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.
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?BaseInfoCatId=293&NewsCatId=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
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:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>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 -&gt; Upgrade.). Also used to emphasize text (e.g., Important!).</td>
</tr>
<tr>
<td><strong>Italics</strong></td>
<td>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).</td>
</tr>
<tr>
<td><strong>Blue Text</strong></td>
<td>Used for cross references to other sections within this documentation (e.g., refer to Ring Tones on page 633), for hyperlinks to non-Yealink websites (e.g., RFC 3315) or for hyperlinks to Yealink Technical Support website.</td>
</tr>
<tr>
<td><strong>Blue Text in Italics</strong></td>
<td>Used for hyperlinks to Yealink resources outside of this documentation such as the Yealink documentations (e.g., Yealink SIP IP Phones Auto Provisioning Guide_V81).</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;&gt;</td>
<td>Indicates that you must enter information specific to phone or network. For example, when you see &lt;MAC&gt;, enter your phone’s 12-digit MAC address. If you see &lt;phoneIPAddress&gt;, enter your phone’s IP address.</td>
</tr>
<tr>
<td>- &gt;</td>
<td>Indicates that you need to select an item from a menu. For example, Settings -&gt; Basic indicates that you need to select Basic from the Settings menu via phone user interface. <strong>Note:</strong> 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 to see it.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Permitted parameter value</th>
<th>Default parameter value</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.auto_answer</td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td>(Ranged from 1 to 16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Scope of variable X**

**Web path**

**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:

![MAC.cfg segment](image)

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:

![Auto Answer Configuration](image)

**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 80.14

The following sections are new for this version:

- Automatic Call Distribution (ACD) on page 516
- XML Browser on page 628

Major updates have occurred to the following sections:

- Wi-Fi on page 51
- Power Indicator LED on page 145
- Power Saving on page 157
- Dial Plan using Digit Map String Rules on page 242
- Local Conference on page 367
- Call Park on page 401
- Door Phone on page 451
- CSTA Control on page 471
- Lightweight Directory Access Protocol (LDAP) on page 481
- Noise Suppression on page 681
- Smart Noise Block on page 682
- Video Settings on page 713
- Appendix B: Time Zones on page 799

Changes for Release 80, Guide Version 80.13

The following sections are new for this version:

- Noise Suppression on page 681
- Smart Noise Block on page 682

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 471
● Real-Time Transport Protocol (RTP) Ports on page 620
● Noise Suppression on page 681
● Smart Noise Block on page 682

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
● Customizing a Local Contact File on page 270
● Auto Answer on page 294
● Intercom on page 422
● Appendix C: Trusted Certificates on page 800

Changes for Release 80, Guide Version 80.11

Major update had occurred to the following section:

● Door Phone on page 451
# 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 ........................ xii
  - VoIP Principle .................................................................................. xii
  - SIP Components ............................................................................... xiii
- Summary of Changes ........................................................................... xiv
  - Changes for Release 80, Guide Version 80.14 ............................... 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 ............................... xv

## Table of Contents ................................................................................. xvii

## 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 ............................................................. 33
PPPoE ......................................................................................................................... 39
Configuring Transmission Methods of the Internet Port and PC Port .................... 41
Configuring PC Port Mode ........................................................................................ 45
Web Server Type ....................................................................................................... 47
Wi-Fi .......................................................................................................................... 51
VLAN ......................................................................................................................... 54
IPv6 Support .............................................................................................................. 67
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 ...................................................................................................... 168
Page Tips for Expansion Module ............................................................................. 170
Account Registration ............................................................................................... 171
Multiple Line Keys per Account .............................................................................. 179
# Table of Contents

- Call Display ......................................................................................................................... 183
- Display Method on Dialing ................................................................................................. 185
- Time and Date ....................................................................................................................... 187
  - NTP Time Server ............................................................................................................... 188
  - Time and Date Settings ..................................................................................................... 193
- Daylight Saving Time (DST) ................................................................................................. 196
- Language .............................................................................................................................. 204
  - Specifying the Language to Use ...................................................................................... 212
- Softkey Layout ..................................................................................................................... 214
  - Customizing Softkey Layout Template File ..................................................................... 216
- Key As Send ........................................................................................................................... 222
- Dial Plan ............................................................................................................................... 226
  - 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 ..................................................................................................................... 267
- Local Directory .................................................................................................................... 268
  - Configuring a Local Contact File ..................................................................................... 269
- Live Dialpad ........................................................................................................................ 276
- Speed Dial ............................................................................................................................. 281
- Call Waiting ......................................................................................................................... 283
- Auto Redial ......................................................................................................................... 288
- Auto Answer ......................................................................................................................... 291
- IP Direct Auto Answer ......................................................................................................... 294
- Allow IP Call ......................................................................................................................... 299
- Accept SIP Trust Server Only ............................................................................................. 300
- Call Completion ................................................................................................................... 302
- Anonymous Call .................................................................................................................. 303
- Anonymous Call Rejection .................................................................................................. 306
- Do Not Disturb (DND) .......................................................................................................... 310
- Busy Tone Delay ................................................................................................................. 314
- Return Code When Refuse ................................................................................................... 326
- Early Media .......................................................................................................................... 328
- 180 Ring Workaround .......................................................................................................... 330
- Use Outbound Proxy in Dialog ......................................................................................... 330
- SIP Session Timer ............................................................................................................... 333
Session Timer ................................................................. 335
Call Hold ........................................................................... 338
Music on Hold (MoH) .......................................................... 342
Call Forward .................................................................... 344
Call Transfer .................................................................... 364
Local Conference ............................................................. 367
Network Conference ......................................................... 369
Transfer on Conference Hang Up ....................................... 371
Feature Key Synchronization .............................................. 372
Transfer Mode via Dsskey .................................................. 374
Directed Call Pickup .......................................................... 375
Group Call Pickup ............................................................ 384
Dialog Info Call Pickup ....................................................... 392
Recent Call In Dialing ........................................................ 395
ReCall ............................................................................ 397
Call Number Filter ............................................................ 400
Call Park ........................................................................ 401
Calling Line Identification Presentation (CLIP) .................... 412
Connected Line Identification Presentation (COLP) ............ 417
Mute ............................................................................ 419
Allow Mute ..................................................................... 419
Keep Mute ...................................................................... 421
Intercom ........................................................................ 422
Outgoing Intercom Calls ................................................... 423
Incoming Intercom Calls .................................................... 429
Call Timeout .................................................................... 432
Ringing Timeout ............................................................... 433
Send user=phone .............................................................. 433
SIP Send MAC .................................................................. 435
SIP Send Line .................................................................. 437
Reserve # in User Name ..................................................... 439
Password Dial .................................................................. 441
Unregister When Reboot .................................................... 443
100 Reliable Retransmission .............................................. 444
Reboot in Talking .............................................................. 446
Answer By Hand ............................................................... 448
Call Recording Using Soft Key ......................................... 449
Silent Mode ..................................................................... 450
Door Phone ..................................................................... 451
Mobile Account ............................................................... 466
Quick Login ..................................................................... 470
CSTA Control ................................................................. 471

Configuring Advanced Features ...................................... 473
Configuring Audio Features ................................................. 633

