



# Yealink Microsoft<sup>®</sup> Skype for Business<sup>™</sup>Edition IP Phones Administrator Guide

Version 8.21 May. 2016

## Copyright

#### Copyright © 2016 YEALINK (XIAMEN) NETWORK TECHNOLOGY CO., LTD

Copyright © 2016 Yealink(Xiamen) Network Technology CO., LTD. All rights reserved. No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Yealink(Xiamen) Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

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

### 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.

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.

## **Declaration of Conformity**

Hereby, Yealink(Xiamen) Network Technology CO., LTD. declares that this phone is in conformity with the essential requirements and other relevant provisions of the CE, FCC. Statements of compliance can be obtained by contacting support@yealink.com.

## **CE Mark Warning**

These devices are marked with the CE mark in compliance with EC Directives 2014/35/EU and 2014/30/EU.

#### Part 15 FCC Rules

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device is compliant with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

#### **Class B Digital Device or Peripheral**

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

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

### **WEEE Warning**



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

### **Customer Feedback**

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

## **GNU GPL INFORMATION**

Yealink IP phone firmware contains third-party software under the GNU General Public License (GPL). Yealink uses software under the specific terms of the GPL. Please refer to the GPL for the exact terms and conditions of the license.

The original GPL license, source code of components licensed under GPL and used in Yealink products can be downloaded from Yealink web site:

http://www.yealink.com/GPLOpenSource.aspx?BaseInfoCateId=293&NewsCateId=293&CateId=293.

### **About This Guide**

This guide is intended for administrators who need to properly deploy Yealink IP phones with Skype for Business Server. It provides details on the functionality and configuration of IP phones.

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

### **Documentations**

This guide covers SIP-T48G, SIP-T46G, SIP-T42G, SIP-T41P and SIP-T40P IP phones. The following related documents are available:

- Quick Start Guides, which describe how to assemble IP phones and configure the most basic features available on IP phones.
- User Guides, which describe the basic and advanced features available on IP phones.
- Auto Provisioning Guide, which describes how to provision IP phones using the configuration files.
- Description of Configuration Parameters in CFG Files, which describes all configuration parameters in configuration files.
- Deployment Guide, which describes how to deploy phones in a Microsoft Skype for Business Server environment.
- Updating Phone Firmware from Microsoft Skype for Business Server Guide, which describes how to upgrade firmware via Skype for Business Server.

For support or service, please contact your Yealink reseller or go to Yealink Technical Support online: <a href="http://support.yealink.com/">http://support.yealink.com/</a>.

### **Conventions Used in Yealink Documentations**

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	

Convention	Description
	menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (e.g., Click on <b>Security</b> -> <b>License</b> ). Also used to emphasize text (e.g., <b>Configuration File</b> ).
Italics	Used to show the format of examples (e.g., http(s)://[IPv6 address]), or to show the title of a section in the reference documentations available on the Yealink Technical Support Website (e.g., Triggering the IP phone to Perform the Auto Provisioning).
Blue Text	Used for cross references to other sections within this documentation (e.g., refer to Troubleshooting).
Blue Text in Italics	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (e.g., Yealink_Microsoft_Skype_for_Business_Edition_IP_Phones_Aut o_Provisioning_Guide).

### In This Guide

The information detailed in this guide is applicable to the IP phones running Skype for Business firmware version 8 or higher. The firmware format is like x.x.x.rom. The second x from left must be greater than or equal to 8 (e.g., the firmware version of SIP-T46G IP phone: 28.8.0.21.rom). This administrator guide includes the following chapters:

- Chapter 1, "Product Overview" describes the SIP components and SIP IP phones.
- Chapter 2, "Getting Started" describes how to install and connect IP phones, configuration methods and resource files.
- Chapter 3, "Configuring Basic Features" describes how to configure the basic features on IP phones.
- Chapter 4, "Configuring Advanced Features" describes how to configure the advanced features on IP phones.
- Chapter 5, "Configuring Audio Features" describes how to configure the audio features on IP phones.
- Chapter 6, "Configuring Security Features" describes how to configure the security features on IP phones.
- Chapter 7, "Troubleshooting" describes how to troubleshoot IP phones and provides some common troubleshooting solutions.
- Chapter 8, "Appendix" provides the glossary, reference information about IP phones compliant with RFC 3261, SIP call flows and the sample configuration files.

### Summary of Changes

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

### Changes for Release 8, Guide Version 8.21

This version is updated to incorporate SIP-T46G, SIP-T42G, SIP-T41P and SIP-T40P IP phones. And SIP-T22/T22P IP phones are removed from version 8.

The following sections are new for this version:

- Conventions Used in Yealink Documentations on page v
- Expansion Module on page 23
- Contrast on page 83
- Sign out on page 98
- Updating Status Automatically on page 99
- Loading Language Packs on page 121
- Directory on page 139
- Pre Dial Tone on page 163
- Boss-Admin Feature on page 194
- Calendar on page 198
- EXP40 Expansion Module on page 206
- Multicast Paging on page 209
- Action URI on page 217
- Voice Mail Tone on page 260
- Skype for Business Feature License on page 281
- License Status on page 283

Major update has occurred to the following sections:

- Physical Features of IP Phones on page 18
- Connecting the IP Phones on page 25
- Reading Icons on page 32
- Configuration Files on page 35
- PPPoE on page 58
- Sign in on page 87
- Saving Call Log on page 153
- E911 on page 191
- BToE on page 204

- LLDP on page 221
- Phone Lock on page 288
- 802.1X Authentication on page 305
- Viewing Log Files on page 317

## **Table of Contents**

About This Guide	v
Documentations	N/
Conventions Used in Yealink Documentations	v v
	vi
Summary of Changes	vii
Changes for Release 8, Guide Version 8.21	vii
Table of Contents	ix
Product Overview	15
VoIP Principle	15
SIP Components	16
SIP Phone Models	17
Physical Features of IP Phones	
Key Features of IP Phones	21
Expansion Module	23
Getting Started	25
Connecting the IP Phones	25
Attaching the Stand and the Optional Wall Mount Bracket	
Connecting the Handset and Optional Headset	
Connecting the Power and Network	
Initialization Process Overview	
Verifying Startup	
Reading Icons	
Configuration Methods	
Phone User Interface	35
Web User Interface	35
Configuration Files	35
Obtaining Configuration Files and Resource Files	
Provisioning Server	
Supported Provisioning Protocols	
Setting up the Provisioning Server	
Deploying Phones from the Provisioning Server	
Configuring Basic Network Parameters	40

DHCP	40
DHCP Option	44
Configuring Network Parameters Manually	53
PPPoE	58
Configuring Transmission Methods of the Internet Port and PC Port	61
Configuring PC Port Mode	64
Branch Office Resiliency	66
Upgrading Firmware	67
Upgrading Firmware via Web User Interface	67
Upgrading Firmware from the Provisioning Server	68
Updating Phone Firmware from Skype for Business Server	73

## Configuring Basic Features ......79

Power Indicator LED	80
Contrast	
Backlight	85
Sign in	
User Sign-in	
PIN Sign-in	
Device Pairing for Online	94
Sign out	
Updating Status Automatically	
Web Server Type	
Time and Date	
NTP Time Server	
Time and Date Settings	
Daylight Saving Time	
Language	
Loading Language Packs	121
Specifying the Language to Use	
Key As Send	
Dial Plan	
Dial-now	
Directory	
Skype for Business Directory	
Local Directory	142
Saving Call Log	
Missed Call Log	
Dial Search Delay	
Live Dialpad	
Call Waiting	
Pre Dial Tone	
Redial Tone	164
Ringer Device for Headset	

Auto Answer	167
Always On Line	169
Busy Tone Delay	171
Return Code When Refuse	172
Early Media	173
180 Ring Workaround	174
Call Hold	175
Allow Trans Exist Call	177
Call Number Filter	179
DTMF	181
Suppress DTMF Display	183
Transfer via DTMF	185
Play Local DTMF Tone	187
Allow Mute	189
Voice Mail without PIN	190
E911	191
E911 Location Tip	192
Boss-Admin Feature	194
Calendar	198
Setting up a Skype Conference in Outlook	198
Setting up an Appointment in Outlook	198
Setting up a Meeting in Outlook	199
Setting up an Event in Outlook	200
Using the Calendar	201
ВТОЕ	204
EXP40 Expansion Module	206
Assigning Skype for Business Contacts to EXP40	206

### 

Multicast Paging	
Sending RTP Stream	
Receiving RTP Stream	
Action URI	
Configuring Trusted IP Address for Action URI	
Capturing the Current Screen of the Phone	
VLAN	
LLDP	
CDP	
Manual Configuration for VLAN	
DHCP VLAN	232
Quality of Service	
IPv6 Support	

Ring Tones	249
Tones	253
Voice Mail Tone	
Headset Prior	
Dual Headset	
Audio Codecs	
Acoustic Clarity Technology	272
Acoustic Echo Cancellation	272
Background Noise Suppression	273
Automatic Gain Control	273
Voice Activity Detection	274
Comfort Noise Generation	275
Jitter Buffer	277

### 

Skype for Business Feature License	
License Status	
User Password	
Administrator Password	
Auto-Logout Time	
Phone Lock	
Account Lock	
Transport Layer Security	
Encrypting Configuration Files	
802.1X Authentication	

### 

Troubleshooting Methods	
Viewing Log Files	
Capturing Packets	
Enabling Watch Dog Feature	
Getting Information from Status Indicators	329
Analyzing Configuration File	
Troubleshooting Solutions	
IP Address Issues	
Audio Issues	
Upgrading Issues	
Provisioning Issues	
Resetting Issues	
Rebooting Issues	
Protocols and Ports Issues	
Display Issues	
Time and Date Issues	

System Log Issues	
Password Issues	
Other Issues	340
Appendix	343
Appendix A: Glossary	343
Appendix B: Time Zones	
Appendix C: Trusted Certificates	
Appendix D: SIP (Session Initiation Protocol)	
RFC and Internet Draft Support	
SIP Request	351
SIP Header	352
SIP Responses	353
SIP Session Description Protocol (SDP) Usage	356
Appendix E: SIP Call Flows	356
Successful Call Setup and Disconnect	356
Unsuccessful Call Setup—Called User is Busy	359
Unsuccessful Call Setup—Called User Does Not Answer	
Successful Call Setup and Call Hold	
Successful Call Setup and Call Waiting	
Call Transfer without Consultation	
Call Transfer with Consultation	
Call Conference	
Index	

### **Product Overview**

This chapter contains the following information about IP phones:

- VoIP Principle
- SIP Components
- SIP Phone Models

### **VoIP** Principle

#### VolP

**VoIP** (Voice over Internet Protocol) is a technology using 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 endpoints. Like other VoIP protocols, SIP is designed to address 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 attributes of an end-to-end call.

SIP provides capabilities to:

- Determine the location of the target endpoint -- SIP supports address resolution, name mapping, and call redirection.
- Determine media capabilities of the target endpoint -- Via Session Description Protocol (SDP), SIP determines the "lowest level" of common services between endpoints. Conferences are established using only media capabilities that can be supported by all endpoints.
- Determine the availability of the target endpoint -- A call cannot be completed because the target endpoint is unavailable, SIP determines whether the called party is already on the IP phone or does not answer in the allotted number of rings. It then returns a message indicating why the target endpoint is unavailable.
- Establish a session between the origin and target endpoint -- The call can be completed, SIP establishes a session between endpoints. SIP also supports mid-call changes, such as the addition of another endpoint to the conference or the change of a media characteristic or codec.
- Handle the transfer and termination of calls -- SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions between all parties.

### **SIP** Components

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can function as one of following roles:

- User Agent Client (UAC) -- A client application that initiates the SIP request.
- User Agent Server (UAS) -- A server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.

#### User Agent Client (UAC)

The UAC is an application that initiates up to six feasible SIP requests to the UAS. The six requests issued by the UAC are: INVITE, ACK, OPTIONS, BYE, CANCEL and REGISTER. When the SIP session is being initiated by the UAC SIP component, the UAC determines the information essential for the request, which is the protocol, the port and the IP address of the UAS to which the request is being sent. This information can be dynamic and will make it challenging to put through a firewall. For this reason, it may be recommended to open the specific application type on the firewall. The UAC is also capable of using the information in the request URI to establish the course of the SIP

request to its destination, as the request URI always specifies the host which is essential. The port and protocol are not always specified by the request URI. Thus if the request does not specify a port or protocol, a default port or protocol is contacted. It may be preferential to use this method when not using an application layer firewall. Application layer firewalls like to know what applications are flowing through which ports and it is possible to use content types of other applications other than the one you are trying to let through what has been denied.

#### User Agent Server (UAS)

UAS is a server that hosts the application responsible for receiving the SIP requests from a UAC, and on reception it returns a response to the request back to the UAC. The UAS may issue multiple responses to the UAC, not necessarily a single response. Communication between UAC and UAS is client/server and peer-to-peer.

Typically, a SIP endpoint is capable of functioning as both a UAC and a UAS, but it functions only as one or the other per transaction. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiates the request.

### SIP Phone Models

This section introduces SIP-T48G, SIP-T46G, SIP-T42G, SIP-T41P and SIP-T40P models with Skype for Business firmware. They are designed to work with Skype for Business client. These IP phones are characterized by a large number of functions, which simplify business communication with a high standard of security.

The SIP-T48G, SIP-T46G, SIP-T42G, SIP-T41P and SIP-T40P IP phones provide a powerful and flexible IP communication solution for Ethernet TCP/IP networks, delivering excellent voice quality. When these IP phones are registered with Skype for Business Server, you can interact with your Skype for Business contacts list on your IP phones through Microsoft's Active Directory.

IP phones comply with the SIP standard (RFC 3261), and they can only be used within a network that supports this model of phone.

For a list of key features available on Yealink IP phones running the latest firmware, refer to Physical Features of IP Phones on page 18.

In order to operate as SIP endpoints in your network successfully, IP phones must meet the following requirements:

- A working IP network is established.
- VoIP gateways are configured for SIP.
- The latest (or compatible) firmware of IP phones is available.
- The Skype for Business Server is active and configured to receive and send SIP messages.

### **Physical Features of IP Phones**

This section lists the available physical features of SIP-T48G, SIP-T46G, SIP-T42G, SIP-T41P and SIP-T40P IP phones.

#### SIP-T48G



#### **Physical Features:**

- 7" 800 x 480 pixel color touch screen with backlight
- 24 bit depth color
- 1 Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 26 keys including 7 feature keys
- 1\*RJ9 (4P4C) handset port
- 1\*RJ9 (4P4C) headset port
- 2\*RJ45 10/100/1000Mbps Ethernet ports
- 4 LEDs: 1\*power, 1\*mute, 1\*headset, 1\*speakerphone
- Power adapter: AC 100~240V input and DC 5V/2A output
- Power over Ethernet (IEEE 802.3af)
- Built-in USB port, support Bluetooth headset
- Wall Mount

#### SIP-T46G



#### **Physical Features:**

- 4.3" 480 x 272 pixel color display with backlight
- 24 bit depth color
- 1 Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 40 keys
- 1\*RJ9 (4P4C) handset port
- 1\*RJ9 (4P4C) headset port
- 2\*RJ45 10/100/1000Mbps Ethernet ports
- 6 LEDs: 1\*power, 1\*line, 1\*Boss Admin key, 1\*mute, 1\*headset, 1\*speakerphone
- Power adapter: AC 100~240V input and DC 5V/2A output
- Power over Ethernet (IEEE 802.3af)
- Built-in USB port, support Bluetooth headset
- Wall Mount

#### SIP-T42G



#### **Physical Features:**

- 192 x 64 graphic LCD
- 1 Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 34 keys
- 1\*RJ9 (4P4C) handset port
- 1\*RJ9 (4P4C) headset port
- 2\*RJ45 10/100/1000Mbps Ethernet ports
- 1\*RJ12 (6P6C) EHS36 headset adapter port
- 6 LEDs: 1\*power, 1\*line, 1\*Boss/Admin key, 1\*mute, 1\*headset, 1\*speakerphone
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)
- Wall Mount

#### SIP-T41P



#### **Physical Features:**

- 192 x 64 graphic LCD
- 1 Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 34 keys
- 1\*RJ9 (4P4C) handset port
- 1\*RJ9 (4P4C) headset port
- 2\*RJ45 10/100Mbps Ethernet ports
- 1\*RJ12 (6P6C) EHS36 headset adapter port
- 6 LEDs: 1\*power, 1\*line, 1\*Boss/Admin key, 1\*mute, 1\*headset, 1\*speakerphone

- Power adapter: AC 100~240V input and DC 5V/1.2A output
- Power over Ethernet (IEEE 802.3af)
- Wall Mount

#### SIP-T40P



#### **Physical Features:**

- 132 x 64 graphic LCD
- 1 Skype for Business account
- HD Voice: HD Codec, HD Handset, HD Speaker
- 31 keys
- 1\*RJ9 (4P4C) handset port
- 1\*RJ9 (4P4C) headset port
- 2\*RJ45 10/100Mbps Ethernet ports
- 1\*RJ12 (6P6C) EHS36 headset adapter port
- 3 LEDs: 1\*power, 1\*line, 1\*Boss/Admin key
- Power adapter: AC 100~240V input and DC 5V/600mA output
- Power over Ethernet (IEEE 802.3af)
- Wall Mount

### Key Features of IP Phones

In addition to physical features introduced above, IP phones also support the following key features when running the latest firmware:

- Phone Features
  - **Call Options**: call waiting, call hold, call mute, call forward and call transfer.

- **Basic Features**: DND, live dialpad, dial plan, caller identity, auto answer.
- Codecs and Voice Features
  - Wideband codec: G.722
  - Narrowband codec: G.711, G.726, G.729, iLBC, G723 (G723 is not applicable to SIP-T40P IP phones)
  - VAD, CNG, AEC, PLC, AJB, AGC
  - Full-duplex speakerphone with AEC
- Network Features
  - SIP v1 (RFC2543), v2 (RFC3261)
  - Proxy mode and peer-to-peer SIP link mode
  - IP assignment: Static/DHCP/PPPoE (PPPoE is not applicable to SIP-T42G/T41P/T40P IP phones)
  - VLAN assignment: LLDP/Static/DHCP/CDP
  - Bridge mode for PC port
  - HTTP/HTTPS server
  - DNS client
  - DHCP server
  - IPv6 support

#### Management

- FTP/TFTP/HTTP auto-provision
- Configuration: browser/phone/auto-provision
- Dial number via SIP server
- Dial URL via SIP server
- Security
  - HTTPS (server/client)
  - Transport Layer Security (TLS)
  - VLAN (802.1q), QoS
  - Digest authentication using MD5/MD5-sess
  - Secure configuration file via AES encryption
  - Phone lock for personal privacy protection

- Admin/User configuration mode
- 802.1X authentication

### **Expansion Module**

This section introduces EXP40 expansion modules. EXP40 is only applicable to SIP-T48G and SIP-T46G IP phones.

#### EXP40



#### **Physical Features:**

- Rich visual experience with 160 x 320 graphic LCD
- 20 physical keys each with a dual-color LED
- 20 additional keys through page switch
- Supports up to 6 modules daisy-chain
- Power adapter: AC 100~240V input and DC 5V/1.2A output
- 2\*RJ-12 (6P6C) ports for data in and out
- Wall Mount

## **Getting Started**

This chapter provides basic information and installation instructions of IP phones. This chapter provides the following sections:

- Connecting the IP Phones
- Initialization Process Overview
- Verifying Startup
- Reading Icons
- Configuration Methods
- Obtaining Configuration Files and Resource Files
- Provisioning Server
- Configuring Basic Network Parameters
- Branch Office Resiliency
- Upgrading Firmware

### Connecting the IP Phones

This section introduces how to install SIP-T48G, SIP-T46G, SIP-T42G, SIP-T41P and SIP-T40P IP phones with components in packaging contents.

- 1. Attach the stand and the optional wall mount bracket
- 2. Connect the handset and optional headset
- 3. Connect the network and power
- **Note** The optional accessories are not included in packaging contents. You need to purchase them separately if required.

### Attaching the Stand and the Optional Wall Mount Bracket

#### To attach the stand and the optional wall mount bracket:

For SIP-T48G:





Wall Mount Method (Optional)

**Note** The top two slots on SIP-T48G IP phones are plugged up by silica gel. You need to pull out silica gel before attaching the wall mount bracket.

For SIP-T46G:



**Desk Mount Method** 



Wall Mount Method (Optional)

#### For SIP-T42G/T41P/T40P:



**Desk Mount Method** 



#### Wall Mount Method (Optional)

Note The hookswitch tab has a lip which allows the handset to stay on-hook when the IP phone is mounted vertically.

> For more information on how to mount the IP phone to a wall, refer to Yealink Wall Mount Quick Installation Guide.

### Connecting the Handset and Optional Headset

#### To connect the handset and optional headset:

For SIP-T48G/T46G:



#### For SIP-T42G/T41P/T40P:



## Note Wireless headset adapter EHS36 or Bluetooth USB dongle BT40 should be purchased separately.

For more information on how to use the EHS36 on the IP phone, refer to Yealink EHS36 User Guide.

Bluetooth USB dongle BT40 can only be used on the SIP-T48G/T46G IP phones. For more information on how to use the Bluetooth on SIP-T48G/T46G IP phones, refer to Yealink Bluetooth USB Dongle BT40 User Guide.

The EXT port on SIP-T48G/T46G IP phones can also be used to connect the expansion module EXP40.

### **Connecting the Power and Network**

#### AC Power (Optional)

#### To connect the AC power and network:

- 1. Connect the DC plug of the power adapter to the DC5V port on the IP phone and connect the other end of the power adapter into an electrical power outlet.
- 2. Connect the included or a standard Ethernet cable between the Internet port on the IP phone and the one on the wall or switch/hub device port.



#### Note

The IP phone should be used with Yealink original power adapter only. The use of the third-party power adapter may cause the damage to the phone.

IP Phone Model	Power Specification
SIP-T48G	5V/2A
SIP-T46G	5V/2A
SIP-T42G	5V/1.2A
SIP-T41P	5V/1.2A
SIP-T40P	5V/600mA

Power specifications are listed below:

#### **Power over Ethernet**

With the included or a regular Ethernet cable, IP phones can be powered from a PoE-compliant switch or hub.

#### To connect the PoE:

1) Connect the Ethernet cable between the Internet port on the IP phone and an available port on the in-line power switch/hub.



Note

If in-line power switch/hub is provided, you don't need to connect the phone to the power adapter. Make sure the switch/hub is PoE-compliant.

The IP phone can also share the network with another network device such as a PC (personal computer). It is an optional connection.

**Important!** Do not unplug or remove the power while the IP phone is updating firmware and configurations.

### Initialization Process Overview

The initialization process of the IP phone is responsible for network connectivity and operation of the IP phone in your local network.

Once you connect your IP phone to the network and to an electrical supply, the IP phone begins its initialization process.

During the initialization process, the following events take place:

#### Loading the ROM file

The ROM file resides in the flash memory of the IP phone. The IP phone comes from the factory with a ROM file preloaded. During initialization, the IP phone runs a bootstrap loader that loads and executes the ROM file.

#### **Configuring the VLAN**

If the IP phone is connected to a switch, the switch notifies the IP phone of the VLAN information defined on the switch (if using LLDP or CDP). The IP phone can then proceed with the DHCP request for its network settings (if using DHCP).

#### Querying the DHCP (Dynamic Host Configuration Protocol) Server

The IP phone is capable of querying a DHCP server. DHCP is enabled on the IP phone by default. The following network parameters 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 network parameters of the IP phone manually if any of them is not supplied by the DHCP server. For more information on configuring network parameters manually, refer to Configuring Network Parameters Manually on page 53.

#### Contacting the provisioning server

If the IP phone is configured to obtain configurations from the provisioning server, it will connect to the provisioning server and download the configuration file(s) during startup. The IP phone will be able to resolve and update configurations written in the configuration file(s). If the IP phone does not obtain configurations from the provisioning server, the IP phone will use configurations stored in the flash memory.

#### **Updating firmware**

If the access URL of firmware is defined in the configuration file, the IP phone will download firmware from the provisioning server. If the MD5 value of the downloaded firmware file differs from that of the image stored in the flash memory, the IP phone will perform a firmware update.

#### Downloading the resource files

In addition to configuration file(s), the IP phone may require resource files before it can

deliver service. These resource files are optional, but if some particular features are being deployed, these files are required.

The followings show examples of resource files:

- Language packs
- Ring tones

### Verifying Startup

After connected to the power and network, the IP phone begins the initializing process by cycling through the following steps:

- 1. The power indicator LED illuminates solid red.
- 2. The message "Welcome Initializing... please wait" appears on the LCD screen when the IP phone starts up.
- 3. The main LCD screen displays the following:
  - Time and date
  - Soft key labels
- 4. Press the OK key to check the IP phone status, the LCD screen displays the valid IP address, MAC address, firmware version, etc.

If the IP phone has successfully passed through these steps, it starts up properly and is ready for use.

### **Reading Icons**

Icons associated with different features may appear on the LCD screen. The following table provides a description for each icon on IP phones.

T48G	T46G	T42G/T41P	T40P	Description
/	/			Network is unavailable
*		*	/	Local Favorites
Ø		<b>A</b>	<b>N</b>	Call Mute
5	¢	/	/	Call Forward
< <u> </u>	/	/	/	Answer a call
C	/	/	/	Place a call
		0	0	Call Hold

T48G	T46G	T42G/T41P	T40P	Description
	/	/	/	Call Resume
+	/	/	/	Add a new call
	/	/	/	View more soft keys
(+)	/	/	/	Attended transfer
×	/	/	/	Blind transfer
	/	/	/	Call Park
	/	/	/	Invite a new call to the Skype for Business conference
~	/	/	/	View the conference participants
~	/	/	/	View the dial-in number and conference ID
$\odot$	/	/	/	Auto Redial
20	/	/	/	Forward incoming calls to voice mail
	/	/	/	Enter message center
$\bigcirc$	/	/	/	Reject or cancel a call
Ľ	ど	$\mathbf{N}$		Received Calls
V	2	5	K	Placed Calls
6	¢	>	5	Missed Calls
/	(e	Ľ	t	Forwarded Calls
*	<b>4</b> *	/	/	Bluetooth mode is on
*	<b>e</b>	/	/	Bluetooth headset is both paired and connected
<	/	/	/	Return to previous screen
		• <b>(</b> )	• <b>(</b> )	Hands-free speakerphone mode
()	()	/	/	Location is not set

T48G	T46G	T42G/T41P	T40P	Description
/	/	00	00	Voice Mail
/	AA	AA	AA	Auto Answer
$\mathbf{\Sigma}$		$\checkmark$	$\searrow$	Unread voice mail
$\diamond$	$\diamond$			Read voice mail
	/	/	/	Enable the conference announcement
	/	/	/	Disable the conference announcement
/	0	2	2	Organizer
<b>e</b>	8	2.	2.	Presenter
9	9	20		Attendee
<b>(</b> )		Ţ	F	Conference lock
/	Ń	∎ <b>(</b> ×	r∏×	Ringer volume is 0
	A	₄	Co	Phone Lock
0	٠	$\checkmark$	$\checkmark$	Available
•	•	!	-	Busy
•	0			DND (Do Not Disturb)
0	•	L	L	Be Right Back/Off Work/Away
	•	X	X	Off Line
•	•	?	?	Unknown

### **Configuration Methods**

IP phones can be configured automatically through configuration files stored on a central provisioning server, manually via phone user interface or web user interface, or by a combination of the automatic and manual methods.

The recommended method for configuring IP phones is automatically through a central provisioning server. If a central provisioning server is not available, the manual method

will allow changes to most features.

The following sections describe how to configure IP phones using each method.

- Phone User Interface
- Web User Interface
- Configuration Files

#### Phone User Interface

An administrator or a user can configure and use IP phones via phone user interface. Access to specific features is restricted to the administrator. The default password is "admin"(case-sensitive). Not all features are available on phone user interface. For more information, refer to Yealink phone-specific user guide.

### Web User Interface

An administrator or a user can configure IP phones via web user interface. The default user name and password for the administrator to log into the web user interface are both "admin" (case-sensitive). Most features are available for configuring via web user interface. IP phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to Web Server Type on page 100.

#### **Configuration Files**

An administrator can deploy and maintain a mass of IP phones using configuration files. The configuration files consist of:

- Common CFG file
- MAC-Oriented CFG file

#### **Common CFG file**

A Common CFG file contains parameters that affect the basic operation of the IP phone, such as language and volume. It will be effectual for all IP phones of the same model. The common CFG file has a fixed name for each IP phone model. The name of the Common CFG file for each IP phone model is:

- SIP-T48G: y00000000035.cfg
- SIP-T46G: y0000000028.cfg
- SIP-T42G: y0000000029.cfg
- SIP-T41P: y0000000036.cfg
- SIP-T40P: y0000000054.cfg

#### MAC-Oriented CFG file

A MAC-Oriented CFG file contains parameters unique to a particular phone. It will only be effectual for a specific IP phone. The MAC-Oriented CFG file is named after the MAC address of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of the MAC-Oriented CFG file must be 00156574b150.cfg (case-sensitive).

#### **Central Provisioning**

IP phones can be centrally provisioned from a provisioning server using the configuration files (<y000000000xx>.cfg and <MAC>.cfg). You can use a text-based editing application to edit configuration files, and then store configuration files to a provisioning server. For more information on the provisioning server, refer to Provisioning Server on page 37.

IP phones can obtain the provisioning server address during startup. Then IP phones download configuration files from the provisioning server, resolve and update the configurations written in configuration files. This entire process is called auto provisioning. For more information on auto provisioning, refer to

Yealink\_Microsoft\_Skype\_for\_Business\_Edition\_IP\_Phones\_Auto\_Provisioning\_Guide.

### **Obtaining Configuration Files and Resource Files**

When configuring particular features, you may need to upload resource files (e.g., language) to IP phones. If the resource file is to be used for all IP phones of the same model, the resource file access URL is best specified in the <y000000000xx>.cfg file. However, if you want to specify the desired phone to use the resource file, the resource file access URL should be specified in the <MAC>.cfg file.

Templo	File Name	
	Common CFG file	Common.cfg
Configuration Files	MAC-Oriented CFG file	MAC.cfg
	AutoDST Template	AutoDST.xml
Resource Files	Language Packs	For example, 000.GUI.English.lang
	Keypad Input	
	Method File	ime.txt

The names of the Yealink-supplied template files are:
Templo	File Name	
	Dial-now Template	dialnow.xml
	Contact File	contact.xml

You can ask the distributor or Yealink FAE for template files. You can also obtain the template files online:

http://www.yealink.com/solution\_info.aspx?ProductsCateID=1248&cateid=1248&BaseI nfoCateId=1328&Cate\_Id=1248&parentcateid=1328.

### To download template files:

- 1. Go to Yealink Document Download Page and select the desired phone model.
- 2. Download and extract the combined configuration files to your local system.
- 3. Open the folder you uncompressed to and identify the template file you will edit.

For some features, you can customize the filename as required. The following table lists the special characters supported by Yealink IP phones:

Server Platform	HTTP/HTTPS	TFTP/FTP
Windows	<pre>Support: ~`!@\$^(),.';[]{}(including space) Not Support:   &lt;&gt;:" / \ *? # % &amp; = +</pre>	<pre>Support: ~`!@\$^(),.';[]{}%&amp;=+ (including space) Not Support:   &lt;&gt;:" / \*?#</pre>
Linux	Support: ~`!@\$^()_ -,.';[]{} <>:" (including space) Not Support: / \ *?# % & = +	<pre>Support: ~`!@\$^(),.';[]{}  &lt;&gt;:"%&amp; = + (including space) Not Support: / \ *?#</pre>

# **Provisioning Server**

# **Supported Provisioning Protocols**

IP phones perform the auto provisioning function of downloading configuration files, downloading resource files and upgrading firmware. The transfer protocol is used to download files from the provisioning server. IP phones support several transport protocols for provisioning, including FTP, TFTP, HTTP, and HTTPS protocols. And you can specify the transport protocol in the provisioning server address, for example, http://xxxxxxx. If not specified, the TFTP protocol is used. The provisioning server address can be IP address, domain name or URL. If a user name and password are specified as part of the provisioning server address, for example, http://user:pwd@/server/dir, they will be used only if the server supports them.

Note A URL should contain forward slashes instead of back slashes and should not contain spaces. Escape characters are not supported.

If a user name and password are not specified as part of the provisioning server address, the User Name and Password of the provisioning server configured on the IP phone will be used.

There are two types of FTP methods—active and passive. IP phones are not compatible with active FTP.

## Setting up the Provisioning Server

The provisioning server can be on the local LAN or anywhere on the Internet. Use the following procedure as a recommendation if this is your first provisioning server setup. For more information on how to set up a provisioning server, refer to Yealink\_Microsoft\_Skype\_for\_Business\_Edition\_IP\_Phones\_Auto\_Provisioning\_Guide.

#### To set up the provisioning server:

- 1. Install a provisioning server application or locate a suitable existing server.
- 2. Create an account and home directory.
- 3. Set security permissions for the account.
- 4. Create configuration files and edit them as desired.
- 5. Copy the configuration files and resource files to the provisioning server.

For more information on how to deploy IP phones using configuration files, refer to Deploying Phones from the Provisioning Server on page 38.

**Note** Typically all phones are configured with the same server account, but the server account provides a means of conveniently partitioning the configuration. Give each account a unique home directory on the server and change the configuration on a

## Deploying Phones from the Provisioning Server

The parameters in the new downloaded configuration files will override the duplicate parameters in files downloaded earlier. During auto provisioning, IP phones download the common configuration file first, and then the MAC-Oriented file. Therefore any parameter in the MAC-Oriented configuration file will override the same one in the common configuration file.

Yealink supplies configuration files for each phone model, which is delivered with the IP phone firmware. The configuration files, supplied with each firmware release, must be

used with that release. Otherwise, configurations may not take effect, and the IP phone will behave without exception. Before you configure parameters in the configuration files, Yealink recommends that you create new configuration files containing only those parameters that require changes.

#### To deploy IP phones from the provisioning server:

- 1. Create per-phone configuration files by performing the following steps:
  - a) Obtain a list of phone MAC addresses (the bar code label on the back of the IP phone or on the outside of the box).
  - **b)** Create per-phone <MAC>.cfg files by using the MAC-Oriented CFG file from the distribution as templates.
  - c) Edit the parameters in the file as desired.
- 2. Create new common configuration files by performing the following steps:
  - a) Create <y00000000xx>.cfg files by using the Common CFG file from the distribution as templates.
  - **b)** Edit the parameters in the file as desired.
- 3. Copy configuration files to the home directory of the provisioning server.
- 4. Reboot IP phones to trigger the auto provisioning process.

IP phones discover the provisioning server address, and then download the configuration files from the provisioning server.

For more information on configuration files, refer to Configuration Files on page 35. For protecting against unauthorized access, you can encrypt configuration files. For more information on encrypting configuration files, refer to Encrypting Configuration Files on page 301.

During the auto provisioning process, the IP phone supports the following methods to discover the provisioning server address:

- **DHCP**: DHCP option can be used to provide the address or URL of the provisioning server to IP phones. When the IP phone requests an IP address using the DHCP protocol, the resulting response may contain option 66 or the custom option (if configured) that contains the provisioning server address.
- **Static**: You can manually configure the server address via phone user interface or web user interface.

For more information on the above methods, refer to Yealink\_Microsoft\_Skype\_for\_Business\_Edition\_IP\_Phones\_Auto\_Provisioning\_Guide.

# **Configuring Basic Network Parameters**

In order to get your IP phones running, you must perform basic network setup, such as IP address and subnet mask configuration. This section describes how to configure basic network parameters for IP phones.

Note

This section mainly introduces IPv4 network parameters. IP phones also support IPv6. For more information on IPv6, refer to IPv6 Support on page 238.

# 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. IP phones comply with the DHCP specifications documented in RFC 2131. If using DHCP, IP phones connected to the network become operational without having to be manually assigned IP addresses and additional network parameters.

## Procedure

DHCP can be configured using the configuration files or locally.

		Configure DHCP on the IP phone.	
Configuration File	<mac>.cfg</mac>	Parameter:	
		network.internet_port.type	
Local		Configure DHCP on the IP phone.	
	WahlkarIntarfaca	Navigate to:	
		http:// <phonelpaddress>/servlet ?p=network&amp;q=load</phonelpaddress>	
	Phone User Interface	Configure DHCP on the IP phone.	

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default		
network.internet_port.type	0, 1 or 2	0		
Description:				
Configures the Internet (WAN) port type for IPv4.				
0-DHCP				
1-PPPoE (not applicable to SIP-T42G/T41P/T40P IP phones)				

Parameters	Permitted Values	Default	
2-Static IP Address			
<b>Note</b> : It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			
Network->Basic->IPv4 Config			
Phone User Interface:			
Menu->Advanced (default password: a	dmin) ->Network->WAN	Port->IPv4	

#### To configure DHCP via web user interface:

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

		Log Out
Yealink   1466	Status Account Network Fe	atures Settings Directory Security
Basic	Internet Port	NOTE
PC Port Advanced	Mode(IPv4/IPv6) IPv4 IPv4 Config	OHCP The network configurations will be acquired from DHCP server.      Static IP Address Specify the IP address, Subnet Mask, Default Gateway, Primary DNS, Secondary DNS fields manually.      PPPOE Contact your ISP if it should be used.      Off     Off     You can click here to get more guides.
	PPPoE     Ver Name     Password	**

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 IP phone.

### To configure DHCP via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4.
- **2.** Press  $(\cdot)$  or  $(\cdot)$ , or the **Switch** soft key to select **DHCP** from the **Type** field.
- 3. Press the **Save** soft key to accept the change.

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

## Static DNS

Static DNS address(es) can be configured and used even though DHCP is enabled.

## Procedure

Static DNS can be configured using the configuration files or locally.

		Configure the static DNS feature.
	<y000000000xx>.cfg</y000000000xx>	Parameters:
		network.static_dns_enable
Configuration File		Configure static DNS address.
	<mac> cfa</mac>	Parameters:
	<macz.ciq< td=""><td>network.primary_dns</td></macz.ciq<>	network.primary_dns
		network.secondary_dns
Local		Configure the static DNS feature.
		Configure static DNS address.
	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		<pre>?p=network&amp;q=load</pre>
	Phone User Interface	Configure the static DNS feature.
		Configure static DNS address.

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default	
network.static_dns_enable	0 or1	0	
Description:			
Triggers the static DNS feature to on or c	off.		
<b>0</b> -Off			
<b>1</b> -On			
If it is set to 0 (Off), the IP phone will use the IPv4 DNS obtained from DHCP.			
If it is set to 1 (On), the IP phone will use manually configured static IPv4 DNS.			
<b>Note</b> : It works only if the value of the parameter "network.internet_port.type" is set to 0 (DHCP). If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			

Network->Basic->IPv4 Config->Static DNS

Parameters	Permitted Values	Default		
Phone User Interface:				
Menu->Advanced (default password: a	dmin)->Network->WAN			
Port->IPv4->DHCP->Static DNS	Γ			
network.primary_dns	IPv4 Address	Blank		
Description:				
Configures the primary IPv4 DNS server.				
Example:				
network.primary_dns = 202.101.103.55				
Note: It works only if the value of the par	ameter "network.static_	_dns_enable" is set		
to 1 (On). If you change this parameter,	the IP phone will reboot	to make the		
change take effect.				
Web User Interface:				
Network->Basic->IPv4 Config->Static IP A	Address->Primary DNS			
Phone User Interface:				
Menu->Advanced (default password: admin) ->Network->WAN				
Port->IPv4->DHCP->Static DNS (Enabled)	)->Primary DNS			
network.secondary_dns IPv4 Address Blank				
Description:				
Configures the secondary IPv4 DNS serve	er.			
Example:				
network.secondary_dns = 202.101.103.54	4			
<b>Note</b> : It works only if the value of the parameter "network.static_dns_enable" is set to 1 (On). If you change this parameter, the IP phone will reboot to make the change take effect.				
Web User Interface:				
Network->Basic->IPv4 Config->Static IP Address->Secondary DNS				
Phone User Interface:				
Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4->DHCP->Static DNS (Enabled)->Secondary DNS				

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

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

Voglink						Log Out
	Status	ccount Network	Features	Settings	Directory	Security
Basic	Internet Po	rt				NOTE
PC Port	IPv4 Config	Mode(IPv4/IPv6)	IPv4	• 🕜		DHCP The network configurations will
Advanced	C	DHCP 2 Static IP Address 2 IP Address Subnet Mask Gateway Static DNS Primary DNS	<ul> <li>On Off</li> <li>202.201.101.55</li> </ul>			be acquired from DHCP server. Static IP Address Specify the IP address, Subnet Mask, Default Gateway, Primary DNS, Secondary DNS fields manually. PPPOE Contact your ISP if it should be used. Quo can click here to get
	C	Secondary DNS PPPoE ? User Name Password	202.201.101.54			more guides.

5. Click Confirm to accept the change.

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

6. Click OK to reboot the IP phone.

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

- Press Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4->DHCP.
- **2.** Press  $(\cdot)$  or  $(\cdot)$ , or the **Switch** soft key to select **Enabled** from the **Static DNS** field.
- 3. Enter the desired values in the Primary DNS and Secondary DNS fields respectively.
- 4. Press the Save soft key to accept the change.

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

# **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 IP phone with the network. IP phones broadcast DISCOVER messages to request the network information carried in DHCP options, and the DHCP server responds with specific values in corresponding options.

The following table lists common DHCP options supported by IP phones.

Parameter	DHCP Option	Description
Subnet Mask	1	Specify the client's subnet mask.

Parameter	DHCP Option	Description
Time Offset	2	Specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).
Router	3	Specify a list of IP addresses for routers on the client's subnet.
Time Server	4	Specify a list of time servers available to the client.
Domain Name Server	6	Specify a list of domain name servers available to the client.
Log Server	7	Specify a list of MIT-LCS UDP servers available to the client.
Host Name	12	Specify the name of the client.
Domain Server	15	Specify the domain name that client should use when resolving hostnames via DNS.
Broadcast Address	28	Specify the broadcast address in use on the client's subnet.
Network Time Protocol Servers	42	Specify a list of NTP servers available to the client by IP address.
Vendor-Specific	43 (vendor class ID: CPE-OCPHONE)	Specify virtual local area network (VLAN) ID.
Information	43 (vendor class ID: MS-UC-Client)	Specify Skype for Business Server pool certificate provisioning service URL.
Vendor Class Identifier	60	Identify the vendor type.
TFTP Server Name	66	Identify a TFTP server when the 'sname' field in the DHCP header has been used for DHCP options.
Boot file Name	67	Identify a boot file when the 'file' field in the DHCP header has been used for DHCP options.
Skype for Business Server	120	Specify a list of Skype for Business Servers available to the client.

For more information on DHCP options, refer to

http://www.ietf.org/rfc/rfc2131.txt?number=2131 or

http://www.ietf.org/rfc/rfc2132.txt?number=2132.

If you do not have the ability to configure the DHCP options for discovering the provisioning server on the DHCP server, an alternate method of automatically discovering the provisioning server address is required. Connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address is one possibility. For more information, refer to http://www.ietf.org/rfc/rfc3925.txt?number=3925.

The following shows the common options when deploying Yealink IP phones with Skype for Business Server. For more information, refer to https://technet.microsoft.com/en-us/library/gg398088%28v=ocs.14%29.aspx.

## DHCP Option 66 and Option 43

Yealink IP phones support obtaining the provisioning server address by detecting DHCP options during startup.

The phone will automatically detect the option 66 for obtaining the provisioning server address. DHCP option 66 is used to identify the TFTP server.

DHCP option 43 is a vendor-specific option, which is used to transfer the vendor-specific information. The administrator can use vendor class identifier, specified by DHCP option 60, to send the IP phone a customized configuration in option 43. Depending on the vendor class ID it is configured for, the option 43 might have different values. Two vendor class identifiers are used when deploying with the Skype for Business Server: a VLAN ID request (vendor class ID: CPE-OCPHONE) and a certificate provisioning service URL request (vendor class ID: MS-UC-Client). For more information on DHCP option 60, refer to DHCP Option 60 on page 48.

To use DHCP option 66 and option 43, make sure the DHCP Active feature is enabled.

### Procedure

DHCP active can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure DHCP active. <b>Parameters:</b> auto_provision.dhcp_option.enabl e
Local	Web User Interface	Configure DHCP active. <b>Navigate to:</b> http:// <phonelpaddress>/servlet?p =settings-autop&amp;q=load</phonelpaddress>

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default					
auto_provision.dhcp_option.enable	0 or 1	1					
Description:							
Triggers the DHCP Option feature to on a	or off.						
0-Off							
1-On							
If it is set to 1 (On), the IP phone will obto detecting DHCP options.	If it is set to 1 (On), the IP phone will obtain the provisioning server address by detecting DHCP options.						
Web User Interface:							
Settings->Auto Provision->DHCP Active	Settings->Auto Provision->DHCP Active						
Phone User Interface:							
None							

### To configure the DHCP active feature via web user interface:

- 1. Click on Settings->Auto Provision.
- 2. Mark the **On** radio box in the **DHCP Active** field.

				Log Out
Yealink   1466	Etatus Assaurt Naturale	Settings	Directory	Cogniti
	Status Account Network	reatures	Directory	Security
Preference	Auto Provision			NOTE
Time@Date	PNP Active	🖲 On 🗇 Off 🅜		Auto Provision
Timeocoace	DHCP Active	🖲 On 🔘 Off 🕜		The auto provision parameters
Upgrade	Custom Option(128~254)	0		for administrator.
Auto Provision	DHCP Option Value	MS-UC-Client		You can click here to get more quides.
Configuration	Server URL		0	inere galacor
Dist Dise	User Name		0	
Diai Pian	Password	•••••	0	
Voice	Common AES Key	•••••• 🕜		
Tones	MAC-Oriented AES Key	•••••• 🕜		
Phone Lock	Zero Active	Enabled 🔹 🕜		
Thome Lock	Wait Time(0~100s)	5		
Location	Power On	🖲 On 🔘 Off 🕜		
EXP Module	Repeatedly	🔍 On 🖲 Off 🕜		
ВТоЕ	Interval(Minutes)	1440		
	Weekly	🛇 On 🖲 Off 🕜		
	Time	00 : 00 - 00 : 00 🕜		
		✓ Sunday ✓ Monday		
	Deve of March	Tuesday		
	Day of Week	🖭 wednesday 🛛 🕜		
		🗹 Friday		
		Saturday		
		Autoprovision Now		

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

# **DHCP Option 60**

DHCP option 60 is used to identify the vendor class ID. By default, the vendor class ID is MS-UC-Client (case-sensitive).

## Procedure

DHCP option 60 can be configured using the configuration files or locally.

		Configure DHCP option 60.
Configuration File	<v000000000xx> cfa</v000000000xx>	Parameters:
		auto_provision.dhcp_option.opti on60_value
Local		Configure DHCP option 60.
	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		?p=settings-autop&q=load

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default				
auto_provision.dhcp_option.option60_value	String within 99 characters	MS-UC-Client				
Description:						
Configures the value (vendor class ID) of DHC	P option 60.					
Web User Interface:						
Settings->Auto Provision->DHCP Option Value						
Phone User Interface:						
None						

To configure DHCP option 60 on the IP phone via web user interface:

1. Click on Settings->Auto Provision.

2. Enter the desired host name in the DHCP Option Value filed.

Voglink							Log Out
	Status	Account	Network	Features	Settings	Directory	Security
Preference		Auto Provision					NOTE
Time&Date		PNP Active DHCP Active		● On © Off ● On © Off	0		Auto Provision The auto provision parameters
Upgrade		Custom Option(128-	-254)		0		for administrator.
Auto Provision		DHCP Option Value		MS-UC-Client	0		You can click here to get more guides.
Configuration		Server URL				0	
Dial Plan		User Name Password		•••••		0	
Voice		Common AES Key		•••••	0		
Tones		MAC-Oriented AES K	ey	•••••	0		
Phone Lock		Zero Active		Enabled	• 🕜		
Lock		Wait Time(0~100s)		5	0		
Location		Power On		🖲 On 🔘 Off	0		
EXP Module		Repeatedly		🔘 On 🖲 Off	0		
ВТОЕ		Interval(Minutes)		1440	0		
		Weekly		🔘 On 🖲 Off	0		
		Time		00 : 00 - 0	0 : 00		
		Day of Week		<ul> <li>✓ Sunday</li> <li>✓ Monday</li> <li>✓ Tuesday</li> <li>✓ Tuesday</li> <li>✓ Wednesday</li> <li>✓ Thursday</li> <li>✓ Friday</li> <li>✓ Saturday</li> </ul>	0		

3. Click Confirm to accept the change.

## DHCP Option 42 and Option 2

Yealink IP phones support using the NTP server address offered by DHCP.

DHCP option 42 is used to specify a list of NTP servers available to the client by IP address. NTP servers should be listed in order of preference. DHCP option 2 is used to specify the offset of the client's subnet in seconds from Coordinated Universal Time (UTC).

To update time with the offset time offered by the DHCP server, make sure the DHCP Time feature is enabled at the path **Settings->Time & Date->DHCP Time**. For more information on how to configure DHCP time feature, refer to NTP Time Server on page 105.

## DHCP Option 12 Hostname on the IP Phone

This option specifies the host name of the client. The name may or may not be qualified with the local domain name (based on RFC 2132). See RFC 1035 for character restrictions.

## Procedure

DHCP option 12 hostname can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Configure the DHCP option 12 hostname. <b>Parameters:</b> network.dhcp_host_name
Local	Web User Interface	Configure the DHCP option 12 hostname. Navigate to: http:// <phonelpaddress>/servlet 2p=features-general&amp;g=load</phonelpaddress>

# Details of Configuration Parameters:

Parameters	Permitted Values	Default				
network.dhcp_host_name	rk.dhcp_host_name String within 99 characters					
Description:						
Configures the DHCP option 12 hostnam	ne on the IP phone.					
For SIP-T48G IP phones:						
The default value is SIP-T48G.						
For SIP-T46G IP phones:						
The default value is SIP-T46G.						
For SIP-T42G IP phones:						
The default value is SIP-T42G.						
For SIP-T41P IP phones:						
The default value is SIP-T41P.						
For SIP-T40P IP phones:						
The default value is SIP-T40P						
<b>Note:</b> If you change this parameter, the take effect.	IP phone will reboot to r	make the change				
Web User Interface:						
Features->General Information->DHCP H	Features->General Information->DHCP Hostname					
Phone User Interface:						
None						

To configure DHCP option 12 hostname on the IP phone via web user interface:

- 1. Click on Features-> General Information.
- 2. Enter the desired host name in the DHCP Hostname filed.

				_			Log Out
YEAIINK   T46G	Status Acco	unt Network	Features	Settings	Directory	Security	
General Information Audio Remote Control Bluetooth	General Inf Call Waltin Key As Se Busy Tono Return Co Time-Out	ormation ? Ig Ind Ind Delay (Seconds) de when refuse for Dial-Now Rule	Enabled # 0 603 (Decline) 1	· 0 · 0 · 0 · 0 · 0		Call Waiting           This call feature a phone to accept calls during the constraint of	llows your other incoming onversation. the send key.
Power LED	Dial Searci 180 Ring	h Delay Workaround	1 Disabled -	• 0		You can click more guides.	here to get
	DHCP Hos	tname	SIP-T46G	0			
	E911 Loca	ation Tip	Enabled	• 🕜			
	Update C	necking Time	24	0			
	Use DHCP	Option 120	Disabled	• 0			
	SFB Cert :	Service URL	https://xmpool.yealin	kuc.cor 🕜			
	Enable SF	B Automation	Disabled	• 🕜			
	SFB Inact	ive Time	5	0			
	SFB Away	Time	5	0			
	Device Pa	iring for Online	Enabled	• 0			

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 IP phone.

# **DHCP Option 120**

Yealink IP phones support obtaining Skype for Business Server address from DHCP. DHCP option 120 is used to specify a list of Skype for Business Servers available to the client.

### Procedure

DHCP option 120 can be configured using the configuration files or locally.

		Configure DHCP option 120.		
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:		
		sip.option120_get_lync_server.enable		
Local		Configure DHCP option 120.		
	Wab Usar Interface	Navigate to:		
		http:// <phonelpaddress>/servlet?p=f eatures-general&amp;q=load</phonelpaddress>		

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default					
sip.option120_get_lync_server.enable	0 or 1	0					
Description:							
Enables or disables the IP phones to obt	ain the Skype for Busines	ss Server address					
from DHCP by detecting DHCP option 1	20.						
0-Disabled							
1-Enabled							
Web User Interface:							
Features->General Information->Use DH	Features->General Information->Use DHCP Option 120						
Phone User Interface:							
None							

To configure DHCP option 120 on the IP phone via web user interface:

- 1. Click on Features-> General Information.
- 2. Select desired value from the pull-down list of Use DHCP Option 120.

Vaglink					-			Log Out
	Status Account	Network	Features	Settin	gs	Directory	Security	
General	General Informatio	on 🕜					NOTE	<b></b>
Audio	Call Waiting Key As Send		Enabled #	•	0		Call Waiting This call feature allows	s your
Pemote Control	Busy Tone Delay (	Seconds)	0	•	0		phone to accept othe calls during the conve	er incoming rsation.
Remote control	Return code when	n refuse	603 (Decline)	•	0		Key As Send	
Bluetooth	Time-Out for Dial-I	Now Rule	1		0		Select * or # as the s	end key.
Power LED	Dial Search Delay		1		0		You can click here	e to get
	180 Ring Workaro	und	Disabled	•	0		more guides.	
			:					
			12072102					
	DHCP Hostname		SIP-T46G		0			
	E911 Location Tip		Enabled	-	0			
	Update Checking	120	24	_	0			
	SER Cart Saprica I	120	Enabled	•	0			
	Enable SEB Autom	ation	Disabled	inkuc.cor	0			
	SEB Inactive Time	acion	5		6			
	SEB Away Time		5	() 	6			
	Device Pairing for	Online	Enabled	•	0			
	Confin	m	(	Cancel				

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

# **Configuring Network Parameters Manually**

If DHCP is disabled or IP phones cannot obtain network parameters from the DHCP server, you need to configure them manually. The following parameters should be configured for IP phones to establish network connectivity:

- IP Address
- Subnet Mask
- Default Gateway
- Primary DNS
- Secondary DNS

### Procedure

Network parameters can be configured manually using the configuration files or locally.

		Configure network parameters of the IP phone manually.	
	<mac>.cfg</mac>	Parameters:	
		network.internet_port.type	
Configuration File		network.ip_address_mode	
Configuration File		network.internet_port.ip	
		network.internet_port.mask	
		network.internet_port.gateway	
		network.primary_dns	
		network.secondary_dns	
		Configure network parameters of	
Local	Web User Interface	Naviaate to:	
		http:// <phonelpaddress>/servlet</phonelpaddress>	
		?p=network&q=load	
	Phone User Interface	Configure network parameters of the IP phone manually.	

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
network.internet_port.type	0, 1 or 2	0
Description:		
Configures the Internet (WAN) port type for IPv4.		

Parameters	Permitted Values	Default	
0-DHCP			
1-PPPoE (not applicable to SIP-T42G/T41P/T40P IP phor	ies)		
2-Static IP Address			
<b>Note</b> : It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			
Network->Basic->IPv4 Config			
Phone User Interface:			
Menu->Advanced (default password: admin)->Netwo	rk->WAN Port->IPv4		
network.ip_address_mode	0, 1 or 2	0	
Description:			
Configures the IP address mode.			
<b>0</b> -IPv4			
<b>1</b> -IPv6			
<b>2</b> -IPv4 & IPv6			
<b>Note:</b> If you change this parameter, the IP phone will retake effect.	eboot to make the a	change	
Web User Interface:			
Network->Basic->Internet Port->Mode(IPv4/IPv6)			
Phone User Interface:			
Menu->Advanced (default password: admin) ->Netwo	ork->WAN Port->IP M	ode	
network.internet_port.ip	IPv4 Address	Blank	
Description:			
Configures the IPv4 address.			
Example:			
network.internet_port.ip = 192.168.1.20			
<b>Note</b> : It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			
Network->Basic->IPv4 Config->Static IP Address->IP Address			
Phone User Interface:			

Parameters	Permitted Values	Default	
Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4->Static IP ->IP Address			
network.internet_port.mask	Subnet Mask	Blank	
Description:			
Configures the IPv4 subnet mask.			
Example:			
network.internet_port.mask = 255.255.255.0			
<b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			
Network->Basic->IPv4 Config->Static IP Address->Subn	et Mask		
Phone User Interface:			
Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4->Static IP->Subnet Mask			
network.internet_port.gateway IPv4 Address Blank			
Description:			
Configures the IPv4 default gateway.			
Example:			
network.internet_port.gateway = 192.168.1.254			
<b>Note</b> : It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			
Network->Basic->IPv4 Config->Static IP Address->Gateway			
Phone User Interface:			
Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4->Static IP->Gateway			
network.primary_dns	IPv4 Address	Blank	

Parameters	Permitted Values	Default
Description:		
Configures the primary IPv4 DNS server.		
Example:		
network.primary_dns = 202.101.103.55		
<b>Note</b> : It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the IP phone will reboot to make the change take effect.		
Web User Interface:		
Network->Basic->IPv4 Config->Static IP Address->Prime	iry DNS	
Phone User Interface:		
Menu->Advanced (default password: admin) ->Netwo IP->Primary DNS	ork->WAN Port->IPv4	->Static
network.secondary_dns IPv4 Address Blant		Blank
Description:		
Configures the secondary IPv4 DNS server.		
Example:		
network.secondary_dns = 202.101.103.54		
<b>Note</b> : It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "network.internet_port.type" is set to 2 (Static IP Address). If you change this parameter, the IP phone will reboot to make the change take effect.		
Web User Interface:		
Network->Basic->IPv4 Config->Static IP Address->Secondary DNS		
Phone User Interface:		
Menu->Advanced (default password: admin) ->Netwo IP->Secondary DNS	ork->WAN Port->IP∨4	->Static

## To configure the IP address mode via web user interface:

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

2. Select desired value from the pull-down list of Mode(IPv4/IPv6).

Yealink 1466	Status Account Network Features Settings Directory	Log Out Security
Basic	Internet Port	NOTE
PC Port Advanced	Mode(IPV4/IPv6) IPV4 ♥ ♥ IPv4 Config ● DHCP ♥	DHCP The network configurations will be acquired from DHCP server.
	Static IP Address     IP Address	Static IP Address Specify the IP address, Subnet Mask, Default Gateway, Primary DNS, Secondary DNS fields manually.
	Subnet Mask Gateway	PPPoE Contact your ISP if it should be used.
	Static DNS On Off Primary DNS	You can click here to get more guides.
	Secondary DNS	-

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 IP phone.

To configure a static IPv4 address via web user interface:

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

Yealink 1466		Log Out
	Status Account Network Features Settings Directory	Security
Pacie	Internet Port	NOTE
PC Port	Mode(IPv4/IPv6) IPv4 V ?	DHCP The network configurations will
Advanced		Static IP Address Specify the IP address, Subnet
	IP Address 192.168.1.10	Mask, Default Gateway, Primary DNS, Secondary DNS fields manually.
	Subnet Mask         255.255.255.0           Gateway         192.168.1.254	PPPoE Contact your ISP if it should be used
	Static DNS   On Off	Vou can click here to get
	Primary DNS 202.101.103.55	more guides.
	Secondary DNS 202.101.103.54 ×	

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

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

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

#### To configure the IP mode via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Network->WAN Port.
- Press (•) or (•), or the Switch soft key to select IPv4, IPv6 or IPv4 & IPv6 from the IP Mode field.
- 3. Press the Save soft key to accept the change.

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

### To configure a static IPv4 address via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Network->WAN Port->IPv4.
- 2. Press  $(\cdot)$  or  $(\cdot)$ , or the Switch soft key to select the Static IP from the Type field.
- Enter the desired value in the IP Address, Subnet Mask, Gateway, Primary DNS and Secondary DNS field respectively.
- 4. Press the Save soft key to accept the change.

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

# **PPPoE**

PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol used by Internet Service Providers (ISPs) to provide Digital Subscriber Line (DSL) high speed Internet services. PPPoE allows an office or building-full of users to share a common DSL connection to the Internet. PPPoE connection is supported by the IP phone Internet port. Contact your ISP for the PPPoE user name and password. PPPoE is not applicable to SIP-T42G/T41P/T40P IP phones IP phones.

### Procedure

PPPoE can be configured using the configuration files or locally.

		-
	<mac>.cfg</mac>	Configure PPPoE on the IP phone.
		Parameters:
		network.internet_port.type
Configuration File		Configure the user name and password for PPPoE on the IP phone.
	<y000000000xx>.cfg</y000000000xx>	Parameters:
		network.pppoe.user
		network.pppoe.password
	Web User Interface	Configure PPPoE on the IP
Local		phone.
		Configure the user name and
		password for PPPoE on the IP
		Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>

	?p=network&q=load
Phone User Interface	Configure PPPoE on the IP phone. Configure the user name and password for PPPoE on the IP phone.

# Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.internet_port.type	0, 1 or 2	0
Description:		
Configures the Internet (WAN) port type for IPv4.		
0-DHCP		
1-PPPoE (not applicable to SIP-T42G/T41P/T40P IP phor	nes)	
2-Static IP Address		
<b>Note</b> : It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). If you change this parameter, the IP phone will reboot to make the change take effect.		
Web User Interface:		
Network->Basic->IPv4 Config		
Phone User Interface:		
Menu->Advanced (default password: admin)->Netwo	rk->WAN Port->IPv4	
network.pppoe.user	String within 32 characters	Blank
Description:		
Configures the user name for PPPoE connection.		
Example:		
network.pppoe.user = Xmyl0592123		
<b>Note</b> : It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "network.internet_port.type" is set to 1 (PPPoE). If you change this parameter, the IP phone will reboot to make the change take effect. It is not applicable to SIP-T42G/T41P/T40P IP phones IP phones.		
Web User Interface:		
Network->Basic->IPv4 Config->PPPoE->User Name		
Phone User Interface:		

Parameters	Permitted Values	Default
Menu->Advanced (default password: admin) ->Netwo Port->IPv4->PPPoE->PPPoE User	ork->WAN	
network.pppoe.password	String within 99 characters	Blank
Description:		
Configures the password for PPPoE connection.		
Example:		
network.pppoe.password = yealink123		
<b>Note</b> : It works only if the value of the parameter "network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "network.internet_port.type" is set to 1 (PPPoE). If you change this parameter, the IP phone will reboot to make the change take effect. It is not applicable to SIP-T42G/T41P/T40P IP phones.		
Web User Interface:		
Network->Basic->IPv4 Config->PPPoE->Password		
Phone User Interface:		
Menu->Advanced (default password: admin) ->Netwo Port->IPv4->PPPoE->PPPoE Password	ork->WAN	

### To configure PPPoE via web user interface:

- 1. Click on **Network**->**Basic**.
- 2. In the IPv4 Config block, mark the PPPoE radio box.
- 3. Enter the user name and password in corresponding fields.

