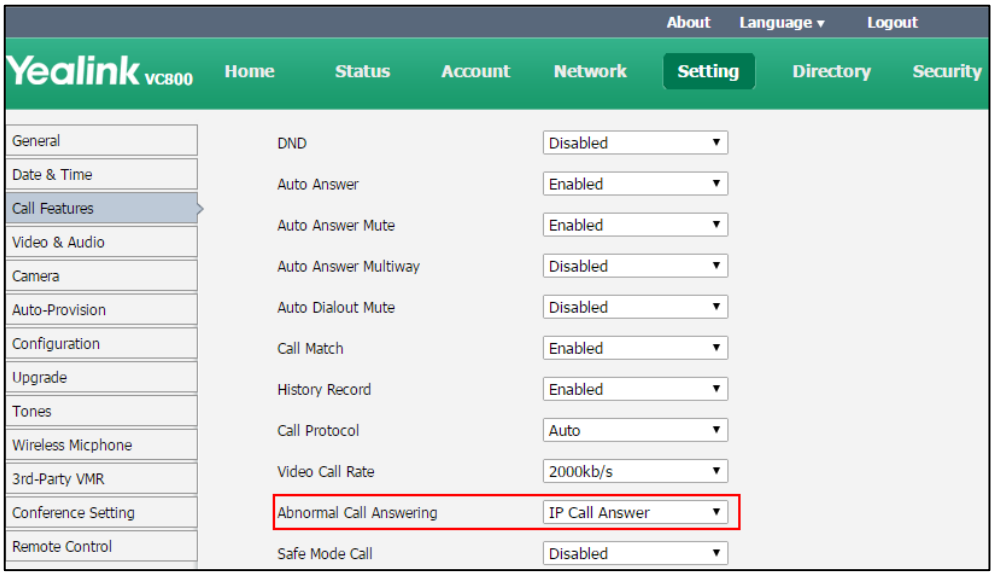
The abnormal call answering parameter on the system is described below:

Parameter	Description	Configuration Method
Abnormal Call Answering	Specifies the account type for answering abnormal SIP incoming calls. • **Disabled**–reject the abnormal SIP incoming calls. • **Account Answer**–use the SIP account to answer the abnormal SIP incoming calls. • **IP Call Answer—**use IP address to answer the abnormal SIP incoming calls. **Default:** IP Call Answer	Web User Interface

To configure abnormal call answering via web user interface:

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

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



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

Configuring Safe Mode Call

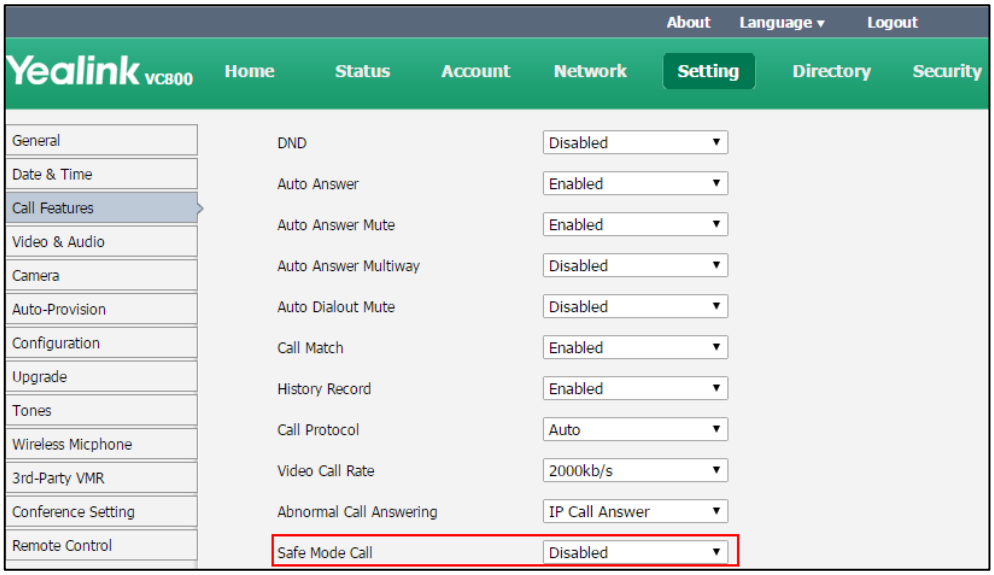
Safe Mode Call feature is used to verify whether the incoming H.323 call is coming from a H.323 endpoint.

The Safe Mode Call parameter on the system is described below:

Parameter	Description	Configuration Method
Safe Mode Call	Enables or disables the Safe Mode Call feature • **Disabled**–Answer incoming H.323 calls directly without validation. • **Enabled—**Verify whether the incoming H.323 call is coming from a H.323 endpoint. If it is, the VC800&VC500 video conferencing system will answer it. If not, the incoming call will be rejected. **Default:** Enabled	Web User Interface

To configure Safe Mode Call via web user interface:

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



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

System Integrated with Control Systems

The Yealink video conferencing systems provide an API interface for the third-party control system. The API commands can be sent to Yealink video conferencing systems over LAN or serial port, to realize controlling the Yealink video conferencing systems.

LAN Connection: Make sure the Yealink video conferencing system and the control system should be in the same network segment. API commands can be sent to video conferencing system through TCP protocol. The control system needs to know the IP address and TCP port of the Yealink video conferencing system.

Serial Connection: You can use the API with a serial connection to control Yealink video conferencing system. The USB port on the Yealink video conferencing system can be connected to the serial port on the control system through a USB to RS-232 cable.

For more information, refer to *Yealink VC Deployment and User Manual for Control Systems* and *API Commands Introduction for Yealink Video Conferencing System*.

Control system parameters are described below.

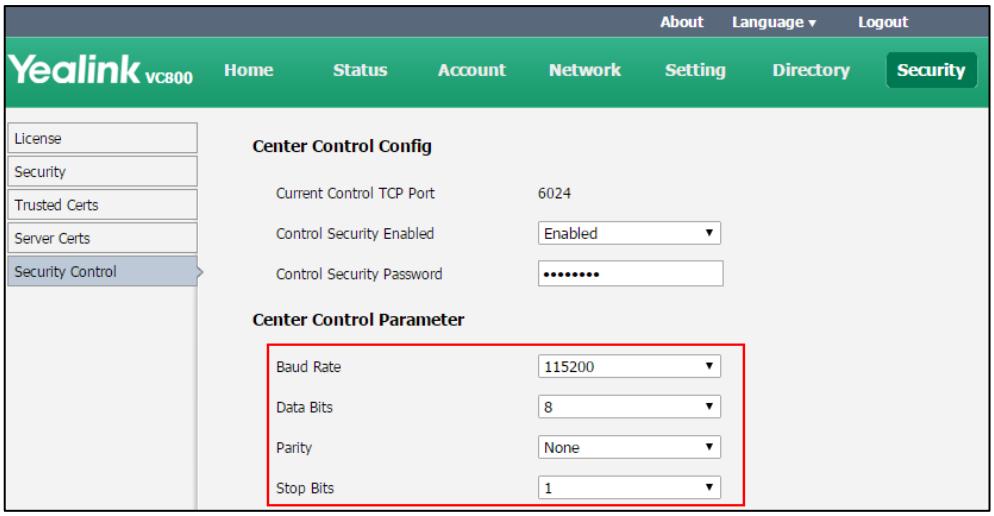
Parameter	Description	Configuration Method
Current Control TCP Port	Control TCP port (read-only). **Default:** 6024	Web User Interface
Control Security Enabled	Enables or disables an authentication password when the control system tries to connect to the video conferencing system. **Default:** Enabled	Web User Interface
Control Security	Configures the authentication	Web User Interface

Parameter	Description	Configuration Method
Password	password when the control system tries to connect to the video conferencing system.	
Baud Rate	Configures the baud rate. Available baud rates are: • **2400** • **4800** • **9600** • **19200** • **38400** • **115200** **Default:** 115200 **Note**: It must be the same rate for control system and Yealink video conferencing system.	Web User Interface
Data Bits	Configures the data bits. Available data bits are: • **7** • **8** **Default:** 8 **Note**: It must be the same data bits for control system and Yealink video conferencing system.	Web User Interface
Parity	Configures the parity. Available parity are: • **None** • **Odd** • **Even** • **Space** **Default:** None **Note**: It must be the same parity for control system and Yealink video conferencing system.	Web User Interface
Stop Bits	Configures the stop bits.	Web User Interface

Parameter	Description	Configuration Method
	Available stop bits are: • **1** • **2** **Default:** 1 **Note**: It must be the same stop bits for control system and Yealink video conferencing system.	