Redial Tone ........................................................................ 633
Ring Tones ........................................................................... 634
Distinctive Ring Tones .......................................................... 639
Tones .................................................................................. 646
Voice Mail Tone .................................................................... 653
Ringer Device for Headset ...................................................... 654
Headset Prior ........................................................................ 656
Dual Headset ......................................................................... 658
Sending Volume ..................................................................... 659
Audio Codecs ........................................................................ 661
Supported Audio Codecs .......................................................... 662
Packetization Time (PTime) ....................................................... 667
Opus Sample Rate ................................................................................................. 670
Acoustic Clarity Technology ............................................................................. 672
Acoustic Echo Cancellation (AEC) ..................................................................... 672
Background Noise Suppression (BNS) ................................................................. 673
Automatic Gain Control (AGC) .......................................................................... 674
Voice Activity Detection (VAD) .......................................................................... 674
Comfort Noise Generation (CNG) ...................................................................... 675
Jitter Buffer .......................................................................................................... 677
Noise Suppression ............................................................................................... 681
Smart Noise Block ............................................................................................... 682
DTMF ................................................................................................................... 683
Methods of Transmitting DTMF Digit ................................................................. 684
Suppress DTMF Display ...................................................................................... 689
Transfer via DTMF ............................................................................................... 691
Play Local DTMF Tone ......................................................................................... 693
Voice Quality Monitoring (VQM) ........................................................................ 694
RTCP-XR ............................................................................................................. 695
VQ-RTCPXR ........................................................................................................ 696

Configuring Video Features ............................................................................. 713

Video Settings .................................................................................................... 713
Video Codecs ...................................................................................................... 715

Configuring Security Features ......................................................................... 719

User and Administrator Passwords .................................................................... 719
Auto-Logout Time ............................................................................................... 721
Phone Lock .......................................................................................................... 722
Transport Layer Security (TLS) .......................................................................... 728
Secure Real-Time Transport Protocol (SRTP) ...................................................... 739
Encrypting and Decrypting Files ........................................................................ 743
Configuration Parameters .................................................................................. 743
Encrypting and Decrypting Configuration Files .................................................. 747

Troubleshooting ................................................................................................. 751

Troubleshooting Methods .................................................................................. 751
Viewing Log Files ............................................................................................... 751
Capturing Packets ............................................................................................ 765
Enabling Watch Dog Feature ............................................................................. 770
Getting Information from Status Indicators ....................................................... 771
Getting Information from Talk Statistics ............................................................ 772
Analyzing Configuration Files .......................................................................... 772
Troubleshooting Solutions ................................................................................. 776
Appendix

Appendix A: Glossary
Appendix B: Time Zones
Appendix C: Trusted Certificates
Appendix D: Configuring DSS Keys
Appendix E: Auto Provisioning Flowchart (Keep User Personalized Configuration Settings)
Appendix F: Static Settings
Appendix G: Reading Icons
Appendix H: SIP (Session Initiation Protocol)
Appendix I: SIP Call Flows

IP Address Issues .................................................................................................................. 776
Time and Date Issues .......................................................................................................... 777
Display Issues ...................................................................................................................... 777
Phone Book Issues ............................................................................................................... 778
Audio Issues ....................................................................................................................... 778
Camera and Video Issues .................................................................................................... 779
Wi-Fi and Bluetooth Issues ............................................................................................... 779
Firmware and Upgrading Issues .......................................................................................... 780
Provisioning Issues ............................................................................................................ 781
System Log Issues ............................................................................................................. 782
Resetting Issues ................................................................................................................ 782
Rebooting Issues ................................................................................................................ 787
Protocols and Ports Issues ............................................................................................... 790
Password Issues ................................................................................................................ 792
Power and Startup Issues ................................................................................................. 792
Hardware Issues ................................................................................................................ 792
Other Issues ....................................................................................................................... 793

Appendix .............................................................................................................................. 797

Appendix A: Glossary ........................................................................................................... 797
Appendix B: Time Zones ...................................................................................................... 799
Appendix C: Trusted Certificates ....................................................................................... 800
Appendix D: Configuring DSS Keys .................................................................................... 805
Appendix E: Auto Provisioning Flowchart (Keep User Personalized Configuration Settings) 816
Appendix F: Static Settings .................................................................................................. 817
Appendix G: Reading Icons ............................................................................................... 823
Appendix H: SIP (Session Initiation Protocol) .................................................................... 828
RFC and Internet Draft Support .......................................................................................... 828
SIP Request ........................................................................................................................ 831
SIP Header .......................................................................................................................... 832
SIP Responses .................................................................................................................... 833
SIP Session Description Protocol (SDP) Usage ................................................................. 836
Appendix I: SIP Call Flows ................................................................................................. 836
Successful Call Setup and Disconnect ............................................................................... 837
Unsuccessful Call Setup—Called User is Busy ................................................................. 839
Unsuccessful Call Setup—Called User Does Not Answer ............................................... 841
Successful Call Setup and Call Hold ............................................................................... 843
Successful Call Setup and Call Waiting .......................................................................... 846
Call Transfer without Consultation ................................................................................... 850
Call Transfer with Consultation ....................................................................................... 854
Always Call Forward ......................................................................................................... 859
Busy Call Forward ............................................................................................................ 861
No Answer Call Forward ................................................................................................. 864
Call Conference ............................................................................................................... 867
Index ........................................................................................................... 873
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**

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 54.

**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 33.

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 | 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.internet_port.type</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;y0000000000xx&gt;.cfg</code></td>
<td>configure the static DNS feature.</td>
</tr>
<tr>
<td><code>&lt;MAC&gt;.cfg</code></td>
<td>static.network.static_dns_enable</td>
</tr>
<tr>
<td></td>
<td>Configure static DNS address.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.static_dns_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>static.network.primary_dns</th>
<th>IPv4 Address</th>
<th>Blank</th>
</tr>
</thead>
</table>

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.
## Setting Up Your System

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>(On). If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>static.network.secondary_dns</th>
<th>IPv4 Address</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>DHCP Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask</td>
<td>1</td>
<td>Specify the client’s subnet mask.</td>
</tr>
<tr>
<td>Time Offset</td>
<td>2</td>
<td>Specify the offset of the client’s subnet in seconds from Coordinated Universal Time (UTC).</td>
</tr>
<tr>
<td>Router</td>
<td>3</td>
<td>Specify a list of IP addresses for routers on the client’s subnet.</td>
</tr>
<tr>
<td>Time Server</td>
<td>4</td>
<td>Specify a list of time servers available to the client.</td>
</tr>
<tr>
<td>Domain Name Server</td>
<td>6</td>
<td>Specify a list of domain name servers available to the client.</td>
</tr>
<tr>
<td>Host Name</td>
<td>12</td>
<td>Specify the name of the client.</td>
</tr>
<tr>
<td>Domain Server</td>
<td>15</td>
<td>Specify the domain name that client should use when resolving hostnames via DNS.</td>
</tr>
<tr>
<td>Parameter</td>
<td>DHCP Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Time Protocol Servers</td>
<td>42</td>
<td>Specify a list of NTP servers available to the client by IP address.</td>
</tr>
<tr>
<td>Vendor-Specific Information</td>
<td>43</td>
<td>Identify the vendor-specific information.</td>
</tr>
<tr>
<td>Vendor Class Identifier</td>
<td>60</td>
<td>Identify the vendor type.</td>
</tr>
<tr>
<td>TFTP Server Name</td>
<td>66</td>
<td>Identify a TFTP server when the ‘sname’ field in the DHCP header has been used for DHCP options.</td>
</tr>
</tbody>
</table>

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**

During the startup, the phone will automatically detect the custom option, option 66 or option 43 for obtaining the provisioning server address. The priority of obtaining the provisioning server address is as follows: custom option -> option 66 (identify the TFTP server) -> option 43.

