Yealink

T5 Series/CP960 IP Phones Administrator Guide

Version 80.13
Oct. 2017

Copyright

Copyright © 2017 YEALINK(XIAMEN) NETWORK TECHNOLOGY

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

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

Trademarks

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

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

Warranty

(1) **Warranty**

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

(2) **Disclaimer**

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

(3) **Limitation of Liability**

Yealink and/or its respective suppliers are not responsible for the suitability of the information contained in this document for any reason. The information is provided "as is", and Yealink does not provide any warranty and is subject to change without notice. All risks other than risks caused by use of the information are borne by the recipient. In no event, even if Yealink has been suggested the occurrence of

damages that are direct, consequential, incidental, special, punitive or whatsoever (Including but not limited to loss of business profit, business interruption or loss of business information), shall not be liable for these damages.

End User License Agreement

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

Patent Information

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

Customer Feedback

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

Technical Support

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

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.

Introduction

About This Guide

Yealink administrator guide is intended for administrators who need to properly configure, customize, manage, and troubleshoot the smart media phones rather than end-users. This guide will help you understand the VoIP network and SIP components, and provides descriptions of all available phone features.

This guide describes three methods for configuring IP phones: central provisioning, web user interface and phone user interface. It will help you perform the following tasks:

- Configure your IP phone on a provisioning server
- Configure your phone's features and functions via web/phone user interface
- Troubleshoot some common phone issues

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.

The information detailed in this guide is applicable to firmware version 80 or higher. The firmware format is like x.x.x.x.rom. The second x from left must be greater than or equal to 80 (e.g., the firmware version of SIP-T58V IP phone: 58.80.0.5.rom).

Chapters in This Guide

This administrator guide includes the following chapters:

- Chapter 1, "Product Overview" describes the smart media phones and expansion modules.
- Chapter 2, "Getting Started" describes how Yealink phones fit in your network and how to install and connect IP phones, and also gives you an overview of IP phone's initialization process.
- Chapter 3, "Setting Up Your System" describes some essential information on how to set up your phone network and set up your phone with a provisioning server.
- Chapter 4, "Configuring Basic Features" describes how to configure the basic features on IP phones.
- Chapter 5, "Configuring Advanced Features" describes how to configure the advanced features on IP phones.
- Chapter 6, "Configuring Audio Features" describes how to configure the audio features on IP phones.
- Chapter 7, "Configuring Video Features" describes how to configure the video features on

IP phones.

- Chapter 8, "Configuring Security Features" describes how to configure the security features on IP phones.
- Chapter 9, "Troubleshooting" describes how to troubleshoot IP phones and provides some common troubleshooting solutions.
- Chapter 10, "Appendix" provides the glossary, time zones, trusted certificates, auto provisioning flowchart, reference information about IP phones compliant with RFC 3261, SIP call flows, some other function lists (e.g., DSS keys, reading icons) and index.

Related Documentations

The following related documents for SIP-T58V/A, SIP-T56A and CP960 IP phones 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 how to configure and use the basic and advanced features available on IP phones via phone user interface.
- Auto Provisioning Guide, which describes how to provision IP phones using the configuration files.

  The purpose of *Auto Provisioning Guide* is to serve as a basic guidance for provisioning Yealink IP phones with a provisioning server. If you are new to this process, it is helpful to read this guide.
- Description of Configuration Parameters in CFG Files, which describes all configuration parameters in configuration files.

  Note that Yealink administrator guide contains most of parameters. If you want to find out more parameters not listed in this guide, please refer to *Description of Configuration Parameters in CFG Files* guide.
- y000000000000.boot template boot file.
- <y0000000000xx>.cfg and <MAC>.cfg template configuration files.
- IP Phones Deployment Guide for BroadSoft UC-One Environments, which describes how to configure BroadSoft features on the BroadWorks web portal and IP phones.
- IP Phone Features Integrated with BroadSoft UC-One User Guide, which describes how to configure and use IP phone features integrated with BroadSoft UC-One on Yealink IP phones.

  When the SIP server type is set to BroadSoft, please refer to these two guides to have a better knowledge of configuring and using features integrated with Broadsoft UC-One.

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

Conventions Used in Yealink Documentations

Yealink documentations contain a few typographic conventions and writing conventions.

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

Convention	Description
Bold	Highlights the web/phone user interface items such as menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (e.g., Click on **Settings**->**Upgrade**.). Also used to emphasize text (e.g., **Important!**).
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 Ring Tones on page 601), for hyperlinks to non-Yealink websites (e.g., RFC 3315) or for hyperlinks to Yealink Technical Support website.
Blue Text in Italics	Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (e.g., *Yealink_SIP-T2_Series_T19(P) E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*).

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

Convention	Description
<>	Indicates that you must enter information specific to phone or network. For example, when you see <MAC>, enter your phone's 12-digit MAC address. If you see <phoneIPAddress>, enter your phone's IP address.
->	Indicates that you need to select an item from a menu. For example, **Settings**->**Basic** indicates that you need to select **Basic** from the **Settings** menu via phone user interface. **Note**: By default, the **Settings** menu locates on the second idle screen. You need to swipe left/right to see it. Or, you can also swipe down from the top of the screen to enter the control center

Reading the Configuration Parameter Tables

The feature descriptions discussed in this guide include two tables. One is a summary table of

provisioning methods that you can use to configure the features. The other is a table of details of the configuration parameters that you configure to make the features work.

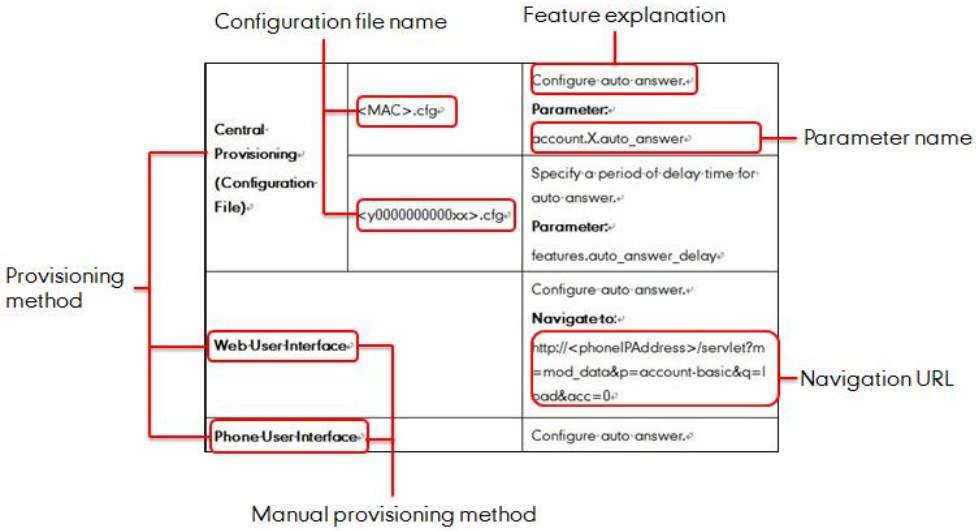
This brief section describes the conventions used in the summary table and configuration parameter table. In order to read the tables and successfully perform configuration changes, an understanding of these conventions is necessary.

Summary Table Format

The following summary table indicates three provisioning methods (central provisioning, web user interface and phone user interface, refer to Provisioning Methods for more information) you can use to configure a feature. Note that the types of provisioning methods available for each feature will vary; not every feature uses all these three methods.

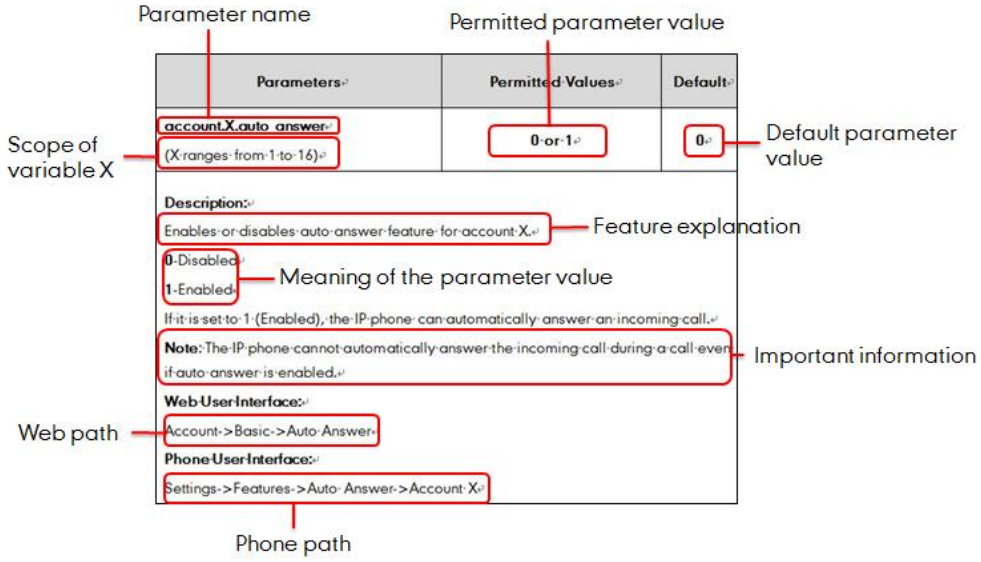
The central provisioning method requires you to configure parameters located in CFG format configuration files that Yealink provides. For more information on configuration files, refer to Configuration Files on page 116. As shown below, the table specifies the configuration file name and the corresponding parameters. That is, the MAC.cfg file contains the *account.X.auto_answer* parameter, and the y0000000000xx.cfg file contains the *feature.auto_answer_delay* parameter.

The web user interface method requires you to configure features by navigating to the specified link. This navigation URL can help you quickly locate the webpage where you can configure the feature.



Configuration Parameter Table Format

The following configuration parameter table describes the parameter that you can configure to make the feature (e.g., auto answer) work.



Note

Sometimes you will see the words "Refer to the following content" in the **Permitted Values** or **Default** field. It means the permitted value or the default value of the parameter has the model difference or there are many permitted values of the parameter, you can get more details from the following **Description** field.

The word "None" in the **Web User Interface** or **Phone User Interface** field means this feature cannot be configurable via web/phone user interface.

The above table also indicates three methods for configuring the feature.

Method 1: Central Provisioning

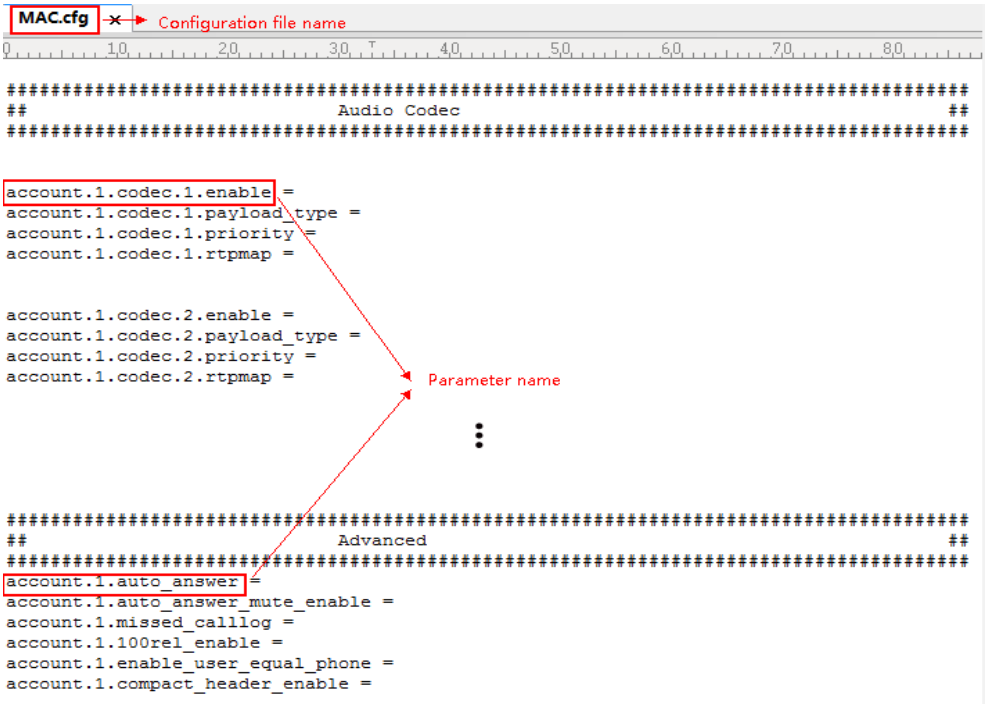
This table specifies the details of *account.X.auto_answer* parameter, which enables or disables the auto answer feature. This parameter is disabled by default. If you want to enable the auto answer feature, open the MAC.cfg file and locate the parameter name *account.X.auto_answer*. Set the parameter value to "1" to enable the auto answer feature or "0" to disable the auto answer feature.

Note that some parameters described in this guide contain one or more variables (e.g., X or Y). But the variables in the parameters described in the CFG file are all replaced with specific value in the scope of variable. You may need to assign a value to the variable before you search and locate the specific parameter in the CFG file.

For example, if you want to enable the auto answer feature for account 1, you need to locate the *account.1.auto_answer* in the MAC.cfg file and then configure it as required (e.g., account.1.auto_answer = 1). If you want to enable the audio codec 1 for account 1, you can

locate the *account.1.codec.1.enable* in the MAC.cfg file and configure it as required (e.g., account.1.codec.1.enable = 1).

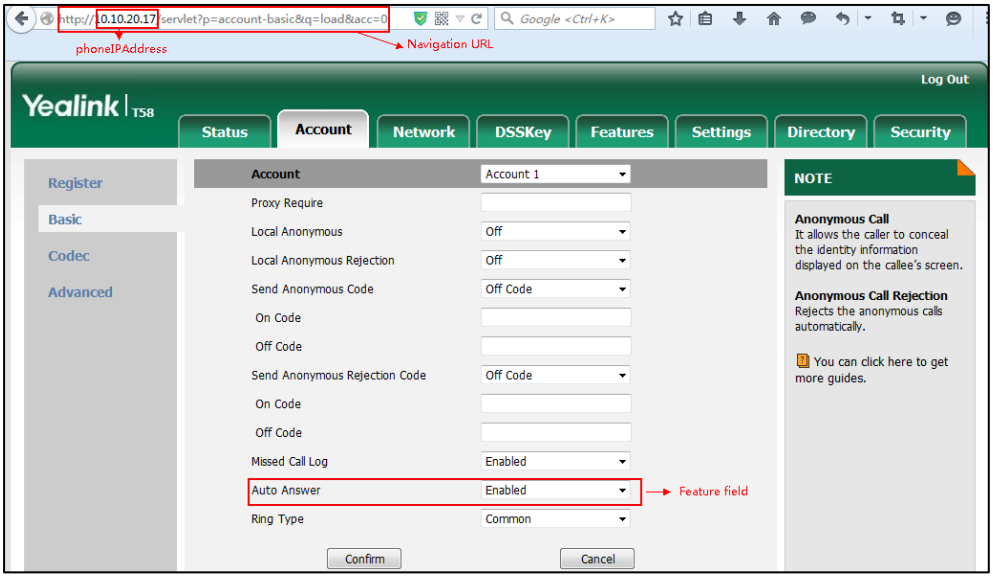
The following shows a segment of MAC.cfg file:



Method 2: Web User Interface

As described in the chapter Summary Table Format, you can directly navigate to the specified webpage to configure the feature. You can also first log into the web user interface, and then locate the feature field according to the web path (e.g., **Account**->**Basic**->**Auto Answer**) to configure it as required.

As shown in the following illustration:

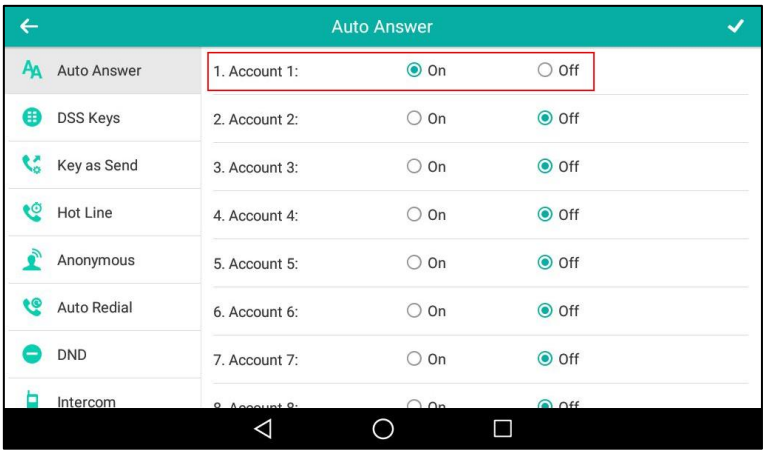


To successfully log into the web user interface, you may need to enter the user name (default: admin) and password (default: admin). For more information, refer to Web User Interface on page 113.

Method 3: Phone User Interface

You can configure features via phone user interface. Access to the desired feature according to the phone path (e.g., **Settings**->**Features**->**Auto Answer**->**Account X**) and then configure it as required.

As shown in the following illustration:



Recommended References

For more information on configuring and administering other Yealink products not included in this guide, refer to product support page at Yealink Technical Support.

To access the latest Release Notes or other guides for Yealink IP phones, refer to the Document Download page for your phone at Yealink Technical Support.

If you want to find Request for Comments (RFC) documents, type *http://www.ietf.org/rfc/rfcNNNN.txt* (NNNN is the RFC number) into the location field of your browser.

This guide mainly takes the SIP-T58V IP phones as example for reference. For more details on other IP phones, refer to *Yealink phone-specific user guide*.

For other references, look for the hyperlink or web info throughout this administrator guide.

Understanding VoIP Principle and SIP Components

This section mainly describes the basic knowledge of VoIP principle and SIP components, which will help you have a better understanding of the phone's deployment scenarios.

VoIP Principle

VoIP

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.

Summary of Changes

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

Changes for Release 80, Guide Version 80.13

Major updates have occurred to the following sections:

- Noise Suppression on page 651
- Smart Noise Block on page 652

Changes for Release 80, Guide Version 80.12

Documentations of the newly released CP960 IP phones have been added.

The following sections are new for this version:

- CSTA Control on page 450
- Real-Time Transport Protocol (RTP) Ports on page 592

Major updates have occurred to the following sections:

- Physical Features of IP Phones on page 2
- Key Features of IP Phones on page 4
- Connecting the IP Phones on page 10
- Power Saving on page 157
- Bluetooth on page 164
- Intercom on page 412
- Customizing a Local Contact File on page 270
- Auto Answer on page 292
- Appendix C: Trusted Certificates on page 770

Changes for Release 80, Guide Version 80.11

Major update had occurred to the following section:

- Door Phone on page 441

Table of Contents

Introduction.....v

About This Guide v
Chapters in This Guide.....v
Related Documentations vi
Conventions Used in Yealink Documentations vii
Reading the Configuration Parameter Tables.....vii
Summary Table Format..... viii
Configuration Parameter Table Format.....ix
Recommended References xi
Understanding VoIP Principle and SIP Components xi
VoIP Principle xii
SIP Components..... xiii
Summary of Changes xiv
Changes for Release 80, Guide Version 80.13 xiv
Changes for Release 80, Guide Version 80.12 xiv
Changes for Release 80, Guide Version 80.11 xiv

Table of Contents.....xv

Product Overview 1

SIP IP Phone Models.....1
Physical Features of IP Phones.....2
Key Features of IP Phones.....4
Expansion Modules 6

Getting Started.....9

What IP Phones Need to Meet.....9
Yealink IP Phones in a Network 9
Connecting the IP Phones 10
Inserting the Camera (only applicable to SIP-T58V/A IP phones) 11
Attaching the Stand and the Optional Wall Mount Bracket (not applicable to CP960 IP phones) 12
Adjust the angle of touch screen (only applicable to SIP-T58V/A IP phones).....14
Connecting the Handset and Optional Headset (not applicable to CP960 IP phones)14
Connecting the Power and Network 15
Connecting the Optional USB Flash Drive.....18

Connecting the Wired Expansion MIC CPE90 (Only Applicable to CP960 IP Phones) .19
Connecting the Optional PC using a Micro USB Cable (Only Applicable to CP960 IP Phones) 19
Connecting the Optional External Speaker (Only Applicable to CP960 IP Phones) 20
Initialization Process Overview.....20
Verifying Startup 21

Setting Up Your System 23

Setting Up Your Phone Network.....23
DHCP.....24
DHCP Option.....28
Configuring Network Parameters Manually.....32
PPPoE.....38
Configuring Transmission Methods of the Internet Port and PC Port.....40
Configuring PC Port Mode 44
Web Server Type.....46
Wi-Fi.....50
VLAN 53
IPv6 Support 66
VPN.....76
Configuring the IP Phone for Use with a Firewall or NAT 80
Quality of Service (QoS).....95
802.1X Authentication 99
Setting Up Your Phones with a Provisioning Server 110
Provisioning Points to Consider 110
Provisioning Methods.....111
Boot Files, Configuration Files and Resource Files 114
Setting Up a Provisioning Server 121
Upgrading Firmware.....124
Keeping User Personalized Settings after Auto Provisioning 132

Configuring Basic Features 143

Power Indicator LED.....145
Notification Popups 149
Wallpaper 152
Screen Saver.....156
Power Saving 157
Backlight 162
Bluetooth.....164
Enable Page Tips 169
Page Tips for Expansion Module.....171
Account Registration 172
Multiple Line Keys per Account 180
Call Display 184

Display Method on Dialing 186
Time and Date 188
NTP Time Server 189
Time and Date Settings 194
Daylight Saving Time (DST) 197
Language 205
Loading Language Packs 206
Specifying the Language to Use 213
Softkey Layout 215
Customizing Softkey Layout Template File 217
Key As Send 223
Dial Plan 227
Dial Plan using XML Template Files 227
Dial Plan using Digit Map String Rules 242
Emergency Dialplan 251
Hotline 255
Off Hook Hot Line Dialing 258
Search Source List In Dialing 260
Customizing a Super Search Template File 260
Save Call Log 263
Call List Show Number 265
Missed Call Log 266
Local Directory 268
Customizing a Local Contact File 268
Configuring Local Directory 275
Live Dialpad 280
Speed Dial 282
Call Waiting 287
Auto Redial 290
Auto Answer 292
IP Direct Auto Answer 297
Allow IP Call 299
Accept SIP Trust Server Only 300
Call Completion 302
Anonymous Call 305
Anonymous Call Rejection 309
Do Not Disturb (DND) 313
Busy Tone Delay 325
Return Code When Refuse 327
Early Media 329
180 Ring Workaround 329
Use Outbound Proxy in Dialog 330
SIP Session Timer 332
Session Timer 334

Call Hold 337
Music on Hold (MoH) 341
Call Forward 343
Call Transfer 363
Local Conference 366
Network Conference 367
Transfer on Conference Hang Up 369
Feature Key Synchronization 371
Transfer Mode via Dsskey 372
Directed Call Pickup 374
Group Call Pickup 382
Dialog Info Call Pickup 389
Recent Call In Dialing 392
ReCall 394
Call Number Filter 397
Call Park 399
Calling Line Identification Presentation (CLIP) 403
Connected Line Identification Presentation (COLP) 407
Mute 410
Allow Mute 410
Keep Mute 411
Intercom 412
Outgoing Intercom Calls 413
Incoming Intercom Calls 419
Call Timeout 422
Ringing Timeout 422
Send user=phone 423
SIP Send MAC 425
SIP Send Line 427
Reserve # in User Name 429
Password Dial 431
Unregister When Reboot 433
100 Reliable Retransmission 434
Reboot in Talking 436
Answer By Hand 438
Call Recording Using Soft Key 439
Silent Mode 440
Door Phone 441
Mobile Account 445
Quick Login 449
CSTA Control 450

Configuring Advanced Features 453

Remote Phone Book 453

Customizing Remote Phone Book Template File 453
Lightweight Directory Access Protocol (LDAP) 461
Busy Lamp Field (BLF) 473
BLF Subscription 473
Visual Alert and Audio Alert for BLF Pickup 477
BLF LED Mode 479
Configuring a BLF Key 482
Busy Lamp Field (BLF) List 486
Hide Feature Access Codes 492
Shared Call Appearance (SCA) 494
Message Waiting Indicator (MWI) 503
Multicast Paging 508
Sending RTP Stream 508
Receiving RTP Stream 519
Call Recording Using DSS Keys (Record and URL Record) 524
Hot Desking 531
Logon Wizard 536
Action URL 540
Action URI 560
Configuring Trusted IP Address for Action URI 564
Scenario A - Capturing the Current Screen of the Phone 566
Scenario B - Placing a Call via Web User Interface 568
Server Redundancy 569
Server Domain Name Resolution 581
Static DNS Cache 584
Real-Time Transport Protocol (RTP) Ports 592
TR-069 Device Management 594

Configuring Audio Features 601

Redial Tone 601
Ring Tones 602
Distinctive Ring Tones 607
Tones 614
Voice Mail Tone 621
Ringer Device for Headset 622
Headset Prior 624
Dual Headset 626
Sending Volume 627
Audio Codecs 629
Supported Audio Codecs 630
Packetization Time (PTime) 638
Opus Sample Rate 640
Acoustic Clarity Technology 642
Acoustic Echo Cancellation (AEC) 642

Background Noise Suppression (BNS) 643
Automatic Gain Control (AGC) 644
Voice Activity Detection (VAD) 644
Comfort Noise Generation (CNG) 645
Jitter Buffer 647
Noise Suppression 651
Smart Noise Block 652
DTMF 654
Methods of Transmitting DTMF Digit 654
Suppress DTMF Display 659
Transfer via DTMF 661
Play Local DTMF Tone 663
Voice Quality Monitoring (VQM) 664
RTCP-XR 665
VQ-RTCPXR 666

Configuring Video Features 683

Video Settings 683
Video Codecs 685

Configuring Security Features 689

User and Administrator Passwords 689
Auto-Logout Time 691
Phone Lock 692
Transport Layer Security (TLS) 698
Secure Real-Time Transport Protocol (SRTP) 709
Encrypting and Decrypting Files 713
Configuration Parameters 713
Encrypting and Decrypting Configuration Files 717

Troubleshooting 721

Troubleshooting Methods 721
Viewing Log Files 721
Capturing Packets 735
Enabling Watch Dog Feature 740
Getting Information from Status Indicators 741
Getting Information from Talk Statistics 742
Analyzing Configuration Files 742
Troubleshooting Solutions 746
IP Address Issues 746
Time and Date Issues 747
Display Issues 747

Phone Book Issues 748
Audio Issues 748
Camera and Video Issues 749
Wi-Fi and Bluetooth Issues 750
Firmware and Upgrading Issues 750
Provisioning Issues 751
System Log Issues 752
Resetting Issues 752
Rebooting Issues 757
Protocols and Ports Issues 760
Password Issues 762
Power and Startup Issues 762
Hardware Issues 762
Other Issues 763

Appendix 767

Appendix A: Glossary 767
Appendix B: Time Zones 769
Appendix C: Trusted Certificates 770
Appendix D: Configuring DSS Keys 775
Appendix E: Auto Provisioning Flowchart (Keep User Personalized Configuration Settings) 786
Appendix F: Static Settings 787
Appendix G: Reading Icons 793
Appendix H: SIP (Session Initiation Protocol) 798
RFC and Internet Draft Support 798
SIP Request 801
SIP Header 802
SIP Responses 803
SIP Session Description Protocol (SDP) Usage 806
Appendix I: SIP Call Flows 806
Successful Call Setup and Disconnect 807
Unsuccessful Call Setup−Called User is Busy 809
Unsuccessful Call Setup−Called User Does Not Answer 811
Successful Call Setup and Call Hold 813
Successful Call Setup and Call Waiting 816
Call Transfer without Consultation 820
Call Transfer with Consultation 824
Always Call Forward 829
Busy Call Forward 831
No Answer Call Forward 834
Call Conference 837

Index 843

Product Overview

This chapter contains the following information about IP phones:

- SIP IP Phone Models
- Expansion Modules

SIP IP Phone Models

This section introduces SIP-T58V/A, SIP-T56A and CP960 IP phone models. These IP phones are endpoints in the overall network topology, which are designed to interoperate with other compatible equipments including application servers, media servers, internet-working gateways, voice bridges, and other endpoints. These IP phones are characterized by a large number of functions, which simplify business communication with a high standard of security and can work seamlessly with a large number of SIP PBXs.

These IP phones provide a powerful and flexible IP communication solution for Ethernet TCP/IP networks, delivering excellent voice quality. The high-resolution graphic display supplies content in multiple languages for system status, call log and directory access. IP phones also support advanced functionalities, including LDAP, Busy Lamp Field, Sever Redundancy and Network Conference.

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 Key Features of IP Phones on page 4.

Physical Features of IP Phones

This section lists the available physical features of SIP-T58V/A, SIP-T56A and CP960 IP phones.

SIP-T58V/A

SIP-T58V

SIP-T58A

Physical Features:

- 7" 1024 x 600 pixel color touch screen with backlight
- Operating System: Android™ 5.1.1
- 16 VoIP accounts
- HD Voice: HD Codec, HD Handset, HD Speaker
- 20 dedicated hard keys, 3 dedicated soft Android keys for BACK, HOME and RECENT
- 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
- 1*USB2.0 port (on the top of the phone), support Yealink USB camera CAM50
- 1*USB2.0 port (on the rear of the phone), support expansion module EXP50, USB flash drive or USB headset
- Built-in Wi-Fi, support 802.11b/g/n
- Built-in Bluetooth 4.0, support Bluetooth headset
- Power over Ethernet (IEEE 802.3af)
- Wall Mountable

SIP-T56A

Physical Features:

- 7" 1024 x 600 pixel color touch screen with backlight
- Operating System: Android™ 5.1.1
- 16 VoIP accounts
- HD Voice: HD Codec, HD Handset, HD Speaker
- 20 dedicated hard keys, 3 dedicated soft Android keys for BACK, HOME and RECENT
- 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
- 1*USB2.0 port, support expansion module EXP50, USB flash drive or USB headset
- Built-in Wi-Fi, support 802.11b/g/n
- Built-in Bluetooth 4.0, support Bluetooth headset
- Power over Ethernet (IEEE 802.3af)
- Wall Mountable

CP960

Physical Features:

- 5" 720 x 1280 pixel color touch screen with backlight
- Operating System: Android™ 5.1.1
- One VoIP accounts
- HD Voice: HD Codec
- 5 Touch keys
- 1*RJ45 10/100Mbps Ethernet ports
- 2*EX mic ports
- 2*USB2.0 ports, support USB flash drive, wireless mic charging cradle
- 1*3.5mm audio-out port, support external speaker
- 1*Micro USB port, support PC
- 2 LED indicators
- Security lock port
- Built-in Wi-Fi, support 802.11b/g/n
- Built-in Bluetooth 4.0, support Bluetooth-enabled mobile phone
- Power over Ethernet (IEEE 802.3af)

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**: emergency call, call waiting, call hold, call mute, call forward, call

transfer, call pickup, five-way audio-only conference, five-way audio-only and video mixed conference (up to three-way video conference, only applicable to SIP-T58V/A IP phones).

- **Basic Features:** DND, auto redial, live dialpad, dial plan, hotline, caller identity, auto answer.
- **Advanced Features:** BLF, server redundancy, distinctive ring tones, remote phone book, LDAP.

- **Codecs and Voice Features**
  - Wideband codec: G.722, Opus
  - Narrowband codec: G.711, G.726, G.729, iLBC, G.723
  - VAD, CNG, AEC, PLC, AJB, AGC
  - Full-duplex speakerphone with AEC
  - Built in microphone array, 360 degree voice pickup (only applicable to CP960 IP phones)
- **Video Features (only applicable to SIP-T58V/A IP phones)**
  - Video codec: H264HP, H264, VP8
  - Image codec: JPEG, PNG, BMP
  - Adaptive bandwidth adjustment
- **Network Features**
  - SIP v1 (RFC 2543), v2 (RFC 3261)
  - NAT Traversal: STUN mode
  - DTMF: INBAND, RFC 2833, SIP INFO
  - Proxy mode and peer-to-peer SIP link mode
  - IP assignment: Static/DHCP/PPPoE
  - VLAN assignment: LLDP/Static/DHCP/CDP
  - Bridge mode for PC port (not applicable to CP960 IP phones)
  - HTTP/HTTPS server
  - DNS client
  - NAT/DHCP server
  - IPv6 support
  - Wi-Fi
- **Management**
  - FTP/TFTP/HTTP/PnP auto-provision
  - Configuration: browser/phone/auto-provision
  - Direct IP call without SIP proxy
  - Dial number via SIP server
  - Dial URL via SIP server

- TR-069

- **Security**
  - HTTPS (server/client)
  - SRTP (RFC 3711)
  - 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 Modules

This section introduces EXP50 expansion modules. The expansion modules are consoles you can connect to Yealink IP phones to add DSS keys, which can be used to assign predefined functionalities for quickly accessing features. If you want to configure the expansion module keys, you have to connect the expansion module(s) to the IP phone in advance.

Expansion modules enable you to handle large volume of calls on a regular basis and expand the functional capability of your IP phone. For more information on how to connect and use the expansion module, refer to *Yealink EXP50 User Guide*.

The following lists the available physical features of the currently supported expansion modules:

EXP50

Physical Features:

- Rich visual experience with 4.3" 272 x 480 pixel color screen
- 20 physical keys each with a dual-color LED

- 3 physical page keys
- Support up to 3 modules daisy-chain
- Only one expansion module is powered by the host phone
- 1*Mini USB port and 1*USB2.0 port for data in and out

Getting Started

This chapter describes where Yealink IP phones fit in your network and provides basic installation instructions of SIP-T58V/T58A/T56A/CP960 IP phones.

This chapter provides the following sections:

- What IP Phones Need to Meet
- Yealink IP Phones in a Network
- Connecting the IP Phones
- Initialization Process Overview
- Verifying Startup

What IP Phones Need to Meet

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

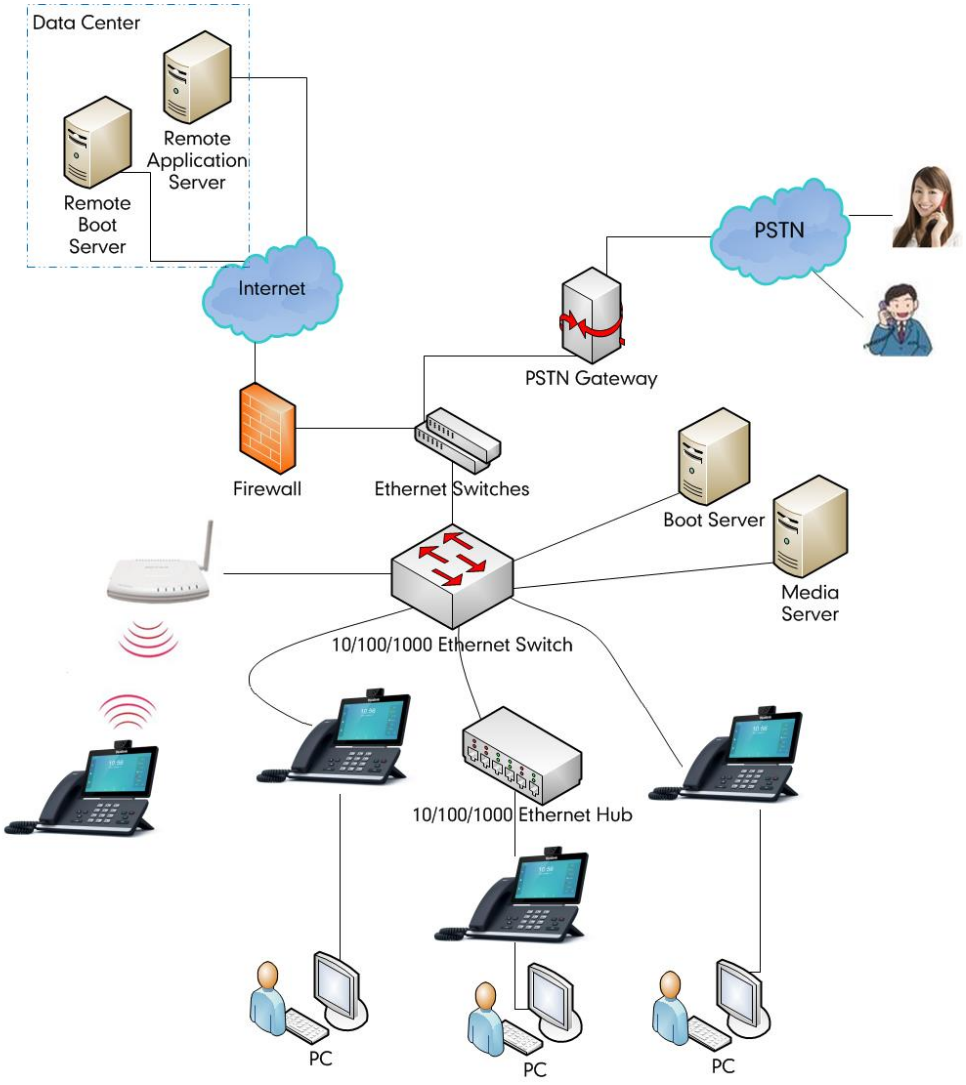
- A working IP network is established.
- VoIP gateways are configured for SIP.
- The latest (or compatible) firmware of IP phones is available.
- A call server is active and configured to receive and send SIP messages.

Yealink IP Phones in a Network

Yealink IP phones can connect physically through a Category 5E (CAT 5E) cable to a Ethernet LAN, and send and receive all data using the same packet-based technology. They can also connect to the wireless network.

Since the IP phone is a data terminal, digitized audio being just another type of data from its perspective, the phone is capable of vastly more than traditional business phones. Moreover, Yealink IP phones run the same protocols as your office personal computer, which means that many innovative applications can be developed without resorting to specialized technology.

There are many ways to set up a phone network using Yealink IP phones. The following shows an example of a network setup:



Connecting the IP Phones

This section introduces how to install SIP-T58V/T58A/T56A/CP960 IP phones with components in packaging contents.

1. Insert the camera (only applicable to SIP-T58V/A IP phones)
2. Attach the stand and the optional wall mount bracket (not applicable to CP960 IP phones)
3. Adjust the angle of touch screen (only applicable to SIP-T58V/A IP phones)
4. Connect the handset and optional headset (not applicable to CP960 IP phones)
5. Connect the power and network
6. Connect the optional USB flash drive
7. Connect the wired expansion MIC CPE90 (only applicable to CP960 IP phones)
8. Connect the optional PC using a micro USB cable (only applicable to CP960 IP phones)

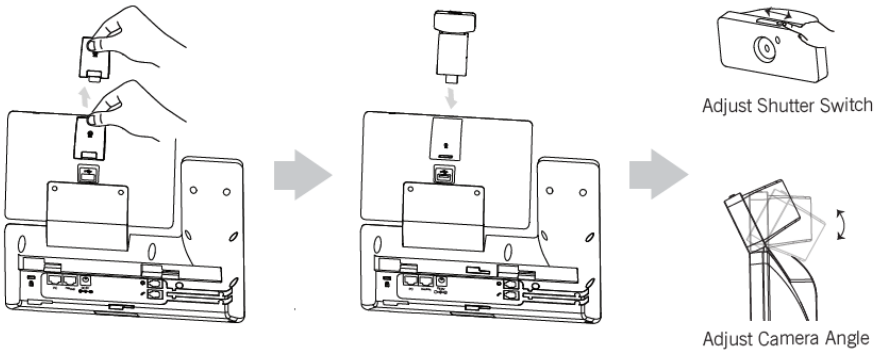
9. Connect the optional external speaker (only applicable to CP960 IP phones)

Note The optional accessories are not included in packaging contents. You need to purchase them separately if required.

Inserting the Camera (only applicable to SIP-T58V/A IP phones)

To insert the camera:

For SIP-T58V/A:

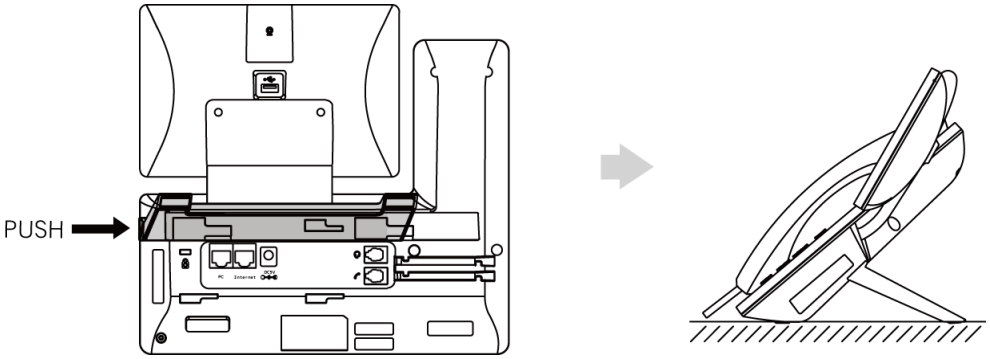


Note The camera is connected to the USB port on the top of the phone. And the IP phone only supports the Yealink original USB camera CAM50. You should purchase it separately for SIP-T58A smart media phone.

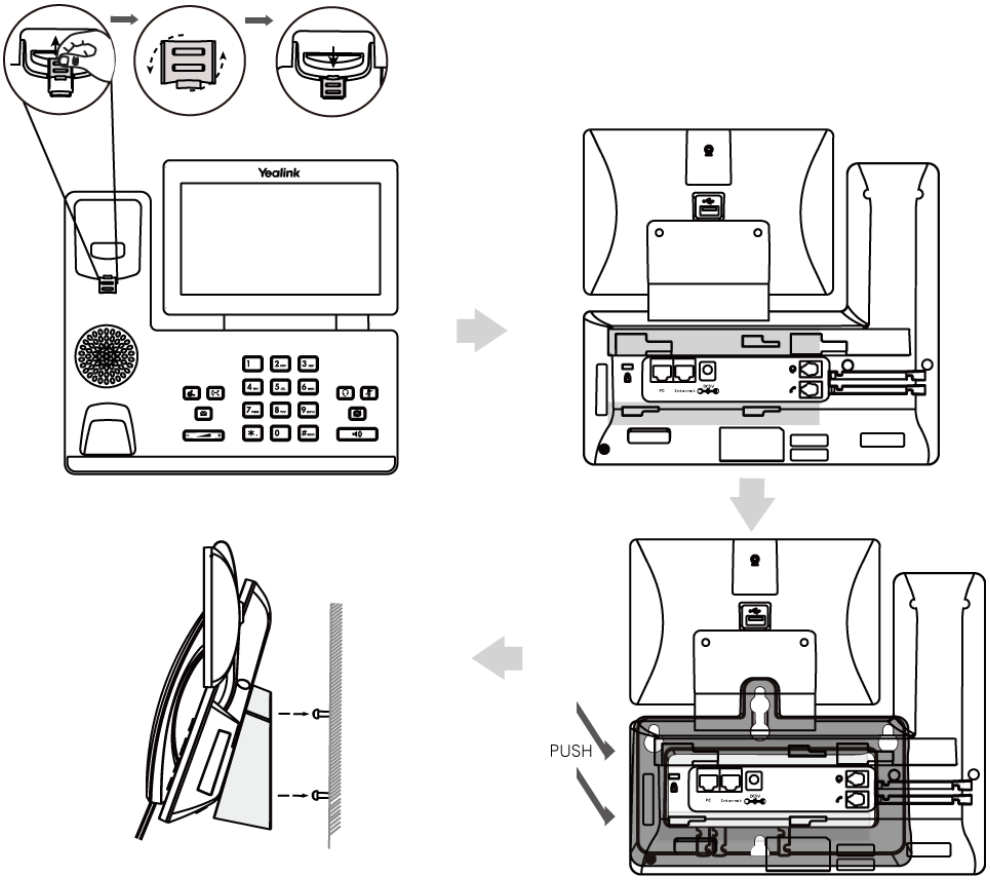
Attaching the Stand and the Optional Wall Mount Bracket (not applicable to CP960 IP phones)

To attach the stand and the optional wall mount bracket:

For SIP-T58V/A:

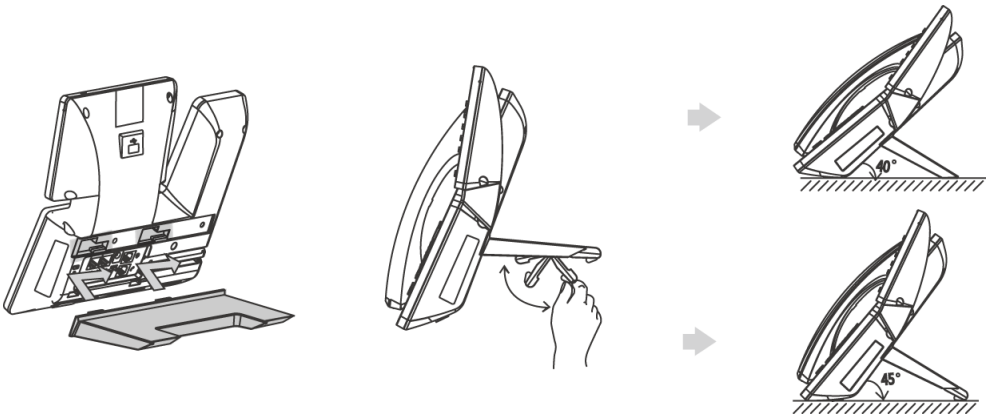


Desk Mount Method

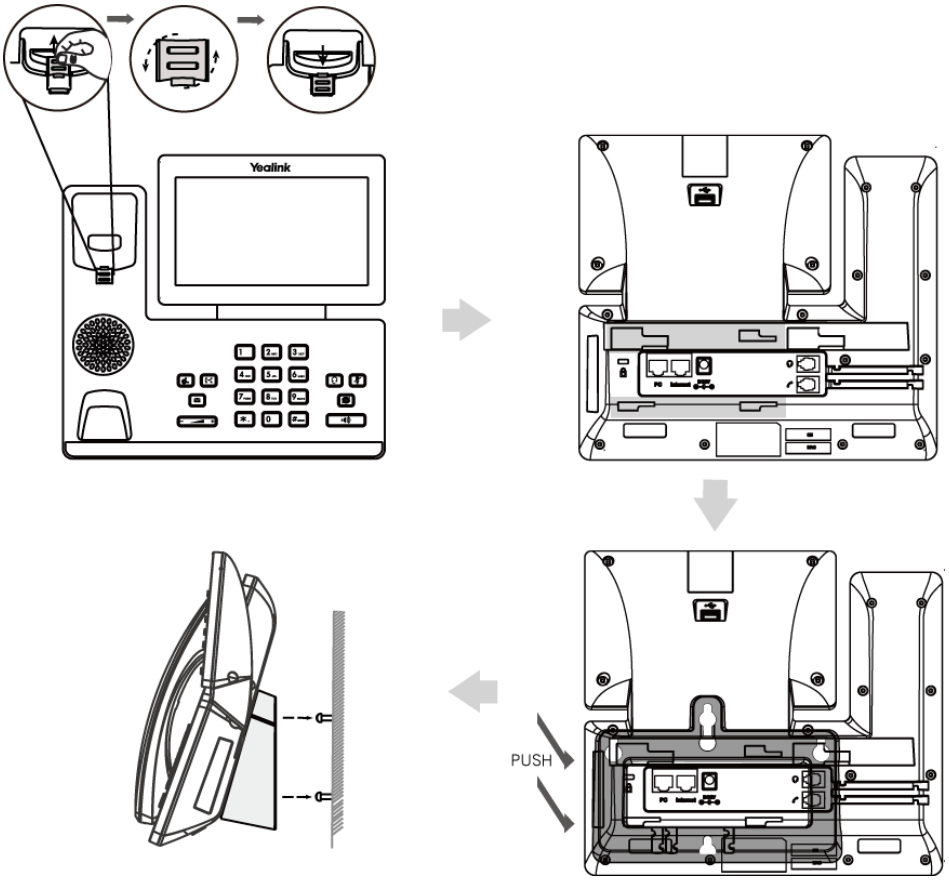


Wall Mount Method (Optional)

For SIP-T56A:



Desk Mount Method



Wall Mount Method (Optional)

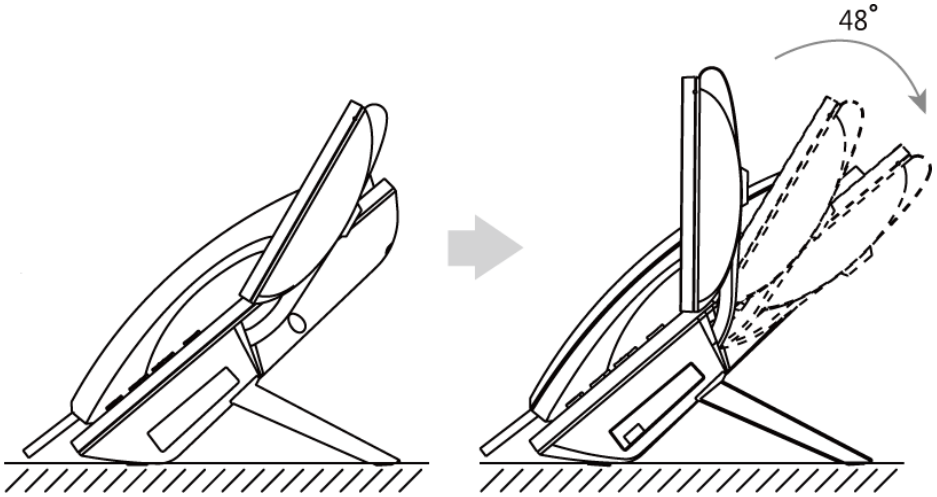
Note The reversible tab has a lip which allows the handset to stay on-hook when the IP phone is mounted vertically.

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

Adjust the angle of touch screen (only applicable to SIP-T58V/A IP phones)

To adjust the angle of touch screen:

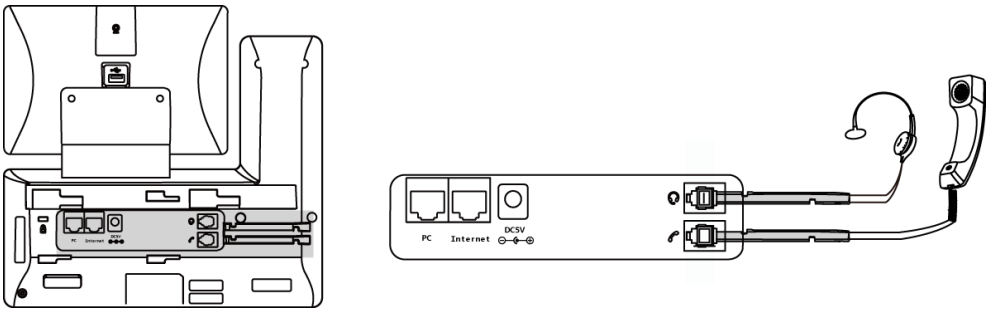
For SIP-T58V/A:



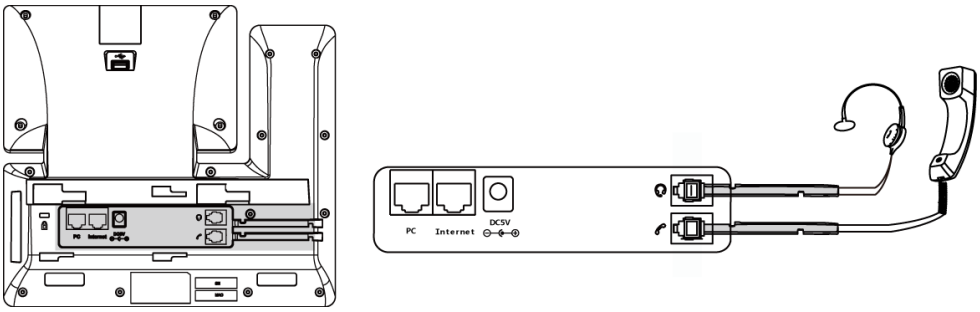
Connecting the Handset and Optional Headset (not applicable to CP960 IP phones)

To connect the handset and optional headset:

For SIP-T58V/A:



For SIP-T56A:



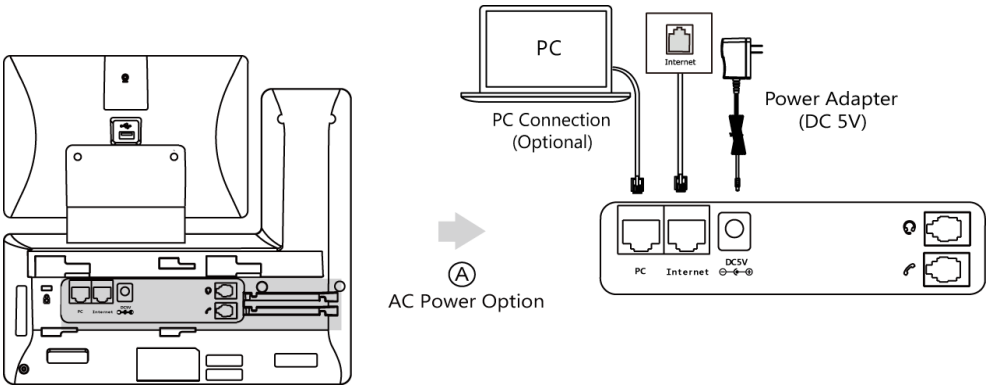
Connecting the Power and Network

AC Power (Optional)

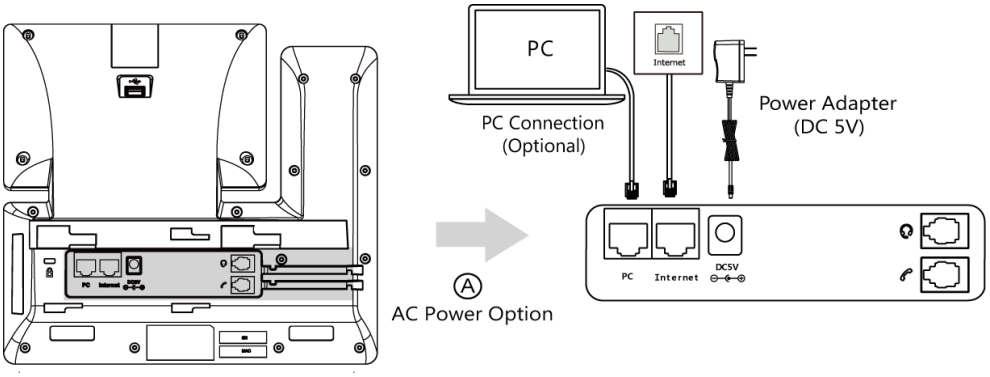
To connect the AC power and network (not applicable to CP960 IP phones):

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 Ethernet cable between the Internet port on the IP phone and the one on the wall or switch/hub device port.

For SIP-T58V/A:



For SIP-T56A:



Note You can also connect the IP phone to a wireless network according to your office environment. For more information, refer to *Yealink phone-specific user guide*.

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.

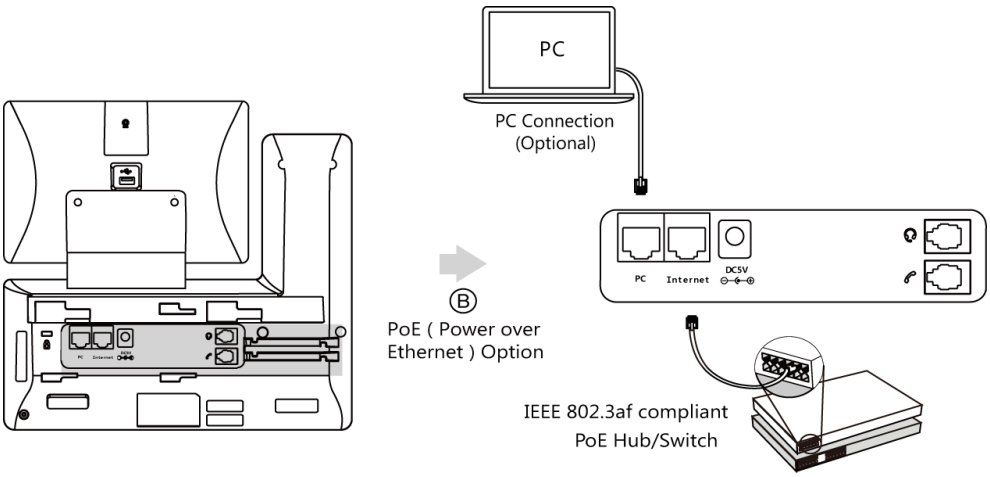
Power over Ethernet (PoE)

With the included Ethernet cable, SIP-T58V/T58A/T56A IP phones can be powered from a PoE-compliant switch or hub. CP960 IP phones can only be powered from a PoE adapter.

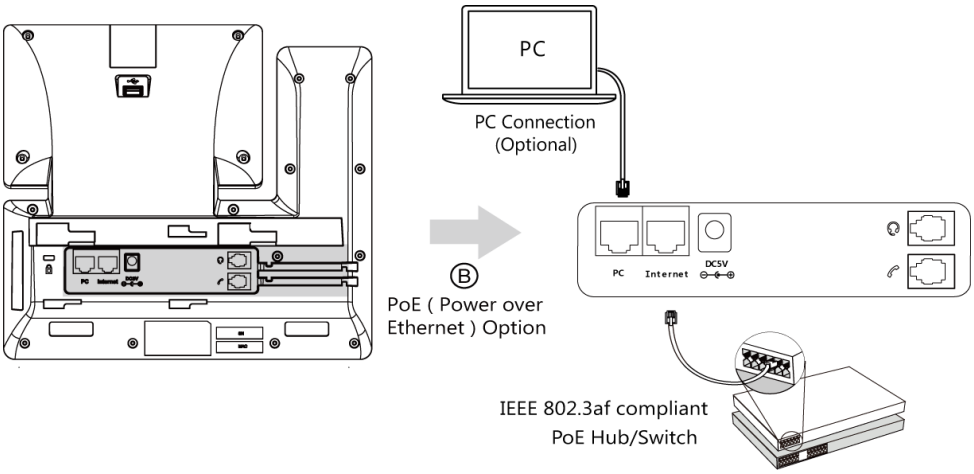
To connect the PoE (for SIP-T58V/T58A/T56A IP phones):

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

For SIP-T58V/A:



For SIP-T56A:



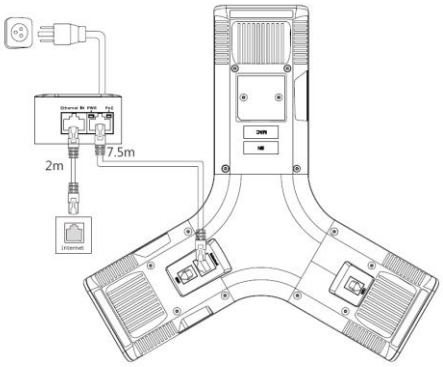
To connect the PoE adapter (for CP960 IP phones):

1) Connect the Ethernet cable between the Internet port on the IP phone and Data & Power Out port on the PoE adapter.

2) Connect the Ethernet cable between the Data In port on the PoE adapter and the one on the wall or switch/hub device port.

3) Connect the power plug of the PoE adapter into an electrical power outlet.

For CP960:



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.

SIP-T58V/T58A/T56A IP phones can also share the network with another network device such as a PC (personal computer). It is an optional connection. We recommend that you use the Ethernet cable provided by Yealink.

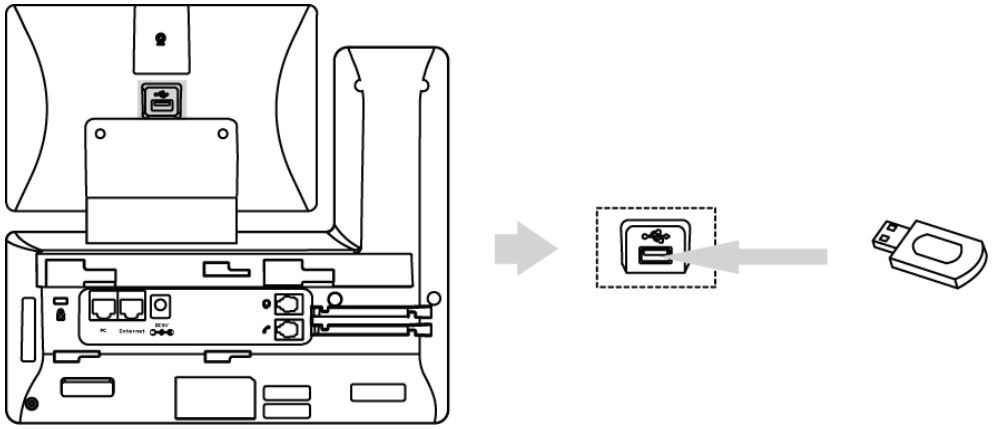
Important! Do not unplug or remove the power while the IP phone is updating firmware and configurations.

Connecting the Optional USB Flash Drive

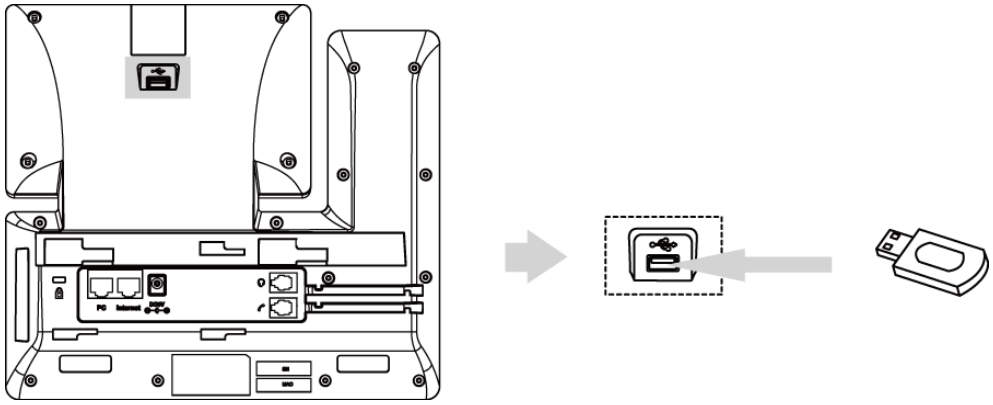
To connect a USB flash drive:

1) Insert a USB flash drive into the USB port on the phone.

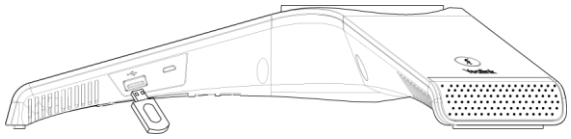
For SIP-T58V/A:



For SIP-T56A:



For CP960:



Note

For SIP-T58V/T58A/T56A, the USB port (on the rear of the phone) can also be used to connect color-screen expansion module EXP50 or USB headset. The IP phone officially supports certain USB headset models. For more information, refer to *Tested headset list compatible with Yealink IP Phone*.

For more information on how to use EXP50, refer to *Yealink EXP50 User Guide*. For more information on how to use USB headset, refer to the documentation from the manufacturer.

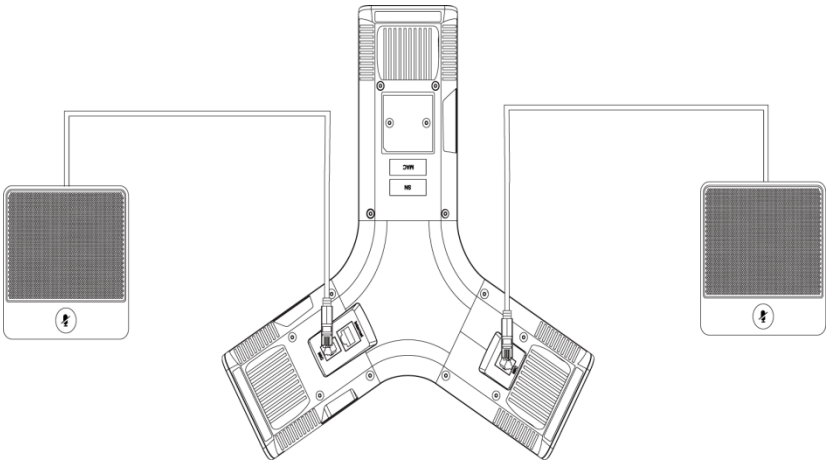
For CP960, the USB port can also be used to connect wireless mic charging cradle to charge the wireless mic CPW90. For more information, refer to *Yealink CP960 User Guide*.

Connecting the Wired Expansion MIC CPE90 (Only Applicable to CP960 IP Phones)

You can connect optional wired expansion MIC CPE90 to enhance the room coverage of the conference phone.

To connect the wired expansion MIC CPE90:

1) Connect the free end of the optional CPE90 cable to one of the MIC ports on the IP phone.

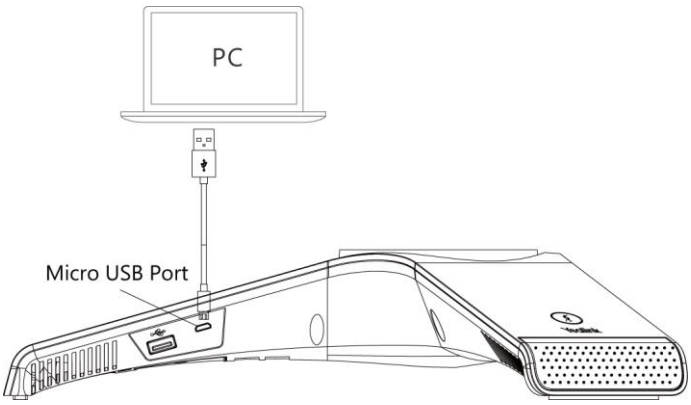


Connecting the Optional PC using a Micro USB Cable (Only Applicable to CP960 IP Phones)

You can connect a PC to listen to the PC audio using your CP960 IP phone.

To connect a PC:

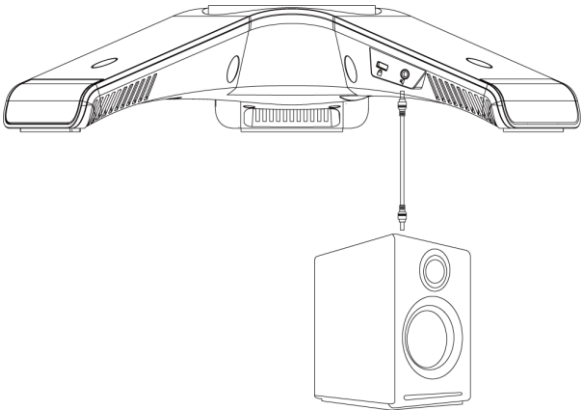
1. Connect the micro USB port of the IP phone and the USB port of the PC using a micro USB cable.



Connecting the Optional External Speaker (Only Applicable to CP960 IP Phones)

To connect an optional external speaker:

1. Connect the 3.5mm audio-out port of the IP phone to the external speaker using a 3.5mm jack cable.



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). For more information on VLAN, refer to VLAN on page 53.

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 32.

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. For more information, refer to Setting Up Your Phones with a Provisioning Server on page 110.

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.

You can manually upgrade firmware if the IP phone does not download firmware from the provisioning server. For more information, refer to Upgrading Firmware on page 124.

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
- Contact files

For more information on resource files, refer to Resource Files on page 118.

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/mute indicator LED illuminates solid red.
2. The message “Welcome Initializing... Please wait” appears on the touch screen when the IP phone starts up.

3. The main touch screen displays the following:
   - Time and date
   - Android keys (for SIP-T58V/T58A/T56A)
   - Pre-installed applications (for CP960)
4. Tap **Settings**->**Status** to check the IP phone status, the touch 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.

Setting Up Your System

This section describes essential information on how to set up your phone network and set up your phones with a provisioning server. It also provides instructions on how to set up a provisioning server, how to deploy Yealink IP phones from the provisioning server, how to upgrade firmware, and how to keep user personalized settings after auto provisioning.

This chapter provides the following sections:

- Setting Up Your Phone Network
- Setting Up Your Phones with a Provisioning Server

Setting Up Your Phone Network

Yealink IP phones operate on an Ethernet local area network (LAN) or wireless network. Local area network design varies by organization and Yealink IP phones can be configured to accommodate a number of network designs.

In order to get your IP phones running, you must perform basic network setup, such as IP address and subnet mask configuration. You can configure the IPv4 or IPv6 network parameters for the phone. You can also configure the appropriate security (VLAN and/or 802.1X authentication) and Quality of Service (QoS) settings for the IP phone.

This chapter describes how to configure all the network parameters for IP phones, and it provides the following sections:

- DHCP
- DHCP Option
- Configuring Network Parameters Manually
- PPPoE
- Configuring Transmission Methods of the Internet Port and PC Port
- Configuring PC Port Mode
- Web Server Type
- Wi-Fi
- VLAN
- IPv6 Support
- VPN
- Configuring the IP Phone for Use with a Firewall or NAT
- Quality of Service (QoS)
- 802.1X Authentication

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 following methods.

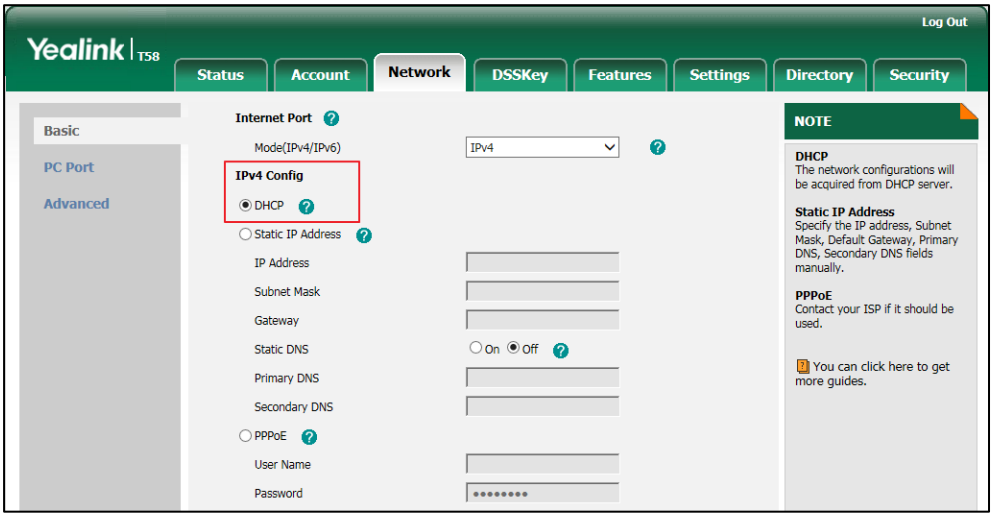
Central Provisioning (Configuration File)	<MAC>.cfg	Configure DHCP on the IP phone. **Parameter:** static.network.internet_port.type
Web User Interface		Configure DHCP on the IP phone. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=network&q=load
Phone User Interface		Configure DHCP on the IP phone.

Details of Configuration Parameter:

Parameter	Permitted Values	Default
static.network.internet_port.type	**0, 1 or 2**	**0**
Description: Configures the Internet port type for IPv4. **0**-DHCP **1**-PPPoE **2**-Static IP Address **Note**: It works only if the value of the parameter "static.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:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type		

To configure DHCP via web user interface:

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



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

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

To configure DHCP via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**WAN Port**->**IPv4**.
2. Tap the **Type** field.
3. Tap **DHCP** in the pop-up dialog box.
4. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.
5. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

Static DNS

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

Procedure

Static DNS can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the static DNS feature. **Parameter:** static.network.static_dns_enable
	<MAC>.cfg	Configure static DNS address.

		Parameters: static.network.primary_dns static.network.secondary_dns
Web User Interface		Configure the static DNS feature**.** Configure static DNS address. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=network&q=load
Phone User Interface		Configure the static DNS feature**.** Configure static DNS address.

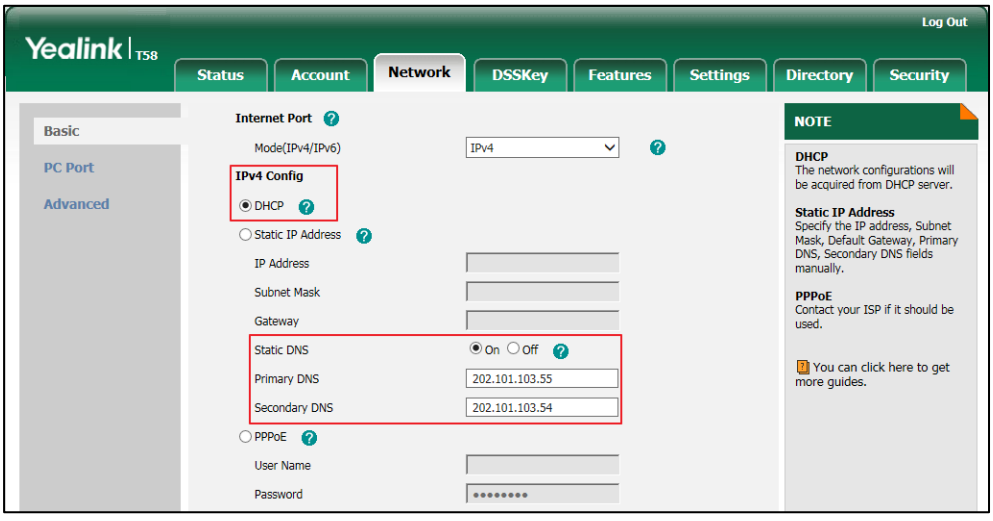
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.static_dns_enable	**0 or 1**	**0**
Description: Triggers the static DNS feature to on or off. **0**-Off **1**-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. **Note**: It works only if the value of the parameter "static.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 **Phone User Interface:** Settings->Advanced (default password: admin)->Network->WAN Port->IPv4->Type (DHCP)->Static DNS		
static.network.primary_dns	**IPv4 Address**	**Blank**
Description: Configures the primary IPv4 DNS server. **Example:** static.network.primary_dns = 202.101.103.55 **Note**: It works only if the value of the parameter "static.network.static_dns_enable" is set to 1		

Parameters	Permitted Values	Default
(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->Primary DNS **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Static DNS (Enabled) ->Primary DNS		
static.network.secondary_dns	**IPv4 Address**	**Blank**
Description: Configures the secondary IPv4 DNS server. **Example:** static.network.secondary_dns = 202.101.103.54 **Note**: It works only if the value of the parameter "static.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:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->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.



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 phone.

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

1. Tap **Settings->Advanced** (default password: admin) ->**Network**->**WAN Port**->**IPv4**.
2. Tap the **Type** field.
3. Tap **DHCP** in the pop-up dialog box.
4. Tap the **Static DNS** field.
5. Tap **Enabled** in the pop-up dialog box.
6. Enter the desired value in the **Primary DNS** and **Secondary DNS** field respectively.
7. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.

8. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

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.
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.

Parameter	DHCP Option	Description
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 Information	43	Identify the vendor-specific information.
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.

For more information on DHCP options, refer to RFC 2131 or RFC 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 RFC 3925. If a single alternate DHCP server responds, this is functionally equivalent to the scenario where the primary DHCP server responds with a valid provisioning server address. If no DHCP servers respond, the INFORM query process will retry and eventually time out.

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 and option 43 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.

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

Procedure

DHCP active can be configured using the following methods.

Central Provisioning	<y0000000000xx>.c	Configure DHCP active.

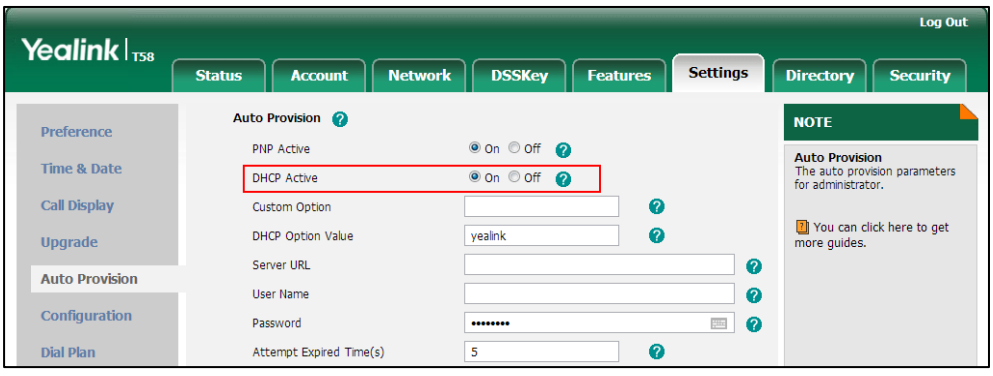
(Configuration File)	fg	**Parameter:** static.auto_provision.dhcp_option.enable
Web User Interface		Configure DHCP active. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-autop&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
static.auto_provision.dhcp_option.enable	**0 or 1**	**1**
Description: Triggers the DHCP active feature to on or off. **0**-Off **1**-On 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 **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.



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 web path **Settings**->**Time & Date**->**DHCP Time**. For more information on how to configure DHCP time feature, refer to NTP Time Server on page 189.

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the DHCP option 12 hostname. **Parameter:** static.network.dhcp_host_name
Web User Interface		Configure the DHCP option 12 hostname. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

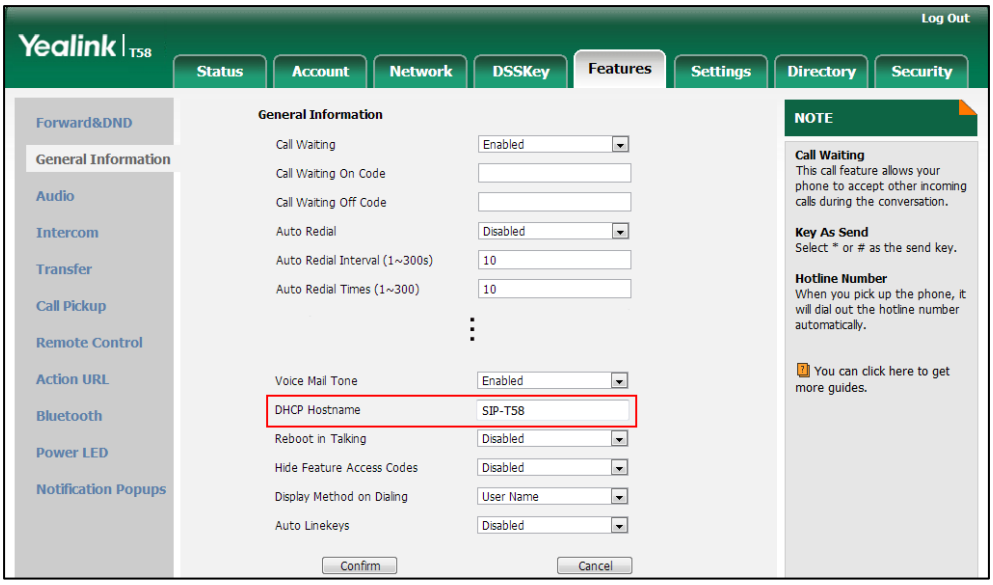
Details of Configuration Parameter:

Parameter	Permitted Values	Default
static.network.dhcp_host_name	**String within 99 characters**	**Refer to the following content**
Description: Configures the DHCP option 12 hostname on the IP phone. **For SIP-T58V/A IP phones**: The default value is SIP-T58. **For SIP-T56A IP phones**: The default value is SIP-T56A. **For CP960 IP phones**: The default value is SIP-CP960. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Features->General Information->DHCP Hostname		

Parameter	Permitted Values	Default
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** field.



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

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

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

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 following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure network parameters of the IP phone manually. **Parameters:** static.network.internet_port.type static.network.ip_address_mode static.network.internet_port.ip static.network.internet_port.mask static.network.internet_port.gateway static.network.primary_dns static.network.secondary_dns
Web User Interface		Configure network parameters of the IP phone manually. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network&q=load
Phone User Interface		Configure network parameters of the IP phone manually.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.internet_port.type	**0, 1 or 2**	**0**
Description: Configures the Internet port type for IPv4. **0**-DHCP **1**-PPPoE **2**-Static IP Address **Note**: It works only if the value of the parameter "static.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:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type		

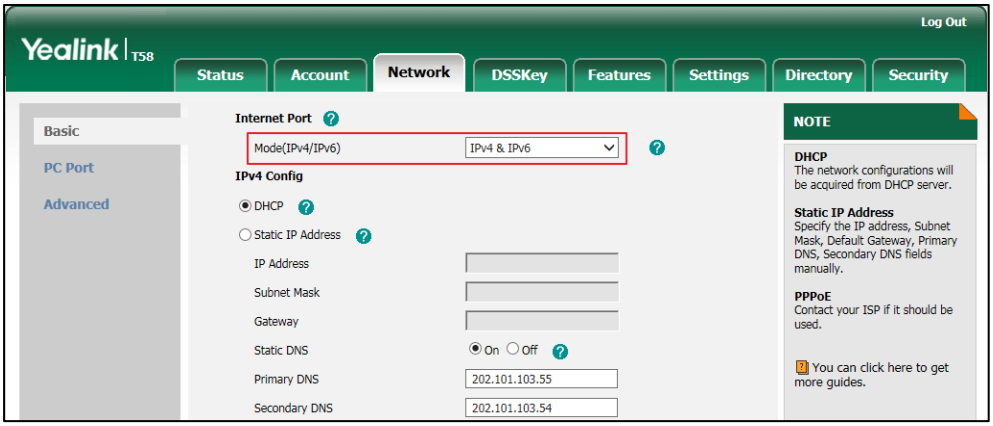
Parameters	Permitted Values	Default
static.network.ip_address_mode	**0, 1 or 2**	**0**
Description: Configures the IP address mode. **0**-IPv4 **1**-IPv6 **2**-IPv4 & IPv6 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->Internet Port->Mode(IPv4/IPv6) **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IP Mode		
static.network.internet_port.ip	**IPv4 Address**	**Blank**
Description: Configures the IPv4 address. **Example:** static.network.internet_port.ip = 192.168.1.20 **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.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:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type (Static IP) ->IP Address		
static.network.internet_port.mask	**Subnet Mask**	**Blank**
Description: Configures the IPv4 subnet mask. **Example:** static.network.internet_port.mask = 255.255.255.0 **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.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:**		

Parameters	Permitted Values	Default
Network->Basic->IPv4 Config->Static IP Address->Subnet Mask **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type (Static IP) ->Subnet Mask		
static.network.internet_port.gateway	**IPv4 Address**	**Blank**
Description: Configures the IPv4 default gateway. **Example:** static.network.internet_port.gateway = 192.168.1.254 **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.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:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type (Static IP) ->Gateway		
static.network.primary_dns	**IPv4 Address**	**Blank**
Description: Configures the primary IPv4 DNS server. **Example:** static.network.primary_dns = 202.101.103.55 **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.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->Primary DNS **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type (Static IP) ->Primary DNS		
static.network.secondary_dns	**IPv4 Address**	**Blank**
Description: Configures the secondary IPv4 DNS server.		

Parameters	Permitted Values	Default
Example: static.network.secondary_dns = 202.101.103.54 **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.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:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type (Static IP) ->Secondary DNS		

To configure the IP address mode via web user interface:

1. Click on **Network**->**Basic**.
2. Select desired value **Mode(IPv4/IPv6)**.



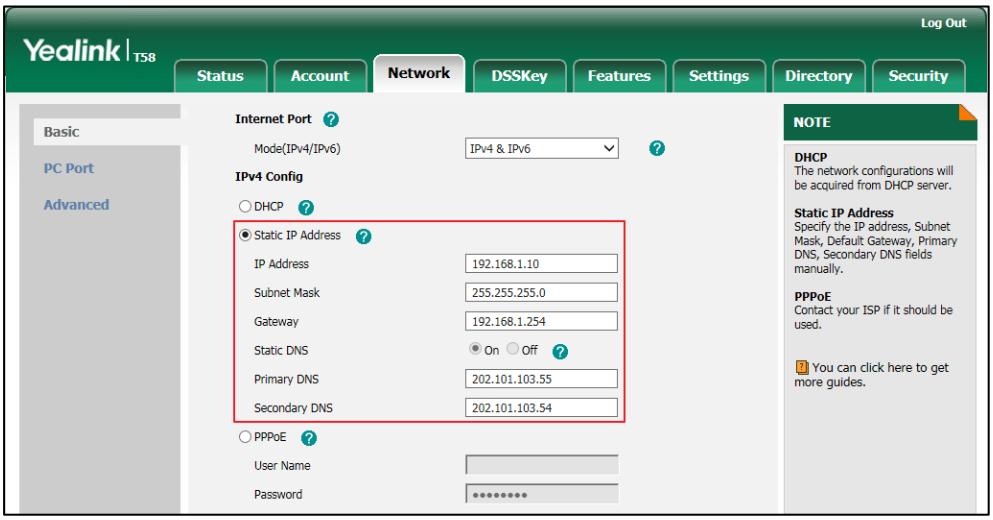
3. Click **Confirm** to accept the change.

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

To configure a static IPv4 address via web user interface:

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



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 phone.

To configure the IP address mode via phone user interface:

1. Tap **Settings->Advanced** (default password: admin) ->**Network**->**WAN Port**.
2. Tap the **Type** field.
3. Tap **IPv4** or **IPv4 and IPv6** in the pop-up dialog box.
4. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.

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

   The settings will take effect after a reboot.

To configure a static IPv4 address via phone user interface:

1. Tap **Settings->Advanced** (default password: admin) ->**Network**->**WAN Port**->**IPv4**.
2. Tap the **Type** field.
3. Tap **Static IP** in the pop-up dialog box.
4. Enter the desired value in the **IP Address**, **Subnet Mask**, **Gateway**, **Primary DNS** and **Secondary DNS** field respectively.
5. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.

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

   The settings will take effect after a reboot.

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.

Procedure

PPPoE can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure PPPoE on the IP phone. **Parameter:** static.network.internet_port.type
	<y0000000000xx>.cfg	Configure the user name and password for PPPoE on the IP phone. **Parameters:** static.network.pppoe.user static.network.pppoe.password
Web User Interface		Configure PPPoE on the IP phone. Configure the user name and password for PPPoE on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&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.

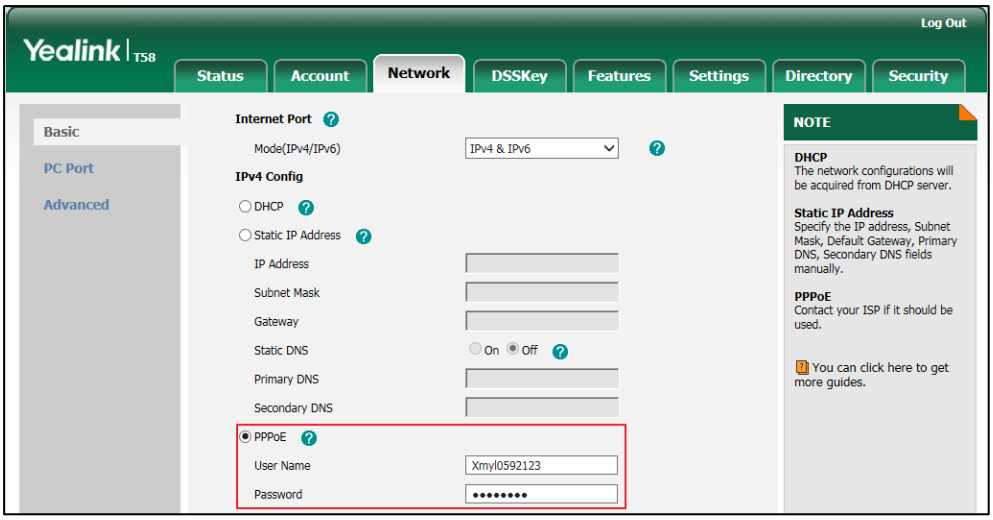
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.internet_port.type	**0, 1 or 2**	**0**
Description: Configures the Internet port type for IPv4. **0**-DHCP **1**-PPPoE **2**-Static IP Address		

Parameters	Permitted Values	Default
Note: It works only if the value of the parameter "static.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:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type		
static.network.pppoe.user	**String within 32 characters**	**Blank**
Description: Configures the user name for PPPoE connection. **Example:** static.network.pppoe.user = Xmyl0592123 **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.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. **Web User Interface:** Network->Basic->IPv4 Config->PPPoE->User Name **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type (PPPoE) ->PPPoE User		
static.network.pppoe.password	**String within 99 characters**	**Blank**
Description: Configures the password for PPPoE connection. **Example:** static.network.pppoe.password = yealink123 **Note**: It works only if the value of the parameter "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6), and "static.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. **Web User Interface:** Network->Basic->IPv4 Config->PPPoE->Password **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv4->Type (PPPoE) ->PPPoE Password		

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.



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 phone.

To configure PPPoE via phone user interface:

1. Tap **Settings->Advanced** (default password: admin) ->**Network**->**WAN Port**->**IPv4**.
2. Tap the **Type** field.
3. Tap **PPPoE** in the pop-up dialog box.
4. Enter the user name and password in corresponding fields.
5. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.
6. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

Configuring Transmission Methods of the Internet Port and PC Port

Yealink SIP-T58V/T58A/T56A IP phones support two Ethernet ports: Internet port and PC port. You can enable or disable the PC port on the IP phones. The CP960 IP phones have Internet port only. Three optional methods of transmission configuration for IP phone Internet port or PC port:

- Auto-negotiate

- Half-duplex
- Full-duplex

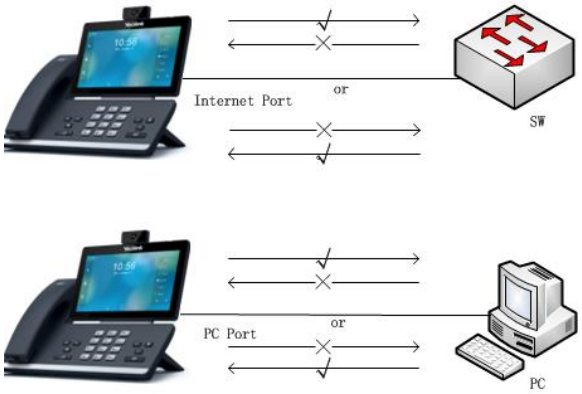
Auto-negotiate is configured for both Internet and PC ports on the IP phone by default.

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.

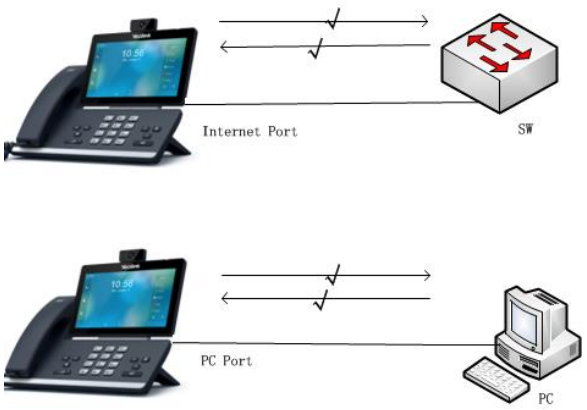
Half-duplex

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 not applicable to CP960 IP phones).



Procedure

The transmission methods of Ethernet ports can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the transmission methods of the Ethernet ports. **Parameters:** static.network.internet_port.speed_duplex static.network.pc_port.speed_duplex
Web User Interface		Configure the transmission methods of the Ethernet ports. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load

Details of Configuration Parameters:

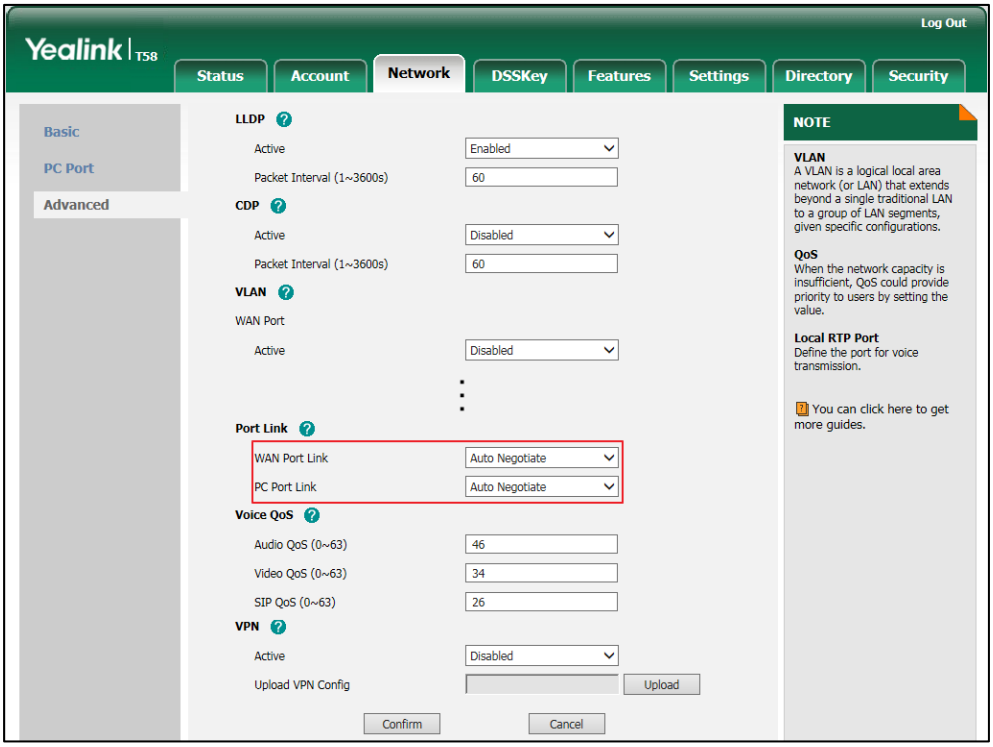
Parameters	Permitted Values	Default
static.network.internet_port.speed_duplex	**0, 1, 2, 3, 4 or 5**	**0**
Description: Configures the transmission method of the Internet port. **0**-Auto Negotiate **1**-Full Duplex 10Mbps **2**-Full Duplex 100Mbps		

Parameters	Permitted Values	Default
3-Half Duplex 10Mbps **4**-Half Duplex 100Mbps **5**-Full Duplex 1000Mbps (not applicable to CP960 IP phones) **Note**: You can set the transmission speed to 1000Mbps/Auto Negotiate to transmit in 1000Mbps if the IP phone is connected to the switch supports Gigabit Ethernet. We recommend that you do not change this parameter. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Port Link->WAN Port Link **Phone User Interface:** None		
static.network.pc_port.speed_duplex	**0, 1, 2, 3 ,4 or 5**	**0**
Description: Configures the transmission method of the PC port. **0**-Auto Negotiate **1**-Full Duplex 10Mbps **2**-Full Duplex 100Mbps **3**-Half Duplex 10Mbps **4**-Half Duplex 100Mbps **5**-Full Duplex 1000Mbps **Note**: It works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiate). It is not applicable to CP960 IP phones. You can set the transmission speed to 1000Mbps/Auto Negotiate to transmit in 1000Mbps if the IP phone is connected to the switch supports Gigabit Ethernet. We recommend that you do not change this parameter. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Port Link->PC Port Link **Phone User Interface:** 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**.



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 phone.

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 port on the IP phones via web user interface or using configuration files. PC port is not applicable to CP960 IP phones.

Procedure

PC port can be configured using the following methods.

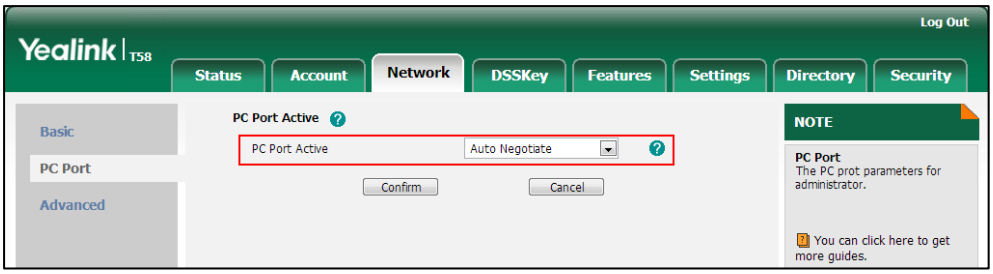
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the PC port. **Parameter:** static.network.pc_port.enable
Web User Interface		Configure the PC port. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-pcport&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
static.network.pc_port.enable	**0 or 1**	**1**
Description: Enables or disables the PC port. **0**-Disabled **1**-Auto Negotiate **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. It is not applicable to CP960 IP phones. **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**.



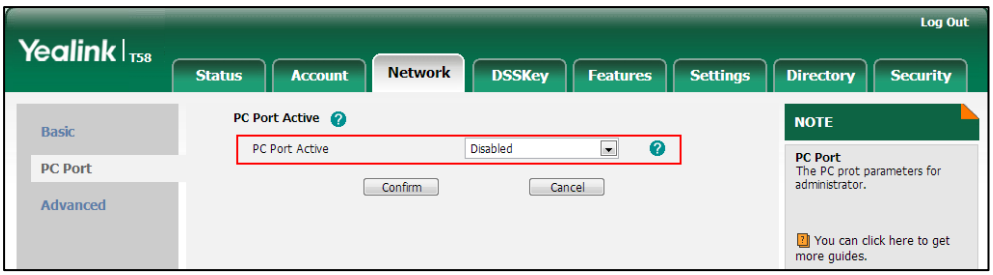
3. Click **Confirm** to accept the change.

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

To 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**.



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

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

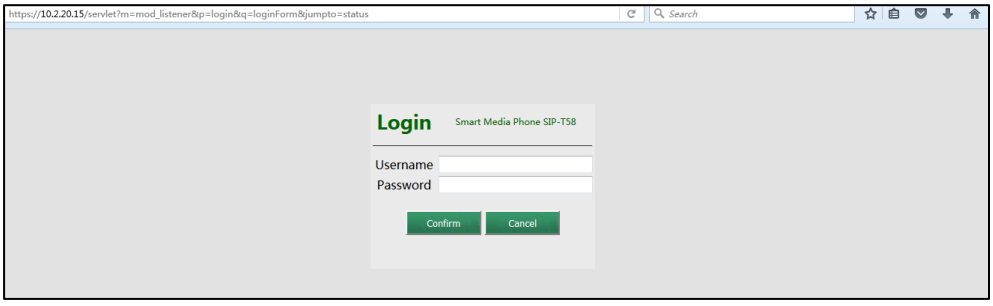
4. Click **OK** to reboot the phone.

Web Server Type

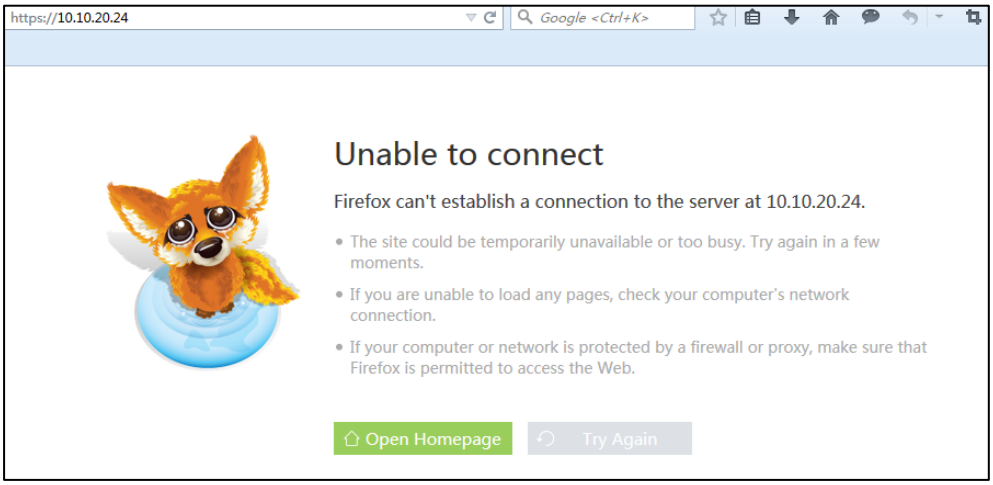
Users can configure the user or administrator features of the phone via web user interface. Web server type determines access protocol of the IP phone's web user interface. IP phones support both HTTP and HTTPS protocols for accessing the web user interface through a web browser such as Microsoft's IE, Mozilla Firefox, Google Chrome and etc. This can be disabled when it is not needed or when it poses a security threat. For more information on accessing the web user interface, refer to Web User Interface on page 113.

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.

When you enable user to access web user interface of the IP phone using the HTTP/HTTPS protocol (take HTTPS protocol for example):



When you disable user to access web user interface of the IP phone using the HTTP/HTTPS protocol (take HTTPS protocol for example):



Procedure

Web server type can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the web access type, HTTP port and HTTPS port. **Parameters:** static.wui.http_enable static.network.port.http static.wui.https_enable static.network.port.https
Web User Interface		Configure the web access type, HTTP port and HTTPS port. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load
Phone User Interface		Configure the web access type, HTTP port and HTTPS port.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.wui.http_enable	**0 or 1**	**1**

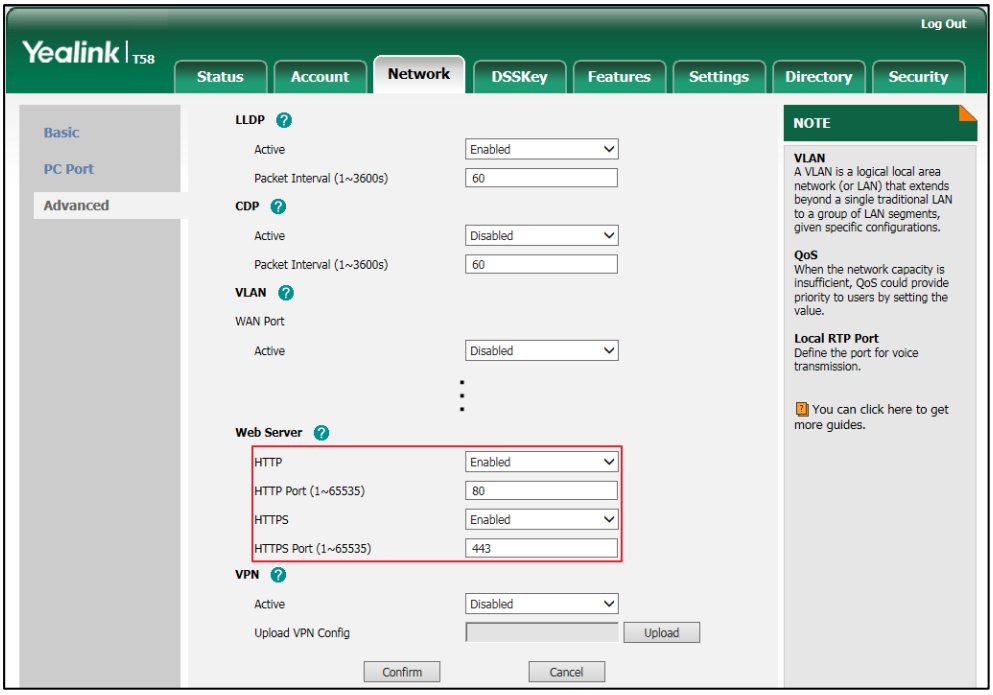
Parameters	Permitted Values	Default
Description: Enables or disables the user to access web user interface of the IP phone using the HTTP protocol. **0**-Disabled **1**-Enabled **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTP **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->Webserver Type->HTTP Status		
static.network.port.http	**Integer from 1 to 65535**	**80**
Description: Configures the HTTP port for the user to access web user interface of the IP phone using the HTTP protocol. **Note**: Please take care when choosing an alternate port. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Web Server->HTTP Port (1~65535) **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->Webserver Type->HTTP Port		
static.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. **0**-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:**		

Parameters	Permitted Values	Default
Settings->Advanced (default password: admin) ->Network->Webserver Type->HTTPS Status		
static.network.port.https	**Integer from 1 to 65535**	**443**
Description: Configures the HTTPS port for the user to access web user interface of the IP phone using the HTTPS protocol. **Note**: Please take care when choosing an alternate port. 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:** Settings->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**.
3. 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.



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 phone.

To configure web server type via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**Webserver Type**.
2. Tap the **HTTP Status** field.
3. Tap **Enabled** in the pop-up dialog box.
4. Enter the desired HTTP port number in the **HTTP Port** field.
5. Tap the **HTTPS Status** field.
6. Tap **Enabled** in the pop-up dialog box.
7. Enter the desired HTTPS port number in the **HTTPS Port** field.
8. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.
9. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

Wi-Fi

Wi-Fi feature enables users to connect their phones to the organization's wireless network. The wireless network is more convenient and cost-effective than wired network.

When the Wi-Fi feature is enabled, the IP phone will automatically scan the available wireless

networks. All the available wireless networks will display in scanning list on the touch screen. Yealink IP phones support connecting to 2.4G wireless network.

Note For SIP-T58V/T58A/T56A IP phones, you have to disable the Wi-Fi feature if you want to use the wired network.

The following advices you need to know when using the IP phones in the wireless network:

a) Check whether the wireless network is normal when the account registers failed or sometimes there is no sound during an active call.

b) Ensure that the bandwidth of your wireless network is able to provide stable and real-time data transmission otherwise the quality of video calls may be affected. We recommend you to use the wired network for video calls.

c) We recommend you do not use the unstable router product in your home/office environment.

d) We recommend you to set the password for the wireless network so as to ensure the network resource will not be occupied by the unknown user.

Procedure

Wi-Fi feature can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure Wi-Fi feature. **Parameter:** static.wifi.enable
Local	Phone User Interface	Configure Wi-Fi feature. Configure the Wi-Fi settings.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
static.wifi.enable	**0 or 1**	**0**
Description: Enables or disables the Wi-Fi feature. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:**		

Parameter	Permitted Values	Default
Settings->Basic->Wi-Fi->Wi-Fi		

To enable the Wi-Fi feature via phone user interface:

1. Swipe down from the top of the screen or swipe left/right to go to the second idle screen.
2. Tap **Settings**->**Basic**->**Wi-Fi**.
3. Tap the **On** radio box in the **Wi-Fi** field.

The phone will automatically search for available wireless networks in your area.

To add a wireless network:

1. Swipe down from the top of the screen or swipe left/right to go to the second idle screen.
2. Tap **Settings**->**Basic**->**Wi-Fi**.
3. Tap the **On** radio box in the **Wi-Fi** field.
4. Tap ⋮ and then tap **Add**.
5. Enter the desired value in the **Network SSID** field.
6. Tap the **Security** field.
7. Tap the desired value in the pop-up dialog box.
   - If you select **WEP** or **WPA/WPA2 PSK**:
     1) Enter the password in the **Password** field.
   - If you select **802.1x EAP**:
     1) Tap the **EAP method** field.
     2) Tap the desired EAP method in the pop-up dialog box.
     - If you select **PEAP**/**TTLS**:
       a) Tap the **Phase-2 authentication** field.
       b) Tap the desired Phase-2 authentication method in the pop-up dialog box.
       c) Enter the identity (username) in the **Identity** field.
       d) Enter the anonymous identity (username) in the **Anonymous identity** field (to be used as the unencrypted identity).
       e) Enter the password in the **Password** field.
     - If you select **TLS**:
       a) Enter the username in the **Identity** field
     - If you select **PWD**:
       a) Enter the username in the **Identity** field.
       b) Enter the password in the **Password** field.
8. You can do the following:
   - Tap the **Show password** checkbox to make the password visible.

- Tap the **Show advanced options** checkbox to configure the HTTP proxy for **Browser** application.

9. Tap **Save** to accept the change.

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*.

VLAN assignment method can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the VLAN assignment method. **Parameter:** static.network.vlan.vlan_change.enable

Details of Configuration Parameter:

Parameter	Permitted Values	Default
static.network.vlan.vlan_change.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to obtain VLAN ID using lower priority of VLAN assignment method or disable VLAN feature when the IP phone cannot obtain VLAN ID using the current VLAN assignment method.		

Parameter	Permitted Values	Default
0-Disabled **1**-Enabled The priority of each method is: LLDP/CDP>Manual>DHCP VLAN. If it is set to 1 (Enabled), the IP phone will attempt to use the lower priority of VLAN assignment method when failing to obtain the VLAN ID using higher priority of VLAN assignment method. If all the methods are attempted, the phone will disable VLAN feature. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		

LLDP

LLDP (Linker Layer Discovery Protocol) is a vendor-neutral Link Layer protocol, which 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 LLDP feature is enabled on IP phones, the IP phones periodically advertise their own information to the directly connected LLDP-enabled switch. The IP phones can also receive LLDP packets from the connected switch. When the application type is "voice", IP phones decide whether to update the VLAN configurations obtained from the LLDP packets. 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

LLDP can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure LLDP feature. **Parameters:** static.network.lldp.enable static.network.lldp.packet_interval
Web User Interface		Configure LLDP feature. **Navigate to**: http://<phoneIPAddress>/servlet?

	m=mod_data&p=network-adv&q=load
Phone User Interface	Configure LLDP feature.

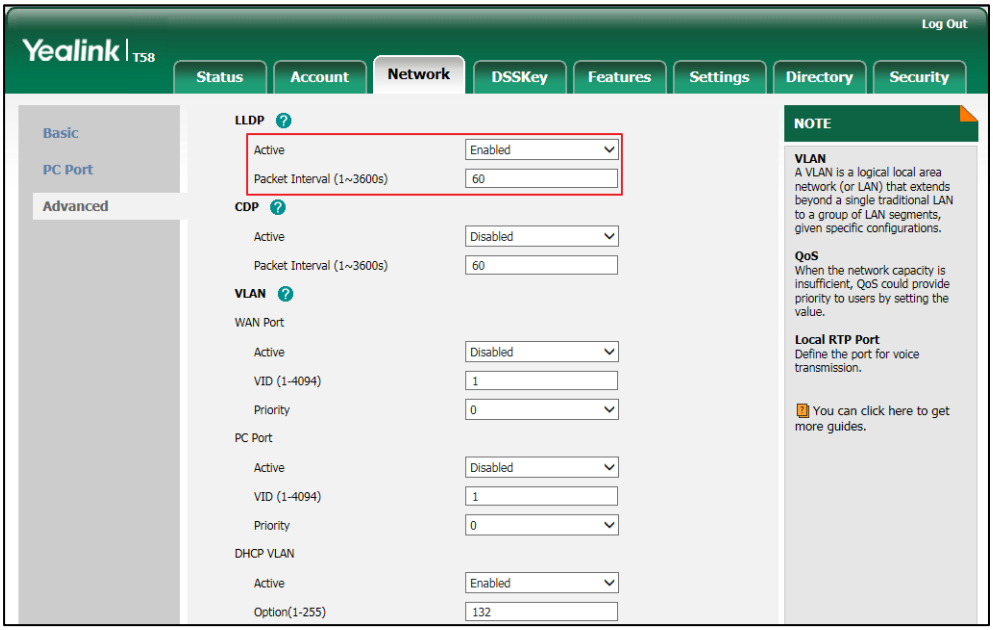
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.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 If it is set to 1 (Enabled), the IP phone will attempt to determine its VLAN ID through LLDP. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->LLDP->Active **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->LLDP->LLDP Status		
static.network.lldp.packet_interval	**Integer from 1 to 3600**	**60**
Description: Configures the interval (in seconds) for the IP phone to send the LLDP (Linker Layer Discovery Protocol) request. **Note:** It works only if the value of the parameter "static.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:** Settings->Advanced (default password: admin) ->Network->LLDP->Packet Interval		

To configure LLDP feature via web user interface:

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

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



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

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

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

To configure LLDP feature via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**LLDP**.
2. Tap the **On** radio box in the **LLDP Status** field.
3. Enter the priority value (1-3600s) in the **Packet Interval** field.
4. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.

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

   The settings will take effect after a reboot.

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure CDP feature. **Parameters:** static.network.cdp.enable static.network.cdp.packet_interval
Web User Interface		Configure CDP feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load
Phone User Interface		Configure CDP feature.

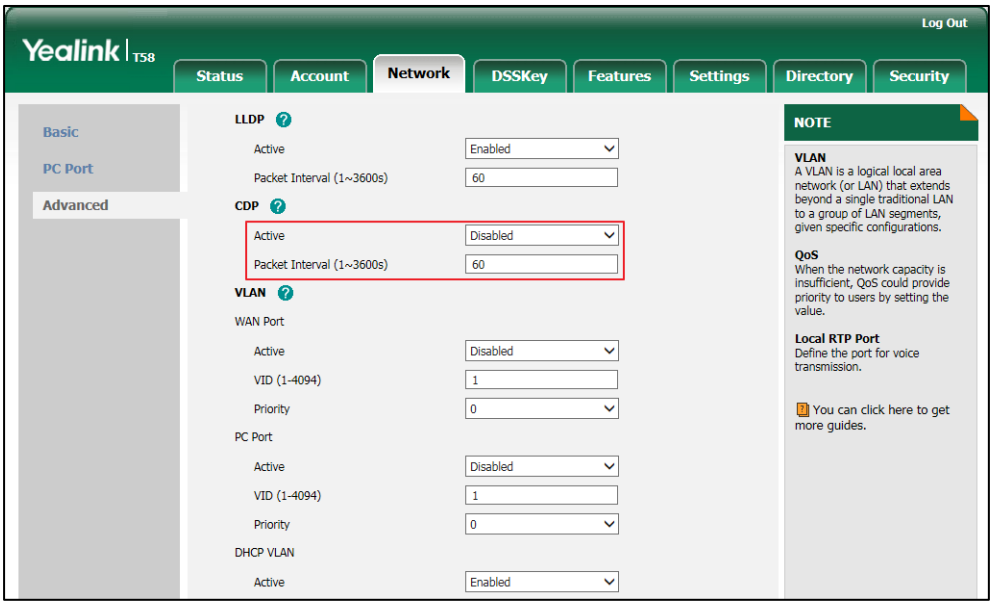
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.cdp.enable	**0 or 1**	**0**
Description: Enables or disables the CDP (Cisco Discovery Protocol) feature on the IP phone. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will attempt to determine its VLAN ID through CDP. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->CDP->Active **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->CDP->CDP Status		
static.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 "static.network.cdp.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take		

Parameters	Permitted Values	Default
effect. **Web User Interface:** Network->Advanced->CDP->Packet Interval (1~3600s) **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->CDP->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.



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 phone.

To configure CDP feature via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**CDP**->**CDP Status**.
2. Tap the **On** radio box in the **CDP Status** field.
3. Enter the priority value (1-3600s) in the **Packet Interval** field.
4. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.
5. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

Manual Configuration for VLAN in the Wired Network

VLAN is disabled on IP phones by default. You can configure VLAN for the Internet port and PC port manually. For CP960 IP phones, you can only configure VLAN for the Internet port manually, because they only have Internet port. 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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure VLAN for the Internet port and PC port manually. **Parameters:** static.network.vlan.internet_port_enable static.network.vlan.internet_port_vid static.network.vlan.internet_port_priority static.network.vlan.pc_port_enable static.network.vlan.pc_port_vid static.network.vlan.pc_port_priority
Web User Interface		Configure VLAN for the Internet port and PC port manually. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load
Phone User Interface		Configure VLAN for the Internet port and PC port manually.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.vlan.internet_port_enable	**0 or 1**	**0**
Description: Enables or disables VLAN for the Internet port. **0**-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->VLAN->WAN Port->Active		

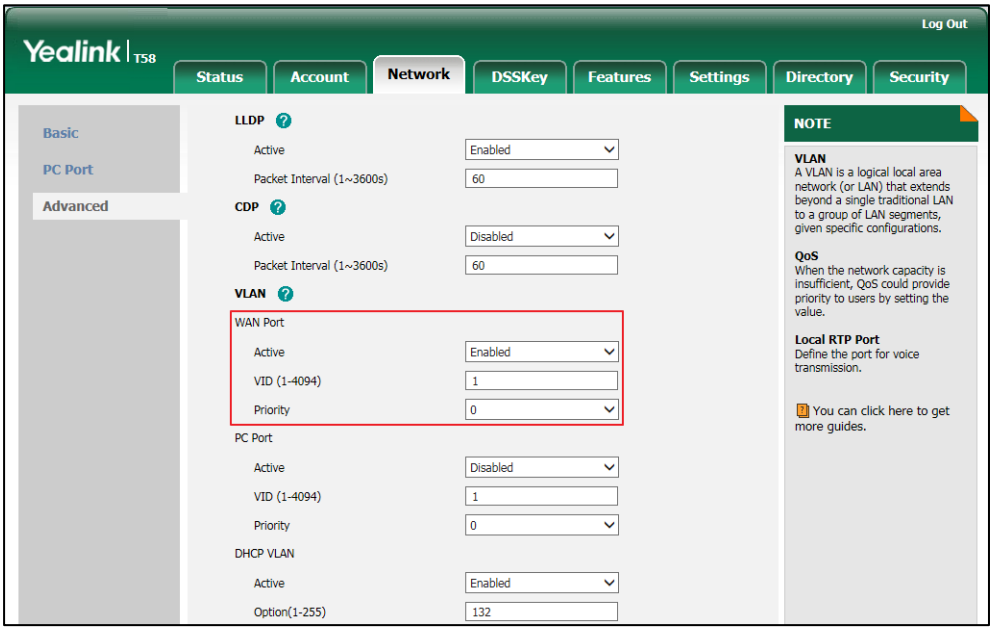
Parameters	Permitted Values	Default
Phone User Interface: Settings->Advanced (default password: admin) ->Network->VLAN->WAN Port->VLAN Status		
static.network.vlan.internet_port_vid	**Integer from 1 to 4094**	**1**
Description: Configures VLAN ID for the Internet port. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->WAN Port->VID (1-4094) **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->VLAN->WAN Port->VID Number		
static.network.vlan.internet_port_priority	**Integer from 0 to 7**	**0**
Description: Configures VLAN priority for the Internet port. 7 is the highest priority, 0 is the lowest priority. **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->WAN Port->Priority **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->VLAN->WAN Port->Priority		
static.network.vlan.pc_port_enable	**0 or 1**	**0**
Description: Enables or disables VLAN for the PC port. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiate). It is not applicable to CP960 IP phones. If you change this parameter, the IP phone will reboot to make the change take effect.		

Parameters	Permitted Values	Default
Web User Interface: Network->Advanced->VLAN->PC Port->Active **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->VLAN->PC Port->VLAN Status		
static.network.vlan.pc_port_vid	**Integer from 1 to 4094**	**1**
Description: Configures VLAN ID for the PC port. **Note:** It works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiate). It is not applicable to CP960 IP phones. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN->PC Port->VID (1-4094) **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->VLAN->PC Port->VID Number		
static.network.vlan.pc_port_priority	**Integer from 0 to 7**	**0**
Description: Configures VLAN priority for the PC port. 7 is the highest priority, 0 is the lowest priority. **Note:** It works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiate). It is not applicable to CP960 IP phones. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->VLAN >PC Port->Priority **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->VLAN->PC Port->Priority		

To configure VLAN for Internet port via web user interface:

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

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



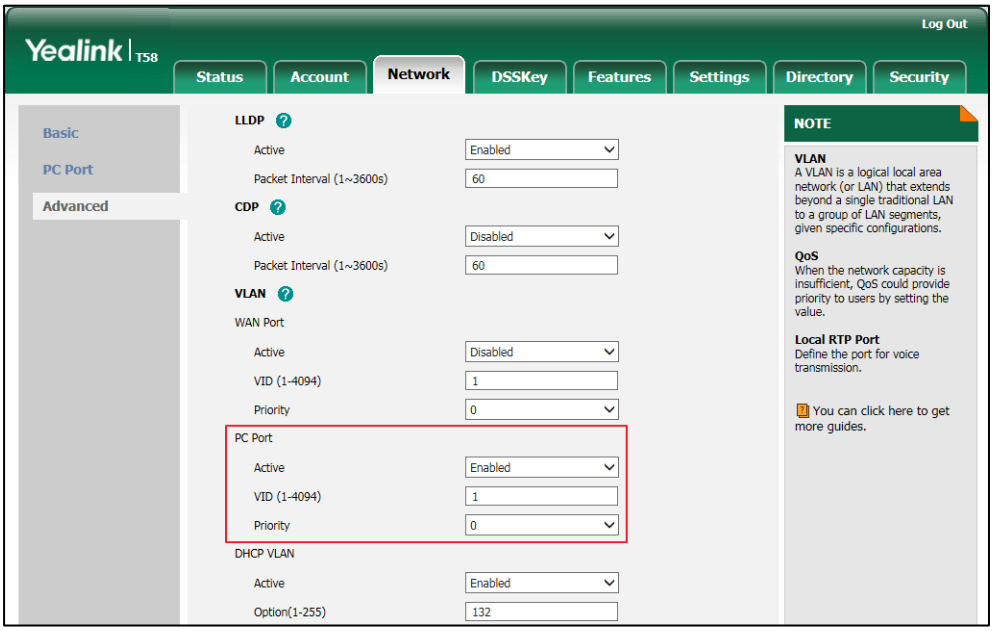
5. Click **Confirm** to accept the change.

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

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

To configure VLAN for PC port via web user interface:

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



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

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

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

To configure VLAN for Internet port (or PC port) via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**VLAN**->**WAN Port** (or **PC Port**).
2. Tap the **On** radio box in 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. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.
6. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure DHCP VLAN discovery feature. **Parameters:** static.network.vlan.dhcp_enable static.network.vlan.dhcp_option
Web User Interface		Configure DHCP VLAN discovery feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load
Phone User Interface		Configure DHCP VLAN discovery feature.

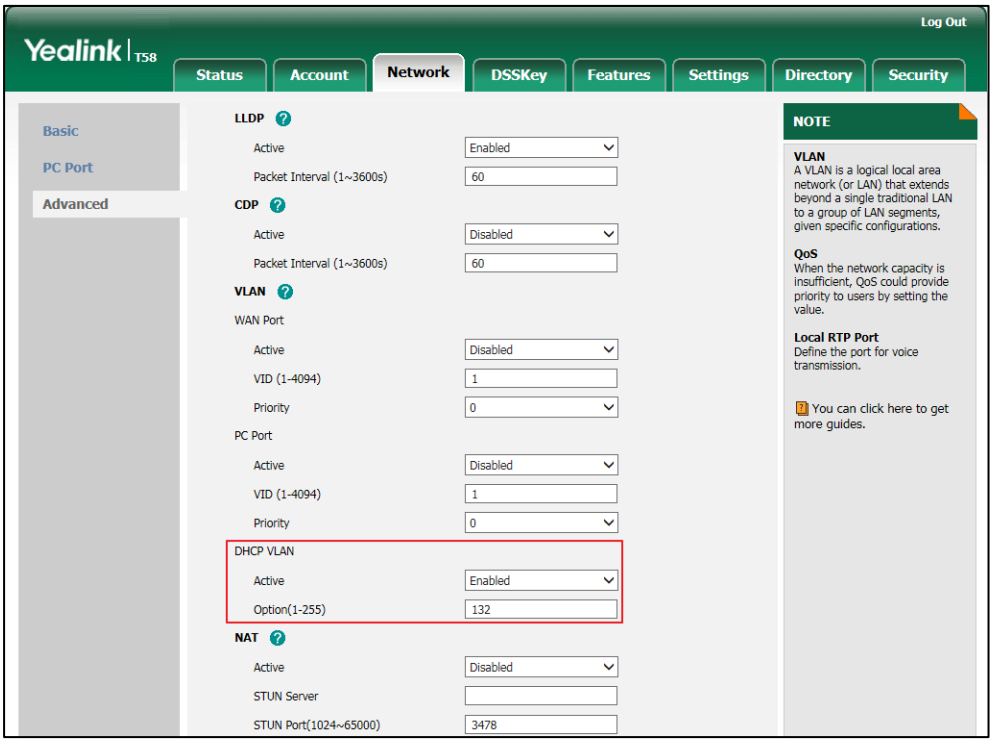
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.vlan.dhcp_enable	**0 or 1**	**1**
Description: Enables or disables DHCP VLAN discovery feature on the IP phone. **0**-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->VLAN->DHCP VLAN->Active **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->VLAN->DHCP VLAN->DHCP VLAN		
static.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 take effect. **Web User Interface:** Network->Advanced->VLAN->DHCP VLAN->Option(1-255) **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->VLAN->DHCP VLAN->Option		

To configure DHCP VLAN discovery via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **DHCP VLAN** block, select the desired value from the pull-down list of **Active**.
3. Enter the desired option in the **Option(1-255)** field.

The default option is 132.



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 phone.

To configure DHCP VLAN discovery via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**VLAN**->**DHCP VLAN**.
2. Tap the **On** radio box in the **DHCP VLAN** field.
3. Enter the desired option in the **Option** field.
4. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.
5. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

IPv6 Support

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

IPv6 is developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. Yealink IP Phone supports IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4&IPv6 dual stack addressing mode. IPv4 uses a 32-bit

address, consisting of four groups of three decimal digits separated by dots; for example, 192.168.1.100. IPv6 uses a 128-bit address, consisting of eight groups of four hexadecimal digits separated by colons; for example, 2026:1234:1:1:215:65ff:fe1f:caa.

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

If you configure the network settings on the phone for an IPv6 network, you can set up an IP address for the phone either by using 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:

DHCPv6	SLAAC (ICMPv6)	How the IP phone obtains the IPv6 address and network 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 manually.

DHCPv6	SLAAC (ICMPv6)	How the IP phone obtains the IPv6 address and network settings?
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 following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the IPv6 address assignment method. **Parameters**: static.network.ip_address_mode static.network.ipv6_internet_port.type static.network.ipv6_internet_port.ip static.network.ipv6_prefix static.network.ipv6_internet_port.gateway static.network.ipv6_icmp_v6.enable
		Configure the IPv6 static DNS address. **Parameters**: static.network.ipv6_primary_dns static.network.ipv6_secondary_dns
	<y0000000000xx>.cfg	Configure the IPv6 static DNS. **Parameter:** static.network.ipv6_static_dns_enable
Web User Interface		Configure the IPv6 address assignment method. Configure the IPv6 static DNS. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network&q=load
Phone User Interface		Configure the IPv6 address assignment method. Configure the IPv6 static DNS. Configure the IPv6 static DNS address.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.ip_address_mode	**0, 1 or 2**	**0**
Description: Configures the IP address mode. **0**-IPv4 **1**-IPv6 **2**-IPv4 & IPv6 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Basic->Internet Port->Mode(IPv4/IPv6) **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IP Mode		
static.network.ipv6_internet_port.type	**0 or 1**	**0**
Description: Configures the Internet port type for IPv6. **0**-DHCP **1**-Static IP Address **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) 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->IPv6 Config **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv6->Type		
static.network.ipv6_static_dns_enable	**0 or 1**	**0**
Description: Triggers the static IPv6 DNS feature to on or off. **0-**Off **1-**On		

If it is set to 0 (Off), the IP phone will use the IPv6 DNS obtained from DHCP. If it is set to 1 (On), the IP phone will use manually configured static IPv6 DNS. **Note:** It works only if the value of the parameter "static.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. **Web User Interface:** Network->Basic->IPv6 Config->IPv6 Static DNS **Phone User Interface:** Settings->Advanced (default: admin) ->Network->WAN Port->IPv6->Type (DHCP) ->Static DNS		
static.network.ipv6_internet_port.ip	**IPv6 address**	**Blank**
Description: Configures the IPv6 address. **Example:** static.network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.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 IP Address->IP Address **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv6->Type (Static IP) ->IP Address		
static.network.ipv6_prefix	**Integer from 0 to 128**	**64**
Description: Configures the IPv6 prefix. **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.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 IP Address->IPv6 Prefix(0~128) **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv6->Type		

(Static IP) ->IPv6 IP Prefix		
static.network.ipv6_internet_port.gateway	**IPv6 address**	**Blank**
Description: Configures the IPv6 default gateway. **Example:** static.network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c:5447:23a6:255 **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6), and "static.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 IP Address->Gateway **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv6->Type (Static IP) ->Gateway		
static.network.ipv6_primary_dns	**IPv6 address**	**Blank**
Description: Configures the primary IPv6 DNS server. **Example:** static.network.ipv6_primary_dns = 3036:1:1:c3c7: c11c:5447:23a6:256 **Note:** It works only if the value of the parameter "static.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 "static.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 IP Address->Primary DNS **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv6->Type (Static IP) ->Primary DNS **Or** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv6->Type (DHCP) ->Static DNS (Enabled) ->Primary DNS		
static.network.ipv6_secondary_dns	**IPv6 address**	**Blank**
Description: Configures the secondary IPv6 DNS server.		

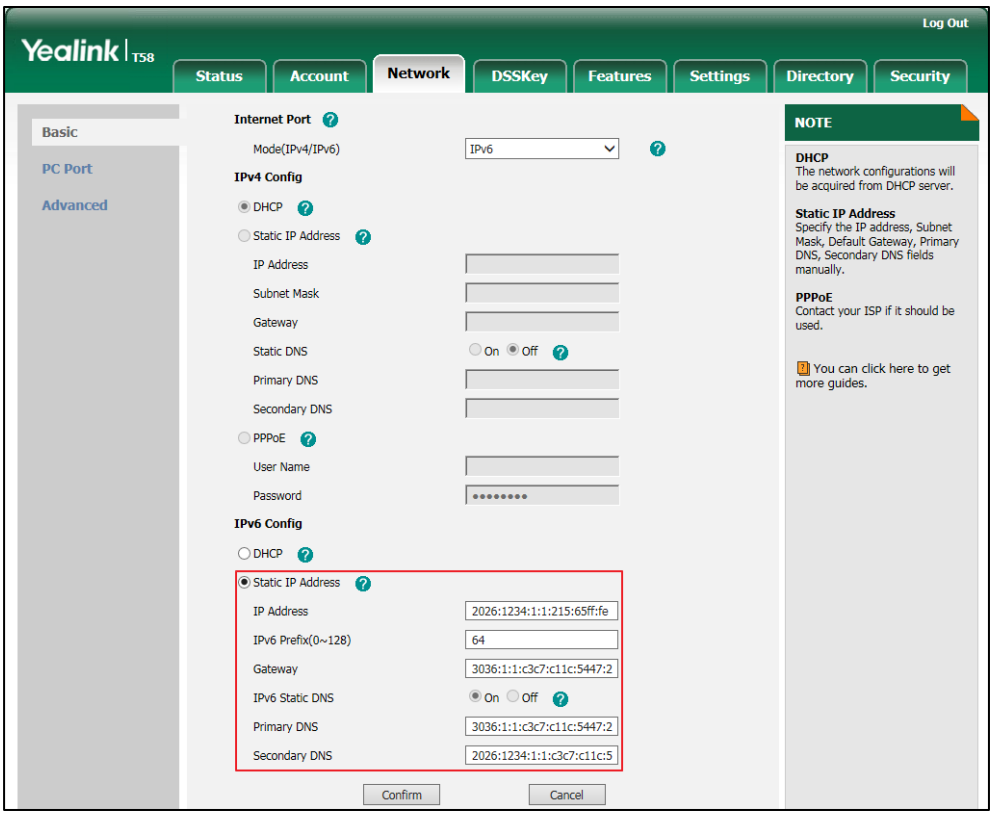
Example: static.network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:c11c:5447:23a6 **Note:** It works only if the value of the parameter "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure the value of the parameter "static.network.ipv6_static_dns_enable" 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 IP Address->Secondary DNS **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv6->Type (Static IP) ->Secondary DNS **Or** Settings->Advanced (default password: admin) ->Network->WAN Port->IPv6->Type (DHCP) ->Static DNS (Enabled) ->Secondary DNS		
static.network.ipv6_icmp_v6.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to obtain IPv6 network settings via SLAAC (Stateless Address Autoconfiguration) method. **0**-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->ICMPv6 Status->Active **Phone User Interface:** None		

To configure IPv6 address assignment method via web user interface:

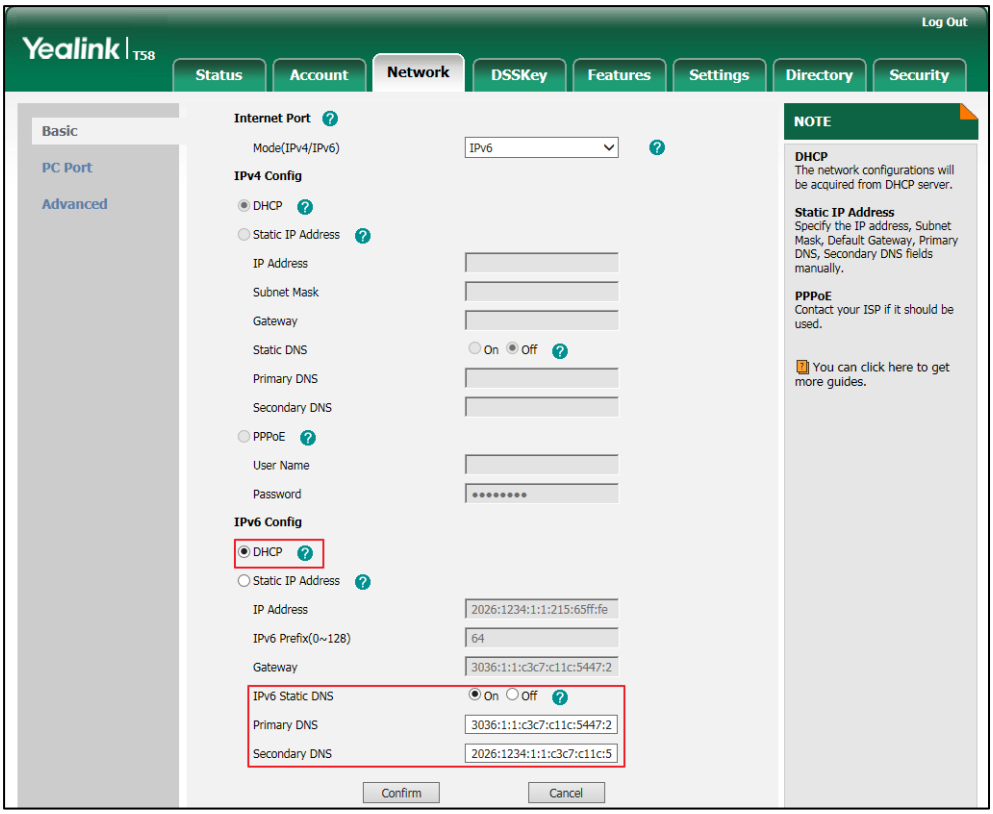
1. Click on **Network**->**Basic**.
2. Select the desired address mode (**IPv6** or **IPv4 & IPv6**) from the pull-down list of **Mode(IPv4/IPv6)**.

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.



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



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

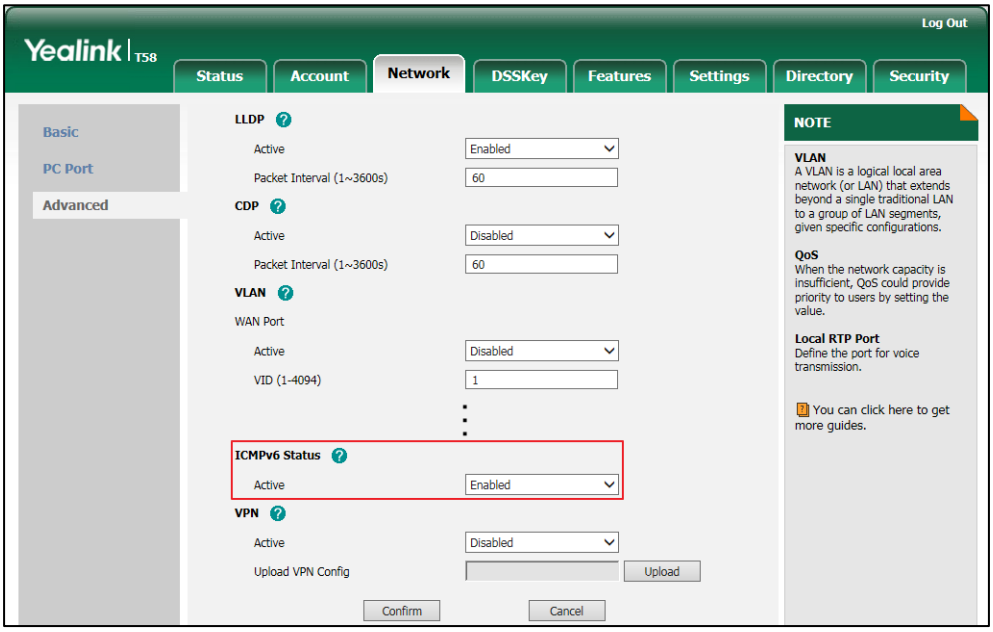
   A dialog box pops up to prompt that the settings will take effect after a reboot.

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

To configure SLAAC feature via web user interface:

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

2. In the **ICMPv6 Status** block, select the desired value from the pull-down list of **Active**.



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 phone.

To configure IPv6 address assignment method via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**WAN Port**.
2. Tap the **IP Mode** field.
3. Tap **IPv6** or **IPv4 and IPv6** in the pop-up dialog box.
4. Tap **IPv6**.
5. Tap the **Type** field.
6. Tap the desired IPv6 address assignment method in the pop-up dialog box.

   If you select the **Static IP**, configure the IPv6 address and other network parameters in the corresponding fields.

7. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.

8. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

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

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**WAN Port**->**IPv6**.
2. Tap the **Type** field.
3. Tap **DHCP** in the pop-up dialog box.
4. Tap the **Static DNS** field.

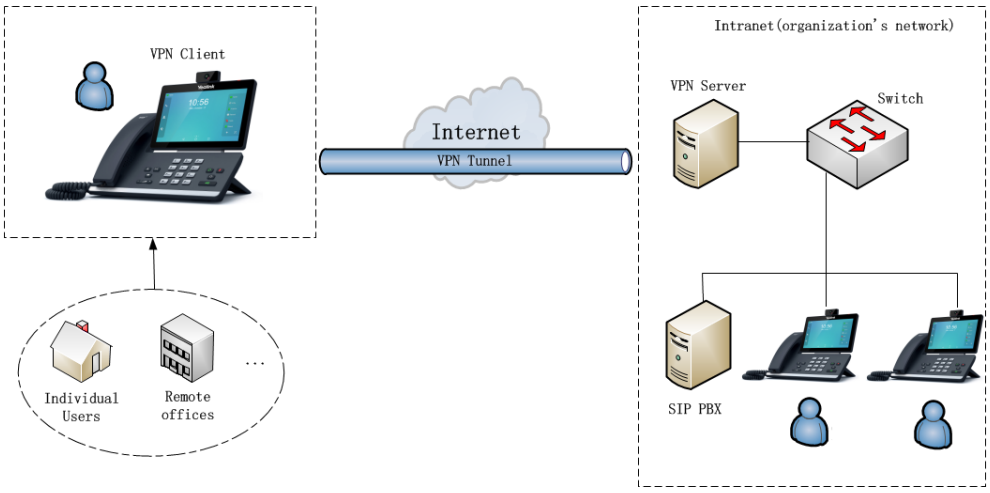
5. Tap **Enabled** in the pop-up dialog box.
6. Enter the desired value in the **Primary DNS** and **Secondary DNS** field respectively.
7. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.
8. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

VPN

VPN (Virtual Private Network) is a secured private network connection built on top of public telecommunication infrastructure, such as the Internet. It has become more prevalent due to benefits of scalability, reliability, convenience and security. VPN provides remote offices or individual users with secure access to their organization's network.



Types of VPN Access

There are two types of VPN access: remote-access VPN (connecting an individual device to a network) and site-to-site VPN (connecting two networks together). Remote-access VPN allows employees to access their company's intranet from home or outside the office, and site-to-site VPN allows employees in geographically separated offices to share one cohesive virtual network. VPN can be also classified by the protocols used to tunnel the traffic. It provides security through tunneling protocols: IPSec, SSL, L2TP and PPTP.

VPN Technology

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

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

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

The following table lists the unified directories of the OpenVPN certificates and key in the configuration file (vpn.cnf) for Yealink IP phones:

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

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

Procedure

VPN can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure VPN feature and upload a TAR file to the IP phone. **Parameters:** static.network.vpn_enable static.openvpn.url
Web User Interface		Configure VPN feature and upload a TAR file to the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load
Phone User Interface		Configure VPN feature.

Details of Configuration Parameters:

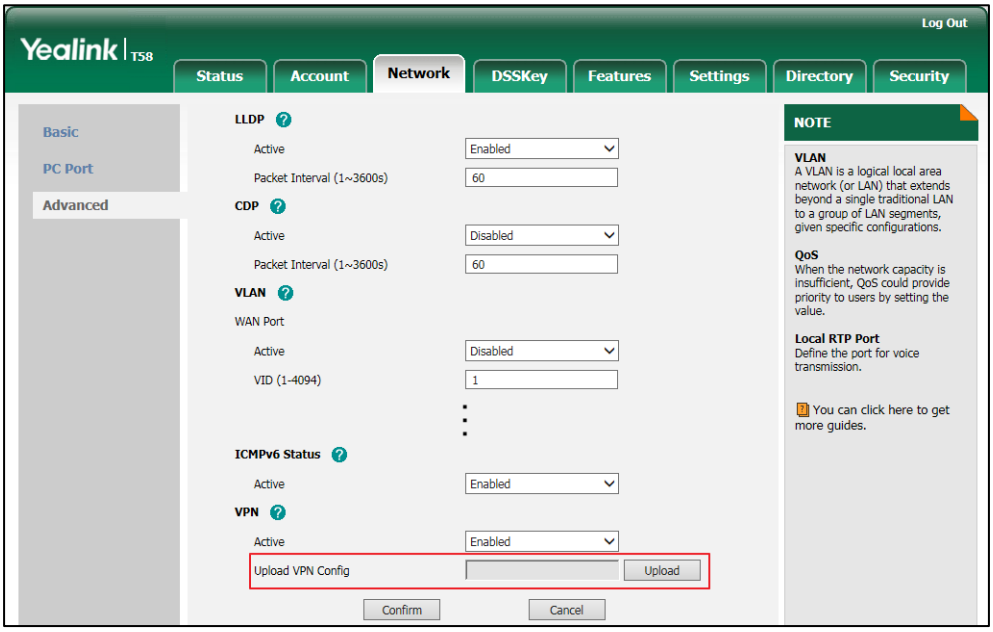
Parameters	Permitted Values	Default
static.network.vpn_enable	**0 or 1**	**0**
Description:		

Parameters	Permitted Values	Default
Enables or disables OpenVPN feature on the IP phone. **0**-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->VPN->Active **Phone User Interface:** Settings->Advanced (default: admin) ->Network->VPN->VPN Active		
static.openvpn.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the *.tar file for OpenVPN. **Example:** static.openvpn.url = http://192.168.10.25/OpenVPN.tar **Web User Interface:** Network->Advanced->VPN->Upload VPN Config **Phone User Interface:** None		

To upload a TAR file and configure VPN via web user interface:

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

2. Click **Upload** to locate and upload the TAR file from the local system.



The web user interface prompts the message "Operating, Please Wait...".

3. In the **VPN** block, select the desired value from the pull-down list of **Active**.
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 phone.

To configure VPN via phone user interface after uploading a TAR file:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**VPN**.
2. Tap the **On** radio box in the **VPN Active** field.

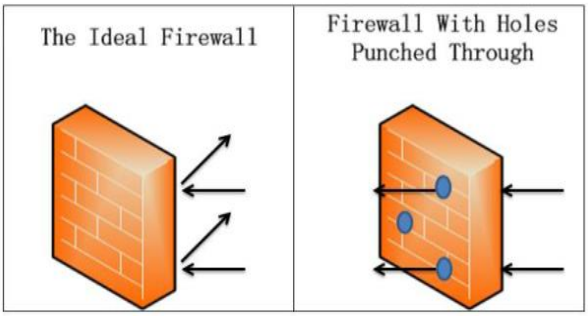
   You must upload the OpenVPN TAR file using configuration files or via web user interface in advance.
3. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.
4. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

Configuring the IP Phone for Use with a Firewall or NAT

A firewall protects an organization's IP network by controlling data traffic from outside the network. If your IP phone communicates with other devices through a firewall, you must configure your firewall to allow incoming and outgoing traffic to the IP phone through the reserved ports and the required ports.



You must configure your firewall to allow incoming and outgoing traffic through the following ports:

Port	Port Type	Description
5060	UDP	SIP (default transport protocol)
5060	TCP	SIP (when selecting the TCP transport protocol)
5061	TCP	SIP (when selecting the TLS transport protocol)
50000-50249 (default range)	TCP/UDP	Reserved ports on the IP phone. For more information, refer to Reserved Ports on page 80.

Reserved Ports

By default, the IP phone communicates through UDP ports in the 50000 - 50249 range for video and voice control. The phone uses only a small number of these ports during a call. The exact number depends on the number of participants in the call, the protocol used, and the number of ports required for the type of call: video or voice. It is not applicable to CP960 IP phones.

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

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

Required ports for a SIP two-way call:

Call Type	Number of Required Ports
Video	4 UDP ports
Voice	2 UDP ports
Each additional video participant requires 4 UDP ports.	
Each additional audio participant requires 2 UDP ports.	

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

Phone	Maximum Connections	Required Ports for a SIP Call	
SIP-T58V/T58A	Three-way video call and two audio-only calls	16 UDP	50000-50015
SIP-T56A	Five-way audio-only conference	10 UDP	50000-50009

Procedure

Reserved ports can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the range of the UDP ports. **Parameters:** sip.min_udp_port sip.max_udp_port
		Configure the range of the TCP ports. **Parameters:** sip.min_tcp_port sip.max_tcp_port
Web User Interface		Configure the range of the UDP ports. Configure the range of the TCP ports. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load

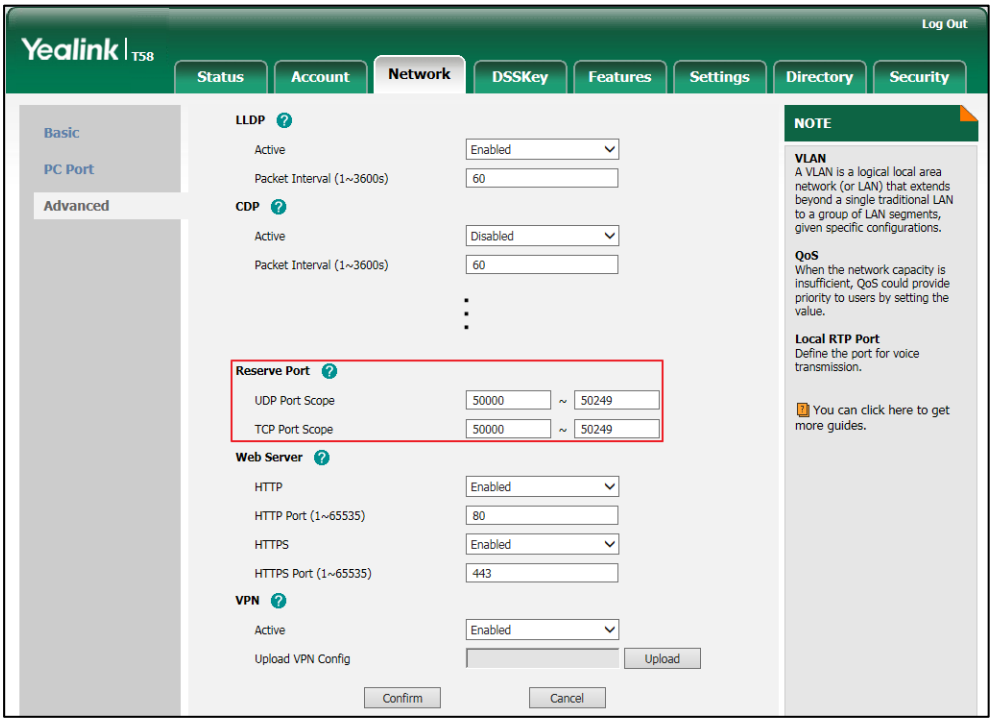
Details of Configuration Parameters:

Parameters	Permitted Values	Default
sip.min_udp_port	**Integer from 1024 to 65535**	**50000**
Description: Configures the minimum UDP port. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. It is not applicable to CP960 IP phones. **Web User Interface:** Network->Advanced->UDP Port Scope **Phone User Interface:** None		
sip.max_udp_port	**Integer from 1024 to 65535**	**50249**
Description: Configures the maximum UDP port. **Note**: The value of the maximum UDP port cannot be less than that of the minimum UDP port (configured by the parameter "sip.min_udp_port"). If you change this parameter, the IP phone will reboot to make the change take effect. It is not applicable to CP960 IP phones. **Web User Interface:** Network->Advanced->UDP Port Scope **Phone User Interface:** None		
sip.min_tcp_port	**Integer from 1024 to 65535**	**50000**
Description: Configures the minimum TCP port. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. It is not applicable to CP960 IP phones. **Web User Interface:** Network->Advanced->TCP Port Scope **Phone User Interface:** None		

Parameters	Permitted Values	Default
sip.max_tcp_port	**Integer from 1024 to 65535**	**50249**
Description: Configures the maximum TCP port. **Note**: The value of the maximum TCP port cannot be less than that of the minimum TCP port (configured by the parameter "sip.min_tcp_port"). If you change this parameter, the IP phone will reboot to make the change take effect. It is not applicable to CP960 IP phones. **Web User Interface:** Network->Advanced->TCP Port Scope **Phone User Interface:** None		

To configure reserved ports via web user interface:

1. Click on **Network**->**Advanced**.
2. Enter the desired UDP port scope in the **UDP Port Scope** field.
3. Enter the desired TCP port scope in the **TCP Port Scope** field.

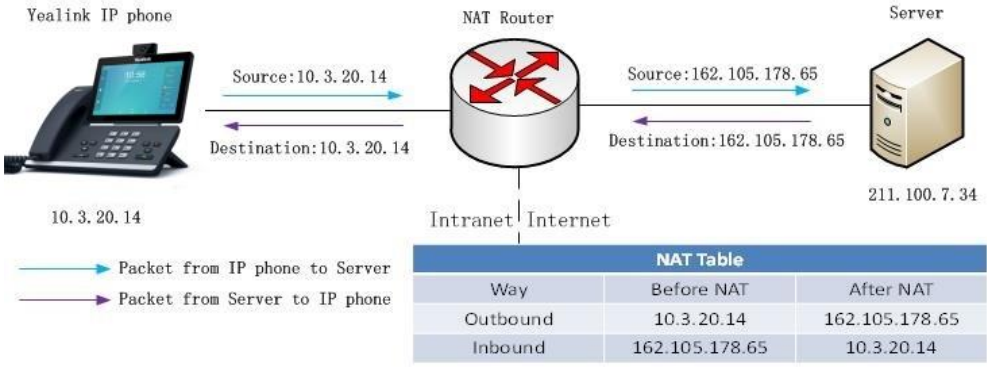


4. Click **Confirm** to accept the change.

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

Network Address Translation (NAT)

Network Address Translation (NAT) is essentially a translation table that maps public IP address and port combinations to private ones. This reduces the need for a large number of public IP addresses. NAT ensures security since each outgoing or incoming request must first go through a translation process.



NAT Table		
Way	Before NAT	After NAT
Outbound	10.3.20.14	162.105.178.65
Inbound	162.105.178.65	10.3.20.14

NAT Types

Symmetrical NAT

In symmetrical NAT, the NAT router stores the address and port where the packet was sent. Only packets coming from this address and port are forwarded back to the private address.

Full Cone NAT

In full cone NAT, all packets from a private address (e.g., iAddr: port1) to public network will be sent through a public address (e.g., eAddr: port2). Packets coming from the address of any server to eAddr: port2 will be forwarded back to the private address (e.g., iAddr: port1).

Address Restricted Cone NAT

Restricted cone NAT works similar like full cone NAT. A public host (hAddr: any) can send packets to iAddr: port1 through eAddr: port2 only if iAddr: port1 has previously sent a packet to hAddr: any. "Any" means the port number doesn't matter.

Port Restricted Cone NAT

Port restricted cone NAT works similar like full cone NAT. A public host (hAddr: hPort) can send packets to iAddr: port1 through eAddr: port2 only if iAddr: port1 has previously sent a packet to hAddr: hPort.

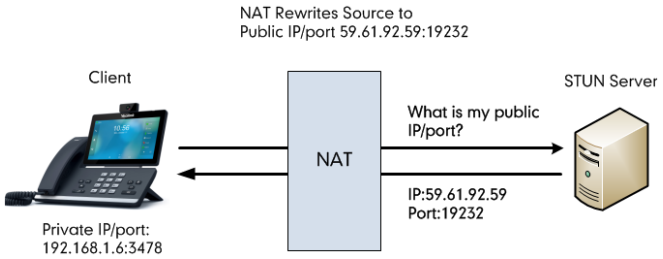
NAT Traversal

In the VoIP environment, NAT breaks end-to-end connectivity.

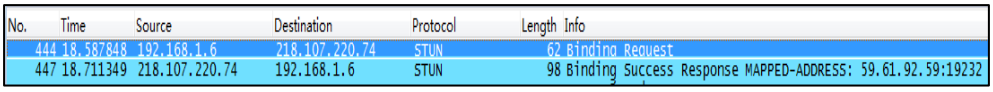
NAT traversal is a general term for techniques that establish and maintain IP connections traversing NAT gateways, typically required for client-to-client networking applications, especially for VoIP deployments. STUN is one of the NAT traversal techniques supported by IP phones.

STUN (Simple Traversal of UDP over NATs)

STUN is a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. The STUN protocol allows entities behind a NAT to first discover the presence of a NAT and the type of NAT (for more information on the NAT types, refer to NAT Types on page 84) and to obtain the mapped (public) IP address and port number that the NAT has allocated for the UDP connections to remote parties. The protocol requires assistance from a third-party network server (STUN server) usually located on public Internet. The IP phone can be configured to act as a STUN client, to send exploratory STUN messages to the STUN server. The STUN server uses those messages to determine the public IP address and port used, and then informs the client.



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



SIP and TLS Source Ports for NAT Traversal

You can configure the SIP and TLS source ports on the IP Phone. Previously, the IP phone used default values (5060 for UDP/TCP and 5061 for TLS). In the configuration files, you can use the following parameters to configure the SIP and TLS source ports:

- Local SIP Port
- TLS SIP Port

If NAT is disabled, the port number shows in the Via and Contact SIP headers of SIP messages. If NAT is enabled, the phone uses the NAT port number (and NAT IP address) in the Via and Contact SIP headers of SIP messages, but still use the configured source port.

Procedure

NAT traversal and STUN server can be configured using the following methods.

<table>
<tr><td rowspan="3">Central Provisioning (Configuration File)</td><td rowspan="2"><y0000000000xx>.cfg</td><td>Configure NAT traversal and STUN server on a phone basis.
Parameters:
sip.nat_stun.enable
sip.nat_stun.server
sip.nat_stun.port</td></tr>
<tr><td>Configure local SIP port and TLS SIP port.
Parameters:
sip.listen_port
sip.tls_listen_port</td></tr>
<tr><td><MAC>.cfg</td><td>Configure NAT traversal on a per-line basis.
Parameter:
account.X.nat.nat_traversal</td></tr>
<tr><td colspan="2" rowspan="3">Web User Interface</td><td>Configure NAT traversal and STUN server on a phone basis.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load</td></tr>
<tr><td>Configure local SIP port and TLS SIP port.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=settings-sip&q=load</td></tr>
<tr><td>Configure NAT traversal on a per-line basis.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=account-register&q=load&acc=0</td></tr>
<tr><td colspan="2">Phone User Interface</td><td>Configure NAT traversal and STUN server on a phone basis.</td></tr>
</table>

	Configure NAT traversal on a per-line basis.