To configure control system via web user interface:

1. Click on **Security**->**Security Control**.
2. Select the desired value from the pull-down lists of **Control Security Enabled**.
3. Enter the desired password in the **Control Security Password** field.
4. Select the desired value from the pull-down lists of **Baud Rate**.
5. Select the desired value from the pull-down lists of **Data Bits**.
6. Select the desired value from the pull-down lists of **Parity**.
7. Select the desired value from the pull-down lists of **Stop Bits**.



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

System Maintenance

This chapter provides basic system maintenance, including upgrading firmware, managing configurations, resetting systems and how to monitor network via SNMP. Topics include:

Upgrading Firmware

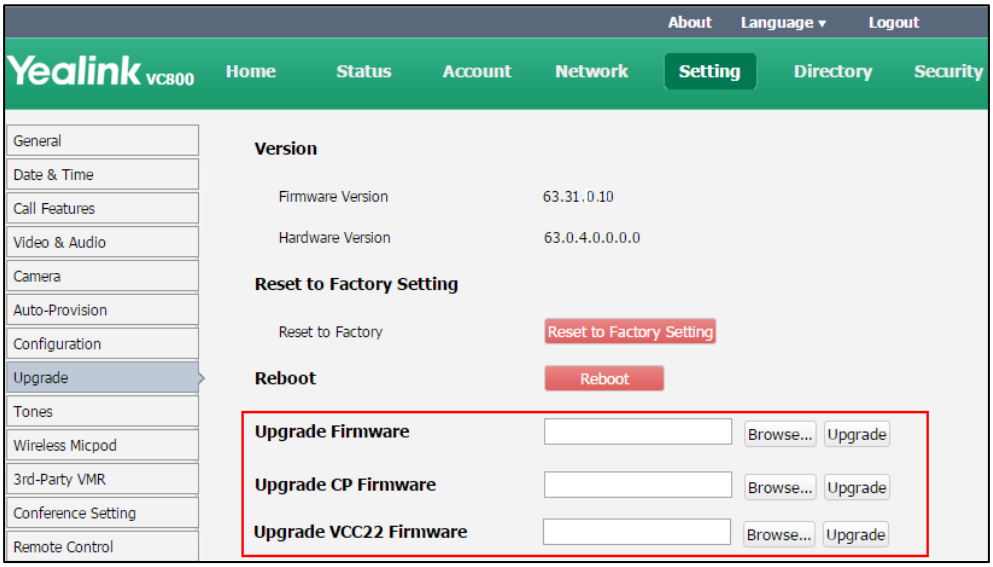
The newly released firmware version may add new features. Because of this, Yealink recommends you to update the latest firmware. You can upgrade the firmware via web user interface.

The firmware name of the VC800/VC500 video conferencing system and VCC22 camera is 63.x.x.x.rom and the firmware name of the CP960 conference phone is: 73.x.x.x.rom (x is the actual firmware version). You can download the latest firmware version from the Yealink website.

To upgrade firmware via web user interface:

1. Click on **Setting**->**Upgrade.**
2. Do one of the following:
   - In the **Upgrade Firmware** field, click **Browse** to locate the VC800/VC500 firmware from your local system.
   - In the **Upgrade CP Firmware** field, click **Browse** to locate the CP960 firmware from your local system.

- In the **Upgrade VCC22 Firmware** field, click **Browse** to locate the VCC22 firmware from your local system.



3. Click **Upgrade** to upgrade the firmware.

   The browser pops up the dialog box "Firmware will be updated. It will take 5 minutes to complete. Please don't power off!".

4. Click **Confirm** to confirm upgrading.

Note **Caution!** Don't remove the Ethernet cable and power cord during the upgrade process. Don't close or refresh the web page when upgrading the firmware via web user interface.

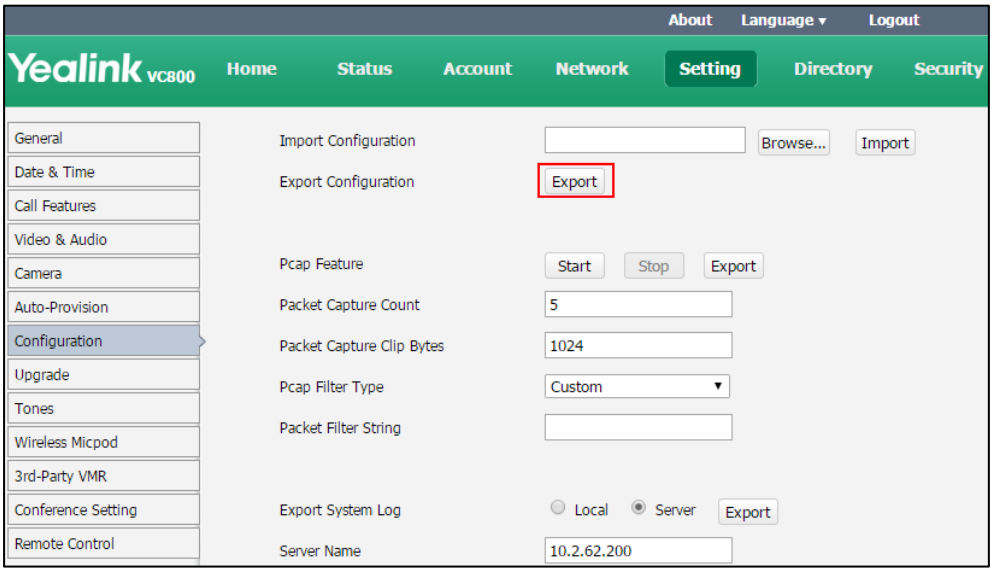
Importing/Exporting Configuration

We may need you to provide the system configurations for the Yealink field application engineers to help analyze problems. You can import configurations to your system to configure your system quickly. The file format of configuration file must be *.bin.

To export the system configurations via web user interface:

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

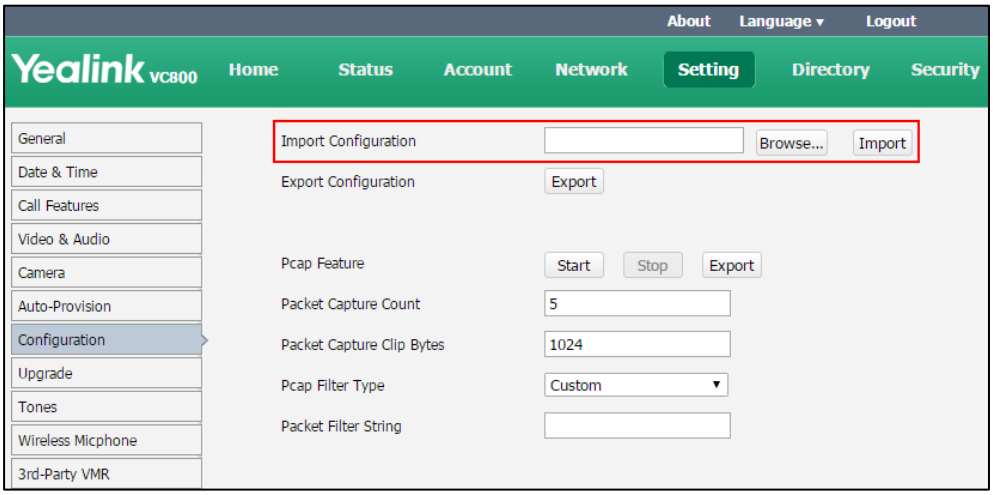
2. Click **Export**.