The IP phone can obtain the Auto Configuration Server (ACS) address by detecting option 43 during startup.

To obtain the server address via DHCP option, make sure the DHCP option is properly configured on the phone. The option must be in accordance with the one defined in the DHCP server.

**Procedure**

DHCP active can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>…</th>
<th>Configure DHCP active.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td></td>
<td>Parameter: static.auto_provisiondhcp_option.enable</td>
</tr>
<tr>
<td>Configure the custom DHCP option.</td>
<td></td>
<td>Parameter: static.auto_provisiondhcp_option.list_user_</td>
</tr>
</tbody>
</table>
## Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
<th>Description</th>
<th>Web User Interface</th>
<th>Phone User Interface:</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.auto_provision.dhcp_option.enable</code></td>
<td>0 or 1</td>
<td>1</td>
<td>Triggers the DHCP active feature to on or off.</td>
<td>Settings &gt; Auto Provision &gt; DHCP Active</td>
<td>None</td>
</tr>
<tr>
<td><code>static.auto_provision.dhcp_option.list_user_options</code></td>
<td>Integer from 128 to 254</td>
<td>Blank</td>
<td>Configures the custom DHCP option for requesting provisioning server address.</td>
<td>Settings &gt; Auto Provision &gt; Custom Option</td>
<td>None</td>
</tr>
</tbody>
</table>

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.

**To configure the custom DHCP option via web user interface:**

1. Click on **Settings** -> **Auto Provision**.
2. Enter the desired value in the **Custom Option** 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 188.

**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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.dhcp_host_name</td>
<td>String within 99 characters</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**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

**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.

![DHCP Hostname Field](image)

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.  
N**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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.internet_port.type</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.network.ip_address_mode</code></td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.network.internet_port.ip</code></td>
<td>IPv4 Address</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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 -> IP4 Config -> Static IP Address -> IP Address

**Phone User Interface:**
Settings -> Advanced (default password: admin) -> Network -> WAN Port -> IPv4 -> Type (Static IP) -> IP Address

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.network.internet_port.mask</code></td>
<td>Subnet Mask</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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:**
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network-&gt;Advanced-&gt;WAN Port-&gt;Type (Static IP) =&gt; Gateway</td>
<td>IPv4 Address</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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->Advanced->WAN Port->Type (Static IP) => Gateway

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.primary_dns</td>
<td>IPv4 Address</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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->Advanced->WAN Port->Type (Static IP) => Primary DNS

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.secondary_dns</td>
<td>IPv4 Address</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Description:**
Configures the secondary IPv4 DNS server.
Setting Up Your System

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
</table>

**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) | Configure PPPoE on the IP phone.  
Parameter: static.network.internet_port.type |
|------------------------------------------|-----------------------------------------------------------------------------------------|
|  <y000000000xx>.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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.internet_port.type</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

Description:

Configures the Internet port type for IPv4.
0-DHCP  
1-PPPoE  
2-Static IP Address
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter &quot;static.network.ip_address_mode&quot; is set to 0 (IPv4) or 2 (IPv4 &amp; IPv6). If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network-&gt;Basic-&gt;IPv4 Config</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Advanced (default password: admin) -&gt;Network-&gt;WAN Port-&gt;IPv4-&gt;Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>static.network.pppoe.user</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the user name for PPPoE connection.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>static.network.pppoe.user = XmyI0592123</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter &quot;static.network.ip_address_mode&quot; is set to 0 (IPv4) or 2 (IPv4 &amp; IPv6), and &quot;static.network.internet_port.type&quot; is set to 1 (PPPoE). If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network-&gt;Basic-&gt;IPv4 Config-&gt;PPPoE-&gt;User Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Advanced (default password: admin) -&gt;Network-&gt;WAN Port-&gt;IPv4-&gt;Type (PPPoE) -&gt;PPPoE User</td>
<td></td>
<td></td>
</tr>
<tr>
<td>static.network.pppoe.password</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the password for PPPoE connection.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>static.network.pppoe.password = yealink123</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter &quot;static.network.ip_address_mode&quot; is set to 0 (IPv4) or 2 (IPv4 &amp; IPv6), and &quot;static.network.internet_port.type&quot; is set to 1 (PPPoE). If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network-&gt;Basic-&gt;IPv4 Config-&gt;PPPoE-&gt;Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Advanced (default password: admin) -&gt;Network-&gt;WAN Port-&gt;IPv4-&gt;Type (PPPoE) -&gt;PPPoE Password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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:

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) | Parameters:  
| <y0000000000xx>.cfg | 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.internet_port.speed_duplex</td>
<td>0, 1, 2, 3, 4 or 5</td>
<td>0</td>
</tr>
</tbody>
</table>

Description:

Configures the transmission method of the Internet port.  
0-Auto Negotiate  
1-Full Duplex 10Mbps  
2-Full Duplex 100Mbps
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-Half Duplex 10Mbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-Half Duplex 100Mbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-Full Duplex 1000Mbps (not applicable to CP960 IP phones)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>static.network.pc_port.speed_duplex</th>
<th>0, 1, 2, 3, 4 or 5</th>
<th>0</th>
</tr>
</thead>
</table>

**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**.

![Yealink IP Phone Configuration](image)

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th><code>&lt;y0000000000xx&gt;.cfg</code></th>
<th>Configure the PC port. <strong>Parameter:</strong> static.network.pc_port.enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td><strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=network-pcport&amp;q=load</td>
<td>Configure the PC port. <strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=network-pcport&amp;q=load</td>
</tr>
</tbody>
</table>
Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.pc_port.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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**.

![Image of Yealink T58 settings](image)

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) | 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-addr&q=load |
| Phone User Interface | Configure the web access type, HTTP port and HTTPS port. |

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.wui.http_enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>
### Setting Up Your System

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the user to access web user interface of the IP phone using the HTTP protocol.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network -&gt; Advanced -&gt; Web Server -&gt; HTTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings -&gt; Advanced (default password: admin) -&gt; Network -&gt; Web Server -&gt; HTTP Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.network.port.http</strong></td>
<td>Integer from 1 to 65535</td>
<td>80</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the HTTP port for the user to access web user interface of the IP phone using the HTTP protocol.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Please take care when choosing an alternate port. If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network -&gt; Advanced -&gt; Web Server -&gt; HTTP Port (1~65535)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings -&gt; Advanced (default password: admin) -&gt; Network -&gt; Web Server -&gt; HTTP Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.wui.https_enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the user to access web user interface of the IP phone using the HTTPS protocol.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network -&gt; Advanced -&gt; Web Server -&gt; HTTPS</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings -&gt; Advanced (default password: admin) -&gt; Network -&gt; Web Server -&gt; HTTPS Status</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### static.network.port.https

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.port.https</td>
<td>Integer from 1 to 65535</td>
<td>443</td>
</tr>
</tbody>
</table>

**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 -> Web Server -> 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** -> **Web Server**.
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**

You can check the Wi-Fi MAC address at the path: **Settings** -> **Status** -> **Wi-Fi MAC** (phone user interface) or **Status** -> **Status** -> **Network Common** -> **Wi-Fi MAC** (web user interface).