		Log Out
Yealink 1466	Cature Assured Network Castures Catting Directory	Conveiter
	Status Account Activity Features Settings Directory	Security
Partie	Internet Port	NOTE
DdSIC	Mode(IPv4/IPv6) IPv4 V	DUICD
PC Port	IPv4 Config	The network configurations will be acquired from DHCP server.
Advanced		Static IP Address
	O Static IP Address 🕜	Specify the IP address, Subnet Mask, Default Gateway, Primary
	IP Address	DNS, Secondary DNS fields manually.
	Subnet Mask	PPPoE
	Gateway	Contact your ISP if it should be used.
	Static DNS On Off	Nou can click here to get
	Primary DNS	more guides.
	Secondary DNS	
	• PPPoE 🕜	
	User Name Xmyl0592123 ×	
	Password	
	IPv6 Config	
	DHCP     O	
	Static IP Address	
	IP Address	

4. Click Confirm to accept the change.

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

5. Click OK to reboot the IP phone.

### To configure PPPoE via phone user interface:

- 1. Press Menu->Advanced (default password: admin)->Network->WAN Port->IPv4.
- **2.** Press  $(\cdot)$  or  $(\cdot)$ , or the **Switch** soft key to select the **PPPoE** from the **Type** field.
- 3. Enter the user name and password in the corresponding fields.
- 4. Press the Save soft key to accept the change.

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

# Configuring Transmission Methods of the Internet Port and PC Port

Yealink SIP-T48G/T46G/T42G/T41P/T40P IP phones support two Ethernet ports: Internet port and PC port. Three optional methods of transmission configuration for IP phone Internet or PC Ethernet ports:

- Auto-negotiate
- Half-duplex
- Full-duplex

Auto-negotiate is configured for both Internet and PC ports on the IP phone by default.

### Auto-negotiate

Auto-negotiate means that two connected devices choose common transmission parameters (e.g., speed and duplex mode) 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. You can configure the Internet port and PC port on the IP phone to automatically negotiate during the transmission.

## Half-duplex

Half-duplex transmission refers to transmitting voice or data in both directions, but in one direction at a time; this means one device can send data on the line, but not receive data simultaneously. You can configure the half-duplex transmission on both Internet port and PC port for the IP phone to transmit in 10Mbps or 100Mbps.



## **Full-duplex**

Full-duplex transmission refers to transmitting voice or data in both directions at the same time; this means one device can send data on the line while receiving data. You can configure the full-duplex transmission on both Internet port and PC port for the IP phone to transmit in 10Mbps, 100Mbps or 1000Mbps (1000Mbps is only applicable to SIP-T48G/T46G/T42G IP phones).



## Procedure

The transmission methods of Ethernet ports can be configured using the configuration files or locally.

Configuration File	0,00000000000 of a	Configure the transmission methods of the Internet (WAN) port.
	<y0000000000xx>.ctg</y0000000000xx>	Parameters:
		network.internet_port.speed_duplex

		network.pc_port.speed_duplex
local	Web User Interface	Configure the transmission methods of the Internet (WAN) port.
Local	web user interface	http:// <phonelpaddress>/servlet?p= network-adv&amp;q=load</phonelpaddress>

# Details of Configuration Parameters:

Parameters	Permitted Values	Default			
network.internet_port.speed_duplex	0, 1, 2, 3, 4 or 5	0			
Description:					
Configures the transmission method of the Internet (W	Configures the transmission method of the Internet (WAN) port.				
<b>0</b> -Auto Negotiate					
1-Full Duplex 10Mbps					
<b>2</b> -Full Duplex 100Mbps					
<b>3</b> -Half Duplex 10Mbps					
<b>4</b> -Half Duplex 100Mbps					
5-Full Duplex 1000Mbps (only applicable to SIP-T48G/T4	46G/T42G IP phones	)			
Web User Interface:					
Network->Advanced->Port Link->WAN Port Link					
Phone User Interface:					
None					
network.pc_port.speed_duplex	0, 1, 2, 3 ,4 or 5	0			
Description:					
Configures the transmission method of the PC (LAN) pa	ort.				
<b>0</b> -Auto Negotiate					
1-Full Duplex 10Mbps					
2-Full Duplex 100Mbps					
3-Half Duplex 10Mbps					
4-Half Duplex 100Mbps					
5-Full Duplex 1000Mbps (only applicable to SIP-T48G/T46G/T42G IP phones)					
Web User Interface:					
Network->Advanced->Port Link->PC Port Link					
Phone User Interface:					

Parameters	Permitted Values	Default
None		

To configure the transmission methods of Ethernet ports via web user interface:

- 1. Click on Network->Advanced.
- 2. Select the desired value from the pull-down list of WAN Port Link.
- 3. Select the desired value from the pull-down list of PC Port Link.

				Log Out
YEAIINK   T46G	Status Account	Network Fea	atures Settings Directo	ory Security
Basic	LLDP 🕜			NOTE
DC Bort		Active	Enabled	VLAN
PC POIL		Packet Interval (1~3600s)	60	A VLAN is a logical local area network (or LAN) that extends
Advanced	СБР 🅜	Active	Enabled V	to a group of LAN segments, given specific configurations.
		Packet Interval (1~3600s)	60	QoS
	VLAN 🕜		,	When the network capacity is insufficient, QoS could provide priority to years by catting the
	WAN Port	Active	Disabled V	value.
		VID (1-4094)	1	Local RTP Port Define the port for voice
		Priority	0 🗸	transmission.
	PC Port	Active	Disabled V	You can click here to get more guides.
		VID (1-4094)	1	
		Priority	0 🗸	
	DHCP VLAN	Active	Enabled V	
		Option (1-255)	132	
	Port Link 🕜			
		WAN Port Link	Auto Negotiate 🗸	
		PC Port Link	Auto Negotiate 🗸 🗸	

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

# **Configuring PC Port Mode**

The PC port on the back of the IP phone is used to connect a PC. You can enable or disable the PC (LAN) port on the IP phones via web user interface or using configuration files.

## Procedure

PC port mode can be configured using the configuration files or locally.

		Configure the PC (LAN) port.
Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Parameter:
		network.pc_port.enable
		Configure the PC (LAN) port.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>

	<pre>?p=network-pcport&amp;q=load</pre>

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default		
network.pc_port.enable	0 or 1	1		
Description:				
Enables or disables the PC (LAN) port.				
0-Disabled				
1-Auto Negotiation				
<b>Note</b> : If you change this parameter, the IP phone will reboot to make the change take effect.				
Web User Interface:				
Network->PC Port->PC Port Active				
Phone User Interface:				
None				

To enable the PC port via web user interface:

- 1. Click on **Network->PC Port**.
- 2. Select Auto Negotiate from the pull-down list of PC Port Active.

Yealink							Log Out
	Status	Account	Network	Features	Settings	Directory	Security
Basic	PC Por	t Active					NOTE
PC Port Advanced		PC Port	Active	Auto Negotiation	<ul> <li>Cancel</li> </ul>		PC Port The PC prot parameters for administrator.

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 IP phone.

### To disable the PC port via web user interface:

1. Click on Network->PC Port.

2. Select **Disabled** from the pull-down list of **PC Port Active**.

Yealink   1466	Status Account Network	Features Settings Directory	Log Out
Basic	PC Port Active		NOTE
PC Port	PC Port Active	Disabled 🔹 🕜	PC Port
Advanced	Confirm	Cancel	administrator.

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 IP phone.

# **Branch Office Resiliency**

Branch office resiliency is critical for multi-site deployments of Skype for Business where the control servers are located at a central site or data center. It allows branch site users to continue to have Enterprise Voice service and voice mail (if voice mail rerouting settings are configured) when the branch site loses the connection to the central site.

When the WAN connection between the branch site and central site is unavailable, the phone goes into resiliency mode:

- Branch site user on the phone stays signed in with an indication of "Limited service due to outage".
- Presence icon on the phone LCD screen is displayed as Unknown icon:
   (SIP-T46G/T48G)/
   (SIP-T42G/T41P/T40P).
- Call between branch site users is established successfully with 2-way audio.
- Conference between branch site users can be established successfully.
- The call history cannot get modified. (Already downloaded call log entries will not be deleted)
- Calls can be placed from the call history on the IP phone.
- Contact list is unavailable but you can search for a contact on the IP phone.
- User is not able to change his presence state manually.
- User is not able to use calendar feature.
- User is not able to receive the voice mail as exchange is unreachable and when IP phone comes out of resiliency mode, it downloads the yet undownloaded voice mail items and updates the voice mail screen.
- Calls between the branch office phones can be transferred to another branch site user.
- Call forward settings cannot be changed.

When the WAN connection between the branch site and central site becomes available, the phone comes out of resiliency mode automatically. Notification of resiliency is automatically dismissed, and you can use phone features as normal.

Note For more information on branch office resiliency, contact your system administrator.

# **Upgrading Firmware**

Yealink supports three methods to upgrade phone firmware:

- Upgrade firmware via web user interface: Download firmware in ROM format, and upload it to the IP phone via web user interface. This method can deploy small number of phones.
- Upgrade firmware from provisioning server: Download firmware in ROM format, and use centralized provisioning method to upgrade the firmware. This method requires setting up a provisioning server, and uses configuration files to provision the IP phone.
- Upgrade firmware from Skype for Business Server: Download firmware in CAB file format, and place the firmware on Skype for Business Server to provision the IP phone.

The following table lists the associated and latest firmware name for each IP phone model (X is replaced by the actual firmware version).

IP Phone Model	Associated Firmware Name	Firmware Name(.rom)	Firmware Name(.cab)
SIP-T48G	35.x.x.rom	35.8.0.21.rom	Yealink_ver_35.8.0.21.cab
SIP-T46G	28.x.x.rom	28.8.0.21.rom	Yealink_ver_28.8.0.21.cab
SIP-T42G/ T41P	29.x.x.rom	29.8.0.21.rom	Yealink_ver_29.8.0.21.cab
SIP-T40P	54.x.x.rom	54.8.0.21.rom	Yealink_ver_54.8.0.21.cab

Note

You can download the latest firmware online:

http://www.yealink.com/solution\_info.aspx?ProductsCateID=1248&cateid=1248&BaseIn foCateId=1328&Cate\_Id=1248&parentcateid=1328.

Do not unplug the network and power cables when the IP phone is upgrading firmware.

## Upgrading Firmware via Web User Interface

To manually upgrade firmware via web user interface, you need to store firmware to your local system in advance.

### To upgrade firmware manually via web user interface:

- 1. Click on Settings->Upgrade.
- 2. Click Browse to locate the required firmware from your local system.
- 3. Click Upgrade.

A dialog box pops up to prompt "Firmware of the SIP Phone will be updated. It will take 5 minutes to complete. Please don't power off!".

Vaglink			Log Out
	Status Account Network	Features Settings Directory	Security
Preference			NOTE
Time&Date	Version ? Firmware Version	28.8.254.131	Reset to Factory Setting Reset all the settings of the
Upgrade	Hardware Version	28.0.0.128.0.0.0	phone to default configurations.
Auto Provision	Reset to Factory Setting	Reset to Factory Setting	Select and Upgrade Firmware Select and upgrade the file from the bard dick or patwork
Configuration	Reboot	Reboot	the hard disk of network.
Dial Plan	Select and Upgrade Firmware 🛛 🥎	Browse No file selected.	You can click here to get more guides.
Voice			

4. Click **OK** to confirm the upgrade.

Do not close and refresh the browser when the IP phone is upgrading firmware via web user interface.

# Upgrading Firmware from the Provisioning Server

IP phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files and firmware from the provisioning server, and then upgrade firmware automatically.

IP phones can download firmware stored on the provisioning server in one of two ways:

- Check for configuration files and then download firmware during startup.
- Automatically check for configuration files and then download firmware at a fixed interval or specific time.

Method of checking for configuration files is configurable.

### Procedure

Configuration changes can be performed using the configuration files or locally.

		Configure the way for the IP phone to check for configuration files.
Configuration	<y000000000xx>.cfg</y000000000xx>	Parameters:
riie		auto_provision.power_on
		auto_provision.repeat.enable

Note

		auto_provision.repeat.minutes
		auto_provision.weekly.enable
		auto_provision.weekly.begin_time
		auto_provision.weekly.end_time
		auto_provision.weekly.dayofweek
		Specify the access URL of firmware.
		Parameter:
		firmware.url
		Configure the way for the IP phone to check for configuration files.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet?p=s</phonelpaddress>
		ettings-autop&q=load

# Details of Configuration Parameters:

Parameters	Permitted Values	Default	
auto_provision.power_on	0 or 1	1	
Description:			
Triggers the power on feature to on or c	ff.		
0-Off			
1-On			
If it is set to 1 (On), the IP phone will perform an auto provisioning process when powered on.			
Web User Interface:			
Settings->Auto Provision->Power On			
Phone User Interface:			
None			
auto_provision.repeat.enable	0 or 1	0	
Description:			
Triggers the repeatedly feature to on or off.			
0-Off			
1-On			
If it is set to 1 (On), the IP phone will perf repeatedly.	form an auto provisioning process		

Parameters	Permitted Values	Default	
Web User Interface:			
Settings->Auto Provision->Repeatedly			
Phone User Interface:			
None			
auto_provision.repeat.minutes	Integer from 1 to 43200	1440	
Description:			
Configures the interval (in minutes) for the IP phone to perform an auto provisioning process repeatedly.			
<b>Note</b> : It works only if the value of the paset to 1 (On).	rameter "auto_provision.repeat.er	nable" is	
Web User Interface:			
Settings->Auto Provision->Interval (Minut	es)		
Phone User Interface:			
None			
auto_provision.weekly.enable	0 or 1	0	
Description:			
Triggers the weekly feature to on or off.			
<b>0</b> -Off			
<b>1</b> -On			
If it is set to 1 (On), the IP phone will perform an auto provisioning process weekly.			
Web User Interface:			
Settings->Auto Provision->Weekly			
Phone User Interface:			
None	r		
auto_provision.weekly.begin_time	Time from 00:00 to 23:59	00:00	

Parameters	Permitted Values	Default		
Description:				
Configures the begin time of the day for the IP phone to perform an auto provisioning process weekly.				
<b>Note</b> : It works only if the value of the parameter "auto_provision.weekly.enable" is set to 1 (On).				
Web User Interface:				
Settings->Auto Provision->Time				
Phone User Interface:				
None				
auto_provision.weekly.end_time	Time from 00:00 to 23:59	00:00		
Description:				
Configures the end time of the day for the IP phone to perform an auto provisioning process weekly.				
<b>Note</b> : It works only if the value of the parameter "auto_provision.weekly.enable" is set to 1 (On).				
Web User Interface:				
Settings->Auto Provision->Time				
Phone User Interface:				
None				
auto_provision.weekly.dayofweek	0, 1, 2, 3, 4, 5, 6 or a combination of these digits	0123456		
Description:				
Configures the days of the week for the IP phone to perform an auto provisioning process weekly.				
<b>0</b> -Sunday				
1-Monday				
<b>2</b> -Tuesday				
3-Wednesday				
<b>4</b> -Thursday				
<b>5</b> -Friday				
<b>6</b> -Saturday				
Example:				
auto_provision.weekly.dayofweek = 01				
It means the IP phone will perform an a	uto provisioning process every Sund	day and		

Parameters	Permitted Values	Default		
Monday.				
Note: It works only if the value of the parameter "auto_provision.weekly.enable" is				
set to 1 (On).				
Web User Interface:				
Settings->Auto Provision->Day of Week				
Phone User Interface:				
None				
firmware.url	URL within 511 characters	Blank		
Description:				
Configures the access URL of the firmware file.				
Example:				
firmware.url = http://192.168.1.20/28.8.0.21.rom				
Note: If you change this parameter, the IP phone will reboot to make the change				
take effect.				
Web User Interface:				
Settings->Upgrade->Select and Upgrade Firmware				
Phone User Interface:				
None				

To configure the way for the IP phone to check for configuration files via web user interface:

1. Click on Settings->Auto Provision.
2. Make the desired change.

				Log Out
Yealink   1466	Status Account Network	Features Settings	Directory	Security
Preference	Auto Provision PNP Active	● On ◎ Off 👩		NOTE
Time&Date	DHCP Active	◎ On ○ Off ?		Auto Provision The auto provision parameters
Upgrade	Custom Option(128~254)	0		for administrator.
Auto Provision	DHCP Option Value	MS-UC-Client		You can click here to get more guides.
Configuration	Server URL		0	
Dial Plan	User Name Password	•••••	0	
Voice	Common AES Key	••••••	· ·	
Tones	MAC-Oriented AES Key	•••••• 0		
Phone Lock	Zero Active	Disabled 🔹 🕜		
Location	Wait Time(0~100s)	5		
LOCATION	Power On	🖲 On 🛇 Off 🕜		
EXP Module	Repeatedly	🛇 On 🖲 Off 🕜		
ВТОЕ	Interval(Minutes)	1440		
	Weekly	🔍 On 🖲 Off 🕜		
	Time Day of Week	00 : 00 - 00 : 00 ? V Sunday V Tuesday V Tuesday V Thursday V Thursday V Thursday V Thursday		
		Autoprovision Now		

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

When the "Power On" is set to **On**, the IP phone will check configuration files stored on the provisioning server during startup and then will download firmware from the server.

## Updating Phone Firmware from Skype for Business Server

You can update firmware of Yealink SIP-T48G, SIP-T46G, SIP-T42G, SIP-T41P and SIP-T40P phones from Skype for Business Server. There are two ways to update firmware from Skype for Business Server:

- Automatic Update
- Manual Update

Before updating firmware from Skype for Business Server, you must upload the update package (\*.CAB) to your Skype for Business Update Server in advance. For more information, refer to Updating Phone Firmware from Microsoft Skype for Business Server.

## Automatic Update

### Reboot

When the IP phone connects to the network and is powered on, it automatically checks if an update is available on Skype for Business Server, regardless of whether a Skype for Business user signs on the IP phone. If there is an update available on Skype for Business Server, the IP phone will automatically update firmware.

### Sign-in

If the IP phone is powered on, and a user signs in, the IP phone automatically checks if an update is available on Skype for Business Server after the designated time.

If there is an update available, and the IP phone is on the idle screen, the IP phone LCD screen pops up a dialog box "New firmware, update now?". You can press the **OK** soft key to update immediately or the **Cancel** soft key to cancel the update.

If there is an update available, but the IP phone is not on the idle screen, the dialog box will pop up after detecting 10 minutes of inactivity on the idle screen.

### Sign-out

If the IP phone is powered on, and no user signs in, the IP phone automatically checks if an update is available on Skype for Business Server after the designated time. If there is an update available, the IP phone will automatically update firmware.

#### Note

The IP phone will not perform an update check when a user signs in/out. It only performs an update check after the designated time. The designated time will be cleared when the IP phone reboots or a user signs in/out.

If there is no update available on Skype for Business Server, the IP phone does not prompt any message after the designated time.

## **Update Checking Time**

Update checking time defines a period of time for IP phone to automatically check a firmware update on Skype for Business Server.

#### Procedure

Update checking time can be configured using the configuration files or locally.

Configuration	<y000000000xx>.cfg</y000000000xx>	Configure update checking time.	
File		Parameters:	
		sfb.update_time	
local	Wab User Interface	Configure update checking time.	
LUCUI	web user intendce	Navigate to:	

http:// <phonelpaddress>/servlet?p=fea</phonelpaddress>
tures-general&q=load

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
sfb.update_time	Integer from 1 to 48	24

#### Description:

Configures the interval (in hours) for the IP phone to automatically check if there is a firmware update available on Skype for Business Server.

If it is set to 1, the IP phone will check if a firmware update is available on the Skype for Business Server every 1 hour. If there is an update available, the IP phone will prompt for an update.

**Note:** If you change this parameter, the IP phone will reboot to make the change take effect.

### Web User Interface:

Features->General Information->Update Checking Time

Phone User Interface:

None

### To configure update checking time via web user interface:

1. Click on Features->General Information.

- Log Out Yealink T46G Status Features Account Settings Directory Security General Information 🕜 NOTE General Information Call Waiting Enabled • 0 **Call Waiting** This call feature allows your phone to accept other incoming calls during the conversation. Audio Key As Send # • 0 • Busy Tone Delay (Seconds) 0 0 Remote Control Return code when refuse 603 (Decline) 2 Key As Send Select \* or # as the send key. Bluetooth Time-Out for Dial-Now Rule 1 0 You can click here to get more guides. Power LED Dial Search Delay 1 0 180 Ring Workaround Disabled -0 DHCP Hostname SIP-T46G 0 E911 Location Tip Enabled 0 Update Checking Time 0 24 Use DHCP Option 120 Enabled • 0 SFB Cert Service URL https://xmpool.yealinkuc.cor Enable SFB Automation Disabled \_ 0 SFB Inactive Time 5 0 SFB Away Time 5 0 Device Pairing for Online - 0 Enabled Confirm Cancel
- 2. Select the desired value from the pull-down list of **Update Checking Time**.

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

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

## **Manual Update**

You can initiate an update immediately, just power off the IP phone and power on it again. The phone will boot up, check for updates and apply the updates. You can also trigger an update manually via phone user interface.

To trigger an update manually via phone user interface:

- 1. Press Menu-> Basic ->Firmware Update.
- 2. Press the Update soft key.

The LCD screen prompts "New firmware, update now?".

Firmware Update			
1. Firmware Update			
	New firmware, update now?		
Cancel		OK	

3. Press the **OK** soft key to confirm the update.

If there is no update available on Skype for Business Server, the LCD screen prompts "The firmware is the latest".

Firmware Update					
1. Firmwa	1. Firmware Update				
	The firmware is the latest				
OK					

# **Configuring Basic Features**

This chapter provides information for making configuration changes for the following basic features:

- Power Indicator LED
- Contrast
- Backlight
- Sign in
- Web Server Type
- Time and Date
- Language
- Dial Plan
- Directory
- Saving Call Log
- Missed Call Log
- Dial Search Delay
- Live Dialpad
- Call Waiting
- Key As Send
- Pre Dial Tone
- Redial Tone
- Ringer Device for Headset
- Auto Answer
- Always On Line
- Busy Tone Delay
- Return Code When Refuse
- Early Media
- 180 Ring Workaround
- Call Hold
- Allow Trans Exist Call
- Call Number Filter
- DTMF

- Allow Mute
- Voice Mail without PIN
- E911
- Boss-Admin Feature
- Calendar
- BToE
- EXP40 Expansion Module

# Power Indicator LED

Power indicator LED indicates power status and phone status.

There are six configuration options for power indicator LED:

#### **Common Power Light On**

Common Power Light On allows the power indicator LED to be turned on.

#### **Ring Power Light Flash**

Ring Power Light Flash allows the power indicator LED to flash when the IP phone receives an incoming call.

#### Voice Mail Power Light Flash

Voice Mail Power Light Flash allows the power indicator LED to flash when the IP phone receives a voice mail.

#### Mute Power Light On

Mute Power Light On allows the power indicator LED to flash when a call is mute.

#### Hold/Held Power Light On

Hold/Held Power Light On allows the power indicator LED to flash when a call is placed on hold or is held.

#### Talk/Dial Power Light On

Talk/Dial Power Light On allows the power indicator LED to be turned on when the IP phone is busy.

#### Procedure

Power indicator LED can be configured using the configuration files or locally.

		Configure the power indicator LED.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:
		phone_setting.common_power_led_

		enable
		phone_setting.ring_power_led_flash_ enable
		phone_setting.mail_power_led_flash _enable
		phone_setting.mute_power_led_flas h_enable
		phone_setting.hold_and_held_powe r_led_flash_enable
		phone_setting.talk_and_dial_power_ led_enable
		Configure the power indicator LED.
Local	Web User Interface	Navigate to:
		http:// <phoneipaddress>/servlet?p=f eatures-powerled&amp;q=load</phoneipaddress>

Parameters	Permitted Values	Default	
phone_setting.common_power_led_enable	0 or 1	0	
Description:			
Enables or disables the power indicator LED to be turned	on.		
<b>0</b> -Disabled (power indicator LED is off)			
1-Enabled (power indicator LED is solid red)			
Web User Interface:			
Features->Power LED->Common Power Light On			
Phone User Interface:			
None			
phone_setting.ring_power_led_flash_enable	0 or 1	1	
Description:			
Enables or disables the power indicator LED to flash when the IP phone receives an			
incoming call.			
<b>0</b> -Disabled (power indicator LED does not flash)			
1-Enabled (power indicator LED fast flashes (300ms) red)			
Web User Interface:			
Features->Power LED->Ring Power Light Flash			

Parameters	Permitted Values	Default			
Phone User Interface:					
None					
phone_setting.mail_power_led_flash_enable	phone_setting.mail_power_led_flash_enable 0 or 1 0				
Description:					
Enables or disables the power indicator LED to flash when voice mail.	the IP phone rea	ceives a			
0-Disabled (power indicator LED does not flash)					
1-Enabled (power indicator LED slow flashes (1000ms) red	)				
Web User Interface:					
Features->Power LED->Voice Mail Power Light Flash					
Phone User Interface:					
None					
phone_setting.mute_power_led_flash_enable 0 or 1 0					
Description:					
Enables or disables the power indicator LED to flash when	a call is mute.				
<b>0</b> -Disabled (power indicator LED does not flash)					
1-Enabled (power indicator LED fast flashes (300ms) red)					
Web User Interface:					
Features->Power LED->Mute Power Light On					
Phone User Interface:					
None					
phone_setting.hold_and_held_power_led_flash_enable	0 or 1	0			
Description:					
Enables or disables the power indicator LED to flash when held.	a call is placed	on hold or is			
<b>0</b> -Disabled (power indicator LED does not flash)					
1-Enabled (power indicator LED fast flashes (500ms) red)					
Web User Interface:					
Features->Power LED->Hold/Held Power Light On					
Phone User Interface:					
None					

Parameters	Permitted Values	Default	
phone_setting.talk_and_dial_power_led_enable	0 or 1	0	
Description:			
Enables or disables the power indicator LED to be turned on when the IP phone is busy.			
<b>0</b> -Disabled (power indicator LED is off)			
1-Enabled (power indicator LED is solid red)			
Web User Interface:			
Features->Power LED->Talk/Dial Power Light On			
Phone User Interface:			
None			

#### To configure the power Indicator LED via web user interface:

- 1. Click on Features->Power LED.
- 2. Select the desired value from the pull-down list of Common Power Light On.
- 3. Select the desired value from the pull-down list of Ringing Power Light Flash.
- 4. Select the desired value from the pull-down list of Voice Mail Power Light Flash.
- 5. Select the desired value from the pull-down list of Mute Power Light Flash.
- 6. Select the desired value from the pull-down list of Hold/Held Power Light Flash.
- 7. Select the desired value from the pull-down list of Talk/Dial Power Light On.

Yealink   1466	Status Account Network	Features Settings Directory	Log Out
General	Power LED:		NOTE
Information	Common Power Light On	Disabled 🔹 🕜	Damas LED
Audio	Ring Power Light Flash	Enabled 👻 🕜	Power LED Setting
Remote Control	Voice Mail Power Light Flash	Enabled 👻 🕜	You can click here to get
itemote control	Mute Power Light On	Disabled 👻 🕜	more guides.
Bluetooth	Hold/Held Power Light On	Disabled 🔹 🕜	
Power LED	Talk/Dial Power Light On	Disabled 🔹 💡	
	Confirm	Cancel	

8. Click Confirm to accept the change.

## Contrast

Contrast determines the readability of the texts displayed on the LCD screen. Adjusting the contrast to a comfortable level can optimize the screen viewing experience. When configured properly, contrast allows users to read the LCD's display with minimal eyestrain. You can configure the LCD's contrast of SIP-T40P and EXP40 connected to

SIP-T48G/T46G IP phones. Make sure the expansion module has been connected to the IP phone before adjustment. Contrast is not applicable to SIP-T42G/T41P IP phones.

## Procedure

Contrast can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure the contrast of the LCD screen. <b>Parameter:</b> phone_setting.contrast
Local	Web User Interface	Configure the contrast of the LCD screen. <b>Navigate to:</b> http:// <phonelpaddress>/servlet ?p=settings-preference&amp;q=load</phonelpaddress>
	Phone User Interface	Configure the contrast of the LCD screen.

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default	
phone_setting.contrast	Integer from 1 to 10	6	
Description:			
Configures the contrast of the LCD screen.			
For T48G/T46G IP phones, it configures the LCD's contrast of the connected EXP40			
only.			
For T40P IP phones, it configures the LCD's contrast of the IP phone.			
<b>Note</b> : We recommend that you set the contrast of the LCD screen to 6 as a more comfortable level. It is not applicable to SIP-T42G/T41P IP phones.			

#### Web User Interface:

Settings->Preference->Contrast

### Phone User Interface:

None

#### To configure the contrast via phone user interface:

### 1. Press Menu->Basic->Display->Contrast Setting.

If EXP40 is not connected to the phone, the Contrast Setting screen displays "No EXP".

2. Press  $(\bullet)$  or  $(\bullet)$ , or the Switch soft key to increase or decrease the intensity of

contrast.

The default contrast level is "6".

3. Press the Save soft key to accept the change.

## Backlight

Backlight determines the brightness of the LCD screen display, allowing users to read easily in dark environments. Backlight time specifies the delay time to change the intensity of the LCD screen when the IP phone is inactive. Backlight turns off quickly if a short backlight time is configured, this may not give users enough time to read messages. Backlight time is applicable to SIP SIP-T48G/T46G/T42G/T41P/T40P IP phones and EXP40 connected to SIP-T48G/T46G IP phones.

Backlight Active Level is used to adjust the backlight intensity of the LCD screen when the phone is active. Backlight Inactive Level is used to adjust the backlight intensity of the LCD screen when the phone is inactive. Backlight Active Level is applicable to SIP-T48G/T46G IP phones and the connected EXP40. Backlight Inactive Level is only applicable to SIP-T48G and SIP-T46G IP phones.

### Note Backlight time is configurable on Skype for Business Server only.

Before you adjust the LCD's backlight of expansion module, make sure the expansion module has been connected to the IP phone.

The following table lists available methods and configuration options to configure the backlight of phone models.

Phone Model (and the connected expansion module)	Configuration Methods	Configuration Options
SIP-T48G/T46G	Configuration Files Web User Interface Phone User Interface	Backlight Inactive Level
SIP-T48G(EXP40)/T46G (EXP40)	Configuration Files Web User Interface Phone User Interface	Backlight Active Level

#### Procedure

Backlight can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure the backlight of the LCD
		screen.
File	,	Parameters:

		phone_setting.inactive_backlight_level
Local	Web User Interface	Configure the backlight of the LCD screen.
		Navigate to:
		http:// <phonelpaddress>/servlet?p=set</phonelpaddress>
		tings-preference&q=load
	Phone User Interface	Configure the backlight of the LCD screen.

Parameters	Permitted Values	Default			
phone_setting.active_backlight_level	Integer from 1 to 10	10			
Description:	Description:				
Configures the intensity of the LCD screer	when the phone is active.				
10 is the highest intensity.					
For T48G/T46G IP phones, it configures the connected EXP40.	e LCD's intensity of the IP phone	and the			
Note: It is applicable to SIP-T48G/T46G IP p	phones and the connected EXF	<sup>5</sup> 40.			
Web User Interface:					
Settings->Preference->Backlight Active Le	evel				
Phone User Interface:					
Menu->Basic->Display->Backlight->Backlig	ght Active Level				
phone_setting.inactive_backlight_level	phone_setting.inactive_backlight_level 0 or 1 1				
Description:					
Configures the intensity of the LCD screer	when the IP phone is inactive.				
0-Off	<b>0</b> -Off				
1-Low					
Note: It is only applicable to SIP-T48G and T46G IP phones.					
Web User Interface:					
Settings->Preference->Backlight Inactive Level					
Phone User Interface:					
Menu->Basic->Display->Backlight->Backlig	ght Inactive Level				

To configure the backlight via web user interface:

- 1. Click on Settings->Preference.
- 2. Select the desired value from the pull-down list of Backlight Inactive Level.
- 3. Select the desired value from the pull-down list of Backlight Active Level.

			Log Out
Yealink   1466	Status Account Network	Features Settings Directory	Security
Preference	Language	English (English)	NOTE
Time & Date	Live Dialpad Inter Digit Time(1~14s)	Disabled V ?	Preference Settings The preference settings for
Upgrade	Backlight Inactive Level	Low V	administrator.  You can click here to get
Auto Provision	Backlight Active Level Watch Dog	B	more guides.
Configuration	Ring Type	Ring1.wav V	
Voice	Upload Ringtone	Browse No file selected.	
Tones	Confirm	Cancel	

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

To configure the backlight via phone user interface:

- 1. Press Menu->Basic->Display->Backlight.
- Press (•) or (•), or the Switch soft key to select the desired level from the Backlight Active Level field.
- 3. Press (•) or (•), or the Switch soft key to select the desired value from the Backlight Inactive Level field.
- 4. Press the Save soft key to accept the change.

## Sign in

Skype for Business users are authenticated against Microsoft Active Directory Domain Service. The following four sign-in methods are available.

- User Sign in: This method uses the user's credentials (sign-in address, user name, and password) to sign into Skype for Business Server. This sign-in method is applicable to Onprem account and Online account.
- **PIN Sign in**: This method uses the user's phone number (or extension) and personal identification number (PIN) to sign into Skype for Business Server. This sign-in method is only applicable to Onprem account.
- **Device Pairing for Online:** This method uses the user's Online account and pairing code to sign into Skype for Business Server. This sign-in method is only applicable to Online account.
- **BTOE Sign-in**: This method uses the Skype for Business client to sign into Skype for Business Server. You need to download and install the Yealink BToE Connector application on your computer first, ant then pair your phone to Skype for Business

client. As a result, you will sign into the Skype for Business client and phone using same account. This sign-in method is applicable to Onprem account and Online account. For more information, refer to Yealink phone-specific user guide.

**Note** If the phone reboots after successful login, the login credentials from the previous Sign-In will be cached. User can sign in successfully without reentering the credentials.

# User Sign-in

### Procedure

User sign-in method can be configured using the configuration files or locally.

		Configure User Sign in (User Credentials) method.
	<mac>.cfg</mac>	Parameters:
Configuration File		account.sign_in.server_address
		account.sign_in.user_name
		account.sign_in.password
		Configure User Sign in (User
		Credentials) method.
	Web User Interface	Navigate to:
Local		http:// <phonelpaddress>/servl</phonelpaddress>
		et?p=account-register-lync&q=
		IOdd&dCC=U
	Phone User Interface	Configure User Sign in (User
		Creaentiais) method.

Parameters	Permitted Values	Default	
account.sign_in.server_address	SIP URI	Blank	
Description:			
Configures the sign-in address for the User Sign in (User Credentials) method.			
The value format is username@domain.com.			
Example:			
account.sign_in.server_address= 2216@yealinkuc.com			
Web User Interface:			

Parameters	Permitted Values	Default	
Account->Register->Login address			
Phone User Interface:			
Sign in->User Sign in->Address			
account.sign_in.user_name	String within 128 characters	Blank	
Description:			
Configures the user name for the User Sign in (U	ser Credentials) method.		
The value format is username@domain.com or	username@domain,		
domain.com\username or domain\username.			
Example:			
account.sign_in.user_name= 2216@yealinkuc.com			
Web User Interface:			
Account->Register->Register Name			
Phone User Interface:			
Sign in->User Sign in->UserName			
account.sign_in.password String within 99 characters		Blank	
Description:			
Configures the password for the User Sign in (User Credentials) method.			
Web User Interface:			
Account->Register->Password			
Phone User Interface:			
Sign in->User Sign in->Password			

To sign into the Skype for Business Server using User Sign-in method via web user interface:

- 1. Click on Account->Register.
- 2. Select User Sign in from the pull-down list of Mode.
- **3.** Enter your Skype for Business user's sign-in address (e.g., 2216@yealinkuc.com) in the **Login address** field.
- 4. Enter your Skype for Business user name (e.g., 2216@yealinkuc.com) in the **Register** Name field.

5. Enter the sign-in password in the **Password** field.

Yealink 1466			Log Out
	Status Account Networ	k Features Settings Directory	Security
Register	Mode	User Sign in 🗸 💡	NOTE
Basic	Register Status	Disabled	Login address
Codec	Register Name	2216@yealinkuc.com	address
	Password	••••••	Register Name Provided by the operator register name.
	Sign In Sign Out	Cancel	Password Provided by the operator Password,

6. Click **Sign In** to accept the change.

To sign into the Skype for Business Server using User Sign in method via phone user interface:

- 1. Press the Sign in soft key.
- 2. Press  $(\cdot)$  or  $(\cdot)$ , or the Switch soft key to select User Sign in.
- 3. Enter your Skype for Business user's sign-in address (e.g., 2216@yealinkuc.com) in the Address field.
- 4. Enter your Skype for Business user name (e.g., 2216@yealinkuc.com) in the UserName field.
- 5. Enter the sign-in password in the **Password** field.



Press (•), (•) or the Switch soft key to select the desired value from the Remember Password filed.

If it is on, the user name and password will be filled automatically when you enter the sign-in address next time.

7. Press the Sign in soft key.

# **PIN Sign-in**

## Procedure

PIN sign-in be configured using the configuration files or locally.

Configuration File	<mac>.cfg</mac>	Configure PIN Sign-in (PIN Authentication) method. <b>Parameters:</b> account.sign_in.pin_number
	<y000000000xx>.cfg</y000000000xx>	Configures the PIN for the PIN Sign-in (PIN Authentication). account.sign_in.pin_password
		Configure PIN Sign-in (PIN Authentication) method. Navigate to:
Local		http:// <phonelpaddress>/servl et?p=account-register-lync&amp;q= load&amp;acc=0</phonelpaddress>
	Web user interface	Configure the certificate address of Skype for Business Server.
		Navigate to: http:// <phonelpaddress>/servl et?p=features-general&amp;q=load</phonelpaddress>
	Phone User Interface	Configure PIN Sign-in (PIN Authentication).

Parameters	Permitted Values	Default		
account.sign_in.pin_number	String within 128 characters	Blank		
Description:				
Configures the IP phone's extension for the PIN	Sign-in (PIN Authentication	) method.		
Web User Interface:				
Account->Register->Extension				
Phone User Interface:				
Sign in->PIN Sign in->Extension				

Parameters	Permitted Values	Default
account.sign_in.pin_password	String within 99 characters	Blank
Description:		
Configures the PIN for the PIN Sign-in (PIN Authe	entication) method.	
Web User Interface:		
Account->Register->Pin		
Phone User Interface:		
Sign in->PIN Sign in-> PIN		

To sign in to Skype for Business Server using the PIN Sign-in (PIN Authentication) method via web user interface:

- 1. Click on Account->Register.
- 2. Select User Sign in from the pull-down list of Mode.
- 3. Enter your Skype for Business user's phone number or extension (e.g., 2216) in the **Extension** field.
- 4. Enter your personal identification number (e.g., user2216) in the Pin field.

Yealink   1466	Status Account Network	k Features Settings Directory	Log Out
Register Basic Codec	Mode Register Status Extension Pin Sign In Sign Out	Pin Sign in V 2 Disabled 2216 2 Cancel	NOTE Login address Provided by the operator login address Register Name Provided by the operator register name.

#### 5. Click **Sign In** to accept the change.

If there is no DHCP Server in your environment, you may fail to sign in phone using PIN Sign-in (PIN Authentication) method, you can manually configure the certificate address of Skype for Business Server to make the phone sign in successfully.

To manually configure the certificate address of Skype for Business Server via web user interface:

1. Click on Features>General Information.

2. Enter the certificate address of Skype for Business Server in the SFB Cert Service URL field.

	Status	Account	Network	Features	Settin	gs	Directory	Security	
General		General Informat	ion 🕜					NOTE	Ì
Information		Call Waiting		Enabled	•	0		Call Waiting	
Audio		Key As Send		#	•	0		This call featu	re allows your
Remote Control		Busy Tone Delay	(Seconds)	0	•	0		calls during th	e conversation.
		Return code whe	en refuse	603 (Decline)	•	0		Key As Send	
Bluetooth		Time-Out for Dial	l-Now Rule	1		0		Select * or #	as the send key.
Power LED		Dial Search Delay		1		0		🛛 You can c	lick here to get
		180 Ring Workar	ound	Disabled	•	0		more guides.	
		DHCP Hostname		SIP-T46G		0			
		DHCP Hostname		SIP-T46G		0			
		E911 Location Ti	ip	Enabled	•	0			
		Update Checking	Time	24		0			
		Use DHCP Option	n 120	Enabled	•	0			
		SFB Cert Service	URL	https://xmpool.ye	alinkuc.cor	2			
		Enable SFB Autor	mation	Disabled	*	0			
		SFB Inactive Time	e	5		0			
		SFB Away Time		5	)	0			

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

To sign in to Skype for Business Server using the PIN Sign-in (PIN Authentication) method via phone user interface:

- 1. Press the Sign in soft key.
- 2. Press ( $\cdot$ ) or ( $\cdot$ ), or the Switch soft key to select PIN Sign in.
- 3. Enter your phone number or extension (e.g., 2216) in the extension field.
- 4. Enter your Pin in the PIN field.



5. Press (•), (•) or the Switch soft key to select the desired value from the Remember Password filed.

If it is on, the PIN will be filled automatically when you enter the phone number or extension next time.

6. Press the Sign in soft key.

# **Device Pairing for Online**

Device Pairing for Online is used to establish the connection between your phone and PC, so that you can sign into phone by web browser. This sign-in method is only applicable to Online account.

### Procedure

Device pairing for online can be using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure device pairing for online method. Parameters: features.device_pairing_for_online. enable
Local	Web User Interface	Configure device pairing for online method. <b>Navigate to:</b> http:// <phonelpaddress>/servlet?p =account-register-lync&amp;q=load&amp;a cc=0</phonelpaddress>
	Phone User Interface	Configure device pairing for online method.

Parameters	Permitted Values	Default
features.device_pairing_for_online.enable	0 or 1	1
Description:		
Enables or disables the user to sign into the Skyr Pairing for Online method.	pe for Business Server using	Device
0-Disabled		
1-Enabled		
Web User Interface:		
Features->General Information->Device Pairing	for Online	
Phone User Interface:		
None		

#### To configure Device Pairing for Online via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of **Device Pairing for Online**.
  - If it is enabled, you can sign into the Skype for Business Server using Device Pairing for Online method.
  - If it is disabled, you cannot sign into the Skype for Business Server using Device Pairing for Online method.

			Log Out
Yealink 146G	Status Account Network	Features Settings	Directory Security
General Information	General Information ? Call Waiting	Enabled V	NOTE Call Waiting This call feature allows your
Remote Control Bluetooth	Busy Tone Delay (Seconds) Return code when refuse	0 V 0 603 (Decline) V 0	phone to accept other incoming calls during the conversation. <b>Key As Send</b> Select * or # as the send key.
Power LED	Time-Out for Dial-Now Rule Dial Search Delay		You can click here to get more guides.
	CED Transition Time		
	SFB Inactive Time SFB Away Time Device Pairing for Online	5 5 Enabled	
	Confirm	Cancel	

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

To sign into Skype for Business Server using Device Pairing for Online method via phone user interface:

1. Press the Sign in soft key.

		Sign in	
	Sign in:	Device Pairing for Online	<>
	Select site:	Australia	<>
Ba	ack	Switch	Sign in

- 2. Press  $(\cdot)$ ,  $(\cdot)$  or the Switch soft key to select Device Pairing for Online.
- Press (, ) or the Switch soft key to select the corresponding country from the Select site field.
- 4. Press the Sign in soft key.

The screen will show the pairing code and URL.

Pairing Code:Y9TUC: tps://pinauthtest1.c	SRCD loudapp.ne
t	Pairing Code:Y9TUC ttps://pinauthtest1.c

- 5. Enter the URL (e.g., https://pinauthtest1.cloudapp.net) in the address bar of the web browser on your PC, and then press **Enter**.
- 6. Enter your email address (e.g., yealink1@lyosbpsmds.ccsctp.net) in the Email address field.

Skype for Business Online Phone Authentication	
Enter your work or school email address,	
yealink1@lyosbpsmds.ccsctp.net	
Verify email	

7. Click Verify email to check the validity of the email address.

The sign-in screen will appear if the email address is valid.

- 8. Enter your Online account and password.
- (Optional) Check the Keep me signed in check box, so that you don't need to enter a password next time.

Office 365
Work or school, or personal Microsoft account
yealink1@lyosbpsmds.ccsctp.net
•••••
✓ Keep me signed in
Sign in

- 10. Click Sign in.
- 11. Enter the pairing code (e.g., YT4DYBCKL) in the Code field.

Device Login	
Enter the code that you received from the application on your device	
YT4DYBCKL	
Yealink Skype for Business Certified Phone Application publisher: Click cancel if you received this code from a	
different application.	
Continue Cancel	

12. Click Continue.



**13.** Click the account to sign in.

If you click Use another account, enter another Online account and password,

and then click **Sign in**. The phone will sign into the Skype for Business Server automatically.

If the Skype for Business Server is configured to forcibly lock the phone. You need to configure an unlock PIN at the initial sign-in.

# Sign out

### Procedure

Sign-out can be configured locally.

Local		Sign out of Skype for Business Server.
	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servl</phonelpaddress>
		et?p=account-register-lync&q=
		load&acc=0
	Phone User Interface	Sign out of Skype for Business Server.

To sign out of Skype for Business Server via web user interface:

1. Click on Account->Register.

Yealink   1466	Status Account Networ	k Features Settings Directory	Log Out
Register	Mode	User Sign in 🔹 🥐	NOTE
Basic	Register Status Login address	Registered 2216@yealinkuc.com ?	Login address Provided by the operator login
Codec	Register Name Password	2216@yealinkuc.com	address Register Name
	Sign In Sign Out	Cancel	Provided by the operator register name. Password Provided by the operator Password.

2. Click Sign Out to accept the change.

#### To sign out of Skype for Business Server:

- 1. Press the **Status** soft key.
- 2. Press ( ) or ( ) to select Sign Out.

The phone signs out of Skype for Business server.

After you sign out of Skype for Business, the account-related features (calling, viewing Skype for Business contacts, calendar, etc.) are not available. However, you can still use other phone features.

# Updating Status Automatically

The Skype for Business Server helps you keep your presence information up-to-date by monitoring idle time of your phone. Phone status will be Inactive when your phone has been idle for the designated time. Phone status will change from Inactive to Away after another designated time.

## Procedure

Updating status automatically can be configured using the configuration files or locally.

		Configures the inactive time (in minutes) of the IP phone.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:
		sfb.presence.inactive_time
		sfb.presence.away_time
Local		Configures the inactive time (in
		minutes) of the IP phone.
	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet?p=fea</phonelpaddress>
		tures-general&q=load

Parameters	Permitted Values	Default		
sfb.presence.inactive_time	e Integer from 5 to 360			
Description:				
Configures the inactive time (in minutes) of	the IP phone, after which the pho	one will		
change its status to Inactive automatically.				
Example:				
If it is set to 5, the IP phone will change its status to Inactive automatically when inactive				
time reaches 5 minutes.				
<b>Note</b> : If you change this parameter, the IP phone will reboot to make the change				
take effect.				
Web User Interface:				
Features->General Information->SFB Away Time				
Phone User Interface:				
None				
sfb.presence.away_time	Integer from 5 to 360	5		

#### Description:

Configures the inactive time (in minutes) of the IP phone, after which the phone will change its status from Inactive to Away automatically.

#### Example:

If it is set to 5, the IP phone whose status is Inactive will change to Away automatically after 5 minutes.

**Note**: If you change this parameter, the IP phone will reboot to make the change take effect.

#### Web User Interface:

Features->General Information->SFB Away Time

#### Phone User Interface:

None

#### To configure the automatic status updating time via web user interface:

- 1. Click on Features->General Information.
- 2. Enter the desired time in the SFB Inactive Time field.
- 3. Enter the desired time in the SFB Away Time field.

ealink 1460								Log U
	Status	Account	Network	Features	Settin	gs	Directory	Security
General	Ge	eneral Informat	ion 🕜					NOTE
Information		Call Waiting		Enabled	•	0		Call Waiting
Audio		Key As Send		#	•	0		This call feature allows your
Remote Control		Busy Tone Delay	(Seconds)	0	•	0		calls during the conversation.
Activite control		Return code whe	en refuse	603 (Decline)	•	0		Key As Send
Bluetooth		Time-Out for Dia	l-Now Rule	1		0		Select * or # as the send key
Power LED		Dial Search Delay		1		0		You can click here to get
		180 Ring Workar	ound	Disabled	•	0		more guides.
		CO11 Leastine Ti	2	SIP-1400		0		
		Egil Location II	P	Enabled		0		
		Update Checking	lime	24		0		
		Use DHCP Option	120	Enabled	•	0		
		SFB Cert Service	URL	https://xmpool.yeali	inkuc.cor	0		
	E.	Enable SFB Auto	mation	Disabled	•	0	r	
		SFB Inactive Tim	e	5		0		
		SFB Away Time		5		0		
		Device Pairing for	Online	Enabled	-	?		

4. Click Confirm to accept the change.

# Web Server Type

Web server type determines access protocol of the IP phone's web user interface. IP phones support 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 pages returned by the web server. Both HTTP and HTTPS port numbers are configurable.

### Procedure

Web server type can be configured using the configuration files or locally.

		Configure the web access type, HTTP port and HTTPS port. <b>Parameters:</b>
Configuration File	<y000000000xx>.cfg</y000000000xx>	wui.http_enable
		network.port.http
		wui.https_enable
		network.port.https
Local		Configure the web access type, HTTP port and HTTPS port.
	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servl et?p=network-adv&amp;q=load</phonelpaddress>
	Phone User Interface	Configure the web access type, HTTP port and HTTPS port.

Parameters	Permitted Values	Default			
wui.http_enable	0 or 1	1			
Description:					
Enables or disables the user to access web user HTTP protocol.	Enables or disables the user to access web user interface of the IP phone using the HTTP protocol.				
0-Disabled					
1-Enabled					
<b>Note</b> : If you change this parameter, the IP phone will reboot to make the change take effect.					
Web User Interface:					
Network->Advanced->Web Server->HTTP					
Phone User Interface:					
Menu->Advanced (default password: admin) ->Network->Webserver Type->HTTP Status					

Parameters	Permitted Values	Default			
network.port.http	Integer from 1 to 65535	80			
Description:					
Configures the HTTP port for the user to access using the HTTP protocol.	web user interface of the IF	' phone			
<b>Note:</b> If you change this parameter, the IP phor take effect.	ne will reboot to make the a	change			
Web User Interface:					
Network->Advanced->Web Server->HTTP Port(1	~65535)				
Phone User Interface:					
Menu->Advanced (default password: admin) - Port	>Network->Webserver Type	e->HTTP			
wui.https_enable	0 or 1	1			
Description:         Enables or disables the user to access web user interface of the IP phone using the HTTPS protocol.         O-Disabled         1-Enabled         Note: If you change this parameter, the IP phone will reboot to make the change take effect.         Web User Interface:         Network->Advanced->Web Server->HTTPS         Phone User Interface:         Menu->Advanced (default password: admin) ->Network->Webserver Type->HTTPS					
network.port.https	Integer from 1 to 65535	443			
Description:	Description:				
Configures the HTTPS port for the user to access web user interface of the IP phone using the HTTPS protocol.					
<b>Note</b> : If you change this parameter, the IP phone will reboot to make the change take effect.					
Web User Interface:					
Network->Advanced->Web Server->HTTPS Port(1~65535)					
Phone User Interface:					

Parameters	Permitted Values	Default	
Menu->Advanced (default password: admin) ->Network->Webserver Type->HTTPS			
Port			

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.
- Enter the desired HTTP port number in the HTTP Port(1~65535) field.
   The default HTTP port number is 80.
- 4. Select the desired value from the pull-down list of HTTPS.
- 5. Enter the desired HTTPS port number in the HTTPS Port(1~65535) field.

The default HTTPS port number is 443.

area tends
al LAN ints, ions.
ity is rovide ig the
o aet
arteal nor ito g

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

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

7. Click **OK** to reboot the IP phone.

#### To configure web server type via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Network->Webserver Type.
- 2. Press  $(\cdot)$  or  $(\cdot)$ , or the Switch soft key to select the desired value from the HTTP

Status field.

- 3. Enter the desired HTTP port number in the HTTP Port field.
- 4. Press (•) or (•), or the Switch soft key to select the desired value from the HTTP Status field.
- 5. Enter the desired HTTPS port number in the HTTPS Port field.
- 6. Press the Save soft key to accept the change.

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

# Time and Date

IP phones maintain a local clock and calendar. Time and date are displayed on the idle screen of IP phones.

Option	Configuration Methods	
	Configuration Files	
NTP time server	Web User Interface	
	Phone User Interface	
	Configuration Files	
Time Zone	Web User Interface	
	Phone User Interface	
<b>T</b> <sup>1</sup>	Web User Interface	
lime	Phone User Interface	
	Configuration Files	
Time Format	Web User Interface	
	Phone User Interface	
Dete	Web User Interface	
Ddie	Phone User Interface	
	Configuration Files	
Date Format	Web User Interface	
	Phone User Interface	
Dauliant Savina Tiraa	Configuration Files	
Daylight saving time	Web User Interface	

The following table lists available configuration methods for time and date.

## **NTP Time Server**

A time server is a PC server that reads the actual time from a reference clock and distributes this information to the clients in a network. The Network Time Protocol (NTP) is the most widely used protocol that distributes and synchronizes time in the network.

The IP phone issues a DHCP request to query Option 42 for obtaining the NTP server and synchronizes the time and date automatically from the NTP time server by default. The NTP time server address can be offered by the DHCP server or configured manually. NTP by DHCP Priority feature can configure the priority for the IP phone to use the NTP time server address offered by the DHCP server or configured manually.

#### 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 IP phone to obtain the time and date from the NTP time server, you must set the time zone.

### Procedure

NTP time server and time zone can be configured using the configuration files or locally.

		Configure NTP by DHCP priority feature and DHCP time feature.
		Parameters:
	<mac>.cfg</mac>	local_time.manual_ntp_srv_prior
		local_time.dhcp_time
		Configure the NTP server, time
Configuration File		zone.
		Parameters:
		local_time.ntp_server1
		local_time.ntp_server2
		local_time.interval
		local_time.time_zone
		local_time.time_zone_name
		Configure NTP by DHCP priority
Local		feature and DHCP time feature.
		Configure the NTP server, time
	Web User Interface	zone.
		Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		<pre>?p=settings-datetime&amp;q=load</pre>

	Phone User Interface	Configure DHCP time feature.
		Configure the NTP server and
		time zone.

Parameters	Permitted Values	Default			
local_time.manual_ntp_srv_prior	0 or 1	0			
Description:					
Configures the priority for the IP phone to use the NTP server address offered by the DHCP server.					
0-High (use the NTP server address offered by the DHCP server preferentially)					
1-Low (use the NTP server address configured manually preferentially)					
Web User Interface:					
Settings->Time & Date->NTP by DHCP Priority					
Phone User Interface:					
None					
local_time.dhcp_time	0 or 1	0			
Description:					
Enables or disables the IP phone to update time with the offset time offered by the					
DHCP server.					
0-Disabled					
1-Enabled					
Note: It is only available to offset from GMT 0.					
Web User Interface:					
Settings->Time & Date->DHCP Time					
Phone User Interface:					
Menu->Basic->Date & Time->DHCP Time					
local_time.ntp_server1	IP Address or Domain Name	cn.pool.ntp.org			

Parameters	Permitted Values	Default			
Description:					
Configures the IP address or the domain name of the NTP server 1.					
Example:					
local_time.ntp_server1 = 192.168.0.5					
Web User Interface:					
Settings->Time & Date->Primary Server					
Phone User Interface:					
Menu->Basic->Date & Time->Gene	eral->SNTP Settings->NTP Serve	rl			
local_time.ntp_server2	IP Address or Domain				
	Name	cn.pool.nip.org			
Description:					
Configures the IP address or the do	omain name of the NTP server	2.			
If the NTP server 1 is not configured	or cannot be accessed, the I	P phone will request			
the time and date from the NTP se	rver 2.				
Example:					
local_time.ntp_server2 = 192.168.0.	6				
Web User Interface:					
Settings->Time & Date->Secondary	Server				
Phone User Interface:	Phone User Interface:				
Menu->Basic->Date & Time->General->SNTP Settings->NTP Server2					
local_time.interval	Integer from 15 to 86400	1000			
Description:					
Configures the interval (in seconds	Configures the interval (in seconds) to update time and date from the NTP server.				
Example:					
local_time.interval = 1000					
Web User Interface:					
Settings->Time & Date->Synchronism (15~86400s)					
Phone User Interface:					
None					
local_time.time_zone	-11 to +14	+8			

Parameters	Permitted Values	Default		
Description:				
Configures the time zone.				
Example:				
local_time.time_zone = +8				
For more available time zones, refe	r to Appendix B: Time Zones c	on page 344.		
Web User Interface:				
Settings->Time & Date->Time Zone				
Phone User Interface:				
Menu->Basic->Date & Time->General->SNTP Settings->Time Zone				
local_time.time_zone_name	String within 32 characters	China(Beijing)		
Description:				
Configures the time zone name.				
The available time zone names dep	pend on the time zone config	jured by the		
parameter "local_time.time_zone" names for each time zone, refer to	. For more information on the Appendix B: Time Zones on p	available time zone age 344.		
Example:				
local_time.time_zone_name = Chir	na(Beijing)			
Note: It works only if the value of the	e parameter "local_time.sum	mer_time" is set to 2		
<b>Note</b> : It works only if the value of the (Automatic) and the parameter "Id	e parameter "local_time.sum ocal_time.time_zone" should l	mer_time" is set to 2 oe configured in		
<b>Note</b> : It works only if the value of the (Automatic) and the parameter "lo advance.	e parameter "local_time.sum ocal_time.time_zone" should l	mer_time" is set to 2 oe configured in		
Note: It works only if the value of the (Automatic) and the parameter "la advance. Web User Interface:	e parameter "local_time.sum ocal_time.time_zone" should l	mer_time" is set to 2 be configured in		
Note: It works only if the value of the (Automatic) and the parameter "la advance. Web User Interface: Settings->Time & Date->Location	e parameter "local_time.sum ocal_time.time_zone" should l	mer_time" is set to 2 oe configured in		
Note: It works only if the value of the (Automatic) and the parameter "la advance. Web User Interface: Settings->Time & Date->Location Phone User Interface:	e parameter "local_time.sum ocal_time.time_zone" should l	mer_time" is set to 2 be configured in		

### 1. Click on Settings->Time & Date.
2. Select the desired value from the pull-down list of NTP by DHCP Priority.

							Log Out
Yealink 1466							
	Status	Account	Network	Features	Settings	Directory	Security
Preference	Time	&Date:					NOTE
Time&Date	DHCP	Time		Disabled	• •	Pussia -	Time Zone
Upgrade	Daylig	ht Saving Time		<ul> <li>Automatic</li> </ul>	Enabled	Disabled ?	in.
Auto Provision	Locat	ion		China(Beijing)	- (	2	NTP Server The server which is used to
Configuration	Fixed	Туре		OST By Date	e 💿 DST By W	eek 🕜	synchronize the clock of the phone.
Dial Plan	Start End D	Date Date		Month Month	Day Ho Day Ho	our	You can click here to get
Voice	Offset	t(minutes)		,		2	more guides.
Tones	NTP E	By DHCP Priority		High	•		
Phone Lock	Prima	ry Server		time.windows.c	om	2	
Location	Secor	ndary Server		time.nist.gov		2	
Location	Synch	nronism (15~86400	)s)	1000	(	2	
EXP Module	Manua	al Time		Disabled	(	2	
BTOE	Time	Format		Hour 24	- (	3	
	Date	Format		WWW MMM DD	• • •	0	
		Confirm	n		Cancel		

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

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

- 1. Click on Settings->Time & Date.
- 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. Select the desired location from the pull-down list of Location.
- 5. Enter the domain name or IP address in the **Primary Server** and **Secondary Server** field respectively.
- 6. Enter the desired time interval in the Synchronism (15~86400s) field.

Vertint			Log Out
	Status Account Network	Features Settings Directory	Security
Preference	Time&Date:		NOTE
Time&Date	DHCP Time	Disabled 🔹 🕜	Time Zone
	Time Zone	+8 China, Singapore, Australia, Russia 🔻 🕜	Choose the time zone you are in.
Upgrade	Daylight Saving Time	🖲 Automatic 🔘 Enabled 🔘 Disabled 🕜	
Auto Provision	Location	China(Beijing) 🔹 🕜	The server which is used to
Configuration	Fixed Type	DST By Date DST By Week      OST By Week     OST     O	synchronize the clock of the phone.
pi-t pi-s	Start Date	Month Day Hour	
Dial Plan	End Date	Month Day Hour	You can click here to get
Voice	Offset(minutes)	<b>0</b>	more guides.
Tones	NTP By DHCP Priority	High	
Dhone Lock	Primary Server	time.windows.com	
Thone Lock	Secondary Server	time.nist.gov	
Location	Synchronism (15~86400s)	1000	
EXP Module	Manual Time	Disabled 🔹 🕐	
ВТОЕ	Time Format	Hour 24 🔹 🕐	
	Date Format	WWW MMM DD 🔹 🕜	
	Confirm	Cancel	

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

### To configure the SNTP settings via phone user interface:

- 1. Press Menu->Basic->Date & Time->General->SNTP Settings.
- 2. Press () or (), or the Switch soft key to select the time zone that applies to your area from the Time Zone field.