3. Click **Confirm** to export the configurations.

To import the system configurations via web user interface:

1. Click on **Setting**->**Configuration**.
2. Click **Browse** to locate a configuration file from your local system.



3. Click **Import** to import the configuration file.

Resetting to Factory

Reset the system to factory configurations after you have tried all appropriate troubleshooting suggestions but still have not solved your problems.

When factory resetting the video system, the following happens:

- The call logs will be deleted.
- Passwords will be reset to default.

- All system parameters will be reset to default values.
- All custom files will be deleted. Such as, certificates, local contacts and registered accounts.

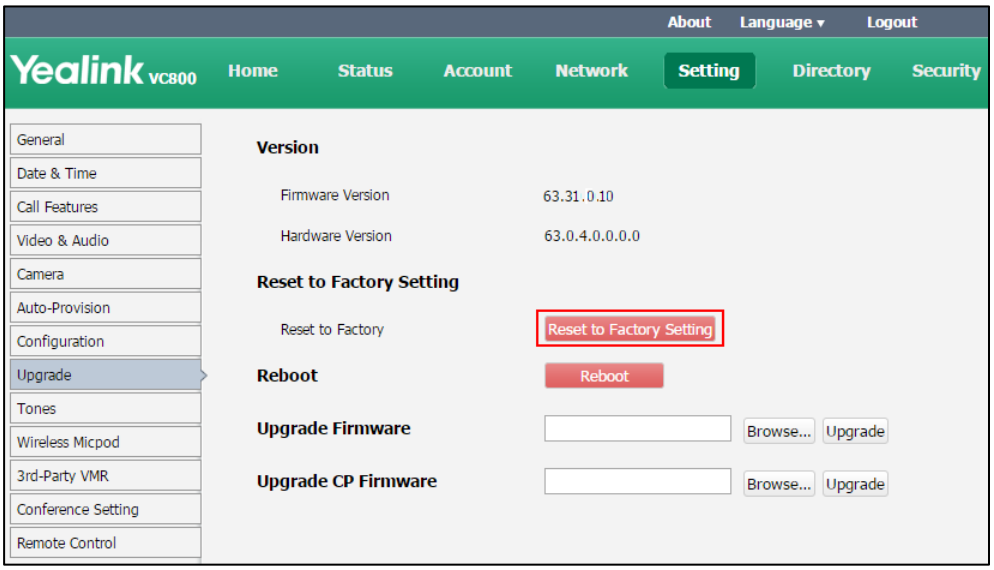
It is not possible to undo a factory reset. But you can export the configuration first, and then you can re-import the configuration to recovery the system after the reset.

You can reset the system via the web user interface, remote control or reset key.

Note Reset of the system may take a few minutes. Do not power off until the phone starts up successfully.

To reset the system via web user interface:

1. Click on **Setting**->**Upgrade**.
2. Click **Reset to Factory Setting**.



The web user interface prompts the message "Reset to factory?".

3. Click **Confirm** to confirm the resetting.

To reset the system via the remote control:

1. Select **More**->**Setting**->**Advanced** (default password: 0000)->**Reboot & Reset**.
2. Select **Reset**, and then press OK.

   The display device prompts" Reset to Factory? "
3. Select **OK**, and then press OK.

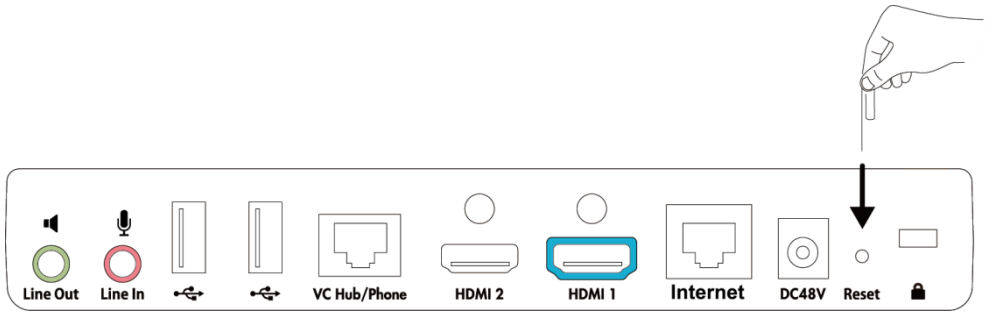
   The system reboots automatically. The system will reset to factory sucessfully after startup.

To reset the system via the rest key:

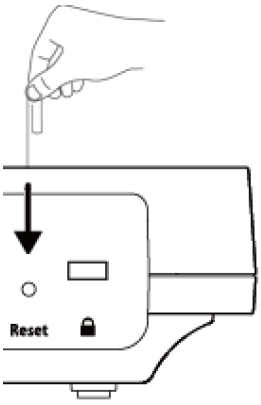
Using tiny objects (for example, the paper clip) to press and hold the reset button for 15 seconds until the screen turns black.

If VCC22 video conferencing cameras connect to the VC800 video conferencing system, you can press and hold the reset button on any VCC22 for 15 seconds to reset the VC800.

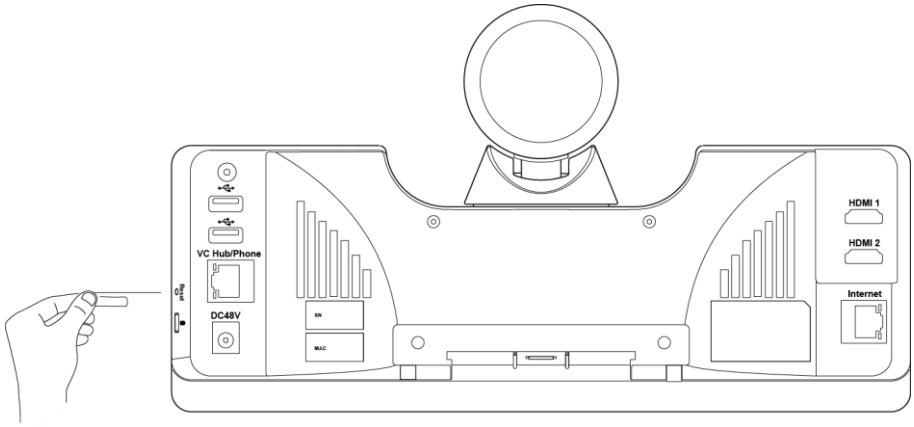
Do not power off the system during the factory restore process. The system reverts to the default factory settings and restarts automatically. This will take a few minutes.



VC800



VCC22



VC500

Note The connected CP960 conference phone will be reset to factory too.

Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using the VC800/VC500 video conferencing system.

Troubleshooting Methods

The system can provide feedback in a variety of forms, such as log files, packets, status indicators and so on, which can help an administrator to find the system problem more easily and resolve it.

The following sections will help you to better understand and resolve the working status of the system.

- Viewing Log Files
- Capturing Packets
- Getting Information from Status Indicators
- Analyzing Configuration Files
- Viewing Call Statistics
- Using Diagnostic Methods

Viewing Log Files

The log files are Yealink specific debug files which may be requested by the Yealink support organization if you need technical support. The current log files are time stamped event log files. You can export the log files to a syslog server or the local system. The administrator can specify the location where the log will be exported to and the severity level of the log.

System Log Level specifies the log level to be recorded. The default system log level is 6.