For SIP-TS8V/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 following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure Wi-Fi feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Parameter:</td>
</tr>
<tr>
<td></td>
<td>static.wifi.enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th>Configure Wi-Fi feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure the Wi-Fi settings.</td>
</tr>
</tbody>
</table>

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.wifi.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**

Enables or disables the Wi-Fi feature.

- **0**: Disabled
- **1**: Enabled

**Web User Interface:**

None
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone User Interface:</td>
<td>Settings &gt; Basic &gt; Wi-Fi &gt; Wi-Fi</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure the VLAN assignment method. Parameter: static.network.vlan.vlan_change.enable</th>
</tr>
</thead>
</table>

### Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.vlan.vlan_change.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>using the current VLAN assignment method. 0-Disabled 1-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Disabled</td>
<td>1-Enabled</td>
<td></td>
</tr>
<tr>
<td>The priority of each method is: LLDP/CDP&gt;Manual&gt;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. <strong>Note:</strong> If you change this parameter, the IP phone will reboot to make the change take effect. <strong>Web User Interface:</strong> None <strong>Phone User Interface:</strong> None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**LLDP**

LLDP (Link 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure LLDP feature. <strong>Parameters:</strong> static.network.lldp.enable static.network.lldp.packet_interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td>Configure LLDP feature. <strong>Navigate to:</strong></td>
</tr>
</tbody>
</table>
Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.network.lldp.enable</code></td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables the LLDP (Link 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.network.lldp.packet_interval</code></td>
<td>Integer from 1 to 3600</td>
<td>60</td>
</tr>
</tbody>
</table>

**Description:**
Configures the interval (in seconds) for the IP phone to send the LLDP (Link 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.
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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure CDP feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>static.network.cdp.enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>static.network.cdp.packet_interval</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure CDP feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Navigate to:</strong></td>
<td></td>
</tr>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=network-adv&amp;q=load</td>
<td></td>
</tr>
</tbody>
</table>

| Phone User Interface | Configure CDP feature. |

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.cdp.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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 effect.
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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.vlan.internet_port_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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
### Setting Up Your System

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong>&lt;br&gt;Settings - &gt; Advanced (default password: admin) - &gt; Network - &gt; VLAN - &gt; WAN Port - &gt; VLAN Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>static.network.vlan.internet_port_vid</code></td>
<td>Integer from 1 to 4094</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**
Configures VLAN ID for the Internet port.

**Note:** It works only if the value of the parameter “static.network.vlan.internet_port_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:**<br>Network - > Advanced - > VLAN - > WAN Port - > VID (1-4094) | | |
| **Phone User Interface:**<br>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:** It works only if the value of the parameter “static.network.vlan.internet_port_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:**<br>Network - > Advanced - > VLAN - > WAN Port - > Priority | | |
| **Web User Interface:**<br>Network - > Advanced - > VLAN - > WAN Port - > Priority | | |
| **Phone User Interface:**<br>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,
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Network->Advanced->VLAN->PC Port->Active

**Phone User Interface:**
Settings->Advanced (default password: admin) -> Network->VLAN->PC Port->VLAN Status

<table>
<thead>
<tr>
<th>static.network.vlan.pc_port_vid</th>
<th>Integer from 1 to 4094</th>
<th>1</th>
</tr>
</thead>
</table>

**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) and the value of the parameter "static.network.vlan.pc_port_enable" is set to 1 (Enabled). 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

<table>
<thead>
<tr>
<th>static.network.vlan.pc_port_priority</th>
<th>Integer from 0 to 7</th>
<th>0</th>
</tr>
</thead>
</table>

**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) and the value of the parameter "static.network.vlan.pc_port_enable" is set to 1 (Enabled). 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure DHCP VLAN discovery feature. Parameters: static.network.vlan.dhcp_enable static.network.vlan.dhcp_option</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td></td>
</tr>
</tbody>
</table>

|------------------------------------------|--------------------------------------------------------------------------------------------------|

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th>Configure DHCP VLAN discovery feature.</th>
</tr>
</thead>
</table>

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.vlan.dhcp_enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.vlan.dhcp_option</td>
<td>Integer from 1 to 255</td>
<td>132</td>
</tr>
</tbody>
</table>

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.
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:

<table>
<thead>
<tr>
<th>DHCPv6</th>
<th>SLAAC (ICMPv6)</th>
<th>How the IP phone obtains the IPv6 address and network settings?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>You have to manually configure the static IPv6 address and other network settings.</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>The IP phone can obtain the IPv6 address via SLAAC, but the other network settings must be configured manually.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>The IP phone can obtain the IPv6 address and the other network settings via DHCPv6.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enabled</td>
<td>The IP phone can obtain the IPv6 address via SLAAC and obtain other network settings via DHCPv6.</td>
</tr>
</tbody>
</table>

Procedure

IPv6 can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure the IPv6 address assignment method.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters:</td>
<td></td>
<td>static.network.ip_address_mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>static.network.ipv6.internet_port.type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>static.network.ipv6.internet_port.ip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>static.network.ipv6.prefix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>static.network.ipv6.internet_port.gateway</td>
</tr>
<tr>
<td></td>
<td></td>
<td>static.network.ipv6.icmp_v6.enable</td>
</tr>
<tr>
<td>&lt;y000000000000x&gt;.cfg</td>
<td></td>
<td>Configure the IPv6 static DNS address.</td>
</tr>
<tr>
<td>Parameters:</td>
<td></td>
<td>static.network.ipv6_primary_dns</td>
</tr>
<tr>
<td></td>
<td></td>
<td>static.network.ipv6_secondary_dns</td>
</tr>
<tr>
<td>Web User Interface</td>
<td></td>
<td>Configure the IPv6 address assignment</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.ip_address_mode</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>static.network.ipv6_internet_port.type</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.ipv6_static_dns_enable = 0 or 1</td>
<td>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. <strong>Note:</strong> It works only if the value of the parameter &quot;static.network.ipv6_internet_port.type&quot; is set to 0 (DHCP). If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**

Network -> Basic -> IPv6 Config -> IPv6 Static DNS

### Phone User Interface:

Settings -> Advanced (default: admin) -> Network -> WAN Port -> IPv6 -> Type (DHCP)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.ipv6_internet_port.ip = 2026:1234:1:1:215:65ff:fe1f:caa</td>
<td>Configures the IPv6 address. <strong>Note:</strong> It works only if the value of the parameter &quot;static.network.ipv6_internet_port.type&quot; is set to 1 (Static IP Address). If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.ipv6_prefix = 64</td>
<td>Integer from 0 to 128</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th><strong>static.network.ipv6_internet_port.gateway</strong></th>
<th><strong>IPv6 address</strong></th>
<th><strong>Blank</strong></th>
</tr>
</thead>
</table>