The default time zone is "GMT+8".

- Enter the domain name or IP address of SNTP server in the NTP Server1 and NTP Server2 field respectively.
- 4. Press () or (), or the Switch soft key to select automatic, enabled and disabled from the Daylight Saving field.
- 5. Press () or (), or the Switch soft key to select the desired location from the Location field.
- 6. Press the Save soft key to accept the change.

# **Time and Date Settings**

You can set the time and date manually when IP phones cannot obtain the time and date from the NTP time server. The time and date display can use one of several different formats.

### Procedure

Time and date can be configured using the configuration files or locally.

		Configure the time and date manually.
		Parameter:
		local_time.manual_time_enable
Configuration File	<mac>.cfg</mac>	Configure the time and date
		formats.
		Parameters:
		local_time.time_format
		local_time.date_format
		Configure the time and date
		manually.
Land		Configure the time and date
LOCAI	web user interface	
		Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		<pre>\$p=settings-aatetime&amp;q=load</pre>

Phone User Interface	Configure the time and date manually. Configure the time and date formats.
----------------------	---

# Details of Configuration Parameters:

Parameters	Permitted Values	Default		
local_time.manual_time_enable	0 or 1	0		
Description:				
Enables or disables the IP phone to	obtain time and date from n	nanual settings.		
<b>0</b> -Diabled (obtain time and date fr	rom NTP server)			
1-Enabled (obtain time and date f	rom manual settings)			
Web User Interface:				
Settings->Time & Date->Manual Tim	ne			
Phone User Interface:				
None				
local_time.time_format	0 or 1	1		
Description:				
Configures the time format.				
<b>0</b> -Hour 12				
<b>1</b> -Hour 24				
If it is set to 0 (Hour 12), the time wil specified.	l be displayed in 12-hour form	at with AM or PM		
If it is set to 1 (Hour 24), the time wil displays as 14:00).	l be displayed in 24-hour form	at (e.g., 2:00 PM		
Web User Interface:				
Settings->Time & Date->Time Forma	at			
Phone User Interface:				
Menu->Basic->Date & Time->Time	& Date Format->Time Format			
local_time.date_format 0, 1, 2, 3, 4, 5 or 6 0				
Description:				
Configures the date format.				
Valid values are:				

Parameters	Permitted Values	Default	
0-WWW MMM DD			
1-DD-MMM-YY			
2-YYYY-MM-DD			
3-DD/MM/YYYY			
4-MM/DD/YY			
5-DD MMM YYYY			
6-WWW DD MMM			
<b>Note</b> : "WWW" represents the abbreviation of the week, "DD" represents a two-digit day, "MMM" represents the first three letters of the month, "YYYY" represents a four-digit year, and "YY" represents a two-digit year.			
Web User Interface:			
Settings->Time & Date->Date Format			
Phone User Interface:			
Menu->Basic->Date & Time->Time a	& Date Format->Date Format		

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

- 1. Click on Settings->Time & Date.
- 2. Select Enabled from the pull-down list of Manual Time.
- 3. Enter the time and date in the corresponding fields.

			Log Out
YEAIINK   T46G	Status Account Network	Features Settings Directory	Security
Preference	Time&Date:		NOTE
Time&Date	DHCP Time	Disabled	Time Zone
	NTP By DHCP Priority	High 👻	Choose the time zone you are
Upgrade	Primary Server	time.windows.com	
Auto Provision	Secondary Server	time.nist.gov	NTP Server The server which is used to
Configuration	Synchronism (15~86400s)	1000	synchronize the clock of the phone.
Comguration	Manual Time	Enabled 🗸 🕜	prove
Dial Plan	Date	Year 2016 Month 4 Day 21	You can click here to get
Voice	Time	Hour 10 Minute 35 Second 19	more guides.
Tones	Time Format	Hour 24 🔹 🕜	
Phone Lock	Date Format	WWW MMM DD 🔹 🕜	
Location	Confirm	Cancel	
EXP Module			
ВТОЕ			

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

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

- 1. Click on Settings->Time & Date.
- 2. Select the desired value from the pull-down list of Time Format.

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

Voglink			Log Out
	Status Account Networ	k Features Settings Directory	Security
Preference	Time&Date:		NOTE
Time&Date	DHCP Time Time Zone	Disabled    Philosophia China, Singapore, Australia, Russia	Time Zone Choose the time zone you are
Upgrade	Daylight Saving Time	Automatic      Enabled      Disabled	in.
Auto Provision	Location	China(Beijing) 🗸 🥜	NTP Server The server which is used to
Configuration	Fixed Type	OST By Date DST By Week     O     DST By The second secon	synchronize the clock of the phone.
Dial Plan	Start Date End Date	Month Day Hour Month Day Hour	You can click here to get
Voice	Offset(minutes)		more guides.
Tones	NTP By DHCP Priority	High 👻	
Phone Lock	Primary Server	time.windows.com	
	Secondary Server	time.nist.gov	
Location	Synchronism (15~86400s)	1000	
EXP Module	Manual Time	Disabled 🔹 💡	
BToE	Time Format	Hour 24 🔹 💡	
	Date Format	WWW MMM DD 👻 🕜	
	Confirm	Cancel	

4. Click Confirm to accept the change.

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

- 1. Press Menu->Basic->Date &Time->General->Manual Settings.
- 2. Enter the specific date and time or press ( ) or ( ) to edit specific date and time in the corresponding fields.
- 3. Press Save to accept the change.

The time and date displayed on the LCD screen will change accordingly.

### To configure the time and date format via phone user interface:

- 1. Press Menu ->Basic->Date &Time ->Time & Date Format.
- Press () or (), or the Switch soft key to select the desired date format from the Date Format field.
- 3. Press (•) or (•), or the Switch soft key to select the desired time format (12 Hour or 24 Hour) from the Time Format field.
- 4. Press the Save soft key to accept the change or the Back soft key to cancel.

# **Daylight Saving Time**

Daylight Saving Time (DST) is the practice of temporary advancing clocks during the summer time 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 the DST at various times, details vary by location. By default, the DST is set to Automatic, so it can be adjusted automatically from the current time zone configuration. You can configure DST for the desired area as required.

## Procedure

Daylight saving time can be configured using the configuration files or locally.

		Configure DST.
		Parameters:
	<mac>.cfg</mac>	local_time.summer_time
<b>Configuration File</b>		local_time.dst_time_type
		local_time.start_time
		local_time.end_time
		local_time.offset_time
		Configure DST.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		<pre>?p=settings-datetime&amp;q=load</pre>

# Details of Configuration Parameters:

Parameters	Permitted Values	Default			
local_time.summer_time	0, 1 or 2	2			
Description:	Description:				
Configures Daylight Saving Time (D	DST) feature.				
0-Disabled					
1-Enabled					
<b>2</b> -Automatic					
Web User Interface:					
Settings->Time & Date->Daylight Sc	aving Time				
Phone User Interface:					
Menu->Basic->Date & Time->Gene	eral->SNTP Settings->Daylight S	aving			
local_time.dst_time_type	0 or 1	0			
Description:					
Configures the DST time type.					
<b>0</b> -DST By Date					
1-DST By Week					
<b>Note</b> : It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).					

Parameters	Permitted Values	Default	
Web User Interface:			
Settings->Time & Date->Fixed Type			
Phone User Interface:			
None			
local_time.start_time 1/1/0			
Description:			
Configures the start time of the DST	Τ.		
Value formats are:			
Month/Day/Hour (for DST By D	ate)		
Month/Day of Week Last in Me	onth/Day of Week/Hour of Do	ay (for DST By Week)	
If "local_time.dst_time_type" is set	to 0 (DST By Date), use the mo	apping:	
Month: 1=January, 2=February,, 1	2=December		
Day: 1=the first day in a month,,	31= the last day in a month		
Hour: 0=0am, 1=1am,, 23=11pm			
If "local_time.dst_time_type" is set	to 1 (DST By Week), use the m	apping:	
Month: 1=January, 2=February,, 1	2=December		
<b>Day of Week Last in Month:</b> 1=the f	irst week in a month,, 5=the	last week in a	
Day of Week: 1=Monday, 2=Tuesda	ay,, 7=Sunday		
Hour of Day: 0=0am, 1=1am,, 23=	=11pm		
<b>Note</b> : It works only if the value of th (Enabled).	e parameter "local_time.sum	mer_time" is set to 1	
Web User Interface:			
For DST By Date:			
Settings->Time & Date->Start Date			
For DST By Week:			
Settings->Time & Date->DST Start M	onth/DST Start Day of Week/[	DST Start Day of	
Week Last in Month/Start Hour of D	ay		
Phone User Interface:			
None			
local_time.end_time Time 12/31/23			
Description:			
Configures the end time of the DST.			

Parameters	Permitted Values	Default		
Value formats are:				
Month/Day/Hour (for DST By D	Date)			
Month/Day of Week Last in M	onth/Day of Week/Hour of Dc	ay (for DST By Week)		
If "local_time.dst_time_type" is set	to 0 (DST By Date), use the mo	apping:		
Month: 1=January, 2=February,,	12=December			
Day: 1=the first day in a month,,	31= the last day in a month			
Hour: 0=0am, 1=1am,, 23=11pm				
If "local_time.dst_time_type" is set	to 1 (DST By Week), use the m	apping:		
Month: 1=January, 2=February,,	12=December			
Day of Week Last in Month: 1=the f month	irst week in a month,, 5=the	last week in a		
Day of Week: 1=Monday, 2=Tuesda	ay,, 7=Sunday			
Hour of Day: 0=0am, 1=1am,, 23=	=11pm			
<b>Note</b> : It works only if the value of the (Enabled).	<b>Note</b> : It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled).			
Web User Interface:				
For DST By Date:				
Settings->Time & Date->End Date				
For DST By Week:				
Settings->Time & Date->DST Stop M Week Last in Month/Stop Hour of D	lonth/DST Stop Day of Week/[ pay	DST Stop Day of		
Phone User Interface:				
None				
local_time.offset_time	Integer from -300 to 300	Blank		
Description:				
Configures the offset time (in minut	tes) of DST.			
Note: It works only if the value of th	e parameter "local_time.sum	mer_time" is set to 1		
(Enabled).				
Web User Interface:				
Settings->Time & Date->Offset(minutes)				
Phone User Interface:				
None				
To configure the DST via web user in	terface:			

1. Click on Settings->Time & Date.

- 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 name or IP address in the **Primary Server** and **Secondary Server** field respectively.
- 5. Enter the desired time interval in the Synchronism (15~86400s) field.
- 6. Mark the Enabled radio box in the Daylight Saving Time field.
  - 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.

Voglink			Log Out
	Status Account Network	Features Settings Directory	Security
Preference	Time&Date:		NOTE
Time&Date	DHCP Time Time Zone	Disabled 🔹 🕜	Time Zone Choose the time zone you are
Upgrade	Daylight Saving Time	Automatic      Enabled      Disabled     O	in.
Auto Provision	Fixed Type	💿 DST By Date 🔘 DST By Week 🛛 🕜	NTP Server The server which is used to
Configuration	Start Date	Month 1 Day 1 Hour 1	synchronize the clock of the phone.
Dial Dlan	End Date	Month 12 Day 12 Hour 12	
Darran	Offset(minutes)	•	You can click here to get more quides
Voice	NTP By DHCP Priority	High 👻	more guides.
Tones	Primary Server	time.windows.com	
Phone Lock	Secondary Server	time.nist.gov 🕜	
	Synchronism (15~86400s)	1000	
Location	Manual Time	Disabled 👻 🕜	
EXP Module	Date Format	WWW MMM DD 🔻 🕜	
ВТОЕ	Confirm	Cancel	

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

Select the desired values of DST Start Month, DST Start Week of Month, DST Start Day of Week, Start Hour of Day; DST Stop Month, DST Stop Week of Month, DST Stop Day of Week and End Hour of Day from the pull-down lists.

Varlink			Log Out
	Status Account Network	Features Settings Directory	Security
Preference	Time&Date:		NOTE
Time&Date	DHCP Time	Disabled	Time Zone
Upgrade	Daylight Saving Time	Automatic      Enabled      Disabled	in.
Auto Provision	Fixed Type	💿 DST By Date 🖲 DST By Week 🕜	NTP Server The server which is used to
Configuration	Start Date	January • First In Mo • Sunday • 00:00 •	synchronize the clock of the phone.
Dial Plan	End Date	January  V First In Mo  V Sunday  V 00:00  V	
Voice	Offset(minutes) NTP By DHCP Priority	(2) High	You can click here to get more guides.
Tones	Primary Server	time.windows.com	
	Secondary Server	time.nist.gov	
Phone Lock	Synchronism (15~86400s)	1000	
Location	Manual Time	Disabled 🗸 🧭	
EXP Module	Date Format	WWW MMM DD 👻 🕜	
ВТОЕ	Confirm	Cancel	

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

## Customizing an AutoDST Template File

The time zone and corresponding DST pre-configurations exist in the AutoDST file. If the DST is set to Automatic, the IP phone obtains the DST configuration from the AutoDST file. You can customize the AutoDST file if required. The AutoDST file allows you to add or modify time zone and DST settings for your area each year.

Before customizing, you need to obtain the AutoDST file. You can ask the distributor or Yealink FAE for DST template. You can also obtain the DST template online:

http://www.yealink.com/solution\_info.aspx?ProductsCateID=1248&cateid=1248&BaseInfoC ateId=1328&Cate\_Id=1248&parentcateid=1328. For more information on obtaining the template file, refer to Obtaining Configuration Files and Resource Files on page 36.

Element	Туре	Values Description	
DSTData	required	no	File root element
DST	required	no	Time Zone item's root element
szTime	required	[+/-][X]:[Y], X=0~13, Y=0~59	Time Zone
szZone	required	String (if the content is more than one city, it is the best to keep their daylight saving time the same)	Time Zone name
іТуре	optional	0/1DST time type0: DST By Date(This item is need1: DST By Weekyou want toconfigure DST.)	
szStart	optional	Month/Day/Hour (for iType=0) Month: 1~12 Day: 1~31 Hour: 0 (midnight)~23 Month/Day of Week Last in Month/Day of Week/Hour of Day (for iType=1) Month: 1~12 Day of Week Last in Month: 1~5 (the last week) Day of Week: 1~7 Hour of Day: 0 (midnight)~23	Start time of the DST
szEnd	optional	Same as szStart	End time of the DST

The following table lists description of each element in the template file:

Element	Туре	Values	Description
szOffset	ontional	Integer from -300 to 300	The offset time (in
32011301	opilorial	minutes) of D	minutes) of DST

### When customizing an AutoDST file, learn the following:

- <DSTData> indicates the start of a template and </DSTData> indicates the end of a template.
- Add or modify time zone and DST settings between <DSTData> and </DSTData>.
- The display order of time zone is corresponding to the szTime order specified in the AutoDST.xml file.
- If the start time of DST is greater than the end time, the valid time of DST is from the start time of this year to the end time of the next year.

### Customizing an AutoDST file:

- 1. Open the AutoDST file using an ASCII editor.
- 2. Add or modify time zone and DST settings as you want in the AutoDST file.

### Example 1:

To modify the DST settings for the existing time zone "+5 Pakistan(Islamabad)" and add DST settings for the existing time zone "+5:30 India(Calcutta)".

-					
A	toDST.xi	ni* ×			
	2	1,0,		.8,0,	100
	<dot <="" statement="" td=""></dot>	szTime="+3:30"	<pre>szZone="Iran(Teheran)" iType="0" szStart="3/22/0"</pre>	szEnd="9/22/0" s	zOffset="60"/>
	<d><dst< th=""><th>szTime="+4"</th><th><pre>szZone="Armenia(Yerevan)" iType="1" szStart="3/5/7/2"</pre></th><th>szEnd="10/5/7/3"</th><th>szOffset="60"/&gt;</th></dst<></d>	szTime="+4"	<pre>szZone="Armenia(Yerevan)" iType="1" szStart="3/5/7/2"</pre>	szEnd="10/5/7/3"	szOffset="60"/>
	<dst< th=""><th>szTime="+4"</th><th>szZone="Azerbaijan(Baku)" iType="1" szStart="3/5/7/4"</th><th>szEnd="10/5/7/5"</th><th>szOffset="60"/&gt;</th></dst<>	szTime="+4"	szZone="Azerbaijan(Baku)" iType="1" szStart="3/5/7/4"	szEnd="10/5/7/5"	szOffset="60"/>
	<dst< s=""></dst<>	szTime="+4"	szZone="Georgia(Tbilisi)" />		
	<dstd><dstd><dstd></dstd></dstd></dstd>	szTime="+4"	szZone="Kazakhstan(Aktau)" />		
	<dst< th=""><th>szTime="+4"</th><th>szZone="Russia(Samara)" /&gt;</th><th></th><th></th></dst<>	szTime="+4"	szZone="Russia(Samara)" />		
	<dst< th=""><th>szTime="+4:30"</th><th>szZone="Afghanistan(Kabul)"/&gt; Modify it:</th><th></th><th></th></dst<>	szTime="+4:30"	szZone="Afghanistan(Kabul)"/> Modify it:		
	<dst< th=""><th>szTime="+5"</th><th>szZone="Kazakhstan (Aqtobe) "/&gt; iType="1" szStart="10/1/7/2" szEnd="</th><th>'4/1/7/3" szOffset="60"</th><th></th></dst<>	szTime="+5"	szZone="Kazakhstan (Aqtobe) "/> iType="1" szStart="10/1/7/2" szEnd="	'4/1/7/3" szOffset="60"	
	<dst< th=""><th>szTime="+5"</th><th>szZone="Kyrgyzstan(Bishkek)" /&gt;</th><th></th><th></th></dst<>	szTime="+5"	szZone="Kyrgyzstan(Bishkek)" />		
	<dst< th=""><th>szTime="+5"</th><th><pre>szZone="Pakistan(Islamabad)" iType="0" szStart="4/15/0"</pre></th><th>szEnd="11/1/0"</th><th>szOffset="60"/&gt;</th></dst<>	szTime="+5"	<pre>szZone="Pakistan(Islamabad)" iType="0" szStart="4/15/0"</pre>	szEnd="11/1/0"	szOffset="60"/>
	<d><dst< td=""></dst<></d>	szTime="+5"	szZone="Russia(Chelyabinsk)" />		
	<dst< s=""></dst<>	szTime="+5:30"	<pre>szZone="India(Calcutta)" iType="1" szStart="9/5/7/3"</pre>	szEnd="4/1/7/2"	szOffset="60"/>
	<dst< s=""></dst<>	szTime="+5:45"	szZone="Nepal (Katmandu) "/>		
	<d>ST</d>	szTime="+6"	szZone="Kazakhstan (Astana, Almaty) "/>	La cat	
	<dst< th=""><th>szTime="+6"</th><th>szZone="Russia(Novosibirsk,Omsk)" /&gt;</th><th>I DST 7</th><th></th></dst<>	szTime="+6"	szZone="Russia(Novosibirsk,Omsk)" />	I DST 7	
	<dst< th=""><th>szTime="+6:30"</th><th>szZone="Myanmar(Naypyitaw)" /&gt;</th><th></th><th></th></dst<>	szTime="+6:30"	szZone="Myanmar(Naypyitaw)" />		
	<dot <="" statement="" td=""></dot>	szTime="+7"	szZone="Russia(Krasnoyarsk)" />		
	<dst< th=""><th>szTime="+7"</th><th>szZone="Thailand(Bangkok)"/&gt;</th><th></th><th></th></dst<>	szTime="+7"	szZone="Thailand(Bangkok)"/>		
	<dst< th=""><th>szTime="+8"</th><th>szZone="China(Beijing)"/&gt;</th><th></th><th></th></dst<>	szTime="+8"	szZone="China(Beijing)"/>		
	<d>ST</d>	szTime="+8"	<pre>szZone="Singapore(Singapore)" /&gt;</pre>		

### Example 2:

Add a new time zone (+6 Paradise) with daylight saving time 30 minutes.

AutoDS	T.xml x	
	10 20	20 40 50 60 70 00 00
CDST	szTime= +4:50	
CDST	szTime-"+5"	SZAONE-"KAZAKASTAI (Adtobe)"/>
CDST	szrime- +5	Szzone- Nyigyzstan (bisnek) //
CDST	szrime= +5	3220 Pakistan (isiamabad) irype-0 $325$ art - 4/13/0 $32$ And - 11/1/0 $3$
CDST	sztime="+5"	
CDST	szTime-"+5:30"	szaone-"India (Calcutta)"/>
CDST	szTime-"+5:45"	
CDOT	szTime- +6 sz	ZZORE FARAISE HType I SZEARC 3/3//2 SZERG 10/3///3 SZORBEC 30 /2
CDAT	szrime= +6	Szzone- Kazakistan (Astana, Aimaty) //
CDST	sztime-"+6"	SZADNE- RUSSIA (NOVOSIDIISK, OMSK) //
CDST	szTime-"+6:30"	szone – Wyanmar (Naypyitaw) //
CDST	szrime-"+/"	SZZONE- KUSSIA (Krasnoyarsk) //
CDST	szrime-"+/"	SZZONE-"TALLANG (BANGKOK)"/>
CDST	szTime="+8"	szZone="China (Beijing)"/>
CDST	szrime-"+8"	szzone-"Singapore (Singapore)" />
<dst< th=""><th>szTime="+8"</th><th>szZone="Australia (Perth)" iType="1" szStart="10/1///2" szEnd="3/5///3" i</th></dst<>	szTime="+8"	szZone="Australia (Perth)" iType="1" szStart="10/1///2" szEnd="3/5///3" i
<dst< th=""><th>szTime="+8"</th><th>szZone="Russia(Irkutsk, Ulan-Ude)"/&gt;</th></dst<>	szTime="+8"	szZone="Russia(Irkutsk, Ulan-Ude)"/>
<dst< th=""><th>szTime="+8:45"</th><th>szione-"Eucla"/&gt;</th></dst<>	szTime="+8:45"	szione-"Eucla"/>
CDST	szTime="+9"	sz2one- Korea (Seoul) "/>
<dst< th=""><th>szTime="+9"</th><th>szZone="Japan (Tokyo)"/&gt;</th></dst<>	szTime="+9"	szZone="Japan (Tokyo)"/>
CDST	szTime="+9"	sz2one="Russia (Yakutsk, Chita)"/>
<dst< th=""><th>szTime="+9:30"</th><th>szZone="Australia (Adelaide)" iType="1" szStart="10/1///2" szEnd="4/1///3</th></dst<>	szTime="+9:30"	szZone="Australia (Adelaide)" iType="1" szStart="10/1///2" szEnd="4/1///3
<dst< th=""><th>szTime="+9:30"</th><th>sz2one="Australia (Darwin)" /&gt;</th></dst<>	szTime="+9:30"	sz2one="Australia (Darwin)" />
<dst< th=""><th>szTime="+10"</th><th><pre>szZone="Australia(Sydney,Melbourne,Canberra)" iType="1" szStart="10/1/7/2"</pre></th></dst<>	szTime="+10"	<pre>szZone="Australia(Sydney,Melbourne,Canberra)" iType="1" szStart="10/1/7/2"</pre>
<dst< th=""><th>szTime="+10"</th><th>sz%one="Australia(Brisbane)"/&gt;</th></dst<>	szTime="+10"	sz%one="Australia(Brisbane)"/>

- 3. Save this file and place it to the provisioning server (e.g., 192.168.1.100).
- 4. Specify the access URL of the AutoDST file in the configuration files.

# Procedure

The access URL of the AutoDST file can be specified using the configuration files.

Configuration File	<mac>.cfg</mac>	Specify the access URL of the AutoDST file. <b>Parameters:</b>
		auto_dst.url

# **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
auto_dst.url	URL within 511 characters	Blank
Description:		
Configures the access URL of the A	utoDST file (AutoDST.xml).	
Example:		
auto_dst.url = tftp://192.168.1.100/AutoDST.xml		
During the auto provisioning process, the IP phone connects to the provisioning		
server "192.168.1.100", and downloads the AutoDST file "AutoDST.xml". After update,		
you will find a new time zone "Paradise" and updated DST of "Pakistan (Islamabad)"		
and "India (Calcutta)" via web user interface: Settings->Time & Date->Time Zone.		
Note: It works only if the value of th	e parameter "local_time.sumi	mer_time" is set to 2

Parameters	Permitted Values	Default
(Automatic).		
Web User Interface:		
None		
Phone User Interface:		
None		

# Language

IP phones support multiple languages. Languages used on the phone user interface and web user interface can be specified respectively as required.

The following table lists languages supported by the phone user interface and the web user interface.

Phone/Web User Interface
English
Chinese Simplified
Chinese Traditional
French
German
Italian
Polish
Portuguese
Spanish
Turkish
Korean (not applicable to phone user
interface of SIP-T40P IP phones)
Russian

# Loading Language Packs

Languages available for selection depend on language packs currently loaded to the IP phone. You can customize the translation of the existing language on the phone user interface or web user interface. You can also make new languages (not included in the available language list) available for use on the phone user interface and web user interface by loading language packs to the IP phone. Language packs can only be loaded using configuration files.

You can ask the distributor or Yealink FAE for language packs. You can also obtain the

language packs online:

http://www.yealink.com/solution\_info.aspx?ProductsCateID=1248&cateid=1248&BaseI nfoCateId=1328&Cate\_Id=1248&parentcateid=1328.

For more information on obtaining the language packs, refer to Obtaining Configuration Files and Resource Files on page 36.

Note

To modify translation of an existing language, do not rename the language file.

The new added language must be supported by the font library on the IP phone. If the characters in the custom language file are not supported by the IP phone, the IP phone will display "?" instead.

## Customizing a Language for Phone User Interface

The following table lists the available languages and associated language packs for the phone user interface:

Available Language	Associated Language Pack
English	000.GUI.English.lang
Chinese Simplified	001.GUI.Chinese_S.lang
Chinese Traditional	002.GUI.Chinese_T.lang
French	003.GUI.French.lang
German	004.GUI.German.lang
Italian	005.GUI.Italian.lang
Polish	006.GUI.Polish.lang
Portuguese	007.GUI.Portuguese.lang
Spanish	008.GUI.Spanish.lang
Turkish	009.GUI.Turkish.lang
Korean	010.GUI.Korean.lang
Russian	011.GUI.Russian.lang

When adding a new language pack for the phone user interface, the language pack must be formatted as "X.GUI.name.lang" (X starts from 012, "name" is replaced with the language name). If the language name is the same as the existing one, the existing language pack will be overridden by the new uploaded one. We recommend that the filename of the new language pack should not be the same as the existing one.

### To customize a language file:

1. Open the desired language template file (e.g., 000.GUI.English.lang) using an ASCII editor.

2. Modify the characters within the double quotation marks on the right of the equal sign. Don't modify the translation item on the left of the equal sign.

The following shows a portion of the language pack "000.GUI.English.lang" for the phone user interface (take SIP-T46G IP phones for example):

/	000.GUI.English.lang ×
	0, , , , , , , , , , , , , , , , , , ,
1	[ Lang ]
2	Modity the item
3	" Conference "="Conference " (e.g., conference).
4	"'*' or '#' as send"="Key as send"
5	"(Empty) "=" (Empty) "
6	"12 Hour"="12 Hour"
7	"120s"="120s"
8	"15s"="15s"
9	"1800s"="1800s"
10	"24 Hour"="24 Hour"
11	"300s"="300s"
12	"30s"="30s"
13	"600s"="600s"
14	"60s"="60s"
15	"802.1x Mode"="802.1x Mode"
16	"802.1x Settings"="802.1x Settings"

- 3. Save the language file and place it to the provisioning server (e.g., 192.168.10.25).
- 4. Specify the access URL of the phone user interface language pack in the configuration files.

If you want to add a new custom language (e.g., Guilan) to your IP phone (e.g., SIP-T46G), prepare the language file named as "011.GUI.Guilan.lang" for downloading. After update, you will find a new language selection "Guilan" on the phone user interface: **Menu->Basic->Language**.

## Procedure

Loading language pack can only be performed using the configuration files.

Configuration File		Specify the access URL of the phone user interface language pack.
	<y000000000xx>.cfg</y000000000xx>	Parameter:
		gui_lang.url
		Delete custom LCD
		language packs of the
		phone user interface.
		Parameter:
		gui_lang.delete

# Details of the Configuration Parameter:

Permitted Values	Default		
URL within 511 characters	Blank		
Description: Configures the access URL of the custom LCD language pack for the phone user interface. Example: gui_lang.url = http://192.168.10.25/000.GUI.English.lang During the auto provisioning process, the IP phone connects to the HTTP provisioning server "192.168.10.25", and downloads the language pack "000.GUI.English.lang". The English language translation will be changed accordingly if you have modified the language template file. If you want to download multiple language packs to the IP phone simultaneously,			
<pre>gui_lang.url = http://192.168.10.25/000.GUI.English.lang gui_lang.url = http://192.168.10.25/001.GUI.Chinese_S.lang Web User Interface: None Phone User Interface: None</pre>			
http://localhost/all or http://localhost/Y.GUI.na me.lang	Blank		
Description:         Deletes the specified or all custom LCD language packs of the phone user interface.         Example:         Delete all custom language packs of the phone user interface:         gui_lang.delete = http://localhost/all         Delete a custom language pack of the phone user interface (e.g., 001.GUI.Chinese_S.lang):         gui_lang.delete = http://localhost/001.GUI.Chinese_S.lang         Web User Interface:         None         Phone User Interface:			
	Permitted Values         URL within 511 characters         D language pack for the phonon         nglish.lang         phone connects to the HTTP properties         anguage pack "000.GUI.Englishing         nglish.lang         hangs         packs to the IP phone simulta         nglish.lang         thinese_S.lang         http://localhost/all or         http://localhost/Y.GUI.na         me.lang         uage packs of the phone use         one user interface:         ne user interface (e.g.,         thinese_S.lang		

Parameter	Permitted Values	Default
None		

# Customizing a Language for Web User Interface

The following table lists available languages and associated language packs for the web user interface:

Available Language	Associated Language Pack
English	1.English.js
Chinese Simplified	2.Chinese_S.js
Chinese Traditional	3.Chinese_T.js
French	4.French.js
German	5.German.js
Italian	6.Italian.js
Polish	7.Polish.js
Portuguese	8.Portuguese.js
Spanish	9.Spanish.js
Turkish	10.Turkish.js
Korean	11.Korean.js
Russian	12.Russian.js

When adding a new language pack for the web user interface, the language pack must be formatted as "Y.name.js" (Y starts from 13, "name" is replaced with the language name). If the language name is the same as the existing one, the existing language file will be overridden by the new uploaded one. We recommend that the name of the new language file should not be the same as the existing languages.

## To customize a language file:

- 1. Open the desired language template file (e.g., 1.English.js) using an ASCII editor.
- Modify the characters within the double quotation marks on the right of the colon. Don't modify the translation item on the left of the colon.

The following shows a portion of the language pack "1.English.js" for the web user interface (take SIP-T46G IP phones for example):



- 3. Save the language file and place it to the provisioning server (e.g., 192.168.10.25).
- **4.** Specify the access URL of the web user interface language pack in the configuration files.

If you want to add a new language (e.g., Wuilan) to IP phones, prepare the language file named as "13.Wuilan.js" for downloading. After update, you will find a new language selection "Wuilan" on the web user interface:

## Settings->Preference->Language.

## Procedure

Loading language pack can only be performed using the configuration files.

	<y000000000xx>.cfg</y000000000xx>	Specify the access URL of the custom language pack for web user interface.
		Parameter:
Configuration File		wui_lang.url
		Delete custom language
		packs of the web user
		interface.
		Parameter:
		wui_lang.delete

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default
wui_lang.url	URL within 511 characters	Blank

Parameter	Permitted Values	Default		
Description:	Description:			
Configures the access URL of the custom lar	nguage pack for the web user	interface.		
Example:				
wui_lang.url = http://192.168.10.25/1.English.	S			
During the auto provisioning process, the IP phone connects to the HTTP provisioning server "192.168.10.25", and downloads the language pack "1.English.js". The English language translation will be changed accordingly if you have modified the language template file.				
If you want to download multiple language packs to the web user interface simultaneously, you can configure as following:				
wui_lang.url = http://192.168.10.25/1.English.	s			
wui_lang.url = http://192.168.10.25/11.Russian	n.js			
Web User Interface:				
None				
Phone User Interface:				
None				
wui_lang.delete	http://localhost/all or http://localhost/Y. <i>name.js</i>	Blank		
Description:				
Delete the specified or all custom web lang	uage packs of the web user ir	nterface.		
Example:				
Delete all custom language packs of the we	eb user interface:			
wui_lang.delete = http://localhost/all				
Delete a custom language pack of the web user interface (e.g., 11.Russian.js):				
wui_lang.delete = http://localhost/11.Russian.js				
Web User Interface:	Web User Interface:			
None				
Phone User Interface:				
None				

# Specifying the Language to Use

The default language used on the phone user interface is English. If the language of your web browser is not supported by the IP phone, the web user interface will use English by default. You can specify the languages for the phone user interface and

web user interface respectively.

## Procedure

Specify the language for the phone user interface or the web user interface using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Specify the languages for the phone user interface and the web user interface. <b>Parameters:</b> lang.gui
		lang.wui
		Specify the language for the web user interface.
Local	Web User Interface	<b>Navigate to</b> : http:// <phonelpaddress>/servlet</phonelpaddress>
		<pre>?p=settings-preference&amp;q=load</pre>
	Phone User Interface	Specify the language for the phone user interface.

# Details of Configuration Parameters:

Parameters	Permitted Values	Default	
lang.gui	Refer to the following content Englis		
Description:			
Configures the language used on th	e phone user interface.		
Permitted Values:			
English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Korean, Russian or the custom language name.			
Example:			
lang.gui = English			
If you want to use the custom language (e.g., Guilan) for the IP phone, configure the parameter "lang.gui = Guilan".			
Web User Interface:			
None			
Phone User Interface:			
Menu->Basic->Language			
lang.wui	Refer to the following content	English	

Parameters	Permitted Values	Default	
Description:			
Configures the language used on th	e web user interface.		
Permitted Values:			
English, Chinese Simplified, Chinese Traditional, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Korean, Russian or the custom language name.			
Example:			
lang.wui = English			
<b>Note</b> : If the language of your browser is not supported by the IP phone, the web user interface will use English by default.			
Web User Interface:			
Settings->Preference->Language			
Phone User Interface:			
None			

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

- 1. Click on Settings->Preference.
- 2. Select the desired language from the pull-down list of Language.

				Log Out
Yealink T46G	Status Account Network	Features Settings	Directory	Security
Preference	Language	English (English)		NOTE
Time & Date	Live Dialpad Backlight Inactive Level	简体中文(Chinese Simplified) 繁体中文(Chinese Traditional)		Preference Settings The preference settings for
Upgrade	Backlight Active Level	Deutsch (German)		administrator.
Auto Provision	Watch Dog	Polski (Polish) Português (Portuguese)		You can click here to get more guides.
Configuration	Ring Type	español (Spanish) türkce (Turkish)		
Dial Plan	Upload Ringtone	한국어 (Korean) Russian (Россия) Upload Cancel	0	
Voice	Confirm	Cancel		
Tones				

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

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

- 1. Press Menu->Basic->Language.
- 2. Press  $\bigcirc$  or  $\bigcirc$  to select the desired language.
- 3. Press the Save soft key to accept the change.

# Key As Send

Key as send allows assigning the pound key or asterisk key as the send key.

Send sound allows the IP phone to play a key tone when a user presses the send key. Key tone allows the IP phone to play a key tone when a user presses any key. Send sound works only if key tone is enabled. Key tone is enabled by default.

# Procedure

Key as send can be configured using the configuration files or locally.

		Configure a send key.
		Parameter:
		features.key_as_send
		Configure send pound key.
		Parameter:
Configuration File	(1/000000000000000000000000000000000000	features.send_pound_key
Configuration File	<y000000000xx>.cig</y000000000xx>	Configure a send sound.
		Parameter:
		features.send_key_tone
		Configure a key tone.
		Parameter:
		features.key_tone
		Configure a send key.
		Configure send pound key.
		Navigate to:
	Web User Interface	http:// <phonelpaddress>/servlet</phonelpaddress>
		?p=features-general&q=load
		Configure a send sound and key
Local		tone.
		Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		?p=features-audio&q=load
	Phone Uper Interface	Configure a send key.
		Configure a key tone.

# Details of Configuration Parameters:

Parameters	Permitted Values	Default			
features.key_as_send	0, 1 or 2	1			
Description:					
Configures the "#" or "*" key as the send key.					
0-Disabled					
1-# key					
<b>2</b> -* key					
If it is set to 0 (Disabled), neither "#" nor "*" can be use	ed as a send key.				
If it is set to 1 (# key), the pound key is used as the send	d key.				
If it is set to 2 (* key), the asterisk key is used as the send	d key.				
Web User Interface:					
Features->General Information->Key As Send					
Phone User Interface:					
Menu->Features->Key as Send					
features.send_pound_key	0 or 1	0			
Description:					
Enables or disables the IP phone to not send any poun #.	d key when pressing	g double			
<b>0</b> -Disabled (Send one pound key by pressing double #	)				
1-Enabled (Do not send any pound key when pressing	double #)				
<b>Note</b> : It works only if the value of the parameter "featu (Enabled)	res.key_as_send" is	set to 1			
Footures Scoperal Information Sound Pound Key					
Phone liser interface:					
Nono					
features.key_tone	0 or 1	1			
Description:					
Enables or disables the IP phone to play a key tone when a user presses any key on					
your phone keypad.					
0-Disabled					
1-Enabled					

Parameters Permitted Values Defaul						
If it is set to 1 (Enabled), the IP phone will play a key tone when a user presses any						
key on your phone keypad.						
Web User Interface:						
Features->Audio->Key Tone						
Phone User Interface:						
None						
features.send_key_tone	0 or 1	1				
Description:						
Enables or disables the IP phone to play a key tone wh	nen a user presses a	send key.				
0-Disabled						
1-Enabled						
If it is set to 1 (Enabled), the IP phone will play a key tone when a user presses a send						
key.						
Note: It works only if the value of the parameter "featu	res.key_tone" is set	to 1				
(Enabled).						
Web User Interface:						
Features->Audio->Send Sound						
Phone User Interface:						
None						

To configure a send key via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of Key As Send.

Yealink 1466	Status Account Network Feature	s Settings Directory	Log Out
General	General Information 🛛 🕜		NOTE
Audio	Call Waiting Enabled Key As Send #	• Ø	Call Waiting This call feature allows your
Remote Control	Busy Tone Delay (Seconds) 0		phone to accept other incoming calls during the conversation.
Bluetooth	Time-Out for Dial-Now Rule 1	0	Key As Send Select * or # as the send key.
Power LED	Dial Search Delay 1 180 Ring Workaround Disabled	• 0	You can click here to get more guides.
	Save Call Log Enabled	• 0	
	Suppress DTMF Display         Disabled           Suppress DTMF Display Delay         Disabled	• 0	

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

### To configure send pound key via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of Send Pound Key.

				Log Out
Yealink   T46G	Account Network	Features Settin	ngs Directory	Security
General	General Information 🛛 🕜			NOTE
Information	Call Waiting	Enabled 👻	0	o-II werken
Audio	Key As Send	#	0	This call feature allows your
Romoto Control	Busy Tone Delay (Seconds)	0 -	0	phone to accept other incoming calls during the conversation.
Remote Control	Return code when refuse	603 (Decline) 👻	0	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	0	Select * or # as the send key.
Power LED	Dial Search Delay	1	0	You can click here to get
	180 Ring Workaround	Disabled 👻	0	more guides.
	Save Call Log	Enabled 👻	0	
	Suppress DTMF Display	Disabled 👻	0	
	Suppress DTMF Display Delay	Disabled 👻	0	
	Play Local DTMF Tone	Enabled -	0	
	DTMF Repetition	3 -	a	
	Multicast Codec	G722 👻	ã	
	Play Hold Tone	Enabled 👻	a	
	Play Hold Tone Delay	30	a	
	Allow Mute	Enabled -	0	
	Dual-Headset	Disabled -	0	
	Auto-Answer Delay(1~4s)	1	0	
	Headset Prior	- Disabled -	0	
	DTME Penbce Tran	Disabled	•	
	Tran Send DTME		0	
	Send Pound Key	Enabled -	0	

3. Click Confirm to accept the change.

To configure a key tone and a send sound via web user interface:

- 1. Click on Features->Audio.
- 2. Select the desired value from the pull-down list of **Key Tone**.
- 3. Select the desired value from the pull-down list of **Send Sound**.

Voglink		Log Out
	Status Account Network Features Settings Directory	Security
General	Audio Settings	NOTE
Information	Call Waiting Tone Enabled 🔹 🥜	Audia
Audio	Key Tone Enabled - 📀	The audio parameters for
Remote Control	Pre Dial Tone Disabled 🔹 🕜	administrator.
Remote control	Send Sound Enabled - 🕜	You can click here to get more quides.
Bluetooth	Redial Tone 🕜	inere galacer
Power LED	Ringer Device for Headset Use Speaker 🔹 🥝	
	BToE as Audio Device (VDI support) Disabled 🔹 🥝	
	Confirm	

4. Click Confirm to accept the change.

### To configure key as send via phone user interface:

- 1. Press Menu->Features->Key as Send.
- 2. Press (•) or (•), or the Switch soft key to select # or \* from the Key as Send field, or select Disabled to disable this feature.
- 3. Press the Save soft key to accept the change.

# **Dial Plan**

Regular expression, often called a pattern, is an expression that specifies a set of strings. A regular expression provides a concise and flexible means to "match" (specify and recognize) strings of text, such as particular characters, words, or patterns of characters. Regular expression is used by many text editors, utilities, and programming languages to search and manipulate text based on patterns.

Regular expression can be used to define IP phone dial plan. Dial plan is a string of characters that governs the way for IP phones to process the inputs received from the IP phone's keypads. The IP phone can receive dial plan through in-band provisioning.

You need to know the following basic regular expression syntax when creating dial plan:

-	The dot "." can be used as a placeholder or multiple placeholders for any string. Example: "12." would match "12 <b>3</b> ", "12 <b>34</b> ", "12 <b>345</b> ", "12 <b>abc</b> ", etc.
х	The "x" can be used as a placeholder for any character. Example: "12x" would match "12 <b>1</b> ", "12 <b>2</b> ", "12 <b>3</b> ", "12 <b>a</b> ", etc.
-	The dash "-" can be used to match a range of characters within the brackets. Example: "[5-7]" would match the number " <b>5</b> ", " <b>6</b> " or " <b>7</b> ".
,	The comma "," can be used as a separator within the bracket. Example: "[2,5,8]" would match the number " <b>2</b> ", " <b>5</b> " or " <b>8</b> ".
[]	The square bracket "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: "91[5-7]1234"would match "91 <b>5</b> 1234", "91 <b>6</b> 1234", "91 <b>7</b> 1234".
()	The parenthesis "()" can be used to group together patterns, for instance, to logically combine two or more patterns. Example: "([1-9])([2-7])3" would match " <b>92</b> 3", " <b>15</b> 3", " <b>67</b> 3", etc.
\$	The "\$" followed by the sequence number of a parenthesis means the characters placed in the parenthesis. The sequence number

stands for the corresponding parenthesis. Example:
A replace rule configuration, Prefix: "001 (xxx)45(xx)", Replace:
"9001\$145\$2". When you dial out "0012354599" on your phone, the IP
phone will replace the number with "9001 <b>235</b> 45 <b>99</b> ". "\$1" means 3
digits in the first parenthesis, that is, "235". "\$2" means 2 digits in the
second parenthesis, that is, "99".

# **Dial-now**

Dial-now is a string used to match numbers entered by the user. When entered numbers match the predefined dial-now rule, the IP phone will automatically dial out the numbers without pressing the send key. IP phones support up to 100 dial-now rules, which can be created either one by one or in batch using a dial-now rule template. For more information on how to customize a dial-now template, refer to Customizing Dial-now Template File on page 137.

# Delay Time for Dial-now Rule

The IP phone will automatically dial out the entered number, which matches the dial-now rule, after a specified period of time.

## Procedure

Dial-now rule can be created using the configuration files or locally.

		Create the dial-now rule for the IP phone.	
		Parameters:	
Configuration File	<y000000000xx>.cfg</y000000000xx>	dialplan.dialnow.rule.X	
		Configure the delay time for the dial-now rule.	
		Parameters:	
		phone_setting.dialnow_delay	
		Create the dial-now rule for the	
		IP phone.	
		Navigate to:	
		http:// <phonelpaddress>/servlet</phonelpaddress>	
Local	Web User Interface	<pre>?p=settings-dialnow&amp;q=load</pre>	
		Configure the delay time for the	
		dial-now rule.	
		Navigate to:	
		http:// <phonelpaddress>/servlet</phonelpaddress>	

		<pre>?p=features-general&amp;q=load</pre>
--	--	---

# Details of Configuration Parameters:

Parameters	Permitted Values Defau				
dialplan.dialnow.rule.X	String within 511 observators	Plank			
(X ranges from 1 to 100)		DIGITIK			
Description:					
Configures the dial-now rule (the stri user).	ing used to match the numbers ente	ered by the			
When entered numbers match the pautomatically dial out the numbers	predefined dial-now rule, the IP photo without pressing the send key.	ne will			
Example:					
dialplan.dialnow.rule.1 = 123					
Web User Interface:					
Settings->Dial Plan->Dial-now->Rule					
Phone User Interface:					
None					
phone_setting.dialnow_delay Integer from 1 to 14 1					
Description:					
Configures the delay time (in secon	ds) for the dial-now rule.				
When entered numbers match the predefined dial-now rule, the IP phone will automatically dial out the entered number after the designated delay time.					
Web User Interface:					
Features->General Information->Time-Out for Dial-Now Rule					
Phone User Interface:					
None					

## To create a dial-now rule via web user interface:

1. Click on Settings->Dial Plan->Dial-now.

2. Enter the desired value in the Rule field.

							Log_Out
YEAIINK   146G	Status	Account	Network	Features	Settings	Directory	Security
Preference	Dial-now						NOTE
Time&Date	Index		Dial-no	w Rule			settings-dialplan-note
	1						<b>B</b>
Upgrade	2						M You can click here to get more guides.
Auto Provision	3						
Configuration	4						
	5						
Dial Plan	6						
Voice	7						
Tones	8						
TORES	9						
Phone Lock	10						
Location							
EXP Module			Rule 1xxx				
BTOE							
		Add	I	Edit	Del		

3. Click Add to add the dial-now rule.

To configure the delay time for the dial-now rule via web user interface:

- 1. Click on Features->General Information.
- 2. Enter the desired time within 0-14 (in seconds) in the **Time-Out for Dial-Now Rule** field.

Yealink   1466	Status Account Network	Features Settin	gs Directory	Log Out
General	General Information 🛛			NOTE
Information	Call Waiting	Enabled -	0	Call Waiting
Audio	Key As Send	#	0	This call feature allows your
Remote Control	Busy Tone Delay (Seconds)	0 🔹	0	calls during the conversation.
	Return code when refuse	603 (Decline) -	0	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	0	Select * or # as the send key.
Power LED	Dial Search Delay	1	0	You can click here to get
	180 Ring Workaround	Disabled 👻	0	more guides.

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

## **Customizing Dial-now Template File**

The dial-now template helps with the creation of multiple dial-now rules. After setup, place the dial-now template to the provisioning server and specify the access URL in the configuration files.

You can ask the distributor or Yealink FAE for dial-now template. You can also obtain the dial-now template online:

http://www.yealink.com/solution\_info.aspx?ProductsCateID=1248&cateid=1248&BaseInfoC ateId=1328&Cate\_Id=1248&parentcateid=1328. For more information on obtaining the

dial-now template, refer to Obtaining Configuration Files and Resource Files on page 36.

When editing a dial-now template, learn the following:

- <DialNow> indicates the start of a template and </DialNow> indicates the end of a template.
- When specifying the line for the dial-now rule, the valid value is 0 or 1. No matter you leave it blank or set it to 0 or 1, the dial-now rule will all be applied to account 1.
- At most 100 rules can be added to the IP phone.

The expression syntax in the dial-now rule template is the same as that introduced in the section Dial Plan on page 134.

### To customize a dial-now template:

- 1. Open the template file using an ASCII editor.
- 2. Create dial-now rules between <DialNow> and </DialNow>.

### For example:

<data DialNowRule="99" LineID="1" />

Where:

DialNowRule="" specifies the dial-now rule.

LineID="" specifies the desired line for this rule. When you leave it blank or enter 0 or enter 1, this dial-now rule will all apply to account 1.

xml version="1.0" encoding="UTF-8"?
<dialnow></dialnow>
<pre><data dialnowrule="11" lineid="1"></data></pre>
<data dialnowrule="22" lineid=""></data>
<pre><data dialnowrule="*xx" lineid="1"></data></pre>
<pre><data dialnowrule="#xx" lineid="1"></data></pre>
<pre><data dialnowrule="000" lineid="1"></data></pre>
<pre><data dialnowrule="106" lineid="1"></data></pre>
<pre><data dialnowrule="101" lineid="1"></data></pre>
<pre><data dialnowrule="11xx" lineid="1"></data></pre>
<pre><data dialnowrule="12[23]x" lineid="1"></data></pre>
<pre><data dialnowrule="124xx" lineid="1"></data></pre>
<pre><data dialnowrule="1251xx" lineid="1"></data></pre>
<pre><data dialnowrule="1[38]xxxxxxxx" lineid="1"></data></pre>
<pre><data dialnowrule="13[1-9]xxx" lineid="1"></data></pre>
<pre><data dialnowrule="1345xxxx" lineid="1"></data></pre>
<pre><data dialnowrule="0[2-9]xxxxxxx" lineid="1"></data></pre>
<pre><data dialnowrule="2xxx" lineid="1"></data></pre>
<pre><data dialnowrule="[3-9]xxxxxxx" lineid="1"></data></pre>
<data dialnowrule="99" lineid="1"></data> 🔨
Add a new dial-now rule

If you want to change the dial-now rule, specify the values within double quotes.

- 3. Save the change and place this file to the provisioning server.
- **4.** Specify the access URL of the dial-now template.

## Procedure

Specify the access URL of the dial-now template using configuration files.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure the access URL of the dial-now template. Parameter:
		dialplan_dialnow.url

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default		
dialplan_dialnow.url	URL within 511 characters	Blank		
Description:				
Configures the access URL of the dial-now rule template file.				
Example:				
dialplan_dialnow.url = http://192.168.10.25/dialnow.xml				
During the auto provisioning process, the IP phone connects to the provisioning server "192.168.10.25", and downloads the dial-now rule file "dialnow.xml".				
Web User Interface:				
None				
Phone User Interface:				
None				

# Directory

The phone directory displays local contacts and all your Skype for Business contacts. You can view contact information on the IP phone.

Users can access directory lists by pressing the **Directory** or **Dir** soft key when the IP phone is idle. The list includes Skype for Business Directory and Local Directory.

# Skype for Business Directory

The Skype for Business directory on your phone displays all Skype for Business contacts on your Skype for Business client. You can view Skype for Business contacts information on the IP phone, but you cannot add, edit or delete Skype for Business contacts on the IP phone.

### To add contacts via Skype for Business client:

1. Enter a few continuous characters of the contact name or continuous numbers of the contact number in the Search field.

The contacts whose name or phone number matches the characters entered will

appear in your contacts list.

2. Right click the contact, and then click Add to Contacts List.

	Skype for Business 🛛 🗕 🗮 🗙			×
<u>File Meet Now Tools</u>	<u>H</u> elp			
What's happening today?				
Lin Wei Available マ Building 51 マ				
<b>L O</b> <sup>27</sup>	2	ē		¢-
2248				×
MY CONTACTS				
+2248				
+2248				
Merry Inactiv	e 5 mins Voi	e Only		
Vierry - mactiv	Send a	n <u>I</u> M		
	<u>C</u> all		Þ	
	Start a	<u>V</u> ideo Call		
	Send a	n <u>E</u> mail Messa	ge	
	Schedu	I <u>l</u> e a Meeting		
	Сору			
	Find Pi	evious Conver	sations	
Other Contacts	Add t <u>o</u>	Contacts List	► Alesta	
	Lag to	o Drivo cy Polot	e Alerts	
	See Co	ntact Card	ionship v	
	RDING OFF			

3. Select the desired group.

The contact is added to the selected group.

### To view Skype for Business contacts via phone user interface:

1. Press the **Directory** soft key.



2. Select the desired group (e.g., Favorites, Delegates, Bosses or Other Contacts) of Skype for Business directory and then press the **Enter** soft key.

# **Skype for Business Favorites**

You can add your Skype for Business contacts as favorites via your Skype for Business client only.

### To add contacts as favorites via Skype for Business client:

- 1. Right click a contact.
- 2. Click Add to Favorites.



To view Skype for Business favorites via phone user interface:

1. Press Directory-> Favorites.



In addition, Skype for Business favorites of SIP-T48G/T46G/T42G/T41P IP phones are also displayed on the idle screen by default. Skype for Business favorites of SIP-T40P IP phones are displayed in the Skype for Business directory only.

# Local Directory

Yealink IP phones also maintain a local directory. The local directory can store up to 1000 contacts. When adding a contact to the local directory, in addition to name and phone numbers, you can also specify the ring tone and group for the contact. Contacts and groups can be added either one by one or in batch using a local contact file. Yealink IP phones support both \*.xml and \*.csv format contact files, but only support \*.xml format download for local contact file.

## **Customizing a Local Contact File**

You can add contacts one by one on the IP phone directly. You can also add multiple contacts at a time and/or share contacts between IP phones using the local contact template file. After setup, place the template file to the provisioning server and specify the access URL of the template file in the configuration files. The existing local contacts on the IP phones will be overridden by the downloaded local contacts.

You can ask the distributor or Yealink FAE for local contact template. You can also obtain the local contact template online:

http://www.yealink.com/solution\_info.aspx?ProductsCateID=1248&cateid=1248&BaseI nfoCateId=1328&Cate\_Id=1248&parentcateid=1328. For more information on obtaining the local contact file, refer to Obtaining Configuration Files and Resource Files on page 36.

Element	Values	Description
root_group	no	Group list's root element.
group	no	Group's root element.
display_name	All Contacts Favoritelist	An element of group. Group name.
ring Favoritelist Format of the value: System ring tone: Auto Resource:Silent.wav Resource:RingN.wav (integer N ranges from 1 to 8) Custom ring tone:		An element of group. Group ring tone.

The following table lists meaning of each variable in the local contact template file:

Element	Values	Description
root_contact	no	Contact list's root element.
contact	no	Contact's root element.
display_name	String	An element of contact. Contact name. <b>Note</b> : This value cannot be blank or duplicated.
office_number	String	Office number of the contact.
mobile_number	String	Mobile number of the contact.
other_number	String	Other number of the contact.
address	String	Contact's address.
line	<ul> <li>Valid Value: -1 or 0</li> <li>-1 stands for Auto (the first registered line)</li> <li>- 0 stands for line1</li> </ul>	Since the IP phones only support 1 account, so no matter -1 or 0 is selected, the contact will all be added to account 1.
ring	Format of the value: System ring tone: Auto Resource:Silent.wav Resource:Splash.wav Resource:RingN.wav (integer N ranges from 1 to 8) Custom ring tone: Custom:Name.wav	An element of contact. Contact ring tone.
email	String	Contact's email address.
title	String	Contact's title.
priority	For SIP-T48G IP phones:         0~32.         For SIP-T46G IP phones:         0~27.         For SIP-T42G/T41P/T40P IP         phones:         0~15.	It is only applicable to local favorites. Favorites display consecutively, according to their priority. The favorite with the lowest number displays first.
group_id_name	Valid Value: All Contacts, Favoritelist	Group name of a contact.

The following shows the procedure of customizing a local contact file for IP phones:

### To customize a local contact file:

- 1. Open the template file using an ASCII editor.
- 2. For each group that you want to add, add the following string to the file. Each starts on a separate line:

<group display\_name="" ring=""/>

**3.** For each contact that you want to add, add the following string to the file. Each starts on a separate line:

<contact display\_name="" office\_number=" mobile\_number="" other\_number="" address=" " line="" ring="" email="" title="" priority="" group\_id\_name="" />

4. Specify the values within double quotes.

For example:

<contact display\_name="Yealink" office\_number="123" mobile\_number="234" other\_number="345" address="china" line="-1" ring="Auto" email="456@yealink.com" title="manager" priority="0" group\_id\_name="All Contacts" />

```
<root_group>
<group display_name="All Contacts" />
<group display_name="Favoritelist" />
<group display_name="Favoritelist" />
<group />
</root_group>
<croot_group>
<contact>
<contact display_name="Yealink" office_number="123" mobile_number="234" other_number="345" address="china"
line="-1" ring="Auto" email="456@yealink.com" title="manager" priority="0" group_id_name="All Contacts" />
</root_contact></ri>
```

- 5. Save the change and place this file to the provisioning server.
- 6. Specify the access URL of the custom local contact template in the configuration files.

For example:

```
local_contact.data.url = tftp://192.168.10.25/contact.xml
```

During the auto provisioning process, the IP phone connects to the provisioning server "192.168.10.25", and downloads the contact file "contact.xml".

## Procedure

Local directory can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Specify the access URL of the local contact file (*.xml). <b>Parameter:</b> local_contact.data.url
Local	Web User Interface	Add a new contact to the local directory. To import or export the local contact file. <b>Navigate to</b> :
	http:// <phonelpaddress>/servlet ?p=contactsbasic&amp;q=load# =1&amp;group=</phonelpaddress>	
----------------------	--	
Phone User Interface	Add a new contact to the local directory.	

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default						
local_contact.data.url	URL within 511 characters	Blank						
Description:								
Configures the access URL of the local contact file (*.xml).								
Example:								
local_contact.data.url = http://192.168.10.2	25/contact.xml							
Web User Interface:								
Directory->Local Directory->Import Local C	ontact File							
Phone User Interface:								
None								

### To add a contact to the local directory via web user interface:

- 1. Click on Directory->Local Directory.
- 2. In the **Contacts** block, enter name, work number, mobile number, home numbers, email, address and title in the corresponding fields.
- 3. Select the desired ring tone from the pull-down list of Ring Tone.

4. Select All Contacts from the pull-down list of Ring Tone.

Vaalink									Log Out
	Status	Account	Network	Feature	es Set	ttings	Directory	Security	
Local Directory	Index	Name	Work Number	Mobile Number	Home Number	All Con	tacts 👻 🔳	NOTE	
Multicast IP	1 2	Yealink	<u>1234</u>	<u>1213</u>	<u>1234</u>	All Co	ntacts	contactsbasic-ne	ote
Settings	3 4 5							You can clic more guides.	k here to get
	6 7 8								
	9 10								
	Page 1 -	Pre Next	Hang Up	Import Lo	Delete	Move T	o All Contac 👻		
	Name	Yeali	nk	Browse***	No file sele	cted.			
	Work Number Mobile Number	1234		Import XI Browse***	ML Expo	rt XML			
	Home Number	1234	@voolinkus.com	Import C	SV Expo	rt CSV	Show Title		
	Addr	Wan	ghai Road						
	Title Bing Topo	Mana	ger						
	Group	Auto	ontacts 👻						
	Add	E	dit						

5. Click Add to add the contact.

To import an XML contact list file via web user interface:

- 1. Click on Directory->Local Directory.
- 2. Click **Browse** to locate a contact list file (the file format must be \*.xml) from your local system.

								Log Out
Yealink 1466								
	Status	Account	Network	Feature	s Set	tings Direc	tory	Security
Local Directory	Index	Name	Work Number	Mobile Number	Home Number	All Contacts 👻		NOTE
Multimet TD	1	+2224				All Contacts		
MULICAST IP	2	2228				All Contacts		contactsbasic-note
Settings	3	John	800001	800001		Favorites		You can click here to get
g-	4	Martin	800002	800002		Favorites		more guides.
	5	2529	0000000000			Favorites		
	7	80034+iync	890030333			All Contacts		
	/	Row				All Contacts		
	9	Vealink	123	234	345	All Contacts		
	10	T COMIN	122	221	<u></u>	74 Contacto		
	Page 1 -	Pre Next	Hang Up	Delete All	Delete	Move To ALC	ontac 🔻	
	Contacts (?	1		Import Loc	al Contact Fi	le 🕜		
	Name			Browse	contact.xm			
	Work Number			Import XM	L Expor	t XML		
	Mobile Number			Browse	No file selec	ted.		
	Home Number			Import CS	V Expor	t CSV 📃 Show 1	Fitle	
	Email							
	Addr							
	Title							
	Ring Tone	Auto	•					
	Group	All Co	ontacts 👻					
	Add	E	dit					

3. Click Import XML to import the contact list.

The web user interface prompts "The original contact will be covered, Continue?".

4. Click **OK** to complete importing the contact list.

### To import a CSV contact list file via web user interface:

- 1. Click on Directory->Local Directory.
- 2. Click **Browse** to locate a contact list file (the file format must be \*.csv) from your local system.

								Log Out
		Status	Account	Network	Features	Settings	Directory	Security
1	Local Directory	Index	Name	Work Number	Mobile He Number Nu	ome All Cor	ntacts 👻 🔲	NOTE
		1	+2224			All G	ontacts 📃	
	Multicast IP	2	2228			All G	ontacts	contactsbasic-note
		3	John	800001	800001	Fav	vorites 📃	
	Settings	4	Martin	800002	800002	Fav	vorites	You can click here to get
		5	2529			Fav	vorites 📃	more guides.
		6	80034+lync	896636333		All C	ontacts 📃	
		7	Adam			Fav	vorites 📃	
		8	Bay			All C	ontacts	
		9	Yealink	<u>123</u>	234 3	4 <u>5</u> All C	ontacts 📃	
		10						
		Page 1 💌	Pre Next	Hang Up	Delete All De	elete Move	To All Contac 🗸	
								-
		Contacts 🧃			Import Local C	ontact File 🕜		
		Name			Browse N	o file selected.		
		Work Number			Import XML	Export XML		
		Mobile Number			Browse co	ontact.csv		
		Home Number			Import CSV	Export CSV	🗹 Show Title	
		Email						
		Addr						
		Title						
		Ring Tone	Auto	•				
		Group	All Co	ntacts 👻				
		Add	E	dit				

3. (Optional.) Check the Show Title checkbox.