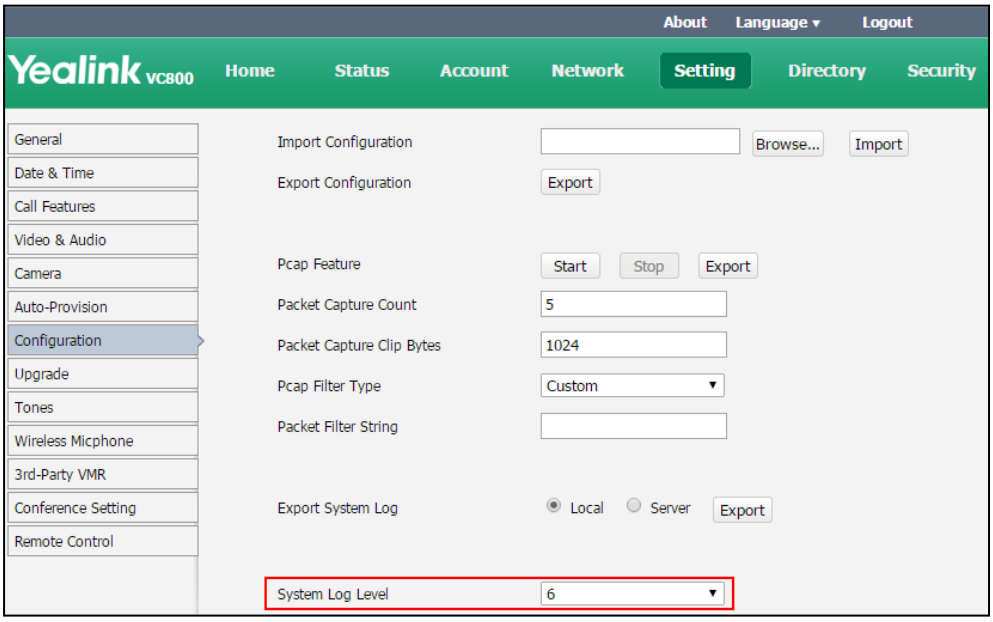
System log level parameters are described below:

Parameter	Description	Configuration Method
Export System Log	Specify where the system log will be exported. **Valid values:** • **Local**-export the system log to the local computer. • **Server**-export the system log to the specified server.	Web User Interface

Parameter	Description	Configuration Method
	Default: Local	
Server Name	Specify the server address where the log will be exported. **Note**: It only works if the parameter "Export System Log" is set to Server.	Web User Interface
System Log Level	Specify the system log level. **Note**: The supported level is 0-6. Higher value indicates more detailed content. **Default**: 6	Web User Interface

To configure the system log level via web user interface:

1. Click on **Setting**->**Configuration**.
2. Select the desired level from the pull-down list of **System Log Level**.

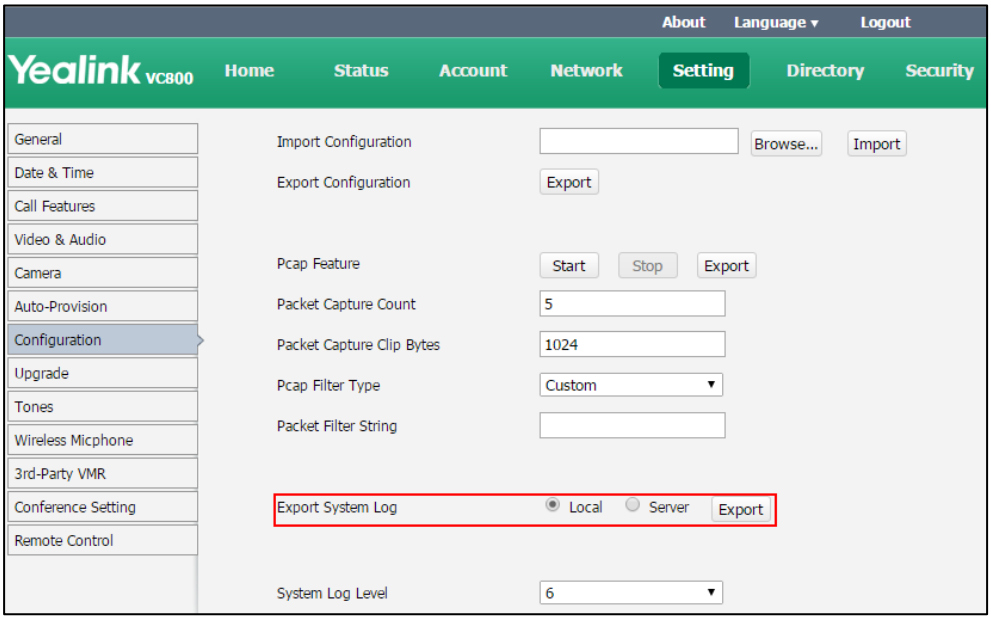


3. Click **Confirm** to accept the change.

To export a log file to the local system via web user interface:

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

2. Mark the **Local** radio box In the **Export System Log** field.



3. Click **Export** to open the file download window, and then save the file to your local system.

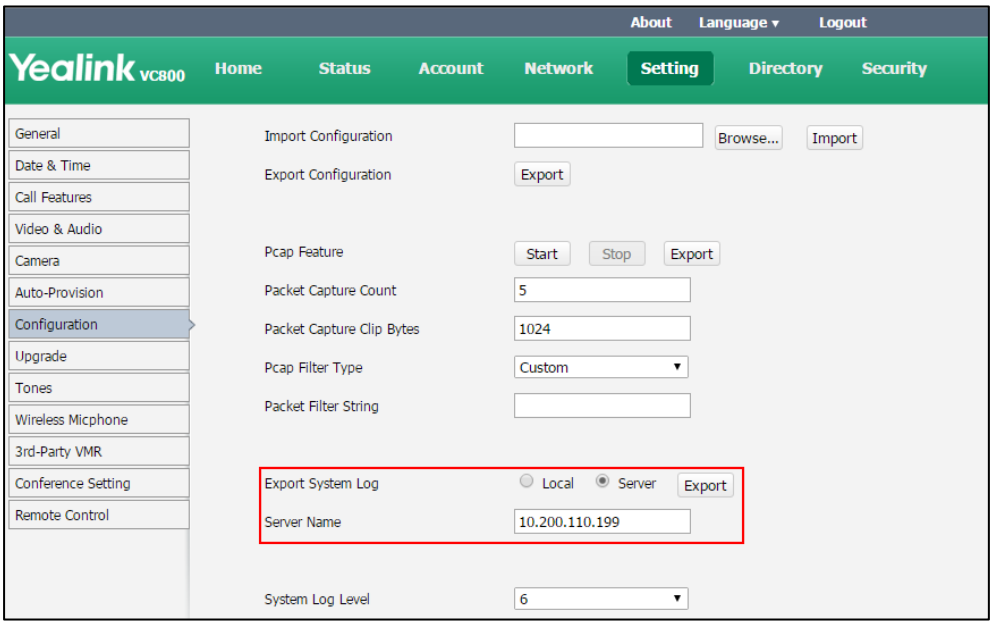
The following figure shows a portion of a log file:

```
  496 root       8876 SW  /yealink/bin/ggsvca_ipp
  497 root       8876 SW  /yealink/bin/ggsvca_ipp
  498 root       8876 SW  /yealink/bin/ggsvca_ipp
  499 root       8876 SW  /yealink/bin/ggsvca_ipp
  500 root       8876 SW  /yealink/bin/ggsvca_ipp
  501 root       8876 SW  /yealink/bin/ggsvca_ipp
  507 root      16424 SW  /yealink/bin/Screen.exe
  508 root      10344 SW  /yealink/bin/sipServer.exx
  509 root      10344 SW  /yealink/bin/sipServer.exx
  515 root      16424 SW  /yealink/bin/Screen.exe
  517 root      16424 SW  /yealink/bin/Screen.exe
  519 root      10344 SW  /yealink/bin/sipServer.exx
  521 root      16424 SW  /yealink/bin/Screen.exe
  522 root      16424 SW  /yealink/bin/Screen.exe
  523 root      16424 SW  /yealink/bin/Screen.exe
  524 root      10344 SW  /yealink/bin/sipServer.exx
  525 root            SW< [IRQ 45]
  526 root      10344 SW  /yealink/bin/sipServer.exx
  527 root      16424 SW  /yealink/bin/Screen.exe
  528 root      16424 SW  /yealink/bin/Screen.exe
  529 root      16424 SW  /yealink/bin/Screen.exe
 1147 root       1788 SWN sleep 1000
 1227 root      10120 SWN ConfigManApp.com
 1228 root       4624 SW  /yealink/bin/mini_httpd -p 80 -d /yealink/html -c cgi
 1229 root       2812 SWN sh -c cd /tmp;ifconfig >> Messages;ps >> Messages;tar
 1230 root       2812 RWN ps
Feb 29 06:01:09 mini_httpd[388]: mini_httpd.c(1510):child process 1227 exit!
Feb 29 06:01:12 mini_httpd[1232]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com,query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1232 exit!
Feb 29 06:01:12 mini_httpd[1233]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com,query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1233 exit!
Feb 29 06:01:12 mini_httpd[1234]: mini_httpd.c(1997):path:/cgi-bin/ConfigManApp.com,query:Id=27
Feb 29 06:01:12 mini_httpd[388]: mini_httpd.c(1510):child process 1234 exit!
```