**Description:**
Configures the IPv6 default gateway.

**Example:**
static.network.ipv6_internet_port.gateway = 3036:1:1:c3c7:c11c5447:23a6:255

**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

<table>
<thead>
<tr>
<th><strong>static.network.ipv6_primary_dns</strong></th>
<th><strong>IPv6 address</strong></th>
<th><strong>Blank</strong></th>
</tr>
</thead>
</table>

**Description:**
Configures the primary IPv6 DNS server.

**Example:**
static.network.ipv6_primary_dns = 3036:1:1:c3c7: c11c5447:23a6:256

**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
To configure IPv6 address assignment method via web user interface:

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

<table>
<thead>
<tr>
<th>parameter</th>
<th>default value</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.ipv6_secondary_dns</td>
<td></td>
<td>Configures the secondary IPv6 DNS server.</td>
</tr>
<tr>
<td>Example:</td>
<td>static.network.ipv6_secondary_dns = 2026:1234:1:1:c3c7:5447:23a6</td>
<td></td>
</tr>
<tr>
<td>Note:</td>
<td>It works only if the value of the parameter &quot;static.network.ip_address_mode&quot; is set to 1 (IPv6) or 2 (IPv4 &amp; IPv6). In DHCP environment, you also need to make sure the value of the parameter &quot;static.network.ipv6_static_dns_enable&quot; is set to 1 (On). If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>parameter</th>
<th>value</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.ipv6_icmp_v6.enable</td>
<td>0 or 1</td>
<td>Enables or disables the IP phone to obtain IPv6 network settings via SLAAC (Stateless Address Autoconfiguration) method.</td>
</tr>
<tr>
<td>Note:</td>
<td>It works only if the value of the parameter &quot;static.network.ipv6_internet_port.type&quot; is set to 0 (DHCP). If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Network->Advanced->ICMPv6 Status->Active

**Phone User Interface:**
None
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.

![VPN Diagram]

**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:

<table>
<thead>
<tr>
<th>VPN files</th>
<th>Description</th>
<th>Unified Directories</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca.crt</td>
<td>CA certificate</td>
<td>/config/openvpn/keys/ca.crt</td>
</tr>
<tr>
<td>client.crt</td>
<td>Client certificate</td>
<td>/config/openvpn/keys/client.crt</td>
</tr>
<tr>
<td>client.key</td>
<td>Private key of the client</td>
<td>/config/openvpn/keys/client.key</td>
</tr>
</tbody>
</table>

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

**Procedure**

VPN can be configured using the following methods.

**Central Provisioning (Configuration File)**

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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.vpn_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables or disables OpenVPN feature on the IP phone.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>static.openvpn.url</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description: Configures the access URL of the *.tar file for OpenVPN.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> static.openvpn.url = <a href="http://192.168.10.25/OpenVPN.tar">http://192.168.10.25/OpenVPN.tar</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong> Network -&gt; Advanced -&gt; VPN -&gt; Upload VPN Config</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

![Image of system settings]

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:

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

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:

<table>
<thead>
<tr>
<th>Call Type</th>
<th>Number of Required Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video</td>
<td>4 UDP ports</td>
</tr>
<tr>
<td>Voice</td>
<td>2 UDP ports</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Phone</th>
<th>Maximum Connections</th>
<th>Required Ports for a SIP Call</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A</td>
<td>Three-way video call and two audio-only calls</td>
<td>16 UDP 50000-50015</td>
</tr>
<tr>
<td>SIP-T56A</td>
<td>Five-way audio-only conference</td>
<td>10 UDP 50000-50009</td>
</tr>
</tbody>
</table>

Procedure

Reserved ports can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the range of the UDP ports.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameters:</strong></td>
<td></td>
</tr>
<tr>
<td>sip.min_udp_port</td>
<td></td>
</tr>
<tr>
<td>sip.max_udp_port</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the range of the UDP ports.</td>
<td></td>
</tr>
<tr>
<td>Configure the range of the TCP ports.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameters:</strong></td>
<td></td>
</tr>
<tr>
<td>sip.min_tcp_port</td>
<td></td>
</tr>
<tr>
<td>sip.max_tcp_port</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Navigate to:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m =mod_data&amp;p=network-adv&amp;q=load</td>
<td></td>
</tr>
</tbody>
</table>
Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.min_udp_port</td>
<td>Integer from 1024 to 65535</td>
<td>50000</td>
</tr>
<tr>
<td>sip.max_udp_port</td>
<td>Integer from 1024 to 65535</td>
<td>50249</td>
</tr>
<tr>
<td>sip.min_tcp_port</td>
<td>Integer from 1024 to 65535</td>
<td>50000</td>
</tr>
</tbody>
</table>

**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_tcp_port

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.max_tcp_port</td>
<td>Integer from 1024 to 65535</td>
<td>50249</td>
</tr>
</tbody>
</table>

**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 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.

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>444</td>
<td>18.5468</td>
<td>179.148.1.6</td>
<td>218.120.220.74</td>
<td>STUN</td>
<td>Binding Request</td>
</tr>
<tr>
<td>447</td>
<td>18.71149</td>
<td>218.107.220.74</td>
<td>192.168.1.6</td>
<td>STUN</td>
<td>Binding Success Response MAPPED-ADDRESS: 59.61.92.59:19232</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
<th>Phone User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure NAT traversal and STUN server on a phone basis.</td>
<td>Configure local SIP port and TLS SIP port.</td>
<td>Configure NAT traversal and STUN server on a phone basis.</td>
</tr>
<tr>
<td>Parameters: sip.nat_stun.enable sip.nat_stun.server sip.nat_stun.port</td>
<td>Parameters: sip.listen_port sip.tls_listen_port</td>
<td></td>
</tr>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Configure NAT traversal on a per-line basis. Parameter: accountX.nat.nat_traversal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=network-adv&amp;q=load</td>
<td>Configure NAT traversal on a per-line basis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=settings-sip&amp;q=load</td>
</tr>
<tr>
<td></td>
<td></td>
<td>navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-register&amp;q=load&amp;acc=0</td>
</tr>
<tr>
<td></td>
<td>Configure local SIP port and TLS SIP port.</td>
<td></td>
</tr>
</tbody>
</table>
Configure NAT traversal on a per-line basis.

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.nat_stun.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>IP address or domain name</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.nat_stun.server</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Integer from 1024 to 65000</th>
<th>3478</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.nat_stun.port</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.listen_port</td>
<td>Integer from 1024 to 65535</td>
<td>5060</td>
</tr>
<tr>
<td>sip.tls_listen_port</td>
<td>Integer from 1024 to 65535</td>
<td>5061</td>
</tr>
</tbody>
</table>

### Description:
Configures the local SIP port.

### Web User Interface:
- Settings -> SIP -> Local SIP Port

### Phone User Interface:
- None

### sip.listen_port

#### Description:
Configures the local SIP port.

#### Web User Interface:
- Settings -> SIP -> Local SIP Port

#### Phone User Interface:
- None

### sip.tls_listen_port

#### Description:
Configures the local SIP port.

#### Web User Interface:
- Settings -> SIP -> Local SIP Port

#### Phone User Interface:
- None
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Configures the local TLS listen port.</td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td>Settings-&gt;SIP-&gt;TLS SIP Port</td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

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**.