It will prevent importing the title of the contact information which is located in the first line of the CSV file.

- 4. Click Import CSV to import the contact list.
- 5. (Optional.) Mark the On radio box in the Delete Old Contacts field.

It will delete all existing contacts while importing the contact list.

6. Select the contact information you want to import into the local directory from the pull-down list of **Index**.

At least one item should be selected to be imported into the local directory.

Yealink 1466							Log Out
	Status	Acco	unt Netwo	ork Featur	es Setting	Directory	Security
Del Oldcontact   Off  Drewiew  NOTE						NOTE	
	Index displa	y name 🛛 🗸	work number 🗸 🗸	ignore 🗸 🗸	ignore 🗸 🗸	email 🗸 i	
	1 disp	lay_name	office_number	mobile_number	other_number	email	contacts-preview-note
	2	Helen	5563	3221	3214		2 You can disk here to get
	3	May	4321		5555		more quides
	4	Yealink	1234	1213	1234	2299@yealinkuc.com	more guides.

7. Click **Import** to complete importing the contact list.

### To export a contact list via web user interface:

- 1. Click on Directory->Local Directory.
- 2. Click Export XML (or Export CSV).
- 3. Click Save to save the contact list to your local system.

### To add a contact to the local directory via phone user interface:

- 1. Press Directory->Local Directory->All Contacts.
- 2. Press the Add soft key.
- **3.** Enter name, address, work number, mobile number, home number, title and email in the corresponding fields.

	Add (	Contact	
1. Name:		Ĭ	Î
2. Address:			
3. Work Num	ber:		
4. Mobile Nur	mber:		
5. Home Num	nber:		
Back	Abc	Delete	Save

- 4. Press (•) or (•), or the Switch soft key to select the desired ring tone from the Ring field.
- 5. Press the Save soft key to accept the change.
- **Note** If the contact name already exists in the directory, the LCD screen will prompt "Contact name existed!".

## **Local Favorites**

You can add local contacts as favorites on the IP phone. You can also reorder your favorites by assigning the contact a different index number.

### To add a local favorite via web user interface:

- 1. Click on Directory->Local Directory.
- 2. In the **Contacts** block, enter the contact name, office, mobile, other numbers, Email, address and title in the corresponding fields.
- 3. Select the desired ring tone from the pull-down list of **Ring Tone**.
- 4. Select the Favorites group from the pull-down list of Group.
- 5. Enter the index number in the Favorite Index fields.

Vo elimite i							Log Out
YEAIINK   T46G	Status	Account	Network	Features	Settings	Directory	Security
Local Directory	Index	Name	Work Number	Mobile Ho Number Nur	me All Con	tacts 👻 🔲	NOTE
Multicast TD	1						contactsbasic-note
Protector	2						
Settings	4						You can click here to get
	5						more guides.
	6						
	7						
	8						
	9						
		Pro Novt	Hang Up	Delete All Del	lete Move T		
	Page 1 +	Te Next	Hang Op	Delece All Del	Move	All Contac +	
	Contacts 🕜	)		Import Local Co	ontact File 🛛 🕜		
	Name	Merry	,	Browse No	file selected.		
	Work Number	2248	@yealinkuc.com	Import XML	Export XML		
	Mobile Number			Browse No	file selected.		
	Home Number			Import CSV	Export CSV	Show Title	
	Email	2248	@yealinkuc.com				
	Addr						
	Title	Mana	ger				
	Favorite Index	2					
	Ring Tone	Auto	•				
	Group	Favor	ites 🔻				
	Add	E	dit				

Favorites display consecutively, according to their index numbers. The contact with the lowest number displays first.

6. Click Add to add the contact.

#### To add a local favorite via phone user interface:

- 1. Press Directory->Local Directory->Favorites.
- 2. Press Add soft key.
- **3.** Enter the contact name, address, work number, mobile number, home number, title and email in the corresponding fields.

	Add (	Contact	
1. Name:			ĵ
2. Address:			
3. Work Numb	er:		
4. Mobile Num	nber:		
5. Home Num	ber:		~
Back	Abc	Delete	Save

- 4. Press (•) or (•), or the Switch soft key to select the desired ring tone from the Ring field.
- 5. Press () or (), or the Switch soft key to select the index number from the Index field.

The contact with the lowest priority number displays first. For more information on the number of priority, refer to priority on page143.

6. Press the Save soft key to accept the change.

## **Managing Local Favorites**

Local favorites and Skype for Business favorites of SIP-T48G/T46G/T42G/T41P IP phones are displayed on the idle screen. By default, local favorites are displayed before the Skype for Business favorites.

You can configure whether to display local favorites on the idle screen and configure the display order of the local favorites. This feature is not applicable to SIP-T40P IP phones.

For example: Alex, John, Martin and Mike are your local favorites, 2224-cgc, 2228, 80045 and William are your Skype for Business favorites.

### For SIP-T48G:

Local favorite is indicated by an 😭 icon. The following figure shows a sample Favorites list.



When the number of favorite contacts is more than 8, the page switch keys will appear on the right side of the Favorites screen. You can tap  $\checkmark$  or  $\checkmark$  to turn pages to view other favorites.

### For SIP-T46G:

Local favorite is indicated by an **o** icon. The following figure shows a sample Favorites list.

	18 13 I	ri Nov 06	
Hedy Alex John Martin	Line Local S Favorites	kype for Business <del>&lt;</del> Favorites 227	2224-cgc 2228 80045 William
i Status	History	La Directory	•••Menu

When the number of favorite contacts is more than 9, the line key located in the bottom right corner of the screen will be used to turn pages. Press it to view other favorites.

### For SIP-T42G/T41P:

Local favorite is indicated by an + icon. The following figure shows a sample Favorites list.

Line 🗲	∎Hedy	10:0859	★Martin
Local 🧹	★ Ale×	Mon Nov 09	<b>★</b> Mike
Favorites	🗙 John	+2227	12
	Status	History Directory	Menu

When the number of favorite contacts is more than 5, the line key located in the bottom right corner of the screen will be used to turn pages. Press it to view other favorites.



Note Only Skype for Business favorites have presence status.

### Procedure

Local favorites can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure whether to display local favorites on the idle screen.
--------------------	-----------------------------------	--

		Parameter:
		sfb.local_favorite.enable
		Configure the display order of
		the local favorites on the idle
		screen.
		Parameter:
		sfb.local_favorite.sort
		Configure whether to display
		local favorites on the idle screen.
		Configure the display order of
local	Wah User Interface	the local favorites on the idle
Local	Web user menuce	screen.
		Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		2n-contacts-settings8 a-load

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default	
sfb.local_favorite.enable	0 or 1	1	
Description:			
Enables or disables the IP phone to display local favori	tes on the idle scree	en.	
0-Disabled			
1-Enabled			
If it is set to 0 (Disabled), only Skype for Business favorite	es are displayed on	the idle	
screen.			
Note: It is only applicable to SIP-T48G/T46G/T42G/T41P	IP phones.		
Web User Interface:			
Directory->Settings->Local Favorite			
Phone User Interface:			
None			
Parameter	Permitted Values	Default	
sfb.local_favorite.sort	1 or 2	1	
Description:			
Configures the order of the local favorites on the idle screen.			

Parameter	Permitted Values	Default	
1-Preferential			
2-General			
If it is set to 1 (Preferential), the local favorites will be di Business favorites on the idle screen.	splayed before the	Skype for	
If it is set to 2 (General), the local favorites will be displa	ayed behind the Sky	pe for	
Business favorites on the idle screen.	Business favorites on the idle screen.		
<b>Note</b> : It works only if the value of the parameter "sfb.local_favorite.enable" is set to (Enabled). And it is only applicable to SIP-T48G/T46G/T42G/T41P IP phones.			
Web User Interface:			
Directory->Settings->Local Favorite			
Phone User Interface:			
None			

To configure the display order of local favorites via web user interface:

- 1. Click on Directory>Settings.
- 2. Select the desired value from the pull-down list of Local Favorite.
- 3. Depending on your selection:
  - If **Disabled** is selected, only Skype for Business favorites are displayed on the idle screen.
  - If **Preferential** is selected, local favorites will be displayed before the Skype for Business favorites on the idle screen.
  - If **General** is selected, the local favorites will be displayed behind the Skype for Business favorites on the idle screen.

Veglink							Log Out
	Status	Account	Network	Features	Settings	Directory	Security
Local Directory Multicast IP		Local Favorite	m	Preferential	Cancel		NOTE contacts-lync-note
Settings							more guides.

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

# Saving Call Log

Call log contains call information such as remote party identification, time and date, and call duration. It can be used to redial previous outgoing calls, return incoming calls, and save contact information from call log lists to the contact directory.

IP phones maintain a local call log. Call log consists of four lists: Missed Calls, Placed

Calls, Received Calls, and Forwarded Calls (Forwarded Calls are not applicable to SIP-T48G IP phones). Each call log list supports up to 100 entries. To store call information, you must enable save call log feature in advance. You can access the call history information via phone user interface only.

## Procedure

Call log can be configured using the configuration files or locally.

		Configure call log feature.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameter:
		features.save_call_history
Local		Configure call log feature.
	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		<pre>?p=features-general&amp;q=load</pre>
	Phone User Interface	Configure call log feature.

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default	
features.save_call_history	0 or 1	1	
Description:			
Enables or disables the IP phone to save the call log.			
0-Disabled			
1-Enabled			
If it is set to 0 (Disabled), the IP phone cannot save the missed calls, placed calls, received calls and the forwarded calls in the call log lists.			
Web User Interface:			
Features->General Information->Save Call Log			
Phone User Interface:			
Menu->Features->History Setting->History Record			

### To save call log feature via web user interface:

1. Click on Features->General Information.

2. Select the desired value from the pull-down list of Save Call Log.

Yealink   1466	Status Account Network	Features Settings	Log Out
General	General Information 🛛 🕜		NOTE
Information	Call Waiting	Enabled 🔹 🥜	
Audio	Key As Send	# • ?	Call Waiting This call feature allows your
Pemote Control	Busy Tone Delay (Seconds)	0 🔹 🥝	calls during the conversation.
Keniote control	Return code when refuse	603 (Decline) 🔹 🥜	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	Select * or # as the send key.
Power LED	Dial Search Delay	1	You can click here to get
	180 Ring Workaround	Disabled 👻 🥜	more guides.
	Save Call Log	Enabled 🔹 🥜	
	Suppress DTMF Display	Disabled 👻 🥜	
	Suppress DTMF Display Delay	Disabled 👻 🥜	
	Play Local DTMF Tone	Enabled 👻 🥜	

3. Click Confirm to accept the change.

#### To configure call log feature via phone user interface:

- 1. Press Menu->Features->History Setting.
- Press (•) or (•), or the Switch soft key to select the desired value from the History Record field.
- 3. Press the Save soft key to accept the change.

User or administrator can access call logs by downloading them to the local system for diagnosis purpose.

#### To export the call logs via web user interface:

- 1. Click on Settings->Configuration.
- 2. Click **Export** to open file download window, and then save the file to your local system.

Varlink			Log Out
	Status Account Network	Features Settings Directory	Security
Preference	Export or Import Configuration	Browse No file selected.	NOTE
Time&Date		Import Export	Configuration
Upgrade	Export Call Log	Evoort	for administrator.
Auto Provision	Export call Edg		You can click here to get more guides.
Configuration	Pcap Feature	Start Stop Export ?	
Dial Plan	Export System Log	🖲 Local 🔘 Server 🕜	
Voice		Export	
Tones	System Log Level	3 👻 😮	
Phone Lock	Confirm	Cancel	
Location			
EXP Module			
ВТОЕ			

### To view the call logs on your local system:

- 1. Open the folder where you save the call logs.
- 2. Double-click the call logs file that is in .xml format.

The following figure shows a portion of a call logs file:

	6
C C C C C C C C C C C C C C C C C C C	A ★ Ø
Contraction Contraction Contraction	0
xml version="1.0" encoding="UTF-8"?	
<pre>- <root_call_log></root_call_log></pre>	
<item born_tick="1447692969" local_sig<="" remote_display_name="2224-cgc" remote_sip_name="2224" remote_sip_server="yealinkuc.com" td=""><td>ip_server="yealinkuc.com" local_sip_name="2227"</td></item>	ip_server="yealinkuc.com" local_sip_name="2227"
duration="0" type="3"/>	
<item born_tick="1447623292" local_sip<="" remote_display_name="Lin Wei" remote_sip_name="+2216" remote_sip_server="yealinkuc.com" td=""><td>ip_server="yealinkuc.com" local_sip_name="2227"</td></item>	ip_server="yealinkuc.com" local_sip_name="2227"
duration="56" type="1"/>	
<item born_trick="1447623275" local_sip<="" remote_display_name="Lin Wei" remote_sip_name="+2216" remote_sip_server="yealinkuc.com" td=""><td>ip_server="yealinkuc.com" local_sip_name="2227"</td></item>	ip_server="yealinkuc.com" local_sip_name="2227"
duration="0" type="1"/>	
<item born_tick="1447623242" local_sip<="" remote_display_name="Lin Wei" remote_sip_name="+2216" remote_sip_server="yealinkuc.com" td=""><td>ip_server="yealinkuc.com" local_sip_name="2227"</td></item>	ip_server="yealinkuc.com" local_sip_name="2227"
uurauone 6 (ypee 1 />	is second busylinking comit least sin same-"2222"
durational "3" two = 1"/o = 2".	p_server= yeannkuc.com local_sip_name= 2227
citem horn tick="1447429356" remote sin server="vealinkuc.com" remote sin name="2216" remote display name="1 in Wei" local sin	server="yealinkuc.com" local_sin_name="2227"
duration="0" type="3"/>	
<item <="" born_tick="1447426426" remote="" sip_name="2227@yealinkuc.com:opague=app:voicemail" sip_server="yealinkuc.com" td=""><td>remote display name="Message Center"</td></item>	remote display name="Message Center"
local_sip_server="yealinkuc.com" local_sip_name="2227" duration="0" type="1"/>	

# Missed Call Log

Missed call log allows the IP phone to display the number of missed calls with an indicator icon on the idle screen, and to log missed calls in the Missed Calls list when the IP phone misses calls. It is configurable on a per-line basis. Once the user accesses the Missed Calls list, the prompt message and indicator icon on the idle screen disappear.

## Procedure

Missed call log can be configured using the configuration files or locally.

		Configure missed call log feature.
<b>Configuration File</b>	<mac>.cfg</mac>	Parameter:
		account.1.missed_calllog
Local		Configure missed call log feature.
	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		<pre>?p=account-basic&amp;q=load&amp;acc</pre>
		=0

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.1.missed_calllog	0 or 1	1
<b>Description:</b> Enables or disables the IP phone to indicate and recor account.	rd missed calls for th	е
0-Disabled		

Parameter	Permitted Values	Default	
1-Enabled			
If it is set to 0 (Disabled), the IP phone does not display and log the missed call in the Missed Calls list when mis	indicator on the idle ssed calls.	e screen	
If it is set to 1 (Enabled), the IP phone displays a message the missed call in the Missed Calls list when missed call	If it is set to 1 (Enabled), the IP phone displays a message on the idle screen and logs the missed call in the Missed Calls list when missed calls.		
<b>Note:</b> It works only if the value of the parameter "features.save_call_history" is set to 1 (Enabled).			
Web User Interface:			
Account->Basic->Missed Call Log			
Phone User Interface:			
None			

To configure missed call log via web user interface:

- 1. Click on Account->Basic.
- 2. Select the desired value from the pull-down list of Missed Call Log.

Yealink	Status Account Network	Features Setting	IS Directory	Log Out
		reatures	js Directory	occurry
Register	Missed Call Log	Enabled 👻	0	NOTE
Deale	Auto Answer	Disabled 👻	0	Denie
Basic	Ring Type	Common 👻	0	The basic parameters for
Codec	Account Lock	Disabled 👻	0	administrator.
	Always On Line	Disabled 👻	0	Proxy Require
	Confirm	Cancel		Nortel server. If you login to Nortel server, the value should be, com.nortelnetworks.firewall
				You can click here to get more guides.

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

# **Dial Search Delay**

Dial search delay defines a period of delay time before the IP phones automatically displays the search results. It is only applicable when searching contacts on the dialing screen.

## Procedure

Dial search delay can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure dial search delay feature.
		Parameter:

		sfb.search_delay_time
		Configure dial search delay feature.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		<pre>?p=features-general&amp;q=load</pre>

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sfb.search_delay_time	Integer from 1 to 10	1
Description:		
Configures the delay time (in seconds) for the IP phone to automatically display the search results on the dialing screen.		
Example:		
sfb.search_delay_time = 1		
Web User Interface:		
Features->General Information->Dial Search Delay		
Phone User Interface:		
None		

### To configure dial search delay via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of **Dial Search Delay**.

			Log Out
Yealink 1466	Status Account Network	Features Settings	Directory Security
General	General Information 🛛 🕜		NOTE
Information	Call Waiting	Enabled 🔹 🥜	
Audio	Key As Send	# • ?	Call Waiting This call feature allows your
Bomoto Control	Busy Tone Delay (Seconds)	0 🔹 🕜	calls during the conversation.
Keniote Control	Return code when refuse	603 (Decline) 🔹 🕜	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	Select * or # as the send key.
Power LED	Dial Search Delay	1	You can click here to get
	180 Ring Workaround	Disabled 🔹 🕜	more guides.
	Save Call Log	Enabled 🔹 🕜	)
	Suppress DTMF Display	Disabled 🔹 🕜	
	Suppress DTMF Display Delay	Disabled 👻 🕜	•
	Play Local DTMF Tone	Enabled 🔹 🕜	)

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

# Live Dialpad

Live dialpad allows IP phones to automatically dial out the entered phone number after a specified period of time.

## Procedure

Live dialpad can be configured using the configuration files or locally.

		Configure live dialpad.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:
Comportation me		phone_setting.predial_autodial
		phone_setting.inter_digit_time
		Configure live dialpad.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		?p=settings-preference&q=load

## Details of Configuration Parameters:

Parameters	Permitted Values	Default		
phone_setting.predial_autodial	0 or 1	0		
Description:				
Enables or disables live dialpad feature.				
0-Disabled				
1-Enabled				
If it is set to 1 (Enabled), the IP phone will automatically number on the dialing screen without pressing a send	y dial out the entere key.	d phone		
Web User Interface:				
Settings->Preference->Live Dialpad				
Phone User Interface:				
None				
phone_setting.inter_digit_time	Integer from 1 to 14	8		
Description:				
Configures the delay time (in seconds) for the IP phone to automatically dial out the entered digits without pressing a send key.				
Note: It works only if the value of the parameter "phon	Note: It works only if the value of the parameter "phone_setting.predial_autodial" is			
set to 1 (Enabled).				

Parameters	Permitted Values	Default
Web User Interface:		
None		
Phone User Interface:		
None		

To configure live dialpad via web user interface:

- 1. Click on Settings->Preference.
- 2. Select the desired value from the pull-down list of Live Dialpad.

				Log Out
Yealink   1466	Status Account Network	Features Settings	Directory	Security
Preference	Language	English (English) 🔻 🕜		NOTE
Time@Date	Live Dialpad	Enabled 🔹 🕜		Dreference Sattings
Timeduate	Backlight Inactive Level	Low 🔻 🕜		The preference settings for
Upgrade	Backlight Active Level	8 🔹 🕜		administrator.
Auto Provision	Watch Dog	Enabled 🔹 🕜		You can click here to get more guides.
Configuration	Ring Type	Ring1.wav 🔹 🕜		
	Upload Ringtone	Browse No file selected.	0	
Dial Plan		Upload Cancel		
Voice	Confirm	Cancel		
Tones	Comm	CallCer		

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

## **Call Waiting**

Call waiting allows IP phones to receive a new incoming call when there is already an active call. The new incoming call is presented to the user visually on the LCD screen. Call waiting tone allows the IP phone to play a short tone, to remind the user audibly of a new incoming call during conversation. Call waiting tone works only if call waiting is enabled. You can customize call waiting tone or select specialized tone sets (vary from country to country) for your IP phone. For more information, refer to Tones on page 253.

### Procedure

Call waiting and call waiting tone can be configured using the configuration files or locally.

		Configure call waiting and call waiting tone.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:
		call_waiting.enable
		call_waiting.tone
Local	Web User Interface	Configure call waiting.

	Navigate to:
	http:// <phonelpaddress>/servlet</phonelpaddress>
	?p=features-general&q=load
	Configure call waiting tone.
	Navigate to:
	http:// <phonelpaddress>/servlet</phonelpaddress>
	<pre>?p=features-audio&amp;q=load</pre>
Phone User Interface	Configure call waiting and call waiting tone.

## Details of Configuration Parameters:

Parameters	Permitted Values	Default
call_waiting.enable	0 or 1	1
Description:		
Enables or disables call waiting feature.		
0-Disabled		
1-Enabled		
If it is set to 0 (Disabled), a new incoming cal phone with a busy message while during a c	I is automatically rejected by call.	the IP
If it is set to 1 (Enabled), the LCD screen will p a call.	resent a new incoming call w	hile during
Web User Interface:		
Features->General Information->Call Waiting	)	
Phone User Interface:		
Menu->Features->Call Waiting->Call Waiting		
call_waiting.tone	0 or 1	1
Description:		
Enables or disables the IP phone to play the	call waiting tone when the IP	phone
receives an incoming call during a call.		
0-Disabled		
1-Enabled		
If it is set to 1 (Enabled), the IP phone will per receiving a new incoming call during a call.	form an audible indicator whe	en
<b>Note</b> : It works only if the value of the parame (Enabled).	eter "call_waiting.enable" is se	et to 1

Parameters	Permitted Values	Default		
Web User Interface:				
Features->Audio->Call Waiting Tone				
Phone User Interface:				
Menu->Features->Call Waiting->Play Tone				

#### To configure call waiting via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of Call Waiting.

				Log Out
	Status Account Network	Features Settin	ngs Directory	Security
General	General Information 🛛 🕜			NOTE
Information	Call Waiting	Enabled 👻	0	
Audio	Key As Send	#	0	Call Waiting This call feature allows your
Bomoto Control	Busy Tone Delay (Seconds)	0 🔹	0	phone to accept other incoming calls during the conversation.
Remote Control	Return code when refuse	603 (Decline) 👻	0	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	0	Select * or # as the send key.
Power LED	Dial Search Delay	1	0	You can click here to get
	180 Ring Workaround	Disabled 👻	0	more guides.
	Save Call Log	Enabled 👻	0	
	Suppress DTMF Display	Disabled 👻	0	
	Suppress DTMF Display Delay	Disabled 👻	0	
	Play Local DTMF Tone	Enabled -	0	

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

To configure call waiting tone via web user interface:

- 1. Click on Features->Audio.
- 2. Select the desired value from the pull-down list of Call Waiting Tone.

Yealink   1466	Status Account Network	Features Settings	Directory	Log Out Security
General	Audio Settings			NOTE
Information	Call Waiting Tone	Enabled 🔹	0	A sufficient of the second
Audio	Key Tone	Enabled 👻 🌔	0	The audio parameters for
Damata Control	Pre Dial Tone	Disabled 🔹	0	administrator.
Remote Control	Send Sound	Enabled 👻	0	You can click here to get
Bluetooth	Redial Tone		0	more guides.
Power LED	Ringer Device for Headset	Use Speaker 👻	0	
	BToE as Audio Device (VDI support)	Disabled 👻	0	
	Confirm	Cancel		

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

### To configure call waiting and call waiting tone via phone user interface:

- 1. Press Menu->Features->Call Waiting.
- 2. Press (•) or (•), or the Switch soft key to select the desired value from the Call

Waiting field.

- Press (•) or (•), or the Switch soft key to select the desired value from the Play Tone field.
- 4. Press the Save soft key to accept the change.

## Pre Dial Tone

Pre dial tone allows IP phones to play key tone in following situations:

- Enter phone numbers without picking up the handset (applicable to SIP-T48G/T46G/T42G/T41P/T40P IP phones).
- Tap (Dial icon) to enter the pre-dialing screen, and then enter phone numbers without picking up the handset (only applicable to SIP-T48G IP phones).

### Procedure

Pre dial tone can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure pre dial tone feature. Parameters:	
		sfb.pre_dial_tone.enable	
		Configure pre dial tone feature.	
local	Wah Usar Interface	Navigate to:	
		http:// <phonelpaddress>/servlet</phonelpaddress>	
		?p=features-audio&q=load	

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
sfb.pre_dial_tone.enable	0 or 1	0

### Description:

Enables or disables the IP phones to play key tone in following situations:

### For SIP-T48G/T46G/T42G/T41P/T40P IP phones:

Enter phone numbers without picking up the handset.

### For SIP-T48G IP phones:

Tap **(Dial** icon) to enter the pre-dialing screen, and then enter phone numbers without picking up the handset.

#### Web User Interface:

Features->Audio->Pre Dial Tone

### Phone User Interface:

Parameters	Permitted Values	Default
None		

### To configure pre dial tone via web user interface:

- 1. Click on Features->Audio.
- 2. Select the desired value from the pull-down list of **Pre Dial Tone**.

Yealink   1466	Status	Account	Features Setti	ngs	Directory	Log Out
General	A	udio Settings				NOTE
Information		Call Waiting Tone	Enabled -	0		Audia
Audio		Key Tone	Enabled -	0		The audio parameters for
Romoto Control		Pre Dial Tone	Disabled 🗸	0		administrator.
Remote Control		Send Sound	Enabled -	0		You can click here to get more guides
Bluetooth		Redial Tone		0		more guides.
Power LED		Ringer Device for Headset	Use Speaker 👻	0		
		BToE as Audio Device (VDI support)	Disabled -	0		
		Confirm	Cancel			

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

## **Redial Tone**

Redial tone allows IP phones to continue to play the dial tone after inputting the preset numbers on the pre-dialing screen.

## Procedure

Redial tone can be configured using the configuration files or locally.

		Configure redial tone feature.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:
		features.redial_tone
		Configure redial tone feature.
local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		?p=features-audio&q=load

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
features.redial_tone	Integer within 6 digits	Blank

Parameters	Permitted Values	Default			
Description:	Description:				
Configures the IP phone to continue to play the dial tone after inputting the preset numbers on the pre-dialing screen.					
Example:	Example:				
features.redial_tone = 125					
The IP phone will continue to play the	dial tone after inputting "125" on the	9			
pre-dialing screen.					
If it is left blank, the IP phone will not p	play the dial tone after inputting num	bers on			
the pre-dialing screen.					
Web User Interface:					
Features->Audio->Redial Tone					
Phone User Interface:					
None					

To configure redial tone via web user interface:

- 1. Click on Features->Audio.
- 2. Enter the desired value in the **Redial Tone** field.

Yealink   1466	Status Account Net	twork Features	Settings	Directory	Log Out
General	Audio Settings			NOTE	
Information	Call Waiting Tone	Enabled	• 🕜	Audio	
Audio	Key Tone	Enabled	• 🕜	The audio	parameters for
Domoto Control	Pre Dial Tone	Disabled	• 🕜	auministrat	01.
Keniote Control	Send Sound	Enabled	• 🕜	You can more quide	n click here to get
Bluetooth	Redial Tone	125	0		
Power LED	Ringer Device for Headset	Use Speaker	• 🕜		
	BToE as Audio Device (VD	DI support) Disabled	• 🕜		
	Confirm		Cancel		

3. Click Confirm to accept the change.

## **Ringer Device for Headset**

The IP phones support either or both speaker and headset ringer devices. Ringer Device for Headset feature allows users to configure which ringer device to be used when receiving an incoming call. For example, if the ringer device is set to Headset, ring tone will be played through your headset.

If the ringer device is set to Headset or Headset&Speaker, the headset should be connected to the IP phone and the headset mode also should be activated in advance. You can press the HEADSET key to activate the headset mode. For more information, refer to the Yealink phone-specific user guide.

## Procedure

Ringer device for headset can be configured using the configuration files or locally.

		Configure the ringer device for the IP phone.	
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:	
		features.ringer_device.is_use_he adset	
		Configure the ringer device for the IP phone.	
Local	Web User Interface	Navigate to:	
		http:// <phonelpaddress>/servlet</phonelpaddress>	
		?p=features-audio&q=load	

## Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.ringer_device.is_use_headset	0, 1 or 2	0
Description:		
Configures the ringer device for the IP ph	one.	
<b>0</b> -Use Speaker		
1-Use Headset		
2-Use Headset & Speaker		
If the ringer device is set to Headset or Headset&Speaker, the headset should be connected to the IP phone and the headset mode also should be activated in advance.		
Web User Interface:		
Features->Audio->Ringer Device for Headset		
Phone User Interface:		
None		

### To configure ringer device for headset via web user interface:

1. Click on **Features**->**Audio**.

2. Select the desired value from the pull-down list of Ringer Device for Headset.

Yealink   1466	Status Account Network	Features Setting	JS Directory	Log Out
General	Audio Settings			NOTE
Information	Call Waiting Tone	Enabled 👻	0	
Audio	Key Tone	Enabled 👻	0	Audio The audio parameters for
Pemote Control	Pre Dial Tone	Disabled 🔹	0	administrator.
Keniote control	Send Sound	Enabled 🔹	0	You can click here to get more guides
Bluetooth	Redial Tone		0	more guides.
Power LED	Ringer Device for Headset	Use Speaker 🔹	0	
	BToE as Audio Device (VDI support)	Disabled 🔹	0	
	Confirm	Cancel		

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

## Auto Answer

Auto answer allows IP phones to automatically answer an incoming call. IP phones will not automatically answer the incoming call during a call even if auto answer is enabled. Auto answer is configurable on a per-line basis. Auto-Answer delay defines a period of delay time before the IP phone automatically answers incoming calls.

## Procedure

Auto answer can be configured using the configuration files or locally.

		Configure auto answer.
	<mac>.cfg</mac>	Parameter:
		account.1.auto_answer
Configuration File		Specify a period of delay time for
	<v00000000vv> cfa</v00000000vv>	auto answer.
	<y000000000000000000000000000000000000< td=""><td>Parameter:</td></y000000000000000000000000000000000000<>	Parameter:
		features.auto_answer_delay
		Configure auto answer.
		Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		<pre>?p=account-basic&amp;q=load&amp;acc</pre>
Local	Web User Interface	=0
		Specify a period of delay time for
		auto answer.
		Navigate to:
		http:// <phonelpaddress>servlet?</phonelpaddress>
		p=features-general&q=load

## Details of Configuration Parameters:

Parameters	Parameters Permitted Values			
account.1.auto_answer	ount.1.auto_answer 0 or 1			
Description:				
Enables or disables auto answer feature f	or the account.			
0-Disabled				
1-Enabled				
If it is set to 1 (Enabled), the IP phone car	automatically answer an incom	ing call.		
<b>Note</b> : The IP phone cannot automatically even if auto answer is enabled.	answer the incoming call during	a call		
Web User Interface:				
Account->Basic->Auto Answer				
Phone User Interface:				
Menu->Features->Auto Answer->Line 1->A	Auto Answer			
features.auto_answer_delay	Integer from 1 to 4	1		
Description:				
Configures the delay time (in seconds) be	efore the IP phone automatically	answers		
an incoming call.				
Web User Interface:				
Features->General Information->Auto-Answer Delay(1~4s)				
Phone User Interface:				
None				

### To configure auto answer via web user interface:

- 1. Click on Account->Basic.
- 2. Select the desired value from the pull-down list of Auto Answer.

Yealink 1466			Log Out
	Status Account Networ	k Features Settings Directo	ory Security
Register	Missed Call Log	Enabled 👻 🕜	NOTE
Pacie	Auto Answer	Enabled 👻 🕜	Paris
DdSIC	Ring Type	Common 👻 🕜	The basic parameters for
Codec	Account Lock	Disabled 🗸 🥐	administrator.
	Always On Line	Disabled 🗸 🥜	Proxy Require A special parameter just for
	Confirm	Cancel	Nortel server. If you login to Nortel server, the value should be, com.nortelnetworks.firewall
			You can click here to get more guides.

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

#### To configure a period of delay time for auto answer via web user interface:

- 1. Click on Features->General Information.
- 2. Enter the desired time in the Auto-Answer Delay(1~4s) field.

Vaclink								Log Out
	Status	Account	Network	Features	Settin	gs	Directory	Security
General		General Informati	on 🕜			_		NOTE
Information		Call Waiting		Enabled	-	0		Call Waiting
Audio		Key As Send		#	•	0		This call feature allows your
Remote Control		Busy Tone Delay	(Seconds)	0	•	0		calls during the conversation.
		Return code whe	n refuse	603 (Decline)	•	0		Key As Send
Bluetooth		Time-Out for Dial	Now Rule	1		0		Select * or # as the send key.
Power LED		Dial Search Delay		1		0		You can click here to get
		180 Ring Workard	und	Disabled	•	0		more guides.
		Save Call Log		Enabled	•	0		
		Suppress DTMF D	isplay	Disabled	•	0		
		Suppress DTMF D	isplay Delay	Disabled	•	?		
		Play Local DTMF	one	Enabled	•	0		
		DTMF Repetition		3	•	0		
		Multicast Codec		G722	•	0		
		Play Hold Tone		Enabled	•	0		
		Play Hold Tone D	elay	30		0		
		Allow Mute		Enabled	•	0		
		Dual-Headset		Disabled	•	0		
		Auto-Answer Del	ay(1~4s)	1		0		

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

To configure auto answer via phone user interface:

- 1. Press Menu->Features->Auto Answer->Line 1-> Auto Answer.
- Press (•) or (•), or the Switch soft key to select the desired value from the Auto Answer field.
- 3. Press the Save soft key to accept the change.

## Always On Line

Always on line feature allow IP phones to maintain the current status until you manually change it. For example, the current status of the IP phone is Available, if the always online feature is enabled, then the IP phone status will stay Available until you manually change it.

### Procedure

Always on line can be configured using the configuration files or locally.

Configuration File	(1000000000000000000000000000000000000	Configure always on line.
	<yuuuuuuuuuuuuxx>.cf g</yuuuuuuuuuuuuxx>	Parameter:
		sfb.always_online.enable

Coring	gure always on line.	
Navig	Navigate to:	
http://	// <phonelpaddress>/servlet?p=a nt-basic&amp;q=load&amp;acc=0</phonelpaddress>	

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default	
sfb.always_online.enable	0 or 1	0	
<b>Description:</b> Enables or disables the IP phone to maintain current st	atus until you manu	ally	
0-Disabled 1-Enabled			
<b>Note</b> : If your phone status is DND before dialing an emergency number, then the IP phone status will be changed to available after the emergency call even if the value of this parameter is set to 1 (Enabled).			
Web User Interface:			
Account->Basic->Always On Line			
Phone User Interface:			
Menu->Basic->Always Online			

### To configure always on line via web user interface:

- 1. Click on Account->Basic.
- 2. Select the desired value from the pull-down list of Always On Line.

Yealink 1466	Status Account Network	Features Settings Directory	Log Out
Register Basic Codec	Missed Call Log Auto Answer Ring Type Account Lock Always On Line Confirm	Enabled   Enabled  Common  Com	NOTE Basic The basic parameters for administrator. Proxy Requite A special parameter just for Notel server. If you login to Notel server, the value should be, com.nortelnetworks.frewall Que you can click here to get more guides.

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

To configure always on line via phone user interface:

1. Press Menu->Basic->Always Online.

- 2. Press () or (), or the Switch soft key to select the desired value from the Always Online field.
- 3. Press the Save soft key to accept the change.

# **Busy Tone Delay**

Busy tone is audible to the other party, indicating that the call connection has been broken when one party releases a call. Busy tone delay can define a period of time during which the busy tone is audible.

## Procedure

Busy tone delay can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Configure busy tone delay. Parameter:
		features.busy_tone_delay
		Configure busy tone delay.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet</phonelpaddress>
		?p=features-general&q=load

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.busy_tone_delay	0, 3 or 5	0
Description:		
Configures the duration time (in seconds) for the busy	tone.	
When one party releases the call, a busy tone is audible	e to the other party	indicating
that the call connection breaks.		
<b>0</b> -Os		
<b>3</b> -3s		
<b>5</b> -5s		
If it is set to 3 (3s), a busy tone is audible for 3 seconds of	on the IP phone.	
Web User Interface:		
Features->General Information->Busy Tone Delay (Seco	onds)	
Phone User Interface:		
None		

### To configure busy tone delay via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of **Busy Tone Delay (Seconds)**.

Yealink	Status Account Network Features	Log Out Settings Directory Security
General	General Information 🛛 🕜	NOTE
Information	Call Waiting Enabled	- Q
Audio	Key As Send #	Call Warting     This call feature allows your
Remote Control	Busy Tone Delay (Seconds) 0	<ul> <li>pnone to accept other incoming</li> <li>calls during the conversation.</li> </ul>
Remote control	Return code when refuse 603 (Decline)	• ? Key As Send
Bluetooth	Time-Out for Dial-Now Rule 1	Select * or # as the send key.
Power LED	Dial Search Delay 1	You can click here to get
	180 Ring Workaround Disabled	✓ ?
	Save Call Log Enabled	• 0
	Suppress DTMF Display Disabled	• 0

3. Click Confirm to accept the change.

## Return Code When Refuse

Return code when refuse defines the return code and reason of the SIP response message for the refused call. The caller's phone LCD screen displays the reason according to the received return code. Available return codes and reasons are:

- 404 (Not Found)
- 480 (Temporarily Not Available)
- 486 (Busy Here)
- 603 (Decline)

### Procedure

Return code for refused call can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Specify the return code and the reason of the SIP response message when refusing a call. <b>Parameter:</b> features.normal_refuse_code	
Local	Web User Interface	Specify the return code and the reason of the SIP response message when refusing a call. <b>Navigate to:</b> http:// <phonelpaddress>/servlet ?p=features-general&amp;q=load</phonelpaddress>	

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default			
features.normal_refuse_code	404, 480, 486 or 603	603			
Description:					
Configures a return code and reason of SIP response messages when the IP phone rejects an incoming call. A specific reason is displayed on the caller's phone LCD screen.					
<b>404</b> -Not Found					
480-Temporarily Not Available					
486-Busy Here					
603-Decline					
If it is set to 486 (Busy Here), the caller's phone LCD screen will display the message "Busy Here" when the callee rejects the incoming call.					
Web User Interface:					
Features->General Information->Return Code When Refuse					
Phone User Interface:					
None					

To specify the return code and the reason when refusing a call via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of Return Code When Refuse.

Yealink 1466	Status Account Network	Features Settings	Log Out Directory Security
General	General Information 🕜		NOTE
Information	Call Waiting	Enabled 🔹 🕜	0-11 11-11-
Audio	Key As Send	# 🔹 🕜	This call feature allows your
Remote Control	Busy Tone Delay (Seconds)	0 🔹 🕜	calls during the conversation.
Kemble control	Return code when refuse	603 (Decline) 🔻 🕜	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	Select * or # as the send key.
Power LED	Dial Search Delay	1	You can click here to get
	180 Ring Workaround	Disabled 🔹 🕜	more guides.
	Save Call Log	Enabled 🔻 🥜	
	Suppress DTMF Display	Disabled 🔹 🕜	

3. Click Confirm to accept the change.

# Early Media

Early media refers to media (e.g., audio and video) played to the caller before a SIP call is actually established. Current implementation supports early media through the

183 message. When the caller receives a 183 message with SDP before the call is established, a media channel is established. This channel is used to provide the early media stream for the caller.

# 180 Ring Workaround

180 ring workaround defines whether to deal with the 180 message received after the 183 message. When the caller receives a 183 message, it suppresses any local ringback tone and begins to play the media received. 180 ring workaround allows IP phones to resume and play the local ringback tone upon a subsequent 180 message received.

## Procedure

180 ring workaround can be configured using the configuration files or locally.

		Configure 180 ring workaround.	
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameter:	
		phone_setting.is_deal180	
		Configure 180 ring workaround.	
local	Web User Interface	Navigate to:	
		http:// <phonelpaddress>/servlet</phonelpaddress>	
		<pre>?p=features-general&amp;q=load</pre>	

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.is_deal180	0 or 1	0
Description:		
Enables or disables the IP phone to deal with the 180 S 183 SIP message.	IP message received	d after the
0-Disabled		
1-Enabled		
If it is set to 1 (Enabled), the IP phone will resume and p upon a subsequent 180 message received.	olay the local ringbo	ick tone
Web User Interface:		
Features->General Information->180 Ring Workaround		
Phone User Interface:		

None

To configure 180 ring workaround via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of 180 Ring Workaround.

Yealink   1466	Status Account Network	Features Settings	Log Out Directory Security
General	General Information 🛛 🕜		NOTE
Information	Call Waiting	Enabled 🔹 🕜	
Audio	Key As Send	# • ?	Call Waiting This call feature allows your
Demote Control	Busy Tone Delay (Seconds)	0 🔹 🕜	phone to accept other incoming calls during the conversation.
Remote Control	Return code when refuse	603 (Decline) 🔹 🕜	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	Select * or # as the send key.
Power LED	Dial Search Delay	1	You can click here to get
	180 Ring Workaround	Disabled 🔹 🕜	more guides.
	Save Call Log	Enabled 👻 🕜	
	Suppress DTMF Display	Disabled 👻 🕜	

3. Click Confirm to accept the change.

# Call Hold

Call hold provides a service of placing an active call on hold. When a call is placed on hold, the IP phones send an INVITE request with HOLD SDP to request remote parties to stop sending media and to inform them that they are being held. IP phones support two call hold methods, one is RFC 3264, which sets the "a" (media attribute) in the SDP to sendonly, recvonly or inactive (e.g., a=sendonly). The other is RFC 2543, which sets the "c" (connection addresses for the media streams) in the SDP to zero (e.g., c=0.0.0.0). Call hold tone allows IP phones to play a warning tone at regular intervals when there is a call on hold. The warning tone is played through the speakerphone.

## Procedure

Call hold can be configured using the configuration files or locally.

		Configure the call hold tone and call hold tone delay.		
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:		
		features.play_hold_tone.enable		
		features.play_hold_tone.delay		
		Configure the call hold tone and call hold tone delay.		
Local	Web User Interface	Navigate to:		
		http:// <phonelpaddress>/servlet</phonelpaddress>		
		<pre>\$p=teatures-general&amp;q=load</pre>		

## Details of Configuration Parameters:

Parameters	Permitted Values	Default		
features.play_hold_tone.enable	0 or 1	1		
Description:				
Enables or disables the IP phone to play a war	ning tone when there is a cc	all on hold.		
0-Disabled				
1-Enabled				
Web User Interface:				
Features->General Information->Play Hold Ton	e			
Phone User Interface:				
None				
features.play_hold_tone.delay	Integer from 3 to 3600	30		
Description:				
Configures the interval (in seconds) at which t when there is a call on hold.	he IP phone play a warning	tone		
If it is set to 30 (30s), the IP phone will play a wo there is a call on hold.	arning tone every 30 second	is when		
<b>Note:</b> It works only if the value of the parameter "features.play_hold_tone.enable" is set to 1 (Enabled).				
Web User Interface:				
Features->General Information->Play Hold Ton	e Delay			
Phone User Interface:				
None				

To configure call hold tone and call hold tone delay via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of **Play Hold Tone**.

	_	_	_	_		_	_	Log Out
	Status	Account	Network	Features	Settin	igs	Directory	Security
General	Ge	eneral Informati	ion 🕜					NOTE
Information		Call Waiting		Enabled	-	0		Coll Wolfdan
Audio		Key As Send		#	•	0		This call feature allows your
Demote Control		Busy Tone Delay	(Seconds)	0	•	0		phone to accept other incomin calls during the conversation.
Remote Control		Return code whe	en refuse	603 (Decline)	•	0		Key As Send
Bluetooth		Time-Out for Dial	-Now Rule	1		0		Select * or # as the send key.
Power LED		Dial Search Delay		1		0		You can click here to get
		180 Ring Workard	ound	Disabled	•	0		more guides.
		Save Call Log		Enabled	•			
		Suppress DTMF D	)isnlav	Disabled	•	0		
		Suppress DTMF D	Nenby Deby	Disabled		6		
		Dby Local DTME 1	Торо	Enabled				
			Tone	Enabled	•			
		DIMF Repetition		3	•	0		
	-	Multicast Codec		G722		0		
		Play Hold Tone		Enabled	-	0		
		Play Hold Tone D	elay	30		0		
		Allow Mute		Enabled	-	0		
		Dual-Headset		Disabled	•	0		
		Auto-Answer Del	ay(1~4s)	1		0		

3. Enter the desired time in the Play Hold Tone Delay field.

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

## Allow Trans Exist Call

Allow trans exist call feature allows users to select transfer-to party's call during multiple calls. It is convenient to transfer the active call to another existing call. It is not applicable to SIP-T48G/T46G IP phones.

### Procedure

Allow trans exist call can be configured using the configuration files or locally.

		Configure allow trans exist call.		
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:		
		transfer.multi_call_trans_enable		
		Configure allow trans exist call.		
local	Web User Interface	Navigate to:		
		http:// <phonelpaddress>/servlet?p=f</phonelpaddress>		
		eatures-general&q=load		

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
transfer.multi_call_trans_enable	0 or 1	1

Parameters	Permitted Values	Default				
Description:						
Enables or disables the IP phone to select transfer-to party's call (a new call or another existing call) during multiple calls when user presses the Tran/Transfer soft key or TRAN/TRANSFER key.						
0-Disabled						
1-Enabled						
If it is set to 1 (Enabled), the user can select to transfer the active call to a new call or another existing call during multiple calls when the user presses the Tran/Transfer soft key or TRAN/TRANSFER key.						
If it is set to 0 (Disabled), the user can transfer the active call to a new call during multiple calls when the user presses the Tran/Transfer soft key or TRAN/TRANSFER key.						
Note: It is not applicable to SIP-T48G/T46G IP phones.						
Web User Interface:						
Features->General Information->Allow Trans Exist Call						
Phone User Interface:						
None						

## To configure allow trans exist call via web user interface:

1. Click on Features-> General Information.

						Log Out
Yealink   1236	Status Account	t Network	Features	Settings	Directory	Security
	General Infor	mation				NOTE
General Information	Call Waiting		Enabled	~		
Audio	Key As Send		#	~		Call Waiting This call feature allows your
Audio	Busy Tone D	elay (Seconds)	0	~		phone to accept other incoming calls during the conversation.
Remote Control	Return Code	When Refuse	603 (Decline)	~		Key As Send
Power LED	Time-Out for	Dial-Now Rule	1			Select " of # as the send key.
	Dial Search D	elay	8			You can click here to get more guides.
			•			
			:			
	Allow Trans	Exist Call	Enabled	•		
	ReLogOffTin	ne(1~1000min)	5			
	Call Number	Filter				
	Voice Mail T	one	Enabled	•		
	dhcp_hostn	ame	SIP-T42G			
	E911 Locati	on Tip	Enabled	•		
	Update Che	cking Time	24			
	Use DHCP O	ption 120	Disabled	•		
	SFB Cert Se	rvice URL				
	Enable SFB	Automation	Disabled	•		
	SFB Inactive	Time	5			
	SFB Away T	ime	5			
	Device Pairin	g for Online	Enabled	•		
		Confirm		Cancel		

2. Select the desired value from the pull-down list of Allow Trans Exist Call.

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

## **Call Number Filter**

Call number filter feature allows IP phone to automatically filter designated characters when dialing.

## Procedure

Call number filter can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Configure the characters the IP phone filters when dialing. <b>Parameters:</b> features.call num filter	
Local	Web User Interface	Configure the characters the IP phone filters when dialing.	
		Navigate to: http:// <phonelpaddress>/servlet?p=f eatures-general&amp;q=load</phonelpaddress>	

## Details of Configuration Parameters:

Parameters	Permitted Values	Default			
features.call_num_filter	String within 99 characters	Blank			
Description:					
Configures the characters the IP phone filters when dialing.					
If the dialed number contains configured characters, the IP phone will automatically filter these characters when dialing.					
Example:					
features.call_num_filter = %					
If you dial 1010%, the IP phone will filter the character % and dial out 1010.					
<b>Note</b> : If it is left blank, the IP phone will not automatically filter any characters when dialing. If you want to filter just a space, you have to set the value to "," (a space first followed by a comma).					
Web User Interface:					
Features->General Information->Call Number Filter					
Phone User Interface:					
None					

To configure the characters the IP phone will filter via web user interface:

1. Click on Features-> General Information.
|                | Statue | Account   | Network                     | Features  | Settin |   | Directory | Security       | )                                    |
|----------------|--------|---|-----------------------------|---|--------|---|-----------|----------------|--------------------------------------|
|                | Status | Account   | Network                     | r cutur co  | Jetun  | ys  | Directory | Security       |                                      |
| General        |        | General Informatio  | n 🕜                         |   |        |   |           | NOTE           |                                      |
| Information    |        | Call Waiting  |                             | Enabled   | •      | 0   |           | Call Waiting   |                                      |
| Audio          |        | Key As Send   |                             | #   | •      | 0   |           | This call feat | ure allows your                      |
| Remote Control |        | Busy Tone Delay (   | Seconds)                    | 0   | •      | ?   |           | calls during t | tept other incom<br>he conversation. |
| Remote control |        | Return code when  | ı refuse                    | 603 (Decline)   | •      | ?   |           | Key As Send    |                                      |
| Bluetooth      |        | Time-Out for Dial-N   | low Rule                    | 1   |        | 0   |           | Select * or #  | as the send key                      |
| Power LED      |        | Dial Search Delay   |                             | 1   |        | 0   |           | 🛽 You can      | click here to get                    |
|                |        | Call Number Filter  |                             | •   |        | 0   | ]         |                |                                      |
|                |        | Call Number Filter<br>Voice Mail Tone   |                             | • %   |        | 0   | ]         |                |                                      |
|                |        | Call Number Filter<br>Voice Mail Tone<br>DHCP Hostname  |                             | %     Enabled     SIP-T46G  | Ŧ      | 0<br>0<br>0   | ]         |                |                                      |
|                |        | Call Number Filter<br>Voice Mail Tone<br>DHCP Hostname<br>E911 Location Tip   |                             | Konstant Sup-T46G Enabled Enabled   | •      | 0<br>0<br>0<br>0  | ]         |                |                                      |
|                |        | Call Number Filter<br>Voice Mail Tone<br>DHCP Hostname<br>E911 Location Tip<br>Update Checking  | Time                        | <ul> <li>%</li> <li>Enabled</li> <li>SIP-T46G</li> <li>Enabled</li> <li>24</li> </ul>                                     | •      | 0<br>0<br>0<br>0  | ]         |                |                                      |
|                |        | Call Number Filter<br>Voice Mail Tone<br>DHCP Hostname<br>E911 Location Tip<br>Update Checking<br>Use DHCP Option   | Time<br>120                 | <ul> <li>%</li> <li>Enabled</li> <li>SIP-T46G</li> <li>Enabled</li> <li>24</li> <li>Disabled</li> </ul>                   | •      | 0<br>0<br>0<br>0<br>0   | ]         |                |                                      |
|                |        | Call Number Filter<br>Voice Mail Tone<br>DHCP Hostname<br>E911 Location Tip<br>Update Checking<br>Use DHCP Option<br>SFB Cert Service U   | Time<br>120<br>IRL          | %<br>Enabled<br>SIP-T46G<br>Enabled<br>24<br>Disabled   | •      | 0<br>0<br>0<br>0<br>0<br>0<br>0                               | ]         |                |                                      |
|                |        | Call Number Filter<br>Voice Mail Tone<br>DHCP Hostname<br>E911 Location Tp<br>Update Checking '<br>Use DHCP Option<br>SFB Cert Service L<br>Enable SFB Autom  | Time<br>120<br>IRL<br>ation | <ul> <li>%</li> <li>Enabled</li> <li>SIP-T46G</li> <li>Enabled</li> <li>24</li> <li>Disabled</li> <li>Disabled</li> </ul> | •      | 0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0<br>0                | ]         |                |                                      |
|                |        | Call Number Filter<br>Voice Mail Tone<br>DHCP Hostname<br>E911 Location Tp<br>Update Checking :<br>Use DHCP Option<br>SFB Cert Service L<br>Enable SFB Autom<br>SFB Inactive Time                   | Time<br>120<br>IRL<br>ation | %     Carabled     SIP-T466     Enabled     Z4     Disabled     Disabled     S  | •      | 9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9      | ]         |                |                                      |
|                |        | Call Number Filter<br>Voice Mall Tone<br>DHCP Hostname<br>E911 Location Tip<br>Update Checking '<br>Use DHCP Option<br>SFB Cert Service L<br>Enable SFB Autom<br>SFB Inactive Time<br>SFB Away Time | Time<br>120<br>IRL<br>ation | %     SIP-T466 Enabled Enabled 24 Disabled Disabled Disabled 5 5 5  | •      | 9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9<br>9 | ]         |                |                                      |

2. Enter the desired character in the Call Number Filter field.

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

### DTMF

DTMF (Dual Tone Multi-frequency), better known as touch-tone, is used for telecommunication signaling over analog telephone lines in the voice-frequency band. DTMF is the signal sent from the IP phone to the network, which is generated when pressing the IP phone's 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)).

	1209 Hz	1336 Hz	1447 Hz	1633 Hz
697 Hz	1	2	3	А
770 Hz	4	5	6	В
852 Hz	7	8	9	С
941 Hz	*	0	#	D

#### **DTMF Keypad Frequencies:**

DTMF digits are transmitted using the RTP Event packets that are sent along with the voice path. 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.

### Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure the number of times for the IP phone to send the end RTP Event packet. Parameter:
		teatures.dtmt.repetition
Local	Web User Interface	Configure the number of times for the IP phone to send the end RTP Event packet.
		Navigate to:
		http:// <phonelpaddress>/servlet ?p=features-general&amp;q=load</phonelpaddress>

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
features.dtmf.repetition	1, 2 or 3	3
Description:		
Configures the repetition times for the IP phone to service call	d the end RTP Event	packet
Web User Interface:		
Features->General Information->DTMF Repetition		
Phone User Interface:		
None		

To configure the number of times to send the end RTP Event packet via web user interface:

1. Click on Features->General Information.

2. Select the desired value (1-3) from the pull-down list of DTMF Repetition.

alink									Log (
	Status	Account	Network	Features	Settin	gs	Directory	Security	
General	(	General Informat	ion 🕜					NOTE	
Information		Call Waiting		Enabled	•	0		Call Waiting	
Audio		Key As Send		#	•	0		This call feat	ure allows your
Remote Control		Busy Tone Delay	(Seconds)	0	•	0		calls during th	ne conversation.
		Return code whe	en refuse	603 (Decline)	•	0		Key As Sen	ł
Bluetooth		Time-Out for Dia	I-Now Rule	1		0		Select * or #	as the send ke
Power LED		Dial Search Delay		1		0		🛛 You can	click here to get
		180 Ring Workar	ound	Disabled	•	0		more guides	•
		Save Call Log		Enabled	•	0			
		Suppress DTMF [	Display	Disabled	•	0			
		Suppress DTMF [	Display Delay	Disabled	•	0			
		Play Local DTMF	Tone	Enabled	•	0			
		DTMF Repetition		3	•	0			
		Multicast Codec		G722	•	0			
		Play Hold Tone		Enabled	•	0			
		Play Hold Tone D	Delay	30		0			
		Allow Mute		Enabled	•	0			
		Dual-Headset		Disabled	•	0			
		Auto-Answer De	lay(1~4s)	1		0			
		Headset Prior		Disabled	•	0			
		DTMF Replace Tr	ran	Disabled	•	0			

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

### Suppress DTMF Display

Suppress DTMF display allows IP phones to suppress the display of DTMF digits during an active call. DTMF digits are displayed as "\*" on the LCD screen. Suppress DTMF display delay defines whether to display the DTMF digits for a short period of time before displaying as "\*".

### Procedure

Configuration changes can be performed using the configuration files or locally.

		Configure suppress DTMF display and suppress DTMF display delay.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:
		features.dtmf.hide
		features.dtmf.hide_delay
		Configure suppress DTMF display and suppress DTMF display delay.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet?p =features-general&amp;q=load</phonelpaddress>

Details	of	Configuration	Parameters:
---------	----	---------------	-------------

Parameters	Permitted Values	Default		
features.dtmf.hide	0 or 1	0		
Description:				
Enables or disables the IP phone to suppress the displa active call.	y of DTMF digits duri	ng an		
0-Disabled				
1-Enabled				
If it is set to 1 (Enabled), the DTMF digits are displayed o	as asterisks.			
Web User Interface:				
Features->General Information->Suppress DTMF Display				
Phone User Interface:				
None				
features.dtmf.hide_delay	0 or 1	0		
Description:				
Enables or disables the IP phone to display the DTMF d displaying asterisks during an active call.	igits for a short peric	d before		
0-Disabled				
1-Enabled				
<b>Note:</b> It works only if the value of the parameter "featu (Enabled).	res.dtmf.hide" is set	to 1		
Web User Interface:				
Features->General Information->Suppress DTMF Display	y Delay			
Phone User Interface:				
None				

To configure suppress DTMF display and suppress DTMF display delay via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of **Suppress DTMF Display**.

3. Select the desired value from the pull-down list of Suppress DTMF Display Delay.

alink									Log
	Status	Account	Network	Features	Settin	ıgs	Directory	Security	
General		General Informat	ion 🕜					NOTE	
Information		Call Waiting		Enabled	-	0		Call Waiting	
Audio		Key As Send		#	•	0		This call featu	re allows your
Remote Control		Busy Tone Delay	(Seconds)	0	-	0		calls during th	e conversation
		Return code who	en refuse	603 (Decline)	•	0		Key As Send	
Bluetooth		Time-Out for Dia	-Now Rule	1		0		Select * or #	as the send ke
Power LED		Dial Search Delay		1		0		🕘 You can d	lick here to ge
		180 Ring Workar	ound	Disabled	•	0		more guides.	
		Save Call Log		Enabled	•	0			
		Suppress DTMF [	Display	Disabled	•	0			
		Suppress DTMF [	Display Delay	Disabled	•	0			
		Play Local DTMF	Tone	Enabled	¥	0			
		DTMF Repetition		3	•	0			
		Multicast Codec		G722	•	0			
		Play Hold Tone		Enabled	•	0			
		Play Hold Tone D	elay	30		0			
		Allow Mute		Enabled	•	0			
		Dual-Headset		Disabled	•	0			
		Auto-Answer De	lay(1~4s)	1		0			
		Headset Prior		Disabled	•	0			
		DTMF Replace Tr	an	Disabled	•	0			

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

### Transfer via DTMF

Call transfer is implemented via DTMF on some traditional servers. The IP phone sends specified DTMF digits to the server for transferring calls to third parties.

### Procedure

Configuration changes can be performed using the configuration files or locally.

		Configure transfer via DTMF.
Configuration File		Parameters:
Conliguration File	<y000000000xx2.c1g< td=""><td>features.dtmf.replace_tran</td></y000000000xx2.c1g<>	features.dtmf.replace_tran
		features.dtmf.transfer
		Configure transfer via DTMF.
local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servl</phonelpaddress>
		et?p=features-general&q=load

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
features.dtmf.replace_tran	0 or 1	0
Description:		
Enables or disables the IP phone to send DTMF sequen pressing the Tran/Transfer soft key or TRAN/TRANSFER key	ces for transfer func ey.	tion when
0-Disabled		
1-Enabled		
If it is set to 0 (Disabled), the IP phone will perform the t pressing the Tran/Transfer soft key or TRAN/TRANSFER ke	ransfer as normal w ey during a call.	hen
If it is set to 1 (Enabled), the IP phone will transmit the c server for performing call transfer when pressing the Tro TRAN/TRANSFER key during a call.	lesignated DTMF dig an/Transfer soft key (	gits to the or
Web User Interface:		
Features->General Information->DTMF Replace Tran		
Phone User Interface:		
None		
features.dtmf.transfer	String within 32 characters	Blank
Description:		
Configures the DTMF digits to be transmitted to perform are: 0-9, *, # and A-D.	n call transfer. Valid	values
Example:		
features.dtmf.transfer = 123		
<b>Note:</b> It works only if the value of the parameter "feature 1 (Enabled).	res.dtmf.replace_tro	an" is set
Web User Interface:		
Features->General Information->Tran Send DTMF		
Phone User Interface:		
None		

#### To configure transfer via DTMF via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of **DTMF Replace Tran**.

				Log C
ealink   1466	tatus Account Network	Features Sett	ings Directory	Security
General	General Information 🛛 🕜			NOTE
Information	Call Waiting	Enabled	0	Coll Walking
Audio	Key As Send	#	0	This call feature allows your
Remote Control	Busy Tone Delay (Seconds)	0	0	calls during the conversation.
	Return code when refuse	603 (Decline)	0	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	0	Select * or # as the send key
Power LED				You can click here to get
		•		more guides.
		•		
	DTMF Replace Tran	Enabled -	0	
	Tran Send DTMF	123	0	
	Send Pound Key	Disabled	0	
	Fwd International	Enabled	0	
	Diversion/History-Info	Disabled	0	
	Auto-Logout Time(1~1000min)	5	0	
	Call Number Filter		0	
	Voice Mail Tone	Enabled	0	
	DHCP Hostname	SIP-T46G	0	
	E911 Location Tip	Enabled	0	
	Update Checking Time	24	0	
	Use DHCP Option 120	Disabled	0	
	SFB Cert Service URL		0	
	Enable SFB Automation	Disabled	0	
		5	0	
	SFB Inactive Time	5	V	
	SFB Inactive Time SFB Away Time	5	0	

3. Enter the specified DTMF digits in the Tran Send DTMF field.

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

### Play Local DTMF Tone

Play local DTMF tone allows IP phones to play a local DTMF tone during an active call. If this feature is enabled, you can hear the DTMF tone when pressing the IP phone's keypad during a call.

#### Procedure

Configuration changes can be performed using the configuration files or locally.