Details of Configuration Parameters:

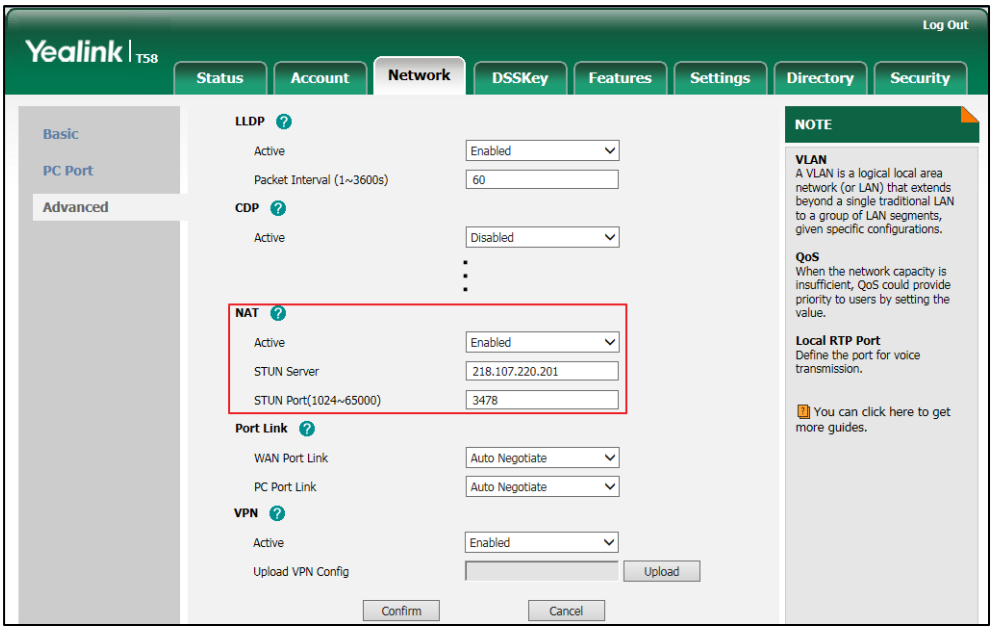
Parameters	Permitted Values	Default
sip.nat_stun.enable	**0 or 1**	**0**
Description: Enables or disables the STUN (Simple Traversal of UDP over NATs) feature on the IP phone. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->NAT->Active **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->NAT->NAT Status		
sip.nat_stun.server	**IP address or domain name**	**Blank**
Description: Configures the IP address or the domain name of the STUN (Simple Traversal of UDP over NATs) server. **Example:** sip.nat_stun.server = 218.107.220.201 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->NAT->STUN Server **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->NAT->STUN Server		
sip.nat_stun.port	**Integer from 1024 to 65000**	**3478**

Parameters	Permitted Values	Default
Description: Configures the port of the STUN (Simple Traversal of UDP over NATs) server. **Example:** sip.nat_stun.port = 3478 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->NAT->STUN Port(1024~65000) **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->NAT->STUN Port		
account.X.nat.nat_traversal	**0 or 1**	**0**
Description: Enables or disables the NAT traversal for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note:** It works only if the value of the parameter "sip.nat_stun.enable" is set to 1 (Enabled). **Web User Interface:** Account->Register->NAT **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->AccountX->NAT Status		
sip.listen_port	**Integer from 1024 to 65535**	**5060**
Description: Configures the local SIP port. **Web User Interface:** Settings->SIP->Local SIP Port **Phone User Interface:** None		
sip.tls_listen_port	**Integer from 1024 to 65535**	**5061**

Parameters	Permitted Values	Default
Description: Configures the local TLS listen port. **Web User Interface:** Settings->SIP->TLS SIP Port **Phone User Interface:** None		

To configure NAT traversal and STUN server via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **NAT** block, select the desired value from the pull-down list of **Active**.
3. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.
4. Enter the port of the STUN server in the **STUN Port(1024~65000)** field.



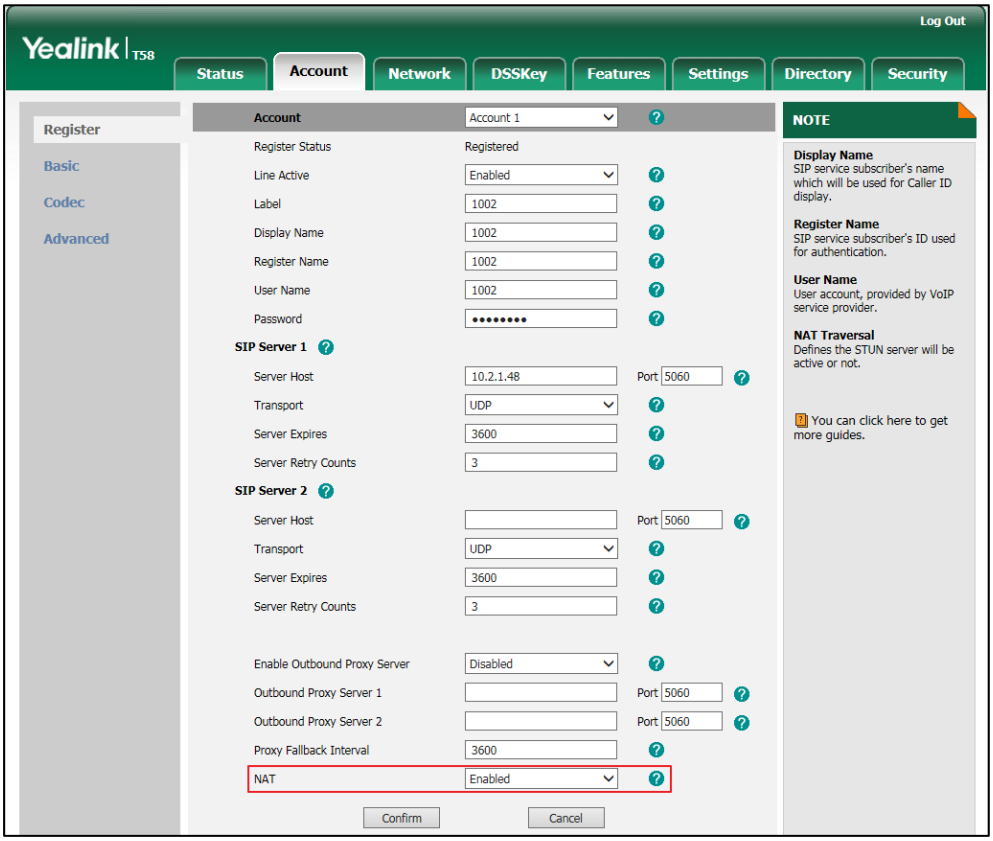
5. Click **Confirm** to accept the change.

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

To configure NAT traversal for account via web user interface:

1. Click on **Account**->**Register**.
2. Select the desired account from the pull-down list of **Account**.

3. Select **Enabled** from the pull-down list of **NAT**.

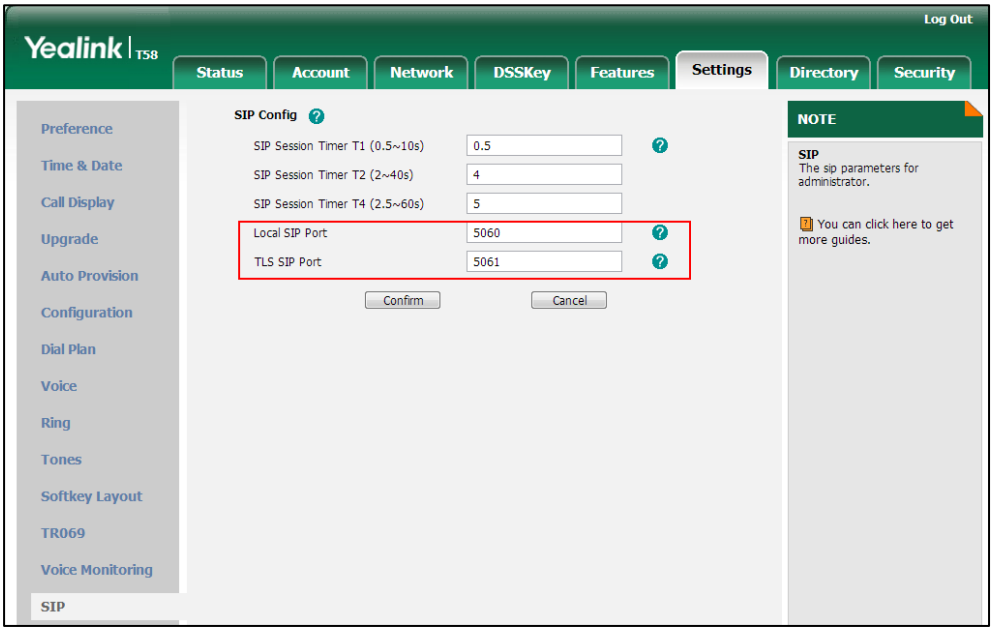


4. Click **Confirm** to accept the change.

To configure local SIP port and TLS SIP port via web user interface:

1. Click on **Settings**->**SIP**.
2. Enter the desired local SIP port in the **Local SIP Port** field.

3. Enter the desired TLS SIP port in the **TLS SIP Port** field.



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

To configure NAT traversal and STUN server via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**NAT**->**NAT Status**.
2. Tap the **On** radio box in the **NAT Status** field.
3. Enter the IP address or the domain name of the STUN server in the **STUN Server** field.
4. Enter the port of the STUN server in the **STUN Port** field.
5. Tap ✓ to accept the change.

   The phone prompts you to reboot the phone.
6. Tap **OK** to reboot the phone.

   The settings will take effect after a reboot.

To configure NAT traversal for a specific account via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Accounts**.
2. Tap the desired account.
3. Tap the **NAT Status** field.
4. Tap **Enabled** in the pop-up dialog box.
5. Tap ✓ to accept the change.

Keep Alive

IP phones can send keep-alive packets to the NAT device for keeping the communication port open.

Procedure

Keep alive feature can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the type of keep-alive packets on a per-line basis. **Parameter:** account.X.nat.udp_update_enable
		Configure the keep-alive interval on a per-line basis. **Parameter:** account.X.nat.udp_update_time
Web User Interface		Configure the type of keep-alive packets on a per-line basis. Configure the keep-alive interval on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

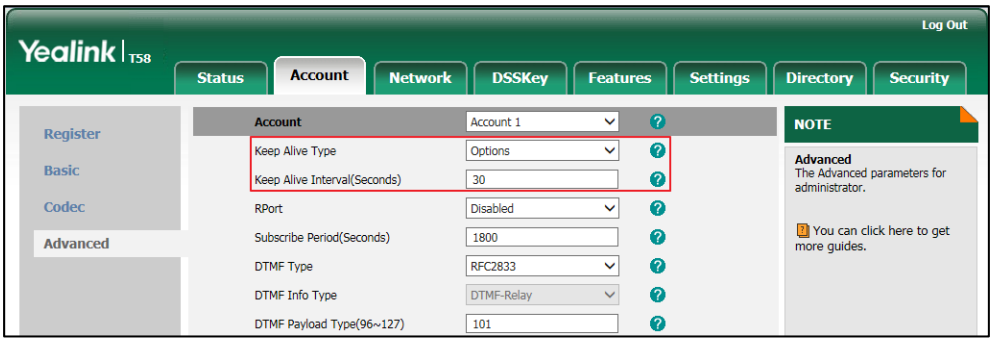
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.nat.udp_update_enable	**0, 1, 2 or 3**	**1**
Description: Configures the type of keep-alive packets sent by the IP phone to the NAT device to keep the communication port open so that NAT can continue to function for account X. **0**-Disabled **1**-Default (the IP phone sends UDP packets to the server) **2**-Options (the IP phone sends SIP OPTIONS packets to the server) **3**-Notify (the IP phone sends SIP NOTIFY packets to the server) If it is set to 0 (Disabled), the IP phone will not send keep-alive packets. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Keep Alive Type **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
account.X.nat.udp_update_time	**Integer from 15 to 2147483647**	**30**
Description: Configures the keep-alive interval (in seconds) for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.nat.udp_update_time = 60 **Note**: It works only if the value of the parameter "account.X.nat.udp_update_enable" is set to 1, 2 or 3. **Web User Interface:** Account->Advanced->Keep Alive Interval(Seconds) **Phone User Interface:** None		

To configure the type of keep-alive packets and keep-alive interval via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Keep Alive Type**.
4. Enter the keep-alive interval in the **Keep Alive Interval(Seconds)** field.



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

Rport

The Session Initiation Protocol (SIP) operates over UDP and TCP. When used with UDP, responses to requests are returned to the source address the request came from, and returned

to the port written into the topmost "Via" header of the request message. However, this behavior is not desirable when the client is behind a Network Address Translation (NAT) or firewall. So a new parameter "rport" for the "Via" header field is required.

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

Procedure

Rport feature can be configured using the following methods.

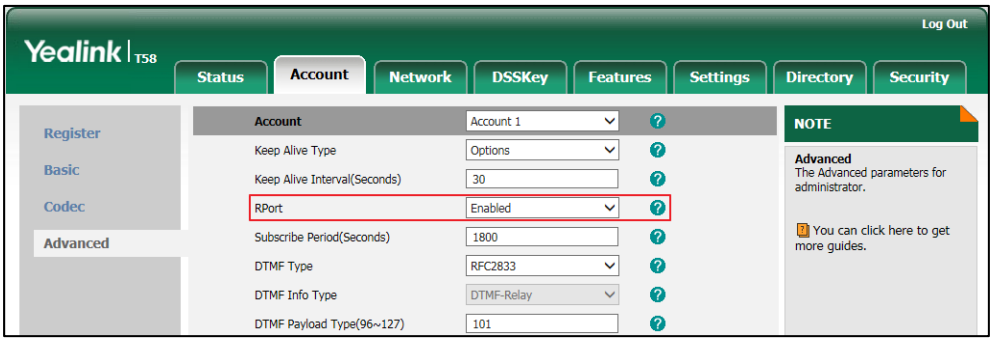
Central Provisioning (Configuration File)	<MAC>.cfg	Configure NAT Rport feature on a per-line basis. **Parameter:** account.X.nat.rport
Web User Interface		Configure NAT Rport feature on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

Details of Configuration Parameter:

Parameter	Permitted Values	Default
account.X.nat.rport	**0, 1 or 2**	**0**
Description: Enables or disables NAT Rport feature for account X. **0**-Disabled **1**-Enabled **2**-enable direct process X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->RPort **Phone User Interface:** None		

To configure Rport feature via web user interface:

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



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

Quality of Service (QoS)

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.

Video QoS

To ensure acceptable visual quality for video, video packets emanated from the IP phones should be configured with a high transmission priority. It is not applicable to CP960 IP phones.

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.

Wi-Fi QoS

Wi-Fi Multimedia (WMM) is based on the IEEE 802.11e standard and provides basic Quality of service (QoS) features to wireless networks. QoS enables Wi-Fi access points to prioritize traffic and optimizes the way shared network resources are allocated among different applications.

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 54.

Procedure

QoS can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the DSCPs for voice packets, SIP packets and video packets. **Parameters**: static.network.qos.audiotos static.network.qos.signaltos static.network.qos.videotos
		Configure the WMM feature in the wireless network. **Parameters**: static.wifi.802_11e.enable
Web User Interface		Configure the DSCPs for voice packets, SIP packets and video packets. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load

Details of Configuration Parameters:

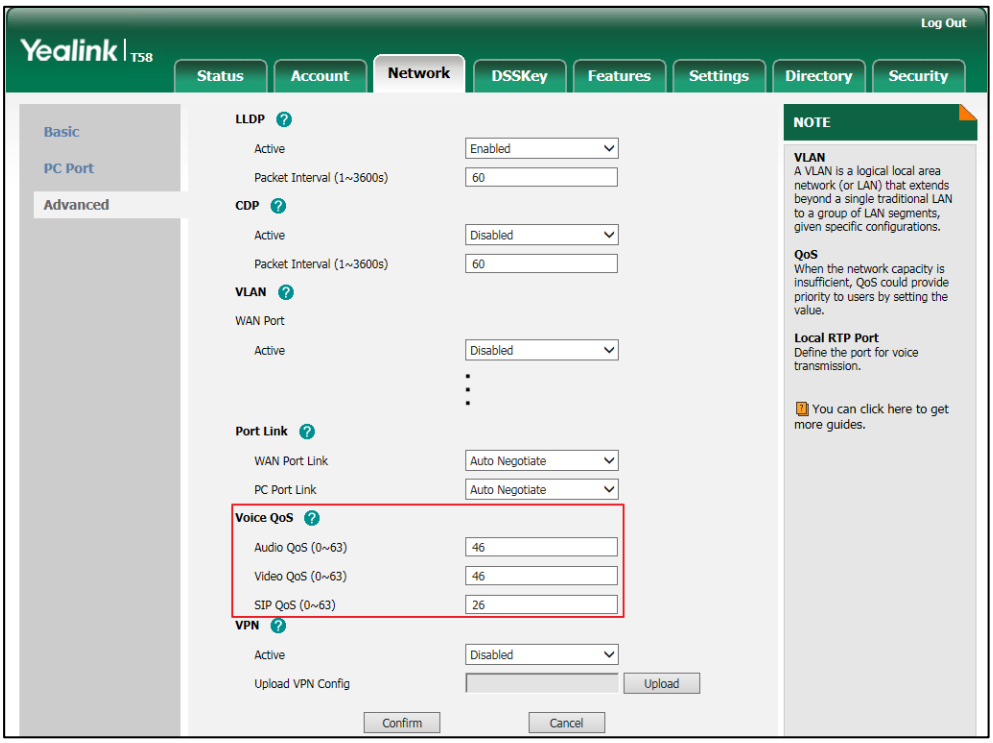
Parameters	Permitted Values	Default
static.network.qos.signaltos	**Integer from 0 to 63**	**26**
Description: Configures the DSCP (Differentiated Services Code Point) for SIP packets. The default DSCP value for SIP packets is 26 (Assured Forwarding). **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Voice QoS->SIP QoS (0~63) **Phone User Interface:** None		
static.network.qos.audiotos	**Integer from 0 to 63**	**46**

Parameters	Permitted Values	Default
Description: Configures the DSCP (Differentiated Services Code Point) for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding). **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->Voice QoS->Audio QoS (0~63) **Phone User Interface:** None		
static.network.qos.videotos	**Integer from 0 to 63**	**34**
Description: Configures the DSCP (Differentiated Services Code Point) for video packets. The default DSCP value for H264 packets is 34 (Assured Forwarding). **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. It is not applicable to CP960 IP phones. **Web User Interface:** Network->Advanced->Voice QoS->Video QoS (0~63) **Phone User Interface:** None		
static.wifi.802_11e.enable	**0 or 1**	**1**
Description: Enables or disables the WMM feature (Wi-Fi MultiMedia) in the wireless network. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** None **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 **Audio QoS (0~63)** field.

3. Enter the desired value in the **Video QoS (0~63)** field.
4. Enter the desired value in the **SIP QoS (0~63)** field.



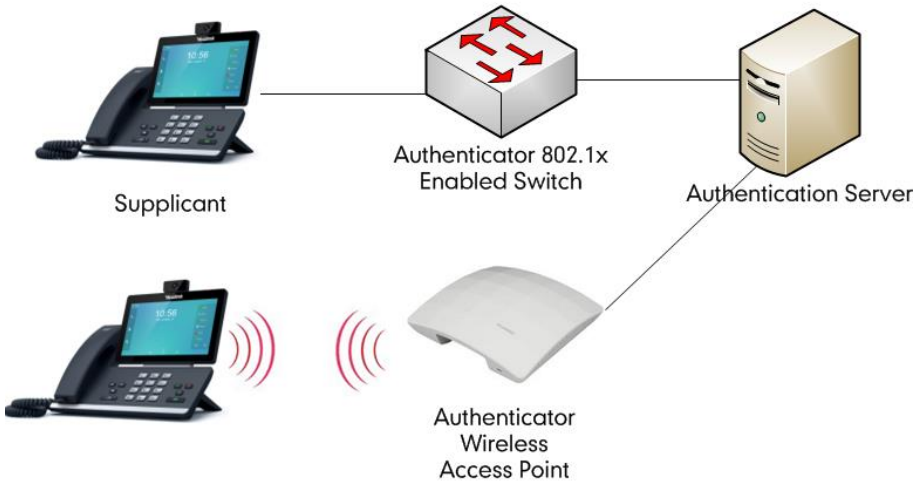
5. Click **Confirm** to accept the change.

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

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.



Yealink IP phones support the following protocols for 802.1X authentication:

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

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

Procedure

802.1X authentication can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the 802.1X authentication. **Parameters:** static.network.802_1x.mode static.network.802_1x.identity static.network.802_1x.md5_password static.network.802_1x.root_cert_url

		static.network.802_1x.client_cert_url
Web User Interface		Configure the 802.1X authentication. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load
Phone User Interface		Configure the 802.1X authentication.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.802_1x.mode	**0, 1, 2, 3, 4, 5, 6 or 7**	**0**
Description: Configures the 802.1x authentication method. **0**-Disabled **1**-EAP-MD5 **2**-EAP-TLS **3**-EAP-PEAP/MSCHAPv2 **4**-EAP-TTLS/EAP-MSCHAPv2 **5**-EAP-PEAP/GTC **6**-EAP-TTLS/EAP-GTC **7**-EAP-FAST **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Network->Advanced->802.1x->802.1x Mode **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->802.1x->802.1x Mode		
static.network.802_1x.identity	**String within 32 characters**	**Blank**
Description: Configures the identity (or user name) for 802.1x authentication. **Example:** static.network.802_1x.identity = admin **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 1, 2, 3, 4, 5, 6 or 7. If you change this parameter, the IP phone will reboot to make the		

Parameters	Permitted Values	Default
change take effect. **Web User Interface:** Network->Advanced->802.1x->Identity **Phone User Interface:** Settings->Advanced (default password: admin) ->Network->802.1x->Identity		
static.network.802_1x.md5_password	**String within 32 characters**	**Blank**
Description: Configures the password for 802.1x authentication. **Example:** static.network.802_1x.md5_password = admin123 **Note:** It works only if the value of the parameter "static.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:** Settings->Advanced (default password: admin) ->Network->802.1x->MD5 Password		
static.network.802_1x.root_cert_url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the CA certificate. **Example:** static.network.802_1x.root_cert_url = http://192.168.1.10/ca.pem **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6 or 7. The format of the CA certificate must be *.pem, *.crt, *.cer or *.der. **Web User Interface:** Network->Advanced->802.1x->CA Certificates **Phone User Interface:** None		
static.network.802_1x.client_cert_url	**URL within 511 characters**	**Blank**
Description:		

Parameters	Permitted Values	Default
Configures the access URL of the device certificate. **Example:** static.network.802_1x.client_cert_url = http://192.168.1.10/client.pem **Note:** It works only if the value of the parameter "static.network.802_1x.mode" is set to 2 (EAP-TLS). The format of the device certificate must be *.pem. **Web User Interface:** Network->Advanced->802.1x->Device Certificates **Phone User Interface:** None		

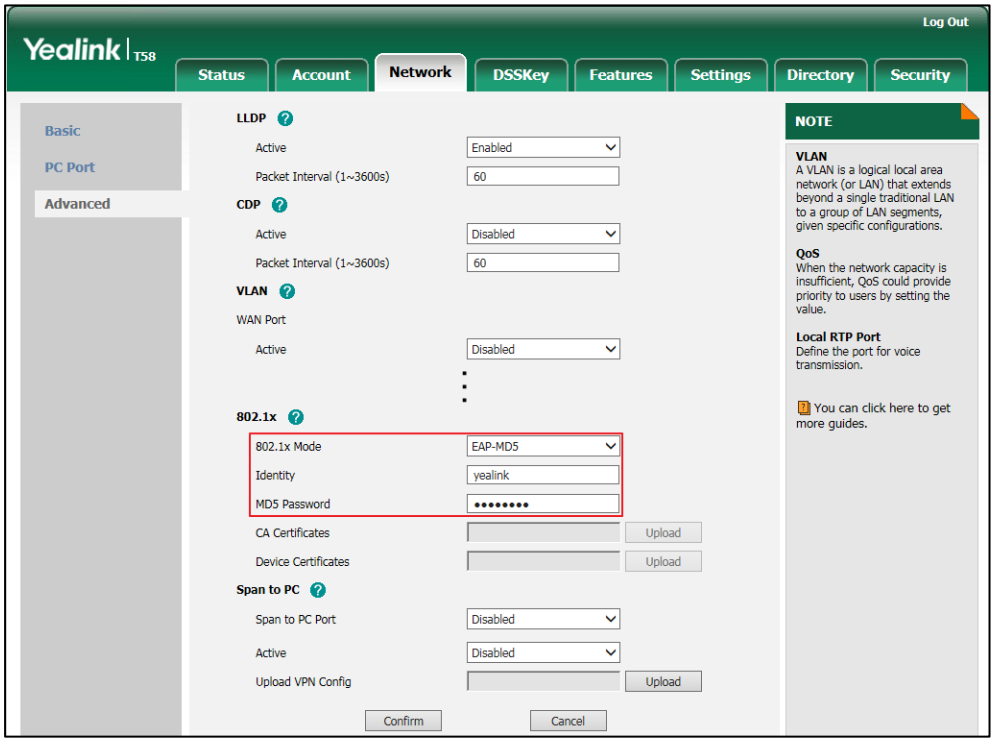
To configure the 802.1X authentication via web user interface:

1. Click on **Network**->**Advanced**.
2. In the **802.1x** block, select the desired protocol from the pull-down list of **802.1x Mode**.

   a) If you select **EAP-MD5**:

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

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



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

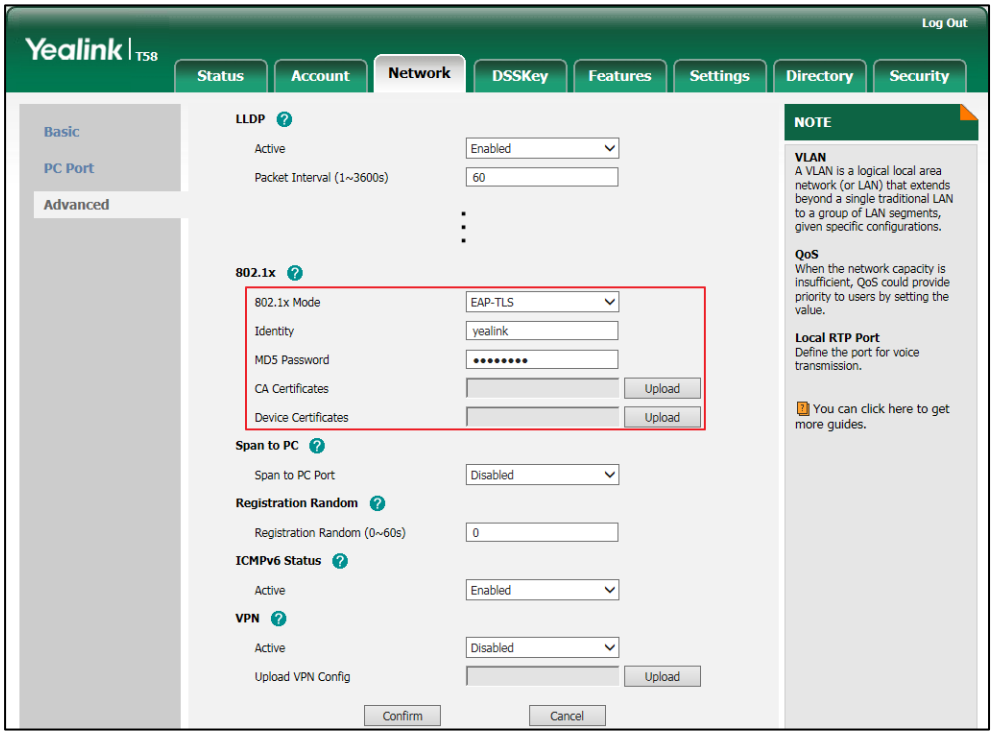
   1) Enter the user name for authentication in the **Identity** field.

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

   3) In the **CA Certificates** field, click **Upload** to select and upload the desired CA

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

4) In the **Device Certificates** field, click **Upload** to select and upload the desired client (*.pem or *.cer) certificate from your local system.

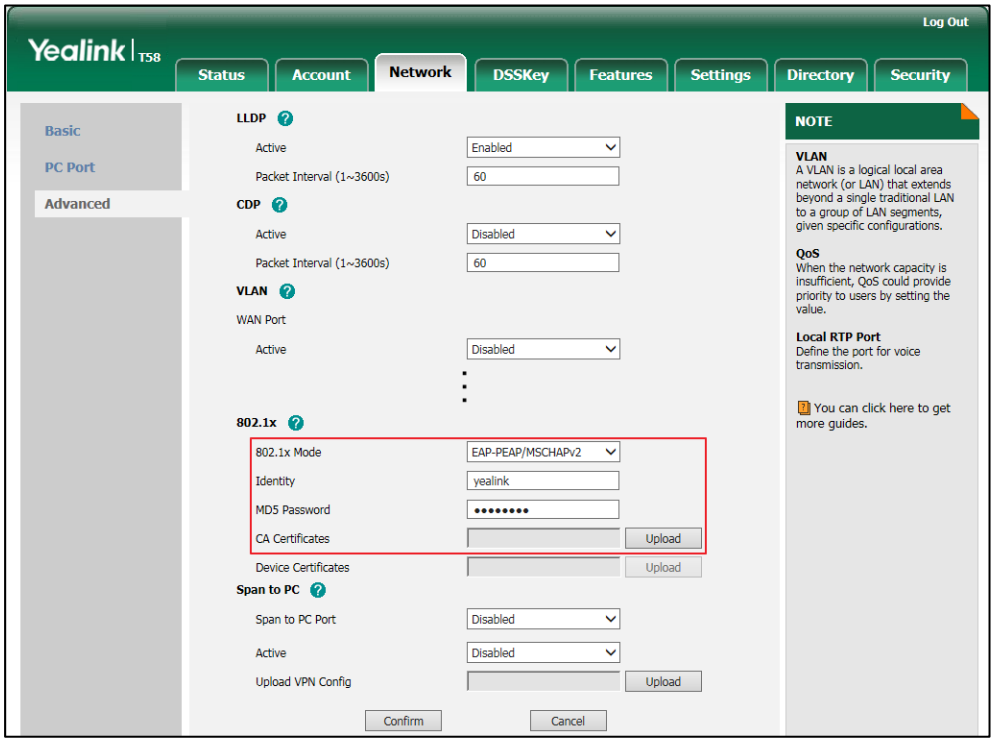


c) If you select **EAP-PEAP/MSCHAPv2**:

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

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

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

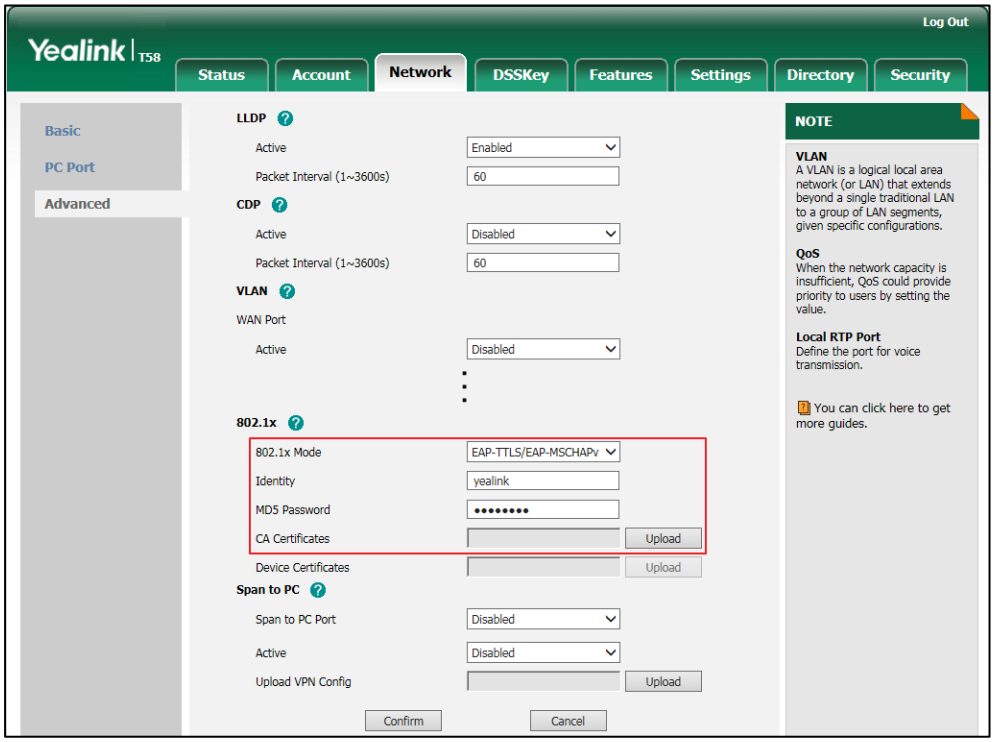


d) If you select **EAP-TTLS/EAP-MSCHAPv2**:

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

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

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

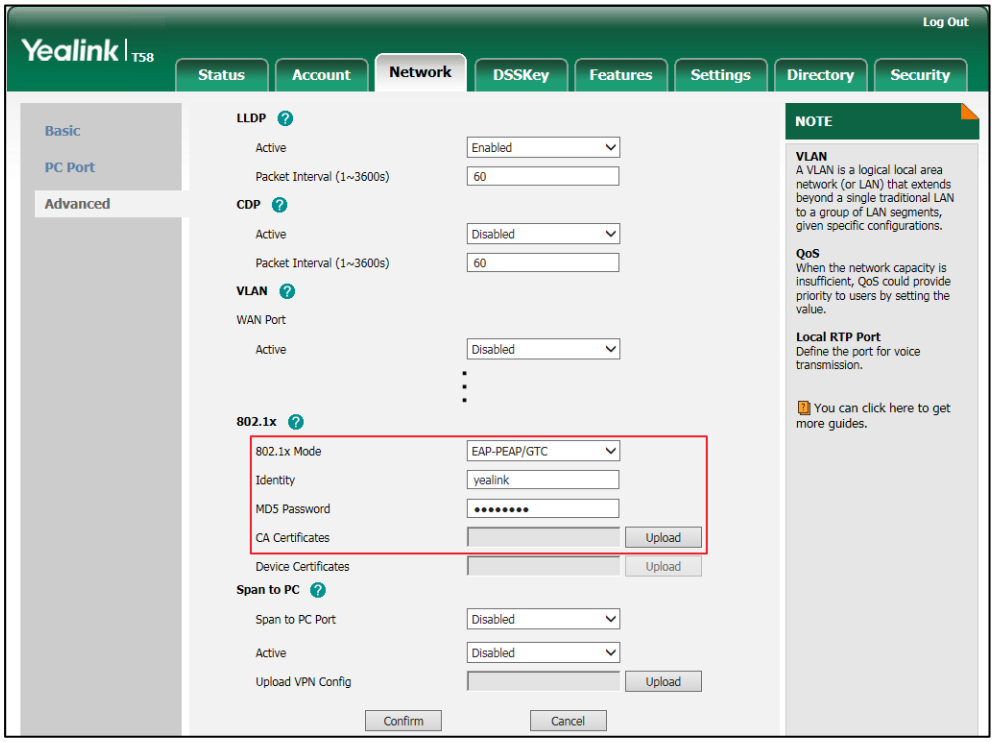


e) If you select **EAP-PEAP/GTC**:

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

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

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

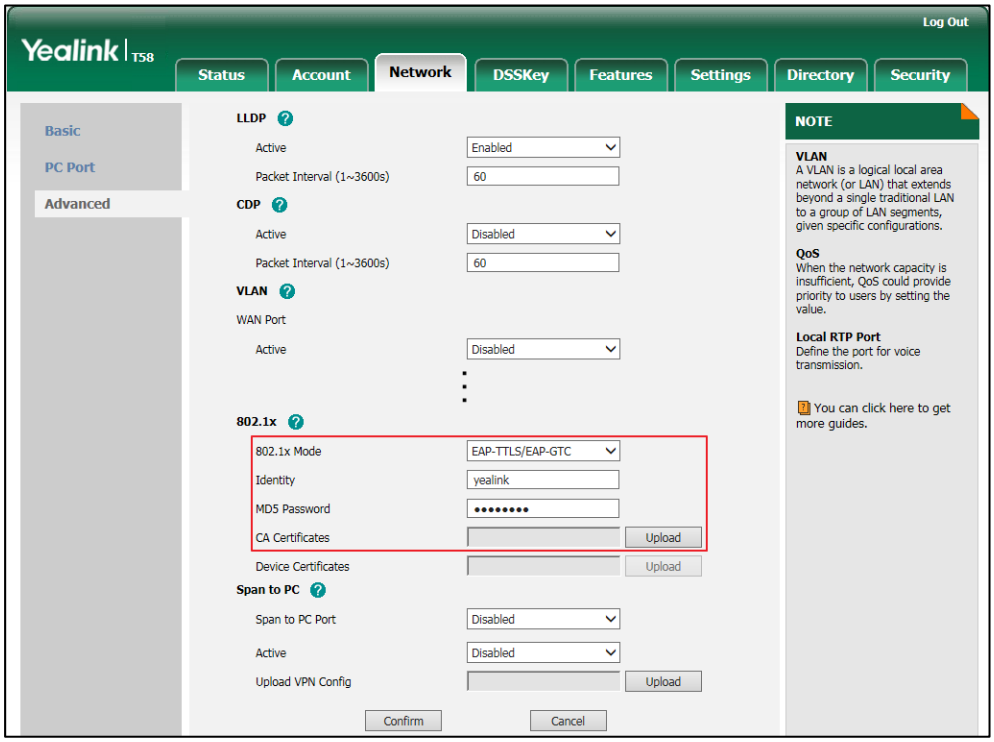


f) If you select **EAP-TTLS/EAP-GTC**:

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 **Upload** to select and upload the desired CA certificate (*.pem, *.crt, *.cer or *.der) from your local system.

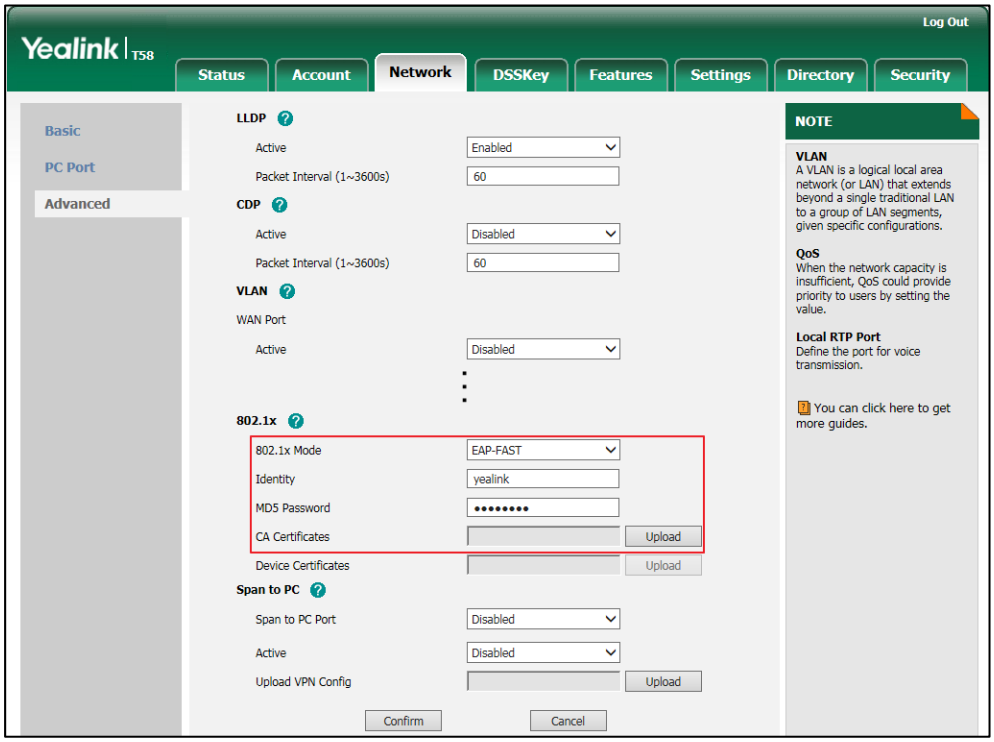


g) If you select **EAP-FAST**:

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

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

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



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

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

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

To configure the 802.1X authentication via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Network**->**802.1x**.
2. Tap 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**:

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

   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. Tap ✔ to accept the change.

   The phone prompts you to reboot the phone.

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

   The settings will take effect after a reboot.

Setting Up Your Phones with a Provisioning Server

This chapter provides basic instructions for setting up your IP phones with a provisioning server.

This chapter consists of the following sections:

- Provisioning Points to Consider
- Provisioning Methods
- Boot Files, Configuration Files and Resource Files
- Setting Up a Provisioning Server
- Upgrading Firmware
- Keeping User Personalized Settings after Auto Provisioning

Provisioning Points to Consider

- If you are provisioning a mass of IP phones, we recommend you to use central provisioning method as your primary configuration method. For more information on central provisioning, refer to Central Provisioning on page 112.
- A provisioning server maximizes the flexibility you have when installing, configuring, upgrading, and managing the IP phones, and enables you to store boot, configuration, log, and contact files on the server. You can set up a provisioning server on the local area network (LAN) or anywhere on the Internet. For more information, refer to Setting Up a Provisioning Server on page 121.
- If the IP phone cannot obtain the address of a provisioning server during startup, and has not been configured with settings from any other source, the IP phone will use configurations stored in the flash memory. If the phone that cannot obtain the address of a

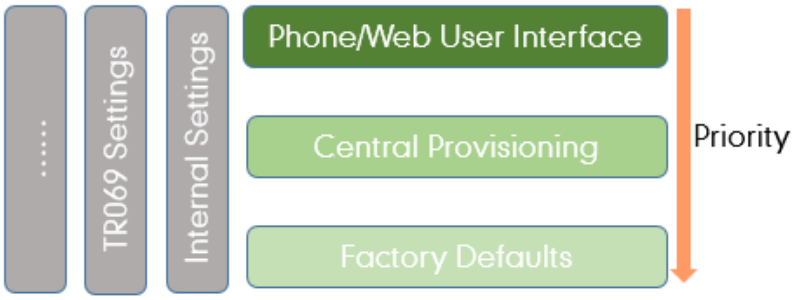
provisioning server has previously been configured with settings it will use those previous settings.

Provisioning Methods

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

There may be a configuration priority among the provisioning methods - settings you make using a higher priority provisioning method override settings made using a lower priority provisioning method.

The precedence order for configuration parameter changes is as follows (highest to lowest):



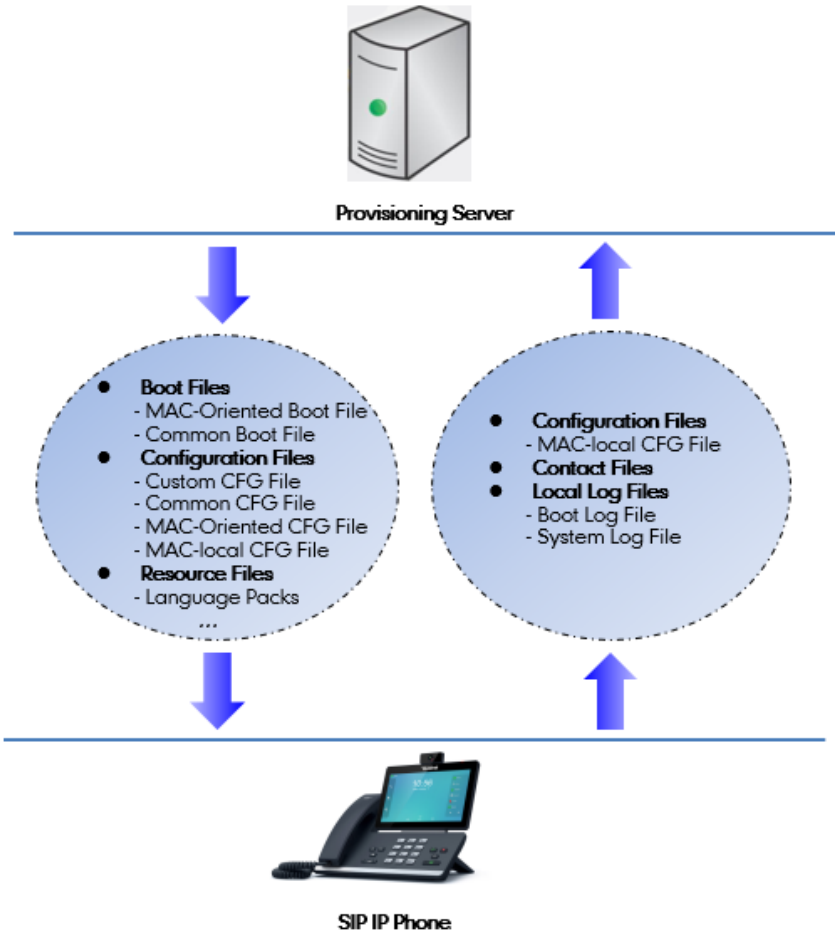
Note

The priority mechanism takes effect only if the value of the parameter "static.auto_provision.custom.protect" is set to 1. For more information on this parameter, refer to Configuration Parameters on page 132.

Static settings have no priority. For example, settings associated with auto provisioning/network/syslog, TR069 settings and internal settings (e.g., the temporary configurations to be used for program running). For more information, refer to Appendix F: Static Settings on page 787.

Central Provisioning

The following figure shows how the phone interoperates with provisioning server when you use the centralized provisioning method:



Using the boot files and configuration files to provision the phones and to modify features and configurations is called the central provisioning method. You can use a text-based editing application to edit boot files and configuration files, and then store boot files and configuration files to a provisioning server. IP phones can be centrally provisioned from a provisioning server. For more information on the provisioning server, refer to Setting Up a Provisioning Server on page 121. For more information on boot files, refer to Boot Files on page 114. For more information on configuration files, refer to Configuration Files on page 116.

IP phones can obtain the provisioning server address during startup. Then IP phones download boot files and 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_SIP-T2_Series_T19(P)_E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*. In addition to the boot files and configuration files, the IP phones also download resource files during auto provisioning. For more information on resource files, refer to Resource Files on page 118.

Yealink IP phones support keeping user personalized configuration settings using the

MAC-local CFG file. For more information on this file, refer to MAC-local CFG File on page 116.

Manual Provisioning

When you manually configure a phone via web user interface or phone user interface, the changes you make will be stored in the MAC-local CFG file. This file is stored on the phone, but a copy can be also uploaded to the provisioning server (if configured). For more information on MAC-local CFG file, refer to MAC-local CFG File on page 116.

There are two ways to manually provision IP phones:

- Web User Interface
- Phone User Interface

Web User Interface

You can configure IP phones via web user interface, a web-based interface that is especially useful for remote configuration. Because features and configurations vary by phone model and firmware version, options available on each page of the web user interface can vary.

An administrator or a user can configure IP phones via web user interface; but accessing the web user interface requires password. The default user name and password for the administrator are both "admin" (case-sensitive). The default user name and password for the user are both "user" (case-sensitive). For more information on configuring passwords, refer to User and Administrator Passwords on page 689.

This method enables you to perform configuration changes on a per-phone basis. Note that the features can be configured via web user interface are limited. So, you can use the web user interface method as the sole configuration method or in conjunction with central provisioning method and phone user interface method. If you are provisioning a mass of IP phones, we recommend you to use central provisioning method as your primary configuration method. For more information on central provisioning, refer to Central Provisioning on page 112.

IP phones support both HTTP and HTTPS protocols for accessing the web user interface. For more information, refer to Web Server Type on page 46.

Phone User Interface

You can configure IP phones via phone user interface on a per-phone basis. As with the web user interface, phone user interface makes configurations available to users and administrators; but the **Advanced** option is only available to administrators and requires an administrator password (default: admin). For more information on configuring password, refer to User and Administrator Passwords on page 689.

If you want to reset all settings made from the phone user interface to default, refer to *Yealink phone-specific user guide*.

Boot Files, Configuration Files and Resource Files

When IP phones are configured with central provisioning method, they will request to download the configuration files and resource files from the provisioning server.

The following sections describe the details of boot files, configuration files and resource files:

- Boot Files
- Configuration Files
- Resource Files
- Obtaining Configuration Files and Resource Files

Boot Files

You can use a boot file to customize the download sequence of configuration files. It is efficiently for you to provision your IP phones in different deployment scenarios, especially when you want to apply a set of features or settings to a group of phones.

Note You can select whether to use the boot file or not for auto provisioning according to your deployment scenario. If you do not use the boot file, proceed to Configuration Files on page 116. That is, you can also use the old mechanism for auto provisioning.

The boot files are valid BOOT files that can be created or edited using a text editor such as UltraEdit. The boot files are first downloaded when you provision the phones using centralized provisioning (refer to Central Provisioning). The configuration parameters are not included in the boot file. You can reference some configuration files that contain parameters in the boot files to be acquired by all your phones and specify the download sequence of these configuration files.

Yealink supports two types of boot files: common boot file and MAC-Oriented boot file.

During auto provisioning, the IP phone first tries to download the MAC-Oriented boot file (refer to MAC-Oriented Boot File), and then download configuration files referenced in the MAC-Oriented boot file in sequence from the provisioning server. If no matched MAC-Oriented boot file is found, the IP phone tries to download the common boot file (refer to Common Boot File) and then downloads configuration files referenced in the common boot file in sequence. If no common boot file is found, the IP phone downloads the common CFG file (refer to Common CFG File) and MAC-Oriented CFG file (refer to MAC-Oriented CFG File) in sequence.

The following figure shows an example of common boot file:

```
#!version:1.0.0.1
#The header above must appear as-is in the first line
include:config <configure/sip.cfg>
include:config "http://10.2.5.206/configure/account.cfg"
```

```
overwrite_mode = 1
```

Learn the following:

- The line beginning with "#" is considered to be a comment.
- The file header "#!version:1.0.0.1" is not a comment and must be placed in the first line. It cannot be edited or deleted.
- Each "include" statement can reference a configuration file. The referenced configuration file format must be *.cfg.
- The contents in the angle brackets or double quotation marks represent the download paths of the referenced configuration files (e.g., http://10.2.5.206/configure/account.cfg). The download path must point to a specific CFG file. The sip.cfg and account.cfg are the specified configuration files to be downloaded during auto provisioning.
- The CFG files are downloaded in the order listed (top to bottom).

The IP phone downloads the boot file first, and then downloads the sip.cfg and account.cfg configuration files from the "configure" directory on the provisioning server in sequence. The parameters in the new downloaded configuration files will override the duplicate parameters in files downloaded earlier.

- "overwrite_mode = 1" means overwrite mode is enabled. The overwrite mode will be applied to the configuration files specified to download. If the value of a parameter in configuration files is left blank or a parameter in configuration files is deleted or commented out, the factory default value can take effect immediately after auto provisioning.

Note Overwrite mode only affects the non-static settings configured using configuration files.
If you do not use the boot file for auto provisioning, overwrite mode is disabled by default and you are not allowed to enable it.

For more information on how to customize boot file, refer to *Yealink_SIP-T2_Series_T19(P)_E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*.

Common Boot File

Common boot file, named y000000000000.boot, is effectual for all phones.

MAC-Oriented Boot File

MAC-Oriented boot file, named <MAC>.boot. It will only be effectual for a specific IP phone. The MAC-Oriented boot file should be created using template boot file in advance.

The MAC-Oriented boot file is named after the MAC address of the IP phone. MAC address, a unique 12-digit serial number assigned to each phone, can be obtained from the bar code on the back of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the

name of the MAC-Oriented boot file is 00156574b150.boot (case-sensitive).

Configuration Files

The configuration files are valid CFG files that can be created or edited using a text editor such as UltraEdit. An administrator can deploy and maintain a mass of Yealink IP phones automatically through configuration files stored on a provisioning server.

Yealink configuration files consist of:

- Common CFG File
- MAC-Oriented CFG File
- MAC-local CFG File
- Custom CFG File

Common CFG File

Common CFG file, named <y0000000000xx>.cfg, 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 following table lists the name of the common CFG file for each IP phone model:

IP Phone Model	Common CFG file
SIP-T58V/A	y000000000058.cfg
SIP-T56A	y000000000056.cfg
CP960	y000000000073.cfg

MAC-Oriented CFG File

MAC-Oriented CFG file, named <MAC>.cfg, contains parameters unique to a particular phone, such as account registration. 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. MAC address, a unique 12-digit serial number assigned to each phone, can be obtained from the bar code on the back of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of the MAC-Oriented CFG file is 00156574b150.cfg (case-sensitive).

MAC-local CFG File

MAC-local CFG file, named <MAC>-local.cfg, contains changes associated with non-static settings that users make via web user interface and phone user interface (for example, updates to time and date formats, ring tones, dial plan and DSS keys). This file generates only if the value of the parameter "static.auto_provision.custom.protect" is set to 1.

The MAC-local CFG file is also named after the MAC address (the bar code label on the back of the IP phone or on the outside of the box) of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of the MAC-local CFG file is 00156574b150-local.cfg (case-sensitive).

Note

After the provisioning priority mechanism is enabled (configured by the parameter "static.auto_provision.custom.protect"), all older changes made via web/phone user interface will not be saved in the <MAC>-local.cfg file. But the older settings still take effect on the phone. For more information on this parameter, refer to Configuration Parameters on page 132.

Keeping User Personalized Settings

The MAC-local CFG file is stored locally on the IP phone and can also be uploaded to the provisioning server/a specific URL (if configured, refer to Configuration Parameters). This file enables users to keep their personalized configuration settings, even though the IP phone reboots or upgrades. For more information on how to keep user personalized settings, refer to Keeping User Personalized Settings after Auto Provisioning on page 132.

Users can also select to clear the user personalized configuration settings. Users can clear the MAC-local CFG file using the following methods:

- To clear the MAC-local CFG file, reset the IP phone to factory configuration settings by selecting **Reset local settings** via phone user interface (navigate to **Settings**->**Advanced Settings** (default password: admin) ->**Reset Config**).
- To clear the MAC-local CFG file, reset the IP phone to factory configuration settings by navigating to the **Upgrade** menu via web user interface and clicking **Reset local setting**.

Configurations defined never be saved to the <MAC>-local.cfg file

Most configurations made by users via phone user interface and web user interface can be saved to the <MAC>-local.cfg file, but some static settings will never be saved to the <MAC>-local.cfg file. For more information, refer to Appendix F: Static Settings on page 787.

You need to reset the phone configurations not saved in the <MAC>-local.cfg file separately. For more information, refer to Resetting Issues on page 752.

By default, the <MAC>-local.cfg file will be stored on the IP phone. The IP phone can be configured to upload this file to the provisioning server each time the file updates. For more information, refer to the parameter "static.auto_provision.custom.sync" described in the section Configuration Parameters on page 132.

Custom CFG File

You can create some new CFG files (e.g., sip.cfg, account.cfg) containing any combination of configuration parameters. This especially useful when you want to apply a set of features or settings to a group of phones using the boot file.

For more information on how to create a new CFG file, refer to *Yealink_SIP-T2_Series_T19(P)E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*.

Resource Files

When configuring some particular features, you may need to upload resource files to IP phones. Resource files are optional, but if the particular feature is being employed, these files are required.

If the resource file is to be used for all IP phones of the same model, the access URL of resource file is best specified in the common CFG file. However, if you want to specify the desired phone to use the resource file, the access URL of resource file should be specified in the MAC-Oriented CFG file. During provisioning, the IP phones will request the resource files in addition to the configuration files. For more information on the access URL of resource file, refer to the corresponding section in this guide.

The followings show examples of resource files:

- Language packs
- Ring tones
- Local contact file

For more information on resource files, refer to Obtaining Configuration Files and Resource Files on page 119.

If you want to delete resource files from a phone at a later date - for example, if you are giving the phone to a new user - you can reset the IP phone to factory configuration settings. For more information, refer to Resetting Issues on page 752.

Obtaining Configuration Files and Resource Files

Yealink supplies some template configuration files and resource files for you, so you can directly edit and customize the files as required. You can ask the distributor or Yealink FAE for template files. You can also obtain the template files online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

The names of the Yealink-supplied template files are:

Template File		File Name	Description
Boot File		y000000000000.boot	Allows you to customize the download sequence of the configuration files during auto provisioning. For more information, refer to Boot Files on page 114.
Configuration Files	Common CFG File	Common.cfg	Allow you to deploy and maintain a mass of Yealink IP phones. For more information, refer to Common CFG File and MAC-Oriented CFG File on page 116.
	MAC-Oriented CFG File	MAC.cfg	
	Custom CFG Files	For example, sip.cfg account.cfg	Allow you to apply a set of features or settings to a group of Yealink IP phones. For more information, refer to Custom CFG File on page 117.
Resource Files	AutoDST Template	AutoDST.xml	Allows you to add or modify time zone and DST settings for your area. For more information, refer to Customizing an AutoDST Template File on page 202.
	Language Packs	For example, 000.GUI.English.lang 1.English_note.xml	Allow you to customize the translation of the existing language on the phone/web user interface. For more information, refer to Loading Language Packs on page 206.

Template File		File Name	Description
		1.English.js	
	Replace Rule Template	dialplan.xml	Allows you to customize multiple replace rules for IP phone dial plan. For more information, refer to Customizing Replace Rule Template File on page 230.
	Dial Now Template	dialnow.xml	Allows you to customize multiple dial now rules for IP phone dial plan. For more information, refer to Customizing Dial-now Template File on page 236.
	Softkey Layout Template (not applicable to CP960 IP phones)	CallFailed.xml CallIn.xml Connecting.xml Dialing.xml RingBack.xml Talking.xml	Allow you to customize soft key layout for different call states. For more information, refer to Customizing Softkey Layout Template File on page 217.
	Super Search Template	super_search.xml	Allows you to customize the search source list for your IP phone. For more information, refer to Customizing a Super Search Template File on page 260.
	Local Contact File	contact.xml	Allows you to add or modify multiple contacts at a time for your IP phone. For more information, refer to Customizing a Local Contact File on page 268.
	Remote Phone Book Template	Department.xml Menu.xml	Allows you to add or modify multiple remote contacts for your IP phone. For more information, refer to Customizing Remote Phone Book Template File on page 453.

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 extracted and identify the template file you will edit according to the table introduced above.

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	**Support:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } (including space) **Not Support:** | < > : " / \ * ? # % & = +	**Support:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } % & = + (including space) **Not Support:** | < > : " / \ * ? #
Linux	**Support:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } | < > : " (including space) **Not Support:** / \ * ? # % & = +	**Support:** ~ ` ! @ $ ^ ( ) _ - , . ' ; [ ] { } | < > : " % & = + (including space) **Not Support:** / \ * ? #

Setting Up a Provisioning Server

This chapter provides basic instructions for setting up a provisioning server and deploying phones from the provisioning server.

This chapter consists of the following sections:

- Why Using a Provisioning Server?
- Supported Provisioning Protocols
- Configuring a Provisioning Server
- Deploying Phones from the Provisioning Server

Why Using a Provisioning Server?

You can use a provisioning server to configure your IP phones. A provisioning server allows for flexibility in upgrading, maintaining and configuring the phone. Configuration files, resource files and log files are normally located on this server.

When IP phones are triggered to perform auto provisioning, it will request to download the configuration files from the provisioning server. During the auto provisioning process, the IP phone will download and update configuration files to the phone flash. For more information on

auto provisioning, refer to *Yealink_SIP-T2_Series_T19(P) E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*.

The IP phones can be configured to periodically upload the log files to a provisioning server, which can help an administrator more easily find the system problem and fix it. For more information log files, refer to Viewing Log Files on page 721.

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 phone will be used.

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

Configuring a Provisioning Server

The provisioning server can be set up 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_SIP-T2_Series_T19(P) E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*.

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 boot files and then edit them as desired.
5. Create configuration files and edit them as desired.
6. 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 123.

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 per-line basis.

Deploying Phones from the Provisioning Server

During auto provisioning, IP phones download the boot file first, and then download the configuration files referenced in the boot file in sequence. The parameters in the new downloaded configuration files will override the duplicate parameters in files downloaded earlier. For more information on boot files and configuration files, refer to Boot Files on page 114 and Configuration Files on page 116.

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 boot 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>.boot files by using the template boot file.
   c) Specify the configuration files paths in the file as desired.
2. Edit the common boot file by performing the following step:
   a) Specify the configuration files paths in the file as desired.
3. Create per-phone configuration files by performing the following steps:
   a) Create per-phone <MAC>.cfg files by using the MAC-Oriented CFG file from the distribution as templates.
   b) Edit the parameters in the file as desired.
4. Create new common configuration files by performing the following steps:
   a) Create <y0000000000xx>.cfg files by using the Common CFG file from the distribution as templates.
   b) Edit the parameters in the file as desired.
5. Copy boot files and configuration files to the home directory of the provisioning server.
6. Reboot IP phones to trigger the auto provisioning process.

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

For protecting against unauthorized access, you can encrypt configuration files. For more information on encrypting configuration files, refer to Encrypting and Decrypting Files on page 712.

Note During auto provisioning, the IP phone tries to download the MAC-Oriented boot file first. If no matched MAC-Oriented boot file is found on the server, the IP phone tries to download the common boot file. If the MAC-Oriented boot file and common boot file exist simultaneously on the provisioning server, the common boot file will be ignored after the IP phone successfully downloads the matched MAC-Oriented boot file.

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

the provisioning server address:

- **Zero Touch:** Zero Touch feature guides you to configure network settings and the provisioning server address via phone user interface after startup.
- **PnP**: PnP feature allows IP phones to discover the provisioning server address by broadcasting the PnP SUBSCRIBE message during startup.
- **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_SIP-T2_Series_T19(P)_E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*.

Upgrading Firmware

This section provides information on upgrading the IP phone firmware. Two methods of firmware upgrade:

- Manually, from the local system for a single phone.
- Automatically, from the provisioning server for a mass of phones.

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 Example
SIP-T58V/T58A/T56A	58.x.x.x.rom	58.80.0.10.rom
CP960	73.x.x.x.rom	73.80.0.10.rom

Note

You can download the latest firmware online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage.

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

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the way for the IP phone to check for configuration files. **Parameters:** static.auto_provision.power_on static.auto_provision.repeat.enable static.auto_provision.repeat.minutes static.auto_provision.weekly.enable static.auto_provision.weekly.begin_time static.auto_provision.weekly.end_time static.auto_provision.weekly.dayofweek static.auto_provision.flexible.enable static.auto_provision.flexible.interval static.auto_provision.flexible.begin_time static.auto_provision.flexible.end_time
		Specify the access URL of firmware. **Parameter:** static.firmware.url
Web User Interface		Configure the way for the IP phone to check for configuration files. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-autop&q=load
		Upgrade firmware. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-upgrade&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.auto_provision.power_on	**0 or 1**	**1**

Parameters	Permitted Values	Default
Description: Triggers the power on feature to on or off. **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		
static.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 perform an auto provisioning process repeatedly. **Web User Interface:** Settings->Auto Provision->Repeatedly **Phone User Interface:** None		
static.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. **Note**: It works only if the value of the parameter "static.auto_provision.repeat.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Interval(Minutes) **Phone User Interface:** None		
static.auto_provision.weekly.enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Triggers the weekly feature to on or off. **0**-Off **1**-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		
static.auto_provision.weekly.begin_time	**Time from 00:00 to 23:59**	**00:00**
Description: Configures the begin time of the day for the IP phone to perform an auto provisioning process weekly. **Note**: It works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Time **Phone User Interface:** None		
static.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. **Note**: It works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Time **Phone User Interface:** None		
static.auto_provision.weekly.dayofweek	**0, 1, 2, 3, 4, 5, 6 or a combination of these digits**	**0123456**

Parameters	Permitted Values	Default
Description: Configures the days of the week for the IP phone to perform an auto provisioning process weekly. **0**-Sunday **1**-Monday **2**-Tuesday **3-**Wednesday **4**-Thursday **5**-Friday **6**-Saturday **Example**: static.auto_provision.weekly.dayofweek = 01 It means the IP phone will perform an auto provisioning process every Sunday and Monday. **Note**: It works only if the value of the parameter "static.auto_provision.weekly.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Day of Week **Phone User Interface:** None		
static.auto_provision.flexible.enable	**0 or 1**	**0**
Description: Triggers the flexible feature to on or off. **0**-Off **1**-On If it is set to 1 (On), the IP phone will perform an auto provisioning process at random between a starting time configured by the parameter "static.auto_provision.flexible.begin_time" and an ending time configured by the parameter "static.auto_provision.flexible.end_time" on a random day within the period configured by the parameter "static.auto_provision.flexible.interval". **Note**: The day within the period is decided based upon the phone's MAC address and does not change with a reboot whereas the time within the start and end is calculated again with every reboot. **Web User Interface:** Settings->Auto Provision->Flexible Auto Provision **Phone User Interface:**		

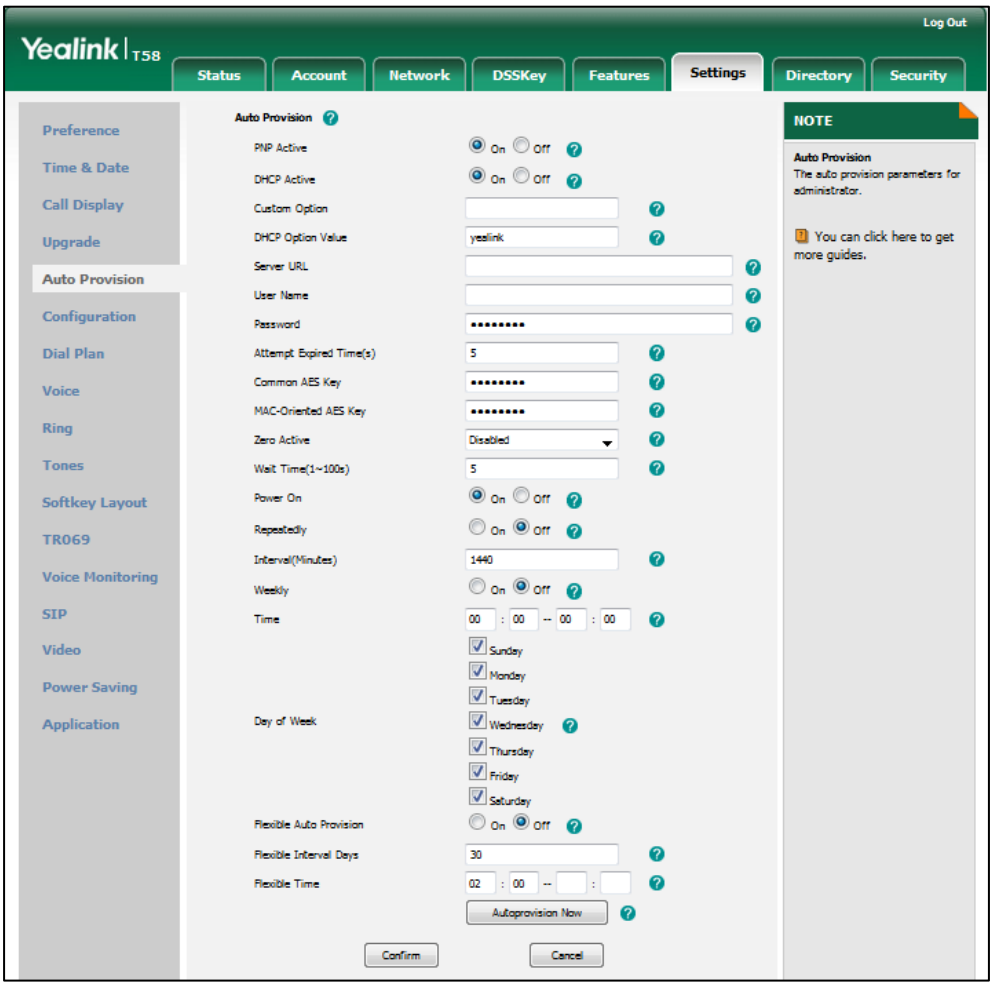
Parameters	Permitted Values	Default
None		
static.auto_provision.flexible.interval	**Integer from 1 to 1000**	**1**
Description: Configures the interval (in days) for the IP phone to perform an auto provisioning process. The auto provisioning occurs on a random day within this period based on the phone's MAC address. **Example**: static.auto_provision.flexible.interval = 30 The IP phone will perform an auto provisioning process on a random day (e.g., 18) based on the phone's MAC address. **Note**: It works only if the value of the parameter "static.auto_provision.flexible.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Flexible Interval Days **Phone User Interface:** None		
static.auto_provision.flexible.begin_time	**Time from 00:00 to 23:59**	**02:00**
Description: Configures the starting time of the day for the IP phone to perform an auto provisioning process at random. **Note**: It works only if the value of the parameter "static.auto_provision.flexible.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Flexible Time **Phone User Interface:** None		
static.auto_provision.flexible.end_time	**Time from 00:00 to 23:59**	**Blank**
Description: Configures the ending time of the day for the IP phone to perform an auto provisioning process at random. If it is left blank or set to a specific value equal to starting time configured by the parameter "static.auto_provision.weekly.begin_time", the IP phone will perform an auto provisioning		

Parameters	Permitted Values	Default
process at the starting time. If it is set to a specific value greater than starting time configured by the parameter "static.auto_provision.weekly.begin_time", the IP phone will perform an auto provisioning process at random between the starting time and ending time. It it is set to a specific value less than starting time configured by the parameter "static.auto_provision.weekly.begin_time", the IP phone will perform an auto provisioning process at random between the starting time on that day and ending time in the next day. **Note**: It works only if the value of the parameter "static.auto_provision.flexible.enable" is set to 1 (On). **Web User Interface:** Settings->Auto Provision->Flexible Time **Phone User Interface:** None		
static.firmware.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the firmware file. **Example:** static.firmware.url = http://192.168.1.20/58.80.0.5.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.



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.

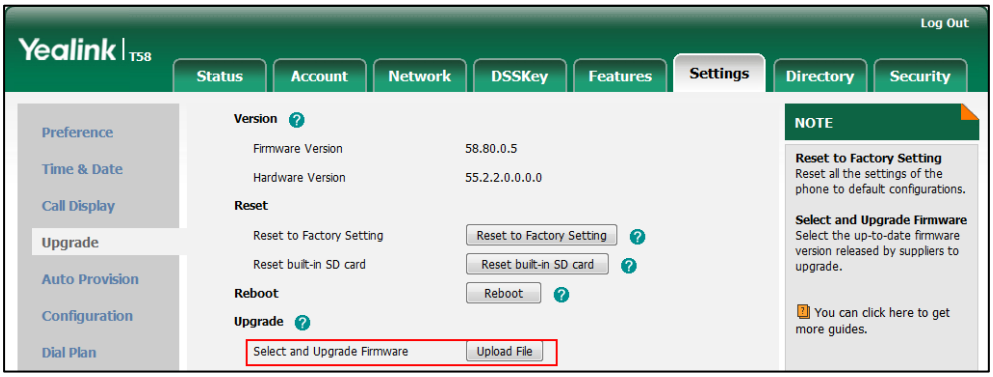
Upgrading Firmware via Web User Interface

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 **Upload File** to locate and upload the required firmware from your local system.



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!".

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

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

Keeping User Personalized Settings after Auto Provisioning

Generally, the administrator deploys phones in batch and timely maintains company phones via auto provisioning, yet some users would like to keep the personalized settings (e.g., ring tones, wallpaper, dial plan, time format or DSS keys), after auto provisioning.

Note Yealink IP phones support FTP, TFTP, HTTP and HTTPS protocols for uploading the MAC-local CFG file. This section takes the TFTP protocol as an example. Before performing the following, make sure the provisioning server supports uploading.

If you are using the HTTP/HTTPS server, you can specify the way the IP phone uploads the MAC-local CFG file to the provisioning server. It is determined by the value of the parameter "static.auto_provision.custom.upload_method".

Configuration Parameters

The following table lists the configuration parameters used to determine the phone behavior for keeping user personalized settings:

Parameters	Permitted Values	Default
static.auto_provision.custom.protect	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to keep user personalized settings after auto provisioning. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), <MAC>-local.cfg file generates and personalized non-static settings configured via web or phone user interface will be kept after auto provisioning. **Note**: The provisioning priority mechanism (phone/web user interface >central provisioning >factory defaults) takes effect only if the value of this parameter is set to 1 (Enabled). If the value of the parameter "overwrite_mode" is set to 1 in the boot file, the value of this parameter will be forced to set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		
static.auto_provision.custom.sync	**0 or 1**	**0**
Description: Enables or disables the IP phone to upload the <MAC>-local.cfg file to the server each time the file updates, and download the <MAC>-local.cfg file from the server during auto provisioning. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will upload the <MAC>-local.cfg file to the provisioning server or a specific server each time the file updates to back up this file. During auto provisioning, the IP phone will download the <MAC>-local.cfg file from the provisioning server or a specific server to override the one stored on the phone. **Note**: It works only if the value of the parameter "static.auto_provision.custom.protect" is set to 1 (Enabled). The upload/download path is configured by the parameter "static.auto_provision.custom.sync.path". **Web User Interface:** None **Phone User Interface:** None		

Parameters	Permitted Values	Default
static.auto_provision.custom.sync.path	**URL**	**Blank**
Description: Configures the URL for uploading/downloading the <MAC>-local.cfg file. If it is left blank, the IP phone will try to upload/download the <MAC>-local.cfg file to/from the root directory of provisioning server. **Note**: It works only if the value of the parameter "static.auto_provision.custom.sync" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		
static.auto_provision.custom.upload_method	**0 or 1**	**0**
Description: Configures the way the IP phone uploads the <MAC>-local.cfg file to the provisioning server (for HTTP/HTTPS server only). **0**-PUT **1**-POST **Note**: It works only if the value of the parameter "static.auto_provision.custom.sync" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		

For more information on how to configure these parameters in different scenarios, refer to the following introduced scenarios.

Scenario A Keep user personalized configuration settings

The administrator wishes to upgrade firmware from the old version to the latest version. Meanwhile, keep user personalized settings after auto provisioning and upgrade.

For more information on the flowchart of keep user personalized configuration settings, refer to Appendix E: Auto Provisioning Flowchart (Keep User Personalized Configuration Settings) on page 786.

Scenario Conditions:

- SIP-T58V IP phone current firmware version: 58.80.0.1. This firmware supports keeping personalized settings and generating a <MAC>-local.cfg file.
- SIP-T58V IP phone target firmware version: 58.80.0.5. This firmware supports keeping personalized settings and generating a <MAC>-local.cfg file.
- SIP-T58V IP phone MAC: 001565770984
- Provisioning server URL: tftp://192.168.1.211
- Place the target firmware to the root directory of the provisioning server.

The old firmware version supports keeping personalized settings and generating a <MAC>-local.cfg file. To keep user personalized settings after auto provisioning and upgrade, you need to configure the value of the parameter "static.auto_provision.custom.protect" to 1 in the configuration file.

Do one of the following operations:

Scenario Operations I:

1. Add/Edit the following parameters in the y000000000058.cfg file or 001565770984.cfg file you want the IP phone to download:

```
static.auto_provision.custom.protect = 1

static.auto_provision.custom.sync = 1

static.firmware.url = tftp://192.168.1.211/58.80.0.5.rom
```

2. Trigger the IP phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to *Triggering the IP Phone to Perform the Auto Provisioning* section in *Yealink_SIP-T2_Series_T19(P) E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*.

   During auto provisioning, the IP phone first downloads the y000000000058.cfg file, and then downloads firmware from the root directory of the provisioning server.

   The IP phone reboots to complete firmware upgrade, and then starts auto provisioning process again which is triggered by phone reboot (the power on mode is enabled by default). It downloads the y000000000058.cfg, 001565770984.cfg and the 001565770984-local.cfg file in sequence from the provisioning server, and then updates configurations in these downloaded configuration files orderly to the IP phone system. The IP phone starts up successfully, and the personalized settings in the 001565770984-local.cfg file are kept after auto provisioning.

   When a user customizes feature configurations via web/phone user interface, the IP phone will save the personalized configuration settings to the 001565770984-local.cfg file on the IP phone, and then upload this file to the provisioning server each time the file updates.

Note If a configuration item is both in the downloaded MAC-local.cfg file and Common CFG file/MAC-Oriented CFG file, setting of the configuration item in the MAC-local CFG file will be written and saved to the IP phone system.

Scenario Operations II:

1. Add/Edit the following parameters in the y000000000058.cfg file or 001565770984.cfg file you want the IP phone to download:

```
static.auto_provision.custom.protect = 1
static.auto_provision.custom.sync = 0
static.firmware.url = tftp://192.168.1.211/58.80.0.5.rom
```

2. Trigger the IP phone to perform the auto provisioning process. For more information on how to trigger auto provisioning process, refer to *Triggering the IP Phone to Perform the Auto Provisioning* section in *Yealink_SIP-T2_Series_T19(P) E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*.

During auto provisioning, the IP phone first downloads the y000000000058.cfg file, and then downloads firmware from the root directory of the provisioning server.

The IP phone reboots to complete firmware upgrade, and then starts auto provisioning process again which is triggered by phone reboot (the power on mode is enabled by default). It downloads the y000000000058.cfg and 001565770984.cfg files in sequence, and then updates configurations in the downloaded configuration files orderly to the IP phone system. As the value of the parameter "static.auto_provision.custom.protect" is set to 1, configurations in the 001565770984-local.cfg file saved on the IP phone are also updated.

The IP phone starts up successfully, and personalized settings are kept after auto provisioning. When a user customizes feature configurations via web/phone user interface, the IP phone will save the personalized settings to the 001565770984-local.cfg file on the IP phone only.

Note

In this scenario, the IP phone will not upload the MAC-local.cfg file to provisioning server and request to download the MAC-local.cfg file from provisioning server during auto provisioning.

If a configuration item is both in the MAC-local.cfg file on the IP phone and Common CFG file/ MAC-Oriented CFG file downloaded from auto provisioning server, setting of the configuration item in the MAC-local CFG file will be written and saved to the IP phone system.

If value of the parameter "static.auto_provision.custom.protect" is set to 0, the personalized settings in the 001565770984-local.cfg file will be overridden after auto provisioning, no matter what the value of the parameter "static.auto_provision.custom.sync" is.

Scenario B Clear user personalized configuration settings

When the IP phone is gave to a new user but many personalized configurations settings of last user are saved on the phone; or when the end user encounters some problems because of the wrong configurations, the administrator or user may wish to clear user personalized configuration settings via phone user interface.

Scenario Conditions:

- SIP-T58V IP phone MAC: 001565770984
- The current firmware of the phone is 58.80.0.5 or later.
- Provisioning server URL: tftp://192.168.1.211
- static.auto_provision.custom.protect = 1

Note

The **Reset local settings** option on the web/phone user interface appears only if the value of the parameter "static.auto_provision.custom.protect" was set to 1.

If the value of the parameter "static.auto_provision.custom.sync" is set to 1, the 001565770984-local.cfg file on the provisioning server will be cleared.

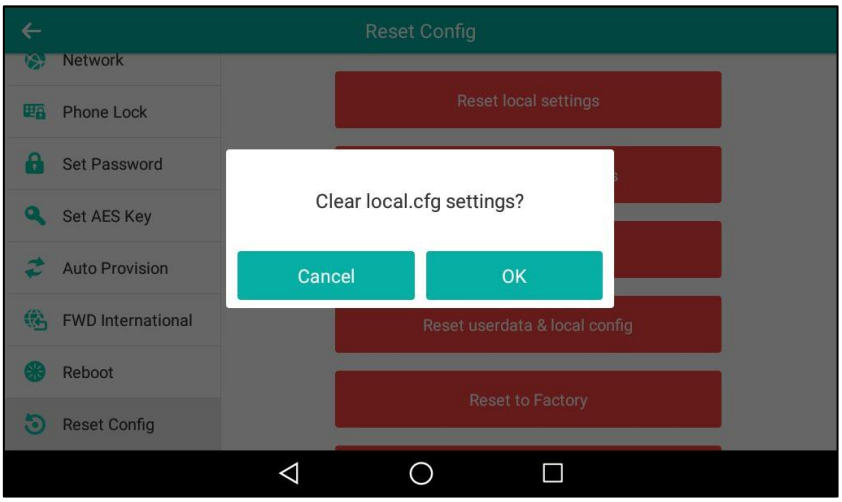
Scenario Operations:

You can clear the personalized configuration settings of the phone via phone or web user interface.

To clear personalized configuration settings via phone user interface:

1. Tap **Settings->Advanced** (default password: admin) ->**Reset Config**.
2. Tap **Reset local settings**.

   The touch screen prompts "Clear local.cfg settings?".



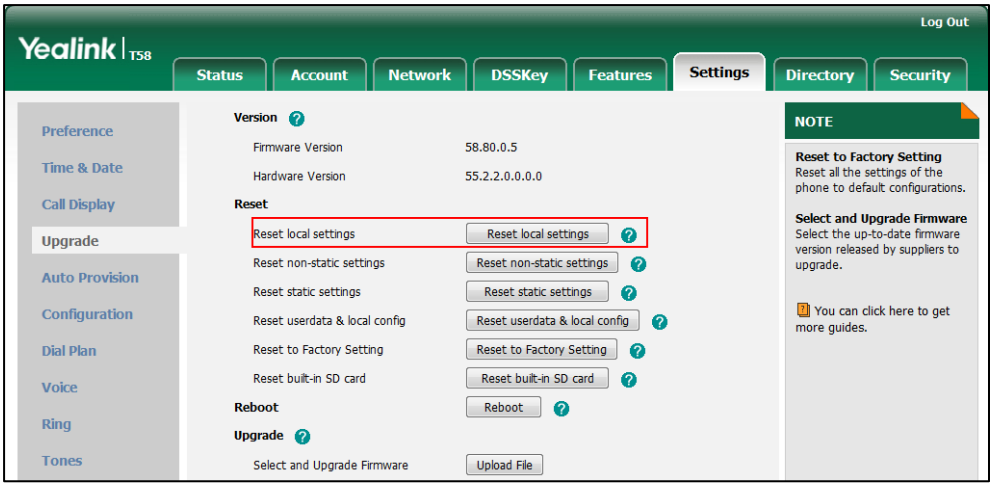
3. Tap **OK**.

The touch screen prompts "Reset local settings, Please wait...".

To clear personalized configuration settings via web user interface:

1. Click on **Settings**->**Upgrade**.

2. Click **Reset local settings**.



The web user interface prompts "Clear local.cfg settings?".

3. Click **OK**.

Configurations in the 001565770984-local.cfg file saved on the phone will be cleared. If the IP phone is triggered to perform auto provisioning after resetting local configuration, it will download the configuration files from the provisioning server and update the configurations to the phone system. As there is no configuration in the 001565770984-local.cfg file, configurations in the y000000000058.cfg/001565770984.cfg file will take effect. If there are no configuration files on the provisioning server, the IP phone will be reset to factory defaults.

Note As the static settings are never saved in the <MAC>-local.cfg file, you need to reset the static settings separately by clicking **Reset static settings** option.

Scenario C Keep user personalized settings after factory reset

The IP phone requires factory reset when it has a breakdown, but the user wishes to keep personalized settings of the phone after factory reset.

Scenario Conditions:

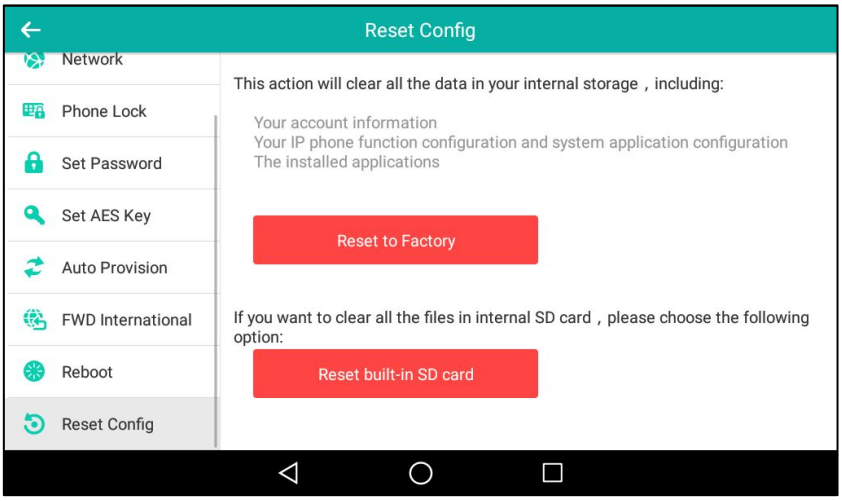
- SIP-T58V IP phone MAC: 001565770984
- Provisioning server URL: tftp://192.168.1.211
- static.auto_provision.custom.sync = 1

Note As the parameter "static.auto_provision.custom.sync" was set to 1, the 001565770984-local.cfg file on the IP phone will be uploaded to the provisioning server at tftp://192.168.1.211.

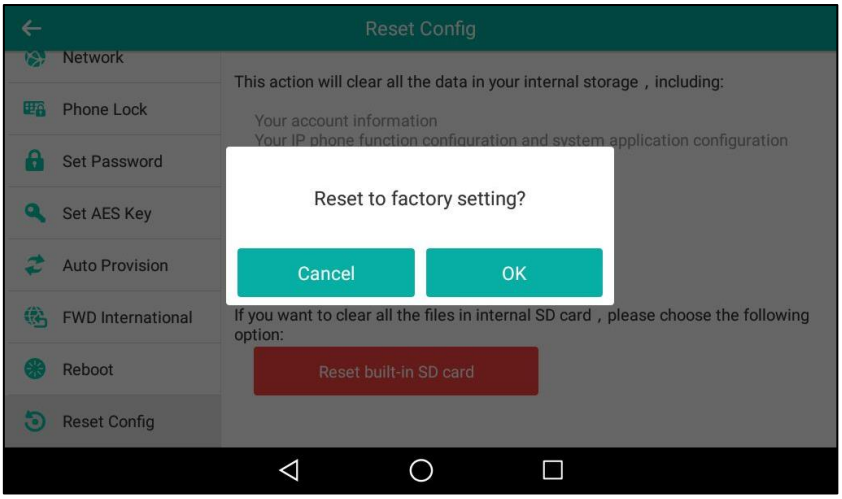
You can keep the personalized settings of the phone after factory reset via phone or web user interface.

To reset the phone to factory via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Reset Config**.
2. Tap **Reset to Factory**.



The touch screen prompts the following warning:



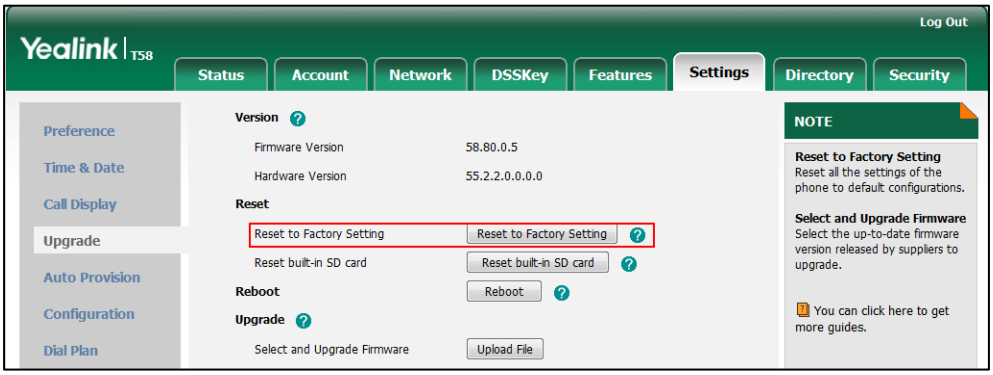
3. Tap **OK**.

The touch screen prompts "Resetting to factory, please wait...".

To reset the phone to factory via web user interface:

1. Click on **Settings**->**Upgrade**.

2. Click **Reset to Factory Setting** to reset the phone.



The web user interface prompts "Do you want to reset to factory?".

3. Click **OK**.

After startup, all configurations of the phone will be reset to factory defaults. So the value of the parameter "static.auto_provision.custom.sync" will be reset to 0. Configurations in the 001565770984-local.cfg file saved on the IP phone will also be cleared. But configurations in the 001565770984-local.cfg file stored on the provisioning server (tftp://192.168.1.211) will not be cleared after reset.

To retrieve personalized settings of the phone after factory reset:

1. Set the values of the parameters "static.auto_provision.custom.sync" and "static.auto_provision.custom.protect" to be 1 in the configuration file (y000000000058.cfg or 001565770984.cfg).
2. Trigger the phone to perform the auto provisioning process.

   As the value of the parameter "static.auto_provision.custom.sync" is set to 1, the IP phone will download the 001565770984-local.cfg file from the provisioning server to override the one stored on the phone. So the configurations in 001565770984-local.cfg file will be updated and stored on the IP phone during auto provisioning. As the value of the parameter "static.auto_provision.custom.protect" is set to 1, the personalized configuration settings will be kept after auto provisioning. As a result, the personalized configuration settings of the phone are retrieved after factory reset.

Scenario D Import or export the local configuration file

The administrator or user can export the local configuration file to check the personalized settings of the phone configured by the user, or import the local configuration file to configure or change settings of the phone.

Scenario Conditions:

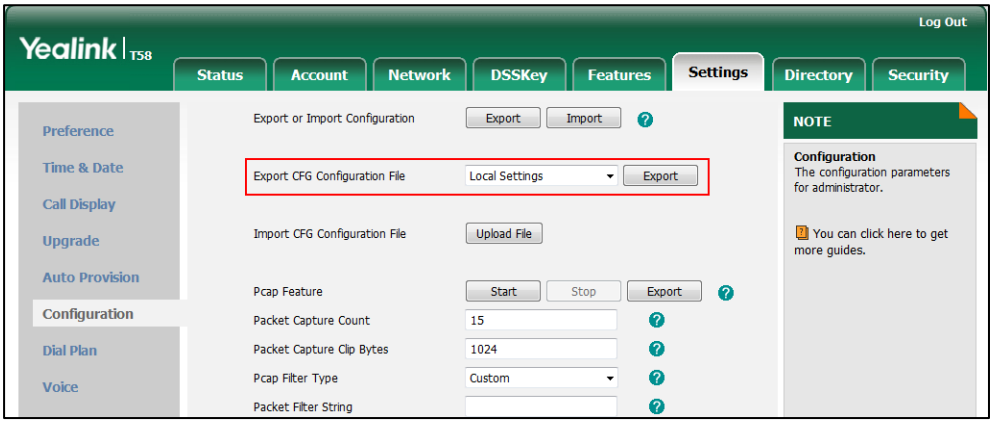
- SIP-T58V IP phone MAC: 001565770984
- The current firmware of the phone is 58.80.0.5 or later.
- Provisioning server URL: tftp://192.168.1.211

Note As the personalized settings of the phone cannot be changed via auto provisioning when the value of the parameter "static.auto_provision.custom.protect" is set to 1, it is cautious to change the settings in the <MAC>-local.cfg file before importing it.

Scenario Operations:

To export local configuration file via web user interface:

1. Click on **Settings**->**Configuration**.
2. Select **Local Settings** from the pull-down list of **Export CFG Configuration File**, and then click **Export** to open file download window, and then save the 001565770984-local.cfg file to the local system.

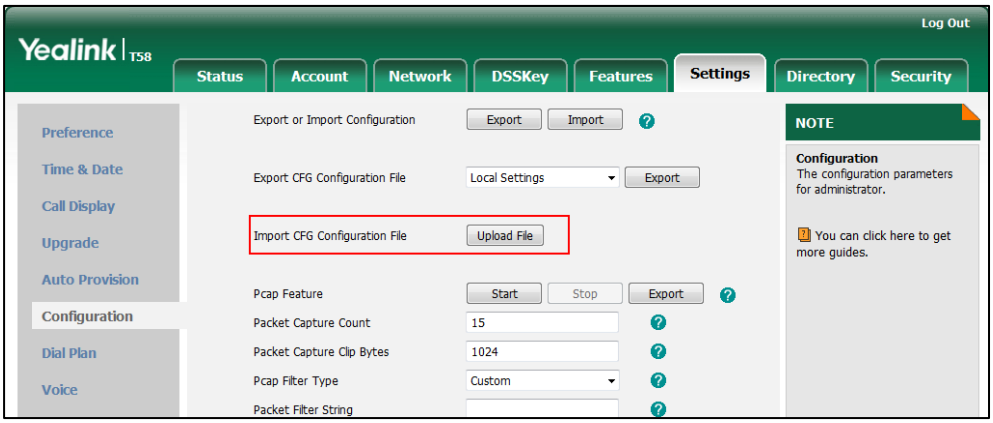


The administrator or user can edit the 001565770984-local.cfg file after exporting.

To import local configuration file via web user interface:

1. Click on **Settings**->**Configuration**.

2. In the **Import CFG Configuration File** field, click **Upload File** to locate and import the 001565770984-local.cfg file from your local system.



The configurations in the imported 001565770984-local.cfg file will override the one in the existing local configuration file. The configurations only in the existing local configuration file will not be cleared. As a result, the configurations in the new 001565770984-local.cfg file contain the configurations only in the existing local configuration file and those in the imported 001565770984-local.cfg file. And this new 001565770984-local.cfg file will be saved to the phone flash and take effect.

Note If the value of the parameter "static.auto_provision.custom.sync" is set to 1, and the 001565770984-local.cfg file is successfully imported, the new 001565770984-local.cfg file will be uploaded to the provisioning server and overrides the existing one on the server.

Configuring Basic Features

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

- Power Indicator LED
- Notification Popups
- Wallpaper
- Screen Saver
- Power Saving
- Backlight
- Bluetooth
- Enable Page Tips
- Page Tips for Expansion Module
- Account Registration
- Multiple Line Keys per Account
- Call Display
- Display Method on Dialing
- Web Server Type
- Time and Date
- Language
- Softkey Layout
- Key As Send
- Dial Plan
- Emergency Dialplan
- Hotline
- Off Hook Hot Line Dialing
- Search Source List In Dialing
- Save Call Log
- Call List Show Number
- Missed Call Log
- Local Directory
- Live Dialpad
- Speed Dial

- Call Waiting
- Auto Redial
- Auto Answer
- IP Direct Auto Answer
- Allow IP Call
- Accept SIP Trust Server Only
- Call Completion
- Anonymous Call
- Anonymous Call Rejection
- Do Not Disturb (DND)
- Busy Tone Delay
- Return Code When Refuse
- Early Media
- 180 Ring Workaround
- Use Outbound Proxy in Dialog
- SIP Session Timer
- Session Timer
- Call Hold
- Call Forward
- Call Transfer
- Local Conference
- Network Conference
- Transfer on Conference Hang Up
- Feature Key Synchronization
- Transfer Mode via Dsskey
- Directed Call Pickup
- Group Call Pickup
- Dialog Info Call Pickup
- Recent Call In Dialing
- ReCall
- Call Number Filter
- Call Park
- Calling Line Identification Presentation (CLIP)
- Connected Line Identification Presentation (COLP)

- Mute
- Intercom
- Call Timeout
- Ringing Timeout
- Send user=phone
- SIP Send MAC
- SIP Send Line
- Reserve # in User Name
- Password Dial
- Unregister When Reboot
- 100 Reliable Retransmission
- Reboot in Talking
- Answer By Hand
- Call Recording Using Soft Key
- Silent Mode
- Door Phone
- Mobile Account
- Quick Login
- CSTA Control

Power Indicator LED

Power indicator LED indicates power status and phone status. It is not applicable to CP960 IP phones.

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.

Ringing Power Light Flash

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

Voice/Text Mail Power Light Flash

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

Mute Power Light Flash

Mute Power Light Flash allows the power indicator LED to flash when a call is muted.

Hold/Held Power Light Flash

Hold/Held Power Light Flash 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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the power indicator LED. **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_flash_enable phone_setting.hold_and_held_power_led_flash_enable phone_setting.talk_and_dial_power_led_enable
Web User Interface		Configure the power indicator LED. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-powerled&q=load

Details of Configuration Parameters:

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. **0**-Disabled (power indicator LED is off) **1**-Enabled (power indicator LED is solid red) **Note**: It is not applicable to CP960 IP phones. **Web User Interface:**		

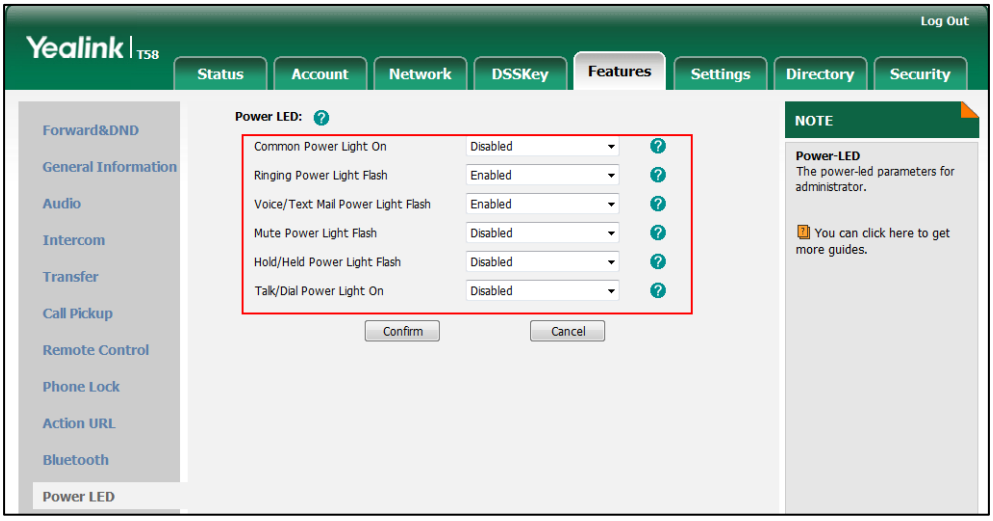
Parameters	Permitted Values	Default
Features->Power LED->Common Power Light On **Phone User Interface:** None		
phone_setting.ring_power_led_flash_enable	**0 or 1**	**1**
Description: Enables or disables the power indicator LED to flash when the IP phone receives an incoming call. **0**-Disabled (power indicator LED does not flash) **1**-Enabled (power indicator LED fast flashes (300ms) red) **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Power LED->Ringing Power Light Flash **Phone User Interface:** None		
phone_setting.mail_power_led_flash_enable	**0 or 1**	**1**
Description: Enables or disables the power indicator LED to flash when the IP phone receives a voice mail. **0**-Disabled (power indicator LED does not flash) **1**-Enabled (power indicator LED slowly flashes (1000ms) red) **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Power LED->Voice/Text 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 muted. **0**-Disabled (power indicator LED does not flash) **1**-Enabled (power indicator LED fast flashes (300ms) red) **Note**: It is not applicable to CP960 IP phones. **Web User Interface:**		

Parameters	Permitted Values	Default
Features->Power LED->Mute Power Light Flash **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 a call is placed on hold or is held. **0**-Disabled (power indicator LED does not flash) **1**-Enabled (power indicator LED fast flashes (500ms) red) **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Power LED->Hold/Held Power Light Flash **Phone User Interface:** None		
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. **0**-Disabled (power indicator LED is off) **1**-Enabled (power indicator LED is solid red) **Note**: It is not applicable to CP960 IP phones. **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/Text 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**.

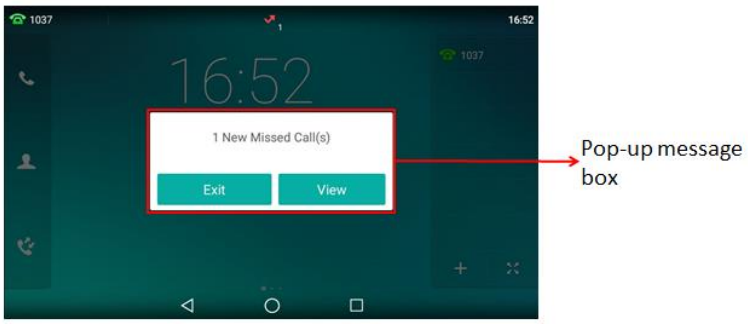


8. Click **Confirm** to accept the change.

Notification Popups

Notification popups feature allows the IP phone to display the pop-up message box when it misses a call, forwards an incoming call to other party or receives a new voice mail.

The following shows an example of missing a call:



Procedure

Notification popups can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure notification popups. **Parameters:** features.voice_mail_popup.enable features.missed_call_popup.enable features.forward_call_popup.enable
Web User Interface		Configure notification popups.

	Navigate to: http://<phoneIPAddress>/servlet?m=mod_data&p=features-notifypop&q=load

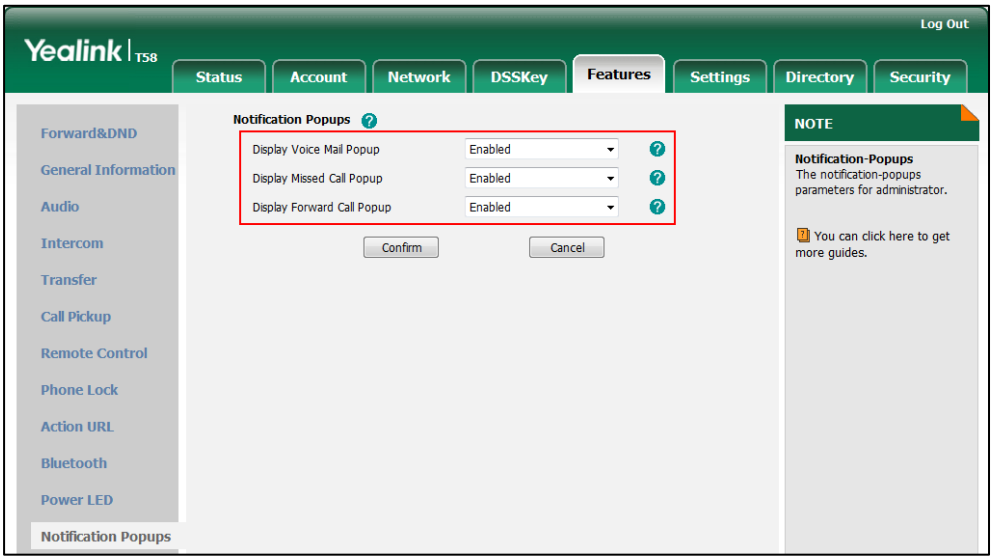
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.voice_mail_popup.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to display the pop-up message box when it receives a new voice mail. **0**-Disabled **1**-Enabled **Note**: If the voice mail pop-up message box disappears, it won't pop up again unless the user receives a new voice mail or the user re-registers the account that has unread voice mail(s). **Web User Interface:** Features->Notification Popups->Display Voice Mail Popup **Phone User Interface:** None		
features.missed_call_popup.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to display the pop-up message box when it misses a call. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Notification Popups->Display Missed Call Popup **Phone User Interface:** None		
features.forward_call_popup.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to display the pop-up message box when it forwards an incoming call to other party. **0**-Disabled		

Parameters	Permitted Values	Default
1-Enabled **Web User Interface:** Features->Notification Popups->Display Forward Call Popup **Phone User Interface:** None		

To configure the notification popups via web user interface:

1. Click on **Features**->**Notification Popups**.
2. Select the desired value from the pull-down list of **Display Voice Mail Popup**.
3. Select the desired value from the pull-down list of **Display Missed Call Popup.**
4. Select the desired value from the pull-down list of **Display Forward Call Popup**.



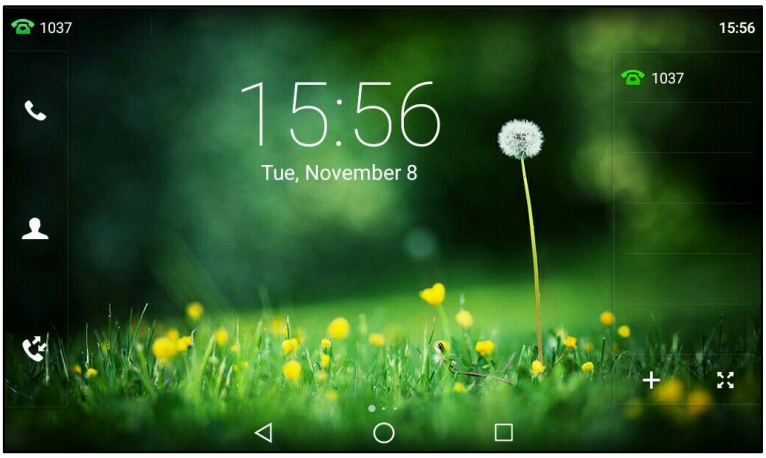
5. Click **Confirm** to accept the change.

Wallpaper

Wallpaper is an image used as the background of the IP phone idle screen and EXP50 (if connected). Users can select an image from phone's built-in background or customize wallpaper from personal pictures. To set the custom wallpaper as the IP phone/EXP50 background, you need to upload the custom wallpaper to the IP phone in advance.

For SIP-T58V/T58A/T56A IP phones, you can also set a custom picture stored in local or USB flash drive as the wallpaper. To set wallpapers stored in a USB flash drive, make sure the USB flash drive containing pictures is connected to your phone. For more information, refer to Connecting the Optional USB Flash Drive on page 18.

The wallpaper must be the image in jpg/png/bmp/jpeg format.



Note The wallpaper will display on the entire screen. Note that the line key labels, time and date, icons, and Android keys will display over the wallpaper.

Procedure

Wallpaper can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the wallpaper displayed on the IP phone. **Parameter:** phone_setting.backgrounds
		Configure the wallpaper displayed on the EXP50. **Parameter:** expansion_module.backgrounds
		Specify the access URL of the custom wallpaper. **Parameter:**

		wallpaper_upload.url
Web User Interface		Configure the wallpaper displayed on the IP phone. Configure the wallpaper displayed on the EXP50. Upload the custom wallpaper. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-preference&q=load
Phone User Interface		Configure the wallpaper displayed on the IP phone. Configure the wallpaper displayed on the EXP50.

Details of the Configuration Parameters:

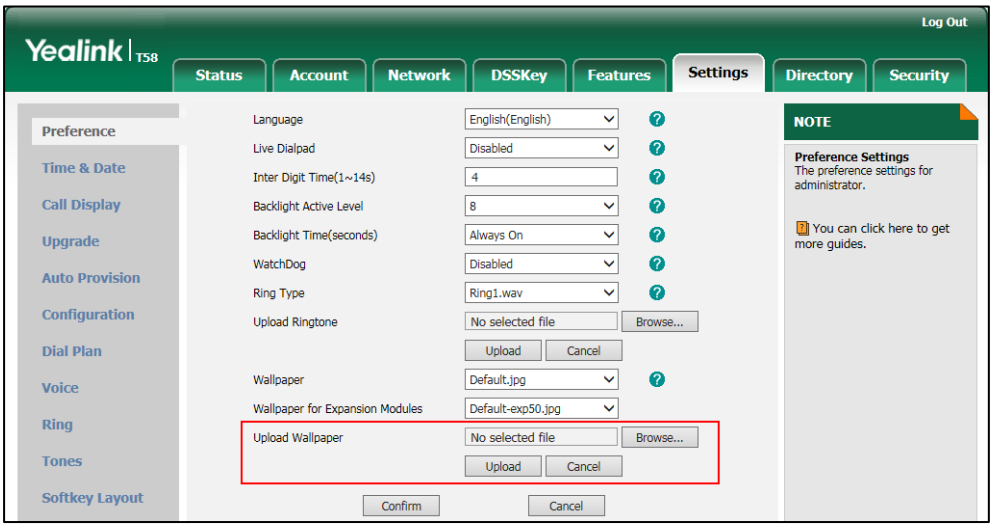
Parameters	Permitted Values	Default
phone_setting.backgrounds	**Refer to the following content**	**Default.jpg**
Description: Configures the wallpaper displayed on the IP phone idle screen. **Permitted Values:** Default.jpg, 01.jpg, 02.jpg, 03.jpg, 04.jpg, 05.jpg, 06.jpg, 07.jpg, 08.jpg, 09.jpg or 10.jpg or custom wallpaper name (e.g., wallpaper.jpg) **Example:** phone_setting.backgrounds = Default.jpg **Web User Interface:** Settings->Preference->Wallpaper **Phone User Interface:** Settings->Basic->Display->Wallpaper		
expansion_module.backgrounds	**Refer to the following content**	**Default-exp50.jpg**
Description: Configures the wallpaper displayed on the EXP50. **Permitted Values:**		

Parameters	Permitted Values	Default
Default-exp50.jpg, 01-exp50.jpg, 02-exp50.jpg, 03-exp50.jpg, 04-exp50.jpg, 05-exp50.jpg, 06-exp50.jpg, 07-exp50.jpg, 08-exp50.jpg, 09-exp50.jpg or 10-exp50.jpg or custom wallpaper name (e.g., wallpaper.jpg) **Example:** expansion_module.backgrounds = Default-exp50.jpg **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Settings->Preference->Wallpaper for Expansion Modules **Phone User Interface:** Settings->Basic->Display->EXP Background		
wallpaper_upload.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the wallpaper image. **Example:** wallpaper_upload.url = http://192.168.10.25/wallpaper.jpg **Note**: The format of the wallpaper image must be *jpg, *.png, *.bmp, *.jpeg. The uploaded custom picture will apply to the IP phones and the connected EXP50. **Web User Interface:** Settings->Preference->Upload Wallpaper **Phone User Interface:** None		

To upload custom wallpaper via web user interface:

1. Click on **Settings**->**Preference**.

2. In the **Upload Wallpaper** field, click **Browse** to locate the wallpaper image from your local system.

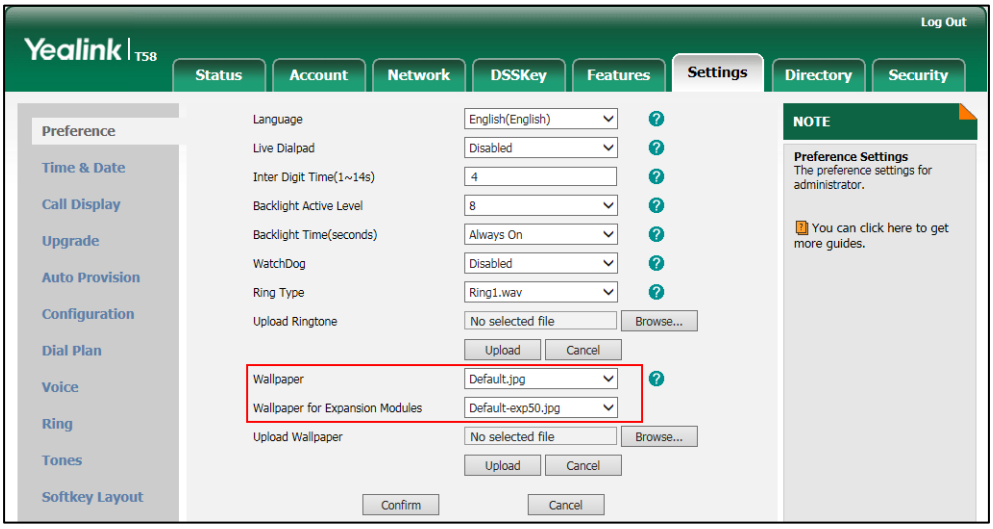


3. Click **Upload** to upload the file.

The uploaded custom picture will apply to the IP phones and the connected EXP50, and appears in the pull-down lists of **Wallpaper** and **Wallpaper for Expansion Modules** synchronously.

To change the wallpaper via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired wallpaper from the pull-down list of **Wallpaper**/**Wallpaper for Expansion Modules**.



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

To change the wallpaper via phone user interface:

1. Swipe down from the top of the screen or swipe left/right to go to the second idle screen.
2. Tap **Settings**->**Basic**->**Display**->**Wallpaper**/**EXP Background**.

3. Do one of the following:

   - Tap **Gallery**.

     Select a desired Gallery album.

     Tap a desired picture to preview, and then tap **Set wallpaper/Set as exp background**.

   - Tap **Wallpapers**.

     Do one of the following:

     - Select a desired wallpaper from the recently used wallpaper list, and then tap **Set wallpaper/Set as exp background**.
     - Tap **Pick image**.

       Tap **Recent** on the top-left of the touch screen.

       Do one of the following:

       - Tap **Images** to see all pictures stored in internal SD card or USB flash drive.
       - Tap **Downloads** to see all pictures you have downloaded.
       - Tap **Gallery** to see all pictures by using **Gallery** application.

         Select a desired picture to preview.

         Tap **Set wallpaper/Set as exp background**.

Screen Saver

The screen saver will automatically start each time the IP phone is idle a certain amount of time. You can stop the screen saver and return to the idle screen at any time by pressing a key on the phone or tapping the touch screen. For SIP-T58V/T58A/T56A IP phones, if you connect a color-screen expansion module EXP50 to the IP phone, the screen saver will start or stop on the phone and EXP50 synchronously.

The IP phone supports four screen saver types: Clock, Colors, Photo Frame and Photo Table. You can only configure the screen saver via phone user interface.

To configure the screen saver via phone user interface:

1. Swipe down from the top of the screen or swipe left/right to go to the second idle screen.
2. Tap **Settings**->**Basic**->**Display**->**Screen Saver**.
3. Tap the **Screen Saver Wait Time** field.
4. Tap the desired time in the pop-up dialog box.
5. Do one of the following:

   - Tap the **Clock** radio box.

     (Optional.) Tap next to the radio box.

     - Tap the **Style** field to set the clock type to **Analog** or **Digital**.
     - Tap the **Night mode** checkbox to display the screensaver dimly for dark rooms.

     Tap to return to the Screen Saver setting screen.

- Tap the **Colors** radio box.
- Tap the **Photo Frame** radio box.

  Tap next to the radio box to select the desired Gallery album(s).

  Tap the desired checkbox or **SELECT ALL** on the top-right of the touch screen.

  Tap to return to the Screen Saver setting screen.
- Tap the **Photo Table** radio box.

  Tap next to the radio box to select the desired Gallery album(s).

  Tap the desired checkbox or **SELECT ALL** on the top-right of the touch screen.

  Tap to return to the Screen Saver setting screen.

6. Tap to accept the change or to cancel.

Power Saving

The power-saving feature is used to turn off the backlight and screen to conserve energy. The IP phone enters power-saving mode after it has been idle for a certain period of time. And the IP phone will exit power-saving mode if a phone event occurs - for example, if the phone has an incoming call or message, or you press a key on the phone or tap the touch screen.

For SIP-T58V/T58A/T56A IP phones, if you connect a color-screen expansion module EXP50 to the IP phone, the IP phone and EXP50 will enter or exit power-saving mode synchronously.

If the screen saver (refer to Screen Saver) is enabled on your phone, power-saving mode will still occur. For example, if a screen saver is configured to display after the phone is idle for 5 minutes, and power-saving mode is configured to turn off the backlight and screen after the phone is idle for 15 minutes, the backlight and screen will be turned off after the screen saver displays for 10 minutes.

You can configure the following power-saving settings:

- **Office Hour**: Configures the starting time and ending time of the day's office hour for each day of the week. You can configure power saving around your work schedule.
- **Idle TimeOut (minutes)**: Configures the period of time before the IP phone enters power-saving mode. You can configure different idle timeouts for office hours and off hours (evenings and weekends). You can also specify a separate timeout period that applies after you use the phone.

By default, the Office Hours Idle TimeOut is much longer than the Off Hours Idle TimeOut. If you use the IP phone, the idle timeout that applies (User Input Extension Idle TimeOut or Office Hours/Off Hours Idle TimeOut) is the timeout with the highest value. If the phone has an incoming call or message, the User Input Extension Idle TimeOut will be ignored.

Note For SIP-T58V/T58A/T56A IP phones, if you disable the power saving feature, the IP phone will automatically enter power-saving mode to protect the screen when the phone is inactive for 72 hours. Image persistence may be caused on LCD if power saving is disabled.

Procedure

Power saving can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the power saving intelligent mode. **Parameter:** features.power_saving.intelligent_mode
		Configure the power saving feature. **Parameter:** features.power_saving.enable
		Configure the office hour. **Parameters:** features.power_saving.office_hour.monday features.power_saving.office_hour.tuesday features.power_saving.office_hour.wednesday features.power_saving.office_hour.thursday features.power_saving.office_hour.friday features.power_saving.office_hour.saturday features.power_saving.office_hour.sunday
		Configure the idle timeout. **Parameters:** features.power_saving.office_hour.idle_timeout features.power_saving.off_hour.idle_timeout features.power_saving.user_input_ext.idle_timeout
Web User Interface		Configure the power saving feature. Configure the office hour. Configure the idle timeout. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-powersaving&q=load

Details of the Configuration Parameters:

Parameters	Permitted Values	Default
features.power_saving.intelligent_mode	**0 or 1**	**1**
Description: Enables or disables the power saving intelligent mode.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone stays in power-saving mode even if the office hour arrives the next day. If it is set to 1 (Enabled), the IP phone will automatically identify the office hour and exit power-saving mode once the office hour arrives the next day. **Web User Interface:** None **Phone User Interface:** None		
features.power_saving.enable	**0 or 1**	**1**
Description: Enables or disables the power saving feature. **0**-Disabled **1**-Enabled **Note**: For CP960 IP phones, the power saving feature is enabled by default. It is not applicable to CP960 IP phones. **Web User Interface:** Settings->Power Saving->Power Saving **Phone User Interface:** None		
features.power_saving.office_hour.idle_timeout	**Refer to the following content**	**Refer to the following content**
Description: Configures the time (in minutes) to wait in the idle state before the IP phone enters power-saving mode during the office hours. **Permitted Values:** 1 to 960 (for SIP-T58V/T58A/T56A) 1 to 240 (for CP960) **For SIP-T58V/T58A/T56A:** The default value is 960. **For CP960:** The default value is 120.		

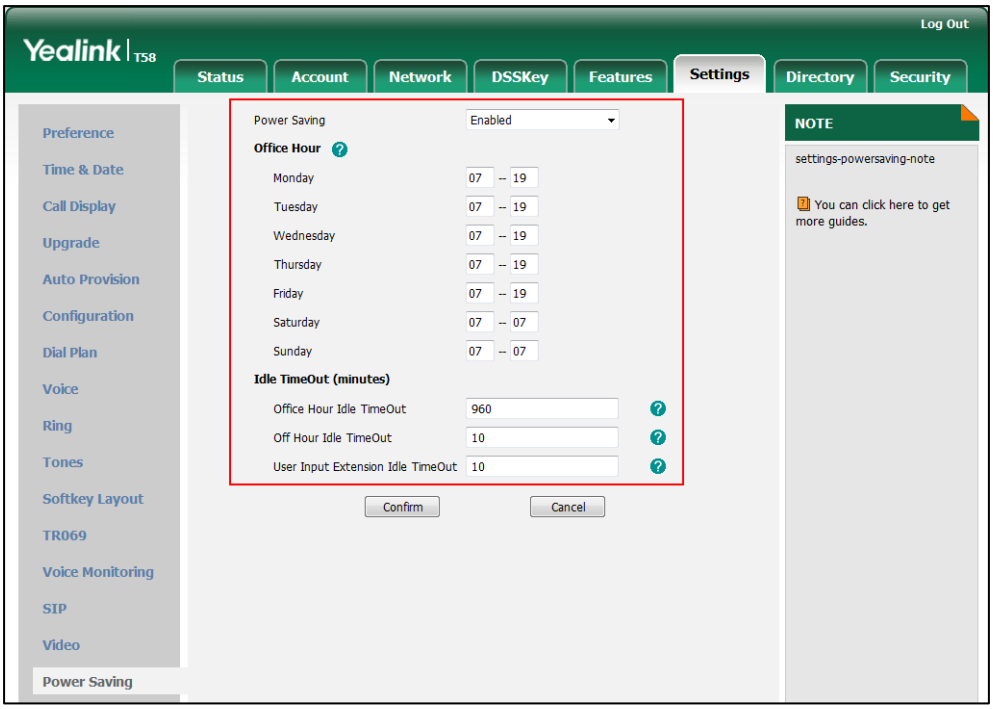
Parameters	Permitted Values	Default
Example: features.power_saving.office_hour.idle_timeout = 120 The IP phone will enter power-saving mode when it has been inactivated for 120 minutes (2 hours) during the office hours. **Web User Interface:** Settings->Power Saving->Office Hour Idle TimeOut **Phone User Interface:** None		
features.power_saving.off_hour.idle_timeout	**Integer from 1 to 10**	**10**
Description: Configures the time (in minutes) to wait in the idle state before the IP phone enters power-saving mode during the non-office hours. **Example**: features.power_saving.off_hour.idle_timeout = 5 The IP phone will enter power-saving mode when it has been inactivated for 5 minutes during the non-office hours. **Web User Interface:** Settings->Power Saving->Off Hour Idle TimeOut **Phone User Interface:** None		
features.power_saving.user_input_ext.idle_timeout	**Integer from 1 to 30**	**10**
Description: Configures the minimum time (in minutes) to wait in the idle state - after using the phone - before the IP phone enters power-saving mode. **Example**: features.power_saving.user_input_ext.idle_timeout = 5 **Web User Interface:** Settings->Power Saving->User Input Extension Idle TimeOut **Phone User Interface:** None		
features.power_saving.office_hour.monday **features.power_saving.office_hour.tuesday**	**Integer from 0 to 23, Integer from**	**7,19** **7,19**

Parameters	Permitted Values	Default
features.power_saving.office_hour.wednesday	**0 to 23**	**7,19**
features.power_saving.office_hour.thursday		**7,19**
features.power_saving.office_hour.friday		**7,19**
features.power_saving.office_hour.saturday		**7,7**
features.power_saving.office_hour.sunday		**7,7**
Description: Configures the starting time and ending time of the day's office hour. Starting time and ending time are separated by a comma. **Example**: features.power_saving.office_hour.monday = 7,19 **Web User Interface:** Settings->Power Saving->Monday/Tuesday/Wednesday/Thursday/Friday/Saturday/Sunday **Phone User Interface**: None		

To configure the power saving feature via web user interface:

1. Click on **Settings**->**Power Saving**.
2. Enter the starting time and ending time respectively in the desired day field.
3. Enter the desired value (1-960) in the **Office Hours Idle TimeOut** field.
4. Enter the desired value (1-10) in the **Off Hours Idle TimeOut** field.

5. Enter the desired value (1-30) in the **User Input Extension Idle TimeOut** field.



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

Backlight

Backlight determines the brightness of the touch screen display, allowing users to read easily in dark environments. Backlight time specifies the delay time to turn off the backlight 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-T58V/T58A/T56A/CP960 IP phones and EXP50 (connected to SIP-T58V/T58A/T56A IP phones).

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

- **Always On:** Backlight is turned on permanently.
- **15s**, **30s**, **60s**, **120s**, **300s**, **600s** or **1800s:** Backlight is turned off when the IP phone is inactive after a preset period of time (in seconds), but it is automatically turned on if the status of the IP phone changes or any key is pressed.

Backlight Active Level is used to adjust the backlight intensity of the touch screen when the phone is active. Backlight Active Level is applicable to SIP-T58V/T58A/T56A/CP960 IP phones and EXP50 (connected to SIP-T58V/T58A/T56A IP phones).

Procedure

Backlight can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the backlight of the touch screen. **Parameters:**

		phone_setting.active_backlight_level phone_setting.backlight_time
Web User Interface		Configure the backlight of the touch screen. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-preference&q=load
Phone User Interface		Configure the backlight of the touch screen.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.active_backlight_level	**Integer from 1 to 10**	**8**
Description: Configures the intensity of the touch screen when the phone is active. 10 is the highest intensity. It configures the LCD's intensity of the IP phone and the connected EXP50. **Web User Interface:** Settings->Preference->Backlight Active Level **Phone User Interface:** Settings->Basic->Display->Backlight->Backlight Active Level		
phone_setting.backlight_time	**0, 15, 30, 60, 120, 300, 600 or 1800**	**0**
Description: Configures the delay time (in seconds) before the backlight is turned off when the IP phone is inactive. **0**-Always On **15**-15 **30**-30 **60**-60 **120**-120 **300**-300 **600**-600 **1800**-1800 If it is set to 0 (Always On), the backlight will not be turned off when the IP phone is inactive. If it is set to 60 (60), the backlight will be turned off when the IP phone is inactivated for 60		

seconds.

Web User Interface:

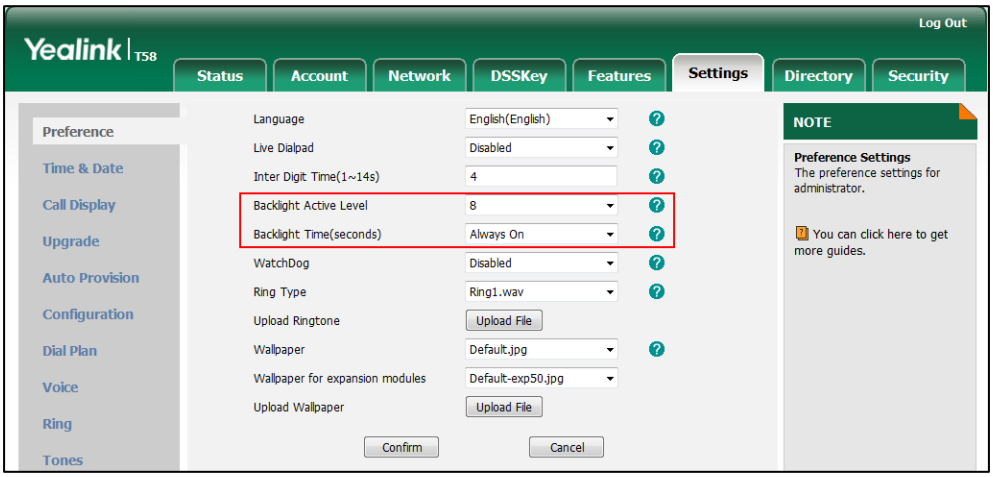
Settings->Preference->Backlight Time(seconds)

Phone User Interface:

Settings->Basic->Display->Backlight->Backlight Time

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 Active Level**.
3. Select the desired value from the pull-down list of **Backlight Time(seconds)**.



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

To configure the backlight via phone user interface:

1. Tap **Settings**->**Basic**->**Display**->**Backlight**.
2. Drag the **Backlight Active Level** slider.
3. Tap the **Backlight Time** field.
4. Tap the desired time in the pop-up dialog box.
5. Tap ✓ to accept the change.

Bluetooth

Bluetooth enables low-bandwidth wireless connections within a range of 10 meters (32 feet). The best performance is in the 1 to 2 meters (3 to 6 feet) range. You can pair and connect the Bluetooth-enable mobile phone with your phone, and make and receive mobile calls on the IP phone.

For CP960 IP phones, you can also use your IP phone as a Bluetooth speaker for your mobile phone and set up a conference among the calls on your IP phone, the PC and connected mobile phone. For more information, refer to *Yealink CP960 user guide*.

For SIP-T58V/T58A/T56A IP phones, you can also connect the other Bluetooth devices (e.g., Bluetooth headset or smart media phone) with your phone. And you can transfer files via Bluetooth, sharing images/videos with other Bluetooth devices. For more information, refer to *Yealink phone-specific user guide*.

You can personalize the Bluetooth device name for the IP phone. The pre-configured Bluetooth device name will display in scanning list of other devices. It is helpful for the other Bluetooth devices to identify and pair with your IP phone.

Procedure

Bluetooth mode can be configured using the following methods.

<table>
<tr><td rowspan="4">Central Provisioning (Configuration File)</td><td rowspan="4"><y0000000000xx>.cfg</td><td>Configure Bluetooth mode.
Parameter:
features.bluetooth_enable</td></tr>
<tr><td>Configure the Bluetooth device name.
Parameter:
features.bluetooth_adapter_name</td></tr>
<tr><td>Configure the Bluetooth permission during the call.
Parameter:
phone_setting.bluetooth_talk.enable</td></tr>
<tr><td>Configure the Bluetooth media audio feature.
Parameter:
bluetooth.a2dp_sink</td></tr>
<tr><td colspan="2">Web User Interface</td><td>Configure Bluetooth mode.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=features-bluetooth&q=load</td></tr>
<tr><td colspan="2">Phone User Interface</td><td>Configure Bluetooth mode.
Configure the Bluetooth device name.</td></tr>
</table>

Details of the Configuration Parameters:

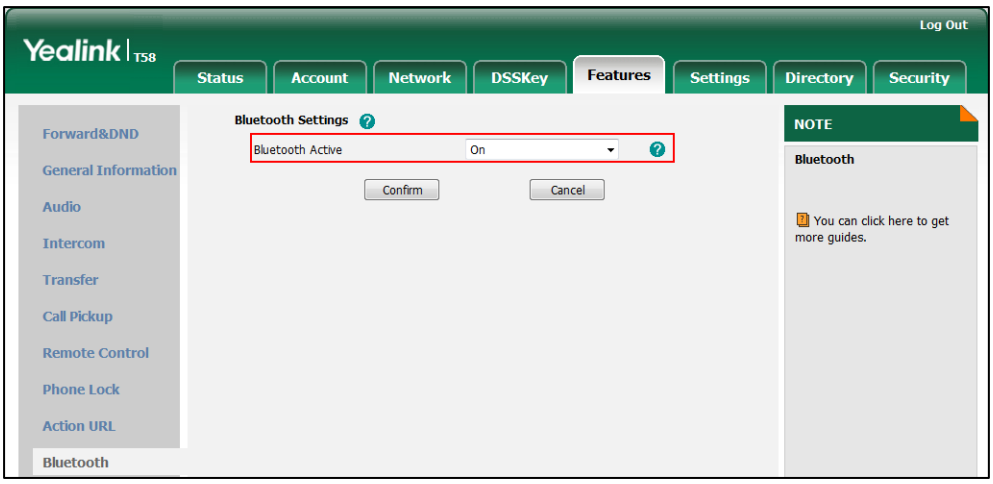
Parameters	Permitted Values	Default
features.bluetooth_enable	**0 or 1**	**0**
Description: Triggers Bluetooth mode to on or off. **0**-Off **1**-On **Note:** To use a Bluetooth headset or connect a Bluetooth device, you must trigger Bluetooth mode to on. **Web User Interface:** Features->Bluetooth->Bluetooth Active **Phone User Interface:** Settings->Basic->Bluetooth->Bluetooth		
features.bluetooth_adapter_name	**String within 64 characters**	**Refer to the following content**
Description: Configures the Bluetooth device name. **For SIP-T58V/A IP phones**: The default value is Yealink-T58. **For SIP-T56A IP phones**: The default value is Yealink-T56A. **For CP960 IP phones**: The default value is Yealink-CP960. **Note**: It works only if the value of the parameter "features.bluetooth_enable" is set to 1 (On). **Web User Interface:** None **Phone User Interface:** Settings->Basic->Bluetooth->Bluetooth (On) ->Edit My Device Information->Device Name		
phone_setting.bluetooth_talk.enable	**0 or 1**	**1**
Description: Enables or disables the user to have the permission to use the Bluetooth feature during the		

Parameters	Permitted Values	Default
call. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
bluetooth.a2dp_sink	**0, 1 or 2**	**1**
Description: Enables or disables the IP phone to receive Bluetooth media audio. **0**-Disabled **1**-Enabled, and you need to activate the Bluetooth media audio manually via phone user interface **2**-Enabled, and the Bluetooth media audio is activated automatically after the Bluetooth-enable mobile phone is connected **Note**: It is only applicable to CP960 IP phones. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** Bluetooth->Bluetooth (On) -> ->Media audio		

To active the Bluetooth mode via web user interface:

1. Click on **Features**->**Bluetooth**.

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



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

To active the Bluetooth mode via phone user interface:

1. Tap **Settings**->**Basic**->**Bluetooth**.
2. Tap the **On** radio box in the **Bluetooth** field.

   The IP phone scans the available Bluetooth devices automatically.

To edit device information via phone user interface:

1. Tap **Settings**->**Basic**->**Bluetooth**.
2. Tap the **On** radio box in the **Bluetooth** field.
3. Tap **Edit My Device Information**.

   The touch screen displays the device name and MAC address. The MAC address cannot be edited.
4. Enter the desired name in the **Device Name** field.
5. Tap ✓ to accept the change.

To activate media audio via phone user interface (only applicable to CP960 IP phones):

1. Do one of the following:
   - Tap .
   - Swipe down from the top of the screen to enter the control center.

     Long tap **Bluetooth**.
   - Tap **Settings** from the home screen.

     Tap **Bluetooth** from the **Basic** block.
2. The touch screen displays the paired and connected mobile phone.
3. Tap after the connected mobile phone name.
4. Tap the switch button in **Media audio** field.
5. Tap ✓ to accept the change.

Enable Page Tips

Enable page tips feature allows users to enable the breathing light or page icon to indicate statuses. It is mainly used in the scenario of configuring multiple line keys (more than six).

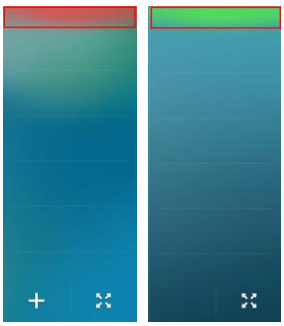
For SIP-T58V/T58A/T56A IP phones, if enable page tips feature is enabled, the breathing light will appear at the top/bottom of the DSS key field when the status of particular feature (e.g., BLF) assigned to the line key on the non-current page changes.

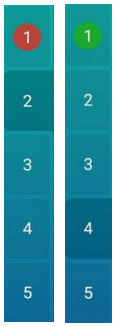
For CP960 IP phones, if enable page tips feature is enabled, the corresponding page icon will turn red/green when the status of particular feature (e.g., BLF) assigned to the line key on the non-current page changes.

The breathing light will flash red or green for different line key types:

Line Key Type	Color Type
Call Park	Red
Intercom	Red
Line	Green
BLF	Red

The following table shows breathing light and page icon to indicate statuses:

Phone Models	Breathing Light	Description
SIP-T58V/T58A/ T56A	(Drag up to view the desired feature key)	• There is a parked call to the line on the non-current page. • The intercom target extension receives an incoming intercom call on the non-current page. • The line receives an incoming call on the non-current page. • The call of the line is hold on the non-current page. • The BLF monitored user receives an incoming call on the non-current page.
	 (Drag down to view the desired feature key)	

Phone Models	Breathing Light	Description
CP960	 (Tap corresponding page icon to view the desired feature key)	

Procedure

Enable page tips can be configured using the following methods.

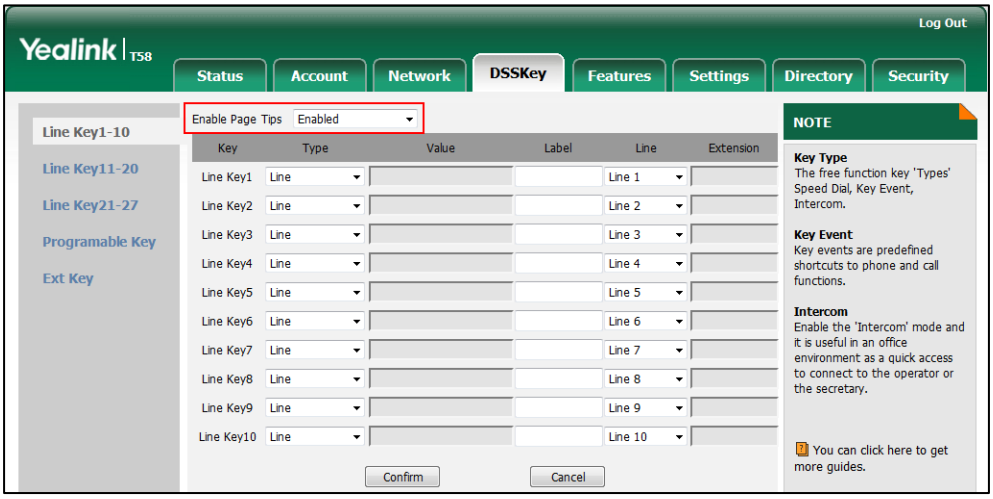
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure enable page tips. **Parameter:** phone_setting.page_tip
Web User Interface		Configure enable page tips. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.page_tip	**0 or 1**	**1**
Description: Enables or disables the breathing light or page icon to indicate states of line keys on the non-current page. **0**-Disabled **1**-Enabled **Web User Interface:** DSSKey->Line Key->Enable Page Tips **Phone User Interface:** None		

To configure enable page tips feature via web user interface:

1. Click on **DSSKey**->**Line Key**.
2. Select **Enabled** from the pull-down list of **Enable Page Tips**.



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

Page Tips for Expansion Module

You are allowed to configure the page switch key LED on the expansion module to indicate when BLF monitored user receives an incoming call on the non-current page. It is only applicable to EXP50 connected to the SIP-T58V/T58A/T56A IP phones.

The following table lists the page switch key LED to indicate different statuses:

LED Status	Description
Off	Indicates non-current pages.
Solid green	Indicates current page.
Flashing red	The BLF monitored user receives an incoming call on the non-current pages.

Procedure

Page tips for expansion module can only be configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure page tips for the page switch keys of the expansion modules. **Parameter:** expansion_module.page_tip.blf_call_in.enable

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
expansion_module.page_tip.blf_call_in.enable	**0 or 1**	**1**
Description: Enables or disables the page switch key LED on the expansion module to indicate when BLF monitored user receives an incoming call on the non-current pages. **0**-Disabled **1**-Enabled **Note**: It is only applicable to EXP50 expansion modules connected to the SIP-T58V/T58A/T56A IP phones. **Web User Interface:** None **Phone User Interface:** None		

Account Registration

Registering a SIP account makes it easier for the IP phones to receive an incoming call, dial an outgoing call. Yealink IP phones support registering multiple accounts on a phone; each account requires an extension or phone number.

The number of the registered accounts must meet the following:

Phone Model	Accounts
SIP-T58V/T58A/T56A	<=16
CP960	1

The IP phones support SIP server redundancy for account registration. For more information, refer to Server Redundancy on page 569. If you want to customize multiple DSS keys to associate with an account, refer to Multiple Line Keys per Account on page 180.

Procedure

Account registration can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the account registration information. **Parameters:** account.X.enable account.X.label account.X.display_name account.X.auth_name account.X.user_name account.X.password account.X.sip_server.Y.address account.X.sip_server.Y.port account.X.outbound_proxy_enable account.X.outbound_proxy.Y.address account.X.outbound_proxy.Y.port
		Configure the interval for the IP phone to retry to re-register when registration fails. **Parameter:** account.X.reg_fail_retry_interval
Web User Interface		Configure the account registration information. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-register&q=load&acc=0
		Configure the interval for the IP phone to retry to register when registration fails. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0
Phone User Interface		Configure the account registration information.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.enable	**0 or 1**	**0**
Description: Enables or disables the account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Register->Line Active **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->Activation		
account.X.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label to be displayed on the touch screen for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Register->Label **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->Label		
account.X.display_name	**String within 99 characters**	**Blank**
Description: Configures the display name to be displayed on the called party's touch screen for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Register->Display Name **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->Display Name		

Parameters	Permitted Values	Default
account.X.auth_name	**String within 99 characters**	**Blank**
Description: Configures the user name for register authentication for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: The user name for register authentication is provided by ITSP. It is always matched with a password (configured by the parameter "account.X.password") used for register authentication, if required by the server. **Web User Interface:** Account->Register->Register Name **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->Register Name		
account.X.user_name	**String within 99 characters**	**Blank**
Description: Configures the register user name for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: The register user name is provided by ITSP. It is used to identify the account. **Web User Interface:** Account->Register->User Name **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->User Name		
account.X.password	**String within 99 characters**	**Blank**
Description: Configures the password for register authentication for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: The password for register authentication is provided by ITSP. **Web User Interface:** Account->Register->Password **Phone User Interface:**		

Parameters	Permitted Values	Default
Settings->Advanced (default password: admin) ->Accounts->Password		
account.X.sip_server.Y.address (Y ranges from 1 to 2)	**String within 256 characters**	**Blank**
Description: Configures the IP address or domain name of the SIP server Y that accepts registrations for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.sip_server.1.address = yealink.pbx.com **Web User Interface:** Account->Register->SIP Server Y->Server Host **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->SIP ServerY		
account.X.sip_server.Y.port (Y ranges from 1 to 2)	**Integer from 0 to 65535**	**5060**
Description: Configures the port of the SIP server Y that specifies registrations for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.sip_server.1.port = 5060 **Note**: If the value of this parameter is set to 0, the port used depends on the value specified by the parameter "account.X.sip_server.Y.transport_type". **Web User Interface:** Account->Register->SIP Server Y->Port **Phone User Interface:** None		
account.X.outbound_proxy_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to send requests to the outbound proxy server for account X. **0**-Disabled		

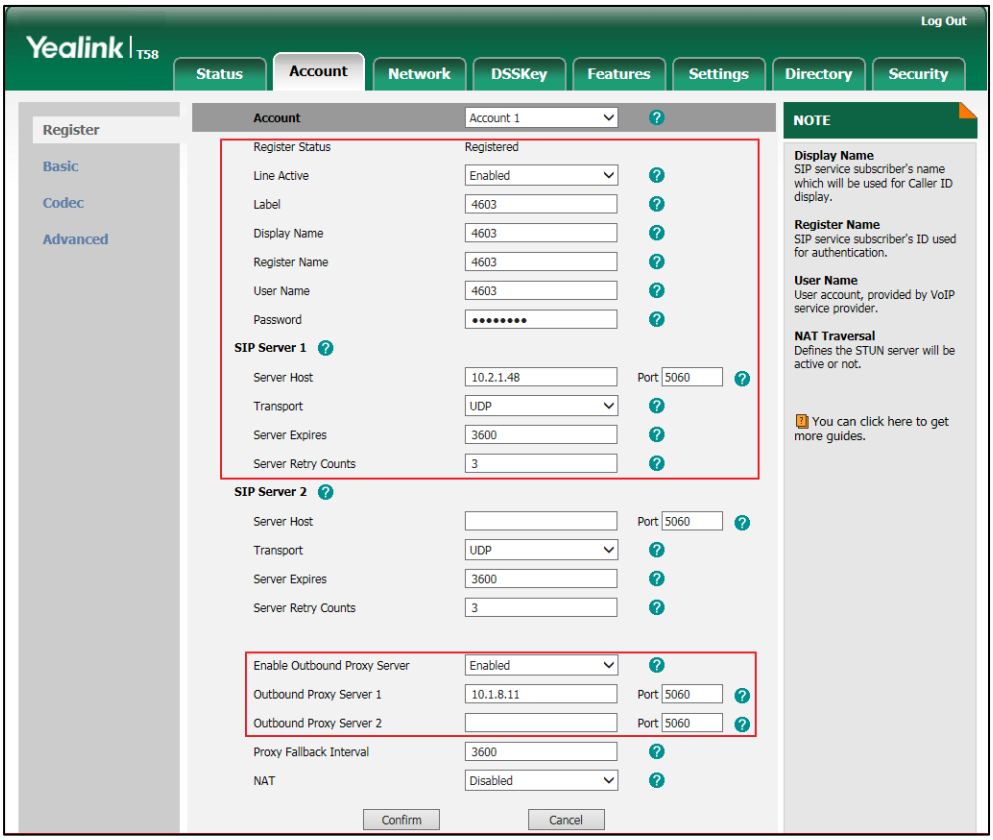
Parameters	Permitted Values	Default
1-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Register->Enable Outbound Proxy Server **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->Outbound Status		
account.X.outbound_proxy.Y.address (Y ranges from 1 to 2)	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the outbound proxy server Y for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.outbound_proxy.1.address = 10.1.8.11 **Note:** It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). **Web User Interface:** Account->Register->Outbound Proxy Server Y **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->Outbound ProxyY		
account.X.outbound_proxy.Y.port (Y ranges from 1 to 2)	**Integer from 0 to 65535**	**5060**
Description: Configures the port of the outbound proxy server Y for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.outbound_proxy.1.port = 5060 **Note:** It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). **Web User Interface:** Account->Register->Outbound Proxy Server Y->Port **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
account.X.reg_fail_retry_interval	**Integer from 0 to 1800**	**30**
Description: Configures the interval (in seconds) for the IP phone to retry to re-register for account X when registration fails. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.reg_fail_retry_interval = 30 **Web User Interface:** Account->Advanced->SIP Registration Retry Timer(0~1800s) **Phone User Interface:** None		

To register an account via web user interface:

1. Click **Account**->**Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **Enabled** from the pull-down list of **Line Active**.
4. Enter the desired value in **Label**, **Display Name**, **Register Name**, **User Name**, **Password** and **SIP Server1/2** field respectively.
5. If you use outbound proxy servers, do the following:
   1) Select **Enabled** from the pull-down list of **Enable Outbound Proxy Server**.

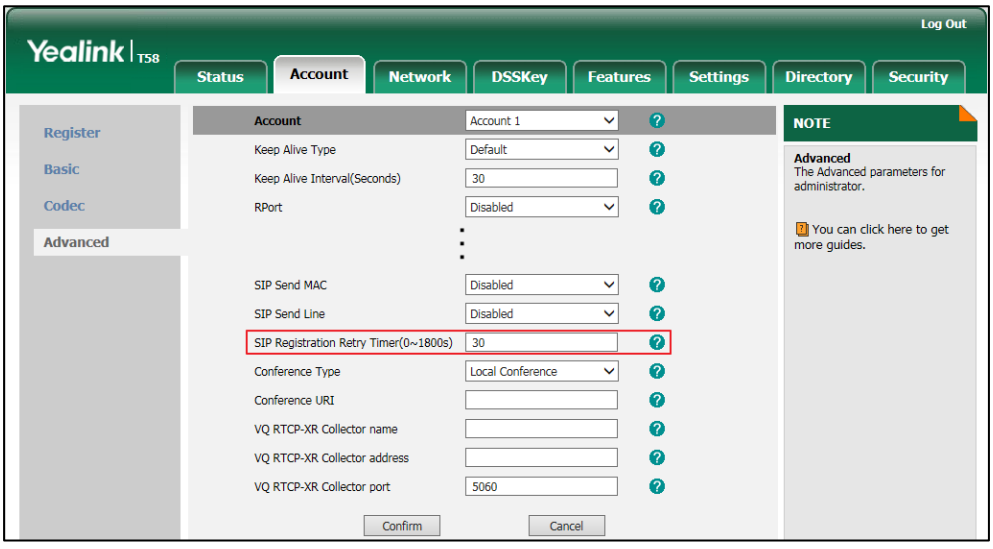
2) Enter the desired IP address or domain name in the **Outbound Proxy Server 1/2** field and the desired port of the outbound proxy server 1/2 in the **Port** field respectively.



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

To configure the interval for re-register when registration fails via web user interface:

1. Click **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Enter the desired interval in the **SIP Registration Retry Timer(0~1800s)** field.



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

To register an account via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Accounts**.
2. Tap the desired account.
3. Tap the **Activation** field.
4. Tap **Enabled** in the pop-up dialog box.
5. Enter the desired value in **Label**, **Display Name**, **Register Name**, **User Name**, **Password** and **SIP Server1/2** field respectively. Contact your system administrator for more information.
6. If you use outbound proxy servers, do the following:
   1) Select **Enabled** from the **Outbound Status** field.
   2) Tap the **Outbound Status** field.
   3) Tap **Enabled** in the pop-up dialog box.
   4) Enter the desired value in the **Outbound Proxy1/2** field respectively. Contact your system administrator for more information.
7. Tap ✓ to accept the change.

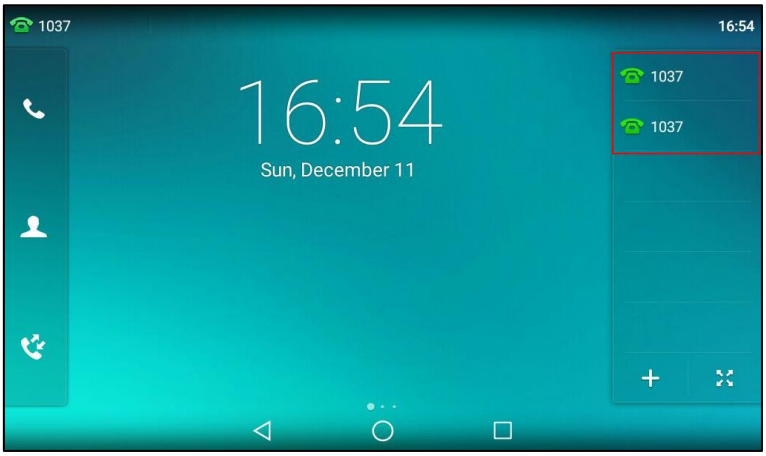
Multiple Line Keys per Account

You can customize the number of DSS keys to be automatically assigned with Line type. It means multiple DSS keys will associate with an account. It is useful for managing a high volume of calls to a line. For more information on how to register accounts, refer to Account Registration on page 172.

The number of the DSS keys associated with an account must meet the following:

Phone Model	Line Key	Ext Key (with expansion modules connected)
SIP-T58V/T58A/T56A	<=27	<=180
CP960	<=30	/

The following shows two line keys associated with a registered account 1037:



Procedure

Multiple line keys per account can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure auto linekeys. **Parameter:** features.auto_linekeys.enable
	<MAC>.cfg	Configure the number of DSS keys to be assigned automatically. **Parameter:** account.X.number_of_linekey
Web User Interface		Configure auto linekeys. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
		Configure the number of DSS keys to be assigned automatically. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

Details of Configuration Parameters:

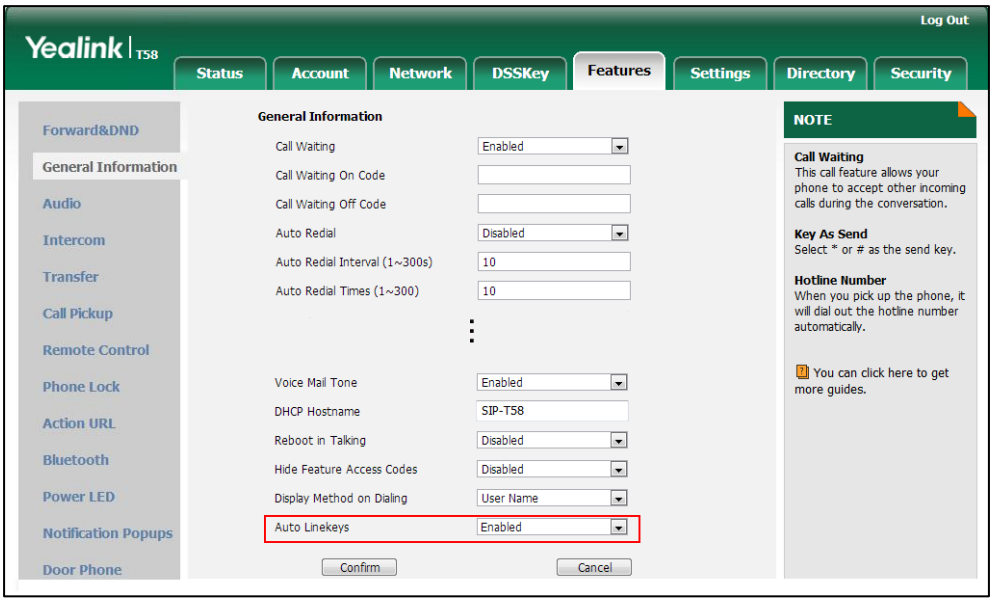
Parameters	Permitted Values	Default
features.auto_linekeys.enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables the DSS keys to be assigned with Line type automatically. **0**-Disabled **1**-Enabled **Note:** The number of the DSS keys is determined by the value of the parameter "account.X.number_of_linekey". **Web User Interface:** Features->General Information->Auto Linekeys **Phone User Interface:** None		
account.X.number_of_linekey	**Integer from 1 to 999**	**1**
Description: Configures the number of DSS keys to be assigned with Line type automatically from the first unused one (unused one means the DSS key is configured as N/A or Line). If a DSS key is used, the IP phone will skip to the next unused DSS key. The order of DSS key assigned automatically is Line Key->Ext Key. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.number_of_linekey = 2 **Note**: It works only if the value of the parameter "features.auto_linekeys.enable" is set to 1 (Enabled). To assign Ext Key, make sure the expansion module has been connected to the phone in advance. **Web User Interface:** Account->Advanced->Number of line key **Phone User Interface:** None		

To configure auto linekeys feature via web user interface:

1. Click on **Features**->**General Information**.
2. Select **Enabled** from the pull-down list of **Auto Linekeys**.

If **Auto LineKeys** is enabled, you can automatically assign multiple DSS keys with Line type for a registered line on the phone.

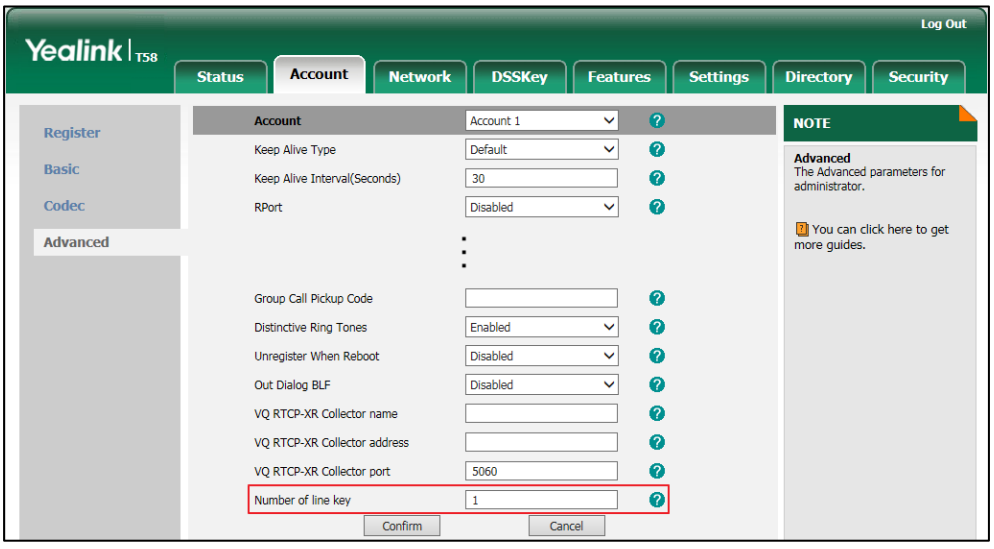


3. Click **Confirm** to accept the change.

To configure the number of line keys via web user interface:

1. Click **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Enter the desired number in the **Number of line key** field.