To export a log file to a syslog server via web user interface:

1. Click on **Setting**->**Configuration**.
2. Mark the **Server** radio box in the **Export System Log** field.

3. Enter the IP address or domain name of the syslog server in the **Server Name** field.



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

Capturing Packets

The administrator can capture packets in three ways: capturing the packets via web user interface, remote control or using the Ethernet software. Engineers can analyze the packets to troubleshoot problems.

Packets parameters are described below:

Parameter	Description	Configuration Method
Pcap Feature	Start and stop capturing packets or export the captured packets.	Web User Interface
Packet Capture Count	Configures the count of the number of packets to capture. **Default:** 5	Web User Interface
Packet Capture Clip Bytes	Configures the number of bytes (in kb) of the packet to capture. **Default:** 1024	Web User Interface
Pcap Filter Type	Configures the filter type of the packet to capture. **Valid Values:** • **Custom**–Customize the packet filter string. • **SIP or H245 or H225**–Capture	Web User Interface

Parameter	Description	Configuration Method
	SIP, H245 and H225 packets. • **RTP**−Capture RTP packets. **Default:** Custom	
Packet Filter String	Customizes the packet filter string. **Syntax:** Protocol+Direction+Host(s)+ Value +Logical Operations+Other Expression **Protocol**: Values: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp. Application-level protocol, such as http, dns and sip are not supported. If no protocol is specified, all the protocols are used. **Direction**: Values: src, dst, src and dst, src or dst If no source or destination is specified, the "src or dst" keywords are applied. For example: "host 10.2.2.2" is equivalent to "src or dst host 10.2.2.2". **Host(s)**: Values: net, port, host, portrange. If no host(s) is specified, the "host" keyword is used. For example: "src 10.1.1.1" is equivalent to "src host 10.1.1.1". **Logical Operations**: Values: not, and, or. Negation ("not") has highest precedence. Alternation ("or") and concatenation ("and") have equal precedence and associate left to right. For example: "not tcp port 3128 and tcp port 23" is 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	Web User Interface

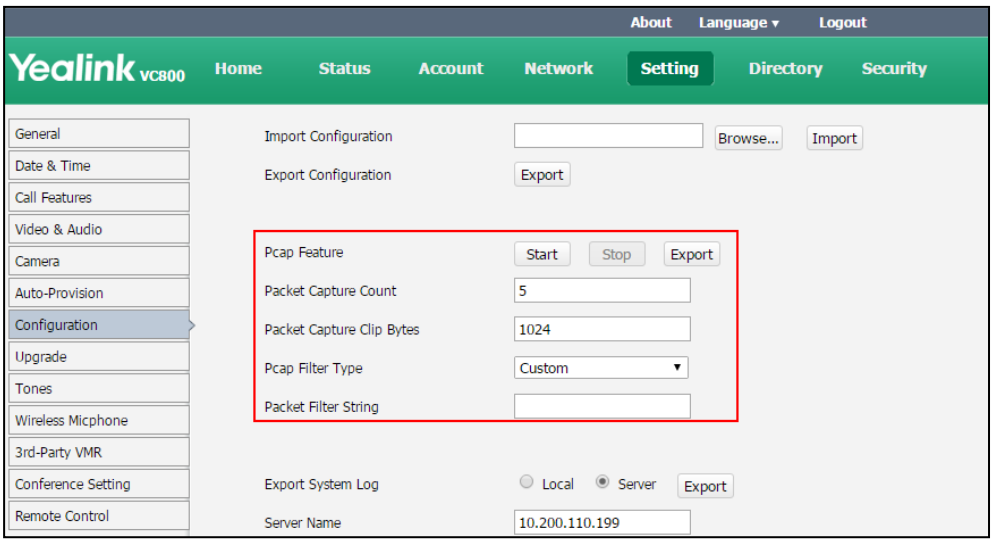
Parameter	Description	Configuration Method
	and tcp port 23)". **Example**: (src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst port range 200-10000 and dst net 10.0.0.0/8 Displays packets with source IP address 10.4.1.12 or source network 10.6.0.0/16, the result is then concatenated with packets having destination TCP port range from 200 to 10000 and destination IP network 10.0.0.0/8. **Default**: Blank **Note**: It only works if the parameter "Pcap Filter Type" is set to Custom.	

To capture packets via web user interface:

1. Click on **Setting**->**Configuration**.
2. Enter the desired value in the **Packet Capture Count** field.
3. Enter the desired value in the **Packet Capture Clip Bytes** field.
4. Select the desired value from the pull-down list of **Pcap Filter Type**.

   If **Custom** is selected, enter the desired packet filter string in the **Packet Filter String** field.
5. Click **Start** to start capturing signal traffic.
6. Reproduce the issue to get stack traces.
7. Click **Stop** to stop capturing.

8. Click **Export** to open the file download window, and then save the file to your local system.



To export a PCAP trace via remote control:

Before capturing packets, make sure a USB flash driver is connected to VC800/VC500 codec, VCH50 video conferencing hub or CP960 conference phone and the USB feature is enabled.

1. Long press ⌫ when the system is idle or during a call.

   The display device prompts "Onekey-capture has been turned on, press the Backspace key for 2s to turn off it".

2. Long press ⌫ for 2 seconds to stop capturing packets.

   The packets are saved in the yealink.debug folder on your USB flash driver.

To capture packets using the Ethernet software:

Connect the Internet ports of the system and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic. You can also set mirror port on a switch to monitor the port connected to the system.

Getting Information from Status Indicators

In some instances, status indicators are helpful for finding system troubles. Status indicators may consist of the power LED, icons on the status bar of the display device or prompt messages.

The following shows two examples of obtaining the system information from status indicators:

- If a LINK failure of the system is detected, the status bar of the display device prompts "Network disconnected".
- If the power LED does not light, it indicates the system is not powered on.

Analyzing Configuration Files

Wrong configurations may have an impact on your system use. You can export configuration file

to check the current configuration of the system and troubleshoot if necessary. For more information on how to export system configuration, refer to Importing/Exporting Configuration on page 238.