		Configure play local DTMF tone.	
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:	
		features.play_local_dtmf_tone_ enable	
Local	Web User Interface	Configure play local DTMF tone.	
		Navigate to:	

	http:// <phonelpaddress>/servl</phonelpaddress>
	et?p=features-general&q=load

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default		
features.play_local_dtmf_tone_enable	0 or 1	1		
Description:				
Enables or disables the IP phone to play a local DTMF	tone during a call.			
0-Disabled				
1-Enabled				
If it is set to 1 (Enabled), you can hear the DTMF tone when pressing the IP phone's				
keypad during a call.				
Web User Interface:				
Features->General Information->Play Local DTMF Tone				
Phone User Interface:				
None				

#### To configure play local DTMF tone via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of Play Local DTMF Tone.

Veglink						_			Log Out
	Status	Account	Network	Features	Setting	js Dii	rectory	Security	
General Information Audio Remote Control Power LED	6	eneral Informati Call Waiting Key As Send Busy Tone Delay Return code whe Time-Out for Dial Dial Search Delay 180 Ring Workart Save Call Log Suppress DTMF C Play Local DTMF C Play Local DTMF T DTMF Repetition Multicast Codec Play Hold Tone D Allow Mute Dual-Headset	on (Seconds) n refuse Now Rule bund isplay isplay Tone elay	Enabled # 0 486 (Busy Here) 1 1 Enabled Enabled Disabled Disabled Enabled 3 6722 Enabled 30 Enabled Disabled Disabled				NOTE Call Waiting This call featur phone to acce calls during the Key As Send Select * or # Or a can can more guides.	re allows your opt other incoming e conversation. as the send key. ick here to get
Power LED		Return code whe Time-Out for Dial Dial Search Delay 180 Ring Workard Save Call Log Suppress DTMF ID Suppress DTMF ID Play Local DTMF ID DTMF Repetition Multicast Code C Play Hold Tone D Allow Mute Dual-Headset	n refuse Now Rule Jund Isplay Isplay Delay Tone	486 (Busy Here) 1 1 Enabled Disabled Disabled 6722 Enabled 30 Enabled Disabled Disabled		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		Key As Send Select * or #	as the seni

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

### Allow Mute

You can mute the microphone of the active audio device during an active call, and then the other party cannot hear you. If allow mute feature is disabled, you cannot mute an active call.

### Procedure

Allow mute can be configured using the configuration files or locally.

		Configure allow mute feature.	
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:	
		features.allow_mute	
Local		Configure allow mute feature.	
	Web User Interface	Navigate to:	
		http:// <phonelpaddress>/servlet?p=f</phonelpaddress>	
		eatures-general&q=load	

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default	
features.allow_mute	0 or 1	1	
Description:			
Enables or disables the IP phone to mute an	active call.		
<b>0</b> -Disabled			
1-Enabled			
Web User Interface:			
Features->General Information->Allow Mute			
Phone User Interface:			
None			

#### To configure allow mute via web user interface:

1. Click on Features-> General Information.

2. Select the desired value from the pull-down list of Allow Mute.

				Log (
Yealink   1466	Status Account Network	Features Settings	Directory	Security
General	General Information 🛛 🕜			NOTE
Information	Call Waiting	Enabled 🔹	2	
Audio	Key As Send	#	2	Call Waiting This call feature allows your
Domoto Control	Busy Tone Delay (Seconds)	0 🔹	2	phone to accept other incom calls during the conversation.
Remote Control	Return code when refuse	603 (Decline) 🔹	2	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	0	Select * or # as the send key
Power LED	Dial Search Delay	1	0	You can click here to get
	180 Ring Workaround	Disabled 👻	2	more guides.
	Save Call Log	Enabled 👻	2	
	Suppress DTMF Display	Disabled 👻	2	
	Suppress DTMF Display Delay	Disabled 👻	2	
	Play Local DTMF Tone	Enabled 👻	2	
	DTMF Repetition	3 🔹	2	
	Multicast Codec	G722 -	2	
	Play Hold Tone	Enabled 👻	2	
	Play Hold Tone Delay	30	2	
	Allow Mute	Enabled 👻	2	

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

### Voice Mail without PIN

Generally, users have to enter a PIN before they access the voice mail box. If voice mail without PIN feature is enabled, users can access voice mail box without entering PIN. It is especially useful for users who often access mailbox from the IP phone in a secure office.

#### Procedure

Voice mail without PIN can be configured using the configuration files.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Configure voice mail without PIN. Parameters:
		account.1.voice_mail.skin_pin.enable

#### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
account.1.voice_mail.skin_pin.enable	0 or 1	0

Parameters	Permitted Values	Default
Description:		
Enables or disables the IP phone to access voice mail	box without entering	g PIN.
0-Disabled		
1-Enabled		
Web User Interface:		
None		
Phone User Interface:		
None		

### E911

E911 (Enhanced 911) is a location technology that enables the called party to identify the geographical location of the calling party. For example, if a caller makes an emergency call to E911, the feature extracts the caller's information for the police department to immediately identify the caller's location. For more information, refer to https://technet.microsoft.com/en-us/library/dn951423.aspx.

The phone sends the following attributes to LIS to get back the location information:

- 1. MAC address
- 2. IP address
- 3. Subnet
- 4. SIP URI
- 5. Chassis ID / Port ID of L2 switch (This information is obtained using LLDP)

During in-band provisioning, the following have been sent from the Frontend server to the IP phone.

- 1. LIS URI
- 2. Enhanced Emergency Enabled
- 3. Location Required
- 4. Emergency Dial String
- 5. Emergency Dial Mask
- 6. Secondary Location Source
- 7. Notify URI
- 8. Conf URI
- 9. Conf Mode

#### Sample:

ms-subnet: 192.168.1.0.

<provisionGroup name="locationPolicy" >

<propertyEntryList >

<property name="EnhancedEmergencyServicesEnabled" >true</property>

<property name="LocationPolicyTagID" >user-tagid</property>

<property name="LocationRequired" >yes</property></property>

<property name="UseLocationForE911Only" >true</property></property>

<property name="EmergencyDialString" >910086</property>

<property name="EmergencyDialMask">911;912</property>

<property

name="NotificationUri" >sip:7000@yealinkuc.com,sip:80040@yealinkuc.com</property> <property name="ConferenceMode" >oneway</property>

When user dials an emergency number, the location of the user set in phone and the IP phone number are sent out as a part of INVITE message.

Sample:



Note

If user's presence status is DND before dialing an emergency number, it will reset to Available from DND when a 911 number is dialed.

### E911 Location Tip

The network administrator configures geographical location on Skype for Business Server for users. After user signs in, the geographical location is downloaded via in-band provisioning. If geographical location is not provisioned by the server and the LocationRequired property of in-band LocationPolicy is set to 'yes' or 'disclaimer' on the Skype for Business Server, a popup opens in the phone's LCD enabling users to either ignore the notification or edit the location information.



#### Procedure

E911 location tip can be configured using the configuration files or locally.

Configuration	<ul> <li></li> <li></li> </ul>	Configure E911 location tip.
File	<yuuuuuuuuuxx>.ct g</yuuuuuuuuuxx>	Parameters:
		sfb.E911_location_tip
Local		Configure E911 location tip.
	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet?p=featur</phonelpaddress>
		es-general&q=load

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default	
sfb.E911_location_tip	0 or 1	1	
Description:			
Enables or disables the idle screen to display the notification "Location is not set" when the location of the IP phone is not set.			
0-Disabled			
1-Enabled			
Web User Interface:			
Features->General Information->E911 Location Tip			
Phone User Interface:			
None			

#### To configure E911 location tip via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of E911 Location Tip.

Vaglink					Log_Out
	Status Account	Network Features	Settings	Directory	Security
General Information Audio Remote Control Bluetooth Power LED	General_Information CallWaiting AsSend BusyToneDelay scop Return_Code_Refuse	e2 0 603 (Decline)	> > > >		NOTE features-general-note You can click here to get more guides.
	dhcp_hostname E911 Location Tip Update Checking Tin Use DHCP Option 12 SFB Cert Service URI Enable SFB Automat SFB Inactive Time SFB Away Time Device Pairing for Or Confirm	SIP-T46G           Enabled           ne         24           0         Disabled           L	V V V V Cancel		

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

### **Boss-Admin Feature**

The boss-admin feature, which is also called boss-delegate feature, enables a "boss" phone and delegates' phones to ring simultaneously when a user calls the boss. When one party answers the call, the other phone will stop ringing. A boss can assign delegates and delegates can manage calls on behalf of the boss's line. For more information, refer to Yealink phone-specific user guide.

#### To assign delegates using Skype for Business client:

- 1. Open Skype for Business client.
- 2. Sign into Skype for Business client as the person who wants to assign a delegate.
- 3. Click the 🔄 button, and then click Call Forwarding Settings.
- 4. Mark the radio box in Simultaneously ring field.

5. Select My Delegates from the pull-down list of Simultaneously ring.

Skype for Business - Option	is	×
General Personal Contacts List Status My Picture Phones Alerts IM Ringtones and Sounds Audio Device Video Device Call Forwarding File Saving Recording Skype Meetings	Call forwarding       Learn More         Calls will ring you at work and not be forwarded.       Image: Calls will ring you at work and not be forwarded.         Image: Calls will be forwarded immediately and not ring your work number.       Image: Calls will be forwarded immediately and not ring your work number.         Image: Calls will ring you at work and also 2248@yealinkuc.com       Image: Calls will ring you at work and also 2248@yealinkuc.com         Your current call forwarding settings:       Image: Calls will ring you at work +2216 and also ring 2248@yealinkuc.com.         Unanswered calls will go to:       Yoice Mail in 20 seconds         These settings will apply:       All the time         Edit my team-call group members       Edit my delegate members         Edit my delegate members       Edit my delegate members	
	OK Cancel Help	

6. In the **Delegates** dialog box, click **Add**. Each delegate must be a Skype for Business contact.

Call Forwardin	Call Forwarding - Delegates								
Delegates can s	Delegates can schedule Skype Meetings, make calls, and receive calls (if the box is checked) on your behalf.								
Receive Calls	Delegate								
Add	Remove	0 - at the same time	-						
King your deleg	ates after this many seconds:	o - at the same time	OK Can	cel					

7. Select the desired delegates from the **Choose a Delegate** dialog box.

	×						
Choose a Delegate							
Choose a contact to answer your calls.							
1							
Lin Wei - Offline 1 day							
2224-cgc - Away 15 mins - No IM							
2228 - Offline 11 days							
William - Offline 2 days							
<u>O</u> K Can	cel						

- 8. Click OK.
- 9. Click OK in the Delegates dialog box.
- 10. Click OK in the Options dialog box.

The boss's phone is able to accept the response (200 OK) to initial SUBSCRIBE and the response contains the current list of provisioned delegates and indication (in <flags>) that delegate ringing is currently enabled.

For example, when a user calls the boss (extension: 2227), the boss's line and his delegates (2216 and 2529) will ring simultaneously.

<flags name="clientflags" value="delegate\_ring

forward\_audio\_app\_invites"></flags>

#### To remove a delegate from Skype for Business client:

- 1. Open Skype for Business client.
- Sign into Skype for Business client as the person who wants to remove a delegate. Make sure My Delegates option is not selected in either the Simultaneously ring or Forward my calls to list.

3. Click Edit my delegate members.

Skype for Business - Option	15
General Personal Contacts List Status My Picture Phones Akerts IM Ringtones and Sounds Audio Device Video Device Video Device Call Forwarding File Saving Recording Skype Meetings	Call forwarding       Learn More         Calls will ring you at work and not be forwarded.       Calls will ring you at work and not be forwarded.         Calls will be forwarded immediately and not ring your work number.       Calls will be forwarded immediately and not ring your work number.         Calls will be forwarded immediately and not ring your work number.       Calls will ring you at work and also ring another phone or person.         Calls will ring you at work and also ring another phone or person.       Calls will ring you at work +2216.         Unanswered calls will go to:       Yoice Mail in 20 seconds         These settings will apply:       All the time         Edit my team-call group members       Edit my team-call group members
	Edit my delegate members       OK     Cancel

4. Check the checkbox of the delegate you want to remove.

Call Forwardin	Call Forwarding - Delegates							
Delegates can s	Delegates can schedule Skype Meetings, make calls, and receive calls (if the box is checked) on your behalf.							
Peceive Calls	Delegate							
	Lin Wei							
Add	Remove							
Ring your deleg	ates after this many seconds:	0 - at the same time	<b>~</b>					
			ОК	Cancel				

- 5. Click Remove.
- 6. Click OK in the Delegates dialog box.
- 7. Click OK in the Options dialog box.

For example, if the boss removes the delegate whose extension is 2216, then the IP phone is able to accept a Notification of modified delegate list and the NOTIFY contains a list of current provisioned delegate:

t name="delegates"><target uri="sip:2529@yealinkuc.com"></target></target></target></target></target>

### Calendar

Yealink Skype for Business phones integrates with the Microsoft Exchange calendar feature. If your phone is configured to connect to the Microsoft Exchange Server, and the Microsoft® Outlook® application is installed at your site, you can view and join Skype conference, appointment, meeting and event in your Microsoft Outlook application from your phone.

### Setting up a Skype Conference in Outlook

#### To set up a Skype conference in outlook:

1. Open Outlook and go to your calendar.



2. Click HOME->New Skype Meeting.



- 3. In the To box, enter the email addresses of your invitees.
- 4. Enter a subject, location, and then select the start and end time.
- 5. Enter the content about the Skype conference.
- 6. Click Send.

A Skype conference reminder will display on the phone screen of organizer and invitees 15 minutes before the Skype conference starts.

**Note** If you change the Skype conference content (e.g., location, subject, time) via outlook after you have sent the invitation, the phone will update the Skype conference content.

### Setting up an Appointment in Outlook

#### To set up an appointment in outlook:

1. Open Outlook and go to your calendar.



FI	LE		HON	1E	SE	END	/ RE	CEIVE	FC	DLI	DER	VIEW	1	ADI	D-INS	
				ç.	9			<b>E</b>		-	Ē					
Арр	New ointn	nent	N Me	ew eting	Ne Iter	ew ns <del>•</del>	٢	Vew Skyp Meeting	e	Т	oday	v Next 7 Days	[	Day	Work Week	V
			New		E	E	- <u>m</u> ai	il Messag	e		Go	To 🕞				Arı
	•		201	6年3	3. 🛄	A	ppo	intment			Þ	2016年3日				
	日	_	_	Ξ		N	leeti	ng				2010	-	57.	,	
	28	29	1	2	1.2	1 C	onta	act		Ð	日			星	朝一	
	6	7	8	9		T	ack			2	28E	I _+		29	B	
	13	14	15	16		-	usk u b			-						
	20	21	22	23	_	A	II Da	y E <u>v</u> ent		ł					_	
	27	28	<b>29</b>	30		N	lore	Items	÷		6	Recurring	јДр	point	ment	
					9	<u>s</u>	kype	Meeting				Recurring	g Me	eting		
			201	6年4	月				6			Recurring	g E <u>v</u> e	ent		
	日	_	=	Ξ	四	Ŧ	六		01	1,	88	Contact	<u>G</u> rou	р		
						1	2				2.	Task Reg	uest			
	3	4	5	6	7	8	9					Internet l	av			
	10	11	12	13	14	15	16			Ľ	<b>.</b>	and an				
	17	18	19	20	21	22	23				-8	Ch <u>o</u> ose H	orm			
	24	25	26	27	28	29	30		13			Choose <u>I</u>	nfoP	ath F	orm	
	1	2	3	4	5	6	7				5	Outlook	Data	<u>F</u> ile		

2. Click Home->New Items->More Items->Recurring Appointment.

- **3.** Enter the appointment time.
- 4. Click OK.
- 5. Enter a subject, location and the appointment content.
- 6. Click Save & Close.

A reminder will display on the phone screen 15 minutes before the appointment starts.

### Setting up a Meeting in Outlook

#### To set up a meeting in outlook:

1. Open Outlook and go to your calendar.



										_						
FIL	E		HON	1E	S	END	/ RE	CEIVE		FO	LDER	VIEW		AD	D-INS	
1	New	ant	N	ew	N	New N		Vew Sky	pe		Today	/ Next 7	D	ay	Work	E W
~ppc	/		New	cung		] E	- <u>m</u> ai	il Messa	ge		Go	To G			TTCCK	Arr
	•		201	6年: 二		A	ppo	intment	t		Þ	2016	年:	3月	]	
	28	29	1	2			l <u>e</u> eti	ng			日			星	明—	
	6	7	8	9	2		ask				28E	3 =+	_	29	E	
	13 20	14 21	15 22	16 23		A	ll Da	y E <u>v</u> ent								
	27	28	29	30		Ν	lore	Items		F	5	Recurring	Арр	oint	ment	
					6	<u>S</u>	kype	Meetin	g			Re <u>c</u> urring	Mee	ting		
			201	6年4	归				6			Recurring	Ever	nt		
	日	_	=	Ξ	四	五	${\rightarrow}$		0		28	Contact G	iroup	)		
						1	2				<b>R</b> .	Task Regu	Jest			
	3	4	5	6	7	8	9					Internet F	ax			
	10	11	12	13	14	15	16					CI	<u></u>			
	17	18	19	20	21	22	23					Ch <u>o</u> ose F	orm.			
	24	25	26	27	28	29	30		1	.3	Q2	Choose <u>I</u> r	foPa	ath F	orm	
	1	2	3	4	5	6	7				5	Outlook [	)ata	<u>F</u> ile		

2. Click Home->New Items->More Items->Recurring Meeting.

- **3.** Enter the meeting time.
- 4. Click OK.
- 5. In the To box, enter the email addresses of your invitees.
- 6. Enter a subject, location and the meeting content.
- 7. Click Send.

A reminder will display on the phone screen of organizer and invitees 15 minutes before the meeting starts.