![Yealink Settings](image)

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.

![Screenshot of SIP configuration settings]

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  

| 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.nat.udp_update_enable</td>
<td>0, 1, 2 or 3</td>
<td>1</td>
</tr>
</tbody>
</table>

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:
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>account.X.nat.udp_update_time</code></td>
<td>Integer from 15 to 2147483647</td>
<td>30</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure NAT Rport feature on a per-line basis. Parameter: account.X.nat.rport</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td>Configure NAT Rport feature on a per-line basis. Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-adv&amp;q=load&amp;acc=0</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.nat.rport</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

**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 55.
**Procedure**

QoS can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y000000000xx&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the DSCPs for voice packets, SIP packets and video packets.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameters:</strong> static.network.qos.audiotos static.network.qos.signaltos static.network.qos.videotos</td>
<td></td>
</tr>
<tr>
<td>Configure the WMM feature in the wireless network.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameters:</strong> static.wifi.802_11e.enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the DSCPs for voice packets, SIP packets and video packets.</td>
</tr>
<tr>
<td><strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=network-adv&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.qos.signaltos</td>
<td>Integer from 0 to 63</td>
<td>26</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.qos.audiotos</td>
<td>Integer from 0 to 63</td>
<td>46</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the DSCP (Differentiated Services Code Point) for voice packets.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The default DSCP value for RTP packets is 46 (Expedited Forwarding).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network-&gt;Advanced-&gt;Voice QoS-&gt;Audio QoS (0~63)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>static.network.qos.videotos</th>
<th>Integer from 0 to 63</th>
<th>34</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the DSCP (Differentiated Services Code Point) for video packets.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The default DSCP value for H264 packets is 34 (Assured Forwarding).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If you change this parameter, the IP phone will reboot to make the change take effect. It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network-&gt;Advanced-&gt;Voice QoS-&gt;Video QoS (0~63)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>static.wifi.802_11e.enable</th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the WMM feature (Wi-Fi MultiMedia) in the wireless network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameters:</th>
<th>Configure the 802.1X authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>static.network.802_1x.mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>static.network.802_1x.identity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>static.network.802_1x.md5_password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>static.network.802_1x.root_cert_url</td>
<td></td>
</tr>
</tbody>
</table>
Setting Up Your System

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.802_1x.mode</td>
<td>0, 1, 2, 3, 4, 5, 6 or 7</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.802_1x.identity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 change take effect.

Configure the 802.1X authentication.

**Navigate to:**
http://<phoneIPAddress>/servlet?m=mod_data&p=network-adv&q=load

Configure the 802.1X authentication.

**Details of Configuration Parameters:**

- **static.network.802_1x.client_cert_url**
### static.network.802_1x.md5_password

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.802_1x.md5_password</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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->Identity

**Phone User Interface:**
Settings->Advanced (default password: admin) -> Network->802.1x->Identity

---

### static.network.802_1x.root_cert_url

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.802_1x.root_cert_url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.802_1x.client_cert_url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Description:**
**Setting Up Your System**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the access URL of the device certificate.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

![Network Configuration](image)

**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.

![YeaLink Network Configuration](image)

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.

![Image of CA Certificate field](image)

**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.
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):

![Priority Diagram]

- **Phone/Web User Interface**
- **Central Provisioning**
- **Internal Settings**
- **TR069 Settings**
- **Factory Defaults**

**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 817.
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 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 719.

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 47.

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 719.