Viewing Call Statistics

You can enter the view call statistics screen during an active call. Information includes:

- **Total Bandwidth:** Uplink Bandwidth and Downlink Bandwidth.
- **Video**: Resolution, Codec, Bandwidth, Frame Rate, Jitter, Total Packet Lost, Packet Lost(%).
- Protocol used during a call.
- Device information of the far site.
- **Audio:** Codec, Bandwidth, Sample Rate, Jitter, Total Packet Lost, Packet Lost(%)
- **Share:** Resolution, Codec, Bandwidth, Frame Rate.

To view call statistics during an all via web user interface:

1. Click **Home**.
2. Hover your cursor over the desired participant, and then click  to view call statistics.

To view call statistics during an all via the remote control:

1. Press ≡ or OK to open **Talk Menu**.
2. Press ▲or ▼to scroll to **Call Statistics** and then press OK.
3. Press ▲or ▼to view call statistics for every participant.
4. Press ⮌ to return.

To view call statistics during an all via the CP960 conference phone:

1. Tap ••• ->  during a call.
   The touch screen displays all participants.
2. Tap the desired participant to view call statistics.

Using Diagnostic Methods

The system supports the following diagnostic methods:

- **Audio Diagnose**: Test the audio input device and audio output device.
- **Camera Diagnose**: Test whether the camera can pan and change focus normally.
- **Ping**: Test whether the system can establish contact with a far-site IP address t entered.
- **Trace Route**: Tests the routing path between the local system and the IP address entered.

Above diagnostic methods can be configured using remote control. Ping and Trance Route can also be configured via web user interface.

To diagnose audio via the remote control:

1. Select **More**->**Setting**-> **Diagnose**.
2. Select **Audio Diagnose**, and then press OK.
3. Speak into the microphone.
4. Check whether the microphone can pick up audio and play back the audio properly.

   If the system plays back the audio normally, it means that audio works well.
5. Press OK to stop audio diagnostics.

To diagnose the camera via the remote control:

1. Select **More**->**Setting**-> **Diagnose**.
2. Select **Camera Diagnose**, and then press OK.
3. Press navigation keys to adjust the camera position.
4. Press or to adjust the focus.

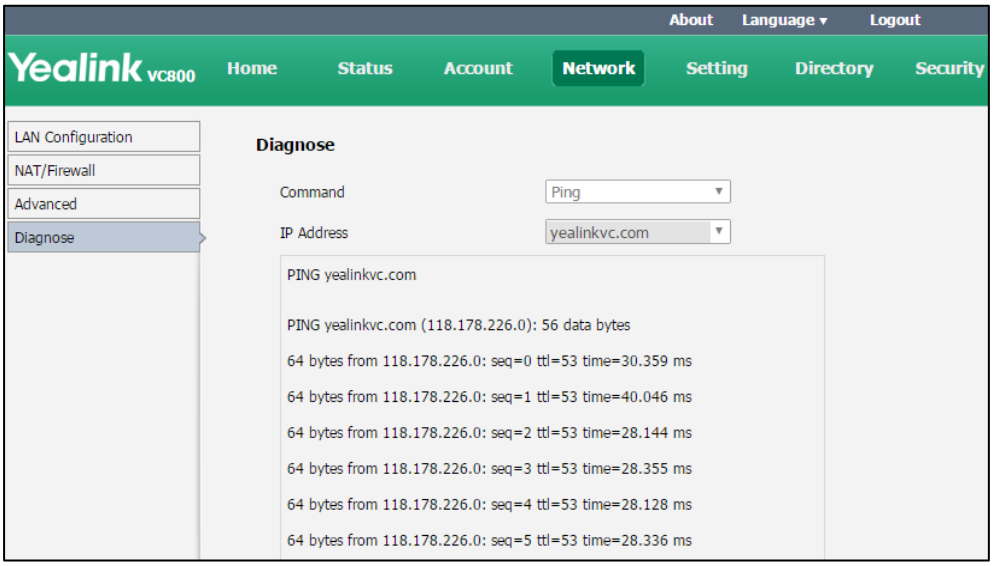
   If the camera can move and zoom normally, it means that the c amera works properly.
5. Press to stop camera diagnose.

To diagnose network via web user interface:

1. Click on **Network**->**Diagnose**.
2. Select the desired diagnostic method from the pull-down list of **Command**.
3. Click **Start** to start diagnosing.

   You can also enter any IP address in the **IP Address** field.

   The web page displays the diagnosis:



4. Click **Stop** to complete diagnosing.

   You can click **Copy** to copy the content to the clipboard.

To diagnose network via the remote control:

1. Select **More**->**Setting**-> **Diagnose**->**Ping**.
2. Select **Start**, and then press OK.
3. The system will Ping **yealinkvc.com** address by default. This will check whether the system can establish contact with the public IP address.
4. You can also enter any IP address (for example, the IP address of the remote system) in the **Ping** field.

   It measures the round-trip time from transmission to reception and reports errors and packet loss. The results of the test include a statistical summary of the response packets received, including the minimum, maximum, and the mean round-trip times.
5. Press ↩ to return to the Diagnose menu.

Trace Route:

1. Select **More**->**Setting**-> **Diagnose** ->**Trace Route**.
2. Select **Start**, and then press OK.
3. The system will trace **yealinkvc.com** address by default.
4. You can also enter any IP address (for example, the IP address of the remote system) in the **Trace Route** field.

   If the test is successful, the system lists the hops between the system and the IP address you entered. You can check whether congestion happens via the time cost between hops.
5. Press ↩ to return to the Diagnose menu.

Troubleshooting Solutions

This chapter provides general troubleshooting solutions to help you solve the problems you might encounter when using your system.

Ensure that the system has not been physically damaged when experiencing a problem. Check whether the cables are loose and the connections are correct and secure. These are common causes of problems.

If problems you encounter are not mentioned in this chapter, you can contact your distributor or Yealink FAE.

General Issues

Why is the display device black?

- Check whether the display device is connected properly to the VC800/VC500 codec.
- Check whether the system is in sleep mode. Press any key on the CP960 conference phone or remote control to resume system operation.
- Check whether the display device is in sleep mode or is turned off. Press the power button

on the remote control or on the display device.

- Check whether you have selected the correct video input source. You can try to change video input source.

Why doesn't the display device display time and date correctly?

- If you have configured the system to obtain the time and date from the NTP server automatically, ensure that SNTP server and time zone are configured correctly in the system and whether the connection between the system and NTP server is working properly.
- If you have configured the system to obtain the time and date manually, ensure that you have configured the time and date correctly.
- Check whether you hide the time. For more information, refer to Hiding Heading Time on page 152.

Why doesn't the remote control work?

- Check whether the system is powered on.
- Check whether the positive and negative charges of the battery are connected correctly.
- Check whether the battery has sufficient power left.
- Check whether no special fluorescent or neon signs nearby.

Why does the system fail to call the far site?

- Check whether the network of the near site is available.
- Check whether the network of the far site is available.
- Check whether the far site enables the DND feature.
- Check whether the accounts have been registered correctly, and the system uses the appropriate account to call the far site.
- Ensure that the number you are calling is correct.
- Check whether the far site rejects your call.
- Check whether the firewall blocks the inbound traffics from the other site.
- Check whether the far site has already up to maximum call-in limitation.
- If the near site is forced to use encryption, ensure that the far site enables encryption too. For more information on call encryption, refer toSecure Real-Time Transport Protocol on page 225 and H.235 on page 228.
- Ensure that the far site supports the same call protocol as the near site.

Why does the system fail to call the far site via IP address?

- Ensure that at least one call protocol is enabled on both sites. For more information, refer to Configuring SIP Settings on page 59 and Configuring H.323 Settings on page 64.

- Ensure that the network is connected correctly.
- Ensure that the network is configured correctly. For more information, refer to Configuring LAN Properties on page 14.
- Ping the IP address of the far site. Contact your system administrator if it fails. For more information, refer to Using Diagnostic Methods on page 250.

Why doesn't the status bar of the display device display IP address?