### Setting up an Event in Outlook

#### To set up an event in outlook:

1. Open Outlook and go to your calendar.



FI	LE		HON	1E	S	SEND / RECEIV			FC	DER	VIEW		ADI	D-INS	
				ç.	9			<b>E</b>							
Ann	New	hent	N Me	ew eting	N- Iter	ew ns <del>v</del>	r	Vew Skype Meeting	2	Toda	y Next 7	D	ay	Work	V
~~~	onnen	ic.iii	New	cung	E	] E	- <u>m</u> ai	il Message		Go	To 🕞			WEEK	Arr
	•		201	6年3		A	ppo	intment		•	2016	Æ	зE	1	
	日	_	_	Ξ	1953	Z N	leeti	na			2010	+	5	1	
	28	29	1	2	8		onta	act		旧			星	朝—	
	6	7	8	9		ы <u>с</u> Г т	le			28E	3 =+	_	29	Β	
	13	14	15	16		1	dSK			-					
	20	21	22	23	_	A	II Da	y E <u>v</u> ent		_					
	27	28	<b>29</b>	30		Ν	lore	Items	×	5	Recurring	<u>A</u> pp	point	ment	
					9	S	kype	Meeting			Re <u>c</u> urring	ј Ме	eting		
			201	6年4	月				CE.		Recurring	I E <u>v</u> e	nt		
	日	_	=	Ξ	四	五	六		0	20	Contact (	Grou	р		
						1	2			<b>R</b> .	Task Reg	uest			
	3	4	5	6	7	8	9				Joternet F	ax			
	10	11	12	13	14	15	16				Character F				
	17	18	19	20	21	22	23				Ch <u>o</u> ose F	orm			
	24	25	26	27	28	29	30		13	1	Choose <u>I</u> r	nfoP	ath F	orm	
	1	2	3	4	5	6	7			5	Outlook [	Data	<u>F</u> ile		

2. Click Home->New Items->More Items->Recurring Event.

- 3. Enter the event time.
- 4. Click OK.
- 5. Enter a subject, location and the event content.
- 6. Click Save & Close.

A reminder will display on the phone screen 15 minutes before the event starts.

### Using the Calendar

To use the calendar feature on your phone, you must sign into the phone using User Sign-in or Device Pairing for Online method. So the phones can display the Microsoft Exchange calendar which gives you quick access to Skype conference, appointment, meeting and event.

### Procedure

Calendar can be configured using the configuration files only.

		Configure calendar feature.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:
		sfb.calendar.enable

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default					
sfb.calendar.enable	0 or 1	1					
Description:							
Enables or disables the calendar feature.							
0-Disabled							
1-Enabled							
If it is set to 1 (Enabled), user can use calence	lar feature on the IP phone.						
If it is set to 0 (Disabled), user cannot use ca	lendar feature on the IP phone	€.					
Web User Interface:							
None							
Phone User Interface:							
Menu->Calendar							

### Viewing the Calendar

You can view all schedules via the calendar on your phone.

#### To view the calendar via phone user interface:

#### 1. Press Menu->Calendar.

The calendar displays the schedules of today by default.



Press to see Month View Press to

Press to see Schedule View

No.	Name	Description
1	Monthview	Shows all the days which have schedules in the
I		selected month.
0	Davision	Shows all schedules of the selected day,
Z	Ddy view	including the subject, start and end time.

No.	Name	Description
		Shows the details of the selected schedule,
3	Schedule view	including the subject, participants, organizer,
		start and end time, location and content.

2. Press the **Back** soft key to return to the pervious screen.

### Working with Schedule Reminders

If you have a schedule, a reminder pop-up is displayed 15 minutes before it starts. The reminder shows the main information of the schedule, including subject and the rest time.



If you receive a reminder of an appointment, meeting or event, you can:

- Press the **Ignore** soft key to permanently remove the reminder from the screen and stop all future reminders for this schedule.
- Press the **Snooze** soft key to temporarily remove the reminder from the screen, until the next schedule reminder. The reminder will appear every 5 minutes before the schedule starts.
- Press the **Detail** soft key to view specific information.

#### If you receive a reminder of a Skype conference, you can:



• Press the **Ignore** soft key to permanently remove the reminder from the screen and stop all future reminders for the Skype conference.

- Press the **Snooze** soft key to temporarily remove the reminder from the screen, until the next schedule reminder. The reminder will appear every 5 minutes before the Skype conference starts.
- Press the **Detail** soft key to view specific information about the Skype conference, including the Skype conference's subject, participants, organizer, start and end time, location and content.
- Press the **Join** soft key to join the Skype conference.
- Note When receives a Skype conference reminder during a call, you can press the Join soft key to join the Skype conference directly. Current call will be held and you can resume it after the Skype conference.

For more information on how to use the calendar feature, refer to the Yealink phone-specific user guide.

### BToE

BToE (Better Together over Ethernet) feature enables SIP IP phones to interoperate with the Skype for Business client for third party call control. You can answer, place, hold and resume audio calls on your phone and the Skype for Business client simultaneously. In order to use BToE, you need to download and install the Yealink BToE Connector application on your computer.

### Procedure

BToE can be configured using the configuration files.

		Configure BToE feature.		
		Parameters:		
Configuration	<y0000000000xx>.cfg</y0000000000xx>	sip.btoe.enable		
File		Configures the BToE paring PIN.		
		Parameters:		
		sip.btoe.secure_pin		
		Configure BToE feature.		
		Configures the BToE paring PIN.		
	Web User Interface	Navigate to:		
Local		http:// <phonelpaddress>/servlet?p=set</phonelpaddress>		
		tings-btoe&q=load		
	Phone User Interface	Configure BToE feature.		
	THORE USER INTERIOCE	Configures the BToE paring PIN.		

### Details of Configuration Parameters:

Parameters	Permitted Values	Default			
sip.btoe.enable	0 or 1	1			
Description:					
Enables or disables the BToE (Better Together over Ethe	ernet) feature.				
0-Disabled					
1-Enabled					
If it is set to 1 (Enabled), BToE is enabled on the phone. Skype for Business Client.	Your phone can po	air with			
If it is set to 1 (Disabled), BToE is disabled on the phone Skype for Business Client.	. Your phone cannc	ot pair with			
Web User Interface:					
Settings->BToE->BToE					
Phone User Interface:					
Menu->Advanced->BToE->BToE					
sip.btoe.secure_pin	String	0000			
Description:					
Configures the BToE paring PIN. Your phone can pair with Skype for Business client when you enter the correct BToE paring PIN on PC.					
Note: It works only if the value of the parameter "sip.bt	oe.enable" is set to	1			
(Enabled).					
Web User Interface:					
Settings->BToE->BToE paring PIN					
Phone User Interface:					
Menu->Advanced->BToE->BToE Pairing Pin					

### To configure BToE feature via web user interface:

- 1. Click on Settings->BToE.
- 2. Select the desired value from the pull-down list of **BTOE**.

3. Enter the desired PIN in the **BToE pairing PIN** field.

Varlink						Log Out	
	Status	Account	Network	Features	Settings	Directory	Security
Preference	В	ToE:					NOTE
Time&Date		BToE BToE Pairing State	115	Enabled	•		settings-btoe-note
Upgrade		BToE paring PIN		0000			You can click here to get more guides.
Auto Provision			Confirm	Cancel			
Configuration							
Dial Plan							
Voice							
Tones							
Phone Lock							
Location							
EXP Module							
ВТОЕ							

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

#### To configure BToE feature via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->BTOE.
- 2. Press (•), (•) or the Switch soft key to select Enabled from the BTOE field.
- 3. Enter the pairing PIN in the **BToE Pairing Pin** filed.

The pairing PIN consists of 4-6 digits, the default PIN is "0000".

4. Press Save soft key to accept the change.

### **EXP40 Expansion Module**

The Yealink EXP40 expansion module is an ideal choice for receptionists, administrative assistants, call center agents, power-users, and executives who need to handle large call volumes on a daily basis.

### Assigning Skype for Business Contacts to EXP40

You can connect an EXP40 expansion module to SIP-T48G/T46G IP phones only. When your SIP-T48G/T46G is registered with a Skype for Business Server, you can assign Skype for Business contacts to line keys on your EXP40 expansion module, so that you can quickly call contact by pressing the corresponding line key. You can also monitor your Skype for Business contacts' presence status from your expansion module. For more information on contact's presence, refer to Reading Icons on page 32.

To use EXP40 expansion modules, connect the Ext jack of the IP phone and the Ext in jack of the expansion module using one supplied cord. If you need to connect multiple expansion modules, connect the Ext out jack of the previous expansion module and

the Ext in jack of the next expansion module using another supplied cord.

Each EXP40 expansion module provides you with 20 lines keys and 2 display pages, supporting a total of 40 lines that you can set up as Skype for Business contacts. You can connect up to 6 EXP40 expansion modules to your phone to support a maximum of 240 line keys per phone.

**Note** Local contacts cannot be displayed on the EXP40 expansion module. Only Skype for Business contacts can be displayed on the EXP40 expansion module.

### Procedure

EXP40 expansion module can be configured locally.

Locally	Web User Interface	Configure the desired Skype for Business group to be displayed on the EXP40 expansion module. <b>Navigate to:</b> http:// <phonelpaddress>/servlet?p= settings-expmodule&amp;g=logd</phonelpaddress>	
	Phone user Interface	Configure the desired Skype for Business group to be displayed on the EXP40 expansion module.	

To assign Skype for Business contacts to the EXP40 expansion module via web user interface:

- 1. Click on Settings->EXP Module.
- 2. Select the desired Skype for Business group from the pull-down list of **ModuleX** (X ranges from 1 to 6 depending on the amount of the connected EXP40).

					Log Out
YEAIIINK   146G	Status	t Network Features	5 Settings	Directory	Security
Preference	Module Number	Display Group	-		NOTE
Time & Date	Module1	Null	·		settings-expmodule-note
Upgrade		Confirm	Cancel		You can click here to get more quides.
Auto Provision					
Configuration					
Dial Plan					
Voice					
Tones					
Phone Lock					
Location					
EXP Module					

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

The selected Skype for Business group will be displayed on the selected expansion module.

# To assign Skype for Business contacts to the EXP40 expansion module via phone user interface:

- 1. Press Menu->Basic->Exp Module.
- Press or , or the Switch soft key to select the desired Skype for Business group from the ModuleX field (X ranges from 1 to 6 depending on the amount of the connected EXP40).



3. Press the Save soft key to accept the change.

The selected Skype for Business group will be displayed on the selected expansion module.

## **Configuring Advanced Features**

This chapter provides information for making configuration changes for the following advanced features:

- Multicast Paging
- Action URI
- VLAN
- Quality of Service
- IPv6 Support

### **Multicast Paging**

Multicast paging allows IP phones to send/receive Real-time Transport Protocol (RTP) streams to/from the pre-configured multicast address(es) without involving SIP signaling. Up to 10 listening multicast addresses can be specified on the IP phone.

### Sending RTP Stream

Users can send an RTP stream without involving SIP signaling by pressing a **Paging** soft key. A multicast address (IP: Port) should be assigned to the multicast paging key, which is defined to transmit RTP stream to a group of designated IP phones. When the IP phone sends the RTP stream to a pre-configured multicast address, each IP phone preconfigured to listen to the multicast address can receive the RTP stream. When the originator stops sending the RTP stream, the subscribers stop receiving it.

#### Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Specify a multicast codec for the IP phone to send the RTP stream. Parameter:
		multicast.codec

		Configure the multicast IP address and port number for a paging list key. Parameter: multicast.paging_address.X.ip_ad dress		
		Configure the multicast paging group name for a paging list key. <b>Parameter:</b> multicast.paging_address.X.label		
		Specify a multicast codec for the IP phone to send the RTP stream. Navigate to: http:// <phonelpaddress>/servlet? p=features-general&amp;q=load</phonelpaddress>		
Local	Web User Interface	Configure the multicast IP address and port number for a paging list key. Configure the multicast paging group name for a paging list key.		
		Navigate to: http:// <phonelpaddress>/servlet? p=contacts-multicastIP&amp;q=load</phonelpaddress>		
	Phone User Interface	Configure the multicast IP address and port number for a paging list key. Configure the multicast paging		
		group name for a paging list key.		

### Details of the Configuration Parameter:

Parameters	Permitted Values	Default
multicast.codec	PCMU, PCMA, G729, G722	G722
Description:		
Configures the codec of multicast paging.		
Example:		
multicast.codec = G722		

Parameters	Permitted Values	Default			
Web User Interface:					
Features->General Information->Multicast C	odec				
Phone User Interface:					
None					
multicast.paging_address.X.ip_address	Strin -	Diamir			
(X ranges from 1 to 10)	Sning	ыалк			
Description:					
Configures the IP address and port number	of the multicast paging	group in the			
paging list.					
It will be displayed on the LCD screen when	placing the multicast p	baging call.			
Example:					
multicast.paging_address.1.ip_address = 224	4.5.6.20:10008				
multicast.paging_address.2.ip_address = 224	4.1.6.25:1001				
Note: The valid multicast IP addresses range	trom 224.0.0.0 to 239.2	55.255.255.			
Web User Interface:					
Directory->Multicast IP->Paging List->Paging	Address				
Phone User Interface:					
Menu->Features->Paging List->Option->Edit-	>Address	ſ			
multicast.paging_address.X.label					
(X ranges from 1 to 10)	Sinig	DIGITK			
Description:					
Configures the name of the multicast paging	g group to be displaye	d in the paging			
list.					
It will be displayed on the LCD screen when	placing the multicast p	baging calls.			
Example:					
multicast.paging_address.1.label = Product					
multicast.paging_address.2.label = Sales					
Web User Interface:	Web User Interface:				
Directory->Multicast IP->Paging List->Label					
Phone User Interface:					
Menu->Features->Paging List->Option->Edit-	>Label				

### To configure a codec for multicast paging via web user interface:

1. Click on Features->General Information.

2. ssSelect the desired codec from the pull-down list of **Multicast Codec**.

No edinda		Log Out
TECIINK   T46G	Status Account Network Features Settings Di	rectory Security
General	General Information 🕜	NOTE
Information	Call Waiting Enabled 🔻 🥐	
Audio	Key As Send #	This call feature allows your
Damata Control	Busy Tone Delay (Seconds) 0 🔹 🤪	phone to accept other incoming calls during the conversation.
Remote Control	Return code when refuse 603 (Decline) 🔹 🍞	Key As Send
Bluetooth	Time-Out for Dial-Now Rule 1	Select * or # as the send key.
Power LED	Dial Search Delay 1	You can click here to get
	180 Ring Workaround Disabled 👻 🍞	more guides.
	Save Call Log Enabled 👻 🕜	
	Suppress DTMF Display Disabled 🗸 🍞	
	Suppress DTMF Display Delay Disabled 🗸 🥜	
	Play Local DTMF Tone Enabled -	
	DTMF Repetition 3 🗸	
	Multicast Codec G722 🗸 🕜	
	Play Hold Tone Enabled 👻 🕜	

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

To configure two sending multicast addresses via web user interface:

- 1. Click on Directory->Multicast IP.
- 2. Enter the sending multicast address and port number in the Paging Address field.
- 3. Enter the label in the Label field.

The label will appear on the LCD screen when sending the RTP multicast.

			_	-	Log Out
YEAIINK   T46G	Status	Network Feat	ures Settings	Directory	Security
Local Directory	Multicast Listening				NOTE
Multicast IP	Paging Barge	10	~		contacts-multicastIP-note
Settings	Paging Priorit	y Active Enable	ed 🗸		You can click here to get
		•			more guides.
	Paging List				
	Index	Paging Address	Label		
	1	224.5.6.20:10008	Product		
	2	224.5.6.20:10001	Sales		
	3				
	4				
	5				
	6				
	7				
	8				
	9		-		
		onfirm	Cancel		

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

To configure paging list via phone user interface:

- 1. Press Menu->Features->Paging List.
- **2.** Press  $(\bullet)$  or  $(\bullet)$  to select a desired paging group.

3. The default tag is Empty if it is not configured before.

Paging List			
1. (Empty)		Î	
2. (Empty)			
3. (Empty)			
4. (Empty)			
5. (Empty)		~	
Back	Option	Paging	

- 4. Press the **Option** soft key, and then press the **Edit** soft key.
- 5. Enter the multicast IP address and port number (e.g., 224.5.6.20:10008) in the Address field.
- 6. The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.

	Edit Pag	ging Address	
1. Number:		1	
2. Address:		224.5.6.20:100	08
3. Label:			
Back	123	Delete	Save

- 7. Enter the group name in the Label field.
- 8. Press the Save soft key to accept the change.
- 9. Repeat steps 2 to 6, you can add more paging groups.

For SIP-T40P IP phones, the third line key will change to be a paging list key automatically. When the phone is idle, you can press the paging list key to access the paging list.

For SIP-T46G/T42G/T41P IP phones, the second line key will change to be a paging list key automatically. When the phone is idle, you can press the paging list key to access the paging list.

For SIP-T48G IP phones: when the phone is idle, you can tap...->Features->Paging list to access the paging list.

### **Receiving RTP Stream**

IP phones can receive an RTP stream from the pre-configured multicast address(es) without involving SIP signaling, and can handle the incoming multicast paging calls differently depending on the configurations of Paging Barge and Paging Priority Active.

#### **Paging Barge**

This parameter defines the priority of the voice call in progress, and decides how the IP phone handles the incoming multicast paging calls when there is already a voice call in progress. If the value of the parameter is configured as disabled, all incoming multicast paging calls will be automatically ignored. If the value of the parameter is the priority value, the incoming multicast paging calls with higher or equal priority are automatically answered and the ones with lower priority are ignored.

#### **Paging Priority Active**

This parameter decides how the IP phone handles the incoming multicast paging calls when there is already a multicast paging call in progress. If the value of the parameter is configured as disabled, the IP phone will automatically ignore all incoming multicast paging calls. If the value of the parameter is configured as enabled, an incoming multicast paging call with higher priority or equal is automatically answered, and the one with lower priority is ignored.

#### Procedure

Configuration changes can be performed using the configuration files or locally.

	<y000000000xx>.cfg</y000000000xx>	Configure the listening multicast address.
		Parameters:
Configuration File		multicast.listen_address.X.ip_address
		multicast.listen_address.X.label
		Configure Paging Barge and Paging Priority Active features.
		Parameters:
		multicast.receive_priority.enable
		multicast.receive_priority.priority
Local	Web User Interface	Configure the listening multicast
		address.
		Configure Paging Barge and Paging
		Navigate to:
		http:// <phonelpaddress>/servlet?p=c</phonelpaddress>
		ontacts-multicastIP&q=load

#### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
------------	------------------	---------

Parameters	Permitted Values	Default		
multicast.listen_address.X.ip_address	IP address: port	Plank		
(X ranges from 1 to 10)	ir dddiess. poli	BIGHK		
Description:				
Configures the multicast address and port numb	er that the IP phone list	tens to.		
Example:	Example:			
multicast.listen_address.1.ip_address = 224.5.6.20	:10008			
Note: The valid multicast IP addresses range from	1 224.0.0.0 to 239.255.25	55.255.		
Web User Interface:				
Directory->Multicast IP->Multicast Listening->Liste	ning Address			
Phone User Interface:				
None				
multicast.listen_address.X.label	String within 99	Diamin		
(X ranges from 1 to 10)	characters	BIONK		
Description:				
(Optional.) Configures the label to be displayed on the LCD screen when receiving the multicast paging calls.				
Example:				
multicast.listen_address.1.label = Paging1				
Web User Interface:				
Directory->Multicast IP->Multicast Listening->Label				
Phone User Interface:				
None				
multicast.receive_priority.enable	0 or 1	1		
Description:				
Enables or disables the IP phone to handle the incoming multicast paging calls when there is an active multicast paging call on the IP phone.				
0-Disabled				
1-Enabled				
If it is set to 0 (Disabled), the IP phone will ignore the incoming multicast paging				
calls when there is an active multicast paging call on the IP phone.				
If it is set to 1 (Enabled), the IP phone will receive the incoming multicast paging call with a higher or equal priority and ignore that with a lower priority.				

### Web User Interface:

Parameters	Permitted Values	Default	
Directory->Multicast IP->Paging Priority Active			
Phone User Interface:			
None			
multicast.receive_priority.priority	Integer from 0 to 10	10	
Description:			
Configures the priority of the voice call (a normal phone call rather than a multicast paging call) in progress.			
1 is the highest priority, 10 is the lowest priority.			
0-Disabled			
1-1			
<b>2</b> -2			
<b>3</b> -3			
4-4			
<b>5</b> -5			
<b>6</b> -6			
7-7			
8-8			
9-9			
<b>10</b> -10			
If it is set to 0 (Disabled), all incoming multicast paging calls will be automatically ignored when a voice call is in progress.			
If it is not set to 0 (Disabled), the IP phone will receive the incoming multicast paging call with a higher or same priority than this value and ignore that with a lower priority than this value when a voice call is in progress.			
Web User Interface:			
Directory->Multicast IP->Paging Barge			
Phone User Interface:			
None			

### To configure a listening multicast address via web user interface:

- 1. Click on Directory->Multicast IP.
- Enter the listening multicast address and port number in the Listening Address field.
   1 is the highest priority and 10 is the lowest priority.
- 3. Enter the label in the Label field.
| Voglink         |                     |                  |          |          |           | Log Out                   |
|-----------------|---------------------|------------------|----------|----------|-----------|---------------------------|
|                 | Status              | Network          | Features | Settings | Directory | Security                  |
| Local Directory | Multicast Listening |                  |          |          |           | NOTE                      |
| Multicast IP    | Paging Barge        |                  | 10       | •        |           | contacts-multicastIP-note |
| Cattings        | Paging Priority     | Active           | Enabled  | •        |           | Vou can click here to get |
| Setungs         | IP Address          | Listening Addres | s        | Label    | priority  | more guides.              |
|                 | 1 IP Address        | 224.5.6.20:10008 | Te       | st       | 1         |                           |
|                 | 2 IP Address        |                  |          |          | 2         |                           |
|                 | 3 IP Address        |                  |          |          | 3         |                           |
|                 | 4 IP Address        |                  |          |          | 4         |                           |
|                 | 5 IP Address        |                  |          |          | 5         |                           |
|                 | 6 IP Address        |                  |          |          | 6         |                           |
|                 | 7 IP Address        |                  |          |          | 7         |                           |
|                 | 8 IP Address        |                  |          |          | 8         |                           |
|                 | 9 IP Address        |                  |          |          | 9         |                           |
|                 | 10 IP Address       |                  |          |          | 10        |                           |

The label will appear on the LCD screen when receiving the RTP multicast.

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

To configure paging barge and paging priority active features via web user interface:

- 1. Click on Directory->Multicast IP.
- 2. Select the desired value from the pull-down list of **Paging Barge**.
- 3. Select the desired value from the pull-down list of **Paging Priority Active**.

alink							Log O
CIINK   T23G	Status	Account	Network	Features	Settings	Directory	Security
local Directory	Multicast Lis	tening					NOTE
Aulticast IP		Paging Barge		10	~		contacts-multicastIP-note
		Paging Priority A	ctive	Enabled	~		You can click here to get more guides.
	1 IP A	ddress Address	Listening Ad	dress	Label	priority 1	-
	2 IP	Address				2	
	3 IP	Address				3	
	4 IP	Address				4	
	5 IP	Address				6	
	7 IP	Address				7	
	8 IP	Address				8	
	9 IP	Address				9	
	10 IP	Address				10	

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

## Action URI

### **HTTP/HTTPS GET Request**

Action URI allows IP phones to interact with web server application by receiving and

handling an HTTP or HTTPS GET request. When receiving a GET request, the IP phone will perform the specified action and respond with a 200 OK message.

## Configuring Trusted IP Address for Action URI

For security reasons, IP phones do not receive and handle HTTP/HTTPS GET requests by default. You need to specify the trusted IP address for action URI. When the IP phone receives a GET request from the trusted IP address for the first time, the LCD screen prompts the message "Allow Remote Control?". You can specify one or more trusted IP addresses on the IP phone, or configure the IP phone to receive and handle the URI from any IP address.

You can use action URI feature to capture the IP phone's current screen. For more information, refer to Capturing the Current Screen of the Phone on page 219.

### Procedure

Specify the trusted IP address for action URI using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Specify the trusted IP address(es) for sending the action URI to the IP phone.	
		Parameter:	
		features.action_uri_limit_ip	
		Specify the trusted IP address(es) for sending the action URI to the IP phone.	
Local	Web User Interface	Navigate to:	
		http:// <phonelpaddress>/servlet? p=features-remotecontrl&amp;q=load</phonelpaddress>	

Details of the Configuration Parameter:

Parameter	Permitted Values	Default				
features.action_uri_limit_ip	IP address or any	Blank				
Description:						
Configures the IP address of the server from which the IP phone receives the action URI requests.						
For discontinuous IP addresses, multiple IP add	resses are separated b	y commas.				
For continuous IP addresses, the format likes *.* 0~255.	•.*.* and the "*" stands	for the values				
For example: 10.10.*.* stands for the IP address	es that range from 10.1	0.0.0 to				

Parameter	Permitted Values	Default			
10.10.255.255.					
If left blank, the IP phone will reject any HTTP G	ET request.				
If it is set to "any", the IP phone will accept and handle HTTP GET requests from any IP address.					
Example:					
features.action_uri_limit_ip = any	features.action_uri_limit_ip = any				
<b>Note</b> : It works only if the value of the parameter "features.action_uri.enable" is set to 1 (Enabled).					
Web User Interface:					
Features->Remote Control->Action URI allow IP	List				
Phone User Interface:					
None					

### To configure the trusted IP address(es) for action URI via web user interface:

- 1. Click on Features->Remote Control.
- 2. Enter the IP address or any in the Action URI allow IP List field.

Multiple IP addresses are separated by commas. If you enter "any" in this field, the IP phone can receive and handle GET requests from any IP address. If you leave the field blank, the IP phone cannot receive or handle any HTTP GET request.

Vaglink			Log Out
	Status Account Network	Features Settings Directory	Security
General Information Audio Remote Control Bluetooth Power LED	Remote control: Action URI allow IP List Confirm	any 🕜	NOTE Remote Control parameters for administrator.For security reasons, IP phones do not receive and handle HTTP/HTPS GET requests by default. You need to specify the trusted IP address for action URI. When the IP phone receives a GET request from the trusted IP address for the first time, the LCD screen prompts the message "Alow Remote Control?". You can specify one or more trusted IP addresses on the IP phone, or configure the IP phone to receive and handle the URI from any. IB address

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

## Capturing the Current Screen of the Phone

You can capture the screen display of the IP phone using the action URI. IP phones support handling an HTTP or HTTPS GET request. The URI format is http(s)://<phoneIPAddress>/screencapture. The captured picture can be saved as a BMP or JPEG file. You can also use the URI "http(s)://<phonelPAddress>/screencapture/download" to capture the screen display first, and then download the image (which is saved as a JPG file and named with the IP phone model and the capture time) to the local system. Before capturing the IP phone's current screen, ensure that the IP address of the PC is included in the trusted IP address for Action URI on the IP phone.

When you capture the screen display, the IP phone may prompt you to enter the user name and password of the administrator if web browser does not remember the user name and password for web user interface login.

**Note** IP phones also support capturing the screen display using the old URI "http://<phonelPAddress>/servlet?command=screenshot".

#### To capture the current screen of the IP phone:

- 1. Enter request URI (e.g., http://10.2.20.126/screencapture) in the browser's address bar and press the Enter key on the keyboard.
- **2.** Do one of the following:
  - If it is the first time you capture the phone's current screen using the computer, the browser will display "Remote control forbidden", and the LCD screen will prompt the message "Allow remote control?".

Press the OK soft key on the IP phone to allow remote control. The phone will return to the previous screen. Refresh the web page.

The browser will display an image showing the IP phone's current screen. You can save the image to your local system.

_2016.04.05_10.22 × +			
0.2.20.126/screencapture		C Q Search	☆ 自 ♥ 4
	10 22 Tue Apr 05		
🕂 Lin Wei			
Daisy			
Hedy			
💦 William			
Boss Admi	in +2216		
i Statu	s OHistory & Directory	Menu	
	,		

- Else, the browser will display an image showing the IP phone's current screen directly. You can save the image to your local system.
- **Note** Frequent capture may affect the IP phone performance. Yealink recommend you to capture the IP phone screen display within a minimum interval of 4 seconds.

# VLAN

VLAN (Virtual Local Area Network) is used to logically divide a physical network 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 IP phone is to insert tag with VLAN information to the packets generated by the IP phone. When VLAN is properly configured for the ports (Internet port and PC port) on the IP phone, the IP phone will tag all packets from these ports with the VLAN ID. The switch receives and forwards the tagged packets to the corresponding VLAN according to the VLAN ID in the tag as described in IEEE Std 802.3.

VLAN on IP phones allows simultaneous access for a regular PC. This feature allows a PC to be daisy chained to an IP phone and the connection for both PC and IP phone to be trunked through the same physical Ethernet cable.

In addition to manual configuration, the IP phone also supports automatic discovery of VLAN via LLDP, CDP or DHCP. The assignment takes effect in this order: assignment via LLDP/CDP, 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 IP phone 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 endpoint:

- Capabilities Discovery -- allows LLDP-MED endpoint to determine the capabilities that the connected switch supports and has enabled.
- Network Policy -- provides voice VLAN configuration to notify the IP phone 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 IP phone is powered, power priority, and how much power the endpoint needs.
- Inventory Management -- provides a means to effectively manage the IP phone and its attributes, such as model number, serial number and software revision.

TLV Type	TLV Name	Description		
	Chassis ID	The network address of the IP phone.		
	Port ID	The MAC address of the IP phone.		
Mandatory TLVs	Time To Live	Seconds until data unit expires.		
		The default value is 180s.		
	End of LLDPDU	Marks end of LLDPDU.		
	System Name	Name assigned to the IP phone.		
	System Nome	The default value is "SIP-T46G".		
		Description of the IP phone.		
	System Description	Description includes firmware version o		
Optional TLVs				
		capabilities.		
	Capabilities	The Telephone capability is supported		
		and enabled by default.		
	Port Description	Description of port that sends data unit.		
	1 on Description	The default value is "WAN PORT".		
		Duplex mode and network speed		
		settings of the IP phone.		
		enabled by default.		
IEEE Std 802.3	MAC/PHY	The advertised capabilities of PMD.		
Organizationally	Configuration/Status	Auto-Negotiation is:		
Specific ILV		100BASE-TX (full duplex mode)		
		100BASE-TX (half duplex mode)		
		10BASE-T (full duplex mode)		
		10BASE-T (half duplex mode)		
TIA		The MED device type of the IP phone		
Organizationally	Media Capabilities	and the supported LLDP-MED TLV type		
Specific TLVs		The supported LLDP-MED TLV types are:		

TLVs supported by the IP phone are summarized in the following table:

TLV Type	TLV Name	Description		
		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 IP phone.		
	Inventory – Firmware Revision	Firmware revision of the IP phone.		
	Inventory – Software Revision	Software revision of the IP phone.		
	Inventory – Serial Number	Serial number of the IP phone.		
	Inventory – Manufacturer Name	Manufacturer name of the IP phone. The default value is "IP_Phone".		
	Inventory – Model Name	Model name of the IP phone. The default value is "T46".		
	Asset ID	Assertion identifier of the IP phone.		

### Procedure

LLDP can be configured using the configuration files or locally.

		Configure LLDP.	
Configuration File	1000000000vv cfa	Parameters:	
Configuration File	<y000000000000000000000000000000000000< td=""><td>network.lldp.enable</td></y000000000000000000000000000000000000<>	network.lldp.enable	
		network.lldp.packet_interval	
		Configure LLDP.	
	Web User Interface	Navigate to:	
Local		http:// <phonelpaddress>/servle</phonelpaddress>	
		t?p=network-adv&q=load	
	Phone User Interface	Configure LLDP feature.	

### Details of Configuration Parameters:

Parameters	Permitted Values	Default					
network.lldp.enable	0 or 1	1					
Description:							
Enables or disables the LLDP (Linker Layer Discovery Protocol) feature on the IP phone.							
0-Disabled							
1-Enabled							
<b>Note:</b> If you change this parameter take effect.	<b>Note:</b> If you change this parameter, the IP phone will reboot to make the change take effect.						
Web User Interface:							
Network->Advanced->LLDP->Activ	е						
Phone User Interface:							
Menu->Advanced (default passwo	ord: admin) ->Network->LL[	DP->LLDP Status					
network.lldp.packet_interval	Integer from 1 to 3600	60					
Description:							
Configures the interval (in seconds) Discovery Protocol) request.	) for the IP phone to send t	the LLDP (Linker Layer					
<b>Note:</b> It works only if the value of the parameter "network.lldp.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take effect.							
Web User Interface:							
Network->Advanced->LLDP->Packet Interval (1~3600s)							
Phone User Interface:							
Menu->Advanced (default passwo	ord: admin) ->Network->LL[	DP->Packet Interval					

### 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.

<b>Vealink</b> Inco	Log 0				
	Status	t Network Fea	tures Settings	Directory	Security
Basic	LLDP 🕜				NOTE
DC Dort		Active	Enabled	-	VIAN
POPOIL		Packet Interval (1~3600s)	60		A VLAN is a logical local area
Advanced	CDP 🕜				beyond a single traditional LAN
		Active	Enabled	•	to a group of LAN segments, given specific configurations.
		Packet Interval (1~3600s)	60		QoS
	VLAN 🕜				When the network capacity is insufficient, OoS could provide
	WAN Port	Active	Disabled	•	priority to users by setting the
		VID (1-4094)	1		Local RTB Boxt
		Priority	0	•	Define the port for voice
	PC Port	Active	Disabled	•	transmission.
		VID (1-4094)	1		You can click here to get more quides.
		Priority	0	•	more guides.
	DHCP VLAN	Active	Enabled	•	
		Option (1-255)	132		
	Port Link 🕜				
		WAN Port Link	Auto Negotiate	•	
		PC Port Link	Auto Negotiate	-	
	Voice QoS 🕜				
		Voice QoS (0~63)	46		
		SIP Qos (0~63)	26		

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 settings will take effect after a reboot.

5. Click OK to reboot the IP phone.

### To configure LLDP feature via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Network->LLDP->LLDP Status.
- Press (•) or (•), or the Switch soft key to select the desired value from the LLDP Status field.
- 3. Enter the priority value (1-3600s) in the Packet Interval field.
- 4. Press the Save soft key to accept the change.

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

### CDP

CDP (Cisco Discovery Protocol) allows IP phones to receive and/or transmit device-related information from/to directly connected devices on the network that are also using the protocol, and store the information about other devices.

When CDP feature is enabled on IP phones, the IP phones periodically advertise their own information to the directly connected CDP-enabled switch. The IP phones can also receive CDP packets from the connected switch. When the VLAN configurations on the IP phones are different from the ones sent by the switch, the IP phones perform an update and reboot. This allows the IP phones to be plugged into any switch, obtain their VLAN IDs, and then start communications with the call control.

### Procedure

CDP can be configured using the configuration files or locally.

		Configure CDP.
	<v0000000000vv> of a</v0000000000vv>	Parameters:
Conliguration rile	<y000000000xx>.crg</y000000000xx>	network.cdp.enable
		network.cdp.packet_interval
		Configure CDP.
	Web User Interface	Navigate to:
Local		http:// <phonelpaddress>/servle</phonelpaddress>
		t?p=network-adv&q=load
	Phone User Interface	Configure CDP feature.

### Details of Configuration Parameters:

<b>.</b> .	<b>-</b>	<b>-</b>			
Parameters	Permitted Values	Detault			
network.cdp.enable	0 or 1	1			
Description:					
Enables or disables the CDP (Cisco	Discovery Protocol) feature	re on the IP phone.			
0-Disabled					
1-Enabled					
<b>Note:</b> If it is set to 1, the IP phone will attempt to determine its VLAN ID through CDP. If you change this parameter, the IP phone will reboot to make the change take effect.					
Web User Interface:					
Network->Advanced->CDP->Activ	Network->Advanced->CDP->Active				
Phone User Interface:					
Menu->Advanced (default passwo	ord: admin) ->Network->C[	DP->CDP Status			
network.cdp.packet_interval Integer from 1 to 3600 60					
Description:					
Configures the interval (in seconds) for the IP phone to send the CDP (Cisco					
Discovery Protocol) request.					
Note: It works only if the value of the parameter "network.cdp.enable" is set to 1					

Parameters	Permitted Values	Default		
(Enabled). If you change this parar	meter, the IP phone will rel	poot to make the		
change take effect.				
Web User Interface:				
Network->Advanced->CDP->Packet Interval (1~3600s)				
Phone User Interface:				
Menu->Advanced (default passwo	ord: admin) ->Network->C[	DP->Packet Interval		

### To configure CDP via web user interface:

- 1. Click on Network->Advanced.
- 2. In the CDP 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.

				Log Out
	Status Account	Network Feat	ures Settings Directo	ory Security
Basic	LLDP 🕜			NOTE
DC Dort		Active	Enabled -	VIAN
POPOIC		Packet Interval (1~3600s)	60	A VLAN is a logical local area
Advanced	CDP 🕜			network (or LAN) that extends beyond a single traditional LAN
		Active	Enabled 👻	to a group of LAN segments, given specific configurations.
		Packet Interval (1~3600s)	60	005
	VLAN 🕜			When the network capacity is insufficient. OoS could provide
	WAN Port	Active	Disabled 👻	priority to users by setting the
		VID (1-4094)	1	value.
		Priority	0 🔹	Define the port for voice
	PC Port	Active	Disabled 👻	transmission.
		VID (1-4094)	1	You can click here to get more guides.
		Priority	0 💌	
	DHCP VLAN	Active	Enabled 🔹	
		Option (1-255)	132	
	Port Link 🕜			
		WAN Port Link	Auto Negotiate 🔹	
		PC Port Link	Auto Negotiate 🔻	
	Voice QoS 🕜			
		Voice QoS (0~63)	46	
		SIP Qos (0~63)	26	

4. Click Confirm to accept the change.

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

5. Click OK to reboot the IP phone.

#### To configure CDP feature via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Network->CDP->CDP Status.
- 2. Press (•) or (•), or the Switch soft key to select the desired value from the CDP Status field.
- 3. Enter the priority value (1-3600s) in the Packet Interval field.

4. Press the Save soft key to accept the change.

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

## Manual Configuration for VLAN

VLAN is disabled on IP phones by default. You can configure VLAN for the Internet port and PC port manually. Before configuring VLAN on the IP phone, you need to obtain the VLAN ID from your network administrator.

### Procedure

VLAN can be configured using the configuration files or locally.

		Configure VLAN for the Internet port and PC port manually.
		Parameters:
		network.vlan.internet_port_enable
Configuration	<y0000000000xx>.cfg</y0000000000xx>	network.vlan.internet_port_vid
File		network.vlan.internet_port_priority
		network.vlan.pc_port_enable
		network.vlan.pc_port_vid
		network.vlan.pc_port_priority
		Configure VLAN for the Internet port and PC port manually.
	Web User Interface	Navigate to:
Local		http:// <phonelpaddress>/servlet?p=n etwork-adv&amp;q=load</phonelpaddress>
	Phone User Interface	Configure VLAN for the Internet port and PC port manually.

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default	
network.vlan.internet_port_enable	0 or 1	0	
Description:			
Enables or disables VLAN for the Internet (WAN) port.			
0-Disabled			
1-Enabled			

Parameters	Permitted Values	Default
Note: If you change this parameter, th	e IP phone will reboot to m	nake the change
take effect.		
Web User Interface:		
Network->Advanced->VLAN->WAN Pc	ort->Active	
Phone User Interface:		
Menu->Advanced (default password: Status	admin) ->Network->VLAN-	>WAN Port->VLAN
network.vlan.internet_port_vid	Integer from 1 to 4094	1
Description:		
Configures VLAN ID for the Internet (W	AN) port.	
<b>Note:</b> If you change this parameter, the take effect.	e IP phone will reboot to m	nake the change
Web User Interface:		
Network->Advanced->VLAN->WAN Pc	ort->VID (1-4094)	
Phone User Interface:		
Menu->Advanced (default password:	admin) ->Network->VLAN-	>WAN Port->VID
Number		
network.vlan.internet_port_priority	Integer from 0 to 7	0
Description:		
Configures VLAN priority for the Interne	et (WAN) port.	
7 is the highest priority, 0 is the lowest p	riority.	
<b>Note:</b> If you change this parameter, the take effect.	e IP phone will reboot to m	nake the change
Web User Interface:		
Network->Advanced->VLAN->WAN Pa	ort->Priority	
Phone User Interface:		
Menu->Advanced (default password:	admin) ->Network->VLAN-	>WAN
Port->Priority		
network.vlan.pc_port_enable	0 or 1	0
Description:		
Enables or disables VLAN for the PC (L/	AN) port.	
0-Disabled		

Parameters	Permitted Values	Default		
1-Enabled				
<b>Note:</b> If you change this parameter, the IP phone will reboot to make the change take effect.				
Web User Interface:				
Network->Advanced->VLAN->PC Port-	>Active			
Phone User Interface:				
Menu->Advanced (default password: Status	admin) ->Network->VLAN-	>PC Port->VLAN		
network.vlan.pc_port_vid	Integer from 1 to 4094	1		
Description:				
Configures VLAN ID for the PC (LAN) po	ort.			
<b>Note:</b> If you change this parameter, the	e IP phone will reboot to m	nake the change		
Web liser interface:				
Network->Advanced->VI AN->PC Port-	->VID (1-4094)			
Phone User Interface:				
Menu->Advanced (default password: Number	admin) ->Network->VLAN-	>PC Port->VID		
network.vlan.pc_port_priority	Integer from 0 to 7	0		
Description:				
Configures VLAN priority for the PC (LA	N) port.			
7 is the highest priority, 0 is the lowest p	riority.			
<b>Note:</b> If you change this parameter, the take effect.	e IP phone will reboot to m	nake the change		
Web User Interface:				
Network->Advanced->VLAN->PC Port->Priority				
Phone User Interface:				
Menu->Advanced (default password:	admin) ->Network->VLAN-	>PC Port->Priority		
o configure VLAN for Internet port via we	eb user interface:			

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

Veglink						Log Out
	Status Accoun	t Network	Features	Settings	Directory	Security
Basic	LLDP 🕜					NOTE
DC Dort		Active	Enable	d	•	VIAN
roroic		Packet Interval (1~36	600s) 60			A VLAN is a logical local area
Advanced	CDP 🕜					beyond a single traditional LAN
		Active	Enable	d	•	to a group of LAN segments, given specific configurations.
		Packet Interval (1~36	600s) 60			QoS
	VLAN 🕜					When the network capacity is insufficient. OoS could provide
	WAN Port	Active	Enable	ed	•	priority to users by setting the
		VID (1-4094)	1			
		Priority	0		-	Define the port for voice
	PC Port	Active	Disable	ed	•	transmission.
		VID (1-4094)	1			You can click here to get more quides.
		Priority	0		•	inore galacor
	DHCP VLAN	Active	Enable	d	•	
		Option (1-255)	132			
	Port Link 🕜					
		WAN Port Link	Auto I	Vegotiate	•	
		PC Port Link	Auto I	Vegotiate	•	
	Voice QoS 💡					
		Voice QoS (0~63)	46			
		SIP Qos (0~63)	26			

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 IP phone.

### To configure VLAN for PC 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 PC 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.

					Log Out
	Status	Network Feat	tures Settings	Directory	Security
Basic	LLDP 🕜				NOTE
DC Dort		Active	Enabled	•	VLAN
POPOIL		Packet Interval (1~3600s)	60		A VLAN is a logical local area
Advanced	CDP 🕜				network (or LAN) that extends beyond a single traditional LAN
		Active	Enabled	•	to a group of LAN segments, given specific configurations.
		Packet Interval (1~3600s)	60		0.05
	VLAN 🕜				When the network capacity is
	WAN Port	Active	Disabled	•	insufficient, QoS could provide priority to users by setting the
	white one	VID (1 4004)	1		value.
		Vib (1-4054)	1		Local RTP Port
		Priority	U	•	transmission.
	PC Port	Active	Enabled	•	Di Yau ann aliak hara ta aat
		VID (1-4094)	1		more guides.
		Priority	0	•	
	DHCP VLAN	Active	Enabled	•	
		Option (1-255)	132		
	Port Link 🕜				
		WAN Port Link	Auto Negotiate	•	
		PC Port Link	Auto Negotiate	•	
	Voice OoS 👩				
			46		
		SID Occ (0-63)	26		
		214 Gos (0~03)	20		

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 IP phone.

### To configure VLAN for Internet port (or PC port) via phone user interface:

- Press Menu->Advanced (default password: admin) ->Network->VLAN->WAN Port (or PC Port).
- Press ( ) or ( ) , or the Switch soft key to select the desired value from the VLAN Status field.
- 3. Enter the VLAN ID (1-4094) in the VID Number field.
- 4. Enter the priority value (0-7) in the Priority field.
- 5. Press the Save soft key to accept the change.

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

### **DHCP VLAN**

IP phones support VLAN discovery via DHCP. When the VLAN Discovery method is set to DHCP, the IP phone will examine 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.

### Procedure

DHCP VLAN can be configured using the configuration files or locally.

		Configure DHCP VLAN discovery feature.	
Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Parameters:	
		network.vlan.dhcp_enable	
		network.vlan.dhcp_option	
		Configure DHCP VLAN	
		discovery feature.	
	Web User Interface	Navigate to:	
Local		http:// <phonelpaddress>/servle</phonelpaddress>	
		t?p=network-adv&q=load	
	Phone User Interface	Configure DHCP VLAN discovery feature.	

### Details of Configuration Parameters:

Parameters	Permitted Values	Default		
network.vlan.dhcp_enable	0 or 1	1		
Description:				
Enables or disables DHCP VLAN dis	covery feature on the IP p	hone.		
0-Disabled				
1-Enabled				
<b>Note:</b> If you change this parameter, the IP phone will reboot to make the change take effect.				
Web User Interface:				
Network->Advanced->VLAN->DHC	CP VLAN->Active			
Phone User Interface:				
Menu->Advanced (default password: admin) ->Network->VLAN->DHCP VLAN->DHCP VLAN				
network.vlan.dhcp_option	Integer from 1 to 255	132		
Description:				
Configures the DHCP option from which the IP phone will obtain the VLAN settings.				
You can configure at most five DHCP options and separate them by commas.				

Note: If you change this parameter, the IP phone will reboot to make the change

Parameters	Permitted Values	Default	
take effect.			
Web User Interface:			
Network->Advanced->VLAN->DHCP VLAN->Option (1-255)			
Phone User Interface:			
Menu->Advanced (default password: admin) ->Network->VLAN->DHCP VLAN->Option			

#### To configure DHCP VLAN discovery via web user interface:

- 1. Click on Network->Advanced.
- 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 (1-255)** field.

The default option is 132.

					Log Out
Yealink   1466	Status	t Network Feat	ures Settings	Directory	Security
Basic	LLDP 🕜				NOTE
PC Port		Active Packet Interval (1~3600s)	Enabled	•	VLAN
Advanced	CDP 🕜				network (or LAN) that extends beyond a single traditional LAN
		Active	Enabled	•	given specific configurations.
	VLAN 🕜	Packet Interval (1~3600s)	60		QoS When the network capacity is insufficient. QoS could provide
	WAN Port	Active	Enabled	•	priority to users by setting the value.
		VID (1-4094)	1		Local RTP Port
		Priority	0	•	Define the port for voice transmission.
	PC Port	Active	Disabled	*	Veu opp dick here to get
		VID (1-4094)	1		more guides.
		Priority	0	•	
	DHCP VLAN	Active	Enabled	•	
	Dout Link	Option (1-255)	132		
	POPL LINK 🕜	WAN Doct Link	Auto Negotista	_	
		WAN POILLINK	Auto Negotiate	-	
	Voice OoS	PC PUIL LIIK	Auto NegOtate	•	
	VOICE (203 🕜	Voice QoS (0~63)	46		
		SIP Qos (0~63)	26		

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

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

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

#### To configure DHCP VLAN discovery via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Network->VLAN->DHCP VLAN.
- Press or , or the Switch soft key to select the desired value from the DHCP VLAN field.

- 3. Enter the desired option in the **Option** field.
- 4. Press the Save soft key to accept the change.

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

## **Quality of Service**

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

QoS provides better network service through the following features:

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

The Best-Effort service is the default QoS model in IP networks. It provides no guarantees for data delivering, which means delay, jitter, packet loss and bandwidth allocation are unpredictable. Differentiated Services (DiffServ or DS) is the most widely used QoS model. It provides a simple and scalable mechanism for classifying and managing network traffic and providing QoS on modern IP networks. Differentiated Services Code Point (DSCP) is used to define DiffServ classes and stored in the first six bits of the ToS (Type of Service) field. Each router on the network can provide QoS simply based on the DiffServ class. The DSCP value ranges from 0 to 63 with each DSCP specifying a particular per-hop behavior (PHB) applicable to a packet. A PHB refers to the packet scheduling, queuing, policing, or shaping behavior of a node on any given packet. Four standard PHBs available to construct a DiffServ-enabled network and achieve QoS:

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

the traditional best effort service from a DS-compliant node.

VoIP is extremely bandwidth and delay-sensitive. QoS is a major issue in VoIP implementations, regarding how to guarantee that packet traffic not be delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee high-quality QoS only if the voice and the SIP packets are given priority over other kinds of network traffic. IP phones support the DiffServ model of QoS.

### Voice QoS

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

### SIP QoS

SIP protocol is used for creating, modifying and terminating two-party or multi-party sessions. To ensure good voice quality, SIP packets emanated from IP phones should be configured with a high transmission priority.

DSCPs for voice and SIP packets can be specified respectively.

**Note** For voice and SIP packets, the IP phone obtains DSCP info from the network policy if LLDP feature is enabled, which takes precedence over manual settings. For more information on LLDP, refer to LLDP on page 221.

### Procedure

QoS can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure the DSCPs for voice packets and SIP packets. Parameters:
		network.gos.rtptos
		network.gos.signaltos
		Configure the DSCPs for voice packets and SIP packets.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/se rvlet?p=network-adv&amp;q=loa d</phonelpaddress>

### Details of Configuration Parameters:

Parameters	Permitted Values	Default	
network.qos.rtptos	Integer from 0 to 63	46	
Description:			
Configures the DSCP (Differentiated Services	Code Point) for voice p	backets.	
The default DSCP value for RTP packets is 46	(Expedited Forwarding)		
<b>Note:</b> If you change this parameter, the IP ph take effect.	one will reboot to make	e the change	
Web User Interface:			
Network->Advanced->Voice QoS (0~63)			
Phone User Interface:			
None			
network.qos.signaltos	Integer from 0 to 63	26	
Description:			
Configures the DSCP (Differentiated Services	Code Point) for SIP pac	ckets.	
The default DSCP value for SIP packets is 26 (	Assured Forwarding).		
<b>Note:</b> If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			
Network->Advanced->SIP QoS (0~63)			
Phone User Interface:			
None			

To configure DSCPs for voice packets and SIP packets via web user interface:

- 1. Click on Network->Advanced.
- 2. Enter the desired value in the Voice QoS (0~63) field.

alink						Log
	Status	ount Network	Features	Settings	Directory	Security
Basic	LLDP 🕜					NOTE
PC Port		Active	Enable	ed	-	VLAN
- OT OTC		Packet Interval (1~36	60 (i00s)			A VLAN is a logical local area
Advanced	CDP 🕜					beyond a single traditional LA
		Active	Enable	ed	•	to a group of LAN segments, given specific configurations.
		Packet Interval (1~36	i00s) 60			QoS
	VLAN 🕜					When the network capacity
	WAN Port	Active	Disable	ed	•	priority to users by setting th
		VID (1-4094)	1			value.
		Priority	0		•	Local RTP Port Define the port for voice
	PC Port	Active	Disable	ed	•	transmission.
		VID (1-4094)	1			You can click here to get
		Priority	0		•	more guides.
	DHCP VLAN	Active	Enable	ed	-	
		Option (1-255)	132			
	Port Link	2				
		WAN Port Link	Auto	Negotiate	•	
		PC Port Link	Auto	Negotiate	•	
	Voice QoS	0				
		Voice QoS (0~63)	46			
		SID Oos (0.,62)	26			

3. Enter the desired value in the SIP QoS (0~63) 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 **OK** to reboot the IP phone.

## IPv6 Support

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

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

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

If you configure the network settings on the IP phone for an IPv6 network, you can set up an IP address for the IP phone either by using SLAAC (ICMPv6), DHCPv6 or by manually entering an IP address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

### **IPv6 Address Assignment Method**

Supported IPv6 address assignment methods:

- **Manual Assignment:** An IPv6 address and other configuration parameters (e.g., DNS server) for the IP phone can be statically configured by an administrator.
- Stateless Address Autoconfiguration (SLAAC)/ ICMPv6: SLAAC is one of the most convenient methods to assign IP addresses to IPv6 nodes. SLAAC requires no manual configuration of the IP phone, minimal (if any) configuration of routers, and no additional servers. To use IPv6 SLAAC, the IP phone must be connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected IP phone to configure itself with IPv6 address, as specified in RFC 4862.
- Stateful DHCPv6: The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC 3315. DHCPv6 enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately or concurrently with the latter to obtain configuration parameters.

### How the IP phone obtains the IPv6 address and network settings?

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

	SLAAC	How the IP phone obtains the IPv6 address and network	
DHCrvo	(ICMPv6)	settings?	
Disabled	Disabled	You have to manually configure the static IPv6 address and other network settings.	
Disabled	Enabled	The IP phone can obtain the IPv6 address via SLAAC, but the other network settings must be configured	
Enabled	Disabled	The IP phone can obtain the IPv6 address and the other network settings via DHCPv6.	
Enabled	Enabled	The IP phone can obtain the IPv6 address via SLAAC and obtain other network settings via DHCPv6.	

### Procedure

IPv6 can be configured using the configuration files or locally.

		Configure the IPv6 address assignment method.
		Parameters:
		network.ip_address_mode
		network.ipv6_internet_port.type
		network.ipv6_internet_port.ip
	<nac> of a</nac>	network.ipv6_prefix
	<mac>.cig</mac>	network.ipv6_internet_port.gateway
Configuration File		network.ipv6_icmp_v6.enable
		Configure the IPv6 static DNS address.
		Parameters:
		network.ipv6_primary_dns
		network.ipv6_secondary_dns
		Configure the IPv6 static DNS.
	<y000000000xx>.cf</y000000000xx>	Configure the IPv6 static DNS. Parameter:
	<y000000000xx>.cf g</y000000000xx>	Configure the IPv6 static DNS. <b>Parameter:</b> network.ipv6_static_dns_enable
	<y000000000xx>.cf g</y000000000xx>	Configure the IPv6 static DNS. <b>Parameter:</b> network.ipv6_static_dns_enable Configure the IPv6 address
	<y000000000xx>.cf g</y000000000xx>	Configure the IPv6 static DNS. <b>Parameter:</b> network.ipv6_static_dns_enable Configure the IPv6 address assignment method.
	<y000000000xx>.cf g Web User Interface</y000000000xx>	Configure the IPv6 static DNS. <b>Parameter:</b> network.ipv6_static_dns_enable Configure the IPv6 address assignment method. Configure the IPv6 static DNS.
	<y000000000xx>.cf g Web User Interface</y000000000xx>	Configure the IPv6 static DNS. Parameter: network.ipv6_static_dns_enable Configure the IPv6 address assignment method. Configure the IPv6 static DNS. Navigate to:
Local	<y000000000xx>.cf g Web User Interface</y000000000xx>	Configure the IPv6 static DNS. Parameter: network.ipv6_static_dns_enable Configure the IPv6 address assignment method. Configure the IPv6 static DNS. Navigate to: http:// <phoneipaddress>/servlet?p= network&amp;q=load</phoneipaddress>
Local	<y000000000xx>.cf g Web User Interface</y000000000xx>	Configure the IPv6 static DNS. Parameter: network.ipv6_static_dns_enable Configure the IPv6 address assignment method. Configure the IPv6 static DNS. Navigate to: http:// <phoneipaddress>/servlet?p= network&amp;q=load Configure the IPv6 address</phoneipaddress>
Local	<y000000000xx>.cf g Web User Interface Phone User</y000000000xx>	Configure the IPv6 static DNS. Parameter: network.ipv6_static_dns_enable Configure the IPv6 address assignment method. Configure the IPv6 static DNS. Navigate to: http:// <phoneipaddress>/servlet?p= network&amp;q=load Configure the IPv6 address assignment method. Quality of the IPv6 to the Dv6</phoneipaddress>
Local	<y000000000xx>.cf g Web User Interface Phone User Interface</y000000000xx>	Configure the IPv6 static DNS. Parameter: network.ipv6_static_dns_enable Configure the IPv6 address assignment method. Configure the IPv6 static DNS. Navigate to: http:// <phoneipaddress>/servlet?p= network&amp;q=load Configure the IPv6 address assignment method. Configure the IPv6 static DNS.</phoneipaddress>

### Details of Configuration Parameters:

Parameters	Permitted Values	Default
network.ip_address_mode	0, 1 or 2	0

Parameters	Permitted Values	Default	
Description:			
Configures the IP address mode.			
<b>0</b> -IPv4			
<b>1</b> -IPv6			
<b>2</b> -IPv4 & IPv6			
<b>Note:</b> If you change this parameter, th take effect.	e IP phone will reboot to	make the change	
Web User Interface:			
Network->Basic->Internet Port->Mode	(IPv4/IPv6)		
Phone User Interface:			
Menu->Advanced (default password:	admin) ->Network->WA1	N Port->IP Mode	
network.ipv6_internet_port.type	0 or 1	0	
Description:			
Configures the Internet (WAN) port typ	be for IPv6.		
0-DHCP			
1-Static IP Address			
<b>Note:</b> It works only if the value of the p to 1 (IPv6) or 2 (IPv4 & IPv6). If you cha to make the change take effect.	arameter "network.ip_ad nge this parameter, the	ddress_mode" is set IP phone will reboot	
Web User Interface:			
Network->Basic->IPv6 Config			
Phone User Interface:			
Menu->Advanced (default password:	admin) ->Network->WA1	N Port->IPv6	
network.ipv6_static_dns_enable	0 or 1	0	
Triggers the static IPv6 DNS feature to a	on or off.		
<b>0-</b> Off			
<b>1-</b> On			
If it is set to 0 (Off), the IP phone will use	e the IPv6 DNS obtained	from DHCP.	
If it is set to 1 (On), the IP phone will use manually configured static IPv6 DNS.			
<b>Note:</b> It works only if the value of the parameter "network.ipv6_internet_port.type" is set to 0 (DHCP). If you change this parameter, the IP phone will reboot to make the change take effect.			

Parameters	Permitted Values	Default	
Web User Interface:			
Network->Basic->IPv6 Config->IPv6 Sta	itic DNS		
Phone User Interface:			
Menu->Advanced (default: admin) -> DNS	Network->WAN Port->IPv	6->DHCP->Static	
network.ipv6_internet_port.ip	IPv6 address	Blank	
Description:			
Configures the IPv6 address.			
Example:			
network.ipv6_internet_port.ip = 2026:12	234:1:1:215:65ff:fe1f:caa		
to 1 (IPv6) or 2 (IPv4 & IPv6), and "network.ipv6_internet_port.type" is set to 1 (Static IP Address). If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			
Network->Basic->IPv6 Config->Static IF	PAddress->IPAddress		
Phone User Interface:			
Menu->Advanced (default password: IP->IP Address	admin) ->Network->WA1	N Port->IPv6->Static	
network.ipv6_prefix	Integer from 0 to 128	64	
Description:			
Configures the IPv6 prefix.			
<b>Note:</b> It works only if the value of the p to 1 (IPv6) or 2 (IPv4 & IPv6), and "netw IP Address). If you change this parame change take effect.	arameter "network.ip_ad ork.ipv6_internet_port.ty ater, the IP phone will reb	ddress_mode" is set pe" is set to 1 (Static poot to make the	
Web User Interface:			
Network->Basic->IPv6 Config->Static IF	PAddress->IPv6 Prefix(0~	128)	
Phone User Interface:			
Menu->Advanced (default password: IP->IPv6 IP Prefix	admin) ->Network->WA1	N Port->IPv6->Static	
network.ipv6_internet_port.gateway	IPv6 address	Blank	

Parameters	Permitted Values	Default	
Description:			
Configures the IPv6 default gateway.			
Example:			
network.ipv6_internet_port.gateway =	3036:1:1:c3c7:c11c:5447	7:23a6:255	
<b>Note:</b> It works only if the value of the p to 1 (IPv6) or 2 (IPv4 & IPv6), and "netw IP Address). If you change this parame change take effect.	arameter "network.ip_ad ork.ipv6_internet_port.ty ater, the IP phone will reb	ddress_mode" is set pe" is set to 1 (Static poot to make the	
Web User Interface:			
Network->Basic->IPv6 Config->Static IF	? Address->Gateway		
Phone User Interface:			
Menu->Advanced (default password: IP->Gateway	admin) ->Network->WAI	N Port->IPv6->Static	
network.ipv6_primary_dns	IPv6 address	Blank	
Description:			
Configures the primary IPv6 DNS server	r.		
Example:			
network.ipv6_primary_dns = 3036:1:1:c	3c7: c11c:5447:23a6:256		
<b>Note:</b> It works only if the value of the p to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP e value of the parameter "network.ipv6_ change this parameter, the IP phone v	arameter "network.ip_ac nvironment, you also ne static_dns_enable" is set will reboot to make the c	ddress_mode" is set ed to make sure the to 1 (On). If you change take effect.	
Web User Interface:			
Network->Basic->IPv6 Config->Static IF	Address->Primary DNS		
Phone User Interface:			
Menu->Advanced (default password: admin) ->Network->WAN Port->IPv6->Static IP->Primary DNS			
Or Menu->Advanced (default passwo	rd: admin) ->Network->V	VAN	
Port->IPv6->DHCP->Static DNS(Enabled	d)->Primary DNS		
network.ipv6_secondary_dns	IPv6 address	Blank	
Description:			
Configures the secondary IPv6 DNS se	rver.		
Example:			

Parameters	Permitted Values	Default	
network.ipv6_secondary_dns = 2026:12	234:1:1:c3c7:c11c:5447:2	3a6	
<b>Note:</b> It works only if the value of the parameter "network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure the value of the parameter "network.ipv6_static_dns_enable" is set to 1 (On). If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			
Network->Basic->IPv6 Config->Static IF	? Address->Secondary DI	NS	
Phone User Interface:			
Menu->Advanced (default password: IP->Secondary DNS	admin) ->Network->WA1	N Port->IPv6->Static	
<b>Or</b> Menu->Advanced (default passwo Port->IPv6->DHCP->Static DNS(Enabled	rd: admin) ->Network->V d)->Secondary DNS	VAN	
network.ipv6_icmp_v6.enable	0 or 1	1	
Description:			
Enables or disables the IP phone to ob (Stateless Address Autoconfiguration)	tain IPv6 network setting method.	s via SLAAC	
0-Disabled			
1-Enabled			
<b>Note:</b> If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to SIP-T48G/T46G IP phones. SLAAC is enabled on SIP-T42G/T41P/T40P IP phones by default. You are not allowed to configure this parameter for those IP phones.			
Web User Interface:			
Network->Advanced->ICMPv6 Status->Active			
Phone User Interface:			
None			

### To configure IPv6 address assignment method via web user interface:

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

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

			Log Out
Yealink 1466	Status Account Network	Features Settings Directory	Security
	Internet Port		NOTE
Basic	Mode(IPv4/IPv6)	IPv6 V	
PC Port	IPv4 Config		DHCP The network configurations will be acquired from DHCP server.
Advanced	OHCP ?		Static IP Address
	Static IP Address 🕜		Specify the IP address, Subnet Mask, Default Gateway, Primary
	IP Address		DNS, Secondary DNS fields manually.
	Subnet Mask		PPPoE
	Gateway		Contact your ISP if it should be used.
	Static DNS	On  Off	New year aliable bases to part
	Primary DNS		more guides.
	Secondary DNS		
	IPv6 Config		
	О рнср 🕜		
	Static IP Address		
	IP Address	2026:1234:1:1:215:65ff:fe1	
	IPv6 Prefix(0~128)	64	
	Gateway	3026:1:1:c3c7:c11c:5447:2	
	IPv6 Static DNS	On Off	
	Primary DNS	3026:1:1:c3c7:c11c:5447:2	
	Secondary DNS	2026:1234:1:1:c3c7:c11c:5	
	Confirm	Cancel	

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

			Log Out
Yealink T46G			
	Status Account Network	Features Settings Directory	Security
	Internet Port		NOTE
Basic	Mode(IPv4/IPv6)	IPv6 V	
PC Port	IPv4 Config		DHCP The network configurations will be acquired from DHCP server.
Advanced	DHCP (?)		Static IP Address
	Static IP Address ??		Specify the IP address, Subnet Mask, Default Gateway, Primary
	IP Address		DNS, Secondary DNS fields manually.
	Subnet Mask		PPPoE
	Gateway		Contact your ISP if it should be used.
	Static DNS	On Off	You can click here to get
	Primary DNS		more guides.
	Secondary DNS		
	IPv6 Config		
	OHCP ?		
	O Static IP Address 🕜		
	IP Address	2026:1234:1:1:215:65ff:fe1	
	IPv6 Prefix(0~128)	64	
	Gateway	3026:1:1:c3c7:c11c:5447:2	
	IPv6 Static DNS	● On ○ Off	
	Primary DNS	3026:1:1:c3c7:c11c:5447:2	
	Secondary DNS	2026:1234:1:1:c3c7:c11c:5	
	Confirm	Cancel	

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 IP phone.

#### To configure SLAAC feature via web user interface (only applicable to SIP-T48G/T46G):

- 1. Click on Network->Advanced.
- In the ICMPv6 Status block, select the desired value from the pull-down list of Active.

					Log Out
Yealink T46G	Status	Network Feat	ures Settings	Directory	Security
	LLDP 🕜				NOTE
Basic		Active	Enabled	~	
PC Port		Packet Interval (1~3600s)	60		A VLAN is a logical local area
Advanced	CDP 🕜				beyond a single traditional LAN
		Active	Enabled	~	to a group of LAN segments, given specific configurations.
		Packet Interval (1~3600s)	60		QoS
	VLAN 🕜				insufficient, QoS could provide
	WAN Port	Active	Disabled	~	value.
		VID (1-4094)	1		Local RTP Port
		Priority	0	~	transmission.
	PC Port	Activo	Disabled	~	You can click here to get
	PC POIL	Active			more guides.
		VID (1-4094)	1		
		Priority	0	~	
		:			
		•			
	Port Link 🕜				
		WAN Port Link	Auto Negotiate	$\checkmark$	
		PC Port Link	Auto Negotiate	~	
	ICMPv6 Status	0			
		Active	Enabled	~	
	C	Confirm	Cancel		

#### 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 **OK** to reboot the IP phone.

#### To configure IPv6 address assignment method via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Network->WAN Port.
- 2. Press (•) or (•) to select IPv4 & IPv6 or IPv6 from the IP Mode field.
- 3. Press ( ) or ( ) to highlight IPv6 and press the Enter soft key.
- 4. Press ( ) or ( ) to select the desired IPv6 address assignment method.

If you select the **Static IP**, configure the IPv6 address and other network parameters in the corresponding fields.

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

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

#### To configure IPv6 static DNS when DHCP is used via phone user interface:

1. Press Menu->Advanced (default password: admin) ->Network->WAN

### Port->IPv6->DHCP.

- 2. Press  $(\cdot)$  or  $(\cdot)$ , or the Switch soft key to select Enabled from the Static DNS field.
- 3. Enter the desired values in the Primary DNS and Second DNS fields respectively.
- 4. Press the Save soft key to accept the change.

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

# **Configuring Audio Features**

This chapter provides information for making configuration changes for the following audio features:

- Ring Tones
- Tones
- Voice Mail Tone
- Headset Prior
- Dual Headset
- Audio Codecs
- Acoustic Clarity Technology

# **Ring Tones**

Ring tones are used to indicate incoming calls acoustically. Users can select a built-in system ring tone or a custom ring tone for the IP phone or account. To set the custom ring tones, you need to upload the custom ring tones to the IP phone in advance.

The ring tone format must meet the following:

IP Phone Model	Format	Single File Size	Total File Size
SIP-T48G/T46G	.wav	<=8MB	<=20MB
SIP-T42G/T41P/T40P	.wav	<=100KB	<=100KB

Note

The ring tone file must be PCMU audio format, mono channel, 8K sample rate and 16 bit resolution.

### Procedure

Ring tones can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Configure a ring tone for the IP phone.	
		Parameter:	
		phone_setting.ring_type	
		Specify the access URL of the	
		custom ring tone.	

		Parameter:
		ringtone.url
		Delete all custom ring tone
		files.
		Parameter:
		ringtone.delete
		Configure a ring tone on a per-line basis.
	<mac>.cfg</mac>	Parameters:
		account.1.ringtone.ring_type
		Upload the custom ring tones.
		Configure a ring tone for the
		IP phone.
		Navigate to:
		http:// <phonelpaddress>/serv</phonelpaddress>
	Web User Interface	let?p=settings-preference&q= load
Local		Configure a ring tone on a
		per-line basis.
		Navigate to:
		http:// <phonelpaddress>/serv</phonelpaddress>
		let?p=account-basic&q=load &acc=0
		Configure a ring tone for the
	Phone User Interface	IP phone.

# Details of the Configuration Parameter:

Parameters	Permitted Values	Default		
phone_setting.ring_type	Refer to the following content	Ring1.wav		
Description:				
Configures a ring tone for the IP phone.				
Example:				
To configure a phone built-in ring tone (e.g., Ring1.wav):				
phone_setting.ring_type = Ring1.wav				
To configure a custom ring tone (e.g., Customring.wav):				
phone_setting.ring_type = Customring.wav				

Parameters	Permitted Values	Default			
Permitted Values:					
Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav).					
Web User Interface:					
Settings->Preference->Ring Type	e				
Phone User Interface:					
Menu->Basic->Sound->General					
account.1.ringtone.ring_type	Refer to the following content	Common			
Description:					
Configures a ring tone for the a	ccount.				
Example:					
account.1.ringtone.ring_type =	Ring3.wav				
It means configuring Ring3.wav	for the account.				
account.1.ringtone.ring_type =	Common				
It means the account will use the ring tone selected for the IP phone configured by the parameter "phone_setting.ring_type".					
Permitted Values:					
Common, Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring wav)					
Web User Interface:					
Account->Basic->Ring Type					
Phone User Interface:					
None					
ringtone.url	URL within 511 characters	Blank			
Description:					
Configures the access URL of the custom ring tone file.					
Example:					
ringtone.url = tftp://192.168.1.100/Customring.wav					
Web User Interface:					
Settings->Preference->Upload Ringtone					
Phone User Interface:					
None					

Parameters	Permitted Values	Default		
ringtone.delete	http://localhost/all	Blank		
Description:				
Deletes all custom ring tone files.				
Example:				
ringtone.delete = http://localhost/all				
Web User Interface:				
None				
Phone User Interface:				
None				

To upload a custom ring tone via web user interface:

- 1. Click on Settings->Preference.
- 2. In the Upload Ringtone field, click Browse to locate a ring tone file (the file format must be \*.wav) from your local system.
- 3. Click **Upload** to upload the file.

Log Out				
	Status Account Network	Features Settings	Directory	Security
Preference	Language	English (English) 🔹 🍞		NOTE
Time&Date	Live Dialpad Backlight Inactive Level	Disabled • ?		Preference Settings
Upgrade	Backlight Active Level	8 • ?		administrator.
Auto Provision	Watch Dog	Enabled 🔹 🕜		You can click here to get more guides.
Configuration	Ring Type	Ring1.wav • ?		
Dial Plan	Upload Ringtone	Browse No file selected. Upload Cancel		
Voice	Confirm	Cancel		

The custom ring tone appears in the pull-down list of **Ring Type**.

To change the ring tone for the IP phone via web user interface:

1. Click on Settings->Preference.
2. Select the desired ring tone from the pull-down list of **Ring Type**.

Yealink   1466	Status Account Network	Features Settings	Directory	Log Out
Preference Time&Date Upgrade Auto Provision Configuration Dial Plan	Language Live Dialpad Backlight Inactive Level Backlight Active Level Watch Dog Ring Type Upload Ringtone	English (English)	0	NOTE Preference Settings The preference settings for administrator. You can click here to get more guides.
Voice Tones	Confirm	Cancel		

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

To change the ring tone for the account via web user interface:

- 1. Click on Account->Basic.
- 2. Select the desired ring tone from the pull-down list of **Ring Type**.

Veglink					Log Out
	Status Account	Network Feat	ures Setting	gs Directory	Security
Register	Missed Call Log	Enabled	•	0	NOTE
Basic	Auto Answer Ring Type	Disable	· ·	0	Basic
Codec	Account Lock	Commo Ring1.v	n rav	0	administrator.
	Always On Line	Ring2.v Ring3.v Ring4.v	av av	0	Proxy Require A special parameter just for Nortel server. If you login to
	Con	firm Ring5.v Ring6.v	rav rav		Nortel server, the value should be, com.nortelnetworks.firewall
		Ring7.v Ring8.v Silent.v	rav rav		You can click here to get
		Splash.	vav		more guides.

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

To select a ring tone for the IP phone via phone user interface:

- 1. Press Menu->Basic->Sound->Ring Tones.
- **2.** Press  $(\bullet)$  or  $(\bullet)$  to select the desired ring tone.
- 3. Press the Save soft key to accept the change.

## Tones

When receiving a message, the IP phone 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 IP phone. The default tones used on IP phones are the US tone sets. Available tone sets for IP phones:

- Australia
- Austria

- Brazil
- Belgium
- Chile
- China
- 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 IP phones for the following conditions.

Condition	Description		
Dial	When in the pre-dialing interface		
Ring Back	Ring-back tone		
Busy	When the callee is busy		
Congestion	When the network is congested		
Call Waiting	Call waiting tone (For more information on call waiting, refer to Call Waiting)		

Condition	Description
Dial Recall	When receiving a call back
Info	When receiving a special message
Stutter	When receiving a voice mail
Auto Answer	When automatically answering a call (For more information on auto answer, refer to Auto Answer)

## Procedure

Tones can be configured using the configuration files or locally.

		Configure the tones for the IP phone.
		Parameters:
		voice.tone.country
		voice.tone.dial
	<y000000000xx>.cfg</y000000000xx>	voice.tone.ring
Configuration File		voice.tone.busy
		voice.tone.congestion
		voice.tone.callwaiting
		voice.tone.dialrecall
		voice.tone.info
		voice.tone.stutter
		voice.tone.autoanswer
		Configure the tones for the IP
		phone.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servl</phonelpaddress>
		et?p=settings-tones&q=load

## Details of Configuration Parameters:

Parameters	Permitted Values	Default		
voice.tone.country	Refer to the following content	Custom		
Description:				
Configures the country tone for the IP phone.				
Permitted Values:				
Custom, Australia, Austria, Brazil, Belgium, Chile, China, Czech, Czech ETSI, Denmark,				

Parameters Permitted Values Default				
Finland, France, Germany, Great Britain, Greece, Hungary, Lithuania, India, Italy, Japan, Mexico, New Zealand, Netherlands, Norway, Portugal, Spain, Switzerland, Sweden, Russia, United States.				
Example:				
voice.tone.country = Custom				
Web User Interface:				
Settings->Tones->Select Country				
Phone User Interface:				
None				
voice.tone.dial	String	Blank		
Description:				
Customizes the dial tone.				
tonelist = element[,element] [,eleme	nt]			
Where				
element = [!]Freq1[+Freq2][+Freq3][+	-Freq4] /Duration			
<b>Freq</b> : the frequency of the tone (ranges from 200 to 4000Hz). If it is set to 0Hz, it means the tone is not played.				
For SIP-T40P:				
A tone is comprised of at most two different frequencies.				
For SIP-T48G/T46G/T42G/T41P:				
A tone is comprised of at most four different frequencies.				
Duration: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms.				
You can configure at most eight different tones for one condition, and separate them by commas. (e.g., 250/200,0/1000,200+300/500,200+500+800+1500/1000).				
If you want the IP phone to play tones once, add an exclamation mark "!" before				
<b>Note</b> : It works only if the value of the parameter "voice.tone.country" is set to Custom.				
Web User Interface:				
Settings->Tones->Dial				
Phone User Interface:				
None				
voice.tone.ring String Blank				

Parameters	Parameters Permitted Values Default				
Description:					
Customizes the ringback tone.					
The value format is Freq/Duration. For the parameter "voice.tone.dial".	or more information on the value	format, refer to			
<b>Note</b> : It works only if the value of the Custom.	parameter "voice.tone.country"	is set to			
Web User Interface:					
Settings->Tones->Ring Back					
Phone User Interface:					
None					
voice.tone.busy	String	Blank			
Description:					
Customizes the tone when the calle	e is busy.				
The value format is Freq/Duration. For the parameter "voice.tone.dial".	or more information on the value	format, refer to			
Note: It works only if the value of the	parameter "voice.tone.country"	is set to			
Custom.					
Web User Interface:					
Settings->Tones->Busy					
Phone User Interface:					
None					
voice.tone.congestion	String	Blank			
Description:					
Customizes the tone when the netwo	ork is congested.				
The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".					
Note: It works only if the value of the parameter "voice.tone.country" is set to					
Custom.					
Web User Interface:					
Settings->Tones->Congestion					
Phone User Interface:					
None					

Parameters	Permitted Values	Default		
voice.tone.callwaiting	String	Blank		
Description:				
Customizes the call waiting tone.				
The value format is Freq/Duration. For the parameter "voice.tone.dial".	or more information on the value	format, refer to		
<b>Note</b> : It works only if the value of the Custom.	parameter "voice.tone.country'	' is set to		
Web User Interface:				
Settings->Tones->Call Waiting				
Phone User Interface:				
None				
voice.tone.dialrecall	String	Blank		
Description:				
Customizes the call back tone.				
The value format is Freq/Duration. For the parameter "voice.tone.dial".	or more information on the value	format, refer to		