   This field appears only if **Auto Linekeys** is enabled.

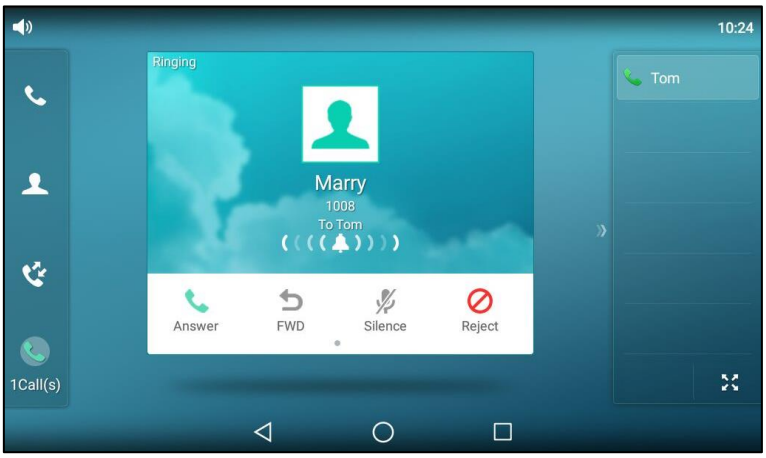


4. Click **Confirm** to accept the change.

Call Display

Display called party information allows the IP phone to present the callee identity in addition to the presentation of caller identity when it receives an incoming call.

The following figure shows an example of screen display when Display Called Party Information feature is enabled on the phone (a call from Marry (phone number: 1008) to Tom.



You can customize the call information to be displayed on the IP phone as required. IP phones support five call information display methods: Number+Name, Name, Name+Number, Number or Full Contact Info (display name<sip:xxx@domain.com>).

Procedure

Call Display can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure display called party information feature. **Parameter:** phone_setting.called_party_info_display.enable
		Specify the call information display method. **Parameter:** phone_setting.call_info_display_method
Web User Interface		Configure display called party information feature. Specify the call information display method. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-calldisplay&q=load

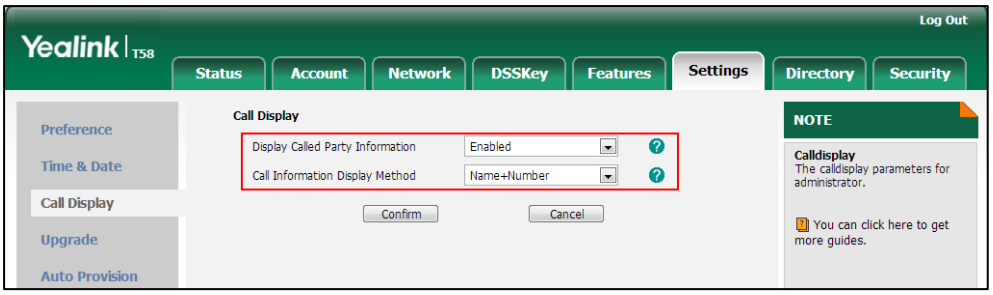
Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.called_party_info_display.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to display the called account information when receiving an incoming call. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Call Display->Display Called Party Information **Phone User Interface:** None		
phone_setting.call_info_display_method	**0, 1, 2, 3 or 4**	**0**
Description: Specifies the call information display method when the IP phone receives an incoming call, dials an outgoing call or is during an active call. **0**-Name+Number **1**-Number+Name **2**-Name **3**-Number **4**-Full Contact Info (display name<sip:xxx@domain.com>) **Web User Interface:** Settings->Call Display->Call Information Display Method **Phone User Interface:** None		

To configure call display features via web user interface:

1. Click on **Settings**->**Call Display**.
2. Select the desired value from the pull-down list of **Display Called Party Information**.

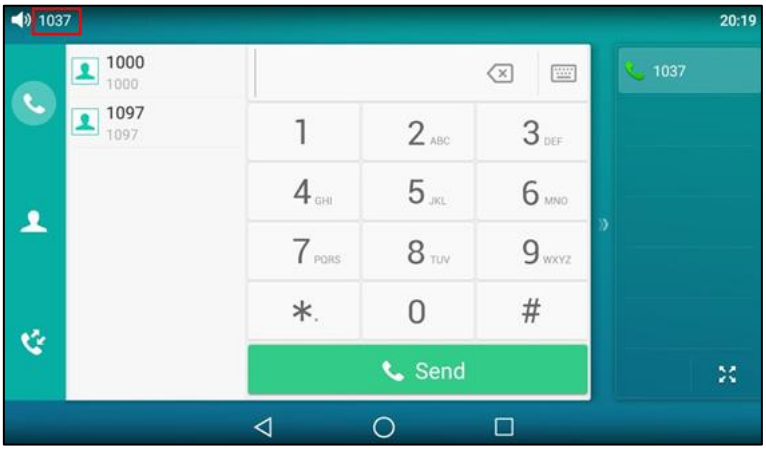
3. Select the desired value from the pull-down list of **Call Information Display Method**.



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

Display Method on Dialing

When the IP phone is on the pre-dialing or dialing screen, the account information will be displayed on the top-left corner of the touch screen.



You can customize the account information to be displayed on the IP phone as required. IP phones support three account information display methods: Label, Display Name or User Name. It is not applicable to CP960 IP phones.

Procedure

Display method on dialing can be configured using the following methods.

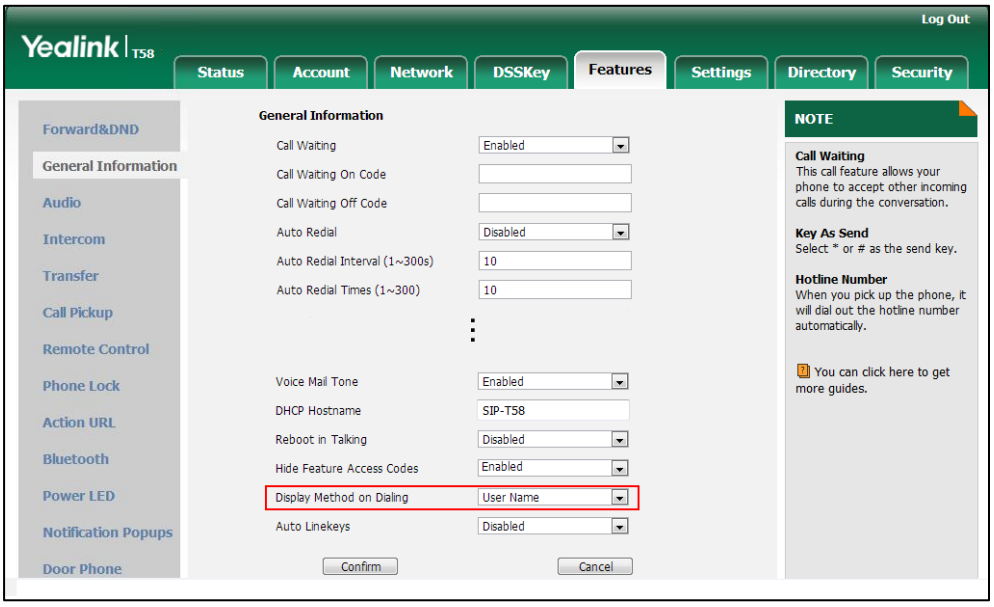
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure display method on dialing. **Parameter:** features.caller_name_type_on_dialing
Web User Interface		Configure display method on dialing. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.caller_name_type_on_dialing	**1, 2 or 3**	**3**
Description: Configures the account information displayed on the top-left corner of the touch screen when the IP phone is on the pre-dialing or dialing screen. **1**-Label **2**-Display Name **3**-User Name **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->General Information->Display Method on Dialing **Phone User Interface:** None		

To configure display method on dialing via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Display Method on Dialing**.



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

Time and Date

The IP phones maintain a local clock. By default, a digit clock widget will be displayed on the home screen when the IP phone starts up. You can check the current time and date on the home screen. You can also check the current time and date on the control center. In addition, phone's time will be also displayed on the right of the status bar. You can check the current time on idle screens.

For more information on clock widget and idle screens, refer to *Yealink phone-specific user guide*.

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

Option	Configuration Methods
NTP time server	Configuration Files Web User Interface Phone User Interface
Time Zone	Configuration Files Web User Interface Phone User Interface
Time	Web User Interface Phone User Interface
Time Format	Configuration Files Web User Interface Phone User Interface
Date	Web User Interface Phone User Interface
Date Format	Configuration Files Web User Interface

Option	Configuration Methods
	Phone User Interface
Daylight Saving Time	Configuration Files Web User Interface

NTP Time Server

A time server is a computer 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 phones synchronize 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 following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure NTP by DHCP priority feature and DHCP time feature. **Parameters:** local_time.manual_ntp_srv_prior local_time.dhcp_time
		Configure the NTP server, time zone. **Parameters:** local_time.ntp_server1 local_time.ntp_server2 local_time.interval local_time.time_zone local_time.time_zone_name
Web User Interface		Configure NTP by DHCP priority feature and DHCP time feature. Configure the NTP server, time

	zone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-datetime&q=load
Phone User Interface	Configure DHCP time feature. Configure the NTP server, time zone.

Details of Configuration Parameters:

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 Greenwich Mean Time (GMT). **Web User Interface:** Settings->Time & Date->DHCP Time **Phone User Interface:** Settings->Basic->Time & Date->DHCP Time->DHCP Time		
local_time.ntp_server1	**IP Address or Domain Name**	**cn.pool.ntp.org**

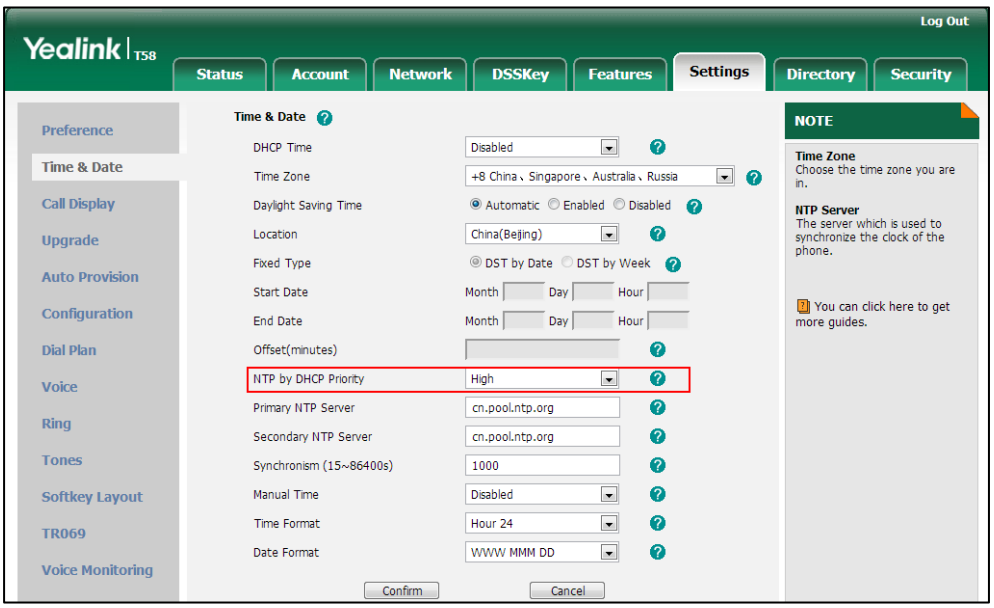
Parameters	Permitted Values	Default
Description: Configures the IP address or the domain name of the NTP server 1. The IP phone will obtain the current time and date from the NTP server 1. **Example:** local_time.ntp_server1 = 192.168.0.5 **Web User Interface:** Settings->Time & Date->Primary NTP Server **Phone User Interface:** Settings->Basic->Time & Date->General->Type (SNTP Settings) ->NTP Server1		
local_time.ntp_server2	**IP Address or Domain Name**	**pool.ntp.org**
Description: Configures the IP address or the domain name of the NTP server 2. If the NTP server 1 is not configured (configured by the parameter "local_time.ntp_server1") or cannot be accessed, the IP phone will request the time and date from the NTP server 2. **Example:** local_time.ntp_server2 = 192.168.0.6 **Web User Interface:** Settings->Time & Date->Secondary NTP Server **Phone User Interface:** Settings->Basic->Time & Date->General->Type (SNTP Settings) ->NTP Server2		
local_time.interval	**Integer from 15 to 86400**	**1000**
Description: 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. For more available time zones, refer to Appendix B: Time Zones on page 769. **Example:** local_time.time_zone = +8 **Web User Interface:** Settings->Time & Date->Time Zone **Phone User Interface:** Settings->Basic->Time & Date->General->Type (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 depend on the time zone configured by the parameter "local_time.time_zone". For more information on the available time zone names for each time zone, refer to Appendix B: Time Zones on page 769. **Example:** local_time.time_zone_name = China(Beijing) **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance. **Web User Interface:** Settings->Time & Date->Location **Phone User Interface:** Settings->Basic->Time & Date->General->Type (SNTP Settings) ->Location		

To configure NTP by DHCP priority feature via web user interface:

1. Click on **Settings**->**Time & Date**.

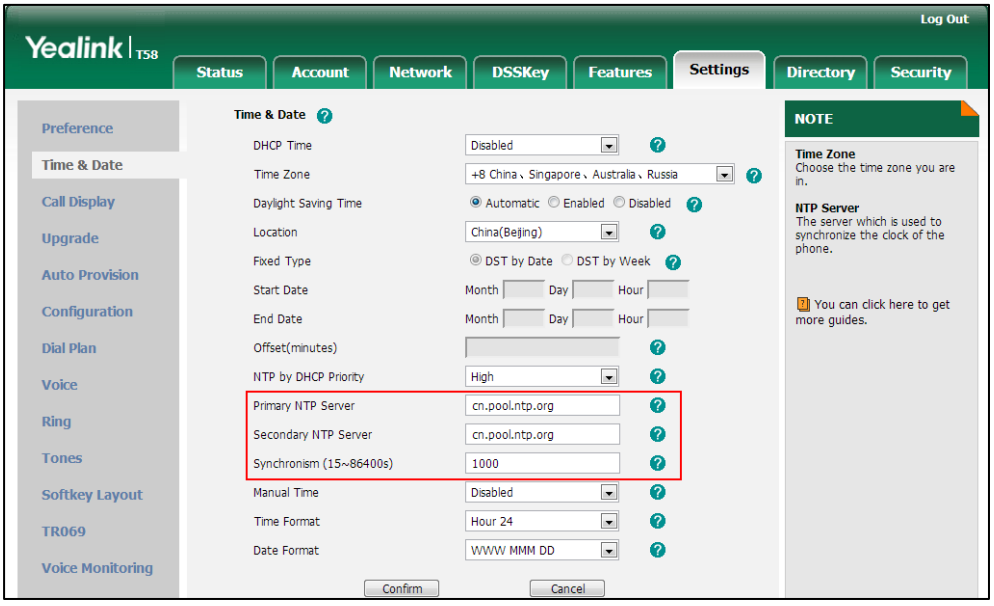
2. Select the desired value from the pull-down list of **NTP by DHCP Priority**.



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 NTP Server** and **Secondary NTP Server** field respectively.
6. Enter the desired time interval in the **Synchronism (15~86400s)** field.



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

To configure the NTP server and time zone via phone user interface:

1. Tap **Settings**->**Basic**->**Time & Date**->**Type**.
2. Tap the **Type** field.
3. Tap **SNTP Settings** in the pop-up dialog box.
4. Tap the **Time Zone** field.
5. Tap the time zone that applies to your area in the pop-up dialog box.
6. Enter the domain name or IP address of SNTP server in the **NTP Server1** and **NTP Server2** field respectively.
7. Tap the **Daylight Saving** field.
8. Tap the desired value in the pop-up dialog box.
9. Tap the **Location** field.

   This field appears only if **Daylight Saving** field is selected to **Automatic**.
10. Tap the desired time zone name in the pop-up dialog box.
11. Tap ✔ 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 following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the time and date manually. **Parameter:** local_time.manual_time_enable
		Configure the time and date formats. **Parameters:** local_time.time_format local_time.date_format
Web User Interface		Configure the time and date manually. Configure the time and date formats. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-datetime&q=load
Phone User Interface		Configure the time and date manually. Configure the time and date formats.

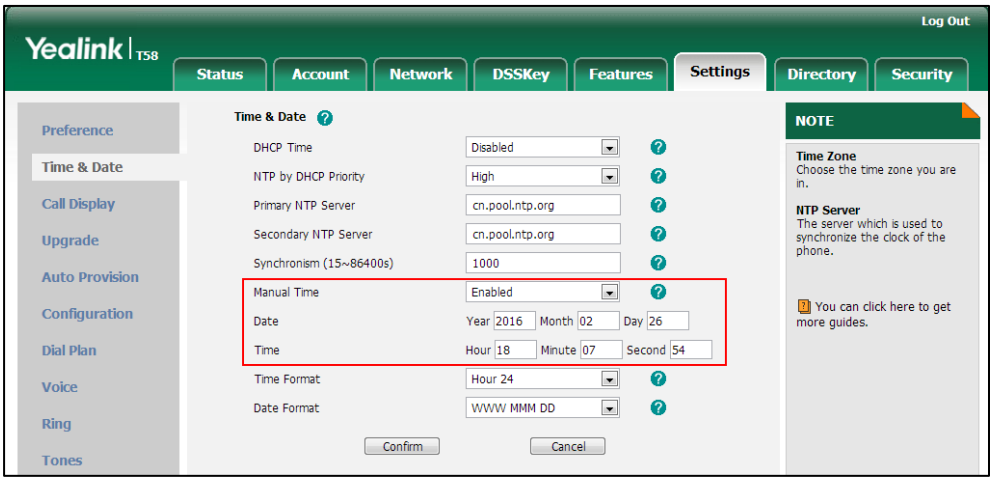
Details of Configuration Parameters:

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 manual settings. **0**-Disabled (obtain time and date from NTP server) **1**-Enabled (obtain time and date from manual settings) **Web User Interface:** Settings->Time & Date->Manual Time **Phone User Interface:** None		
local_time.time_format	**0 or 1**	**1**
Description: Configures the time format. **0**-Hour 12 **1**-Hour 24 If it is set to 0 (Hour 12), the time will be displayed in 12-hour format with AM or PM specified. If it is set to 1 (Hour 24), the time will be displayed in 24-hour format (e.g., 2:00 PM displays as 14:00). **Web User Interface:** Settings->Time & Date->Time Format **Phone User Interface:** Settings->Basic->Display->Time & Date->Time & Date Format->Time Format		
local_time.date_format	**0, 1, 2, 3, 4, 5 or 6**	**0**
Description: Configures the date format for the date displayed in the control center. **Valid values are:** **0**-WWW MMM DD **1**-DD-MMM-YY **2**-YYYY-MM-DD **3**-DD/MM/YYYY		

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

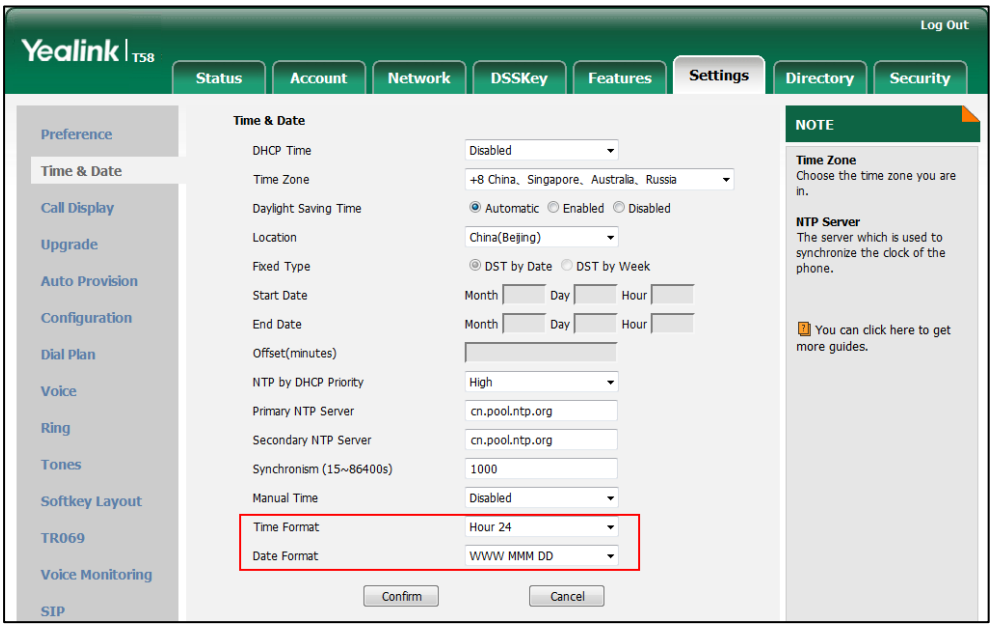


4. Click **Confirm** to accept the change.

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**.



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

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

1. Tap **Settings**->**Basic**->**Time & Date**->**General**.
2. Tap the **Type** field.
3. Tap **Manual Settings** in the pop-up dialog box.
4. Enter the date in the **Date** field.
5. Enter the time in the **Time** field.
6. Tap ✓ to accept the change.

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

1. Swipe down from the top of the screen or swipe left/right to go to the second idle screen.
2. Tap **Settings**->**Basic**->**Time & Date**->**Time & Date Format**.
3. Tap the **Date Format** field.
4. Tap the desired date format in the pop-up dialog box.
5. Tap the **Time Format** field.
6. Tap the desired time format (**12 Hour** or **24 Hour**) in the pop-up dialog box.
7. Tap ✓ to accept the change or ◁ to cancel.

Daylight Saving Time (DST)

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 following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure DST. **Parameters:** local_time.summer_time local_time.dst_time_type local_time.start_time local_time.end_time local_time.offset_time
Web User Interface		Configure DST. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-datetime&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
local_time.summer_time	**0, 1 or 2**	**2**
Description: Configures Daylight Saving Time (DST) feature. **0**-Disabled **1**-Enabled **2**-Automatic **Web User Interface:** Settings->Time & Date->Daylight Saving Time **Phone User Interface:** Settings->Basic->Time & Date->General->Type (SNTP Settings) ->Daylight Saving		
local_time.dst_time_type	**0 or 1**	**0**
Description: Configures the Daylight Saving Time (DST) time type. **0**-DST by Date		

Parameters	Permitted Values	Default
1-DST by Week **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Fixed Type **Phone User Interface:** None		
local_time.start_time	**Time**	**1/1/0**
Description: Configures the start time of the Daylight Saving Time (DST). **Value formats are:** ● Month/Day/Hour (for DST by Date) ● Month/Week of Month/Day of Week/Hour of Day (for DST by Week) If "local_time.dst_time_type" is set to 0 (DST by Date), use the mapping: **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 **Example**: local_time.start_time = 1/1/2 If "local_time.dst_time_type" is set to 1 (DST by Week), use the mapping: **Month**: 1=January, 2=February,..., 12=December **Week of Month**: 1=the first week in a month,..., 5=the last week in a month **Day of Week**: 1=Monday, 2=Tuesday,..., 7=Sunday **Hour of Day**: 0=0am, 1=1am,..., 23=11pm **Example**: local_time.start_time = 1/1/7/0 **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Start Date **Phone User Interface:** None		
local_time.end_time	**Time**	**12/31/23**

Parameters	Permitted Values	Default
Description: Configures the end time of the Daylight Saving Time (DST). **Value formats are:** ● Month/Day/Hour (for DST by Date) ● Month/Week of Month/Day of Week/Hour of Day (for DST by Week) If "local_time.dst_time_type" is set to 0 (DST by Date), use the mapping: **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 **Example**: local_time.start_time = 12/12/22 If "local_time.dst_time_type" is set to 1 (DST by Week), use the mapping: **Month**: 1=January, 2=February,..., 12=December **Week of Month**: 1=the first week in a month,..., 5=the last week in a month **Day of Week**: 1=Monday, 2=Tuesday,..., 7=Sunday **Hour of Day**: 0=0am, 1=1am,..., 23=11pm **Example**: local_time.start_time = 4/3/2/3 **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->End Date **Phone User Interface:** None		
local_time.offset_time	**Integer from -300 to 300**	**Blank**
Description: Configures the offset time (in minutes) of Daylight Saving Time (DST). **Note**: It works only if the value of the parameter "local_time.summer_time" is set to 1 (Enabled). **Web User Interface:** Settings->Time & Date->Offset(minutes) **Phone User Interface:** None		

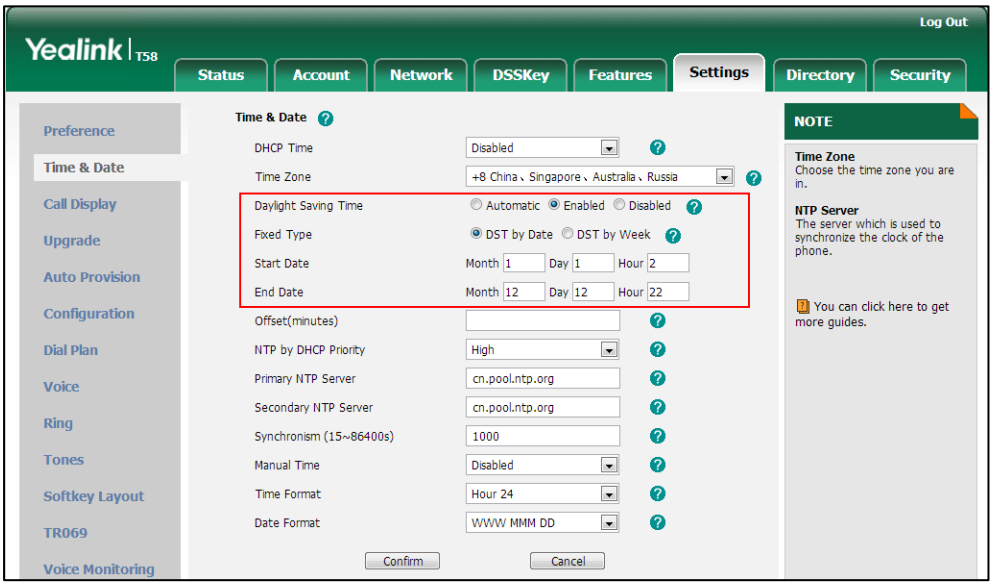
To configure the DST via web user interface:

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. Enter the domain name or IP address in the **Primary NTP Server** and **Secondary NTP 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.

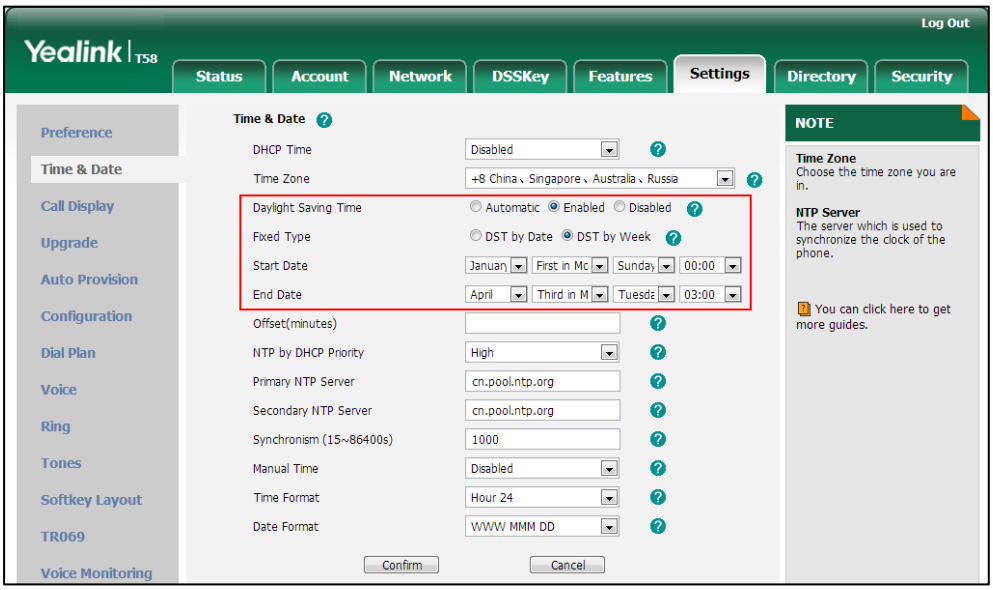
     Enter the start time in the **Start Date** field.

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



- 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.



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://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the template file, refer to Obtaining Configuration Files and Resource Files on page 119.

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

Element	Type	Values	Description
DSTData	required	no	File root element
DST	required	no	Time Zone item's root element
szTime	required	[+/-][X]:[Y], X=0~14, Y=0~59	Time Zone
szZone	required	String (if the content is more than one city, it is the best to	Time Zone name

Element	Type	Values	Description
		keep their daylight saving time the same)	
iType	optional	0/1 **0**: DST by Date **1**: DST by Week	DST time type (This item is needed if you want to configure DST.)
szStart	optional	**Month/Day/Hour** (for **iType=0**) Month: 1~12 Day: 1~31 Hour: 0 (midnight)~23 **Month/Week of Month/Day of Week/Hour of Day** (for **iType=1**) Month: 1~12 Week of 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
szOffset	optional	Integer from -300 to 300	The offset time (in minutes) of DST

When customizing an AutoDST file, learn the following:

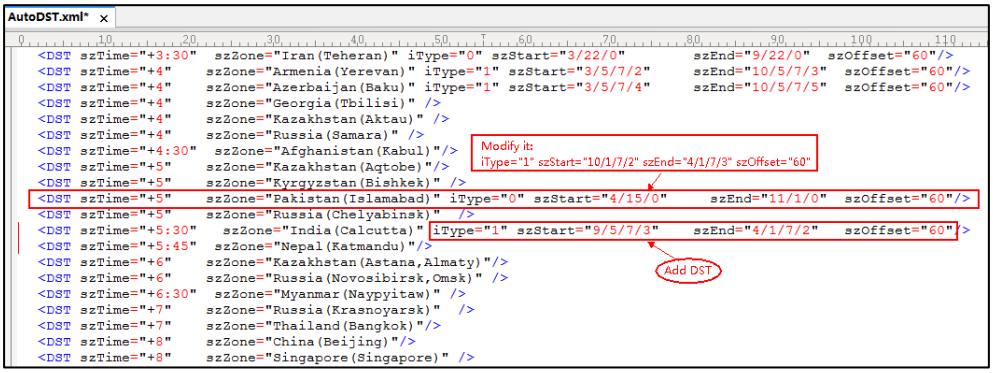
- <DSTData> indicates the start of a template and </DSTData> indicates the end of a template.
- Add or modify time zone and DST settings between <DSTData> and </DSTData>.
- The display order of time zone is corresponding to the szTime order specified in the AutoDST.xml file.
- If the start time of DST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

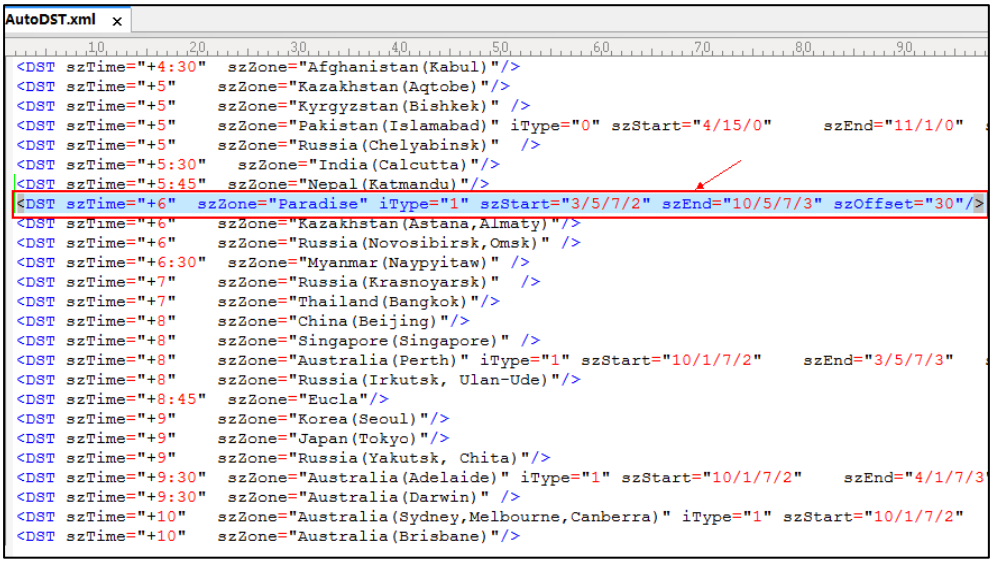
Example 1:

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)".



Example 2:

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



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.

Central Provisioning (Configuration File)	<MAC>.cfg	Specify the access URL of the AutoDST file. **Parameter:** auto_dst.url

Details of Configuration Parameter:

Parameter	Permitted Values	Default
auto_dst.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the AutoDST 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 the parameter "local_time.summer_time" is set to 2 (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

Phone/Web User Interface
Turkish
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://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the language packs, refer to Obtaining Configuration Files and Resource Files on page 119.

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 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
Russian	010.GUI.Russian.lang

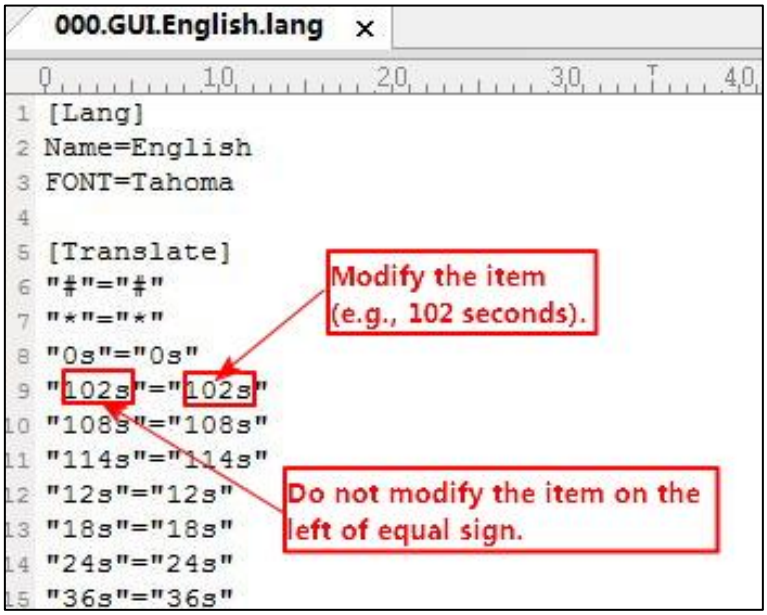
When adding a new language pack for the phone user interface, the language pack must be formatted as "X.GUI.name.lang" (X starts from 011, "name" is replaced with the language name).

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:



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-T58V), prepare the language file named as "011.GUI.Guilan.lang" for downloading. After update, you will find a new language selection "Guilan" on the IP phone user interface: **Settings**->**Basic**->**Language**.

Procedure

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

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL of the phone user interface language pack. **Parameter:** gui_lang.url

		Delete custom LCD language packs of the phone user interface. **Parameter:** gui_lang.delete

Details of the Configuration Parameters:

Parameters	Permitted Values	Default
gui_lang.url	**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 phone simultaneously, you can configure as following: 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		
gui_lang.delete	**http://localhost/all or http://localhost/*Y.GUI.name.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):		

Parameters	Permitted Values	Default
gui_lang.delete = http://localhost/001.GUI.Chinese_S.lang **Web User Interface:** None **Phone User Interface:** None		

Customizing a Language for Web User Interface

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

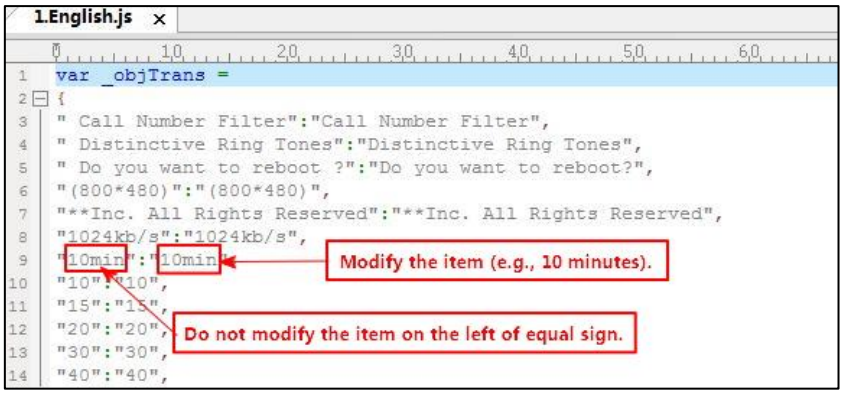
Available Language	Associated Language Pack	Associated Note Language Pack
English	1.English.js	1.English_Note.xml
Chinese Simplified	2.Chinese_S.js	2.Chinese_S_Note.xml
Chinese Traditional	3.Chinese_T.js	3.Chinese_T_Note.xml
French	4.French.js	4.French_Note.xml
German	5.German.js	5.German_Note.xml
Italian	6.Italian.js	6.Italian_Note.xml
Polish	7.Polish.js	7.Polish_Note.xml
Portuguese	8.Portuguese.js	8.Portuguese_Note.xml
Spanish	9.Spanish.js	9.Spanish_Note.xml
Turkish	10.Turkish.js	10.Turkish_Note.xml
Russian	11.Russian.js	11.Russian_Note.xml

When adding a new language pack for the web user interface, the language pack must be formatted as "Y.name.js" (Y starts from 12, "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.
2. 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:



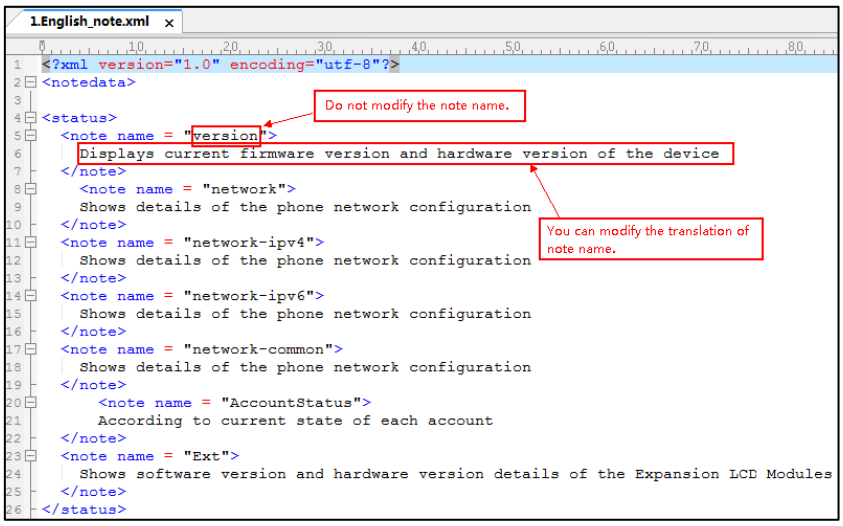
3. Save the language file and place it to the provisioning server (e.g., 192.168.10.25).
4. Specify the access URL of the web user interface language pack in the configuration files.

You can also customize the translation of the Note language pack. The Note information is displayed in the icon of the web user interface. The Note language pack must be formatted as "Y.name_Note.xml" ("Y" and "name" are associated with web language pack).

To customize a Note language file:

1. Open the desired Note language template file (e.g., 1.English_Note.xml) using an ASCII editor.
2. Modify the text of the Note field. Don't modify the name of the Note field.

   The following shows a portion of the Note language pack "1.English_Note.xml" for the web user interface:



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 Note language pack of the web user interface.

If you want to add a new language (e.g., Wuilan) to IP phones, prepare the language file named as "12.Wuilan.js" and "12.Wuilan_Note.xml" for downloading. After update, you will find a new

language selection "Wuilan" on the web user interface: **Settings**->**Preference**->**Language**, and new Note information is displayed in the icon when the new language is selected.

Procedure

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

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL of the custom language pack for web user interface. **Parameter:** wui_lang.url
		Specify the access URL of the custom Note language pack for web user interface. **Parameter:** wui_lang_note.url
		Delete custom language packs and Note language packs of the web user interface. **Parameter:** wui_lang.delete

Details of the Configuration Parameters:

Parameters	Permitted Values	Default
wui_lang.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom language pack for the web user interface. **Example:** wui_lang.url = http://192.168.10.25/1.English.js 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.js wui_lang.url = http://192.168.10.25/11.Russian.js **Web User Interface:**		

Parameters	Permitted Values	Default
None **Phone User Interface:** None		
wui_lang_note.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom Note language pack for web user interface. **Example:** wui_lang_note.url = http://192.168.10.25/1.English_Note.xml During the auto provisioning process, the IP phone connects to the HTTP provisioning server "192.168.10.25", and downloads the Note language pack "1.English_Note.xml". 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 phone simultaneously, you can configure as following: wui_lang.url = http://192.168.10.25/1.English_Note.xml wui_lang.url = http://192.168.10.25/11.Russian_Note.xml **Web User Interface:** None **Phone User Interface:** None		
wui_lang.delete	**http://localhost/all or http://localhost/*Y.name.js***	**Blank**
Description: Delete the specified or all custom web language packs and Note language packs of the web user interface. **Example:** Delete all custom language packs of the web 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 The corresponding Note language pack (e.g., 11.Russian_Note.xml) will also be deleted. **Web User Interface:** None **Phone User Interface:**		

Parameters	Permitted Values	Default
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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the languages for the phone user interface and the web user interface. **Parameters:** static.lang.gui static.lang.wui
Web User Interface		Specify the language for the web user interface. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-preference&q=load
Phone User Interface		Specify the language for the phone user interface.

Details of Configuration Parameters:

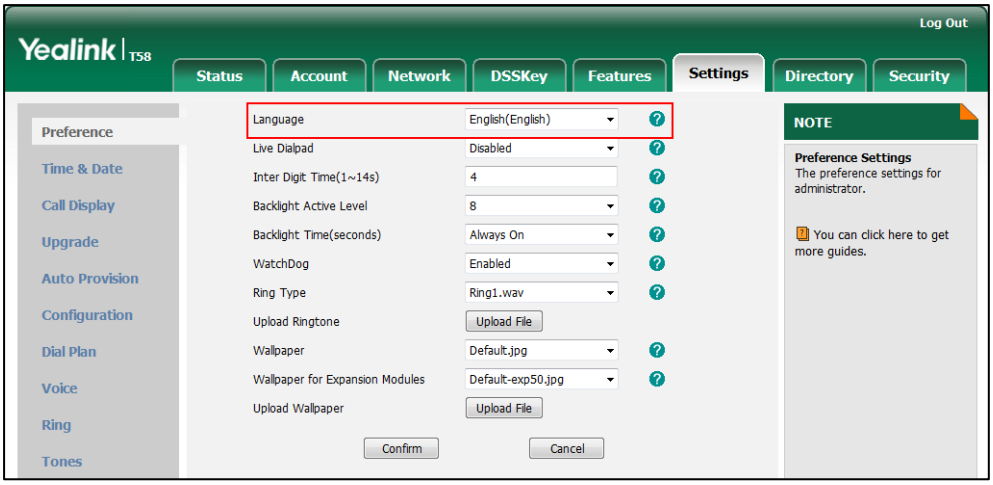
Parameters	Permitted Values	Default
static.lang.gui	**Refer to the following content**	**English**
Description: Configures the language used on the phone user interface. **Permitted Values**: English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian or the custom language name.		

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



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

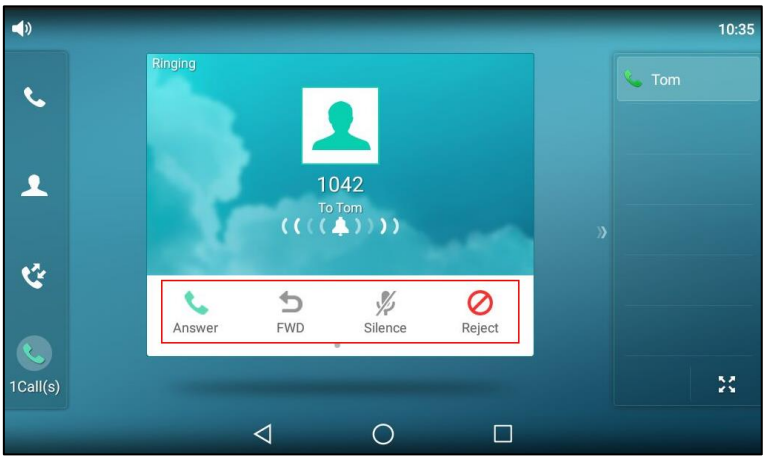
To specify the language for the phone user interface via phone user interface:

1. Tap **Settings**->**Basic**->**Language**.
2. Drag up and down to scroll through the list of available languages.
3. Tap the desired language.
4. Tap ✓ to accept the change.

Softkey Layout

Softkey layout is used to customize the soft keys at the bottom of the touch screen to best meet users' requirements. In addition to specifying which soft keys to display, you can determine their display order. It can be configured based on call states.

The following shows the softkeys displaying on the phone in the CallIn state:



You can configure the softkey layout using the softkey layout templates for different call states. For more information on how to configure a softkey layout template, refer to Customizing Softkey Layout Template File on page 217.

Note It is not applicable to CP960 IP phones.

Procedure

Softkey layout can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the softkey layout. **Parameter:** phone_setting.custom_softkey_enable
Web User Interface		Configure the softkey layout. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-softkey&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.custom_softkey_enable	**0 or 1**	**0**
Description: Enables or disables custom soft keys layout feature. **0**-Disabled **1**-Enabled **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Settings->Softkey Layout->Custom Softkey **Phone User Interface:** None		

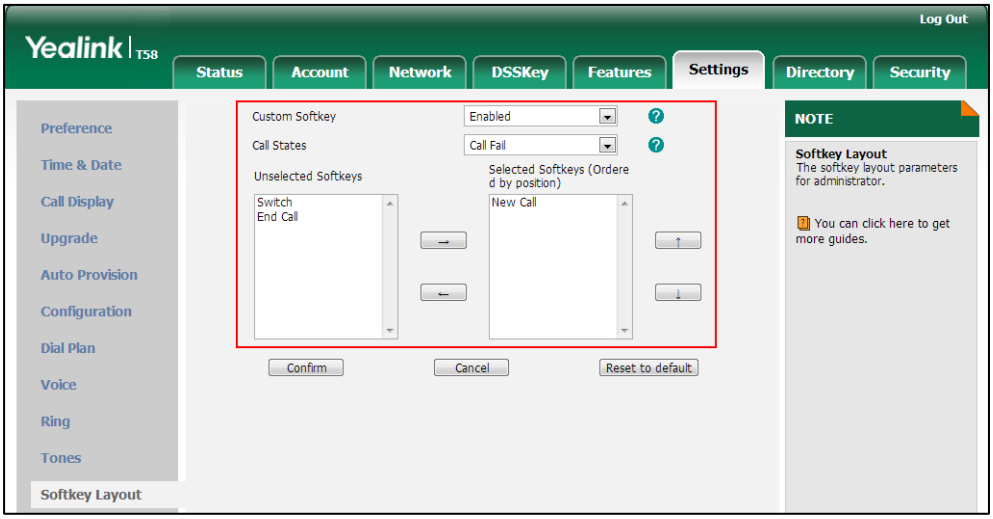
To configure softkey layout via web user interface:

1. Click on **Settings**->**Softkey Layout**.
2. Select the desired value from the pull-down list of **Custom Softkey**.
3. Select the desired state from the pull-down list of **Call States**.
4. Select the desired soft key from the **Unselected Softkeys** column and then click →.

The selected soft key appears in the **Selected Softkeys** column. If more than four soft keys are selected, the selected soft keys will be displayed in two pages. Swipe left or right to see more soft keys.

5. Repeat the step 4 to add more soft keys to the **Selected Softkeys** column.
6. To remove the soft key from the **Selected Softkeys** column, select the desired soft key and then click ← .
7. To adjust the display order of soft keys, select the desired soft key and then click ↓ or ↑ .

   The touch screen displays the soft keys in the adjusted order.



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

Customizing Softkey Layout Template File

The softkey layout template allows you to customize soft key layout for different call states. The call states include CallFailed, CallIn, Connecting, RingBack and Talking.

You can ask the distributor or Yealink FAE for softkey layout template. You can also obtain the softkey layout template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the softkey layout template, refer to Obtaining Configuration Files and Resource Files on page 119.

The following table lists soft keys available for IP phones in different call states.

Call State	Default Soft Keys	Optional Soft Keys
CallFailed	NewCall	End Call
CallIn	Answer Forward Silence	Switch

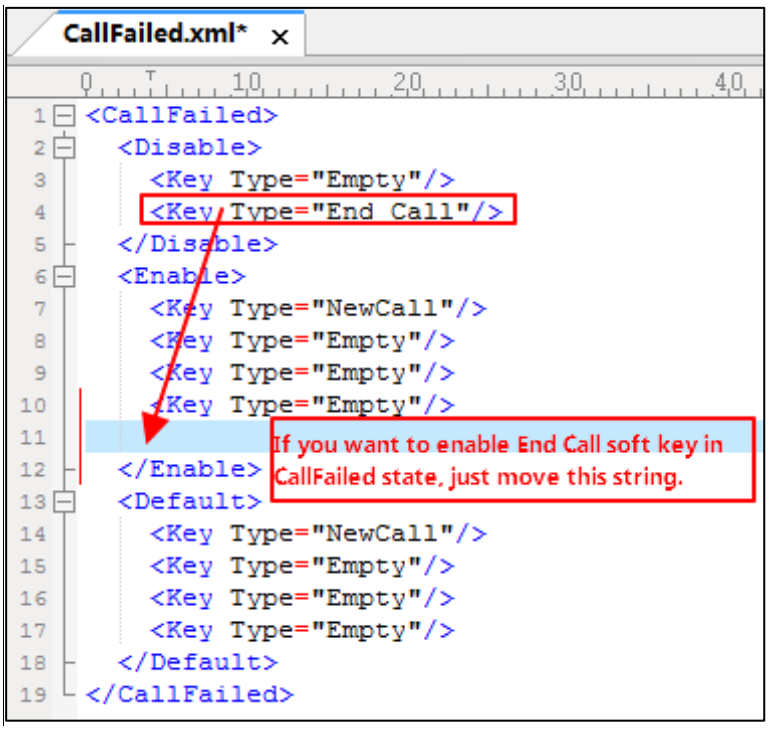
Call State		Default Soft Keys	Optional Soft Keys
		Reject	
Connecting	Connecting	End Call	Switch
	SemiAttendTrans	Transfer End Call	Switch
RingBack	RingBack	End Call	Switch
	SemiAttendTrans Back	Transfer End Call	Switch
Talking	Talk	Transfer Hold Conference End Call	Mute SWAP NewCall Switch Answer Reject PriHold Park GPark RTP Status Record
	Hold	Transfer Resume NewCall End Call	Switch Answer Reject Record
	Held	End Call	Switch Answer Reject NewCall Record
	Conferenced	Hold Split End Call	Switch Answer Reject Mute RTP Status Record

When editing a softkey layout template, learn the following:

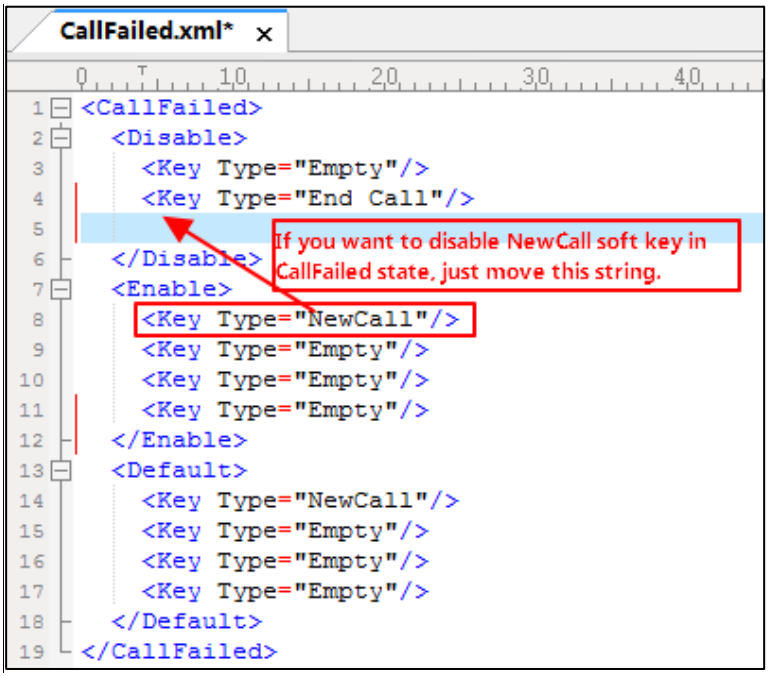
- <Call States> indicates the start of a template and </Call States> indicates the end of a template. For example, <CallFailed></CallFailed>.
- <Disable> indicates the start of the disabled soft key list and </Disable> indicates the end of the soft key list. The disabled soft keys are not displayed on the touch screen.
- Create disabled soft keys between <Disable> and </Disable>.
- <Enable> indicates the start of the enabled soft key list and </Enable> indicates the end of the soft key list. The enabled soft keys are displayed on the touch screen.
- Create enabled soft keys between <Enable> and </Enable>.
- <Default> indicates the start of the default soft key list and </Default> indicates the end of the default soft key list. The default soft keys are displayed on the touch screen by default.

To customize a softkey layout template:

1. Open the template file using an ASCII editor.
2. For each soft key that you want to enable, move the string in the disabled soft key list to enabled soft key list in the file.



For each soft key that you want to disabled, just move the string in the enabled soft key list to disabled soft key list.



3. Save the change and place this file to the provisioning server.
4. Specify the access URL of the softkey layout template in the configuration files.

Procedure

Specify the access URL of the softkey layout template using the following method.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL of the softkey layout template. **Parameters:** custom_softkey_call_failed.url custom_softkey_call_in.url custom_softkey_connecting.url custom_softkey_ring_back.url custom_softkey_talking.url

Details of Configuration Parameters:

Parameters	Permitted Values	Default
custom_softkey_call_failed.url	**URL within 511 characters**	**Blank**
Description:		

Parameters	Permitted Values	Default
Configures the access URL of the custom file for the soft key presented on the touch screen when in the CallFailed state. **Example:** custom_softkey_call_failed.url = http:// 192.168.1.20/XMLfiles/CallFailed.xml During the auto provisioning process, the IP phone connects to the provisioning server "192.168.1.20", and downloads the CallFailed state file from the "XMLfiles" directory. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		
custom_softkey_call_in.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the touch screen when in the CallIn state. **Example:** custom_softkey_call_in.url = http://192.168.1.20/XMLfiles/CallIn.xml During the auto provisioning process, the IP phone connects to the provisioning server "192.168.1.20", and downloads the CallIn state file from the "XMLfiles" directory. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		
custom_softkey_connecting.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the touch screen when in the Connecting (callout) state. **Example:** custom_softkey_connecting.url = http://192.168.1.20/XMLfiles/Connecting.xml During the auto provisioning process, the IP phone connects to the provisioning server "192.168.1.20", and downloads the Connecting state file from the "XMLfiles" directory. **Note**: It is not applicable to CP960 IP phones.		

Parameters	Permitted Values	Default
Web User Interface: None **Phone User Interface:** None		
custom_softkey_ring_back.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the touch screen when in the RingBack state. **Example:** custom_softkey_ring_back.url = http://192.168.1.20/XMLfiles/RingBack.xml During the auto provisioning process, the IP phone connects to the provisioning server "192.168.1.20", and downloads the RingBack state file from the "XMLfiles" directory. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		
custom_softkey_talking.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the touch screen when in the Talking state. **Example:** custom_softkey_talking.url = http://192.168.1.20/XMLfiles/Talking.xml During the auto provisioning process, the IP phone connects to the provisioning server "192.168.1.20", and downloads the Talking state file from the "XMLfiles" directory. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		

Key As Send

Key as send allows assigning the pound key (“#”) or asterisk key (“*”) as the send key.

Send tone 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 on the phone keypad or taps any key on the onscreen dial pad. Send tone works only if key tone is enabled.

Note Key as send feature is not applicable to CP960 IP phones.

Procedure

Key as send can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure a send key. **Parameter:** features.key_as_send
		Configure a send tone. **Parameter:** features.send_key_tone
		Configure a key tone. **Parameter:** features.key_tone
		Configure send pound key. **Parameter:** features.send_pound_key
Web User Interface		Configure a send key. Configure send pound key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
		Configure a send tone or key tone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-audio&q=load
Phone User Interface		Configure a send key. Configure a key tone.

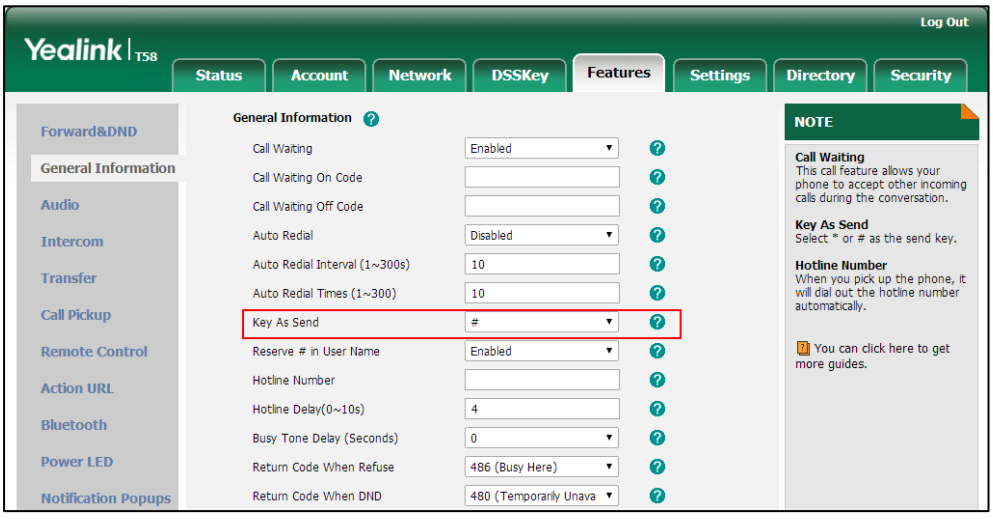
Details of Configuration Parameters:

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 **2**-* key If it is set to 0 (Disabled), neither "#" nor "*" can be used as the send key. If it is set to 1 (# key), the pound key is used as the send key. If it is set to 2 (* key), the asterisk key is used as the send key. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->General Information->Key As Send **Phone User Interface:** Settings->Features->Key as Send->Key as Send		
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 the phone keypad or taps any key on the onscreen dial pad. **0**-Disabled **1**-Enabled 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:** Settings->Basic->Sound->Key Tone->Key Tone		
features.send_key_tone	**0 or 1**	**1**
Description: Enables or disables the IP phone to play a key tone when a user presses a send key. **0**-Disabled		

Parameters	Permitted Values	Default
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 "features.key_tone" is set to 1 (Enabled). **Web User Interface:** Features->Audio->Send Tone **Phone User Interface:** None		
features.send_pound_key	**0 or 1**	**0**
Description: Enables or disables the IP phone not to send any pound key when pressing double #. **0**-Disabled (Send one pound key by pressing double #) **1**-Enabled (Do not send any pound key when pressing double #) **Note**: It works only if the value of the parameter "features.key_as_send" is set to 1 (# key). It is not applicable to CP960 IP phones. **Web User Interface:** Features->General Information->Send Pound Key **Phone User Interface:** None		

To configure a send key via web user interface:

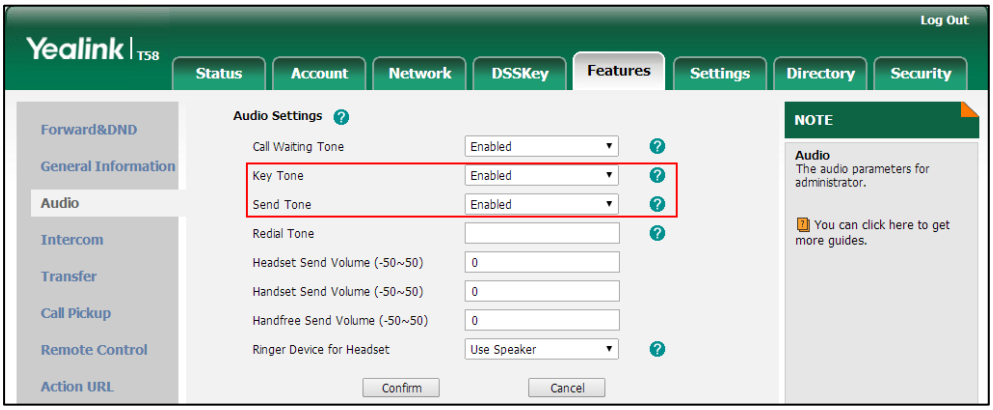
1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Key As Send**.



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

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

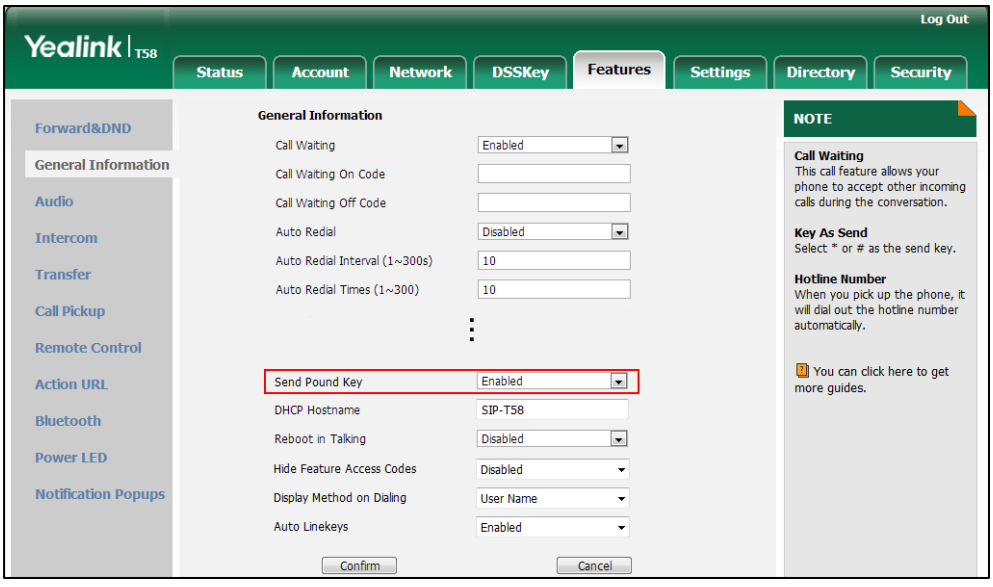
1. Click on **Features**->**Audio**.
2. Select the desired value from the pull-down list of **Key Tone**.
3. Select the desired value from the pull-down list of **Send Tone**.



4. 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**.



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

To configure a send key via phone user interface:

1. Tap **Settings**->**Features**->**Key as Send**.
2. Tap the **Key as Send** field.
3. Tap **#** or ***** in the pop-up dialog box, or tap **Disabled** to disable this feature.
4. Tap ✓ to accept the change.

To configure a key tone via web user interface:

1. Tap **Settings**->**Basic**->**Sound**->**Key Tone**.
2. Tap the **On** radio box in the **Key Tone** field.
3. Tap ✔ to accept the change.

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. You can use regular expression to define 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.

Yealink IP phones support two methods to help creating a dial plan: Dial Plan using XML Template Files (old dial plan mechanism) and Dial Plan using Digit Map String Rules (new dial plan mechanism). Old dial plan method supports replace rule, dial now, area code and block out features, and each dial plan feature need its own matching rule. By contrast, new dial plan supports one or more matching rules in one digit map string. It is helpful for completing multiple dial plan features: replace, dial now, block out, etc by one matching string.

If you enable new dial plan mechanism, old dial plan will be ignored.

Dial Plan using XML Template Files

Yealink IP phones support the following dial plan features:

- Replace Rule
- Dial-now
- Area Code
- Block Out

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**3**", "12**34**", "12**345**", "12**abc**", etc.
x	The "x" can be used as a placeholder for any character. Example: "12x" would match "12**1**", "12**2**", "12**3**", "12**a**", etc.
-	The dash "-" can be used to match a range of characters within the brackets. Example: "[5-7]" would match the number "**5**", "**6**" or "**7**".
,	The comma "," can be used as a separator within the bracket. Example:

	"[2,5,8]" would match the number "**2**", "**5**" or "**8**".
[]	The square bracket "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: "91[5-7]1234"would match "91**5**1234", "91**6**1234", "91**7**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 "**92**3", "**15**3", "**67**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**235**45**99**". "$1" means 3 digits in the first parenthesis, that is, "235". "$2" means 2 digits in the second parenthesis, that is, "99".

Replace Rule

Replace rule is an alternative string that replaces the numbers entered by the user. IP phones support up to 100 replace rules, which can be created either one by one or in batch using a replace rule template. For more information on how to customize a replace rule template, refer to Customizing Replace Rule Template File on page 230.

Procedure

Replace rule can be created using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Create the replace rule for the IP phone. **Parameters:** dialplan.replace.prefix.X dialplan.replace.replace.X dialplan.replace.line_id.X
Web User Interface		Create the replace rule for the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-dialplan&q=load

Details of Configuration Parameters:

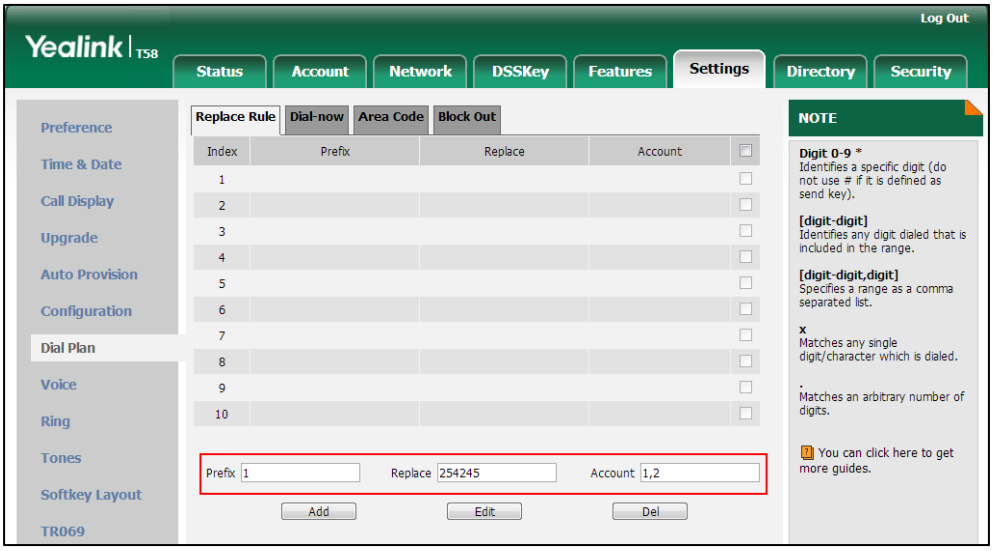
Parameters	Permitted Values	Default
dialplan.replace.prefix.X (X ranges from 1 to 100)	**String within 32 characters**	**Blank**
Description: Configures the entered number to be replaced. **Example:** dialplan.replace.prefix.1 = 1 **Note**: It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Replace Rule->Prefix **Phone User Interface:** None		
dialplan.replace.replace.X (X ranges from 1 to 100)	**String within 32 characters**	**Blank**
Description: Configures the alternate number to replace the entered number. **Example:** dialplan.replace.prefix.1 =1 and dialplan.replace.replace.1 = 254245 When you enter the number "1" and press the send key, the number "254245" will replace the entered number "1". **Note**: It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Replace Rule->Replace **Phone User Interface:** None		
dialplan.replace.line_id.X (X ranges from 1 to 100)	**0, Integer from 1 to 16**	**Blank (for all lines)**
Description: Configures the desired line to apply the replace rule. The digit 0 stands for all lines. If it is left blank, the replace rule will apply to all lines on the IP phone. **Permitted Values:** 0 to 16 (for SIP-T58V/T58A/T56A)		

Parameters	Permitted Values	Default
0, 1 (for CP960) **Example:** dialplan.replace.line_id.1 = 1,2 **Note:** Multiple line IDs are separated by commas. It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Replace Rule->Account **Phone User Interface:** None		

To create a replace rule via web user interface:

1. Click on **Settings**->**Dial Plan**->**Replace Rule**.
2. Enter the string in the **Prefix** field.
3. Enter the string in the **Replace** field.
4. Enter the desired line ID in the **Account** field or leave it blank.

   If you leave this field blank or enter 0, the replace rule will apply to all accounts on the IP phone.



5. Click **Add** to add the replace rule.

Customizing Replace Rule Template File

The replace rule template helps with the creation of multiple replace rules.

You can ask the distributor or Yealink FAE for replace rule template. You can also obtain the

replace rule template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the replace rule template, refer to Obtaining Configuration Files and Resource Files on page 119.

When editing a replace rule template file, learn the following:

- <DialRule> indicates the start of the template file and </DialRule> indicates the end of the template file.
- When specifying the desired line(s) to apply the replace rule, the valid values are 0 and line ID. Multiple line IDs are separated by commas.

  The following table lists valid values of line ID for each phone model.

Phone Model	Values	Description
SIP-T58V/T58A/T56A	0~16	0 stands for all lines 1~16 stand for line1~line16
CP960	0, 1	0 stands for all lines 1 stand for line1

- At most 100 replace rules can be added to the IP phone.

The expression syntax in the replace rule template is the same as that introduced in the section Dial Plan on page 227.

To customize a replace rule template:

1. Open the template file using an ASCII editor.
2. Create replace rules between <DialRule> and </DialRule>.

   For example:

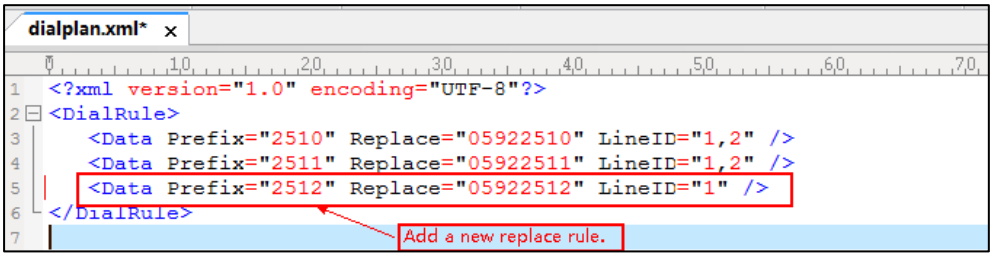
   <Data Prefix="2512" Replace="05922512" LineID="1" />

   Where:

   Prefix="" specifies the numbers to be replaced.

   Replace="" specifies the alternate string instead of what the user enters.

   LineID="" specifies the desired line(s) for this rule. When you leave it blank or enter 0, this replace rule will apply to all lines.



If you want to change the replace 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 replace rule template in the configuration files.

Procedure

Specify the access URL of the replace rule template using the following method.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL of the replace rule template. **Parameter:** dialplan_replace_rule.url

Details of Configuration Parameter:

Parameter	Permitted Values	Default
dialplan_replace_rule.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the replace rule template file. **Example:** dialplan_replace_rule.url = http://192.168.10.25/dialplan.xml During the auto provisioning process, the IP phone connects to the provisioning server "192.168.10.25", and downloads the replace rule file "dialplan.xml". **Note**: It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** None **Phone User Interface:** None		

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 236.

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Create the dial-now rule for the IP phone. **Parameters:** dialplan.dialnow.rule.X dialplan.dialnow.line_id.X
		Configure the delay time for the dial-now rule. **Parameter:** phone_setting.dialnow_delay
Web User Interface		Create the dial-now rule for the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-dialplan&q=load&dial_page=dial-now
		Configure the delay time for the dial-now rule. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of Configuration Parameters:

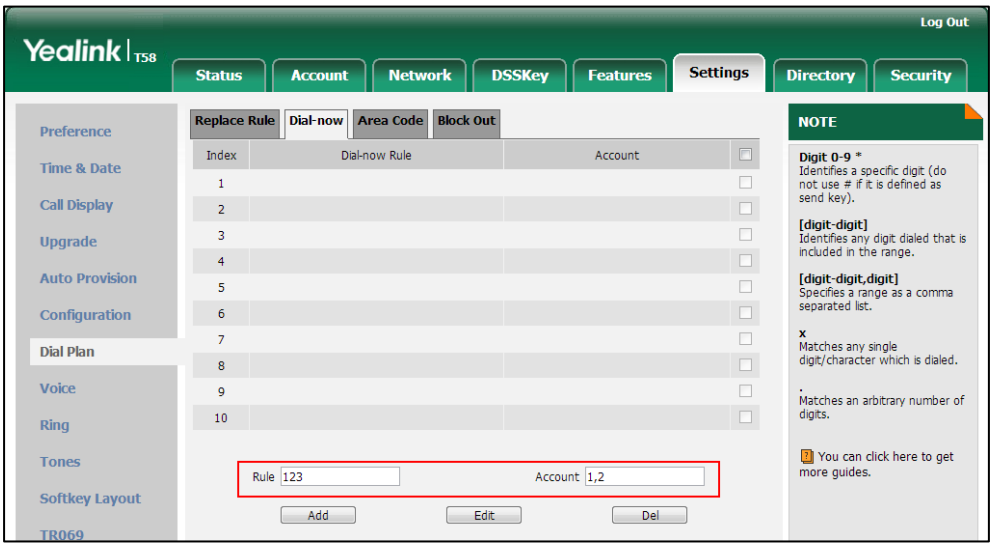
Parameters	Permitted Values	Default
dialplan.dialnow.rule.X (X ranges from 1 to 100)	**String within 511 characters**	**Blank**
Description: Configures the dial-now rule (the string used to match the numbers entered by the user). When entered numbers match the predefined dial-now rule, the IP phone will automatically dial out the numbers without pressing the send key. **Example:** dialplan.dialnow.rule.1 = 123 **Note**: It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled).		

Parameters	Permitted Values	Default
Web User Interface: Settings->Dial Plan->Dial-now->Rule **Phone User Interface:** None		
dialplan.dialnow.line_id.X (X ranges from 1 to 100)	**0, Integer from 1 to 16**	**Blank (for all lines)**
Description: Configures the desired line to apply the dial-now rule. The digit 0 stands for all lines. If it is left blank, the dial-now rule will apply to all lines on the IP phone. **Permitted Values:** 0 to 16 (for SIP-T58V/T58A/T56A) 0, 1 (for CP960) **Example:** dialplan.dialnow.line_id.1 = 1,2 **Note:** Multiple line IDs are separated by commas. It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Dial-now->Account **Phone User Interface:** None		
phone_setting.dialnow_delay	**Integer from 0 to 14**	**1**
Description: Configures the delay time (in seconds) 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. If it is set to 0, the IP phone will automatically dial out the entered number immediately. **Note**: It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **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.
3. Enter the desired line ID in the **Account** field or leave it blank.

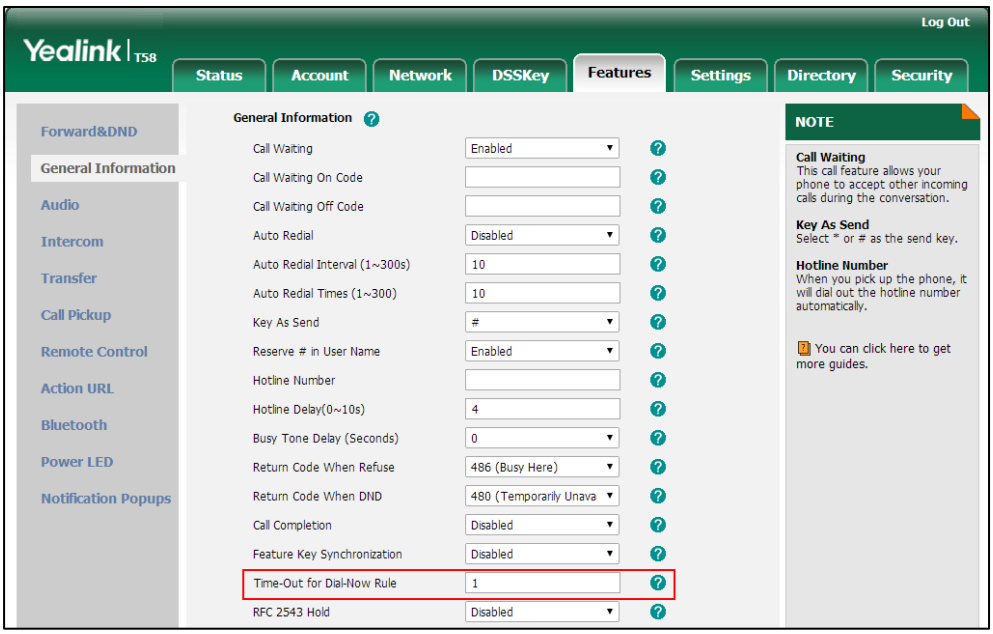
   If you leave this field blank or enter 0, the dial-now rule will apply to all accounts on the IP phone.



4. 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.



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://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the dial-now template, refer to Obtaining Configuration Files and Resource Files on page 119.

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 desired line(s) for the dial-now rule, the valid values are 0 and line ID. Multiple line IDs are separated by commas.

  The following table lists valid values of line ID for each phone model.

Phone Model	Values	Description
SIP-T58V/T58A/T56A	0~16	0 stands for all lines 1~16 stand for line1~line16
CP960	0, 1	0 stands for all lines 1 stand for line1

- 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 227.

To customize a dial-now template:

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

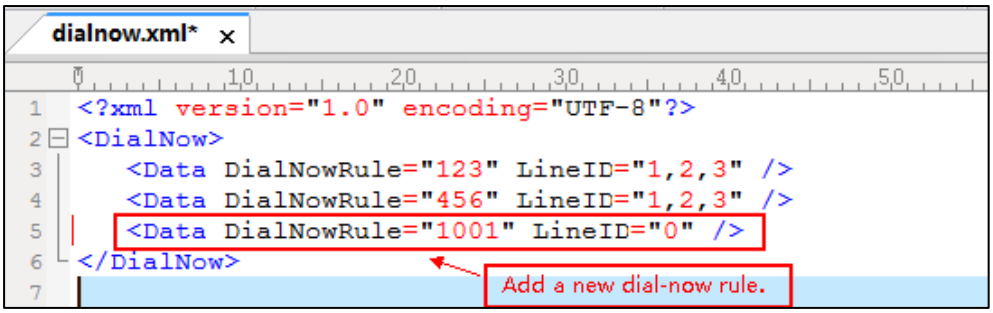
For example:

<Data DialNowRule="1001" LineID="0" />

Where:

DialNowRule="" specifies the dial-now rule.

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



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 the following method.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the access URL of the dial-now template. **Parameter:** dialplan_dialnow.url

Details of Configuration Parameter:

Parameter	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". **Note**: It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:**		

Parameter	Permitted Values	Default
None **Phone User Interface:** None		

Area Code

Area codes are also known as Numbering Plan Areas (NPAs). They usually indicate geographical areas in one country. When entered numbers match the predefined area code rule, the IP phone will automatically add the area code before the numbers when dialing out them. IP phones only support one area code rule.

Procedure

Area code rule can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Create the area code rule and specify the maximum and minimum lengths of entered numbers. **Parameters:** dialplan.area_code.code dialplan.area_code.min_len dialplan.area_code.max_len dialplan.area_code.line_id
Web User Interface		Create the area code rule and specify the maximum and minimum lengths of entered numbers. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-dialplan&q=load&dial_page=area-code

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.area_code.code	**String within 16 characters**	**Blank**
Description: Configures the area code to be added before the entered numbers when dialing out. **Example:**		

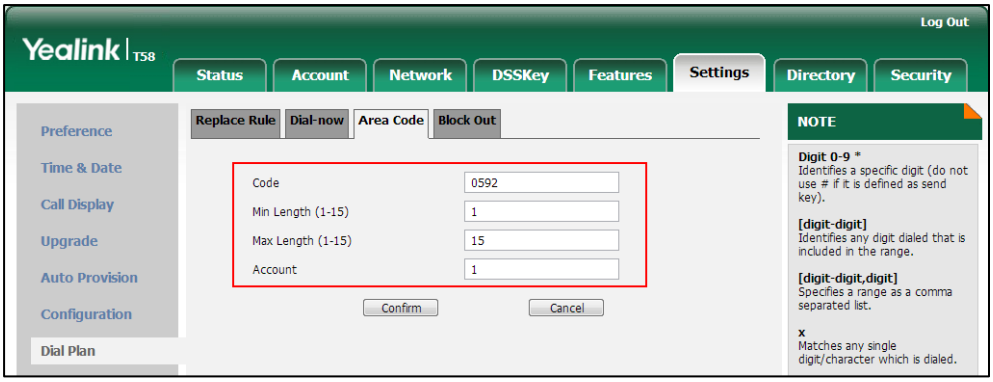
Parameters	Permitted Values	Default
dialplan.area_code.code = 0592 **Note**: The length of the entered number must be between the minimum length configured by the parameter "dialplan.area_code.min_len" and the maximum length configured by the parameter "dialplan.area_code.max_len". It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Area Code->Code **Phone User Interface:** None		
dialplan.area_code.min_len	**Integer from 1 to 15**	**1**
Description: Configures the minimum length of the entered numbers. **Note**: It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Area Code->Min Length (1-15) **Phone User Interface:** None		
dialplan.area_code.max_len	**Integer from 1 to 15**	**15**
Description: Configures the maximum length of the entered numbers. **Note**: The value must be larger than the minimum length. It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Area Code->Max Length (1-15) **Phone User Interface:** None		
dialplan.area_code.line_id	**0, Integer from 1 to 16**	**Blank (for all lines)**
Description: Configures the desired line to apply the area code rule. The digit 0 stands for all lines. If it is left blank, the area code rule will apply to all lines on the IP phone.		

Parameters	Permitted Values	Default
Permitted Values: 0 to 16 (for SIP-T58V/T58A/T56A) 0, 1 (for CP960) **Example:** dialplan.area_code.line_id = 1 **Note:** Multiple line IDs are separated by commas. It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Area Code->Account **Phone User Interface:** None		

To configure an area code rule via web user interface:

1. Click on **Settings**->**Dial Plan**->**Area Code**.
2. Enter the desired values in the **Code**, **Min Length (1-15)** and **Max Length (1-15)** fields.
3. Enter the desired line ID in the **Account** field or leave it blank.

   If you leave this field blank or enter 0, the area code rule will apply to all accounts on the IP phone.



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

Block Out

Block out rule prevents users from dialing out specific numbers. When entered numbers match the predefined block out rule, the touch screen prompts "Forbidden Number". IP phones support up to 10 block out rules.

Procedure

Block out rule can be created using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Create the block out rule for the IP phone. **Parameters:** dialplan.block_out.number.X dialplan.block_out.line_id.X
Web User Interface		Create the block out rule for the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-dialplan&q=load&dial_page=block-out

Details of Configuration Parameters:

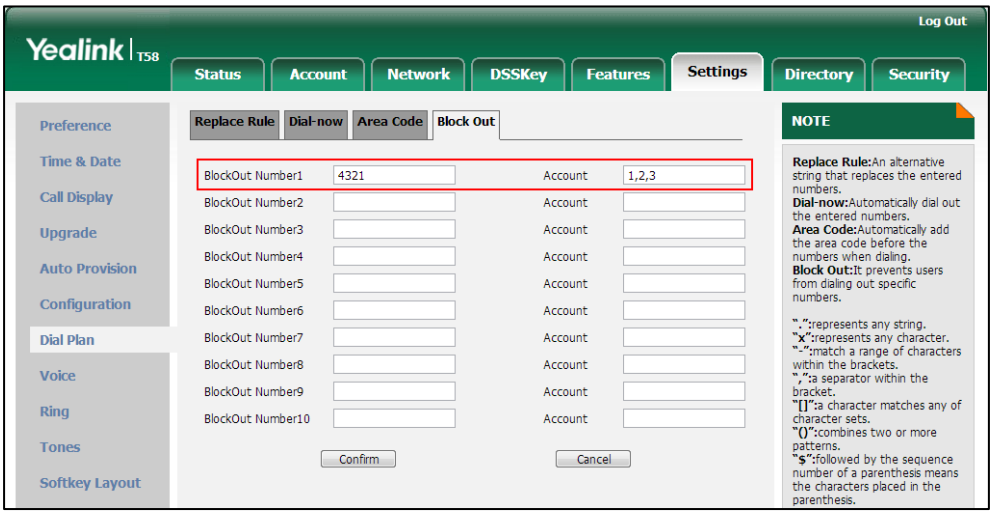
Parameters	Permitted Values	Default
dialplan.block_out.number.X (X ranges from 1 to 10)	**String within 32 characters**	**Blank**
Description: Configures the block out numbers. **Example:** dialplan.block_out.number.1 = 4321 When you dial the number "4321" on your phone, the dialing will fail and the touch screen will prompt "Forbidden Number". **Note**: It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Block Out->BlockOut NumberX **Phone User Interface:** None		
dialplan.block_out.line_id.X (X ranges from 1 to 10)	**0, Integer from 1 to 16**	**Blank (for all lines)**
Description: Configures the desired line to apply the block out rule. The digit 0 stands for all lines. If it is left blank, the block out rule will apply to all lines on the IP phone.		

Parameters	Permitted Values	Default
Permitted Values: 0 to 16 (for SIP-T58V/T58A/T56A) 0, 1 (for CP960) **Example:** dialplan.block_out.line_id.1 = 1,2,3 **Note:** Multiple line IDs are separated by commas. It works only if the values of the parameters "dialplan.digitmap.enable" and "account.X.dialplan.digitmap.enable" are set to 0 (Disabled). **Web User Interface:** Settings->Dial Plan->Block Out->Account **Phone User Interface:** None		

To create a block out rule via web user interface:

1. Click on **Settings**->**Dial Plan**->**Block Out**.
2. Enter the desired value in the **BlockOut NumberX** field.
3. Enter the desired line ID in the **Account** field or leave it blank.

   If you leave this field blank or enter 0, the block out rule will apply to all accounts on the IP phone.



4. Click **Confirm** to add the block out rule.

Dial Plan using Digit Map String Rules

Digit maps, described in RFC 3435, are defined by a single string or a list of strings. If a number entered matches any string of a digit map, the call is automatically placed. If a number entered

matches no string - an impossible match - you can specify the phone's behavior. You can specify the digit map timeout, the period of time before the entered number is dialed out.

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

T	The timer letter "T" indicates a timer expiry. If "T" is used alone (e.g., 123T), the default timeout value of 3 will be used. If "T" is not used alone (e.g., 123<Tx>, x can be a digit from 0 to 99), a complete match occurs when waiting x seconds after inputting 123.
x	The "x" can be used as a placeholder for any digit from 0 to 9. Example: "12x" would match "12**1**", "12**2**", "12**3**", etc.
[]	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**5**1234", "91**6**1234", "91**7**1234".
-	The dash "-" can be used to match a range of digits within the brackets. Example: "[35-7]" would match the number "**3**", "**5**", "**6**" or "**7**". **Note**: The digits must be concrete, e.g., [3-x] is invalid.
.	The dot "." can be used as a placeholder or multiple placeholders, including zero, of occurrences of the preceding construct. Examples: "123.T" would match "12**3**", "12**33**", "12**333**", "12**3333**", etc. "x.T" would match an arbitrary number. "[x*#+].T" would match an arbitrary character. **Note**: If the string ends with a dot (e.g., 123.), a match will occur immediately after inputting the characters before the dot (e., 123) since the dot allows for zero occurrences of the preceding construct. So we recommend you to add a letter "T" after the dot (e.g., 123.T) for inputting more characters.
R	The letter "R" indicates that certain matched strings are replaced. Using a RRR syntax, you can replace the digits between the first two *R*s with the digits between the last two *R*s. Example: "R12R234R" would replace **12** with **234**.
<:>	The letter ":" in the angle bracket indicates that certain matched strings are replaced. Using the <:> syntax, you can replace the digits before the colon with the digits after the colon. Example:

	"<12:234>" would replace **12** with **234**. It is the same with R12R234R.
!	The exclamation mark "!" can be used to prevent users from dialing out specific numbers. It can only be put last in each string of the digit map. Example: "235x!" would match "2351", "2352", "2353", etc. The number starting with 235 will be blocked to dial out.
,	The comma "," can be used as a separator to generate secondary dial tone. Example: "<9,:55>xx", after entering digit "9", secondary dial tone plays and you can complete the remaining two-digit number. **Note**: The secondary dial tone can be customized. For more information, refer to Tones on page 614.

Procedure

Digit map can be created using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure digit map on a phone basis. **Parameters:** dialplan.digitmap.enable dialplan.digitmap.string dialplan.digitmap.interdigit_long_timer dialplan.digitmap.interdigit_short_timer dialplan.digitmap.no_match_action dialplan.digitmap.active.on_hook_dialing dialplan.digitmap.apply_to.on_hook_dial dialplan.digitmap.apply_to.directory_dial dialplan.digitmap.apply_to.forward dialplan.digitmap.apply_to.press_send
	<MAC>.cfg	Configure digit map on a per-line basis. **Parameters:** account.X.dialplan.digitmap.enable account.X.dialplan.digitmap.string account.X.dialplan.digitmap.interdigit_long_timer account.X.dialplan.digitmap.interdigit_short_timer account.X.dialplan.digitmap.no_match_action account.X.dialplan.digitmap.active.on_hook_dialing

		account.X.dialplan.digitmap.apply_to.on_hook_dial account.X.dialplan.digitmap.apply_to.directory_dial account.X.dialplan.digitmap.apply_to.forward account.X.dialplan.digitmap.apply_to.press_send

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.digitmap.enable	**0 or 1**	**0**
Description: Enables or disables the digit map feature for the IP phone. **0**-Disabled **1**-Enabled **Note:** The value configured by the parameter "account.X.dialplan.digitmap.enable" takes precedence over that configured by this parameter. **Web User Interface:** None **Phone User Interface:** None		
dialplan.digitmap.string	**String within 2048 characters**	**[2-9]11 | 0T | 011xxx.T | [0-1][2-9]xx xxxxxxx | [2-9]xx xxxxxxx | [2-9]xxxT | **x.T | +x.T| 00x.T**
Description: Configures digit map pattern used for the dial plan. **Example**: dialplan.digitmap.string = <[2-9]x:86>3.T|0x.!|1xxx **Note**: The string must be compatible with the digit map feature of MGCP described in 2.1.5 of RFC 3435. It works only if the value of the parameter "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.string" takes precedence over that configured by this parameter. **Web User Interface:** None		

Parameters	Permitted Values	Default
Phone User Interface: None		
dialplan.digitmap.interdigit_long_timer	**Integer from 0 to 255**	**10**
Description: Configures the time (in seconds) for the IP phone to wait before dialing an entered number if it matches part of any string of the digit map. If it is set to 0, the IP phone will not dial the entered number if it only a partial match exists. The value of this parameter should be greater than that configured by the parameter "dialplan.digitmap.interdigit_short_timer". **For example**: dialplan.digitmap.string = 1xxT|xxxxx<T1> dialplan.digitmap.interdigit_long_timer = 10 dialplan.digitmap.interdigit_short_timer = 5 When you enter 1, it matches part of two digit maps, the IP phone tries to wait 10 seconds and then dials out 1 if no numbers entered; When you enter 15, it also matches part of two digit maps, the IP phone tries to wait 10 seconds and then dials out 15 if no numbers entered; When you enter 153, it also matches part of two digit maps, the IP phone tries to wait 10 seconds. But after waiting for 5 seconds, it completely matches the first digit map and then immediately dials out 153. **Note:** It works only if the value of the parameter "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.interdigit_long_timer" takes precedence over that configured by this parameter. **Web User Interface:** None **Phone User Interface:** None		
dialplan.digitmap.interdigit_short_timer	**Refer to the following content**	**3**
Description: Configures the timeout interval (in seconds) for any string of digit map. The IP phone will wait this many seconds before matching the entered digits to the dial plan and placing the call. **Valid values are:**		

Parameters	Permitted Values	Default
Single configuration (configure a specific value for the timer letter "T" for all strings with "T" of the digit map) **Example**: dialplan.digitmap.interdigit_short_timer = 5 If the value of the parameter "dialplan.digitmap.string" is set to <[2-9]x:86>3.T|0T, the IP phone will wait 5 seconds before matching the entered digits to this dial plan and placing the call. Distribution configuration (configure a string of positive integers separated by "|" for each string of the digit map in the corresponding position) If there are more digit maps than timeout values, the last timeout is applied to the extra digit map. If there are more timeout values than digit maps, the extra timeout values are ignored. **Example**: dialplan.digitmap.interdigit_short_timer = 4|5|3|6|2|1 If the value of the parameter "dialplan.digitmap.string" is set to <[2-9]x:86>3.T|2T|1xxT|0x.!|[2-9]11T, 4 is applied to the "<[2-9]x:86>3.T" digit map, 5 is applied to "2T" digit map, 3 is applied to "1xxT" digit map, 6 is applied to "0x.!" digit map, 2 is applied to the "[2-9]11T" digit map, the last digit 1 is ignored. **Note:** It works only if the value of the parameter "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.interdigit_short_timer" takes precedence over that configured by this parameter. **Web User Interface:** None **Phone User Interface:** None		
dialplan.digitmap.no_match_action	**0, 1 or 2**	**0**
Description: Configures the behavior when an impossible digit map match occurs. **0**-prevent users from entering a number and immediately dial out the entered numbers **1**-the dialing will fail and the LCD screen will prompt "Forbidden Number" **2**-allow users to accumulate digits and dispatch call manually with the send key or automatically dial out the entered number after a certain period of time configured by the parameter "dialplan.digitmap.interdigit_long_timer" **Note:** It works only if the value of the parameter "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.no_match_action" takes precedence over that		

Parameters	Permitted Values	Default
configured by this parameter. **Web User Interface:** None **Phone User Interface:** None		
dialplan.digitmap.active.on_hook_dialing	**0 or 1**	**0**
Description: Enables or disables the entered numbers to match the predefined string of the digit map in real time. It is only applicable to the on-hook dialing. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.active.on_hook_dialing" takes precedence over that configured by this parameter. It is not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		
dialplan.digitmap.apply_to.on_hook_dial	**0 or 1**	**1**
Description: Enables or disables the entered number to match the predefined string of the digit map after pressing a send key when dialing on-hook or pressing the DSS key (e.g., speed dial, BLF or prefix key). **0**-Disabled **1**-Enabled **Note**: It works only if the value of the parameter "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.on_hook_dial" takes precedence over that configured by this parameter. On-hook dialing is not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		

Parameters	Permitted Values	Default
dialplan.digitmap.apply_to.directory_dial	**0 or 1**	**1**
Description: Enables or disables the digit map to be applied to the numbers dialed from the directory. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.directory_dial" takes precedence over that configured by this parameter. **Web User Interface:** None **Phone User Interface:** None		
dialplan.digitmap.apply_to.forward	**0 or 1**	**1**
Description: Enables or disables the digit map to be applied to the numbers that you want to forward to when performing call forward. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the incoming calls will be forwarded to a desired destination number according to the string of the digit map. **Note:** It works only if the value of the parameter "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.forward" takes precedence over that configured by this parameter. **Web User Interface:** None **Phone User Interface:** None		
dialplan.digitmap.apply_to.press_send	**0 or 1**	**1**
Description: Enables or disables the entered number to match the predefined string of the digit map after pressing a send key. It is only applicable to off-hook dialing.		

Parameters	Permitted Values	Default
The off-hook dialing includes: pick up the handset, press the Speakerphone key or press the line key when the phone is idle. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "dialplan.digitmap.enable" or "account.X.dialplan.digitmap.enable" is set to 1 (Enabled). The value configured by the parameter "account.X.dialplan.digitmap.apply_to.press_send" takes precedence over that configured by this parameter. **Web User Interface:** None **Phone User Interface:** None		

Per-Line Parameters:

The parameters listed in the above table have a per-line equivalent that you can configure. All of the per-line parameters are listed in the following table. Note that the per-line parameters take precedence over the global parameters. For example, "account.X.dialplan.digitmap.enable" takes precedence over "dialplan.digitmap.enable".

X stands for the serial number of the account.

X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)

X is equal to 1 (for CP960)

Per-Line Parameters	Global Parameters
account.X.dialplan.digitmap.enable	**dialplan.digitmap.enable**
account.X.dialplan.digitmap.string	**dialplan.digitmap.string**
account.X.dialplan.digitmap.interdigit_long_timer	**dialplan.digitmap.interdigit_long_timer**
account.X.dialplan.digitmap.interdigit_short_timer	**dialplan.digitmap.interdigit_short_timer**
account.X.dialplan.digitmap.no_match_action	**dialplan.digitmap.no_match_action**
account.X.dialplan.digitmap.active.on_hook_dialing (not applicable to CP960 IP phones)	**dialplan.digitmap.active.on_hook_dialing (not applicable to CP960 IP phones)**

Per-Line Parameters	Global Parameters
account.X.dialplan.digitmap.apply_to.on_hook_dial	**dialplan.digitmap.apply_to.on_hook_dial**
account.X.dialplan.digitmap.apply_to.directory_dial	**dialplan.digitmap.apply_to.directory_dial**
account.X.dialplan.digitmap.apply_to.forward	**dialplan.digitmap.apply_to.forward**
account.X.dialplan.digitmap.apply_to.press_send	**dialplan.digitmap.apply_to.press_send**

Emergency Dialplan

Yealink IP phones support dialing emergency telephone numbers when the phone is locked (refer to Phone Lock). Due to the fact that the IP phone must have a registered account or a configured SIP server, it may not meet the need of dialing emergency telephone number at any time.

Emergency dialplan allows users to dial the emergency telephone number (emergency services number) at any time when the IP phone is powered on and has been connected to the network. It is available even if your phone keypad is locked or no SIP account is registered.

Note Contact your local phone service provider for available emergency numbers in your area.

Emergency Dial Plan

Users can configure the emergency dial plan on the phone (e.g., emergency number, emergency routing). The phone determines if this is an emergency number by checking the emergency dial plan configured on the phone. When placing an emergency call, the call is directed to the configured emergency server. Multiple emergency servers may need to be configured for emergency routing, avoiding that emergency calls couldn't get through because of the server failure. If the phone is not locked, it checks against the regular dial plan (refer to Dial Plan). If the phone is locked, it checks against the emergency dial plan.

Emergency Location Identification Number (ELIN)

The IP Phones support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). LLDP-MED allows the phone to use the location information, Emergency Location Identification Number (ELIN), sent by the switch, as a caller ID for making emergency calls. The outbound identity used in the P-Asserted-Identity (PAI) header of the SIP INVITE request is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN). The administrator can customize the outbound identity. The custom outbound identity will be used if the phone fails to get the LLDP-MED ELIN value.

The following is an example of the PAI header:

P-asserted-identity: <sip: **1234567890**@abc.com > (where 1234567890 is the custom outbound identity.)

P-Access-Network-Info (PANI)

When placing an emergency call, the MAC address of the phone/connected switch should be added in the P-Access-Network-Info (PANI) header of the INVITE message. It helps the aid agency to immediately identify the caller's location, improving rescue efficiency.

The following is an example of the PANI header:

P-Access-Network-Info: IEEE-802.3; eth-location="**00:15:65:74:b1:6e**" (where 00156574B16E is the phone's MAC address.)

Procedure

Emergency dialplan can be configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the emergency dialplan. **Parameters:** dialplan.emergency.asserted_id_source dialplan.emergency.custom_asserted_id dialplan.emergency.server.X.address dialplan.emergency.server.X.port dialplan.emergency.server.X.transport_type dialplan.emergency.X.value dialplan.emergency.X.server_priority

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dialplan.emergency.asserted_id_source	**ELIN or CUSTOM**	**ELIN**
Description: Configures the precedence of source of emergency outbound identities when placing an emergency call. If it is set to ELIN, the outbound identity used in the P-Asserted-Identity (PAI) header of the SIP INVITE request is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN). The custom outbound identity configured by "dialplan.emergency.custom_asserted_id" will be used if the phone fails to get the LLDP-MED ELIN value. If it is set to CUSTOM, the custom outbound identity configured by "dialplan.emergency.custom_asserted_id" will be used; if the value of the parameter		

Parameters	Permitted Values	Default
"dialplan.emergency.custom_asserted_id" is left blank, the LLDP-MED ELIN value will be used. **Note**: If the obtained LLDP-MED ELIN value is blank and no custom outbound identity, the PAI header will not be included in the SIP INVITE request. **Web User Interface:** None **Phone User Interface:** None		
dialplan.emergency.custom_asserted_id	**10-25 digits, SIP URI, or TEL URI**	**Blank**
Description: Configures the custom outbound identity when placing an emergency call. If using a TEL URI, for example, tel:+16045558000. The full URI is included in the P-Asserted-Identity (PAI) header (e.g., <tel:+16045558000>). If using a SIP URI, for example, sip:1234567890123@abc.com. The full URI is included in the P-Asserted-Identity (PAI) header and the address will be replaced by the emergency server (e.g., <sip:1234567890123@emergency.com>). If using a 10-25 digit number, for example, 1234567890. The SIP URI constructed from the number and SIP server (e.g., abc.com) is included in the P-Asserted-Identity (PAI) header (e.g., <sip:1234567890@abc.com>). **Web User Interface:** None **Phone User Interface:** None		
dialplan.emergency.server.X.address (X ranges from 1 to 3)	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the emergency server X to be used for routing calls. **Note**: If the account is registered successfully or failed (the account information has been configured), the emergency calls will be dialed using the following priority: SIP server>emergency server; if the account is not registered, the emergency server will be used. **Web User Interface:** None **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
dialplan.emergency.server.X.port (X ranges from 1 to 3)	**Integer from 1 to 65535**	**5060**
Description: Configures the port of emergency server X to be used for routing calls. **Web User Interface:** None **Phone User Interface:** None		
dialplan.emergency.server.X.transport_type (X ranges from 1 to 3)	**0, 1, 2 or 3**	**0**
Description: Configures the transport method the IP phone uses to communicate with the emergency server X. **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR **Web User Interface:** None **Phone User Interface:** None		
dialplan.emergency.X.value (X ranges from 1 to 255)	**number or SIP URI**	**Refer to the following content**
Description: Configures the emergency number to use on your IP phone so a caller can contact emergency services in the local area when required. **Default**: When X = 1, the default value is 911; When X = 2-255, the default value is Blank. **Web User Interface:** None **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
dialplan.emergency.X.server_priority (X ranges from 1 to 255)	**a combination of digits 1, 2 and 3**	**1, 2, 3**
Description: Configures the priority for the emergency servers to be used. The digits are separated by commas. The servers to be used in the order listed (left to right). The IP phone tries to send the INVITE request to the emergency server with higher priority. If the emergency server with higher priority does not respond correctly to the INVITE, then the phone tries to make the call using the emergency server with lower priority, and so forth. The IP phone tries to send the INVITE request to each emergency server for three times. **Example**: dialplan.emergency.1.server_priority = 2, 1, 3 It means the IP phone sends the INVITE request to the emergency server 2 first. If the emergency server 2 does not respond correctly to the INVITE, then tries to make the call using the emergency server 1. If the emergency server 1 does not respond correctly to the INVITE, then tries to make the call using the emergency server 3. The IP phone tries to send the INVITE request to each emergency server for three times. **Note**: If the IP address of the emergency server with higher priority has not been configured, the emergency server with lower priority will be used. If the account is registered successfully or failed (the account information has been configured), the emergency calls will be dialed using the following priority: SIP server>emergency server; if the account is not registered, the emergency server will be used. **Web User Interface:** None **Phone User Interface:** None		

Hotline

Hotline, sometimes referred to as hot dialing, is a point-to-point communication link in which a call is automatically directed to the preset hotline number. The IP phone automatically dials out the hotline number using the first available line after a specified time interval when you lift the handset, press the Speakerphone key or tap the line key. IP phones only support one hotline number.

Procedure

Hotline can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the hotline number. **Parameter:** features.hotline_number
		Specify the time the IP phone waits before automatically dialing out the hotline number. **Parameter:** features.hotline_delay
Web User Interface		Configure the hotline number. Specify the time the IP phone waits before automatically dialing out the hotline number. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
Phone User Interface		Configure the hotline number. Specify the time the IP phone waits before automatically dialing out the hotline number.

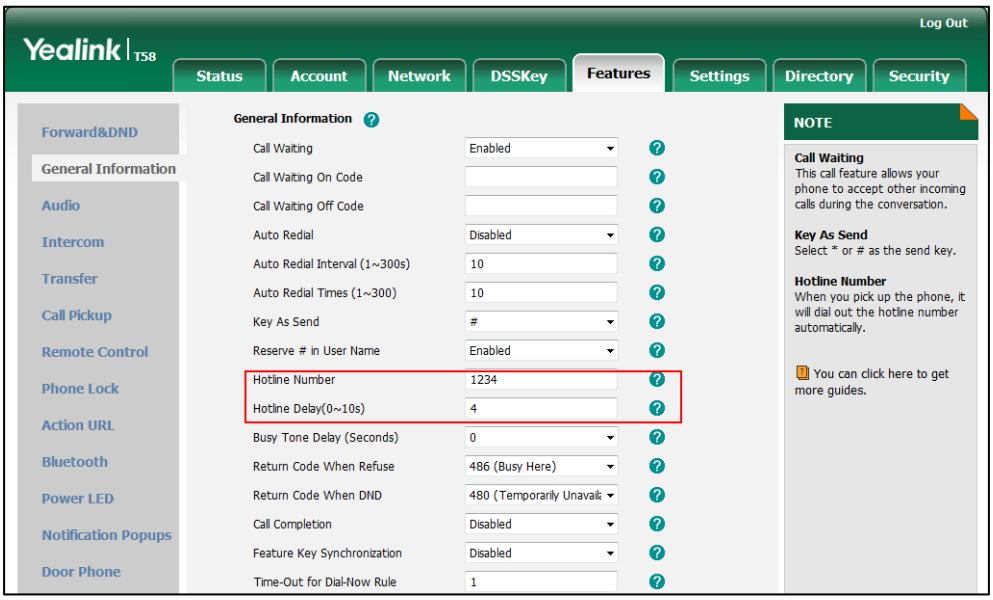
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.hotline_number	**String within 32 characters**	**Blank**
Description: Configures the hotline number that the IP phone automatically dials out when you lift the handset, press the Speakerphone key or tap the line key. Leaving it blank disables hotline feature. **Example:** features.hotline_number = 1234 **Note:** Handset and Speakerphone key are not applicable to CP960 IP phones. **Web User Interface:** Features->General Information->Hotline Number		

Parameters	Permitted Values	Default
Phone User Interface: Settings->Features->Hot Line->Number		
features.hotline_delay	**Integer from 0 to 10**	**4**
Description: Configures the waiting time (in seconds) for the IP phone to automatically dial out the hotline number. If it is set to 0 (0s), the IP phone will immediately dial out the preconfigured hotline number when you lift the handset, press the Speakerphone key or tap the line key. If it is set to a value greater than 0, the IP phone will wait the designated seconds before dialing out the predefined hotline number when you lift the handset, press the Speakerphone key or tap the line key. **Note:** Handset and Speakerphone key are not applicable to CP960 IP phones. **Web User Interface:** Features->General Information->Hotline Delay(0~10s) **Phone User Interface:** Settings->Features->Hot Line->Hotline Delay		

To configure hotline via web user interface:

1. Click on **Features**->**General Information**.
2. Enter the hotline number in the **Hotline Number** field.
3. Enter the delay time in the **Hotline Delay(0~10s)** field.



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

To configure hotline via phone user interface:

1. Tap **Settings**->**Features**->**Hot Line**.
2. Enter the hotline number in the **Number** field.
3. Enter the waiting time (in seconds) in the **Hotline Delay** field.
4. Tap ✓ to accept the change.

Off Hook Hot Line Dialing

For security reasons, IP phones support off hook hot line dialing feature, which allows the phone to first dial out the pre-configured number when the user lifts the handset, presses the Speakerphone key or taps desired line key, dials out a call using the account with this feature enabled. The SIP server may then prompt the user to enter an activation code for call service. Only if the user enters a valid activation code, the IP phone will use this account to dial out a call successfully.

Off hook hot line dialing feature is configurable on a per-line basis and depends on support from a SIP server.

Note

Off hook hot line dialing feature limits the call-out permission of this account and disables the hotline feature. For example, when the phone goes off hook using the account with this feature enabled, the configured hotline number will not be dialed out automatically.

The server actions may vary from different servers.

It is also applicable to the IP call and intercom call.

Procedure

Off hook hot line dialing can be configured using the configuration files.

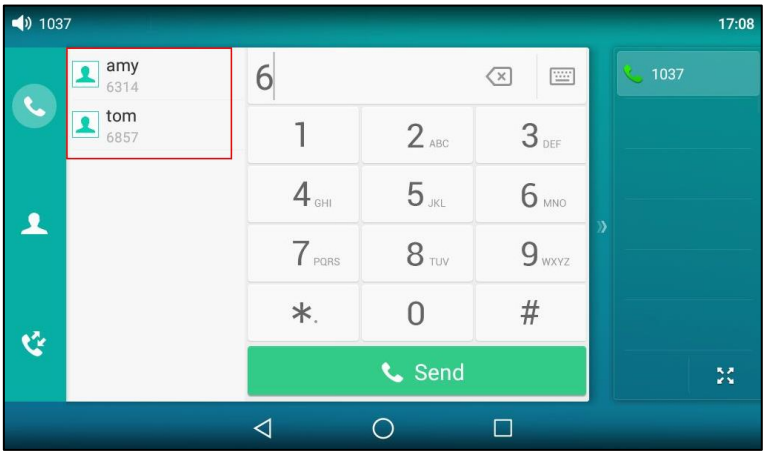
Central Provisioning (Configuration File)	<MAC>.cfg	Configure off hook hot line dialing feature. **Parameter:** account.X.auto_dial_enable
		Specify the number that the phone first dials out. **Parameter:** account.X.auto_dial_num

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.auto_dial_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to first dial out a pre-configured number when a user lifts the handset, presses the Speakerphone key or taps the desired line key or dials out a call using account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the phone will first dial out the pre-configured number (configured by the parameter "account.X.auto_dial_num") when a user lifts the handset, presses the Speakerphone key or taps the desired line key, dials out a call using account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: Handset and Speakerphone key are not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		
account.X.auto_dial_num (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the number that the IP phone first dials out when a user lifts the handset, presses the Speakerphone key or taps the desired line key, dials out a call using account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: It works only if the value of the parameter "account.X.auto_dial_enable" is set to 1 (Enabled). Handset and Speakerphone key are not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		

Search Source List In Dialing

Search source list in dialing allows the IP phone to automatically search entries from the search source list based on the entered string, and display results on the pre-dialing screen. The user can select the desired entry to dial out quickly.



The search source list can be Local Directory, History, Remote Phone Book and LDAP. The search source list can be configured using a supplied super search template file (super_search.xml).

Customizing a Super Search Template File

You can ask the distributor or Yealink FAE for super search template. You can also obtain the super search template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the super search template, refer to Obtaining Configuration Files and Resource Files on page 119.

The following table lists meaning of each variable in the super search template file:

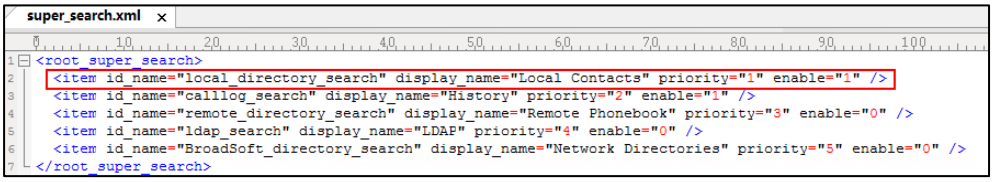
Element	Attribute	Description
root_super_search	No	File root element
Item	No	Super search list's root element
id_name	local_directory_search calllog_search remote_directory_search ldap_search BroadSoft_directory_search	The directory list (For example, "local_directory_search" for the local directory list). **Note**: Do not edit this field.
display_name	Local Contacts History Remote Phonebook LDAP Network Directories	The display name of the directory list. **Note**: We recommend you do not edit this field. Network Directories and BroadSoft

Element	Attribute	Description
		Buddies lists are hidden for IP phones in neutral firmware, which are designed for the BroadWorks environment.
priority	1, 2, 3, 4 and 5. 1 is the highest priority, 5 is the lowest.	The priority of the search results.
enable	0/1, **0**: Disabled **1**: Enabled	Enable or disable the IP phone to search the desired directory list.

Customizing a super search template:

1. Open the template file using an ASCII editor.
2. For each directory list that you want to configure, edit the corresponding string in the file.
3. For example, configure the local directory list, edit the values within double quotes in the following strings:

   <item id_name="local_directory_search" display_name="Local Contacts" priority="1" enable="1"/>



4. Save the change and place this file to the provisioning server (e.g., 192.168.1.20).
5. Specify the access URL of the custom super search template file in the configuration files (e.g., super_search.url = http://192.168.1.20/super_search.xml).

Procedure

Search source list in dialing can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL of the super search template file. **Parameter:** super_search.url
Web User Interface		Configure the search source list in dialing. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=contacts-favorite&q=load

Details of the Configuration Parameter:

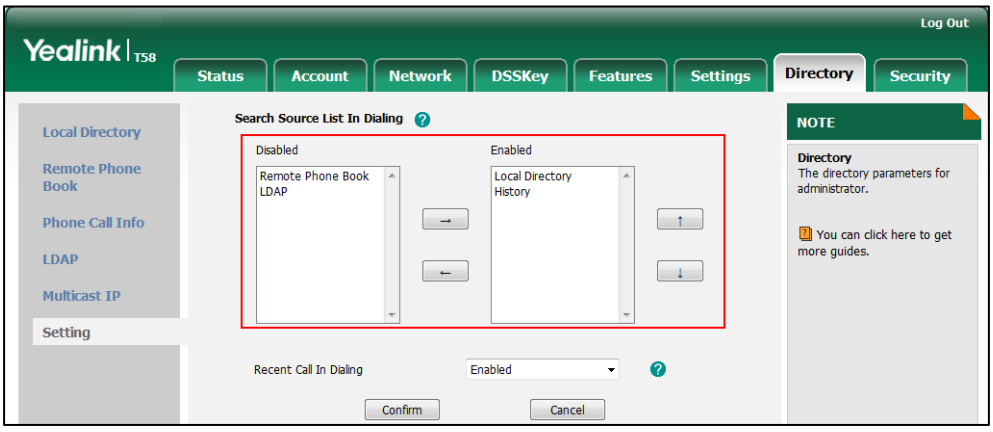
Parameter	Permitted Values	Default
super_search.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the super search template file. **Example**: super_search.url = http://192.168.1.20/super_search.xml During the auto provisioning process, the IP phone connects to the provisioning server "192.168.1.20", and downloads the super search template file "super_search.xml". **Web User Interface:** Directory->Setting->Search Source List In Dialing **Phone User Interface:** None		

To configure search source list in dialing via web user interface:

1. Click on **Directory**->**Setting**.
2. In the **Search Source List In Dialing** block, select the desired list from the **Disabled** column and then click → .

   The selected list appears in the **Enabled** column.
3. Repeat the step 2 to add more lists to the **Enabled** column.
4. To remove a list from the **Enabled** column, select the desired list and then click ←.
5. To adjust the display order of search results, select the desired list and then click ↑ or ↓ .

   The touch screen displays the search results in the adjusted order.



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

Save Call Log

IP phones record and maintain phone events to a call log, also known as a call list. The call log contains call information such as remote party identification, time and date of the call, 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. 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 web user interface: **Directory**->**Phone Call Info**.

Note You can identify call types by the icons from a combined call log list (e.g., Local Log). For more information on icons, refer to Appendix G: Reading Icons on page 793.

Procedure

Call log can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure call log feature. **Parameter:** features.save_call_history
Web User Interface		Configure call log feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
Phone User Interface		Configure call log feature.

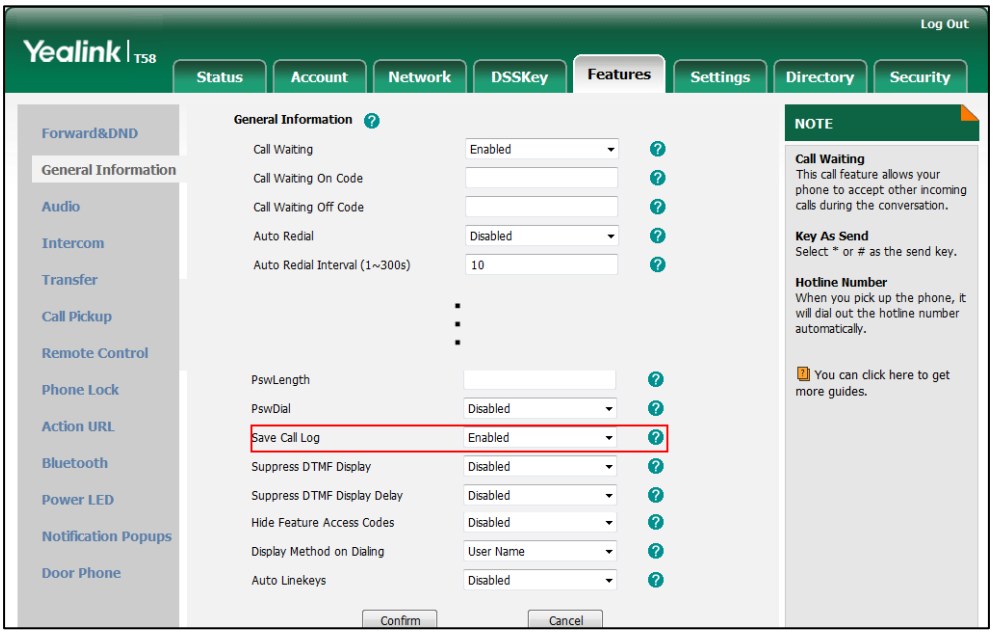
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.save_call_history	**0 or 1**	**1**

Parameter	Permitted Values	Default
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 log the missed calls, placed calls, received calls and forwarded calls in the call log lists. **Web User Interface:** Features->General Information->Save Call Log **Phone User Interface:** Settings->Features->History Record->History Record		

To configure 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**.



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

To configure call log feature via phone user interface:

1. Tap **Settings**->**Features**->**History Record**.
2. Tap the **On** radio box in the **History Record** field.
3. Tap ✓ to accept the change.

Call List Show Number

Call list show number allows the IP phone to show the phone number instead of the name in the call log list. To use this feature, make sure the save call log feature is enabled. For more information on save call log, refer to Save Call Log on page 263.

Procedure

Call list show number can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure call list show number. **Parameter:** features.call_log_show_num
Web User Interface		Configure call list show number. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

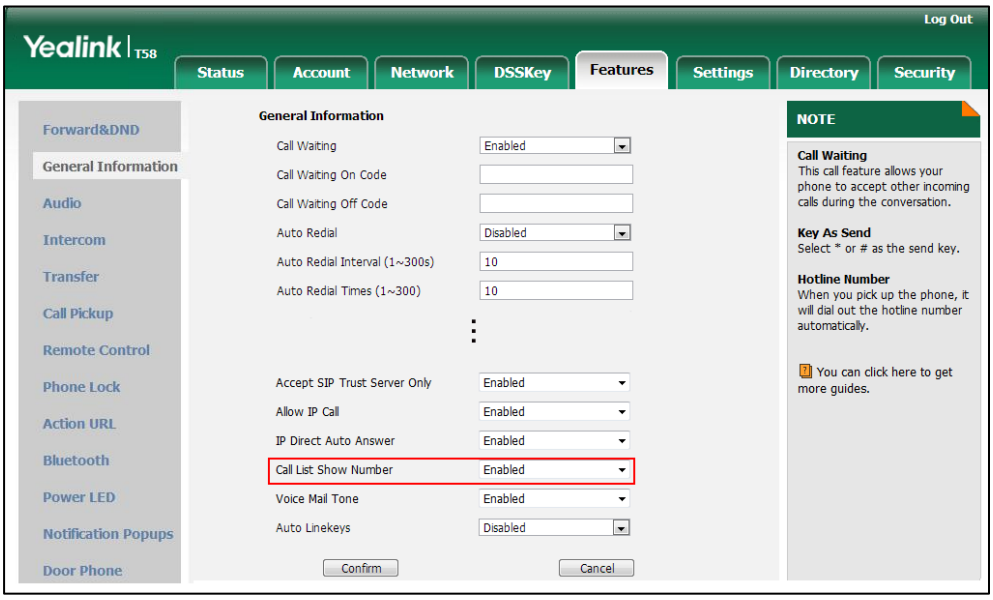
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.call_log_show_num	**0 or 1**	**0**
Description: Enables or disables the IP phone to show the other party's phone number instead of the name in the call log lists. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone will show the other party's name in the call log lists. If it is set to 1 (Enabled), the IP phone will show the other party's phone number in the call log lists. **Note**: It works only if the value of the parameter "features.save_call_history" is set to 1 (Enabled). **Web User Interface:** Features->General Information->Call List Show Number **Phone User Interface:** None		

To configure call list show number via web user interface:

1. Click on **Features**->**General Information**.

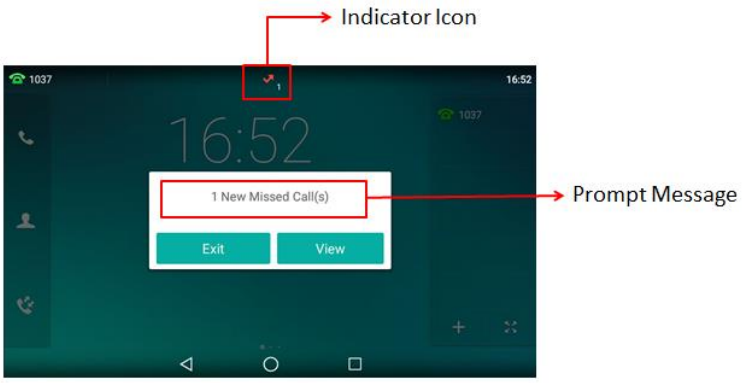
2. Select the desired value from the pull-down list of **Call List Show Number**.



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

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.



You can configure whether to display a prompt message when missing calls. For more information, refer to Notification Popups on page 149.

Procedure

Missed call log can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure missed call log feature. **Parameter:**

		account.X.missed_calllog
Web User Interface		Configure missed call log feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-basic&q=load&acc=0

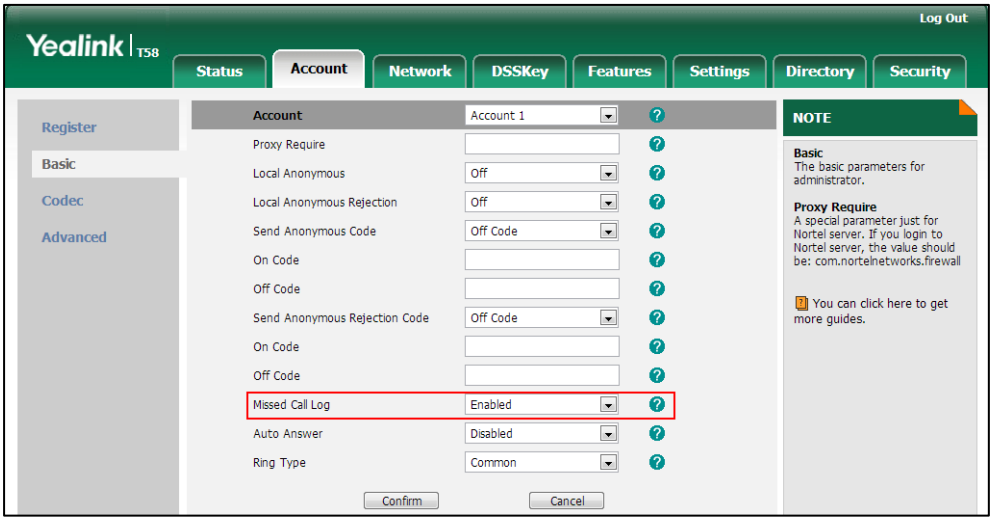
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.missed_calllog	**0 or 1**	**1**
Description: Enables or disables the IP phone to indicate and record missed calls for account X. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone does not display a prompt message and an indicator icon on the idle screen and log the missed call in the Missed Calls list when missing calls. If it is set to 1 (Enabled), the IP phone displays a prompt message and an indicator icon on the idle screen and logs the missed call in the Missed Calls list when missing calls. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note:** It works only if the value of the parameter "features.save_call_history" is set to 1 (Enabled). The prompt message displays only if the value of the parameter "features.missed_call_popup.enable" 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 account from the pull-down list of **Account**.

3. Select the desired value from the pull-down list of **Missed Call Log**.



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

Local Directory

IP phones maintain a local directory. The local directory can store up to 1000 contacts and 48 groups. When adding a contact to the local directory, in addition to name and phone numbers, you can also specify the account, 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://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the local contact file, refer to Obtaining Configuration Files and Resource Files on page 119.

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

Element	Values	Description
root_group	no	Group list's root element.

Element	Values	Description
group	no	Group's root element.
display_name	All Contacts Blacklist	An element of group. Group name.
ring	Format of the value: System ring tone: **Auto** **Silent.wav** **Splash.wav** **RingN.wav** (integer N ranges from 1 to 8) Custom ring tone: **Name.wav**	An element of group. Group ring tone.
root_contact	no	Contact list's root element.
contact	no	Contact's root element.
display_name	String	An element of contact. Contact name. **Note**: 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.
line	-1~15; Multiple line IDs are separated by commas.	The desired line you want to add the contact to. **Note**: It is not applicable to CP960 IP phones.
ring	Format of the value: System ring tone: **Auto** **Silent.wav** **Splash.wav** **RingN.wav** (integer N ranges from 1 to 8) Custom ring tone: **Name.wav**	An element of contact. Contact ring tone.
group_id_name	Valid Value: built-in: All Contacts, Blacklist custom: XXX (e.g., Friend)	Group name of a contact.
default_photo	Format of the value: **Resource: avatar and icon name**	Contact avatar and icon.

Element	Values	Description
	(the built-in picture) **Config: avatar and icon name** (the custom picture)	

The following table lists valid values of line for each phone model.

Phone Model	Values	Description
SIP-T58V/T58A/T56A	-1~15	-1 stands for Auto (the first registered line) 0~15 stand for line1~line16

Customizing a Local Contact File

The following shows the procedure of customizing a local contact file for SIP-T58V/T58A/T56A/CP960 IP phones:

Scenario A - Using the Built-in Avatar for Contact

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:

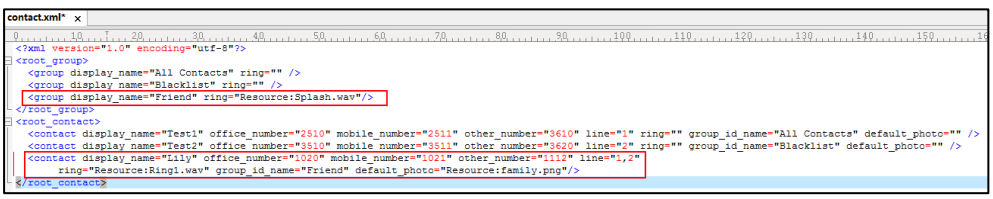
   <group display_name="" ring=""/>
3. For each contact that you want to add, add the following string to the file. Each starts on a separate line:

   <contact display_name="" office_number="" mobile_number="" other_number="" line="" ring="" group_id_name="" default_photo=""/>
4. Specify the values within double quotes.

   For example:

   <group display_name="Friend" ring="Resource:Splash.wav"/>

   <contact display_name="Lily" office_number="1020" mobile_number="1021" other_number="1112" line="1,2" ring="Resource:Ring1.wav" group_id_name="Friend" default_photo="Resource:family.png"/>



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".

Scenario B - Using the Custom Avatar and Icon for Contact

To specify custom avatars and icons for contacts, you need to upload the pictures to the provisioning server in advance.

There are three methods to upload the pictures:

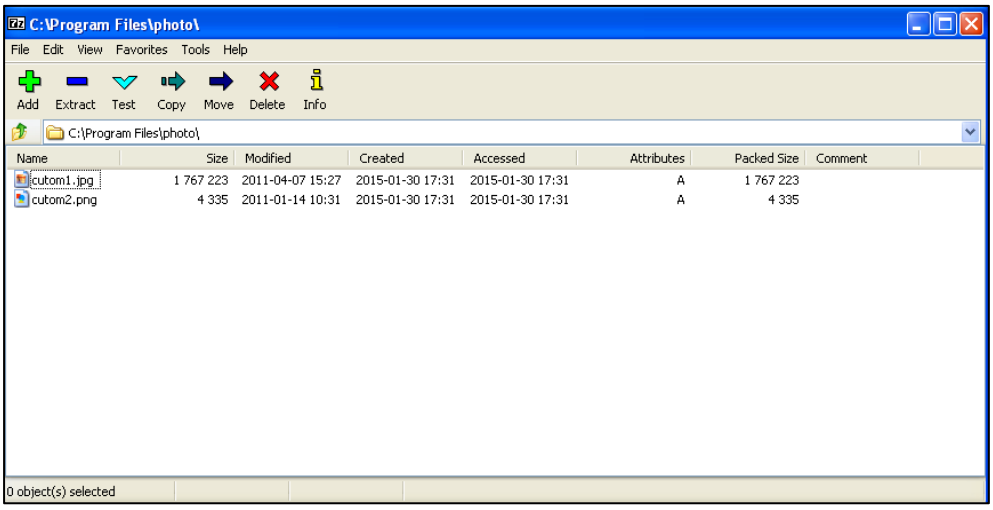
- Upload the pictures to the provisioning server one by one.
- Compress all the pictures to a tar formatted file and then upload the tar formatted file to the provisioning server.
- Compress the contact file and all the pictures to a tar formatted file and then upload the tar formatted file to the provision server.

Preparing the Tar Formatted File

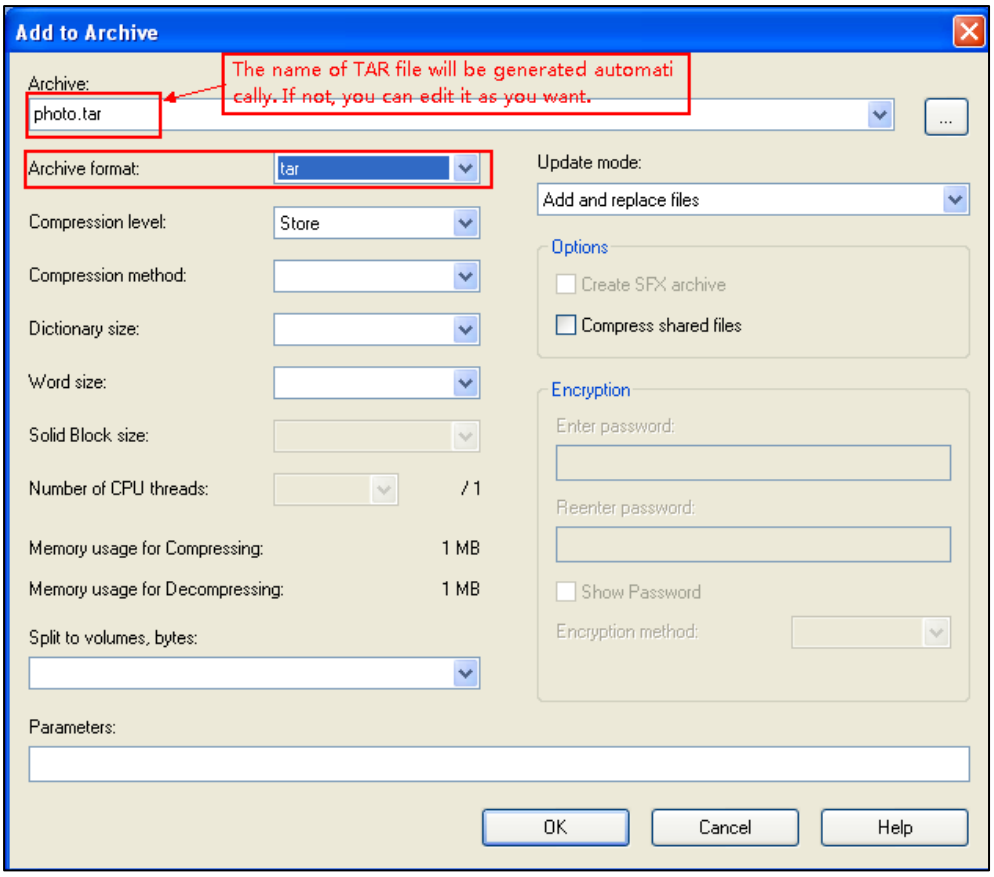
You can package the tar formatted file using the tool 7-Zip or GnuWin32. You can download 7-Zip online: http://www.7-zip.org/ and GnuWin32 online: http://gnuwin32.sourceforge.net/packages/gtar.htm. This section provides you on how to package the tar file using 7-Zip.

To package a tar formatted file using the tool 7-Zip on the Windows platform:

1. Download and install 7-Zip on the local system.
2. Create a folder (e.g., photo) on the local system (e.g., C:\Program Files) and place the file that will be compressed (e.g., cutom1.jpg, cutom2.png) to this folder.
3. Start the 7-Zip file manager application (7zFM.exe).
4. Locate the photo folder from the local system (C:\Program Files\photo\).



5. Select the desired photos that will be compressed.
6. Click the **Add** button.
7. Select **tar** from the pull-down list of **Archive format**.



8. Click the **OK** button.

   A photo.tar file is generated in the directory C:\Program Files\photo.

9. Place this file to the provisioning server (e.g., 192.168.10.25).

Customizing a Local Contact File

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="" line="" ring="" group_id_name="" default_photo=""/>

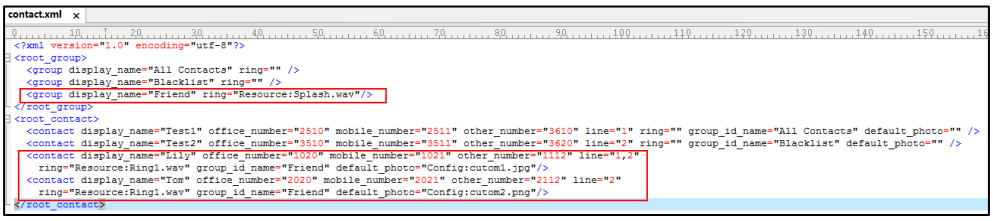
4. Specify the values within double quotes.

   For example:

<group display_name="Friend" ring="Resource: Splash.wav"/>

<contact display_name="Lily" office_number="1020" mobile_number="1021" other_number="1112" line="1,2" ring="Resource:Ring1.wav" group_id_name="Friend" default_photo="Config:custom1.jpg"/>

<contact display_name="Tom" office_number="2020" mobile_number="2021" other_number="2112" line="2" ring="Resource:Ring1.wav" group_id_name="Friend" default_photo="Config:custom2.png"/>



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.

   There are three methods to specify custom avatar and icon for contacts:

   Method 1:

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

   local_contact.photo.url = tftp://192.168.10.25/custom1.jpg

   local_contact.photo.url = tftp://192.168.10.25/custom2.png

   During the auto provisioning process, the IP phone connects to the provisioning server "192.168.10.25", and downloads the contact file "contact.xml" and avatar & icon pictures ("cutom1.jpg" and "cutom2.png").

   Method 2:

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

   local_contact.image.url = tftp://192.168.10.25/photo.tar

   For more information on generating a contact avatar & icon file "photo.tar", refer to Preparing the Tar Formatted File on page 271.

   During the auto provisioning process, the IP phone connects to the provisioning server "192.168.10.25", and downloads the contact file "contact.xml" and avatar & icon file "photo.tar".

   Method 3:

   If the local contact file (ContactData.xml) and custom avatars & icon (photo.tar) are compressed as a tar formatted file (e.g., Contact.tar), you can only configure the following parameter to upload contacts and avatars & icon:

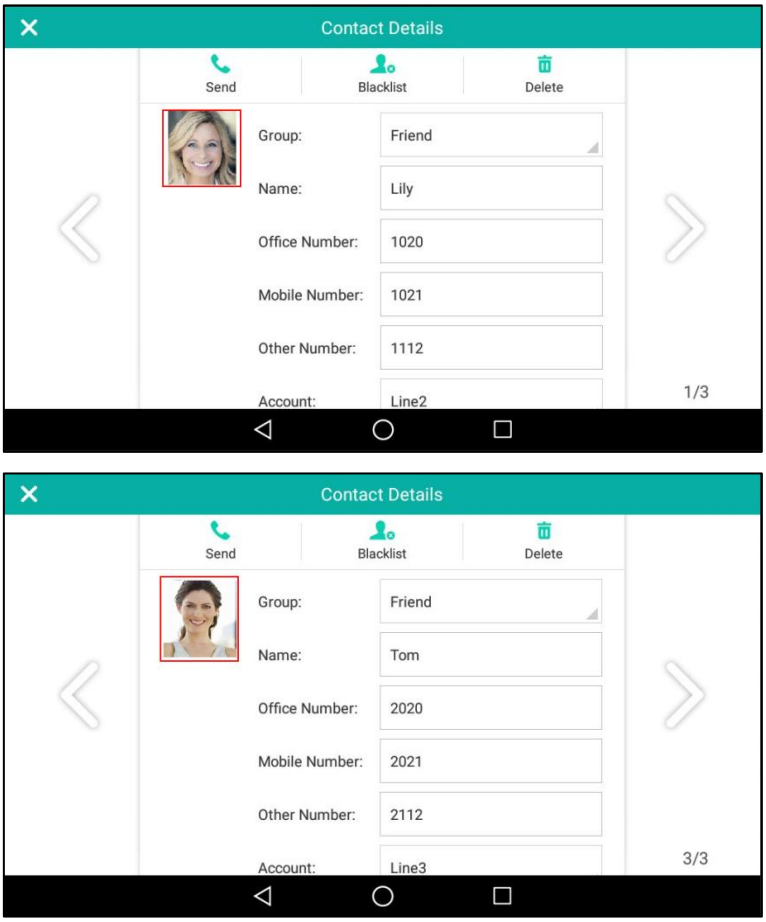
   local_contact.data_photo_tar.url = tftp://192.168.10.25/Contact.tar

   For more information on generating "photo.tar" and "Contact.tar", refer to Preparing the Tar Formatted File on page 271.

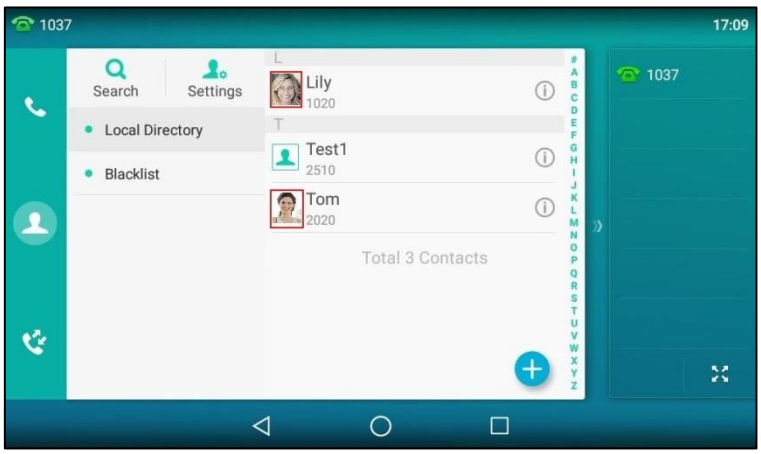
During the auto provisioning process, the IP phone connects to the provisioning server "192.168.10.25", and downloads the file "Contact.tar".

Note Note that if you are using method 3 to specify custom avatar & icon for contacts, the name of the avatars & icon TAR file must be photo.tar (case-sensitive), and the name of the contact XML file must be ContactData.xml (case-sensitive).

The following shows the custom avatars downloaded from the provisioning server:



The following shows the custom icons downloaded from the provisioning server:



Configuring Local Directory

Procedure

Local directory be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL of the local contact file. **Parameter:** local_contact.data.url
		Specify the access URL of a contact avatar & icon file. **Parameter:** local_contact.photo.url
		Specify the access URL of a TAR contact avatar & icon file. **Parameter:** local_contact.image.url
		Specify the access URL of the compressed TAR file consisting of the avatars & icon TAR file and contact XML file. **Parameter:** local_contact.data_photo_tar.url
Web User Interface		Add a new group and a contact to the local directory. To import or export the local contact file. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=contactsbasic&q=load&group=0&page=1
Phone User Interface		Add a new group and a contact to the local directory.

Details of the Configuration Parameters:

Parameters	Permitted Values	Default
local_contact.data.url	**URL within 511**	**Blank**

Parameters	Permitted Values	Default
	characters	
Description: Configures the access URL of the local contact file (*.xml). **Example:** local_contact.data.url = http://192.168.10.25/contact.xml **Web User Interface:** Directory->Local Directory->Import Local Directory File **Phone User Interface:** None		
local_contact.photo.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of a contact avatar & icon file. The format of the picture must be *.png, *.jpg, *.bmp, *.jpeg. The picture file should be uploaded to the provisioning server in advance. **Example**: local_contact.photo.url = tftp://192.168.10.25/Photo.jpg **Web User Interface:** None **Phone User Interface:** None		
local_contact.image.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of a TAR contact avatar & icon file. The format of the picture must be *.png, *.jpg, *.bmp, *.jpeg. The picture file should be compressed as a TAR file in advance and then place it to the provisioning server. **Example:** local_contact.image.url = tftp://192.168.10.25/photo.tar **Web User Interface:** None **Phone User Interface:** None		

Parameters	Permitted Values	Default
local_contact.data_photo_tar.url	**URL within 511 characters**	**Blank**

Description:

Configures the access URL of the compressed TAR file consisting of the avatars & icon TAR file and contact XML file.

All pictures needed for contacts should be compressed as a TAR file in advance.

Example:

local_contact.data_photo_tar.url = tftp://192.168.10.25/Contact.tar

Note: The name of the avatars & icon TAR file must be photo.tar (case-sensitive), and the name of the contact XML file must be ContactData.xml (case-sensitive).

Web User Interface:

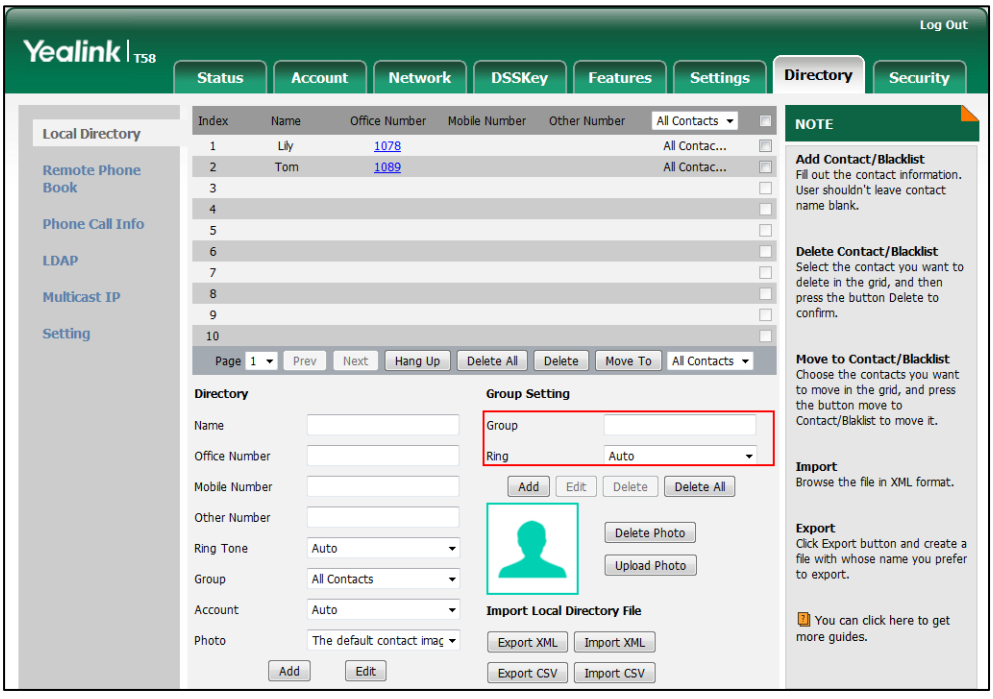
None

Phone User Interface:

None

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

1. Click on **Directory**->**Local Directory**.
2. In the **Group Setting** block, enter the desired group name in the **Group** field.
3. Select the desired ring tone from the pull-down list of **Ring**.

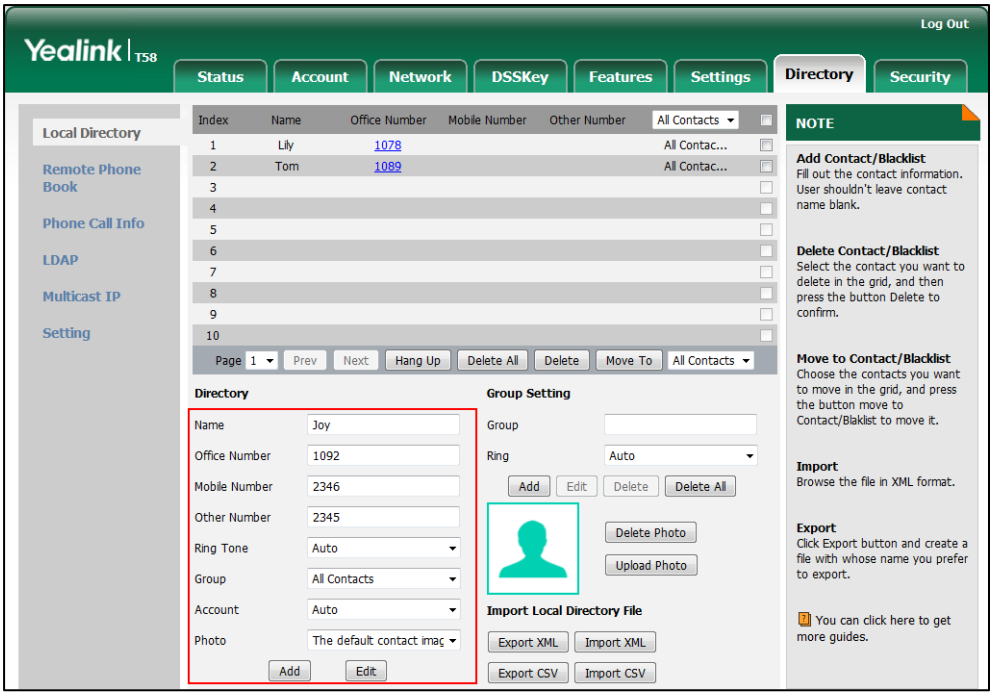


4. Click **Add** to add the group.

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

1. Click on **Directory**->**Local Directory**.
2. In the **Directory** block, enter the name and the office, mobile or other numbers in the corresponding fields.
3. Select the desired ring tone from the pull-down list of **Ring Tone**.
4. Select the desired group from the pull-down list of **Group**.
5. Select the desired account from the pull-down list of **Account**.

   If **Auto** is selected, the IP phone will use the default account when placing calls to the contact from the local directory.
6. Select the desired account from the pull-down list of **Photo**.



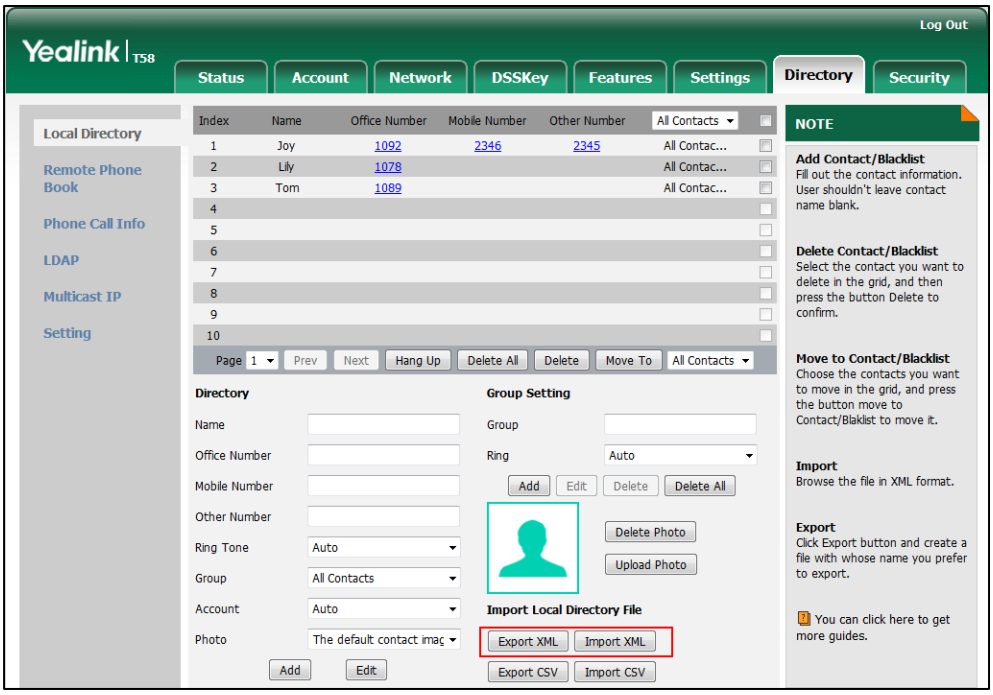
7. Click **Add** to add the contact.

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

1. Tap .
2. Tap **Settings**.
3. Tap **New Group**.
4. Enter the desired group name in the highlighted field.
5. Tap to accept the change.
6. Tap to specify a ring tone for the group.
7. Tap the desired ring tone in the pop-up dialog box.
8. Tap **OK** to accept the change.

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

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



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

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

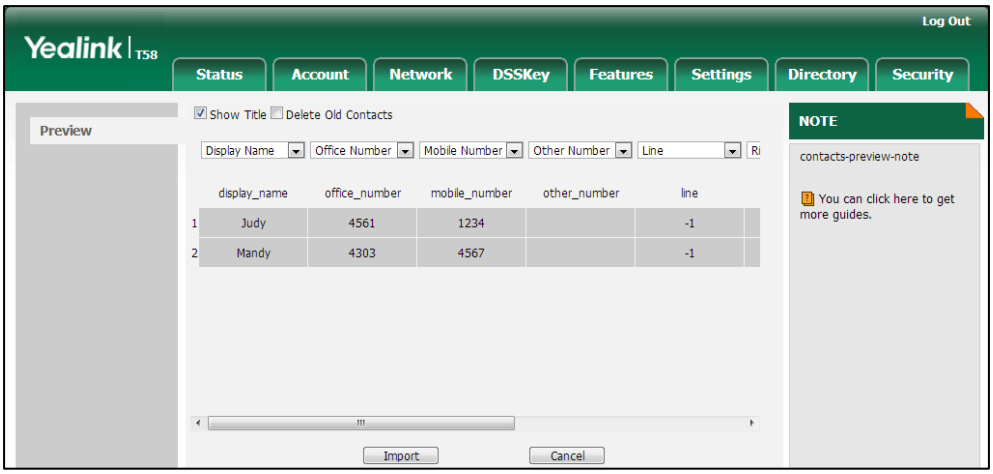
To import a CSV contact list file via web user interface:

1. Click on **Directory**->**Local Directory**.
2. Click **Import CSV** to locate and import a contact list file (the file format must be *.csv) from your local system.
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. (Optional.) Mark the **On** radio box in the **Delete Old Contacts** field.

   It will delete all existing contacts while importing the contact list.
5. Select the contact information you want to import into the local directory from the pull-down list.

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



6. 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. Tap .
2. Tap **Add**.
3. Tap .
4. Enter the name and the office, mobile or other numbers in the corresponding fields.
5. Tap the **Account** field.
6. Tap the desired account in the pop-up dialog box.

   If **Auto** is selected, the phone will use the default account when placing calls to the contact from the local directory.
7. Tap the **Ring** field.
8. Tap the desired ring tone in the pop-up dialog box.
9. Tap the **Photo** field.
10. Tap the desired photo in the pop-up dialog box.
11. Tap to accept the change.

Live Dialpad

Live dialpad allows IP phones to automatically dial out the entered phone number without pressing the send key after a designated period of time.

Procedure

Live dialpad can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure live dialpad. **Parameters:** phone_setting.predial_autodial phone_setting.inter_digit_time
Web User Interface		Configure live dialpad. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-preference&q=load

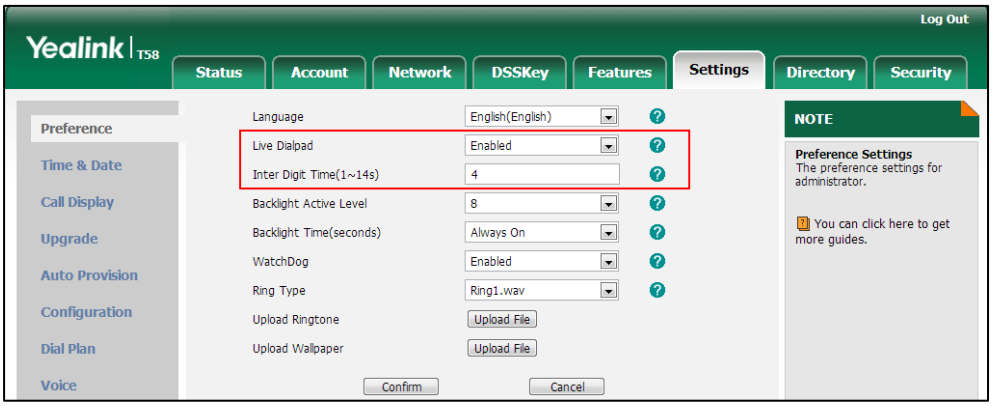
Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.predial_autodial	**0 or 1**	**0**
Description: Enables or disables the live dialpad feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will automatically dial out the entered phone number on the dialing screen without pressing a send key. **Web User Interface:** Settings->Preference->Live Dialpad **Phone User Interface:** None		
phone_setting.inter_digit_time	**Integer from 1 to 14**	**4**
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 "phone_setting.predial_autodial" is set to 1 (Enabled) and the value of the parameter "dialplan.digitmap.enable" is set to 0 (Disabled). **Web User Interface:** Settings->Preference->Inter Digit Time(1~14s) **Phone User Interface:**		

Parameters	Permitted Values	Default
None		

To configure live dialpad via web user interface:

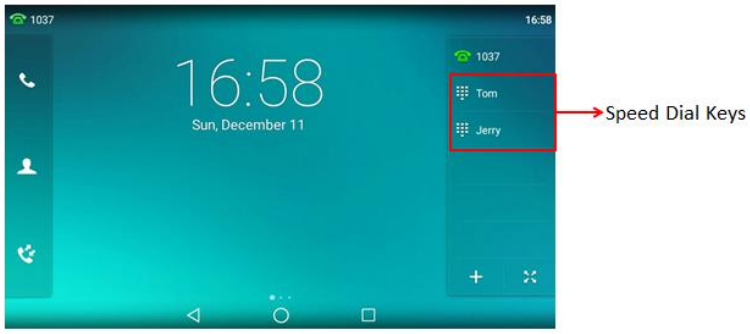
1. Click on **Settings**->**Preference**.
2. Select the desired value from the pull-down list of **Live Dialpad**.
3. Enter the desired delay time in the **Inter Digit Time(1~14s)** field.