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"
```
Setting Up Your System

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 IP Phones Auto Provisioning Guide_V81.

Common Boot File

Common boot file, named y00000000000.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:

<table>
<thead>
<tr>
<th>IP Phone Model</th>
<th>Common CFG file</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/A</td>
<td>y000000000058.cfg</td>
</tr>
<tr>
<td>SIP-T56A</td>
<td>y000000000056.cfg</td>
</tr>
<tr>
<td>CP960</td>
<td>y000000000073.cfg</td>
</tr>
</tbody>
</table>

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 817.

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 782.

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 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 782.
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:

<table>
<thead>
<tr>
<th>Template File</th>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot File</td>
<td>y00000000000.boot</td>
<td>Allows you to customize the download sequence of the configuration files during auto provisioning. For more information, refer to Boot Files on page 114.</td>
</tr>
<tr>
<td>Configuration Files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common CFG File</td>
<td>Common.cfg</td>
<td>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.</td>
</tr>
<tr>
<td>MAC-Oriented CFG File</td>
<td>MAC.cfg</td>
<td></td>
</tr>
<tr>
<td>Custom CFG Files</td>
<td>sip.cfg</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>account.cfg</td>
<td></td>
</tr>
<tr>
<td>Resource Files</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AutoDST Template</td>
<td>AutoDST.xml</td>
<td>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 201.</td>
</tr>
<tr>
<td>Language Packs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>000.GUI.English.lang</td>
<td>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 205.</td>
</tr>
<tr>
<td></td>
<td>1.English_note.xml</td>
<td></td>
</tr>
<tr>
<td>Template File</td>
<td>File Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Replace Rule Template</td>
<td>dialplan.xml</td>
<td>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.</td>
</tr>
<tr>
<td>Dial Now Template</td>
<td>dialnow.xml</td>
<td>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 235.</td>
</tr>
<tr>
<td>Softkey Layout Template (not applicable to CP960 IP phones)</td>
<td>CallFailed.xml, CallIn.xml, Connecting.xml, Dialing.xml, RingBack.xml, Talking.xml</td>
<td>Allow you to customize soft key layout for different call states. For more information, refer to Customizing Softkey Layout Template File on page 216.</td>
</tr>
<tr>
<td>Super Search Template</td>
<td>super_search.xml</td>
<td>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.</td>
</tr>
<tr>
<td>Local Contact File</td>
<td>contact.xml</td>
<td>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 269.</td>
</tr>
<tr>
<td>Remote Phone Book Template</td>
<td>Department.xml, Menu.xml</td>
<td>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 474.</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Platform</th>
<th>HTTP/HTTPS</th>
<th>TFTP/FTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Support: ~ <code>! @ $ ^ ( ) _ - \ .</code> ; [ ] { } (including space)</td>
<td>Support: ~ <code>! @ $ ^ ( ) _ - \ .</code> ; [ ] { } % &amp; = + (including space)</td>
</tr>
<tr>
<td></td>
<td>Not Support:</td>
<td>Not Support:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td>Support: ~ <code>! @ $ ^ ( ) _ - \ .</code> ; [ ] { } &lt; &gt; : &quot;</td>
<td>Support: ~ <code>! @ $ ^ ( ) _ - \ .</code> ; [ ] { } &lt; &gt; : &quot; % &amp; = + (including space)</td>
</tr>
<tr>
<td></td>
<td>Not Support:</td>
<td>Not Support:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 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 751.

### 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 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 742.

**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 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).

<table>
<thead>
<tr>
<th>IP Phone Model</th>
<th>Associated Firmware Name</th>
<th>Firmware Name Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A/T56A</td>
<td>58.x.x.x.rom</td>
<td>58.80.0.10.rom</td>
</tr>
<tr>
<td>CP960</td>
<td>73.x.x.x.rom</td>
<td>73.80.0.10.rom</td>
</tr>
</tbody>
</table>

**Note**

You can download the latest firmware online: [http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage](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.
Method of checking for configuration files is configurable.

**Procedure**

Configuration changes can be performed using the following methods.

| Central Provisioning (Configuration File) |  
|  
|  
| 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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.auto_provision.power_on</td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Triggers the power on feature to on or off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-On</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If it is set to 1 (On), the IP phone will perform an auto provisioning process when powered on.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Auto Provision-&gt;Power On</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 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                               |                  |         |

<p>| static.auto_provision.weekly.enable | 0 or 1 | 0 |</p>
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Triggers the weekly feature to on or off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>0</strong>: Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>1</strong>: On</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If it is set to 1 (On), the IP phone will perform an auto provisioning process weekly.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Auto Provision-&gt;Weekly</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.auto_provision.weekly.begin_time</strong></td>
<td>Time from 00:00 to 23:59</td>
<td>00:00</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the begin time of the day for the IP phone to perform an auto provisioning process weekly.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter &quot;static.auto_provision.weekly.enable&quot; is set to 1 (On).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Auto Provision-&gt;Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.auto_provision.weekly.end_time</strong></td>
<td>Time from 00:00 to 23:59</td>
<td>00:00</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the end time of the day for the IP phone to perform an auto provisioning process weekly.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter &quot;static.auto_provision.weekly.enable&quot; is set to 1 (On).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Auto Provision-&gt;Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.auto_provision.weekly.dayofweek</strong></td>
<td>0, 1, 2, 3, 4, 5, 6 or a combination of these digits</td>
<td>0123456</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the days of the week for the IP phone to perform an auto provisioning process weekly.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>static.auto_provision.weekly.dayofweek = 01</td>
<td></td>
</tr>
<tr>
<td>It means the IP phone will perform an auto provisioning process every Sunday and Monday.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter “static.auto_provision.weekly.enable” is set to 1 (On).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Settings -&gt; Auto Provision -&gt; Day of Week</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>static.auto_provision.flexible.enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Triggers the flexible feature to on or off.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>static.auto_provision.flexible.begin_time = 01</td>
<td></td>
</tr>
<tr>
<td>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”.</td>
<td>static.auto_provision.flexible.end_time = 01</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Settings -&gt; Auto Provision -&gt; Flexible Auto Provision</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
## Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.flexible.interval</td>
<td>Integer from 1 to 1000</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.flexible.interval = 30</td>
<td>The IP phone will perform an auto provisioning process on a random day (e.g., 18) based on the phone’s MAC address.</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It works only if the value of the parameter “static.auto_provision.flexible.enable” is set to 1 (On).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Web User Interface:
Settings -> Auto Provision -> Flexible Interval Days

### Phone User Interface:
None

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.auto_provision.flexible.begin_time</td>
<td>Time from 00:00 to 23:59</td>
<td>02:00</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the starting time of the day for the IP phone to perform an auto provisioning process at random.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It works only if the value of the parameter “static.auto_provision.flexible.enable” is set to 1 (On).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Web User Interface:
Settings -> Auto Provision -> Flexible Time

### Phone User Interface:
None

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.auto_provision.flexible.end_time</td>
<td>Time from 00:00 to 23:59</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the ending time of the day for the IP phone to perform an auto provisioning process at random.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>process at the starting time.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter “static.auto_provision.flexible.enable” is set to 1 (On).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Auto Provision-&gt;Flexible Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**static.firmware.url**

**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.

![Upgrade Settings](image)

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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.auto_provision.custom.protect</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Description</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>auto_provision.custom.sync</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

#### 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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.auto_provision.custom.sync.path</code></td>
<td>URL</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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 816.
**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 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 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 5.8.0.0.5 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?”.  

   ![Reset local settings screen](image)

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 y0000000000058.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**.

   ![Reset Config screen](image)

   The touch screen prompts the following warning:

   ![Warning screen](image)

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.

![Image of Yealink Web Interface](image)

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 5.8.0.0 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.

![Image of Yealink T5 phone settings](image)

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.

MissCall Power Light Flash
MissCall Power Light Flash allows the power indicator LED to flash when the IP phone misses a call.

Procedure
Power indicator LED can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the power indicator LED.</td>
<td>Parameters:</td>
</tr>
<tr>
<td></td>
<td>phone_setting.common_power_led_enable</td>
</tr>
<tr>
<td></td>
<td>phone_setting.ring_power_led_flash_enable</td>
</tr>
<tr>
<td></td>
<td>phone_setting.mail_power_led_flash_enable</td>
</tr>
<tr>
<td></td>
<td>phone_setting.mute_power_led_flash_enable</td>
</tr>
<tr>
<td></td>
<td>phone_setting.hold_and_held_power_led_flash_enable</td>
</tr>
<tr>
<td></td>