- Check whether the network is available.
- Check whether the LAN property is configured correctly. For more information on LAN property configuration, refer to Configuring LAN Properties on page 14.
- Check whether the system has enabled the hide IP address feature. For more information on disabling the hide IP address feature, refer to Hiding IP Address on page 151.

Why does the network keep losing packets?

- Check whether the network is available and the LED indicator on the left of the Internet port illuminates green.
- Try to use the low speed connection to check whether packets are lost. Deficient bandwidth is an important reason for packet loss.
- Check the configuration of the network speed and duplex mode on the system, switch and router.

Camera Issues

Why can't I adjust the camera angle and focus?

- You can adjust the camera when the system is idle or during a call. The camera cannot be adjusted when the system is in the menu screen.
- Ensure that the batteries in the remote control are in good working condition, and installed correctly.
- Aim the remote control at the sensor when operating the unit.
- Ensure that no objects are obstructing the sensor on the front of the camera.
- Ensure that the LED on the front of the camera flashes green when you use the remote control to operate the unit.
- Ensure that what you are controlling is the local camera.
- Reboot the system.
- If the above suggestions cannot solve your problem, perhaps the remote control is broken. You can contact your system administrator for help.

Why can't adjust the remote camera during an active call?

- Use the remote control to control the local camera to check whether the remote control can be used normally.
- Ensure that the far site has enabled the far-end camera control feature. For more information, refer to Far-end Camera Control on page 181.
- Ensure that you are controlling the remote camera. Press OK, and then select **Other**->**Near/Far Camera** during an active call and then select the remote video image.
- Ensure that the far site supports the same call protocol as the near site. For more information, refer to Camera Control Protocol on page 182.

Why is the video quality bad?

- Ensure that the display device has suitable resolution.
- Check whether the packet has been lost. For more information on packet loss, refer to Viewing Call Statistics on page 250.
- Ensure that camera settings are configured correctly, such as brightness and white balance.
- Avoid high-intensity indoor light or direct sunlight on the camera.

Video & Audio Issues

Why can't I hear the audio during a call?

- Ensure that the local audio output device is connected correctly.
- Use audio diagnose to check whether the audio device is working normally.
- Ensure that the ringer volume is not set to the minimum.
- Check whether the far site is muted.

Why can't the far site hear the local audio?

- Ensure that the local audio input device is connected correctly.
- Ensure that speakers are not obscured or damaged. Do not stack items on top of the CP960 conference phone.
- Check whether the near site is muted.
- Check whether the system has enabled the auto answer mute feature.
- Check whether the system has enabled the auto dialout mute feature.

Why can't I hear the other site clearly during a call?

- Ensure that the speaker volume of the far site is not set too low.
- Muffled audio reception from the far side may be caused by highly reverberant rooms. Speak in close proximity to the phone.

- Adjust the priority order for your audio codec if you have chosen a low-bandwidth audio codec to be first. For more information, refer to Audio Codecs on page 101.
- Dust and debris may cause audio quality. Do not use any kind of liquid or aerosol cleaner on the phone. A soft, slightly damp cloth should be sufficient to clean the top surface of the phone if necessary.

Why is the voice quality poor?

Users may receive poor voice quality during a call, such as intermittent voice, low volume, echo or other noise. It is difficulty to diagnosis the root causes of the voice anomalies. The possible reasons are:

- Users sit too far from or near to the microphone.
- The audio pickup device is moved frequently.
- Intermittent voice is probably caused by voice packet loss or jitter. Voice packet loss may occur due to network congestion. Jitter may occur due to information reorganization of the transmission or receiving equipment, such as, delay processing, retransmission mechanism or buffer overflow.
- Noise devices, such as computers or fans, may make it difficult to hear each other's voices clearly.
- Wires may also cause this problem. Replace the old with the new cables, and then reconnect to check whether the new cables provide better connectivity.

Why can't I view the local video image?

- Check whether the camera is powered on, and the LED indicator illuminates green.
- Check whether the camera is selected for the current video input source.
- Check the screen layout to see whether the remote video image is shown in full size.

Why can't I view the menu?

- Check whether the Display1 port of VC800/VC500 codec is connected to the HDMI port on the display device.

Why can't I start presentation?

- Check whether a PC is connected to the VCH50 video conferencing hub.
- Check whether the PC is sending a signal.
- Check the call statistics to see whether the system is sharing content.
- Ensure that dual-stream is configured correctly. For more information, refer to Dual-Stream Protocol on page 170.

Why does the far-site display black screen when local starts a presentation?

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. This may lead to failure.

You can configure network address adapter to let the content to be sent to the actual public IP address.

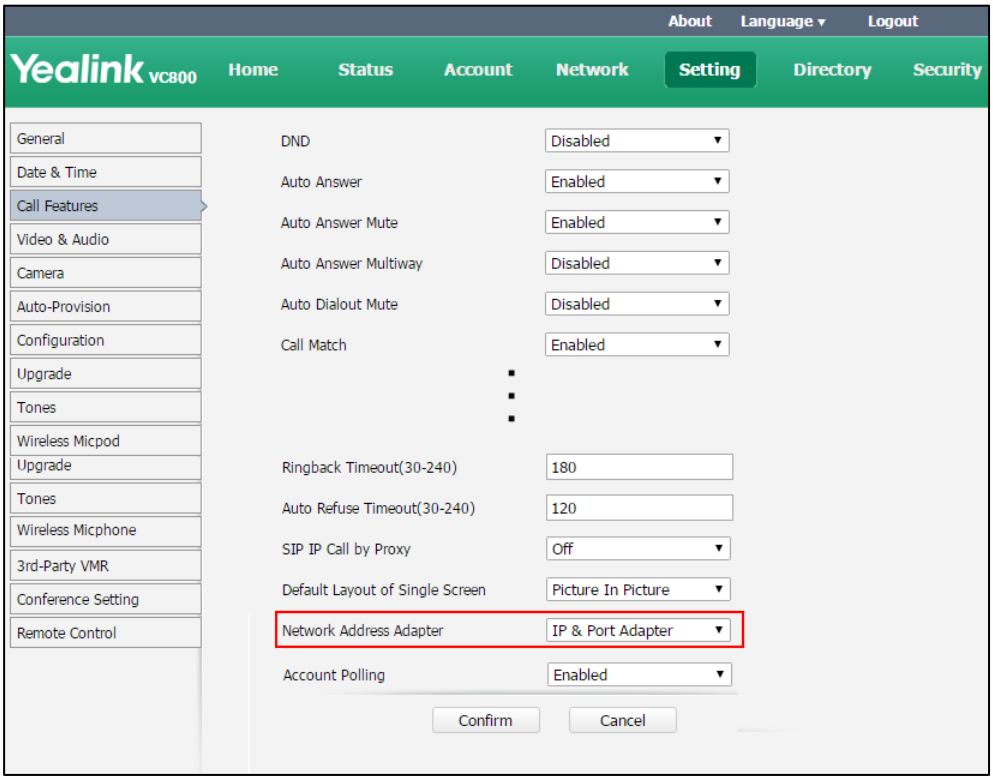
Network address adapter parameter is described below:

Parameter	Description	Configuration Method
Network address adapter	Enables or disables the network address adapter feature. **Valid values:** • **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. **Default:** IP & Port Adapter **Note:** IP address and port can be negotiated through the SDP protocol.	Web User Interface

To configure the network address adapter via web user interface:

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

2. Select the desired level from the pull-down list of **Network Address Adapter**.



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

System Maintenance

How to prevent monitor burn-in?

Refer to your monitor's documentation for specific recommendations and instructions. The following guidelines help prevent image burn-in:

- Ensure that static images are not displayed for long periods.
- Be aware that meetings that last more than an hour without much movement can have the same effect as a static image.
- Configure the automatic sleep time to be 1 hours or less.
- Consider decreasing the monitor's sharpness, brightness, and contrast settings if they are set to their maximum values.