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

Speed Dial

Speed dial allows users to speed up dialing the numbers frequently used or hard to remember using dedicated DSS keys.



Procedure

Speed dial key can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Assign a speed dial key. **Parameter:** linekey.X.type/ programablekey.X.type/

		expansion_module.X.key.Y.type linekey.X.line/ programablekey.X.line/ expansion_module.X.key.Y.line linekey.X.value/ programablekey.X.value/ expansion_module.X.key.Y.value linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Assign a speed dial key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface		Assign a speed dial key.

Speed Dial Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type	**13**	**Refer to the following content**
Description: Configures a DSS key as a speed dial key on the IP phone. The digit **13** stands for the key type **Speed Dial**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 13 **Default:**		

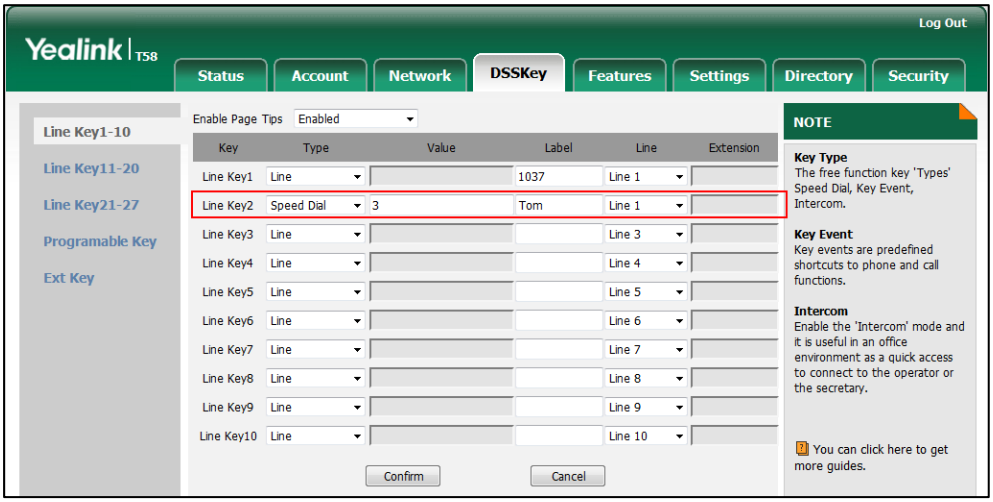
Parameters	Permitted Values	Default
For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For programable keys: **For SIP-T58V/T58A/T56A IP phones:** When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key/Programable Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.line/ programablekey.X.line/ expansion_module.X.key.Y.line	**Refer to the following content**	**1-16 for lines 1-16, 1 for programable keys**
Description: Configures the desired line to apply the speed dial key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Permitted Values:** 1 to 16 (for SIP-T58V/T58A/T56A) 1 (for CP960) 1-Line 1 2-Line 2		

Parameters	Permitted Values	Default
… 16-Line 16 **Example:** linekey.2.line = 1 **Web User Interface:** DSSKey->Line Key/Programable Key->Line **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Account ID		
linekey.X.value/ programablekey.X.value/ expansion_module.X.key.Y.value	**String within 99 characters**	**Blank**
Description: Configures the extension you want to dial out. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.value = 1008 **Web User Interface:** DSSKey->Line Key/Programable Key->Value **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Value		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)		

Parameters	Permitted Values	Default
Web User Interface: DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a speed dial key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **Speed Dial** from the pull-down list of **Type**.
3. Enter the phone number or extension you want to dial out in the **Value** field.
4. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
5. Select the desired line from the pull-down list of **Line**.



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

To configure a speed dial key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **Speed Dial** in the pop-up dialog box.
5. Tap the **Account ID** field.
6. Tap the desired line in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Enter the phone number or extension you want to dial out in the **Value** field.
9. Tap ✓ 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 touch 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 614.

The call waiting on code and call waiting off code configured on IP phones are used to activate/deactivate the server-side call waiting feature. They may vary on different servers.

Procedure

Call waiting and call waiting tone can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure call waiting and call waiting tone. **Parameters:** call_waiting.enable call_waiting.tone call_waiting.on_code call_waiting.off_code
Web User Interface		Configure call waiting. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
		Configure call waiting tone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-audio&q=load
Phone User Interface		Configure call waiting and call waiting tone.

Details of Configuration Parameters:

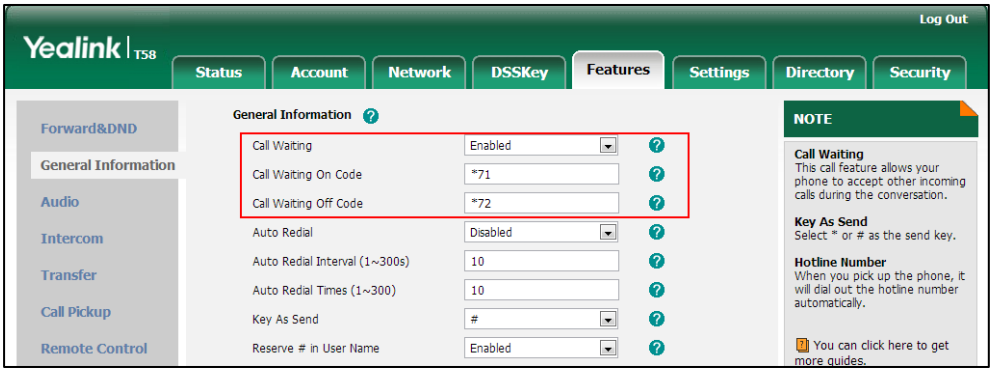
Parameters	Permitted Values	Default
call_waiting.enable	**0 or 1**	**1**

Parameters	Permitted Values	Default
Description: Enables or disables call waiting feature. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), a new incoming call is automatically rejected by the IP phone with a busy signal (configured by the parameter "features.normal_refuse_code") while during a call. If it is set to 1 (Enabled), the touch screen will present a new incoming call while during a call. In both cases, users can put an active call on hold to make outgoing calls. **Web User Interface:** Features->General Information->Call Waiting **Phone User Interface:** Settings->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 perform an audible indicator when receiving a new incoming call during a call. **Note**: It works only if the value of the parameter "call_waiting.enable" is set to 1 (Enabled). **Web User Interface:** Features->Audio->Call Waiting Tone **Phone User Interface:** Settings->Features->Call Waiting->Play Tone		
call_waiting.on_code	**String within 32 characters**	**Blank**
Description: Configures the call waiting on code to activate the server-side call waiting feature. The IP phone will send the call waiting on code to the server when you activate call waiting feature on the IP phone.		

Parameters	Permitted Values	Default
Example: call_waiting.on_code = *71 **Web User Interface:** Features->General Information->Call Waiting On Code **Phone User Interface:** Settings->Features->Call Waiting->On Code		
call_waiting.off_code	**String within 32 characters**	**Blank**
Description: Configures the call waiting off code to deactivate the server-side call waiting feature. The IP phone will send the call waiting off code to the server when you deactivate call waiting feature on the IP phone. **Example:** call_waiting.off_code = *72 **Web User Interface:** Features->General Information->Call Waiting Off Code **Phone User Interface:** Settings->Features->Call Waiting->Off Code		

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**.
3. (Optional.) Enter the call waiting on code in the **Call Waiting On Code** field.
4. (Optional.) Enter the call waiting off code in the **Call Waiting Off Code** field.

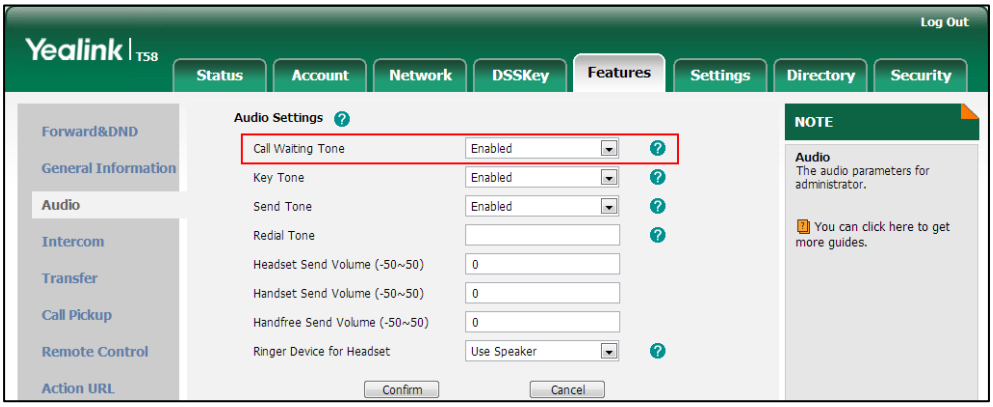


5. Click **Confirm** to accept the change.

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**.



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

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

1. Tap **Settings**->**Features**->**Call Waiting**.
2. Tap the **On** radio box in the **Call Waiting** field.
3. Tap the **On** radio box in the **Play Tone** field.
4. (Optional.) Enter the call waiting on code in the **On Code** field.
5. (Optional.) Enter the call waiting off code in the **Off Code** field.
6. Tap ✓ to accept the change.

Auto Redial

Auto redial allows IP phones to redial a busy number after the first attempt. Both the number of attempts and waiting time between redials are configurable.

Procedure

Auto redial can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure auto redial feature. **Parameters:** auto_redial.enable auto_redial.interval auto_redial.times
Web User Interface		Configure auto redial feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
Phone User Interface		Configure auto redial feature.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
auto_redial.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to automatically redial the dialed number when the callee is temporarily unavailable. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will dial the previous dialed out number automatically when the dialed number is temporarily unavailable. **Web User Interface:** Features->General Information->Auto Redial **Phone User Interface:** Settings->Features->Auto Redial->Auto Redial		
auto_redial.interval	**Integer from 1 to 300**	**10**
Description: Configures the interval (in seconds) for the IP phone to wait between redials. The IP phone redials the dialed number at regular intervals till the callee answers the call. **Note**: It works only if the value of the parameter "auto_redial.enable" is set to 1 (Enabled). **Web User Interface:** Features->General Information->Auto Redial Interval (1~300s) **Phone User Interface:** Settings->Features->Auto Redial->Redial Interval		
auto_redial.times	**Integer from 1 to 300**	**10**
Description: Configures the auto redial times when the callee is temporarily unavailable. The IP phone tries to redial the dialed number as many times as configured till the callee answers the call. **Note**: It works only if the value of the parameter "auto_redial.enable" is set to 1 (Enabled). **Web User Interface:** Features->General Information->Auto Redial Times (1~300) **Phone User Interface:**		

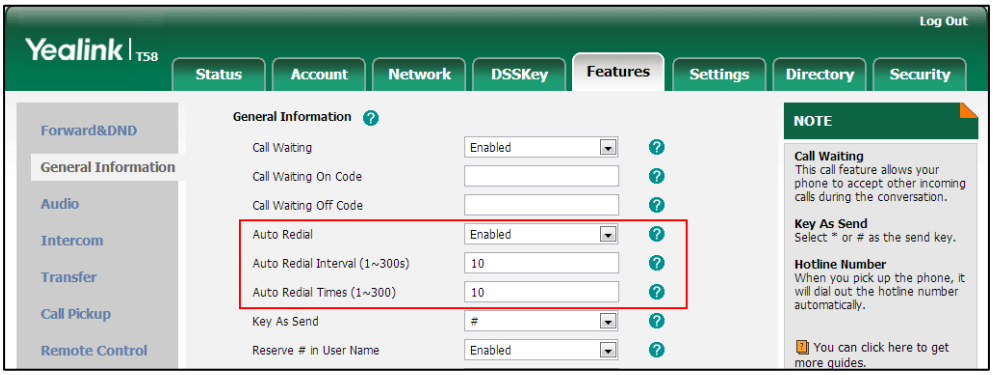
Parameters	Permitted Values	Default
Settings->Features->Auto Redial->Redial Times		

To configure auto redial via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Auto Redial**.
3. Enter the waiting time in the **Auto Redial Interval (1~300s)** field.

   The default value is 10.
4. Enter the desired times in the **Auto Redial Times (1~300)** field.

   The default value is 10.



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

To configure auto redial via phone user interface:

1. Tap **Settings**->**Features**->**Auto Redial**.
2. Tap the **On** radio box in the **Auto Redial** field.
3. Enter the waiting time (in seconds) in the **Redial Interval** field.
4. Enter the desired times in the **Redial Times** field.
5. Tap ✓ 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.

Auto Answer Tone

Auto answer tone allows the IP phone to play a tone when an incoming call is automatically answered. You can customize the auto answer tone or select specialized tone sets (vary from country to country) for your IP phone. For more information, refer to Tones on page 614.

Auto Answer Mute

Auto answer mute allows IP phones to mute the local microphone when an incoming call is automatically answered. It is only applicable to CP960 IP phones.

Note Auto answer is not applicable to automatically answer an IP address call. Automatically answering an IP address call works only if IP direct auto answer feature is enabled. For more information, refer to IP Direct Auto Answer on page 297.

Procedure

Auto answer can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure auto answer and auto answer mute. **Parameter:** account.X.auto_answer account.X.auto_answer_mute_enable
	<y0000000000xx>.cfg	Specify a period of delay time for auto answer. **Parameter:** features.auto_answer_delay
		Configure auto answer tone. **Parameter:** features.auto_answer_tone.enable
Web User Interface		Configure auto answer. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-basic&q=load&acc=0
		Specify a period of delay time for auto answer. Configure auto answer tone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
Phone User Interface		Configure auto answer.

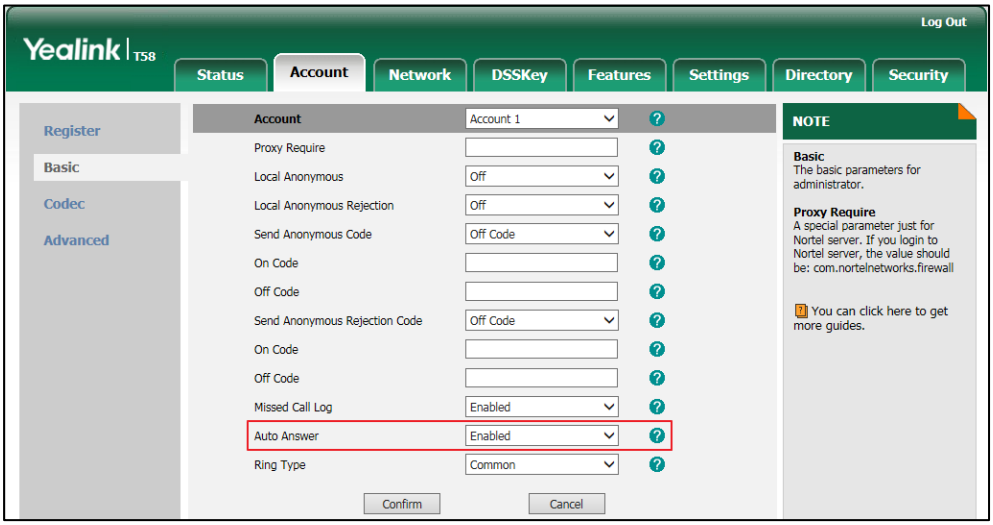
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.auto_answer	**0 or 1**	**0**
Description: Enables or disables auto answer feature for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone can automatically answer an incoming call. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: The IP phone cannot automatically answer the incoming call during a call even if auto answer is enabled. **Web User Interface:** Account->Basic->Auto Answer **Phone User Interface:** Settings->Features->Auto Answer->Account X		
features.auto_answer_delay	**Integer from 1 to 4**	**1**
Description: Configures the delay time (in seconds) before the IP phone automatically answers an incoming call. **Note**: It works only if the value of the parameter "account.X.auto_answer" is set to 1 (Enabled). **Web User Interface:** Features->General Information->Auto-Answer Delay(1~4s) **Phone User Interface:** None		
features.auto_answer_tone.enable	**0 or 1**	**1**
Description: Enables or disables the phone to play a warning tone when an incoming call is automatically answered. **0**-Disabled **1**-Enabled **Note**: For the call coming from a SIP account, it works only if the value of the parameter		

Parameters	Permitted Values	Default
"account.X.auto_answer" is set to 1 (Enabled). It is also applicable to IP calls. **Web User Interface:** Features->General Information->Enable auto answer tone **Phone User Interface:** None		
account.X.auto_answer_mute_enable (X is equal to 1)	**0 or 1**	**0**
Description: Enables or disables auto answer mute feature for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will mute the microphone when an incoming call is automatically answered, and then the other party cannot hear you. **Note:** It is only applicable to CP960 IP phones. It works only if the values of parameters "account.X.auto_answer" and "features.allow_mute" are set to 1 (Enabled). **Web User Interface:** Account->Basic->Auto Answer Mute **Phone User Interface:** Settings->Features->Auto Answer->Account 1-> Auto Answer (On) ->Auto Answer Mute		

To configure auto answer via web user interface:

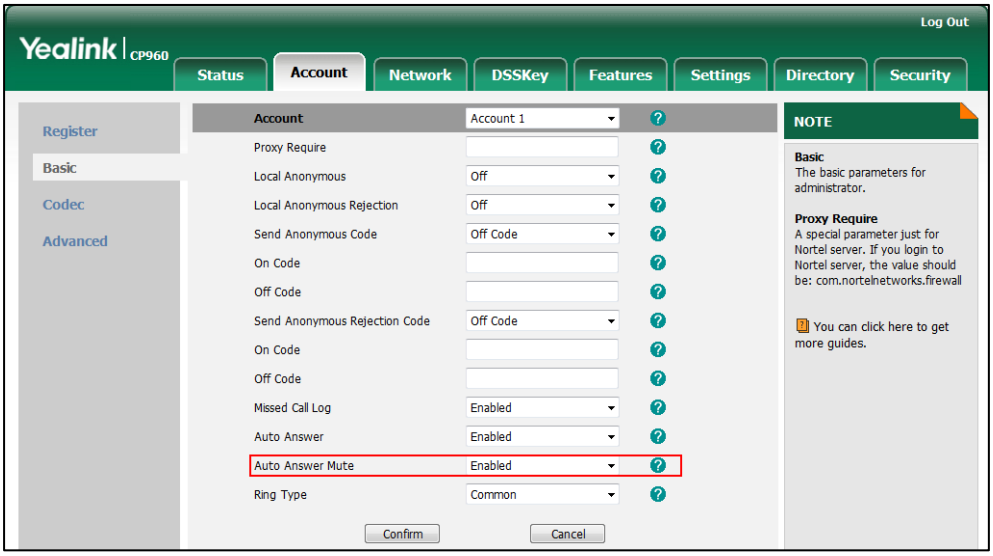
1. Click on **Account**->**Basic**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Auto Answer**.



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

To configure auto answer mute via web user interface (only applicable to CP960 IP phones):

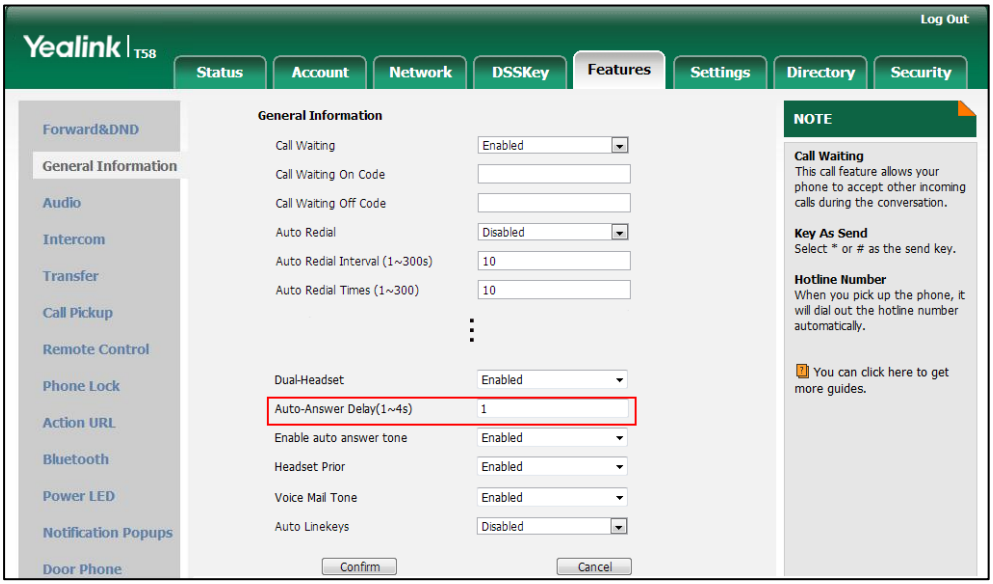
1. Click on **Account**->**Basic**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Auto Answer Mute**.



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

To configure a period of delay time for auto answer via web user interface:

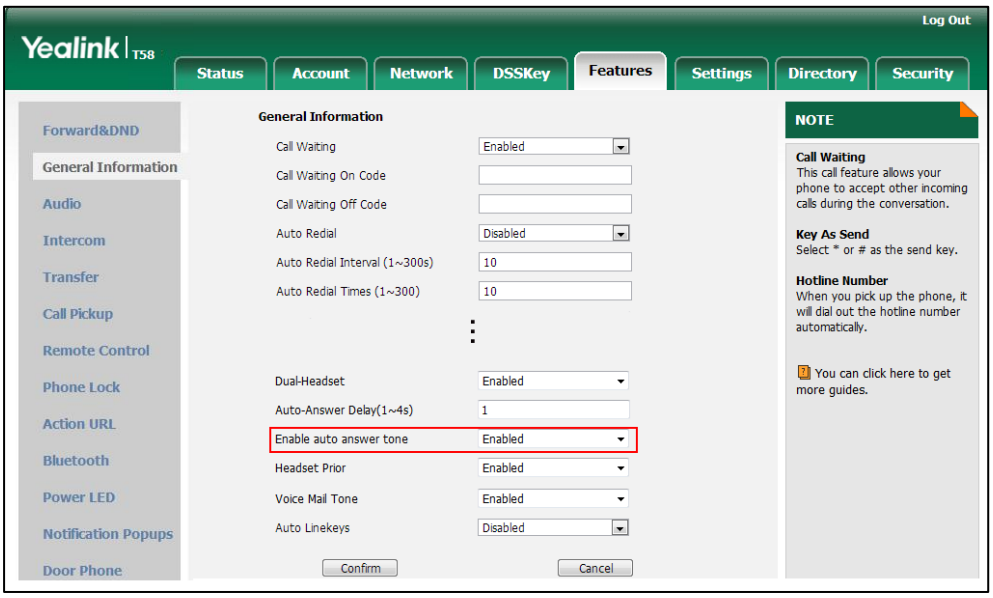
1. Click on **Features**->**General Information**.
2. Enter the desired time in the **Auto-Answer Delay(1~4s)** field.



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

To configure auto answer tone via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value in the pull-down list of **Enable auto answer tone**.



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

To configure auto answer via phone user interface:

1. Tap **Settings**->**Features**->**Auto Answer**.
2. Tap the **On** radio box for the desired account.
3. Tap ✓ to accept the change.

To configure auto answer mute via phone user interface (only applicable to CP960 IP phone):

1. Tap **Settings**->**Features**->**Auto Answer**->**Account1**.
2. Turn **Auto Answer** on.
3. Turn **Auto Answer Mute** on or off.

   This field appears only if **Auto Answer** is enabled.
4. Tap ✓ to accept the change.

IP Direct Auto Answer

IP direct auto answer allows IP phones to automatically answer an IP address call. IP direct auto answer works only if allow IP call is enabled. For more information on allow IP call, refer to Allow IP Call on page 299.

Procedure

IP direct auto answer can only be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure IP direct auto answer feature. **Parameter:** features.ip_call.auto_answer.enable
Web User Interface		Configure IP direct auto answer feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

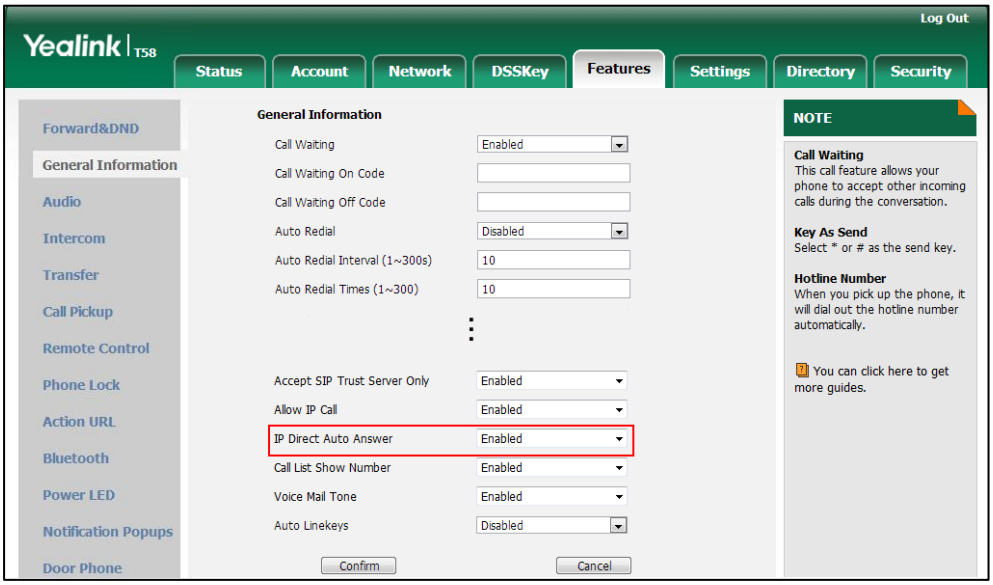
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.ip_call.auto_answer.enable	**0 or 1**	**0**
Description: Enables or disables the auto answer feature for IP call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone can automatically answer an IP call. **Note**: It works only if the value of the parameter "features.direct_ip_call_enable" is set to 1 (Enabled). The IP phone cannot automatically answer the incoming IP call during a call even if IP call auto answer is enabled. **Web User Interface:** Features->General Information->IP Direct Auto Answer **Phone User Interface:** None		

To configure IP direct auto answer via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **IP Direct Auto Answer**.



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

Allow IP Call

Allow IP Call feature allows IP phones to receive or place an IP address call. You can neither receive nor place an IP address call if allow IP call feature is disabled.

Procedure

Allow IP call can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure allow IP call. **Parameter:** features.direct_ip_call_enable
Web User Interface		Configure allow IP call. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

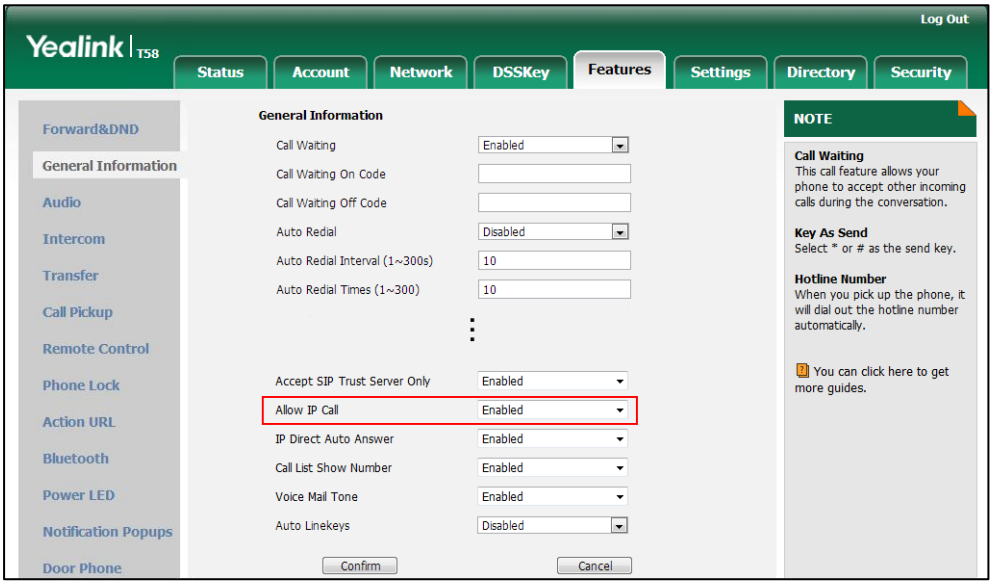
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.direct_ip_call_enable	**0 or 1**	**1**
Description:		

Parameter	Permitted Values	Default
Enables or disables allow IP address call. **0**-Disabled **1**-Enabled **Note**: If you want to receive an IP address call, make sure the value of the parameter "sip.trust_ctrl" is set to 0 (Disabled). **Web User Interface:** Features->General Information->Allow IP Call **Phone User Interface:** None		

To configure allow IP call feature via web user interface:

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



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

Accept SIP Trust Server Only

Accept SIP trust server only enables the IP phones to only accept the SIP message from your SIP server and outbound proxy server. It can prevent the phone receiving ghost calls from random numbers like 100, 1000, etc. To stop this from happening, you also need to disable allow IP call feature. For more information on allow IP call, refer to Allow IP Call on page 299.

Procedure

Accept SIP trust server only can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure accept SIP trust server only. **Parameter:** sip.trust_ctrl
Web User Interface		Configure accept SIP trust server only. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

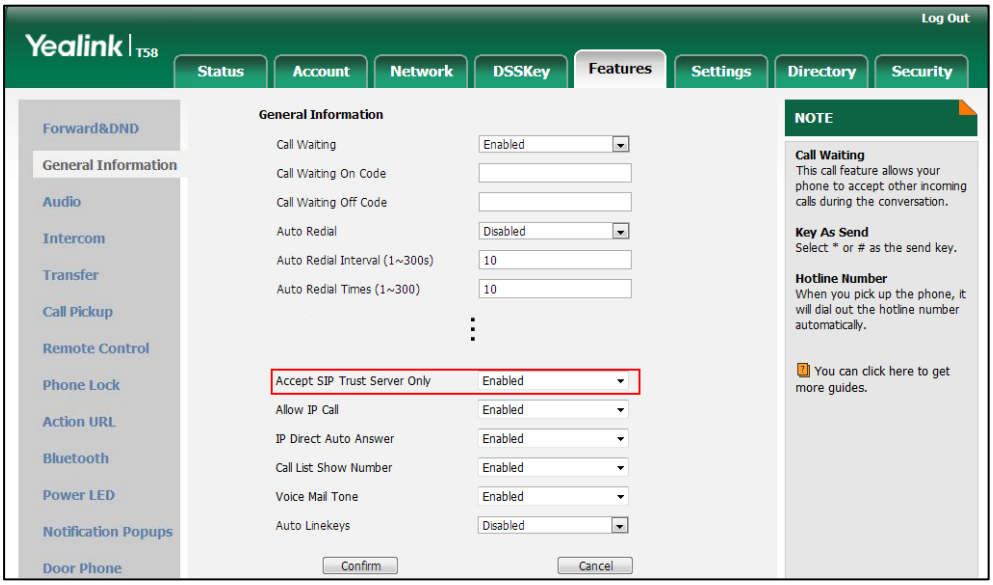
Details of Configuration Parameter:

Parameter	Permitted Values	Default
sip.trust_ctrl	**0 or 1**	**0**
Description: Enables or disables the IP phone to only accept the SIP message from the SIP server and outbound proxy server. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Accept SIP Trust Server Only **Phone User Interface:** None		

To configure accept SIP trust server only feature via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Accept SIP Trust Server Only**.



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

Call Completion

Call completion allows users to monitor the busy party and establish a call when the busy party becomes available to receive a call. Two factors commonly prevent a call from connecting successfully:

- Callee does not answer
- Callee actively rejects the incoming call before answering

IP phones support call completion using the SUBSCRIBE/NOTIFY method, which is specified in draft-poetzl-sipping-call-completion-00, to subscribe to the busy party and receive notifications of their status changes.

The caller subscribes for update notifications of the dialog event from the busy party. Example of a SUBSCRIBE message:

```
SUBSCRIBE sip:1000@10.10.20.34:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.20.32:5060;branch=z9hG4bK2880274891
From: "10111" <sip:10111@10.2.1.48:5060>;tag=8643512
To: <sip:1000@10.2.1.48:5060>;tag=4025601441
Call-ID: 4_2103527761@10.10.20.32
CSeq: 2 SUBSCRIBE
Contact: <sip:10111@10.2.1.48:5060>
Accept: application/dialog-info+xml
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Expires: 60
Event: dialog
```

```
Content-Length: 0
```

Example of a NOTIFY message (The subscription (SUBSCRIBE message) of the dialog event "Call Completion" is confirmed by the busy party):

```
NOTIFY sip:10111@10.10.20.32:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.20.31:5060;branch=z9hG4bK1830418099
From: <sip:1000@10.2.1.48:5060>;tag=1032948194
To: "10111" <sip:10111@10.2.1.48:5060>;tag=722495580
Call-ID: 0_160090766@10.10.20.32
CSeq: 2 NOTIFY
Contact: <sip:1000@10.10.20.31:5060>
Content-Type: application/dialog-info+xml
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Subscription-State: active;expires=60
Event: dialog
Content-Length:     584

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="1" state="full"
entity="sip:1000@10.2.1.48:5060">
<dialog id="65626" call-id="0_3138198645@10.10.20.31" local-tag="2331766736" remote-tag="1786911541"
direction="initiator">
<state>confirmed</state>
<local>
<identity>sip:1000@10.2.1.48:5060</identity>
<target uri="sip:1000@10.2.1.48:5060"/>
</local>
<remote>
<identity>sip:1@10.2.1.48:5060</identity>
<target uri="sip:1@10.2.1.48:5060"/>
</remote>
</dialog>
<dialog id="65622">
<state>terminated</state>
</dialog>
</dialog-info>
```

Example of a NOTIFY message (The busy party has finished the call and is available again. A new notification update from the busy party is received by the caller):

```
NOTIFY sip:10111@10.10.20.32:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.20.31:5060;branch=z9hG4bK3431394016
From: <sip:1000@10.2.1.48:5060>;tag=1558968605
To: "10111" <sip:10111@10.2.1.48:5060>;tag=140677866
```

```
Call-ID: 0_2584152566@10.10.20.32
CSeq: 5 NOTIFY
Contact: <sip:1000@10.10.20.31:5060>
Content-Type: application/dialog-info+xml
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Subscription-State: active;expires=48
Event: dialog
Content-Length:    217

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4" state="partial"
entity="sip:1000@10.2.1.48:5060">
<dialog id="65644">
<state>terminated</state>
</dialog>
</dialog-info>
```

Procedure

Call completion can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure call completion. **Parameter:** features.call_completion_enable
Web User Interface		Configure call completion. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
Phone User Interface		Configure call completion.

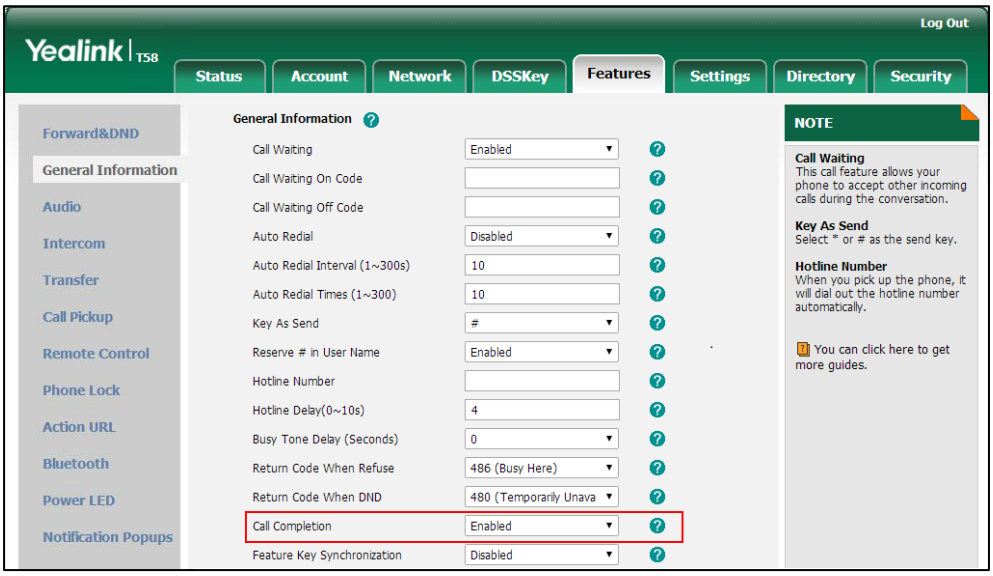
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.call_completion_enable	**0 or 1**	**0**
Description: Enables or disables call completion feature. If a user places a call and the callee is temporarily unavailable to answer the call, call completion feature allows notifying the user when the callee becomes available to receive a call.		

Parameter	Permitted Values	Default
0-Disabled **1**-Enabled If it is set to 1 (Enabled), the caller is notified when the callee becomes available to receive a call. **Web User Interface:** Features->General Information->Call Completion **Phone User Interface:** Settings->Features->Call Completion->Call Completion		

To configure call completion via web user interface:

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



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

To configure call completion via phone user interface:

1. Tap **Settings**->**Features**->**Call Completion**.
2. Tap the **On** radio box in the **Call Completion** field.
3. Tap ✓ to accept the change.

Anonymous Call

Anonymous call allows the caller to conceal the identity information displayed on the callee's screen. The callee's phone touch screen prompts an incoming call from anonymity. Anonymous call is configurable on a per-line basis.

Example of anonymous SIP header:

```
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK3074920774
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=131654239
To: <sip:1006@10.2.1.48:5060>
Call-ID: 0_288363101@10.3.20.14
CSeq: 1 INVITE
Contact: <sip:1009@10.3.20.14:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Allow-Events: talk,hold,conference,refer,check-sync
P-Preferred-Identity: <sip:1009@10.2.1.48>
Privacy: id
Content-Length: 302
```

The anonymous call on code and anonymous call off code configured on IP phones are used to activate/deactivate the server-side anonymous call feature. They may vary on different servers. Send Anonymous Code feature allows IP phones to send anonymous on/off code to the server.

Procedure

Anonymous call can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure anonymous call. **Parameters:** account.X.anonymous_call account.X.send_anonymous_code account.X.anonymous_call_oncode account.X.anonymous_call_offcode
Web User Interface		Configure anonymous call. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-basic&q=load&acc=0
Phone User Interface		Configure anonymous call.

Details of Configuration Parameters:

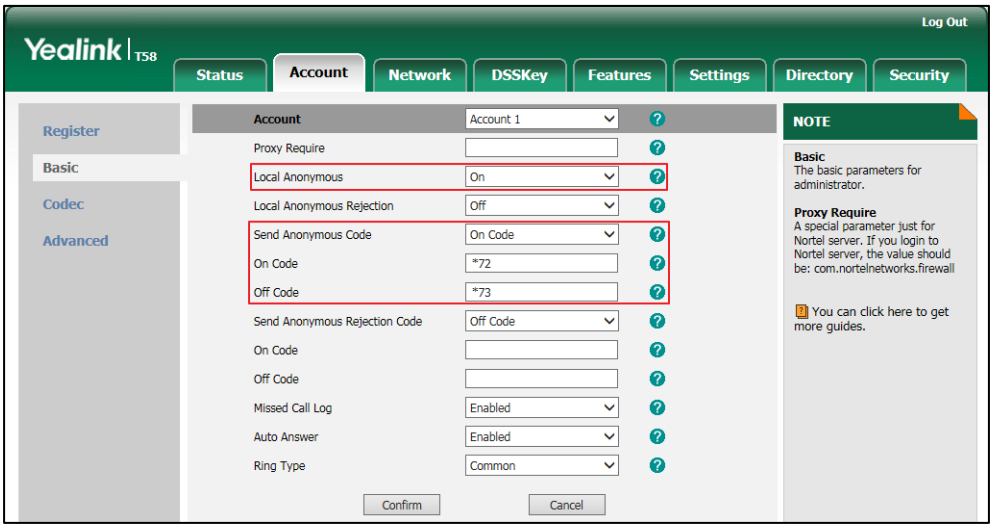
Parameters	Permitted Values	Default
account.X.anonymous_call	**0 or 1**	**0**
Description: Triggers the anonymous call feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), the IP phone will block its identity from showing up to the callee when placing a call. The callee's phone touch screen presents anonymous instead of the caller's identity. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Basic->Local Anonymous **Phone User Interface:** Settings->Features->Anonymous->Line X->Local Anonymous		
account.X.send_anonymous_code	**0 or 1**	**0**
Description: Configures the IP phone to send anonymous on/off code to activate/deactivate the server-side anonymous call feature for account X. **0**-Off Code **1**-On Code If it is set to 0 (Off Code), the IP phone will send anonymous off code to the server when you deactivate the anonymous call feature. If it is set to 1 (On Code), the IP phone will send anonymous on code to the server when you activate the anonymous call feature. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Basic->Send Anonymous Code **Phone User Interface:** Settings->Features->Anonymous->Line X->Send Anony Code		
account.X.anonymous_call_oncode	**String within 32 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the anonymous call on code to activate the server-side anonymous call feature for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.anonymous_call_oncode = *72 **Note:** It works only if the value of the parameter "account.X.send_anonymous_code" is set to 1 (On Code). **Web User Interface:** Account->Basic->Send Anonymous Code->On Code **Phone User Interface:** Settings->Features->Anonymous->Line X->On Code		
account.X.anonymous_call_offcode	**String within 32 characters**	**Blank**
Description: Configures the anonymous call off code to deactivate the server-side anonymous call feature for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.anonymous_call_offcode = *73 **Note:** It works only if the value of the parameter "account.X.send_anonymous_code" is set to 0 (Off Code). **Web User Interface:** Account->Basic->Send Anonymous Code->Off Code **Phone User Interface:** Settings->Features->Anonymous->Line X->Off Code		

To configure anonymous call via web user interface:

1. Click on **Account**->**Basic**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Local Anonymous**.
4. Select the desired value from the pull-down list of **Send Anonymous Code**.
5. (Optional.) Enter the anonymous call on code in the **On Code** field.

6. (Optional.) Enter the anonymous call off code in the **Off Code** field.



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

To configure the anonymous call via phone user interface:

1. Tap **Settings**->**Features**->**Anonymous**.
2. Tap the desired line.
3. Tap the **On** radio box in the **Local Anonymous** field.
4. (Optional.) Tap the **On** or **Off** radio box in the **Send Anony Code** field.
5. (Optional.) Enter the anonymous call on code and off code respectively in the **On Code** and **Off Code** field beneath the **Send Anony Code** field.
6. Tap ✓ to accept the change.

Anonymous Call Rejection

Anonymous call rejection allows IP phones to automatically reject incoming calls from callers whose identity has been deliberately concealed. The anonymous caller's phone touch screen presents "Anonymity Disallowed". Anonymous call rejection is configurable on a per-line basis.

Example of anonymous call rejection SIP header:

SIP/2.0 **433 Anonymity Disallowed**

Via: SIP/2.0/UDP 10.10.20.32:5060;branch=z9hG4bK2816884590

From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=2625078618

To: <sip:1058@10.2.1.48:5060>;tag=2781829106

Call-ID: 4_510565349@10.10.20.32

CSeq: 1 INVITE

Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH, UPDATE, MESSAGE

User-Agent: Yealink T58 58.80.0.5

Allow-Events: talk, hold, conference, refer, check-sync

```
Content-Length: 0
```

The anonymous call rejection on code and anonymous call rejection off code configured on IP phones are used to activate/deactivate the server-side anonymous call rejection feature. They may vary on different servers. Send Anonymous Rejection Code feature allows IP phones to send anonymous call rejection on/off code to the server.

Procedure

Anonymous call rejection can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure anonymous call rejection. **Parameters:** account.X.reject_anonymous_call account.X.send_anonymous_rejection_code account.X.anonymous_reject_oncode account.X.anonymous_reject_offcode
Web User Interface		Configure anonymous call rejection. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-basic&q=load&acc=0
Phone User Interface		Configure anonymous call rejection.

Details of Configuration Parameters:

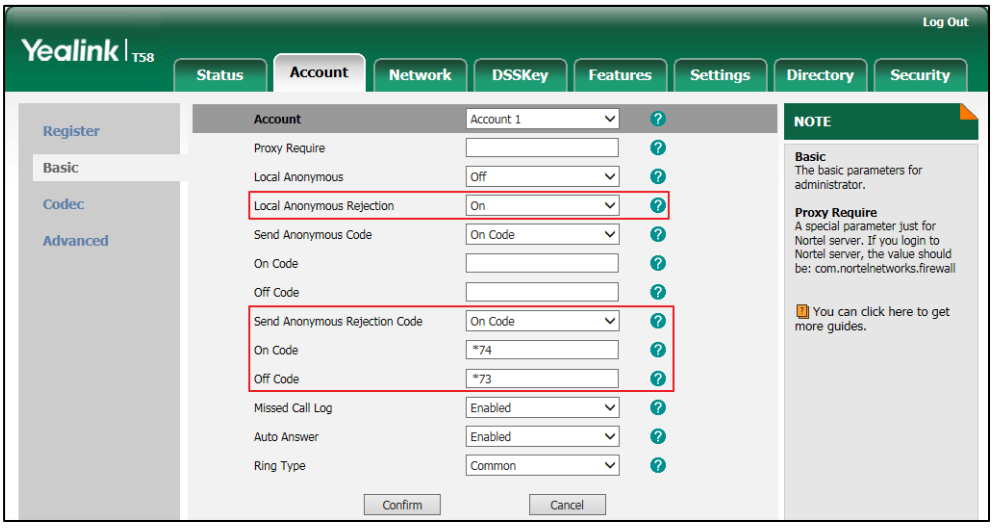
Parameters	Permitted Values	Default
account.X.reject_anonymous_call	**0 or 1**	**0**
Description: Triggers the anonymous call rejection feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), the IP phone will automatically reject incoming calls from users enabled anonymous call feature. The anonymous user's phone touch screen presents "Anonymity Disallowed". X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Basic->Local Anonymous Rejection **Phone User Interface:** Settings->Features->Anonymous->Line X->Anonymous Rejection		

Parameters	Permitted Values	Default
account.X.send_anonymous_rejection_code	**0 or 1**	**0**
Description: Configures the IP phone to send anonymous rejection on/off code to activate/deactivate the server-side anonymous call rejection feature for account X. **0**- Off code **1**- On code If it is set to 0 (Off Code), the IP phone will send anonymous rejection off code to the server when you deactivate the anonymous call rejection feature. If it is set to 1 (On Code), the IP phone will send anonymous rejection on code to the server when you activate the anonymous call rejection feature. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Basic->Send Anonymous Rejection Code **Phone User Interface:** Settings->Features->Anonymous->Line X->Send Rejection Code		
account.X.anonymous_reject_oncode	**String within 32 characters**	**Blank**
Description: Configures the anonymous call rejection on code to activate the server-side anonymous call rejection feature for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.anonymous_reject_oncode = *74 **Note:** It works only if the value of the parameter "account.X.send_anonymous_rejection_code" is set to 1 (On Code). **Web User Interface:** Account->Basic->Send Anonymous Rejection Code->On Code **Phone User Interface:** Settings->Features->Anonymous->Line X->On Code		
account.X.anonymous_reject_offcode	**String within 32 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the anonymous call rejection off code to deactivate the server-side anonymous call rejection feature for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.anonymous_reject_offcode = *75 **Note:** It works only if the value of the parameter "account.X.send_anonymous_rejection_code" is set to 0 (Off Code). **Web User Interface:** Account->Basic->Send Anonymous Rejection Code->Off Code **Phone User Interface:** Settings->Features->Anonymous->Line X->Off Code		

To configure anonymous call rejection via web user interface:

1. Click on **Account**->**Basic**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Local Anonymous Rejection**.
4. Select the desired value from the pull-down list of **Send Anonymous Rejection Code**.
5. (Optional.) Enter the Send Anonymous Rejection on code in the **On Code** field.
6. (Optional.) Enter the Send Anonymous Rejection off code in the **Off Code** field.



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

To configure anonymous call rejection via phone user interface:

1. Tap **Settings**->**Features**->**Anonymous Call**.
2. Tap the desired line.
3. Tap the **On** radio box in the **Anonymous Rejection** field.
4. (Optional.) Tap the **On** or **Off** radio box in the **Send Rejection Code** field.
5. (Optional.) Enter the anonymous call rejection on code and off code respectively in the **On Code** and **Off Code** field beneath the **Send Rejection Code** field.
6. Tap ✔ to accept the change.

Do Not Disturb (DND)

DND allows IP phones to ignore incoming calls. Incoming calls received while DND is enabled are logged in the Missed Calls list. DND feature can be configured on a phone or a per-line basis depending on the DND mode. Two DND modes:

- **Phone** (default): DND feature is effective for the IP phone.
- **Custom**: DND feature can be configured for each or all accounts.

DND can be enabled locally through the phone or through a server. A user can activate or deactivate DND using the DND key on the phone. The server-side DND feature disables the local DND and call forward settings. If the server-side DND feature is enabled on any of the IP phone's registrations, the other registrations are not affected. For more information on call forward, refer to Call Forward on page 343.

The DND on code and DND off code configured on IP phones are used to activate/deactivate the server-side DND feature. They may vary on different servers.

Return Message When DND

This feature defines the return code and the reason of the SIP response message for the rejected incoming call when DND is enabled on the IP phone. The caller's phone touch screen displays the received return code.

DND Emergency

This feature allows users to receive the incoming calls from some authorized numbers even if the DND feature is enabled. This feature is disabled by default.

Procedure

DND can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure DND in the custom mode. **Parameters:** account.X.dnd.enable account.X.dnd.on_code account.X.dnd.off_code
	<y0000000000xx>.cfg	Configure the DND mode. **Parameter:** features.dnd_mode
		Configure DND in the phone mode. **Parameters:** features.dnd.enable features.dnd.on_code features.dnd.off_code
		Specify the authorized numbers when DND is enabled. **Parameters:** features.dnd.emergency_enable features.dnd.emergency_authorized_number
		Specify the return code and the reason of the SIP response message when DND is enabled. **Parameter:** features.dnd_refuse_code
		Assign a DND key. **Parameters:** linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Configure DND. Specify the authorized numbers when DND is enabled. **Navigate to**:

	http://<phoneIPAddress>/servlet?m=mod_data&p=features-forward&q=load
	Specify the return code and the reason of the SIP response message when DND is enabled. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
	Assign a DND key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface	Configure DND. Assign a DND key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dnd_mode	**0 or 1**	**0**
Description: Configures the DND mode for the IP phone. **0**-Phone **1**-Custom If it is set to 0 (Phone), DND feature is effective for the IP phone. If it is set to 1 (Custom), you can configure DND feature for each or all accounts. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Forward&DND->DND->Mode **Phone User Interface:** None		
account.X.dnd.enable (X ranges from 1 to 16)	**0 or 1**	**0**
Description: Triggers DND feature to on or off for account X.		

Parameters	Permitted Values	Default
0-Off **1**-On If it is set to 1 (On), the IP phone will reject incoming calls with a busy signal (configured by the parameter "features.dnd_refuse_code") on account X. **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.dnd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->DND->DND Status **Phone User Interface:** Settings->Features->DND->AccountX->Status		
account.X.dnd.on_code (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the DND on code to activate the server-side DND feature for account X. The IP phone will send the DND on code to the server when you activate DND feature for account X on the IP phone. **Example:** account.1.dnd.on_code = *73 **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.dnd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->DND On Code **Phone User Interface:** Settings->Features->DND->AccountX->On Code		
account.X.dnd.off_code (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the DND off code to deactivate the server-side DND feature for account X. The IP phone will send the DND off code to the server when you deactivate DND feature for account X on the IP phone. **Example:** account.1.dnd.off_code = *74 **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.dnd_mode" is set to 1 (Custom). **Web User Interface:**		

Parameters	Permitted Values	Default
Features->Forward&DND->DND Off Code **Phone User Interface:** Settings->Features->DND->AccountX->Off Code		
features.dnd.enable	**0 or 1**	**0**
Description: Triggers DND feature to on or off for the IP phone. **0**-Off **1**-On If it is set to 1 (On), the IP phone will reject incoming calls with a busy signal (configured by the parameter "features.dnd_refuse_code") on the IP phone. **Note:** It works only if the value of the parameter "features.dnd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->DND->DND Status **Phone User Interface:** Settings->Features->DND->Status		
features.dnd.on_code	**String within 32 characters**	**Blank**
Description: Configures the DND on code to activate the server-side DND feature. The IP phone will send the DND on code to the server when you activate DND feature on the IP phone. **Example:** features.dnd.on_code = *71 **Note:** It works only if the value of the parameter "features.dnd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->DND->DND On Code **Phone User Interface:** Settings->Features->DND->On Code		
features.dnd.off_code	**String within 32 characters**	**Blank**
Description: Configures the DND off code to deactivate the server-side DND feature. The IP phone will send the DND off code to the server when you deactivate DND feature on the IP phone. **Example:**		

Parameters	Permitted Values	Default
features.dnd.off_code = *72 **Note:** It works only if the value of the parameter "features.dnd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->DND->DND Off Code **Phone User Interface:** Settings->Features->DND->Off Code		
features.dnd.emergency_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to receive incoming calls from authorized numbers when DND feature is enabled. **0**-Disabled **1**-Enabled **Note**: The authorized numbers are configured by the parameter "features.dnd.emergency_authorized_number". **Web User Interface:** Features->Forward&DND->DND->DND Emergency **Phone User Interface:** None		
features.dnd.emergency_authorized_number	**String within 511 characters**	**Blank**
Description: Configures the authorized numbers the IP phone can receive incoming calls from even if DND feature is enabled. Multiple numbers are separated by commas. **Example:** features.dnd.emergency_authorized_number = 123,124 **Note:** It works only if the value of the parameter "features.dnd.emergency_enable" is set to 1 (Enabled). **Web User Interface:** Features->Forward&DND->DND->DND Authorized Numbers **Phone User Interface:** None		
features.dnd_refuse_code	**404, 480, 486 or 603**	**480**

Parameters	Permitted Values	Default
Description: Configures a return code and reason of SIP response messages when rejecting an incoming call by DND. A specific reason is displayed on the caller's phone touch screen. **404**-Not Found **480**-Temporarily Unavailable **486**-Busy Here **603**-Decline If it is set to 486 (Busy Here), the caller's phone touch screen will display the reason "Busy Here" when the callee enables DND. **Web User Interface:** Features->General Information->Return Code When DND **Phone User Interface:** None		

DND Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

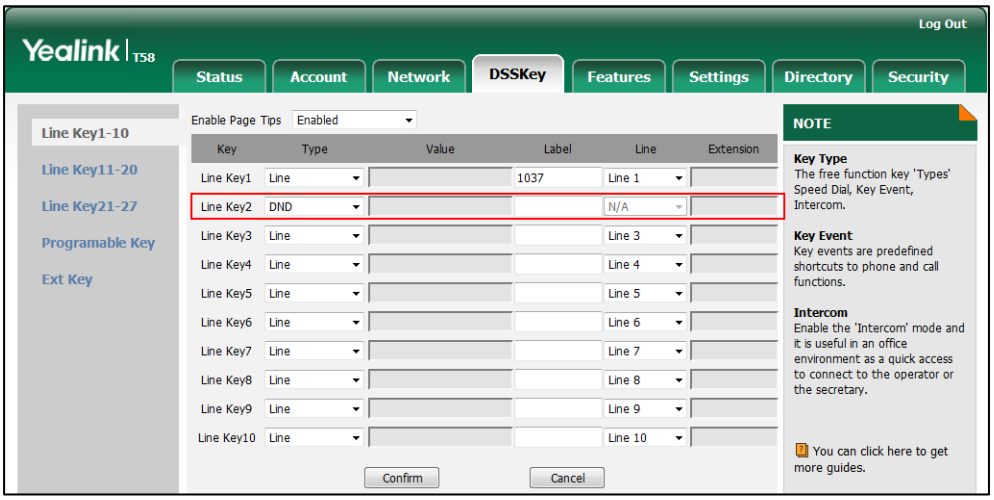
Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type	**5**	**Refer to the following content**
Description: Configures a DSS key as a DND key on the IP phone. The digit **5** stands for the key type **DND**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 5		

Parameters	Permitted Values	Default
Default: For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For programable keys: **For SIP-T58V/T58A/T56A IP phones:** When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key/Programable Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a DND key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **DND** from the pull-down list of **Type**.
3. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.

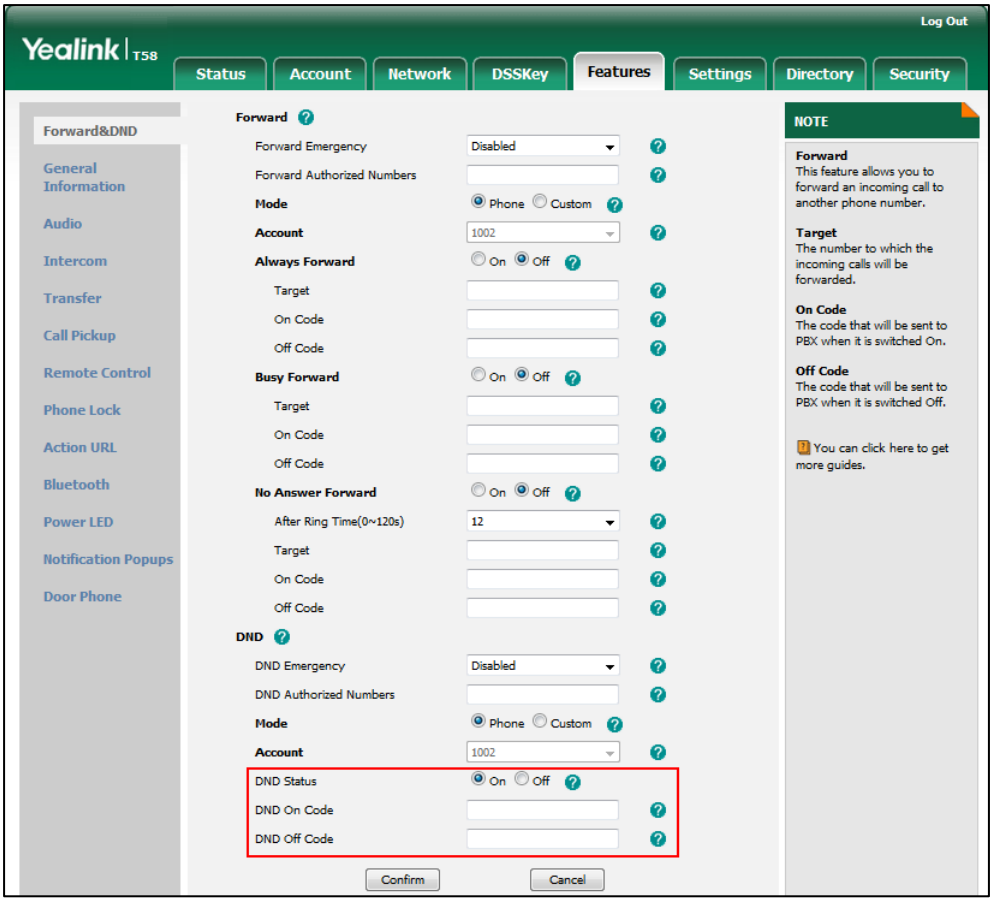


4. Click **Confirm** to accept the change.

To configure DND feature via web user interface:

1. Click on **Features**->**Forward&DND**.
2. In the **DND** block, mark the desired radio box in the **Mode** field.
   a) If you mark the **Phone** radio box:
      1) Mark the desired radio box in the **DND Status** field.
      2) (Optional.) Enter the DND on code in the **DND On Code** field.

3) (Optional.) Enter the DND off code in the **DND Off Code** field.



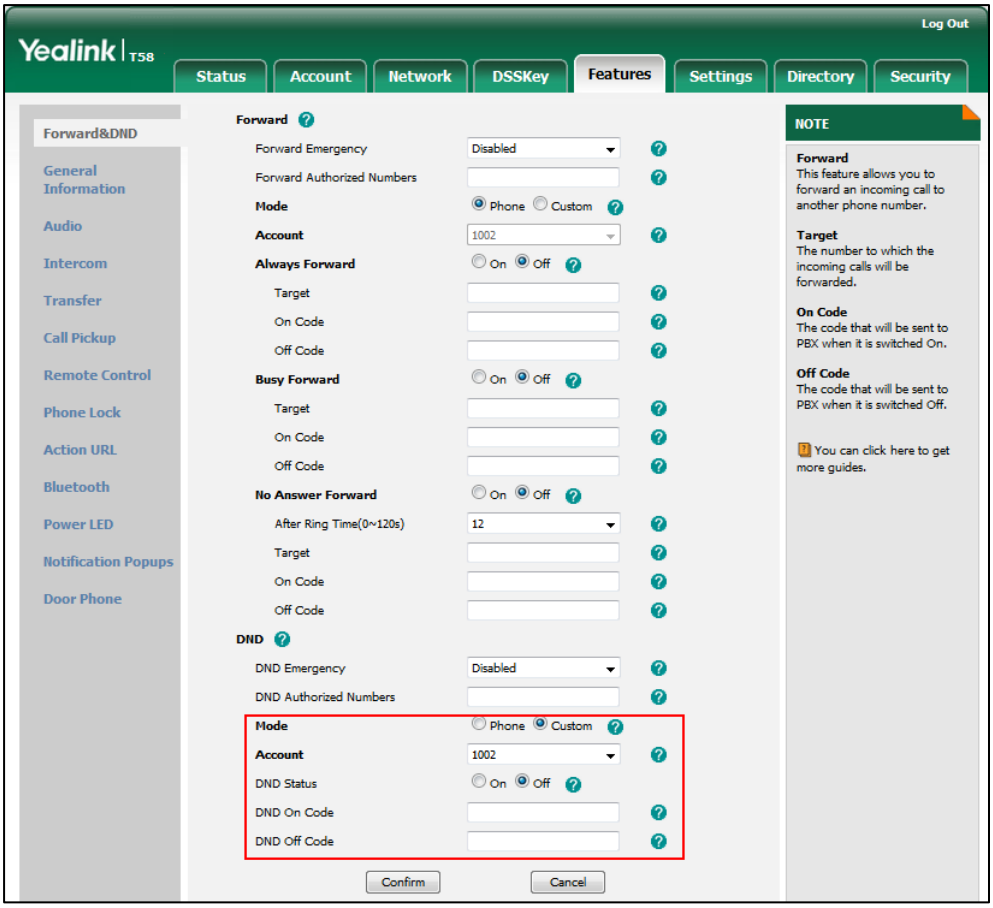
b) If you mark the **Custom** radio box:

1) Select the desired account from the pull-down list of **Account**.

2) Mark the desired radio box in the **DND Status** field.

3) (Optional.) Enter the DND on code in the **DND On Code** field.

4) (Optional.) Enter the DND off code in the **DND Off Code** field.



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

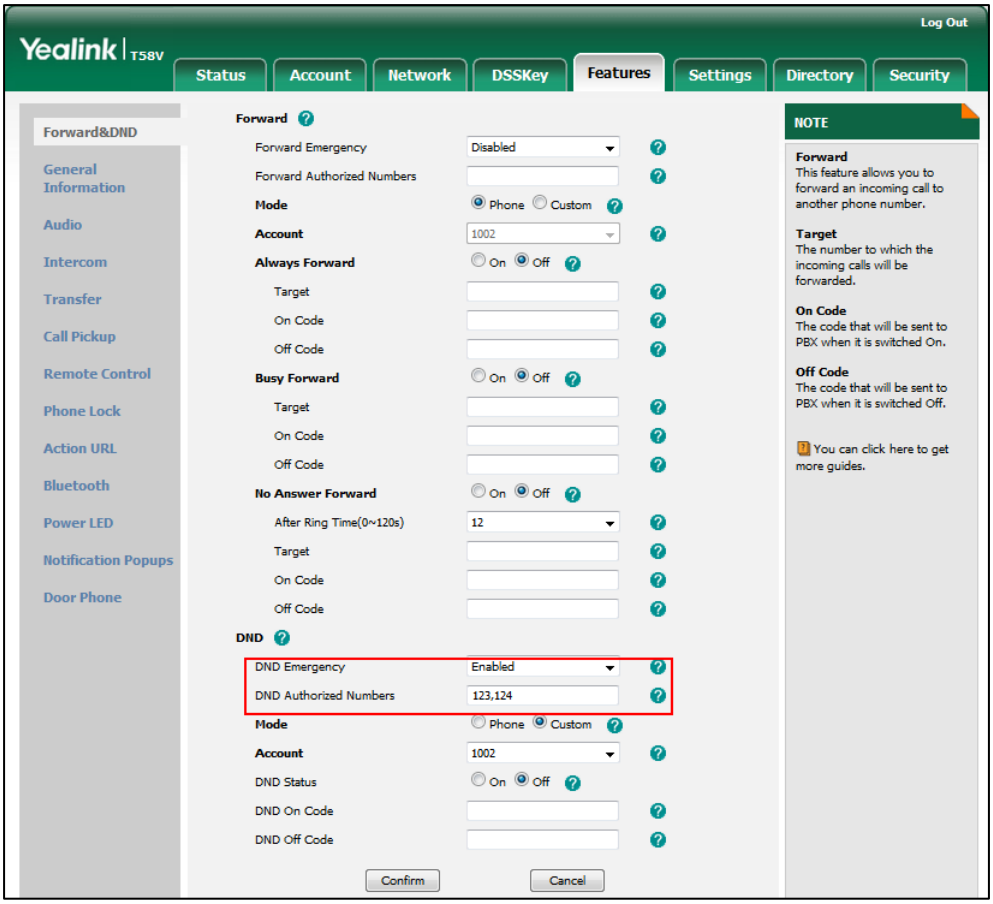
To specify the authorized numbers when DND is enabled via web user interface:

1. Click on **Features**->**General Information**.

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

3. Enter the desired value in the **DND Authorized Numbers** field.

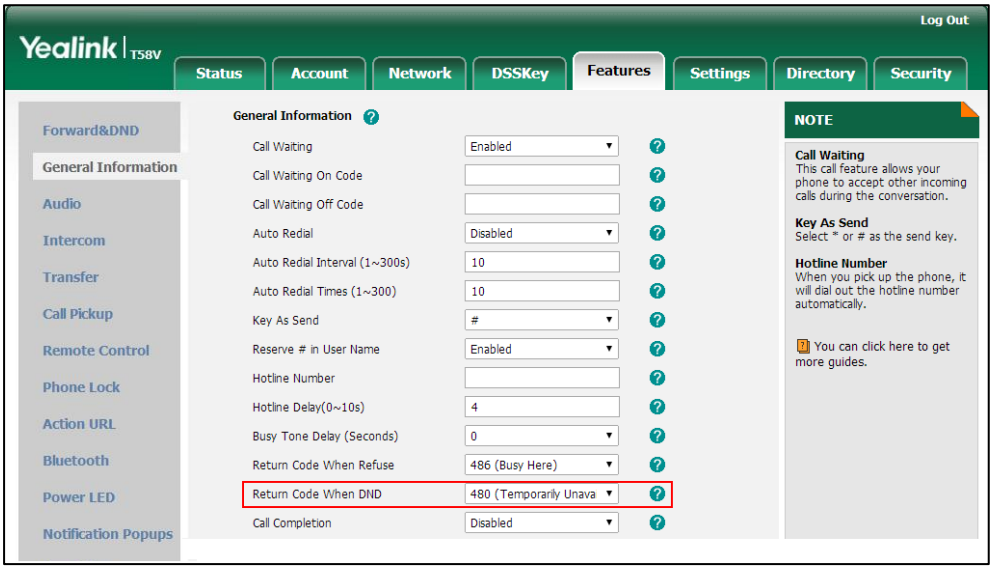
Multiple numbers are separated by commas.



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

To specify the return code and the reason when DND is enabled via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Return Code When DND**.



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

To configure a DND key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **DND** in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Tap ✓ to accept the change.

To configure DND in the phone mode via phone user interface:

1. Tap the DND key when the IP phone is idle.

To configure DND in the custom mode for a specific account via phone user interface:

1. Tap the DND key when the IP phone is idle.

   The touch screen displays a list of accounts registered on the IP phone.
2. Tap the desired account.
3. Tap the **On** radio box in the **Status** field.

   You can configure DND in the custom mode for all accounts by tapping ⋮ ->**All On**.
4. Tap ✓ 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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure busy tone delay. **Parameter:** features.busy_tone_delay
Web User Interface		Configure busy tone delay. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&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 to the other party indicating that the call connection breaks.

0-0s

3-3s

5-5s

If it is set to 3 (3s), a busy tone is audible for 3 seconds on the IP phone.

Web User Interface:

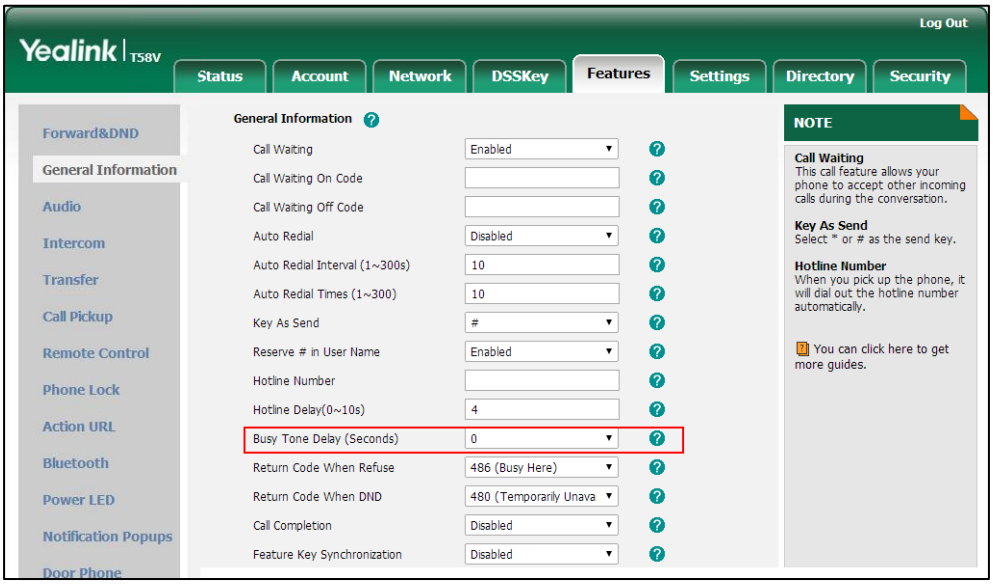
Features->General Information->Busy Tone Delay (Seconds)

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)**.

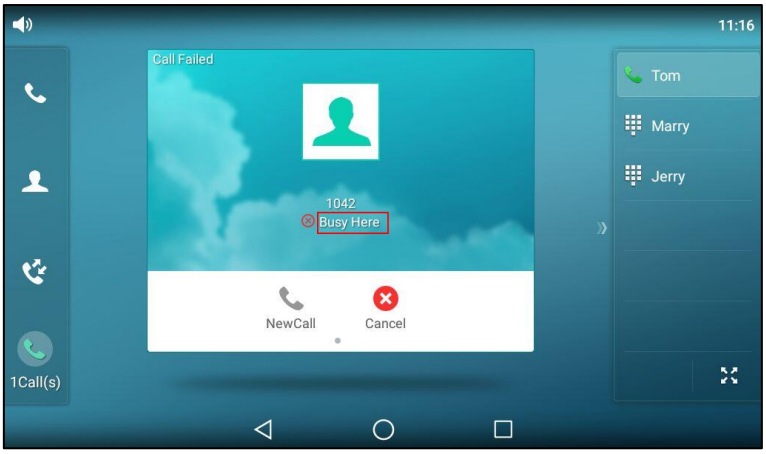


3. Click **Confirm** to accept the change.

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 touch screen displays the reason according to the received return code. Available return codes and reasons are:

- 404 (Not Found)
- 480 (Temporarily Unavailable)
- 486 (Busy Here)
- 603 (Decline)



Procedure

Return code for refused call can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the return code and the reason of the SIP response message when refusing a call. **Parameter:** features.normal_refuse_code
Web User Interface		Specify the return code and the reason of the SIP response message when refusing a call. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.normal_refuse_code	**404, 480, 486 or 603**	**486**

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 touch screen.

404-Not Found

480-Temporarily Unavailable

486-Busy Here

603-Decline

If it is set to 486 (Busy Here), the caller's phone touch screen will display the message "Busy Here" when the callee rejects the incoming call.

Web User Interface:

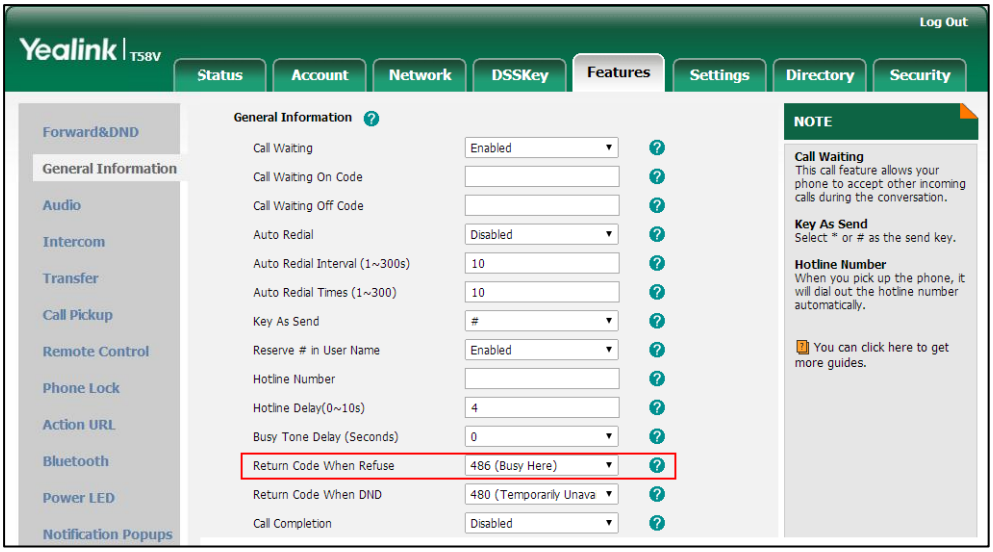
Features->General Information->Return Code When Refuse

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**.



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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure 180 ring workaround. **Parameter:** phone_setting.is_deal180
Web User Interface		Configure 180 ring workaround. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

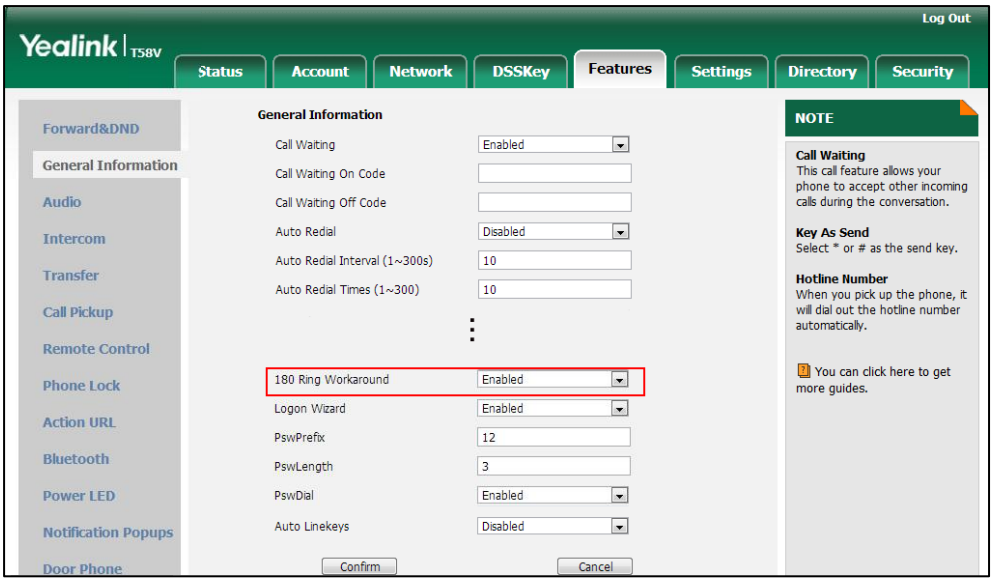
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.is_deal180	**0 or 1**	**1**
Description: Enables or disables the IP phone to deal with the 180 SIP message received after the 183 SIP message. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will resume and play the local ringback tone upon a subsequent 180 message received. **Web User Interface:** Features->General Information->180 Ring Workaround		

Parameter	Permitted Values	Default
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**.



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

Use Outbound Proxy in Dialog

An outbound proxy server can receive all initiating request messages and route them to the designated destination. If the IP phone is configured to use an outbound proxy server within a dialog, all SIP request messages from the IP phone will be sent to the outbound proxy server forcibly.

Note To use this feature, make sure the outbound server has been correctly configured on the IP phone. For more information on how to configure outbound server, refer to Account Registration on page 172.

Procedure

Use outbound proxy in dialog can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify whether to use outbound proxy in a dialog. **Parameter:**

		sip.use_out_bound_in_dialog
Web User Interface		Specify whether to use outbound proxy in a dialog. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

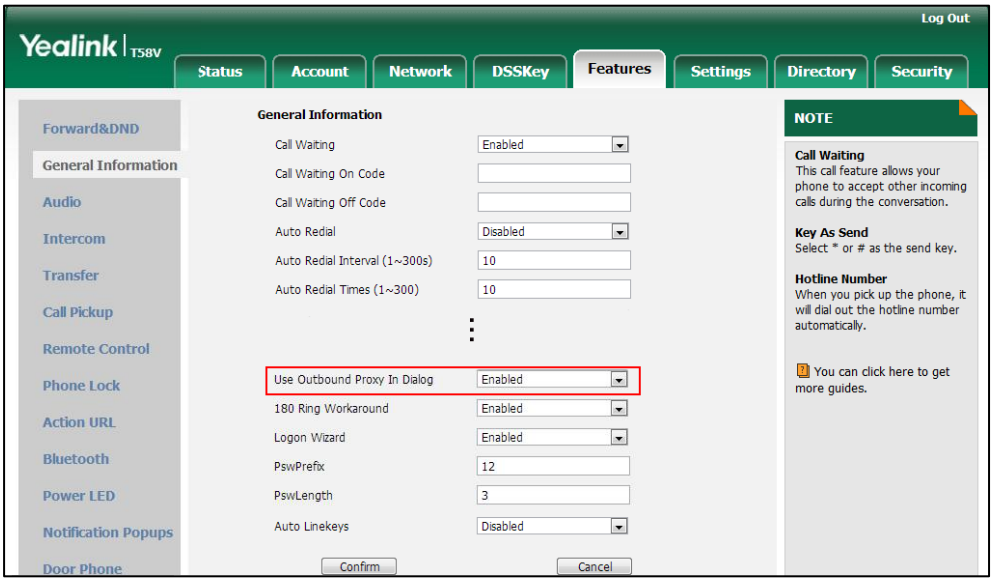
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.use_out_bound_in_dialog	**0 or 1**	**1**
Description: Enables or disables the IP phone to send all SIP requests to the outbound proxy server forcibly in a dialog. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), only the new SIP request messages from the IP phone will be sent to the outbound proxy server in a dialog. If it is set to 1 (Enabled), all the SIP request messages from the IP phone will be forced to send to the outbound proxy server in a dialog. **Note**: It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled) and the outbound server address has been correctly configured on the phone. **Web User Interface:** Features->General Information->Use Outbound Proxy In Dialog **Phone User Interface:** None		

To configure use outbound proxy in dialog via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Use Outbound Proxy In Dialog**.



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

SIP Session Timer

SIP session timers T1, T2 and T4 are SIP transaction layer timers defined in RFC 3261. These session timers are configurable on IP phones.

Timer T1

Timer T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server.

Timer T2

Timer T2 represents the maximum retransmitting time of any SIP request message. The re-transmitting and doubling of T1 will continue until the retransmitting time reaches the T2 value.

Example:

The user registers a SIP account for the IP phone and then set the value of Timer T1, Timer T2 respectively (Timer T1: 0.5, Timer T2: 4). The SIP registration request message will be re-transmitted between the IP phone and SIP server. The re-transmitting and doubling of Timer T1 (0.5) will continue until the retransmitting time reaches the Timer T2 (4). The total registration request retry time will be less than 64 times of T1 (64 * 0.5 = 32). The re-transmitting interval in sequence is: 0.5s, 1s, 2s, 4s, 4s, 4s, 4s, 4s, 4s and 4s.

Timer T4

Timer T4 represents the time the network will take to clear messages between the SIP client and server.

Procedure

SIP session timer can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure SIP session timer. **Parameters:** sip.timer_t1 sip.timer_t2 sip.timer_t4
Web User Interface		Configure SIP session timer. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-sip&q=load

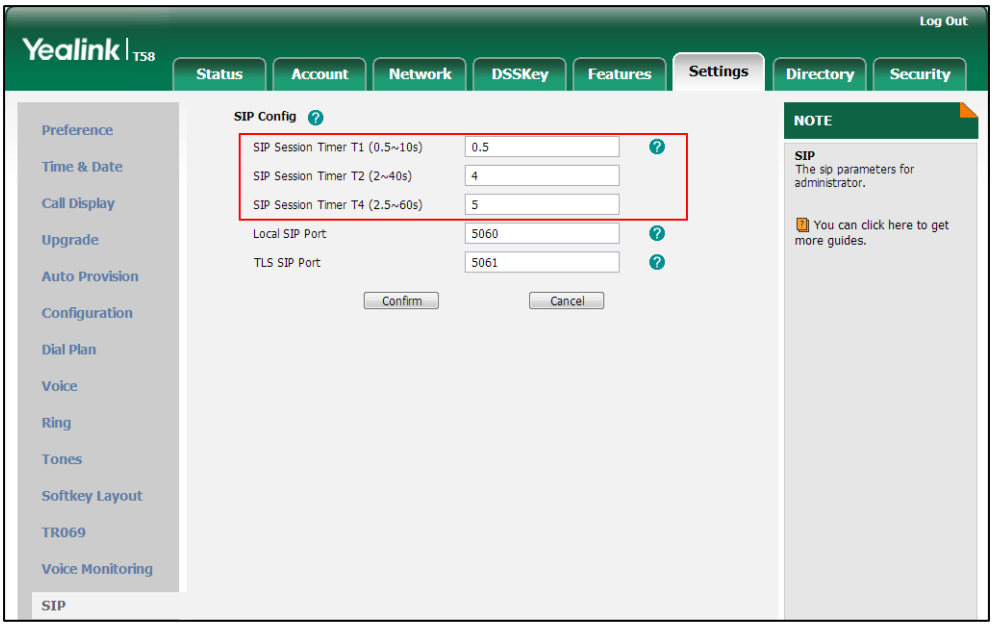
Details of Configuration Parameters:

Parameters	Permitted Values	Default
sip.timer_t1	**Float from 0.5 to10**	**0.5**
Description: Configures the SIP session timer T1 (in seconds). T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server. **Web User Interface:** Settings->SIP->SIP Session Timer T1 (0.5~10s) **Phone User Interface:** None		
sip.timer_t2	**Float from 2 to 40**	**4**
Description: Configures the SIP session timer T2 (in seconds). Timer T2 represents the maximum retransmitting time of any SIP request message. **Web User Interface:** Settings->SIP->SIP Session Timer T2 (2~40s) **Phone User Interface:** None		
sip.timer_t4	**Float from 2.5 to**	**5**

Parameters	Permitted Values	Default
	60	
Description: Configures the SIP session timer of T4 (in seconds). T4 represents the maximum duration a message will remain in the network. **Web User Interface:** Settings->SIP->SIP Session Timer T4 (2.5~60s) **Phone User Interface:** None		

To configure session timer via web user interface:

1. Click on **Settings**->**SIP**.
2. Enter the desired value in the **SIP Session Timer T1 (0.5~10s)** field.
3. Enter the desired value in the **SIP Session Timer T2 (2~40s)** field.
4. Enter the desired value in the **SIP Session Timer T4 (2.5~60s)** field.



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

Session Timer

Session timer allows a periodic refresh of SIP sessions through an UPDATE request, to determine whether a SIP session is still active. Session timer is specified in RFC 4028. IP phones support two refresher modes: UAC and UAS. Whether the endpoint functions as a UAC or a UAS depends on the UA that initiates the SIP request. If the initiator is configured as UAC, the other client or the SIP server will function as a UAS. If the initiator is configured as UAS, the other client or the SIP

server will function as a UAC. The session expiration is negotiated via the Session-Expires header in the INVITE message. The negotiated refresher is always the UAC and it will send an UPDATE request at the negotiated session expiration. The value "refresher=uac" included in the UPDATE message means that the UAC performs the refresh.

Example of UPDATE message (UAC mode):

```
UPDATE sip:1058@10.10.20.34:5060 SIP/2.0
Via: SIP/2.0/UDP 10.10.20.32:5060;branch=z9hG4bK2104991394
From: "10111" <sip:10111@10.2.1.48:5060>;tag=2170397024
To: <sip:1058@10.2.1.48:5060>;tag=200382096
Call-ID: 4_1556494084@10.10.20.32
CSeq: 2 UPDATE
Contact: <sip:10111@10.10.20.32:5060>
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Session-Expires: 90;refresher=uac
Supported: timer
Content-Length: 0
```

Procedure

Session timer can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure session timer. **Parameters:** account.X.session_timer.enable account.X.session_timer.expires account.X.session_timer.refresher
Web User Interface		Configure session timer. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

Details of Configuration Parameters:

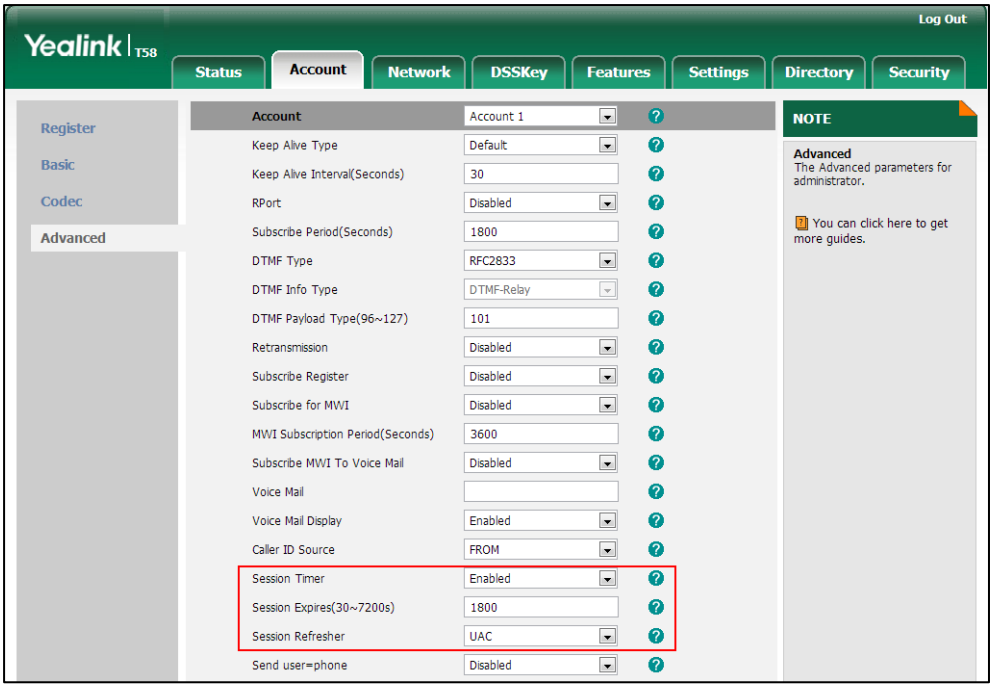
Parameters	Permitted Values	Default
account.X.session_timer.enable	**0 or 1**	**0**
Description: Enables or disables the session timer for account X. **0**-Disabled		

Parameters	Permitted Values	Default
1-Enabled If it is set to 1 (Enabled), IP phone will send periodic UPDATE requests to refresh the session during a call. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Session Timer **Phone User Interface:** None		
account.X.session_timer.expires	**Integer from 30 to 7200**	**1800**
Description: Configures the interval (in seconds) for refreshing the SIP session during a call for account X. For example, an UPDATE will be sent after 50% of its value has elapsed. If it is set to 1800 (1800s), the IP phone will refresh the session during a call before 900 seconds. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.session_timer.expires = 1800 **Note**: It works only if the value of the parameter "account.X.session_timer.enable" is set to 1 (Enabled). **Web User Interface:** Account->Advanced->Session Expires(30~7200s) **Phone User Interface:** None		
account.X.session_timer.refresher	**0 or 1**	**0**
Description: Configures the function of the endpoint who initiates the SIP request for account X. **0**-UAC **1**-UAS X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: It works only if the value of the parameter "account.X.session_timer.enable" is set to 1		

Parameters	Permitted Values	Default
(Enabled). **Web User Interface:** Account->Advanced->Session Refresher **Phone User Interface:** None		

To configure session timer via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Session Timer**.
4. Enter the desired time interval in the **Session Expires(30~7200s)** field.
5. Select the desired refresher from the pull-down list of **Session Refresher**.



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

Call Hold

Call hold provides a service of placing an active call on hold. The purpose of call hold is to pause activity on the existing call so that you can use the phone for another task (e.g., to place or receive another call).

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the call hold tone and call hold tone delay. **Parameters:** features.play_hold_tone.enable features.play_hold_tone.delay
		Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. **Parameter:** sip.rfc2543_hold
Web User Interface		Configure the call hold tone and call hold tone delay. Specify whether RFC 2543 (c=0.0.0.0) outgoing hold signaling is used. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

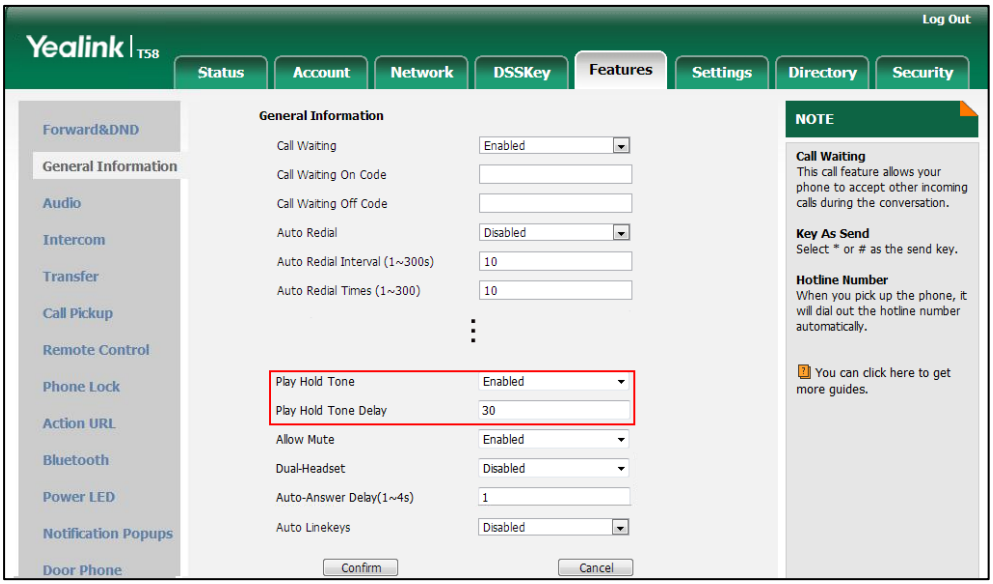
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.play_hold_tone.enable	**0 or 1**	**1**

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to play a warning tone when there is a call on hold. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Play Hold Tone **Phone User Interface:** None		
features.play_hold_tone.delay	**Integer from 3 to 3600**	**30**
Description: Configures the interval (in seconds) at which the IP phone play a warning tone when there is a call on hold. If it is set to 30 (30s), the IP phone will play a warning tone every 30 seconds when there is a call on hold. **Note:** 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 Tone Delay **Phone User Interface:** None		
sip.rfc2543_hold	**0 or 1**	**0**
Description: Enables or disables the IP phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), SDP media direction attributes (such as a=sendonly) per RFC 3264 is used when placing a call on hold. If it is set to 1 (Enabled), SDP media connection address c=0.0.0.0 per RFC 2543 is used when placing a call on hold. **Web User Interface:** Features->General Information->RFC 2543 Hold **Phone User Interface:** None		

To configure call hold tone and call hold tone delay via web user interface:

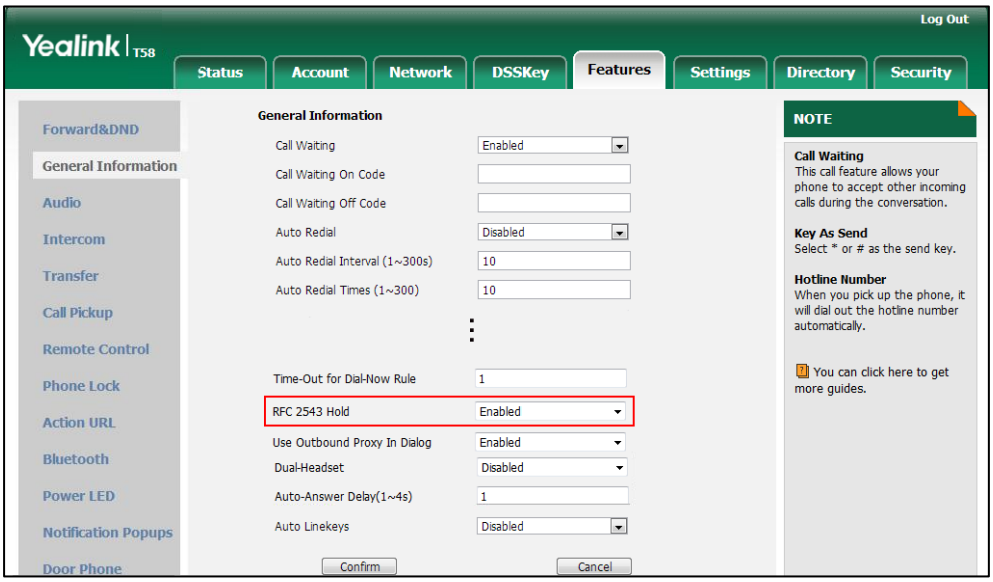
1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Play Hold Tone**.
3. Enter the desired time in the **Play Hold Tone Delay** field.



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

To configure call hold method via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **RFC 2543 Hold**.



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

Music on Hold (MoH)

Music on Hold (MoH) is the business practice of playing recorded music to fill the silence that would be heard by the party who has been placed on hold. To use this feature, specify a SIP URI pointing to a MoH server account. When a call is placed on hold, the IP phone will send an INVITE message to the specified MoH server account according to the SIP URI. The MoH server account automatically responds to the INVITE message and immediately plays audio from some source located anywhere (LAN, Internet) to the held party. For more information, refer to draft RFC draft-worley-service-example.

Note Music on Hold is not available on all servers. It is no need to specify the SIP URI if the MoH feature is enabled by default on the server and the server can play audio to the held party. For more information, contact your server administrator.

Procedure

Music on hold can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure music on hold on a per-line basis. **Parameter:** account.X.music_server_uri
		Configure the way on how the IP phone processes music on hold when placing an active call on hold. **Parameter:** account.X.music_on_hold_type
Web User Interface		Configure music on hold on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

Details of Configuration Parameters:

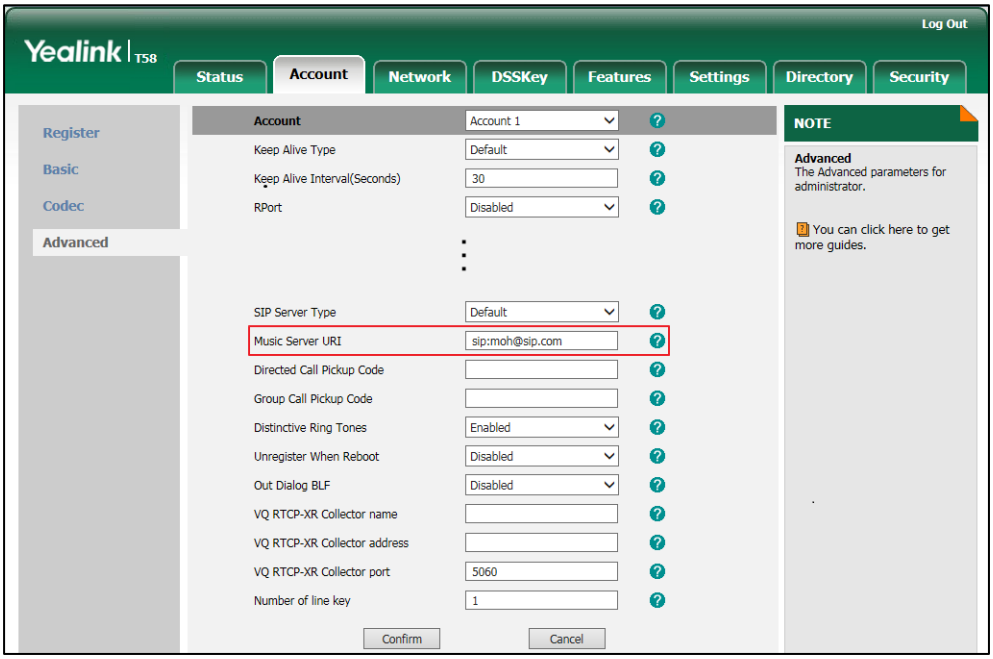
Parameters	Permitted Values	Default
account.X.music_server_uri	**SIP URI within 256 characters**	**Blank**
Description:		

Parameters	Permitted Values	Default
Configures the address of the Music On Hold server for account X. The URI points to a Music On Hold (MoH) server. Examples for valid values: <10.1.3.165>, 10.1.3.165, sip:moh@sip.com, <sip:moh@sip.com>, <yealink.com> or yealink.com. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.music_server_uri = sip:moh@sip.com **Note**: The DNS query in this parameter only supports A query. **Web User Interface:** Account->Advanced->Music Server URI **Phone User Interface:** None		
account.X.music_on_hold_type	**0 or 1**	**0**
Description: Configures the way to process Music On Hold when placing an active call on hold for account X. **0**-Calling the Music On Hold server before holding **1**-Calling the Music On Hold server after holding X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** None **Phone User Interface:** None		

To configure MoH via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

3. Enter the SIP URI (e.g., sip:moh@sip.com) in the **Music Server URI** field.



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

Call Forward

Call forward allows users to redirect an incoming call to a third party. IP phones redirect an incoming INVITE message by responding with a 302 Moved Temporarily message, which contains a Contact header with a new URI that should be tried. Three types of call forward:

- **Always Forward** -- Forward the incoming call immediately.
- **Busy Forward** -- Forward the incoming call when the IP phone or the specified account is busy.
- **No Answer Forward** -- Forward the incoming call after a period of ring time.

Call forward can be configured on a phone or a per-line basis depending on the call forward mode. The following describes the call forward modes:

- **Phone** (default)**:** Call forward feature is effective for the IP phone.
- **Custom:** Call forward feature can be configured for each or all accounts.

The server-side call forward settings disable the local call forward settings. If the server-side call forward feature is enabled on any of the IP phone's registrations, the other registrations are not affected. DND activated on the IP phone disables the local no answer forward settings.

The call forward on code and call forward off code configured on IP phones are used to activate/deactivate the server-side call forward feature. They may vary on different servers.

Diversion/History-Info

IP phones support the redirected call information sent by the SIP server with Diversion header, per draft-levy-sip-diversion-08, or History-info header, per RFC 4244. The Diversion/History-info header is used to inform the IP phone of a call's history. For example, when a phone has been set to enable call forward, the Diversion/History-info header allows the receiving phone to indicate who the call was from, and from which phone number it was forwarded.

Forward International

Forward international allows users to forward an incoming call to an international telephone number (the prefix is 00). This feature is enabled by default.

Forward Emergency

Forward emergency allows the incoming calls from some authorized numbers not to be forwarded when the call forward feature is enabled. The incoming call will not be logged in the Forwarded Calls list. This feature is disabled by default.

Procedure

Call forward can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure call forward in custom mode. **Parameters:** account.X.always_fwd.enable account.X.always_fwd.target account.X.always_fwd.on_code account.X.always_fwd.off_code account.X.busy_fwd.enable account.X.busy_fwd.target account.X.busy_fwd.on_code account.X.busy_fwd.off_code account.X.timeout_fwd.enable account.X.timeout_fwd.target account.X.timeout_fwd.timeout account.X.timeout_fwd.on_code account.X.timeout_fwd.off_code

	<y0000000000xx>.cfg	Specify the authorized numbers when call forward is enabled. **Parameters:** features.forward.emergency.enable features.forward.emergency.authorized_number
		Configure the call forward mode. **Parameter:** features.fwd_mode
		Configure call forward in phone mode. **Parameters:** forward.always.enable forward.always.target forward.always.on_code forward.always.off_code forward.busy.enable forward.busy.target forward.busy.on_code forward.busy.off_code forward.no_answer.enable forward.no_answer.target forward.no_answer.timeout forward.no_answer.on_code forward.no_answer.off_code
		Configure diversion/history-info feature. **Parameter:** features.fwd_diversion_enable
		Configure forward international. **Parameter:** forward.international.enable

Web User Interface	Specify the authorized numbers when call forward is enabled. Configure call forward. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-forward&q=load
	Configure diversion/history-info feature. Configure forward international. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
Phone User Interface	Configure call forward. Configure forward international.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.fwd_mode	**0 or 1**	**0**
Description: Configures the call forward mode for the IP phone. **0**-Phone **1**-Custom If it is set to 0 (Phone), call forward feature is effective for the IP phone. If it is set to 1 (Custom), you can configure call forward feature for each or all accounts. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Forward&DND->Forward->Mode **Phone User Interface:** None		
account.X.always_fwd.enable (X ranges from 1 to 16)	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Triggers always forward feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number (configured by the parameter "account.X.always_fwd.target") immediately. **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->Always Forward->On/Off **Phone User Interface:** Settings->Features->Call Forward->AccountX->Always Forward->Always Forward		
account.X.always_fwd.target (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the destination number of the always forward for account X. **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Example:** account.1.always_fwd.target = 1003 **Web User Interface:** Features->Forward&DND->Forward->Always Forward->Target **Phone User Interface:** Settings->Features->Call Forward->AccountX->Always Forward->Forward To		
account.X.always_fwd.on_code (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the always forward on code to activate the server-side always forward feature for account X. The IP phone will send the always forward on code and the pre-configured destination number (configured by the parameter "account.X.always_fwd.target") to the server when you activate always forward feature for account X on the IP phone. **Example:** account.1.always_fwd.on_code = *72		

Parameters	Permitted Values	Default
Note: It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->Always Forward->On Code **Phone User Interface:** Settings->Features->Call Forward->AccountX->Always Forward->On Code		
account.X.always_fwd.off_code (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the always forward off code to deactivate the server-side always forward feature for account X. The IP phone will send the always forward off code to the server when you deactivate always forward feature for account X on the IP phone. **Example:** account.1.always_fwd.off_code = *73 **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->Always Forward->Off Code **Phone User Interface:** Settings->Features->Call Forward->AccountX->Always Forward->Off Code		
account.X.busy_fwd.enable (X ranges from 1 to 16)	**0 or 1**	**0**
Description: Triggers busy forward feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number (configured by the parameter "account.X.busy_fwd.target") when the callee is busy. **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->Busy Forward **Phone User Interface:**		

Parameters	Permitted Values	Default
Settings->Features->Call Forward->AccountX->Busy Forward->Busy Forward		
account.X.busy_fwd.target (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the destination number of the busy forward for account X. **Example:** account.1.busy_fwd.target = 3602 **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->Busy Forward->Target **Phone User Interface:** Settings->Features->Call Forward->AccountX->Busy Forward->Forward To		
account.X.busy_fwd.on_code (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the busy forward on code to activate the server-side busy forward feature for account X. The IP phone will send the busy forward on code and the pre-configured destination number (configured by the parameter "account.X.busy_fwd.target") to the server when you activate busy forward feature for account X on the IP phone. **Example:** account.1.busy_fwd.on_code = *74 **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->Busy Forward->On Code **Phone User Interface:** Settings->Features->Call Forward->AccountX->Busy Forward->On Code		
account.X.busy_fwd.off_code (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the busy forward off code to deactivate the server-side busy forward feature for account X.		

Parameters	Permitted Values	Default
The IP phone will send the busy forward off code to the server when you deactivate busy forward feature for account X on the IP phone. **Example:** account.1.busy_fwd.off_code = *75 **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->Busy Forward->Off Code **Phone User Interface:** Settings->Features->Call Forward->AccountX->Busy Forward->Off Code		
account.X.timeout_fwd.enable (X ranges from 1 to 16)	**0 or 1**	**0**
Description: Triggers no answer forward feature to on or off for account X. **0**-Off **1**-On If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number (configured by the parameter "account.X.timeout_fwd.target") after a period of ring time. **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward **Phone User Interface:** Settings->Features->Call Forward->AccountX->No Answer Forward->No Answer Forward		
account.X.timeout_fwd.target (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the destination number of the no answer forward for account X. **Example:** account.1.timeout_fwd.target = 3603 **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:**		

Parameters	Permitted Values	Default
Features->Forward&DND->Forward->No Answer Forward->Target **Phone User Interface:** Settings->Features->Call Forward->AccountX->No Answer Forward->Forward To		
account.X.timeout_fwd.timeout (X ranges from 1 to 16)	**Integer from 0 to 20**	**2**
Description: Configures ring times (N) to wait before forwarding incoming calls for account X. Incoming calls will be forwarded when not answered after N*6 seconds. **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->After Ring Time(0~120s) **Phone User Interface:** Settings->Features->Call Forward->AccountX->No Answer Forward->After Ring Time		
account.X.timeout_fwd.on_code (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the no answer forward on code to activate the server-side no answer forward feature for account X. The IP phone will send the no answer forward on code and the pre-configured destination number (configured by the parameter "account.X.timeout_fwd.target") to the server when you activate no answer forward feature for account X on the IP phone. **Example:** account.1.timeout_fwd.on_code = *76 **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->On Code **Phone User Interface:** Settings->Features->Call Forward->AccountX->No Answer Forward->On Code		
account.X.timeout_fwd.off_code (X ranges from 1 to 16)	**String within 32 characters**	**Blank**
Description: Configures the no answer forward off code to deactivate the server-side no answer		

Parameters	Permitted Values	Default
forward feature for account X. The IP phone will send the no answer forward off code to the server when you deactivate no answer forward feature for account X on the IP phone. **Example:** account.1.timeout_fwd.off_code = *77 **Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter "features.fwd_mode" is set to 1 (Custom). **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->Off Code **Phone User Interface:** Settings->Features->Call Forward->AccountX->No Answer Forward->Off Code		
features.forward.emergency.enable	**0 or 1**	**0**
Description: Enables or disables the incoming calls from some authorized numbers not to be forwarded when the call forward feature is enabled. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Forward&DND->Forward->Forward Emergency **Phone User Interface:** None		
features.forward.emergency.authorized_number	**String within 511 characters**	**Blank**
Description: Configures the authorized numbers not to be forwarded even if call forward feature is enabled. Multiple numbers are separated by commas. **Example:** features.forward.emergency.authorized_number = 123,124 **Note:** It works only if the value of the parameter "features.forward.emergency.enable" is set to 1 (Enabled). **Web User Interface:** Features->Forward&DND->Forward->Forward Authorized Numbers **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
forward.always.enable	**0 or 1**	**0**
Description: Triggers the always forward feature to on or off for the IP phone. **0**-Off **1**-On If it is set to 1 (On), incoming calls are forwarded to the destination number (configured by the parameter "forward.always.target") immediately. **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->Always Forward **Phone User Interface:** Settings->Features->Call Forward->Always Forward->Always Forward		
forward.always.target	**String within 32 characters**	**Blank**
Description: Configures the destination number of the always forward for the IP phone. **Example:** forward.no_answer.target = 3601 **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->Always Forward->Target **Phone User Interface:** Settings->Features->Call Forward->Always Forward->Forward To		
forward.always.on_code	**String within 32 characters**	**Blank**
Description: Configures the always forward on code to activate the server-side always forward feature. The IP phone will send the always forward on code and the pre-configured destination number (configured by the parameter "forward.always.target") to the server when you activate always forward feature on the IP phone. **Example:** forward.always.on_code = *72 **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone).		

Parameters	Permitted Values	Default
Web User Interface: Features->Forward&DND->Forward->Always Forward->On Code **Phone User Interface:** Settings->Features->Call Forward->Always Forward->On Code		
forward.always.off_code	**String within 32 characters**	**Blank**
Description: Configures the always forward off code to deactivate the server-side always forward feature. The IP phone will send the always forward off code to the server when you deactivate always forward feature on the IP phone. **Example:** forward.always.off_code = *73 **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->Always Forward->Off Code **Phone User Interface:** Settings->Features->Call Forward->Always Forward->Off Code		
forward.busy.enable	**0 or 1**	**0**
Description: Triggers the busy forward feature to on or off for the IP phone. **0**-Off **1**-On If it is set to 1 (On), incoming calls are forwarded to the destination number (configured by the parameter "forward.busy.target") when the callee is busy. **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->Busy Forward **Phone User Interface:** Settings->Features->Call Forward->Busy Forward->Busy Forward		
forward.busy.target	**String within 32 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the destination number of the busy forward for the IP phone. **Example:** forward.busy.target = 3602 **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->Busy Forward->Target **Phone User Interface:** Settings->Features->Call Forward-> Busy Forward->Forward To		
forward.busy.on_code	**String within 32 characters**	**Blank**
Description: Configures the busy forward on code to activate the server-side busy forward feature. The IP phone will send the busy forward on code and the pre-configured destination number (configured by the parameter "forward.busy.target") to the server when you activate busy forward feature on the IP phone. **Example:** forward.busy.on_code = *74 **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->Busy Forward->On Code **Phone User Interface:** Settings->Features->Call Forward->Busy Forward->On Code		
forward.busy.off_code	**String within 32 characters**	**Blank**
Description: Configures the busy forward off code to deactivate the server-side busy forward feature. The IP phone will send the busy forward off code to the server when you deactivate busy forward feature on the IP phone. **Example:** forward.busy.off_code = *75 **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->Busy Forward->Off Code		

Parameters	Permitted Values	Default
Phone User Interface: Settings->Features->Call Forward->Busy Forward->Off Code		
forward.no_answer.enable	**0 or 1**	**0**
Description: Triggers the no answer forward feature to on or off for the IP phone. **0**-Off **1**-On If it is set to 1 (On), incoming calls are forwarded to the destination number (configured by the parameter "forward.no_answer.target") after a period of ring time. **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward **Phone User Interface:** Settings->Features->Call Forward->No Answer Forward->No Answer Forward		
forward.no_answer.target	**String within 32 characters**	**Blank**
Description: Configures the destination number of the no answer forward for the IP phone. **Example:** forward.no_answer.target = 3603 **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->Target **Phone User Interface:** Settings->Features->Call Forward->No Answer Forward->Forward To		
forward.no_answer.timeout	**Integer from 0 to 20**	**2**

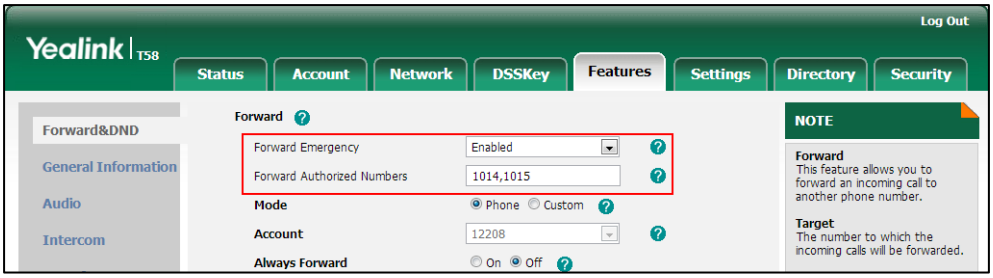
Parameters	Permitted Values	Default
Description: Configures ring times (N) to wait before forwarding incoming calls. Incoming calls will be forwarded when not answered after N*6 seconds. **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->After Ring Time (0~120s) **Phone User Interface:** Settings->Features->Call Forward->No Answer Forward->After Ring Time		
forward.no_answer.on_code	**String within 32 characters**	**Blank**
Description: Configures the no answer forward on code to activate the server-side no answer forward feature. The IP phone will send the no answer forward on code and the pre-configured destination number (configured by the parameter "forward.no_answer.target") to the server when you activate no answer forward feature on the IP phone. **Example:** forward.no_answer.on_code = *76 **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:** Features->Forward&DND->Forward->No Answer Forward->On Code **Phone User Interface:** Settings->Features->Call Forward->No Answer Forward->On Code		
forward.no_answer.off_code	**String within 32 characters**	**Blank**
Description: Configures the no answer forward off code to deactivate the server-side no answer forward feature. The IP phone will send the no answer forward off code to the server when you deactivate no answer forward feature on the IP phone. **Example:** forward.no_answer.off_code = *77 **Note:** It works only if the value of the parameter "features.fwd_mode" is set to 0 (Phone). **Web User Interface:**		

Parameters	Permitted Values	Default
Features->Forward&DND->Forward->No Answer Forward->Off Code **Phone User Interface:** Settings->Features->Call Forward->No Answer Forward->Off Code		
features.fwd_diversion_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to present the diversion information when an incoming call is forwarded to your IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Diversion/History-Info **Phone User Interface:** None		
forward.international.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to forward incoming calls to international numbers (the prefix is 00). **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Fwd International **Phone User Interface:** Settings->Advanced (default password: admin)->FWD International->FWD International		

To specify the authorized numbers when call forward is enabled via web user interface:

1. Click on **Features**->**Forward&DND**.
2. Select the desired value from the pull-down list of **Forward Emergency**.
3. Enter the desired value in the **Forward Authorized Numbers** field.

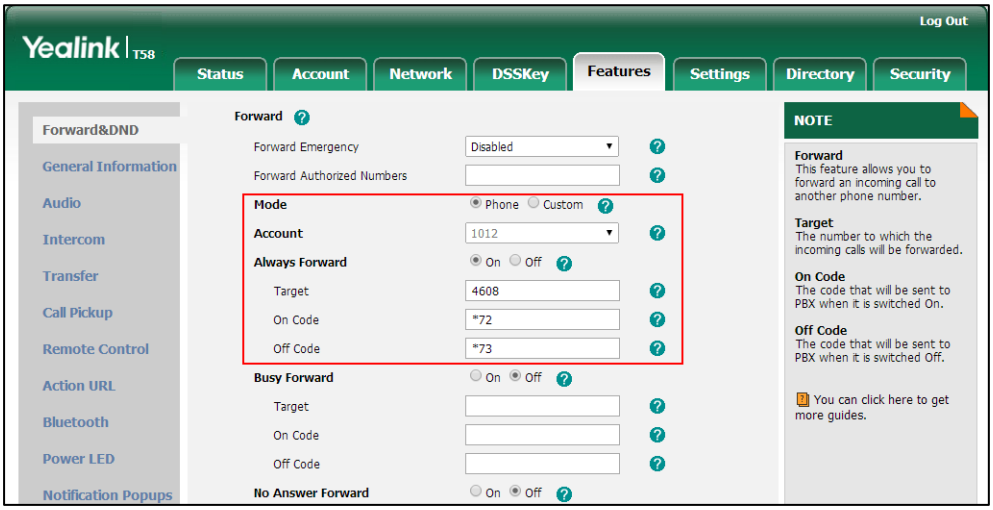
Multiple numbers are separated by commas.



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

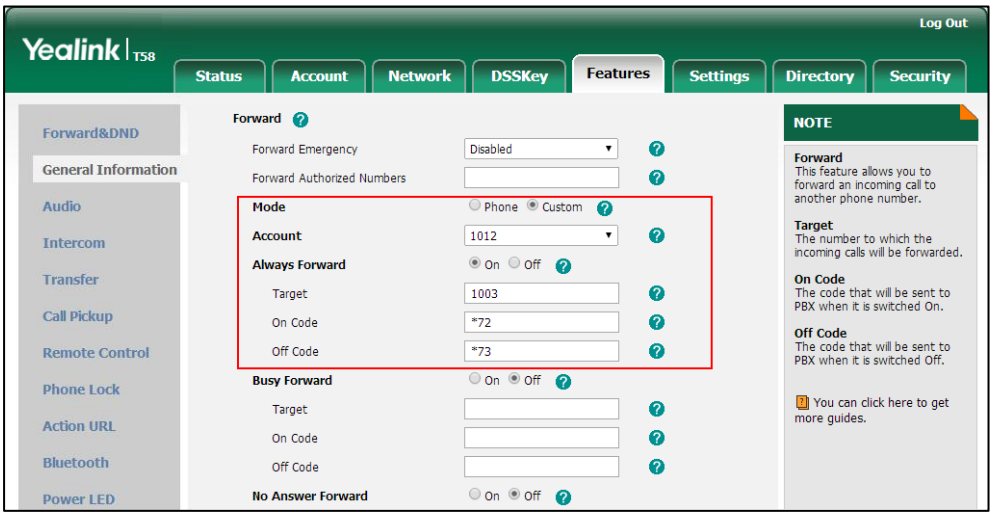
To configure call forward via web user interface:

1. Click on **Features**->**Forward&DND**.
2. In the **Forward** block, mark the desired radio box in the **Mode** field.
   a) If you mark the **Phone** radio box:
      1) Mark the desired radio box in the **Always/Busy/No Answer Forward** field.
      2) Enter the destination number you want to forward in the **Target** field.
      3) (Optional.) Enter the on code and off code in the **On Code** and **Off Code** fields.
      4) Select the ring time to wait before forwarding from the pull-down list of **After Ring Time(0~120s)** (only for the no answer forward).



b) If you mark the **Custom** radio box:
   1) Select the desired account from the pull-down list of **Account**.
   2) Mark the desired radio box in the **Always/Busy/No Answer Forward** field.
   3) Enter the destination number you want to forward in the **Target** field.
   4) Enter the on code and off code in the **On Code** and **Off Code** fields.

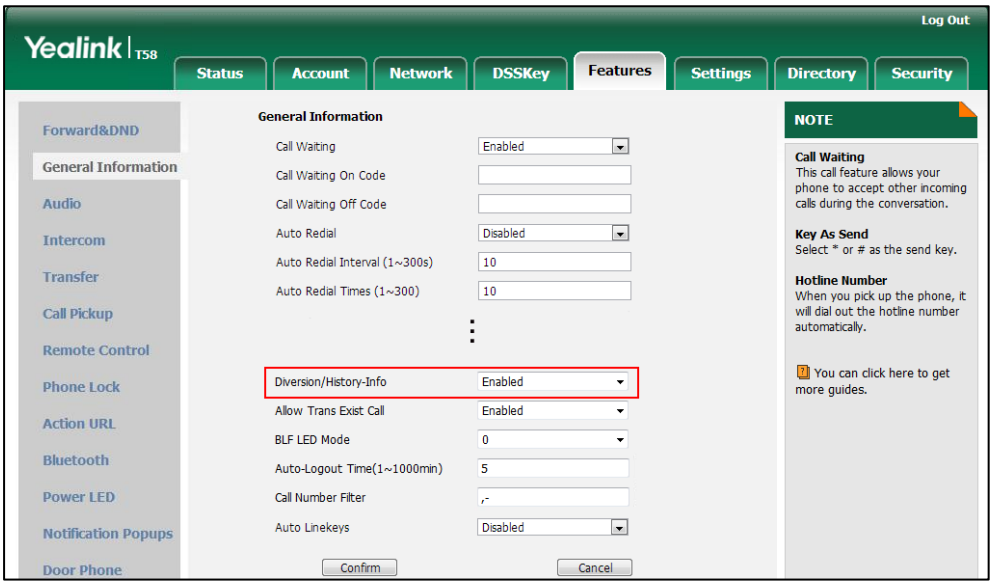
5) Select the ring time to wait before forwarding from the pull-down list of **After Ring Time(0~120s)** (only for the no answer forward).



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

To configure Diversion/History-Info feature via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Diversion/History-Info**.

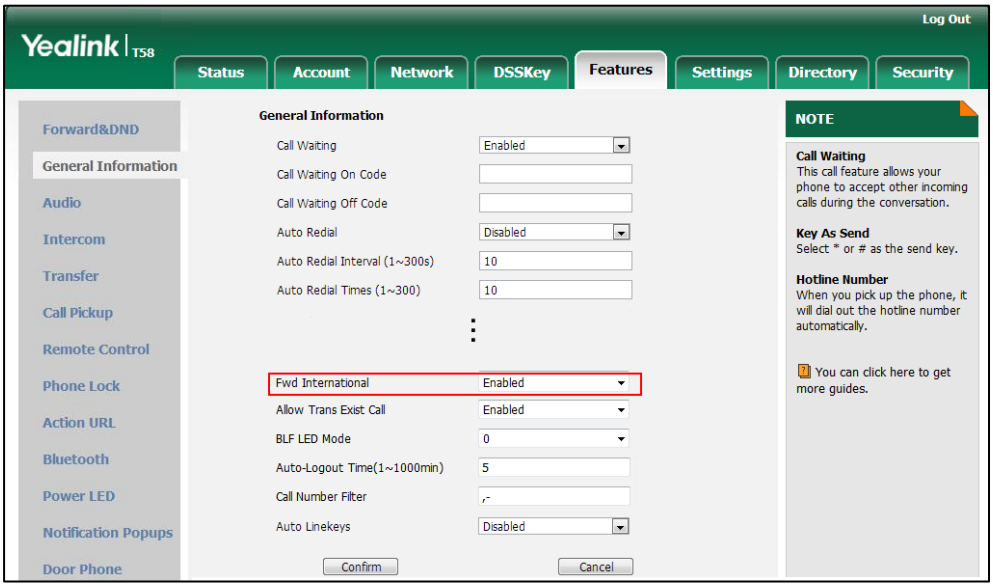


3. Click **Confirm** to accept the change.

To configure forward international via web user interface:

1. Click on **Features**->**General Information**.

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



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

To configure call forward in phone mode via phone user interface:

1. Tap **Settings**->**Features**->**Call Forward**.
2. Tap the desired forwarding type.
3. Depending on your selection:
   a) If you tap **Always Forward**:
      1) Tap the **On** radio box in the **Always Forward** field.
      2) Enter the destination number you want to forward all incoming calls to in the **Forward To** field.
      3) (Optional.) Enter the always forward on code or off code respectively in the **On Code** or **Off Code** field.
   b) If you tap **Busy Forward**:
      1) Tap the **On** radio box in the **Busy Forward** field.
      2) Enter the destination number you want to forward incoming calls to when the phone is busy in the **Forward To** field.
      3) (Optional.) Enter the busy forward on code or off code respectively in the **On Code** or **Off Code** field.
   c) If you tap **No Answer Forward**:
      1) Tap the **On** radio box in the **No Answer Forward** field.
      2) Enter the destination number you want to forward unanswered incoming calls to in the **Forward To** field.
      3) Tap the **After Ring Time** field.
      4) Tap the desired ring time to wait before forwarding in the pop-up dialog box.

      The default ring time is 12 seconds.

5) (Optional.) Enter the no answer forward on code or off code respectively in the **On Code** or **Off Code** field.

4. Tap ✓ to accept the change.

To configure call forward in custom mode via phone user interface:

1. Tap **Settings**->**Features**->**Call Forward**.
2. Tap the desired account.
3. Tap the desired forwarding type.
4. Depending on your selection:

a) If you tap **Always Forward**:

1) Tap the **On** radio box in the **Always Forward** field.
2) Enter the destination number you want to forward all incoming calls to in the **Forward To** field.
3) (Optional.) Enter the always forward on code or off code respectively in the **On Code** or **Off Code** field.

You can also enable always forward for all accounts. Do the following:

1) Tap ⋮, and then tap **All Lines**.

The touch screen prompts "Copy to all lines?".

2) Tap **OK** to accept the change or **Cancel** to cancel.

b) If you select **Busy Forward**:

1) Tap the **On** radio box in the **Busy Forward** field.
2) Enter the destination number you want to forward incoming calls to when the phone is busy in the **Forward To** field.
3) (Optional.) Enter the busy forward on code or off code respectively in the **On Code** or **Off Code** field.

You can also enable busy forward for all accounts. Do the following:

1) Tap ⋮, and then tap **All Lines**.

The touch screen prompts "Copy to all lines?".

2) Tap **OK** to accept the change or **Cancel** to cancel.

c) If you select **No Answer Forward**:

1) Tap the **On** radio box in the **No Answer Forward** field.
2) Enter the destination number you want to forward unanswered incoming calls to in the **Forward To** field.
3) Tap the **After Ring Time** field.
4) Tap the desired ring time to wait before forwarding from the pull-down list.

The default ring time is 12 seconds.

5) (Optional.) Enter the no answer forward on code or off code respectively in the **On Code** or **Off Code** field.

You can also enable no answer forward for all accounts. Do the following:

1) Tap , and then tap **All Lines**.

   The touch screen prompts "Copy to all lines?".

2) Tap **OK** to accept the change or **Cancel** to cancel.

5. Tap , and then tap **Save** to accept the change.

To configure forward international via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**FWD International.**
2. Tap the **FWD International** field.
3. Tap the desired value in the pop-up dialog box.
4. Tap to accept the change.

Call Transfer

Call transfer enables IP phones to transfer an existing call to a third party. For example, if party A is in an active call with party B, party A can transfer this call to party C (the third party). Then, party B will begin a new call with party C and party A will disconnect.

IP phones support call transfer using the REFER method specified in RFC 3515 and offer three types of transfer:

- **Blind Transfer** -- Transfer a call directly to another party without consulting. Blind transfer is implemented by a simple REFER method without Replaces in the Refer-To header.
- **Semi-attended Transfer** -- Transfer a call after hearing the ringback tone. Semi-attended transfer is implemented by a REFER method with Replaces in the Refer-To header.
- **Attended Transfer** -- Transfer a call with prior consulting. Attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

Normally, call transfer is completed by tapping the transfer key. Blind transfer on hook and attended transfer on hook features allow the IP phone to complete the transfer through on-hook. Blind transfer on hook and attended transfer on hook features are not applicable to CP960 IP phones.

When a user performs a semi-attended transfer, semi-attended transfer feature determines whether to display the prompt "**n New Missed Call(s)**" ("n" indicates the number of the missed calls) on the destination party's phone touch screen.

Procedure

Call transfer can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify whether to complete the transfer through on-hook. **Parameters:** transfer.blind_tran_on_hook_enable transfer.on_hook_trans_enable
		Configure semi-attended transfer feature. **Parameter:** transfer.semi_attend_tran_enable
Web User Interface		Specify whether to complete the transfer through on-hook. Configure semi-attended transfer feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-transfer&q=load

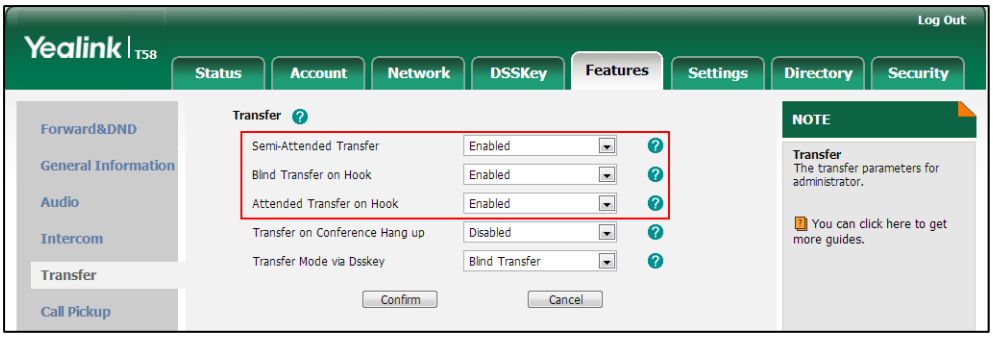
Details of Configuration Parameters:

Parameters	Permitted Values	Default
transfer.blind_tran_on_hook_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to complete the blind transfer through on-hook besides tapping the **Transfer** soft key or TRANSFER/TRAN key. **0**-Disabled **1**-Enabled **Note**: It is not applicable to CP960 IP phones. Blind transfer means transfer a call directly to another party without consulting. **Web User Interface:** Features->Transfer->Blind Transfer On Hook **Phone User Interface:** None		
transfer.on_hook_trans_enable	**0 or 1**	**1**

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to complete the semi-attended/attended transfer through on-hook besides tapping the **Transfer** soft key or TRANSFER/TRAN key. **0**-Disabled **1**-Enabled **Note**: It is not applicable to CP960 IP phones. Semi-attended transfer means transfer a call after hearing the ringback tone; Attended transfer means transfer a call with prior consulting. **Web User Interface:** Features->Transfer->Attended Transfer On Hook **Phone User Interface:** None		
transfer.semi_attend_tran_enable	**0 or 1**	**1**
Description: Enables or disables the transfer-to party's phone not to prompt a missed call on the touch screen before displaying the caller ID when completing a semi-attended transfer. **0**-Disabled **1**-Enabled **Note**: Semi-attended transfer means transfer a call after hearing the ringback tone. **Web User Interface:** Features->Transfer->Semi-Attended Transfer **Phone User Interface:** None		

To configure call transfer via web user interface:

1. Click on **Features**->**Transfer**.
2. Select the desired values from the pull-down lists of **Semi-Attended Transfer**, **Blind Transfer on Hook** and **Attended Transfer on Hook**.



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

Local Conference

Local conference requires a host phone to process the audio of all parties. Yealink IP phones support up to 5 parties (including yourself) in a local conference call.

For SIP-T58V/T58A IP phones, you can create up to three-way video conference call and five-way audio-only and video mixed conference. The audio-only and video mixed conference supports five parties participated (including yourself) at the same time including a maximum of three-way video calls. For more information, refer to *Yealink T58V & T58A user guide*.

For CP960 IP phones, you can set up a conference among the calls on your IP phone, the PC and connected mobile phone. For more information, refer to *Yealink CP960 user guide*.

Procedure

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

Configuration File	<MAC>.cfg	Configure local conference. **Parameter:** account.X.conf_type
Local	Web User Interface	Configure local conference. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

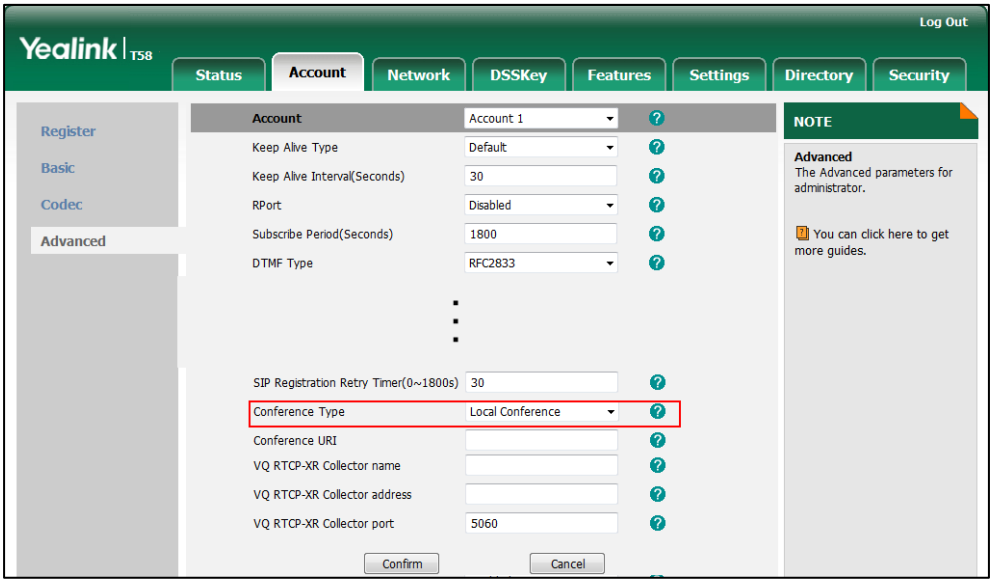
Details of Configuration Parameter:

Parameter	Permitted Values	Default
account.X.conf_type	**0 or 2**	**0**
Description: Configures the network conference type for SIP account X. **0**-Local Conference **2**-Network Conference If it is set to 0 (Local Conference), conferences are set up on the IP phone locally. If it is set to 2 (Network Conference), conferences are set up by the server. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:**		

Parameter	Permitted Values	Default
Account->Advanced->Conference Type **Phone User Interface:** None		

To configure the local conference via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **Local Conference** from the pull-down list of **Conference Type**.



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

Network Conference

Network conference, also known as centralized conference, provides users with flexibility of call with multiple participants (more than three). IP phones implement network conference using the REFER method specified in RFC 4579. This feature depends on support from a SIP server.

Procedure

Network conference can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure network conference. **Parameters:** account.X.conf_type account.X.conf_uri
Web User Interface		Configure network conference.

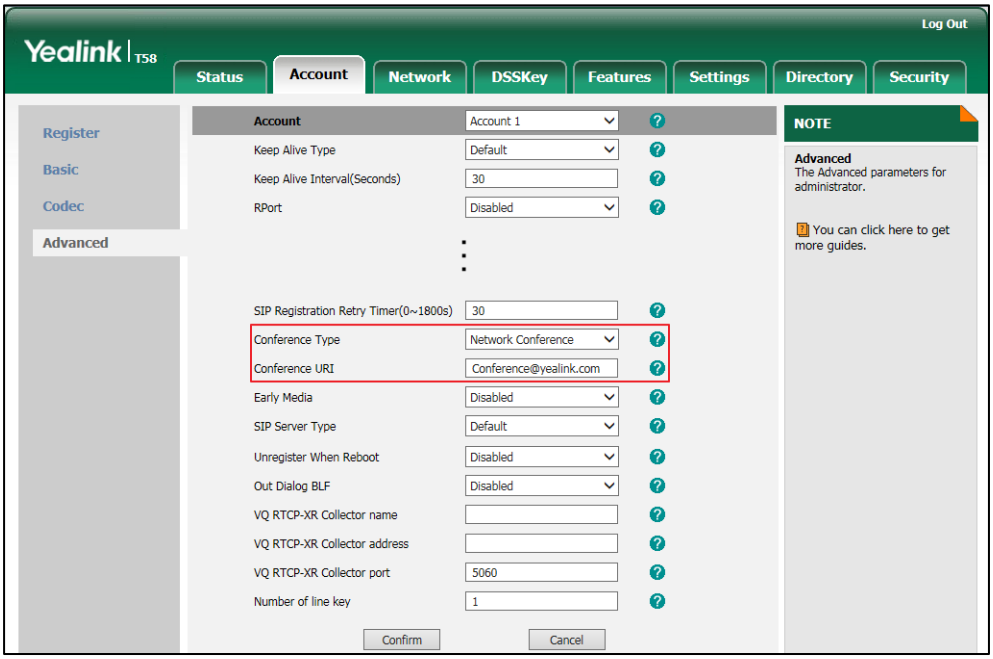
	Navigate to: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.conf_type	**0 or 2**	**0**
Description: Configures the network conference type for account X. **0**-Local Conference **2**-Network Conference If it is set to 0 (Local Conference), conferences are set up on the IP phone locally. If it is set to 2 (Network Conference), conferences are set up by the server. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Conference Type **Phone User Interface:** None		
account.X.conf_uri	**SIP URI within 511 characters**	**Blank**
Description: Configures the network conference URI for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.conf_uri = conference@example.com **Note**: It works only if the value of the parameter "account.X.conf_type" is set to 2 (Network Conference). **Web User Interface:** Account->Advanced->Conference URI **Phone User Interface:** None		

To configure the network conference via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **Network Conference** from the pull-down list of **Conference Type**.
4. Enter the conference URI in the **Conference URI** field.



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

Transfer on Conference Hang Up

For a local conference, all parties drop the call when the conference initiator drops the conference call. Transfer on conference hang up feature allows the other two parties to remain connected when the conference initiator drops the conference call. Network conference does not have a conference initiator, so if any party exits the network conference, the remaining parties are still connected. For more information on network conference, refer to Network Conference on page 367.

Procedure

Transfer on conference hang up can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the transfer on conference hang up. **Parameter:** transfer.tran_others_after_conf_enable
Web User Interface		Configure the transfer on conference hang up.

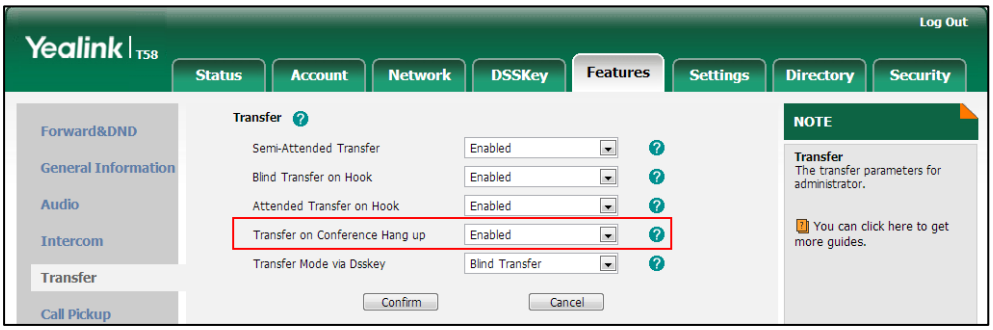
	Navigate to: http://<phoneIPAddress>/servlet?m=mod_data&p=features-transfer&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
transfer.tran_others_after_conf_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to transfer the local conference call to the other two parties after the conference initiator drops the local conference call. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), all parties are disconnected when the conference initiator drops the conference call. If it is set to 1 (Enabled), the other two parties remain connected when the conference initiator drops the conference call. **Note**: It works only if the value of parameter "account.X.conf_type" is set to 0 (Local Conference). **Web User Interface:** Features->Transfer->Transfer on Conference Hang up **Phone User Interface:** None		

To configure transfer on conference hang up via web user interface:

1. Click on **Features**->**Transfer**.
2. Select the desired value from the pull-down list of **Transfer on Conference Hang up**.



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

Feature Key Synchronization

Feature key synchronization provides the capability to synchronize the status of the following features between the IP phone and the server:

- Do Not Disturb (DND)
- Call Forwarding Always (CFA)
- Call Forwarding Busy (CFB)
- Call Forwarding No Answer (CFNA)

If feature key synchronization is enabled, a user changes the status of one of these features on the server, and then the server notifies the phone of synchronizing the status. Conversely, if the user changes the feature status on the phone, the IP phone notifies the server of synchronizing the status.

Procedure

Feature key synchronization can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure feature key synchronization. **Parameter:** bw.feature_key_sync
Web User Interface		Configure feature key synchronization. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

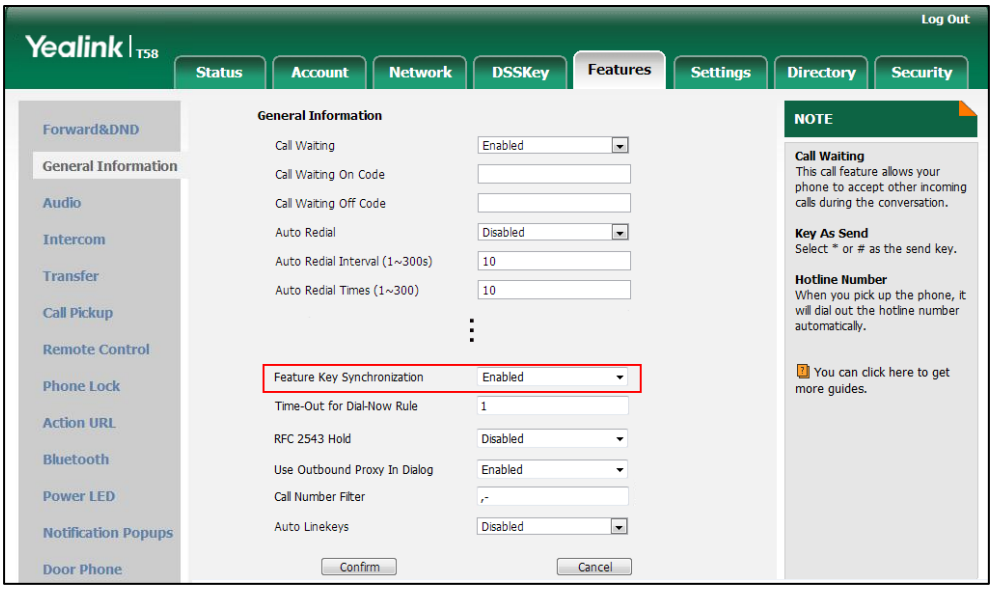
Details of Configuration Parameter:

Parameter	Permitted Values	Default
bw.feature_key_sync	**0 or 1**	**0**
Description: Enables or disables feature key synchronization. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Feature Key Synchronization **Phone User Interface:**		

Parameter	Permitted Values	Default
None		

To configure feature key synchronization via web user interface:

1. Click on **Features**->**General Information**.
2. Select **Enabled** from the pull-down list of **Feature Key Synchronization**.



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

Transfer Mode via Dsskey

Transfer mode via dsskey enables IP phones to handle the current call differently via the DSS key. IP phones support three transfer modes: New Call, Blind Transfer and Attended Transfer. For more information on Blind Transfer and Attended Transfer, refer to Call Transfer on page 363.

The transfer mode via dsskey feature is available when the DSS key is assigned to the following features:

- Speed dial
- Transfer
- BLF/BLF List

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Procedure

Transfer mode via dsskey can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the transfer mode via dsskey. **Parameter:** transfer.dsskey_deal_type
Web User Interface		Configure the transfer mode via dsskey. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-transfer&q=load

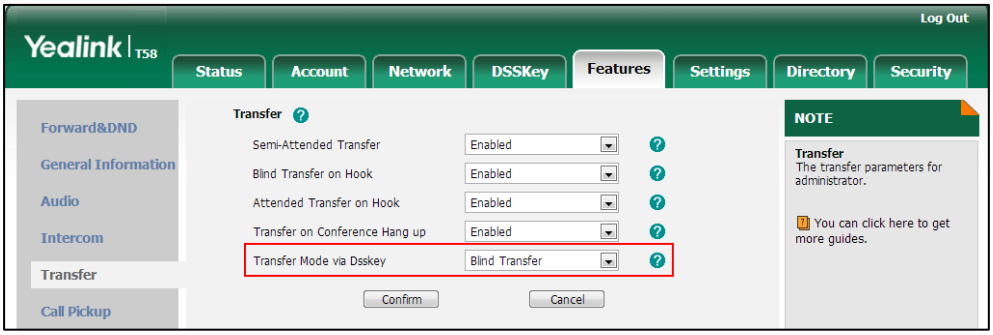
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
transfer.dsskey_deal_type	**0, 1 or 2**	**2**
Description: Configures the transfer mode when user presses the DSS key during an active call. **0**-New Call **1**-Attended Transfer **2**-Blind Transfer **Note**: To use this feature, you need to configure the DSS key as a speed dial, transfer or BLF/BLF List in advance. **Web User Interface:** Features->Transfer->Transfer Mode via Dsskey **Phone User Interface:** None		

To configure transfer mode via dsskey via web user interface:

1. Click on **Features**->**Transfer**.

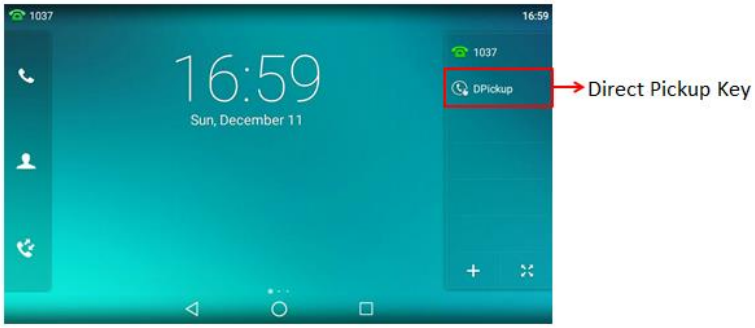
2. Select the desired value from the pull-down list of **Transfer Mode via Dsskey**.



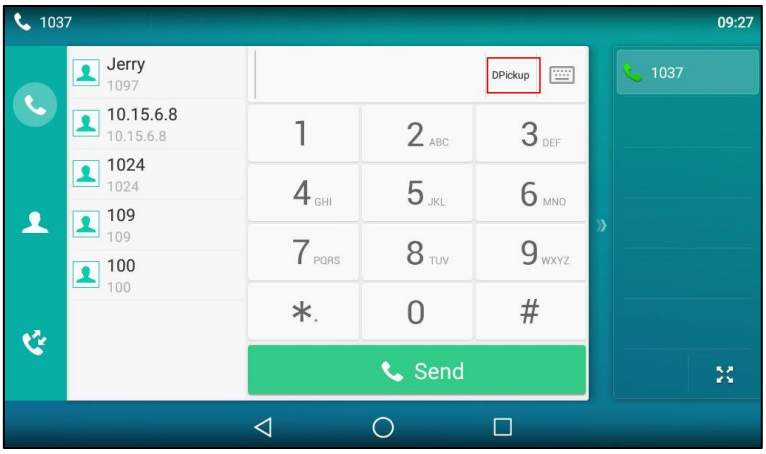
3. Click **Confirm** to accept the change.

Directed Call Pickup

Directed call pickup is used for picking up an incoming call on a specific extension. A user can pick up the incoming call using a directed pickup key or **DPickup** key. This feature depends on support from a SIP server. For many SIP servers, directed call pickup requires a directed pickup code, which can be configured on a phone or a per-line basis.



When you enable directed call pickup, the touch screen will display a **DPickup** key when you pick up the handset, press the Speakerphone key or tap the line key. As shown below:



Note It is recommended not to configure the directed call pickup key and the **DPickup** key simultaneously. If you do, the directed pickup key will not be used correctly.

Procedure

Directed call pickup can be configured using the following methods.

<table>
<tr><td rowspan="3">Central Provisioning (Configuration File)</td><td rowspan="2"><MAC>.cfg</td><td>Configure the directed call pickup code on a per-line basis.
Parameter:
account.X.direct_pickup_code</td></tr>
<tr><td>Configure directed call pickup features on a phone basis.
Parameters:
features.pickup.direct_pickup_enable
features.pickup.direct_pickup_code</td></tr>
<tr><td><y0000000000xx>.cfg</td><td>Assign a directed call pickup key.
Parameters:
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type
linekey.X.line/ programablekey.X.line/ expansion_module.X.key.Y.line
linekey.X.value/ programablekey.X.value/ expansion_module.X.key.Y.value
linekey.X.label/ expansion_module.X.key.Y.label</td></tr>
<tr><td colspan="2" rowspan="2">Web User Interface</td><td>Assign a directed call pickup key.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load</td></tr>
<tr><td>Configure directed call pickup code on a per-line basis.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0</td></tr>
</table>

	Configure directed call pickup feature on a phone basis. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-callpickup&q=load
Phone User Interface	Assign a directed call pickup key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.direct_pickup_code	**String within 32 characters**	**Blank**
Description: Configures the directed call pickup code for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.direct_pickup_code = *68 **Note**: The directed call pickup code configured on a per-line basis ("account.X.direct_pickup_code") takes precedence over that configured on a phone basis ("features.pickup.direct_pickup_code"). **Web User Interface:** Account->Advanced->Directed Call Pickup Code **Phone User Interface:** None		
features.pickup.direct_pickup_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to display the **DPickup** key when the IP phone is on the pre-dialing screen. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Call Pickup->Directed Call Pickup **Phone User Interface:** None		

Parameters	Permitted Values	Default
features.pickup.direct_pickup_code	**String within 32 characters**	**Blank**
Description: Configures the directed call pickup code on a phone basis. **Example:** features.pickup.direct_pickup_code = *97 **Note**: The directed call pickup code configured on a per-line basis ("account.X.direct_pickup_code") takes precedence over that configured on a phone basis ("features.pickup.direct_pickup_code"). **Web User Interface:** Features->Call Pickup->Directed Call Pickup Code **Phone User Interface:-** None		

Directed Call Pickup Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type	**9**	**Refer to the following content**
Description: Configures a DSS key as a directed call pickup key on the IP phone. The digit **9** stands for the key type **Direct Pickup**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)		

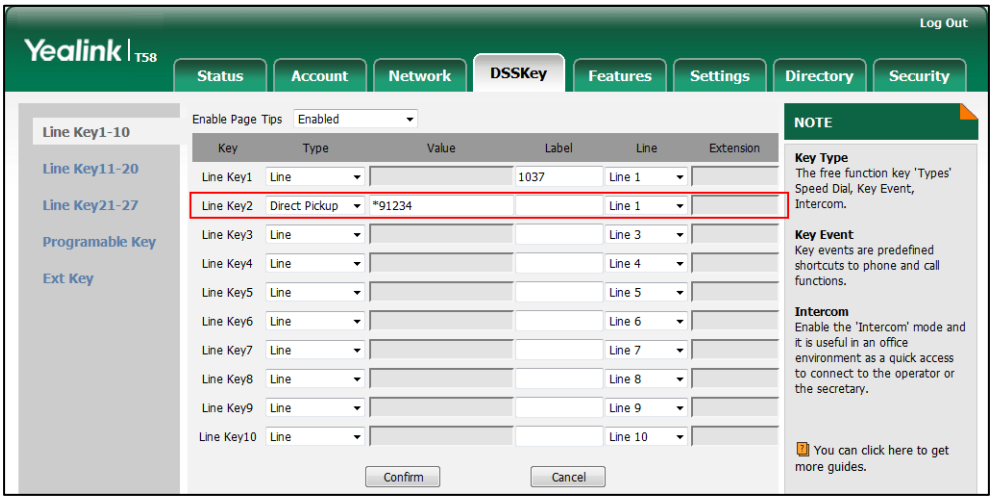
Parameters	Permitted Values	Default
Example: linekey.2.type = 9 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For programable keys: **For SIP-T58V/T58A/T56A IP phones:** When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key/Programable Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.line/ programablekey.X.line/ expansion_module.X.key.Y.line	**Refer to the following content**	**1-16 for lines 1-16, 1 for programable keys**
Description: Configures the desired line to apply the directed call pickup key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Permitted Values:**		

Parameters	Permitted Values	Default
1 to 16 (for SIP-T58V/T58A/T56A) 1 (for CP960) 1-Line 1 2-Line 2 … 16-Line 16 **Example:** linekey.2.line = 1 **Web User Interface:** DSSKey->Line Key/Programable Key->Line **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Account ID		
linekey.X.value/ programablekey.X.value/ expansion_module.X.key.Y.value	**String within 99 characters**	**Blank**
Description: Configures the directed call pickup feature code followed by the monitored extension. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.value = *971008 **Web User Interface:** DSSKey->Line Key/Programable Key->Value **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Value		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys:		

Parameters	Permitted Values	Default
X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a directed call pickup key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **Direct Pickup** from the pull-down list of **Type**.
3. Enter the directed call pickup code followed by the specific extension in the **Value** field.
4. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
5. Select the desired line from the pull-down list of **Line**.

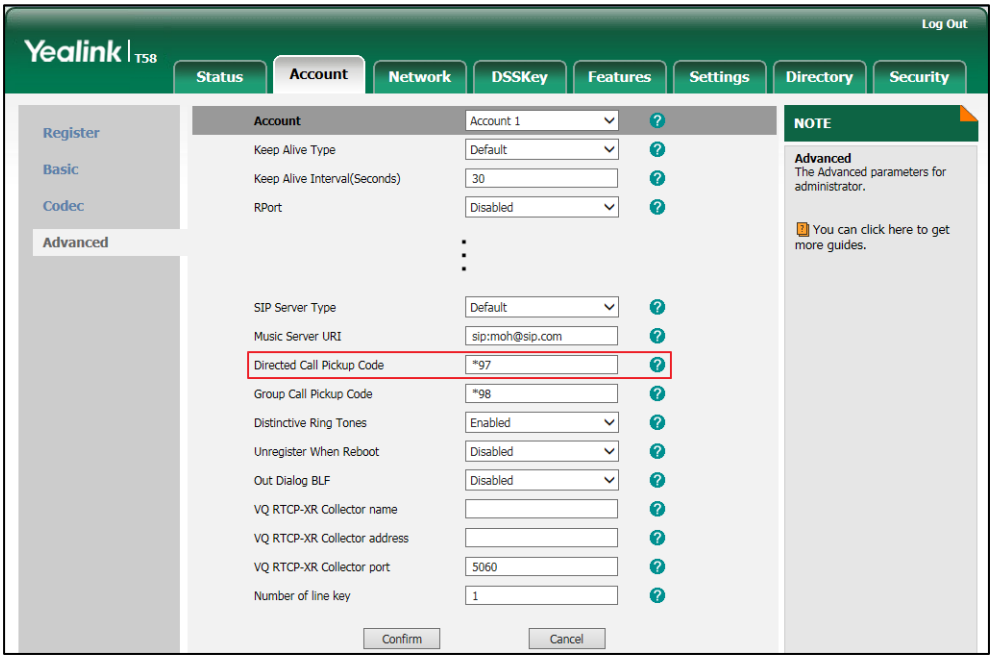


6. Click **Confirm** to accept the change.

To configure the directed call pickup code on a per-line basis via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

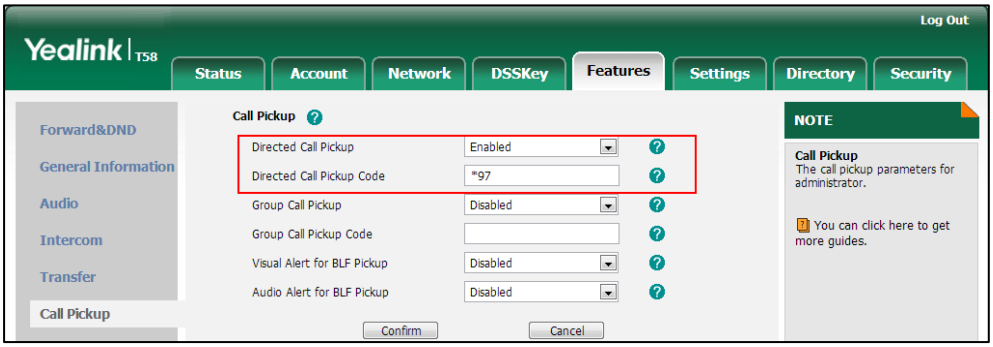
3. Enter the directed call pickup code in the **Directed Call Pickup Code** field.



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

To configure directed call pickup feature on a phone basis via web user interface:

1. Click on **Features**->**Call Pickup**.
2. Select the desired value from the pull-down list of **Directed Call Pickup**.
3. Enter the directed call pickup code in the **Directed Call Pickup Code** field.