<b>Note</b> : It works only if the value of the Custom.	parameter "voice.tone.country'	' is set to		
Web User Interface:				
Settings->Tones->Dial Recall				
Phone User Interface:				
None				
voice.tone.info	String	Blank		
Description:				
Customizes the info tone. The phone will play the info tone with the special				
information, for example, the number you are calling is not in service.				
The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".				
<b>Note</b> : It works only if the value of the parameter "voice.tone.country" is set to Custom.				
Web User Interface:	Web User Interface:			

Settings->Tones->Info

Parameters	Permitted Values	Default			
Phone User Interface:					
None					
voice.tone.stutter	String	Blank			
Description:					
Customizes the tone when the IP ph	one receives a voice mail.				
The value format is Freq/Duration. For the parameter "voice.tone.dial".	or more information on the value	format, refer to			
<b>Note</b> : It works only if the value of the Custom.	parameter "voice.tone.country'	' is set to			
Web User Interface:					
Settings->Tones->Stutter					
Phone User Interface:					
None					
voice.tone.autoanswer String Blank					
Description:					
Customizes the warning tone for aut	o answer.				
The value format is Freq/Duration. For the parameter "voice.tone.dial".	The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".				
<b>Note</b> : It works only if the value of the parameter "voice.tone.country" is set to Custom.					
Web User Interface:					
Settings->Tones->Auto Answer					
Phone User Interface:					
None					

### To configure tones via web user interface:

- 1. Click on Settings->Tones.
- 2. Select the desired value from the pull-down list of Select Country.

<b>fealink</b>   1466					Log Ou
	Status Account	Network Features	Settings Dire	ctory	Security
Preference	Select_Country	Custom	•	0	NOTE
	Dial			0	-
Time&Date	Ring Back			0	The tones parameters for
Upgrade	Busy			0	administrator.
Auto Provision	Congestion			0	7 You can click here to get
Configuration	Call Waiting			0	more guides.
comgaration	Dial Recall			0	
Dial Plan	Info			0	
Voice	Stutter			0	
Tones	Auto Answer			0	
Phone Lock	Conf	ìrm	Cancel		

If you select **Custom**, you can customize a tone for each condition of the IP phone.

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

## Voice Mail Tone

Voice mail tone feature allows the IP phone to play a warning tone when receiving a new voice mail. You can customize the warning tone or select specialized tone sets (vary from country to country) for your IP phone. For more information, refer to Tones on page 253.

#### Procedure

Voice mail tone can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure whether to play a warning tone when the IP phone receives a new voice mail.		
		Parameters:		
		features.voice_mail_tone_enable		
local	Web User Interface	Configure whether to play a warning tone when the IP phone receives a new voice mail.		
	Web user interface	Navigate to:		
		http:// <phonelpaddress>/servlet? p=features-general&amp;q=load</phonelpaddress>		

#### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.voice_mail_tone_enable	0 or 1	1

Parameter	Permitted Values	Default
Description:		
Enables or disables the IP phone to play a warning ton voice mail.	e when it receives c	new
0-Disabled		
1-Enabled		
Web User Interface:		
Features->General Information->Voice Mail Tone		
Phone User Interface:		
None		

#### To configure voice mail tone via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of **Voice Mail Tone**.

				Log Out
Yealink   1466	Status Account Network	Features Settings	Directory	Security
General Information Audio Remote Control Bluetooth Power LED	General Information (2) Cal Waiting Key As Send Busy Tone Delay (Seconds) Return code when refuse Time-Out for Dial-Now Rule Dial Search Delay	Enabled • • • • • • • • • • • • • • • • • • •	0 0 0 0 0	NOTE Call Waiting This call feature allows your phone to accept other incoming calls during the conversation. Key As Send Select * or # as the send key. You can click here to get more guides.
	Cal Number Filter Voice Mail Tone DHCP Hostname E911 Location Tip Update Checking Time Use DHCP Option 120 SFB Cert Service URL Enable SFB Automation SFB Inactive Time SFB Away Time Device Pairing for Online Confirm	Enabled   Enabled  SIP-T466  Enabled  24  Disabled  Disabled  5  5  Enabled  Cancel	0 0 0 0 0 0 0 0 0 0 0	

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

# **Headset Prior**

Headset prior allows users to use headset preferentially if a headset is physically connected to the IP phone. This feature is especially useful for permanent or full-time headset users.

### Procedure

Headset prior can be configured using the configuration files or locally.

		Configure headset prior.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameter:
		features.headset_prior
		Configure headset prior.
		Navigate to:
Local	Web User Interface	http:// <phonelpaddress></phonelpaddress>
		/servlet?p=features-gene
		ral&q=load

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default				
features.headset_prior	0 or 1	0				
Description:						
Enables or disables headset prior feature. You need to press the HEADSET key to activate the headset mode in advance.						
0-Disabled						
1-Enabled						
If it is set to 1 (Enabled), the headset mode will not be deactivated until the user presses the HEADSET key again.						
If it is set to 0 (Disabled), the headset mode can be deactivated by pressing the speakerphone key or the HEADSET key except the HANDSET key.						
Web User Interface:						
Features->General Information->Headset Prior						
Phone User Interface:						

None

#### To configure headset prior via web user interface:

1. Click on Features->General Information.

alink									LOL
	Status	Account	Network	Features	Settin	gs	Directory	Security	
General	(	General Informat	ion 🕜					ΝΟΤΕ	
Information		Call Waiting		Enabled	•	0		Call Waiting	
Audio		Key As Send		#	•	0		This call featu	re allows your
Remote Control		Busy Tone Delay	(Seconds)	0	•	0		calls during th	e conversatior
		Return code whe	en refuse	603 (Decline)	•	0		Key As Send	
Bluetooth		Time-Out for Dia	I-Now Rule	1		0		Select * or #	as the send k
Power LED		Dial Search Delay		1		0		🛛 You can c	lick here to g
		180 Ring Workar	ound	Disabled	•	0		more guides.	
		Save Call Log		Enabled	•	?			
		Suppress DTMF [	Display	Disabled	•	0			
		Suppress DTMF [	Display Delay	Disabled	•	0			
		Play Local DTMF	Tone	Enabled	•	0			
		DTMF Repetition		3	-	0			
		Multicast Codec		G722	•	0			
		Play Hold Tone		Enabled	•	?			
		Play Hold Tone D	Delay	30		0			
		Allow Mute		Enabled	•	0			
		Dual-Headset		Disabled	•	0			
		Auto-Answer De	lay(1~4s)	1		0			

2. Select the desired value from the pull-down list of Headset Prior.

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

# **Dual Headset**

Dual headset allows users to use two headsets on one IP phone. To use this feature, users need to physically connect two headsets to the headset and handset jacks respectively. Once the IP phone connects to a call, the user with the headset connected to the headset jack has full-duplex capabilities, while the user with the headset connected to the handset jack is only able to listen.

### Procedure

Dual headset can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Configure dual headset. <b>Parameter:</b> features.headset_training
Local	Web User Interface	Configure dual headset. <b>Navigate to:</b> http:// <phonelpaddress>/ser vlet?p=features-general&amp;q=l oad</phonelpaddress>

## Details of the Configuration Parameter:

Parameter	Parameter Permitted Values				
features.headset_training	0 or 1	0			
Description:					
Enables or disables dual headset	feature.				
0-Disabled					
1-Enabled					
If it is set to 1 (Enabled), users can use two headsets on one phone. When the IP phone joins in a call, the users with the headset connected to the headset jack have a full-duplex conversation, while the users with the headset connected to the handset jack are only allowed to listen to.					
Web User Interface:					
Features->General Information->Dual-Headset					
Phone User Interface:					
None					

#### To configure dual headset via web user interface:

- 1. Click on Features->General Information.
- 2. Select the desired value from the pull-down list of **Dual-Headset**.

			Log Out
Yealink   T46G	Etatua Account Natural	Features Cottings	Directory
	Status Account Network	settings	Directory Security
General	General Information 🛛 🕜		NOTE
Information	Call Waiting	Enabled 🔹 🕐	Call Waiting
Audio	Key As Send	# 🔹 🕐	This call feature allows your
Remote Control	Busy Tone Delay (Seconds)	0 🔹 📀	calls during the conversation.
	Return code when refuse	603 (Decline) 🔹 🥎	Key As Send
Bluetooth	Time-Out for Dial-Now Rule	1	Select * or # as the send key.
Power LED	Dial Search Delay	1	You can click here to get
	180 Ring Workaround	Disabled 🔹 🕜	more guides.
	Save Call Log	Enabled 🔹 🕐	
	Suppress DTMF Display	Disabled 🔹 💡	
	Suppress DTMF Display Delay	Disabled 🔹 🕜	
	Play Local DTMF Tone	Enabled 🔹 🕜	
	DTMF Repetition	3 🔹 🕜	
	Multicast Codec	G722 🔻 🕜	
	Play Hold Tone	Enabled 🔹 🕜	
	Play Hold Tone Delay	30	
	Allow Mute	Enabled 🔹 🕜	
	Dual-Headset	Disabled 👻 🕜	
	Auto-Answer Delay(1~4s)	1	
	Headset Prior	Enabled 🔹 💡	

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

# Audio Codecs

CODEC is an abbreviation of COmpress-DECompress, 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 signal with minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for audio transmission.

The audio codec that the IP phone uses to establish a call should be supported by the SIP server. When placing a call, the IP phone 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.

IP Phone Model	Supported Audio Codecs	Default Audio Codecs
SIP-T48G/T46G/T42G/T41P	G722, PCMA, PCMU, G729, G726-16, G726-24, G726-32, G726-40, iLBC, G723_53, G723_63	G722, РСМА, РСМИ, G729
SIP-T40P	G722, PCMA, PCMU, G729, G726-16, G726-24, G726-32, G726-40, iLBC	G722, РСМА, РСМИ, G729

The following table lists the audio codecs supported by each phone model:

The following table summarizes the supported audio codecs on IP phones:

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
G722	G.722	RFC 3551	64 Kbps	16 Ksps	20ms
РСМА	G.711	RFC 3551	64 Kbps	8 Ksps	20ms
PCMU	G.711 u-law	RFC 3551	64 Kbps	8 Ksps	20ms
G729	G.729	RFC 3551	8 Kbps	8 Ksps	20ms
G726-16	G.726	RFC 3551	16 Kbps	8 Ksps	20ms
G726-24	G.726	RFC 3551	24 Kbps	8 Ksps	20ms
G726-32	G.726	RFC 3551	32 Kbps	8 Ksps	20ms
G726-40	G.726	RFC 3551	40 Kbps	8 Ksps	20ms
G723_53/	C 723 1	PEC 3551	5.3kbps	8 Kini	30ms
G723_63	0.723.1	KI C 3331	6.3kbps	8 ksps	00113
il BC	ilBC	PEC 3050	15.2 Kbps	8 Krnr	20ms
ILDC	ILDC	KI C 3732	13.33 Kbps	8 Ksps	30ms

### **Packetization Time**

Ptime (Packetization Time) is a measurement of the duration (in milliseconds) of the audio data in each RTP packet sent to the destination, and defines how much network bandwidth is used for the RTP stream transfer. Before establishing a conversation, codec and ptime are negotiated through SIP signaling. The valid values of ptime range from 10 to 60, in increments of 10 milliseconds. The default ptime is 20ms. You can also disable the ptime negotiation.

Codecs and priorities of these codecs are configurable on a per-line basis. The attribute "rtpmap" is used to define a mapping from RTP payload codes to a codec, clock rate and other encoding parameters.

Codec	Configuration Methods	Priority	RTPmap
G722	Configuration Files Web User Interface	1	9
PCMU	Configuration Files Web User Interface	2	0
РСМА	Configuration Files Web User Interface	3	8
G729	Configuration Files Web User Interface	4	18
G723_53	Configuration Files Web User Interface	0	4
G723_63	Configuration Files Web User Interface	0	4
G726-16	Configuration Files Web User Interface	0	103
G726-24	Configuration Files Web User Interface	0	104
G726-32	Configuration Files Web User Interface	0	102
G726-40	Configuration Files Web User Interface	0	105
ilbC	Configuration Files Web User Interface	0	106

The corresponding attributes of the codec are listed as follows:

### Procedure

Configuration changes can be performed using the configuration files or locally.

		Configure the codecs to use on a per-line basis.
		Parameters:
		account.1.codec.Y.enable
Configuration File		account.1.codec.Y.payload_type
Comportation me	<mac>.cig</mac>	Configure the priority and rtpmap for the enabled codec.
		Parameters:
		account.1.codec.Y.priority
		account.1.codec.Y.rtpmap
		Configure the codecs to use on a per-line basis.
		Configure the priority for the
Local	Web User	enabled codec.
	Interface	Navigate to:
		http:// <phonelpaddress>/servlet?</phonelpaddress>
		p=account-codec&q=load&acc= 0
		0

## Details of Configuration Parameters:

Parameters	Permitted Values	Default			
account.1.codec.Y.enable	0 or 1	Refer to the following			
(Y ranges from 1 to 11)	0 or 1	content			
Description:					
Enables or disables the specified cod	dec for the account.				
0-Disabled					
1-Enabled					
Default:	Default:				
For SIP-T48G/T46G/T42G/T41P:					
When Y=1, the default value is 1;					
When Y=2, the default value is 1;					
When Y=3, the default value is 0;					
When Y=4, the default value is 0;					
When Y=5, the default value is 1;					

Parameters	Permitted Values	Default	
When Y=6, the default value is 1;			
When Y=7, the default value is 0;			
When Y=8, the default value is 0;			
When Y=9, the default value is 0;			
When Y=10, the default value is 0;			
When Y=11, the default value is 0;			
For SIP-T40P:			
When Y=1, the default value is 1;			
When Y=2, the default value is 1;			
When Y=3, the default value is 1;			
When Y=4, the default value is 1;			
When Y=5, the default value is 0;			
When Y=6, the default value is 0;			
When Y=7, the default value is 0;			
When Y=8, the default value is 0;			
When Y=9, the default value is 0;			
Example:			
account.1.codec.1.enable = 1			
It means that the codec PCMU is en	abled on the account.		
Web User Interface:			
Account->Codec			
Phone User Interface:			
None			
account.1.codec.Y.payload_type	Refer to the	Refer to the following	
(Y ranges from 1 to 11)	following content	content	
Description:			
Configures the codec for the account.			
Permitted Values:			
G722, PCMU, PCMA, G729, G726-16, G726-24, G726-32, G726-40, iLBC, G723_53,			
G723_63			
For SIP-T48G/T46G/T42G/T41P:			
When Y=1, the default value is PCMU;			
When Y=2, the default value is PCMA;			
When Y=3, the default value is G723	_53;		

Parameters	Permitted Values	Default	
When Y=4, the default value is G723	_63;		
When Y=5, the default value is G729,	;		
When Y=6, the default value is G722,	;		
When Y=7, the default value is iLBC;			
When Y=8, the default value is G726	-16;		
When Y=9, the default value is G726	-24;		
When Y=10, the default value is G72	6-32;		
When Y=11, the default value is G72	6-40;		
For SIP-T40P:			
When Y=1, the default value is PCML	J;		
When Y=2, the default value is PCMA	Α;		
When Y=3, the default value is G729,	;		
When Y=4, the default value is G722,	;		
When Y=5, the default value is iLBC;			
When Y=6, the default value is G726	-16;		
When Y=7, the default value is G726	-24;		
When Y=8, the default value is G726	-32;		
When Y=9, the default value is G726	-40;		
Example:			
account.1.codec.1.payload_type =	PCMU		
Web User Interface:			
Account->Codec			
Phone User Interface:			
None			
account.1.codec.Y.priority	Interestiven 0 to 12	Refer to the following	
(Y ranges from 1 to 11)	meger from 0 10 12	content	
Description:			
Configures the priority of the enabled codec for the account.			
For SIP-T48G/T46G/T42G/T41P:			
When Y=1, the default value is 2;			
When Y=2, the default value is 3;			
When Y=3, the default value is 0;			
When Y=4, the default value is 0;			
When Y=5, the default value is 4;			

Parameters	Permitted Values	Default		
When Y=6, the default value is 1;				
When Y=7, the default value is 0;				
When Y=8, the default value is 0;				
When Y=9, the default value is 0;				
When Y=10, the default value is 0;				
When Y=11, the default value is 0;				
For SIP-T40P:				
When Y=1, the default value is 2;				
When Y=2, the default value is 3;				
When Y=3, the default value is 4;				
When Y=4, the default value is 1;				
When Y=5, the default value is 0;				
When Y=6, the default value is 0;				
When Y=7, the default value is 0;				
When Y=8, the default value is 0;				
When Y=9, the default value is 0;				
Example:				
account.1.codec.1.priority = 2				
Web User Interface:				
Account->Codec				
Phone User Interface:				
None				
account.1.codec.Y.rtpmap	Integer	Refer to the following		
(Y ranges from 1 to 11)	from 0 to 127	content		
Description:				
Configures the rtpmap of the audio	codec for the account	t.		
For SIP-T48G/T46G/T42G/T41P:				
When Y=1, the default value is 0;				
When Y=2, the default value is 8;				
When Y=3, the default value is 4;				
When Y=4, the default value is 4;				
When Y=5, the default value is 18;				
When Y=6, the default value is 9;				
When Y=7, the default value is 106;				

Parameters	Permitted Values	Default
When Y=8, the default value is 103;		
When Y=9, the default value is 104;		
When Y=10, the default value is 102;		
When Y=11, the default value is 105;		
For SIP-T40P:		
When Y=1, the default value is 0;		
When Y=2, the default value is 8;		
When Y=3, the default value is 18;		
When Y=4, the default value is 9;		
When Y=5, the default value is 106;		
When Y=6, the default value is 103;		
When Y=7, the default value is 104;		
When Y=8, the default value is 102;		
When Y=9, the default value is 105;		
Example:		
account.1.codec.1.rtpmap = 0		
Web User Interface:		
None		
Phone User Interface:		
None		

To configure the codecs to use and adjust the priority of the enabled codecs on a per-line basis via web user interface:

- 1. Click on Account->Codec.
- 2. Select the desired account from the pull-down list of Account.
- Select the desired codec from the Disable Codecs column and then clic → .
   The selected codec appears in the Enable Codecs column.
- 4. Repeat the step 4 to add more codecs to the Enable Codecs column.
- 5. To remove the codec from the Enable Codecs column, select the desired codec and then click .

To adjust the priority of codecs, select the desired codec and then clicl ↑
 or ↓

Yealink	Status	Account	Network	Features	Settings	Directory	Log Out Security
Register Basic Codec	Aud	io Codecs Disable Co 6726-40 6726-24 6726-24 6726-24 6726-24 6726-24 6722-63 6723_63 6723_63 6723_53 Confi	decs	Enable Codecs G722 PCMU PCMA G729	î L Cancel		NOTE Codecs Choose the codecs you want to use. You can click here to get more guides.

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

# Acoustic Clarity Technology

## **Acoustic Echo Cancellation**

Acoustic Echo Cancellation (AEC) is used to reduce acoustic echo from a voice call to provide natural full-duplex communication patterns. It also increases the capacity achieved through silence suppression by preventing echo from traveling across a network. IP phones employ advanced AEC for hands-free operation. AEC is not normally required for calls via the handset. In certain situation, where echo is experienced by the remote party, AEC may be used to reduce/avoid echo when the user uses the handset.

Note Utilizing acoustic echo cancellation will introduce a small delay increase into audio path which might cause a lower voice quality.

#### Procedure

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure AEC. Parameter:
		voice.echo_cancellation
Local		Configure AEC.
	Web User Interface	Navigate to:
		http:// <phonelpaddress> /servlet?p=settings-voice &amp;q=load</phonelpaddress>

AEC can be configured using the configuration files or locally.

#### Details of the Configuration Parameter:

Parameter	Permitted Values	Default	
voice.echo_cancellation	0 or 1	1	
Description:			
Enables or disables AEC (Ad	coustic Echo Canceller) feat	ure on the IP phone.	
0-Disabled			
1-Enabled			
Web User Interface:			
Settings->Voice->Echo Cancellation->ECHO			
Phone User Interface:			
None			

#### To configure AEC via web user interface:

- 1. Click on **Settings**->**Voice**.
- 2. Select the desired value from the pull-down list of ECHO.

Voglink			Log Out
	Status Account Network	Features Settings Directory	Security
Preference	Echo Cancellation 🕜		NOTE
Time&Date	ЕСНО	Enabled - 🕜	VAD
Upgrade	CNG	Disabled    Cartery Contraction    Cartery Contraction    Cartery Contraction     Cartery Contraction     Cartery Contraction     Cartery Contraction     Cartery Contraction     Cartery Contraction     Cartery Contraction     Cartery Contraction     Cartery Contraction     Cartery Contraction     Cartery Contraction     Cartery Contraction      Cartery Contraction       Cartery Contraction	Voice Activity Detection.
Auto Provision	JITTER BUFFER 💡		Comfort Noise Generation.
Configuration	Туре	Adaptive O Fixed	JITTER BUFFER It is a shared data area where
Dial Plan	Min Delay	60	stored, and sent to the voice
Voice	Normal	120	You can click here to get
Tones	Confirm	Cancel	more guides.

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

## **Background Noise Suppression**

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

## **Automatic Gain Control**

Automatic Gain Control (AGC) is applicable to hands-free operation and is used to keep audio output at nearly a constant level by adjusting the gain of signals in certain

circumstances. This increases the effective user-phone radius and helps with the intelligibility of talkers.

## **Voice Activity Detection**

Voice Activity Detection (VAD) is used in speech processing to detect the presence or absence of human speech. When detecting period of "silence", VAD replaces that silence efficiently with special packets that indicate silence is occurring. It can facilitate speech processing, and deactivate some processes during non-speech section of an audio session. VAD can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

### Procedure

VAD can be configured using the configuration files or locally.

		Configure VAD.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameter:
		voice.vad
		Configure VAD.
Local		Navigate to:
	Web User Interface	http:// <phonelpaddress> /servlet?p=settings-voice</phonelpaddress>
		&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default		
voice.vad	0 or 1	0		
Description:				
Enables or disables VAD (Vo	oice Activity Detection) featu	ure on the IP phone.		
0-Disabled				
1-Enabled				
Web User Interface:				
Settings->Voice->Echo Cancellation->VAD				
Phone User Interface:				
None				

#### To configure VAD via web user interface:

1. Click on Settings->Voice.

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

Yealink 17466	Status Account Network	Features Settings Directory	Log Out
Preference	Echo Cancellation 🕜		NOTE
Time&Date	ECHO	Enabled	VAD
Upgrade	CNG	Enabled	CNG
Auto Provision	JITTER BUFFER 🕜		Comfort Noise Generation.
Configuration	Туре	Adaptive O Fixed	JITTER BUFFER It is a shared data area where value packets can be collected
Dial Plan	Min Delay	60	stored, and sent to the voice
Dia Francisco - Constantino -	Max Delay	240	processor in evenly.
Voice	Normal	120 🕜	You can click here to get
Tones	Confirm	Cancel	more guides.

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

## **Comfort Noise Generation**

Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation. It is a part of the silence suppression or VAD handling for VoIP technology. CNG, in conjunction with VAD algorithms, quickly responds when periods of silence occur and inserts artificial noise until voice activity resumes. The insertion of artificial noise gives the illusion of a constant transmission stream, so that background sound is consistent throughout the call and the listener does not think the line has released. The purpose of VAD and CNG is to maintain an acceptable perceived QoS while simultaneously keeping transmission costs and bandwidth usage as low as possible.

Note VAD is used to send CN packets when phone detect a "silence" period; CNG is used to generate comfortable noise when phone receives CN packets from the other side.

For example, A is talking with B.

A: VAD=1, CNG=1

B: VAD=0, CNG=1

If A mutes the call, since VAD=1, A will send CN packets to B. When receiving CN packets, B will generate comfortable noise.

If B mutes the call, since VAD=0, B will not send CN packets to A. So even if CNG=1 (B), A will not hear comfortable noise.

### Procedure

CNG can be configured using the configuration files or locally.

		Configure CNG.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameter:
		voice.cng
		Configure CNG.
		Navigate to:
Local	Web User Interface	http:// <phonelpaddress> /servlet?p=settings-voice &amp;q=load</phonelpaddress>

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default		
voice.cng	0 or 1	1		
Description:				
Enables or disables CNG (Comforto	able Noise Generatio	n) feature on the IP phone.		
0-Disabled				
1-Enabled				
Web User Interface:				
Settings->Voice->Echo Cancellation->CNG				
Phone User Interface:				
None				

#### To configure CNG via web user interface:

- 1. Click on Settings->Voice.
- 2. Select the desired value from the pull-down list of CNG.

			Log Out
Yealink   1466	Status Account Network	Features Settings Directory	Security
Preference	Echo Cancellation 💡		NOTE
Time&Date	ECHO VAD	Enabled • ? Disabled • ?	VAD Voice Activity Detection.
Upgrade	CNG	Enabled 👻 🕜	CNG
Auto Provision	JITTER BUFFER 🕜		Comfort Noise Generation.
Configuration	Туре	Adaptive      Fixed	JITTER BUFFER It is a shared data area where voice packets can be collected.
Dial Plan	Min Delay Max Delay	240 2	stored, and sent to the voice processor in evenly.
Voice	Normal	120	You can click here to get
Tones	Confirm	Cancel	more guides.

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

## **Jitter Buffer**

Jitter buffer is a shared data area where voice packets can be collected, stored, and sent to the voice processor in even intervals. Jitter is a term indicating variations in packet arrival time, which can occur because of network congestion, timing drift or route changes. The jitter buffer, located at the receiving end of the voice connection, intentionally delays the arriving packets so that the end user experiences a clear connection with very little sound distortion. IP phones support two types of jitter buffers: fixed and adaptive. A fixed jitter buffer adds the fixed delay to voice packets. You can configure the delay time for the static jitter buffer on IP phones. An adaptive jitter buffer is capable of adapting the changes in the network's delay. The range of the delay time for the dynamic jitter buffer added to packets can be also configured on IP phones.

### Procedure

Jitter buffer can be configured using the configuration files or locally.

		Configure the mode of jitter buffer and the delay time for jitter buffer.
Configuration File	(	Parameters:
Configuration File	<y000000000xx>.cfg</y000000000xx>	voice.jib.adaptive
		voice.jib.min
		voice.jib.max
		voice.jib.normal
		Configure the mode of jitter buffer and the delay time for jitter buffer.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress> /servlet?p=settings-voice &amp;q=load</phonelpaddress>

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default
voice.jib.adaptive	0 or 1	1
Description:		
Configures the type of jitter buffer.		

Parameters	Permitted Values Default					
0-Fixed						
1-Adaptive						
Web User Interface:						
Settings->Voice->JITTER BUFFER->Type						
Phone User Interface:						
None						
voice.jib.min	Integer from 0 to 400	60				
Description:						
Configures the minimum delay time (in	n milliseconds) of jitter buffer.					
<b>Note</b> : It works only if the value of the p (Adaptive).	arameter "voice.jib.adaptiv	e" is set to 1				
Web User Interface:						
Settings->Voice->JITTER BUFFER->Min D	pelay					
Phone User Interface:						
None						
voice.jib.max	roice.jib.max Integer from 0 to 400 240					
Description:						
Configures the maximum delay time (	in milliseconds) of jitter buffe	r.				
<b>Note</b> : It works only if the value of the p (Adaptive).	<b>Note</b> : It works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive).					
Web User Interface:						
Settings->Voice->JITTER BUFFER->Max [	Delay					
Phone User Interface:						
None						
voice.jib.normal	voice.jib.normal Integer from 0 to 400 120					
Description:						
Configures the normal delay time (in r	nilliseconds) of jitter buffer.					
<b>Note</b> : It works only if the value of the parameter "voice.jib.adaptive" is set to 0 (Fixed).						
Web User Interface:						
Settings->Voice->JITTER BUFFER->Norm	al					

Parameters	Permitted Values	Default
Phone User Interface:		
None		

To configure Jitter Buffer via web user interface:

- 1. Click on Settings->Voice.
- 2. Mark the desired radio box in the **Type** field.
- Enter the minimum delay time for adaptive jitter buffer in the Min Delay field.
   The valid value ranges from 0 to 300.
- Enter the maximum delay time for adaptive jitter buffer in the Max Delay field. The valid value ranges from 0 to 300.
- Enter the fixed delay time for fixed jitter buffer in the Normal field.
   The valid value ranges from 0 to 300.

			Log Out
Yealink   146G	Status Account Network	Features Settings Directory	Security
Preference	Echo Cancellation 🕜		NOTE
Time&Date	ECHO VAD	Enabled	VAD Voice Activity Detection.
Upgrade	CNG	Enabled 🗸	CNG
Auto Provision	JITTER BUFFER		Comfort Noise Generation.
Configuration	Type Min Doby	Adaptive      Fixed	JITTER BUFFER It is a shared data area where voice packets can be collected,
Dial Plan	Max Delay	240	stored, and sent to the voice processor in evenly.
Voice	Normal	120	You can click here to get
Tones	Confirm	Cancel	more guides.

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

# **Configuring Security Features**

This chapter provides information for making configuration changes for the following security-related features:

- Skype for Business Feature License
- User Password
- Administrator Password
- Auto-Logout Time
- Phone Lock
- Account Lock
- Transport Layer Security
- Encrypting Configuration Files
- 802.1X Authentication

## Skype for Business Feature License

By default, the Skype for Business phone has a built-in Skype for Business feature license, which allows user to use Yealink phones in a Skype for Business environment directly.

If users purchase SIP phones which aren't running Skype for Business firmware, while the user wants to upgrade firmware to a Skype for Business firmware, then a Skype for Business feature license is needed to be uploaded to the IP phone after the update. Contact Yealink resellers to purchase the license.

### Procedure

Skype for Business feature license can be configured using the configuration files or locally.

Configuration File <y000000000xx>.cfg</y000000000xx>		Specify the access URL of Skype for Business feature license. <b>Parameter:</b> lync_license_dat.url		
Local	Web User Interface	Specify the access URL of Skype for Business feature license. <b>Navigate to:</b> http:// <phoneipaddress>/servlet ?p=security-license&amp;q=load</phoneipaddress>		

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default		
lync_license_dat.url	String within 99 characters	Blank		
Description:				
Configures the access URL of the Skype f	or Business feature license.			
Example:				
lync_license_dat.url = http://192.168.1.20	/License_\$MAC.dat			
Example:				
The IP phones will replace the characters "\$MAC" with its MAC addresses during auto provisioning. For example, the MAC address of one SIP-T46G IP phone is 00156543EC97. When performing auto provisioning, the IP phone will request to download the License_00156543ec97.dat file from the provisioning server address "http://192.168.1.20".				
Web User Interface:				
Security->License				
Phone User Interface:				
None				
<b>Note:</b> If you change this parameter, the I take effect.	P phone will reboot to make the a	change		

#### To upload the Skype for Business feature license via web user interface:

- 1. Click on **Security->License**.
- 2. Click **Browse** to select the license from your local system.

Vealink					Log Out		
	Status	Account	Network	Features	Settings	Directory	Security
License Password Trusted Certificates	<b>Im</b> Uple	port License		Br	Upload		NOTE security-license-note You can click here to get more guides.
Server Certificates							

3. Click **Upload** to upload the certificate.

## **License Status**

You can view the Skype for Business Server license status via web user interface.

#### To view the Skype for Business license status via web user interface:

1. Click on Status->SFB Status

Yealink   1466	Status Account	Network Features Set	Log Out
Status	Phone Status		NOTE
SFB Status	License Status	Installed	status-lync-note
			You can click here to get more guides.

# **User Password**

Some menu options are protected by two privilege levels, user and administrator, each with its own password. When logging into the web user interface, you need to enter the user name and password to access various menu options.

A user or an administrator can change the user password. The default user password is "user". For security reasons, the user or administrator should change the default user password as soon as possible.

### Procedure

User password can be changed using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Change the user password of the IP phone. <b>Parameter:</b> security.user_password
Local	Web User Interface	Change the user password of the IP phone. <b>Navigate to:</b> http:// <phoneipaddress>/servlet ?p=security&amp;q=load</phoneipaddress>

#### Details of the Configuration Parameter:

Parameter	Permitted Values	Default		
security.user_password	String within 32 characters	user		
Description:				
Configures the password of the user for p	hone's web user interface acces	s.		
The IP phone uses "user" as the default u	ser password.			
The valid value format is username:new p	bassword.			
Example:				
security.user_password = user:123 means setting the password of user (current user name is "user") to password 123.				
<b>Note</b> : IP phones support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via web user interface only.				
Web User Interface:				
Security->Password				
Phone User Interface:				
None				

To change the user password via web user interface:

- 1. Click on **Security->Password**.
- 2. Select user from the pull-down list of User Type.
- 3. Enter new password in the New Password and Confirm Password fields.

Valid characters are ASCII characters 32-126(0x20-0x7E) except 58(3A).

Yealink	Status Account Network	Features Settings	Log Out
License Password Trusted Certificates Server Certificates	User Type Old Password New Password Confirm Password Confirm	user	NOTE User Type Select your type. If you log in as user, you can only change your own password. If you login as an administrator, you can modify both the user's and admin's passwords.

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

Note

If logging into the web user interface of the IP phone using User sign-in method, you need to enter the old user password in the **Old Password** field.

# Administrator Password

Advanced menu options are strictly used by administrators. Users can configure them only if they have administrator privileges. The administrator password can only be changed by an administrator. The default administrator password is "admin". For security reasons, the administrator should change the default administrator password as soon as possible.

### Procedure

Administrator password can be changed using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Change the administrator password. <b>Parameter</b> : security.user_password
Local	Web User Interface	Change the administrator password. <b>Navigate to</b> : http:// <phonelpaddress>/servlet ?p=security&amp;q=load</phonelpaddress>
	Phone User Interface	Change the administrator password.

### Details of the Configuration Parameter:

Parameter	Permitted Values	Default
security.user_password	String within 32 characters	admin
	L	1

#### Description:

Configures the password of the administrator for phone's web user interface access. The IP phone uses "admin" as the default administrator password.

#### Example:

security.user\_password = admin:123 means setting the password of administrator (current user name is "admin") to password 123.

**Note**: IP phones support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via web user interface only.

#### Web User Interface:

Security->Password

Phone User Interface:

Parameter	Permitted Values	Default
Menu-> Advanced->Set Password		

To change the administrator password via web user interface:

- 1. Click on Security->Password.
- 2. Select admin from the pull-down list of User Type.
- 3. Enter the current administrator password in the Old Password field.
- 4. Enter new password in the New Password and Confirm Password fields.

Valid characters are ASCII characters 32-126(0x20-0x7E) except 58(3A).

Vealink				Log Out
St	Status Account Network	Features Set	ttings Directory	Security
License	User Type	admin 👻	0	NOTE
Password	Old Password	•••••	0	User Type
Trusted Certificates	New Password Confirm Password	•••••	0	Select your type. If you log in as user, you can only change your own password. If you login
Server Certificates				as an administrator, you can modify both the user's and
	Confirm	Cancel		admin's passwords.

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

To change the administrator password via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Set Password.
- 2. Enter the current administrator password in the Current PWD field.
- Enter new password in the New PWD field and Confirm PWD field.
   Valid characters are ASCII characters 32-126(0x20-0x7E).
- 4. Press the **Save** soft key to accept the change.

# Auto-Logout Time

Auto-logout time defines a specific period of time during which the IP phones will automatically log out if you have not performed any actions via web user interface. Once logging out, you must re-enter username and password for web access authentication.

#### Procedure

Auto-logout time can be configured using the configuration files or locally.

		Configure auto-logout time.
Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Parameter:
		features.relog_offtime

local		Configure auto-logout time.		
	Web User Interface	Navigate to:		
		http:// <phonelpaddress>/servlet ?p=features-general&amp;q=load</phonelpaddress>		

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default		
features.relog_offtime	Integer from 1 to 1000	5		
Description:				
Configures the timeout interval (in minutes	) for web access authenticatior	۱.		
Example:				
features.relog_offtime = 5				
If you log into the web user interface and leave it for 5 minutes, it will automatically log out.				
<b>Note</b> : If you change this parameter, the IP phone will reboot to make the change take effect.				
Web User Interface:				
Features->General Information->Auto-Log	out Time(1~1000min)			
Phone User Interface:				
None				

To configure the auto-logout time via web user interface:

1. Click on Features->General Information.

2. Enter the desired auto-logout time in Auto-Logout Time(1~1000min) field.

alink									Log (
	Status	Account	Network	Features	Settin	gs	Directory	Security	
General		General Informati	ion 🕜					NOTE	
Information		Call Waiting		Enabled	•	0		Call Waiting	
Audio		Key As Send		#	•	0		This call feature	ire allows your ept other incom
Remote Control		Busy Tone Delay	(Seconds)	0	•	0		calls during th	e conversation.
		Return code whe	n refuse	603 (Decline)	•	0		Key As Send	1
Bluetooth				:				Select * or #	as the send key
Power LED				•				🛛 You can d	click here to get
		Auto-Logout Tim	e(1~1000min)	5		0		more guides	
		Call Number Filter				0	•		
		Voice Mail Tone		Enabled	•	0			
		DHCP Hostname		SIP-T46G		0			
		E911 Location Tip	0	Enabled	•	0			
		Update Checking	Time	24		0			
		Use DHCP Option	120	Disabled	•	0			
		SFB Cert Service	URL			0			
		Enable SFB Autor	nation	Disabled	-	0			
		SFB Inactive Time	2	5		0			
		SFB Away Time		5		0			
		Device Pairing for	Online	Enabled	•	0			
		Confi	rm		Cancel				

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

## Phone Lock

If system administrator sets the policy "ucEnforcePinLock" = true on the Skype for Business Fronted Server, user can use phone lock feature to lock the IP phone to prevent it from unauthorized use. And the IP phone will prompt the user to configure an n-digit unlock PIN at the initial sign-in.

U	Unlock PIN Setting			
New PIN:	PIN's length	must be from 6 to	15	
Confirm PIN:				
:	123	Delete	Save	

The minimum PIN length is dictated in the policy information pushed during the in-band provisioning as a value in "<ucMinPinLength></ucMinPinLength>", so the PIN length should be greater than or equal to the specified value. Once the IP phone is locked, a user must enter the unlock PIN to unlock it.
#### Do one of the following to lock the IP phone:

- Long press the pound key when the IP phone is idle.
- Press Menu->Basic->Phone Unlock PIN. Then select Lock the phone, and then press the OK soft key.
- The phone will be locked automatically if when it has been inactive for the designated time. The time is specified in the ucTimeout policy on Skype for Business Frontend Server.

If you enable phone lock feature, available features are limited. They are described as below:

- **1.** User is able to receive calls.
- 2. User is able to dial emergency numbers.
- 3. User cannot make any outbound call.
- 4. User cannot forward an incoming call to another user.
- 5. User cannot search the directory.
- 6. User cannot see favorite lists displayed on the screen.
- 7. User cannot access voicemail without first unlocking the phone or providing a voicemail PIN.

If the Skype for Business Server is configured not to lock the phone, the phone will not have the phone lock feature.

If the Skype for Business Server is configured to forcibly lock the phone, the phone lock feature will be enabled on the phone by default. User can also disable the phone lock feature as needed. The following introduces how to disable or enable the phone lock feature on the phone.

### Procedure

Phone lock configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Configure the phone lock feature. <b>Parameter</b> :	
		sfb.phone_lock.enable	
		Configure the phone lock feature.	
	Web User Interface	Change the unlock PIN.	
least		Navigate to:	
Local		http:// <phonelpaddress>/servlet</phonelpaddress>	
		?p=features-phonelock&q=load	
	Phone User Interface	Configure the phone lock feature.	

	Change the unlock PIN.
--	------------------------

## **Details of Configuration Parameter:**

Parameters	Permitted Values	Default		
sfb.phone_lock.enable	0 or1	0		
Description:				
Enables or disables the phone lock feature	Jre.			
0- Enabled				
1- Disabled				
If it is set to 0 (Enabled), the IP phone will prompt the user to configure an n-digit unlock PIN at the initial sign-in.				
Web User Interface:				
Settings->Phone Lock				
Phone User Interface:				
None				

#### To configure phone lock via web user interface:

- 1. Click on Settings->Phone Lock.
- 2. Select the desired value from the pull-down list of **Phone Lock**.
  - If it is enabled, users need to configure a unlock PIN before sign-in.
  - If it is disabled, users do not need to configure a unlock PIN before sign-in and the phone will not be locked.
- 3. Enter the unlock PIN in the Phone Unlock PIN(6~15 Digit) field.

Voalink			Log Out
	Status Account Network	Features Settings Directory	Security
Preference Time&Date Upgrade Auto Provision Configuration Dial Plan	Phone Lock Phone Unlock PIN(6~15 Digit) Confirm	Enabled  Cancel	NOTE settings-phonelock-note
Voice Tones Phone Lock			

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

#### To change the phone Unlock PIN via phone user interface:

- 1. Press Menu->Basic->Phone Unlock PIN->Change PIN.
- 2. Enter the current unlock PIN in the Current PIN field.
- 3. Enter the new unlock PIN in the New PIN field.
- 4. Enter the new unlock PIN again in the Confirm PIN field.
- 5. Press the Save soft key to accept the change.

# Account Lock

Account lock is used to lock the account on the IP phone. It can prevent your account being signed in or signed out randomly. If account lock feature is enabled, users are prompted for administrator password to sign in or sign out. This feature is especially useful for public area telephone users.

### Procedure

Account lock can be configured using the configuration files or locally.

		Configure account lock.
Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Parameters:
		sfb.account_lock.enable
		Configure account lock.
	Web User Interface	Navigate to:
Local		http:// <phonelpaddress>/servlet?</phonelpaddress>
		p=account-basic&q=load&acc=0
	Phone User Interface	Configure account lock.

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default	
sfb.account_lock.enable	0 or 1	0	
Description:			
Enables or disables the IP phone to lock the	account to prevent the acco	unt being	
signed in or signed out randomly.			
0-Disabled			
1-Enabled			
If it is set to 1 (Enabled), the IP phone will prompt for administrator password to sign in			
Web liser interface:			

Parameters	Permitted Values	Default
Account->Basic->Account Lock		
Phone User Interface:		
Menu->Advanced (default password: admin	n)->Account Lock	

#### To configure account lock feature via web user interface:

- 1. Click on Account->Basic.
- 2. Select the desired value from the pull-down list of Account Lock.

Yealink   1466	Status Account Network	Features Settings	Log Out
Register	Missed Call Log	Enabled 🔹 🕐	NOTE
Basic	Auto Answer Ring Type	Disabled • ? Common • ?	<b>Basic</b> The basic parameters for
Codec	Account Lock	Disabled • ?	administrator. Proxy Require
	Confirm	Cancel	A special parameter just for Nortel server. If you login to Nortel server, the value should be, com.nortelnetworks.firewall
			You can click here to get more guides.

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

To configure the account lock feature via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Account Lock.
- 2. Press  $(\cdot)$  or  $(\cdot)$ , or the Switch soft key to select **On** from the Account Lock field.
- 3. Press the Save soft key to accept the change.

# **Transport Layer Security**

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing IP phones to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

TLS protocol is composed of two layers: TLS Record Protocol and TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The TLS protocol uses asymmetric encryption for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for integrity.

• Symmetric encryption: For symmetric encryption, the encryption key and the

corresponding decryption key can be told by each other. In most cases, the encryption key is the same as the decryption key.

• Asymmetric encryption: For asymmetric encryption, each user has a pair of cryptographic keys – a public encryption key and a private decryption key. The information encrypted by the public key can only be decrypted by the corresponding private key and vice versa. Usually, the receiver keeps its private key. The public key is known by the sender, so the sender sends the information encrypted by the known public key, and then the receiver uses the private key to decrypt it.

IP phones support TLS version 1.0. A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the TLS/SSL network protocol. IP phones support the following cipher suites:

- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the IP phone and TLS server to establish an encrypted communication channel:

Eile	Ę	Edit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u> <u>Statistics</u>	Telephony <u>T</u> ools <u>H</u> elp		
	ï		¥   🖻 🛃 🗙 🛃 占	🔍 🗢 🖨 🛱	7 🕹	
Filte	er:			•	<ul> <li>Expressi</li> </ul>	ion Clear Apply
No.		Time	Source	Destination	Protocol	Info
	1	0.000000	192.168.3.86	192.168.0.230	SSLV3	Client Hello
	2	0.021345	192.168.0.230	192.168.3.86	SSLV3	Server Hello, Certificate, Server Key Exchange, Server Hello Done
	3	0.954947	192.168.3.86	192.168.0.230	SSLV3	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
	4	0.970099	192.168.0.230	192.168.3.86	SSLV3	Change Cipher Spec, Encrypted Handshake Message
	5	1.012295	192.168.3.86	192.168.0.230	SSLV3	Application Data, Application Data
	6	1.013562	192.168.0.230	192.168.3.86	SSLV3	Application Data
	7	1.013667	192.168.0.230	192.168.3.86	SSLV3	Application Data
	ir.	ma 13 · 652	bytes on wire (5216	hits) 652 hytes	canture	d (5216 bits)
	t k	nernet TT	Src: Vmware 72:09:2e	(00.0c.20.72.c0.2	a) Det	viamenve 11.12.b7 (00.15.65.11.12.b7)
	Totempet Protocol sec: 102168 ( 230 (102168 ( 230) pet: 102168 3 86 (102168 3 86)					
	Transmission Control Protocol Src Port: https://doi.org/10.1000/192100.1000 (192100.1000) Seq: 1482 Ack: 437 Len: 586					
E S	sector socket laver					
1.00		and sources				

Step1: IP phone sends "Client Hello" message proposing SSL options.

**Step2:** Server responds with "Server Hello" message selecting the SSL options, sends its public key information in "Server Key Exchange" message and concludes its part of the negotiation with "Server Hello Done" message.

**Step3:** IP phone sends session key information (encrypted by server's public key) in the "Client Key Exchange" message.

**Step4:** Server sends "Change Cipher Spec" message to activate the negotiated options for all future messages it will send.

IP phones can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon appears on the LCD screen after the successful TLS negotiation.

## Certificates

The IP phone can serve as a TLS client or a TLS server. The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate**: When the IP phone requests a TLS connection with a server, the IP phone should verify the certificate sent by the server to decide whether it is trusted based on the trusted certificates list. The IP phone has 44 built-in trusted certificates. You can upload 10 custom certificates at most. The format of the trusted certificate files must be \*.pem,\*.cer,\*.crt and \*.der and the maximum file size is 5MB. For more information on 44 trusted certificates, refer to Appendix C: Trusted Certificates on page 346.
- Server Certificate: When clients request a TLS connection with the IP phone, the IP phone sends the server certificate to the clients for authentication. The IP phone has two types of built-in server certificates: a unique server certificate and a generic server certificate. You can only upload one server certificate to the IP phone. The old server certificate will be overridden by the new one. The format of the server certificate files must be \*.pem and \*.cer and the maximum file size is 5MB.
- **A unique server certificate**: It is unique to an IP phone (based on the MAC address) and issued by the Yealink Certificate Authority (CA).

- A generic server certificate: It issued by the Yealink Certificate Authority (CA). Only if no unique certificate exists, the IP phone may send a generic certificate for authentication.

The IP phone can authenticate the server certificate based on the trusted certificates list. The trusted certificates list and the server certificates list contain the default and custom certificates. You can specify the type of certificates the IP phone accepts: default certificates, custom certificates or all certificates.

Common Name Validation feature enables the IP phone to mandatorily validate the common name of the certificate sent by the connecting server. And Security verification rules are compliant with RFC 2818.

**Note** In TLS feature, we use the terms trusted and server certificate. These are also known as CA and device certificates.

Resetting the IP phone to factory defaults will delete custom certificates by default. But this feature is configurable using the configuration files. For more information on the configuration parameter, refer to Transport Layer Security on page 292.

## Procedure

Configuration changes can be performed using the configuration files or locally.

	<y00000000xx>.cfg</y00000000xx>	Configure trusted certificates
		teature.
		Parameters:
		security.trust_certificates
		security.ca_cert
		security.cn_validation
		Configure server certificates feature.
		Parameters:
		security.dev_cert
Configuration		Upload the trusted certificates.
File		Parameter:
		trusted_certificates.url
		trusted_certificates.url Delete all uploaded trusted
		trusted_certificates.url Delete all uploaded trusted certificates.
		trusted_certificates.url Delete all uploaded trusted certificates. <b>Parameter:</b>
		trusted_certificates.url Delete all uploaded trusted certificates. Parameter: trusted_certificates.delete
		trusted_certificates.url Delete all uploaded trusted certificates. Parameter: trusted_certificates.delete Upload the server certificates.
		trusted_certificates.url Delete all uploaded trusted certificates. Parameter: trusted_certificates.delete Upload the server certificates. Parameter:
		trusted_certificates.url Delete all uploaded trusted certificates. Parameter: trusted_certificates.delete Upload the server certificates. Parameter: server_certificates.url

		certificates.
		Parameter:
		server_certificates.delete
		Configure trusted certificates feature.
		Upload the trusted certificates.
		Navigate to:
Local	Web User Interface	http:// <phonelpaddress>/servlet?p=t rusted-cert&amp;q=load</phonelpaddress>
		Configure server certificates feature.
		Upload the server certificates.
		Navigate to:
		http:// <phonelpaddress>/servlet?p=</phonelpaddress>
		server-cert&q=load

## Details of Configuration Parameters:

Parameters	Permitted Values	Default				
security.trust_certificates	0 or 1	1				
Description:	Description:					
Enables or disables the IP phone to only trust th Certificates list.	ne server certificates in th	ne Trusted				
0-Disabled						
1-Enabled						
If it is set to 0 (Disabled), the IP phone will trust the server no matter whether the certificate sent by the server is valid or not.						
If it is set to 1 (Enabled), the IP phone will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, the IP phone will trust the server.						
<b>Note:</b> If you change this parameter, the IP phone will reboot to make the change take effect.						
Web User Interface:						
Security->Trusted Certificates->Only Accept Trusted Certificates						
Phone User Interface:						
None						
security.ca_cert 0, 1 or 2 2						

Parameters	Permitted Values	Default			
Description:					
Configures the type of certificates in the Truste authenticate for TLS connection.	ed Certificates list for the	IP phone to			
0-Default Certificates					
1-Custom Certificates					
2-All Certificates					
<b>Note:</b> If you change this parameter, the IP pho take effect.	one will reboot to make th	he change			
Web User Interface:					
Security->Trusted Certificates->CA Certificates					
Phone User Interface:					
None					
security.cn_validation 0 or 1 0					
Description:					
Enables or disables the IP phone to mandatori SubjectAltName of the certificate sent by the	ly validate the Common server.	Name or			
0-Disabled					
1-Enabled					
<b>Note:</b> If you change this parameter, the IP pho take effect.	one will reboot to make th	ne change			
Web User Interface:					
Security->Trusted Certificates->Common Name	e Validation				
Phone User Interface:					
None					
security.dev_cert	security.dev_cert 0 or 1 0				
Description:					
Configures the type of the device certificates for the IP phone to send for TLS authentication.					
0-Default Certificates					
1-Custom Certificates					
<b>Note:</b> If you change this parameter, the IP phone will reboot to make the change take effect.					

Parameters	Permitted Values	Default			
Web User Interface:					
Security->Server Certificates->Device Certific	ates				
Phone User Interface:					
None					
trusted_certificates.url	URL within 511 characters	Blank			
Description:					
Configures the access URL of the custom trus the connecting server.	ted certificate used to au	thenticate			
Example:					
trusted_certificates.url = http://192.168.1.20/t	c.crt				
<b>Note</b> : The certificate you want to upload mu format.	st be in *.pem, *.crt, *.cer (	or *.der			
Web User Interface:					
Security->Trusted Certificates->Load trusted of	ertificates file				
Phone User Interface:					
None					
trusted_certificates.delete	http://localhost/all	Blank			
Description:	·				
Deletes all uploaded trusted certificates.					
Example:					
trusted_certificates.delete = http://localhost/	all				
Web User Interface:					
None					
Phone User Interface:					
None					
server_certificates.url	URL within 511 characters	Blank			
Description:	1	1			
Configures the access URL of the certificate	he IP phone sends for aut	hentication			
Example:					
server_certificates.url = http://192.168.1.20/cd	a.pem				

Parameters	Permitted Values	Default				
Note: The certificate you want to upload must	<b>Note</b> : The certificate you want to upload must be in *.pem or *.cer format.					
Web User Interface:						
Security->Server Certificates->Load server cer	file					
Phone User Interface:						
None						
server_certificates.delete	http://localhost/all	Blank				
Description:						
Deletes all uploaded server certificates.						
Example:						
server_certificates.delete = http://localhost/al	l					
Web User Interface:	Web User Interface:					
None						
Phone User Interface:						
None						

To configure the trusted certificates via web user interface:

- 1. Click on Security->Trusted Certificates.
- 2. Select the desired values from the pull-down lists of Only Accept Trusted Certificates, Common Name Validation and CA Certificates.

Voglink						Log Out
	Status	Account	Network Features	Settings	Directory	Security
License	Index ID	Issued To	Issued By	Expiration	Delete	NOTE
Password	1	yealinkuc-YLAD-CA-1	Jan 12	2 11:40:48 2020 GMT	r 🖻	Trusted Certificates
Trusted Certificates	2					The trusted certificates list.
Server Certificates	4					You can click here to get more guides.
	5					
	6					
	7					
	8					
	10					
					Delete	
			Only Accept Trusted Certificates	Disabled	• 🕜	
			Common Name Validation	Disabled	• 🕜	
		l	CA Certificates	All Certificates	• 🕜	
	Im	port Trusted Certif	icates 🕜			
	Loa	ad trusted certificates	file Browse No file select	ed. Up	load	
		Confirm	n	Cancel		

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

#### To upload a trusted certificate via web user interface:

- 1. Click on Security->Trusted Certificates.
- 2. Click **Browse** to select the certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

Vaclink							Log Out
	Status	Account	Network	Features	Settings	Directory	Security
License	Index ID	Issued To	Issued By		Expiration	Delete	NOTE
Decruord	1	yealinkuc-YLAD-CA-1		Jan 12	11:40:48 2020 GM	IT 📃	Tructed Contificator
Passworu	2						The trusted certificates list.
Trusted Certificates	3						You can click here to get
Server Certificates	4						more guides.
	5						
	6						
	7						
	8						
	9						
	10						
						Delete	
			Only Accept Trust	ed Certificates	Disabled	• 0	
			Common Name Va	lidation	Disabled	• 0	
			CA Certificates		All Certificates	• 0	
	Im	port Trusted Certif	icates 🕜				
	Lo	ad trusted certificates	file Browse.	. No file select	ed. U	pload	
		Confirm	n		Cancel		

3. Click **Upload** to upload the certificate.

To configure the server certificates via web user interface:

- 1. Click on Security->Server Certificates.
- 2. Select the desired value from the pull-down list of **Device Certificates**.

Yealink	Status Account	Network	Features Settings	Directory	Log Out
License Password	Issued To	Issued By	Expiration	Delete	NOTE Server Certificates The server certificates list
Trusted Certificates Server Certificates	Import Server Cert	tificates ? Browse	No file selected.	Upload	You can click here to get more guides.
	Con	nfirm	Cancel		

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

To upload a server certificate via web user interface:

1. Click on Security->Server Certificates.

2. Click **Browse** to select the certificate (\*.pem and \*.cer) from your local system.

Yealink	Status	unt Network	Features Setting	s Directory	Log Out
License	Issued To	Issued By	Expiration	Delete Delete	NOTE Server Certificates
Trusted Certificates	Import Server	Device Certificate	s Custom Cerl	ificates 🔻 🕜	The server certificates list.
Server Certificates	Load server cer	file Browse	No file selected.	Upload	more guides.

3. Click **Upload** to upload the certificate.

A dialog box pops up to prompt "Success: The Server Certificate has been loaded! Rebooting, please wait...".

# **Encrypting Configuration Files**

Encrypted configuration files can be downloaded from the provisioning server to protect against unauthorized access and tampering of sensitive information (e.g., login passwords, registration information). Yealink supplies a configuration encryption tool for encrypting configuration files. The encryption tool encrypts plaintext <y000000000xx>.cfg and <MAC>.cfg files (one by one or in batch) using 16-character symmetric keys (the same or different keys for configuration files) and generates encrypted configuration files with the same file name as before. This tool also encrypts the plaintext 16-character symmetric keys using a fixed key, which is the same as the one built in the IP phone, and generates new files named as <xx\_Security>.enc (xx indicates the name of the configuration file, for example, y0000000028\_Security.enc for y0000000028.cfg file). This tool generates another new file named as Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

For a Microsoft Windows platform, you can use a Yealink-supplied encryption tool "Config\_Encrypt\_Tool.exe" to encrypt the <y000000000xx>.cfg and <MAC>.cfg files respectively.

**Note** Yealink also supplies a configuration encryption tool (yealinkencrypt) for Linux platform if required. For more information, refer to Yealink Configuration Encryption Tool User Guide.

For security reasons, administrator should upload encrypted configuration files, <y000000000xx\_Security>.enc and/or <MAC\_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the IP phone requests to download <y000000000xx>.cfg file first. If the downloaded configuration file is encrypted, the IP phone will request to download <y00000000xx\_Security>.enc file (if enabled) and decrypt it into the plaintext key (e.g., key2) using the built-in key (e.g., key1). Then the IP phone decrypts <y00000000xx>.cfg file using key2. After decryption, the IP phone resolves configuration files and updates configuration settings onto the IP phone system.

The way the IP phone processes the <MAC>.cfg file is the same to that of the<y000000000xx>.cfg file.

### **Procedure to Encrypt Configuration Files**

#### To encrypt the <y000000000xx>.cfg file:

1. Double click "Config\_Encrypt\_Tool.exe" to start the application tool.

The screenshot of the main page is shown as below:

Select File(s)		Browse
Target Directory	C:\Users\Administrator\Desktop\Configuration E	Browse
AES Model	C Manual <ul> <li>Auto Generate</li> </ul>	
AES KEY	FRaqbC8vvSA1XvpFV	Re-Generate
	Encrypt	

When you start the application tool, a file folder named "Encrypted" is created automatically in the directory where the application tool is located.

 Click Browse to locate configuration file(s) (e.g., y0000000028.cfg) from your local system in the Select File(s) field.

To select multiple configuration files, you can select the first file and then press and hold the **Ctrl** key and select the next files.

 (Optional.) Click Browse to locate the target directory from your local system in the Target Directory field.

The tool uses the file folder "Encrypted" as the target directory by default.

4. (Optional.) Mark the desired radio box in the AES Model field.

If you mark the **Manual** radio box, you can enter an AES key in the **AES KEY** field or click **Re-Generate** to generate an AES key in the **AES KEY** field. The configuration file(s) will be encrypted using the AES key in the **AES KEY** field.

If you mark the **Auto Generate** radio box, the configuration file(s) will be encrypted using random AES key. The AES keys of configuration files are different.

**Note** AES keys must be 16 characters and the supported characters contain:  $0 \sim 9$ ,  $A \sim Z$ ,  $a \sim z$  and the following special characters are also supported: # \* \* + , - . : = ? @ [] ^ {} .

5. Click **Encrypt** to encrypt the configuration file(s).

Select File(s)	C:\Users'	Config_Encrypt_Tool	× 000000000	Browse
Target Directory AES Model	C:\Users'	Encrypt Files Success!	figuration E	Browse
AES KEY	ZdtFNGiy	OK		Re-Generate

#### 6. Click OK.

The target directory will be automatically opened. You can find the encrypted CFG file(s), encrypted key file(s) and an Aeskey.txt file storing plaintext AES key(s).

😂 Encrypted						
File Edit View Favorites Tools	Help					
🜀 Back 👻 🕥 👻 🏂 🔎 Si	🕲 Back - 😥 - 🏂 🔎 Search 🎼 Folders 🛄 -					
Address 🗁 C:\Documents and Settings\	quefd\Desktop\Encrypted					
	Name 🔺 Size	е Туре	Date Modified			
File and Folder Tasks 🛛 🖄	Aeskey 1 Ki	8 Text Document	10/14/2014 7:01 PM			
💋 Make a new folder	y00000000028.ctg 6 Ki	B CFG File	10/14/2014 7:01 PM			
Publish this folder to the	job000000028_Security.enc	5 ENC FIIE	10)14)2014 7:01 MM			
Share this folder						
Other Places 🙁						
🚱 Desktop						
🗎 My Documents						
C Shared Documents						
S My Computer						
My Network Places						
Details 🛛 🕉						

## Procedure

AES keys can be configured using the configuration files.

		Configure AES keys.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:
		auto_provision.aes_key_16.com
		auto_provision.aes_key_16.mac
Local		Configure AES keys.
	Web User Interface	Navigate to:
		http:// <phonelpaddress>/servlet?</phonelpaddress>
		p=settings-autop&q=load
	Phone User Interface	Configure AES keys.

## Details of Configuration Parameters:

Parameters	Permitted Values	Default					
auto_provision.aes_key_16.com 16 characters Blank							
Description:							
Configures the plaintext AES key for decrypti	ng the Common CFG file.						
The valid characters contain: 0 ~ 9, A ~ Z, a ~ are also supported: #  % * + , : = ? @ [] ^	~ z and the following speci _{}~.	al characters					
Example:							
auto_provision.aes_key_16.com = 012345678	9abcdef						
Web User Interface:							
Settings->Auto Provision->Common AES Key							
Phone User Interface:							
Menu->Advanced ->Set AES Key->Common							
auto_provision.aes_key_16.mac	16 characters	Blank					
Description:							
Configures the plaintext AES key for decrypti	ng the MAC-Oriented CFC	G file.					
The valid characters contain: 0 ~ 9, A ~ Z, a ~ are also supported: #  % * + , : = ? @ [ ] ^	~ z and the following speci _{}~.	al characters					
Example:							
auto_provision.aes_key_16.mac = 0123456789abmins							
Web User Interface:							
Settings->Auto Provision->MAC-Oriented AES Key							
Phone User Interface:	Phone User Interface:						
Menu-> Advanced ->Set AES Key->MAC-Orie	ented						

## To configure AES keys via web user interface:

- 1. Click on Settings->Auto Provision.
- 2. Enter the values in the Common AES Key and MAC-Oriented AES Key fields.

AES keys must be 16 characters and the supported characters contain: 0-9, A-Z, a-z and the following special characters are also supported: #  $\% * + , - . := ? @ [] ^_ {} .$ 

							Log Out
	Status	Network	Features	Settings	Directory	Security	
Preference	Auto Provision					NOTE	
Time&Date	PNP Active		On Off     Off     On Off			Auto Provisi	
Upgrade	Custom Option(	28~254)		0		for administra	tor.
Auto Provision	DHCP Option Va	ue	MS-UC-Client	0		You can c	lick here to get
Configuration	Server URL		tftp://10.2.5.223/y	000000000028.cfg	0	more guides.	
comgaration	User Name				0		
Dial Plan	Password		•••••		0		
Voice	Common AES Ke	у	•••••	0			
Tones	MAC-Oriented A	S Key	•••••	0			
Phone Lock	Zero Active		Enabled	• 🕜			
Phone Lock	Wait Time(0~10	Ds)	5	0			
Location	Power On		🖲 On 🔘 Off 🌘				
EXP Module	Repeatedly		🔘 On 🖲 Off 🧉				
ВТоЕ	Interval(Minutes		1440	0			
	Weekly		🔍 On 🔍 Off 🧉				
	Time		00 : 00 - 00	: 00 🕜			
			Sunday Monday Tuesday				
	Day of Week		Wednesday  Thursday  Friday Saturday  Autoprovision N	ow 🕜			

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

To configure AES keys via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Set AES Key.
- 2. Enter the values in the Common and MAC-Oriented fields.

AES keys must be 16 characters and the supported characters contain: 0-9, A-Z, a-z and the following special characters are also supported: #  $\% * + , - . := ? @ [] ^ {} .$ 

3. Press the Save soft key to accept the change.

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

protected side of the network.

IP phones support protocols EAP-MD5, EAP-TLS, EAP-PEAP/MSCHAPv2, EAP-TTLS/EAP-MSCHAPv2, EAP-PEAP/GTC, EAP-TTLS/EAP-GTC and EAP-FAST for 802.1X authentication.

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

## Procedure

802.1X authentication can be configured using the configuration files or locally.

		Configure the 802.1X authentication.	
		Parameters:	
		network.802_1x.mode	
Configuration File	<y0000000000xx>.ctg</y0000000000xx>	network.802_1x.identity	
		network.802_1x.md5_password	
		network.802_1x.root_cert_url	
		network.802_1x.client_cert_url	
		Configure the 802.1X	
		authentication.	
	Web User Interface	Navigate to:	
Local		http:// <phonelpaddress>/servle</phonelpaddress>	
		t?p=network-adv&q=load	
	Phone User Interface	Configure the 802.1X authentication.	

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default		
network.802_1x.mode	0, 1, 2, 3, 4, 5, 6 or 7	0		
Description:				
Configures the 802.1x authentication r	method.			
0-Disabled				
1-EAP-MD5				
<b>2</b> -EAP-TLS				
3-EAP-PEAP/MSCHAPv2				
4-EAP-TTLS/EAP-MSCHAPv2				
5-EAP-PEAP/GTC				
6-EAP-TTLS/EAP-GTC				

Parameters	Permitted Values	Default			
7-EAP-FAST					
<b>Note:</b> If you change this parameter, the take effect.	e IP phone will reboot to make th	ne change			
Web User Interface:					
Network->Advanced->802.1x->802.1x	Mode				
Phone User Interface:					
Menu->Advanced (default password:	admin) ->Network->802.1x ->802	.1x Mode			
network.802_1x.identity String within 32 characters Blank					
Description:					
Configures the user name for 802.1x a	uthentication.				
Example:					
network.802_1x.identity = admin					
<b>Note:</b> It works only if the value of the p 2, 3, 4, 5, 6 or 7. If you change this pare change take effect.	arameter "network.802_1x.mode ameter, the IP phone will reboot	" is set to 1, to make the			
Web User Interface:					
Network->Advanced->802.1x->Identity	4				
Phone User Interface:					
Menu->Advanced (default password:	admin) ->Network->802.1x ->Ide	ntity			
network.802_1x.md5_password	String within 32 characters	Blank			
Description:					
Configures the password for 802.1x au	thentication.				
Example:					
network.802_1x.md5_password = adm	in123				
<b>Note:</b> It works only if the value of the parameter "network.802_1x.mode" is set to 1, 3, 4, 5, 6 or 7. If you change this parameter, the IP phone will reboot to make the change take effect.					
Web User Interface:					
Network->Advanced->802.1x->MD5 Password					
Phone User Interface:					
Menu->Advanced (default password:	admin) ->Network->802.1x ->MD	5 Password			
network.802_1x.root_cert_url	URL within 511 characters	Blank			

Parameters	Permitted Values Def					
Description:	Description:					
Configures the access URL of the CA a	certificate.					
Example:						
network.802_1x.root_cert_url = http://1	92.168.1.10/ca.pem					
<b>Note:</b> It works only if the value of the p 3, 4, 5, 6 or 7. The format of the certific	arameter "network.802_1x.mode ate must be *.pem, *.crt, *.cer or	e" is set to 2, *.der.				
Web User Interface:						
Network->Advanced->802.1x->CA Ce	rtificates					
Phone User Interface:						
None						
network.802_1x.client_cert_url	URL within 511 characters	Blank				
Description:						
Configures the access URL of the devi	ce certificate.					
Example:						
network.802_1x.client_cert_url = http://	/192.168.1.10/client.pem					
Note: It works only if the value of the p	arameter "network.802_1x.mode	e" is set to 2				
(EAP-TLS). The format of the certificate must be *.pem.						
Web User Interface:						
Network->Advanced->802.1x->Device Certificates						
Phone User Interface:						
None						

#### To configure the 802.1X authentication via web user interface:

- 1. Click on Network->Advanced.
- In the 802.1x block, select the desired protocol from the pull-down list of 802.1x Mode.

a) If you select EAP-MD5:

Veglink						Log Out
	Status Account	Network	Features	Settings	Directory	Security
Basic	LLDP 🕜				_	NOTE
PC Port		Active Packet Interval (1~36	Enab 600s) 60	led	<b>⊻</b>	VLAN A VLAN is a logical local area
Advanced	CDP 🕜					network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments,
		Active	Enab	led	<b>⊻</b>	given specific configurations.
	VLAN 🕜					When the network capacity is insufficient, QoS could provide priority to users by setting the
	WAN Port	Active	Disab	led	~	value.
		VID (1-4094)	1			Define the port for voice transmission.
		PHONEY	•		<u> </u>	You can click here to get more quides.
	802.1x 💡		:			
		802.1x Mode	EAP-	MD5	$\checkmark$	
		Identity	yeali	ık		
		CA Certificates			Browse	
		Device Certificates	Upla	ad [	Browse	
	Span to PC 🛛 🕜	Span to PC Port	Disab	led	<b>~</b>	

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

b) If you select EAP-TLS:

- 2) Leave the MD5 Password field blank.
- 3) In the CA Certificates field, click Browse to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.
- 4) In the **Device Certificates** field, click **Browse** to select the desired client (\*.pem or \*.cer) certificate from your local system.

						Log Out
	Status	Network	Features	Settings	Directory	Security
Basic	LLDP 🕜		-		5	NOTE
PC Port		Active Packet Interval (1~360	0s) 60	a <b>`</b>		VLAN A VLAN is a logical local area network (or LAN) that extends
Advanced	CDP 🕜	Active	Enable	d N		beyond a single traditional LAN to a group of LAN segments, given specific configurations.
		Packet Interval (1~360	0s) 60			QoS When the network capacity is
	WAN Port	Active	Disable	ed 💉	<ul> <li>Image: A start of the start of</li></ul>	priority to users by setting the value.
		VID (1-4094)	1			Local RTP Port Define the port for voice transmission.
		Priority	•		<b>~</b>	You can click here to get more guides.
	802.1x 🕜		•			
		802.1x Mode	EAP-TL	_S	<ul> <li>✓</li> </ul>	
		Identity	yealink	(		
		MD5 Password	•••••	····	Browse	
		CA Certificates	Upload	d		
		Device Certificates	Upload	d	Browse	
	Span to PC	Span to PC Port	Disable	ed 🔹	~	

5) Click Upload to upload the certificates.

c) If you select EAP-PEAP/MSCHAPv2:

- 2) Enter the password for authentication in the MD5 Password field.
- 3) In the CA Certificates field, click Browse to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

Voglink						Log Out
	Status	Network	Features	Settings	Directory	Security
Basic PC Port	LLDP 🕜	Active Packet Interval (1~36	Enabl	ed		NOTE VLAN A VLAN is a logical local area
Advanced	CDP 🕜	Active Packet Interval (1~36	Enabl	ed		network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations. QoS When the network capacity is
	VLAN 🥝 WAN Port	Active VID (1-4094)	Disab	ed		insufficient, QoS could provide priority to users by setting the value. Local RTP Port Define the port for voice transmission.
	802.1x 🕜	Priority	•		•	You can click here to get more guides.
		802.1x Mode Identity MD5 Password	EAP- yealir	PEAP/MSCHAPv2		
		CA Certificates Device Certificates	Upla	ad	Browse	
	Span to PC 🛛 💡	Span to PC Port	Disab	ed	<b>~</b>	

4) Click Upload to upload the certificate.

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

- 2) Enter the password for authentication in the MD5 Password field.
- 3) In the CA Certificates field, click Browse to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

				Log Out
YEAIINK   T46G	Status Account	Network	eatures Settings Direct	ory Security
Basic	LLDP 🕜			NOTE
PC Port		Active Packet Interval (1~3600s)	Enabled V	VLAN A VLAN is a logical local area
Advanced	CDP 🕜	Anthre	[solid b]	network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given prooffic configurations
		Active Packet Interval (1~3600s)	Enabled V	QoS When the network canacity is
	VLAN 🕜		Disabled V	insufficient, QoS could provide priority to users by setting the value.
	WAN Port	Active VID (1-4094)	1	Local RTP Port Define the port for voice
		Priority	0 ~	Transmission.
			-	more guides.
	802.1x 💔	802.1x Mode	EAP-TTLS/EAP-MSCHAPv V	
		Identity	yealink	
		MD5 Password	Browse	
		Device Certificates	Upload Browse	
	Span to PC 💡		Upload	
		Span to PC Port	Disabled V	

4) Click Upload to upload the certificate.

e) If you select EAP-PEAP/GTC:

- 2) Enter the password for authentication in the MD5 Password field.
- 3) In the CA Certificates field, click Browse to select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

				Log Out
Yealink   1466	Status	Network Feat	ures Settings Directory	Security
Basic	LLDP 🕜			NOTE
DC Dort		Active		VLAN
TO TOTE	0	Packet Interval (1~3600s)	60	A VLAN is a logical local area network (or LAN) that extends
Advanced	CDP 🕜	Antivo	Enabled V	to a group of LAN segments, given specific configurations
		Resident later val. (4, 2000a)		OoS
	VI AN	Packet Interval (1~3000s)	60	When the network capacity is insufficient. OoS could provide
	VLAN 😈	A = 10	Disabled V	priority to users by setting the value.
	WAN Port	Active		Local RTP Port
		VID (1-4094)	1	Define the port for voice transmission.
		Priority	0 ~	Veu can click here to get
		:		more guides.
	802.1x 🕜			
		802 1x Mode	FAP-PFAP/GTC	
		Identity	vealink	
		MD5 Password		
		1100 1 00010	Browse	
		CA Certificates	Upload	
		Device Certificates	Browse	
	Span to PC 🛛 🛛		Орюац	
		Span to PC Port	Disabled V	

- 4) Click Upload to upload the certificate.
- f) If you select EAP-TTLS/EAP-GTC:
  - 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 select the desired CA certificate (\*.pem, \*.crt, \*.cer or \*.der) from your local system.

					Log Out
Yealink 1466	Status	Network Feat	Settings	Directory	Security
	Account		Jures Octaings	Directory	occurry
Basic	LLDP 🕜				NOTE
busic		Active	Enabled	~	VLAN
PC Port		Packet Interval (1~3600s)	60		A VLAN is a logical local area network (or LAN) that extends
Advanced	CDP 🕜				beyond a single traditional LAN to a group of LAN segments,
		Active	Enabled	~	given specific configurations.
		Packet Interval (1~3600s)	60		QoS When the network capacity is
	VLAN 🕜				priority to users by setting the
	WAN Port	Active	Disabled	~	value.
		VID (1-4094)	1		Define the port for voice
		Priority	0	$\checkmark$	
		•			You can click here to get more guides.
	902 1v 🗿	:			
	002.1X <b>1</b>	902 1x Mode	FAD-TTI S/FAD-GTC	$\overline{}$	
		Identity	vesliek		
		MDE Dessured	yediirik		
		MDD Passworu		Browse	
		CA Certificates	Upload		
		Device Certificates		Browse	
	Span to PC 🛛 🔞		obioad		
		Span to PC Port	Disabled	~	

4) Click Upload to upload the certificate.

g) If you select EAP-FAST:

- 1) Enter the user name for authentication in the Identity field.
- 2) Enter the password for authentication in the MD5 Password field.

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

				Log Out
	Status	Network Fea	tures Settings Directory	Security
Basic	LLDP 🕜			NOTE
PC Port		Active Packet Interval (1~3600s)	Enabled V	VLAN A VLAN is a logical local area
Advanced	CDP 🕜	Active	Enabled	to a group of LAN segments, given specific configurations.
		Packet Interval (1~3600s)	60	QoS When the network capacity is
	VLAN 🕜 WAN Port	Active	Disabled V	priority to users by setting the value.
		VID (1-4094)	1	Local RTP Port Define the port for voice transmission.
		Priority	•	You can click here to get more guides.
	802.1x 🕜			
		802.1x Mode	EAP-FAST	
		Identity	yealink	
		MD5 Password		
		CA Certificates	Upload Browse	
		Device Certificates	Browse	
	Span to PC 🛛 🕜	Span to PC Port	Disabled	

4) Click Upload to upload the certificate.

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 IP phone.

#### To configure the 802.1X authentication via phone user interface:

- 1. Press Menu->Advanced (default password: admin) ->Network->802.1x.
- Press (•)or (•), or the Switch soft key to select the desired value from the 802.1x
   Mode field.

#### 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.

#### c) If you select EAP-PEAP/MSCHAPv2:

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

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

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

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

e) If you select EAP-PEAP/GTC:

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

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

f) If you select EAP-TTLS/EAP-GTC:

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

- 2) Enter the password for authentication in the MD5 Password field.
- g) If you select EAP-FAST:

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

- 2) Enter the password for authentication in the MD5 Password field.
- 3. Click Save to accept the change.

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

# Troubleshooting

This chapter provides an administrator with general information for troubleshooting some common problems that he (or she) may encounter while using IP phones.

# **Troubleshooting Methods**

IP phones can provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help an administrator more easily find the system problem and fix it.