How to reboot the system?

When you do one of the following, the system will reboot:

- Reboot system
- Reset system
- Upgrade firmware

- Configure some features need to take effect after a reboot

You can reboot the system in the following ways:

- Select **More**->**Setting**->**Advanced** (default password: 0000) ->**Reboot & Reset**->**Reboot**, and then press OK .
- Log into web user interface and click on **Setting**->**Upgrade**->**Reboot**, and then click **Confirm**.

Why does the system fail to upgrade?

- Ensure that the firmware is different from the firmware currently in use.
- Ensure that the downloaded firmware applies to the system.
- Ensure that the system is powered on normally, and the network is available during the upgrade process.
- When upgrading firmware via web user interface, ensure that the web user interface is not refreshed or closed during the upgrade process.

Appendix

Appendix A: Time Zones

Time Zone	Time Zone Name
−11:00	Samoa
−10:00	United States-Hawaii-Aleutian
−10:00	United States-Alaska-Aleutian
−09:30	French Polynesia
−09:00	United States-Alaska Time
−08:00	Canada(Vancouver, Whitehorse)
−08:00	Mexico(Tijuana, Mexicali)
−08:00	United States-Pacific Time
−07:00	Canada(Edmonton, Calgary)
−07:00	Mexico(Mazatlan, Chihuahua)
−07:00	United States-Mountain Time
−07:00	United States-MST no DST
−06:00	Canada-Manitoba(Winnipeg)
−06:00	Chile(Easter Islands)
−06:00	Mexico(Mexico City, Acapulco)
−06:00	United States-Central Time
−05:00	Bahamas(Nassau)
−05:00	Canada(Montreal, Ottawa, Quebec)
−05:00	Cuba(Havana)
−05:00	United States-Eastern Time
−04:30	Venezuela(Caracas)
−04:00	Canada(Halifax, Saint John)
−04:00	Chile(Santiago)
−04:00	Paraguay(Asuncion)
−04:00	United Kingdom-Bermuda(Bermuda)
−04:00	United Kingdom(Falkland Islands)
−04:00	Trinidad&Tobago
−03:30	Canada-New Foundland(St.Johns)
−03:00	Denmark-Greenland(Nuuk)
−03:00	Argentina(Buenos Aires)
−03:00	Brazil(no DST)
−03:00	Brazil(DST)
−02:30	Newfoundland and Labrador
−02:00	Brazil(no DST)
−01:00	Portugal(Azores)

Time Zone	Time Zone Name
0	GMT
0	Greenland
0	Denmark-Faroe Islands(Torshavn)
0	Ireland(Dublin)
0	Portugal(Lisboa, Porto, Funchal)
0	Spain-Canary Islands(Las Palmas)
0	United Kingdom(London)
0	Morocco
+01:00	Albania(Tirane)
+01:00	Austria(Vienna)
+01:00	Belgium(Brussels)
+01:00	Caicos
+01:00	Chad
+01:00	Spain(Madrid)
+01:00	Croatia(Zagreb)
+01:00	Czech Republic(Prague)
+01:00	Denmark(Kopenhagen)
+01:00	France(Paris)
+01:00	Germany(Berlin)
+01:00	Hungary(Budapest)
+01:00	Italy(Rome)
+01:00	Luxembourg(Luxembourg)
+01:00	Macedonia(Skopje)
+01:00	Netherlands(Amsterdam)
+01:00	Namibia(Windhoek)
+01:00	Poland (Warsaw)
+02:00	Estonia(Tallinn)
+02:00	Finland(Helsinki)
+02:00	Gaza Strip(Gaza)
+02:00	Greece(Athens)
+02:00	Israel(Tel Aviv)
+02:00	Jordan(Amman)
+02:00	Latvia(Riga)
+02:00	Lebanon(Beirut)
+02:00	Moldova(Kishinev)
+02:00	Russia(Kaliningrad)
+02:00	Romania(Bucharest)
+02:00	Syria(Damascus)
+02:00	Turkey(Ankara)
+02:00	Ukraine(Kyiv, Odessa)
+03:00	East Africa Time

Time Zone	Time Zone Name
+03:00	Iraq(Baghdad)
+03:00	Russia(Moscow)
+03:30	Iran(Teheran)
+04:00	Armenia(Yerevan)
+04:00	Azerbaijan(Baku)
+04:00	Georgia(Tbilisi)
+04:00	Kazakhstan(Aktau)
+04:00	Russia(Samara)
+04:30	Afghanistan(Kabul)
+05:00	Kazakhstan(Aqtobe)
+05:00	Kyrgyzstan(Bishkek)
+05:00	Pakistan(Islamabad)
+05:00	Russia(Chelyabinsk)
+05:30	India(Calcutta)
+05:45	Nepal(Katmandu)
+06:00	Kazakhstan(Astana, Almaty)
+06:00	Russia(Novosibirsk, Omsk)
+06:30	Myanmar(Naypyitaw)
+07:00	Russia(Krasnoyarsk)
+07:00	Thailand(Bangkok)
+08:00	China(Beijing)
+08:00	Singapore(Singapore)
+08:00	Australia(Perth)
+08:00	Russia(Irkutsk, Ulan-Ude)
+08:45	Eucla
+09:00	Korea(Seoul)
+09:00	Japan(Tokyo)
+09:00	Russia(Yakutsk, Chita)
+09:30	Australia(Adelaide)
+09:30	Australia(Darwin)
+10:00	Australia(Sydney, Melbourne, Canberra)
+10:00	Australia(Brisbane)
+10:00	Australia(Hobart)
+10:00	Russia(Vladivostok)
+10:30	Australia(Lord Howe Islands)
+11:00	New Caledonia(Noumea)
+11:00	Russia(Srednekolymsk Time)
+11:30	Norfolk Island
+12:00	New Zealand(Wellington, Auckland)
+12:00	Russia(Kamchatka Time)
+12:45	New Zealand(Chatham Islands)

Time Zone	Time Zone Name
+13:00	Tonga(Nukualofa)
+13:30	Chatham Islands
+14:00	Kiribati

Appendix B: Trusted Certificates

Yealink video conferencing system trusts the following CAs by default:

- VeriSign Class 3 Public Primary Certification Authority - G5
- GeoTrust Universal CA
- Equifax Secure eBusiness CA-1
- Thawte Server CA
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 4 Public Primary Certification Authority - G3
- Thawte Premium Server CA
- thawte Primary Root CA - G2
- thawte Primary Root CA - G3
- GeoTrust Global CA 2
- GeoTrust Universal CA 2
- GeoTrust Primary Certification Authority
- GeoTrust Global CA
- Class 3 Public Primary Certification Authority
- -Thawte Personal Freemail CA
- thawte Primary Root CA
- -VeriSign Universal Root Certification Authority
- Equifax Secure Certificate Authority
- DigiCert High Assurance EV Root CA
- Equifax Secure Global eBusiness CA-1
- Yealink Equipment Issuing CA
- GeoTrust Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G4
- Deutsche Telekom Root CA 2
- Class 1 Public Primary Certification Authority
- Symantec Class 3 Secure Server CA - G4
- Symantec Class 3 Secure Server CA – G

- quickconnect.starleaf.com
- yealinkvc.com
- StarLeaf CA
- Class 1 Public Primary Certification Authority - G2
- Class 2 Public Primary Certification Authority - G2
- Class 3 Public Primary Certification Authority - G2
- Class 4 Public Primary Certification Authority - G2

Note Yealink endeavors to maintain a built-in list of most common used CA Certificates. Due to memory constraints, we cannot ensure a complete set of certificates. If you are using a certificate from a commercial Certificate Authority not in the list above, you can send a request to your local distributor. At this point, you can upload your particular CA certificate into your phone. For more information on uploading custom CA certificate, refer to Transport Layer Security on page 217.