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

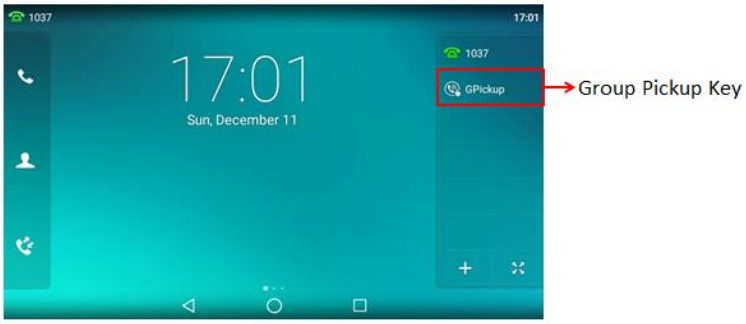
To configure a directed pickup key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Select the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **DPickup** in the pop-up dialog box.

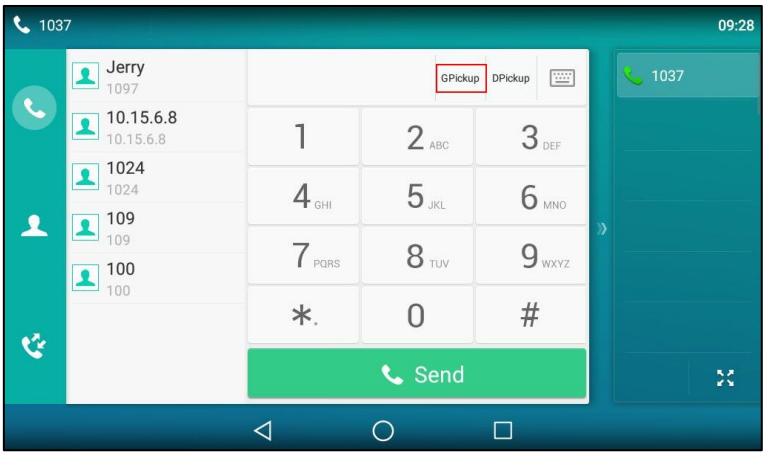
7. Tap the **Account ID** field.
8. Tap the desired line in the pop-up dialog box.
9. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
10. Enter the directed call pickup code followed by the specific extension in the **Value** field.
11. Tap ✓ to accept the change.

Group Call Pickup

Group call pickup is used for picking up incoming calls within a pre-defined group. If the group receives many incoming calls at once, the user will pick up the first incoming call, using a group pickup key or the **GPickup** key. This feature depends on support from a SIP server. For many SIP servers, group call pickup requires a group pickup code, which can be configured on a phone or a per-line basis.



When you enable group call pickup, the touch screen will display a **GPickup** key when you pick up the handset, press the Speakerphone key or tap the line key. As shown below:



Procedure

Group call pickup can be configured using the following methods.

Central Provisioning	<MAC>.cfg	Configure the group call pickup code on a per-line basis.

(Configuration File)		**Parameters:** account.X.group_pickup_code
		Configure group call pickup features on a phone basis. **Parameters:** features.pickup.group_pickup_enable features.pickup.group_pickup_code
	<y0000000000xx>.cfg	Assign a group call pickup key. **Parameters:** linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type linekey.X.line/ programablekey.X.line/ expansion_module.X.key.Y.line linekey.X.value/ programablekey.X.value/ expansion_module.X.key.Y.value linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Assign a group call pickup key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
		Configure the group call pickup code on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0
		Configure group call pickup feature on a phone basis. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-callpickup&q=load
Phone User Interface		Assign a group call pickup key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.pickup.group_pickup_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to display the **GPickup** key when the IP phone is on the pre-dialing screen. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Call Pickup->Group Call Pickup **Phone User Interface:** None		
account.X.group_pickup_code	**String within 32 characters**	**Blank**
Description: Configures the group pickup code for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.group_pickup_code = *69 **Note**: The group call pickup code configured on a per-line basis (configured by the parameter "account.X.group_pickup_code") takes precedence over that configured on a phone basis (configured by the parameter "features.pickup.group_pickup_code"). **Web User Interface:** Account->Advanced->Group Call Pickup Code **Phone User Interface:** None		
features.pickup.group_pickup_code	**String within 32 characters**	**Blank**
Description: Configures the group call pickup code on a phone basis. **Example:** features.pickup.group_pickup_code = *98 **Note**: The group call pickup code configured on a per-line basis (configured by the		

Parameters	Permitted Values	Default
parameter "account.X.group_pickup_code") takes precedence over that configured on a phone basis (configured by the parameter "features.pickup.group_pickup_code"). **Web User Interface:** Features->Call Pickup->Group Call Pickup Code **Phone User Interface:** None		

Group Call Pickup Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

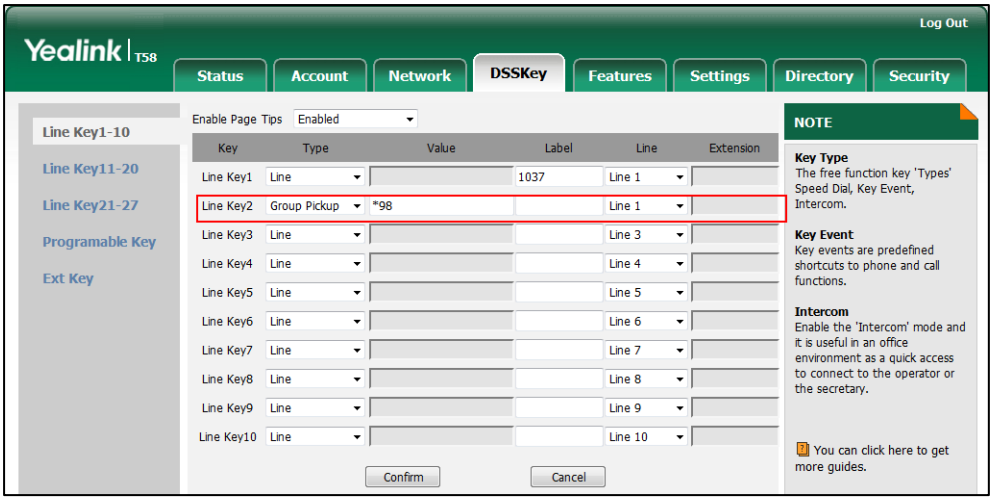
Parameters	Permitted Values	Default
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type	**23**	**Refer to the following content**
Description: Configures a DSS key as a group call pickup key on the IP phone. The digit **23** stands for the key type **Group Pickup**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 23 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0.		

Parameters	Permitted Values	Default
For programable keys: **For SIP-T58V/T58A/T56A IP phones:** When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key/Programable Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.line/ programablekey.X.line/ expansion_module.X.key.Y.line	**Refer to the following content**	**1-16 for lines 1-16, 1 for programable keys**
Description: Configures the desired line to apply the group call pickup key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Permitted Values:** 1 to 16 (for SIP-T58V/T58A/T56A) 1 (for CP960) 1-Line 1 2-Line 2 … 16-Line 16 **Example:** linekey.2.line = 1 **Web User Interface:**		

Parameters	Permitted Values	Default
DSSKey->Line Key/Programable Key->Line **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Account ID		
linekey.X.value/ programablekey.X.value/ expansion_module.X.key.Y.value	**String within 99 characters**	**Blank**
Description: Configures the group call pickup feature code. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.value = *98 **Web User Interface:** DSSKey->Line Key/Programable Key->Value **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Value		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a group call pickup key via web user interface:

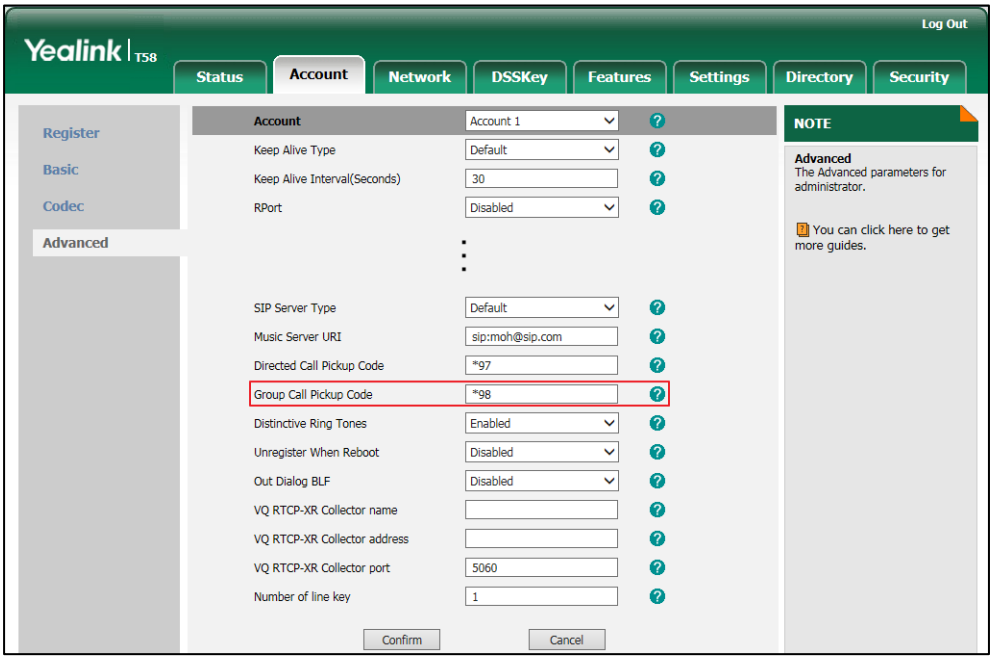
1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **Group Pickup** from the pull-down list of **Type**.
3. Enter the group call pickup code in the **Value** field.
4. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
5. Select the desired line from the pull-down list of **Line**.



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

To configure the group call pickup code on a per-line basis via web user interface:

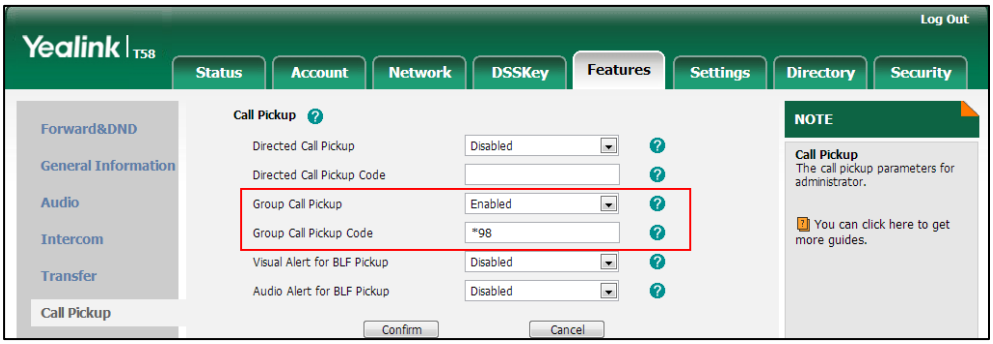
1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Enter the group call pickup code in the **Group Call Pickup Code** field.



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

To configure group call pickup feature on a phone basis via web user interface:

1. Click on **Features**->**Call Pickup**.
2. Select the desired value from the pull-down list of **Group Call Pickup**.
3. Enter the group call pickup code in the **Group Call Pickup Code** field.



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

To configure a group pickup key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Select the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **Group Pick Up** in the pop-up dialog box.
7. Tap the **Account ID** field.
8. Tap the desired line in the pop-up dialog box.
9. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
10. Enter the group call pickup code in the **Value** field.
11. Tap ✓ to accept the change.

Dialog Info Call Pickup

Call pickup is implemented through SIP signals on some specific servers. When this feature is enabled, IP phones support picking up incoming calls via the INVITE message which includes a Replaces header in the message body. The value of Replaces is derived from a NOTIFY message with dialog-info event. A user can pick up an incoming call by tapping the DSS key used to monitor a specific extension (such as the BLF key). For more information on BLF, refer to Busy Lamp Field (BLF) on page 473.

If the visual alert for blf pickup feature is enabled, a user can also pick up an incoming call by tapping the **DPickup** key. For more information on visual alert for blf pickup, refer to Visual Alert and Audio Alert for BLF Pickup on page 477.

Note In this way, you do not need to configure the directed call pickup code.

Example of the dialog-info carried in NOTIFY message:

```
<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="6" state="partial"
entity="sip:1011@10.2.1.48:5060">
<dialog id="65603" call-id="0_1756536024@10.10.20.34" local-tag="3408640225" remote-tag="3779921438"
direction="recipient">
<state>early</state>
<local>
<identity>sip:1011@10.2.1.48:5060</identity>
<target uri="sip:1011@10.2.1.48:5060"/>
</local>
<remote>
<identity>sip:1058@10.2.1.48:5060</identity>
<target uri="sip:1058@10.2.1.48:5060"/>
</remote>
</dialog>
</dialog-info>
```

Example of the Replaces carried in INVITE message:

```
Via: SIP/2.0/UDP 10.10.20.18:5060;branch=z9hG4bK2026058891
From: "1010" <sip:1010@10.2.1.48:5060>;tag=826048502
To: <sip:1058@10.2.1.48:5060>
Call-ID: 0_572446084@10.10.20.18
CSeq: 1 INVITE
Contact: <sip:1010@10.10.20.18:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Replaces: 0_1756536024@10.10.20.34;to-tag=3779921438;from-tag=3408640225
Allow-Events: talk,hold,conference,refer,check-sync
Supported: replaces
Content-Length:    304
```

Procedure

Dialog info call pickup can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure dialog info call pickup. **Parameter**: account.X.dialoginfo_callpickup
Web User Interface		Configure dialog info call pickup. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

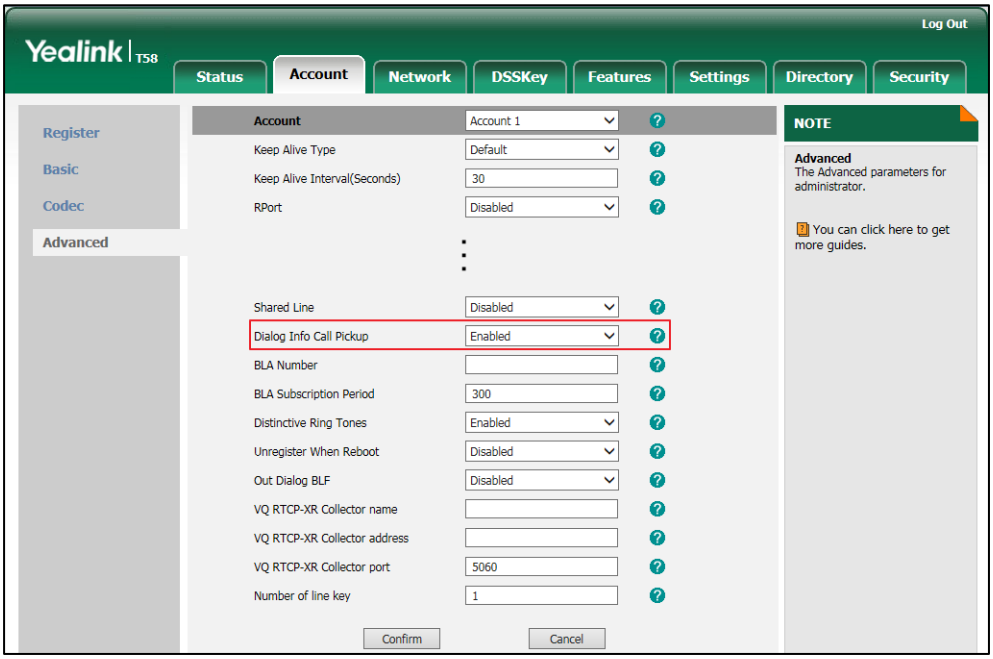
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.dialoginfo_callpickup	**0 or 1**	**0**
Description: Enables or disables the IP phone to pick up a call according to the Replaces header of the INVITE message for account X. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), call pickup is implemented through SIP signals. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Dialog Info Call Pickup **Phone User Interface:** None		

To configure dialog info call pickup via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

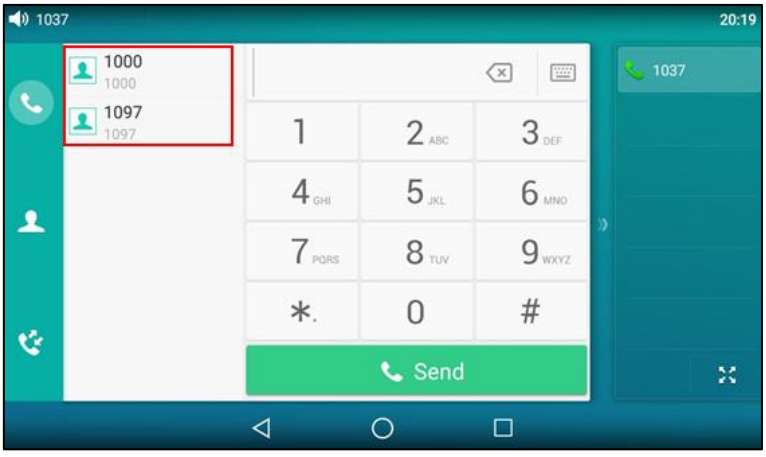
3. Select the desired value from the pull-down list of **Dialog Info Call Pickup**.



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

Recent Call In Dialing

Recent call in dialing feature allows users to view the placed calls list when the phone is on the pre-dialing screen. Users can select to place a call from the placed calls list. For some phones, you may need to drag up and down to scroll through the list of placed call number.



Procedure

Recent call in dialing can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure recent call in dialing feature. **Parameter:**

		super_search.recent_call
Web User Interface		Configure recent call in dialing feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=contacts-favorite&q=load

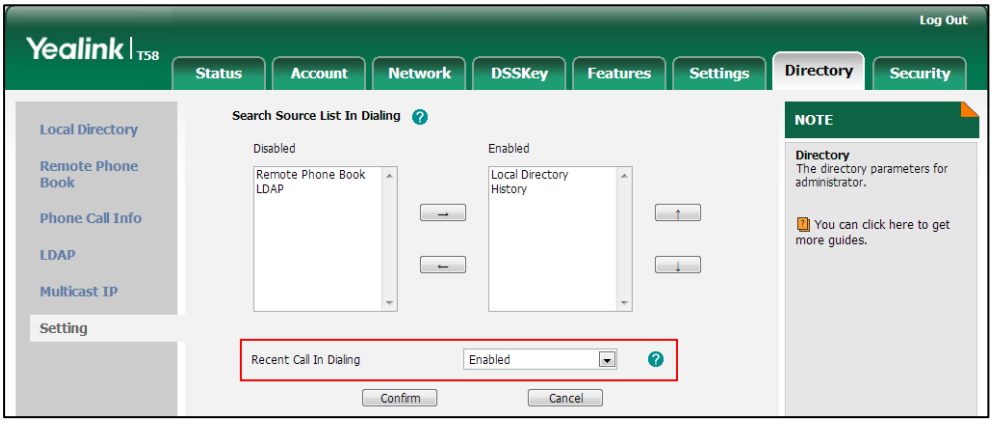
Details of Configuration Parameter:

Parameter	Permitted Values	Default
super_search.recent_call	**0 or 1**	**Refer to the following content**
Description: Enables or disables recent call in dialing feature. **0**-Disabled **1**-Enabled **For SIP-T58V/T58A/T56A IP phones:** The default value is 0. **For CP960 IP phones:** The default value is 1. If it is set to 1 (Enabled), you can see the placed calls list when the IP phone is on the pre-dialing screen. **Web User Interface:** Directory->Setting->Recent Call In Dialing **Phone User Interface:** None		

To configure recent call in dialing via web user interface:

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

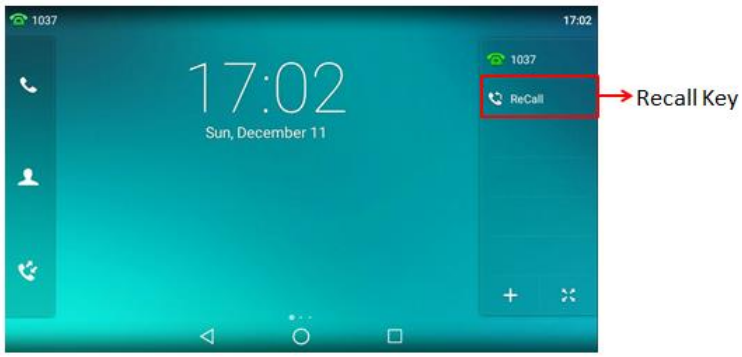
2. Select the desired value from the pull-down list of **Recent Call In Dialing**.



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

ReCall

ReCall, also known as last call return, allows users to place a call back to the last caller. Recall is implemented on IP phones using a recall key. When you tap the recall key, you will place a call to the phone number that last called you.



Procedure

Recall key can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Assign a recall key. **Parameter:** linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Assign a recall key. **Navigate to**:

	http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface	Assign a recall key.

ReCall Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type	**7**	**Refer to the following content**

Description:

Configures a DSS key as a recall key on the IP phone.

The digit **7** stands for the key type **ReCall**.

For line keys:

X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)

X ranges from 1 to 30 (for CP960)

For programable keys:

X ranges from 12 to 14 (for SIP-T58V/T58A/T56A)

For ext keys:

X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)

Example:

linekey.2.type = 7

Default:

For line keys:

For SIP-T58V/T58A/T56A IP phones:

The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0.

For CP960 IP phones:

The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0.

For programable keys:

For SIP-T58V/T58A/T56A IP phones:

When X=12, the default value is 0 (NA).

When X=13, the default value is 0 (NA).

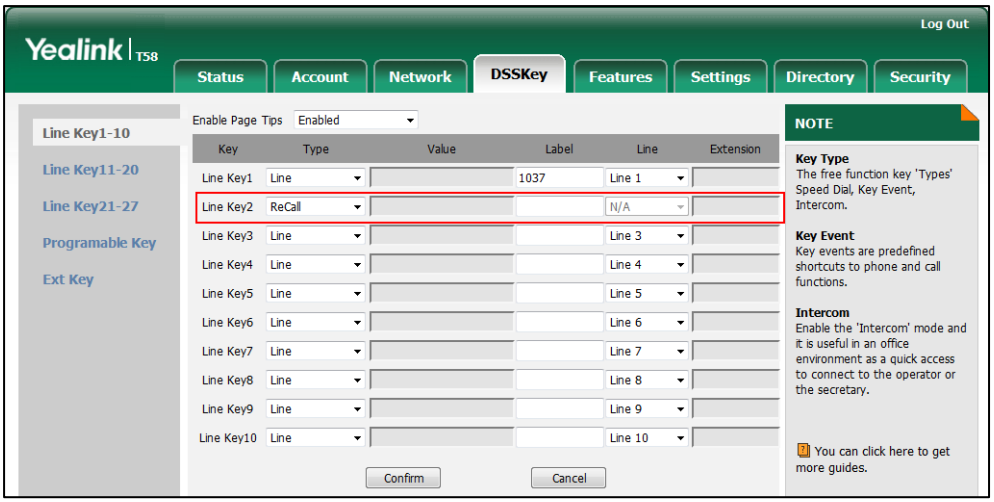
When X=14, the default value is 2 (Forward).

Parameters	Permitted Values	Default
For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key/Programable Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a recall key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **ReCall** from the pull-down list of **Type**.

3. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.



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

To configure a recall key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Select the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **ReCall** in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Tap ✓ 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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the characters the IP phone filters when dialing. **Parameter:** features.call_num_filter
Web User Interface		Configure the characters the IP phone filters when dialing. **Navigate to**:

	http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.call_num_filter	**String within 99 characters**	**?,-( )**

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 = ,-12

If you dial 3-61, the IP phone will filter the characters - and 1, and then dial out 36.

Note: 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:

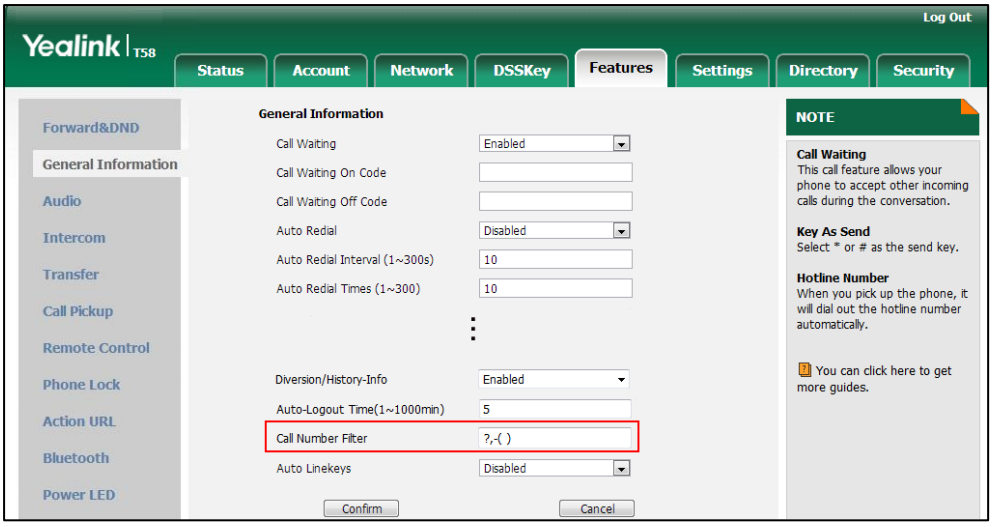
Features->General Information->Call Number Filter

Phone User Interface:

None

To configure the characters the IP phone will filter via web user interface:

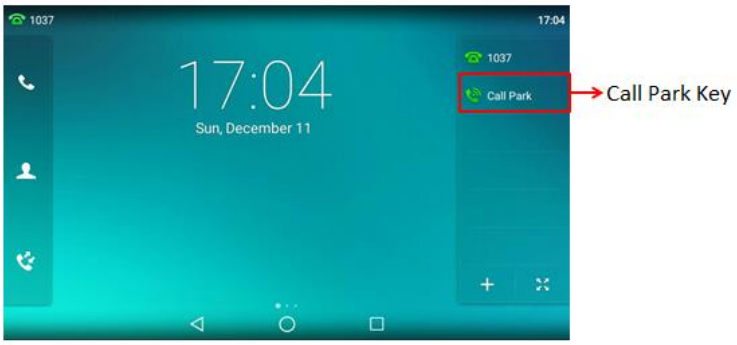
1. Click on **Features**->**General Information**.
2. Enter the desired characters in the **Call Number Filter** field.



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

Call Park

Call park allows users to park a call on a special extension and then retrieve it on any other phone in the system. Users can park calls on the extension, known as call park orbit, by tapping a call park key. If the call is parked successfully, users will hear a voice prompt confirming that the call was parked. The current call is placed on hold and can be retrieved on another IP phone. To retrieve a parked call, dial the call park retrieve code to retrieve the parked call. If the parked call is not retrieved within a period of time assigned by the system, the phone performing call park will receive call back. This feature depends on support from a SIP server.



Procedure

Call park key can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Assign a call park key. **Parameters:** linekey.X.type/ expansion_module.X.key.Y.type linekey.X.line/ expansion_module.X.key.Y.line linekey.X.value/ expansion_module.X.key.Y.value linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Assign a call park key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface		Assign a call park key.

Call Park Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

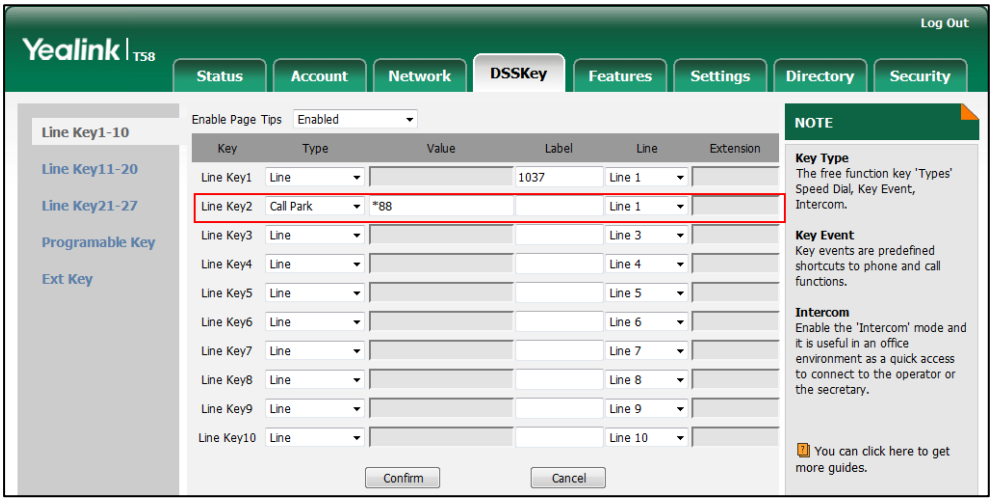
Parameters	Permitted Values	Default
linekey.X.type/ expansion_module.X.key.Y.type	**10**	**Refer to the following content**
Description: Configures a DSS key as a call park key on the IP phone. The digit **10** stands for the key type **Call Park**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 10 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.line/ expansion_module.X.key.Y.line	**Refer to the following content**	**1-16 for lines 1-16**

Parameters	Permitted Values	Default
Description: Configures the desired line to apply the call park key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Permitted Values:** 1 to 16 (for SIP-T58V/T58A/T56A) 1 (for CP960) 1-Line 1 2-Line 2 … 16-Line 16 **Example:** linekey.2.line = 1 **Web User Interface:** DSSKey->Line key->Line **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Account ID		
linekey.X.value/ expansion_module.X.key.Y.value	**String within 99 characters**	**Blank**
Description: Configures the call park feature code. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.value = *88 **Web User Interface:** DSSKey->Line key->Value **Phone User Interface:**		

Parameters	Permitted Values	Default
Settings->Features->DSS Keys->Line Key X->Value		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key ->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a call park key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Ext Key**).
2. In the desired DSS key field, select **Call Park** from the pull-down list of **Type**.
3. Enter the desired value (e.g., call park feature code) in the **Value** field.
4. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
5. Select the desired line from the pull-down list of **Line**.



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

To configure a call park key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.

2. Select the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **Call Park** in the pop-up dialog box.
7. Tap the **Account ID** field.
8. Tap the desired line in the pop-up dialog box.
9. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
10. Enter the desired value (e.g., call park feature code) in the **Value** field.
11. Tap ✓ to accept the change.

Calling Line Identification Presentation (CLIP)

Calling Line Identification Presentation (CLIP) allows IP phones to display the caller identity, derived from a SIP header contained in the INVITE message when receiving an incoming call. IP phones support deriving caller identity from three types of SIP header: From, P-Asserted-Identity (PAI) and Remote-Party-ID (RPID). Identity presentation is based on the identity in the relevant SIP header.

Note If the caller already exists in the local directory, the local contact name assigned to the caller should be preferentially displayed and stored in the call log.

The following sessions show the enhancements of calling line identification presentation according to the calling line identification source configured on the IP phones.

Caller ID source = FROM

1) The IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the calling line identification information will be hidden and the IP phone touch screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the IP phone presents the caller identification derived from the FROM header.

Caller ID source = PAI

1) The IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP phone touch screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the IP phone checks and

presents the caller identification from the P-Asserted-Identity header.

Caller ID source = PAI-FROM

1) The IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP phone touch screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the IP phone checks and presents the caller identification from the P-Asserted-Identity header.

4) If there is not P-Asserted-Identity header in the INVITE request, the IP phone presents the caller identification derived from the FROM header.

Caller ID source = RPID-FROM

1) The IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP phone touch screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the IP phone checks and presents the caller identification from the Remote-Party-ID header.

4) If there is not Remote-Party-ID header in the INVITE request, the IP phone presents the caller identification derived from the FROM header.

Caller ID source = PAI-RPID-FROM

1) The IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP phone touch screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the IP phone checks and presents the caller identification from the P-Asserted-Identity header.

4) If there is not P-Asserted-Identity header in the INVITE request, the IP phone checks and presents the caller identification from the Remote-Party-ID header.

5) If there is not Remote-Party-ID header in the INVITE request, the IP phone presents the caller identification derived from the FROM header.

Caller ID source = RPID-PAI-FROM

1) The IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the INVITE request, the caller identification information will be hidden and the IP phone touch screen presents anonymous.

2) If there is not any Privacy: id header in the INVITE request, the IP phone checks and presents the caller identification from the P-Preferred-Identity header.

3) If there is not P-Preferred-Identity header in the INVITE request, the IP phone checks and presents the caller identification from the Remote-Party-ID header.

4) If there is not Remote-Party-ID header in the INVITE request, the IP phone checks and presents the caller identification from the P-Asserted-Identity header.

5) If there is not P-Asserted-Identity in the INVITE request, the IP phone presents the caller identification derived from the FROM header.

For more information on calling line identification presentation, refer to *Calling and Connected Line Identification Presentation on Yealink IP Phones*.

Procedure

CLIP can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the presentation of the caller identity. **Parameter:** account.X.cid_source
		Specify whether to process Privacy header field. **Parameter:** account.X.cid_source_privacy
		Specify whether to process the P-Preferred-Identity (PPI) header for caller identity presentation. **Parameter:** account.X.cid_source_ppi
Web User Interface		Configure the presentation of the caller identity. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

Details of the Configuration Parameter:

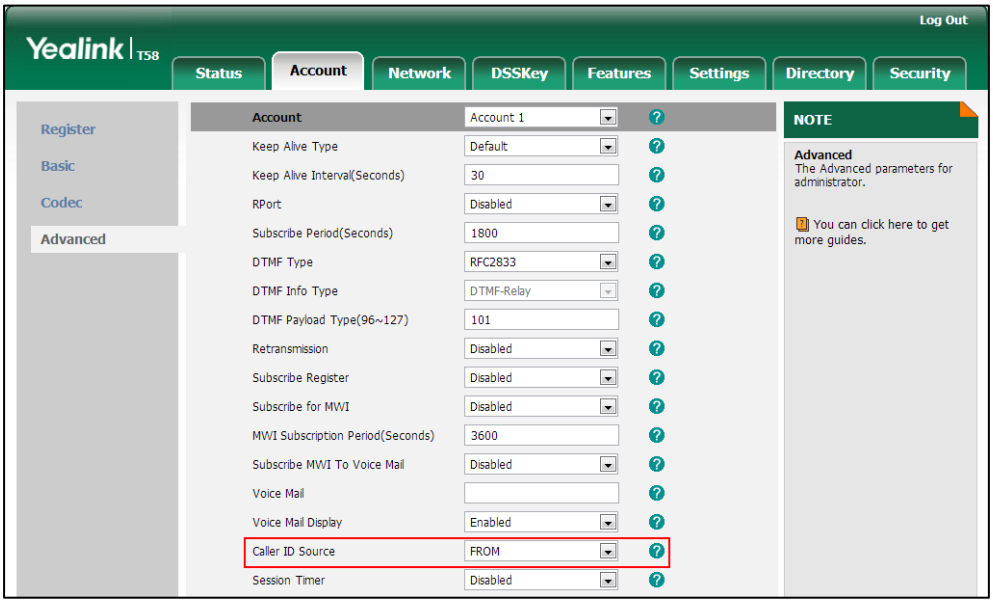
Parameters	Permitted Values	Default
account.X.cid_source	**0, 1, 2, 3, 4 or 5**	**0**
Description: Configures the presentation of the caller identity when receiving an incoming call for		

Parameters	Permitted Values	Default
account X. **0**-FROM **1**-PAI **2**-PAI-FROM **3**-RPID-PAI-FROM **4**-PAI-RPID-FROM **5**-RPID-FROM X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Caller ID Source **Phone User Interface:** None		
account.X.cid_source_privacy	**0 or 1**	**1**
Description: Enables or disables the IP phone to process Privacy header field in the SIP message for account X. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone doesn't process Privacy header. If it is set to 1 (Enabled), the caller identification information will be hidden and the IP phone touch screen presents anonymous if there is a Privacy: id in the INVITE request. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** None **Phone User Interface:** None		
account.X.cid_source_ppi	**0 or 1**	**1**
Description: Enables or disables the IP phone to process the P-Preferred-Identity (PPI) header for caller identity presentation when receiving an incoming call for account X. **0**-Disabled		

Parameters	Permitted Values	Default
1-Enabled If it is set to 0 (Disabled), the IP phone doesn't process P-Preferred-Identity (PPI) header. If it is set to 1 (Enabled), the IP phone presents the caller identification from the P-Asserted-Identity (PPI) header. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** None **Phone User Interface:** None		

To configure the presentation of the caller identity via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Caller ID Source**.



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

Connected Line Identification Presentation (COLP)

Connected Line Identification Presentation (COLP) allows IP phones to display the identity of the connected party specified for outgoing calls. IP phones can display the Dialed Digits, or the identity in a SIP header (Remote-Party-ID or P-Asserted-Identity) received, or the identity in the From header carried in the UPDATE message sent by the callee as described in RFC 4916.

Connected line identification presentation is also known as Called line identification presentation. In some cases, the remote party will be different from the called line identification presentation due to call diversion.

Note If the callee already exists in the local directory, the local contact name assigned to the callee should be preferentially displayed.

The following sessions show the enhancements of connected line identification according to the connected line identification source configured on the IP phones.

Connected Line Identification source = PAI-RPID

1) The IP phone checks Privacy: id header preferentially, if there is a Privacy: id in the 18X or 200OK response, the connected line identification information will be hidden and the IP phone touch screen presents anonymous.

2) If there is not any Privacy: id header in the 18X or 200OK response, the IP phone checks and presents the connected line identification from the P-Asserted-Identity header.

3) If there is not P-Asserted-Identity header in the I8X or 200OK response, the IP phone presents the connected line identification from the Remote-Party-ID header. If no, the IP phone presents the connected line identification according to the dialed digits.

Connected Line Identification source = Dialed digits

Yealink IP phones present the connected line identification according to the dialed digits.

Connected Line Identification source = RFC4916

Yealink IP phones support to present the connected line identification from UPDATE message following the RFC 4916.

1) The IP phone receives an UPDATE message during a call, the connected line identification on the touch screen should be refreshed according the FROM SIP carried in the UPDATE message.

For more information on connected line identification presentation, refer to *Calling and Connected Line Identification Presentation on Yealink IP Phones*.

Procedure

COLP can be configured only using the configuration files.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the presentation of the callee's identity. **Parameter:** account.X.cp_source
		Specify whether to process Privacy header field. **Parameter:**

		account.X.cid_source_privacy

Details of the Configuration Parameters:

Parameters	Permitted Values	Default
account.X.cp_source	**0, 1 or 2**	**0**
Description: Configures the presentation of the callee's identity for account X. **0**-PAI-RPID **1**-Dialed Digits **2**-RFC 4916 When the RFC 4916 is enabled on the IP phone, the caller sends the SIP request message which contains the from-change tag in the Supported header. The caller then receives an UPDATE message from the callee, and displays the identity in the "From" header. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** None **Phone User Interface:** None		
account.X.cid_source_privacy	**0 or 1**	**1**
Description: Enables or disables the IP phone to process Privacy header field in the SIP message for account X. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone doesn't process Privacy header. If it is set to 1 (Enabled), the caller identification information will be hidden and the IP phone touch screen presents anonymous if there is a Privacy: id in the INVITE request. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** None **Phone User Interface:** None		

Mute

Yealink IP phones support muting the microphone of the active audio device (handset, headset or speakerphone) during an active call or while dialing. You can activate the mute feature by pressing the MUTE key. Normally, mute feature is automatically deactivated when the active call ends. You can enable keep mute feature to keep the mute state persist across the calls.

Allow Mute

You can mute the microphone of the active audio device during an active call, and then the other party cannot hear you.

Procedure

Allow mute can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure allow mute feature. **Parameter:** features.allow_mute
Web User Interface		Configure allow mute feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

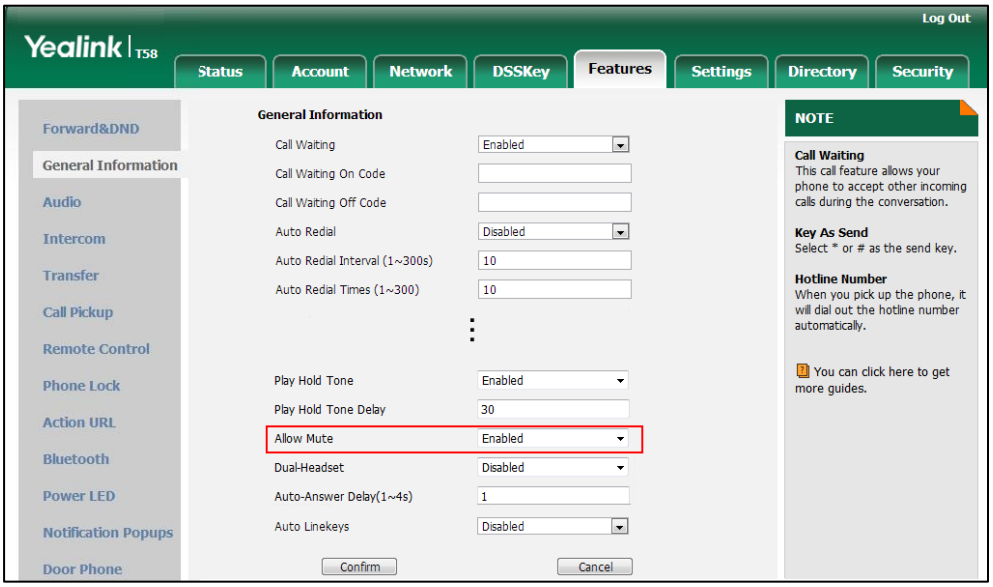
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.allow_mute	**0 or 1**	**1**
Description: Enables or disables the IP phone to mute an active call. **0**-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**.



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

Keep Mute

Keep mute, also known as persistent mute, allows you to keep the mute state of your phone persist across calls. Once the keep mute feature is enabled, you can activate the mute feature by pressing the MUTE key in an idle state or any other states.

By default, the mute feature is automatically deactivated when the active call ends. When you enable keep mute feature and activate the mute feature, the phone stays in the mute state until you press the MUTE key again or until the phone restarts.

Procedure

Keep mute can be configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure keep mute feature. **Parameter:** features.keep_mute.enable

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.keep_mute.enable	**0 or 1**	**Refer to the following content**
Description:		

Parameter	Permitted Values	Default
Enables or disables the keep mute feature for the IP phone. **0**-Disabled **1**-Enabled **For SIP-T58V/T58A/T56A IP phones**: The default value is 0. **For CP960 IP phones**: The default value is 1. If it is set to 0 (Disabled), mute feature is automatically deactivated when the active call ends. If it is set to 1 (Enabled), the mute state can be kept across calls after the mute feature is activated until you manually deactivate the mute feature or the phone restarts. **Note**: For SIP-T58V/T58A/T56A IP phones, if it is set to 1 (Enabled), you cannot customize the Mute key. It works only if the value of the parameter "features.allow_mute" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		

Intercom

Intercom allows establishing an audio conversation directly. The IP phone can answer intercom calls automatically.

Intercom can be also used to monitor a specific user for status changes on IP phones. For example, you can configure an intercom key on a supervisor's phone to monitor the IP phone user status (busy or idle). When the monitored user places a call, a busy indicator on the supervisor's phone indicates that the user's phone is in use. When the monitored user is idle, the supervisor can tap the intercom key to automatically connect with a preconfigured target extension for outgoing intercom calls. When the monitored user receives an incoming call, the supervisor can tap the intercom key to pick up the call directly. To pick up the call, you have to configure the directed call pickup code in advance. You can configure the directed call pickup code when configuring an intercom key.

IP phones support this feature using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265. And this feature depends on support from a SIP server.

Icon indicator (configured as an intercom key)

Icons	Description
	Intercom idle state

Icons	Description
	Intercom ringing state
Callout	Intercom callout state
Talking	Intercom talking state
	Intercom failed state

Outgoing Intercom Calls

Intercom is a useful feature in office environments to quickly connect with an operator or secretary. Users can tap an intercom key to automatically initiate an outgoing intercom call with a remote extension.

Procedure

Intercom can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the intercom subscription. **Parameters:** features.intercom.led.enable features.intercom.subscribe.enable sip.intercom_sub.enable
		Assign an intercom key. **Parameters:** linekey.X.type/ expansion_module.X.key.Y.type linekey.X.line/ expansion_module.X.key.Y.line linekey.X.value/ expansion_module.X.key.Y.value linekey.X.pickup_value/ expansion_module.X.key.Y.pickup_value linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Assign an intercom key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load

Phone User Interface	Assign an intercom key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.intercom.led.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to display different intercom key icons when the status of monitored user changes. **0**-Disabled **1**-Enabled **Note**: It works only if the value of the parameter "features.intercom.subscribe.enable" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		
features.intercom.subscribe.enable	**0 or 1**	**0**
Description: For SIP-T58V/T58A/T56A IP phones: Enables or disables intercom subscription for the IP phone. For CP960 IP phones: Enables or disables the IP phone to update corresponding information according to the status returned by the intercom subscription. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
sip.intercom_sub.enable	**0 or 1**	**0**
Description: Enables or disables intercom subscription for the IP phone.		

Parameters	Permitted Values	Default
0-Disabled **1**-Enabled **Note**: It is only applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		

Intercom Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ expansion_module.X.key.Y.type	**14**	**Refer to the following content**
Description: Configures a DSS key as an intercom key. The digit **14** stands for the key type **Intercom**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 14 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For ext keys:		

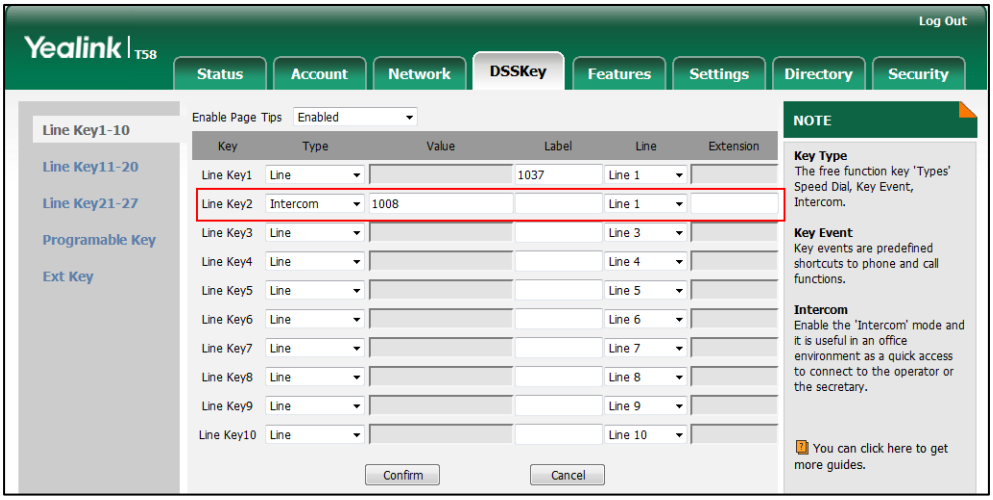
Parameters	Permitted Values	Default
For SIP-T58V/T58A/T56A IP phones: When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.line/ expansion_module.X.key.Y.line	**Refer to the following content**	**1-16 for lines 1-16**
Description: Configures the desired line to apply the intercom key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Permitted Values:** 1 to 16 (for SIP-T58V/T58A/T56A) 1 (for CP960) 1-Line 1 2-Line 2 … 16-Line 16 **Example:** linekey.2.line = 1 **Web User Interface:** DSSKey->Line key->Line **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Account ID		
linekey.X.value/ expansion_module.X.key.Y.value	**String within 99 characters**	**Blank**
Description: Configures the intercom number. For line keys:		

Parameters	Permitted Values	Default
X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.value = 1008 **Web User Interface:** DSSKey->Line key->Value **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Value		
linekey.X.pickup_value/ expansion_module.X.key.Y.pickup_value	**String within 256 characters**	**Blank**
Description: Configures the pickup code for BLF feature, intercom feature. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** line.2.pickup_value = *88 **Note:** This parameter only applies to BLF/intercom feature. **Web User Interface:** DSSKey->Line Key->Extension **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Extension		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys:		

Parameters	Permitted Values	Default
X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure an intercom key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Ext Key**).
2. In the desired DSS key field, select **Intercom** from the pull-down list of **Type**.
3. Enter the remote extension number in the **Value** field.
4. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
5. (Optional.) Enter the directed call pickup code in the **Extension** field.
6. Select the desired line from the pull-down list of **Line**.



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

To configure an intercom key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Select the desired DSS key.
3. Tap the **Type** field.
4. Tap **Intercom** in the pop-up dialog box.
5. Tap the **Account ID** field.
6. Tap the desired line in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Enter the remote extension number in the **Value** field.
9. (Optional.) Enter the directed call pickup code in the **Extension** field.

10. Tap ✔ to accept the change.

Incoming Intercom Calls

The IP phone can process incoming calls differently depending on settings. There are four configuration options for incoming intercom calls:

Accept Intercom

Accept Intercom allows the IP phone to answer an incoming intercom call.

Intercom Mute

Intercom Mute allows the IP phone to mute the microphone for incoming intercom calls.

Intercom Tone

Intercom Tone allows the IP phone to play a warning tone before answering an intercom call.

Intercom Barge

Intercom Barge allows the IP phone to automatically answer an incoming intercom call while an active call is in progress. The active call will be placed on hold.

If you disable this feature, the IP phone will handle an incoming intercom call like a waiting call while there is already an active call on the IP phone.

Procedure

Incoming intercom calls can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure incoming intercom call feature. **Parameters:** features.intercom.allow features.intercom.mute features.intercom.tone features.intercom.barge
Web User Interface		Configure incoming intercom call feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-intercom&q=load
Phone User Interface		Configure incoming intercom call feature.

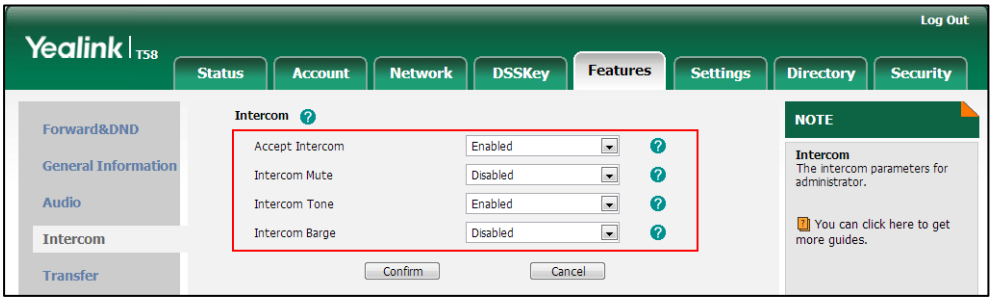
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.intercom.allow	**0 or 1**	**1**
Description: Enables or disables the IP phone to answer an incoming intercom call. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone will reject incoming intercom calls and sends a busy signal (configured by the parameter "features.normal_refuse_code") to the caller. If it is set to 1 (Enabled), the IP phone will automatically answer an incoming intercom call. **Web User Interface:** Features->Intercom->Accept Intercom **Phone User Interface:** Settings->Features->Intercom->Accept Intercom		
features.intercom.mute	**0 or 1**	**0**
Description: Enables or disables the IP phone to mute the microphone when answering an intercom call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the microphone is muted for intercom calls, and then the other party cannot hear you. **Note:** It works only if the value of the parameter "features.intercom.allow" is set to 1 (Enabled). **Web User Interface:** Features->Intercom->Intercom Mute **Phone User Interface:** Settings->Features->Intercom->Intercom Mute		
features.intercom.tone	**0 or 1**	**1**
Description: Enables or disables the IP phone to play a warning tone when answering an intercom call. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "features.intercom.allow" is set to 1		

Parameters	Permitted Values	Default
(Enabled). **Web User Interface:** Features->Intercom->Intercom Tone **Phone User Interface:** Settings->Features->Intercom->Intercom Tone		
features.intercom.barge	**0 or 1**	**0**
Description: Enables or disables the IP phone to answer an incoming intercom call while there is already an active call on the IP phone. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone will handle an incoming intercom call like a waiting call while there is already an active call on the IP phone. If it is set to 1 (Enabled), the IP phone will automatically answer the intercom call while there is already an active call on the IP phone and place the active call on hold. **Note:** It works only if the values of parameters "features.intercom.allow" and "call_waiting.enable" are set to 1 (Enabled). **Web User Interface:** Features->Intercom->Intercom Barge **Phone User Interface:** Settings->Features->Intercom->Intercom Barge		

To configure intercom via web user interface:

1. Click on **Features**->**Intercom**.
2. Select the desired values from the pull-down lists of **Accept Intercom**, **Intercom Mute**, **Intercom Tone** and **Intercom Barge**.



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

To configure intercom via phone user interface:

1. Tap **Settings**->**Features**->**Intercom**.
2. Tap the desired values in the **Accept Intercom**, **Intercom Mute**, **Intercom Tone** and **Intercom Barge** fields.
3. Tap ✔ to accept the change.

Call Timeout

Call timeout defines a specific period of time within which the IP phone will cancel the dialing if the call is not answered.

Procedure

Call timeout can only be configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the duration time in the ringback state. **Parameter:** phone_setting.ringback_timeout

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.ringback_timeout	**Integer from 0 to 3600**	**180**
Description: Configures the duration time (in seconds) in the ringback state. If it is set to 180, the phone will cancel the dialing if the call is not answered within 180 seconds. **Web User Interface:** None **Phone User Interface:** None		

Ringing Timeout

Ringing timeout defines a specific period of time within which the IP phone will stop ringing if the call is not answered.

Procedure

Ringing timeout can only be configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the duration time in the ringing state. **Parameter:** phone_setting.ringing_timeout

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
phone_setting.ringing_timeout	**Integer from 0 to 3600**	**120**
Description: Configures the duration time (in seconds) in the ringing state. If it is set to 180, the phone will stop ringing if the call is not answered within 180 seconds. **Web User Interface:** None **Phone User Interface:** None		

Send user=phone

When placing a call, the IP phone will send an INVITE request to the proxy server. Send user=phone feature allows adding user=phone to the SIP header of the INVITE message.

Example of a SIP INVITE message:

```
INVITE sip:101@10.2.1.48:5060;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.3.20.6:5060;branch=z9hG4bK2475812834
From: "1010" <sip:1010@10.2.1.48:5060>;tag=3747068208
To: <sip:101@10.2.1.48:5060;user=phone>
Call-ID: 0_4008470062@10.3.20.6
CSeq: 1 INVITE
Contact: <sip:1010@10.3.20.6:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Allow-Events: talk,hold,conference,refer,check-sync
```

Content-Length: 300

Procedure

Send user=phone can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure send user=phone feature on a per-line basis. **Parameter:** account.X.enable_user_equal_phone
Web User Interface		Configure send user=phone feature on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

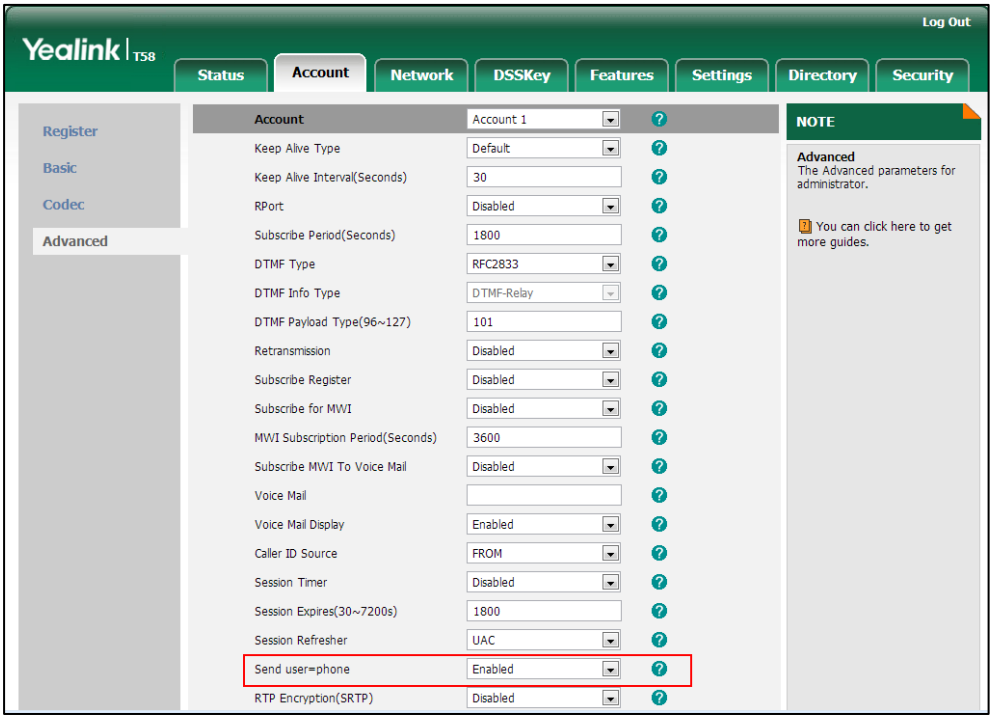
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.enable_user_equal_phone	**0 or 1**	**0**
Description: Enables or disables the IP phone to add "user=phone" to the SIP header of the INVITE message for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Send user=phone **Phone User Interface:** None		

To configure send user=phone feature via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

3. Select the desired value from the pull-down list of **Send user=phone**.



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

SIP Send MAC

The IP phone can send the MAC address in the REGISTER message. SIP send MAC allow adding "Mac:<PhoneMACAddress>" (e.g., Mac: 00:15:65:74:b1:50) to the SIP header of the REGISTER message.

Example of a SIP REGISTER message:

```
REGISTER sip:10.2.1.48:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK3593117201
From: "11" <sip:11@10.2.1.48:5060>;tag=2788360609
To: "11" <sip:11@10.2.1.48:5060>
Call-ID: 1_1863786852@10.3.20.14
CSeq: 2 REGISTER
Contact: <sip:11@10.3.20.14:5060;line=cc75882e976e208>
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Expires: 0
Allow-Events: talk,hold,conference,refer,check-sync
Mac: 00:15:65:74:b1:50
```

Content-Length: 0

Procedure

SIP send MAC can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure SIP send MAC on a per-line basis. **Parameter:** account.X.register_mac
Web User Interface		Configure SIP send MAC on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

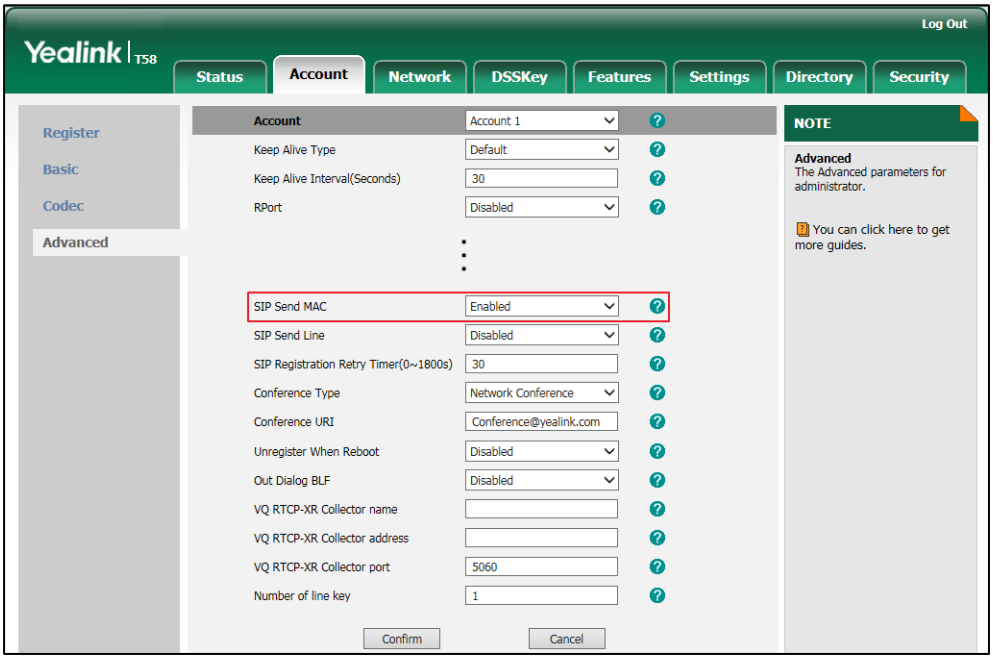
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.register_mac	**0 or 1**	**0**
Description: Enables or disables the IP phone to add MAC address to the SIP header of the REGISTER message for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->SIP Send MAC **Phone User Interface:** None		

To configure SIP send MAC feature via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

3. Select the desired value from the pull-down list of **SIP Send MAC**.



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

SIP Send Line

The IP phone can send the line number in the REGISTER message. SIP send line allow adding "Line:<linenumber>"(e.g., Line: 1) to the SIP header of the REGISTER message. The line number is a number between 0 and 15.

The following table lists line number values for each phone model.

Phone Model	Line Number	Description
SIP-T58V/T58A/T56A	0~15	0~15 stand for line1~line16
CP960	0	0 stand for line1

Example of a SIP REGISTER message:

```
REGISTER sip:10.2.1.48:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK3990593443
From: "11" <sip:11@10.2.1.48:5060>;tag=255071842
To: "11" <sip:11@10.2.1.48:5060>
Call-ID: 1_2369214377@10.3.20.14
CSeq: 2 REGISTER
Contact: <sip:11@10.3.20.14:5060;line=1da6aa8d7254654>
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
```

```
Expires: 0
Allow-Events: talk,hold,conference,refer,check-sync
Line: 1
Content-Length: 0
```

Procedure

SIP send line can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure SIP send line on a per-line basis. **Parameter:** account.X.register_line
Web User Interface		Configure SIP send line on a per-line basis. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

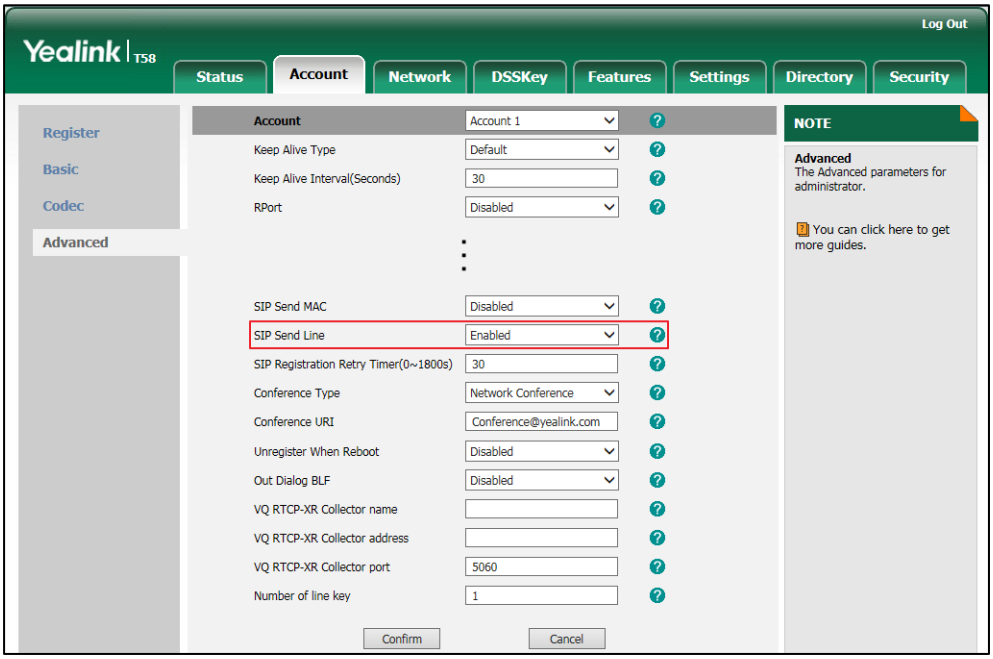
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.register_line	**0 or 1**	**0**
Description: Enables or disables the IP phone to add line number to the SIP header of the REGISTER message for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->SIP Send Line **Phone User Interface:** None		

To configure SIP send Line feature via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

3. Select the desired value from the pull-down list of **SIP Send Line**.



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

Reserve # in User Name

Reserve # in User Name feature allows IP phones to reserve "#" in user name. When Reserve # in User Name feature is disabled, "#" will be converted into "%23". For example, the user registers an account (user name: 1010#) on the phone, the phone will send 1010%23 instead of 1010# in the REGISTER message or INVITE message to SIP server.

Example of a SIP REGISTER message:

```
INVITE sip:2@10.2.1.48:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.6:5060;branch=z9hG4bK1867789050
From: "1010" <sip:1010%23@10.2.1.48:5060>;tag=1945988802
To: <sip:2@10.2.1.48:5060>
Call-ID: 0_2336101648@10.3.20.6
CSeq: 1 INVITE
Contact: <sip:1010%23@10.3.20.6:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length:  300
```

Procedure

Reserve # in User Name can be configured using the following methods.

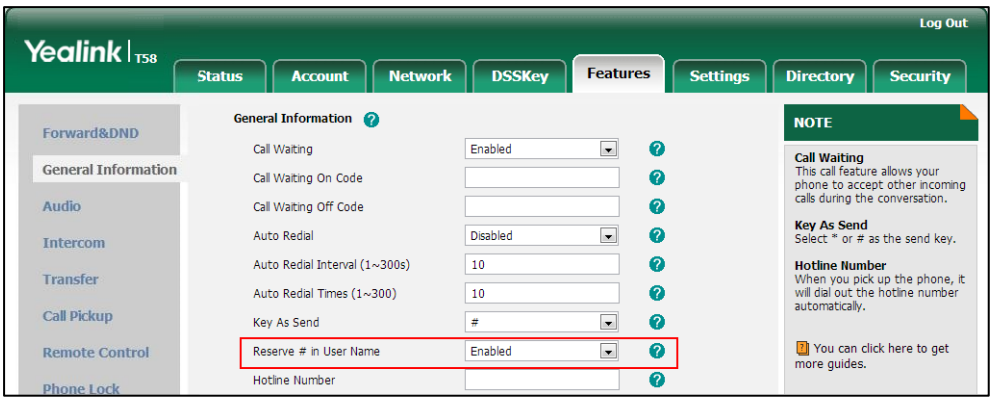
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure reserve # in user name. **Parameter:** sip.use_23_as_pound
Web User Interface		Configure reserve # in user name. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.use_23_as_pound	**0 or 1**	**1**
Description: Enables or disables the IP phone to reserve the pound sign (#) in the user name. **0**-Disabled (convert the pound sign into "%23") **1**-Enabled **Web User Interface:** Features->General Information->Reserve # in User Name **Phone User Interface:** None		

To configure reserve # in user name feature via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **Reserve # in User Name**.



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

Password Dial

Password dial feature allows the callee number to be partly displayed on the IP phone when placing a call. The hidden digits are displayed as asterisks on the touch screen. This feature is especially useful for users always placing important and confidential calls.

Procedure

Password dial feature can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure password dial feature. **Parameters:** features.password_dial.enable features.password_dial.prefix features.password_dial.length
Web User Interface		Configure password dial feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of the Configuration Parameters:

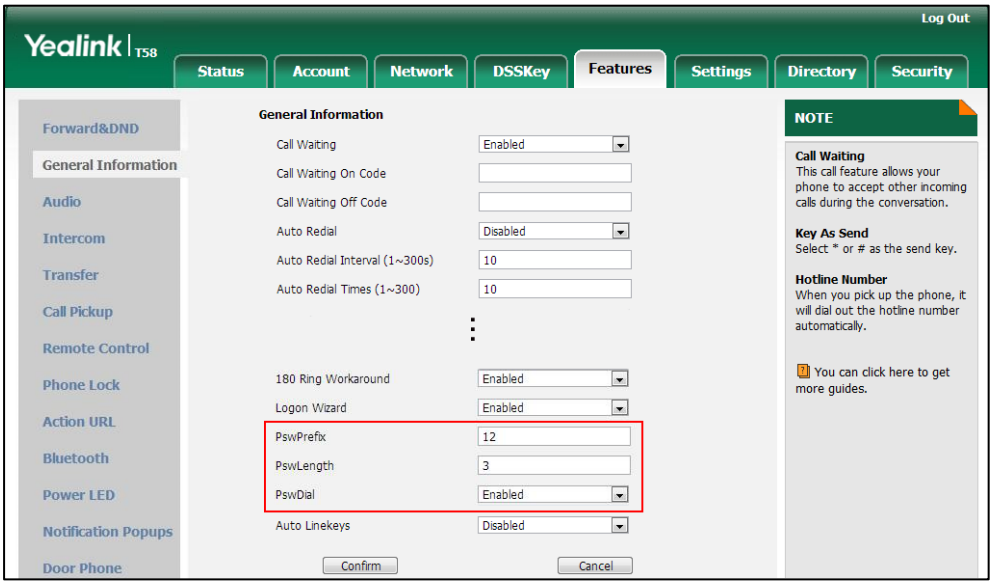
Parameters	Permitted Values	Default
features.password_dial.enable	**0 or 1**	**0**
Description: Enables or disables password dial feature for the IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->PswDial **Phone User Interface:** None		
features.password_dial.prefix	**String within 32 characters**	**Blank**
Description: Configures the prefix of the password dial number. **Example**: features.password_dial.prefix = 12		

Parameters	Permitted Values	Default
Web User Interface: Features->General Information->PswPrefix **Phone User Interface:** None		
features.password_dial.length	**Integer from 0 to 99**	**Blank**
Description: Configures the number of digits to be hidden. The hidden digits are displayed as asterisks on the touch screen. **Example**: features.password_dial.length = 3 If you set the prefix to 12 (configured by the parameter "features.password_dial.prefix") and the length to 3, when you want to dial the number 123456, the entered number is displayed as 12***6 on the touch screen. **Web User Interface:** Features->General Information->PswLength **Phone User Interface:** None		

To configure password dial feature via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired value from the pull-down list of **PswDial**.
3. Enter the prefix of password dial in the **PswPrefix** field.

4. Enter the desired number of hidden digits in the **PswLength** field.



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

Unregister When Reboot

Unregister when reboot feature allows IP phones to unregister first before re-registering the account when finishing a reboot.

Procedure

Unregister when reboot can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure unregister when reboot. **Parameter:** account.X.unregister_on_reboot
Web User Interface		Configure unregister when reboot. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

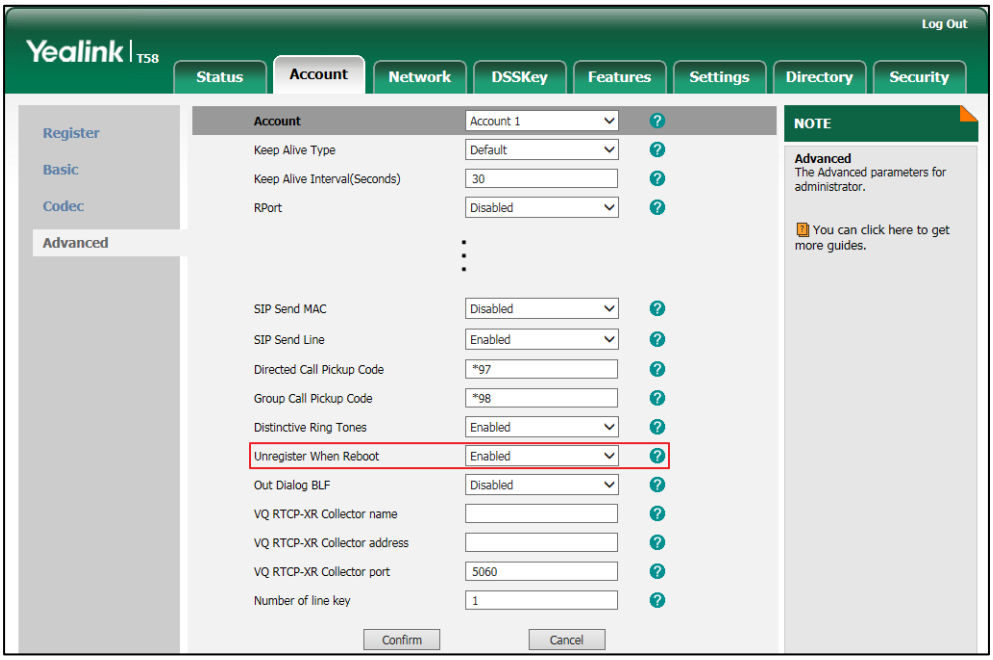
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.unregister_on_reboot	**0 or 1**	**0**
Description: Enables or disables the IP phone to unregister first before re-registering account X when		

Parameter	Permitted Values	Default
finishing a reboot. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Unregister When Reboot **Phone User Interface:** None		

To configure unregister when reboot via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Unregister When Reboot**.



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

100 Reliable Retransmission

As described in RFC 3262, 100rel tag is for reliability of provisional responses. When present in a Supported header, it indicates that the IP phone can send or receive reliable provisional responses. When present in a Require header in a reliable provisional response, it indicates that the response is to be sent reliably.

Example of a SIP INVITE message:

```
INVITE sip:1024@pbx.yealink.com:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.6.197:5060;branch=z9hG4bK1708689023
From: "1025" <sip:1025@pbx.yealink.com:5060>;tag=1622206783
To: <sip:1024@pbx.yealink.com:5060>
Call-ID: 0_537569052@10.3.6.197
CSeq: 2 INVITE
Contact: <sip:1025@10.3.6.197:5060>
Authorization: Digest username="1025", realm="pbx.yealink.com", nonce="BroadWorksXi5stub71Ts2nb05BW",
uri="sip:1024@pbx.yealink.com:5060", response="f7e9d35c55af45b3f89beae95e913171", algorithm=MD5,
cnonce="0a4f113b", qop=auth, nc=00000001
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH,
UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Supported: 100rel
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length:    302
```

Procedure

100 Reliable Retransmission can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the 100 reliable retransmission feature. **Parameter:** account.X.100rel_enable
Web User Interface		Configure the 100 reliable retransmission feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

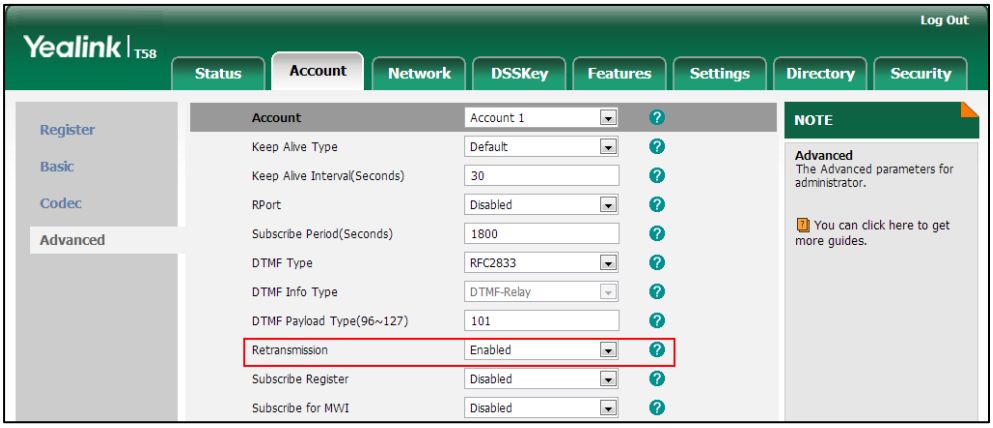
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.100rel_enable	**0 or 1**	**0**
Description: Enables or disables the 100 reliable retransmission feature for account X.		

Parameter	Permitted Values	Default
0-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Retransmission **Phone User Interface:** None		

To configure 100 reliable retransmission via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Retransmission**.



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

Reboot in Talking

Reboot in talking feature allows IP phones to reboot during an active call when it receives a reboot request by action URI. For more information on action URI, refer to Action URI on page 560.

IP phones do not receive and handle HTTP/HTTPS GET requests by default. To use this feature, you need to specify the trusted IP address(es) for action URI in advance. For more information, refer to Configuring Trusted IP Address for Action URI on page 564.

Procedure

Reboot in talking can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure reboot in talking. **Parameter:** features.reboot_in_talk_enable
Web User Interface		Configure reboot in talking. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

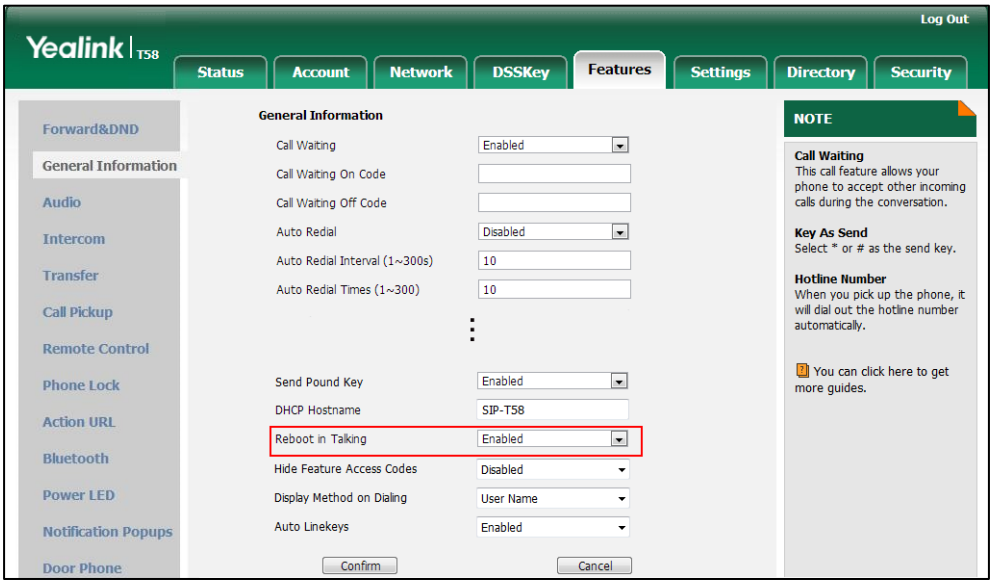
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.reboot_in_talk_enable	**0 or 1**	**0**
Description: Enables or disables the phone to reboot during a call when it receives a reboot request by action URI. **0**-Disabled **1**-Enabled **Note**: It works only if the value of the parameter "features.action_uri_limit_ip" is set to "any" or trusted IP address(es) and it is not the first time for the IP phone to receive HTTP/HTTPS GET request from the trusted IP address(es). **Web User Interface:** Features->General Information->Reboot in Talking **Phone User Interface:** None		

To configure reboot in talking via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **Reboot in Talking**.



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

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

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

Answer By Hand

Answer by hand feature allows you to answer an incoming call by picking up the handset, pressing the Speakerphone key or pressing the HEADSET key directly. It is not applicable to CP960 IP phones.

If you disable answer by hand feature, you need to tap the corresponding line key or the **Answer** soft key to answer an incoming call after picking up the handset, pressing the Speakerphone key or pressing the HEADSET key.

Procedure

Answer by hand can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure answer by hand. **Parameter:** features.off_hook_answer.enable

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.off_hook_answer.enable	**0 or 1**	**1**

Parameter	Permitted Values	Default
Description: Enables or disables the IP phone to answer an incoming call by picking up the handset, pressing the Speakerphone key or pressing the HEADSET key directly. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), you need to tap the corresponding line key or the **Answer** soft key to answer an incoming call after picking up the handset, pressing the Speakerphone key or pressing the HEADSET key. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		

Call Recording Using Soft Key

Yealink IP phones support recording calls (audio-only calls or video calls) or conferences during a call. By default, the recorded files are saved in the internal SD card. You can also save the recorded files in the connected USB flash drive. For SIP-T58V/T58A/T56A IP phones, if you connect the USB flash drive to the IP phone, the recorded files will be saved according to the priority: USB flash drive >Internal SD card. For CP960 IP phones, if you connect the USB flash drive to the IP phone, you can choose to save the recorded files to the Internal SD card or USB flash drive.

In addition, the IP phones allow users to record audio and access audio recording files by **Recorder** application. For more information, refer to *Yealink phone-specific user guide*.

You can also record audio-only calls by tapping record/URL record key. For more information, refer to Record and URL Record on page 524.

Note Before recording any call, especially those involving PSTN, it is necessary to know about the rules and restrictions of any governing call-recording in the place you are in. It is also very important to have the consent of the person you are calling before recording the conversation.

Procedure

Call recording feature can be only configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the recording feature. **Parameter:**

		features.call_recording.enable

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.call_recording.enable	**0 or 1**	**1**
Description: Enables or disables the call recording feature for the IP phone. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), you can record the audio or video call by tapping the **Record** soft key (for SIP-T58V/T58A/T56A)/ (for CP960) during a call. **Note**: To save the recorded files to the USB flash drive, make sure the USB flash drive has been connected to the IP phone in advance. **Web User Interface:** None **Phone User Interface:** None		

Silent Mode

You can use silent mode feature to block the incoming call/message from producing ring tone/notification tone from phone's speaker. It is helpful for users not to be disturbed by the tone.

Yealink IP phones support the following three methods to enable the silent mode feature:

- Turn on the silent mode via phone user interface at the path: **Settings**->**Basic**->**Sound**.
- Swipe down from the top of the screen to enter the control center, tap **Silent**.
- Press the Volume key to adjust the ringer volume to the minimum.

By default, the users can enable or disable the silent mode. You can disable the users to configure it.

Procedure

Silent mode permission can be configured using the following method.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify whether the users have the permission to configure the silent mode feature. **Parameter:** phone_setting.permit_silent_mode.enable

Details of the Configuration Parameter:

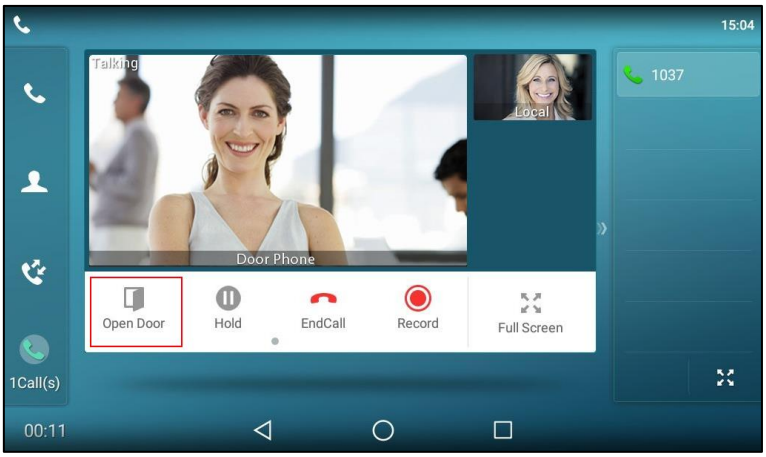
Parameter	Permitted Values	Default
phone_setting.permit_silent_mode.enable	**0 or 1**	**1**
Description: Enables or disables the user to have the permission to use the silent mode feature. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the **Silent Mode** item will disappear from the phone user interface at the path: **Settings**->**Basic**->**Sound**. Users can neither enable the silent mode feature from the control center or via phone user interface, nor adjust the ringer volume to minimum. **Web User Interface:** None **Phone User Interface:** None		

Door Phone

Door phone is used to control the opening of the door giving access to any kind of buildings, offices, or apartment blocks. You can control the opening of the door on the IP phone. The IP phone is only compatible with the door phone of 2N. It is not applicable to CP960 IP phones.

You can pair up to two door phones on the IP phone. You can also configure call settings for the door phone call.

When the doorbell key on the door phone is pressed, the IP phone will ring. After answering the call, you can tap the **Open Door** soft key to open the door.



In addition to the IP phone, door phone should be configured. For more information on how to configure the door phone, refer to the documentation from the 2N.

Procedure

Door phone settings can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the door phone information. **Parameters:** features.doorphone.X.display_name features.doorphone.X.phone_number
		Configure the unlock PIN of the door phone. **Parameter:** features.doorphone.X.unlock_pin
		Configure the call settings for door phone call. **Parameters:** features.doorphone.X.full_screen features.doorphone.X.send_audio features.doorphone.X.send_video
Web User Interface		Configure the door phone information. Configure the unlock PIN of the door phone. Configure the call settings between the door phone and IP phone.

	Navigate to: http://<phoneIPAddress>/servlet?m=mod_data&p=features-doorphone&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.doorphone.X.display_name (X ranges from 1 to 2)	**String within 99 characters**	**Blank**
Description: Configures the display name to be displayed on the IP phone's screen for door phone. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Door Phone->Display Name **Phone User Interface:** None		
features.doorphone.X.phone_number (X ranges from 1 to 2)	**String within 32 characters**	**Blank**
Description: Configures the phone number of the door phone. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Door Phone->Phone Number **Phone User Interface:** None		
features.doorphone.X.unlock_pin (X ranges from 1 to 2)	**String within 99 characters**	**Blank**
Description: Configures the unlock PIN. The unlock PIN is the switch code of the door phone plus "*". You should configure the switch code as DTMF mode on the door phone. **Example:** features.doorphone.1.unlock_pin=8888* **Note**: It is not applicable to CP960 IP phones. **Web User Interface:**		

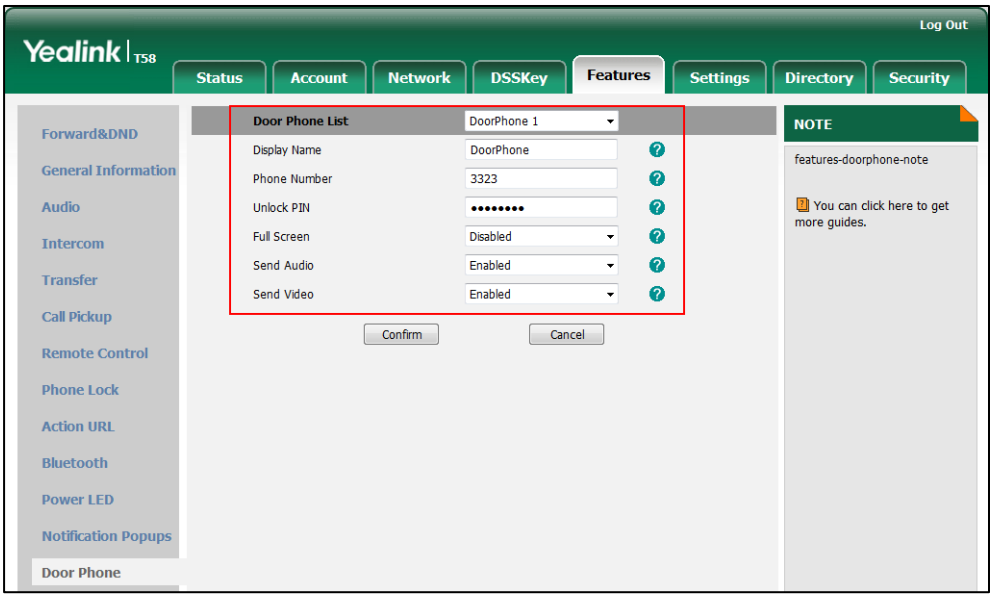
Features->Door Phone->Unlock PIN **Phone User Interface:** None		
features.doorphone.X.full_screen (X ranges from 1 to 2)	**0 or 1**	**0**
Description: Enables or disables the IP phone to display the door phone call in full-screen mode automatically. **0**-Disabled **1**-Enabled **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Door Phone->Full Screen **Phone User Interface:** None		
features.doorphone.X.send_audio (X ranges from 1 to 2)	**0 or 1**	**1**
Description: Enables or disables the IP phone to transmit audio during a door phone call. **0**-Disabled **1**-Enabled **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Door Phone->Send Audio **Phone User Interface:** None		
features.doorphone.X.send_video (X ranges from 1 to 2)	**0 or 1**	**1**
Description: Enables or disables the IP phone to transmit your video during a door phone call. **0**-Disabled **1**-Enabled **Note:** It is not applicable to SIP-T56A/CP960 IP phones. **Web User Interface:** Features->Door Phone->Send Video **Phone User Interface:**		

None

To configure allow mute via web user interface:

1. Click on **Features**->**Door Phone**.
2. Select the desired door phone from the pull-down list of **Door Phone List**.
3. Enter the display name of the door phone in the **Display Name** field.
4. Enter the number of the door phone in the **Phone Number** field.

   If you leave it blank or enter the wrong number, the IP phone will take the incoming door phone call as a normal call.
5. Enter the unlock PIN in the **Unlock PIN** field.
6. Select the desired value from the pull-down list of **Full Screen**.
7. Select the desired value from the pull-down list of **Send Audio**.
8. Select the desired value from the pull-down list of **Send Video**.



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

Mobile Account

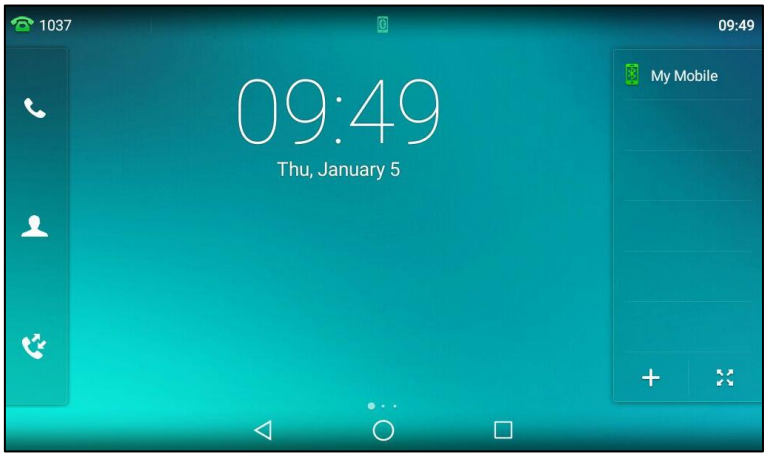
Yealink IP phones support connecting a Bluetooth-enabled mobile phone. After connection, the IP phone will automatically find an available DSS key and assign the DSS key for Mobile Account. The Mobile Account key's default label is "My Mobile". If there is no available DSS key, you may assign it manually.

The Mobile Account key can be used in the following scenarios:

- Accept the incoming mobile call if there is an incoming call to your mobile phone.
- Make a call through a mobile phone. But the IP phone acts as a hands free device for your mobile phone.

- Reconnect the last paired Bluetooth-Enabled mobile phone if the distance between mobile phone and IP phone is more than 10 meters or the Bluetooth mode on the mobile phone is deactivated.

The following shows the IP phone automatically assigns a Mobile Account key:



For more information on how to use your phone in conjunction with Bluetooth-enabled mobile phone, refer to the *Yealink phone-specific user guide*.

Procedure

Mobile account key can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Assign a mobile account key. **Parameters:** linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Assign a mobile account key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface		Assign a mobile account key.

Mobile Account Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Mobile account key can be configured only if the mobile phone has been connected successfully.

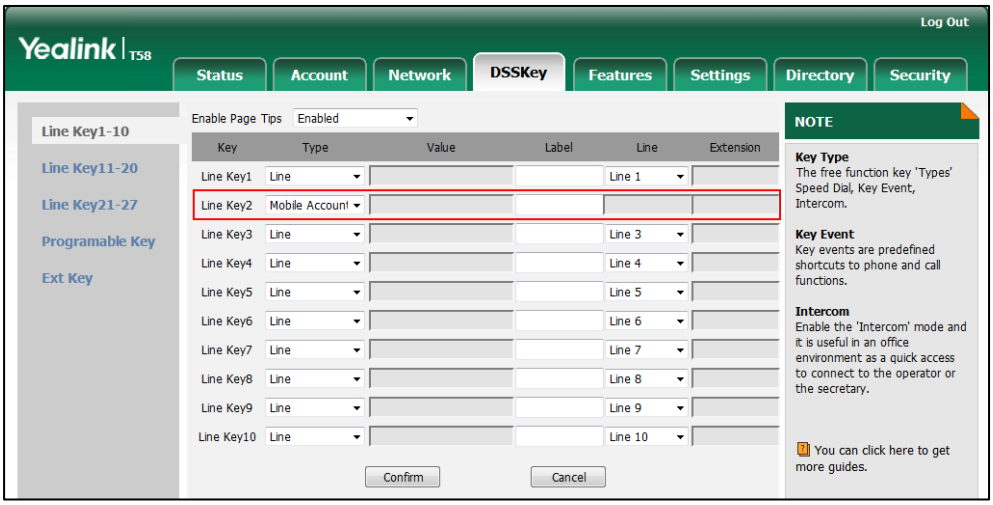
Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type</td><td>77</td><td>Refer to the following content</td></tr>
<tr><td colspan="3">Description:
Configures a DSS key as an XML Browser key on the IP phone.
The digit 77 stands for the key type Mobile Account.
For line keys:
X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)
X ranges from 1 to 30 (for CP960)
For ext keys:
X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)
Example:
linekey.2.type =77
Default:
For line keys:
For SIP-T58V/T58A/T56A IP phones:
The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0.
For CP960 IP phones:
The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0.
For programable keys:
For SIP-T58V/T58A/T56A IP phones:
When X=12, the default value is 0 (NA).
When X=13, the default value is 0 (NA).
When X=14, the default value is 2 (Forward).
For ext keys:
For SIP-T58V/T58A/T56A IP phones:
When Y= 1 to 60, the default value is 0 (NA).
Web User Interface:
DSSKey->Line Key/Programable Key/Ext Key->Type
Phone User Interface:
Settings->Features->DSS Keys->Line Key X->Type</td></tr>
<tr><td>linekey.X.label/ expansion_module.X.key.Y.label</td><td>String within 99 characters</td><td>Blank</td></tr>
</table>

Parameters	Permitted Values	Default
Description: (Optional.) Configures the label displayed on the LCD screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key/Ext Key->Label **Phone User Interface:** Setting->Features->DSS Keys->Line Key X->Label		

To configure a mobile account key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **Mobile Account** from the pull-down list of **Type**.
3. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.



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

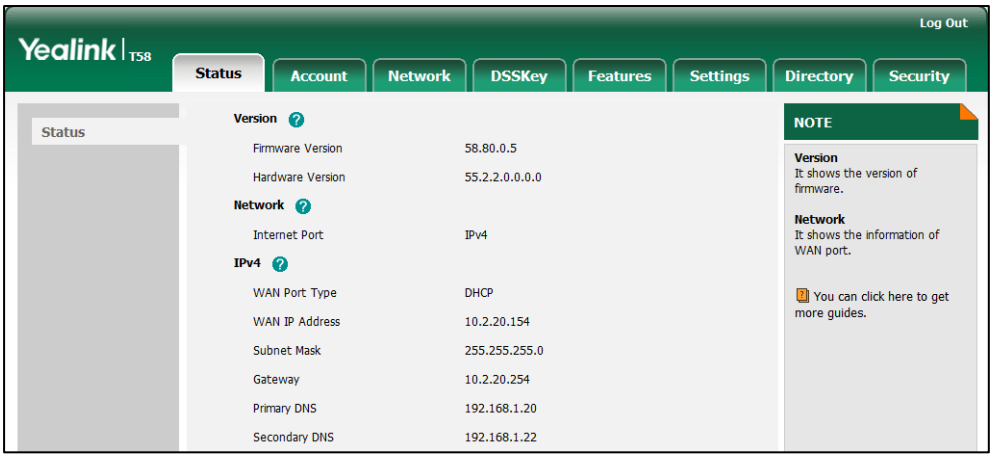
To configure a call park key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Select the desired DSS key.
3. Tap the **Type** field.
4. Tap **Mobile Account** in the pop-up dialog box.
5. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.

6. Tap ✓ to accept the change.

Quick Login

Quick login feature allows users to fast access to web user interface using the request URI "https://username:password@phoneIPAddress" (e.g., https://admin:admin@192.168.0.10). You will navigate to the **Status** web page after accessing the web user interface. It is helpful for users to quickly log into the web user interface without entering the username and password in the login page.



Note The use of the quick login feature may be restricted by the web explorer (e.g., Internet Explorer). For security purposes, we recommend you to use this feature in a secure network environment.

Procedure

Quick login can be configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure quick login. **Parameter**: wui.quick_login

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
wui.quick_login	**0 or 1**	**0**
Description: Enables or disables the quick login feature. **0**-Disabled **1**-Enabled		

Parameter	Permitted Values	Default
If it is set to 1 (Enabled), you can quickly log into the web user interface using a request URI (e.g., https://admin:admin@192.168.0.10). **Note**: It works only if the value of the parameter "static.wui.https_enable" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		

CSTA Control

User Agent Computer Supported Telecommunications Applications (uaCSTA) is explained in detail in Using CSTA for SIP Phone User Agents (uaCSTA) and Services for Computer Supported Telecommunications Applications Phase III.

The uaCSTA feature on the phone may be used for remote control of the phone from computer applications such as PC softphone. You can use the application to control the phone to perform basic call operations. For example, place a call, answer a call, end a call and transfer a call to another party.

It is only applicable to CP960 IP phones.

Procedure

The uaCSTA feature can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure uaCSTA feature. **Parameter:** features.csta_control.enable
Web User Interface		Configure uaCSTA feature. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-remotecontrl&q=load

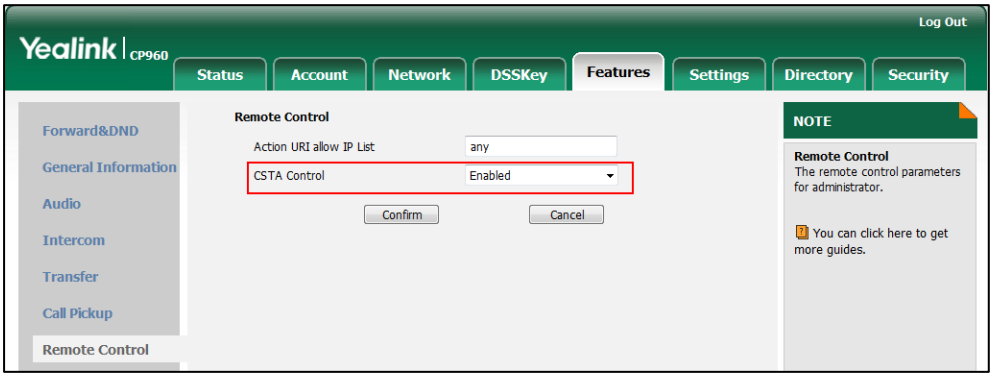
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.csta_control.enable	**0 or 1**	**0**
Description:		

Parameter	Permitted Values	Default
Enables or disables the uaCSTA (User Agent Computer Supported Telecommunications Applications) feature on the IP phone. **0**-Disabled **1**-Enabled **Note**: It is only applicable to CP960 IP phones. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Features->Remote Control->CSTA Control **Phone User Interface:** None		

To configure uaCSTA feature via web user interface:

1. Click on **Features**->**Remote Control**.
2. Select the desired value from the pull-down list of the **CSTA Control**.



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 phone.

Configuring Advanced Features

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

- Remote Phone Book
- Lightweight Directory Access Protocol (LDAP)
- Busy Lamp Field (BLF)
- Busy Lamp Field (BLF) List
- Hide Feature Access Codes
- Shared Call Appearance (SCA)
- Message Waiting Indicator (MWI)
- Multicast Paging
- Call Recording Using DSS Keys (Record and URL Record)
- Hot Desking
- Logon Wizard
- Action URL
- Action URI
- Server Redundancy
- Static DNS Cache
- Real-Time Transport Protocol (RTP) Ports
- TR-069 Device Management

Remote Phone Book

Remote phone book is a centrally maintained phone book, stored on the remote server. Users only need the access URL of the remote phone book. The IP phone can establish a connection with the remote server and download the phone book, and then display the remote phone book entries on the phone user interface. IP phones support up to 5 remote phone books. Remote phone book is customizable.

Note We recommend you to download less than 5000 remote contacts from the remote server.

Customizing Remote Phone Book Template File

You can customize the remote phone book for IP phones as required. You can also add multiple

remote contacts at a time and/or share remote contacts between IP phones using the supplied template files (Menu.xml and Department.xml). The Menu.xml file defines departments of a remote phone book. The Department.xml file defines contact lists for a department, which is nested in Menu.xml file. After setup, place the files (Menu.xml and Department.xml) to the provisioning server, and specify the access URL of the file (Menu.xml) in the configuration files.

You can ask the distributor or Yealink FAE for remote XML phone book template. You can also obtain the remote XML phone book template online: http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage. For more information on obtaining the remote phone book template, refer to Obtaining Configuration Files and Resource Files on page 119.

When creating a Department.xml file, learn the following:

- <YealinkIPPhoneDirectory> indicates the start of a department file and </YealinkIPPhoneDirectory> indicates the end of a department file.
- Create contact lists for a department between <DirectoryEntry> and </DirectoryEntry>.

To customize a Department.xml file:

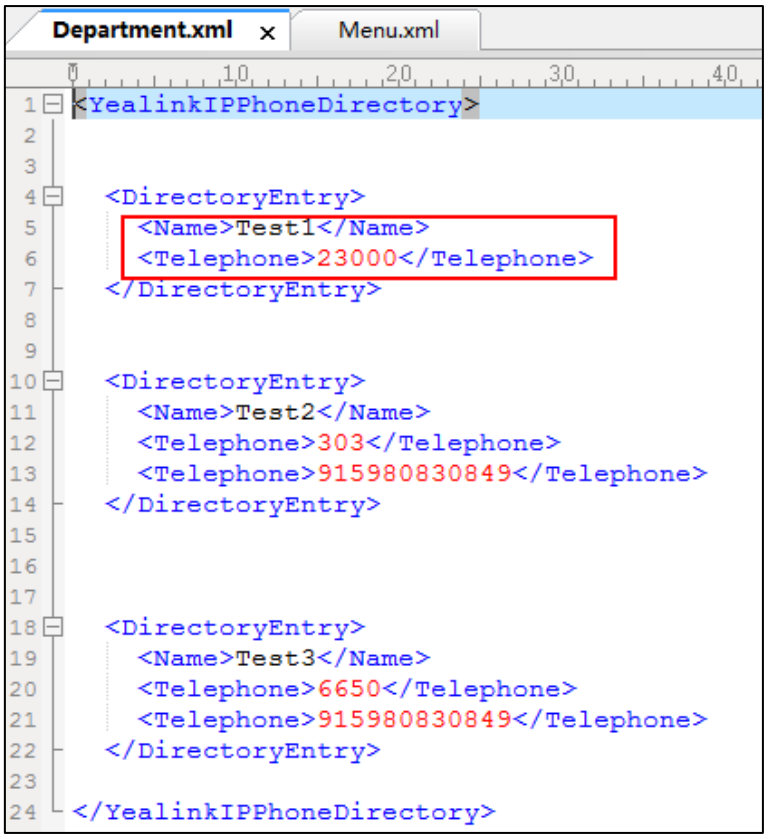
1. Open the template file using an ASCII editor.
2. For each contact that you want to add, add the following strings to the file. Each starts on a separate line:

```
<Name> Test1</Name>
<Telephone>23000</Telephone>
```

Where:

Specify the contact name between <Name> and </Name>.

Specify the contact number between <Telephone> and </Telephone>.



3. Save the file and place this file to the provisioning server.

When creating a Menu.xml file, learn the following:

- <YealinkIPPhoneMenu> indicates the start of a remote phone book file and </YealinkIPPhoneMenu> indicates the end of a remote phone book file.
- Create the title of a remote phone book between <Title> and </Title>.
- <MenuItem>indicates the start of specifying a department file and </MenuItem> indicates the end of specifying a department file.
- <SoftKeyItem> indicates the start of specifying an XML file and </SoftKeyItem> indicates the end of specifying an XML file.

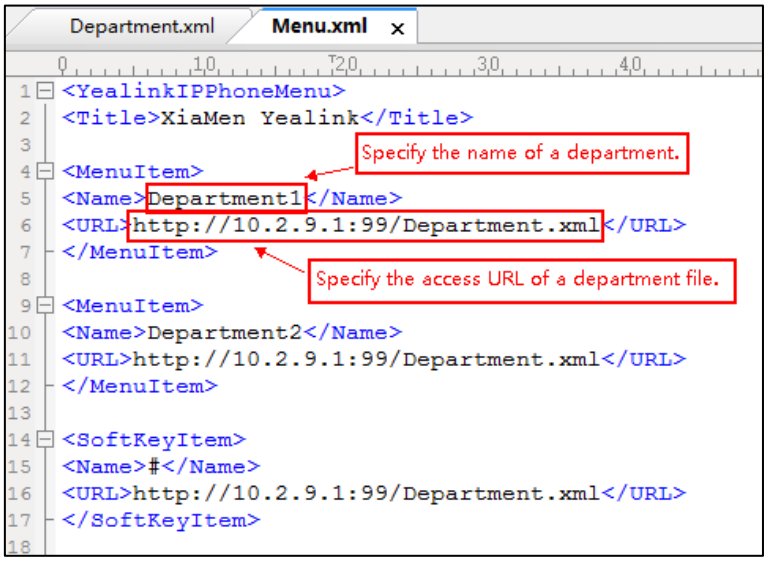
To customize a Menu.xml file:

1. Open the template file using an ASCII editor.

2. For each department that you want to add, add the following strings to the file. Each starts on a separate line:

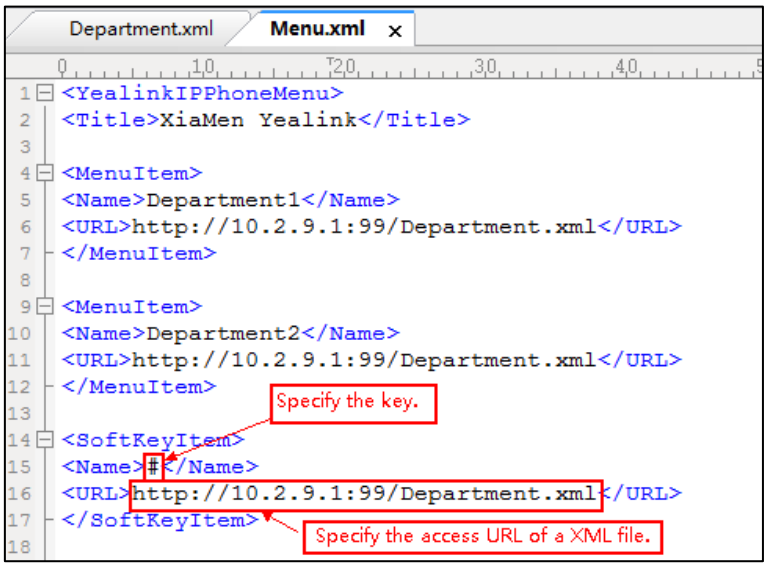
```
<MenuItem>
<Name>Department1</Name>
```

```
<URL>http://10.2.9.1:99/Department.xml</URL>
</MenuItem>
```



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

```
<SoftKeyItem>
<Name>#</Name>
<URL> http://10.2.9.1:99/Department.xml</URL>
</SoftKeyItem>
```



4. Save the file and place this file to the provisioning server.
5. Specify the access URL of the remote phone book (remote_phonebook.data.1.url = http://192.168.1.20/Menu.xml).

During the auto provisioning process, the IP phone connects to the provisioning server "192.168.1.20", and downloads the remote phone book file "Menu.xml".

Note Yealink supplies a phonebook generation tool to generate a remote XML phone book. For more information, refer to *Yealink Phonebook Generation Tool User Guide*.

Incoming/Outgoing Call Lookup allows IP phones to search the entry names from the remote phone book for incoming/outgoing calls. Update Time Interval specifies how often IP phones refresh the local cache of the remote phone book.

Procedure

Remote phone book can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL and the display name of the remote phone book. **Parameters:** remote_phonebook.data.X.url remote_phonebook.data.X.name remote_phonebook.display_name
		Specify whether to query the entry name from the remote phone book for outgoing/incoming calls. **Parameter:** features.remote_phonebook.enable
		Specify how often the IP phone refreshes the local cache of the remote phone book. **Parameter:** features.remote_phonebook.flash_time
		Specify whether to refresh the local cache of the remote phone book at a time when accessing the remote phone book. **Parameter:** features.remote_phonebook.enter_update_enable
Web User Interface		Specify the access URL and the display name of the remote phone book. Specify whether to query the entry name from the remote phone book for

	outgoing/incoming calls. Specify how often the IP phone refreshes the local cache of the remote phone book. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=contacts-remote&q=load

Details of Configuration Parameters:

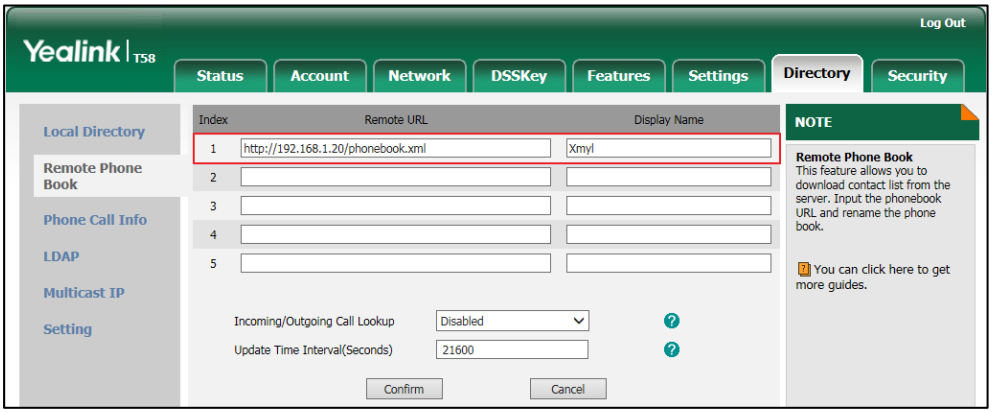
Parameters	Permitted Values	Default
remote_phonebook.data.X.url (X ranges from 1 to 5)	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the remote phone book. **Example:** remote_phonebook.data.1.url = http://192.168.1.20/phonebook.xml **Note:** The size of a remote phone book file should be less than 60M. **Web User Interface:** Directory->Remote Phone Book->Remote URL **Phone User Interface:** None		
remote_phonebook.data.X.name (X ranges from 1 to 5)	**String within 99 characters**	**Blank**
Description: Configures the display name of the remote phone book item. **Example:** remote_phonebook.data.1.name = Xmyl "Xmyl" will be displayed on the touch screen at the phone path -> ***Remote Phone Book***. The name of ***Remote Phone Book*** can be configured by the parameter "remote_phonebook.display_name" introduced below. **Web User Interface:** Directory->Remote Phone Book->Display Name **Phone User Interface:** None		
remote_phonebook.display_name	**String within 99**	**Blank**

Parameters	Permitted Values	Default
	characters	
Description: Configures the display name of the remote phone book. **Example:** remote_phonebook.display_name = Friends If it is left blank, Remote Phone Book will be the display name. **Web User Interface:** None **Phone User Interface:** None		
features.remote_phonebook.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to perform a remote phone book search for an incoming or outgoing call and display the matched results on the touch screen. **0**-Disabled **1**-Enabled **Web User Interface:** Directory->Remote Phone Book->Incoming/Outgoing Call Lookup **Phone User Interface:** None		
features.remote_phonebook.flash_time	**0, Integer from 3600 to 1296000**	**21600**
Description: Configures how often to refresh the local cache of the remote phone book. If it is set to 3600, the IP phone will refresh the local cache of the remote phone book every 3600 seconds (1 minute). If it is set to 0, the IP phone will not refresh the local cache of the remote phone book. **Web User Interface:** Directory->Remote Phone Book->Update Time Interval(Seconds) **Phone User Interface:** None		
features.remote_phonebook.enter_update_enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables the IP phone to refresh the local cache of the remote phone book at a time when accessing the remote phone book. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		

To specify access URL of the remote phone book via web user interface:

1. Click on **Directory**->**Remote Phone Book**.
2. Enter the access URL in the **Remote URL** field.
3. Enter the name in the **Display Name** field.

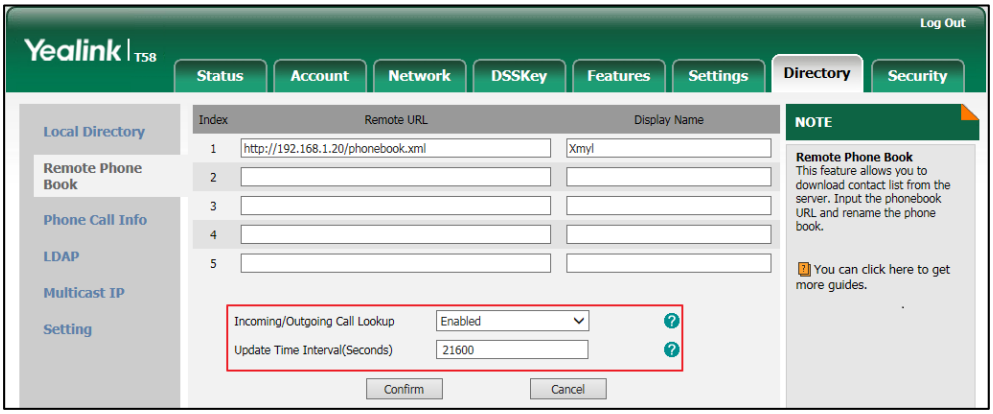


4. Click **Confirm** to accept the change.

To configure incoming/outgoing call lookup and update time interval via web user interface:

1. Click on **Directory**->**Remote Phone Book**.
2. Select the desired value from the pull-down list of **Incoming/Outgoing Call Lookup**.

3. Enter the desired time in the **Update Time Interval(Seconds)** field.



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

Lightweight Directory Access Protocol (LDAP)

LDAP is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. IP phones can be configured to interface with a corporate directory server that supports LDAP version 2 or 3. The following LDAP servers are supported:

- Microsoft Active Directory
- Sun ONE Directory Server
- Open LDAP Directory Server
- Microsoft Active Directory Application Mode (ADAM)

The biggest plus for LDAP is that users can access the central LDAP directory of the corporation using IP phones. Therefore they do not have to maintain the directory locally. Users can search and dial out from the LDAP directory, and save LDAP entries to the local directory. LDAP entries displayed on the IP phone are read only, which cannot be added, edited or deleted by users. When an LDAP server is properly configured, the IP phone can look up entries from the LDAP server in a wide variety of ways. The LDAP server indexes all the data in its entries, and "filters" can be used to select the desired entry or group, and return the desired information.

Configurations on the IP phone limit the amount of the displayed entries when querying from the LDAP server, and decide how attributes are displayed and sorted.

You can set a DSS key to be an LDAP key, and then tap the LDAP key to enter the LDAP search screen when the IP phone is idle.

LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on IP phones.

Abbreviation	Name	Description
gn	givenName	First name
cn	commonName	LDAP attribute is made up from given name joined to surname.
sn	surname	Last name or family name
dn	distinguishedName	Unique identifier for each entry
dc	dc	Domain component
-	company	Company or organization name
-	telephoneNumber	Office phone number
mobile	mobilephoneNumber	Mobile or cellular phone number
ipPhone	IPphoneNumber	Home phone number

For more information on LDAP, refer to *LDAP Phonebook on Yealink IP Phones*.

Procedure

LDAP can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure LDAP. **Parameters:** ldap.enable ldap.name_filter ldap.number_filter ldap.tls_mode ldap.host ldap.port ldap.base ldap.user ldap.password ldap.max_hits ldap.name_attr ldap.numb_attr ldap.display_name ldap.version ldap.call_in_lookup

		ldap.call_out_lookup ldap.ldap_sort ldap.incoming_call_special_search.enable
		Assign an LDAP key. **Parameters:** linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Configure LDAP. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=contacts-LDAP&q=load
		Assign an LDAP key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface		Assign an LDAP key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
ldap.enable	**0 or 1**	**0**
Description: Enables or disables LDAP feature on the IP phone. **0**-Disabled **1**-Enabled **Web User Interface:** Directory->LDAP->Enable LDAP **Phone User Interface:** None		
ldap.name_filter	**String within 99 characters**	**Blank**
Description: Configures the search criteria for LDAP contact names look up.		

Parameters	Permitted Values	Default
The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the name prefix entered by the user. **Example:** ldap.name_filter = (|(cn=%)(sn=%)) When the cn or sn of the LDAP contact starts with the entered prefix, the record will be displayed on the touch screen. ldap.name_filter = (&(cn=*)(sn=%)) When the cn of the LDAP contact is set and the sn of the LDAP contact start with the entered prefix, the records will be displayed on the phone touch screen. ldap.name_filter = (!(cn=%)) When the cn of the LDAP contact does not start with the entered prefix, the records will be displayed on the phone touch screen. **Web User Interface:** Directory->LDAP->LDAP Name Filter **Phone User Interface:** None		
ldap.number_filter	**String within 99 characters**	**Blank**
Description: Configures the search criteria for LDAP contact numbers look up. The "*" symbol in the filter stands for any number. The "%" symbol in the filter stands for the number prefix entered by the user. **Example:** ldap.number_filter = (|(telephoneNumber=%)(mobile=%)(ipPhone=%)) When the number prefix of the telephoneNumber, mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the touch screen. ldap.number_filter = (&(telephoneNumber=*)(mobile=%)) When the telephoneNumber of the LDAP contact is set and the mobile of the LDAP contact starts with the entered prefix, the record will be displayed on the phone touch screen. **Web User Interface:** Directory->LDAP->LDAP Number Filter **Phone User Interface:** None		
ldap.tls_mode	**0, 1 or 2**	**0**

Parameters	Permitted Values	Default
Description: Configures the connection mode between the LDAP server and the IP phone. **0**-LDAP−Unencrypted connection between LDAP server and the IP phone (port 389 is used by default). **1**-LDAP TLS Start−TLS/SSL connection between LDAP server and the IP phone (port 389 is used by default). **2**-LDAPs−TLS/SSL connection between LDAP server and the IP phone (port 636 is used by default). **Web User Interface:** Directory->LDAP->LDAP TLS Mode **Phone User Interface:** None		
ldap.host	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the LDAP server. **Example:** ldap.host = 192.168.1.20 **Web User Interface:** Directory->LDAP->Server Address **Phone User Interface:** None		
ldap.port	**Integer from 1 to 65535**	**389**
Description: Configures the port of the LDAP server. **Example:** ldap.port = 389 **Web User Interface:** Directory->LDAP->Port **Phone User Interface:** None		
ldap.base	**String within 99 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the LDAP search base which corresponds to the location of the LDAP phone book from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time. **Example:** ldap.base = dc=yealink,dc=cn **Web User Interface:** Directory->LDAP->Base **Phone User Interface:** None		
ldap.user	**String within 99 characters**	**Blank**
Description: Configures the user name used to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the user name to login the LDAP server. **Example:** ldap.user = cn=manager,dc=yealink,dc=cn **Web User Interface:** Directory->LDAP->Username **Phone User Interface:** None		
ldap.password	**String within 99 characters**	**Blank**
Description: Configures the password used to login the LDAP server. This parameter can be left blank in case the server allows anonymous to login. Otherwise you will need to provide the password to login the LDAP server. **Example:** ldap.password = secret **Web User Interface:** Directory->LDAP->Password **Phone User Interface:** None		

Parameters	Permitted Values	Default
ldap.max_hits	**Integer from 1 to 32000**	**50**
Description: Configures the maximum number of search results to be returned by the LDAP server. If it is set to blank, the LDAP server will return all searched results. **Example:** ldap.max_hits = 50 **Note**: A very large value of this parameter will slow down the LDAP search speed, therefore it should be configured according to the available bandwidth. **Web User Interface:** Directory->LDAP->Max Hits (1~32000) **Phone User Interface:** None		
ldap.name_attr	**String within 99 characters**	**Blank**
Description: Configures the name attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple name attributes separated by spaces. **Example:** ldap.name_attr = cn sn This requires the "cn" and "sn" attributes set for each contact record on the LDAP server. **Web User Interface:** Directory->LDAP->LDAP Name Attributes **Phone User Interface:** None		
ldap.numb_attr	**String within 99 characters**	**Blank**
Description: Configures the number attributes of each record to be returned by the LDAP server. It compresses the search results. You can configure multiple number attributes separated by spaces. **Example:** ldap.numb_attr = mobile ipPhone		

Parameters	Permitted Values	Default
This requires the "mobile" and "ipPhone" attributes set for each contact record on the LDAP server. **Web User Interface:** Directory->LDAP->LDAP Number Attributes **Phone User Interface:** None		
ldap.display_name	**String within 99 characters**	**Blank**
Description: Configures the display name of the contact record displayed on the touch screen. The value must start with "%" symbol. **Example:** ldap.display_name = %cn The cn of the contact record is displayed on the touch screen. **Web User Interface:** Directory->LDAP->LDAP Display Name **Phone User Interface:** None		
ldap.version	**2 or 3**	**3**
Description: Configures the LDAP protocol version supported by the IP phone. Make sure the protocol value corresponds with the version assigned on the LDAP server. **Web User Interface:** Directory->LDAP->Protocol **Phone User Interface:** None		
ldap.call_in_lookup	**0 or 1**	**0**
Description: Enables or disables the IP phone to perform an LDAP search when receiving an incoming call. **0**-Disabled **1**-Enabled		

Parameters	Permitted Values	Default
Web User Interface: Directory->LDAP->LDAP Lookup For Incoming Call **Phone User Interface:** None		
ldap.call_out_lookup	**0 or 1**	**1**
Description: Enables or disables the IP phone to perform an LDAP search when placing a call. **0**-Disabled **1**-Enabled **Web User Interface:** Directory->LDAP->LDAP Lookup For Callout **Phone User Interface:** None		
ldap.ldap_sort	**0 or 1**	**0**
Description: Enables or disables the IP phone to sort the search results in alphabetical order or numerical order. **0**-Disabled **1**-Enabled **Web User Interface:** Directory->LDAP->LDAP Sorting Results **Phone User Interface:** None		
ldap.incoming_call_special_search.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to search the telephone numbers starting with "+" symbol and "00" from the LDAP server if the incoming phone number starts with"+" or "00". When completing the LDAP search, the all search results will be displayed on the touch screen. **0**-Disabled **1**-Enabled For example, If the phone receives an incoming call from the phone number 0044123456789, it will		

Parameters	Permitted Values	Default
search 0044123456789 from the LDAP sever first, if no result found, it will search +44123456789 from the server again. The phone will display all the search results. **Note:** It works only if the value of the parameter "ldap.call_in_lookup" is set to 1 (Enabled). You may need to set the value of the parameter "ldap.name_filter" to be (|(cn=%)(sn=%)(telephoneNumber=%)(mobile=%)) for searching the telephone numbers starting with "+" symbol. **Web User Interface:** None **Phone User Interface:** None		

LDAP Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

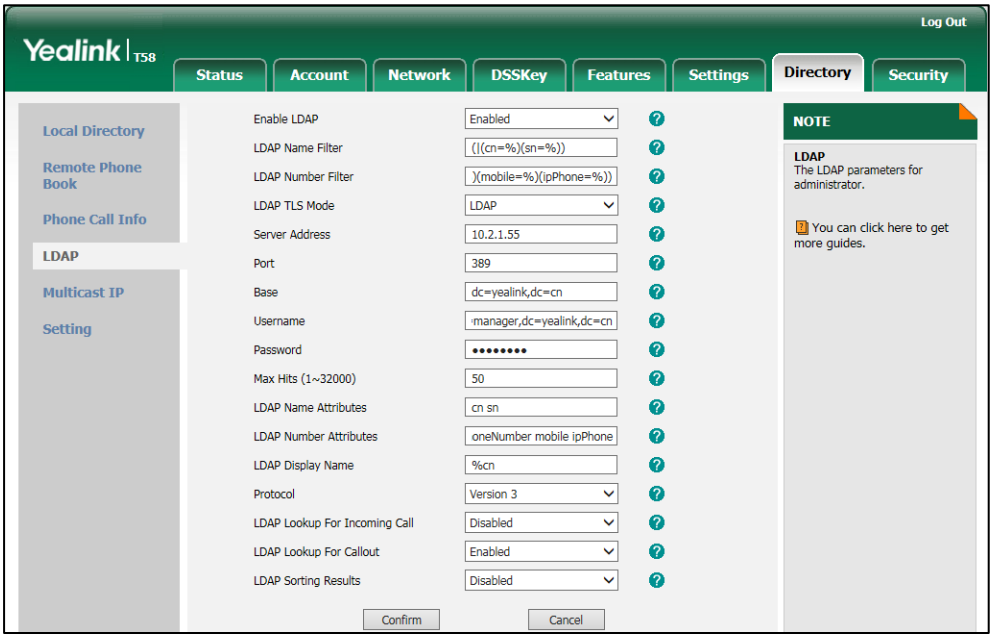
Parameters	Permitted Values	Default
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type	**38**	**Refer to the following content**
Description: Configures a DSS key as an LDAP key on the IP phone. The digit **38** stands for the key type **LDAP**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 38 **Default:** For line keys:		

Parameters	Permitted Values	Default
For SIP-T58V/T58A/T56A IP phones: The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For programable keys: **For SIP-T58V/T58A/T56A IP phones:** When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key/Programable Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure LDAP via web user interface:

1. Click on **Directory**->**LDAP**.
2. Enter the values in the corresponding fields.

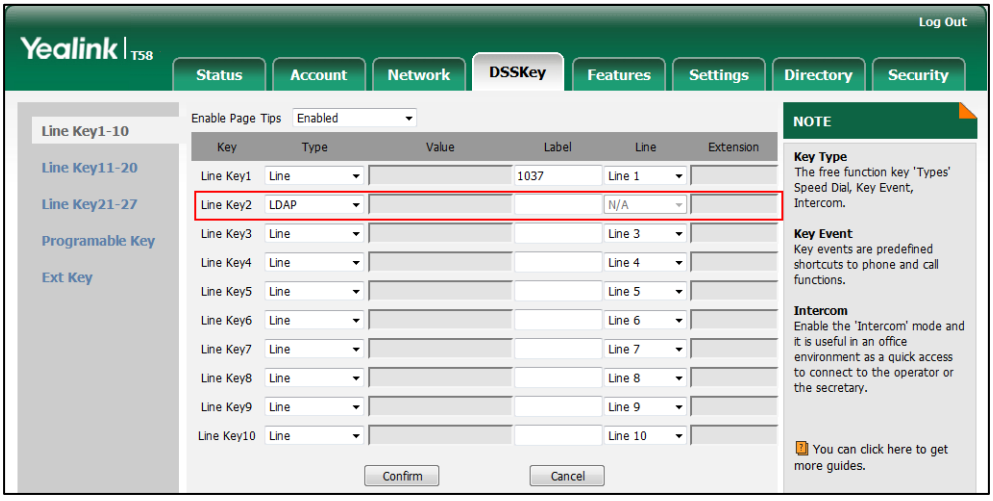
3. Select the desired values from the corresponding pull-down lists.



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

To configure an LDAP key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **LDAP** from the pull-down list of **Type**.
3. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.



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

To configure an LDAP key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.

4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **LDAP** in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Tap ✓ to accept the change.

Busy Lamp Field (BLF)

BLF is used to monitor a specific user for status changes on IP phones. For example, you can configure a BLF key on a supervisor's phone to monitor the IP phone user status (busy or idle). When the monitored user places a call, a busy indicator on the supervisor's phone indicates that the user's phone is in use.

When the monitored user is idle, the supervisor can tap the BLF key to dial out the phone number. When the monitored user receives an incoming call, the supervisor can tap the BLF key to pick up the call directly. When the monitored user is in a call, the supervisor can tap the BLF key to interrupt and set up a conference call.

BLF Subscription

IP phones support BLF using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265. This feature depends on support from a SIP server.

When the IP phone is configured to monitor a specific user, it sends a SUBSCRIBE message to the server. A NOTIFY message which includes XML in the message body is sent to the IP phone to inform the current state of monitored user. Once status of the monitored user is changed from idle to busy or vice versa, the IP phone is notified from the server with a NOTIFY message. You can manually configure the period of the BLF subscription.

Example of a SUBSCRIBE message:

```
SUBSCRIBE sip:1011@10.3.20.2:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.1:5060;branch=z9hG4bK2940676338
From: "1010" <sip:1010@10.2.1.48:5060>;tag=2493044525
To: <sip:1011@10.2.1.48:5060>;tag=2527548726
Call-ID: 0_3538292381@10.3.20.1
CSeq: 2 SUBSCRIBE
Contact: <sip:1010@10.3.20.1:5060>
Accept: application/dialog-info+xml
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Expires: 30
Event: dialog
Content-Length: 0
```

Example of a NOTIFY message (<state>confirmed</state> shows the call has been established):

```
NOTIFY sip:1010@10.3.20.1:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.2:5060;branch=z9hG4bK276311022
From: <sip:1011@10.2.1.48:5060>;tag=3436332841
To: "1010" <sip:1010@10.2.1.48:5060>;tag=3098567568
Call-ID: 0_4117916748@10.3.20.1
CSeq: 4 NOTIFY
Contact: <sip:1011@10.3.20.2:5060>
Content-Type: application/dialog-info+xml
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Subscription-State: active;expires=17
Event: dialog
Content-Length:    534

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="3" state="partial"
entity="sip:1011@10.2.1.48:5060">
<dialog id="74" call-id="0_2561109579@10.3.20.1" local-tag="2778958897" remote-tag="1132018898"
direction="recipient">
<state>confirmed</state>
<local>
<identity>sip:1011@10.2.1.48:5060</identity>
<target uri="sip:1011@10.2.1.48:5060"/>
</local>
<remote>
<identity>sip:1010@10.2.1.48:5060</identity>
<target uri="sip:1010@10.2.1.48:5060"/>
</remote>
</dialog>
</dialog-info>
```

Procedure

BLF subscription can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the period of the BLF subscription. **Parameter:** account.X.blf.subscribe_period
		Configure the event of the BLF subscription. **Parameter:** account.X.blf.subscribe_event

		Configure whether to handle NOTIFY messages out of the BLF dialog. **Parameter:** account.X.out_dialog_blf_enable
Web User Interface		Configure the period of the BLF subscription. Configure whether to handle NOTIFY messages out of the BLF dialog. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-adv&q=load&acc=0

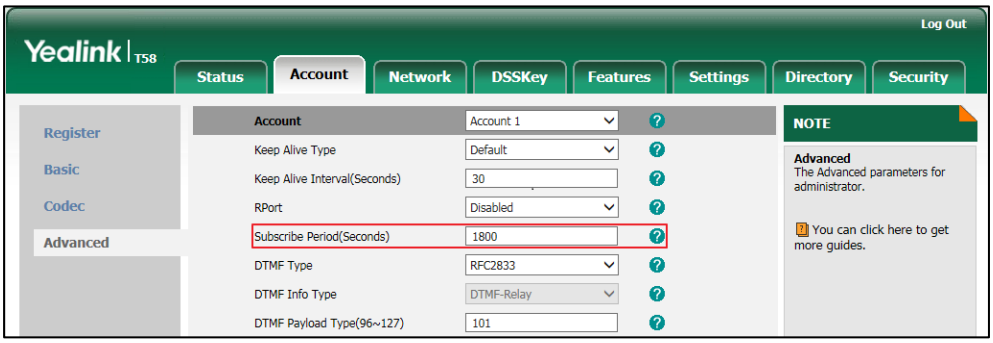
Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.blf.subscribe_period	**Integer from 30 to 2147483647**	**1800**
Description: Configures the period (in seconds) of the BLF subscription for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) The IP phone is able to successfully refresh the SUBSCRIBE before expiration of the SUBSCRIBE dialog. **Web User Interface:** Account->Advanced->Subscribe Period(Seconds) **Phone User Interface:** None		
account.X.blf.subscribe_event	**0 or 1**	**0**
Description: Configures the event of the BLF subscription for account X. **0**-dialog **1**-presence X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** None		

Parameters	Permitted Values	Default
Phone User Interface: None		
account.X.out_dialog_blf_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to handle NOTIFY messages out of the BLF dialog for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Out Dialog BLF **Phone User Interface:** None		

To configure BLF subscription via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Enter the desired period of BLF subscription in the **Subscribe Period(Seconds)** field.

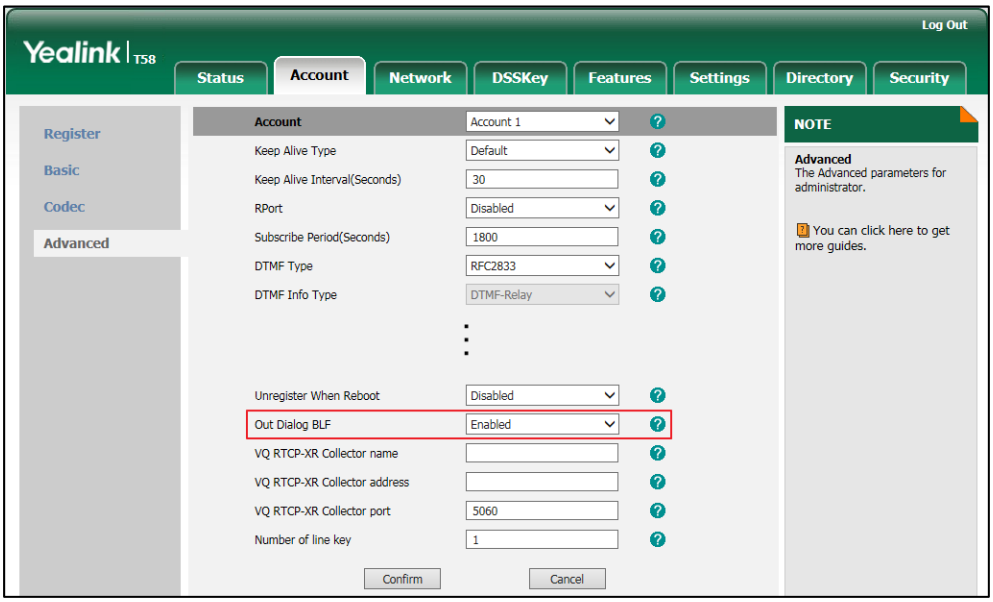


4. Click **Confirm** to accept the change.

To configure out dialog BLF via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

3. Select the desired value from the pull-down list of **Out Dialog BLF**.



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

Visual Alert and Audio Alert for BLF Pickup

Visual and audio alert for BLF pickup allow the supervisor's phone to play an alert tone and display a visual prompt (e.g., "6001<-6002", 6001 is the monitored extension which receives an incoming call from 6002) when the monitored user receives an incoming call. In addition to the BLF key, visual alert for BLF pickup feature enables the supervisor to pick up the monitored user's incoming call by tapping the **DPickup** key. The directed call pickup code must be configured in advance. For more information on how to configure the directed call pickup code for the **DPickup** key, refer to Directed Call Pickup on page 374.

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify whether to use visual alert and audio alert for BLF pickup. **Parameters:** features.pickup.blf_visual_enable features.pickup.blf_audio_enable Configure ring type for BLF pickup.

Web User Interface	Specify whether to use visual alert and audio alert for BLF pickup. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-callpickup&q=load

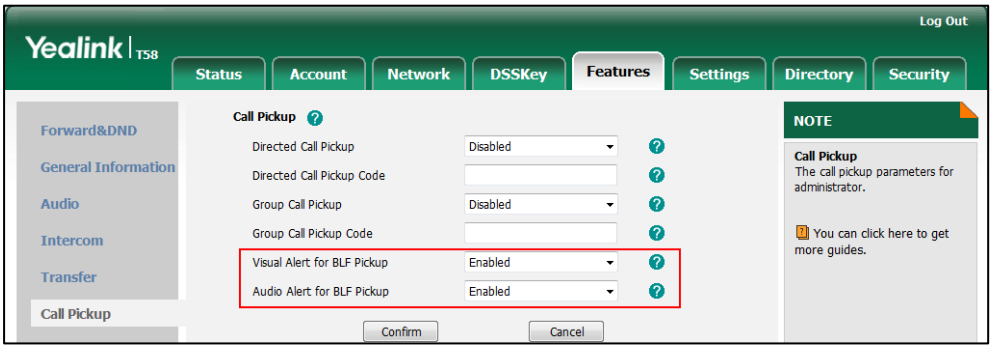
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.pickup.blf_visual_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to display a visual alert when the monitored user receives an incoming call. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Call Pickup->Visual Alert for BLF Pickup **Phone User Interface:** None		
features.pickup.blf_audio_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to play an audio alert when the monitored user receives an incoming call. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Call Pickup->Audio Alert for BLF Pickup **Phone User Interface:** None		

To configure visual alert and audio alert for BLF pickup via web user interface:

1. Click on **Features**->**Call Pickup**.
2. Select the desired value from the pull-down list of **Visual Alert for BLF Pickup**.

3. Select the desired value from the pull-down list of **Audio Alert for BLF Pickup**.



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

BLF LED Mode

BLF LED Mode provides five kinds of definition for the BLF/BLF List key LED status. BLF LED mode is only applicable to the expansion module EXP50 connected to SIP-T58V/T58A/T56A IP phones. The following table lists the LED statuses of the BLF key when BLF LED Mode is set to 0, 1, 2, 3 or 4 respectively. The default value of BLF LED mode is 0.

BLF LED mode feature is also applicable to BLF list key. For more information on BLF List key, refer to Busy Lamp Field (BLF) List on page 486.

Expansion Module Key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 0)

LED Status	Description
Solid green	The monitored user is idle.
Fast-flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is dialing. The monitored user is talking. The monitored user's conversation is placed on hold (This LED status requires server support).
Slow-flashing red (1s)	The call is parked against the monitored user's phone number.
Off	The monitored user does not exist.

Expansion Module Key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 1)

LED Status	Description
Fast-flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is dialing. The monitored user is talking.

LED Status	Description
	The monitored user's conversation is placed on hold (This LED status requires server support).
Slowly-flashing red (1s)	The call is parked against the monitored user's phone number.
Off	The monitored user is idle. The monitored user does not exist.

Expansion Module Key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 2)

LED Status	Description
Fast-flashing red (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is dialing. The monitored user is talking. The monitored user's conversation is placed on hold (This LED status requires server support).
Slowly-flashing red (1s)	The call is parked against the monitored user's phone number.
Off	The monitored user is idle. The monitored user does not exist.

Expansion Module Key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 3)

LED Status	Description
Fast-flashing green (200ms)	The monitored user receives an incoming call.
Solid red	The monitored user is dialing. The monitored user is talking. The monitored user's conversation is placed on hold (This LED status requires server support).
Slowly-flashing red (1s)	The call is parked against the monitored user's phone number.
Off	The monitored user is idle. The monitored user does not exist.

Expansion Module Key LED (configured as a BLF key or a BLF List key and BLF LED Mode is set to 4. This mode is specifically designed for the Genband server.)

LED Status	Description
Solid green	The monitored user is talking.
Slowly-flashing green (1s)	The monitored user does not exist.
Off	The monitored user is idle.

Procedure

BLF LED mode can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure BLF LED mode. **Parameter:** features.blf_led_mode
Web User Interface		Configure BLF LED mode. **Navigate to**: http://<phoneIPAddress>/servlet?p=features-general&q=load

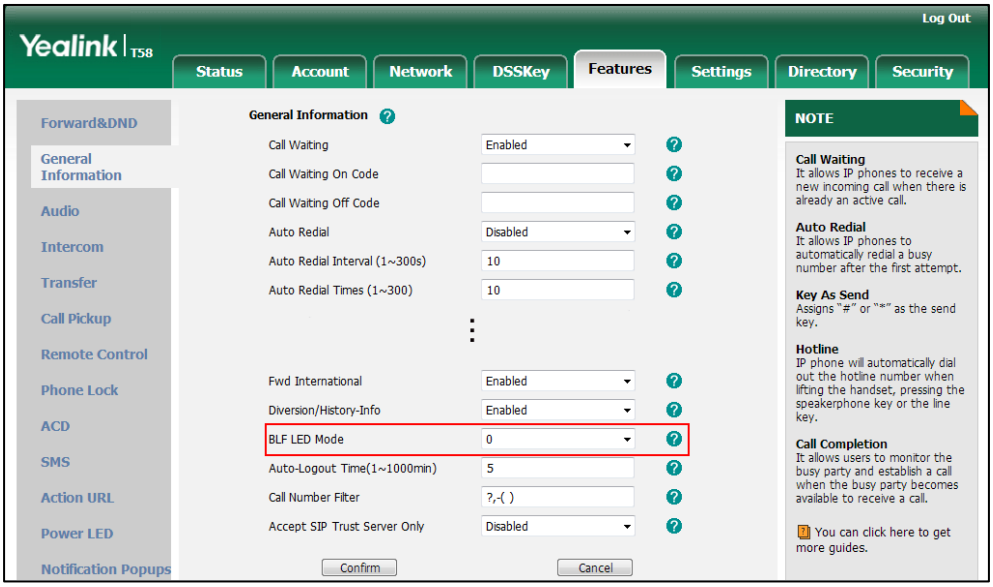
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.blf_led_mode	**0, 1, 2, 3 or 4**	**0**
Description: Configures BLF LED mode and provides five kinds of definition for the BLF/BLF List key LED status. **Note:** It is only applicable to the expansion module EXP50 connected to SIP-T58V/T58A/T56A IP phones. For the Genband server, you can set the value of this parameter to 4. **Web User Interface:** Features->General Information->BLF LED Mode **Phone User Interface:** None		

To configure BLF LED mode via web user interface:

1. Click on **Features**->**General Information**.

2. Select the desired value from the pull-down list of **BLF LED Mode**.



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

Configuring a BLF Key

You can configure a BLF key on a supervisor's phone to monitor the IP phone user status (busy or idle). For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Procedure

BLF key can be configured using the following methods.

Central Provisioning (Configuration File)	y0000000000xx.cfg	Assign a BLF key. **Parameters:** linekey.X.type/ expansion_module.X.key.Y.type linekey.X.line/ expansion_module.X.key.Y.line linekey.X.value/ expansion_module.X.key.Y.value linekey.X.pickup_value/ expansion_module.X.key.Y.pickup_value linekey.X.label/ expansion_module.X.key.Y.label

Web User Interface	Assign a BLF key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface	Assign a BLF key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ expansion_module.X.key.Y.type	**16**	**Refer to the following content**

Description:

Configures a DSS key as a BLF key on the IP phone.

The digit **16** stands for the key type **BLF**.

For line keys:

X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)

X ranges from 1 to 30 (for CP960)

For ext keys:

X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)

Example:

linekey.2.type = 16

Default:

For line keys:

For SIP-T58V/T58A/T56A IP phones:

The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0.

For CP960 IP phones:

The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0.

For ext keys:

For SIP-T58V/T58A/T56A IP phones:

When Y= 1 to 60, the default value is 0 (NA).

Web User Interface:

DSSKey->Line Key->Type

Phone User Interface:

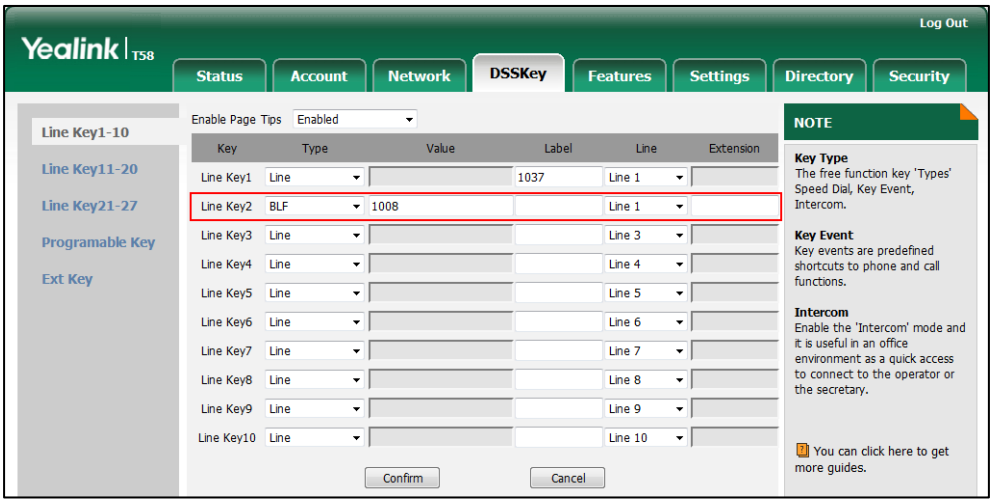
Settings->Features->DSS Keys->Line Key X->Type

Parameters	Permitted Values	Default
linekey.X.line/ expansion_module.X.key.Y.line	**Refer to the following content**	**1-16 for lines 1-16**
Description: Configures the desired line to apply the BLF key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Permitted Values:** 1 to 16 (for SIP-T58V/T58A/T56A) 1 (for CP960) 1-Line 1 2-Line 2 … 16-Line 16 **Example:** linekey.2.line = 1 **Web User Interface:** DSSKey->Line Key->Line **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Account ID		
linekey.X.value/ expansion_module.X.key.Y.value	**String within 99 characters**	**Blank**
Description: Configures the phone number or extension of the monitored user. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.value = 1008		

Parameters	Permitted Values	Default
Web User Interface: DSSKey->Line Key->Value **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Value		
linekey.X.pickup_value/ expansion_module.X.key.Y.pickup_value	**String within 256 characters**	**Blank**
Description: Configures the pickup code for BLF feature. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** line.2.pickup_value = *88 **Note:** This parameter only applies to BLF/intercom feature. **Web User Interface:** DSSKey->Line Key->Extension **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Extension		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a BLF key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Ext Key**).
2. In the desired DSS key field, select **BLF** from the pull-down list of **Type**.
3. Enter the phone number or extension you want to monitor in the **Value** field.
4. Select the desired line from the pull-down list of **Line**.
5. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
6. (Optional.) Enter the directed call pickup code in the **Extension** field.



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

To configure a BLF key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **BLF** in the pop-up dialog box.
5. Tap the **Account ID** field.
6. Tap the desired line in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Enter the phone number or extension you want to monitor in the **Value** field.
9. (Optional.) Enter the directed call pickup code in the **Extension** field.
10. Tap ✓ to accept the change.

Busy Lamp Field (BLF) List

BLF List allows a list of specific extensions to be monitored for status changes. It enables the monitoring phone to subscribe to a list of users, and receive notifications of the status of monitored users. Different indicators on the monitoring phone show the status of monitored users. The monitoring user can also be notified about calls being parked/no longer parked against any monitored user. IP phones support BLF list using a SUBSCRIBE/NOTIFY mechanism

as specified in RFC 3265. This feature depends on support from a SIP server.

Procedure

BLF List can be configured using the following methods.

<table>
<tr><td rowspan="4">Central Provisioning (Configuration File)</td><td><MAC>.cfg</td><td>Configure BLF List.
Parameters:
account.X.blf.blf_list_uri
account.X.blf_list_code
account.X.blf_list_barge_in_code
account.X.blf_list_retrieve_call_parked_code</td></tr>
<tr><td rowspan="3">y0000000000xx.cfg</td><td>Specify whether to automatically configure the BLF list keys.
Parameter:
phone_setting.auto_blf_list_enable</td></tr>
<tr><td>Configure the order of BLF list keys assigned automatically.
Parameter:
phone_setting.blf_list_sequence_type</td></tr>
<tr><td>Assign a BLF List key.
Parameters:
linekey.X.type/ expansion_module.X.key.Y.type
linekey.X.line/ expansion_module.X.key.Y.line</td></tr>
<tr><td colspan="2" rowspan="2">Web User Interface</td><td>Configure BLF List.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0</td></tr>
<tr><td>Assign a BLF List key.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load</td></tr>
<tr><td colspan="2">Phone User Interface</td><td>Assign a BLF List key.</td></tr>
</table>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.auto_blf_list_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to automatically configure the BLF list keys. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
phone_setting.blf_list_sequence_type	**0 or 1**	**0**
Description: Configures the order of BLF list keys assigned automatically. **0**-Line Key->Ext Key **1**-Ext Key->Line Key **Note**: It is not applicable to CP960 IP phones. It works only if the value of the parameter "phone_setting.auto_blf_list_enable" is set to 1 (Enabled). To assign Ext Key, make sure the expansion module has been connected to the phone in advance. **Web User Interface:** None **Phone User Interface:** None		
account.X.blf.blf_list_uri	**String within 256 characters**	**Blank**
Description: Configures the BLF List URI to monitor a list of users for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.blf.blf_list_uri = 4609@pbx.yealink.com **Web User Interface:**		

Parameters	Permitted Values	Default
Account->Advanced->BLF List URI **Phone User Interface:** None		
account.X.blf_list_code	**String within 32 characters**	**Blank**
Description: Configures the feature access code for directed call pickup for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.blf_list_code = *97 **Web User Interface:** Account->Advanced->BLF List Pickup Code **Phone User Interface:** None		
account.X.blf_list_barge_in_code	**String within 32 characters**	**Blank**
Description: Configures the feature access code for directed call pickup with barge-in for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.blf_list_barge_in_code = *33 **Web User Interface:** Account->Advanced->BLF List Barge In Code **Phone User Interface:** None		
account.X.blf_list_retrieve_call_parked_code	**String within 32 characters**	**Blank**
Description: Configures the feature access code for the call park retrieve for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960)		

Parameters	Permitted Values	Default
Example: account.1.blf_list_retrieve_call_parked_code = *88 **Web User Interface:** Account->Advanced->BLF List Retrieve Call Parked Code **Phone User Interface:** None		

BLF List Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

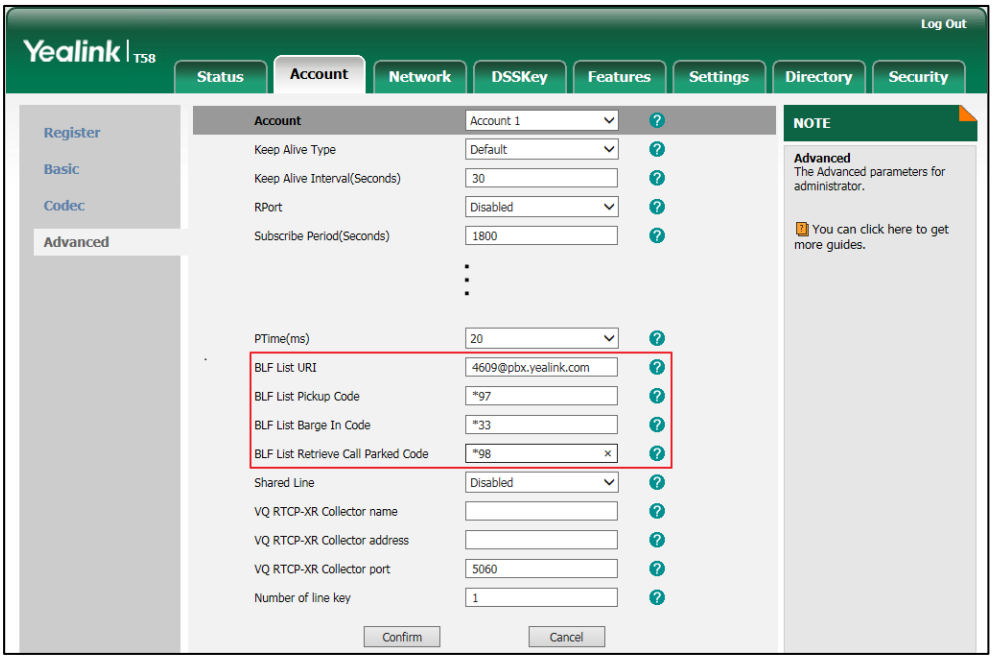
Parameters	Permitted Values	Default
linekey.X.type/ expansion_module.X.key.Y.type	**39**	**Refer to the following content**
Description: Configures a DSS key as a BLF List key on the IP phone. The digit **39** stands for the key type **BLF List**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 39 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For ext keys: **For SIP-T58V/T58A/T56A IP phones:**		

Parameters	Permitted Values	Default
When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.line/ expansion_module.X.key.Y.line	**Refer to the following content**	**1-16 for lines 1-16**
Description: Configures the desired line to apply the BLF List key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Permitted Values:** 1 to 16 (for SIP-T58V/T58A/T56A) 1 (for CP960) 1-Line 1 2-Line 2 … 16-Line 16 **Example:** linekey.1.line = 1 **Web User Interface:** DSSKey->Line Key->Line **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Account ID		

To configure the BLF List settings via web user interface:

1. Click on **Account->Advanced**.
2. Select the account (e.g., account 1) from the pull-down list of **Account**.
3. Enter the BLF List URI in the **BLF List URI** field.
4. (Optional.) Enter the directed pickup code in the **BLF List Pickup Code** field.
5. (Optional.) Enter the barge-in code in the **BLF List Barge In Code** field.

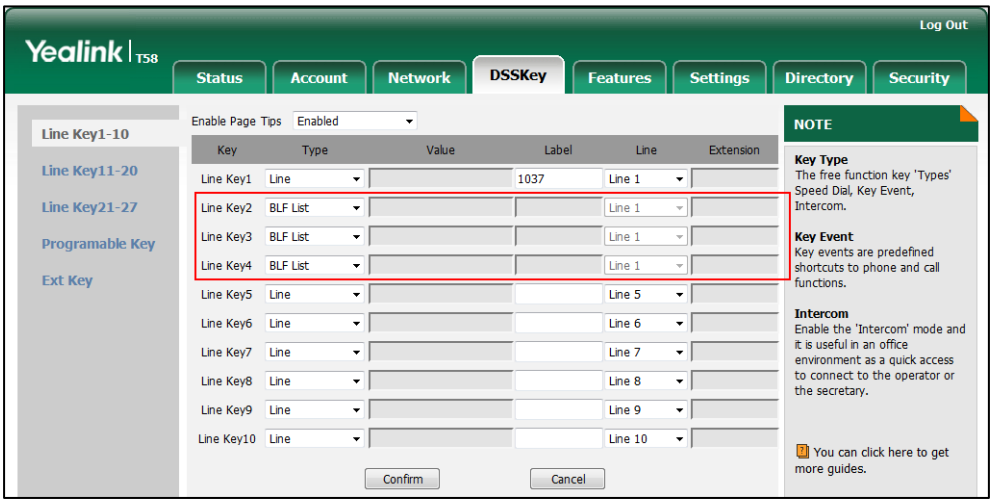
6. (Optional.) Enter the retrieve call parked code in the **BLF List Retrieve Call Parked Code** field.



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

To configure BLF List keys manually via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Ext Key**).
2. In the desired DSS key field, select **BLF List** from the pull-down list of **Type**.
3. Repeat the step 2, configure more BLF list keys.



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

Hide Feature Access Codes

Hide Feature Access Codes feature enables the IP phone to display the feature name instead of

the dialed feature access code automatically. For example, the dialed call park code will be replaced by the identifier "Call Park" when you park an active call.
The hide feature access codes feature is applicable to the following features:

- Voice Mail
- Pick up
- Group Pick up
- Barge In
- Retrieve
- Call Park
- Call Pull

Procedure

The hide feature access codes feature can be configured using the following methods.