The following are helpful for better understanding and resolving the working status of the IP phone.

- Viewing Log Files
- Capturing Packets
- Enabling Watch Dog Feature
- Getting Information from Status Indicators
- Analyzing Configuration File

## **Viewing Log Files**

If your IP phone encounters some problems, commonly the log files are needed. You can export the log files to a local system, a syslog server or the Skype for Business Server. You can also specify the severity level of the log to be reported to a log file. The default system log level is 3.

In the configuration files, you can use the following parameters to configure system log settings:

- syslog.log\_level -- Specify the system log level. The following lists the log level of events you can log:
  - 0: system is unusable
  - 1: action must be taken immediately
  - 2: critical condition
  - 3: error conditions
  - 4: warning conditions
  - 5: normal but significant condition
  - 6: informational

- **syslog.mode** Specify the system log to be exported to the syslog server or local system.
- **syslog.server** -- Specify the IP address or domain name of the syslog server to which the log will be exported.

## Configuring the Severity Level of the Log

## Procedure

Severity level can be configured using the configuration files or locally.

	<y000000000xx>.cfg</y000000000xx>	Configure the severity level of the logs to be reported to a log file.
Configuration File		Parameters:
		syslog.log_level
	Web User Interface	Configure the severity level of the logs to be reported to a log file.
Local		Navigate to:
		http:// <phonelpaddress>/servlet?m</phonelpaddress>
		=mod_data&p=settings-config&q=l
		oad

## **Details of Configuration Parameters:**

Parameters	Permitted Values	Default		
syslog.log_level	Integer from 0 to 6	3		
Description:				
Configures the detail level of syslog	information to be exp	orted.		
0-system is unusable				
1-action must be taken immediate	ly			
2-critical condition				
3-error conditions				
4-warning conditions				
5-normal but significant condition				
<b>6</b> -informational				
<b>Note</b> : If you change this parameter, the IP phone will reboot to make the change take effect.				
Web User Interface:				

Parameters	Permitted Values	Default	
Settings->Configuration->System Log Level			
Phone User Interface:			
None			

To configure the level of the system log via web user interface:

- 1. Click on Settings->Configuration.
- 2. Select the desired level from the pull-down list of System Log Level.

Vealink			Log Out
	Status Account Network	Features Settings Directory	Security
Preference	Export or Import Configuration	Browse No file selected.	NOTE
Time&Date Upgrade	Support Coll Log	Event 0	Configuration The configuration parameters for administrator.
Auto Provision	Export Call Log	Export	You can click here to get more guides.
Configuration	Pcap Feature	Start Stop Export 🧭	
Dial Plan	Export System Log	Local      Server	
Voice		Export	
Tones	System Log Level	0 • • •	
Phone Lock	Confirm	Cancel	

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

The system log level is set as 6, the informational level.

**Note** Informational level may make some sensitive information accessible (e.g., password dial number), we recommend that you reset the system log level to 3 after providing the syslog file.

## Exporting the Log File to the Local System

#### Procedure

Log setting can be configured using the configuration files or locally.

		Configure the syslog mode.
Configuration File	<y000000000xx>.cfg</y000000000xx>	Parameters:
		syslog.mode
	Web User Interface	Configure the syslog mode.
Local		Navigate to:
		http:// <phonelpaddress>/servlet?m</phonelpaddress>
		=mod_data&p=settings-config&q=l

	oad

### **Details of Configuration Parameters:**

Parameters	Permitted Values	Default	
syslog.mode	0 or 1	0	
Description:			
Configures the IP phone to export lo	g files to the local systen	n or a syslog server.	
<b>0</b> -Local			
1-Server			
<b>Note:</b> If you change this parameter, the IP phone will reboot to make the change take effect.			
Web User Interface:			
Settings->Configuration->Export System Log			
Phone User Interface:			
None			

#### To export a log file to the local system via web user interface:

- 1. Click on Settings->Configuration.
- 2. Mark the Local radio box in the Export System Log field.

A dialog box pops up to prompt "Warning: Some settings you changed take effect when you restart your machine! Do you want to reboot now?". The configuration will take effect after a reboot.

- 3. Click **OK** to reboot the IP phone.
- 4. Reproduce the issue (e.g., account registration).

5. Click **Export** to open file download window, and then save the file to your local system.

Veglink			Log Out
	Status Account Networ	k Features Settings Directory	Security
Preference	Export or Import Configuration	Browse No file selected.	NOTE
Time&Date		Import Export	Configuration
Upgrade	Event Cilling		for administrator.
Auto Provision	Export Call Log	Export	You can click here to get more guides.
Configuration	Pcap Feature	Start Stop Export ?	
Dial Plan	Export System Log		
Voice		Export	
Tones	System Log Level	3 🗸 🖓	
Phone Lock	Confirm	Cancel	
Location			
EXP Module			
ВТОЕ			

A log file named **syslog.tar** is successfully exported to your local system.

#### To view the log file on your local system:

- 1. Extract the combined log files to your local system.
- 2. Open the folder you extracted to and identify the files you will view.

The following figure shows a portion of a <mac>.log (e.g., 0015659188F2.log) - an account registration:

Sep 24 00:53:35 sua [509]: DLG <6+info > [000] REGISTER sip:yealinkuc.com SIP/2.0^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Via: SIP/2.0/TLS 10.10.20.39:5061;rport;branch=z9hG4bK1839199345^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] From: "2227" <sip:2227@yealinkuc.com>;tag=2513018937;epid=00156574b16e00^M</sip:2227@yealinkuc.com>
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] To: "2227" <sip:2227@yealinkuc.com>^M</sip:2227@yealinkuc.com>
Sep 24/ DLG <6+info > [000] Call-ID: 0 2880835069^M
sep 2/ The "6+info" means you DLG <6+info > [000] CSeq: 5 REGISTER^M
Sep 2 got the correct systog. DLG <6+info > [000] Contact: <sip:2227@10.10.20.39:5061;transport=tls;line=b7052276b8e4e07>;+sip.instance="<urn:uuid:8c8c93be-e22a-539b-8ac9< td=""></urn:uuid:8c8c93be-e22a-539b-8ac9<></sip:2227@10.10.20.39:5061;transport=tls;line=b7052276b8e4e07>
Sep 24 DLG <6+info > [000] Authorization: TLS-DSK realm="SIP Communications Service", response=5E3115A40F43E8311D598865A69BBA1DEA218065, opaque="6
Sep 24 00:53:35 sua 1: DLG <6+info > [000] Allow: INVITE, INFO, FRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, FUBLISH, UPDATE, MESSAGE^M
Sep 24 00:53:35 sua [509] DLG <6+info > [000] Max-Forwards: 70^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] User-Agent: UCCAPI/15.0.4707.1000 OC/15.0.4707.1000 (Skype for Business)^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Ms-keep-alive: UAC:hop-hop=yes^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Allow-Events: talk,hold,conference,refer,check-sync^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Supported: timer^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Ms-subnet: 10.10.20.0°M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Ms-device-info: MAC=00:15:65:74:b1:6e; vendor=UCCAPI/15.0.4707.1000 OC/15.0.4707.1000 (Skype for Business); version=44.8
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Event: registration^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Supported: path, gruu-10, adhoclist, martc-event-categories^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Supported: ms-userservices-state-notification <sup>*</sup> M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Supported: ms-cluster-failover^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Supported: ms-bypass^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] Expires: 0^M
Sep 24 00:53:35 sua [509]: DLG <6+1NEO > [000] Content-Length: 0^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] ^M
Sep 24 00:53:35 sua [509]: DLG <6+info > [000]
Sep 24 00:53:35 sua [509]: NET <5+notice> [000] ===>>>> TLS socket 192.168.6.53:5061: send 1302 bytes
Sep 24 00:53:35 sua [509]: FSM <6+info > [000] free transaction ressource 6 0_2880835069
Sep 24 00:53:35 sua [509]: FSM <6+info > [255] free nict ressource
Sep 24 00:53:35 sua [509]: NET <5+notice> [255] <<<<=== TLS socket 192.168.6.53:5061: read 934 bytes
Sep 24 00:53:35 sua [509]: SIP <6+info > [SIP] match line:name:2227 host:yealinkuc.com
Sep 24 00:53:35 sua [509]: DLG <5+notice> [000] Message recv: (from src=192.168.6.53:5061 len=934)
Sep 24 00:53:35 sua [509]: DLG <6+info > [000]
Sep 24 00:53:35 sua [509]: DLG <6+info > [000] SIP/2.0 200 OK^M

## Exporting the Log File to a Syslog Server

## Procedure

Log setting can be configured using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Configure the syslog mode.
		Parameters:

		syslog.mode
		Configure the IP address or domain
		name of the syslog server where to
		export the log files.
		Parameters:
		syslog.server
	Web User Interface	Configure the syslog mode.
		Configure the IP address or domain
		name of the syslog server where to
local		export the log files.
		Navigate to:
		http:// <phonelpaddress>/servlet?m</phonelpaddress>
		=mod_data&p=settings-config&q=l
		oad

## Details of Configuration Parameters:

Parameters	Permitted Values	Default		
syslog.mode	0, 1 or 2	0		
Description:				
Configures the IP phone to export lo	g files to the local system	n ir a syslog server.		
<b>0</b> -Local				
1-Server				
<b>Note:</b> If you change this parameter take effect.	r, the IP phone will rebo	ot to make the change		
Web User Interface:				
Settings->Configuration->Export Sys	tem Log			
Phone User Interface:				
None				
syslog.server Blank Blank				
Description:				
Configures the IP address or domain name of the syslog server when exporting log				
to the syslog server.				
Example:				
syslog.server = 192.168.1.100				
Note: It works only if the value of the parameter "syslog.mode" is set to 1 (Server). If				

Parameters	Permitted Values	Default
you change this parameter, the IP phone will reboot to make the change take		
effect.		
Web User Interface:		
Settings->Configuration->Server Name		
Phone User Interface:		
None		

To configure the IP phone to export the system log to a syslog server via web user interface:

- 1. Click on Settings->Configuration.
- 2. Mark the Server radio box in the Export System Log field.
- Enter the IP address or domain name of the syslog server in the Server Name field.
   For example, the IP address of your syslog server is 192.168.1.100.

		Log Out
YEAIINK   T46G	Status Account Network Features Settings Directory	Security
Preference	Export or Import Configuration Browse No file selected.	NOTE
Time&Date	Import Export	Configuration The configuration parameters
Upgrade	Export Calling	for administrator.
Auto Provision		You can click here to get more guides.
Configuration	Pcap Feature Start Stop Export Q	
Dial Plan	Export System Log 💿 Local 💿 Server 👔	
Voice	Server Name 192.168.1.100	
Tones	System Log Level 3 🔹 🕜	
Phone Lock	Confirm	
Location		
EXP Module		
ВТОЕ		

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

A dialog box pops up to prompt "Do you want to restart your machine?". The configuration will take effect after a reboot.

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

The system log will be exported successfully to the desired syslog server (192.168.1.100) after a reboot.

#### To view the log file on your syslog server:

You can view the system log file in the desired folder on the syslog server. The location of the folder may differ from the syslog server. For more information, refer to the network resources.

The following figure shows a portion of the system log:

-	
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] Via: SIP/2.0/TLS 192.168.6.53:5061;branch=z9hG4bK0CAB2A67.2404489A7E5A4DFD;branched=FALSE
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] Authentication-Info: TLS-DSK gop="auth", opaque="CC727F09", srand="FCC812C9", snum="11", rspauth="fa155b7ab469f09d47db1e97
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] Max-Forwards: 70
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] To: <sip:2227@yealinkuc.com>;tag=468936962;epid=00156574b16e00</sip:2227@yealinkuc.com>
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] Content-Length: 6631
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] From: <sip:2227@yealinkuc.com>;tag=9E3A0080</sip:2227@yealinkuc.com>
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] Call-ID: 0 4102263140
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] CSeq: 2 BENOTIFY
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] Require: eventlist
Oct 19 09:00:45 sua [554]: DLG <6+info	> [000] Content-Type: multipart/related; type="application/rlmi+xml";start=resourceList; boundary=c79b776193274c4eabc0314ff114c5d7
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] Event: presence
Oct 19 09:00:45 sua [554]: DLG <6+info	· [000]
Oct 19 09:00:45 sua [554]: FSM <6+info	<ul> <li>[-01] allocating transaction ressource 14 0 4102263140</li> </ul>
Oct 19 09:00:45 sua [554]: FSM <6+info	[-01] allocating NIST context
Oct 19 09:00:45 sua [554]: FSM <6+info	[000] missing a contact in invite!
Oct 19 09:00:45 sua [554]: SUA <6+info	[000] ****eCore event: (0x0043)ECORE_SUBSCRIPTION_NOTIFY ****
Oct 19 09:00:45 Log [597]: IDUI<6+info	> PHONE KEY HEADSET CTRL strLineIcon(Lync Available.dob) eLineState(2).
Oct 19 09:00:45 sua [554]: SUB <5+notice	[000] notify receive sub type=12
Oct 19 09:00:45 sua [554]: APP <6+info	SIP] <ipc_ntfp>:msg=0x00040211(262673), wparam=0, lparam=2, size=120</ipc_ntfp>
Oct 19 09:00:45 sua [554]: DLG <6+info	[000] cb nict kill transaction (id=14)
Oct 19 09:00:45 Log [597]: IDUI<6+info	<ul> <li>Update m pIconList. ylVecStatusList size(0).</li> </ul>
Oct 19 09:00:45 Log [597]: IDUI<6+info	UpdateData :: UpdateData iRangeMask(4).
Oct 19 09:00:45 Log [597]: IDUI<6+info	Account is available[1], Lock is Loaded[1]
Oct 19 09:00:45 Log [597]: IDUI<6+info	UpdateSoftkey. eState(0).
Oct 19 09:00:45 Log [597]: UIMG<6+info	CMainWnd::UpdateWnd() begin draw
Oct 19 09:00:45 Log [597]: IDUI<6+info	Show :: UpdateData(IRT_ALL).
Oct 19 09:00:45 Log [597]: IDUI<6+info	UpdateData :: UpdateData iRangeMask(255).
Oct 19 09:00:45 Log [597]: IDUI<6+info	Account is available[1], Lock is Loaded[1]
Oct 19 09:00:45 Log [597]: IDUI<6+info	<ul> <li>UpdateSoftkey. eState(0).</li> </ul>
Oct 19 09:00:45 Log [597]: IDUI<6+info	StateItem.m nId(0). StateItem.m strHint(), strNotifyText(), strNotifyIcon().

## Exporting the Log File to the Skype for Business Server

You can upload system log to the Skype for Business Server via phone user interface only.

When performing a log upload, The HTTP POST sent from IP phone has following Headers:

UCDevice\_Type: "with a value of "3PIP".

UCDevice\_ID: containing a unique string identifying the phone.

The UCDevice\_ID contains at minimum the following entries:

- 1. VendorName-phone manufacturer name
- 2. DeviceModel-phone model
- 3. MAC address
- 4. Firmware version

#### Sample:

UCDevice\_ID: Yealink\_SIP-T46G\_28.8.0.1\_00156574B1D6E\r\n UCDevice\_Type: 3PIP\r\n

#### To export a log file to the Skype for Business Server via phone user interface:

1. Press Menu->Basic ->Log Upload.

A dialog box pops up to prompt "Log Upload Success! ".

The log file can be found on the Skype for Business Server

at %ocsfilestore%\%domain%-WebServices-1\DeviceUpdateLogs\Cient.

## **Capturing Packets**

You can capture packet in two ways: capturing the packets via web user interface or using the Ethernet software. You can analyze the packet captured for troubleshooting purpose.
## Capturing the Packets via Web User Interface

#### To capture packets via web user interface:

- 1. Click on Settings->Configuration.
- 2. Click Start to start capturing signal traffic.
- 3. Reproduce the issue to get stack traces.
- 4. Click Stop to stop capturing.
- 5. Click **Export** to open the file download window, and then save the file to your local system.

No orline la l				Log Out
<b>YEAIINK</b>   T46G	Status Account	Network Features	Settings Directory	/ Security
Preference	Export or Import Configu	uration Browse No file	e selected.	NOTE
Time&Date		Import	Export	Configuration
Upgrade				for administrator.
Auto Provision	Export Call Log	Export	] (?)	You can click here to get more guides.
Configuration	Pcap Feature	Start	top Export 🕜	
Dial Plan	Export System Log	Eccal Serve	0	
Voice		Export	]	
Tones	System Log Level	3	• 🕜	
Phone Lock	Confirm		Cancel	
Location				
EXP Module				
ВТОЕ				

### Capture the Packets Using the Ethernet Software

#### Receiving data packets from the HUB

Connect the Internet port of the IP phone and the PC to the same HUB, and then use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

#### Receiving data packets from PC port

Connect the Internet port of the IP phone to the Internet and the PC port of the IP phone to a PC. Before capturing the signal traffic, make sure the data packets can be received from the WAN (Internet) port to the PC (LAN) port.

### Procedure

Span to PC Port can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Port. Parameter:
		Configure span to PC

		network.span_to_pc_port
		Configure span to PC Port.
local	Web User Interface	Navigate to:
		http:// <phonelpaddress s<="" td=""></phonelpaddress>
		ervlet?p=network-adv&q
		=load

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default		
network.span_to_pc_port	0 or 1	0		
Description:				
Enables or disables the IP phone to (Internet) port to the PC (LAN) port	o span data packets received	I from the WAN		
0-Disabled				
1-Enabled				
If it is set to 1 (Enabled), all data packets from WAN port can be received by PC port.				
<b>Note</b> : If you change this parameter, the IP phone will reboot to make the change take effect.				
Web User Interface:				
Network->Advanced->Span to PC->Span to PC Port				
Phone User Interface:				
None				

### To enable span to pc port via web user interface:

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

alink							
	Status	Account	Network	Features	Settings	Directory	Security
		op 🕜					NOTE
asic			Active	Enabl	ed	~	
C Port			Packet Interval (1~360	00s) 60			A VLAN is a logical local a
dvanced	CDI	P 🕜					beyond a single traditiona
			Active	Enabl	ed	~	given specific configuratio
			Packet Interval (1~36	00s) 60			QoS When the network canaci
	VL/	AN 🕜					insufficient, QoS could pro
	W	AN Port	Active	Disab	ed	$\sim$	value.
			VID (1-4094)	1			Local RTP Port Define the port for voice
							transmission.
				:			You can click here to more guides.
	802	2.1x 🕜					
			802.1x Mode	Disab	ed	~	
			Identity				
			MD5 Password	0 0 0 0			
			CA Certificates			Browser	
				Uploa	d		
			Device Certificates	Uploa	d		
	Spa	an to PC 🕜					
			Span to PC Port	Enabl	ed	-	
	ICM	IPv6 Status	0				
			Active	Enabl	ed	•	

2. Select Enabled from the pull-down list of Span to PC Port.

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 IP phone.

Then you can use Sniffer, Ethereal or Wireshark software to capture the signal traffic.

## **Enabling Watch Dog Feature**

The IP phone provides a troubleshooting feature called "Watch Dog", which helps you monitor the IP phone status and provides the ability to get stack traces from the last time the IP phone failed. If Watch Dog feature is enabled, the IP phone will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via web user interface.

### Procedure

Watch dog can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg</y0000000000xx>	Configure watch dog feature.
		Parameter: watch_dog.enable

		Configure watch dog feature.
Local	Web User Interface	Navigate to:
		http:// <phonelpaddress></phonelpaddress>
		/servlet?p=settings-prefer
		ence&q=load

## Details of the Configuration Parameter:

Parameter	Permitted Values	Default		
watch_dog.enable	0 or 1	1		
Description:				
Enables or disables Watch Dog fec	iture.			
0-Disabled	0-Disabled			
1-Enabled				
If it is set to 1 (Enabled), the IP phor	ne will reboot automatically w	when the system is		
broken down.				
Web User Interface:				
Settings->Preference->Watch Dog				
Phone User Interface:				
None				

To configure watch dog feature via web user interface:

- 1. Click on Settings->Preference.
- 2. Select the desired value from the pull-down list of Watch Dog.

			Log Out
	Status Account Network	Features Settings Directory	Security
Preference	Language	English (English)	NOTE
Time&Date	Live Dialpad Backlight Inactive Level	Disabled   Cov   Cov   Cov   Cov   Cov   Cov   Cov  Cov	Preference Settings The preference settings for
Upgrade	Backlight Active Level	8 🗸 🖉	administrator.
Auto Provision	Watch Dog	Enabled 👻 🕜	You can click here to get more guides.
Configuration	Ring Type	Ring1.wav 🗸 🕜	, i i i i i i i i i i i i i i i i i i i
Dial Plan	Upload Ringtone	Browse No file selected.	
Voice	Confirm	Cancel	
Tones			

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

# **Getting Information from Status Indicators**

Status indicators may consist of the power LED, MESSAGE key LED, line key indicator, headset key indicator and the on-screen icon.

The following shows two examples of obtaining the IP phone information from status indicators on SIP-T46G IP phones:

- If a LINK failure of the IP phone is detected, a prompting message "Network unavailable" will appear on the LCD screen.
- If a voice mail is received, the MESSAGE key LED illuminates.

For more information on the icons, refer to Reading Icons on page 32.

# Analyzing Configuration File

Wrong configurations may have an impact on your phone use. You can export BIN file to check the current configuration of the IP phone and troubleshoot if necessary. You can also import configuration files for a quick and easy configuration. The BIN file is an encrypted file. For more information on BIN file, contact your Yealink reseller.

### Procedure

Configuration changes can be performed using the configuration files or locally.

Configuration File	<y000000000xx>.cfg</y000000000xx>	Specify the access URL for the custom configuration files. <b>Parameter:</b> configuration.url
Local	Web User Interface	Export or import the custom configuration files. <b>Navigate to</b> : http:// <phonelpaddress>/servlet 2p=settings-config&amp;g=logd</phonelpaddress>

Details of the Configuration Parameter:

Parameter	Permitted Values	Default	
configuration.url	URL within 511 characters	Blank	
Description:			
Configures the access URL for the custom configuration files.			
<b>Note</b> : The file format of custom configuration file must be *.bin.			

Parameter	Permitted Values	Default		
Web User Interface:				
Settings->Configuration->Export or Import Configuration				
Phone User Interface:				
None				

#### To export configuration files via web user interface:

- 1. Click on Settings->Configuration.
- 2. In the Export or Import Configuration block, click Export to open the file download window, and then save the file to your local system.

Voalink			Log Out
	Status Account Network	Features Settings Directory	Security
Preference	Export or Import Configuration	Browse No file selected.	NOTE
Time&Date		Import Export	Configuration
Upgrade			for administrator.
Auto Provision	Export Call Log	Export	You can click here to get more guides.
Configuration	Pcap Feature	Start Stop Export ?	
Dial Plan	Export System Log	Local      Server     O     Server     Server	
Voice		Export	
Tones	System Log Level	3 🗸 🗸	
Phone Lock	Confirm	Cancel	
Location			
EXP Module			
ВТОЕ			

To import configuration file via web user interface:

1. Click on Settings->Configuration.

2. In the Export or Import Configuration block, click Browse to locate a configuration file from your local system.

Voglink			Log Out
TECHINK   T46G	Status Account Network	Features Settings Directory	Security
Preference	Export or Import Configuration	Browse No file selected.	NOTE
Time&Date		Import Export	Configuration
Upgrade	Function Line	Finat	for administrator.
Auto Provision	Export Call Log	Export	You can click here to get more guides.
Configuration	Pcap Feature	Start Stop Export ?	
Dial Plan	Export System Log	🖲 Local 💿 Server 🕜	
Voice		Export	
Tones	System Log Level	3 🗸 🔇	
Phone Lock	Confirm	Cancel	
Location			
EXP Module			
ВТОЕ			

3. Click Import to import the configuration file.

# **Troubleshooting Solutions**

This section describes solutions to common issues that may occur while using the IP phone. Upon encountering a scenario not listed in this section, contact your Yealink reseller for further support.

## **IP Address Issues**

### Why doesn't the IP phone get an IP address?

Do one of the following:

- Ensure that the Ethernet cable is plugged into the Internet port on the IP phone and the Ethernet cable is not loose.
- Ensure that the Ethernet cable is not damaged.
- Ensure that the IP address and related network parameters are set correctly.
- Ensure that your network switch or hub is operational.

### How to solve the IP conflict problem?

Do one of the following:

• Reset another available IP address for the IP phone.

Check network configuration via phone user interface at the path
 Menu->Advanced->Network->WAN Port->IPv4 (or IPv6). If the Static IP is selected, select DHCP instead.

## Is there a specific format in configuring IPv6 on Yealink IP phones?

#### Scenario 1:

If the IP phone obtains the IPv6 address, the format of the URL to access the web user interface is "[IPv6 address]" or "http(s)://[IPv6 address]". For example, if the IPv6 address of your phone is "fe80::204:13ff:fe30:10e", you can enter the URL (e.g., "[fe80::204:13ff:fe30:10e]" or "http(s)://[fe80::204:13ff:fe30:10e])" in the address bar of a web browser on your PC to access the web user interface.

### Scenario 2:

Yealink IP phones support using FTP, TFTP, HTTP and HTTPS protocols to download configuration files or resource files. You can use one of these protocols for provisioning. When provisioning your IP phone obtaining an IPv6 address, the provisioning server should support IPv6 and the format of the access URL of the provisioning server can be "*tftp://[IPv6 address or domain name]*". For example, if the provisioning server address is "2001:250:1801::1", the access URL of the provisioning server can be "*tftp://[2001:250:1801::1]/*". For more information on provisioning, refer to Yealink\_Microsoft\_Skype\_for\_Business\_Edition\_IP\_Phones\_Auto\_Provisioning\_Guide.

## Audio Issues

### How to increase or decrease the volume?

Press the volume key to increase or decrease the ringer volume when the IP phone is idle or ringing, or to adjust the volume of engaged audio device (handset, speakerphone or headset) when there is an active call in progress.

## Why do I get poor sound quality during a call?

If you have poor sound quality/acoustics like intermittent voice, low volume, echo or other noises, the possible reasons could be:

- Users are seated too far out of recommended microphone range and sound faint, or are seated too close to sensitive microphones and cause echo.
- Intermittent voice is mainly caused by packet loss, due to network congestion, and jitter, due to message recombination of transmission or receiving equipment (e.g., timeout handling, retransmission mechanism, buffer under run).
- Noisy equipment, such as a PC or a fan, may cause voice interference. Turn off

any noisy equipment.

• Line issues can also cause this problem; disconnect the old line and redial the call to ensure another line may provide better connection.

### Why is there no sound when the other party picks up the call?

If the caller and receiver cannot hear anything - there is no sound at all when the other party picks up the call, the possible reason could be: the IP phone cannot send the real-time transport protocol (RTP) streams, in which audio data is transmitted, to the connected call.

Try to disable the 180 ring workaround feature. For more information, refer to 180 Ring Workaround on page 174.

### Why does the IP phone play the local ringback tone instead of media when

### placing a long distance number without plus 0?

Ensure that the 180 ring workaround feature is disabled. For more information, refer to 180 Ring Workaround on page 174.

# **Upgrading Issues**

### Why doesn't the IP phone upgrade firmware successfully?

Do one of the following:

- Ensure that the target firmware is not the same as the current firmware.
- Ensure that the target firmware is applicable to the IP phone model.
- Ensure that the current or the target firmware is not protected.
- Ensure that the power is on and the network is available in the process of upgrading.
- Ensure that the web browser is not closed or refreshed when upgrading firmware via web user interface.
- Ensure that the target firmware on the Skype for Business Server is available.

## How can I verify the firmware generation and version of the IP phone?

Press the **OK** key when the IP phone is idle to check the firmware version. For example: 28.8.0.21.



	ltem	Description				
		A fixed number for each IP phone model.				
		• 35: SIP-T48G				
1	28	• 28: SIP-T46G				
		• 29: SIP-T42G/ SIP-T41P				
		• 54: SIP-T40P				
		Firmware generation.				
2	8	Note: The larger it is, the newer the firmware				
		generation is.				
3	0	A fixed number.				
		Firmware version.				
4	21	Note: With the same firmware generation,				
	Ζ1	the larger it is, the newer the firmware version				
		is.				

## Why doesn't the IP phone update the configuration?

Do one of the following:

- Ensure that the configuration is set correctly.
- Reboot the IP phone. Some configurations require a reboot to take effect.
- Ensure that the configuration is applicable to the IP phone model.
- The configuration may depend on support from a server.

## **Provisioning Issues**

### What is auto provisioning?

Auto provisioning refers to the update of IP phones, including update on configuration parameters, local phone book, firmware and so on. You can use auto provisioning on a single phone, but it makes more sense in mass deployment.

## **Resetting Issues**

Generally, some common issues may occur while using the IP phone. You can reset your phone to factory configurations after you have tried all troubleshooting suggestions but do not solve the problem. Resetting the phone to factory configurations clears the flash parameters, removes log files, user data, and cached data, and resets the administrator password to admin. All custom settings will be overwritten after resetting.

You can reset the IP phone to default factory configurations. The default factory configurations are the settings that reside on the IP phone after it has left the factory. For more information, refer to How to reset the IP phone to default factory configurations? on page 335.

### How to reset the IP phone to default factory configurations?

#### To reset the IP phone via web user interface:

- 1. Click on Settings->Upgrade.
- 2. Click Reset to Factory Setting in the Reset to Factory Setting field.

The web user interface prompts the message "Do you want to reset to factory?".

Vaglink			Log Out
	Status Account Network	Features Settings Director	y Security
Preference			NOTE
Time&Date	Version 🕜 Firmware Version	28.8.0.21	Reset to Factory Setting Reset all the settings of the
Upgrade	Hardware Version	28.1.0.128.0.0.0	phone to default configurations.
Auto Provision	Reset to Factory Setting Reboot	Reset to Factory Setting	Select and Upgrade Firmware Select and upgrade the file from the hard disk or network.
Configuration	Select and Upgrade Firmware 🕜	Browse No file selected	You can click here to get
Dial Plan	•	Upgrade	more guides.
Voice			

3. Click **OK** to confirm the resetting.

The IP phone will be reset to factory successfully after startup.

Note Reset of your phone may take a few minutes. Do not power off until the IP phone starts up successfully.

# **Rebooting Issues**

## How to reboot the IP phone via web/phone user interface?

You can reboot your IP phone via web/phone user interface.

#### To reboot the phone via phone user interface:

- 1. Press Menu->Advanced (default password: admin).
- 2. Press ( $\bullet$ ) or ( $\bullet$ ) to scroll to **Reboot**, and then press the **Enter** soft key.
- 3. Press Reboot soft key.

The LCD screen prompts "Reboot the phone?".

4. Press the **OK** soft key to reboot the phone.

The phone begins rebooting. Any reboot of the IP phone may take a few minutes.

#### To reboot the IP phone via web user interface:

- 1. Click on Settings->Upgrade.
- 2. Click **Reboot** to reboot the IP phone.

Veglink			Log Out
	Status Account Network	Features Settings Directory	Security
Preference Time&Date Upgrade Auto Provision Configuration Dial Plan Voice	Version  () Firmware Version Hardware Version Reset to Factory Setting Reboot Select and Upgrade Firmware ()	28.8.0.21 28.1.0.128.0.0.0 Reset to Factory Setting Reboot	NOTE Reset to Factory Setting Reset all the settings of the phone to default configurations. Select and Upgrade the fifter the hard disk or network. The vacuum of the hard disk or network. The vacuum of the hard disk or network.

The phone begins rebooting. Any reboot of the IP phone may take a few minutes.

# Protocols and Ports Issues

# What communication protocols and ports do Yealink IP phones support?

Source Device	Source IP	Source Port	Destination Device	Destination IP	Destination Port (Listening port)	Protocol	Description of destination port
IP phones IP phones of IP phones		2~65535	IP phone or voice gateway	IP address of IP phone or voice gateway	Determined by destination device.	UDP	RTP protocol port, it is used to send or receive audio stream.
		1024~65535	SIP Server	IP address of SIP server	Determined by destination device.	UDP/TCP	SIP protocol port, it is used for signaling interaction with SIP server.
	IP address	1024~65535	File server	IP address of file server	Determined by destination device.	TCP	HTTP protocol port, it is used to download file.
	of IP phones	of IP phones 1024~65535	АА	IP address of AA	Determined by destination device.	TCP	HTTP protocol port, it is used for AA communication.
		68	DHCP Server	IP address of DHCP server	67	UDP	DHCP protocol port, it is used to obtain IP address from DHCP server.
		1024~65535	NTP Server	IP address of NTP server	123	UDP	NTP protocol port, it is used to synchronize time from NTP time server.

Source	Source	Source Port	Destination	Destingtion IP	Destination Port	Brotocol	Description of destingtion part
Device	IP	source Pon	Device	Destination IP	(Listening port)	PIOIOCOI	Description of destination por
							Syslog protocol port, it is used
		1024~65535	Systoa Server	IP address of	514		for IP phones to upload
		1021 00000		syslog server	011	0D1	syslog information to syslog
							server.
	IP				1~65535	TCP	HTTP port (default value: 80)
PC	address				1~45535	TCP	HTTP port (default value: 113)
	of PC				1-00000		
	IP						SIP protocol port it is used for
	address				1024~45534		signaling interaction with SIP
311 361461	of SIP	Determined			1024-05554		server
	Server	by the	ID in h a in a a	nes IP address of IP phones			
	IP	destination	ir priories				
	address	device.					
IP phone	of IP						RTP protocol port, it is used by
of voice	phone				2~65535	UDP	destination device to send or
gateway	or voice						receive audio stream.
	gatewa						
	У						

# **Display Issues**

## Why is the LCD screen blank?

Do one of the following:

- Ensure that the IP phone is properly plugged into a functional AC outlet.
- Ensure that the IP phone is plugged into a socket controlled by a switch that is on.
- If the IP phone is plugged into a power strip, try plugging it directly into a wall outlet.
- If your phone is PoE powered, ensure that you are using a PoE-compliant switch or hub.

## **Time and Date Issues**

## Why doesn't the IP phone display time and date correctly?

Check if the IP phone is configured to obtain the time and date from the NTP server automatically. If your phone is unable to access the NTP server, configure the time and date manually.

# System Log Issues

### Why cannot I export the system log to a syslog server?

Do one of the following:

- Ensure that the syslog server supports saving the syslog files exported from IP phone.
- Ensure that you have configured the syslog server address correctly via web user interface on your IP phone.
- Reboot the IP phone. The configurations require a reboot to take effect.

# **Password Issues**

## How to restore the administrator password?

Factory reset can restore the original password. All custom settings will be overwritten after reset.

# **Other Issues**

### How do I find the basic information of the IP phone?

Press **Menu-> Status** when the IP phone is idle to check the basic information (e.g., IP address, MAC address and firmware version).

## What is the difference between enabling and disabling the RFC 2543 Hold

### feature?

Capturing packets after you enable the RFC 2543 Hold feature. SDP media direction attributes (such as a=sendonly) per RFC 2543 is used in the INVITE message when placing a call on hold.

Eile	Edit View Go	Capture Analyze	Statistics Telephony Tools	Internals Help	lp	
	<b>M                                    </b>	🖻 🖬 🗶 🏻	≜∣©、⇔⇔⊙⊽:		IQ, Q, Q, 🗹   👹 🗹 🍕 %   🕅	
Filte	r: sip			Expression	n Clear Apply	
No.	Time	Source	Destination	Protocol	Length Info	
	54 2.018991	10.3.20.14	10.3.5.199	SIP/SDP	904 Request: INVITE sip:1021@10.3.5.199:5060, with session description	
	55 2.021424	10.3.5.199	10.3.20.14	SIP	314 status: 100 Trying	
	56 2.034665	10.3.5.199	10.3.20.14	SIP	342 Status: 487 Request Cancelled	
	57 2.037965	10.3.20.14	10.3.5.199	SIP	305 Request: ACK sip:1010@10.3.5.199:5060	
	58 2.251601	10.3.5.199	10.3.20.14	SIP	547 Status: 180 Ringing	
	60 4.650231	10.3.5.199	10.3.20.14	SIP/SDP	746 Status: 200 OK, with session description	
	61 4.670808	10.3.20.14	10.3.20.4	SIP	405 Request: ACK sip:1021@10.3.20.4:5063	
	192 6.064543	10.3.5.199	10.3.20.14	SIP	342 Status: 487 Request Cancelled	
-	193 6.067820	10.3.20.14	10.3.5.199	SIP	305 Request: ACK s1p:1010@10.3.5.199:5060	
	263 6.733904	10.3.20.14	10.3.20.4	SIP/SDP	918 Request: INVIIE stp:1021@10.3.20.4:5063, in-dialog, with session description	
	264 6.741532	10.3.20.4	10.3.20.14	SIP SIP	336 Status: 100 rying	
	26/ 6./90510	10.3.20.4	10.3.20.14	SIP/SDP	746 Status: 200 ok, with session description	
	209 0.805/0/	10.5.20.14	10.3.20.4	216	403 Request. ACK SID.1021010.5.20.4.3005	
•					m	
=	Message Body	1				
	Session De	scription Prot	ocol			
	Session	Description Pro	otocol version (v): 0			
	Owner/Cr Session	eator, Session	Id (o): - 20037 20038	IN IP4 10.3.	3.20.14	
	E Connect	on Information	(c): IN IP4 10.3.20.14			
	E Time Des	cription, acti	ve time (t): 0 0			
	🕀 Media De	scription, name	e and address (m): aud	0 11854 RTP	P/AVP 18 9 0 8 101	
	media Attribute (a): rtpmap:18 G729/8000					
	Media Attribute (a): fmtp:18 annexb=no					
	Media Attribute (a): rtpmap:9 G722/8000					
	Media Attribute (a): rtpmap:0 PCMU/8000					
	Media Attribute (a): rtpmap:8 PCMA/8000					
	Media Attribute (a): rtpmap:101 telephone-event/8000					
	🗉 Media At	tribute (a): fi	mtp:101 0-15			
	🖲 Media At	tribute (a): p	time:20			
	Media At	tribute (a): s	endonly			

Capturing packets after you disable the RFC 2543 Hold feature. SDP media connection address c=0.0.0.0 per RFC 3264 is used in the INVITE message when placing a call on hold.

Ele Edit View Go	Capture Analyze	Statistics Telephony Tools	Internals Help			
		AIQ & & B 7			A 🕅 🗖 🎉   🛱	
Filter: sip			<ul> <li>Expression</li> </ul>	Clear Apply		
No. Time	Source	Destination	Protocol	Length Info		
56 3.074205	10.3.20.14	10.3.5.199	SIP/SDP	904 Reques	t: INVITE sip:1021@10.3.5.199:506	0, with session description
57 3.076752	10.3.5.199	10.3.20.14	SIP	314 Status	: 100 Trying	
59 3.328526	10.3.5.199	10.3.20.14	SIP	546 Status	: 180 Ringing	
60 5.121648	10.3.5.199	10.3.20.14	SIP/SDP	745 Status	: 200 OK, with session descriptio	n
61 5.141647	10.3.20.14	10.3.20.4	SIP	403 Reques	t: ACK s1p:1021@10.3.20.4:5063	
85 5.463380	10.3.20.9	224.0.1.75	SIP	544 Reques	t: SUBSCRIBE s1p:MAC001565770984@	224.0.1.75
182 6.4290/3	10.3.20.14	10.3.20.4	SIP/SDP	914 Reques	t: INVITE 51p:1021@10.3.20.4:5063	, in-dialog, with session description
187 6 482474	10.3.20.4	10.3.20.14	SIP STD/CDD	742 Status	: 200 OK with session description	n
189 6 496305	10 3 20 14	10 3 20 4	STP	404 Reques	t: ACK sin:1021010 3 20 4:5063	
105 01150505	1015120121	201312014	521	tot negues	er men sipilolitetersteersteersteerstees	
III Message Head	er					
E Message Body						
E Session De	scription Prot	ocol				
Session	Description Pr	otocol version (v): 0				
Owner/Cr	eator, Session	Id (o): - 20038 20039	IN IP4 10.3.	20.14		
Session	Name (s): SDP	data				
Connecti	on Information	(c): IN IP4 0.0.0.0				
Connec	tion Network T	ype: IN				
Connec	tion Address T	ype: IP4				
Connec	tion Address:	0.0.0.0				
E Time Des	cription, acti	ve time (t): 0 0	1			
Hedia De	Media Description, name and address (m): audio 11856 RTP/AVP 18 9 0 8 101					
B Media Attribute (a): rtpmapile G/29/6000						
Media Attribute (a): rtpman; G722/8000						
Media Attribute (a): rtpmap:0 972/0000						
I Media At	media Attribute (a): rtpmap: 8 pc/a/8000					
E Media At	tribute (a): r	tpmap:101 telephone-ev	ent/8000			
🗉 Media At	tribute (a): f	mtp:101 0-15				
🖲 Media At	tribute (a): p	time:20				
Media At	Madia Attribute (a): inactive					

For more information on RFC 2543 hold feature, refer to Call Hold on page 175. For more information on capturing packets, refer to Capturing Packets on page 324.

# What will happen if I connect both PoE cable and power adapter? Which has

# the higher priority?

IP phones use the PoE preferentially.

# Appendix

# Appendix A: Glossary

**802.1x**--an IEEE Standard for port-based Network Access Control (PNAC). It is a part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

**ACS** (Auto Configuration server)--responsible for auto-configuration of the Central Processing Element (CPE).

**Cryptographic Key**--a piece of variable data that is fed as input into a cryptographic algorithm to perform operations such as encryption and decryption, or signing and verification.

**DHCP** (Dynamic Host Configuration Protocol)--built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

**DHCP Option--**can be configured for specific values and enabled for assignment and distribution to DHCP clients based on server, scope, class or client-specific levels.

**DNS** (Domain Name System)--a hierarchical distributed naming system for PC, services, or any resource connected to the Internet or a private network.

**EAP-MD5** (Extensible Authentication Protocol-Message Digest Algorithm 5)--only provides authentication of the EAP peer to the EAP server but not mutual authentication.

**EAP-TLS** (Extensible Authentication Protocol-Transport Layer Security) –provides for mutual authentication, integrity-protected cipher suite negotiation between two endpoints.

**PEAP-MSCHAPv2** (Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2) –provides for mutual authentication, but does not require a client certificate on the IP phone.

**FAC** (Feature Access Code)--special patterns of characters that are dialed from a phone keypad to invoke particular features.

**HTTP** (Hypertext Transfer Protocol)--used to request and transmit data on the World Wide Web.

**HTTPS** (Hypertext Transfer Protocol over Secure Socket Layer)--a widely-used communications protocol for secure communication over a network.

**IEEE** (Institute of Electrical and Electronics Engineers)--a non-profit professional association headquartered in New York City that is dedicated to advancing technological innovation and excellence.

LAN (Local Area Network)--used to interconnects network devices in a limited area such as a home, school, PC laboratory, or office building.

**MIB** (Management Information Base)--a virtual database used for managing the entities in a communications network.

OID (Object Identifier)--assigned to an individual object within a MIB.

**ROM** (Read-only Memory)--a class of storage medium used in PC and other electronic devices.

RTP (Real-time Transport Protocol)--provides end-to-end service for real-time data.

**TCP** (Transmission Control Protocol)--a transport layer protocol used by applications that require guaranteed delivery.

UDP (User Datagram Protocol)--a protocol offers non-guaranteed datagram delivery.

**URI** (Uniform Resource Identifier)--a compact sequence of characters that identifies an abstract or physical resource.

URL (Uniform Resource Locator)--specifies the address of an Internet resource.

**VLAN** (Virtual LAN)-- a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

**VoIP** (Voice over Internet Protocol)--a family of technologies used for the delivery of voice communications and multimedia sessions over IP networks.

**WLAN** (Wireless Local Area Network)--a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

**XML-RPC** (Remote Procedure Call Protocol)--which uses XML to encode its calls and HTTP as a transport mechanism.

Time Zone	Time Zone Name
-11	Samoa
-10	United States-Hawaii-Aleutian, United States-Alaska-Aleutian
-9:30	French Polynesia
-9	United States-Alaska Time
-8	Canada(Vancouver,Whitehorse), Mexico(Tijuana,Mexicali),
	United States-Pacific Time
-7	Canada(Edmonton,Calgary), Mexico(Mazatlan,Chihuahua),

# Appendix B: Time Zones

Time Zone	Time Zone Name
	United States-MST no DST, United States-Mountain Time
,	Canada-Manitoba(Winnipeg), Chile(Easter Islands),
-6	Mexico(Mexico City,Acapulco), United States-Central Time
	Bahamas(Nassau), Canada(Montreal,Ottawa,Quebec),
-5	Cuba(Havana), United States-Eastern Time
-4:30	Venezuela(Caracas)
	Canada(Halifax,Saint John), Chile(Santiago),
-4	Paraguay(Asuncion), United Kingdom-Bermuda(Bermuda),
	United Kingdom(Falkland Islands), Trinidad&Tobago
-3:30	Canada-New Foundland(St.Johns)
2	Argentina(Buenos Aires), Brazil(DST), Brazil(no DST),
-3	Denmark-Greenland(Nuuk)
-2:30	Newfoundland and Labrador
-2	Brazil(no DST)
-1	Portugal(Azores)
	Denmark-Faroe Islands(Torshavn), GMT, Greenland,
0	Ireland(Dublin), Morocco, Portugal(Lisboa,Porto,Funchal),
	Spain-Canary Islands(Las Palmas), United Kingdom(London)
	Albania(Tirane), Austria(Vienna), Belgium(Brussels),
	Caicos, Chad, Croatia(Zagreb), Czech Republic(Prague),
+1	Denmark(Kopenhagen), France(Paris), Germany(Berlin),
	Hungary(Budapest), Italy(Rome), Luxembourg(Luxembourg),
	Macedonia(Skopje), Namibia(Windhoek),
	Netherlands(Amsterdam), Spain(Madrid)
	Estonia(Tallinn), Finland(Helsinki), Gaza Strip(Gaza),
	Greece(Athens), Israel(Tel Aviv), Jordan(Amman), Latvia(Riga),
+2	Lebanon(Beirut), Moldova(Kishinev), Romania(Bucharest),
	Russia(Kaliningrad), Syria(Damascus), Turkey(Ankara),
	Ukraine(Kyiv, Odessa)
+3	East Africa Time, Iraq(Baghdad), Russia(Moscow)
+3:30	Iran(Teheran)
+4	Armenia(Yerevan), Azerbaijan(Baku), Georgia(Tbilisi),
	Kazakhstan(Aktau), Russia(Samara)
+4:30	Afghanistan(Kabul)
+5	Kazakhstan(Aqtobe), Kyrgyzstan(Bishkek), Pakistan(Islamabad),
	Russia(Chelyabinsk)
+5:30	India(Calcutta)
+5:45	Nepal(Katmandu)
+6	Kazakhstan(Astana, Almaty), Russia(Novosibirsk,Omsk)
+6:30	Myanmar(Naypyitaw)
+7	Russia(Krasnoyarsk), Thailand(Bangkok)
+8	Australia(Perth), China(Beijing), Russia(Irkutsk, Ulan-Ude),

Time Zone	Time Zone Name				
	Singapore(Singapore)				
+8:45	Eucla				
+9	Japan(Tokyo), Korea(Seoul), Russia(Yakutsk,Chita)				
+9:30	Australia(Adelaide), Australia(Darwin)				
. 10	Australia(Brisbane), Australia(Hobart),				
+10	Australia(Sydney,Melboume,Canberra), Russia(Vladivostok)				
+10:30	Australia(Lord Howe Islands)				
+11	New Caledonia(Noumea), Russia(Srednekolymsk Time)				
+11:30	Norfolk Island				
+12	New Zealand (Wellington, Auckland), Russia (Kamchatka Time)				
+12:45	New Zealand(Chatham Islands)				
+13	Tonga(Nukualofa)				
+13:30	Chatham Islands				
+14	Kiribati				

# Appendix C: Trusted Certificates

Yealink IP phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom AG Root CA-2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary CA
- GeoTrust Primary CA G2 ECC
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA
- Thawte Primary Root CA G1 (EV)
- Thawte Primary Root CA G2 (ECC)
- Thawte Primary Root CA G3 (SHA256)
- Thawte Server CA
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority G2
- VeriSign Class 1 Public Primary Certification Authority G3

- VeriSign Class 2 Public Primary Certification Authority G2
- VeriSign Class 2 Public Primary Certification Authority G3
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 3 Public Primary Certification Authority G2
- VeriSign Class 3 Public Primary Certification Authority G3
- VeriSign Class 3 Public Primary Certification Authority G4
- VeriSign Class 3 Public Primary Certification Authority G5
- VeriSign Class 4 Public Primary Certification Authority G2
- VeriSign Class 4 Public Primary Certification Authority G3
- VeriSign Universal Root Certification Authority
- Microsoft\_IT\_SSL\_SHA2.cer
- CNNIC\_Root.cer
- baltimoreCyberTrust.cer
- UserTrust.cer
- AAA Certificate Services.cer
- DigiCert Assured ID Root CA.cer
- Entrust.net Certification Authority (2048).cer
- Entrust Root Certification Authority
- Entrust.net Secure Server Certification Authority
- GTE CyberTrust Global Root.cer
- Starfield Class 2 Certification Authority.cer
- AddTrust External CA Root
- Go Daddy Class 2 Certification Authority
- StartCom Certification Authority
- 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 292.

# Appendix D: SIP (Session Initiation Protocol)

This section describes how Yealink IP phones comply with the IETF definition of SIP as described in RFC 3261.

This section contains compliance information in the following:

RFC and Internet Draft Support

- SIP Request
- SIP Header
- SIP Responses
- SIP Session Description Protocol (SDP) Usage

# **RFC and Internet Draft Support**

The following RFC's and Internet drafts are supported:

- RFC 1321—The MD5 Message-Digest Algorithm
- RFC 1889—RTP Media control
- RFC 2112—Multipart MIME
- RFC 2327—SDP: Session Description Protocol
- RFC 2387—The MIME Multipart/Related Content-type
- RFC 2543—SIP: Session Initiation Protocol
- RFC 2617—Http Authentication: Basic and Digest access authentication
- RFC 2782—A DNS RR for specifying the location of services (DNS SRV)
- RFC 2806—URLs for Telephone Calls
- RFC 2833—RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 2915—The Naming Authority Pointer (NAPTR) DNS Resource Record
- RFC 2976—The SIP INFO Method
- RFC 3087—Control of Service Context using SIP Request-URI
- RFC 3261—SIP: Session Initiation Protocol (replacement for RFC 2543)
- RFC 3262—Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263—Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264—An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3265—Session Initiation Protocol (SIP) Specific Event Notification
- RFC 3266—Support for IPv6 in Session Description Protocol (SDP)
- RFC 3310—HTTP Digest Authentication Using Authentication and Key Agreement (AKA)
- RFC 3311—The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3312—Integration of Resource Management and SIP
- RFC 3313—Private SIP Extensions for Media Authorization
- RFC 3323—A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3324—Requirements for Network Asserted Identity
- RFC 3325—SIP Asserted Identity
- RFC 3326—The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3361—DHCP-for-IPv4 Option for SIP Servers

- RFC 3372—SIP for Telephones (SIP-T): Context and Architectures
- RFC 3398—ISUP to SIP Mapping
- RFC 3420—Internet Media Type message/sipfrag
- RFC 3428—Session Initiation Protocol (SIP) Extension for Instant Messaging
- RFC 3455—Private Header (P-Header) Extensions to the SIP for the 3GPP
- RFC 3486—Compressing the Session Initiation Protocol (SIP)
- RFC 3489—STUN Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515—The Session Initiation Protocol (SIP) Refer Method
- RFC 3550—RTP: Transport Protocol for Real-Time Applications
- RFC 3555—MIME Type Registration of RTP Payload Formats
- RFC 3581—An Extension to the SIP for Symmetric Response Routing
- RFC 3608—SIP Extension Header Field for Service Route Discovery During Registration
- RFC 3611—RTP Control Protocol Extended Reports (RTCP XR)
- RFC 3665—Session Initiation Protocol (SIP) Basic Call Flow Examples
- RFC 3666—SIP Public Switched Telephone Network (PSTN) Call Flows.
- RFC 3680—SIP Event Package for Registrations
- RFC 3702—Authentication, Authorization, and Accounting Requirements for the SIP
- RFC 3711—The Secure Real-time Transport Protocol (SRTP)
- RFC 3725—Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3842—A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- RFC 3856—A Presence Event Package for Session Initiation Protocol (SIP)
- RFC 3863—Presence Information Data Format
- RFC 3890—A Transport Independent Bandwidth Modifier for the SDP
- RFC 3891—The Session Initiation Protocol (SIP) "Replaces" Header
- RFC 3892—The Session Initiation Protocol (SIP) Referred-By Mechanism
- RFC 3959—The Early Session Disposition Type for SIP
- RFC 3960—Early Media and Ringing Tone Generation in SIP
- RFC 3966—The tel URI for telephone number
- RFC 3968—IANA Registry for SIP Header Field
- RFC 3969—IANA Registry for SIP URI
- RFC 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4083—3GPP Release 5 Requirements on SIP
- RFC 4235—An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)

- RFC 4244—An Extension to the SIP for Request History Information
- RFC 4317—Session Description Protocol (SDP) Offer/Answer Examples
- RFC 4353—A Framework for Conferencing with the SIP
- RFC 4458—SIP URIs for Applications such as Voicemail and Interactive Voice Response (IVR)
- RFC 4475—Session Initiation Protocol (SIP) Torture
- RFC 4485—Guidelines for Authors of Extensions to the SIP
- RFC 4504—SIP Telephony Device Requirements and Configuration
- RFC 4566—SDP: Session Description Protocol.
- RFC 4568—Session Description Protocol (SDP) Security Descriptions for Media Streams
- RFC 4575—A SIP Event Package for Conference State
- RFC 4579—SIP Call Control Conferencing for User Agents
- RFC 4583—Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- RFC 4662—A SIP Event Notification Extension for Resource Lists
- RFC 4730—Event Package for KPML
- RFC 5009—P-Early-Media Header
- RFC 5079—Rejecting Anonymous Requests in SIP
- RFC 5359—Session Initiation Protocol Service Examples
- RFC 5589—Session Initiation Protocol (SIP) Call Control Transfer
- RFC 5630—The Use of the SIPS URI Scheme in SIP
- RFC 5806—Diversion Indication in SIP
- RFC 5954—Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261
- RFC 6026—Correct Transaction Handling for 2xx Responses to SIP INVITE Requests
- RFC 6141—Re-INVITE and Target-Refresh Request Handling in SIP
- draft-ietf-sip-cc-transfer-05.txt—SIP Call Control Transfer
- draft-anil-sipping-bla-02.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-anil-sipping-bla-03.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
- draft-ietf-sip-privacy-00.txt—SIP Extensions for Caller Identity and Privacy, November
- draft-ietf-sip-privacy-04.txt—SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks
- draft-levy -sip-diversion-08.txt—Diversion Indication in SIP
- draft-ietf-sipping-cc-conferencing-03.txt—SIP Call Control Conferencing for User Agents

- draft-ietf-sipping-cc-conferencing-05.txt—Connection Reuse in the Session Initiation Protocol (SIP)
- draft-ietf-sipping-rtcp-summary-02.txt—Session Initiation Protocol Package for Voice Quality Reporting Event
- draft-ietf-sip-connect-reuse-06.txt—Connection Reuse in the Session Initiation Protocol (SIP)
- draft-ietf-bliss-shared-appearances-15.txt—Shared Appearances of a Session Initiation Protocol (SIP) Address of Record (AOR)

To find the applicable Request for Comments (RFC) document, go to http://www.ietf.org/rfc.html and enter the RFC number.

# **SIP Request**

Method	Supported	Notes
REGISTER	Yes	
INVITE	Yes	Yealink IP phones support mid-call changes such as placing a call on hold as signaled by a new INVITE that contains an existing Call-ID.
ACK	Yes	
CANCEL	Yes	
BYE	Yes	
OPTIONS	Yes	
SUBSCRIBE	Yes	
NOTIFY	Yes	
REFER	Yes	
PRACK	Yes	
INFO	Yes	
MESSAGE	Yes	
UPDATE	Yes	
PUBLISH	Yes	

The following SIP request messages are supported:

# **SIP Header**

The following SIP request headers are supported:

**Note** In the following table, a "Yes" in the Supported column means the header is sent and properly parsed.

Method	Supported	Notes
Accept	Yes	
Alert-Info	Yes	
Allow	Yes	
Allow-Events	Yes	
Authorization	Yes	
Call-ID	Yes	
Call-Info	Yes	
Contact	Yes	
Content-Length	Yes	
Content-Type	Yes	
CSeq	Yes	
Diversion	Yes	
History-Info	Yes	
Event	Yes	
Expires	Yes	
From	Yes	
Max-Forwards	Yes	
Min-SE	Yes	
P-Asserted-Identity	Yes	
P-Preferred-Identity	Yes	
Proxy-Authenticate	Yes	
Proxy-Authorization	Yes	
RAck	Yes	
Record-Route	Yes	

Method	Supported	Notes
Refer-To	Yes	
Referred-By	Yes	
Remote-Party-ID	Yes	
Replaces	Yes	
Require	Yes	
Route	Yes	
RSeq	Yes	
Session-Expires	Yes	
Subscription-State	Yes	
Supported	Yes	
То	Yes	
User-Agent	Yes	
Via	Yes	

# **SIP Responses**

The following SIP responses are supported:

## 1xx Response—Information Responses

1xx Response	Supported	Notes
100 Trying	Yes	
180 Ringing	Yes	
181 Call Is Being Forwarded	Yes	
183 Session Progress	Yes	

**Note** In the following table, a "Yes" in the Supported column means the header is sent and properly parsed. The phone may not actually generate the response.

## 2xx Response—Successful Responses

2xx Response	Supported	Notes
200 OK	Yes	
202 Accepted	Yes	In REFER transfer.

### 3xx Response—Redirection Responses

3xx Response	Supported	Notes
300 Multiple Choices	Yes	
301 Moved Permanently	Yes	
302 Moved Temporarily	Yes	

## 4xx Response—Request Failure Responses

4xx Response	Supported	Notes
400 Bad Request	Yes	
401 Unauthorized	Yes	
402 Payment Required	Yes	
403 Forbidden	Yes	
404 Not Found	Yes	
405 Method Not Allowed	Yes	
406 Not Acceptable	No	
407 Proxy Authentication Required	Yes	
408 Request Timeout	Yes	
409 Conflict	No	
410 Gone	No	
411 Length Required	No	
413 Request Entity Too Large	No	
414 Request-URI Too Long	Yes	
415 Unsupported Media Type	Yes	
416 Unsupported URI Scheme	No	
420 Bad Extension	No	

4xx Response	Supported	Notes
421 Extension Required	No	
423 Interval Too Brief	Yes	
480 Temporarily Unavailable	Yes	
481 Call/Transaction Does Not Exist	Yes	
482 Loop Detected	Yes	
483 Too Many Hops	No	
484 Address Incomplete	Yes	
485 Ambiguous	No	
486 Busy Here	Yes	
487 Request Terminated	Yes	
488 Not Acceptable Here	Yes	
491 Request Pending	No	
493 Undecipherable	No	

# 5xx Response—Server Failure Responses

5xx Response	Supported	Notes
500 Internal Server Error	Yes	
501 Not Implemented	Yes	
502 Bad Gateway	No	
503 Service Unavailable	No	
504 Gateway Timeout	No	
505 Version Not Supported	No	

## 6xx Response—Global Responses

6xx Response	Supported	Notes
600 Busy Everywhere	Yes	
603 Decline	Yes	
604 Does Not Exist Anywhere	No	
606 Not Acceptable	No	

# SIP Session Description Protocol (SDP) Usage

SDP Headers	Supported
v—Protocol version	Yes
o—Owner/creator and session identifier	Yes
a—Media attribute	Yes
c—Connection information	Yes
m—Media name and transport address	Yes
s—Session name	Yes
t—Active time	Yes

# Appendix E: SIP Call Flows

SIP uses six request methods:

INVITE—Indicates a user is being invited to participate in a call session.

ACK—Confirms that the client has received a final response to an INVITE request.

BYE—Terminates a call and can be sent by either the caller or the callee.

CANCEL—Cancels any pending searches but does not terminate a call that has already been accepted.

OPTIONS—Queries the capabilities of servers.

REGISTER-Registers the address listed in the To header field with a SIP server.

The following types of responses are used by SIP and generated by the IP phone or the SIP server:

- SIP 1xx—Informational Responses
- SIP 2xx—Successful Responses
- SIP 3xx—Redirection Responses
- SIP 4xx—Client Failure Responses
- SIP 5xx—Server Failure Responses
- SIP 6xx—Global Failure Responses

# Successful Call Setup and Disconnect

The following figure illustrates the scenario of a successful call. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

#### The call flow scenario is as follows:

- 1. User A calls User B.
- 2. User B answers the call.
- 3. User B hangs up.



Step	Action	Description
Fl	INVITE—User A to Proxy Server	<ul> <li>User A sends a SIP INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</li> <li>In the INVITE request:</li> <li>The IP address of User B is inserted in the Request-URI field.</li> <li>User A is identified as the call session initiator in the From field.</li> </ul>

Step	Action	Description
		• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		• The transaction number within a single call leg is identified in the CSeq field.
		• The media capability User A is ready to receive is specified.
		• The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	100 Trying—User B to Proxy Server	User B sends a SIP 100 Trying response to the proxy server. The 100 Trying response indicates that the INVITE request has been received by User B.
F4	100 Trying—Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has been received by User B.
F5	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the User B is being alerted.
F6	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F7	200 OK— User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F8	200OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F9	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy

Step	Action	Description
		server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F10	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F11	BYE—User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.
F12	BYE—Proxy Server to User A	The proxy server forwards the SIP BYE request to User A to notify that User B wants to release the call.
F13	200 OK—User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response indicates that User A has received the BYE request. The call session is now terminated.
F14	200 OK—Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B to indicate that User A has received the BYE request. The call session is now terminated.

# Unsuccessful Call Setup—Called User is Busy

The following figure illustrates the scenario of an unsuccessful call caused by the called user's being busy. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

### The call flow scenario is as follows:

- 1. User A calls User B.
- 2. User B is busy on the IP phone and unable or unwilling to take another call.



The call cannot be set up successfully.

Step	Action	Description
F1	INVITE—User A to Proxy Server	<ul> <li>User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</li> <li>In the INVITE request:</li> <li>The IP address of User B is inserted in the Request-URI field.</li> <li>User A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> <li>The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	100 Trying—User B to Proxy	User B sends a SIP 100 Trying response to
Step	Action	Description
------	-----------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
	Server	the proxy server. The 100 Trying response indicates that the INVITE request has been received by User B.
F4	100 Trying—Proxy Server to User A	The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has already been received.
F5	486 Busy Here—User B to Proxy Server	User B sends a SIP 486 Busy Here response to the proxy server. The 486 Busy Here response is a client error response indicating that User B is successfully connected but User B is busy on the IP phone and unable or unwilling to take the call.
F6	486 Busy Here—Proxy Server to User A	The proxy server forwards the 486 Busy Here response to notify User A that User B is busy.
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The SIP ACK message indicates that User A has received the 486 Busy Here message.
F8	ACK—Proxy Server to User B	The proxy server forwards the SIP ACK to User B to indicate that the 486 Busy Here message has already been received.

# Unsuccessful Call Setup—Called User Does Not Answer

The following figure illustrates the scenario of an unsuccessful call caused by the called user's no answering. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

- 1. User A calls User B.
- 2. User B does not answer the call.
- 3. User A hangs up.

The call cannot be set up successfully.



Step	Action	Description
Fl	INVITE—User A to Proxy Server	<ul> <li>User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.</li> <li>In the INVITE request:</li> <li>The IP address of User B is inserted in the Request-URI field.</li> <li>User A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified</li> </ul>
		<ul> <li>The port on which User B is</li> </ul>
		prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards

Step	Action	Description
		the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	CANCEL—User A to Proxy Server	User A sends a SIP CANCEL request to the proxy server after not receiving an appropriate response within the time allocated in the INVITE request. The SIP CANCEL request indicates that User A wants to disconnect the call.
F6	CANCEL—Proxy Server to User B	The proxy server forwards the SIP CANCEL request to notify User B that User A wants to disconnect the call.
F7	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The SIP 200 OK response indicates that User B has received the CANCEL request.
F8	200 OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to notify User A that the CANCEL request has been processed successfully.

# Successful Call Setup and Call Hold

The following figure illustrates a successful call setup and call hold. In this scenario, the two end users are User A and User B. User A and User B are located at Yealink SIP IP phones.

- 1. User A calls User B.
- 2. User B answers the call.

3. User A places User B on hold.



Step	Action	Description
		User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The IP address of User B is inserted in the Request-URI field.
		• User A is identified as the call session initiator in the From field.
Fl	INVITE—User A to Proxy Server	• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		<ul> <li>The transaction number within a single call leg is identified in the CSeq field.</li> </ul>
		• The media capability User A is ready to receive is specified.
		• The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on hold.
F13	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.

# Successful Call Setup and Call Waiting

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call, one of the participants receives and answers an incoming call from a third party. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

- 1. User A calls User B.
- 2. User B answers the call.
- **3.** User C calls User B.
- 4. User B accepts the call from User C.



Step	Action	Description
		User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The IP address of User B is inserted in the Request-URI field.
		• User A is identified as the call session initiator in the From field.
F1	INVITE—User A to Proxy Server	• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		<ul> <li>The transaction number within a single call leg is identified in the CSeq field.</li> </ul>
		<ul> <li>The media capability User A is ready to receive is specified.</li> </ul>
		• The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies proxy server that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User C to Proxy Server	<ul> <li>User C sends a SIP INVITE message to the proxy server. The INVITE request is an invitation to User A to participate in a call session.</li> <li>In the INVITE request:</li> <li>The IP address of User A is inserted in the Request-URI field.</li> <li>User C is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User C is ready to receive is specified.</li> <li>The port on which User A is prepared to receive the RTP data is specified.</li> </ul>
F10	INVITE—Proxy Server to User A	The proxy server maps the SIP URI in the To field to User A. The proxy server sends the INVITE message to User A.
F11	180 Ringing—User A to Proxy Server	User A sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F12	180 Ringing—Proxy Server to User C	The proxy server forwards the 180 Ringing response to User C. User C hears the ring-back tone indicating that User A is being alerted.

Step	Action	Description
F13	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F14	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F15	200 OK—User B to Proxy Server	User B sends a 200 OK to the proxy server. The 200 OK response indicates that the INVITE was successfully processed.
F16	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on hold.
F17	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F18	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F19	200 OK—User A to Proxy Server	User A sends a 200 OK response to the proxy server. The 200 OK response notifies that the connection has been made.
F20	200 OK—Proxy Server User C	The proxy server forwards the 200 OK message to User C.
F21	ACK—User C to Proxy Server	User C sends a SIP ACK to the proxy server. The ACK confirms that User C has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User A	The proxy server forwards the SIP ACK to User A to confirm that User C has received the 200 OK response.

# Call Transfer without Consultation

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to a third party without consultation. This is called a blind transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

- 1. User A calls User B.
- 2. User B answers the call.
- 3. User B transfers the call to User C.
- 4. User C answers the call.

Step	Action	Description
F1	INVITE—User A to Proxy Server	<ul> <li>User A sends an INVITE message to the proxy server. The INVITE request is an invitation to User B to participate in a call session.</li> <li>In the INVITE request:</li> <li>The IP address of User B is inserted in the Request-URI field.</li> <li>User A is identified as the call session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is ready to receive is specified.</li> <li>The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being

Step	Action	Description
		alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	REFER—User B to Proxy Server	User B sends a REFER message to the proxy server. User B performs a blind transfer of User A to User C.
F10	202 Accepted—Proxy Server to User B	The proxy server sends a SIP 202 Accept response to User B. The 202 Accepted response notifies User B that the proxy server has received the REFER message.
F11	REFER—Proxy Server to User A	The proxy server forwards the REFER message to User A.
F12	202 Accepted—User A to Proxy Server	User A sends a SIP 202 Accept response to the proxy server. The 202 Accepted response indicates that User A accepts the transfer.
F13	BYE—User B to Proxy Server	User B terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User B wants to release the call.

Step	Action	Description
F14	BYE—Proxy Server to User A	The proxy server forwards the BYE request to User A.
F15	2000K—User A to Proxy Server	User A sends a SIP 200 OK response to the proxy server. The 200 OK response confirms that User A has received the BYE request.
F16	2000K—Proxy Server to User B	The proxy server forwards the SIP 200 OK response to User B.
F17	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F18	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C.
F19	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F20	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted
F21	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies the proxy server that the connection has been made.
F22	2000K—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F23	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F24	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that User A has received the 200 OK response. The call session is now active.

# Call Transfer with Consultation

The following figure illustrates a successful call between Yealink SIP IP phones in which two parties are in a call and then one of the parties transfers the call to the third party with consultation. This is called attended transfer. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

- 1. User A calls User B.
- 2. User B answers the call.
- 3. User A calls User C.
- 4. User C answers the call.
- 5. User A transfers the call to User C.

Call is established between User B and User C.



Step	Action	Description
		User A sends an INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session.
		In the INVITE request:
		• The IP address of User B is inserted in the Request-URI field.
		• User A is identified as the call session initiator in the From field.
F1	INVITE—User A to Proxy Server	• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.
		<ul> <li>The transaction number within a single call leg is identified in the CSeq field.</li> </ul>
		<ul> <li>The media capability User A is ready to receive is specified.</li> </ul>
		• The port on which User B is prepared to receive the RTP data is specified.
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.

Step	Action	Description
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server, The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE was successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on hold.
F13	ACK—User A to Proxy Server	User A sends an ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C. The proxy server sends

Step	Action	Description
		the INVITE request to User C.
F17	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User C is being alerted.
F19	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User C	The proxy server forwards the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.
F23	REFER—User A to Proxy Server	User A sends a REFER message to the proxy server. User A performs a transfer of User B to User C.
F24	202 Accepted—Proxy Server to User A	The proxy server sends a SIP 202 Accepted response to User A. The 202 Accepted response notifies User A that the proxy server has received the REFER message.
F25	REFER—Proxy Server to User B	The proxy server forwards the REFER message to User B.
F26	202 Accepted—User B to Proxy Server	User B sends a SIP 202 Accept response to the proxy server. The 202 Accepted

Step	Action	Description
		response indicates that User B accepts the transfer.
F27	BYE—User A to Proxy Server	User A terminates the call session by sending a SIP BYE request to the proxy server. The BYE request indicates that User A wants to release the call.
F28	BYE—Proxy Server to User B	The proxy server forwards the BYE request to User B.
F29	200OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that User B has received the BYE request.
F30	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.

# **Call Conference**

The following figure illustrates successful 3-way calling between Yealink IP phones in which User A mixes two RTP channels and therefore establishes a conference between User B and User C. In this call flow scenario, the end users are User A, User B, and User C. They are all using Yealink SIP IP phones, which are connected via an IP network.

- **1.** User A calls User B.
- 2. User B answers the call.
- 3. User A places User B on hold.
- 4. User A calls User C.
- 5. User C answers the call.

6. User A mixes the RTP channels and establishes a conference between User B and User C.



Step	Action	Description
F1	INVITE—User A to Proxy Server	User A sends the INVITE message to a proxy server. The INVITE request is an invitation to User B to participate in a call session. In the INVITE request: • The IP address of User B is inserted in the Request-URI field. • User A is identified as the call

Step	Action	Description
		<ul> <li>session initiator in the From field.</li> <li>A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</li> </ul>
		<ul> <li>The transaction number within a single call leg is identified in the CSeq field.</li> <li>The media capability User A is</li> </ul>
		<ul> <li>ready to receive is specified.</li> <li>The port on which User B is prepared to receive the RTP data is specified.</li> </ul>
F2	INVITE—Proxy Server to User B	The proxy server maps the SIP URI in the To field to User B. Proxy server forwards the INVITE message to User B.
F3	180 Ringing—User B to Proxy Server	User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F4	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User B is being alerted.
F5	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F6	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.
F7	ACK—User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F8	ACK—Proxy Server to User B	The proxy server sends the SIP ACK to User B. The ACK confirms that the proxy server has received the 200 OK response. The call session is now active.

Step	Action	Description
F9	INVITE—User A to Proxy Server	User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call on hold.
F10	INVITE—Proxy Server to User B	The proxy server forwards the mid-call INVITE message to User B.
F11	200 OK—User B to Proxy Server	User B sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the INVITE is successfully processed.
F12	200 OK—Proxy Server to User A	The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User A that User B is successfully placed on hold.
F13	ACK—User A to Proxy Server	User A sends the ACK message to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now temporarily inactive. No RTP packets are being sent.
F14	ACK—Proxy Server to User B	The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.
F15	INVITE—User A to Proxy Server	User A sends a SIP INVITE request to the proxy server. In the INVITE request, a unique Call-ID is generated and the Contact-URI field indicates that User A requests the call.
F16	INVITE—Proxy Server to User C	The proxy server maps the SIP URI in the To field to User C. The proxy server sends the SIP INVITE request to User C.
F17	180 Ringing—User C to Proxy Server	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.
F18	180 Ringing—Proxy Server to User A	The proxy server forwards the 180 Ringing response to User A. User A hears the ring-back tone indicating that User

Step	Action	Description
		C is being alerted.
F19	200OK—User C to Proxy Server	User C sends a SIP 200 OK response to the proxy server. The 200 OK response notifies User A that the connection has been made.
F20	200OK—Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A. The 200 OK response notifies User A that the connection has been made.
F21	ACK— User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK confirms that User A has received the 200 OK response. The call session is now active.
F22	ACK—Proxy Server to User C	The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.

# Index

#### Numeric

180 Ring Workaround174802.1X Authentication305

#### Α

About This Guide v Account Lock 291 Acoustic Echo Cancellation 272 Action URI 209 Administrator Password 285 Allow Mute 189 Always On Line 169 Appendix 343 Appendix A: Glossary 343 Appendix B: Time Zones 344 Appendix C: Trusted Certificates 346 Appendix D: SIP 347 Appendix E: SIP Call Flows 356 Audio Codecs 265 Auto Answer 167 Auto-Logout Time 286 Automatic Gain Control 273

## B

Background Noise Suppression 273 Backlight 84 Boss/Admin Feature 194 BToE 204 Busy Tone Delay 171

# С

Call Hold 175 Call Number Filter 179 Call Waiting 160 Capturing Packets 324 CDP 225 Comfort Noise Generation 275 **Configuration Files** 35 Configuration Methods 34 Configuring Advanced features 206 Configuring Basic Features 79 Configuring Basic Network Parameters 40 **Configuring Security Features** 281 Connecting the IP phone 25 Contrast 83 Conventions Used in Yealink Documentations v

#### D

DHCP 40 DHCP Option 44 DHCP VLAN 232 Dial-now 135 Dial Plan 134 Dial Search Delay 157 Documentations v DTMF 181 Dual Headset 263

#### Ε

E911 Location Tip 191 Early Media 173 Enabling the Watch Dog Feature 327 Encrypting Configuration Files 301 EXP40 Expansion Module 206 Expansion Module 23

#### G

Getting Information from Status Indicators 329 Getting Started 25

#### Н

H.323 15 Headset Prior 261

#### I

Index 385 Initialization Process Overview 30 In This Guide v IPv6 Support 238

### J

Jitter Buffer 277

#### Κ

Key As Send 130

### L

Language 121 Live Dialpad 159 LLDP 221

#### Μ

Missed Call Log 155 Multicast Paging 209

## Ρ

Phone Lock 288 Phone User Interface 35 Physical Features of IP Phones 18 Power Indicator LED 80 PPPoE 57 Pre Dial Tone 163 Product Overview 15

#### Q

Quality of Service 235

#### R

Reading Icons32Redial Tone164

Return Code When Refuse172Ringer Device for Headset165Ring Tones249

### S

Saving Call Log 153 Sign in 87 Sign out 95 SIP 15 SIP Components 16 SIP Header 352 SIP Phone Models 17 SIP Responses 353 SIP Request 351 SIP Session Description Protocol Usage 356 Skype for Business Feature License 281 Skype for Business Status 283 Specifying the Language to Use 127 Static DNS 42 Suppress DTMF Display 183

# T

Table of ContentsixTime and Date104Tones253Transfer via DTMF185Transport Layer Security (TLS)292Troubleshooting317Troubleshooting Methods317Troubleshooting Solutions331

#### U

Update Checking Time 74 Updating Status Automatically 98 Upgrading Firmware 66 User Password 283

#### ۷

Verifying Startup 32 Viewing Log Files 317 VLAN 221 Voice Activity Detection 274 Voice Mail Tone 260 Voice Mail without PIN 190 VoIP Principle 15

## W

Web Server Type93Web User Interface35