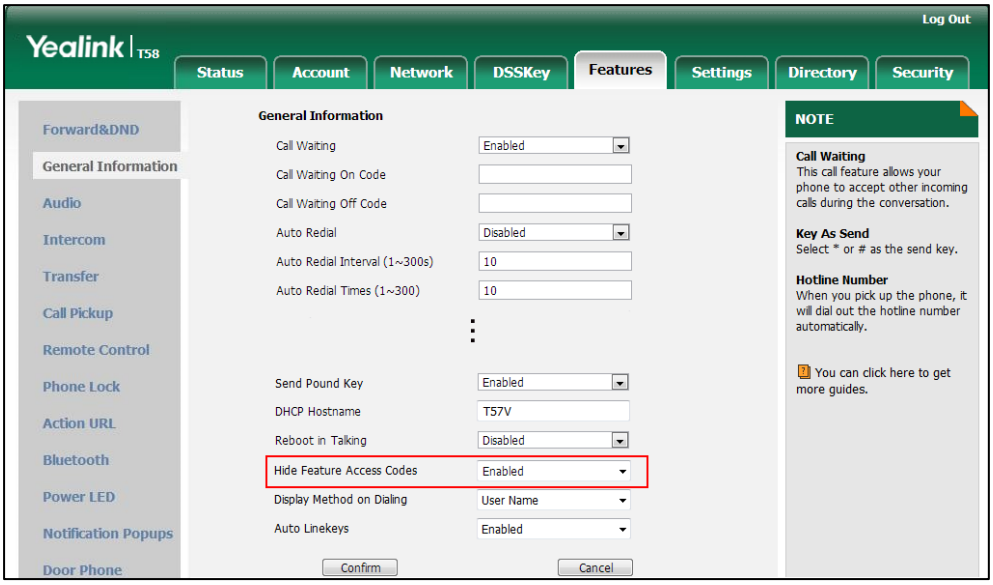
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the hide feature access codes feature. **Parameter:** features.hide_feature_access_codes.enable
Web User Interface		Configure the hide feature access codes feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.hide_feature_access_codes.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to display feature name instead of the feature access code when dialing or in talk. **0**-Disabled **1**-Enabled **Web User Interface:** Features->General Information->Hide Feature Access Codes **Phone User Interface:** None		

To enable hide feature access codes feature via web user interface:

1. Click on **Features**->**General Information**.
2. Select **Enabled** from the pull-down list of **Hide Feature Access Codes**.



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

Shared Call Appearance (SCA)

SCA allows users to share an extension which can be registered on two or more IP phones at the same time. For more information on how to register accounts, refer to Account Registration on page 172. If you want to customize multiple DSS keys to associate with an account, refer to Multiple Line Keys per Account on page 180.

Any IP phone can be used to originate or receive calls on the shared line. An incoming call can be presented to multiple phones simultaneously. The incoming call can be answered on any IP phone but not all. A call that is active on one IP phone will be presented visually to other IP phones that share the call appearance.

IP phones support SCA using a SUBSCRIBE/NOTIFY mechanism as specified in RFC 3265. The events used are:

- "call-info" for call appearance state notification
- "line-seize" for the IP phone to ask to seize the line

SCA supports the IP phones barging in an active call. In addition, SCA has the call pull capability. Call pull feature allows users to retrieve an existing call from another shared phone that is in active or public hold status.

If the call is placed on public hold, the held call is available for any shared party to retrieve. If the call is placed on private hold, the held call is only available for the hold party to retrieve. You need to configure either the private hold soft key or a private hold key before you place the call on private hold.

Procedure

SCA can be configured using the following methods.

<table>
<tr><td rowspan="4">Central Provisioning (Configuration File)</td><td rowspan="2"><MAC>.cfg</td><td>Configure the registration line type.
Parameter:
account.X.shared_line</td></tr>
<tr><td>Configure the call pull feature access code.
Parameter:
account.X.shared_line_callpull_code</td></tr>
<tr><td rowspan="2"><y0000000000xx>.cfg</td><td>Configure the private hold soft key.
Parameters:
phone_setting.custom_softkey_enable
custom_softkey_talking.url</td></tr>
<tr><td>Assign a private hold key.
Parameters:
linekey.X.type/ expansion_module.X.key.Y.type
linekey.X.label/ expansion_module.X.key.Y.label</td></tr>
<tr><td colspan="2" rowspan="3">Web User Interface</td><td>Configure the registration line type.
Configure the call pull feature access code.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0</td></tr>
<tr><td>Configure the private hold soft key.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=settings-softkey&q=load</td></tr>
<tr><td>Assign a private hold key.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load</td></tr>
<tr><td colspan="2">Phone User Interface</td><td>Assign a private hold key.</td></tr>
</table>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.shared_line	**0 or 1**	**0**
Description: Configures the registration line type for account X. **0**-Disabled **1**-Shared Call Appearance If it is set to 0 (Disabled), the shared line feature is disabled. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Shared Line **Phone User Interface:** None		
account.X.shared_line_callpull_code	**String within 32 characters**	**Blank**
Description: Configures the call pull feature access code to retrieve an existing call from another shared phone that is in active or public hold status for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: It works only if the value of the parameter "account.X.shared_line" is set to 1 (Shared Call Appearance). **Web User Interface:** Account->Advanced->Call Pull Feature Access Code **Phone User Interface:** None		

Private Hold Soft Key

Note that configuring the private hold soft key may affect the softkey layout in the Talking state. For more information, refer to Softkey Layout on page 215.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.custom_softkey_enable	**0 or 1**	**0**
Description: Enables or disables custom soft keys layout feature. **0**-Disabled **1**-Enabled **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Settings->Softkey Layout->Custom Softkey **Phone User Interface:** None		
custom_softkey_talking.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom file for the soft key presented on the touch screen when in the Talking state. **Example:** custom_softkey_talking.url = http://192.168.1.20/XMLfiles/Talking.xml During the auto provisioning process, the IP phone connects to the provisioning server "192.168.1.20", and downloads the Talking state file from the "XMLfiles" directory. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		

Private Hold Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

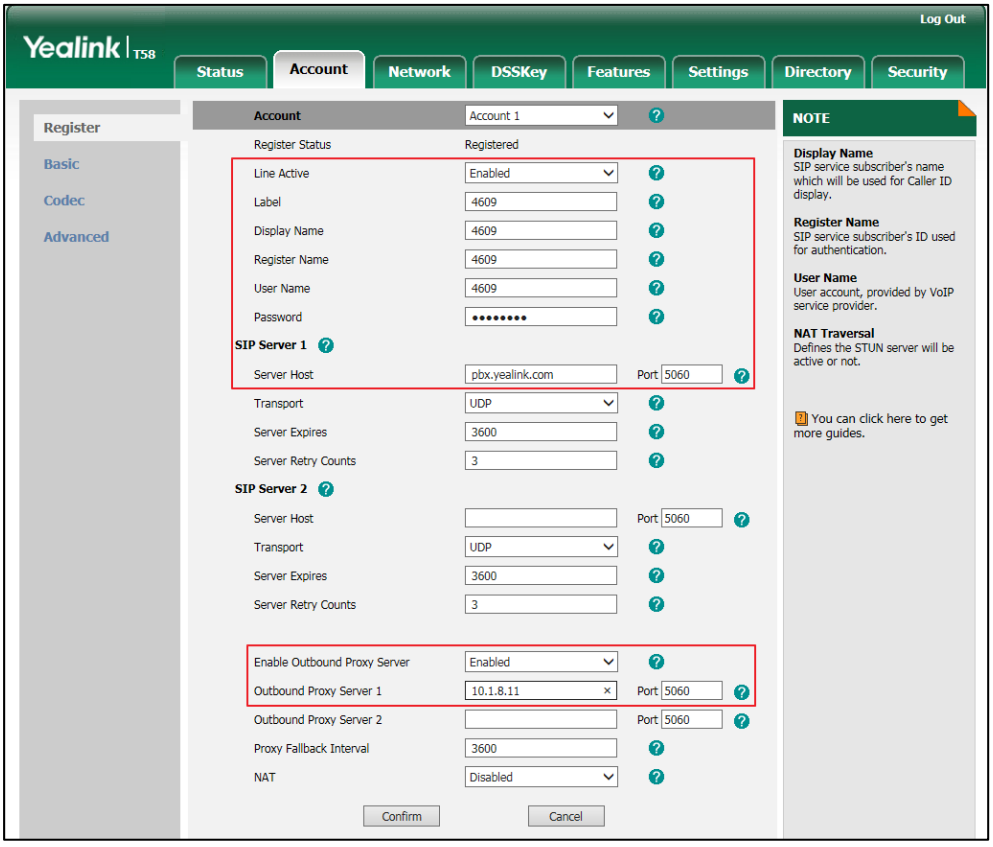
Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ expansion_module.X.key.Y.type	**20**	**Refer to the following content**
Description: Configures a DSS key to be a private hold key on the IP phone. The digit **20** stands for the key type **Private Hold**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 20 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For programable keys: **For SIP-T58V/T58A/T56A IP phones:** When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key/Programable Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**

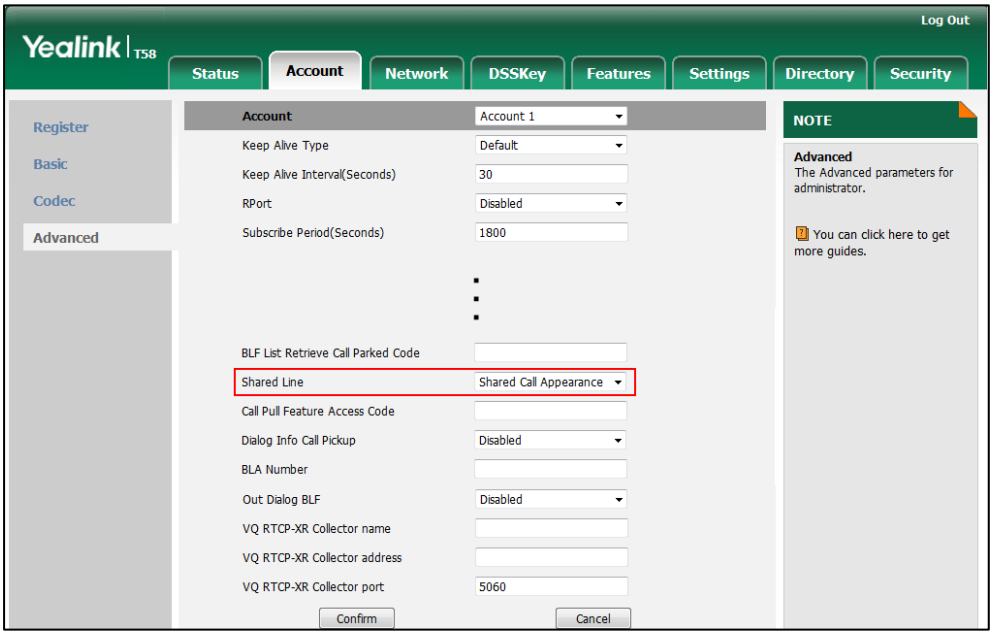
Parameters	Permitted Values	Default
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure the shared line settings on the primary phone via web user interface:

1. Register the primary account (e.g., 4609).



2. Click on **Advanced**, select **Shared Call Appearance** from the pull-down list of **Shared Line**.

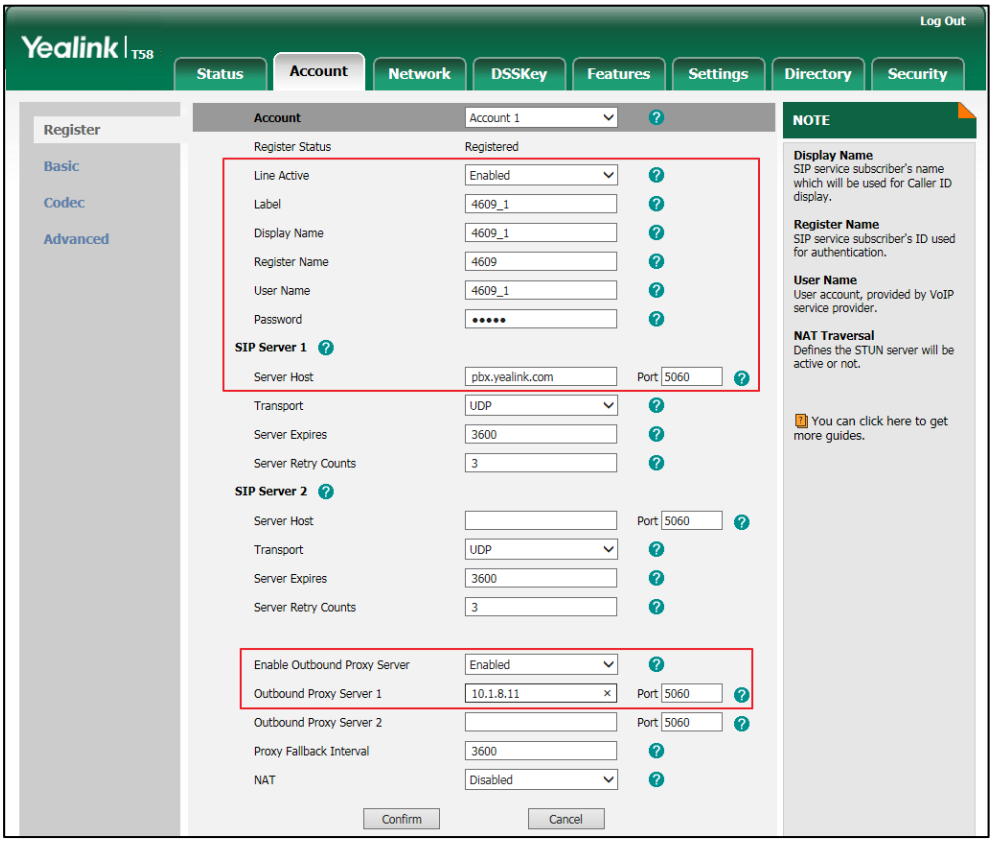


3. Click **Confirm** to accept the change.

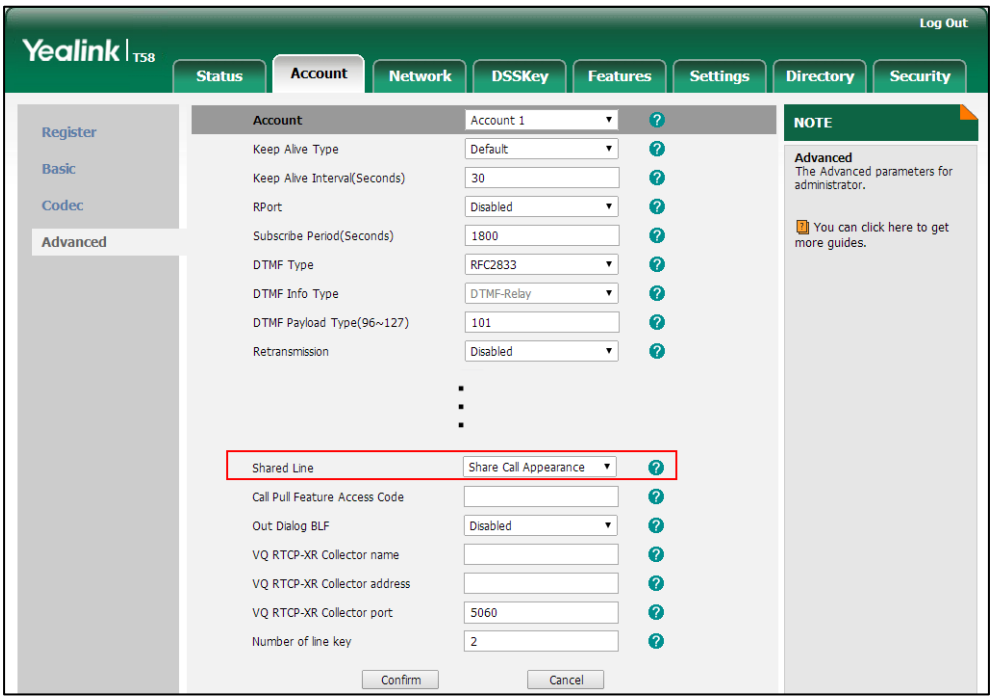
To configure the shared line settings on alternate phone via web user interface:

1. Register the alternate account (e.g., 4609_1).

   (Enter the primary account 4609 in the **Register Name** field.)



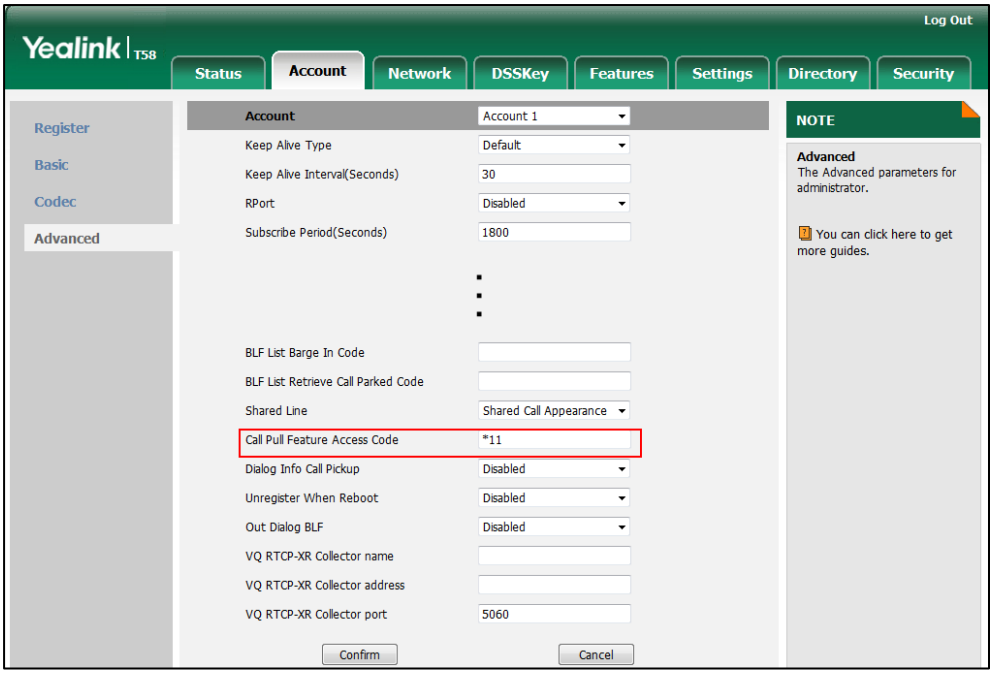
2. Click on **Advanced**, select **Shared Call Appearance** from the pull-down list of **Shared Line**.



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

To configure the call pull feature access code via web user interface:

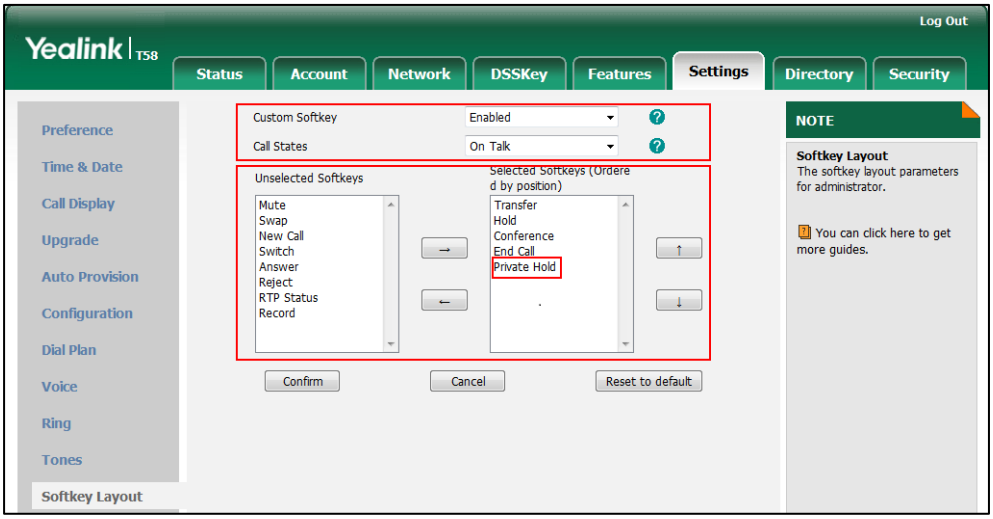
1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Enter the call pull feature access code (e.g., *11) in the **Call Pull Feature Access Code** field.



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

To configure the private hold soft key via web user interface (not applicable to CP960 IP phones):

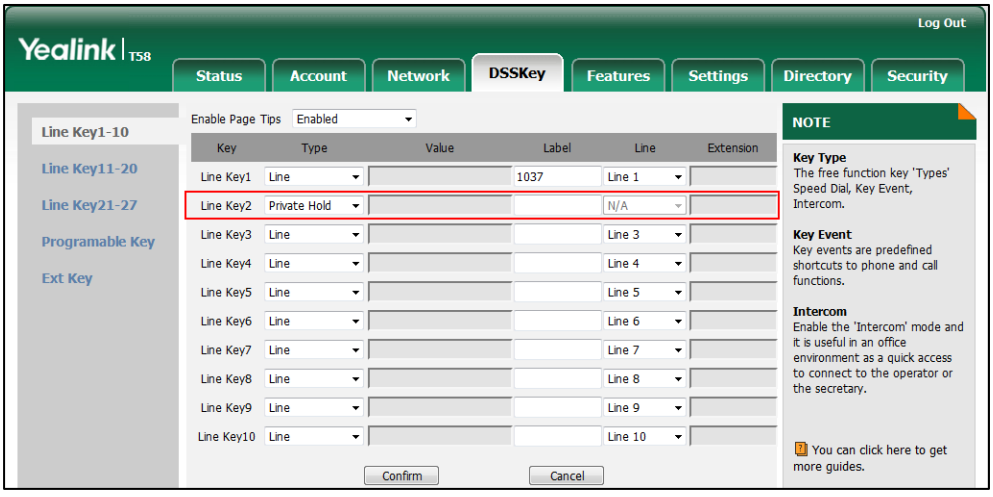
1. Click on **Settings**->**Softkey Layout**.
2. Select **Enabled** from the pull-down list of **Custom Softkey**.
3. Select **On Talk** from the pull-down list of **Call States**.
4. Select **Private Hold** from the **Unselected Softkeys** column and then click →.
   The **Private Hold** appears in the **Selected Softkeys** column.



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

To configure a private hold key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **Private Hold** from the pull-down list of **Type**.
3. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.



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

To configure a private hold key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the **Type** field.
3. Tap **Key Event** in the pop-up dialog box.
4. Tap the **Key Type** field.
5. Tap **Private Hold** in the pop-up dialog box.
6. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
7. Tap ✔ to accept the change.

Message Waiting Indicator (MWI)

Message Waiting Indicator (MWI) informs users of the number of messages waiting in their mailbox without calling the mailbox. IP phones support both audio and visual MWI when receiving new voice messages. MWI will be indicated in three ways: a warning tone, an indicator message (including a voice mail icon) on the touch screen and the power indicator LED slowly flashes red. For more information on power indicator LED, refer to Power Indicator LED on page 145.

IP phones support both solicited and unsolicited MWI.

Unsolicited MWI

Unsolicited MWI is a server related feature. The IP phone sends a SUBSCRIBE message to the server for message-summary updates. The server sends a message-summary NOTIFY within the subscription dialog each time the MWI status changes.

Solicited MWI

For solicited MWI, you must enable MWI subscription feature on IP phones. IP phones support subscribing the MWI messages to the account or the voice mail number.

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure subscribe for MWI. **Parameters:** account.X.subscribe_mwi account.X.subscribe_mwi_expires
		Configure subscribe MWI to voice mail. **Parameter:** account.X.subscribe_mwi_to_vm

		Configure the voice mail number on a per-line basis. **Parameter:** voice_mail.number.X
		Configure the presentation of audio and visual MWI. **Parameter:** account.X.display_mwi.enable
Web User Interface		Configure subscribe for MWI. Configure subscribe MWI to voice mail. Configure the voice mail number on a per-line basis. Configure the presentation of audio and visual MWI. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0
Phone User Interface		Configure the voice mail number on a per-line basis.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.subscribe_mwi	**0 or 1**	**0**

Description:

Enables or disables the IP phone to subscribe the message waiting indicator for account X.

0-Disabled

1-Enabled

If it is set to 1 (Enabled), the IP phone will send a SUBSCRIBE message to the server for message-summary updates.

If it is set to 0 (Disabled), the server automatically sends a message-summary NOTIFY in a new dialog each time the MWI status changes. (This requires server support)

X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)

X is equal to 1 (for CP960)

Web User Interface:

Account->Advanced->Subscribe for MWI

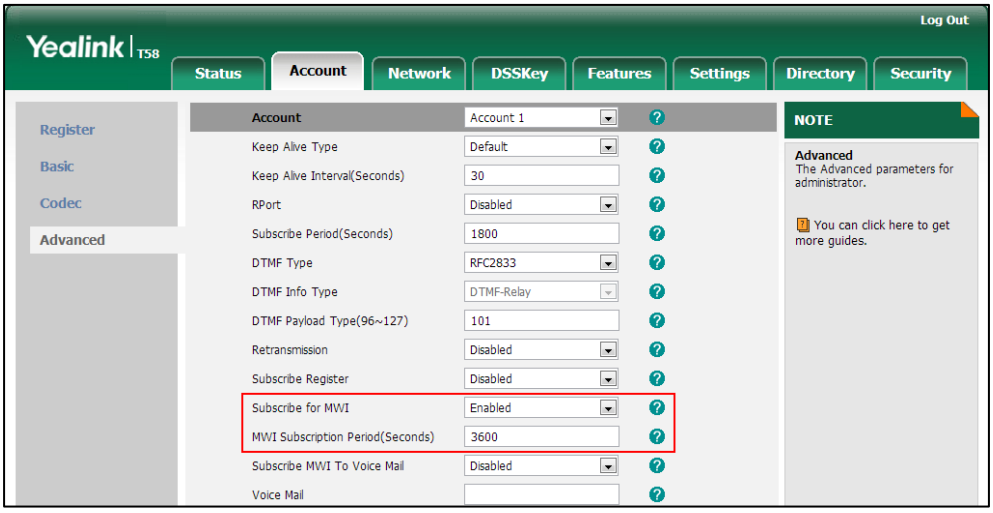
Parameters	Permitted Values	Default
Phone User Interface: None		
account.X.subscribe_mwi_expires	**Integer from 0 to 84600**	**3600**
Description: Configures MWI subscribe expiry time (in seconds) for account X. The IP phone is able to successfully refresh the SUBSCRIBE for message-summary events before expiration of the subscription dialog. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: It works only if the value of the parameter "account.X.subscribe_mwi" is set to 1 (Enabled). **Web User Interface:** Account->Advanced->MWI Subscription Period (Seconds) **Phone User Interface:** None		
account.X.subscribe_mwi_to_vm	**0 or 1**	**0**
Description: Enables or disables the IP phone to subscribe the message waiting indicator to the voice mail number for account X. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone will subscribe the message waiting indicator to the account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: It works only if the value of the parameter "account.X.subscribe_mwi" is set to 1 (Enabled) and "voice_mail.number.X" is configured. **Web User Interface:** Account->Advanced->Subscribe MWI To Voice Mail **Phone User Interface:** None		
voice_mail.number.X	**String within 99 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the voice mail number for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** voice_mail.number.1 = 1234 **Web User Interface:** Account->Advanced->Voice Mail **Phone User Interface:** Message->Voice Mail->Set Voice Mail->AccountX Code		
account.X.display_mwi.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to present audio and visual MWI when receiving new voice messages. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: It always works at the time of Unsolicited MWI; at the time of solicited MWI, MWI subscription feature should be configured in advance. To present audio MWI, you also need to set the value of the parameter "features.voice_mail_tone_enable" to 1 (Enabled) in advance. **Web User Interface:** Account->Advanced->Voice Mail Display **Phone User Interface:** None		

To configure subscribe for MWI via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **Subscribe for MWI**.

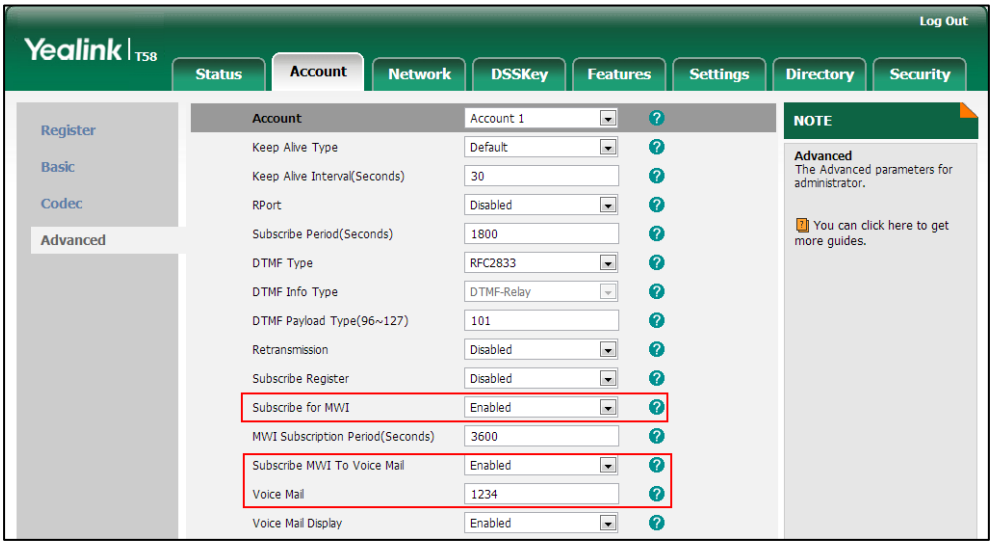
4. Enter the period time in the **MWI Subscription Period(Seconds)** field.



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

To configure subscribe MWI to voice mail via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **Enabled** from the pull-down list of **Subscribe for MWI**.
4. Select the desired value from the pull-down list of **Subscribe MWI To Voice Mail**.
5. Enter the desired voice number in the **Voice Mail** field.

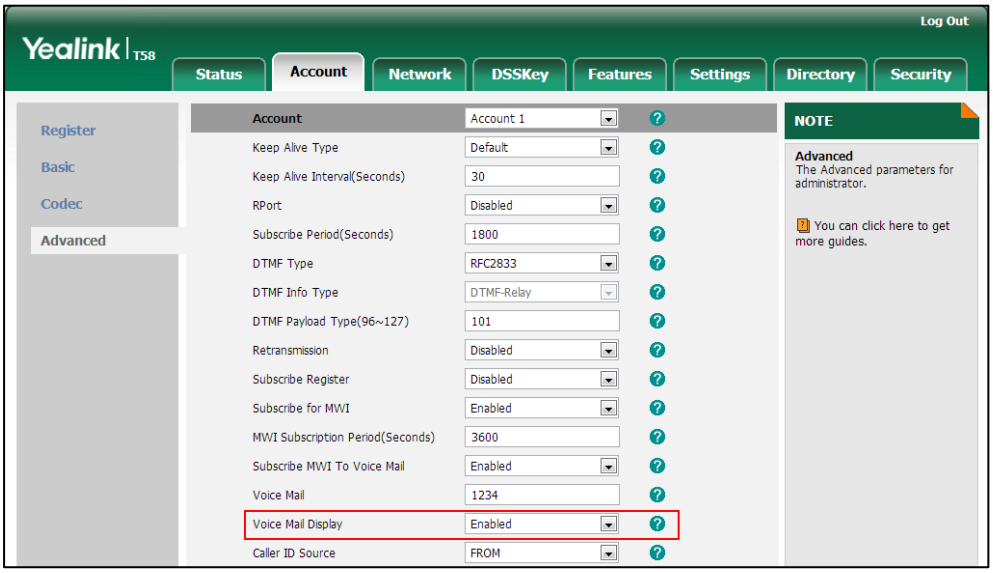


6. Click **Confirm** to accept the change.

To configure the presentation of audio and visual MWI via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

3. Select the desired value from the pull-down list of **Voice Mail Display**.



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

Multicast Paging

Multicast paging allows IP phones to send/receive Real-time Transport Protocol (RTP) streams to/from the pre-configured multicast address(es) on the desired channel without involving SIP signaling. Up to 31 listening multicast addresses can be specified on the IP phone.

Yealink IP phones support the following 31 channels:

- **0**: Yealink IP phones running old firmware version (old paging mechanism) and third-party devices (e.g., Cisco IP phones) supporting paging with Yealink IP phones running old firmware version are all grouped into the channel 0. This is for compatibility with the old Yealink IP phones and third-party devices.
- **1 to 25**: each corresponds to the Polycom's channel 1 to 25 respectively. This is for compatibility with the Polycom IP phones.
- **26 to 30**: This is for separate communication among the Yealink IP phones running new firmware version (new paging mechanism).

The IP phones will automatically ignore all incoming multicast paging calls on the different channel.

Sending RTP Stream

Users can send an RTP stream without involving SIP signaling by tapping a configured multicast paging key or a paging list key. A multicast address (IP: Port) and a channel (0 to 30) should be assigned to the multicast paging key, which is defined to transmit RTP stream to a group of designated IP phones on the desired channel.

When the IP phone sends the RTP stream to a pre-configured multicast address belongs to a desired channel, each IP phone preconfigured to listen to the multicast address on the same channel 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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	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_address
		Configure the channel of the multicast paging group for a paging list key. **Parameter:** multicast.paging_address.X.channel
		Configure the multicast paging group name for a paging list key. **Parameter:** multicast.paging_address.X.label
		Assign a multicast paging key. **Parameters:** linekey.X.type/ expansion_module.X.key.Y.type linekey.X.value/ expansion_module.X.key.Y.value linekey.X.label/ expansion_module.X.key.Y.label linekey.X.extension/ expansion_module.X.key.Y.extension
		Assign a paging list key. **Parameter:** linekey.X.type/programmable.X.type/ expansion_module.X.key.Y.type linekey.X.label/programmable.X.label/

		expansion_module.X.key.Y.label
Web User Interface		Specify a multicast codec for the IP phone to send the RTP stream. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
		Configure the multicast IP address and port number for a paging list key. Configure the multicast paging group name for a paging list key. Configure the channel of the multicast paging group for a paging list key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=contacts-multicastIP&q=load
		Assign a multicast paging key or a paging list key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface		Configure the multicast IP address and port number for a paging list key. Configure the channel of the multicast paging group for a paging list key. Configure the multicast paging group name for a paging list key. Assign a multicast paging key or a paging list key.

Details of the Configuration Parameters:

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 Codec **Phone User Interface:** None		
multicast.paging_address.X.ip_address (X ranges from 1 to 31)	**String**	**Blank**
Description: Configures the IP address and port number of the multicast paging group in the paging list. It will be displayed on the touch screen when placing the multicast paging call. **Example:** multicast.paging_address.1.ip_address = 224.5.6.20:10008 multicast.paging_address.2.ip_address = 224.1.6.25:1001 **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. **Web User Interface:** Directory->Multicast IP->Paging List->Paging Address **Phone User Interface:** Settings->Features->Paging List->Option->Edit->Address		
multicast.paging_address.X.label (X ranges from 1 to 31)	**String**	**Blank**
Description: Configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the touch screen when placing the multicast paging calls. **Example:** multicast.paging_address.1.label = Product multicast.paging_address.2.label = Sales **Web User Interface:** Directory->Multicast IP->Paging List->Label **Phone User Interface:** Settings->Features->Paging List->Option->Edit->Label		
multicast.paging_address.X.channel (X ranges from 1 to 31)	**Integer from 0 to 30**	**0**
Description:		

Parameters	Permitted Values	Default
Configures the channel of the multicast paging group in the paging list. If it is set to 0, all the Yealink IP phones running old firmware version (old paging mechanism) or prior or Yealink IP phones listens to channel 0 or third-party available devices (e.g., Cisco IP phones) in the paging group can receive the RTP stream. If it is set to 1 to 25, the Polycom or Yealink IP phones preconfigured to listen to the channel can receive the RTP stream. It it is set to 26 to 30, the Yealink IP phones preconfigured to listen to the channel can receive the RTP stream. **Example:** multicast.paging_address.1.channel = 3 multicast.paging_address.2.channel = 5 **Web User Interface:** Directory->Multicast IP->Paging List->Channel **Phone User Interface:** Settings->Features->Paging List->Option->Edit->Channel		

Multicast Paging Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ expansion_module.X.key.Y.type	**24**	**Refer to the following content**
Description: Configures a DSS key as a multicast paging key on the IP phone. The digit **24** stands for the key type **Multicast Paging**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:**		

Parameters	Permitted Values	Default
linekey.2.type = 24 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.value/ expansion_module.X.key.Y.value	**String within 99 characters**	**Blank**
Description: Configures the multicast IP address and port number. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.value = 224.5.5.6:10008 **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. **Web User Interface:** DSSKey->Line Key->Value **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Value		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description:		

Parameters	Permitted Values	Default
(Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		
linekey.X.extension/ expansion_module.X.key.Y.extension	**String within 256 characters**	**Blank**
Description: Configures the channel of multicast paging group. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.extension = 2 **Note:** This parameter only applies to multicast paging feature. **Web User Interface:** Dsskey->Line Key/Programable Key->Extension **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Channel		

Paging List key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type	**66**	**Refer to the following content**

Description:

Configures a DSS key as a paging list key on the IP phone.

The digit **66** stands for the key type **Paging List**.

For line keys:

X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)

X ranges from 1 to 30 (for CP960)

For programable keys:

X ranges from 12 to 14 (for SIP-T58V/T58A/T56A)

For ext keys:

X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)

Example:

linekey.2.type = 66

Default:

For line keys:

For SIP-T58V/T58A/T56A IP phones:

The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0.

For CP960 IP phones:

The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0.

For programable keys:

For SIP-T58V/T58A/T56A IP phones:

When X=12, the default value is 0 (NA).

When X=13, the default value is 0 (NA).

When X=14, the default value is 2 (Forward).

For ext keys:

For SIP-T58V/T58A/T56A IP phones:

When Y= 1 to 60, the default value is 0 (NA).

Web User Interface:

DSSKey->Line Key/Programable Key->Type

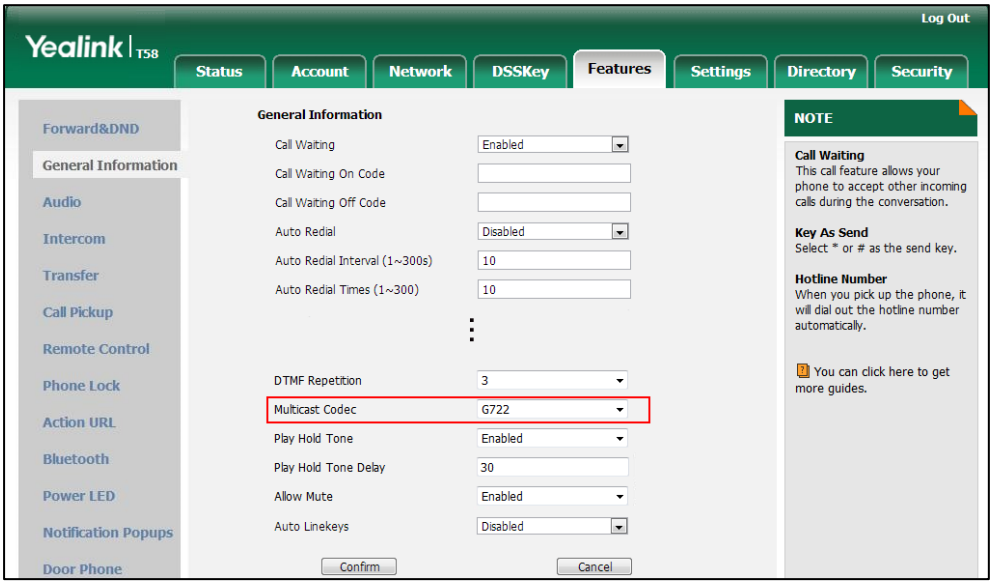
Phone User Interface:

Settings->Features->DSS Keys->Line Key X->Type

Parameters	Permitted Values	Default
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a codec for multicast paging via web user interface:

1. Click on **Features**->**General Information**.
2. Select the desired codec from the pull-down list of **Multicast Codec**.



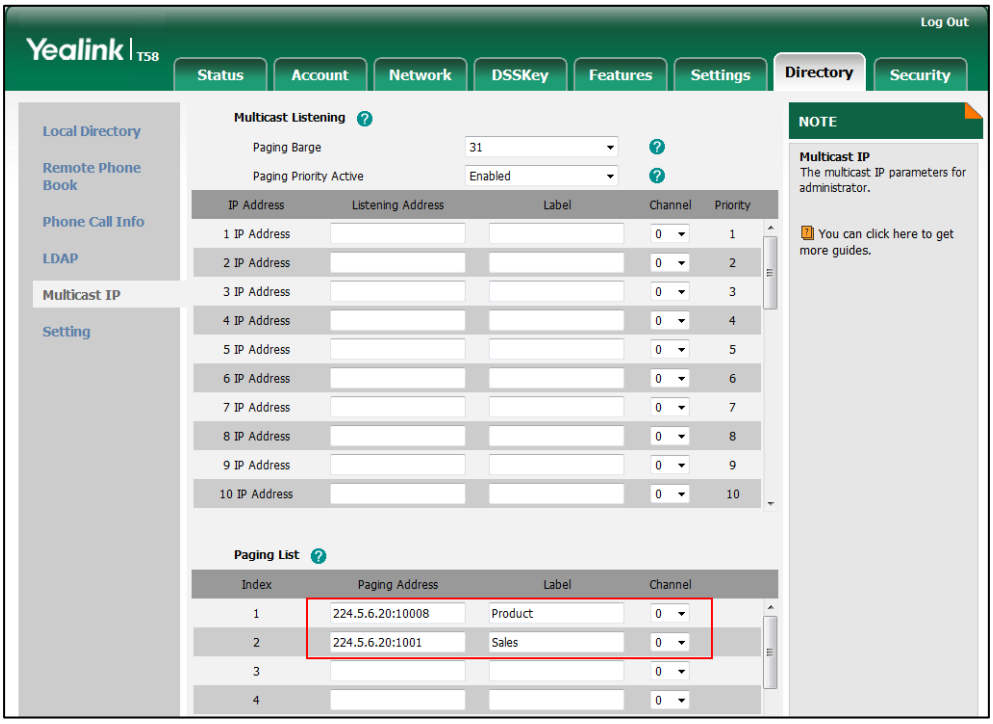
3. Click **Confirm** to accept the change.

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 touch screen when sending the RTP multicast.

4. Select the desired channel from the pull-down list of **Channel**.



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

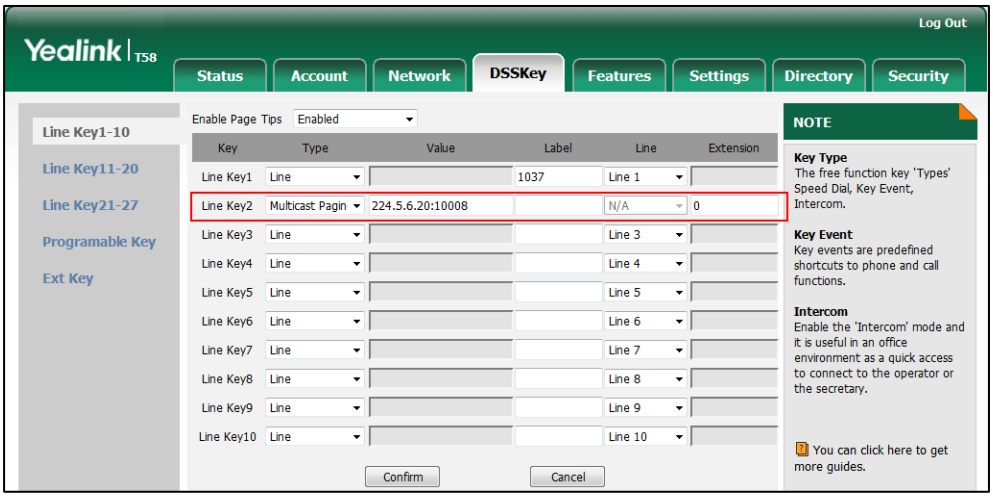
To configure a multicast paging key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Ext Key**).
2. In the desired DSS key field, select **Multicast Paging** from the pull-down list of **Type**.
3. Enter the multicast IP address and port number in the **Value** field.

   The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.
4. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.

5. Enter the desired channel in the **Extension** field.

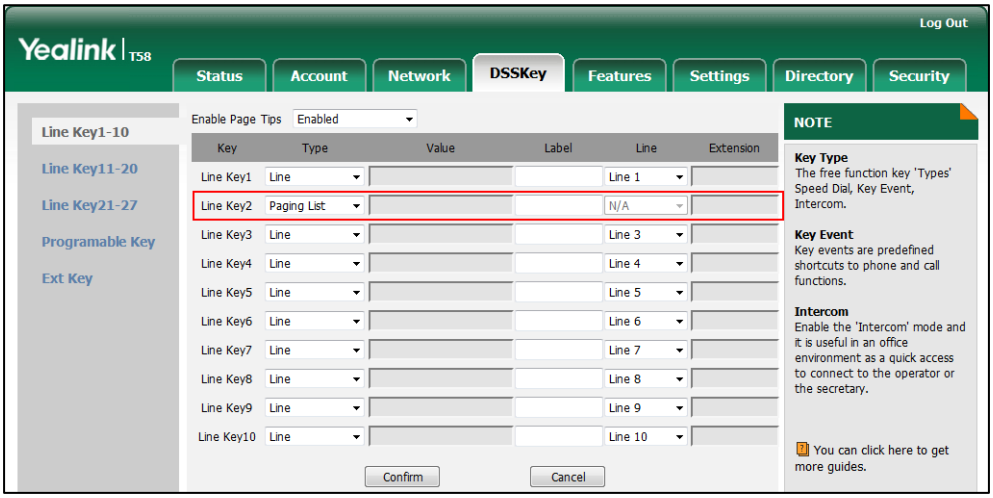
   The valid channel ranges from 0 to 30.



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

To configure a paging list key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **Paging List** from the pull-down list of **Type**.
3. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.



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

To configure a multicast paging key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **Multicast Paging** in the pop-up dialog box.

7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Enter the multicast IP address and port number in the **Value** field.
9. Enter the desired channel in the **Channel** field.
10. Tap ✓ to accept the change.

To configure a paging list key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **Paging List** in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Tap ✓ to accept the change.

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the listening multicast address. **Parameters:** multicast.listen_address.X.ip_address multicast.listen_address.X.label multicast.listen_address.X.channel multicast.listen_address.X.volume multicast.receive.use_speaker
		Configure Paging Barge and Paging Priority Active features. **Parameters:** multicast.receive_priority.enable multicast.receive_priority.priority
Web User Interface		Configure the listening multicast address. Configure Paging Barge and Paging Priority Active features. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=contacts-multicastIP&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
multicast.listen_address.X.ip_address (X ranges from 1 to 31)	**IP address: port**	**Blank**
Description: Configures the multicast address and port number that the IP phone listens to. **Example:** multicast.listen_address.1.ip_address = 224.5.6.20:10008 **Note**: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255. **Web User Interface:** Directory->Multicast IP->Multicast Listening->Listening Address **Phone User Interface:** None		
multicast.listen_address.X.label	**String within 99**	**Blank**

Parameters	Permitted Values	Default
(X ranges from 1 to 31)	**characters**	
Description: (Optional.) Configures the label to be displayed on the touch 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.listen_address.X.channel (X ranges from 1 to 31)	**Integer from 0 to 30**	**0**
Description: Configures the channel that the IP phone listens to. If it is set to 0, the IP phone can receive an RTP stream of the pre-configured multicast address from the IP phones running old firmware version (old paging mechanism), from the IP phones listen to the channel 0, or from the available third-party devices (e.g., Cisco IP phones). If it is set to 1 to 25, the IP phone can receive an RTP stream of the pre-configured multicast address on the channel 1 to 25 respectively from Yealink or Polycom IP phones. It it is set to 26 to 30, the IP phone can receive the RTP stream of the pre-configured multicast address on the channel 26 to 30 respectively from Yealink IP phones. **Example:** multicast.listen_address.1.channel = 2 **Web User Interface:** Directory->Multicast IP->Multicast Listening->Channel **Phone User Interface:** None		
multicast.listen_address.X.volume (X ranges from 1 to 31)	**Integer from 0 to 15**	**0**
Description: Configures the volume of the speaker when receiving the multicast paging calls. If it is set to 0, the current volume of the speaker takes effect. The volume of the speaker can be adjusted by pressing the Volume key in advance when the phone is during a call. You can also adjust the volume of the speaker during the paging call.		

Parameters	Permitted Values	Default
If it is set to 1 to 15, the configured volume takes effect and the current volume of the speaker will be ignored. You are not allowed to adjust the volume of the speaker during the paging call. **Example:** multicast.listen_address.1.volume = 1 **Web User Interface:** None **Phone User Interface:** None		
multicast.receive.use_speaker	**0 or 1**	**0**
Description: Enables or disables the IP phone to always use the speaker as the audio device when receiving the multicast paging calls. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the engaged audio device will be used when receiving the multicast paging calls. **Web User Interface:** None **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:** Directory->Multicast IP->Paging Priority Active **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
multicast.receive_priority.priority	**Integer from 0 to 31**	**31**
Description: Configures the priority of the voice/video call (a normal phone call rather than a multicast paging call) in progress. 1 is the highest priority, 31 is the lowest priority. **0**-Disabled **1**-1 **2**-2 **3**-3 **…** **31**-31 If it is set to 0 (Disabled), all incoming multicast paging calls will be automatically ignored when a voice/video 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/video call is in progress. **Web User Interface:** Directory->Multicast IP->Paging Barge **Phone User Interface:** None		

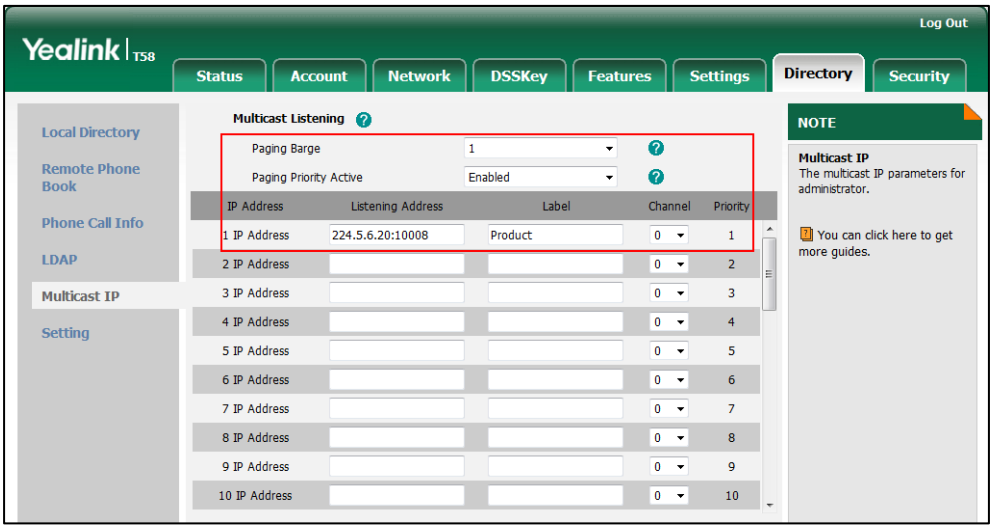
To configure multicast listening addresses via web user interface:

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**.
4. Enter the multicast IP address(es) and port number (e.g., 224.5.6.20:10008) which the phone listens to for incoming RTP multicast in the **Listening Address** field.

   1 is the highest priority and 31 is the lowest priority.
5. Enter the label in the **Label** field.

   Label will appear on the touch screen when receiving the multicast RTP stream.

6. Select the desired channel from the pull-down list of **Channel**.



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

Call Recording Using DSS Keys (Record and URL Record)

Yealink IP phones support record calls by tapping the call record key. It depends on support from a SIP server. When the user taps the call record key, the IP phone sends a record request to the server. IP phones themselves do not have memory to store the recording, what they can do is to trigger the recording and indicate the recording status.

Normally, there are 2 main methods to trigger a recording on a certain server. We call them record and URL record. Record is for the IP phone to send the server a SIP INFO message containing a specific header. URL record is for the IP phone to send the server an HTTP GET message containing a specific URL. The server processes these messages and decides to start or stop a recording.

Note If it is a video call, you can only record the audio but not video by tapping record/URL record key. For more information on recording video calls, refer to Call Recording Using Soft Key on page 439.

Record

When a user taps a record key for the first time during a call, the IP phone sends a SIP INFO message to the server with the specific header "Record: on", and then the recording starts.

Example of a SIP INFO message:

```
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK1870385345
From: "1009" <sip:1009@10.2.1.48:5060>;tag=1385842459
To: <sip:1006@10.2.1.48:5060>;tag=2383911905
Call-ID: 0_1289812066@10.3.20.14
CSeq: 2 INFO
Contact: <sip:1009@10.3.20.14:5060>
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Record: on
Content-Length: 0
```

When the user taps the record key for the second time, the IP phone sends a SIP INFO message to the server with the specific header "Record: off", and then the recording stops.

Example of a SIP INFO message:

```
Via: SIP/2.0/UDP 10.3.20.14:5060;branch=z9hG4bK175716007
From: "1009" <sip:1009@10.2.1.48:5060>;tag=1385842459
To: <sip:1006@10.2.1.48:5060>;tag=2383911905
Call-ID: 0_1289812066@10.3.20.14
CSeq: 3 INFO
Contact: <sip:1009@10.3.20.14:5060>
Max-Forwards: 70
User-Agent: Yealink T58 58.80.0.5
Record: off
Content-Length: 0
```

URL Record

When a user taps a URL record key for the first time during a call, the IP phone sends an HTTP GET message to the server.

Example of an HTTP GET message:

```
GET /URLRecord/record.xml HTTP/1.1\r\n
Request Method: GET
Request URI: /URLRecord/record.xml
Request version: HTTP/1.1
Host: 10.3.5.97:8080\r\n
User-agent: Yealink T58 58.80.0.5 00:15:65:74:B1:50\r\n
```

If the recording is successfully started, the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
 <Title>
```

```
    </Title>
 <Text>
    The recording session is successfully started.
    </Text>
<YealinkIPPhoneText>
```

If the recording fails for some reasons, for example, the recording box is full, the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
 <Title>
    </Title>
 <Text>
    Probably the recording box is full.
    </Text>
<YealinkIPPhoneText>
```

When the user taps the URL record key for the second time, the IP phone sends an HTTP GET message to the server, and then the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
 <Title>
    </Title>
 <Text>
    The recording session is successfully stopped.
    </Text>
<YealinkIPPhoneText>
```

Procedure

Record or URL record key can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Assign a record key. **Parameters:** linekey.X.type/ expansion_module.X.key.Y.type linekey.X.label/ expansion_module.X.key.Y.label
		Assign a URL record key. **Parameters:** linekey.X.type/ expansion_module.X.key.Y.type linekey.X.value/

		expansion_module.X.key.Y.value linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Assign a record key and URL record key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface		Assign a record key and URL record key.

Record Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
linekey.X.type/ expansion_module.X.key.Y.type	**25**	**Refer to the following content**
Description: Configures a DSS key as a record key on the IP phone. The digit **25** stands for the key type **Record**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 25 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0.		

Parameters	Permitted Values	Default
For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

URL Record Key

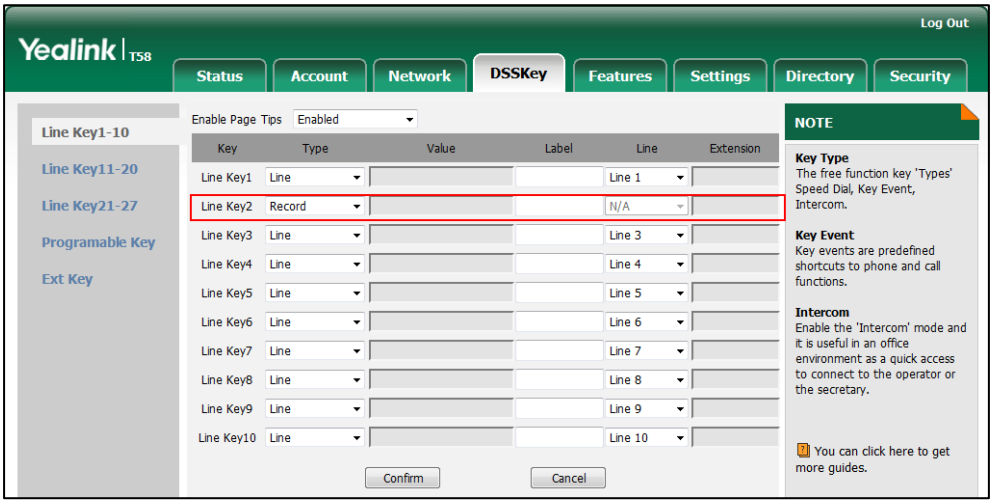
Parameters	Permitted Values	Default
linekey.X.type/ expansion_module.X.key.Y.type	**35**	**Refer to the following content**
Description: Configures a DSS key as a URL record key on the IP phone. The digit **35** stands for the key type **URL Record**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960)		

Parameters	Permitted Values	Default
For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.type = 35 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.value/ expansion_module.X.key.Y.value	**String within 99 characters**	**Blank**
Description: Configures the URL to record a call. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.2.value = http://10.3.5.97:8080/URLRecord/record.xml **Web User Interface:** DSSKey->Line Key->Value **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Value		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**

Parameters	Permitted Values	Default
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a record key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Ext Key**).
2. In the desired DSS key field, select **Record** from the pull-down list of **Type**.
3. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.

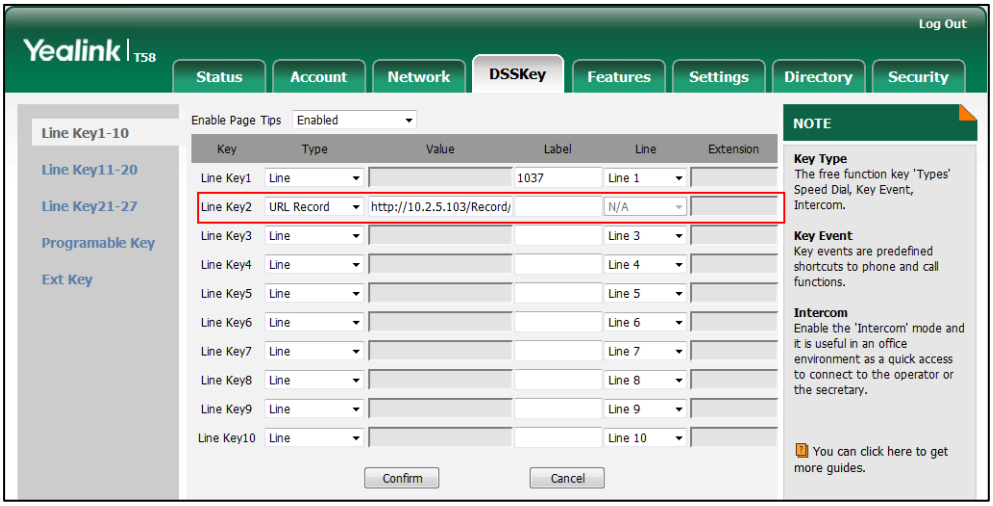


4. Click **Confirm** to accept the change.

To configure a URL record key via web user interface:

1. Click on **DSSKey**->**Line Key**.
2. In the desired DSS key field, select **URL Record** from the pull-down list of **Type**.
3. Enter the URL in the **Value** field.

4. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.



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

To configure a record key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **Record** in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Tap ✓ to accept the change.

To configure a URL record key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **URL Record** in the pop-up dialog box.
5. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
6. Enter the URL in the **Value** field.
7. Tap ✓ to accept the change.

Hot Desking

Hot desking originates from the definition of being the temporary physical occupant of a work station or surface by a particular employee. A primary motivation for hot desking is cost reduction. Hot desking is regularly used in places where not all employees are in the office at

the same time, or not in the office for a long time, which means actual personal offices would often be vacant, consuming valuable space and resources.

Hot desking allows a user to clear registration configurations of all accounts on the IP phone, and then register his account on line 1. To use this feature, you need to assign a hot desking key.

Procedure

Hot Desking feature can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the hot desking login wizard. **Parameters:** hotdesking.dsskey_register_name_enable hotdesking.dsskey_username_enable hotdesking.dsskey_password_enable hotdesking.dsskey_sip_server_enable hotdesking.dsskey_outbound_enable
		Assign a hot desking key. **Parameters:** linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type linekey.X.label/ expansion_module.X.key.Y.label
Web User Interface		Assign a hot desking key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
Phone User Interface		Assign a hot desking key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
hotdesking.dsskey_register_name_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to provide input field of register name on the hot desking login wizard when tapping the Hot Desking key. **0**-Disabled **1**-Enabled **Web User Interface:**		

Parameters	Permitted Values	Default
None **Phone User Interface:** None		
hotdesking.dsskey_username_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to provide input field of user name on the hot desking login wizard when tapping the Hot Desking key. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
hotdesking.dsskey_password_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to provide input field of password on the hot desking login wizard when tapping the Hot Desking key. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
hotdesking.dsskey_sip_server_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to provide input field of SIP server on the hot desking login wizard when tapping the Hot Desking key. **0**-Disabled **1**-Enabled **Web User Interface:** None		

Parameters	Permitted Values	Default
Phone User Interface: None		
hotdesking.dsskey_outbound_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to provide input field of outbound server on the hot desking login wizard when tapping the Hot Desking key. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		

Hot Desking Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

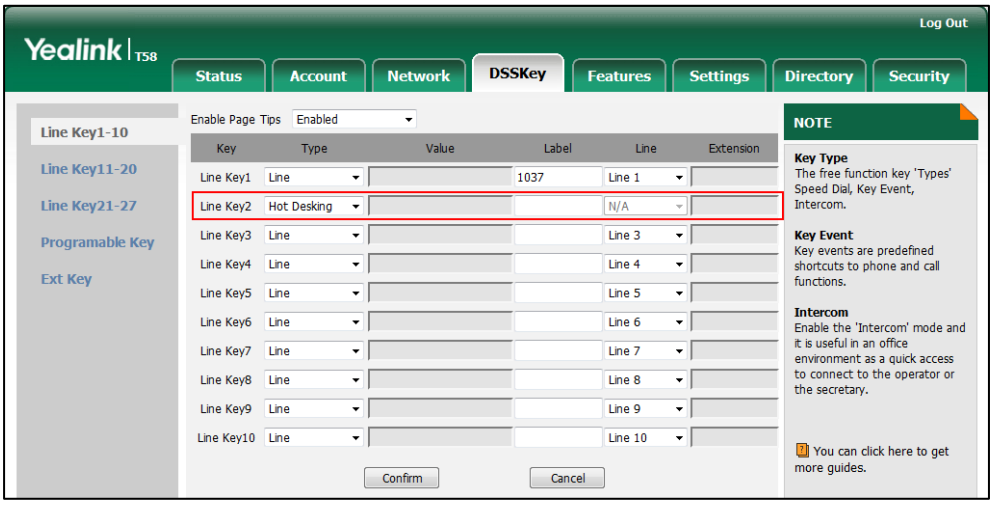
Parameters	Permitted Values	Default
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type	**34**	**Refer to the following content**
Description: Configures a DSS key as a hot desking key on the IP phone. The digit **34** stands for the key type **Hot Desking**. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:**		

Parameters	Permitted Values	Default
linekey.2.type = 34 **Default:** For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For programable keys: **For SIP-T58V/T58A/T56A IP phones:** When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key/Programable Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Type		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the touch screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure a hot desking key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).

2. In the desired DSS key field, select **Hot Desking** from the pull-down list of **Type**.
3. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.



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

To configure a hot desking key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **Hot Desking** in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Tap ✓ to accept the change.

Logon Wizard

Logon wizard allows IP phones to provide the logon wizard during the first startup.

Note Logon wizard feature works only if there is no registered account on the IP phone.

Procedure

Logon wizard can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the logon wizard. **Parameters:** phone_setting.logon_wizard hotdesking.startup_register_name_enable

		hotdesking.startup_username_enable hotdesking.startup_password_enable hotdesking.startup_sip_server_enable hotdesking.startup_outbound_enable
Web User Interface		Configure the logon wizard. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of the Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.logon_wizard	**0 or 1**	**0**
Description: Enables or disables the IP phone to provide the logon wizard during the first startup. **0**-Disabled **1**-Enabled **Note:** It works only if there is no registered account on the IP phone. **Web User Interface:** Features->General Information->Logon Wizard **Phone User Interface:** None		
hotdesking.startup_register_name_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to provide input field of register name on the logon wizard during the first startup. **0**-Disabled **1**-Enabled **Note:** It works only if there is no registered account on the IP phone and the value of the parameter "phone_setting.logon_wizard" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		

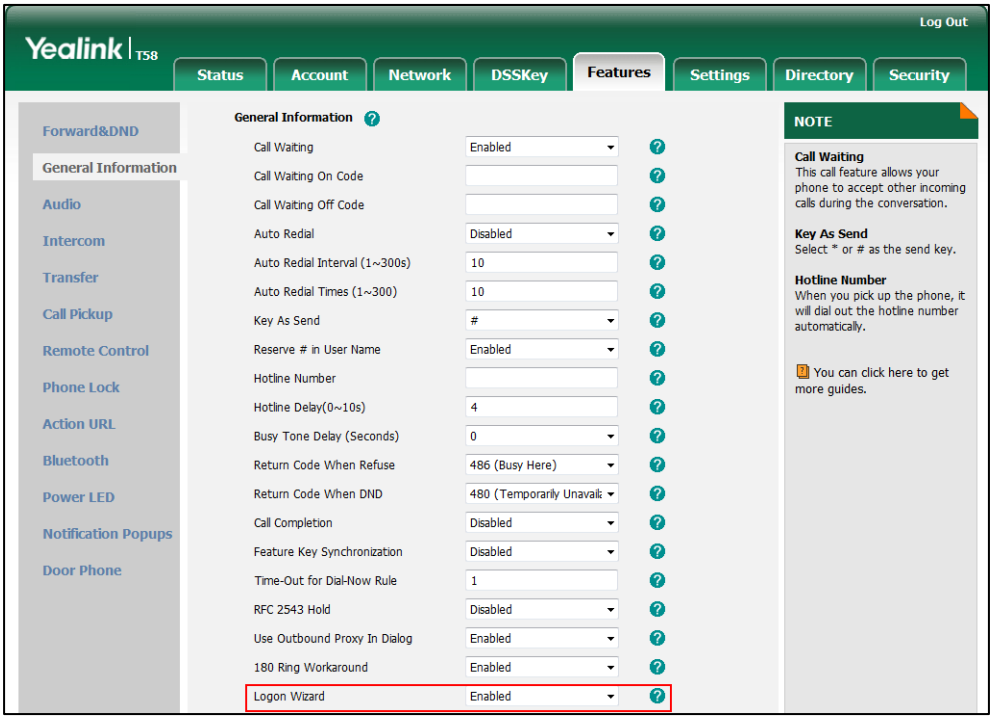
Parameters	Permitted Values	Default
hotdesking.startup_username_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to provide input field of user name on the logon wizard during the first startup. **0**-Disabled **1**-Enabled **Note:** It works only if there is no registered account on the IP phone and the value of the parameter "phone_setting.logon_wizard" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		
hotdesking.startup_password_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to provide input field of password on the logon wizard during the first startup. **0**-Disabled **1**-Enabled **Note:** It works only if there is no registered account on the IP phone and the value of the parameter "phone_setting.logon_wizard" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		
hotdesking.startup_sip_server_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to provide input field of SIP server on the logon wizard during the first startup. **0**-Disabled **1**-Enabled **Note:** It works only if there is no registered account on the IP phone and the value of the parameter "phone_setting.logon_wizard" is set to 1 (Enabled).		

Parameters	Permitted Values	Default
Web User Interface: None **Phone User Interface:** None		
hotdesking.startup_outbound_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to provide input field of outbound server on the logon wizard during the first startup. **0**-Disabled **1**-Enabled **Note:** It works only if there is no registered account on the IP phone and the value of the parameter "phone_setting.logon_wizard" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		

To configure logon wizard feature via web user interface:

1. Click on **Features**->**General Information**.

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



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

Action URL

Action URL allows IP phones to interact with web server applications by sending an HTTP or HTTPS GET request. You can specify a URL that triggers a GET request when a specified event occurs. Action URL can only be triggered by the pre-defined events (e.g., Open DND). The valid URL format is: *http(s)://<serverIPAddress>/help.xml?*.

The following table lists the pre-defined events for action URL.

Event	Description
Setup Completed	When the IP phone completes startup.
Registered	When the IP phone successfully registers an account.
Unregistered	When the IP phone logs off the registered account.
Register Failed	When the IP phone fails to register an account.
Off Hook	When the IP phone is off hook (not applicable to CP960 IP phones).
On Hook	When the IP phone is on hook (not applicable to CP960 IP phones).
Incoming Call	When the IP phone receives an incoming call.
Outgoing Call	When the IP phone places a call.

Event	Description
Established	When the IP phone establishes a call.
Terminated	When the IP phone terminates a call.
Open DND	When the IP phone enables the DND mode.
Close DND	When the IP phone disables the DND mode.
Open Always Forward	When the IP phone enables the always forward.
Close Always Forward	When the IP phone disables the always forward.
Open Busy Forward	When the IP phone enables the busy forward.
Close Busy Forward	When the IP phone disables the busy forward.
Open NoAnswer Forward	When the IP phone enables the no answer forward.
Close NoAnswer Forward	When the IP phone disables the no answer forward.
Transfer Call	When the IP phone transfers a call.
Blind Transfer	When the IP phone blind transfers a call.
Attended Transfer	When the IP phone performs the semi-attended/attended transfer.
Hold	When the IP phone places a call on hold.
UnHold	When the IP phone resumes a hold call.
Held	When a call of the IP phone is held.
UnHeld	When a held call is resumed.
Mute	When the IP phone mutes a call.
UnMute	When the IP phone unmutes a call.
Missed Call	When the IP phone misses a call.
IP Changed	When the IP address of the IP phone changes.
Idle To Busy	When the state of the IP phone changes from idle to busy.
Busy To Idle	When the state of phone changes from busy to idle.
Reject Incoming Call	When the IP phone rejects an incoming call.
Answer New-In Call	When the IP phone answers a new call.
Transfer Failed	When the IP phone fails to transfer a call.
Transfer Finished	When the IP phone completes to transfer a call.
Forward Incoming Call	When the IP phone forwards an incoming call.
Autop Finish	When the IP phone completes auto provisioning via power on.

Event	Description
Open Call Waiting	When the IP phone enables the call waiting.
Close Call Waiting	When the IP phone disables the call waiting.
Headset	When the IP phone presses the HEADSET key (not applicable to CP960 IP phones).
Handfree	When the IP phone presses the Speakerphone key (not applicable to CP960 IP phones).
Cancel Call Out	When the IP phone cancels an outgoing call in the ring-back state.
Remote Busy	When an outgoing call is rejected.
Call Remote Canceled	When the remote party cancels the outgoing call in the ringing state.

An HTTP or HTTPS GET request may contain variable name and variable value, separated by "=". Each variable value starts with $ in the query part of the URL. The valid URL format is: http(s)://<serverIPAddress>/help.xml?variable name=$variable value. Variable name can be customized by users, while the variable value is pre-defined. For example, a URL "*http://192.168.1.10/help.xml?mac=$mac*" is specified for the event Mute, $mac will be dynamically replaced with the MAC address of the IP phone when the IP phone mutes a call.

The following table lists pre-defined variable values.

Variable Value	Description
$mac	The MAC address of the IP phone.
$ip	The IP address of the IP phone.
$model	The IP phone model.
$firmware	The firmware version of the IP phone.
$active_url	The SIP URI of the current account when the IP phone places a call, receives an incoming call or establishes a call.
$active_user	The user part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
$active_host	The host part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.
$local	The SIP URI of the caller when the IP phone places a call. The SIP URI of the callee when the IP phone receives an incoming call.

Variable Value	Description
$remote	The SIP URI of the callee when the IP phone places a call. The SIP URI of the caller when the IP phone receives an incoming call.
$display_local	The display name of the caller when the IP phone places a call. The display name of the callee when the IP phone receives an incoming call.
$display_remote	The display name of the callee when the IP phone places a call. The display name of the caller when the IP phone receives an incoming call.
$call_id	The call-id of the active call.
$callerID	The display name of the caller when the IP phone receives an incoming call.
$calledNumber	The phone number of the callee when the IP phone places a call.

Procedure

Action URL can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure action URL. **Parameters:** action_url.setup_completed action_url.registered action_url.unregistered action_url.register_failed action_url.off_hook action_url.on_hook action_url.incoming_call action_url.outgoing_call action_url.call_established action_url.dnd_on action_url.dnd_off action_url.always_fwd_on action_url.always_fwd_off action_url.busy_fwd_on action_url.busy_fwd_off

		action_url.no_answer_fwd_on action_url.no_answer_fwd_off action_url.transfer_call action_url.blind_transfer_call action_url.attended_transfer_call action_url.hold action_url.unhold action_url.held action_url.unheld action_url.mute action_url.unmute action_url.missed_call action_url.call_terminated action_url.busy_to_idle action_url.idle_to_busy action_url.ip_change action_url.forward_incoming_call action_url.reject_incoming_call action_url.answer_new_incoming_call action_url.transfer_finished action_url.transfer_failed action_url.setup_autop_finish action_url.call_waiting_on action_url.call_waiting_off action_url.headset action_url.handfree action_url.cancel_callout action_url.remote_busy action_url.call_remote_canceled
Web User Interface		Configure action URL. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-actionurl&q=load

Details of Configuration Parameters:

<table>
<tr><th>Parameters</th><th>Permitted Values</th><th>Default</th></tr>
<tr><td>action_url.setup_completed</td><td>URL within 511 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the action URL the IP phone sends after startup.
The value format is: http(s)://<serverIPAddress>/help.xml? variable name=variable value.
Valid variable values are:
● $mac
● $ip
● $model
● $firmware
● $active_url
● $active_user
● $active_host
● $local
● $remote
● $display_local
● $display_remote
● $call_id
● $callerID
● $calledNumber
Example:
action_url.setup_completed = http://192.168.0.20/help.xml?IP=$ip
Web User Interface:
Features->Action URL->Setup Completed
Phone User Interface:
None</td></tr>
<tr><td>action_url.registered</td><td>URL within 511 characters</td><td>Blank</td></tr>
<tr><td colspan="3">Description:
Configures the action URL the IP phone sends after an account is registered.
Example:
action_url.registered = http://192.168.0.20/help.xml?IP=$ip</td></tr>
</table>

Parameters	Permitted Values	Default
Web User Interface: Features->Action URL->Registered **Phone User Interface:** None		
action_url.unregistered	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends after an account is unregistered. **Example**: action_url.unregistered = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Unregistered **Phone User Interface:** None		
action_url.register_failed	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends after a register failed. **Example**: action_url.register_failed = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Register Failed **Phone User Interface:** None		
action_url.off_hook	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when off hook. **Example**: action_url.off_hook = http://192.168.0.20/help.xml?IP=$ip **Note**: It is not applicable to CP960 IP phones.		

Parameters	Permitted Values	Default
Web User Interface: Features->Action URL->Off Hook **Phone User Interface:** None		
action_url.on_hook	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when on hook. **Example**: action_url.on_hook = http://192.168.0.20/help.xml?IP=$ip **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Action URL->On Hook **Phone User Interface:** None		
action_url.incoming_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when receiving an incoming call. **Example**: action_url.incoming_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Incoming Call **Phone User Interface:** None		
action_url.outgoing_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when placing a call. **Example**: action_url.outgoing_call = http://192.168.0.20/help.xml?IP=$ip		

Parameters	Permitted Values	Default
Web User Interface: Features->Action URL->Outgoing Call **Phone User Interface:** None		
action_url.call_established	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when establishing a call. **Example**: action_url.call_established = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Established **Phone User Interface:** None		
action_url.dnd_on	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when DND feature is enabled. **Example**: action_url.dnd_on = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Open DND **Phone User Interface:** None		
action_url.dnd_off	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when DND feature is disabled. **Example**: action_url.dnd_off = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Close DND		

Parameters	Permitted Values	Default
Phone User Interface: None		
action_url.always_fwd_on	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when always forward feature is enabled. **Example**: action_url.always_fwd_on = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Open Always Forward **Phone User Interface:** None		
action_url.always_fwd_off	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when always forward feature is disabled. **Example**: action_url.always_fwd_off = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Close Always Forward **Phone User Interface:** None		
action_url.busy_fwd_on	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when busy forward feature is enabled. **Example**: action_url.busy_fwd_on = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Open Busy Forward **Phone User Interface:** None		

Parameters	Permitted Values	Default
action_url.busy_fwd_off	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when busy forward feature is disabled. **Example**: action_url.busy_fwd_off = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Close Busy Forward **Phone User Interface:** None		
action_url.no_answer_fwd_on	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when no answer forward feature is enabled. **Example**: action_url.no_answer_fwd_on = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Open NoAnswer Forward **Phone User Interface:** None		
action_url.no_answer_fwd_off	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when no answer forward feature is disabled. **Example**: action_url.no_answer_fwd_off = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Close NoAnswer Forward **Phone User Interface:** None		
action_url.transfer_call	**URL within 511 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the action URL the IP phone sends when performing a transfer. **Example**: action_url.transfer_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Transfer Call **Phone User Interface:** None		
action_url.blind_transfer_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when performing a blind transfer. **Example**: action_url.blind_transfer_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Blind Transfer **Phone User Interface:** None		
action_url.attended_transfer_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when performing an attended/semi-attended transfer. **Example**: action_url.attended_transfer_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Attended Transfer **Phone User Interface:** None		
action_url.hold	**URL within 511 characters**	**Blank**
Description:		

Parameters	Permitted Values	Default
Configures the action URL the IP phone sends when placing a call on hold. **Example**: action_url.hold = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Hold **Phone User Interface:** None		
action_url.unhold	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when resuming a hold call. **Example**: action_url.unhold = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->UnHold **Phone User Interface:** None		
action_url.held	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when a call is held. **Example**: action_url.held = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** None **Phone User Interface:** None		
action_url.unheld	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when a call being held is resumed. **Example**:		

Parameters	Permitted Values	Default
action_url.unheld = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** None **Phone User Interface:** None		
action_url.mute	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when muting a call. **Example**: action_url.mute = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Mute **Phone User Interface:** None		
action_url.unmute	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when un-muting a call. **Example**: action_url.unmute = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->UnMute **Phone User Interface:** None		
action_url.missed_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when missing a call. **Example**: action_url.missed_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:**		

Parameters	Permitted Values	Default
Features->Action URL->Missed Call **Phone User Interface:** None		
action_url.call_terminated	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when terminating a call. **Example**: action_url.call_terminated = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Terminated **Phone User Interface:** None		
action_url.busy_to_idle	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when changing the state of the IP phone from busy to idle. **Example:** action_url.busy_to_idle = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Busy To Idle **Phone User Interface:** None		
action_url.idle_to_busy	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when changing the state of the IP phone from idle to busy. **Example**: action_url.idle_to_busy = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Idle To Busy		

Parameters	Permitted Values	Default
Phone User Interface: None		
action_url.ip_change	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when changing the IP address of the IP phone. **Example**: action_url.ip_change = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->IP Changed **Phone User Interface:** None		
action_url.forward_incoming_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when forwarding an incoming call. **Example**: action_url.forward_incoming_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Forward Incoming Call **Phone User Interface:** None		
action_url.reject_incoming_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when rejecting an incoming call. **Example**: action_url.reject_incoming_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Reject Incoming Call **Phone User Interface:** None		

Parameters	Permitted Values	Default
action_url.answer_new_incoming_call	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when answering a new incoming call. **Example**: action_url.answer_new_incoming_call = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Answer New-In Call **Phone User Interface:** None		
action_url.transfer_finished	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when completing a call transfer. **Example**: action_url.transfer_finished = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Transfer Finished **Phone User Interface:** None		
action_url.transfer_failed	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when failing to transfer a call. **Example**: action_url.transfer_failed = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Transfer Failed **Phone User Interface:** None		
action_url.setup_autop_finish	**URL within 511 characters**	**Blank**

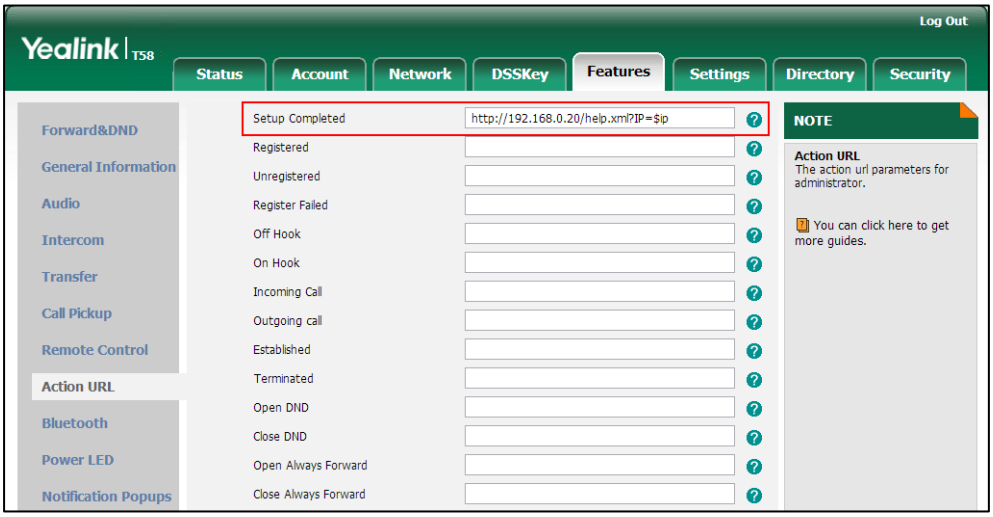
Parameters	Permitted Values	Default
Description: Configures the action URL the IP phone sends when completing auto provisioning via power on. **Example**: action_url.setup_autop_finish = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Autop Finish **Phone User Interface:** None		
action_url.call_waiting_on	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when call waiting feature is enabled. **Example**: action_url.call_waiting_on = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Open Call Waiting **Phone User Interface:** None		
action_url.call_waiting_off	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when call waiting feature is disabled. **Example**: action_url.call_waiting_off = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Close Call Waiting **Phone User Interface:** None		
action_url.headset	**URL within 511 characters**	**Blank**
Description:		

Parameters	Permitted Values	Default
Configures the action URL the IP phone sends when pressing the HEADSET key. **Example**: action_url.headset = http://192.168.0.20/help.xml?IP=$ip **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Action URL->Headset **Phone User Interface:** None		
action_url.handfree	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when pressing the Speakerphone key. **Example**: action_url.handfree = http://192.168.0.20/help.xml?IP=$ip **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->Action URL->Handfree **Phone User Interface:** None		
action_url.cancel_callout	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when cancelling the outgoing call in the ring-back state. **Example**: action_url.cancel_callout = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Cancel Call Out **Phone User Interface:** None		
action_url.remote_busy	**URL within 511 characters**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the action URL the IP phone sends when the outgoing call is rejected. **Example**: action_url.remote_busy = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Remote Busy **Phone User Interface:** None		
action_url.call_remote_canceled	**URL within 511 characters**	**Blank**
Description: Configures the action URL the IP phone sends when the remote party cancels the outgoing call in the ringing state. **Example**: action_url.call_remote_canceled = http://192.168.0.20/help.xml?IP=$ip **Web User Interface:** Features->Action URL->Call Remote Canceled **Phone User Interface:** None		

To configure action URL via web user interface:

1. Click on **Features**->**Action URL**.
2. Enter the action URLs in the corresponding fields.



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

Action URI

HTTP/HTTPS GET Request

Opposite to action URL, 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. A GET request may contain variable named as "key" and variable value, which are separated by "=". The valid URI format is: *http(s)://<phoneIPAddress>/servlet?key=variable value*. For example: http://10.10.20.10/servlet?key=SPEAKER.

Note Yealink IP phones are compatible with other two old valid URI formats: *http(s)://<phoneIPAddress>/cgi-bin/ConfigManApp.com?key=variable value* and *http(s)://<phoneIPAddress>/cgi-bin/cgiServer.exx?key=variable value*.

SIP Notify Message

In addition, Yealink IP phones support performing the specified action immediately by accepting a SIP NOTIFY message with the "Event: ACTION-URI" header from a SIP proxy server. The message body of the SIP NOTIFY message may contain variable named as "key" and variable value, which are separated by "=".

This method is especially useful for users always working in the small office/home office where a secure firewall may prevent the HTTP or HTTPS GET request from the external network.

Note If you want to only accept the SIP NOTIFY message from your SIP server and outbound proxy server, you have to enable the Accept SIP Trust Server Only feature. For more information, refer to Accept SIP Trust Server Only on page 300.

Example of a SIP Notify with the variable value (SPEAKER):

Message Header

NOTIFY sip:3583@10.2.40.10:5062 SIP/2.0

Via: SIP/2.0/UDP 10.2.40.27:5063;branch=z9hG4bK4163876675

From: <sip:3586@10.2.1.48>;tag=2900480538

To: "3583" <sip:3583@10.2.1.48>;tag=490600926

Call-ID: 2923387519@10.2.40.10

CSeq: 4 NOTIFY

Contact: <sip:3586@10.2.40.27:5063>

Max-Forwards: 70

User-Agent: Yealink T58 58.80.0.5

Event: ACTION-URI

Content-Type: message/sipfrag

Content-Length: 6

Message Body

key=SPEAKER

The following table lists pre-defined variable values:

Variable Value	Phone Action
OK	Tap **Settings**->**Status**.
SPEAKER	Press the Speakerphone key (not applicable to CP960 IP phones).
F_TRANSFER	Transfer a call to another party.
VOLUME_UP	Increase the volume.
VOLUME_DOWN	Decrease the volume.
MUTE	Mute a call.
F_HOLD/HOLD	Place an active call on hold.
F_CONFERENCE	Tap the **Conference** soft key (not applicable to CP960 IP phones).
Cancel/CANCEL/X	Cancel actions or reject incoming calls or end a call.
0-9/*/POUND	Press the keypad (0-9, * or #) (not applicable to CP960 IP phones).
L1-LX	Tap the line keys (X=27).
MSG	Press the MESSAGE key (not applicable to CP960 IP phones).
HEADSET	Press the HEADSET key (not applicable to CP960 IP phones).
RD	Redial the last dialed number (not applicable to CP960 IP phones).
Reboot	Reboot the phone.
AutoP	Perform auto provisioning.
DNDOn	Activate the DND feature.
DNDOff	Deactivate the DND feature.

Variable Value	Phone Action
number=xxx&outgoing_uri=y	Place a call to xxx from SIP URI y. **Example**: http://10.3.20.10/servlet?key=number=1234&outgoing_uri=1006@10.2.1.48 (1234 means the number you dial out; 1006@10.2.1.48 means the SIP URL you dial from.)
OFFHOOK	Pick up the handset (not applicable to CP960 IP phones).
ONHOOK	Hang up the handset (not applicable to CP960 IP phones).
ANSWER/ASW/Asw	Answer a call.
Reset	Reset a phone.
ATrans=xxx	Perform a semi-attended/attended transfer to xxx.
BTrans=xxx	Perform a blind transfer to xxx.
CALLEND/CallEnd	End a call.
CallWaitingOn	Activate the call waiting feature.
CallWaitingOff	Deactivate the call waiting feature.
AlwaysFwdOn/BusyFwdOn/NoAnswFwdOn=xxx=n	Activate an always/busy/no answer forward feature to xxx for the IP phone ("xxx" means the destination number). The valid value of "n" means the duration time (seconds) before forwarding incoming calls (n is the times of 6, e.g., 24). It is only applicable to no answer forward feature. **Note**: It works only if the call forward mode is Phone, the always/busy/no answer forward feature will apply to all the accounts on the phone. **Example**: http://10.10.20.10/servlet?key=NoAnswFwdOn=1001=24

Variable Value	Phone Action
AlwaysFwdOff/BusyFwdOff/NoAnswFwdOff	Deactivate the always/busy/no answer forward feature for the IP phone. **Note**: It works only if the call forward mode is Phone, the always/busy/no answer forward feature will apply to all the accounts on the phone. **Example**: http://10.10.20.10/servlet?key=NoAnswFwdOff
ASW/CANCEL/HOLD/UNHOLD:xxx	Answer/end/hold/unhold a call (xxx refers to the call-id of the active call). **Example**: http://10.10.20.10/servlet?key=ASW:33093 **Note**: To get the call-id of the active call, configure the action URL: *http(s)://<serverIPAddress>/help.xml?CallId=$call_id*. For more information, refer to Action URL on page 540.
phonecfg=get[&accounts=x][&dnd=x][&fw=x]	Get firmware version, registration, DND or forward configuration information. The valid value of "x" is 0 or 1, 0 means you do not need to get configuration information. 1 means you want to get configuration information. **Note**: The valid URI is: *http(s)://<phoneIPAddress>/servlet?phonecfg=get[&accounts=x][&dnd=x][&fw=x]* **Example**: http://10.10.20.10/servlet?phonecfg=get[&accounts=1][&dnd=0][&fw=1]

Note

The variable value is not applicable to all events. For example, the variable value "MUTE" is only applicable when the IP phone is during a call.

When authentication is required, you change the URI format. You can enter "p=login&q=login&username=xxx&pwd=yyy&jumpto=URI&" before the variable "key". xxx refers to the login user name and yyy refers to the login password. In addition, you can also use the following URI format: *http(s)://username:password@<phoneIPAddress>/servlet?key=variable value* or *http(s)://<phoneIPAddress>/servlet?key=variable value&@username:password*.

Yealink IP phones also support a combination of the variable values in the URI, but the order of the variable value is determined by the operation of the phone. The valid URI format is: *http(s)://<phoneIPAddress>/servlet?key=variable value[;variable value]*. Variable values are separated by a semicolon from each other.

The following shows an example for answering an incoming call then mute the call immediately:

http://10.3.20.10/servlet?key=ASW;MUTE.

Configuring Trusted IP Address for Action URI

For security reasons, IP phones do not 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 touch 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.

If you are using SIP NOTIFY message method, you do not need to specify the trusted IP address for action URI. But you should enable the IP phone to receive the action URI requests. When the IP phone receives a SIP NOTIFY message with the "Event: ACTION-URI" header from a SIP proxy server for the first time, the LCD screen also prompts the message "Allow remote control?".

You can use action URI feature to capture the phone's current screen. For more information, refer to Scenario A - Capturing the Current Screen of the Phone on page 566.

Procedure

Specify the trusted IP address for action URI using the following methods.

<table>
<tr><td rowspan="3">Central Provisioning (Configuration File)</td><td rowspan="3"><y0000000000xx>.cfg</td><td>Configure the IP phone to receive the action URI requests.
Parameter:
features.action_uri.enable</td></tr>
<tr><td>Configure the IP phone to pop up the Allow Remote Control prompt.
Parameter:
features.show_action_uri_option</td></tr>
<tr><td>Specify the trusted IP address(es) for sending the action URI to the IP phone.
Parameter:
features.action_uri_limit_ip</td></tr>
<tr><td colspan="2">Web User Interface</td><td>Specify the trusted IP address(es) for sending the action URI to the IP phone.</td></tr>
</table>

	Navigate to: http://<phoneIPAddress>/servlet?m=mod_data&p=features-remotecontrl&q=load

Details of the Configuration Parameters:

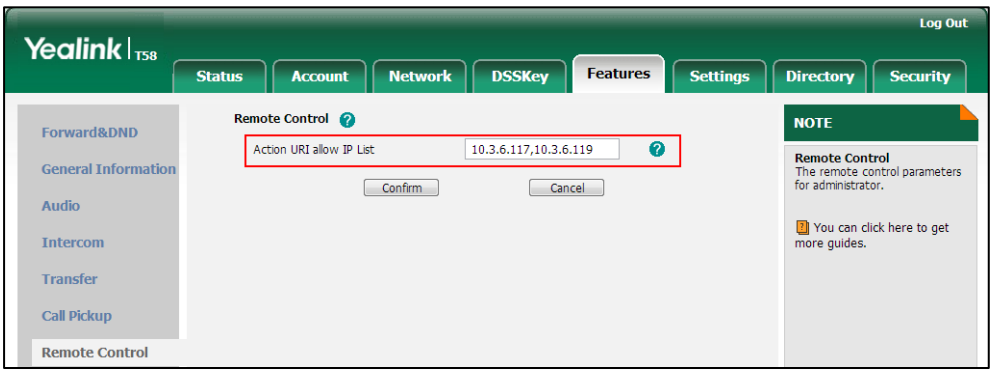
Parameters	Permitted Values	Default
features.action_uri.enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to receive the action URI requests. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
features.show_action_uri_option	**0 or 1**	**1**
Description: Enables or disables the phone to pop up the Allow Remote Control prompt. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the phone will not pop up the Allow Remote Control prompt when receiving an HTTP or HTTPS GET request, or receiving a SIP NOTIFY message with the "Event: ACTION-URI" header. The phone will directly perform the specified action. **Note**: It works only if the value of the parameter "features.action_uri.enable" is set to 1 (Enabled). **Web User Interface:** None **Phone User Interface:** None		
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		

Parameters	Permitted Values	Default
requests. For discontinuous IP addresses, multiple IP addresses are separated by commas. For continuous IP addresses, the format likes *.*.*.* and the "*" stands for the values 0~255. For example: 10.10.*.* stands for the IP addresses that range from 10.10.0.0 to 10.10.255.255. If left blank, the IP phone will reject any HTTP GET 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 **Note**: 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.



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

Scenario A - 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)://<phoneIPAddress>/screencapture/download" to capture the screen display first, and then download the image (which is saved as a JPG file and named with the phone model and the capture time) to the local system. Before capturing the phone's current screen, ensure that the IP address of the computer is included in the trusted IP address for Action URI on the phone. For more information on the trusted IP address, refer to Configuring Trusted IP Address for Action URI on page 564.

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://<phoneIPAddress>/servlet?command=screenshot".

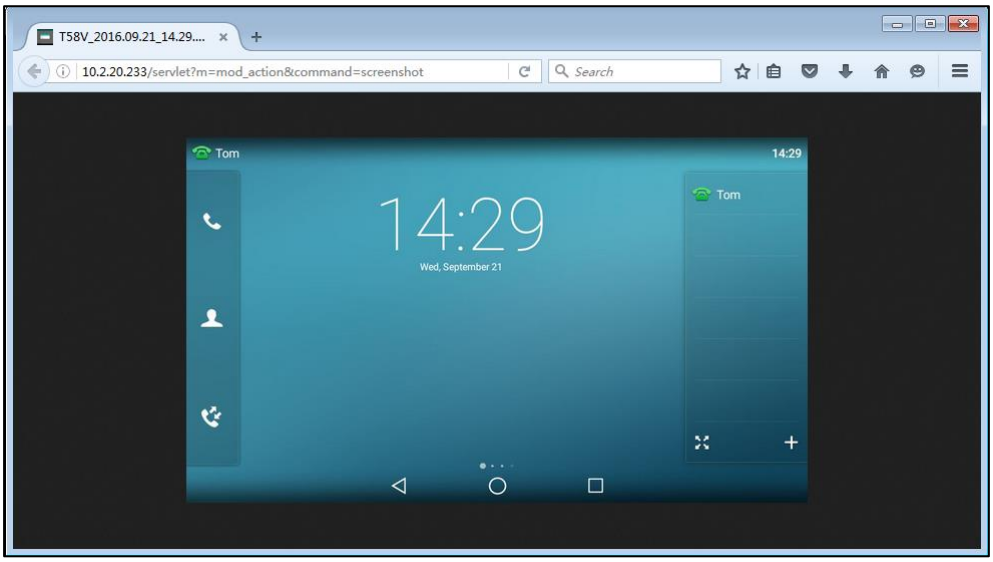
To capture the current screen of the phone:

1. Enter request URI (e.g., http://10.10.20.233/servlet?m=mod_action&command=screenshot) 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 touch screen will prompt the message "Allow remote control?".

     Tap **OK** on the phone to allow remote control.

     Refresh the web page.

     The browser will display an image showing the phone's current screen. You can save the image to your local system.



- Else, the browser will display an image showing the phone's current screen directly. You can save the image to your local system.

Note Frequent capture may affect the phone performance. Yealink recommend you to capture the phone screen display within a minimum interval of 4 seconds.

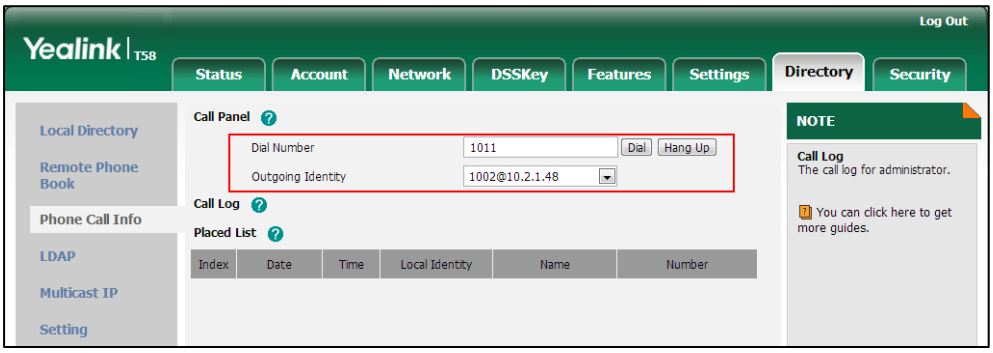
Scenario B - Placing a Call via Web User Interface

You can place a call via web user interface. Before doing it, ensure that the IP address of your computer is included in the trusted IP address for Action URI on the phone. For more information on the trusted IP address, refer to Configuring Trusted IP Address for Action URI on page 564.

If you place a call via web user interface but the trusted IP address has not been configured, the web user interface prompts "Call fail".

To place a call via web user interface:

1. Click on **Directory**->**Phone Call Info**.
2. Select the desired account from the pull-down list of **Outgoing Identity**.
3. Enter the callee's number in the **Dial Number** field.



4. Click **Dial** to dial out the number.

The web user interface prompts "Call Success" and the phone will automatically dial out the number. You can click **Cancel** to end the call.

If it is the first time you place a call via web user interface, the touch screen will prompt the message "Allow remote control?". Tap **OK** on the phone to allow remote control and then the phone will automatically dial out the number.

Note You can also place an IP direct call via web user interface. The IP phone supports either IPv4 or IPv6 address.

Server Redundancy

Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for events where the server needs to be taken offline for maintenance, the server fails, or the connection between the IP phone and the server fails.

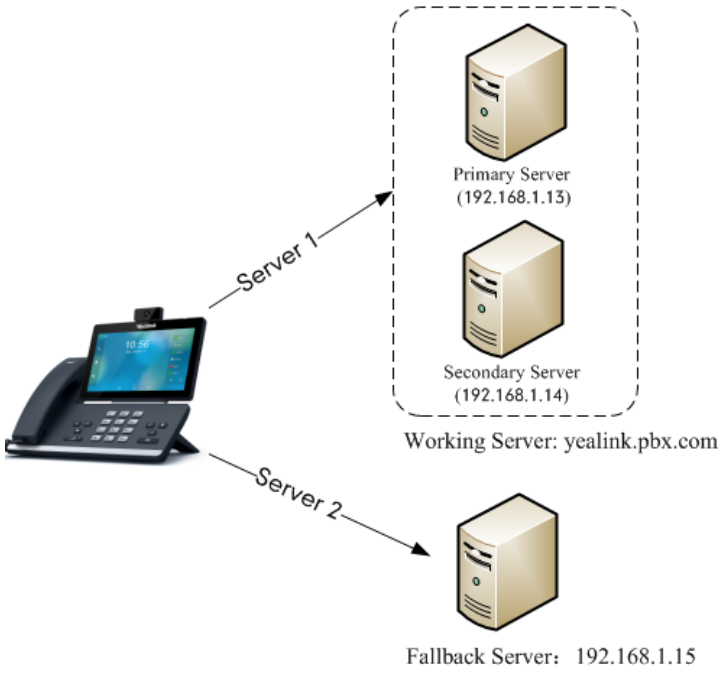
Two types of redundancy are possible. In some cases, a combination of the two may be deployed:

- **Failover:** In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/off-line. This mode of operation should be done using the DNS mechanism from the primary to the secondary server. Therefore, if you want to use this mode, the server must be configured with a domain name.
- **Fallback:** In this mode, a second less featured call server with SIP capability takes over call control to provide basic calling capability, but without some advanced features (for example, shared line and MWI) offered by the working server. IP phones support configuration of two servers per SIP registration for fallback purpose.

Note For concurrent registration mode, it has certain limitation when using some advanced features, and for successive registration mode, the phone service may have a brief interrupt while the server fails. So we recommend you to use the failover mode for server redundancy because this mode can ensure the continuity of the phone service and you can use all the call features while the server fails.

Phone Configuration for Redundancy Implementation

To assist in explaining the redundancy behavior, an illustrative example of how an IP phone may be configured is shown as below. In the example, server redundancy for fallback and failover purposes is deployed. Two separate servers (a working server and a fallback server) are configured for per line registration.



Working Server: Server 1 is configured with the domain name of the working server. For example: yealink.pbx.com. DNS mechanism is used such that the working server is resolved to multiple servers with different IP addresses for failover purpose. The working server is deployed in redundant pairs, designated as primary and secondary servers. The primary server (e.g., 192.168.1.13) has the highest priority server in a cluster of servers resolved by the DNS server. The secondary server (e.g., 192.168.1.14) backs up a primary server when the primary server fails and offers the same functionality as the primary server.

Fallback Server: Server 2 is configured with the IP address of the fallback server. For example, 192.168.1.15. A fallback server offers less functionality than the working server.

Outgoing Call When the Working Server Connection Fails

When a user initiates a call, the IP phone will go through the following steps to connect the call:

1. Sends the INVITE request to the primary server.
2. If the primary server does not respond correctly to the INVITE (that is, the primary server responds to the INVITE with 503 message or the request for responding with 100 Trying message times out (64*T1 seconds, defined in RFC 3261)), then tries to make the call using the secondary server.
3. If the secondary server is also unavailable, the IP phone will try the fallback server until it either succeeds in making a call or exhausts all servers at which point the call will fail.

At the start of a call, server availability is determined by SIP signaling failure. SIP signaling failure

depends on the SIP protocol being used as described below:

- If TCP is used, then the signaling fails if the connection or the send fails.
- If UDP is used, then the signaling fails if ICMP is detected or if the signal times out. If the signaling has been attempted through all servers in the list (this list contains all the server addresses resolved by the DNS server) and this is the last server, then the signaling fails after the complete UDP timeout defined in RFC 3261. If it is not the last server in the list, the maximum number of retries depends on the configured retry counts (configured by the parameter "account.X.sip_server.Y.retry_counts").

Phone Registration

Registration method of the failover mode:

The IP phone must always register to the primary server first except in failover conditions. If this is unsuccessful, the phone will re-register as many times as configured until the registration is successful. When the primary server registration is unavailable, the secondary server will serve as the working server. As soon as the primary server registration succeeds, it returns to being the working server.

Registration methods of the fallback mode include (not applicable to outbound proxy servers):

- **Concurrent registration (default)**: The IP phone registers to SIP server 1 and SIP server 2 (working server and fallback server) at the same time. Note that although the IP phone registers to two SIP servers, only one server works at the same time. In a failure situation, a fallback server can take over the basic calling capability, but without some advanced features (for example, shared lines and MWI) offered by the working server.
- **Successive registration**: The IP phone only registers to one server at a time. The IP phone first registers to the working server. In a failure situation, the IP phone registers to the fallback server, and the fallback server can take over all calling capabilities.

For more information on server redundancy, refer to *Server Redundancy on Yealink IP Phones*.

Procedure

Server redundancy can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the SIP server redundancy. **Parameters:** account.X.sip_server.Y.address account.X.sip_server.Y.port account.X.sip_server.Y.expires account.X.sip_server.Y.retry_counts

		Configure the outbound proxy server redundancy. **Parameters:** account.X.outbound_proxy_enable account.X.outbound_proxy.Y.address account.X.outbound_proxy.Y.port **Fallback Mode:** account.X.fallback.redundancy_type account.X.fallback.timeout account.X.outbound_proxy_fallback_interval **Failover Mode:** account.X.sip_server.Y.failback_mode account.X.sip_server.Y.failback_timeout account.X.sip_server.Y.register_on_enable
Web User Interface		Configure the server redundancy on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-register&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.sip_server.Y.address (Y ranges from 1 to 2)	**String within 256 characters**	**Blank**
Description: Configures the IP address or domain name of the SIP server Y that accepts registrations for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.sip_server.1.address = yealink.pbx.com **Web User Interface:** Account->Register->SIP Server Y->Server Host **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->Account X->SIP ServerY		

Parameters	Permitted Values	Default
account.X.sip_server.Y.port (Y ranges from 1 to 2)	**Integer from 0 to 65535**	**5060**
Description: Configures the port of the SIP server Y that specifies registrations for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.sip_server.1.port = 5060 **Note**: If the value of this parameter is set to 0, the port used depends on the value specified by the parameter "account.X.sip_server.Y.transport_type". **Web User Interface:** Account->Register->SIP Server Y->Port **Phone User Interface:** None		
account.X.sip_server.Y.expires (Y ranges from 1 to 2)	**Integer from 30 to 2147483647**	**3600**
Description: Configures the registration expiration time (in seconds) of the SIP server Y for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.sip_server.1.expires = 3600 **Web User Interface:** Account->Register->SIP Server Y->Server Expires **Phone User Interface:** None		
account.X.sip_server.Y.retry_counts (Y ranges from 1 to 2)	**Integer from 0 to 20**	**3**
Description: Configures the retry times for the IP phone to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960)		

Parameters	Permitted Values	Default
Web User Interface: Account->Register->SIP Server Y->Server Retry Counts **Phone User Interface:** None		
account.X.sip_server.Y.register_on_enable (Y ranges from 1 to 2)	**0 or 1**	**0**
Description: Enables or disables the IP phone to register to the secondary server before sending requests to it for account X when encountering a failover. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone will directly send the requests to the secondary server. If it is set to 1 (Enabled), the IP phone will register to the secondary server first, and then send the requests to it. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** None **Phone User Interface:** None		
account.X.outbound_proxy_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to send requests to the outbound proxy server for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Register->Enable Outbound Proxy Server **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->AccountX->Outbound Status		

Parameters	Permitted Values	Default
account.X.outbound_proxy.Y.address (Y ranges from 1 to 2)	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the outbound proxy server Y for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.outbound_proxy.1.address = 10.1.8.11 **Note:** It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). **Web User Interface:** Account->Register->Outbound Proxy Server Y **Phone User Interface:** Settings->Advanced (default password: admin) ->Accounts->Outbound ProxyY		
account.X.outbound_proxy.Y.port (Y ranges from 1 to 2)	**Integer from 0 to 65535**	**5060**
Description: Configures the port of the outbound proxy server Y for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.outbound_proxy.1.port = 5060 **Note:** It works only if the value of the parameter "account.X.outbound_proxy_enable" is set to 1 (Enabled). **Web User Interface:** Account->Register->Outbound Proxy Server Y->Port **Phone User Interface:** None		
account.X.fallback.redundancy_type	**0 or 1**	**0**
Description: Configures the registration mode for the IP phone in fallback mode. **0**-Concurrent Registration **1**-Successive Registration		

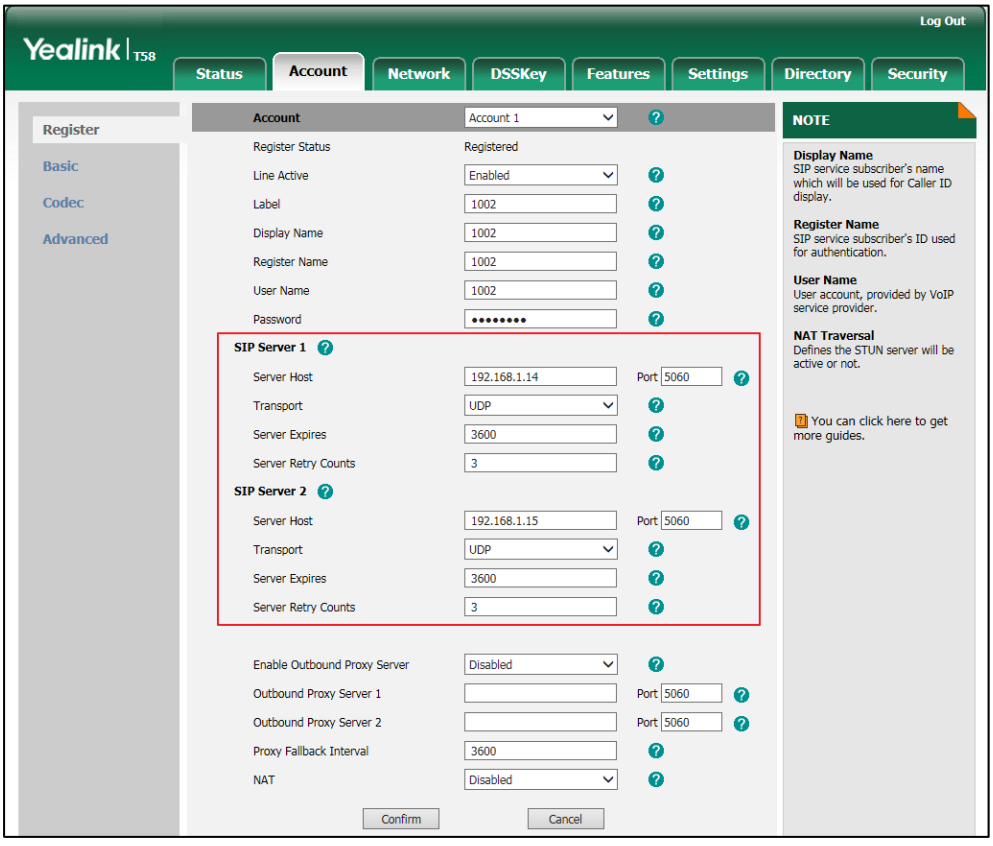
Parameters	Permitted Values	Default
X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note:** It is not applicable to outbound proxy servers. **Web User Interface:** None **Phone User Interface:** None		
account.X.fallback.timeout	**Integer from 10 to 2147483647**	**120**
Description: Configures the time interval (in seconds) for the IP phone to detect whether the working server is available by sending the registration request for account X after the fallback server takes over call control. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: It works only if the value of the parameter "account.X.fallback.redundancy_type" is set to 1 (Successive Registration). It is not applicable to outbound proxy servers. **Web User Interface:** None **Phone User Interface:** None		
account.X.outbound_proxy_fallback_interval	**Integer from 0 to 65535**	**3600**
Description: Configures the time interval (in seconds) for the IP phone to detect whether the working outbound proxy server is available by sending the registration request after the fallback server takes over call control. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.outbound_proxy_fallback_interval = 3600 **Note:** It is only applicable to outbound proxy servers. **Web User Interface:** Account->Register->Proxy Fallback Interval		

Parameters	Permitted Values	Default
Phone User Interface: Settings->Advanced (default password: admin) ->Accounts->AccountX->Proxy Fallback Interval		
account.X.sip_server.Y.failback_mode (Y ranges from 1 to 2)	**0, 1, 2 or 3**	**0**
Description: Configures the failback mode for the IP phone to retry the primary server in failover for account X. **0**-newRequests: all requests are sent to the primary server first, regardless of the last server that was used. If the primary server does not respond correctly, the IP phone will try to send requests to the secondary server. **1**-DNSTTL: the IP phone will send requests to the last registered server first. If the TTL for the DNS A records on the registered server expires, the phone will retry to send requests to the primary server. **2**-Registration: the IP phone will send requests to the last registered server first. If the registration expires, the phone will retry to send requests to the primary server. **3**-duration: the IP phone will send requests to the last registered server first. If the time defined by the parameter "account.X.sip_server.Y.failback_timeout" expires, the phone will retry to send requests to the primary server. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note**: DNSTTL, Registration and duration mode can only be processed when the IP phone is idle (that is, no incoming/outbound calls, no active calls or meetings, etc.). **Web User Interface:** None **Phone User Interface:** None		
account.X.sip_server.Y.failback_timeout (Y ranges from 1 to 2)	**0, Integer from 60 to 65535**	**3600**
Description: Configures the time (in seconds) for the phone to retry to send requests to the primary server after failing over to the current working server for account X. If you set the parameter to 0, the IP phone will not send requests to the primary server until a failover event occurs with the current working server. If you set the parameter from 1 to 59, the timeout will be 60 seconds. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)		

Parameters	Permitted Values	Default
X is equal to 1 (for CP960) **Note:** It works only if the value of the parameter "account.X.sip_server.Y.failback_mode" is set to 3 (duration). **Web User Interface:** None **Phone User Interface:** None		

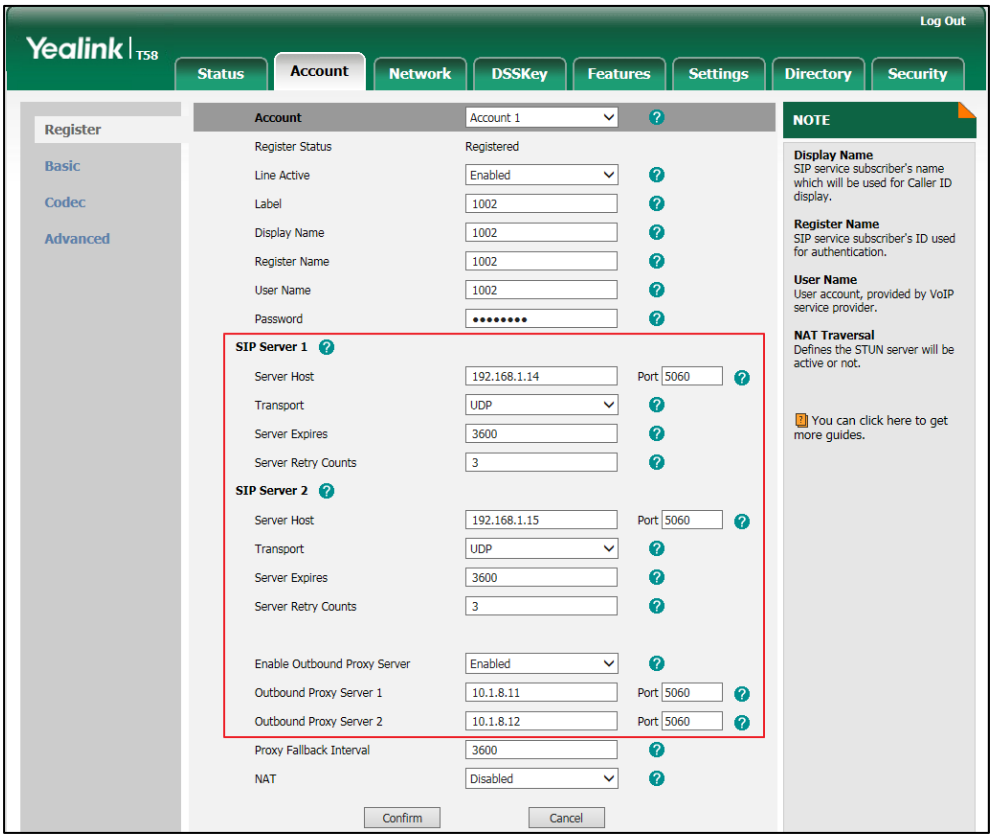
To configure server redundancy for fallback purpose via web user interface:

1. Click on **Account**->**Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Configure registration parameters of the selected account in the corresponding fields.
4. Configure parameters of SIP server 1 and SIP server 2 in the corresponding fields.



5. If you use outbound proxy servers, do the following:
   1) Select **Enabled** from the pull-down list of **Enable Outbound Proxy Server**.

2) Configure parameters of outbound proxy server 1 and outbound proxy server 2 in the corresponding fields.



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

To configure server redundancy for failover purpose via web user interface:

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

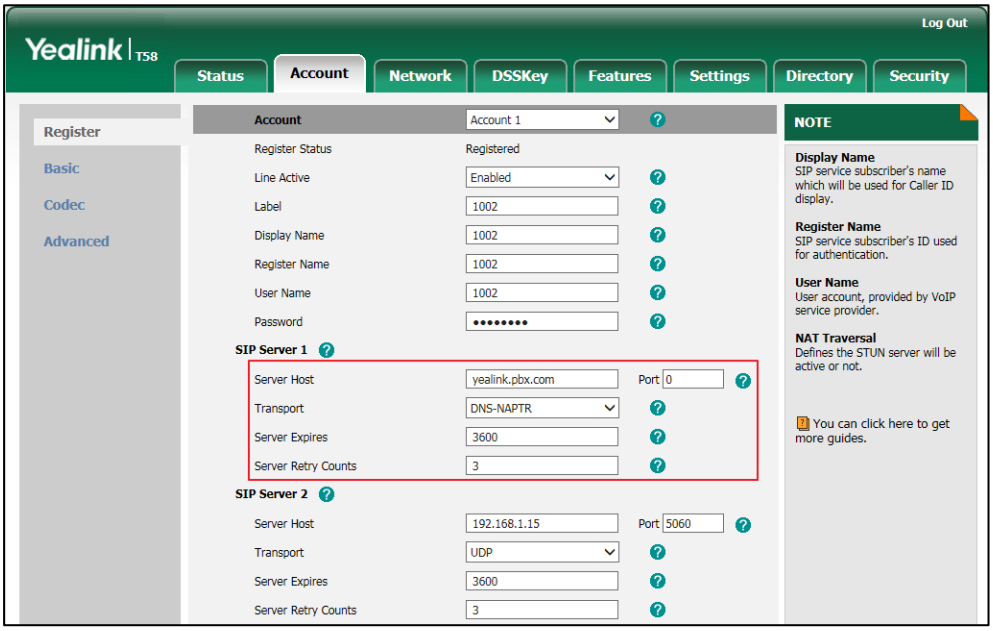
2. Select the desired account from the pull-down list of **Account**.

3. Configure registration parameters of the selected account in the corresponding fields.

4. Configure parameters of the SIP server 1 or SIP server 2 in the corresponding fields.

You must set the port of SIP server to 0 for NAPTR, SRV and A queries.

5. Select **DNS-NAPTR** from the pull-down list of **Transport**.

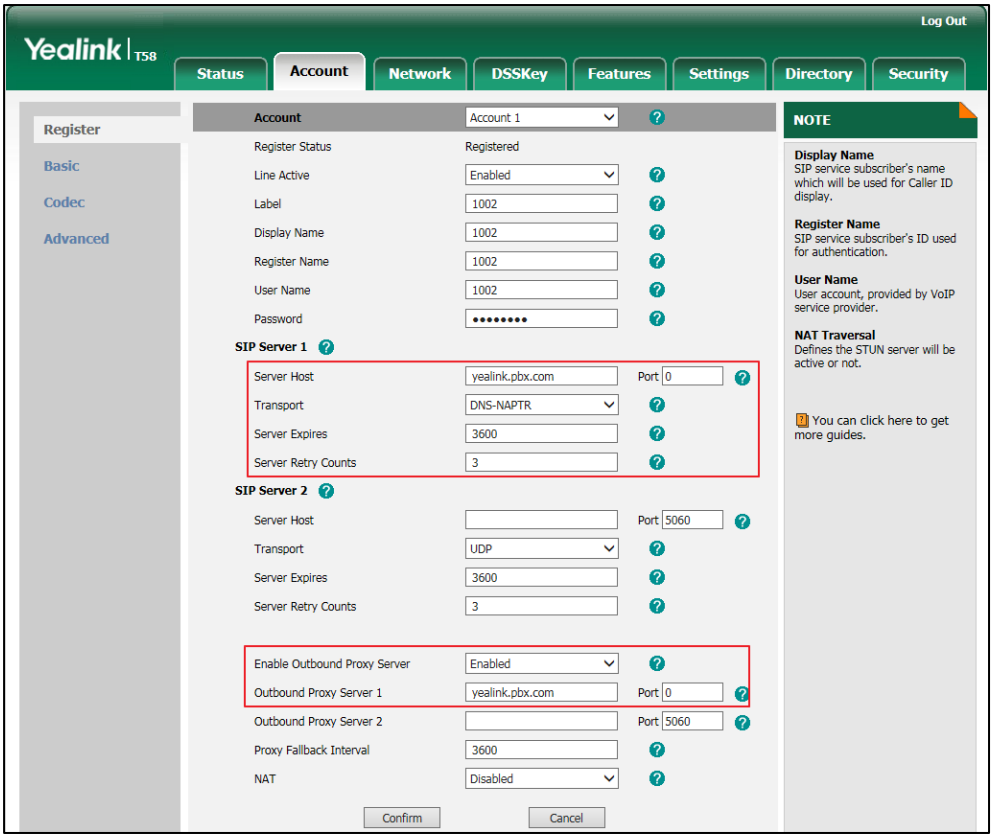


6. If you use outbound proxy servers, do the following:

   1) Select **Enabled** from the pull-down list of **Enable Outbound Proxy Server**.

   2) Configure parameters of outbound proxy server 1/2 in the corresponding fields.

   You must set the port of outbound proxy server to 0 for NAPTR, SRV and A queries.



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

Server Domain Name Resolution

If a domain name is configured for a server, the IP address(es) associated with that domain name will be resolved through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV and A queries, which allows the IP phone to adapt to various deployment environments. The IP phone performs NAPTR query for the NAPTR pointer and transport protocol (UDP, TCP and TLS), the SRV query on the record returned from the NAPTR for the target domain name and the port number, and the A query for the IP addresses.

If an explicit port (except 0) is specified, A query will be performed only. If a server port is set to 0 and the transport type is set to DNS-NAPTR, NAPTR and SRV queries will be tried before falling to A query. If no port is found through the DNS query, 5060 will be used.

The following details the procedures of DNS query for the IP phone to resolve the domain name (e.g., yealink.pbx.com) of working server into the IP address, port and transport protocol.

NAPTR (Naming Authority Pointer)

First, the IP phone sends NAPTR query to get the NAPTR pointer and transport protocol. Example of NAPTR records:

	order	pref	flags	service	regexp	replacement
IN NAPTR	90	50	"s"	"SIP+D2T"	""	_sip._tcp.yealink.pbx.com
IN NAPTR	100	50	"s"	"SIP+D2U"	""	_sip._udp.yealink.pbx.com

Parameters are explained in the following table:

Parameter	Description
order	Specify preferential treatment for the specific record. The order is from lowest to highest, lower order is more preferred.
pref	Specify the preference for processing multiple NAPTR records with the same order value. Lower value is more preferred.
Flags	The flag "s" means to perform an SRV lookup.
service	Specify the transport protocols: SIP+D2U: SIP over UDP SIP+D2T: SIP over TCP SIP+D2S: SIP over SCTP SIPS+D2T: SIPS over TCP
regexp	Always empty for SIP services.
replacement	Specify a domain name for the next query.

The IP phone picks the first record because its order of 90 is lower than 100. The pref parameter

is unimportant as there is no other record with order 90. The flag "s" indicates performing the SRV query next. TCP will be used, targeted to a host determined by an SRV query of "_sip._tcp.yealink.pbx.com". If the flag of the NAPTR record returned is empty, the IP phone will perform NAPTR query again according to the previous NAPTR query result.

SRV (Service Location Record)

The IP phone performs an SRV query on the record returned from the NAPTR for the host name and the port number. Example of SRV records:

	Priority	Weight	Port	Target
IN SRV	0	1	5060	server1.yealink.pbx.com
IN SRV	0	2	5060	server2.yealink.pbx.com

Parameters are explained in the following table:

Parameter	Description
Priority	Specify preferential treatment for the specific host entry. Lower priority is more preferred.
Weight	When priorities are equal, weight is used to differentiate the preference. The preference is from highest to lowest. Keep the same to load balance.
Port	Identify the port number to be used.
Target	Identify the actual host for an A query.

SRV query returns two records. The two SRV records point to different hosts and have the same priority 0. The weight of the second record is higher than the first one, so the second record will be picked first. The two records also contain a port "5060", the IP phone uses this port. If the Target is not a numeric IP address, the IP phone performs an A query. So in this case, the IP phone uses "server1.yealink.pbx.com" and "server2.yealink.pbx.com" for the A query.

A (Host IP Address)

The IP phone performs an A query for the IP address of each target host name. Example of A records:

Server1.yealink.pbx.com IN A 192.168.1.13

Server2.yealink.pbx.com IN A 192.168.1.14

The IP phone picks the IP address "192.168.1.14" first.

Procedure

SIP Server Domain Name Resolution can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the transport protocol on the IP phone.

		Parameters: account.X.sip_server.Y.transport_type account.X.naptr_build
Web User Interface		Configure the transport protocol on the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-register&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.sip_server.Y.transport_type (Y ranges from 1 to 2)	**0, 1, 2 or 3**	**0**
Description: Configures the transport method the IP phone uses to communicate with the SIP server for account X. **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR If the value of this parameter is set to 3 (DNS-NAPTR), the value of the parameter "account.X.sip_server.Y.address" is set to a host name and the value of the parameter "account.X.sip_server.Y.port" is set to 0, the IP phone will perform the DNS NAPTR and SRV queries for the transport protocol, ports and servers. If the value of this parameter is set to 3 (DNS-NAPTR), the value of the parameter "account.X.sip_server.Y.address" is set to an IP address and the value of the parameter "account.X.sip_server.Y.port" is set to an explicit port (except 0), then UDP is used. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Register->SIP Server Y->Transport **Phone User Interface:** None		
account.X.naptr_build	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Configures the way of SRV query for the IP phone to be performed when no result is returned from NAPTR query for account X. **0**-SRV query using UDP only **1**-SRV query using UDP, TCP and TLS X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** None **Phone User Interface:** None		

Static DNS Cache

Failover redundancy can only be utilized when the configured domain name of the server is resolved to multiple IP addresses. If the IP phone is not configured with a DNS server, or the DNS query returns no result from a DNS server, you can statically configure a set of DNS NAPTR/SRV/A records into the IP phone. The IP phone will attempt to resolve the domain name of the SIP server with static DNS cache.

When the IP phone is configured with a DNS server, it will behave as follows to resolve domain name of the server:

- The IP phone performs a DNS query to resolve the domain name from the DNS server.
- If the DNS query returns no results for the domain name, or the returned record cannot be contacted, the values in the static DNS cache (if configured) are used when their configured time intervals are not elapsed.
- If the configured time interval is elapsed, the IP phone will attempt to perform a DNS query again.
- If the DNS query returns a result, the IP phone will use the returned record from the DNS server and ignore the statically configured cache values.

When the IP phone is not configured with a DNS server, it will behave as follows:

- The IP phone attempts to resolve the domain name within the static DNS cache.
- The IP phone will always use the results returned from the static DNS cache.

Support for negative caching of DNS queries as described in RFC 2308 is also provided to allow faster failover when prior DNS queries have returned no results from the DNS server.

IP phones can be configured to use static DNS cache preferentially. Static DNS cache is

configurable on a per-line basis.

Procedure

Static DNS cache can be configured only using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure NAPTR/SRV/A records. **Parameters:** dns_cache_naptr.X.name dns_cache_naptr.X.flags dns_cache_naptr.X.order dns_cache_naptr.X.preference dns_cache_naptr.X.replace dns_cache_naptr.X.service dns_cache_naptr.X.ttl dns_cache_srv.X.name dns_cache_srv.X.port dns_cache_srv.X.priority dns_cache_srv.X.target dns_cache_srv.X.weight dns_cache_srv.X.ttl dns_cache_a.X.name dns_cache_a.X.ip dns_cache_a.X.ttl
	<MAC>.cfg	Configure the IP phone whether to cache the additional DNS records. **Parameter:** account.X.dns_cache_type
		Configure the IP phone whether to use static DNS cache preferentially. **Parameter:** account.X.static_cache_pri

Details of Configuration Parameters:

Parameters	Permitted Values	Default
dns_cache_naptr.X.name (X ranges from 1 to 12)	**Domain name**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the domain name to which NAPTR record X refers. **Example:** dns_cache_naptr.1.name = yealink.pbx.com **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.flags (X ranges from 1 to 12)	**S, A, U or P**	**Blank**
Description: Configures the flag of NAPTR record X. (Always "S" for SIP, which means to do an SRV lookup on whatever is in the replacement field). **S**-Do an SRV lookup next **A**-Do an A lookup next **U**-No need to do a DNS query next **P**-Service custom by the user **Example:** dns_cache_naptr.1.flags = S **Note**: For more details of the permitted flags, refer to RFC 2915. **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.order (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the order of NAPTR record X. NAPTR record with lower order is more preferred. For example, NAPTR record with the order 90 has the higher priority than that with the order 100 because 90 is lower than 100. **Example:** dns_cache_naptr.1.order = 90 **Web User Interface:**		

Parameters	Permitted Values	Default
None **Phone User Interface:** None		
dns_cache_naptr.X.preference (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the preference of NAPTR record X. NAPTR record with lower value is more preferred when the multiple NAPTR records have the same order value. **Example:** dns_cache_naptr.1.preference = 50 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.replace (X ranges from 1 to 12)	**Domain name with SRV prefix**	**Blank**
Description: Configures a domain name to be used for the next SRV query in NAPTR record X. **Example:** dns_cache_naptr.1.replace = _sip._tcp.yealink.pbx.com **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.service (X ranges from 1 to 12)	**String within 32 characters**	**Blank**
Description: Configures the transport protocol available for the server in NAPTR record X. **SIP+D2U**: SIP over UDP **SIP+D2T**: SIP over TCP **SIP+D2S**: SIP over SCTP **SIPS+D2T**: SIPS over TCP		

Parameters	Permitted Values	Default
Example: dns_cache_naptr.1.service = SIP+D2T **Note**: For more information, refer to RFC 2915. **Web User Interface:** None **Phone User Interface:** None		
dns_cache_naptr.X.ttl (X ranges from 1 to 12)	**Integer from 30 to 2147483647**	**300**
Description: Configures the time interval (in seconds) that NAPTR record X may be cached before the record should be consulted again. **Example:** dns_cache_naptr.1.ttl = 3600 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.name (X ranges from 1 to 12)	**Domain name with SRV prefix**	**Blank**
Description: Configures the domain name in SRV record X. **Example:** dns_cache_srv.1.name = _sip._tcp.yealink.pbx.com **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.port (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the port to be used in SRV record X.		

Parameters	Permitted Values	Default
Example: dns_cache_srv.1.port = 5060 **Note**: For more information, refer to RFC 2782. **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.priority (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description: Configures the priority for the target host in SRV record X. Lower priority is more preferred. For example, SRV record with the priority value 0 is more preferred than that with the priority value 1 because 0 is lower than 1. **Note**: For more information, refer to RFC 2782. **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.target (X ranges from 1 to 12)	**Domain name**	**Blank**
Description: Configures the domain name of the target host for an A query in SRV record X. **Example:** dns_cache_srv.1.target = server1.yealink.pbx.com **Note**: For more information, refer to RFC 2782. **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.weight (X ranges from 1 to 12)	**Integer from 0 to 65535**	**0**
Description:		

Parameters	Permitted Values	Default
Configures the weight of the target host in SRV record X. When priorities are equal, weight is used to differentiate the preference. Higher weight value is more preferred. **Example:** dns_cache_srv.1.weight = 1 **Note**: For more information, refer to RFC 2782. **Web User Interface:** None **Phone User Interface:** None		
dns_cache_srv.X.ttl (X ranges from 1 to 12)	**Integer from 30 to 2147483647**	**300**
Description: Configures the time interval (in seconds) that SRV record X may be cached before the record should be consulted again. **Example:** dns_cache_srv.1.ttl = 3600 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_a.X.name (X ranges from 1 to 12)	**Domain name**	**Blank**
Description: Configures the domain name in A record X. **Example:** dns_cache_a.1.name = yealink.pbx.com **Web User Interface:** None **Phone User Interface:** None		
dns_cache_a.X.ip (X ranges from 1 to 12)	**IP address**	**Blank**

Parameters	Permitted Values	Default
Description: Configures the IP address that the domain name in A record X maps to. **Example:** dns_cache_a.1.ip = 192.168.1.13 **Web User Interface:** None **Phone User Interface:** None		
dns_cache_a.X.ttl (X ranges from 1 to 12)	**Integer from 30 to 2147483647**	**300**
Description: Configures the time interval (in seconds) that A record X may be cached before the record should be consulted again. **Example:** dns_cache_a.1.ttl = 3600 **Web User Interface:** None **Phone User Interface:** None		
account.X.dns_cache_type	**0, 1 or 2**	**1**
Description: Configures whether the IP phone uses the DNS cache for domain name resolution of the server and caches the additional DNS records for account X. **0**-Perform real-time DNS query rather than using DNS cache. **1**-Use DNS cache, but do not cache the additional DNS records. **2**-Use DNS cache and cache the additional DNS records. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.dns_cache_type = 1 **Web User Interface:** None **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
account.X.static_cache_pri	**0 or 1**	**0**
Description: Configures whether preferentially to use the static DNS cache for domain name resolution of the server for account X. **0**-Use domain name resolution from the DNS server preferentially **1**-Use static DNS cache preferentially X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.static_cache_pri = 1 **Web User Interface:** None **Phone User Interface:** None		

Real-Time Transport Protocol (RTP) Ports

The Real-time Transport Protocol (RTP) is a network protocol for delivering audio over IP networks. The phone is compatible with RFC 1889 - RTP: A Transport Protocol for Real-Time Applications - and the updated RFC 3550. It treats all RTP streams as bi-directional from a control perspective and expects that both RTP end points will negotiate the respective destination IP addresses and ports.

You can specify the IP phone's RTP port range. Since the IP phone supports conferencing and multiple RTP streams, it can use several ports concurrently. The UDP port used for RTP streams is traditionally an even-numbered port. For example, the default RTP min port on the IP phones is 11780. The first voice session sends RTP on port 11780. Additional calls would then use ports 11782, 11784, 11786, etc. up to the max port.

Procedure

RTP ports can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure RTP ports. **Parameters:** static.network.port.max_rtpport static.network.port.min_rtpport

Web User Interface	Configure RTP ports. **Navigate to**: http://<phoneIPAddress>/servlet?p=network-adv&q=load

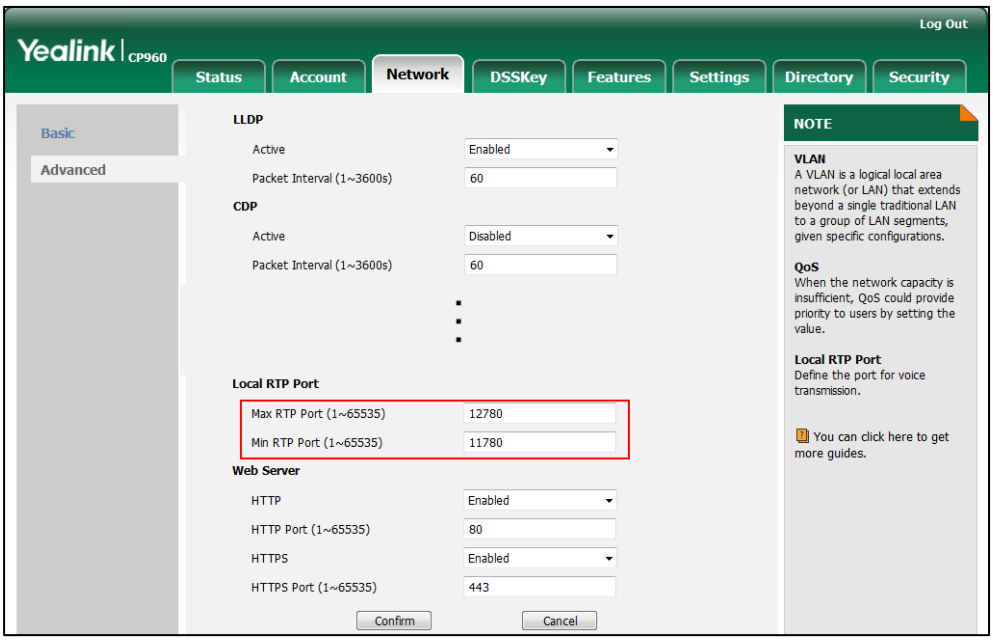
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.network.port.min_rtpport	**Integer from 1 to 65535**	**11780**
Description: Configures the minimum local RTP port. **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to CP960 IP phones. **Web User Interface:** Network->Advanced->Local RTP Port->Min RTP Port(1~65535) **Phone User Interface:** None		
static.network.port.max_rtpport	**Integer from 1 to 65535**	**12780**
Description: Configures the maximum local RTP port. **Note**: The value of the maximum local RTP port cannot be less than that of the minimum local RTP port (configured by the parameter "static.network.port.min_rtpport"). If you change this parameter, the IP phone will reboot to make the change take effect. It is only applicable to CP960 IP phones. **Web User Interface:** Network->Advanced->Local RTP Port->Max RTP Port(1~65535) **Phone User Interface:** None		

To configure the minimum and maximum RTP port via web user interface:

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

2. In the **Local RTP Port** block, enter the max and min RTP port in the **Max RTP Port(1~65535)** and **Min RTP Port(1~65535)** field respectively.



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 phone.

TR-069 Device Management

TR-069 is a technical specification defined by the Broadband Forum, which defines a mechanism that encompasses secure auto-configuration of a CPE (Customer-Premises Equipment), and incorporates other CPE management functions into a common framework. TR-069 uses common transport mechanisms (HTTP and HTTPS) for communication between CPE and ACS (Auto Configuration Servers). The HTTP(S) messages contain XML-RPC methods defined in the standard for configuration and management of the CPE.

TR-069 is intended to support a variety of functionalities to manage a collection of CPEs, including the following primary capabilities:

- Auto-configuration and dynamic service provisioning
- Software or firmware image management
- Status and performance monitoring
- Diagnostics

The following table provides a description of RPC methods supported by IP phones.

RPC Method	Description
GetRPCMethods	This method is used to discover the set of methods supported by the CPE.
SetParameterValues	This method is used to modify the value of one or more CPE parameters.
GetParameterValues	This method is used to obtain the value of one or more CPE parameters.
GetParameterNames	This method is used to discover the parameters accessible on a particular CPE.
GetParameterAttributes	This method is used to read the attributes associated with one or more CPE parameters.
SetParameterAttributes	This method is used to modify attributes associated with one or more CPE parameters.
Reboot	This method causes the CPE to reboot.
Download	This method is used to cause the CPE to download a specified file from the designated location. File types supported by IP phones are: ● Firmware Image ● Configuration File
Upload	This method is used to cause the CPE to upload a specified file to the designated location. File types supported by IP phones are: ● Configuration File ● Log File
ScheduleInform	This method is used to request the CPE to schedule a one-time Inform method call (separate from its periodic Inform method calls) sometime in the future.
FactoryReset	This method resets the CPE to its factory default state.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	This method is used to add a new instance of an object defined on the CPE.
DeleteObject	This method is used to remove a particular instance of an object.

For more information on TR-069, refer to *Yealink TR-069 TechNote*.

Procedure

TR-069 can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure TR-069 feature. **Parameters:** static.managementserver.enable static.managementserver.username static.managementserver.password static.managementserver.url static.managementserver.connection_request_username static.managementserver.connection_request_password static.managementserver.periodic_inform_enable static.managementserver.periodic_inform_interval
Web User Interface		Configure TR-069 feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-tr069&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.managementserver.enable	**0 or 1**	**0**
Description: Enables or disables the TR-069 feature. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->TR069->Enable TR069 **Phone User Interface:** None		

Parameters	Permitted Values	Default
static.managementserver.username	**String within 128 characters**	**Blank**
Description: Configures the user name for the IP phone to authenticate with the ACS (Auto Configuration Servers). Leave it blank if no authentication is required. **Example:** static.managementserver.username = tr69 **Web User Interface:** Settings->TR069->ACS Username **Phone User Interface:** None		
static.managementserver.password	**String within 64 characters**	**Blank**
Description: Configures the password for the IP phone to authenticate with the ACS (Auto Configuration Servers). Leave it blank if no authentication is required. **Example:** static.managementserver.password = tr69 **Web User Interface:** Settings->TR069->ACS Password **Phone User Interface:** None		
static.managementserver.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the ACS (Auto Configuration Servers). **Example:** static.managementserver.url = http://officetelprov.orangero.net:8080/ftacs-digest/ACS **Note:** Yealink IP phones also support obtaining the URL of the ACS by detecting DHCP option 43. For more information on DHCP option 43, refer to DHCP Option on page 28. **Web User Interface:**		

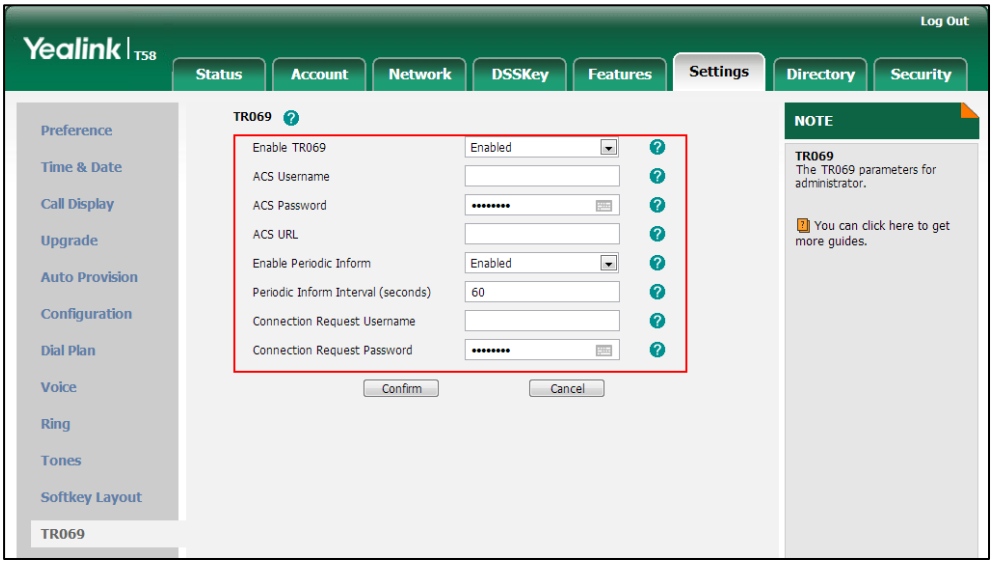
Parameters	Permitted Values	Default
Settings->TR069->ACS URL **Phone User Interface:** None		
static.managementserver.connection_request_username	**String within 128 characters**	**Blank**
Description: Configures the user name for the IP phone to authenticate the incoming connection requests of the ACS (Auto Configuration Servers). **Example:** static.managementserver.connection_request_username = accuser **Web User Interface:** Settings->TR069->Connection Request Username **Phone User Interface:** None		
static.managementserver.connection_request_password	**String within 64 characters**	**Blank**
Description: Configures the password for the IP phone to authenticate the incoming connection requests of the ACS (Auto Configuration Servers). **Example:** static.managementserver.connection_request_password = acspwd **Web User Interface:** Settings->TR069->Connection Request Password **Phone User Interface:** None		
static.managementserver.periodic_inform_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to periodically report its configuration information to the ACS (Auto Configuration Servers). **0**-Disabled **1**-Enabled **Web User Interface:**		

Parameters	Permitted Values	Default
Settings->TR069->Enable Periodic Inform **Phone User Interface:** None		
static.managementserver.periodic_inform_interval	**Integer from 5 to 4294967295**	**60**
Description: Configures the interval (in seconds) for the IP phone to report its configuration to the ACS (Auto Configuration Servers). **Note**: It works only if the value of the parameter "static.managementserver.periodic_inform_enable" is set to 1 (Enabled). **Web User Interface:** Settings->TR069->Periodic Inform Interval (seconds) **Phone User Interface:** None		

To configure TR-069 via web user interface:

1. Click on **Settings**->**TR069**.
2. Select **Enabled** from the pull-down list of **Enable TR069**.
3. Enter the user name and password authenticated by the ACS in the **ACS Username** and **ACS Password** fields.
4. Enter the URL of the ACS in the **ACS URL** field.
5. Select the desired value from the pull-down list of **Enable Periodic Inform**.
6. Enter the desired time in the **Periodic Inform Interval (seconds)** field.

7. Enter the user name and password authenticated by the IP phone in the **Connection Request Username** and **Connection Request Password** fields.



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

Configuring Audio Features

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

- Redial Tone
- Ring Tones
- Distinctive Ring Tones
- Tones
- Voice Mail Tone
- Ringer Device for Headset
- Headset Prior
- Dual Headset
- Sending Volume
- Audio Codecs
- Acoustic Clarity Technology
- DTMF
- Voice Quality Monitoring (VQM)

Redial Tone

Redial tone allows IP phones to continue to play the dial tone after inputting the preset numbers on the pre-dialing screen. It is not applicable to CP960 IP phones.

Procedure

Redial tone can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure redial tone feature. **Parameter:** features.redial_tone
Web User Interface		Configure redial tone feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-audio&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.redial_tone	**Integer within 6 digits**	**Blank**

Description:

Configures the IP phone to continue to play the dial tone after inputting the preset numbers on the pre-dialing screen.

Example:

features.redial_tone = 123

The IP phone will continue to play the dial tone after inputting "123" on the pre-dialing screen.

If it is left blank, the IP phone will not play the dial tone after inputting numbers on the pre-dialing screen.

Note: It is not applicable to CP960 IP phones.

Web User Interface:

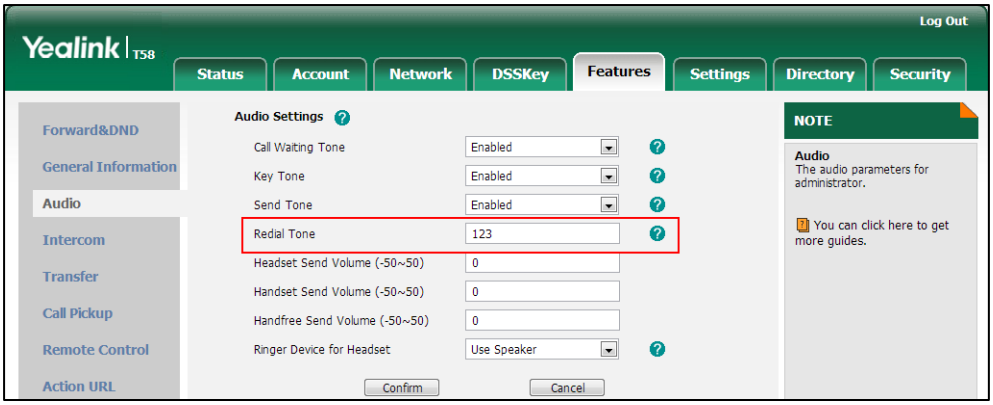
Features->Audio->Redial Tone

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.



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

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 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:

Phone Model	Format	Single File Size
SIP-T58V/T58A/T56A	.wav	<=8MB
CP960	.wav	<=8MB

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	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
	<MAC>.cfg	Configure a ring tone on a per-line basis. **Parameter:** account.X.ringtone.ring_type
Web User Interface		Upload the custom ring tones. Configure a ring tone for the IP phone. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-preference&q=load
		Configure a ring tone on a per-line basis. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=account-basic&q=load&acc=0
Phone User Interface		Configure a ring tone for the IP phone. Configure a ring tone for the account.

Details of the Configuration Parameters:

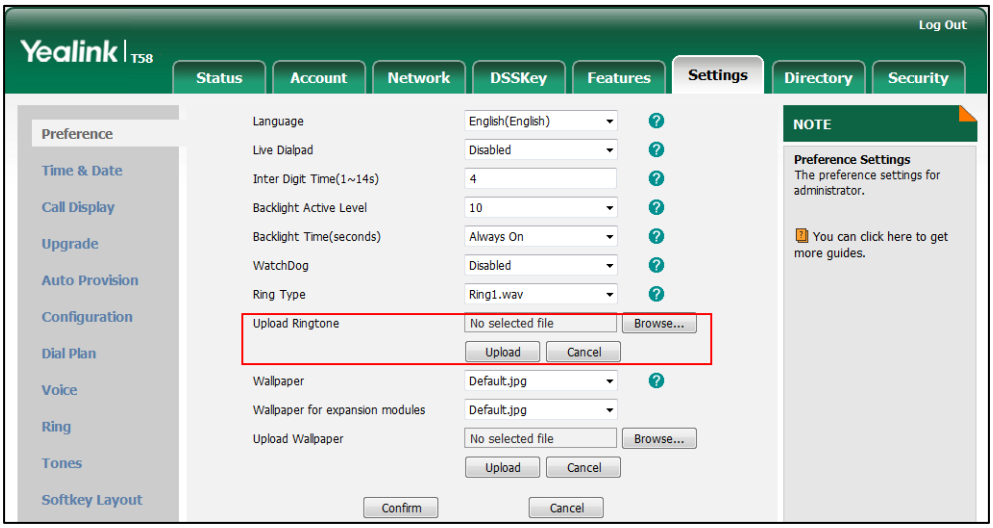
Parameters	Permitted Values	Default
phone_setting.ring_type	**Refer to the following content**	**Ring1.wav**
Description: Configures a ring tone for the IP phone. **Permitted Values:** Ring1.wav, Ring2.wav, Ring3.wav, Ring4.wav, Ring5.wav, Ring6.wav, Ring7.wav, Ring8.wav, Silent.wav, Splash.wav or custom ring tone name (e.g., Customring.wav). **Example:** phone_setting.ring_type = Ring1.wav **Web User Interface:** Settings->Preference->Ring Type **Phone User Interface:** Settings->Basic->Sound->Ring Tones->Common		
account.X.ringtone.ring_type	**Refer to the following content**	**Common**
Description: Configures a ring tone for account X. **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). X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example**: account.1.ringtone.ring_type = Ring3.wav It means account1 will use the Ring3.wav as the ring tone. account.1.ringtone.ring_type = Common It means account1 will use the ring tone selected for the IP phone configured by the parameter "phone_setting.ring_type". **Web User Interface:** Account->Basic->Ring Type **Phone User Interface:**		

Parameters	Permitted Values	Default
Settings->Basic->Sound->Ring Tones->Account X		
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		
ringtone.delete	**http://localhost/all**	**Blank**
Description: Delete 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.

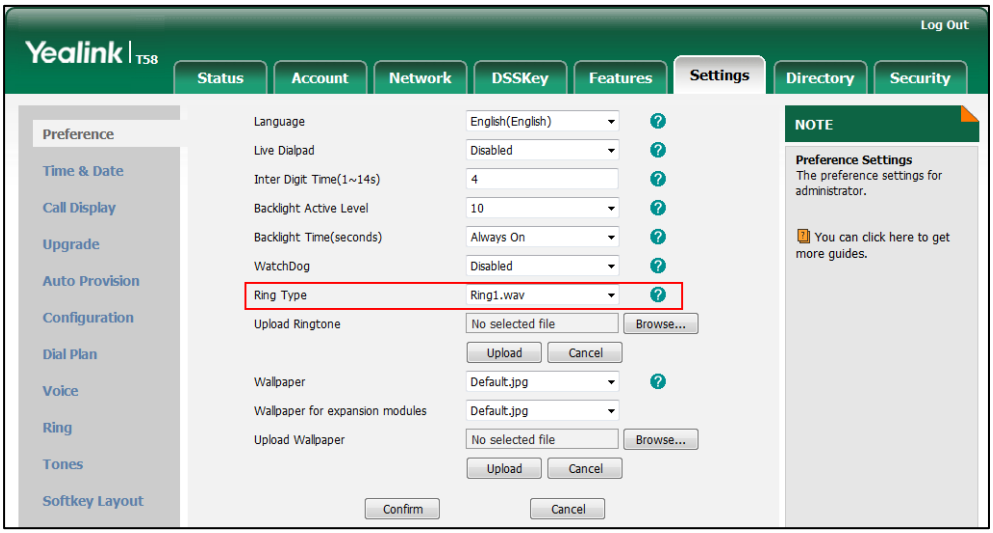
3. Click **Upload** to upload the file.



The custom ring tone appears in the pull-down list of **Ring Type**.

To change the ring tone for the phone via web user interface:

1. Click on **Settings**->**Preference**.
2. Select the desired ring tone from the pull-down list of **Ring Type**.

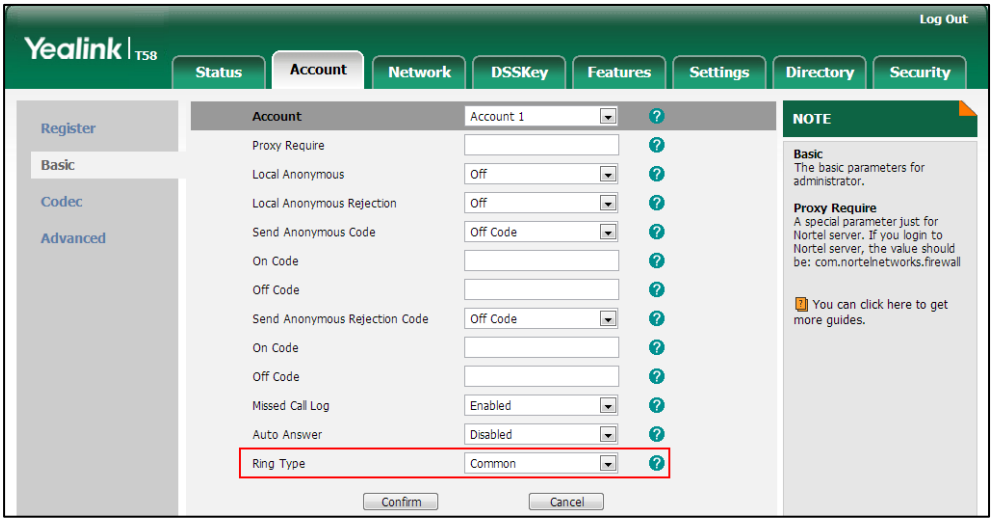


3. Click **Confirm** to accept the change.

To change the ring tone for the account via web user interface:

1. Click on **Account**->**Basic**.
2. Select the desire account from the pull-down list of **Account**.
3. Select the desired ring tone from the pull-down list of **Ring Type**.

If **Common** is selected, this account will use the ring tone selected for the phone.



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

To select a ring tone for the phone via phone user interface:

1. Tap **Settings**->**Basic**->**Sound**->**Ring Tones**->**Common**.
2. Tap the desired ring tone.
3. Tap ✓ to accept the change.

To select a ring tone for the account via phone user interface:

1. Tap **Settings**->**Basic**->**Sound**->**Ring Tones**.
2. Tap the desired account.
3. Tap the desired ring tone.

   If **Common** is selected, this account will use the ring tone selected for the phone.
4. Tap ✓ to accept the change.

Distinctive Ring Tones

Distinctive ring tones allows certain incoming calls to trigger IP phones to play distinctive ring tones. The IP phone inspects the INVITE request for an "Alert-Info" header when receiving an incoming call. If the INVITE request contains an "Alert-Info" header, the IP phone strips out the URL or keyword parameter and maps it to the appropriate ring tone.

Note If the caller already exists in the local directory, the ring tone assigned to the caller should be preferentially played.

Alert-Info headers in the following four formats:

1) Alert-Info: Bellcore-drN

2) Alert-Info: ringtone-N (or Alert-Info: MyMelodyN)

3) Alert-Info: <URL>

4) Alert-Info: info=info text;x-line-id=0

1) Alert-Info: Bellcore-drN

When the Alter-Info header contains the keyword "Bellcore-drN", the IP phone will play the desired ring tone.

The following table identifies the corresponding ring tone:

Value of N	**Ring Tone** (features.alert_info_tone = 1)	**Ring Tone** (features.alert_info_tone = 0)
1	Bellcore-dr1	Ring1.wav
2	Bellcore-dr2	Ring2.wav
3	Bellcore-dr3	Ring3.wav
4	Bellcore-dr4	Ring4.wav
5	Bellcore-dr5	Ring5.wav
6	Ring6.wav	
7	Ring7.wav	
8	Ring8.wav	
9	Silent.wav	
10	Splash.wav	
N<1 or N>10	Ring1.wav	

Examples:

Alert-Info: http://127.0.0.1/Bellcore-dr1

Alert-Info: test/Bellcore-dr1

Alert-Info: Bellcore-dr1

Alert-Info: Bellcore-dr1;x-line-id=1

Alert-Info: <http://10.1.0.31>;info=Bellcore-dr1

The following table identifies the different Bellcore ring tone patterns and cadences (These ring tones are designed for the BroadWorks server).

Bellcore Tone	Pattern ID	Pattern	Cadence	Minimum Duration (ms)	Nominal Duration (ms)	Maximum Duration (ms)
Bellcore-dr1 (standard)	1	Ringing		1800	2000	2200
		Silent		3600	4000	4400
Bellcore-dr2	2	Ringing	Long	630	800	1025
		Silent		315	400	525
		Ringing	Long	630	800	1025
		Silent		3475	4000	4400
Bellcore-dr3	3	Ringing	Short	315	400	525
		Silent		145	200	525
		Ringing	Short	315	400	525
		Silent		145	200	525
		Ringing	Long	630	800	1025
		Silent		2975	4000	4400
Bellcore-dr4	4	Ringing	Short	200	300	525
		Silent		145	200	525
		Ringing	Long	800	1000	1100
		Silent		145	200	525
		Ringing	Short	200	300	525
		Silent		2975	4000	4400
Bellcore-dr5	5	Ringing		450	500	550

Note If the user is waiting for a call, "Bellcore-dr5" is a ring splash tone that reminds the user that the DND or Always Call Forward feature is enabled on the server side.

2) Alert-Info: ringtone-N (or Alert-Info: MyMelodyN)

When the Alter-Info header contains the keyword "ringtone-N" or "MyMolodyN", the IP phone will play the corresponding local ring tone (RingN.wav), or play the first local ring tone (Ring1.wav) in about 10 seconds if "N" is greater than 10 or less than 1.

Examples:

```
Alert-Info: ringtone-2
Alert-Info: ringtone-2;x-line-id=1
```

```
Alert-Info: <http://10.1.0.31>;info=ringtone-2
Alert-Info: <http://127.0.0.1/ringtone-2>
Alert-Info: MyMelody2
Alert-Info: MyMelody2;x-line-id=1
Alert-Info: <http://10.1.0.31>;x-line-id=0;info=MyMelody2
```

The following table identifies the corresponding local ring tone:

Value of N	Ring Tone
1	Ring1.wav
2	Ring2.wav
3	Ring3.wav
4	Ring4.wav
5	Ring5.wav
6	Ring6.wav
7	Ring7.wav
8	Ring8.wav
9	Silent.wav
10	Splash.wav
N<1 or N>10	Ring1.wav

3) Alert-Info: <URL>

When the Alert-Info header contains a remote URL, the IP phone will try to download the WAV ring tone file from the URL and then play the remote ring tone if the value of the parameter "account.X.alert_info_url_enable" is set to 1 (or the item called "Distinctive Ring Tones" on the web user interface is Enabled), or play the preconfigured local ring tone in about 10 seconds if the value of the parameter "account.X.alert_info_url_enable" is set to 0 or if the IP phone fails to download the remote ring tone.

Example:

```
Alert-Info: http://192.168.0.12:8080/Custom.wav
```

4) Alert-Info: info=info text;x-line-id=0

When the Alert-Info header contains an info text, the IP phone will map the text with the Internal Ringer Text preconfigured (or the value of the parameter "distinctive_ring_tones.alert_info.X.text" is configured) on the IP phone, and then play the ring tone associated with the Internal Ringer

Text (the ring tone can be configured by the parameter "distinctive_ring_tones.alert_info.X.ringer"). If no internal ringer text maps, the IP phone will play the preconfigured local ring tone in about 10 seconds.

Example:

```
Alert-Info: info=family;x-line-id=0
Alert-Info: <http://10.1.0.31>;info=family
Alert-Info: <http://10.1.0.31>;info=family;x-line-id=0
```

Auto Answer

If the INVITE request contains the following type of strings, the IP phone will answer incoming calls automatically without playing the ring tone:

- Alert-Info: Auto Answer
- Alert-Info: info = alert-autoanswer
- Alert-Info: answer-after = 0 (or Alert-Info: Answer-After = 0)

If enable auto answer tone feature is enabled, the phone plays a warning tone to alert the user before answering the incoming call. For more information on Enable auto answer tone, refer to Auto Answer on page 292.

Note If the Alert-Info header contains multiple types of keywords, the IP phone will process the keywords in the following order: AutoAnswer>URL>info

Procedure

Distinctive ring tones can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure distinctive ring tones. **Parameter:** account.X.alert_info_url_enable
	<y0000000000xx>.cfg	Configure the internal ringer text and internal ringer file. **Parameters:** features.alert_info_tone distinctive_ring_tones.alert_info.X.text distinctive_ring_tones.alert_info.X.ringer
Web User Interface		Configure distinctive ring tones. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

	Configure the internal ringer text and internal ringer file. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-ring&q=load

Details of Configuration Parameters:

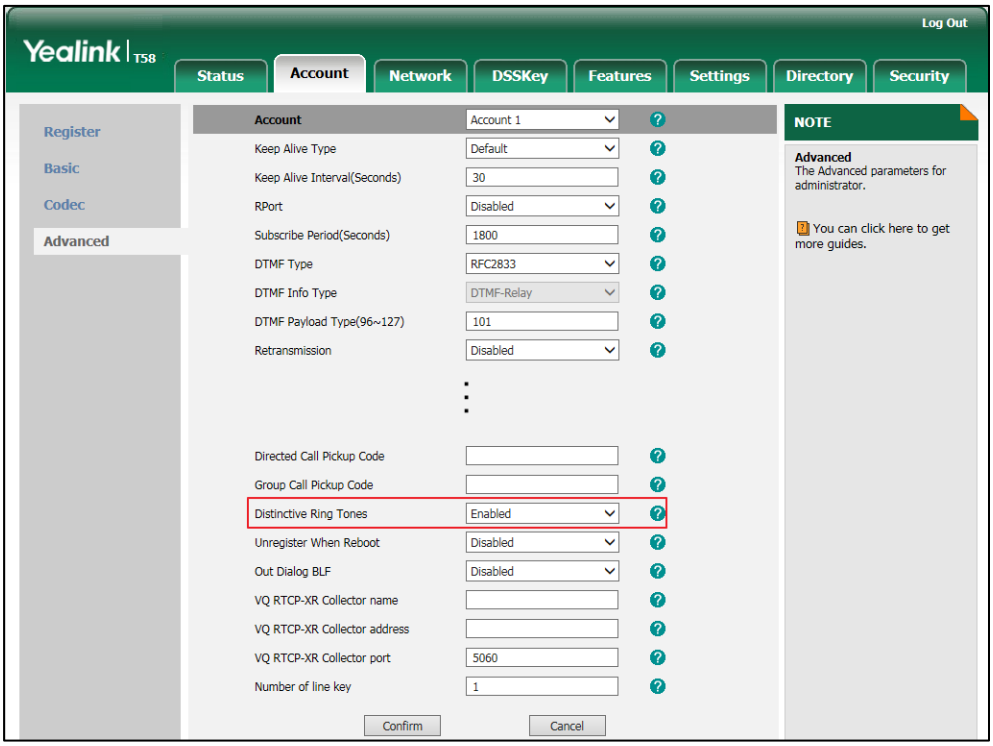
Parameters	Permitted Values	Default
account.X.alert_info_url_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to download the ring tone from the URL contained in the Alert-Info header for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->Distinctive Ring Tones **Phone User Interface:** None		
features.alert_info_tone	**0 or 1**	**0**
Description: Enables or disables the IP phone to map the keywords in the Alert-info header to the specified Bellcore ring tones. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		
distinctive_ring_tones.alert_info.X.text (X ranges from 1 to 10)	**String within 32 characters**	**Blank**
Description: Configures the internal ringer text to map the keywords contained in the Alert-Info header.		

Parameters	Permitted Values	Default
Example: distinctive_ring_tones.alert_info.1.text = Family **Web User Interface:** Settings->Ring->Internal Ringer Text **Phone User Interface:** None		
distinctive_ring_tones.alert_info.X.ringer (X ranges from 1 to 10)	**Integer from 1 to 10**	**1**
Description: Configures the desired ring tones for each internal ringer text. The value ranges from 1 to 10, the digit stands for the appropriate ring tone. **1**-Ring1.wav **2**-Ring2.wav **3**-Ring3.wav **4**-Ring4.wav **5**-Ring5.wav **6**-Ring6.wav **7**-Ring7.wav **8**-Ring8.wav **9**-Silent.wav **10**-Splash.wav **Web User Interface:** Settings->Ring->Internal Ringer File **Phone User Interface:** None		

To configure distinctive ring tones via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

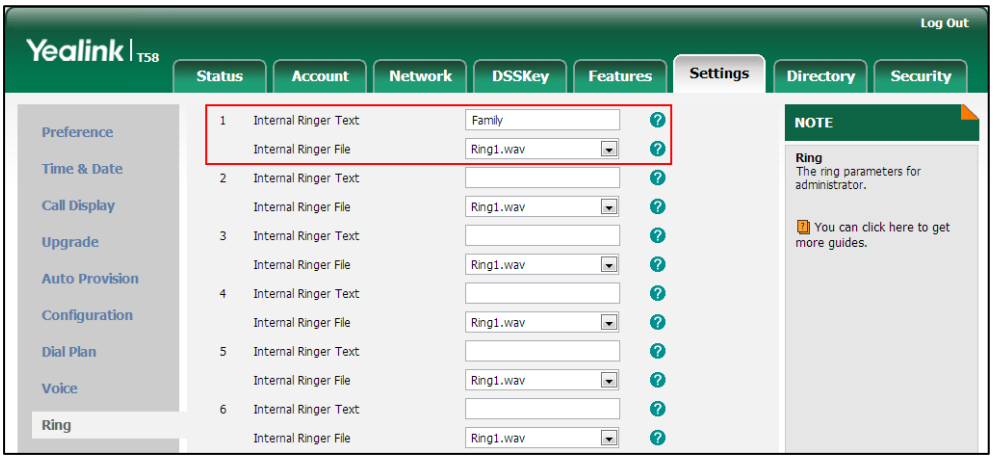
3. Select the desired value from the pull-down list of **Distinctive Ring Tones**.



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

To configure the internal ringer text and internal ringer file via web user interface:

1. Click on **Settings**->**Ring**.
2. Enter the keywords in the **Internal Ringer Text** fields.
3. Select the desired ring tones for each text from the pull-down lists of **Internal Ringer File**.



4. Click **Confirm** 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
- China
- Czech
- Denmark
- Finland
- France
- Germany
- Great Britain
- Greece
- Hungary
- Lithuania
- India
- Italy
- Japan
- Mexico
- New Zealand
- Netherlands
- Norway
- Portugal
- Spain
- Switzerland
- Sweden
- Russia
- United States
- Chile
- Czech ETSI

Configured tones can be heard on IP phones for the following conditions.

Condition	Description
Dial	When on the pre-dialing screen (not applicable to CP960 IP phones)

Condition	Description
Secondary Dial	When adding a comma "," to the digit map (For more information on digit map, refer to Dial Plan using Digit Map String Rules)
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)
Dial Recall	When receiving a call back
Info	When receiving a special message
Stutter	When receiving a voice mail (For more information on voice mail tone, refer to Voice Mail Tone)
Auto Answer	When automatically answering a call (For more information on auto answer, refer to Auto Answer)

Procedure

Tones can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the tones for the IP phone. **Parameters:** voice.tone.country voice.tone.dial voice.tone.secondary_dial voice.tone.ring voice.tone.busy voice.tone.congestion voice.tone.callwaiting voice.tone.dialrecall voice.tone.info voice.tone.stutter voice.tone.autoanswer
Web User Interface		Configure the tones for the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m

	=mod_data&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, 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] [,element]… Where **element** = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration **Freq**: the frequency of the tone (ranges from 200 to 4000Hz). If it is set to 0Hz, it means the tone is not played. 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 tones (e.g., !250/200,0/1000,200+300/500,200+500+800+1500/1000). **Note**: It is not applicable to CP960 IP phones. It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:**		

Parameters	Permitted Values	Default
Settings->Tones->Dial **Phone User Interface:** None		
voice.tone.secondary_dial	**String**	**350+440/3000**
Description: Customizes the secondary dial tone. 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. If you want to disable this warning tone, set it to 0. **Web User Interface:** Settings->Tones->Secondary Dial **Phone User Interface:** None		
voice.tone.ring	**String**	**Blank**
Description: Customizes the ringback tone. 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->Ring Back **Phone User Interface:** None		
voice.tone.busy	**String**	**Blank**
Description: Customizes the tone when the callee is busy. 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->Busy		

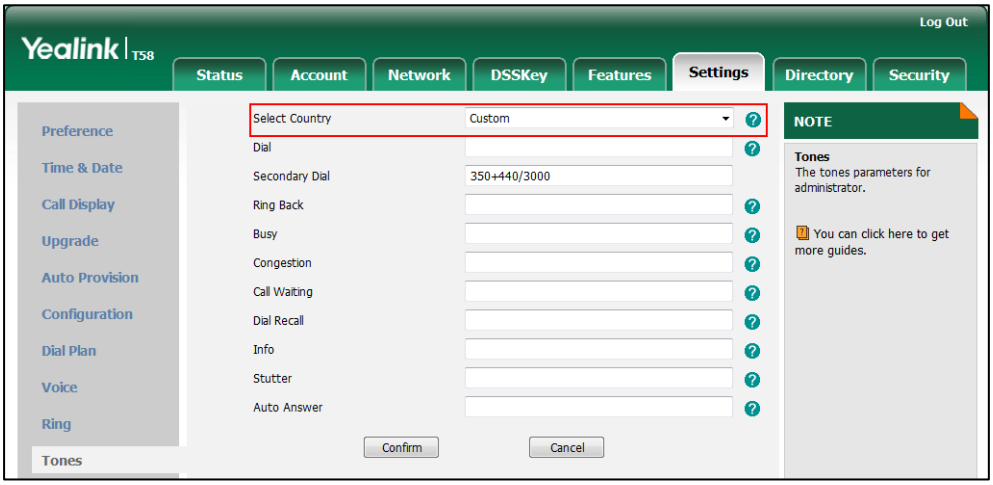
Parameters	Permitted Values	Default
Phone User Interface: None		
voice.tone.congestion	**String**	**Blank**
Description: Customizes the tone when the network is congested. The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial". **Note**: 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		
voice.tone.callwaiting	**String**	**Blank**
Description: Customizes the call waiting tone. 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->Call Waiting **Phone User Interface:** None		
voice.tone.dialrecall	**String**	**Blank**
Description: Customizes the call back tone. 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->Dial Recall **Phone User Interface:** None		

Parameters	Permitted Values	Default
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". **Note**: It works only if the value of the parameter "voice.tone.country" is set to Custom. **Web User Interface:** Settings->Tones->Info **Phone User Interface:** None		
voice.tone.stutter	**String**	**Blank**
Description: Customizes the tone when the IP phone receives a voice mail. 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->Stutter **Phone User Interface:** None		
voice.tone.autoanswer	**String**	**Blank**
Description: Customizes the warning tone for auto answer. 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->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**.

   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 614.

Procedure

Voice mail tone can be configured using the following methods.

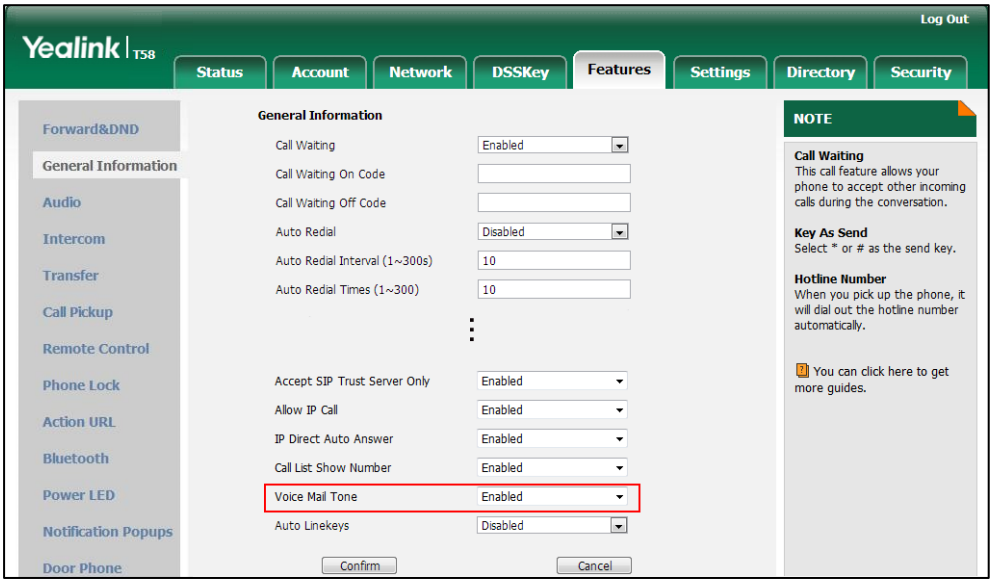
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure whether to play a warning tone when the IP phone receives a new voice mail. **Parameter:** features.voice_mail_tone_enable
Web User Interface		Configure whether to play a warning tone when the IP phone receives a new voice mail. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.voice_mail_tone_enable	**0 or 1**	**1**
Description: Enables or disables the IP phone to play a warning tone when it receives a new voice mail. **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**.



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 (wired headset, Bluetooth headset or USB 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 *Yealink phone-specific user guide*.

Note It is not applicable to CP960 IP phones.

Procedure

Ringer device for headset can be configured using the following methods.

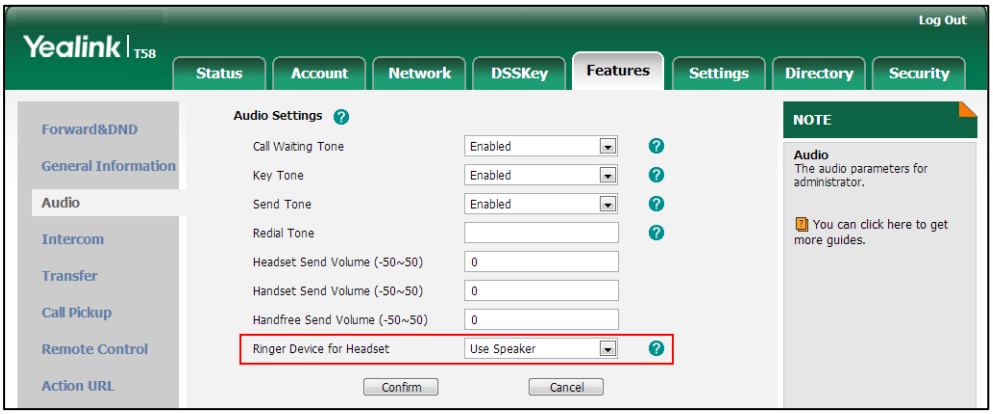
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the ringer device for the IP phone. **Parameter:** features.ringer_device.is_use_headset
Web User Interface		Configure the ringer device for the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-audio&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.ringer_device.is_use_headset	**0, 1 or 2**	**0**
Description: Configures the ringer device for the IP phone. **0**-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. **Note**: It is not applicable to CP960 IP phones. **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**.



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.

Note It is not applicable to CP960 IP phones.

Procedure

Headset prior can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure headset prior. **Parameter:** features.headset_prior
Web User Interface		Configure headset prior. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

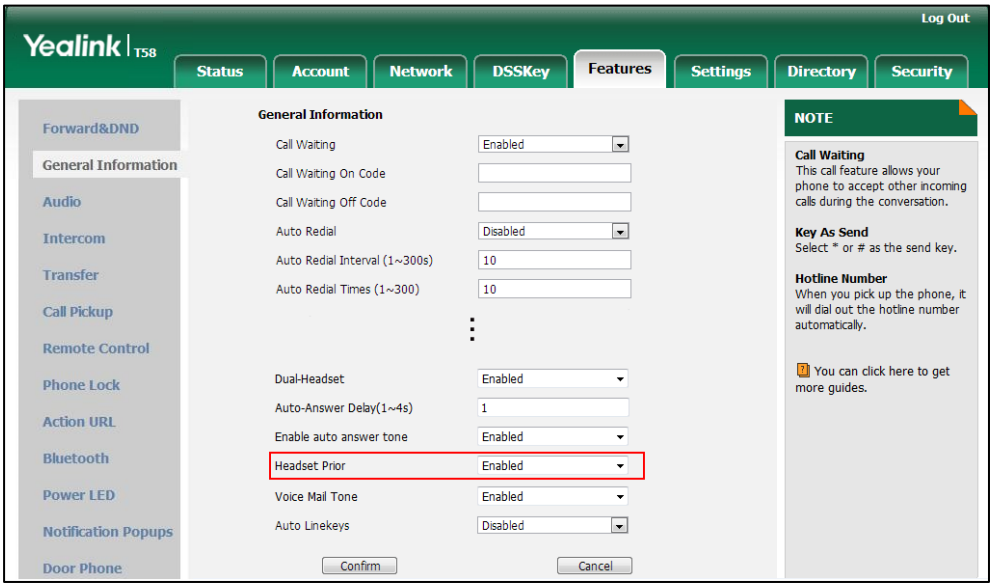
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.headset_prior	**0 or 1**	**0**

Parameter	Permitted Values	Default
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 0 (Disabled), the headset mode can be deactivated by pressing the Speakerphone key or the HEADSET key except off-hook. If it is set to 1 (Enabled), the headset mode will not be deactivated until the user presses the HEADSET key again. **Note**: It is not applicable to CP960 IP phones. **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**.
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.

Note Bluetooth headset and USB headset are unavailable when dual headset is enabled.

It is not applicable to CP960 IP phones.

Procedure

Dual headset can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure dual headset. **Parameter:** features.headset_training
Web User Interface		Configure dual headset. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

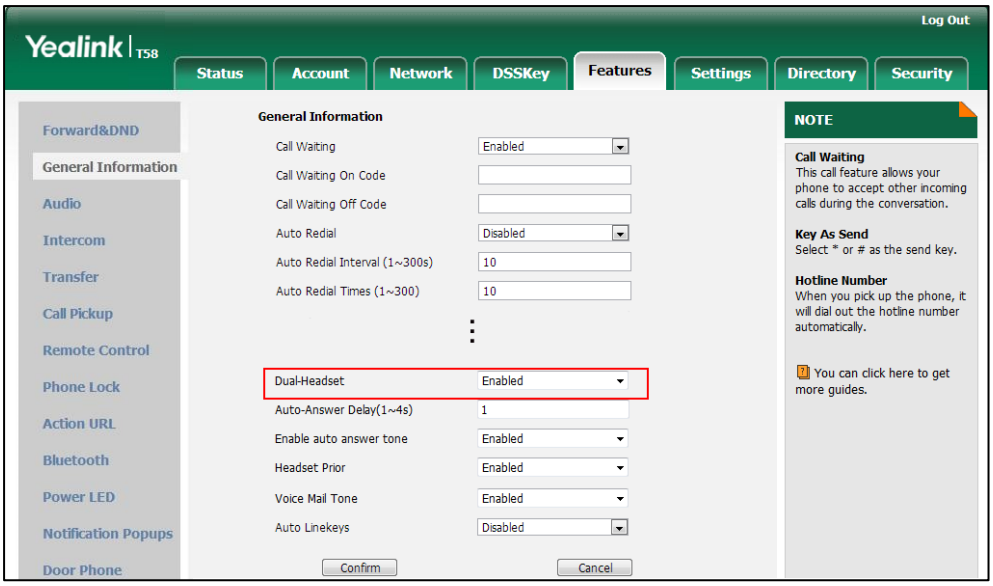
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
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. **Note**: It is not applicable to CP960 IP phones. **Web User Interface:** Features->General Information->Dual-Headset		

Parameter	Permitted Values	Default
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**.



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

Sending Volume

Sending volume allows user to adjust the sending volume of currently engaged audio devices (handset, speakerphone or headset) when the phone is in use.

Procedure

Sending volume can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the sending volume of the speaker. **Parameter:** voice.handfree_send
		Configure the sending volume of the handset. **Parameter:** voice.handset_send

		Configure the sending volume of the headset. **Parameter:** voice.headset_send
Web User Interface		Configure the sending volume of the speaker/handset/headset. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-audio&q=load

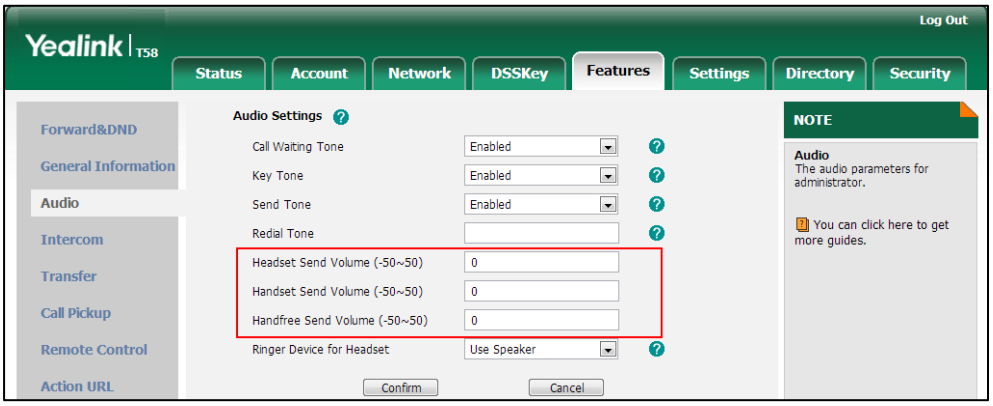
Details of the Configuration Parameters:

Parameters	Permitted Values	Default
voice.handfree_send	**Integer from -50 to 50**	**0**
Description: Configures the sending volume of the speaker. **Note:** We recommend that you modify this parameter cautiously. An unreasonable value may render the voice quality bad. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Features->Audio->Handfree Send Volume (-50~50) **Phone User Interface:** None		
voice.handset_send	**Integer from -50 to 50**	**0**
Description: Configures the sending volume of the handset. **Note:** It is not applicable to CP960 IP phones. We recommend that you modify this parameter cautiously. An unreasonable value may render the voice quality bad. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Features->Audio->Handset Send Volume (-50~50) **Phone User Interface:** None		

Parameters	Permitted Values	Default
voice.headset_send	**Integer from -50 to 50**	**0**
Description: Configures the sending volume of the headset. **Note:** It is not applicable to CP960 IP phones. We recommend that you modify this parameter cautiously. An unreasonable value may render the voice quality bad. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Features->Audio->Headset Send Volume (-50~50) **Phone User Interface:** None		

To configure sending volume via web user interface:

1. Click on **Features**->**Audio**.
2. Enter the desired value in the **Headset Send Volume (-50~50)** field.
3. Enter the desired value in the **Handset Send Volume (-50~50)** field.
4. Enter the desired value in the **Handfree Send Volume (-50~50)** field.



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

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

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 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.

Supported Audio Codecs

The following table lists the audio codecs supported by SIP-T58V/T58A/T56A/CP960 IP phones:

Phone Model	Supported Audio Codecs	Default Audio Codecs
SIP-T58V/T58A/T56A/ CP960	G.722.1c(48kb/s), G.722.1c(32kb/s), G.722.1c(24kb/s), G.722.1(24kb/s), G722, PCMU, PCMA, G729, G726-40, G726-32, G726-24, G726-16, iLBC, G723_53, G723_63, Opus	G.722.1c(48kb/s), G.722.1c(32kb/s), G.722.1c(24kb/s), G.722.1(24kb/s), G722, PCMU, PCMA, G729

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

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

The following table summarizes the supported audio codecs on IP phones:

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
G.722.1c	G.722.1	RFC 5577	48 Kbps	32 Ksps	20ms
G.722.1c		RFC 5577	32 Kbps	32 Ksps	20ms
G.722.1c		RFC 5577	24 Kbps	32 Ksps	20ms
G.722.1	G.722.1	RFC 5577	24 Kbps	16 Ksps	20ms
G722	G.722	RFC 3551	64 Kbps	16 Ksps	20ms
PCMA	G.711 a-law	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

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
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/ G723_63	G.723.1	RFC 3551	5.3 Kbps 6.3 Kbps	8 Ksps	30ms
iLBC	iLBC	RFC 3952	15.2 Kbps 13.33 Kbps	8 Ksps	20ms 30ms
Opus	Opus	RFC 6716	8-12 Kbps 16-20 Kbps 28-40 Kbps 48-64 Kbps 64-128 Kbps	8 Ksps 12 Ksps 16 Ksps 24 Ksps 48 Ksps	20ms

Note The network bandwidth necessary to send the encoded audio is typically 5~10% higher than the bit rate due to packetization overhead. For example, a two-way G.722 audio-only call at 64 Kbps consumes about 135 Kbps of network bandwidth.

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.

The corresponding attributes of the codec for SIP-T58V/T58A/T56A are listed as follows:

Codec	Configuration	Priority	RTPmap
G.722.1c(48kb/s)	Configuration Files Web User Interface	1	121
G.722.1c(32kb/s)	Configuration Files Web User Interface	2	122
G.722.1c(24kb/s)	Configuration Files Web User Interface	3	123
G.722.1(24kb/s)	Configuration Files Web User Interface	4	124
G722	Configuration Files Web User Interface	5	9
PCMU	Configuration Files	6	0

Codec	Configuration	Priority	RTPmap
	Web User Interface		
PCMA	Configuration Files Web User Interface	7	8
G729	Configuration Files Web User Interface	8	18
Opus	Configuration Files Web User Interface	0	107
G726-40	Configuration Files Web User Interface	0	105
G726-32	Configuration Files Web User Interface	0	102
G726-24	Configuration Files Web User Interface	0	104
G726-16	Configuration Files Web User Interface	0	103
iLBC	Configuration Files Web User Interface	0	106
G723_53	Configuration Files Web User Interface	0	4
G723_63	Configuration Files Web User Interface	0	4

Audio Codec Configuration

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the codecs to use on a per-line basis. **Parameter:** account.X.codec.<payload_type>.enable

		Configure the priority and rtpmap for the enabled codec. **Parameters:** account.X.codec.<payload_type>.priority account.X.codec.<payload_type>.rtpmap
Web User Interface		Configure the codecs to use on a per-line basis. Configure the priority and rtpmap for the enabled codec. **Navigate to**: http://<phoneIPAddress>/servlet?p=account-codec&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.codec.<payload_type>.enable (where <payload_type> should be replaced by the name of audio codec)	**0 or 1**	**Refer to the following content**
Description: Enables or disables the specified codec for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Valid Audio Codec**: G722.1c(48kb/s), G722.1c(32kb/s), G722.1c(24kb/s), G722.1(24kb/s), G722, PCMU, PCMA, G729, Opus, G726-40, G726-32, G726-24, G726-16, iLBC, G723_63, G723_53 **Default:** When audio codec is G.722.1c(48kb/s), the default value is 1; When audio codec is G.722.1c(32kb/s), the default value is 1; When audio codec is G.722.1c(24kb/s), the default value is 1; When audio codec is G.722.1(24kb/s), the default value is 1; When audio codec is G722, the default value is 1; When audio codec is PCMU, the default value is 1; When audio codec is PCMA, the default value is 1; When audio codec is G729, the default value is 1;		

Parameters	Permitted Values	Default
When audio codec is Opus, the default value is 0; When audio codec is G726-40, the default value is 0; When audio codec is G726-32, the default value is 0; When audio codec is G726-24, the default value is 0; When audio codec is G726-16, the default value is 0; When audio codec is iLBC, the default value is 0; When audio codec is G723_63, the default value is 0; When audio codec is G723_53, the default value is 0; **Example:** account.1.codec.g722_1c_48kpbs.enable = 1 account.1.codec.g722_1c_32kpbs.enable = 1 account.1.codec.g722_1c_24kpbs.enable = 1 account.1.codec.g722_1_24kpbs.enable = 1 account.1.codec.g722.enable = 1 account.1.codec.pcmu.enable = 1 account.1.codec.pcma.enable = 1 account.1.codec.g729.enable = 1 account.1.codec.opus.enable = 0 account.1.codec.g726_40.enable = 0 account.1.codec.g726_32.enable = 0 account.1.codec.g726_24.enable = 0 account.1.codec.g726_16.enable = 0 account.1.codec.ilbc.enable = 0 account.1.codec.g723_63.enable = 0 account.1.codec.g723_53.enable = 0 It means that the codecs G.722.1c(48kb/s), G.722.1c(32kb/s), G.722.1c(24kb/s), G.722.1(24kb/s), G722, PCMU, PCMA and G729 are enabled on the account 1. **Note**: The name of audio codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect. **Web User Interface:** Account->Codec->Audio Codec **Phone User Interface:** None		
account.X.codec.<payload_type>.priority (where <payload_type> should be replaced by	**Integer from 0 to 8**	**Refer to the following**

Parameters	Permitted Values	Default
the name of audio codec)		**content**

Description:

Configures the priority of the enabled audio codec for account X.

X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)

X is equal to 1 (for CP960)

Valid Audio Codec:

G722.1c(48kb/s), G722.1c(32kb/s), G722.1c(24kb/s), G722.1(24kb/s), G722, PCMU, PCMA, G729, Opus, G726-40, G726-32, G726-24, G726-16, iLBC, G723_63, G723_53

Default:

When audio codec is G722.1c(48kb/s), the default value is 1;

When audio codec is G722.1c(32kb/s), the default value is 2;

When audio codec is G722.1c(24kb/s), the default value is 3;

When audio codec is G722.1(24kb/s), the default value is 4;

When audio codec is G722, the default value is 5;

When audio codec is PCMU, the default value is 6;

When audio codec is PCMA, the default value is 7;

When audio codec is G729, the default value is 8;

When audio codec is Opus, the default value is 0;

When audio codec is G726_40, the default value is 0;

When audio codec is G726_32, the default value is 0;

When audio codec is G726_24, the default value is 0;

When audio codec is G726_16, the default value is 0;

When audio codec is iLBC, the default value is 0;

When audio codec is G723_63, the default value is 0;

When audio codec is G723_53, the default value is 0;

Example:

account.1.codec.g722_1c_48kpbs.priority = 1

account.1.codec.g722_1c_32kpbs.priority = 2

account.1.codec.g722_1c_24kpbs.priority = 3

account.1.codec.g722_1_24kpbs.priority = 4

account.1.codec.g722.priority = 5

account.1.codec.pcmu.priority = 6

account.1.codec.pcma.priority = 7

account.1.codec.g729.priority = 8

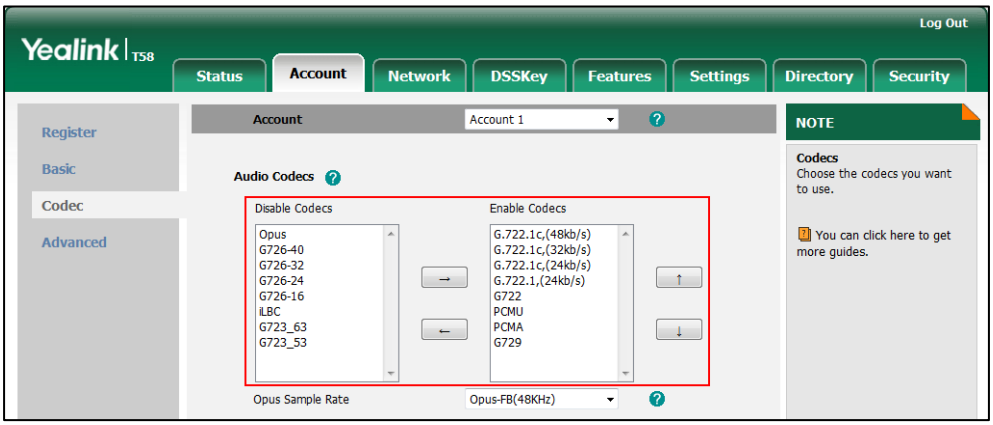
account.1.codec.opus.priority = 0

Parameters	Permitted Values	Default
account.1.codec.g726_40.priority = 0 account.1.codec.g726_32.priority = 0 account.1.codec.g726_24.priority = 0 account.1.codec.g726_16.priority = 0 account.1.codec.ilbc.priority = 0 account.1.codec.g723_63.priority = 0 account.1.codec.g723_53.priority = 0 **Note:** The name of audio codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect. **Web User Interface:** Account->Codec->Audio Codec **Phone User Interface:** None		
account.X.codec.<payload_type>.rtpmap (where <payload_type> should be replaced by the name of audio codec)	**Integer from 0 to 127**	**Refer to the following content**
Description: Configures the rtpmap of the audio codec for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Valid Audio Codec**: G722.1c(48kb/s), G722.1c(32kb/s), G722.1c(24kb/s), G722.1(24kb/s), G726-16, G726-24, G726-32, G726-40, iLBC, Opus **Default:** When audio codec is G722.1c(48kb/s),the default value is 121; When audio codec is G722.1c(32kb/s),the default value is 122; When audio codec is G722.1c(24kb/s),the default value is 123; When audio codec is G722.1(24kb/s),the default value is 124; When audio codec is G726-40, the default value is 105; When audio codec is G726-32, the default value is 102; When audio codec is G726-24, the default value is 104; When audio codec is G726-16, the default value is 103; When audio codec is iLBC, the default value is 106; When audio codec is Opus, the default value is 107; **Example:**		

Parameters	Permitted Values	Default
account.1.codec.g722_1c_48kpbs.rtpmap = 121 account.1.codec.g722_1c_32kpbs.rtpmap = 122 account.1.codec.g722_1c_24kpbs.rtpmap = 123 account.1.codec.g722_1_24kpbs.rtpmap = 124 account.1.codec.g726_40.rtpmap = 105 account.1.codec.g726_32.rtpmap = 102 account.1.codec.g726_24.rtpmap = 104 account.1.codec.g726_16.rtpmap = 103 account.1.codec.ilbc.rtpmap = 108 account.1.codec.opus.rtpmap = 107 **Note:** The name of audio codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect. **Web User Interface:** None **Phone User Interface:** None		

To configure the codecs to use and adjust the priority of the enabled codecs via web user interface:

1. Click on **Account**->**Codec**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired codec from the **Disable Codecs** column and then click →.
   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 ←.
6. To adjust the priority of codecs, select the desired codec and then click ↑ or ↓.



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

Packetization Time (PTime)

Ptime 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.

The following table summarizes the valid values of ptime for each audio codec:

Codec	Packetization Time (Minimun)	Packetization Time (Maximun)
G.722.1c(48kb/s)	20ms	60ms
G.722.1c(32kb/s)	20ms	60ms
G.722.1c(24kb/s)	20ms	60ms
G.722.1(24kb/s)	20ms	60ms
G722	10ms	40ms
PCMA	10ms	40ms
PCMU	10ms	40ms
G729	10ms	80ms
G726-16	10ms	30ms
G726-24	10ms	30ms
G726-32	10ms	30ms
G726-40	10ms	30ms
G723_53/G723_63	30ms	60ms
iLBC	20ms	30ms
Opus	10ms	20ms

Procedure

PTime can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the ptime. **Parameter:** account.X.ptime

Web User Interface	Configure the ptime. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

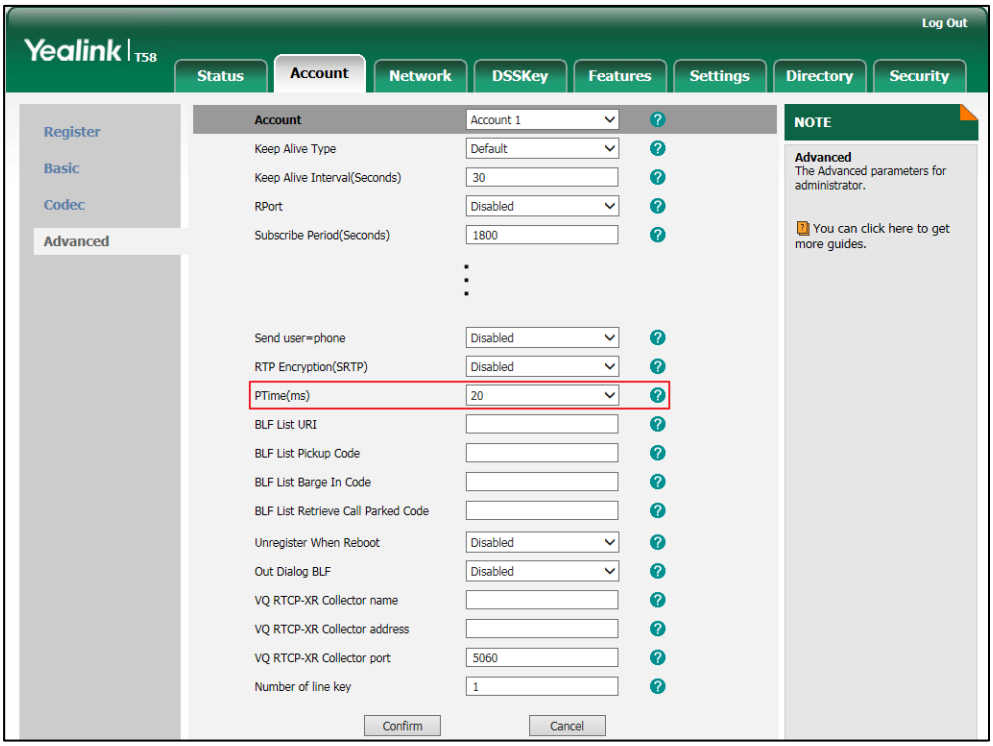
Details of Configuration Parameter:

Parameter	Permitted Values	Default
account.X.ptime	**0, 10, 20, 30, 40, 50 or 60**	**20**
Description: Configures the ptime (in milliseconds) for the codec for account X. **0**-Disabled **10**-10 **20**-20 **30**-30 **40**-40 **50**-50 **60**-60 If it is set to 0 (Disabled), the ptime negotiation is disabled. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.ptime = 20 **Web User Interface:** Account->Advanced->PTime(ms) **Phone User Interface:** None		

To configure the ptime for the account via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.

3. Select the desired value from the pull-down list of **PTime(ms)**.



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

Opus Sample Rate

You can configure the following types of sample rate for Opus audio codec:

- Opus-FB(48KHz)
- Opus-SWB(24KHz)
- Opus-WB(16KHz)
- Opus-MB(12KHz)
- Opus-NB(8KHz)

Procedure

Opus sample rate can be only configured via web user interface.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the Opus sample rate. **Parameter:** account.X.codec.opus.para
Web User Interface		Configure the Opus sample rate. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-codec&q=load&acc=

	0

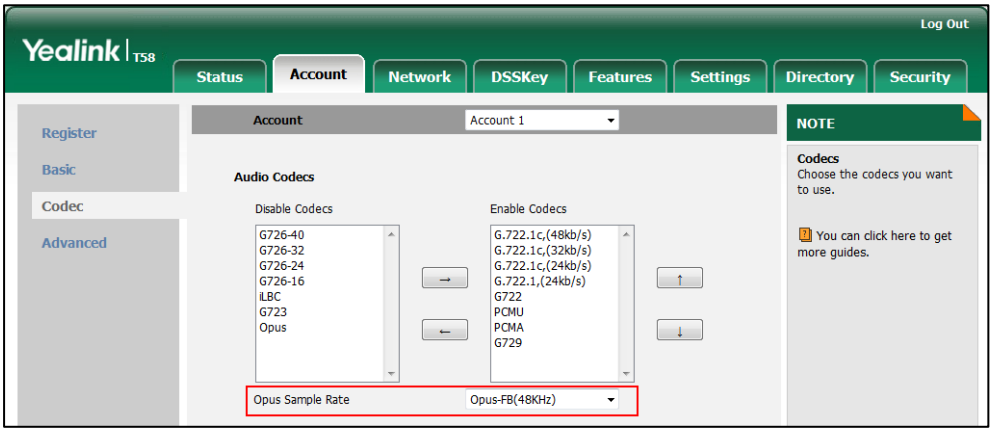
Details of Configuration Parameter:

Parameter	Permitted Values	Default
account.X.codec.opus.para	**Opus-FB, Opus-SWB, Opus-WB, Opus-MB, Opus-NB**	**Opus-FB**
Description: Configures the sample rate for the Opus codec. **Opus-FB**-Opus-FB(48KHz) **Opus-SWB**-Opus-SWB(24KHz) **Opus-WB**-Opus-WB(16KHz) **Opus-MB**-Opus-MB(12KHz) **Opus-NB**-Opus-NB(8KHz) X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Example:** account.1.codec.opus.para = Opus-FB **Web User Interface:** Account->Codec->Opus Sample Rate **Phone User Interface:** None		

To configure the opus sample rate via web user interface:

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

2. Select the desired value from the pull-down list of **Opus Sample Rate**.



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

Acoustic Clarity Technology

Acoustic Echo Cancellation (AEC)

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

AEC can be configured using the following methods.

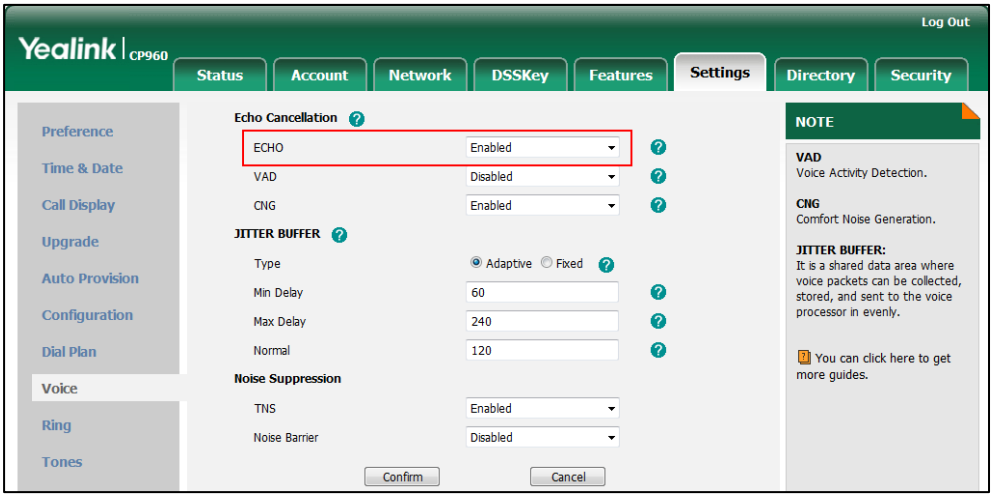
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure AEC. **Parameter:** voice.echo_cancellation
Web User Interface		Configure AEC. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-voice&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.echo_cancellation	**0 or 1**	**1**
Description: Enables or disables the AEC (Acoustic Echo Canceller) feature 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**.



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

Background Noise Suppression (BNS)

Background noise suppression (BNS) is designed primarily for hands-free operation and reduces background noise to enhance communication in noisy environments.

Automatic Gain Control (AGC)

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 soft-talkers.

Voice Activity Detection (VAD)

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 following methods.

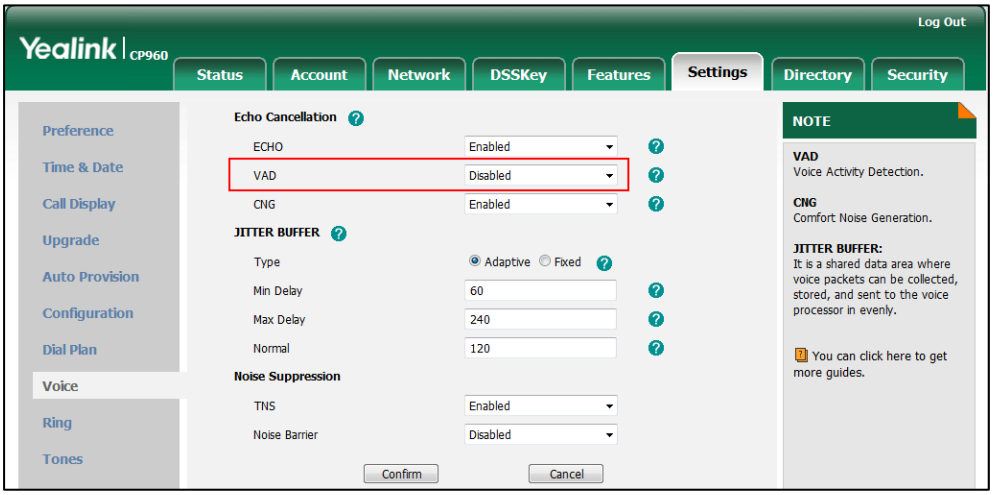
Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure VAD. **Parameter:** voice.vad
Web User Interface		Configure VAD. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-voice&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.vad	**0 or 1**	**0**
Description: Enables or disables the VAD (Voice Activity Detection) feature 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**.



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

Comfort Noise Generation (CNG)

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure CNG. **Parameter:** voice.cng
Web User Interface		Configure CNG. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-voice&q=load

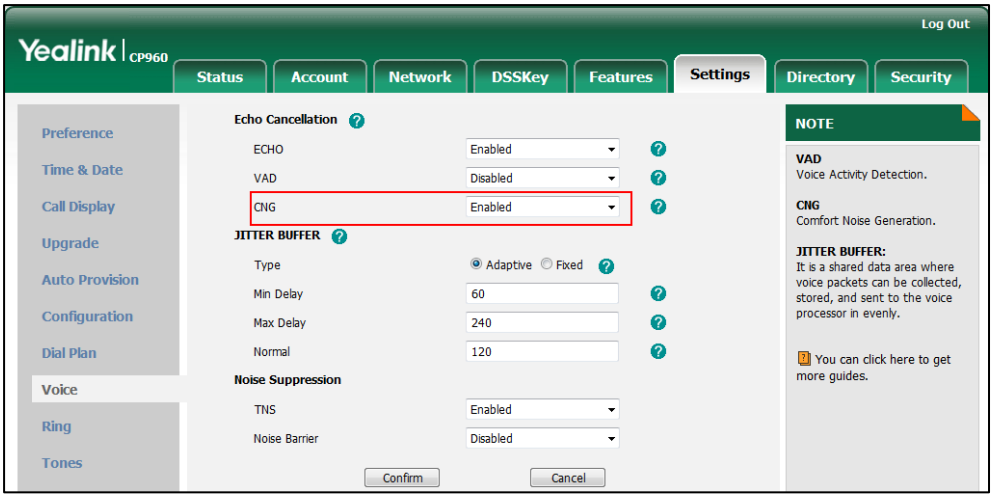
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
voice.cng	**0 or 1**	**1**
Description: Enables or disables the CNG (Comfortable Noise Generation) 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**.



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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the mode of jitter buffer and the delay time for jitter buffer in the wired network. **Parameters:** 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 in the wireless network.

		Parameters: voice.jib.wifi.adaptive voice.jib.wifi.min voice.jib.wifi.max voice.jib.wifi.normal
Web User Interface		Configure the mode of jitter buffer and the delay time for jitter buffer in the wired/wireless network. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-voice&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
voice.jib.adaptive	**0 or 1**	**1**
Description: Configures the type of jitter buffer in the wired network. **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 milliseconds) of jitter buffer in the wired network. **Note**: It works only if the value of the parameter "voice.jib.adaptive" is set to 1 (Adaptive). **Web User Interface:** Settings->Voice->JITTER BUFFER->Min Delay **Phone User Interface:** None		
voice.jib.max	**Integer from 0 to 400**	**240**

Parameters	Permitted Values	Default
Description: Configures the maximum delay time (in milliseconds) of jitter buffer in the wired network. **Note**: 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	**Integer from 0 to 400**	**120**
Description: Configures the normal delay time (in milliseconds) of jitter buffer in the wired network. **Note**: It works only if the value of the parameter "voice.jib.adaptive" is set to 0 (Fixed). **Web User Interface:** Settings->Voice->JITTER BUFFER->Normal **Phone User Interface:** None		
voice.jib.wifi.adaptive	**0 or 1**	**1**
Description: Configures the type of jitter buffer in the wireless network. **0**-Fixed **1**-Adaptive **Web User Interface:** None **Phone User Interface:** None		
voice.jib.wifi.min	**Integer from 0 to 500**	**60**
Description: Configures the minimum delay time (in milliseconds) of jitter buffer in the wireless network. **Note**: It works only if the value of the parameter "voice.jib.wifi.adaptive" is set to 1 (Adaptive). The value of the minimum delay time should be less than or equal to that of the normal delay time (configured by the parameter "voice.jib.wifi.normal"). **Web User Interface:**		

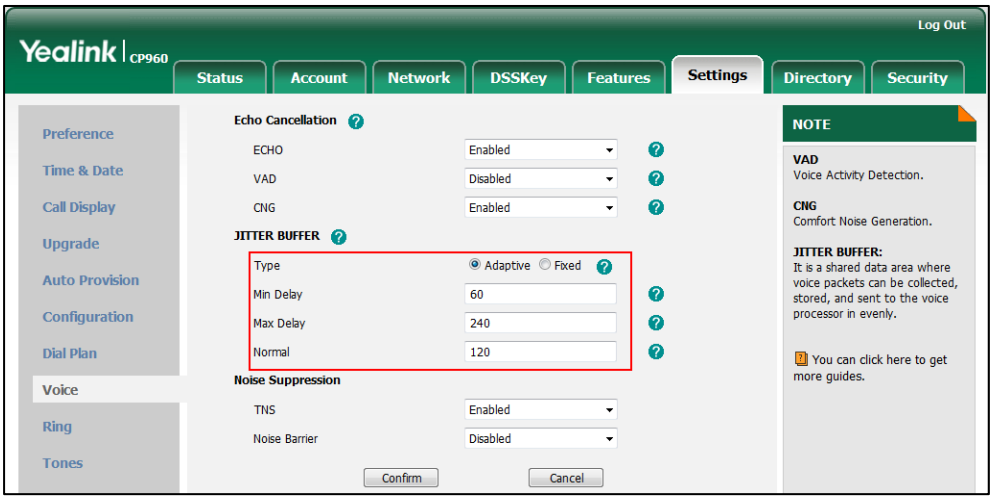
Parameters	Permitted Values	Default
None **Phone User Interface:** None		
voice.jib.wifi.max	**Integer from 0 to 500**	**500**
Description: Configures the maximum delay time (in milliseconds) of jitter buffer in the wireless network. **Note**: It works only if the value of the parameter "voice.jib.wifi.adaptive" is set to 1 (Adaptive). **Web User Interface:** None **Phone User Interface:** None		
voice.jib.wifi.normal	**Integer from 0 to 500**	**240**
Description: Configures the normal delay time (in milliseconds) of jitter buffer in the wireless network. **Note**: It works only if the value of the parameter "voice.jib.wifi.adaptive" is set to 0 (Fixed). The value of the normal delay time should be less than or equal to that of the maximum delay time (configured by the parameter "voice.jib.wifi.max"). **Web User Interface:** None **Phone User Interface:** None		

To configure Jitter Buffer in the wired network via web user interface:

1. Click on **Settings**->**Voice**.
2. Mark the desired radio box in the **Type** field.
3. Enter the minimum delay time for adaptive jitter buffer in the **Min Delay** field.
   The valid value ranges from 0 to 400.
4. Enter the maximum delay time for adaptive jitter buffer in the **Max Delay** field.
   The valid value ranges from 0 to 400.

5. Enter the fixed delay time for fixed jitter buffer in the **Normal** field.

   The valid value ranges from 0 to 400.



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

Noise Suppression

The impact noise in the room are picked-up, including paper rustling, coffee mugs, coughing, typing, and silverware striking plates. These noises, when transmitted to remote participants, can be very distracting.

You can enable the Noise Suppression feature to suppress these noises.

Procedure

Noise Suppression can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure Noise Suppression. **Parameter:** voice.tns.enable
Web User Interface		Configure the Noise Suppression. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-voice&q=load

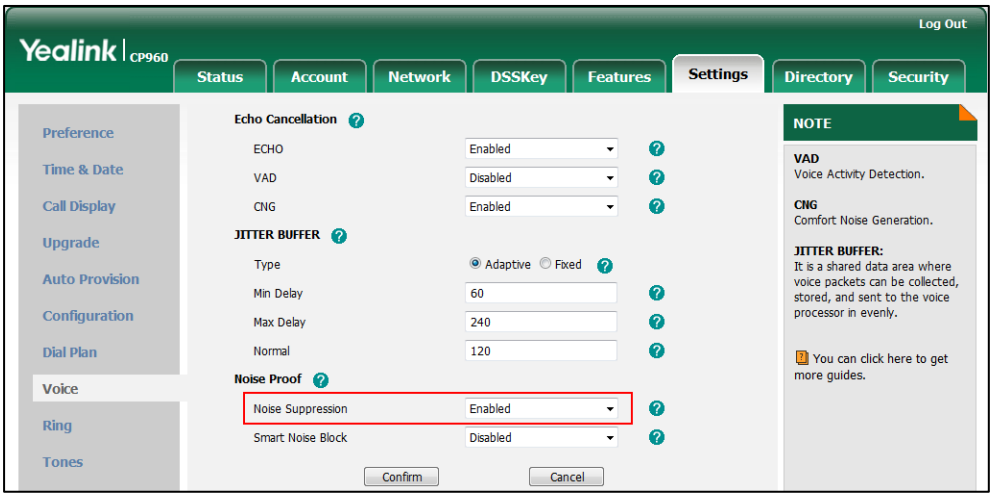
Details of Configuration Parameter:

Parameter	Permitted Values	Default
voice.tns.enable	**0 or 1**	**1**

Parameter	Permitted Values	Default
Description: Enables or disables the Noise Suppression feature on the IP phones. **0**-Disabled **1**-Enabled **Note**: It is only applicable to CP960 IP phones. **Web User Interface:** Settings->Voice->Noise Proof->Noise Suppression **Phone User Interface:** None		

To configure Noise Suppression via web user interface:

1. Click on **Settings**->**Voice**.
2. Select the desired value from the pull-down list of **Noise Suppression**.



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

Smart Noise Block

You can use the Smart Noise Block feature to block out the noises when there is no speech in a call.

Procedure

Smart Noise Block can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure Smart Noise Block. **Parameter:** voice.ans_nb.enable

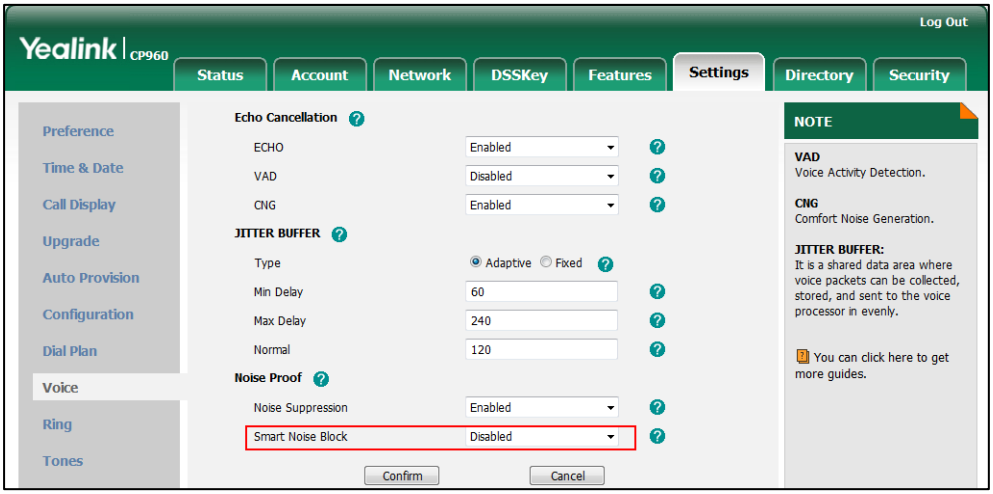
Web User Interface	Configure Smart Noise Block. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-voice&q=load

Details of Configuration Parameter:

Parameter	Permitted Values	Default
voice.ans_nb.enable	**0 or 1**	**0**
Description: Enables or disables the Smart Noise Block feature on the IP phones. **0**-Disabled **1**-Enabled **Note**: It works only if the value of the parameter "voice.tns.enable" is set to 1 (Enabled). It is only applicable to CP960 IP phones. **Web User Interface:** Settings->Voice->Noise Proof->Smart Noise Block **Phone User Interface:** None		

To configure Smart Noise Block via web user interface:

1. Click on **Settings**->**Voice**.
2. Select the desired value from the pull-down list of **Smart Noise Block**.



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)).

DTMF Keypad Frequencies:

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

Methods of Transmitting DTMF Digit

Three methods of transmitting DTMF digits on SIP calls:

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

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

RFC 2833

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

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

INBAND

DTMF digits are transmitted within the audio of the IP phone conversation. It uses the same

codec as your voice and is audible to conversation partners.

SIP INFO

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

Procedure

Configuration changes can be performed using the following methods.

<table>
<tr><td rowspan="4">Central Provisioning (Configuration File)</td><td><MAC>.cfg</td><td>Configure the method of transmitting DTMF digit and the payload type.
Parameters:
account.X.dtmf.type
account.X.dtmf.dtmf_payload
account.X.dtmf.info_type</td></tr>
<tr><td rowspan="3"><y0000000000xx>.cfg</td><td>Configure the number of times for the IP phone to send the end RTP Event packet.
Parameter:
features.dtmf.repetition</td></tr>
<tr><td>Configure the duration time for DTMF.
Parameter:
features.dtmf.duration</td></tr>
<tr><td>Configure the frequency level of DTMF digits.
Parameter:
features.dtmf.volume</td></tr>
<tr><td colspan="2" rowspan="2">Web User Interface</td><td>Configure the method of transmitting DTMF digits and the payload type.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0</td></tr>
<tr><td>Configure the number of times for the IP phone to send the end RTP Event packet.
Navigate to:
http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load</td></tr>
</table>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.dtmf.type	**0, 1, 2 or 3**	**1**
Description: Configures the DTMF type for account X. **0**-INBAND **1**-RFC 2833 **2**-SIP INFO **3**-RFC2833 + SIP INFO If it is set to 0 (INBAND), DTMF digits are transmitted in the voice band. If it is set to 1 (RFC 2833), DTMF digits are transmitted by RTP Events compliant to RFC 2833. If it is set to 2 (SIP INFO), DTMF digits are transmitted by the SIP INFO messages. If it is set to 3 (RFC2833 + SIP INFO), DTMF digits are transmitted by RTP Events compliant to RFC 2833 and the SIP INFO messages. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->DTMF Type **Phone User Interface:** None		
account.X.dtmf.dtmf_payload	**Integer from 96 to 127**	**101**
Description: Configures the value of DTMF payload for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note:** It works only if the value of parameter "account.X.dtmf.type" is set to 1 (RFC2833) or 3 (RFC2833 + SIP INFO). **Web User Interface:** Account->Advanced->DTMF Payload Type(96~127) **Phone User Interface:** None		
account.X.dtmf.info_type	**1, 2 or 3**	**1**
Description:		

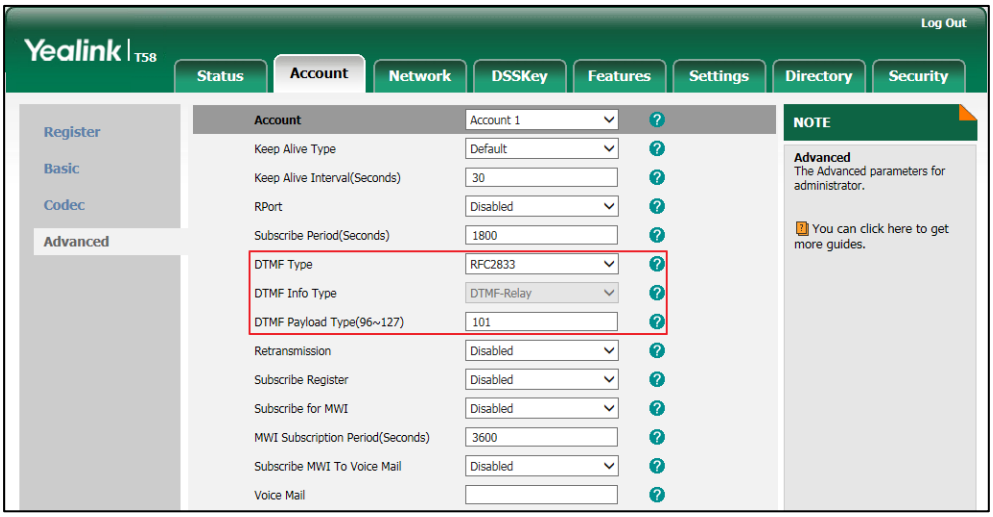
Parameters	Permitted Values	Default
Configures the DTMF info type. **1**-DTMF-Relay **2**-DTMF **3**-Telephone-Event X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Note:** It works only if the value of parameter "account.X.dtmf.type" is set to 2 (SIP INFO) or 3 (RFC2833 + SIP INFO). **Web User Interface:** Account->Advanced->DTMF Info Type **Phone User Interface:** None		
features.dtmf.repetition	**1, 2 or 3**	**3**
Description: Configures the repetition times for the IP phone to send the end RTP Event packet during an active call. **Web User Interface:** Features->General Information->DTMF Repetition **Phone User Interface:** None		
features.dtmf.duration	**Integer from 0 to 300**	**100**
Description: Configures the duration time (in milliseconds) for DTMF. **Note**: If the time interval to between two DTMF digits is less than this value, two or more same DTMF digits could be identified as one DTMF digit. This may cause the loss of one or more DTMF digits. For example, 2662 may be identified as 262. If so, you can modify the value of this parameter to a little lower than the default value. **Web User Interface:** None **Phone User Interface:** None		
features.dtmf.volume	**Integer from -33 to 0**	**-10**

Parameters	Permitted Values	Default
Description: Configures the frequency level of DTMF digits (in db). **Web User Interface:** None **Phone User Interface:** None		

To configure the method of transmitting DTMF digits via web user interface:

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

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

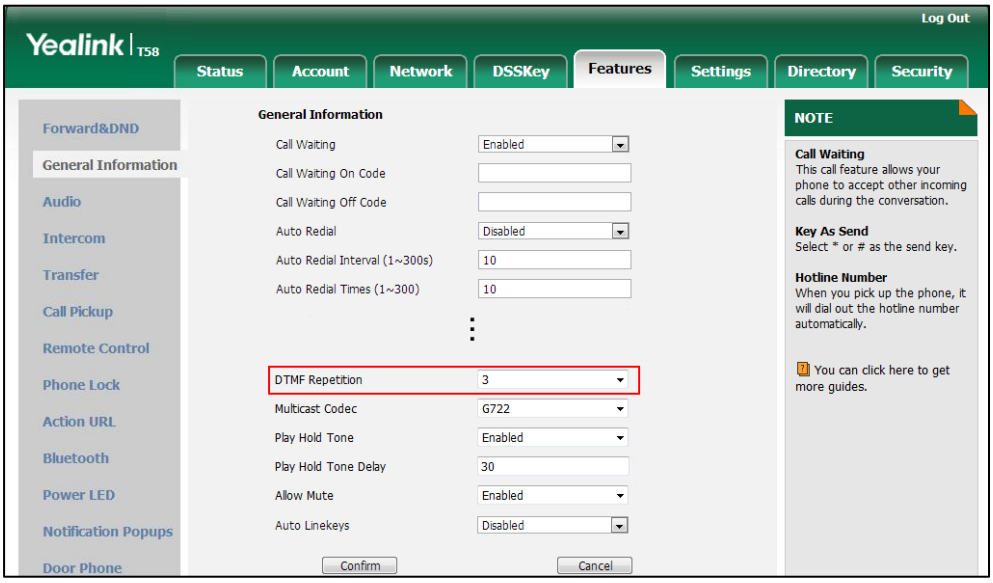


5. Click **Confirm** to accept the change.

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**.



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 touch 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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure suppress DTMF display and suppress DTMF display delay. **Parameters:** features.dtmf.hide features.dtmf.hide_delay
Web User Interface		Configure suppress DTMF display and suppress DTMF display delay. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

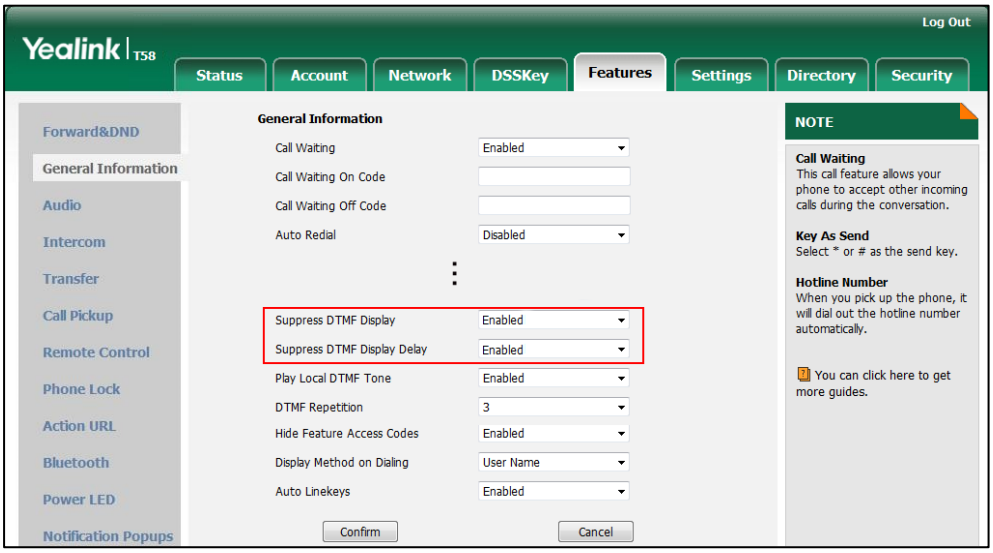
Details of Configuration Parameters:

Parameters	Permitted Values	Default
features.dtmf.hide	**0 or 1**	**0**
Description: Enables or disables the IP phone to suppress the display of DTMF digits during an active call. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the DTMF digits are displayed 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 digits for a short period before displaying asterisks during an active call. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "features.dtmf.hide" is set to 1 (Enabled). **Web User Interface:** Features->General Information->Suppress DTMF Display 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**.



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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure transfer via DTMF. **Parameters:** features.dtmf.replace_tran features.dtmf.transfer
Web User Interface		Configure transfer via DTMF. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

Details of Configuration Parameters:

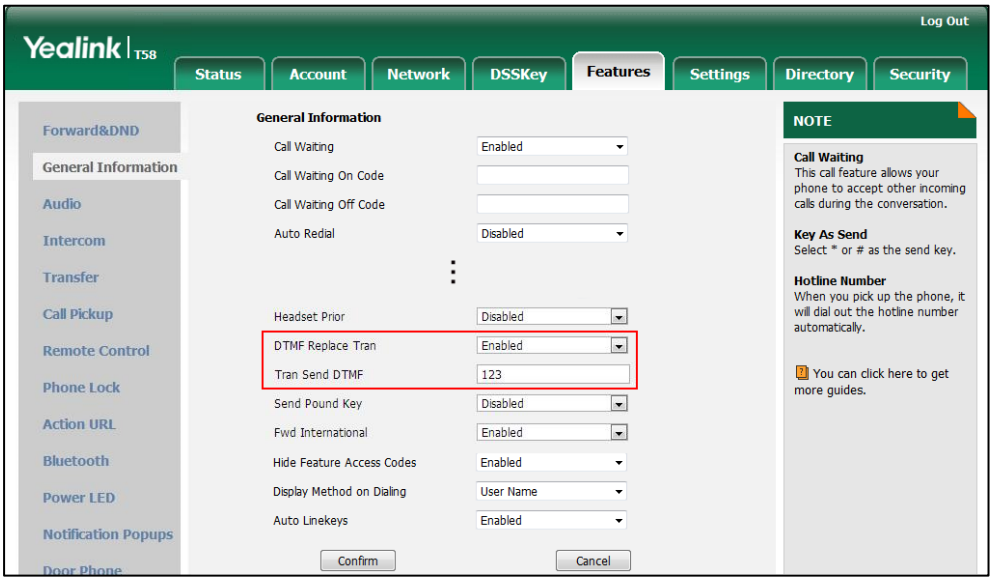
Parameters	Permitted Values	Default
features.dtmf.replace_tran	**0 or 1**	**0**
Description:		

Parameters	Permitted Values	Default
Enables or disables the IP phone to send DTMF sequences for transfer function when tapping the **Transfer** soft key or pressing TRANSFER/TRAN key. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone will perform the transfer as normal when tapping the **Transfer** soft key or pressing TRANSFER/TRAN key during a call. If it is set to 1 (Enabled), the IP phone will transmit the designated DTMF digits to the server for performing call transfer when tapping the **Transfer** soft key or pressing TRANSFER/TRAN key during a call. **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 call transfer. Valid values are: 0-9, *, # and A-D. **Example:** features.dtmf.transfer = 123 **Note:** It works only if the value of the parameter "features.dtmf.replace_tran" is set to 1 (Enabled). **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**.

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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure play local DTMF tone. **Parameter:** features.play_local_dtmf_tone_enable
Web User Interface		Configure play local DTMF tone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

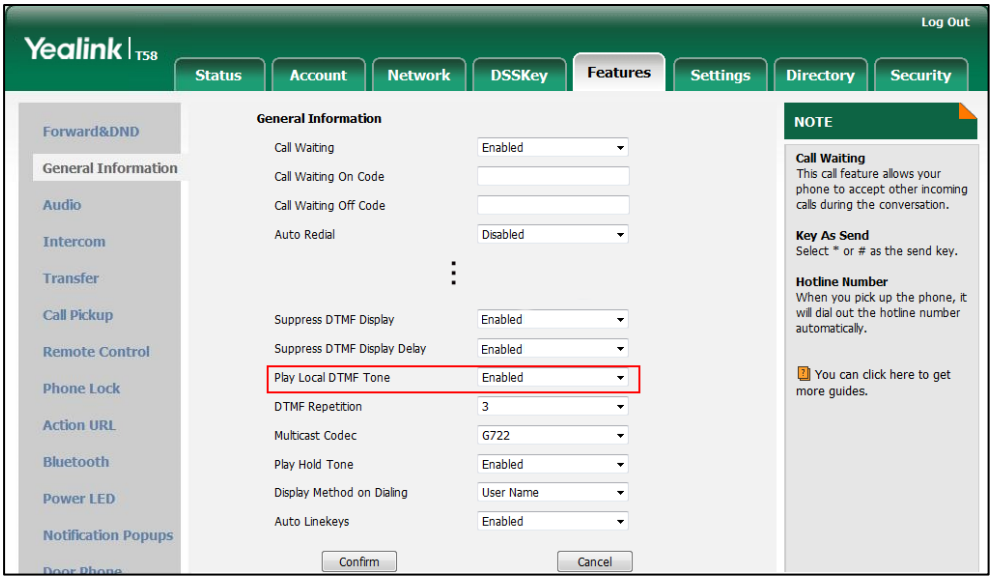
Details of Configuration Parameter:

Parameter	Permitted Values	Default
features.play_local_dtmf_tone_enable	**0 or 1**	**1**
Description:		

Parameter	Permitted Values	Default
Enables or disables the IP phone to play a local DTMF tone. **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**.



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

Voice Quality Monitoring (VQM)

Voice quality monitoring feature allows the IP phones to generate various quality metrics for listening quality and conversational quality. These metrics can be sent between the phones in RTCP-XR packets. These metrics can also be sent in SIP PUBLISH messages to a central voice quality report collector. Two mechanisms for voice quality monitoring are supported by Yealink IP phones:

- RTCP-XR
- VQ-RTCPXR

RTCP-XR

The RTCP-XR mechanism, compliant with RFC 3611-RTP Control Extended Reports (RTCP XR), provides the metrics contained in RTCP-XR packets for monitoring the quality of calls. These metrics include network packet loss, delay metrics, analog metrics and voice quality metrics.

Procedure

RTCP-XR can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure RTCP-XR. **Parameters:** voice.rtcp_xr.enable phone_setting.rtcp_xr_report.enable

Details of Configuration Parameters:

Parameters	Permitted Values	Default
voice.rtcp_xr.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to send RTCP-XR packets. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		
phone_setting.rtcp_xr_report.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to periodically (every 5 seconds) send RTCP-XR packets to another participating phone during a call for call quality monitoring and diagnosing. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "voice.rtcp_xr.enable" is set to 1 (Enabled). If you change this parameter, the IP phone will reboot to make the change take effect.		

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

VQ-RTCPXR

The VQ-RTCPXR mechanism, compliant with RFC 6035, sends the service quality metric reports contained in SIP PUBLISH messages to the central report collector. Three types of quality reports can be enabled:

- **Session**: Generated at the end of a call.
- **Interval**: Generated during a call at a configurable period.
- **Alert**: Generated when the call quality degrades below a configurable threshold.

A wide range of performance metrics are generated in the following three ways:

- Based on current values, such as jitter, jitter buffer max and round trip delay.
- Covers the time period from the beginning of the call until the report is sent, such as network packet loss.
- Computed using other metrics as input, such as listening Mean Opinion Score (MOS-LQ) and conversational Mean Opinion Score (MOS-CQ).

To operate with central report collector, IP phones must be configured to forward their voice quality reports to the specified report collector. You can specify the report collector on a per-line basis.

Users can check the voice quality data of the last call via web user interface or phone user interface. Users can also specify the options of the RTP status to be displayed on the phone user interface. Options of the RTP status to be displayed on the web user interface cannot be specified.

Procedure

VQ-RTCPXR can be configured using the following methods.

Central Provisioning (Configuration	<y0000000000xx>.cfg	Configure the generation of session packets. **Parameter:** phone_setting.vq_rtcpxr.session_report.enable

File)		Configure the generation of interval packets. **Parameters:** phone_setting.vq_rtcpxr.interval_report.enable phone_setting.vq_rtcpxr_interval_period
		Configure the generation of alert packets. **Parameters:** phone_setting.vq_rtcpxr_moslq_threshold_warning phone_setting.vq_rtcpxr_moslq_threshold_critical phone_setting.vq_rtcpxr_delay_threshold_warning phone_setting.vq_rtcpxr_delay_threshold_critical
		Configure the phone to display RTP status showing the voice quality report of the last call on the web user interface. **Parameter:** phone_setting.vq_rtcpxr.states_show_on_web.enable
		Configure the phone to display RTP status showing the voice quality report of the last call or the current call on the phone user interface. **Parameter:** phone_setting.vq_rtcpxr.states_show_on_gui.enable

		Configure the options of the RTP status displayed on the phone user interface. **Parameters:** phone_setting.vq_rtcpxr_display_start_time.enable phone_setting.vq_rtcpxr_display_stop_time.enable phone_setting.vq_rtcpxr_display_local_call_id.enable phone_setting.vq_rtcpxr_display_remote_call_id.enable phone_setting.vq_rtcpxr_display_local_codec.enable phone_setting.vq_rtcpxr_display_remote_codec.enable phone_setting.vq_rtcpxr_display_jitter.enable phone_setting.vq_rtcpxr_display_jitter_buffer_max.enable phone_setting.vq_rtcpxr_display_packets_lost.enable phone_setting.vq_rtcpxr_display_symm_oneway_delay.enable phone_setting.vq_rtcpxr_display_round_trip_delay.enable phone_setting.vq_rtcpxr_display_moslq.enable phone_setting.vq_rtcpxr_display_moscq.enable
	<MAC>.cfg	Configure the central report collector. **Parameters:** account.X.vq_rtcpxr.collector_name account.X.vq_rtcpxr.collector_server_host account.X.vq_rtcpxr.collector_server_port
Web User Interface		Configure VQ-RTCPXR. Configure the phone to display RTP status showing the voice quality report of the last call on the web user interface. Configure the phone to display RTP status showing the voice quality report of the last call or the current call on the phone user interface. Configure the options of the RTP status

	displayed on the phone user interface. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-voicemonitoring&q=load
	Configure the central report collector. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.vq_rtcpxr.session_report.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to send a session quality report to the central report collector at the end of each call. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Voice Monitoring->VQ RTCP-XR Session Report **Phone User Interface:** None		
phone_setting.vq_rtcpxr.interval_report.enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to send an interval quality report to the central report collector periodically throughout a call. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Voice Monitoring->VQ RTCP-XR Interval Report **Phone User Interface:** None		
phone_setting.vq_rtcpxr_interval_period	**Integer from 5 to 20**	**20**
Description:		

Parameters	Permitted Values	Default
Configures the interval (in seconds) for the IP phone to send an interval quality report to the central report collector periodically throughout a call. **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.interval_report.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Period for Interval Report **Phone User Interface:** None		
phone_setting.vq_rtcpxr_moslq_threshold_warning	**15 to 40**	**Blank**
Description: Configures the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a warning alert quality report to the central report collector. For example, a configured value of 35 corresponds to the MOS score 3.5. When the MOS-LQ value computed by the phone is less than or equal to 3.5, the phone will send a warning alert quality report to the central report collector. When the MOS-LQ value computed by the phone is greater than 3.5, the phone will not send a warning alert quality report to the central report collector. If it is set to blank, warning alerts are not generated due to MOS-LQ. **Web User Interface:** Settings->Voice Monitoring->Warning threshold for Moslq **Phone User Interface:** None		
phone_setting.vq_rtcpxr_moslq_threshold_critical	**15 to 40**	**Blank**
Description: Configures the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a critical alert quality report to the central report collector. For example, a configured value of 28 corresponds to the MOS score 2.8. When the MOS-LQ value computed by the phone is less than or equal to 2.8, the phone will send a critical alert quality report to the central report collector. When the MOS-LQ value computed by the phone is greater than 2.8, the phone will not send a critical alert quality report to the central report collector. If it is set to blank, critical alerts are not generated due to MOS-LQ. **Web User Interface:**		

Parameters	Permitted Values	Default
Settings->Voice Monitoring->Critical threshold for Moslq **Phone User Interface:** None		
phone_setting.vq_rtcpxr_delay_threshold_warning	**10 to 2000**	**Blank**
Description: Configures the threshold value of one way delay (in milliseconds) that causes the phone to send a warning alert quality report to the central report collector. For example, If it is set to 500, when the value of one way delay computed by the phone is greater than or equal to 500, the phone will send a warning alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a warning alert quality report to the central report collector. If it is set to blank, warning alerts are not generated due to one way delay. One-way delay includes both network delay and end system delay. **Web User Interface:** Settings->Voice Monitoring->Warning threshold for Delay **Phone User Interface:** None		
phone_setting.vq_rtcpxr_delay_threshold_critical	**10 to 2000**	**Blank**
Description: Configures the threshold value of one way delay (in milliseconds) that causes phone to send a critical alert quality report to the central report collector. For example, If it is set to 500, when the value of one way delay computed by the phone is greater than or equal to 500, the phone will send a critical alert quality report to the central report collector; when the value of one way delay computed by the phone is less than 500, the phone will not send a critical alert quality report to the central report collector. If it is set to blank, critical alerts are not generated due to one way delay. One-way delay includes both network delay and end system delay. **Web User Interface:** Settings->Voice Monitoring->Critical threshold for Delay **Phone User Interface:** None		
phone_setting.vq_rtcpxr.states_show_on_web.enable	**0 or 1**	**0**

Parameters	Permitted Values	Default
Description: Enables or disables the voice quality data of the last call to be displayed on web interface at the path **Status**->**RTP Status**. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Voice Monitoring->Display Report options on Web **Phone User Interface:** None		
phone_setting.vq_rtcpxr.states_show_on_gui.enable	**0 or 1**	**0**
Description: Enables or disables the voice quality data of the last call or current call to be displayed on the touch screen. You can view the voice quality data of the last call on the phone at the path **Settings**->**Status**->**RTP Status**. You can view the voice quality data of the current call by tapping the **RTP Status** soft key during a call. **0**-Disabled **1**-Enabled **Web User Interface:** Settings->Voice Monitoring->Display Report options on phone **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_start_time.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Start Time on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->Start Time **Phone User Interface:** None		

Parameters	Permitted Values	Default
phone_setting.vq_rtcpxr_display_stop_time.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Current Time or Stop Time on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->Current Time **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_local_call_id.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Local User on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->Local User **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_remote_call_id.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Remote User on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->Remote User **Phone User Interface:**		

Parameters	Permitted Values	Default
None		
phone_setting.vq_rtcpxr_display_local_codec.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Local Codec on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->Local Codec **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_remote_codec.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Remote Codec on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->Remote Codec **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_jitter.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Jitter on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->Jitter		

Parameters	Permitted Values	Default
Phone User Interface: None		
phone_setting.vq_rtcpxr_display_jitter_buffer_max.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display JitteBufferMax on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->JitteBufferMax **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_packets_lost.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display Packets Lost on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->Packets Lost **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_symm_oneway_delay.enable	**0 or 1**	**0**
Description: Enables or disables the phone to display SymmOneWayDelay on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled).		

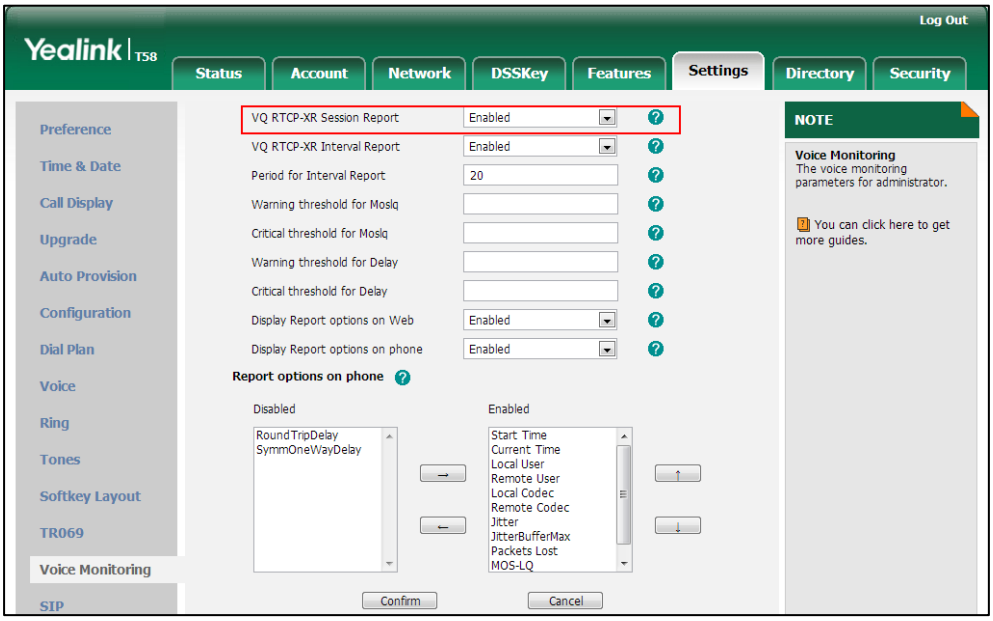
Parameters	Permitted Values	Default
Web User Interface: Settings->Voice Monitoring->Report options on phone->SymmOneWayDelay **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_round_trip_delay.enable	**0 or 1**	**0**
Description: Enables or disables the phone to display RoundTripDelay on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->RoundTripDelay **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_moslq.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display MOS-LQ on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter "phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->MOS-LQ **Phone User Interface:** None		
phone_setting.vq_rtcpxr_display_moscq.enable	**0 or 1**	**1**
Description: Enables or disables the phone to display MOS-CQ on the touch screen. **0**-Disabled **1**-Enabled **Note:** It works only if the value of the parameter		

Parameters	Permitted Values	Default
"phone_setting.vq_rtcpxr.states_show_on_gui.enable" is set to 1 (Enabled). **Web User Interface:** Settings->Voice Monitoring->Report options on phone->MOS-CQ **Phone User Interface:** None		
account.X.vq_rtcpxr.collector_name	**String within 32 characters**	**Blank**
Description: Configures the host name of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->VQ RTCP-XR Collector name **Phone User Interface:** None		
account.X.vq_rtcpxr.collector_server_host	**IPv4 Address**	**Blank**
Description: Configures the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->VQ RTCP-XR Collector address **Phone User Interface:** None		
account.X.vq_rtcpxr.collector_server_port	**Integer from 1 to 65535**	**5060**
Description: Configures the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X.		

Parameters	Permitted Values	Default
X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->VQ RTCP-XR Collector port **Phone User Interface:** None		

To configure session report for VQ-RTCPXR via web user interface:

1. Click on **Settings**->**Voice Monitoring**.
2. Select the desired value from the pull-down list of **VQ RTCP-XR Session Report.**

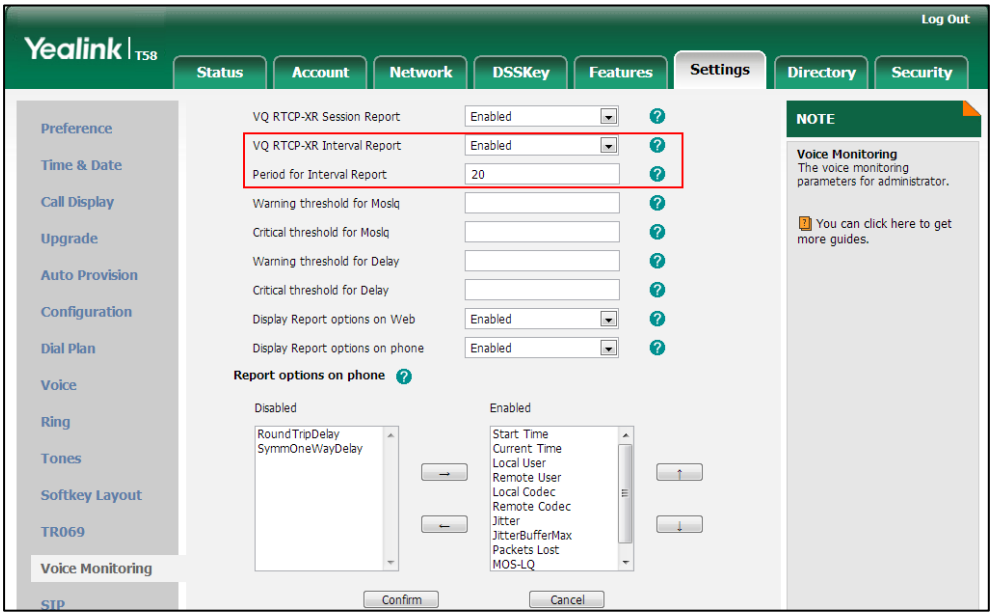


3. Click **Confirm** to accept the change.

To configure interval report for VQ-RTCPXR via web user interface:

1. Click on **Settings**->**Voice Monitoring**.
2. Select the desired value from the pull-down list of **VQ RTCP-XR Interval Report**.

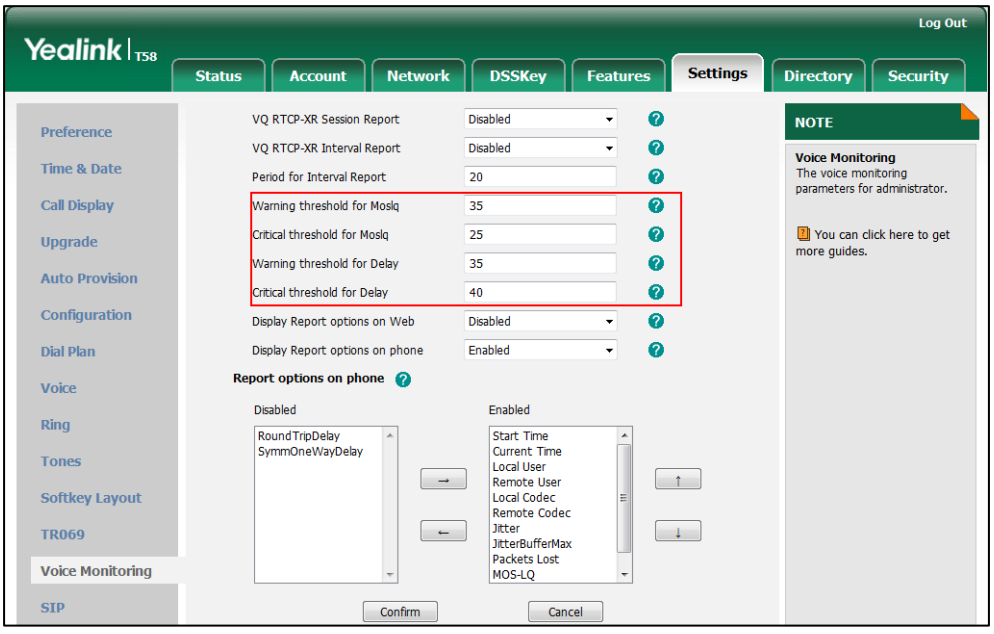
3. Enter the desired value in the **Period for Interval Report** field.



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

To configure alert report for VQ-RTCPXR via web user interface:

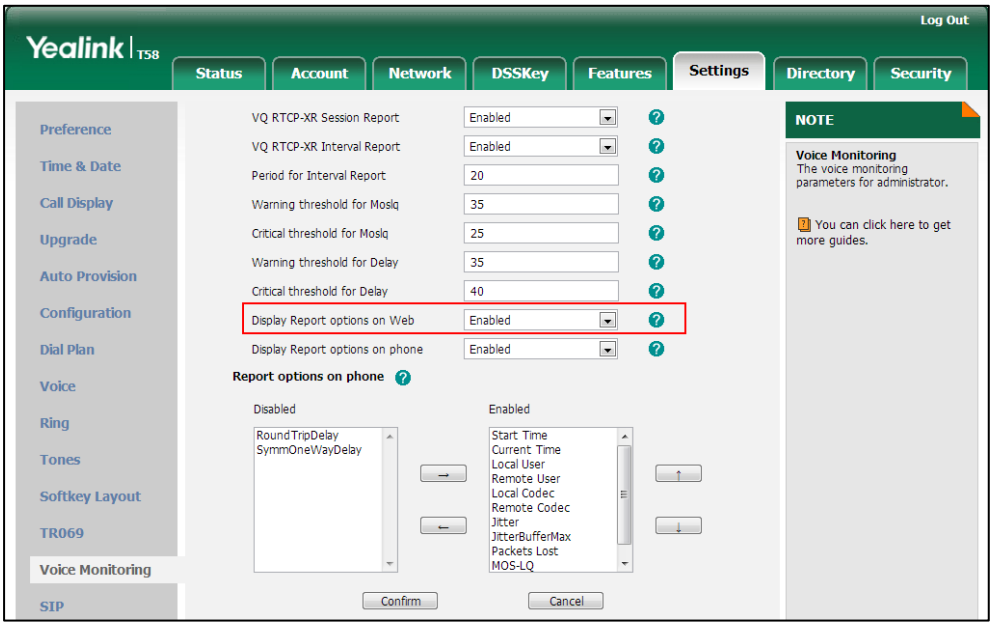
1. Click on **Settings**->**Voice Monitoring**.
2. Enter the desired value in the **Warning threshold for Moslq** field.
3. Enter the desired value in the **Critical threshold for Moslq** field.
4. Enter the desired value in the **Warning threshold for Delay** field.
5. Enter the desired value in the **Critical threshold for Delay** field.



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

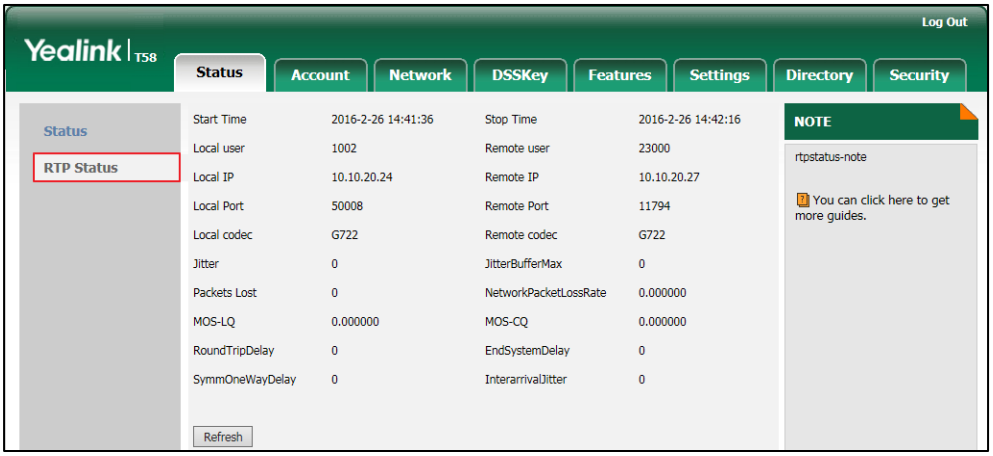
To configure RTP status displayed on the web page via web user interface:

1. Click on **Settings**->**Voice Monitoring**.
2. Select the desired value from the pull-down list of **Display Report options on Web**.



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

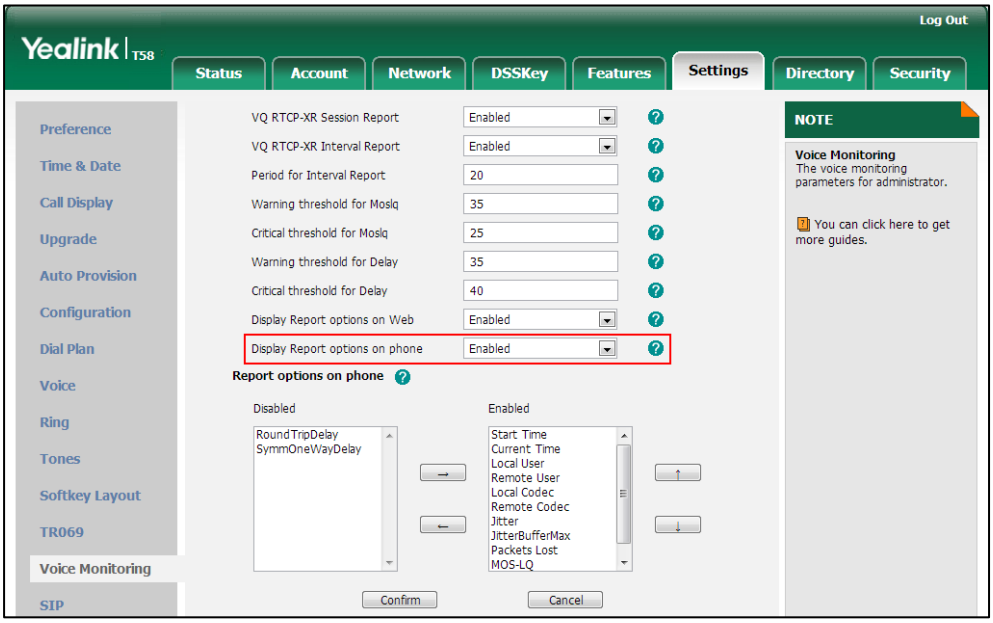
   The RTP status will appear on the web user interface at the path: **Status->RTP Status**.



To configure RTP status displayed on the touch screen via web user interface:

1. Click on **Settings**->**Voice Monitoring**.

2. Select the desired value from the pull-down list of **Display Report options on phone**.



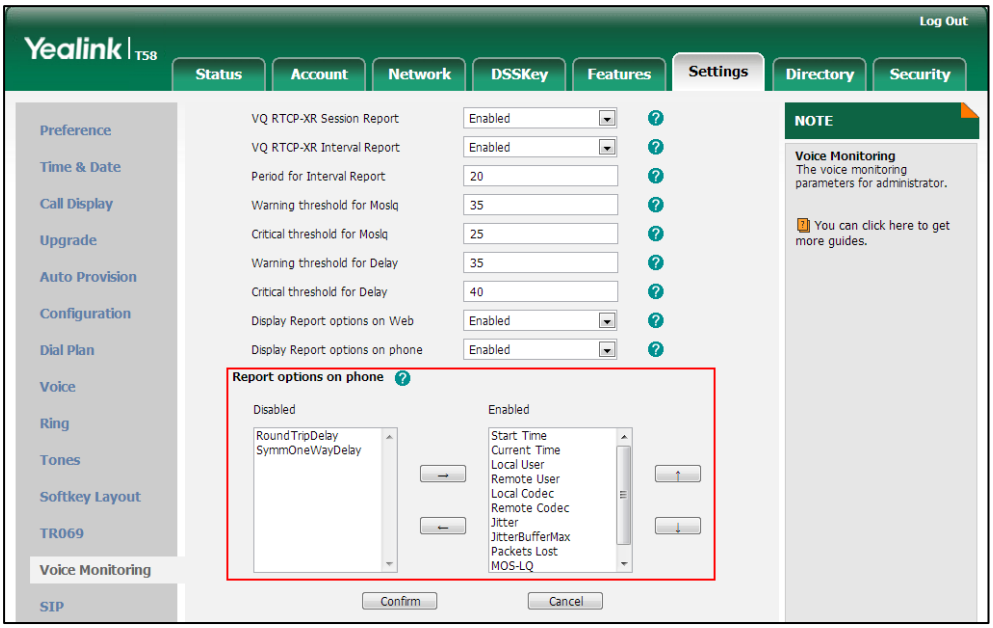
3. Click **Confirm** to accept the change.

The RTP status will appear on the phone user interface at the path: **Settings**->**Status**->**RTP Status**.

To configure the options of the RTP status displayed on the touch screen via web user interface:

1. Click on **Settings**->**Voice Monitoring**.
2. In the **Report options on phone** block**,** select the desired list from the **Disabled** column and then click → .

   The selected list appears in the **Enabled** column.

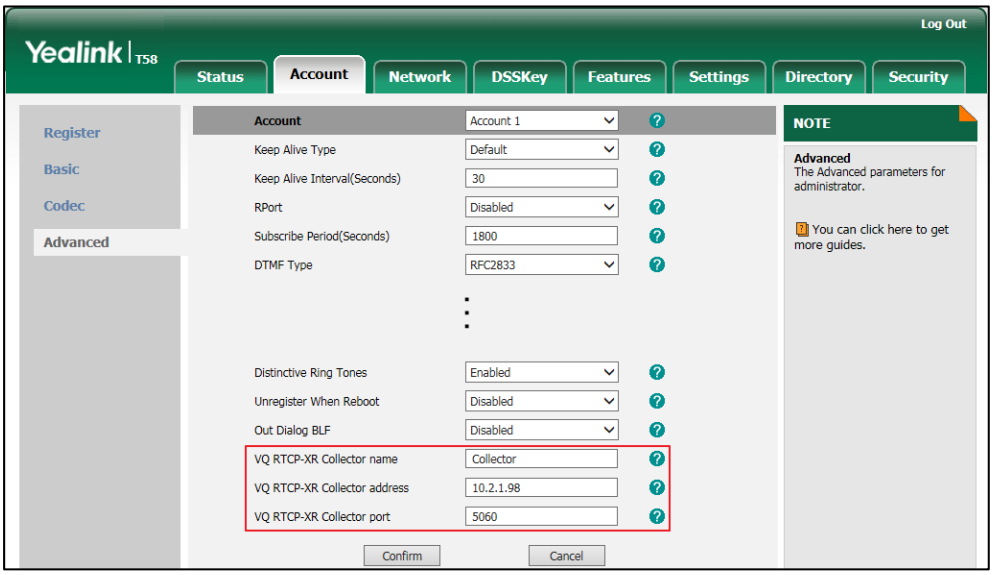


3. Repeat the step 2 to add more items to the **Enabled** column.
4. To remove an item from the **Enabled** column, select the desired item and then click .
5. To adjust the display order of enabled items, select the desired item and then click or .

   The touch screen will display the item(s) in the adjusted order.
6. Click **Confirm** to accept the change.

To configure the central report collector via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Enter the host name of the central report collector in the **VQ RTCP-XR Collector name** field.
4. Enter the IP address of the central report collector in the **VQ RTCP-XR Collector address** field.
5. Enter the port of the central report collector in the **VQ RTCP-XR Collector port** field.



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

Configuring Video Features

The SIP-T58V/A IP phones support transmission and reception of high quality video images. The video is compatible with RFC 3984 - RTP Payload Format for H.264 Video, RFC 7741 - on RTP Payload Format for VP8 Video.
This section provides information for making configuration changes for the following video-related features:

- Video Settings
- Video Codecs

Video Settings

The SIP-T58V/A IP phones support using USB camera for point-to-point video calls. Users can place and answer video calls. The IP phones support transmission and reception of high quality video images. You can configure camera flicker to optimize video calling. Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source the light is powered by.

Toggle Between Audio-only or Video Calls

The video call feature is enabled by default. You can disable this feature as required. When you disable the video call feature, the calls are audio-only.

Procedure

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

Configuration File	<y0000000000xx>.cfg	Configure the video settings. **Parameters:** video.enable camera.flicker
Local	Web User Interface	Configure the video settings. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-camera&q=load

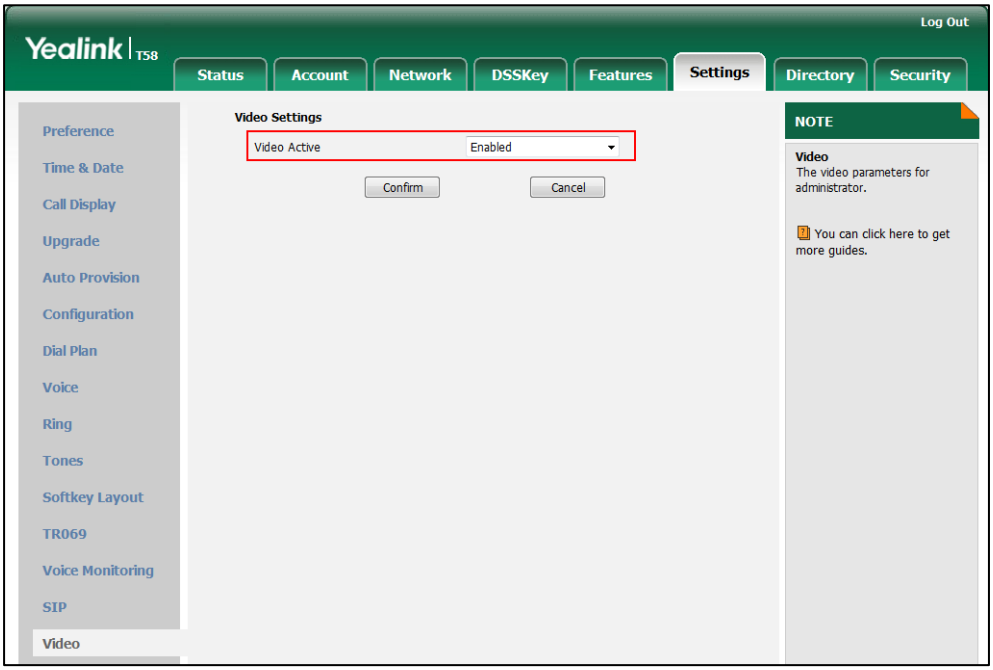
Details of the Configuration Parameters:

Parameters	Permitted Values	Default
video.enable	**0 or 1**	**1**
Description: Enables or disables the video call feature for the IP phone. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), video is not sent in outgoing calls and not received in incoming calls. All calls are audio-only. If it is set to 1 (Enabled), video is sent in outgoing calls and received in incoming calls. **Note**: It is not applicable to SIP-T56A/CP960 IP phones. **Web User Interface:** Settings->Video->Video Active **Phone User Interface:** None		
camera.flicker	**50 or 60**	**50**
Description: Configures the value of camera flicker frequency (Hz). **50**-50Hz **60**-60Hz **Note**: Indoor lights powered by a 50Hz or 60Hz power source can produce a flicker. You can adjust the camera flicker frequency according to the power source the light is powered by. It is not applicable to SIP-T56A/CP960 IP phones. **Web User Interface:** None **Phone User Interface:** None		

To active the call video feature and configure the auto video feature via web user interface:

1. Click on **Settings**->**Video**.

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



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

Video Codecs

CODEC is an abbreviation of COmTap-DEComTap, 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 video signal with minimum number of bits while retaining the quality. This can effectively reduce the frame size and the bandwidth required for video transmission.

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

RTPmap

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.

The following table lists the video codecs supported by SIP-T58V/A phone model:

Name	MIME Type	Bit Rate	Frame Rate	Frame Size
H.264 BP	H264/90000	90 kbps to 2048 kbps	5 fps to 30 fps	Tx: CIF, 360P, W448P, 720P Rx: Conventional Size Below 720P
H.264 HP	H264/90000			
VP8	VP8/90000	128kbps to 2048 kbps		

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure the video codecs to use on a per-line basis. **Parameter:** account.X.video.<payload_type>.enable
		Configure the priority and rtpmap for the enabled video codec. **Parameter:** account.X.video.<payload_type>.priority
Web User Interface		Configure the video codecs to use on a per-line basis. Configure the priority for the enabled video codec. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=account-codec&q=load&acc=0

Details of Configuration Parameters:

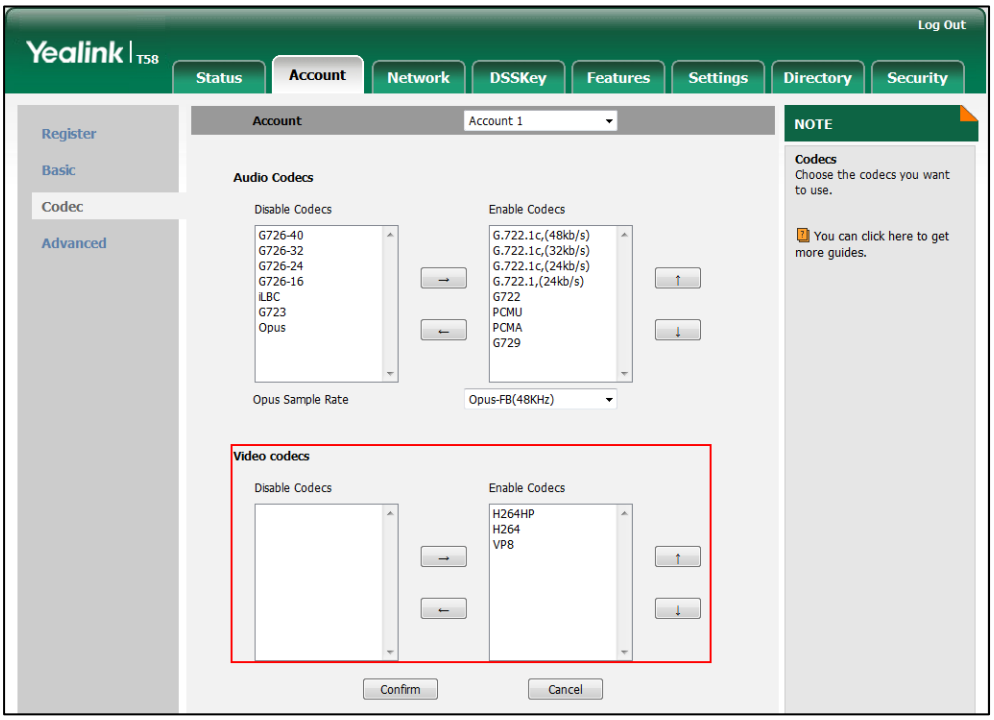
Parameters	Permitted Values	Default
account.X.video.<payload_type>.enable (where <payload_type> should be replaced by the name of video codec)	**0 or 1**	**1**
Description: Enables or disables the specified video codec for account X. **0**-Disabled **1**-Enabled X ranges from 1 to 16 **Valid Video Codec**: H264, H264HP, VP8 **Default:** When video codec is H264, the default value is 1; When video codec is H264HP, the default value is 1; When video codec is VP8, the default value is 1; **Example:**		

Parameters	Permitted Values	Default
account.1.video.h264.enable = 1 account.1.video.h264hp.enable = 1 account.1.video.vp8.enable = 1 It means that the codecs H264, H264HP, VP8 are enabled on the account 1. **Note:** The name of video codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect. It is not applicable to SIP-T56A/CP960 IP phones. **Web User Interface:** Account->Codec->Video Codec **Phone User Interface:** None		
account.X.video.<payload_type>.priority (where <payload_type> should be replaced by the name of video codec)	**1, 2 or 3**	**Refer to the following content**
Description: Configures the priority of the enabled video codec for account X. X ranges from 1 to 16 **Valid Video Codec**: H264, H264HP, VP8 **Default:** When video codec is H264, the default value is 2; When video codec is H264HP, the default value is 1; When video codec is VP8, the default value is 3; **Example:** account.1.video.h264.priority = 2 account.1.video.h264hp.priority = 1 account.1.video.vp8.priority = 3 **Note:** The name of video codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect. It is not applicable to SIP-T56A/CP960 IP phones. **Web User Interface:** Account->Codec->Video Codec **Phone User Interface:** None		

To configure the video codecs and adjust the priority of the enabled video codecs on a per-account basis via web user interface:

1. Click on **Account**->**Codec**.
2. Select the desired account from the pull-down list of **Account**.
3. In the **Video Codecs** field, select the desired codec from the **Disable Codecs** column and then click → .

   The selected codec appears in the **Enable Codecs** column.
4. Repeat the step 3 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 ← .
6. To adjust the priority of codecs, select the desired codec and then click ↑ or ↓ .



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

Configuring Security Features

This chapter provides information for making configuration changes for the following security-related features:

- User and Administrator Passwords
- Auto-Logout Time
- Phone Lock
- Transport Layer Security (TLS)
- Secure Real-Time Transport Protocol (SRTP)
- Encrypting and Decrypting Files

User and Administrator Passwords

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. The default user password is "user" and the default administrator password is "admin".

For security reasons, the user or administrator should change the default user or administrator password as soon as possible. A user or an administrator can change the user password. The administrator password can only be changed by an administrator.

Advanced menu options are strictly used by administrators. Users can configure them only if they have administrator privileges.

Procedure

User or administrator password can be changed using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Change the user or administrator password of the IP phone. **Parameter:** static.security.user_password
Web User Interface		Change the user or administrator password of the IP phone. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=security&q=load
Phone User Interface		Change the administrator password of the IP phone.

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
static.security.user_password	**String within 32 characters**	**user**

Description:

Configures the password of the user or administrator for phone's web user interface access.

The IP phone uses "user" as the default user password and "admin" as the default administrator password.

The valid value format is username:new password.

Example:

static.security.user_password = user:123 means setting the password of user (current user name is "user") to password 123.

static.security.user_password = admin:456 means setting the password of administrator (current user name is "admin") to password 456.

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:

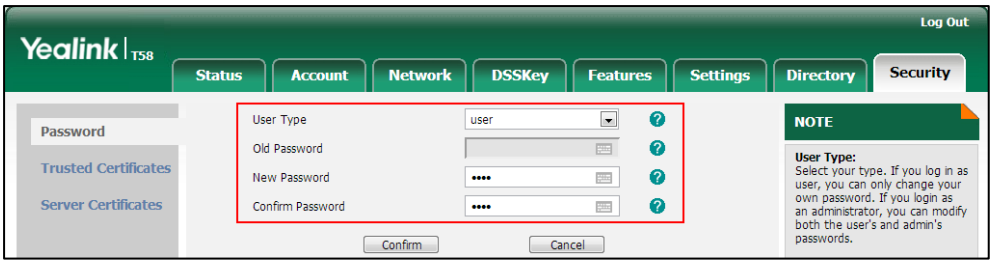
Settings->Advanced (default password: admin) ->Set Password

Note: You cannot change the user password via phone user interface.

To change the user or administrator password via web user interface:

1. Click on **Security**->**Password**.
2. Select the desired value (**user** or **admin**) 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).



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

Note If logging into the web user interface of the phone with the user credential, you need to enter the old user password in the **Old Password** field.

To change the administrator password via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Set Password**.
2. Enter the current administrator password in the **Current PWD** field.
3. Enter new password in the **New PWD** field and **Confirm PWD** field.
   Valid characters are ASCII characters 32-126(0x20-0x7E).
4. Tap ✔ 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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure auto-logout time. **Parameter**: features.relog_offtime
Web User Interface		Configure auto-logout time. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load

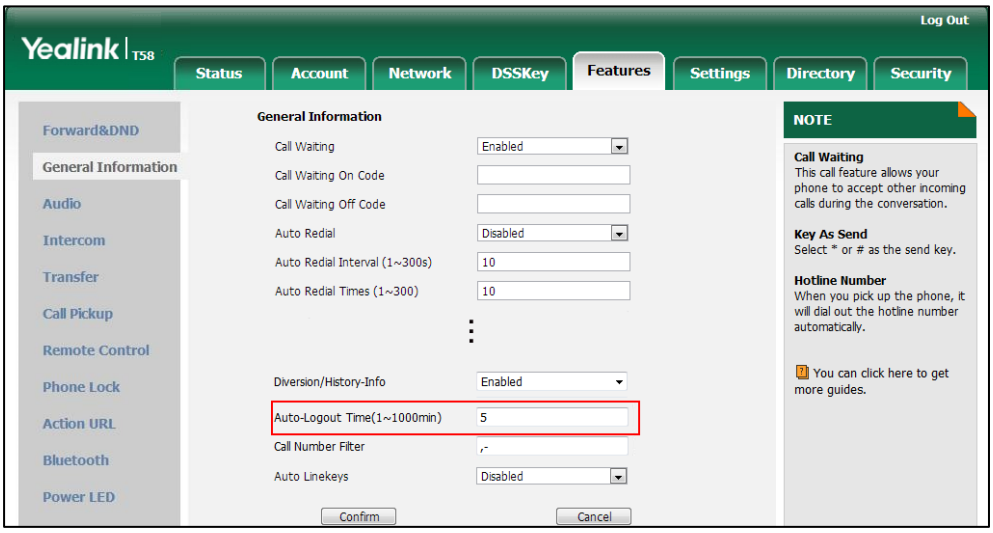
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
features.relog_offtime	**Integer from 1 to 1000**	**5**
Description: Configures the timeout interval (in minutes) for web access authentication. **Example**: features.relog_offtime = 5 If you log into the web user interface and leave it for 5 minutes, it will automatically log out. **Web User Interface:** Features->General Information->Auto-Logout Time(1~1000min) **Phone User Interface:**		

Parameter	Permitted Values	Default
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.



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

Phone Lock

Phone lock is used to lock the IP phone to prevent it from unauthorized use. Once the IP phone is locked, the user must enter the password to unlock it. The IP phone will not be locked immediately after the phone lock feature is enabled. One of the following steps is also needed:

- Long press the pound key when the IP phone is idle (not applicable to CP960 IP phones).
- Press the phone lock key (if configured) when the IP phone is idle.

In addition to the above steps, you can configure the IP phone to automatically lock the phone after a period of time.

Procedure

Phone lock can be configured using the configuration files or locally.

Configuration File	<y0000000000xx>.cfg	Configure the phone lock feature. **Parameters:** phone_setting.phone_lock.enable
		Change the unlock PIN. **Parameter:** phone_setting.phone_lock.unlock_pin
		Configure the IP phone to automatically lock the phone after a time interval. **Parameter:** phone_setting.phone_lock.lock_time_out
		Configure emergency numbers. **Parameter:** phone_setting.emergency.number
		Assign a phone lock key. **Parameters:** linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type linekey.X.label/ expansion_module.X.key.Y.label
Local	Web User Interface	Configure the phone lock feature. Change the unlock PIN. Configure the IP phone to automatically lock the phone after a time interval. Configure emergency numbers. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=features-phonelock&q=load
		Assign a phone lock key. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&model=2&q=load
	Phone User Interface	Configure the phone lock feature. Change the unlock PIN. Configure the IP phone to automatically lock

		the phone after a time interval. Assign a phone lock key.

Details of Configuration Parameters:

Parameters	Permitted Values	Default
phone_setting.phone_lock.enable	**0 or 1**	**0**
Description: Enables or disables the phone lock feature. **0**-Disabled **1**-Enabled **Web User Interface:** Features->Phone Lock->Phone Lock Enable **Phone User Interface:** Settings->Advanced (default password: admin) ->Phone Lock->Lock Enable		
phone_setting.phone_lock.unlock_pin	**Characters within 15 digits**	**123**
Description: Configures the password for unlocking the phone. **Web User Interface:** Features->Phone Lock->Phone Unlock PIN(0~15 Digit) **Phone User Interface:** Settings->Basic->Change PIN		
phone_setting.phone_lock.lock_time_out	**Integer from 0 to 3600**	**0**
Description: Configures the interval (in seconds) to automatically lock the phone. The default value is 0 (the phone is locked only by long pressing the pound key or pressing the phone lock key). **Note**: It works only if the value of the parameter "phone_setting.phone_lock.enable" is set to 1(Enabled). Pound key is not applicable to CP960 IP phones. **Web User Interface:** Features->Phone Lock->Phone Lock Time Out(0~3600s) **Phone User Interface:** Settings->Advanced (default password: admin) ->Phone Lock->Lock Time Out		

Parameters	Permitted Values	Default
phone_setting.emergency.number	**String within 99 characters**	**112,911,110**
Description: Configures emergency numbers. Multiple emergency numbers are separated by commas. If the value of the parameter "phone_setting.phone_lock.enable" is set to 1 (Enabled), you can only allow to dial emergency numbers configured by "phone_setting.emergency.number". **Web User Interface:** Features->Phone Lock->Emergency **Phone User Interface:** None		

Phone Lock Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 775.

Details of Configuration Parameters:

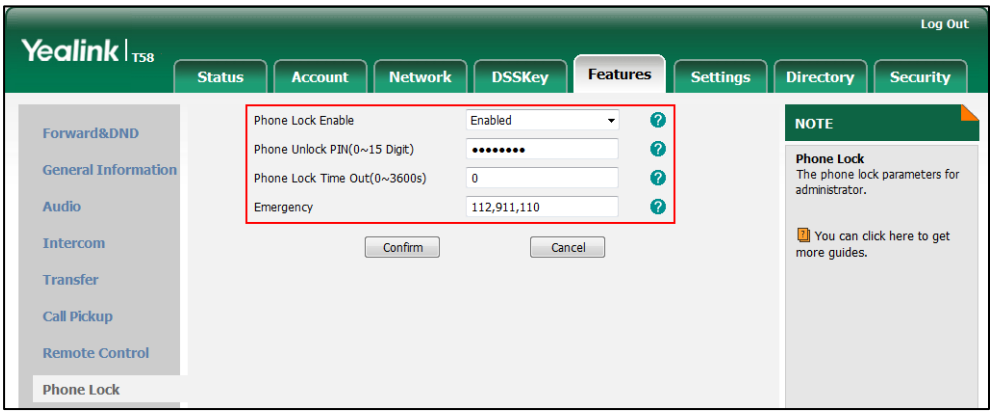
Parameters	Permitted Values	Default
linekey.X.type/ programablekey.X.type/ expansion_module.X.key.Y.type	**50**	**Refer to the following content**
Description: Configures a DSS key as a phone lock key on the IP phone. The digit **50** stands for the key type **Phone Lock.** For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For programable keys: X ranges from 12 to 14 (for SIP-T58V/T58A/T56A) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Example:** linekey.1.type = 50		

Parameters	Permitted Values	Default
Default: For line keys: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. For programable keys: **For SIP-T58V/T58A/T56A IP phones:** When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). For ext keys: **For SIP-T58V/T58A/T56A IP phones:** When Y= 1 to 60, the default value is 0 (NA). **Web User Interface:** DSSKey->Line Key/ Programable Key->Type **Phone User Interface:** Settings->Features->DSS Keys->Line Keys X->Type		
linekey.X.label/ expansion_module.X.key.Y.label	**String within 99 characters**	**Blank**
Description: (Optional.) Configures the label displayed on the LCD screen for each DSS key. For line keys: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X ranges from 1 to 30 (for CP960) For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A) **Web User Interface:** DSSKey->Line Key->Label **Phone User Interface:** Settings->Features->DSS Keys->Line Key X->Label		

To configure phone lock via web user interface:

1. Click on **Features**->**Phone Lock**.
2. Select the desired value from the pull-down list of **Phone Lock Enable**.

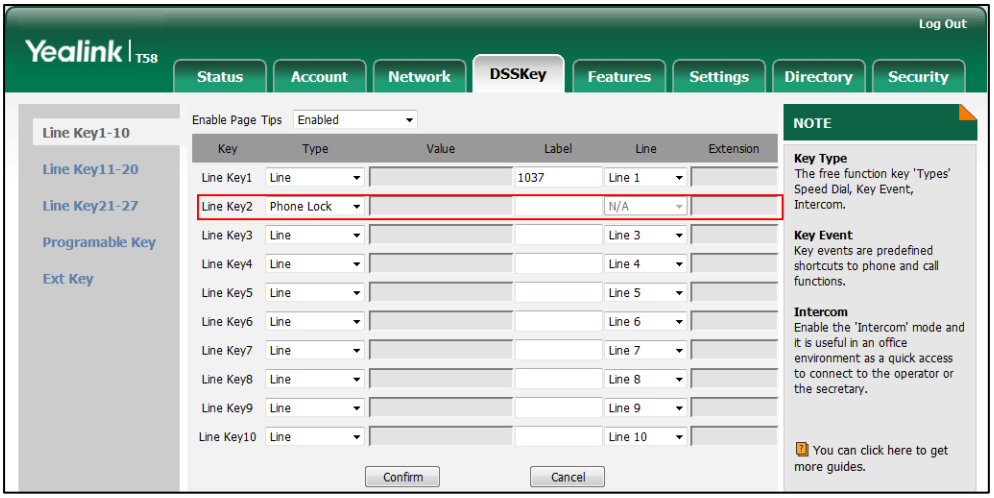
3. Enter the unlock PIN in the **Phone Unlock PIN(0~15 Digit)** field.
4. Enter the desired time in the **Phone Lock Time Out(0~3600s)** field.



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

To configure a phone lock key via web user interface:

1. Click on **DSSKey**->**Line Key** (or **Programable Key**/**Ext Key**).
2. In the desired DSS key field, select **Phone Lock** from the pull-down list of **Type**.
3. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.



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

To configure the type of phone lock via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Phone Lock**.
2. Tap the **Lock Enable** field.
3. Tap **Enabled** in the pop-up dialog box to enable this feature.
4. Enter the desired interval of automatic phone lock in the **Lock Time Out** field.
5. Tap ✓ to accept the change.

To change the unlock PIN via phone user interface:

1. Tap **Settings**->**Basic Settings**->**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. Tap ✓ to accept the change.

To configure a phone lock key via phone user interface:

1. Tap **Settings**->**Features**->**DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **Key Event** in the pop-up dialog box.
5. Tap the **Key Type** field.
6. Tap **Phone Lock** in the pop-up dialog box.
7. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
8. Tap ✓ to accept the change.

Transport Layer Security (TLS)

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.

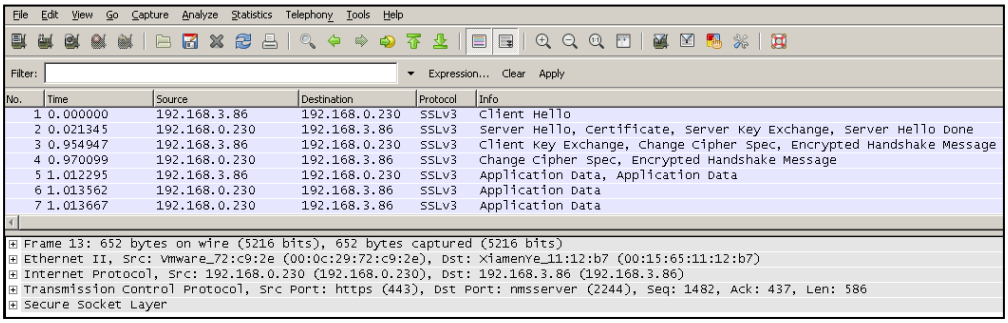
The TLS protocol uses asymmetric encryption for authentication of key exchange, symmetric encryption for confidentiality, and message authentication codes for integrity.

- **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
- DES-CBC3-MD5
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- RC2-CBC-MD5
- IDEA-CBC-SHA
- DHE-DSS-RC4-SHA
- RC4-SHA
- RC4-MD5
- RC4-64-MD5
- EXP1024-DHE-DSS-DES-CBC-SHA
- EXP1024-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
- EXP1024-DHE-DSS-RC4-SHA
- EXP1024-RC4-SHA
- EXP1024-RC4-MD5
- EXP-EDH-RSA-DES-CBC-SHA
- EXP-EDH-DSS-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-RC4-MD5

The following figure illustrates the TLS messages exchanged between the IP phone and TLS server to establish an encrypted communication channel:



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 touch 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 186 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 186 trusted certificates, refer to Appendix C: Trusted Certificates on page 770.
- **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 by the parameter "static.phone_setting.reserve_certs_enable" using the configuration files.

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure TLS on a per-line basis. **Parameter:** account.X.sip_server.Y.transport_type
	<y0000000000xx>.cfg	Configure trusted certificates feature. **Parameters:** static.security.trust_certificates static.security.ca_cert static.security.cn_validation
		Configure server certificates feature. **Parameter:** static.security.dev_cert
		Upload the trusted certificates. **Parameter:** static.trusted_certificates.url
		Delete all uploaded trusted certificates. **Parameter:** static.trusted_certificates.delete
		Upload the server certificates. **Parameter:** static.server_certificates.url

		Delete all uploaded server certificates. **Parameter:** static.server_certificates.delete
		Configure the custom certificates. **Parameter:** static.phone_setting.reserve_certs_enable
Web User Interface		Configure TLS on a per-line basis. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=account-register&q=load&ac=0
		Configure trusted certificates feature. Upload the trusted certificates. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=trusted-cert&q=load
		Configure server certificates feature. Upload the server certificates. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=server-cert&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
account.X.sip_server.Y.transport_type (Y ranges from 1 to 2)	**0, 1, 2 or 3**	**0**
Description: Configures the transport method the IP phone uses to communicate with the SIP server for account X. **0**-UDP **1**-TCP **2**-TLS **3**-DNS-NAPTR X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960)		

Parameters	Permitted Values	Default
Web User Interface: Account->Register->SIP Server Y->Transport **Phone User Interface:** None		
static.security.trust_certificates	**0 or 1**	**1**
Description: Enables or disables the IP phone to only trust the server certificates in the Trusted Certificates list. **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. **Note:** 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		
static.security.ca_cert	**0, 1 or 2**	**2**
Description: Configures the type of certificates in the Trusted Certificates list for the IP phone to authenticate for TLS connection. **0**-Default Certificates **1**-Custom Certificates **2**-All Certificates **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->CA Certificates **Phone User Interface:**		

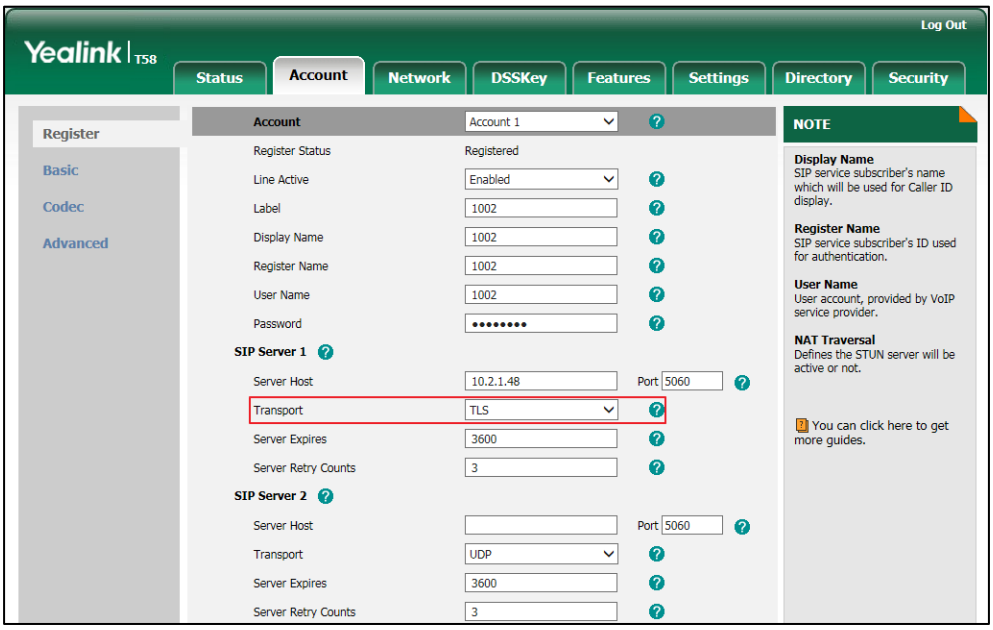
Parameters	Permitted Values	Default
None		
static.security.cn_validation	**0 or 1**	**0**
Description: Enables or disables the IP phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server. **0**-Disabled **1**-Enabled **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Security->Trusted Certificates->Common Name Validation **Phone User Interface:** None		
static.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 **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Security->Server Certificates->Device Certificates **Phone User Interface:** None		
static.trusted_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom trusted certificate used to authenticate the connecting server. **Example:** static.trusted_certificates.url = http://192.168.1.20/tc.crt		

Parameters	Permitted Values	Default
Note: The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format. **Web User Interface:** Security->Trusted Certificates->Load trusted certificates file **Phone User Interface:** None		
static.trusted_certificates.delete	**http://localhost/all**	**Blank**
Description: Deletes all uploaded trusted certificates. **Example:** static.trusted_certificates.delete = http://localhost/all **Web User Interface:** None **Phone User Interface:** None		
static.server_certificates.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the server certificate the IP phone sends for authentication. **Example**: static.server_certificates.url = http://192.168.1.20/ca.pem **Note**: 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		
static.server_certificates.delete	**http://localhost/all**	**Blank**
Description: Deletes all uploaded server certificates. **Example:** static.server_certificates.delete = http://localhost/all **Web User Interface:**		

Parameters	Permitted Values	Default
None **Phone User Interface:** None		
static.phone_setting.reserve_certs_enable	**0 or 1**	**0**
Description: Enables or disables the IP phone to reserve custom certificates after it is reset to factory defaults. **0**-Disabled **1**-Enabled **Web User Interface:** None **Phone User Interface:** None		

To configure TLS on a per-line basis via web user interface:

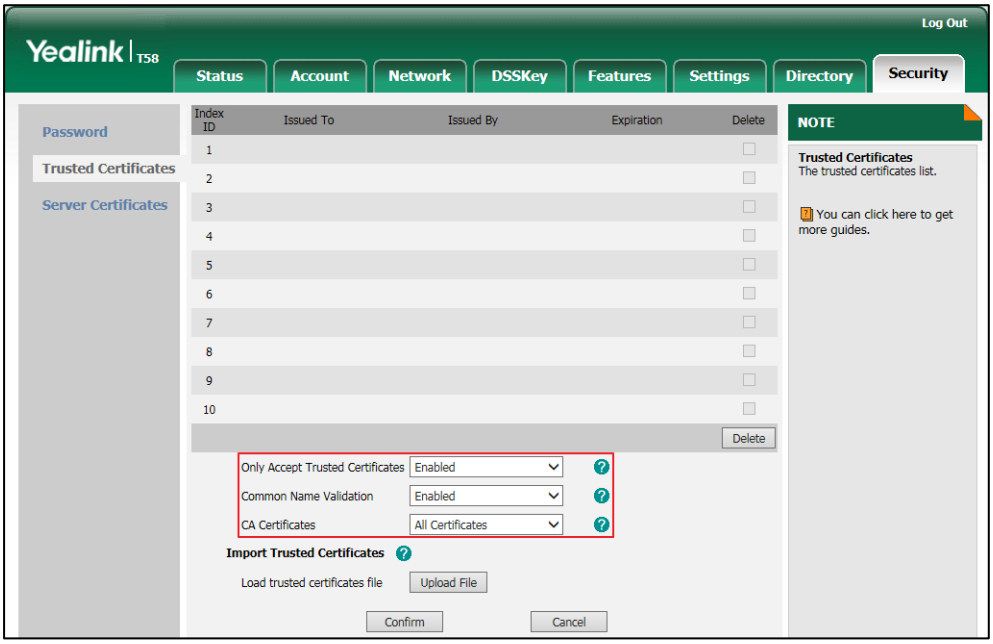
1. Click on **Account**->**Register**.
2. Select the desired account from the pull-down list of **Account**.
3. Select **TLS** from the pull-down list of **Transport**.



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

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**.



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

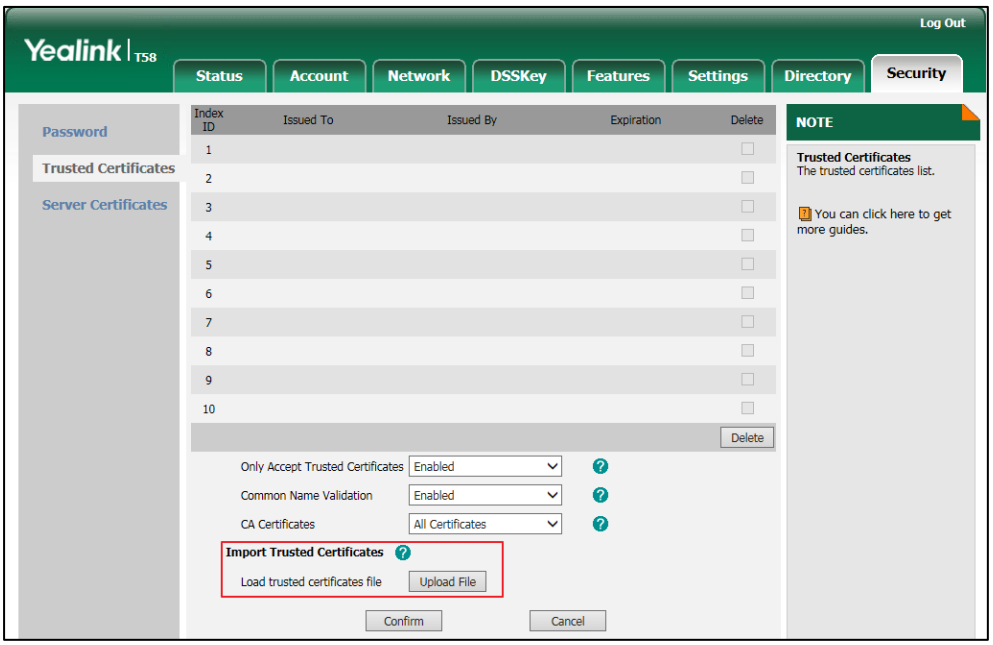
   A dialog box pops up to prompt that the settings will take effect after a reboot.

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

To upload a trusted certificate via web user interface:

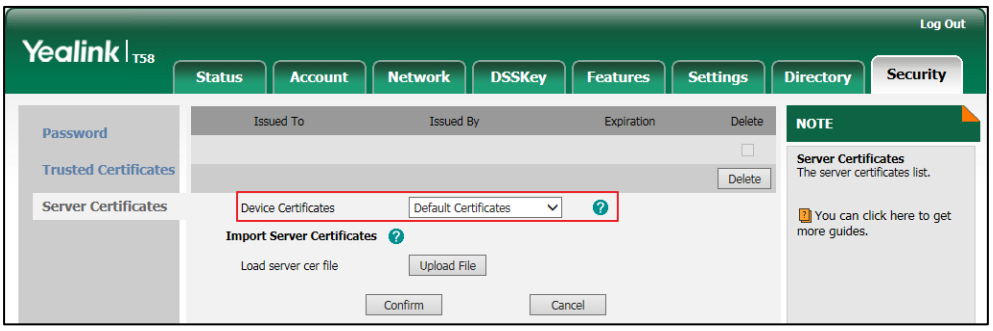
1. Click on **Security**->**Trusted Certificates**.

2. Click **Upload File** to select and upload the certificate (*.pem, *.crt, *.cer or *.der) from your local system.



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**.

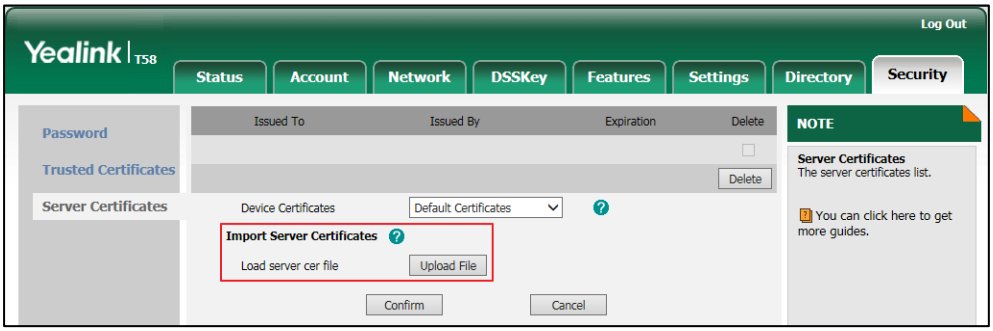


3. Click **Confirm** to accept the change.

To upload a server certificate via web user interface:

1. Click on **Security**->**Server Certificates**.

2. Click **Upload File** to select and upload the certificate (*.pem and *.cer) from your local system.



Secure Real-Time Transport Protocol (SRTP)

Secure Real-Time Transport Protocol (SRTP) encrypts the RTP during VoIP phone calls to avoid interception and eavesdropping. The parties participating in the call must enable SRTP feature simultaneously. When this feature is enabled on both phones, the type of encryption to utilize for the session is negotiated between the IP phones. This negotiation process is compliant with RFC 4568.

When a user places a call on the enabled SRTP phone, the IP phone sends an INVITE message with the RTP encryption algorithm to the destination phone. As described in RFC 3711, RTP streams may be encrypted using an AES (Advanced Encryption Standard) algorithm.

Example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 50020 RTP/AVP 118 9 0 8 18 101
a=rtpmap:118 opus/48000/2
a=fmtp:118 sprop-maxcapturerate=48000; maxaveragebitrate=40000;
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=ptime:20
a=sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NWM5YmZkZDk5YjI1OTg2MDgwOTM5ZjIxNmJkNTY5
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:N2M1NmMzZTI2MGFkZjY5YWYzMGE5MWViYTljNzg4
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NjMxYmIzMDIxNGExM2JkYWQxZTMyODQ1MThkYzg0
m=video 50022 RTP/AVP 97 98 99 117
```

```
b=TIAS:2097152
a=rtpmap:97 H264/90000
a=fmtp:97 profile-level-id=64001f; packetization-mode=1
a=rtpmap:98 H264/90000
a=fmtp:98 profile-level-id=42801f
a=rtpmap:99 H264/90000
a=fmtp:99 profile-level-id=42801f; packetization-mode=1
a=rtpmap:117 YL-FPR/90000
a=fmtp:117 yl-capset=7;yl-ver=1;yl-ext=19
a=ptime:20
a=rtcp-fb:* ccm fir
a=sendrecv
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NDdmNGIxYjJiNjkwYmEwNDg4MDVlYmMyYTA0YThl
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:IGE3NjY1MmZjYWEzOTQ4ZmU3ODEwZWQ3MWI3ZWYx
a=crypto:3 F8_128_HMAC_SHA1_80 inline:ZjlmZjg3Yjk5MmRkYTBjNDI0ZDRlNzFjZTc2MGIx
```

The callee receives the INVITE message with the RTP encryption algorithm, and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.

Example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 50068 RTP/SAVP 118 9 0 8 18 101
a=rtpmap:118 opus/48000/2
a=fmtp:118 sprop-maxcapturerate=48000; maxaveragebitrate=40000;
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=ptime:20
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:ZDgyNzVlNzZkODQ5OTZhYmY4N2ZlNTI0ZjIyYTRl
a=sendrecv
m=video 50070 RTP/SAVP 97 98 99 117
b=TIAS:2097000
a=rtpmap:97 H264/90000
```

```
a=fmtp:97 profile-level-id=64001f; packetization-mode=1
a=rtpmap:98 H264/90000
a=fmtp:98 profile-level-id=42801f
a=rtpmap:99 H264/90000
a=fmtp:99 profile-level-id=42801f; packetization-mode=1
a=rtpmap:117 YL-FPR/90000
a=fmtp:117 yl-capset=7;yl-ver=1;yl-ext=19
a=ptime:20
a=rtcp-fb:* ccm fir
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NzVjNDQ1NTQgY2YzYmQ2YzJhZjc0MzZmNmJiMzM1
a=sendrecv
```

SRTP is configurable on a per-line basis. When SRTP is enabled on both IP phones, RTP streams will be encrypted, and a lock icon appears on the touch screen of each IP phone after successful negotiation.

Note If you enable SRTP, then you should also enable TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to Transport Layer Security (TLS) on page 698.

Procedure

SRTP can be configured using the following methods.

Central Provisioning (Configuration File)	<MAC>.cfg	Configure SRTP feature on a per-line basis. **Parameter:** account.X.srtp_encryption
Web User Interface		Configure SRTP feature on a per-line basis. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

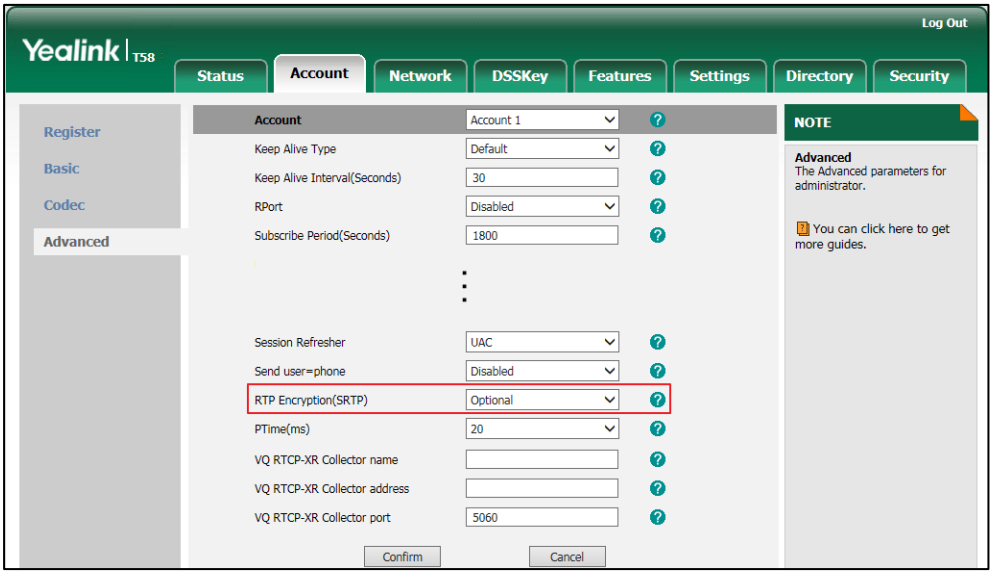
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
account.X.srtp_encryption	**0, 1 or 2**	**0**
Description:		

Parameter	Permitted Values	Default
Configures whether to use audio/video encryption service for account X. **0**-Disabled **1**-Optional **2**-Compulsory If it is set to 0 (Disabled), the IP phone will not use audio/voice encryption service. If it is set to 1 (Optional), the IP phone will negotiate with the other IP phone what type of encryption to utilize for the session. If it is set to 2 (Compulsory), the IP phone is forced to use SRTP during a call. X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **Web User Interface:** Account->Advanced->RTP Encryption(SRTP) **Phone User Interface:** None		

To configure SRTP feature via web user interface:

1. Click on **Account**->**Advanced**.
2. Select the desired account from the pull-down list of **Account**.
3. Select the desired value from the pull-down list of **RTP Encryption(SRTP)**.



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

Encrypting and Decrypting Files

Yealink IP phones support downloading encrypted files from the server and encrypting files before/when uploading them to the server. You can encrypt the following files: MAC-Oriented CFG file (<MAC>.cfg), Common CFG file (y0000000000xx.cfg), MAC-local CFG file (<MAC>-local.cfg) or other custom CFG files (e.g., sip.cfg, account.cfg)

To encrypt/decrypt files, you may have to configure an AES key.

Configuration Parameters

Procedure

Configuration changes can be performed using the following methods.

<table>
<tr><td rowspan="4">Central Provisioning (Configuration File)</td><td rowspan="4"><y0000000000xx>.cfg</td><td>Configure whether to only download and resolve the encrypted files.
Parameter:
static.auto_provision.update_file_mode</td></tr>
<tr><td>Configure the decryption method.
Parameter:
static.auto_provision.aes_key_in_file</td></tr>
<tr><td>Configure AES keys.
Parameters:
static.auto_provision.aes_key_16.com
static.auto_provision.aes_key_16.mac</td></tr>
<tr><td>Specify if the MAC-local CFG file is encrypted when it is uploaded from the phone to the server.
Parameter:
static.auto_provision.encryption.config</td></tr>
<tr><td colspan="2">Web User Interface</td><td>Configure AES keys.
Navigate to:
http://<phoneIPAddress>/servlet?p=settings-autop&q=load</td></tr>
<tr><td colspan="2">Phone User Interface</td><td>Configure AES keys.</td></tr>
</table>

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.auto_provision.update_file_mode	**0 or 1**	**0**
Description: Enables or disables the IP phone only to download the encrypted files. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone will download the configuration files (e.g., sip.cfg, account.cfg, <MAC>-local.cfg) and <MAC>-contact.xml file from the server during auto provisioning no matter whether the files are encrypted or not. And then resolve these files and update settings onto the IP phone system. If it is set to 1 (Enabled), the IP phone will only download the encrypted configuration files (e.g., sip.cfg, account.cfg, <MAC>-local.cfg) or <MAC>-contact.xml file from the server during auto provisioning, and then resolve these files and update settings onto the IP phone system. **Web User Interface:** None **Phone User Interface:** None		
static.auto_provision.aes_key_in_file	**0 or 1**	**0**
Description: Enables or disables the IP phone to decrypt configuration files using the encrypted AES keys. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the IP phone will decrypt the encrypted configuration files using plaintext AES keys configured on the IP phone. If it is set to 1 (Enabled), the IP phone will download <xx_Security>.enc files (e.g., <sip_Security>.enc, <account_Security>.enc) during auto provisioning, and then decrypts these files into the plaintext keys (e.g., key2, key3) respectively using the phone built-in key (e.g., key1). The IP phone then decrypts the encrypted configuration files using corresponding key (e.g., key2, key3). **Web User Interface:** None **Phone User Interface:**		

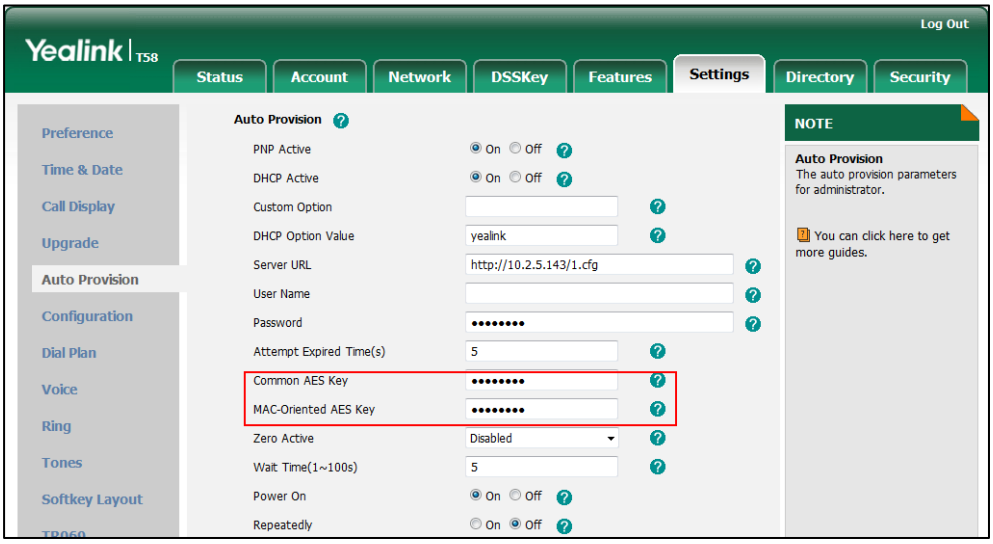
Parameters	Permitted Values	Default
None		
static.auto_provision.aes_key_16.com	**16 characters**	**Blank**
Description: Configures the plaintext AES key for encrypting/decrypting the Common CFG/Custom CFG file. The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: **# $ % * + , - . : = ? @ [ ] ^ _ { } ~**. **Example:** static.auto_provision.aes_key_16.com = 0123456789abcdef **Note**: For decrypting, it works only if the value of the parameter "static.auto_provision.aes_key_in_file" is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter "static.auto_provision.aes_key_16.mac" is left blank, the IP phone will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com". **Web User Interface:** Settings->Auto Provision->Common AES Key **Phone User Interface:** Settings->Advanced Settings (default password: admin) ->Auto Provision->Common		
static.auto_provision.aes_key_16.mac	**16 characters**	**Blank**
Description: Configures the plaintext AES key for encrypting/decrypting the MAC-Oriented files (<MAC>.cfg, <MAC>-local.cfg and <MAC>-contact.xml). The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: **# $ % * + , - . : = ? @ [ ] ^ _ { } ~**. **Example:** static.auto_provision.aes_key_16.mac = 0123456789abmins **Note**: For decrypting, it works only if the value of the parameter "static.auto_provision.aes_key_in_file" is set to 0 (Disabled). If the downloaded MAC-Oriented file is encrypted and the parameter "static.auto_provision.aes_key_16.mac" is left blank, the IP phone will try to encrypt/decrypt the MAC-Oriented file using the AES key configured by the parameter "static.auto_provision.aes_key_16.com". **Web User Interface:** Settings->Auto Provision->MAC-Oriented AES Key **Phone User Interface:**		

Parameters	Permitted Values	Default
Settings->Advanced Settings (default password: admin) ->Auto Provision->MAC-Oriented AES		
static.auto_provision.encryption.config	**0 or 1**	**0**
Description: Enables or disables the IP phone to encrypt <MAC>-local.cfg file using the plaintext AES key. **0**-Disabled **1**-Enabled If it is set to 0 (Disabled), the MAC-local CFG file is uploaded unencrypted and replaces the one (encrypted or unencrypted) stored on the server if you have configured to back up the MAC-local CFG file to the server by the parameter "static.auto_provision.custom.sync". If it is set to 1 (Enabled), the MAC-local CFG file is uploaded encrypted and replaces the one (encrypted or unencrypted) stored on the server if you have configured to back up the MAC-local CFG file to the server by the parameter "static.auto_provision.custom.sync". The plaintext AES key is configured by the parameter "static.auto_provision.aes_key_16.mac". **Web User Interface:** None **Phone User Interface:** None		

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: **# $ % * + , - . : = ? @ [ ] ^ _ { } ~**.



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

To configure AES keys via phone user interface:

1. Tap **Settings->Advanced** (default password: admin) ->**Set AES Key**.
2. Enter the values in the **Common AES** and **MAC-Oriented AES** 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. Tap ✓ to accept the change.

Encrypting and Decrypting 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 configuration files (e.g., account.cfg, <y0000000000xx>.cfg, <MAC>.cfg) (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.

Note You can also configure the <MAC>-local.cfg files to be automatically encrypted using 16-character symmetric keys when uploading to the server (by setting the value of the parameter "static.auto_provision.encryption.config" to 1).

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, y000000000058_Security.enc for

y000000000058.cfg file, account_Security.enc for account.cfg). 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 configuration 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, <xx_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the IP phone requests to download the boot file first and then download the referenced configuration files. For more information on boot file, refer to Boot Files on page 114. For example, the IP phone downloads account.cfg file and it is encrypted. The IP phone will request to download <account_Security>.enc file (if enabled) and decrypt it into the the plaintext key (e.g., key2) using the built-in key (e.g., key1). Then the IP phone decrypts account.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 other configuration files is the same to that of the account.cfg file.

Procedure to Encrypt Configuration Files

To encrypt the <y0000000000xx>.cfg file:

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.

   The screenshot of the main page is shown as below:

   When you start the application tool, a file folder named "Encrypted" is created automatically in the directory where the application tool is located.

2. Click **Browse** to locate configuration file(s) (e.g., y000000000058.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.

3. (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.

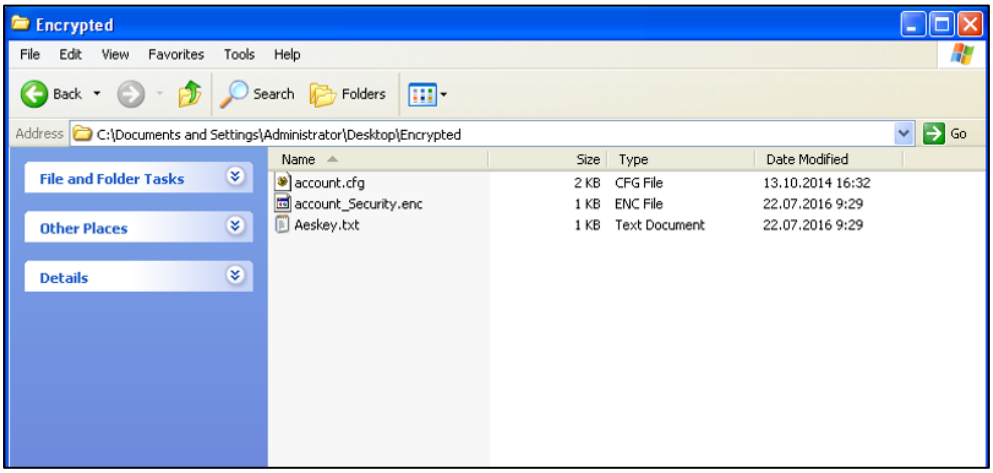
   If you mark the **Auto Generate** radio box, the configuration file(s) will be encrypted using random AES key. The AES keys of configuration files are different.

Note AES keys must be 16 characters and the supported characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: **# $ % * + , - . : = ? @ [ ] ^ _ { } ~**.

5. Click **Encrypt** to encrypt the configuration file(s).

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).



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
- Getting Information from Talk Statistics
- Analyzing Configuration File

Viewing Log Files

If your IP phone encounters some problems, commonly the log files are needed. You can configure the phone to periodically upload the log files to the provisioning server (only support an FTP/TFTP as the provisioning server). There are two types of log files on the provisioning server: <MAC>-boot.log (e.g., 0015659188f2-boot.log) and <MAC>-sys.log (0015659188f2-sys.log). The <MAC>-boot.log file is uploaded to the provisioning server after every boot. The <MAC>-sys.log file is uploaded periodically to the provisioning server. You can export the log files to a syslog server or the local system. 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:

- **static.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

- **static.syslog.mode** - Specify the system log to be exported to the provisioning server, syslog server or local system.
- **static.syslog.server** -- Specify the IP address or domain name of the syslog server to which the log will be exported.
- **static.syslog.log_upload_period** - Specify the period (in seconds) of the log uploads to the provisioning server.
- **static.syslog.ftp.post_mode** - Specify whether the log files on the provisioning server are overwritten or appended.
- **static.syslog.ftp.max_logfile** - Specify the maximum size of the log files can be stored on the provisioning server.
- **static.syslog.ftp.append_limit_mode** - Specify the behavior when log file on the provisioning server reaches the max size.
- **static.syslog.bootlog_upload_wait_time** - Specify the waiting time before the phone uploads the log file to the provisioning server.
- **static.auto_provision.server.url** - Specify the access URL of the syslog server or provisioning server.

Configuring the Severity Level of the Log

Procedure

Severity level can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the severity level of the logs to be reported to a log file. **Parameter:** static.syslog.log_level
Web User Interface		Configure the severity level of the logs to be reported to a log file. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-config&q=load

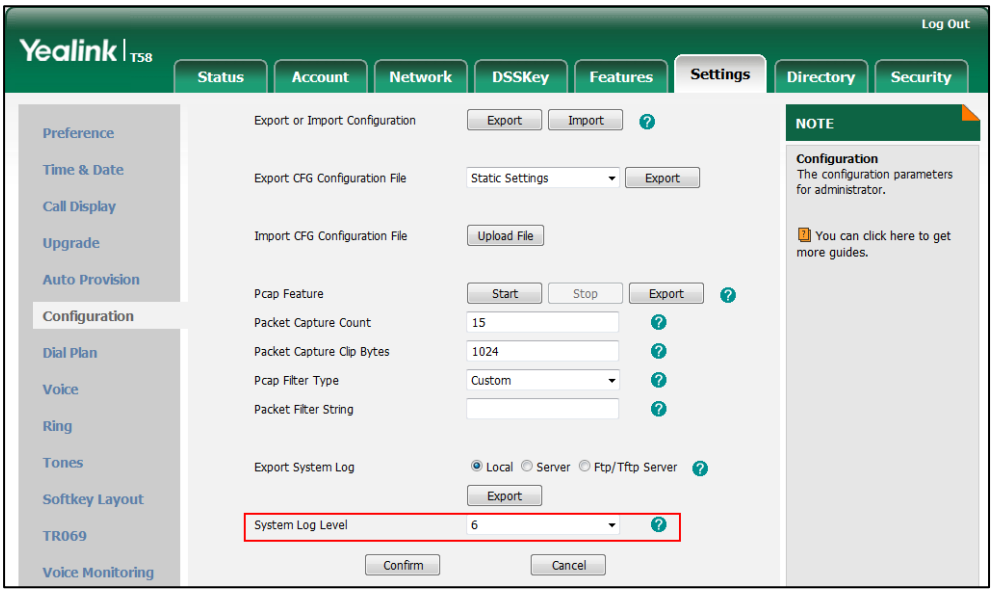
Details of Configuration Parameter:

Parameter	Permitted Values	Default
static.syslog.log_level	**Integer from 0 to 6**	**3**
Description:		

Parameter	Permitted Values	Default
Configures the detail level of syslog information to be exported. **0**-system is unusable **1**-action must be taken immediately **2**-critical condition **3**-error conditions **4**-warning conditions **5**-normal but significant condition **6**-informational **Note**: If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** 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**.



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), 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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the syslog mode. **Parameter:** static.syslog.mode
Web User Interface		Configure the syslog mode. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-config&q=load

Details of Configuration Parameter:

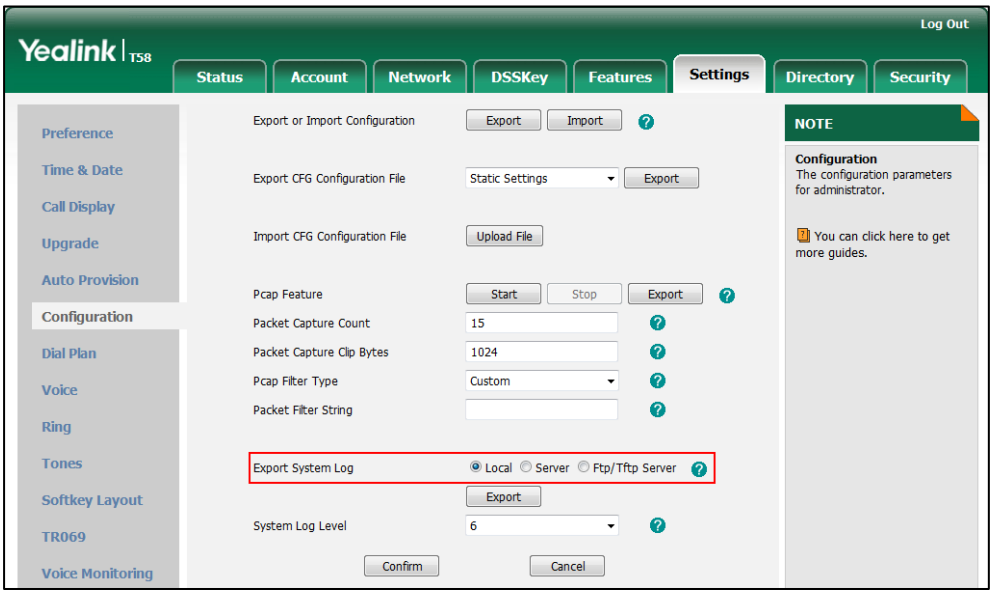
Parameter	Permitted Values	Default
static.syslog.mode	**0, 1 or 2**	**0**
Description: Configures the IP phone to export log files to the local system, syslog server or an FTP/TFTP Server (provisioning server). **0**-Local **1**-Server **2**-FTP/TFTP Server **Note:** If you change this parameter, the 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 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.

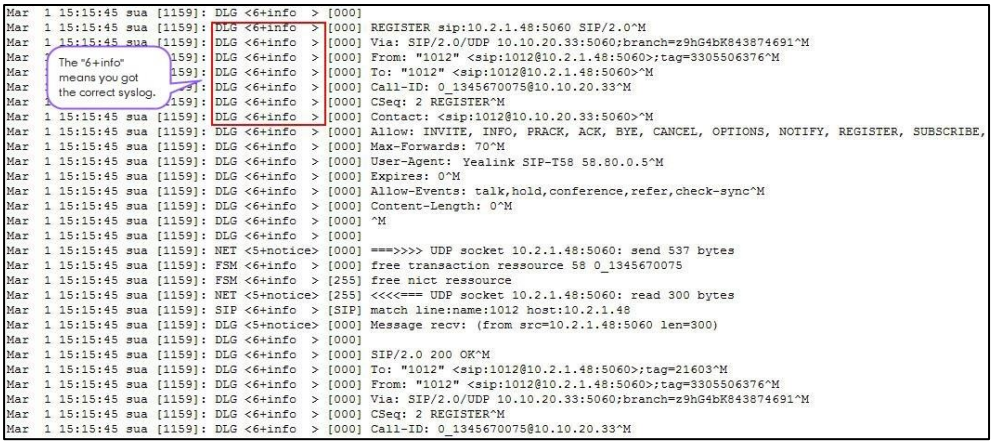


A log file named **syslog.tar** is successfully exported to your local system.

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:



Exporting the Log File to a Syslog Server

Procedure

Log setting can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the syslog mode. **Parameter:** static.syslog.mode
		Configure the IP address or domain name of the syslog server where to export the log files. **Parameter:** static.syslog.server
Web User Interface		Configure the syslog mode. Configure the IP address or domain name of the syslog server where to export the log files. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-config&q=load

Details of Configuration Parameters:

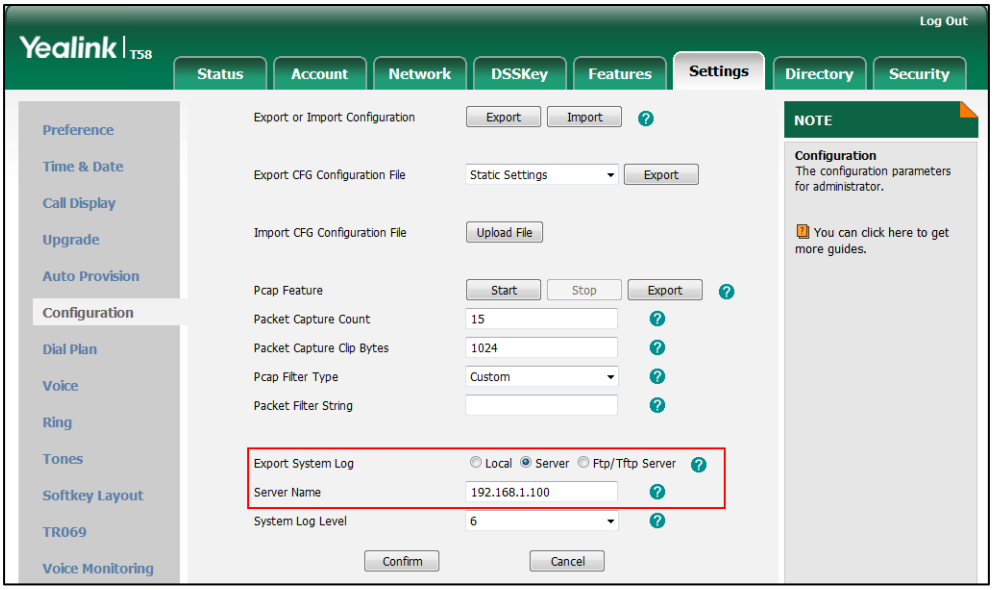
Parameters	Permitted Values	Default
static.syslog.mode	**0, 1 or 2**	**0**
Description: Configures the IP phone to export log files to the local system, syslog server or an FTP/TFTP Server (provisioning server). **0**-Local **1**-Server **2**-FTP/TFTP Server **Note:** If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Export System Log **Phone User Interface:** None		

Parameters	Permitted Values	Default
static.syslog.server	**IP address or domain name**	**Blank**
Description: Configures the IP address or domain name of the syslog server when exporting log to the syslog server. **Example:** static.syslog.server = 192.168.1.100 **Note:** It works only if the value of the parameter "static.syslog.mode" is set to 1 (Server). If 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 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.
3. 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.



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

   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.

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

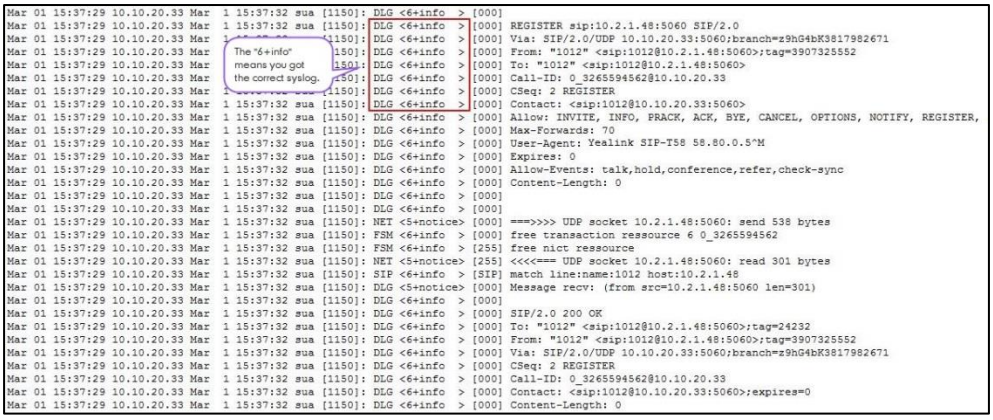
   The system log will be exported successfully to the desired syslog server (192.168.1.100) after a reboot.

6. Reproduce the issue.

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:



Exporting the Log File to a Provisioning Server (FTP/TFTP Server)

Procedure

Log setting can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the syslog mode. **Parameter:** static.syslog.mode
		Configure the period (in seconds) of the log uploads to the provisioning server. **Parameter:** static.syslog.log_upload_period
		Configure whether the log files on the provisioning server are overwritten or appended. **Parameter:** static.syslog.ftp.post_mode

		Configure the maximum size of the log files can be stored on the provisioning server. **Parameter:** static.syslog.ftp.max_logfile
		Configure the behavior when log file on the provisioning server reaches the max size. **Parameter:** static.syslog.ftp.append_limit_mode
		Configure the waiting time before the phone uploads the log file to the provisioning server. **Parameter:** static.syslog.bootlog_upload_wait_time
		Configure the access URL of the provisioning server. **Parameter:** static.auto_provision.server.url
Web User Interface		Configure the syslog mode. Configure the period (in seconds) of the log uploads to the provisioning server. Configure whether the log files on the provisioning server are overwritten or appended. Configure the maximum size of the log files on the provisioning server. Configure the behavior when log file on the provisioning server reaches the max size. Configure the waiting time before the phone uploads the log file to the provisioning server. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-config&q=load

	Configure the access URL of the provisioning server. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-autop&q=load

Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.syslog.mode	**0, 1 or 2**	**0**
Description: Configures the IP phone to export log files to the local system, syslog server or an FTP/TFTP Server (provisioning server). **0**-Local **1**-Server **2**-FTP/TFTP Server **Note:** 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		
static.syslog.log_upload_period	**Integer from 30 to 2592000**	**30**
Description: Configures the period of the log upload (in seconds) to the provisioning server. **Example:** static.syslog.log_upload_period = 60 **Note:** It works only if the value of the parameter "static.syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Upload Period **Phone User Interface:** None		

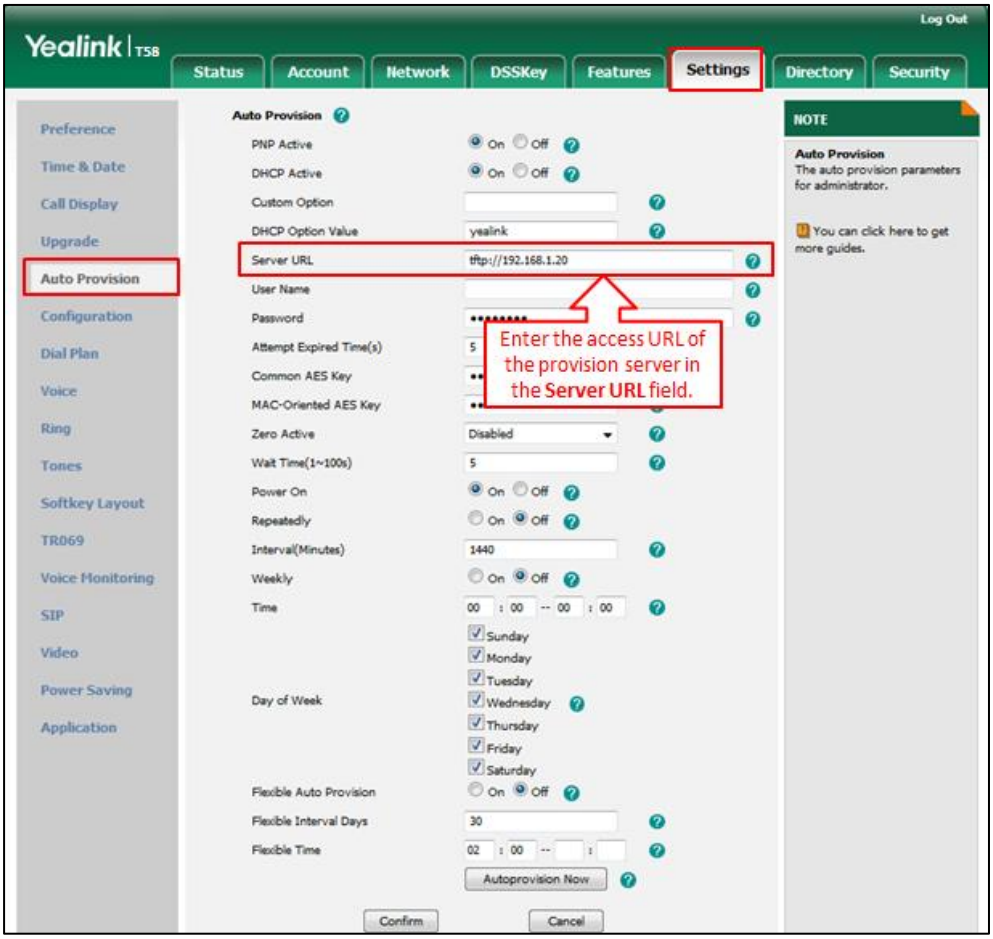
Parameters	Permitted Values	Default
static.syslog.ftp.post_mode	**1 or 2**	**1**
Description: Configures whether the log files on the provisioning server are overwritten or appended. **1-**Post Append (not applicable to TFTP Server) **2-**Post Stor If it is set to 1 (Post Append), the log files on the provisioning server are appended. If it is set to 2 (Post Stor), the log files on the provisioning server are overwritten. **Note:** It works only if the value of the parameter "static.syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Post Mode **Phone User Interface:** None		
static.syslog.ftp.max_logfile	**Integer from 200 to 65535**	**512**
Description: Configures the maximum size of the log files (in KB) can be stored on the provisioning server. **Example:** static.syslog.ftp.max_logfile = 511 **Note:** It works only if the value of the parameter "static.syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Append Limit Size **Phone User Interface:** None		
static.syslog.ftp.append_limit_mode	**1 or 2**	**1**
Description: Configures the behavior when log file on the provisioning server reaches the max size. **1**-Append Delete		

Parameters	Permitted Values	Default
2-Append Stop If it is set to 1 (Append Delete), the IP phone will delete the old log and start over. If it is set to 2 (Append Stop), the IP phone will stop uploading log. **Note:** It works only if the value of the parameter "static.syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Append Limit Mode **Phone User Interface:** None		
static.syslog.bootlog_upload_wait_time	**Integer from 1 to 86400**	**120**
Description: Configures the waiting time (in seconds) before the phone uploads the log file to the provisioning server. **Example:** static.syslog.bootlog_upload_wait_time = 121 **Note:** It works only if the value of the parameter "static.syslog.mode" is set to 2 (FTP/TFTP Server). If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** None **Phone User Interface:** None		
static.auto_provision.server.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the provisioning server. **Example:** static.auto_provision.server.url = tftp://10.3.6.133/ **Web User Interface:** Settings->Auto Provision->Server URL **Phone User Interface:** None		

To configure the URL of the provisioning server via web user interface:

1. Click on **Settings**->**Auto Provision**.
2. Enter the URL of the FTP/TFTP server in the **Server URL** field.

   For example, if the IP address TFTP server is 192.168.1.20, then the URL "tftp://192.168.1.20/" is where the IP phone exports the system log. For more information on TFTP server, refer to *Yealink_SIP-T2_Series_T19(P) E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*.

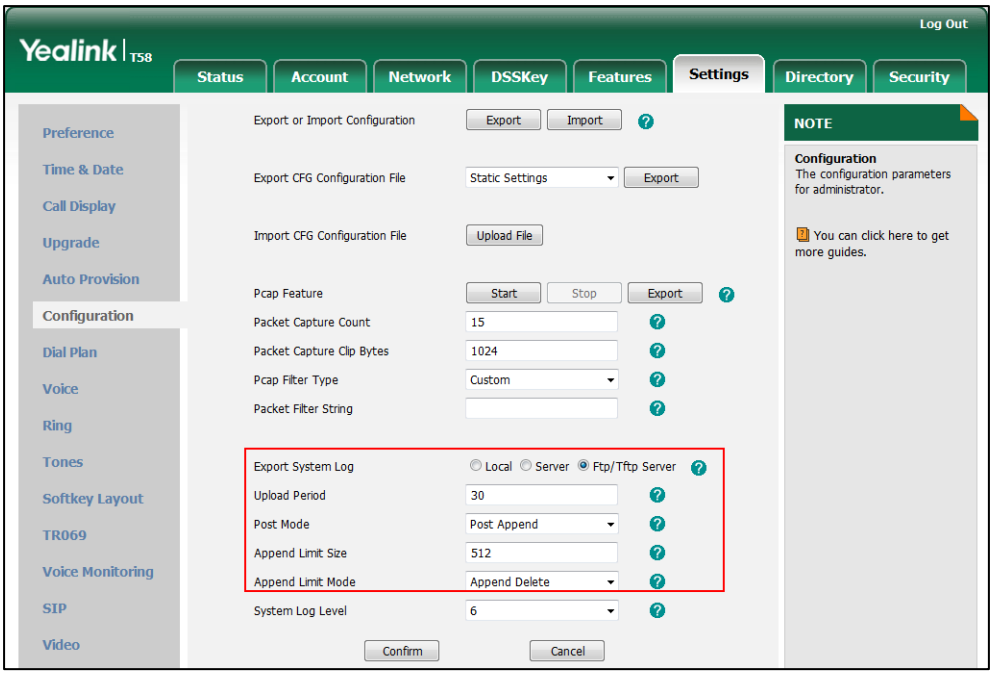


3. Click **Confirm** to accept the change.

To configure the phone to export the system log to an FTP/TFTP server via web user interface:

1. Click on **Settings**->**Configuration**.
2. Mark the **Ftp/Tftp server** radio box in the **Export System Log** field.
3. Enter the upload period of the log files in the **Upload Period** field.
4. Select the desired post mode from the pull-down list of **Post Mode.**
5. Enter the limit size of the log files in the **Append Limit Size** field.

6. Select the desired limit mode from the pull-down list of **Append Limit Mode.**



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

   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.

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

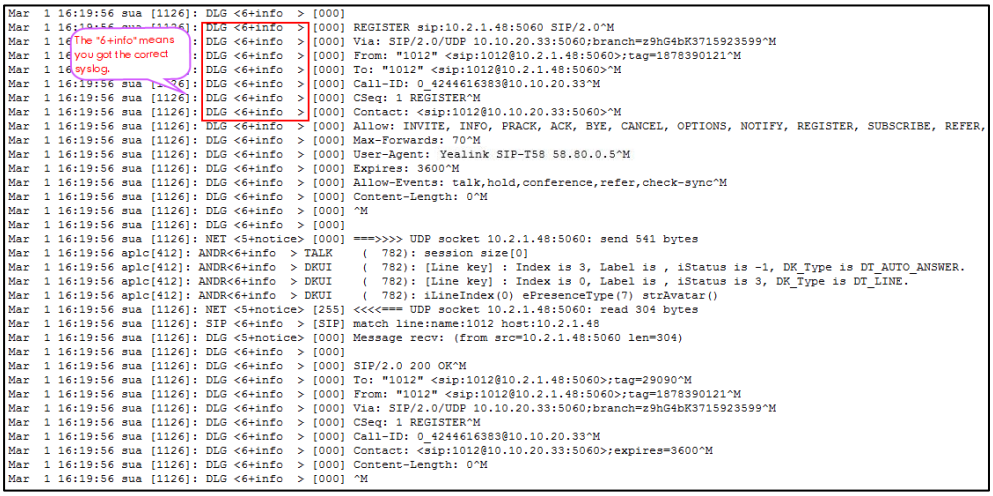
   The system log will be exported successfully to the desired FTP/TFTP server after a reboot.

9. Reproduce the issue.

To view the log file on your FTP/TFTP server:

You can view the system log file in the root directory folder you have configured on the FTP/TFTP server.

The following figure shows a portion of a <MAC>-boot.log (e.g., 0015659188f2-boot.log):



The following figure shows a portion of a <MAC>-sys.log (e.g., 0015659188f2-sys.log):

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

Yealink IP phones support exporting the packets file to the local system and analyze it. You can configure the maximum size and the filter type of the packets.

Procedure

Pcap feature can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure Pcap feature. **Parameters:** packet_capture.max_file_counts packet_capture.max_file_bytes packet_capture.filter_type packet_capture.filter
Web User Interface		Configure Pcap feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-config&q=load

Details of the Configuration Parameters:

Parameters	Permitted Values	Default
packet_capture.max_file_counts	**Integer from 1 to 100**	**15**
Description: Configures the count of the number of packets to capture. **Web User Interface:** Settings->Configuration->Packet Capture Count **Phone User Interface:** None		
packet_capture.max_file_bytes	**Integer from 100 to 1024**	**1024**
Description: Configures the maximum size (in KB) of every packet to capture. **Web User Interface:** Settings->Configuration->Packet Capture Clip Bytes **Phone User Interface:** None		
packet_capture.filter_type	**0, 1 or 2**	**0**
Description: Configures the filter type of the packet to capture. **0**-Custom **1**-SIP or H245 or H225 **2**-RTP If it is set to 0 (Custom), the IP phone captures the packets according to the custom packet filter string (configured by the parameter "packet_capture.filter"). If it is set to 1 (SIP or H245 or H225), the IP phone captures the SIP, H245 or H225 packets. It depends on the supportive protocol of the IP phone. If it is set to 2 (RTP), the IP phone captures the RTP packets. **Web User Interface:** Settings->Configuration->Pcap Filter Type **Phone User Interface:** None		
packet_capture.filter	**String within 255**	**Blank**

Parameters	Permitted Values	Default
	characters	

Description:

Customizes the packet filter string.

If it is left blank, the IP phone will not automatically filter any string when capturing packets.

Syntax:

Protocol+Direction+Host(s)+ Value +Logical Operations+Other Expression

Protocol:

Values: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp.

Application-level protocol, such as http, dns and sip are not supported.

If no protocol is specified, all the protocols are used.

Direction:

Values: src, dst, src and dst, src or dst.

If no source or destination is specified, the "src or dst" keywords are applied.

For example: "host 10.2.2.2" is equivalent to "src or dst host 10.2.2.2".

Host(s):

Values: net, port, host, portrange.

If no host(s) is specified, the "host" keyword is used.

For example: "src 10.1.1.1" is equivalent to "src host 10.1.1.1".

Logical Operations:

Values: not, and, or.

Negation ("not") has highest precedence. Alternation ("or") and concatenation ("and") have equal precedence and associate left to right.

For example:

"not tcp port 3128 and tcp port 23" is equivalent to "(not tcp port 3128) and tcp port 23".

"not tcp port 3128 and tcp port 23" is NOT equivalent to "not (tcp port 3128 and tcp port 23)".

Example: (src host 10.4.1.12 or src net 10.6.0.0/16) and tcp dst port range 200-10000 and dst net 10.0.0.0/8

Displays packets with source IP address 10.4.1.12 or source network 10.6.0.0/16, the result is then concatenated with packets having destination TCP port range from 200 to 10000 and destination IP network 10.0.0.0/8.

Note: It works only if the value of the parameter “packet_capture.filter_type” is set to 0 (Custom).

Web User Interface:

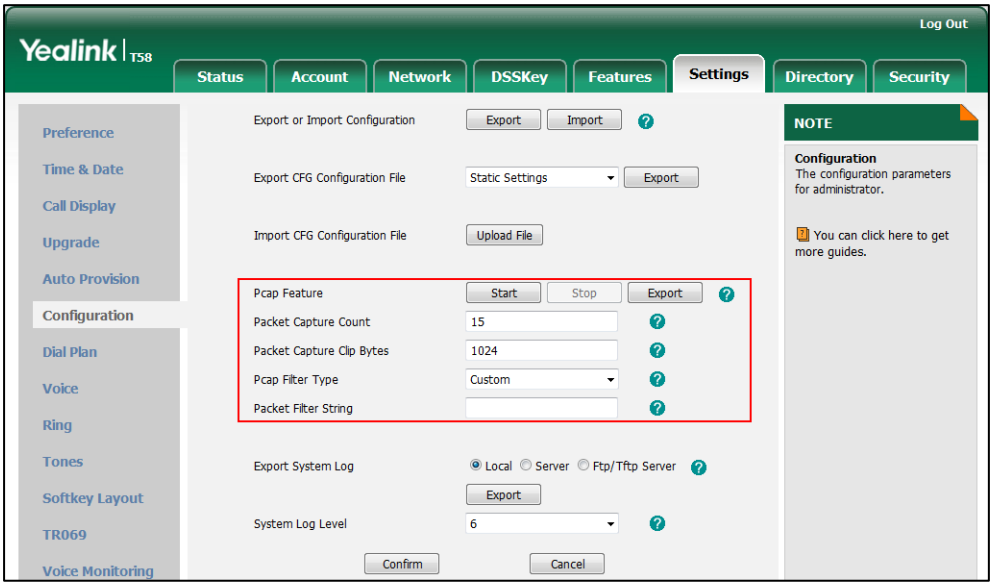
Settings->Configuration->Packet Filter String

Parameters	Permitted Values	Default
Phone User Interface: None		

To capture packets via web user interface:

1. Click on **Settings**->**Configuration**.
2. Enter the desired value in the **Packet Capture Count** field.
3. Enter the desired value in the **Packet Capture Clip Bytes** field.
4. Select the desired value from the pull-down list of **Pcap Filter Type**.

   If **Custom** is selected, enter the desired packet filter string in the **Packet Filter String** field.
5. Enter the desired value in the **Packet Filter String** field.
6. Click **Start** to start capturing signal traffic.
7. Reproduce the issue to get stack traces.
8. Click **Stop** to stop capturing.
9. Click **Export** to open the file download window, and then save the file to your local system.



Capturing 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

Internet port to the PC port. It is not applicable to CP960 IP phones.

Procedure

Span to PC port can be configured using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure span to PC port. **Parameter:** static.network.span_to_pc_port
Web User Interface		Configure span to PC port. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load

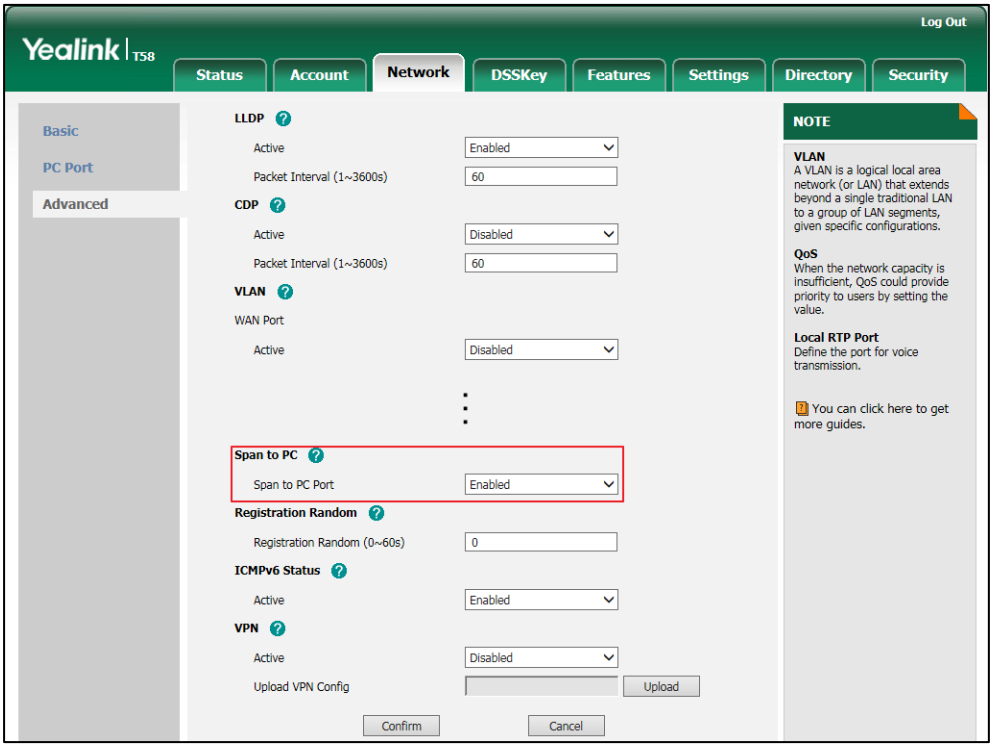
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
static.network.span_to_pc_port	**0 or 1**	**0**
Description: Enables or disables the IP phone to span data packets received from the Internet port to the PC port. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), all data packets from Internet port can be received by PC port. **Note**: It is not applicable to CP960 IP phones. It works only if the value of the parameter "static.network.pc_port.enable" is set to 1 (Auto Negotiate). 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**.

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 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 following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure Watch Dog feature. **Parameter:** static.watch_dog.enable
Web User Interface		Configure Watch Dog feature. **Navigate to**: http://<phoneIPAddress>/servlet?m=mo

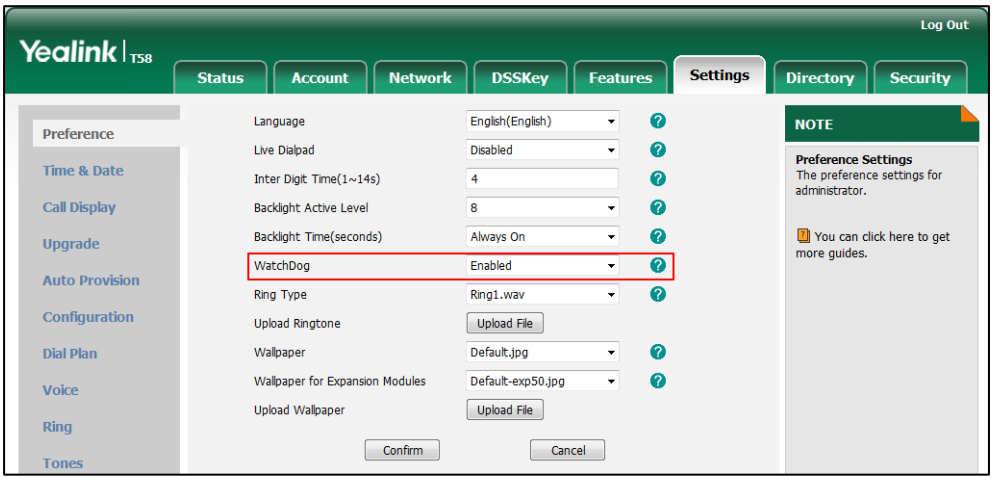
	d_data&p=settings-preference&q=load

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
static.watch_dog.enable	**0 or 1**	**1**
Description: Enables or disables the Watch Dog feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), the IP phone will reboot automatically when the system is broken down. **Web User Interface:** Settings->Preference->WatchDog **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 **WatchDog**.



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

Getting Information from Status Indicators

Status indicators may consist of the power 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-T58V IP phones:

- If a LINK failure of the IP phone is detected, a prompting message "Network unavailable" and the icon will appear on the touch screen.
- If the headset mode is enabled, the headset key LED illuminates.

For more information on the icons, refer to Appendix G: Reading Icons on page 793.

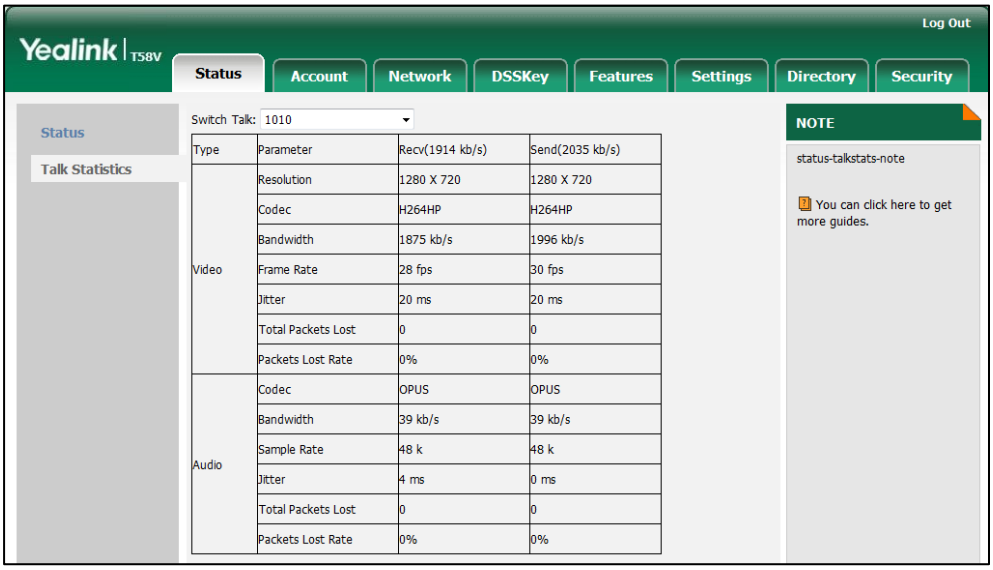
Getting Information from Talk Statistics

Talk statistics may consist of the video and audio data during an active call.

You can view the talk statistics during an active call via web phone user interface. Information includes:

- **Video**: Resolution, Codec, Bandwidth (Uplink Bandwidth and Downlink Bandwidth), Frame Rate, Jitter, Total Packet Lost, Packet Lost Rate. It is not applicable to SIP-T56A/CP960 IP phones.
- **Audio:** Codec, Bandwidth (Uplink Bandwidth and Downlink Bandwidth), Sample Rate, Jitter, Total Packet Lost, Packet Lost Rate

The following shows the IP phone information when having an active call with 1010 (the phone number):



Type	Parameter	Recv(1914 kb/s)	Send(2035 kb/s)
Video	Resolution	1280 X 720	1280 X 720
	Codec	H264HP	H264HP
	Bandwidth	1875 kb/s	1996 kb/s
	Frame Rate	28 fps	30 fps
	Jitter	20 ms	20 ms
	Total Packets Lost	0	0
	Packets Lost Rate	0%	0%
Audio	Codec	OPUS	OPUS
	Bandwidth	39 kb/s	39 kb/s
	Sample Rate	48 k	48 k
	Jitter	4 ms	0 ms
	Total Packets Lost	0	0
	Packets Lost Rate	0%	0%

Analyzing Configuration Files

Wrong configurations may have an impact on your phone use. You can export configuration 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.

Six types of configuration files can be exported to your local system:

- config.bin

- <MAC>-all.cfg
- <MAC>-local.cfg
- <MAC>-static.cfg
- <MAC>-non-static.cfg
- <MAC>-config.cfg

We recommend you to edit the exported CFG file instead of the BIN file to change the phone's current settings. For more information on configuration files, refer to Configuration Files on page 116.

BIN Configuration Files

The config.bin file is an encrypted file. For more information on config.bin file, contact your Yealink reseller.

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Specify the access URL for the custom configuration files. **Parameter:** static.configuration.url
Web User Interface		Export or import the custom configuration files. **Navigate to**: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-config&q=load

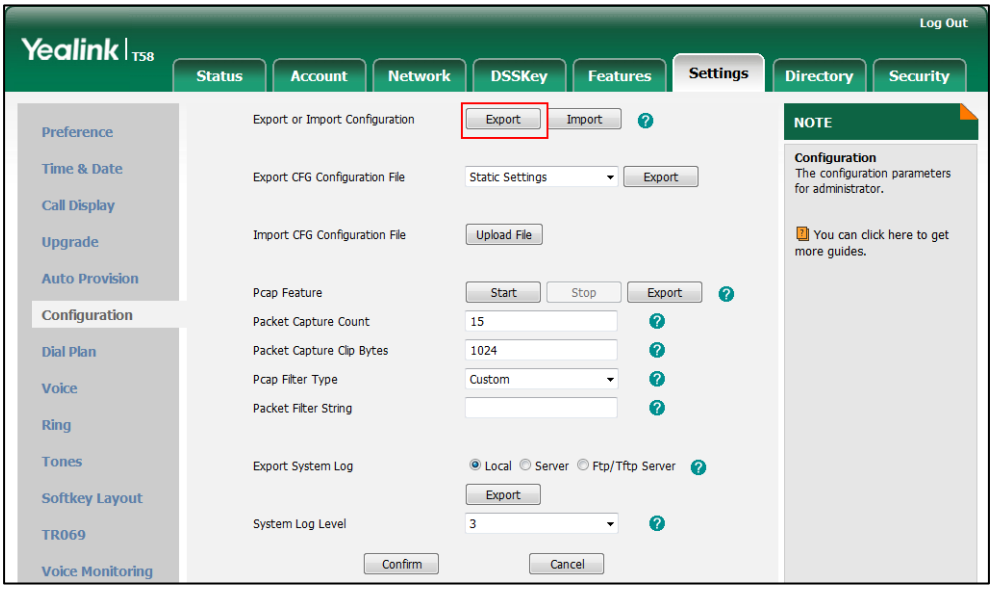
Details of the Configuration Parameter:

Parameter	Permitted Values	Default
static.configuration.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL for the custom configuration files. **Note**: The file format of custom configuration file must be *.bin. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Export or Import Configuration **Phone User Interface:**		

Parameter	Permitted Values	Default
None		

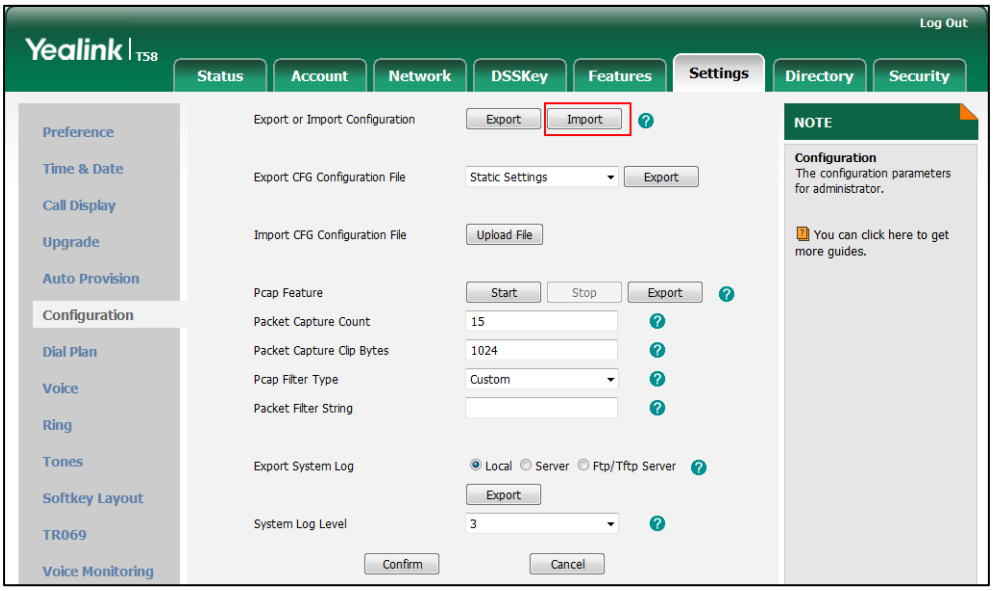
To export BIN configuration files via web user interface:

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.



To import a BIN configuration file via web user interface:

1. Click on **Settings**->**Configuration**.
2. In the **Export or Import Configuration** block, click **Import** to locate and import a BIN configuration file from your local system.



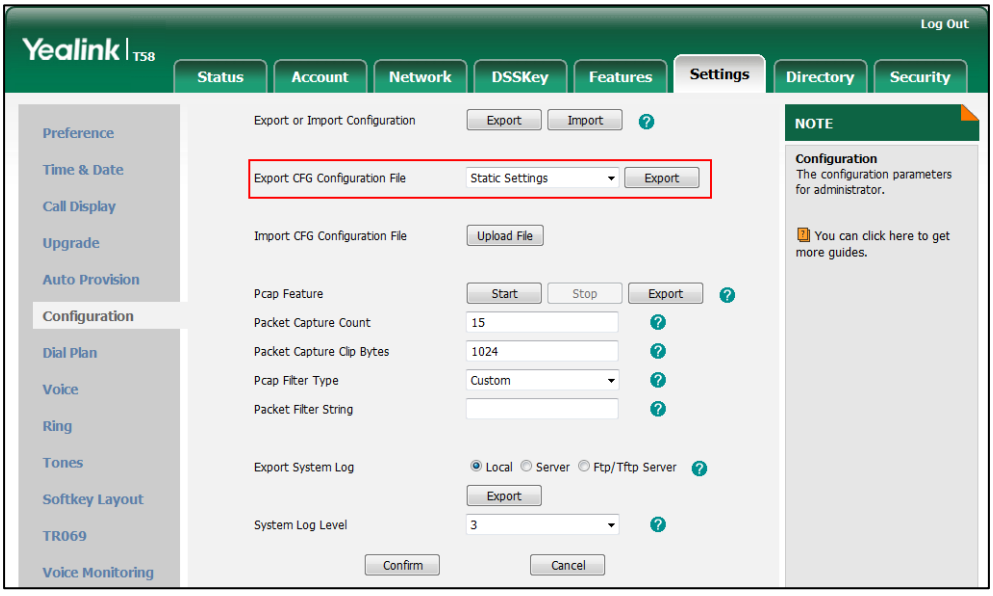
CFG Configuration Files

Five CFG configuration files can be exported:

- **<MAC>-local.cfg**: It contains changes associated with non-static settings made via phone user interface and web user interface. It can be exported only if the value of the parameter "static.auto_provision.custom.protect" is set to 1.
- **<MAC>-all.cfg**: It contains all changes made via phone user interface, web user interface and using configuration files.
- **<MAC>-static.cfg**: It contains all changes associated with static settings (e.g., network settings) made via phone user interface, web user interface and using configuration files.
- **<MAC>-non-static.cfg**: It contains all changes associated with non-static settings made via phone user interface, web user interface and using configuration files.
- **<MAC>-config.cfg**: It contains changes made using configuration files. It can be exported only if the value of the parameter "static.auto_provision.custom.protect" is set to 1.

To export CFG configuration files via web user interface:

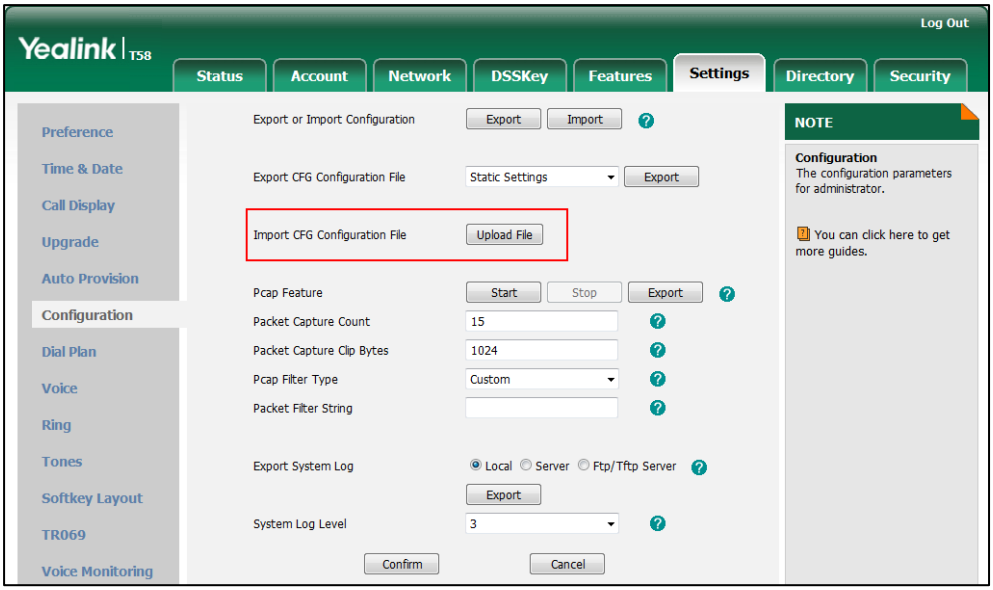
1. Click on **Settings**->**Configuration**.
2. Select the desired CFG configuration file from the pull-down list of **Export CFG Configuration File**.
3. Click **Export** to open file download window, and then save the file to your local system.



To import CFG configuration files via web user interface:

1. Click on **Settings**->**Configuration**.

2. In the **Import CFG Configuration File** block, click **Upload File** to locate and import a CFG configuration file from your local system.



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:

If your phone connects to the wired network:

- 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.
- Ensure that the Wi-Fi feature is disabled.

If your phone connects to the wireless network:

- If the network is secure, ensure the entered password is right.
- Ensure your gateway/router enables the wireless network feature.

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 **Settings**->**Advanced** (default password: admin) ->**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_SIP-T2_Series_T19(P) E2_T4_Series_T5_Series_W5_Series_CP_Series_IP_Phones_Auto_Provisioning_Guide_V81*.

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.

Display Issues

Why is the touch 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.

Why does the IP phone display "No Service"?

The touch screen prompts "No Service" message when there is no available SIP account on the IP phone.

Do one of the following:

- Ensure that an account is actively registered on the IP phone at the path **Settings**->**Status**->**Accounts**.
- Ensure that the SIP account parameters have been configured correctly.

Phone Book Issues

What is the difference between a remote phone book and a local phone book?

A remote phone book is placed on a server, while a local phone book is placed on the IP phone flash. A remote phone book can be used by everyone that can access the server, while a local phone book can only be used by a specific phone. A remote phone book is always used as a central phone book for a company; each employee can load it to obtain the real-time data from the same server.

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 when there is an incoming call arrives on the phone, to adjust the volume of engaged audio device (handset, speakerphone or headset) when there is an active call in progress, or to adjust the media volume when the phone is not on the idle screen.

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 computer 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 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 329.

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 329.

Camera and Video Issues

Why is the video quality bad?

- Ensure that the display device has suitable resolution.
- Check whether the packet has been lost. For more information on packet loss, refer to Getting Information from Talk Statistics on page 742.
- Ensure that camera settings are configured correctly, such as brightness and white balance.
- Avoid high-intensity indoor light or direct sunlight on the camera.

Why can’t I preview local camera when the phone is idle?

If the camera is properly connected to the IP phone but there are no images on the screen when you launch **Camera** application or swipe down from the top of the screen and then tap **Video**, you may need to replace the camera.

Why is there some dazzle light on the images when previewing the local camera?

If the camera lens is oily or soiled, there may be some dazzle light on the images. Please try to clean it up.

Wi-Fi and Bluetooth Issues

Why is the wireless signal strength low?

Ensure the IP phone and your gateway/router are within the working range and there is no obvious interference (walls, doors, etc.) between them.

Why can't I connect the IP phone to the 2.4G wireless network?

If you successfully connect the IP phone to the 2.4G wireless network, but the video images is not smooth. Or, you cannot connect the IP phone to the 2.4G wireless network.

- Check if there are too many wireless devices connecting to the same 2.4G wireless network.
- Verify whether the distance between IP phone and the wireless router is too far.

Why can't I connect the Bluetooth device with the IP phone all the time?

Try to delete the registration information of the Bluetooth device on both IP phone and Bluetooth device, and then pair and connect it again. Contact Yealink field application engineer and your Bluetooth device manufacturer for more information.

Why the Bluetooth headset affects IP phone's voice quality?

You may not experience the best voice quality if you use a Bluetooth headset while the 2.4 GHz band is enabled or while you are in an environment with many other Bluetooth devices. This possible loss in voice quality is due to inherent limitations with Bluetooth technology.

Firmware and Upgrading Issues

Why doesn't the IP phone upgrade firmware successfully?

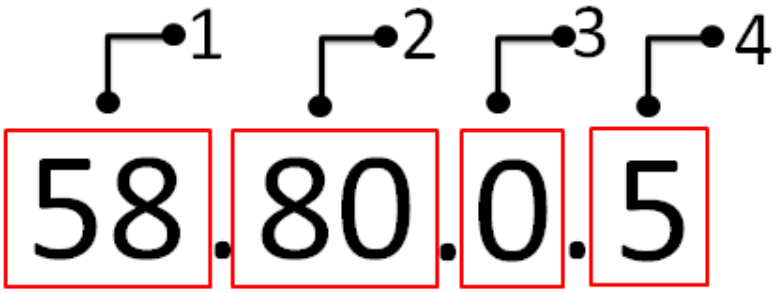
Do one of the following:

- 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.

How can I verify the firmware generation and version of the phone?

Tap **Settings**->**Status** when the IP phone is idle to check the firmware version. For example:

58.80.0.5.



	Item	Description
1	58	Firmware ID. The firmware ID for each IP phone model is: • 58: SIP-T58V/T58A/T56A • 73: CP960
2	80	Firmware generation. **Note**: The larger it is, the newer the firmware generation is.
3	0	A fixed number.
4	5	Firmware version. **Note**: With the same firmware generation, 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 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.

What is PnP?

Plug and Play (PnP) is a method for IP phones to acquire the provisioning server address. With PnP enabled, the IP phone broadcasts the PnP SUBSCRIBE message to obtain a provisioning server address during startup. Any SIP server recognizing the message will respond with the preconfigured provisioning server address, so the IP phone will be able to download the CFG files from the provisioning server. PnP depends on support from a SIP server.

System Log Issues

Why can't I export the system log to a provisioning server (FTP/TFTP server)?

Do one of the following:

- Ensure that the FTP/TFTP server is downloaded and installed on your local system.
- Ensure that you have configured the FTP/TFTP server address correctly via web user interface on your IP phone.
- Reboot the phone. The configurations require a reboot to take effect.

Why can't 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 phone. The configurations require a reboot to take effect.

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.

Six ways to reset the phone:

- **Reset local settings**: All configurations saved in the <MAC>-local.cfg file on the IP phone will be reset. Changes associated with non-static settings made via web user interface and phone user interface are saved in the <MAC>-local.cfg file.
- **Reset non-static settings**: All non-static settings on the phone will be reset. After resetting the non-static settings, the IP phone will perform the auto provisioning process immediately.

- **Reset static settings**: All static settings on the phone will be reset.
- **Reset userdata & local config**: All the local cache data (e.g., userdata, history, directory) will be cleared. And all configurations saved in the <MAC>-local.cfg configuration file on the IP phone will be reset.
- **Reset to factory Setting**: All configurations on the phone will be reset.
- **Reset build-in SD card**: All the files in the internal SD card will be cleared.

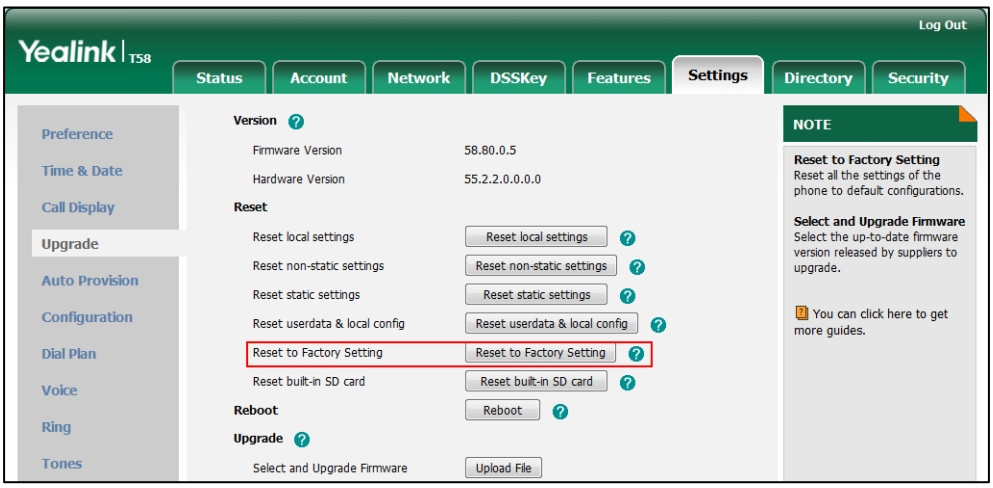
You can reset the IP phone to default factory configurations. The default factory configurations are the settings that reside on the IP phone after it has left the factory. You can also reset the IP phone to custom factory configurations if required. The custom factory configurations are the settings that defined by the user to keep some custom settings after resetting.

Note The **Reset local settings/Reset non-static settings/Reset static settings/Reset userdata & local config** option on the web user interface appears only if the value of the parameter "static.auto_provision.custom.protect" is set to 1.

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?".

3. Click **OK** to confirm the resetting.

The IP phone will be reset to factory sucessfully after startup.

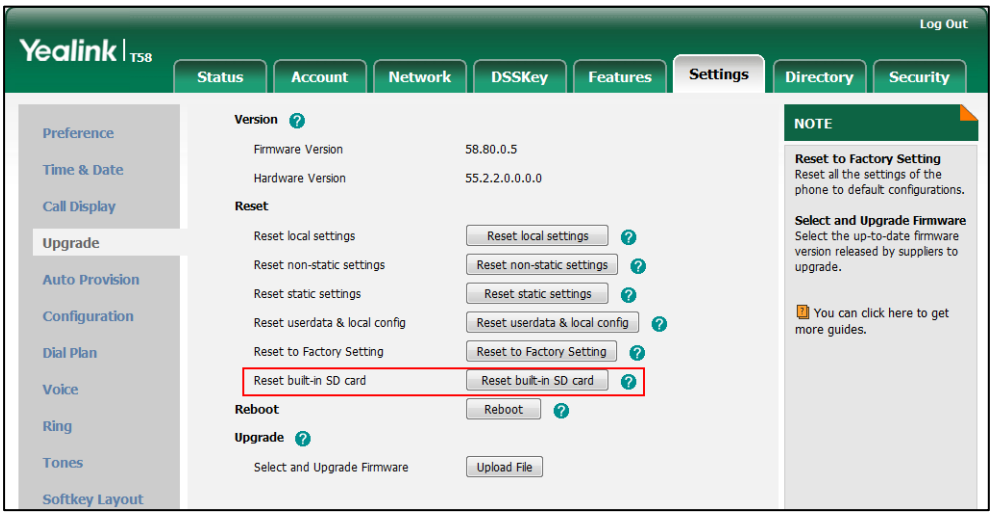
Note Reset of your phone may take a few minutes. Do not power off until the phone starts up successfully.

Resetting the IP phone to factory settings will delete all configuration information on the phone. Please backup all the settings before resetting.

How to reset internal SD card to factory?

To reset the internal SD card to factory:

1. Click on **Settings**->**Upgrade**.
2. Click **Reset build-in SD card** in the **Reset build-in SD card** field.



The web user interface prompts the message "Reset build-in SD card to factory?".

3. Click **OK** to confirm the resetting.

And all the data (e.g., pictures, audio and video files) in the internal will be cleared if you reset the internal SD card.

How to reset the IP phone to custom factory configurations?

Procedure

Configuration changes can be performed using the following methods.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the Import Factory Configuration feature. **Parameter:** static.features.custom_factory_config.enable
		Configure the access URL of the custom factory configuration files. **Parameter:** static.custom_factory_configuration.url
Web User Interface		Configure the access URL of the custom factory configuration files. **Navigate to:** http://<phoneIPAddress>/servlet?m=mod_data&p=settings-config&q=load

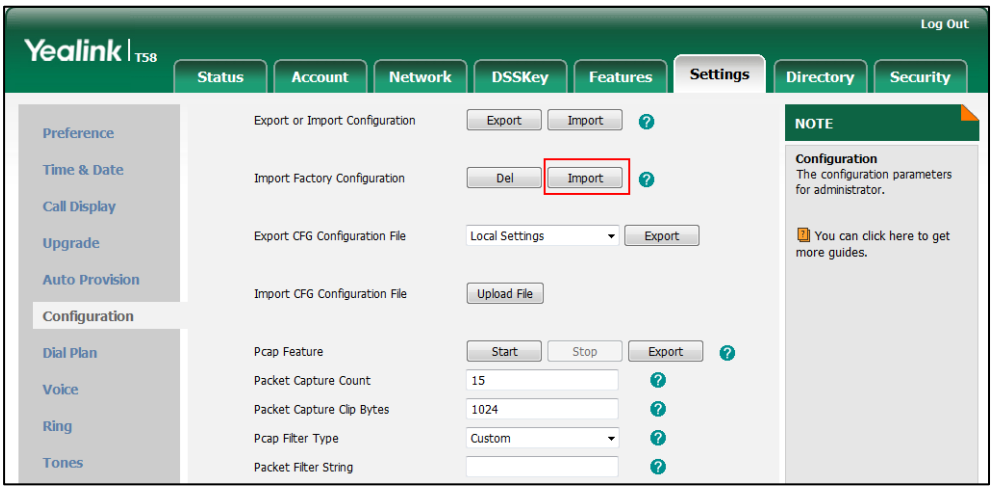
Details of Configuration Parameters:

Parameters	Permitted Values	Default
static.features.custom_factory_config.enable	**0 or 1**	**0**
Description: Enables or disables the Import Factory Configuration feature. **0**-Disabled **1**-Enabled If it is set to 1 (Enabled), **Import Factory Configuration** item will be displayed on the IP phone's web user interface at the path **Settings**->**Configuration**. You can import a custom factory configuration file or delete the user-defined factory configuration via web user interface. **Web User Interface:** None **Phone User Interface:** None		
static.custom_factory_configuration.url	**URL within 511 characters**	**Blank**
Description: Configures the access URL of the custom factory configuration files. **Note**: It works only if the value of the parameter "static.features.custom_factory_config.enable" is set to 1 (Enabled) and the file format of custom factory configuration file must be *.bin. If you change this parameter, the IP phone will reboot to make the change take effect. **Web User Interface:** Settings->Configuration->Import Factory Configuration **Phone User Interface:** None		

To import the custom factory configuration files via web user interface:

1. Click on **Settings**->**Configuration**.

2. Click **Import** to locate and import the custom factory configuration file from your local system.

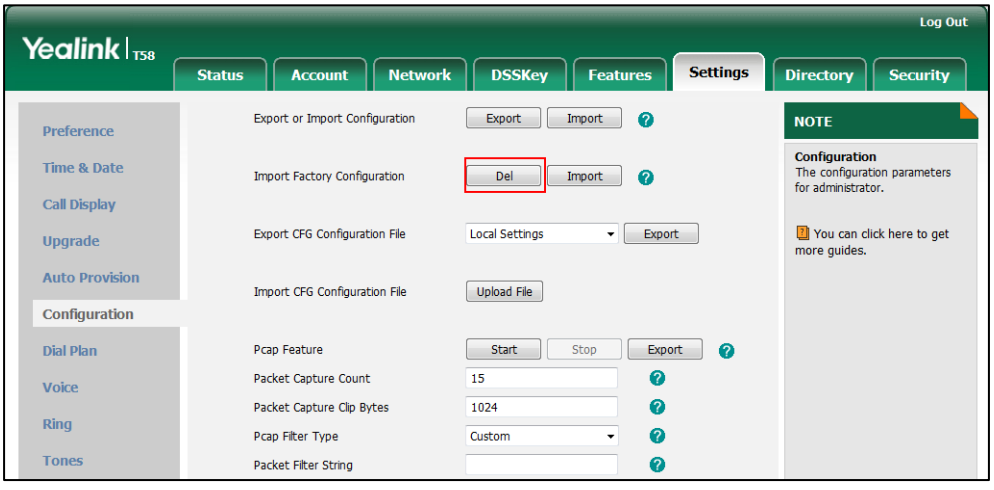


When the custom factory configuration file is imported successfully, you can reset the IP phone to custom factory configurations. For more information on how to reset to factory configuration via web user interface, refer to How to reset the IP phone to default factory configurations? on page 753.

You can delete the user-defined factory configurations via web user interface.

To delete the custom factory configuration files via web user interface:

1. Click on **Settings**->**Configuration**.
2. Click **Del** in the **Import Factory Configuration** field.



The web user interface prompts the message "Are you sure delete user-defined factory configuration?".

3. Click **OK** to delete the custom factory configuration files.

   The imported custom factory file will be deleted. The IP phone will be reset to default factory configurations after resetting.

Rebooting Issues

How to reboot the IP phone remotely?

IP phones support remote reboot by a SIP NOTIFY message with "Event: check-sync" header. Whether the IP phone reboots or not depends on the value of the parameter "sip.notify_reboot_enable". If the value is set to 1, or the value is set to 0 and the header of the SIP NOTIFY message contains an additional string "reboot=true", the IP phone will reboot immediately.

The NOTIFY message is formed as shown:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=true
```

Procedure

Changes can only be configured using the configuration files.

Central Provisioning (Configuration File)	<y0000000000xx>.cfg	Configure the IP phone behavior when receiving a SIP NOTIFY message which contains the header "Event: check-sync". **Parameter:** sip.notify_reboot_enable

Details of the Configuration Parameter:

Parameter	Permitted Values	Default
sip.notify_reboot_enable	**0, 1 or 2**	**1**
Description: Configure the IP phone behavior when receiving a SIP NOTIFY message which contains the header "Event: check-sync". **0**-The IP phone will reboot only if the SIP NOTIFY message contains an additional string "reboot=true". **1**-The IP phone will be forced to reboot. **2**-The IP phone will ignore the SIP NOTIFY message.		

Parameter	Permitted Values	Default
Web User Interface: None **Phone User Interface:** None		

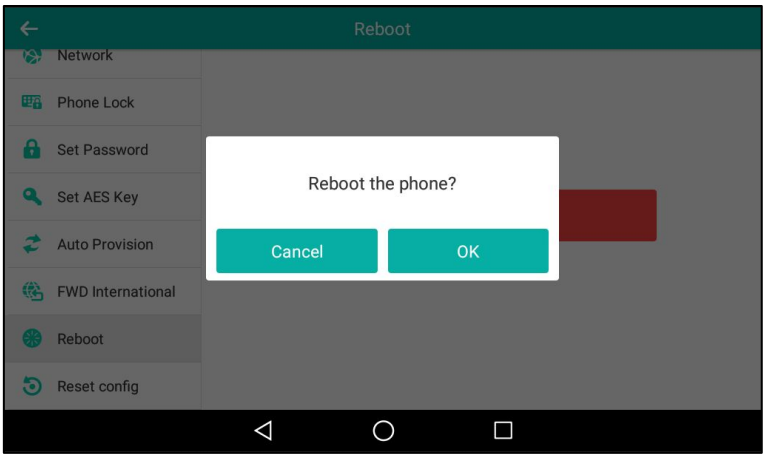
How to reboot the IP phone via web/phone user interface?

You can reboot your IP phone via web/phone user interface.

To reboot the phone via phone user interface:

1. Tap **Settings**->**Advanced** (default password: admin) ->**Reboot**.
2. Tap **Reboot**.

   The touch screen prompts the following warning:

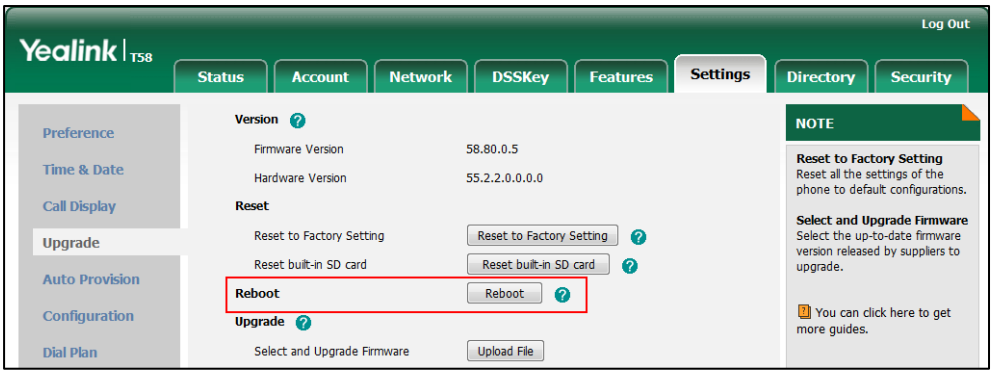


3. Tap **OK** to reboot the phone.

   The phone begins rebooting. Any reboot of the phone may take a few minutes.

To reboot the phone via web user interface:

1. Click on **Settings**->**Upgrade**.
2. Click **Reboot** to reboot the IP phone.



The phone begins rebooting. Any reboot of the 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 address 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.
		1024~65535	TR-069 Server	IP address of TR-069 server	Determined by destination device.	TCP	TR-069 protocol port, it is used to communicate with TR-069server.
		1024~65535	File server	IP address of file server	Determined by destination device.	TCP	HTTP protocol port, it is used to download file.
		1024~65535	Remote phone book server	IP address of remote phone book server	Determined by destination device.	TCP	HTTP protocol port, it is used to access the remote phone book.
		1024~65535	AA	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	LDAP Server	IP address of LDAP server	Determined by destination device.	TCP	LDAP protocol port, it is used to obtain the contact information

Source Device	Source IP	Source Port	Destination Device	Destination IP	Destination Port (Listening port)	Protocol	Description of destination port
							from LDAP 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.
		1024~65535	Syslog Server	IP address of syslog server	514	UDP	Syslog protocol port, it is used for IP phones to upload syslog information to syslog server.
		1024~65535	PNP Server	IP address of PNP server (Default value: 224.0.1.75)	5059	UDP/TCP	Protocol port, it is used to obtain the URL of updating file from PNP server.
			Multipaging	Multipaging	65000 65001		
PC	IP address of PC	Determined by the destination device.	IP phones	IP address of IP phones	1~65535	TCP	HTTP port (default value: 80)
					1~65535	TCP	HTTP port (default value: 443)
SIP Server	IP address of SIP Server				1024~65534	UDP/TCP	SIP protocol port, it is used for signaling interaction with SIP server.
IP phone of voice gateway	IP address of IP phone or voice gateway				2~65535	UDP	RTP protocol port, it is used by destination device to send or receive audio stream.
TR-069 Server	IP address of TR-069 Server				1024~65535	TCP	TR-069 protocol port, it is used to communicate with TR-069server.

Password Issues

How to restore the administrator password?

Factory reset can restore the original password. All custom settings will be overwritten after reset.

Power and Startup Issues

What will happen if I connect both PoE cable and power adapter? Which has the higher priority?

IP phones use the PoE preferentially.

Why does the IP phone have no power?

If no lights appear on the IP phone when it is powered up, do one of the following:

- Reboot your IP phone.
- Replace the power adapter.

Why is the touch screen black?

If the power indicator LED is on, the keypad is usable but the touch screen is black, please reboot your IP phone.

Why does the IP phone always display the Yealink logo?

If your IP phone does not boot, check if the provisioning server is accessible on the network and a valid software firmware and valid configuration files are available. Try to use recovery mode to get your phone ready. For more information on recovery mode, refer to *Recovery Mode on Yealink IP Phones*.

Why can't IP phone supply power for device using USB port?

The USB port of Yealink IP phone has a limit current of 525 ~ 875mA. Make sure that the device is USB flash drive or mobile hard disk with low power.

Hardware Issues

Why is the sending/receiving volume of the speaker too low?

- If there is no volume sending from the speaker or sending volume is too low, the Hands-free MIC cable may not have been properly connected.

- If there is no volume receiving from the speaker or receiving volume is too low, the speaker cable may not have been properly connected.

Why is the sending/receiving volume of the headset or handset too low?

Ensure that the headset or handset is not damaged. If the headset or handset is usable, it may be the codec problem on the mainboard.

Why is there no response when pressing the keys on the keypad?

Do one of the following:

- Ensure that the keypad cables is properly connected and not damaged.
- Check if the keypad surface is clean.

Why is there no response when tapping the items on the touch screen?

Do one of the following:

- Ensure that the FPC of the touch screen is properly connected.
- Check if the touch screen is damaged.

Why is the LED off when pressing the hard key with LED indicator?

Make sure that the cable of keypad board is properly connected. If the cable is properly connected, it may be the LED on the board is damaged.

Other Issues

How do I find the basic information of the IP phone?

Tap **Settings**->**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 among user name, register name and display name?

Both user name and register name are defined by the server. User name identifies the account, while register name matched with a password is for authentication purposes. Display name is the caller ID that will be displayed on the callee's phone touch screen. Server configurations may override the local ones.

What do "on code" and "off code" mean?

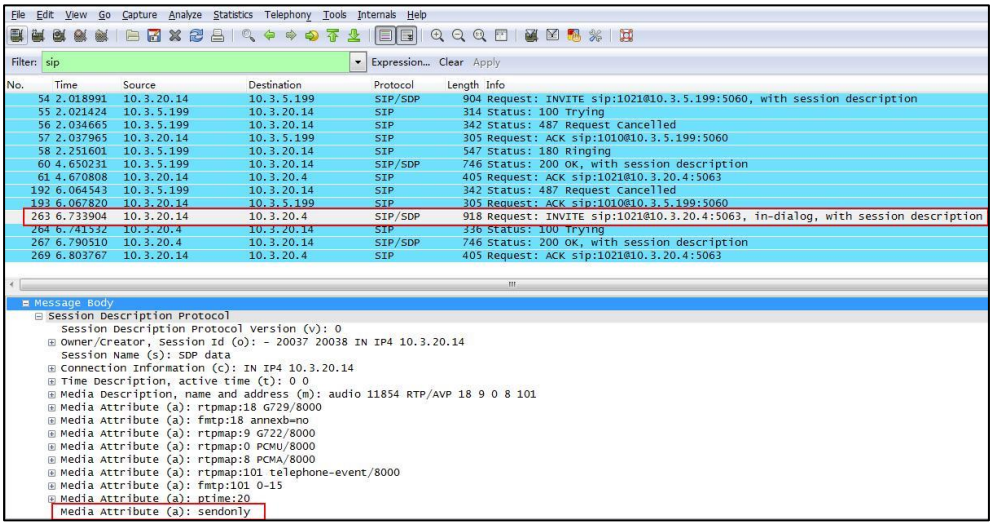
They are codes that the IP phone sends to the server when a certain action takes place. On code is used to activate a feature on the server side, while off code is used to deactivate a feature on the server side.

For example, if you set the Always Forward on code to be *78 (may vary on different servers), and the target number to be 201. When you enable Always Forward on the IP phone, the IP phone sends *78201 to the server, and then the server will enable Always Forward feature on the server side, hence being able to get the right status of the extension.

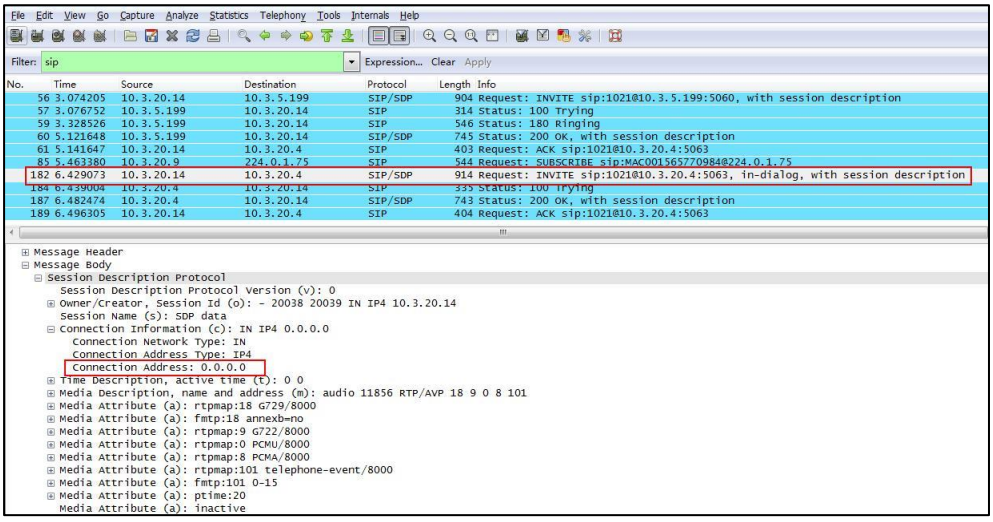
For anonymous call/anonymous call rejection feature, the phone will send either the on code or off code to the server according to the value of Send Anonymous Code/Send Rejection Code. For more information, refer to Anonymous Call on page 305 and Anonymous Call Rejection on page 309.

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.



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.



For more information on RFC 2543 hold feature, refer to Call Hold on page 337. For more

information on capturing packets, refer to Capturing Packets on page 735.

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 computers, 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, computer 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.

PnP (Plug and Play)**--**a term used to describe the characteristic of a computer bus, or device specification, which facilitates the discovery of a hardware component in a system, without the need for physical device configuration, or user intervention in resolving resource conflicts.

ROM (Read-only Memory)**--**a class of storage medium used in computers 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.

Appendix B: Time Zones

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), United States-MST no DST, United States-Mountain Time
-6	Canada-Manitoba(Winnipeg), Chile(Easter Islands), Mexico(Mexico City,Acapulco), United States-Central Time
-5	Bahamas(Nassau), Canada(Montreal,Ottawa,Quebec), Cuba(Havana), United States-Eastern Time
-4:30	Venezuela(Caracas)
-4	Canada(Halifax,Saint John), Chile(Santiago), Paraguay(Asuncion), United Kingdom-Bermuda(Bermuda), United Kingdom(Falkland Islands), Trinidad&Tobago
-3:30	Canada-New Foundland(St.Johns)
-3	Argentina(Buenos Aires), Brazil(DST), Brazil(no DST), Denmark-Greenland(Nuuk)
-2:30	Newfoundland and Labrador
-2	Brazil(no DST)
-1	Portugal(Azores)
0	Denmark-Faroe Islands(Torshavn), GMT, Greenland, Ireland(Dublin), Morocco, Portugal(Lisboa,Porto,Funchal), Spain-Canary Islands(Las Palmas), United Kingdom(London)
+1	Albania(Tirane), Austria(Vienna), Belgium(Brussels), Caicos, Chad, Croatia(Zagreb), Czech Republic(Prague), Denmark(Kopenhagen), France(Paris), Germany(Berlin), Hungary(Budapest), Italy(Rome), Luxembourg(Luxembourg), Macedonia(Skopje), Namibia(Windhoek), Netherlands(Amsterdam), Spain(Madrid)
+2	Estonia(Tallinn), Finland(Helsinki), Gaza Strip(Gaza), Greece(Athens), Israel(Tel Aviv), Jordan(Amman), Latvia(Riga), 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)

Time Zone	Time Zone Name
+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), Singapore(Singapore)
+8:45	Eucla
+9	Japan(Tokyo), Korea(Seoul), Russia(Yakutsk,Chita)
+9:30	Australia(Adelaide), Australia(Darwin)
+10	Australia(Brisbane), Australia(Hobart), 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 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 Certification Authority
- GeoTrust Primary Certification Authority G2
- GeoTrust Universal CA
- GeoTrust Universal CA2
- Thawte Personal Freemail CA
- Thawte Premium Server CA

- Thawte Primary Root CA
- Thawte Primary Root CA - G2
- Thawte Primary Root CA - G3
- 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
- ISRG Root X1 (Let's Encrypt Authority X1 and Let's Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)
- Baltimore CyberTrust Root
- DST Root CA X3
- Verizon Public SureServer CA G14-SHA2
- AddTrust External CA Root
- Go Daddy Class 2 Certification Authority
- Class 2 Primary CA
- Cybertrust Public SureServer SV CA
- DigiCert Assured ID Root G2
- DigiCert Assured ID Root G3
- DigiCert Assured ID Root CA
- DigiCert Global Root G2
- DigiCert Global Root G3
- DigiCert Global Root CA
- DigiCert Trusted Root G4
- Entrust Root Certification Authority
- Entrust Root Certification Authority - G2
- Entrust.net Certification Authority (2048)
- GeoTrust Primary Certification Authority - G3

- GlobalSign Root CA
- GlobalSign
- Starfield Root Certificate Authority - G2
- TC TrustCenter Class 2 CA II
- TC TrustCenter Class 3 CA II
- TC TrustCenter Class 4 CA II
- TC TrustCenter Universal CA I
- TC TrustCenter Universal CA III
- Thawte Universal CA Root
- VeriSign Class 3 Secure Server CA - G2
- VeriSign Class 3 Secure Server CA – G3
- Thawte SSL CA
- StartCom Certification Authority
- StartCom Certification Authority G2
- Starfield Services Root Certificate Authority - G2
- RapidSSL CA
- Go Daddy Root Certificate Authority - G2
- Cybertrust Global Root
- COMODOSSLCA
- COMODO RSA Domain Validation Secure Server CA
- COMODO RSA Certification Authority
- AmazonRootCA4
- AmazonRootCA3
- AmazonRootCA2
- AmazonRootCA1
- Yealink Root CA
- Yealink Equipment Issuing CA
- (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
- AAA Certificate Services
- AC Raíz Certicámara S.A.
- ACCVRAIZ1
- ACEDICOM Root
- Actalis Authentication Root CA
- AddTrust Class 1 CA Root
- AddTrust Public CA Root
- AddTrust Qualified CA Root
- AffirmTrust Commercial

- AffirmTrust Networking
- AffirmTrust Premium
- AffirmTrust Premium ECC
- America Online Root Certification Authority 1
- America Online Root Certification Authority 2
- ApplicationCA
- Atos TrustedRoot 2011
- A-Trust-nQual-03
- Autoridad de Certificacion Firmaprofesional CIF A62634068
- Buypass Class 2 CA 1
- Buypass Class 2 Root CA
- Buypass Class 3 CA 1
- Buypass Class 3 Root CA
- CA Disig
- CA Disig Root R1
- CA Disig Root R2
- Certigna
- Certinomis - Autorité Racine
- certSIGN ROOT CA
- Certum CA
- Certum Trusted Network CA
- Chambers of Commerce Root
- Chambers of Commerce Root - 2008
- China Internet Network Information Center EV Certificates Root
- CNNIC ROOT
- COMODO Certification Authority
- COMODO ECC Certification Authority
- ComSign Secured CA
- DST ACES CA X6
- D-TRUST Root Class 3 CA 2 2009
- D-TRUST Root Class 3 CA 2 EV 2009
- EBG Elektronik Sertifika Hizmet Sağlayıcısı
- EC-ACC
- EE Certification Centre Root CA
- e-Guven Kok Elektronik Sertifika Hizmet Saglayicisi
- Entrust Root Certification Authority - EC1
- Entrust.net Secure Server Certification Authority

- ePKI Root Certification Authority
- E-Tugra Certification Authority
- FNMT Clase 2 CA
- Global Chambersign Root
- Global Chambersign Root – 2008
- GlobalSign Root CA - R3
- Government Root Certification Authority
- GTE CyberTrust Global Root
- Hellenic Academic and Research Institutions RootCA 2011
- Hongkong Post Root CA 1
- IGC/A
- Izenpe.com
- Juur-SK
- KISA RootCA 1
- KISA RootCA 3
- Microsec e-Szigno Root CA
- Microsec e-Szigno Root CA 2009
- NetLock Arany (Class Gold) Főtanúsítvány
- NetLock Expressz (Class C) Tanusitvanykiado
- NetLock Kozjegyzoi (Class A) Tanusitvanykiado
- NetLock Uzleti (Class B) Tanusitvanykiado
- Network Solutions Certificate Authority
- OISTE WISeKey Global Root GA CA
- QuoVadis Root CA 2
- QuoVadis Root CA 3
- QuoVadis Root Certification Authority
- Root CA Generalitat Valenciana
- RSA Security 2048 V3
- Secure Certificate Services
- Secure Global CA
- SecureSign RootCA11
- SecureTrust CA
- Security Communication EV RootCA1
- Security Communication RootCA1
- Security Communication RootCA2
- Sonera Class2 CA
- Staat der Nederlanden Root CA

- Staat der Nederlanden Root CA - G2
- Starfield Class 2 Certification Authority
- Swisscom Root CA 1
- Swisscom Root CA 2
- Swisscom Root EV CA 2
- SwissSign Gold CA - G2
- SwissSign Silver CA - G2
- TDC Internet Root CA
- TeliaSonera Root CA v1
- Trusted Certificate Services
- Trustis FPS Root CA
- T-TeleSec GlobalRoot Class 3
- TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3
- TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (c) Aralık 2007
- TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. (c) Kasım 2005
- TWCA Global Root CA
- TWCA Root Certification Authority
- UTN - DATACorp SGC
- UTN-USERFirst-Hardware
- ValiCert Class 1 Policy Validation Authority
- ValiCert Class 2 Policy Validation Authority
- ValiCert Class 3 Policy Validation Authority
- Visa eCommerce Root
- Wells Fargo Root Certificate Authority
- WellsSecure Public Root Certificate Authority
- XRamp Global 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 (TLS) on page 698.

Appendix D: Configuring DSS Keys

This section provides the DSS key parameters you can configure on IP phones. DSS key consists of line key, programable key and ext key.

The following table lists the number of DSS keys you can configure for each phone model:

Phone Model	Line Key	Programable Key	Ext Key
SIP-T58V/T58A/T56A	27	3	60
CP960	30	0	0

Note The programable key takes effect only if the IP phone is idle.
The ext key takes effect only if the expansion module is connected to the IP phone.

The following tables list relationship between the values of X in the following parameters and programable keys for each phone model.

X ranges from 12 to 14.

programablekey.X.type =

programablekey.X.line =

programablekey.X.value =

programablekey.X.xml_phonebook =

programablekey.X.history_type =

programablekey.X.pickup_value =

X \ Phone Model	SIP-T58V/T58A/T56A
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	Hold
13	Mute
14	Tran

DSS key can be assigned with various key features. The parameters of the DSS key are detailed in the following:

Parameter linekey.X.type	**Configuration File** <y0000000000xx>.cfg
Parameter programablekey.X.type	
Parameter- expansion_module.X.key.Y.type	
Description	Configures key feature for the DSS key. **For line keys**: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **For programable keys** (not applicable to CP960 IP phones): X ranges from 12 to 14 **For ext keys** (not applicable to CP960 IP phones): X ranges from 1 to 3, Y ranges from 1 to 60 **For line keys:** **Valid types are:** **0**-N/A **1**-Conference (not applicable to CP960 IP phones) **2**-Forward **3**-Transfer (not applicable to CP960 IP phones) **4**-Hold (not applicable to CP960 IP phones) **5**-DND **7**-ReCall **9**-Direct Pickup **10**-Call Park **11**-DTMF **12**-Voice Mail **13**-Speed Dial **14**-Intercom **15**-Line **16**-BLF **17**-URL **18**-Group Listening (not applicable to CP960 IP

	phones) **20**-Private Hold **22**-XML Group **23**-Group Pickup **24**-Multicast Paging **25**-Record **34**-Hot Desking **35**-URL Record **38**-LDAP **39**-BLF List **40**-Prefix **41**-Zero Touch **45**-Local Group **50**-Phone Lock **61**-Directory **66**-Paging List **77**-Mobile Account **For programable keys:** **Valid types are:** **0**-N/A **2**-Forward **5**-DND **7**-ReCall **9**-Direct Pickup **13**-Speed Dial **20**-Private Hold **22**-XML Group **23**-Group Pickup **28**-History **30**-Menu **33**-Status **34**-Hot Desking **38**-LDAP **41**-Zero Touch **43**-Local Directory **45**-Local Group **47**-XML Directory

	51-Switch Account Up **52**-Switch Account Down **61**-Directory **66**-Paging List **77**-Mobile Account **For ext keys:** **Valid types are:** **0**-NA **1**-Conference **2**-Forward **3**-Transfer **4**-Hold **5**-DND **7**-ReCall **9**-Direct Pickup **10**-Call Park **11**-DTMF **12**-Voice Mail **13**-Speed Dial **14**-Intercom **15**-Line **16**-BLF **17**-URL **18**-Group Listening **20**-Private Hold **22**-XML Group **23**-Group Pickup **24**-Multicast Paging **25**-Record **34**-Hot Desking **35**-URL Record **38**-LDAP **39**-BLF List **40**-Prefix **41**-Zero Touch **45**-Local Group **50**-Phone Lock

	61-Directory **66**-Paging List **77**-Mobile Account
Format	Integer
Default Value	**For line keys**: **For SIP-T58V/T58A/T56A IP phones:** The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0. **For CP960 IP phones:** The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0. **For programable keys**: When X=12, the default value is 0 (NA). When X=13, the default value is 0 (NA). When X=14, the default value is 2 (Forward). **For ext keys**: When Y=1-60, the default value is 0 (NA).
Range	Valid values are: **0**-N/A **1**-Conference **2**-Forward **3-**Transfer **4**-Hold **5**-DND **7**-ReCall **8**-SMS **9**-Direct Pickup **10**-Call Park **11**-DTMF **12**-Voice Mail **13**-Speed Dial **14**-Intercom **15**-Line **16**-BLF **17**-URL **18**-Group Listening **20**-Private Hold

	22-XML Group **23**-Group Pickup **24**-Multicast Paging **25**-Record **28**-History **30**-Menu **33**-Status **34**-Hot Desking **35**-URL Record **38**-LDAP **39**-BLF List **40-**Prefix **41**-Zero Touch **43**-Local Directory **45**-Local Group **47-**XML Directory **50**-Phone Lock **51**-Switch Account Up **52**-Switch Account Down **61**-Directory **66**-Paging List **77**-Mobile Account
Example	linekey.1.type = 8

Parameter- linekey.X.line	**Configuration File** <y0000000000xx>.cfg
Parameter- programablekey.X.line	
Parameter- expansion_module.X.key.Y.line	
Description	Configures the desired line to apply the key feature. **For line keys**: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **For programable keys** (not applicable to CP960 IP

	phones): X ranges from 12 to 14 **For ext keys** (not applicable to CP960 IP phones): X ranges from 1 to 3, Y ranges from 1 to 60
Format	Integer
Default Value	For the programable key and ext key, the default value is not applicable. For the line key, when X=1, the default value is 1. When X=2, the default value is 2. When X=3 the default value is 3 … When X=16 the default value is 16.
Range	**Permitted Values**: 1 to 16 (for SIP-T58V/T58A/T56A) 1 (for CP960) 1-Line 1 2-Line 2 … 16-Line 16
Example	linekey.1.line = 2

Parameter- linekey.X.value	**Configuration File** <y0000000000xx>.cfg
Parameter- programablekey.X.value	
Parameter- expansion_module.X.key.Y.value	
Description	Configures the value for some key features. **For line keys**: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **For programable keys** (not applicable to CP960 IP phones): X ranges from 12 to 14 **For ext keys** (not applicable to CP960 IP phones): X ranges from 1 to 3, Y ranges from 1 to 60

Format	String
Default Value	Blank
Range	String within 99 characters
Example	When you assign the Speed Dial to the line key, this parameter is used to specify the number you want to dial out. linekey.1.value = 1001

Parameter- linekey.X.label	**Configuration File** <y0000000000xx>.cfg
Parameter- expansion_module.X.key.Y.label	
Description	(Optional.) Configures the label displaying on the touch screen for each line key and each soft key. This is an optional configuration. **For line keys**: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **For ext keys** (not applicable to CP960 IP phones): X ranges from 1 to 3, Y ranges from 1 to 60
Format	String
Default Value	Blank
Range	String within 99 characters
Example	linekey.1.label = Dir

Parameter- linekey.X.pickup_value	**Configuration File** <y0000000000xx>.cfg
Parameter- expansion_module.X.key.Y.pickup_value	
Description	Configures the pickup code for BLF feature. This parameter is only applicable to BLF feature. **For line keys**: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960)

	For ext keys (not applicable to CP960 IP phones): X ranges from 1 to 3, Y ranges from 1 to 60
Format	String
Default Value	Blank
Range	String within 256 characters
Example	linekey.1.pickup_value = *88

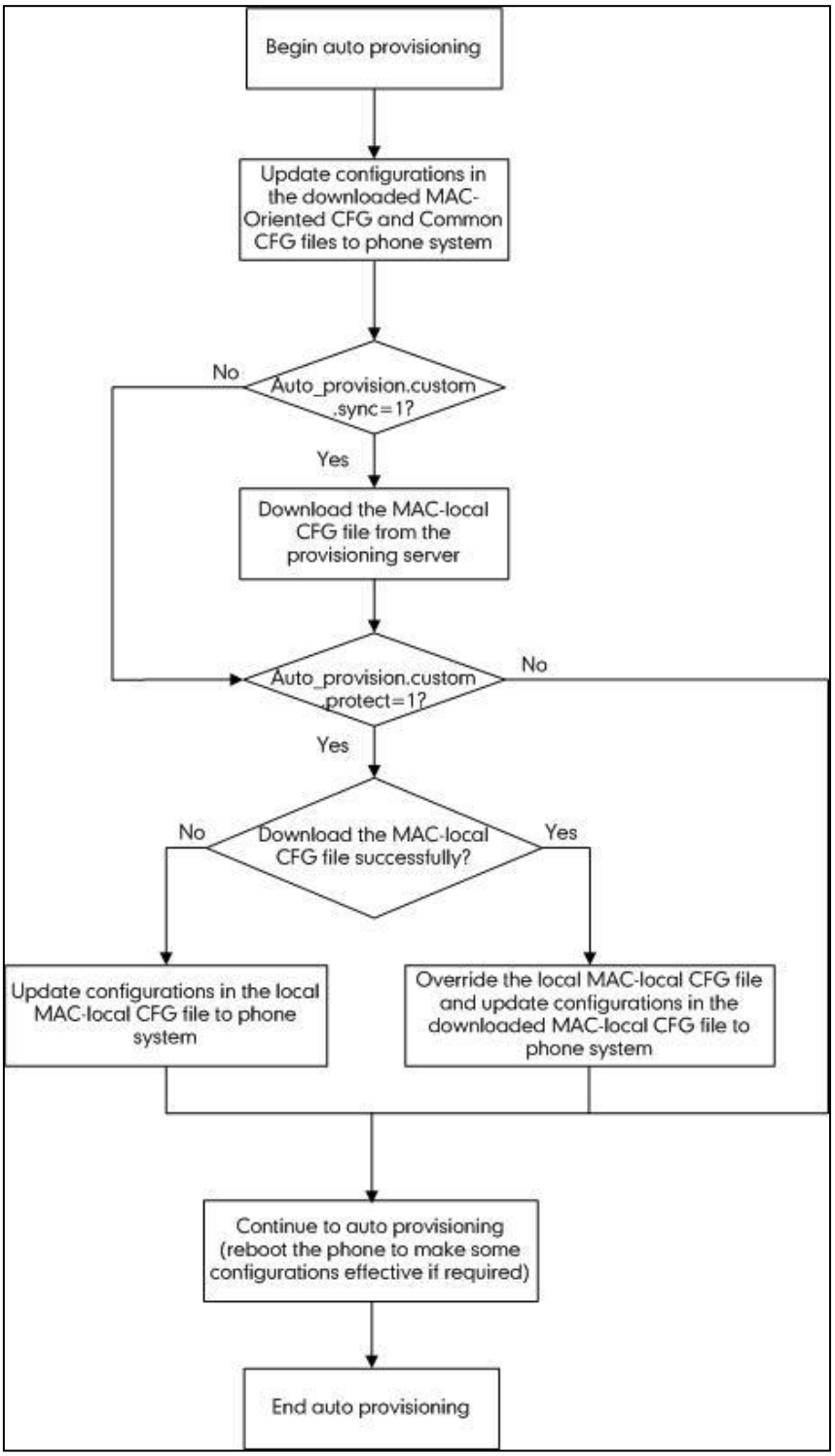
Parameter- linekey.X.xml_phonebook	**Configuration File** <y0000000000xx>.cfg
Parameter- programablekey.X.xml_phonebook	
Parameter- expansion_module.X.key.Y.xml_phonebook	
Description	Configures the desired group or remote phone book when multiple groups or remote phone books are configured on the IP phone. This parameter is only applicable to Local Group/XML Group features. **For line keys**: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **For programable keys** (not applicable to CP960 IP phones): X ranges from 12 to 14 **For ext keys** (not applicable to CP960 IP phones): X ranges from 1 to 3, Y ranges from 1 to 60
Format	Integer
Default Value	0
Range	0 to 48
Example	Configures the second remote phone book. linekey.1.xml_phonebook = 1

Parameter- linekey.X.extension	**Configuration File** <y0000000000xx>.cfg

Parameter- expansion_module.X.key.Y.extension	
Description	Configures the channel of multicast paging group This parameter is only applicable to multicast paging features. **For line keys**: X ranges from 1 to 27 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960) **For ext keys** (not applicable to CP960 IP phones): X ranges from 1 to 3, Y ranges from 1 to 60
Format	Integer
Default Value	0
Range	0 to 48
Example	Configures the second remote phone book. linekey.1.extension= 1

Appendix E: Auto Provisioning Flowchart (Keep User Personalized Configuration Settings)

The following shows auto provisioning flowchart for Yealink IP phones when a user wishes to keep user personalized configuration settings.



Appendix F: Static Settings

You may need to know the differences between the parameters started with "static." and other common parameters:

- All static settings have no priority. They take effect no matter what method (web user interface or phone user interface or configuration files) you are using for provisioning.
- All static settings are never be saved to <MAC>-local.cfg file.
- All static settings are not affected by the overwrite mode. That is, the actual values will not be changed even if you delete the parameters associated with static settings, or you clear the values of the parameters associated with static settings in the configuration files.

The following table lists all static settings:

Function	Parameters
Network	static.network.ip_address_mode
	static.network.ipv6_prefix
	static.network.ipv6_internet_port.type
	static.network.ipv6_internet_port.ip
	static.network.ipv6_internet_port.gateway
	static.network.ipv6_primary_dns
	static.network.ipv6_secondary_dns
	static.network.ipv6_icmp_v6.enable
	static.network.internet_port.type
	static.network.internet_port.ip
	static.network.internet_port.mask
	static.network.internet_port.gateway
	static.network.primary_dns
	static.network.secondary_dns
	static.network.dhcp_host_name
	static.network.pppoe.user
	static.network.pppoe.password
	static.network.pc_port.enable
	static.network.internet_port.speed_duplex
	static.network.pc_port.speed_duplex

Function	Parameters
	static.network.static_dns_enable
	static.network.ipv6_static_dns_enable
	static.network.vlan.pc_port_mode
	static.network.dns.ttl_enable
	static.network.dhcp.server_mac1
	static.network.dhcp.server_mac2
	static.network.mtu_value
	static.network.vlan.internet_port_enable
	static.network.vlan.internet_port_vid
	static.network.vlan.internet_port_priority
	static.network.vlan.pc_port_enable
	static.network.vlan.pc_port_vid
	static.network.vlan.pc_port_priority
	static.network.vlan.dhcp_enable
	static.network.vlan.dhcp_option
	static.network.vlan.vlan_change.enable
	static.network.port.http
	static.network.port.https
	static.network.qos.signaltos
	static.network.qos.audiotos
	static.network.qos.videotos
	static.wifi.802_11e.enable
	static.network.802_1x.mode
	static.network.802_1x.identity
	static.network.802_1x.md5_password
	static.network.802_1x.root_cert_url
	static.network.802_1x.client_cert_url
	static.network.802_1x.proxy_eap_logoff.enable
	static.network.vpn_enable

Function	Parameters
	static.openvpn.url
	static.network.lldp.enable
	static.network.lldp.packet_interval
	static.network.span_to_pc_port
	static.network.cdp.enable
	static.network.cdp.packet_interval
Wi-Fi	static.wifi.enable
Autoprovision	static.auto_provision.power_on
	static.auto_provision.attempt_before_failed
	static.auto_provision.retry_delay_after_file_transfer_failed
	static.auto_provision.server.type
	static.auto_provision.user_agent_mac.enable
	static.auto_provision.dns_resolv_nosys
	static.auto_provision.dns_resolv_nretry
	static.auto_provision.dns_resolv_timeout
	static.auto_provision.custom.sync
	static.auto_provision.custom.sync.path
	static.auto_provision.custom.protect
	static.auto_provision.custom.upload_method
	static.auto_provision.attempt_expired_time
	static.network.attempt_expired_time
	static.auto_provision.reboot_force.enable
	static.auto_provision.pnp_enable
	static.auto_provision.dhcp_option.enable
	static.auto_provision.dhcp_option.list_user_options
	static.auto_provision.dhcp_option.option60_value
	static.auto_provision.repeat.enable
	static.auto_provision.repeat.minutes
	static.auto_provision.weekly.enable

Function	Parameters
	static.auto_provision.weekly.dayofweek
	static.auto_provision.weekly.begin_time
	static.auto_provision.weekly.end_time
	static.auto_provision.flexible.enable
	static.auto_provision.flexible.interval
	static.auto_provision.flexible.begin_time
	static.auto_provision.flexible.end_time
	static.auto_provision.server.url
	static.auto_provision.server.username
	static.auto_provision.server.password
	static.auto_provision.update_file_mode
	static.auto_provision.encryption.config
	static.auto_provision.aes_key_in_file
	static.auto_provision.aes_key_16.com
	static.auto_provision.aes_key_16.mac
	static.autoprovision.X.name
	static.autoprovision.X.code
	static.autoprovision.X.url
	static.autoprovision.X.user
	static.autoprovision.X.password
	static.autoprovision.X.com_aes
	static.autoprovision.X.mac_aes
	static.auto_provision.url_wildcard.pn
	static.zero_touch.enable
	static.zero_touch.wait_time
	static.zero_touch.network_fail_wait_times
	static.zero_touch.network_fail_delay_times
	static.features.hide_zero_touch_url.enable
TR069	static.managementserver.enable

Function	Parameters
	static.managementserver.username
	static.managementserver.password
	static.managementserver.url
	static.managementserver.connection_request_username
	static.managementserver.connection_request_password
	static.managementserver.periodic_inform_enable
	static.managementserver.periodic_inform_interval
Security	static.security.user_name.user
	static.security.user_name.admin
	static.security.user_name.var
	static.security.user_password
	static.security.trust_certificates
	static.security.ca_cert
	static.security.dev_cert
	static.security.cn_validation
	static.phone_setting.reserve_certs_enable
3-level Permissions	static.security.var_enable
	static.web_item_level.url
	static.security.default_access_level
Certificates	static.trusted_certificates.url
	static.trusted_certificates.delete
	static.server_certificates.url
	static.server_certificates.delete
Custom Factory Configuration	static.features.custom_factory_config.enable
	static.custom_factory_configuration.url
Custom Configuration	static.configuration.url
	static.custom_mac_cfg.url
Syslog	static.syslog.mode
	static.syslog.server

Function	Parameters
	static.syslog.log_level
	static.syslog.log_upload_period
	static.syslog.ftp.post_mode
	static.syslog.ftp.max_logfile
	static.syslog.ftp.append_limit_mode
	static.syslog.bootlog_upload_wait_time
Watch_dog	static.watch_dog.enable
WEB HTTP(S)	static.wui.https_enable
	static.wui.http_enable
Language	static.lang.wui
	static.lang.gui
Others	static.firmware.url
	static.features.default_account

Appendix G: Reading Icons

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

T58V/A	T56A	CP960	Description
			Network is unavailable
			Private line registers successfully
			Registration failed
(Flashing)	(Flashing)	(Flashing)	Registering
		/	Hands-free (speakerphone) mode
		/	Handset mode
		/	Headset mode
			Voice Mail
			Auto Answer
			Do Not Disturb
			Call Forward
		/	Call Hold (video)
		/	Call Hold (audio-only)
		/	Call Mute
			Keep Mute
		/	Call is encrypted (video)

T58V/A	T56A	CP960	Description
		/	Call is encrypted (audio-only)
			Silent mode
	/	/	Camera is not detected
			Phone Lock
			Received Calls
			Placed Calls
			Missed Calls
			Forwarded Calls
			Recording box is full
			A call cannot be recorded
			Recording starts successfully
			Recording cannot be started
			Recording cannot be stopped
			VPN is enabled
			Bluetooth mode is on
		/	Bluetooth headset is both paired and connected
			Bluetooth-Enabled mobile phone is both paired and connected
			Wi-Fi mode is on
			The default local caller photo and local contact icon
			The default mobile caller photo and mobile contacts icon

T58V/A	T56A	CP960	Description
		/	DSS Key
			Line key type is Line (line is seized)
			Line key type is Speed Dial
			Line key type is Mobile Account (Bluetooth-Enabled mobile phone is connected successfully)
			Line key type is Mobile Account (Bluetooth-Enabled mobile phone connection failed)
(Flashing)	(Flashing)	(Flashing)	Line key type is Mobile Account (Bluetooth-Enabled mobile phone is connecting)
			Line key type is BLF/BLF List (BLF/BLF list idle state)
			Line key type is BLF/BLF List (BLF/BLF list ringing state)
			Line key type is BLF/BLF List (BLF hold state)
			Line key type is BLF/BLF List (BLF/BLF list callout state)
			Line key type is BLF/BLF List (BLF/BLF list failed state)
			Line key type is BLF/BLF List (BLF list call park state)
			Line key type is Voice Mail
			Line key type is Direct Pickup
			Line key type is Group Pickup
			Line key type is Call Park (park successfully/call park idle state)
			Line key type is Call Park (call park ringing state)
			Park failed
			Line key type is Intercom (intercom idle state)

T58V/A	T56A	CP960	Description
			Line key type is Intercom (intercom ringing state)
Callout	Callout	Callout	Line key type is Intercom (intercom callout state)
Talking	Talking	Talking	Line key type is Intercom (intercom talking state)
			Line key type is Intercom (intercom failed state)
			Line key type is DTMF/Prefix
			Line key type is Local Group/XML Group/LDAP
		/	Line key type is Conference
			Line key type is Forward
		/	Line key type is Transfer
		/	Line key type is Hold
			Line key type is DND
			Line key type is Recall
			Line key type is Record/URL Record
			Line key type is Record/URL Record (recording starts successfully)
			Line key type is Multicast Paging/Group Listening (Group Listening is not applicable CP960 IP phones)
			Line key type is Hot Desking
			Line key type is Zero Touch
			Line key type is URL
			The shared line/bridged line is idle
			The shared line receives ring-back tone

T58V/A	T56A	CP960	Description
(Flashing)	(Flashing)	(Flashing)	
(Flashing)	(Flashing)	(Flashing)	The shared line receives an incoming call
			The shared line is in conversation
			The shared line conversation is placed on public hold
			USB flash drive is detected
			High Definition Voice
		/	Screenshot captured
		/	Downloading file
		/	Uploading file
		/	Upcoming alarm
		/	Unread email

Appendix H: 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

The following SIP request messages are supported:

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	

Method	Supported	Notes
PUBLISH	Yes	

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	

Method	Supported	Notes
RAck	Yes	
Record-Route	Yes	
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	
To	Yes	
User-Agent	Yes	
Via	Yes	

SIP Responses

The following SIP responses are supported:

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.

1xx Responses—Provisional

1xx Response	Supported	Notes
100 Trying	Yes	
180 Ringing	Yes	
181 Call Is Being Forwarded	Yes	
182 Queued	Yes	
183 Session Progress	Yes	

2xx Responses—Successful

2xx Response	Supported	Notes
200 OK	Yes	
202 Accepted	Yes	In REFER transfer.

3xx Responses—Redirection

3xx Response	Supported	Notes
300 Multiple Choices	Yes	
301 Moved Permanently	Yes	
302 Moved Temporarily	Yes	
305 Use Proxy	Yes	
380 Alternative Service	No	

4xx Responses—Request Failure

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	

4xx Response	Supported	Notes
416 Unsupported URI Scheme	No	
420 Bad Extension	No	
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 Responses—Server Failure

5xx Response	Supported	Notes
500 Server Internal Error	Yes	
501 Not Implemented	Yes	
502 Bad Gateway	No	
503 Service Unavailable	Yes	
504 Server Time-out	No	
505 Version Not Supported	No	
513 Message Too Large	No	

6xx Response—Global Failures

6xx Response	Supported	Notes
600 Busy Everywhere	Yes	

6xx Response	Supported	Notes
603 Decline	Yes	
604 Does Not Exist Anywhere	No	
606 Not Acceptable	No	

SIP Session Description Protocol (SDP) Usage

SDP Headers	Supported
v–Session Description Protocol Version	Yes
o–Owner/Creator, Session Id	Yes
a–Media Attribute	Yes
c–Connection Information	Yes
b–Bandwidth Information	Yes
m–Media Description, name and address	Yes
s–Session Name	Yes
t–Time Description, active time	Yes

Appendix I: 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–Provisional Responses

SIP 2xx–Successful Responses

SIP 3xx–Redirection Responses

SIP 4xx–Request Failure Responses

SIP 5xx—Server Failure Responses

SIP 6xx—Global Failures Responses

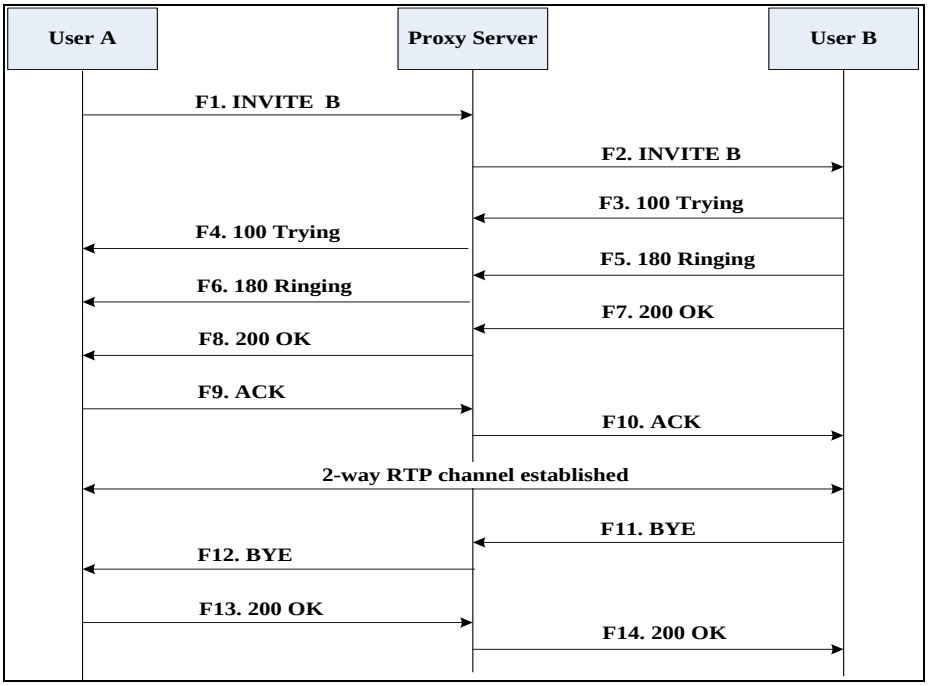
For more information on SIP Responses, refer to SIP Responses on page 803.

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
F1	INVITE—User A to Proxy Server	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. 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

Step	Action	Description
		initiator in the From field. ● 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 server. The ACK confirms that User A has received the 200 OK response. The call session is

Step	Action	Description
		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.

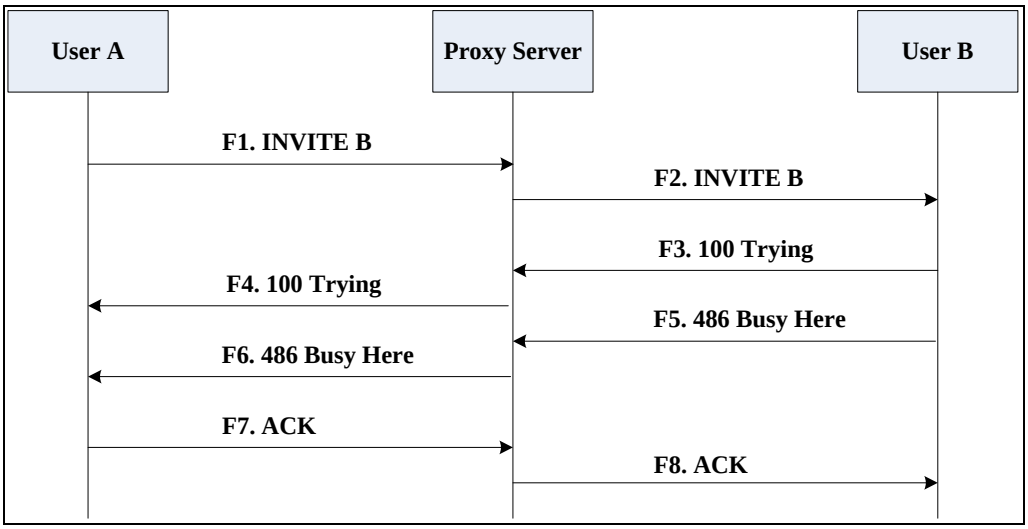
Unsuccessful Call Setup—Called User is Busy

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	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 session initiator in the From field. ● 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. Proxy server forwards 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

Step	Action	Description
		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.

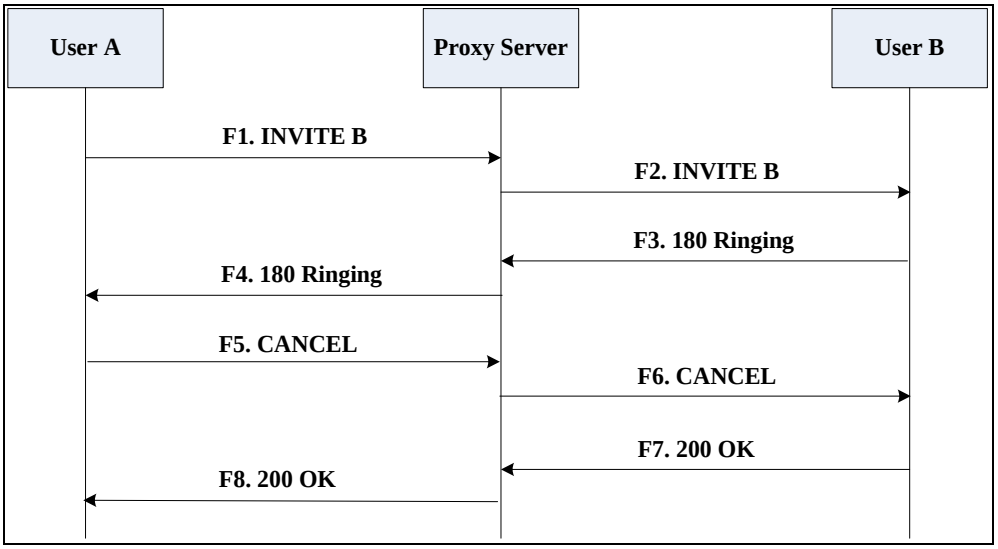
Unsuccessful Call Setup—Called User Does Not Answer

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.

The call flow scenario is as follows:

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
F1	INVITE–User A to Proxy Server	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. ● 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. 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.

Step	Action	Description
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.

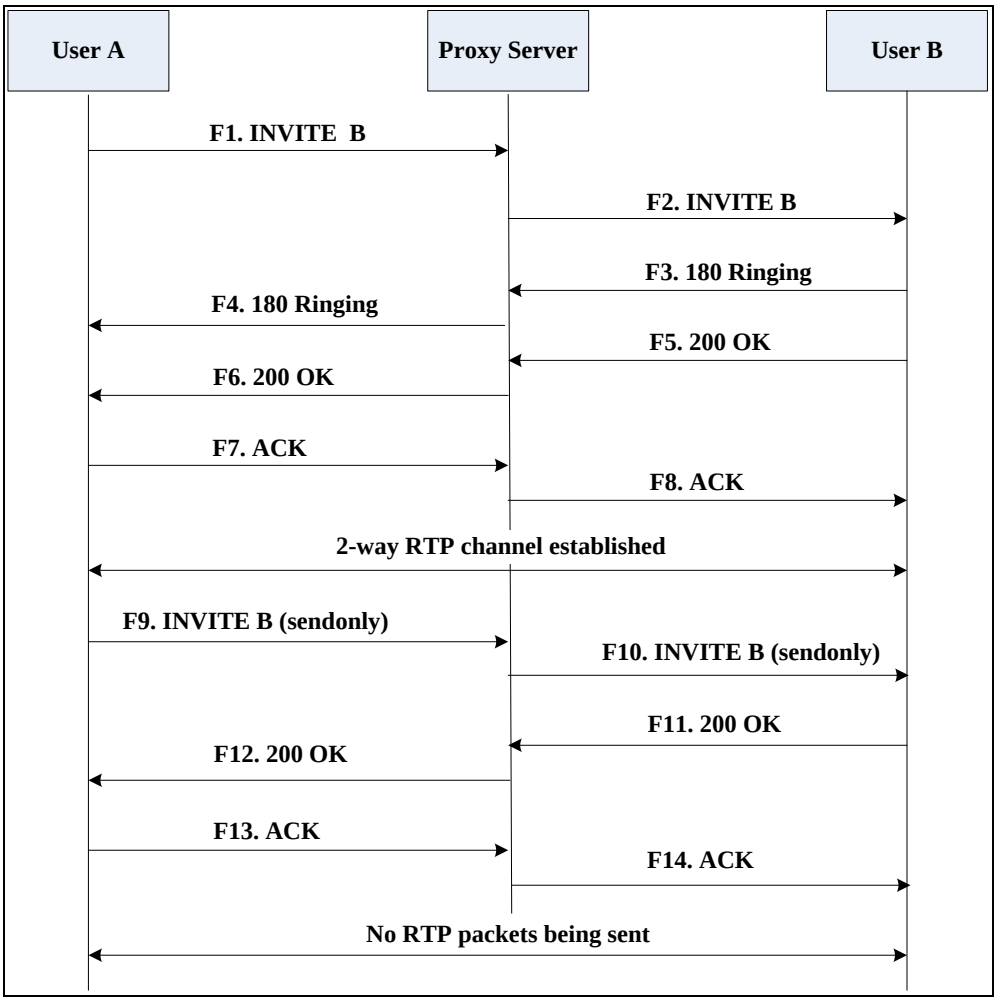
Successful Call Setup and Call Hold

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.

The call flow scenario is as follows:

1. User A calls User B.
2. User B answers the call.

3. User A places User B on hold.



Step	Action	Description
F1	INVITE–User A to Proxy Server	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. ● 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.

Step	Action	Description
		• 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.
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

Step	Action	Description
		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.

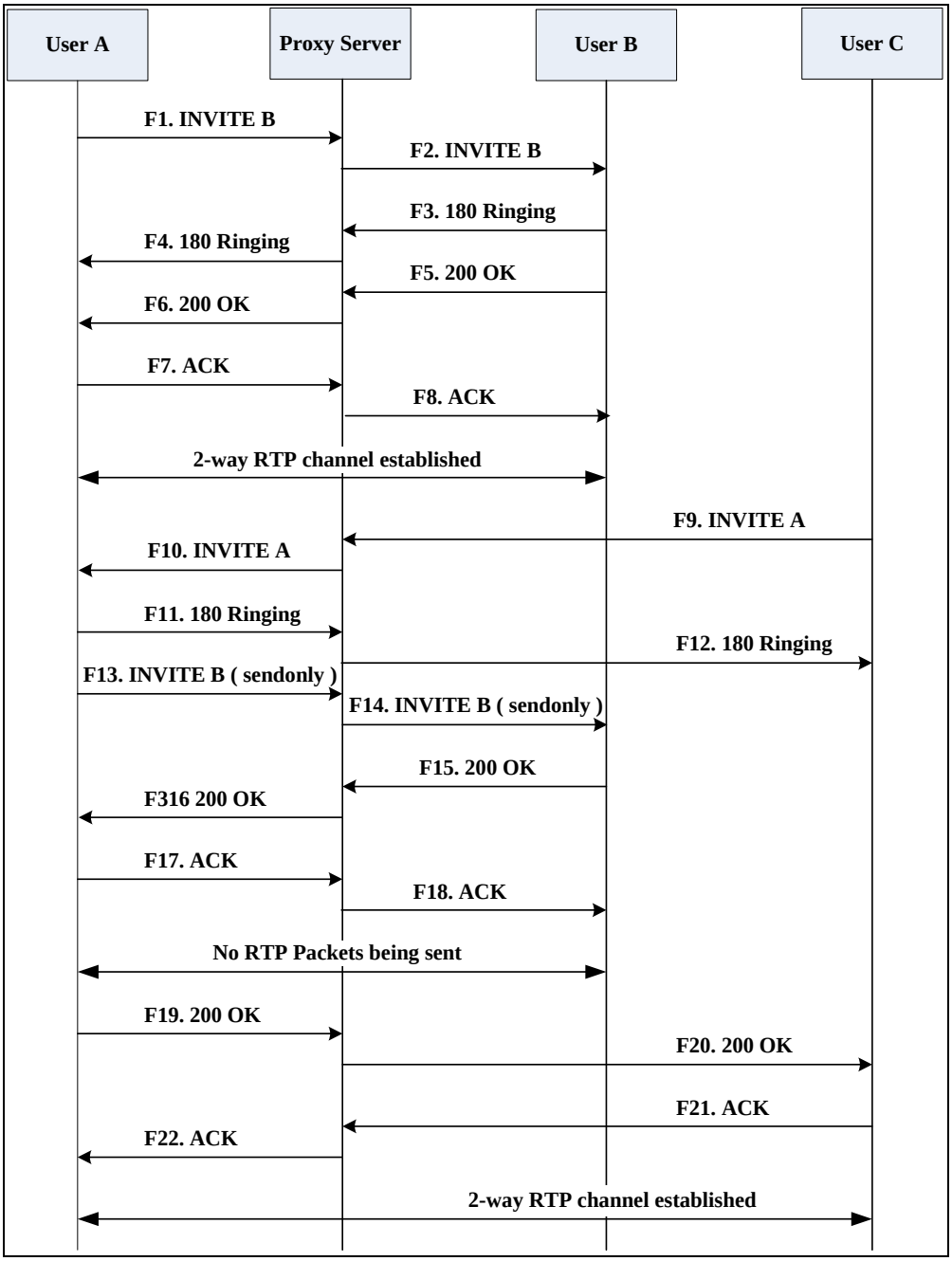
Successful Call Setup and Call Waiting

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.

The call flow scenario is as follows:

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
F1	INVITE–User A to Proxy Server	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.

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	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.
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	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

Step	Action	Description
		session. In the INVITE request: ● The IP address of User A is inserted in the Request-URI field. ● User C is identified as the call session initiator in the From field. ● 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 C is ready to receive is specified. ● The port on which User A is prepared to receive the RTP data is specified.
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.
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

Step	Action	Description
		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.

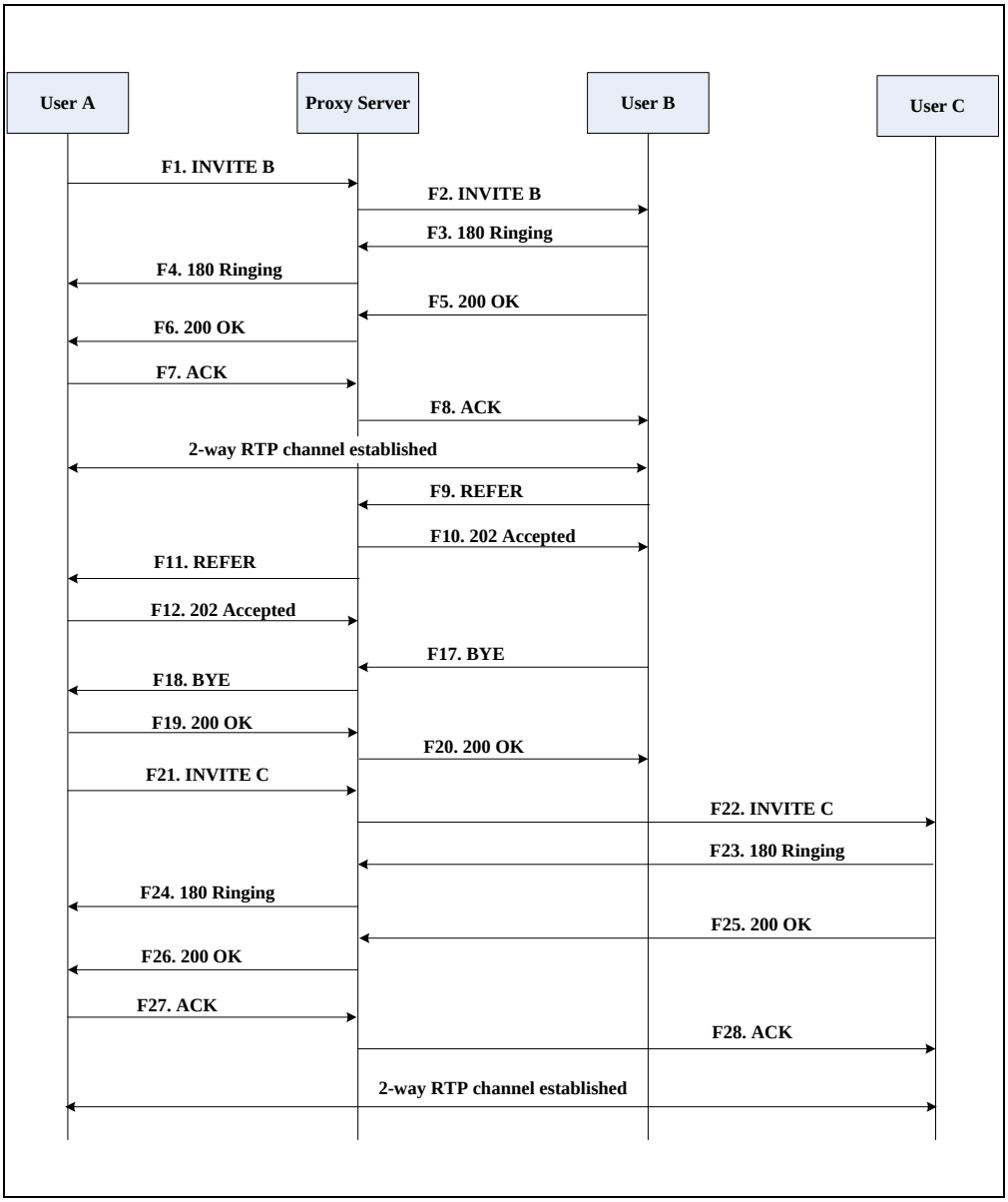
Call Transfer without Consultation

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.

The call flow scenario is as follows:

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.

Call is established between User A and User C.



Step	Action	Description
F1	INVITE–User A to Proxy Server	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. 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. ● A unique numeric identifier is assigned to the call and is inserted in

Step	Action	Description
		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	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.
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

Step	Action	Description
		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.
F14	BYE−Proxy Server to User A	The proxy server forwards the BYE request to User A.
F15	200OK−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	200OK−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.

Step	Action	Description
F22	200OK–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.

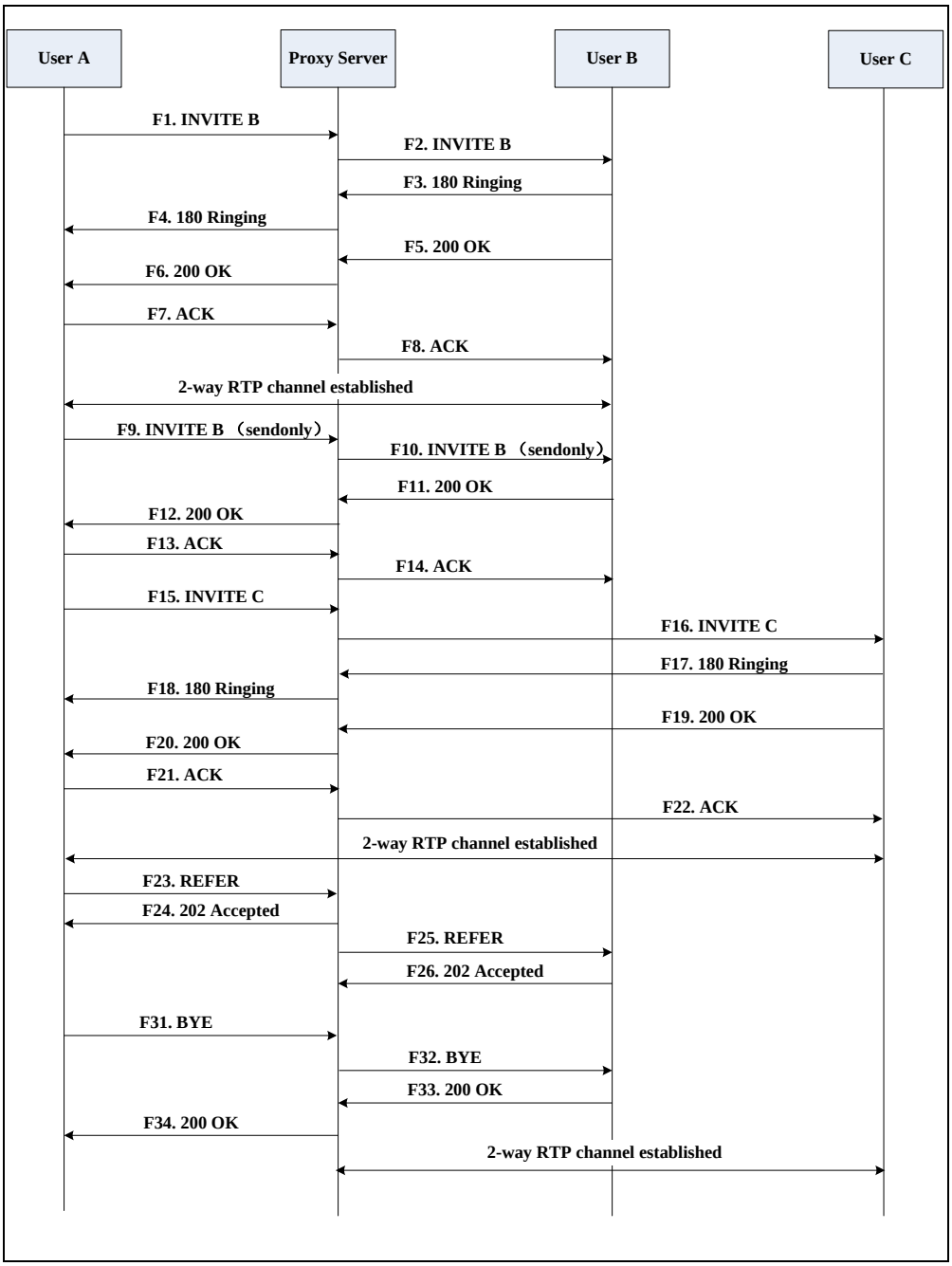
Call Transfer with Consultation

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.

The call flow scenario is as follows:

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
F1	INVITE−User A to Proxy Server	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

Step	Action	Description
		initiator in the From field. ● 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	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.
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

Step	Action	Description
		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 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

Step	Action	Description
		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 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.

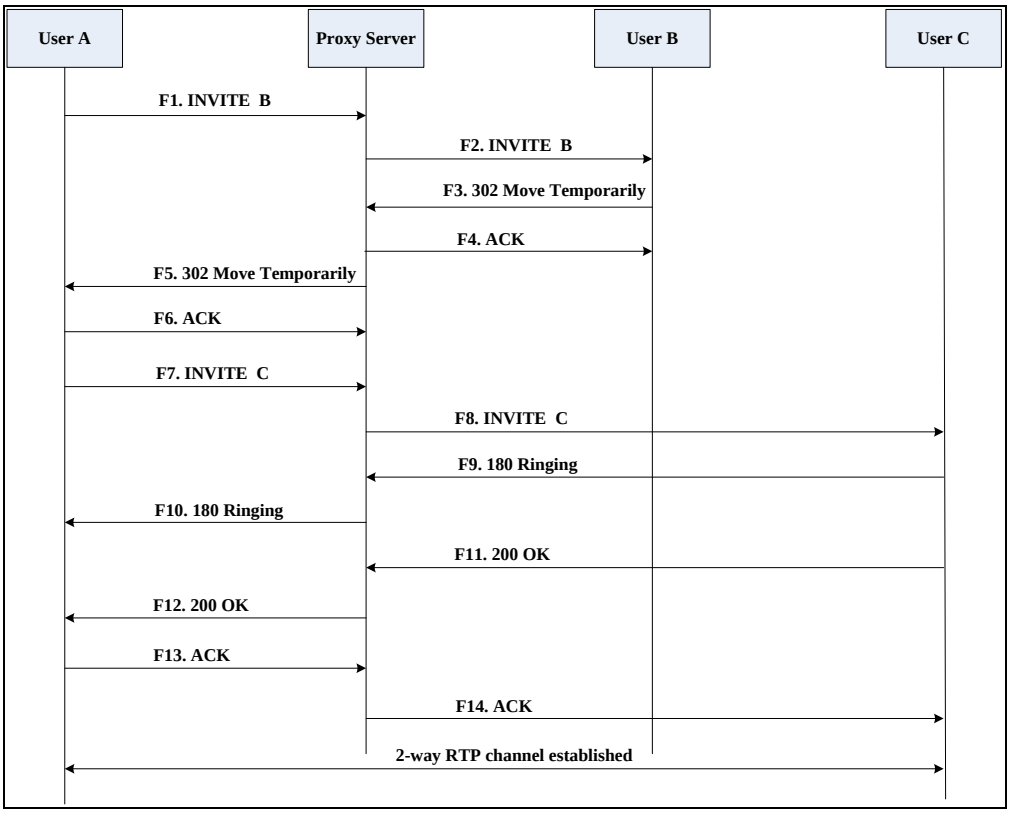
Always Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled always call forward. The incoming call is immediately forwarded to User C when User A calls User B. 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.

The call flow scenario is as follows:

1. User B enables always call forward, and the destination number is User C.
2. User A calls User B.
3. User B forwards the incoming call to User C.
4. User C answers the call.

   Call is established between User A and User C.



Step	Action	Description
F1	INVITE–User A to Proxy Server	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 the User B is inserted in the Request-URI field.

Step	Action	Description
		● User A is identified as the call session initiator in the From field. ● 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	302 Move Temporarily–User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F4	ACK–Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the 302 Move Temporarily message.
F5	302 Move Temporarily–Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F6	ACK–User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the 302 Move Temporarily message.
F7	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 requested the call.
F8	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.
F9	180 Ringing–User C to Proxy	User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response

Step	Action	Description
	Server	indicates that the user is being alerted.
F10	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.
F11	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.
F12	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.
F13	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.
F14	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.

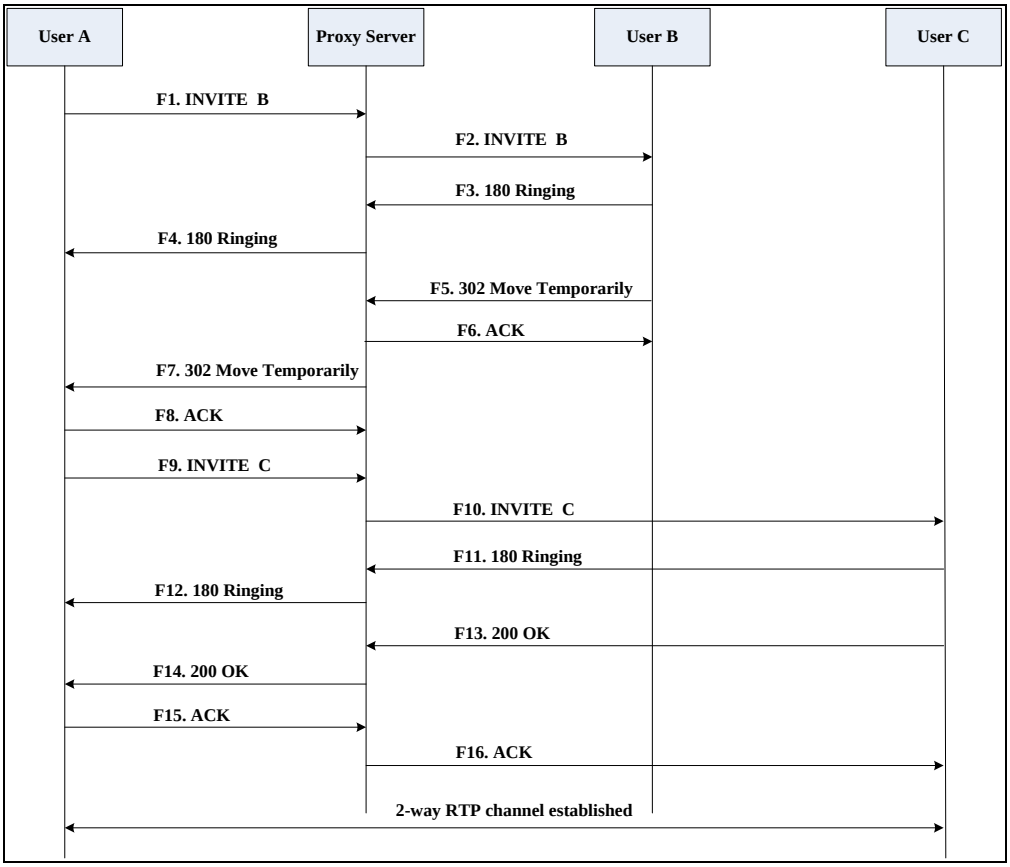
Busy Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled busy call forward. The incoming call is forwarded to User C when User B is busy. 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.

The call flow scenario is as follows:

1. User B enables busy call forward, and the destination number is User C.
2. User A calls User B.
3. User B is busy.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A 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 session initiator in the From field. ● 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.

Step	Action	Description
		• 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	302 Move Temporarily−User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK−Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the ACK message.
F7	302 Move Temporarily−Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK−User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	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.
F10	INVITE−Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	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.
F12	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.

Step	Action	Description
F13	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.
F14	200OK–Proxy Server to User A	The proxy server forwards the SIP 200 OK response to User A.
F15	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.
F16	ACK–Proxy Server to User C	The proxy server sends the ACK message to User C.

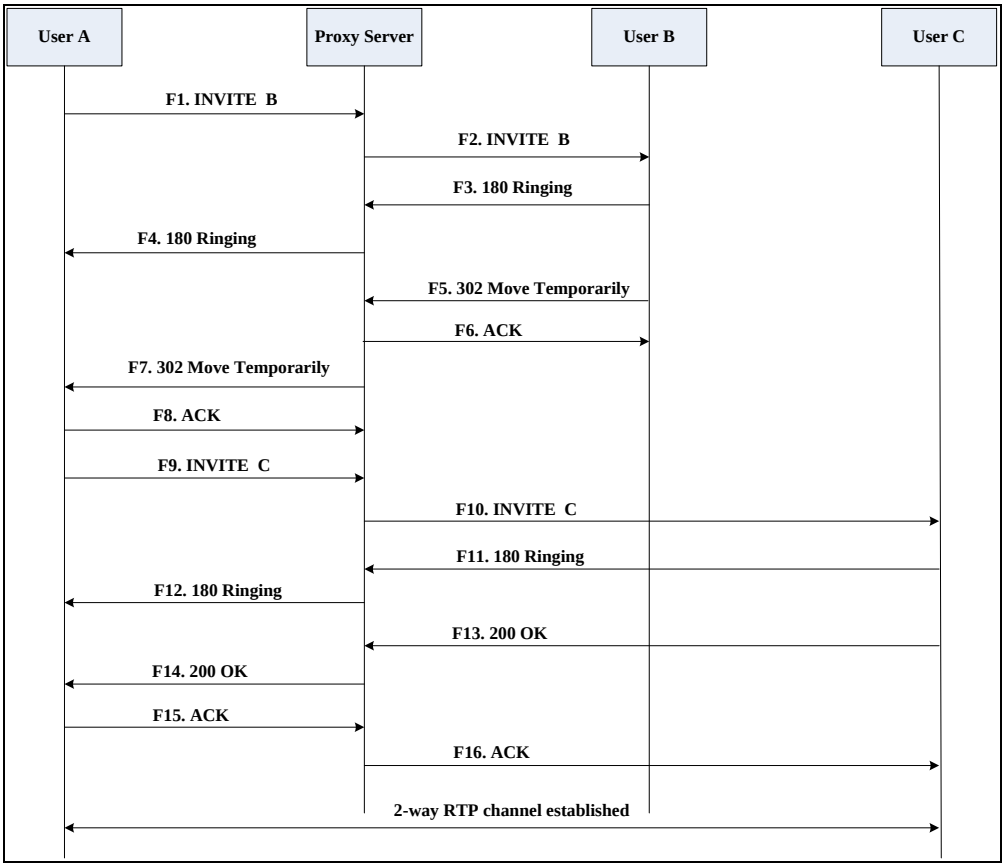
No Answer Call Forward

The following figure illustrates successful call forwarding between Yealink SIP IP phones in which User B has enabled no answer call forward. The incoming call is forwarded to User C when User B does not answer the incoming call after a period of time. 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.

The call flow scenario is as follows:

1. User B enables no answer call forward, and the destination number is User C.
2. User A calls User B.
3. User B does not answer the incoming call.
4. User B forwards the incoming call to User C.
5. User C answers the call.

Call is established between User A 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 session initiator in the From field. ● 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.

Step	Action	Description
		• 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	302 Move Temporarily–User B to Proxy Server	User B sends a SIP 302 Moved Temporarily message to the proxy server. The message indicates that User B is not available at SIP phone B. User B rewrites the contact-URI.
F6	ACK–Proxy Server to User B	The proxy server sends a SIP ACK to User B, the ACK message notifies User B that the proxy server has received the ACK message.
F7	302 Move Temporarily–Proxy Server to User A	The proxy server forwards the 302 Moved Temporarily message to User A.
F8	ACK–User A to Proxy Server	User A sends a SIP ACK to the proxy server. The ACK message notifies the proxy server that User A has received the ACK message.
F9	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.
F10	INVITE–Proxy Server to User C	The proxy server forwards the SIP INVITE request to User C.
F11	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.
F12	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.

Step	Action	Description
F13	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.
F14	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.
F15	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.
F16	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.

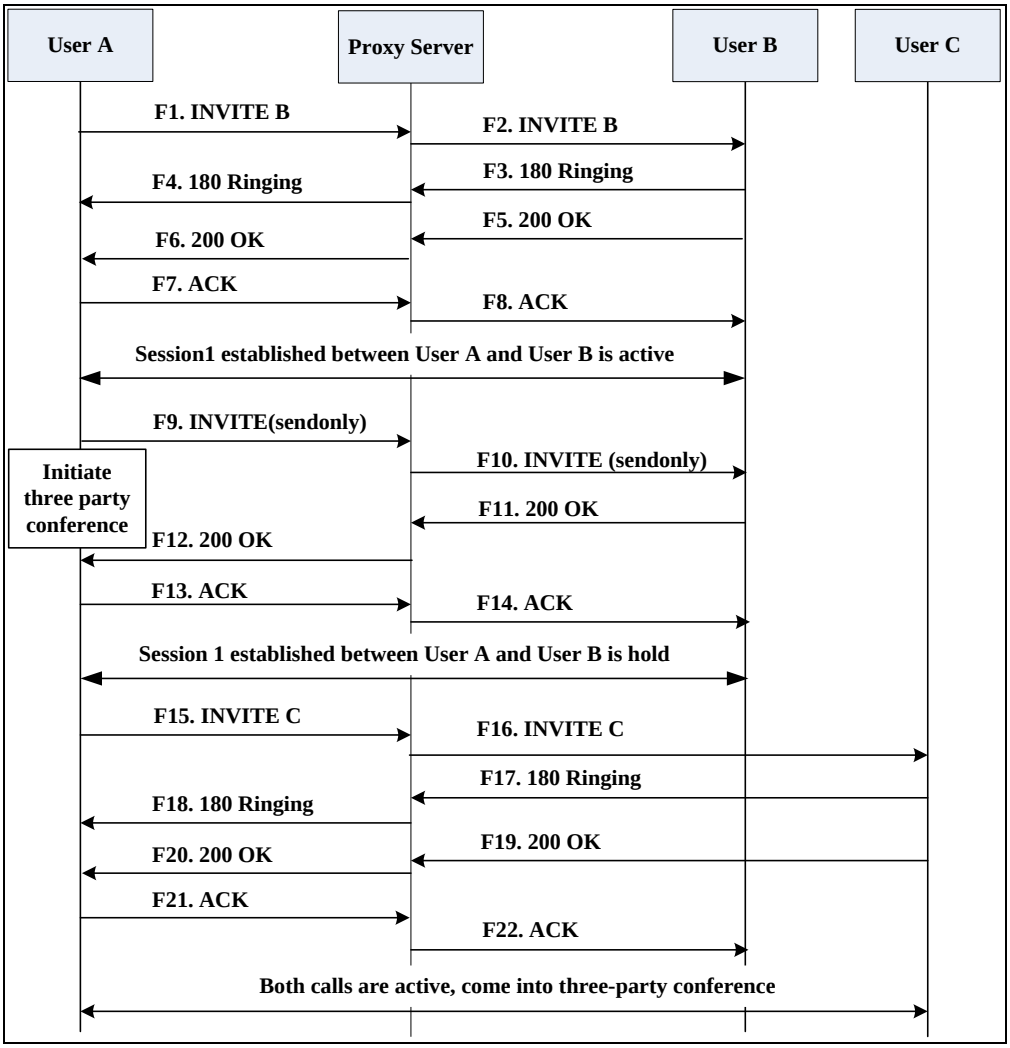
Call Conference

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.

The call flow scenario is as follows:

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 session initiator in the From field. ● A unique numeric identifier is assigned to the call and is inserted in the Call-ID field. ● The transaction number within a

Step	Action	Description
		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. 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.
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

Step	Action	Description
		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 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.

Step	Action	Description
		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

100 Reliable Retransmission 434
180 Ring Workaround 329
802.1X Authentication 99

A

About This Guide v
Accept SIP Trust Server Only 300
Account Registration 172
Acoustic Echo Cancellation (AEC) 642
Action URL 540
Action URI 560
Allow IP Call 299
Always Forward 343
Analyzing Configuration Files 742
Anonymous Call 305
Anonymous Call Rejection 309
Answer By Hand 438
Appendix 767
Appendix A: Glossary 767
Appendix B: Time Zones 769
Appendix C: Trusted Certificates 770
Appendix D: Configuring DSS Keys 775
Appendix E: Auto Provisioning Flowchart 784
Appendix F: Static Settings 787
Appendix G: Reading Icons 793
Appendix H: SIP 798
Appendix I: SIP Call Flows 806
Area Code 238
Attended Transfer 358
Audio Codecs 629
Auto Answer 292
Auto-Logout Time 691
Automatic Gain Control (AGC) 644
Auto Redial 290

B

Backlight 156
Background Noise Suppression (BNS) 643
Blind Transfer 358
Block Out 240
Bluetooth 164
Boot Files, Configuration Files and Resource Files 114
Busy Forward 343
Busy Lamp Field (BLF) 473
Busy Lamp Field (BLF) List 486
Busy Tone Delay 321

C

Call Completion 302
Call Forward 343
Call Hold 337
Call Number Filter 397
Call Park 399
Call Timeout 422
Call Transfer 358
Call Recording Using DSS Keys (Record and URL Record) 524
Call Recording Using Soft Key 439
Call Waiting 286
Calling Line Identification Presentation (CLIP) 403
Central Provisioning 112
Connected Line Identification Presentation (COIP) 407
Capturing Packets 735
Capturing the Current Screen of the Phone 566
CDP 57
Chapters in This Guide v
Comfort Noise Generation (CNG) 645
Common CFG Files 116
Configuration Parameter Table Format ix
Configuring a Provisioning Server 122

Configuring Audio Features 601
Configuring Advanced Features 440
Configuring Basic Features 143
Configuring Video Features 651
Configuring Security Features 689
Connecting the IP phone 10
Conventions Used in Yealink Documentations vii
CSTA Control 450

D

Deploying Phones from the Provisioning Server 123
DHCP 24
DHCP Option 28
Dial Plan 227
Dial-now 232
Dial-now Template File 236
Directed Call Pickup 374
Display Method on Dialing 186
Distinctive Ring Tones 607
Do Not Disturb (DND) 313
Door Phone 441
DTMF 651
Dual Headset 626

E

Early Media 329
Enable Page Tips 168
Encrypting and Decrypting Files 713
Enabling the Watch Dog Feature 740
Emergency Dialplan 251
Expansion Modules 4

F

Feature Key Synchronization 369

G

Getting Information from Status Indicators 741
Getting Information from Talk Statistics 742
Getting Started 9
Group Call Pickup 382

H

H.323 xii
Headset Prior 622
Hide Feature Access Codes 492
Hot Desking 531
Hotline 242

I

Index 843
Initialization Process Overview 18
Intercom 412
Introduction v
IPv6 Support 51
IP Direct Auto Answer 297

J

Jitter Buffer 647

K

Keep User Personalized Settings after Auto Provisioning 132
Key As Send 223
Key Features of IP Phones 4

L

Language 205
Lightweight Directory Access Protocol (LDAP) 461
Live Dialpad 280
LLDP 54
Loading Language Packs 206
Local Conference 366
Local Contact File 268
Local Directory 268
Logon Wizard 536

M

MAC-local CFG File 116
MAC-Oriented CFG File 116
Manual Provisioning 112

Message Waiting Indicator (MWI) 503
Missed Call Log 266
Mobile Account 445
Multicast Paging 508
Multiple Line Keys per Account 180
Music on Hold (MoH) 341
Mute 410

N

NAT Traversal 84
Network Address Translation (NAT) 84
Network Conference 366
No Answer Forward 343
Noise Suppression 651
Notification Popups 149

O

Obtaining Configuration Files and Resource Files 119
Off Hook Hot Line Dialing 258

P

Page Tips for Expansion Module 171
Password Dial 431
Phone User Interface 113
Physical Features of IP Phones 4
Power Indicator LED 145
Power Saving 157
Product Overview 1
Provisioning Methods 110
Provisioning Points to Consider 110

Q

Quality of Service (QoS) 95
Quick Login 449

R

Reading the Configuration Parameter Tables vii
Recommended References xi
Reboot in Talking 436
ReCall 394
Resource Files 116
Redial Tone 601
Related Documentations vi
Remote Phone Book 453
Remote Phone Book Template File 453
Replace Rule 228
Replace Rule Template File 230
Reserve # in User Name 429
Reserved Ports 80
Return Message When DND 313
Return Code When Refuse 327
RFC and Internet Draft Support 798
Ringer Device for Headset 622
Ringing Timeout 422
Ring Tones 601
RTCP-XR 665
Real-Time Transport Protocol (RTP) Ports 592

S

Save Call Log 263
Search Source List in Dialing 260
Secure Real-Time Transport Protocol (SRTP) 709
Semi-attended Transfer 358
Send user=phone 423
Sending Volume 627
Server Redundancy 569
Session Timer 334
Setting Up Your Phone Network 23
Setting Up Your Phones with a Provisioning Server 110
Setting Up Your System 23
Shared Call Appearance (SCA) 494
Silent Mode 440
SIP xiii
SIP Components xiii
SIP Header 802
SIP IP Phone Models 1
SIP Request 801
SIP Responses 803
SIP Send Line 427
SIP Send MAC 425
SIP Session Description Protocol Usage 806
SIP Session Timer 332
Smart Noise Block 652
Softkey Layout 215

Specifying the Language to Use 213
Speed Dial 282
Static DNS 25
STUN 85
Summary Table Format viii
Supported Provisioning Protocols 122
Suppress DTMF Display 659

T

Table of Contents xv
Time and Date 188
Transfer on Conference Hang Up 369
Transfer Mode via Dsskey 372
Transfer via DTMF 661
Transport Layer Security (TLS) 692
Troubleshooting 721
Troubleshooting Methods 721
Troubleshooting Solutions 746
TR-069 Device Management 592

U

Understanding VoIP Principle and SIP Components xi
Unregister When Reboot 433
Upgrading Firmware 123
Use Outbound Proxy in Dialog 330
User Agent Client (UAC) 839
User Agent Server (UAS) 457
User and Administrator Password 689

V

Verifying Startup 21
Video Codecs 685
Video Settings 683
Viewing Log Files 721
VLAN 51
VLAN Feature in the Wireless Network 66
Voice Activity Detection (VAD) 644
Voice Mail Tone 621
Voice Quality Monitoring (VQM) 651
VoIP Principle xii
VPN 76
VQ-RTCPXR 666

W

Wallpaper 152
Web Server Type 46
Web User Interface 113
What IP Phones Need to Meet 9
Why Using a Provisioning Server? 121
Wi-Fi 46

Y

Yealink IP Phones in a Network 9