<td>phone_setting.talk_and_dial_powerLed_enable</td>
</tr>
<tr>
<td></td>
<td>phone_setting.missed_call_powerLed_flash.enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure the power indicator LED.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to:</td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-powerled&amp;q=load</td>
</tr>
</tbody>
</table>

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.common_power_led_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

Description:
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables or disables the power indicator LED to be turned on.</td>
<td>0 - Disabled (power indicator LED is off) 1 - Enabled (power indicator LED is solid red)</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Features -&gt; Power LED -&gt; Common Power Light On</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.ring_power_led_flash_enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Enables or disables the power indicator LED to flash when the IP phone receives an incoming call.</td>
<td></td>
</tr>
<tr>
<td>0 - Disabled (power indicator LED does not flash)</td>
<td>1 - Enabled (power indicator LED fast flashes (300ms) red)</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Features -&gt; Power LED -&gt; Ringing Power Light Flash</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.mail_power_led_flash_enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Enables or disables the power indicator LED to flash when the IP phone receives a voice mail.</td>
<td></td>
</tr>
<tr>
<td>0 - Disabled (power indicator LED does not flash)</td>
<td>1 - Enabled (power indicator LED slowly flashes (1000ms) red)</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter “account.X.display_mwi.enable” is set to 1 (Enabled). It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Features -&gt; Power LED -&gt; Voice/Text Mail Power Light Flash</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.mute_power_led_flash_enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the power indicator LED to flash when a call is muted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 : Disabled (power indicator LED does not flash)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 : Enabled (power indicator LED fast flashes (300ms) red)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Power LED -&gt; Mute Power Light Flash</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.hold_and_held_power_led_flash_enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the power indicator LED to flash when a call is placed on hold or is held.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 : Disabled (power indicator LED does not flash)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 : Enabled (power indicator LED fast flashes (500ms) red)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Power LED -&gt; Hold/Held Power Light Flash</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.talk_and_dial_power_led_enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the power indicator LED to be turned on when the IP phone is busy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 : Disabled (power indicator LED is off)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 : Enabled (power indicator LED is solid red)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Power LED -&gt; Talk/Dial Power Light On</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.missed_call_power_led_flash.enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the power indicator LED to flash when the IP phone misses a call.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disabled (power indicator LED is off)</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Enabled (power indicator LED slowly flashes (1000ms) red)</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** It works only if the value of the parameter “account.X.missed_calllog” is set to 1 (Enabled). It is not applicable to CP960 IP phones.

**Web User Interface:**
Features -> Power LED -> MissCall Power Light Flash

**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. Select the desired value from the pull-down list of **MissCall Power Light Flash**.
9. 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:

![Pop-up message box]

**Procedure**

Notification popups can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure notification popups.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Configuration File)</td>
<td></td>
<td>Parameters:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features.voice_mail_popup.enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features.missed_call_popup.enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features.forward_call_popup.enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure notification popups.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Navigate to:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-notifypop&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.voice_mail_popup.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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:** It works only if the value of the parameter "account.X.display_mwi.enable" is set to 1 (Enabled). 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
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>features.missed_call_popup.enable</code></td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables the IP phone to display the pop-up message box when it misses a call.
- 0 - Disabled
- 1 - Enabled

**Note:** It works only if the value of the parameter “account.X.missed_calls” is set to 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
- 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**.

![Image of Display Forward Call Popup settings]

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.

To upload the custom wallpaper via web user interface, note that the image format must meet the following:

<table>
<thead>
<tr>
<th>Format</th>
<th>Resolution</th>
<th>Single File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.jpg</td>
<td>&lt;=2.0 megapixels</td>
<td>&lt;=5MB</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.backgrounds</td>
<td>Refer to the following content</td>
<td>Default.jpg</td>
</tr>
</tbody>
</table>

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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom wallpaper name (e.g., wallpaper.jpg)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>phone_setting.backgrounds = Default.jpg</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Preference-&gt;Wallpaper</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Basic-&gt;Display-&gt;Wallpaper</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>expansion_module.backgrounds</th>
<th>Refer to the following content</th>
<th>Default-exp50.jpg</th>
</tr>
</thead>
</table>

**Description:**
Configures the wallpaper displayed on the EXP50.

**Permitted Values:**
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

<table>
<thead>
<tr>
<th>wallpaper_upload.url</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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:**
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 \(\longleftarrow\) 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 \(\longleftarrow\) 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 \(\longleftarrow\) to return to the Screen Saver setting screen.

6. Tap \(\checkmark\) to accept the change or \(\longleftarrow\) 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.

<table>
<thead>
<tr>
<th>Method</th>
<th>Details</th>
</tr>
</thead>
</table>
| **Central Provisioning (Configuration File)** | 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.power_saving.intelligent_mode</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**

Enables or disables the power saving intelligent mode.

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

<table>
<thead>
<tr>
<th>features.power_saving.enable</th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>features.power_saving.office_hour.idle_timeout</th>
<th>Integer from 1 to 240</th>
<th>120</th>
</tr>
</thead>
</table>

**Description:**

Configures the time (in minutes) to wait in the idle state before the IP phone enters power-saving mode during the office hours.

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.power_saving.off_hour.idle_timeout</td>
<td>Integer from 1 to 10</td>
<td>10</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.power_saving.user_input_ext.idle_timeout</td>
<td>Integer from 1 to 30</td>
<td>10</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.power_saving.office_hour.monday</td>
<td>Integer from 0 to 23, 7,19</td>
<td>7,19</td>
</tr>
<tr>
<td>features.power_saving.office_hour.tuesday</td>
<td>Integer from 0 to 23, 7,19</td>
<td>7,19</td>
</tr>
<tr>
<td>features.power_saving.office_hour.wednesday</td>
<td>Integer from 0 to 23, 7,19</td>
<td>7,19</td>
</tr>
<tr>
<td>features.power_saving.office_hour.thursday</td>
<td>Integer from 0 to 23, 7,19</td>
<td>7,19</td>
</tr>
</tbody>
</table>
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.power_saving.office_hour.friday</td>
<td></td>
<td>7,19</td>
</tr>
<tr>
<td>features.power_saving.office_hour.saturday</td>
<td></td>
<td>7,7</td>
</tr>
<tr>
<td>features.power_saving.office_hour.sunday</td>
<td></td>
<td>7,7</td>
</tr>
</tbody>
</table>

**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) | 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.active_backlight_level</td>
<td>Integer from 1 to 10</td>
<td>8</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th><strong>features.bluetooth_enable</strong>&lt;br&gt;Configure Bluetooth mode.&lt;br&gt;<strong>Parameter:</strong>&lt;br&gt;features.bluetooth_enable</th>
<th>Configure Bluetooth mode.&lt;br&gt;<strong>Parameter:</strong>&lt;br&gt;features.bluetooth_adapter_name&lt;br&gt;Configure the Bluetooth device name.&lt;br&gt;<strong>Parameter:</strong>&lt;br&gt;phone_setting.bluetooth_talk.enable&lt;br&gt;Configure the Bluetooth permission during the call.&lt;br&gt;<strong>Parameter:</strong>&lt;br&gt;bluetooth.a2dp_sink&lt;br&gt;Configure the Bluetooth media audio feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td>Configure Bluetooth mode. <strong>Navigate to:</strong>&lt;br&gt;http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-bluetooth&amp;q=load</td>
<td>Configure Bluetooth mode.</td>
</tr>
<tr>
<td>Phone User Interface</td>
<td>Configure Bluetooth mode.</td>
<td>Configure the Bluetooth device name.</td>
</tr>
</tbody>
</table>

**Details of the Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.bluetooth_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.bluetooth_adapter_name</td>
<td>String within 64 characters</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**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 call.

0 - Disabled
1 - Enabled

### Web User Interface:
None

### Phone User Interface:
None

| bluetooth.a2dp_sink | 0, 1 or 2 | 1 |
### Configuring Basic Features

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

#### To activate 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 activate 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:

<table>
<thead>
<tr>
<th>Line Key Type</th>
<th>Color Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Park</td>
<td>Red</td>
</tr>
<tr>
<td>Intercom</td>
<td>Red</td>
</tr>
<tr>
<td>Line</td>
<td>Green</td>
</tr>
<tr>
<td>BLF</td>
<td>Red</td>
</tr>
</tbody>
</table>
The following table shows breathing light and page icon to indicate statuses:

<table>
<thead>
<tr>
<th>Phone Models</th>
<th>Breathing Light</th>
<th>Description</th>
</tr>
</thead>
</table>
| SIP-T58V/T58A/T56A | ![Breathing Light Image](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 up to view the desired feature key) |
| CP960 | ![Breathing Light Image](Tap corresponding page icon to view the desired feature key) | \(\text{(Tap corresponding page icon to view the desired feature key)}\) |

**Procedure**

Enable page tips can be configured using the following methods.

| Central Provisioning (Configuration File) | Configure enable page tips. | Parameter: phone_setting.page_tip |
| Web User Interface | Configure enable page tips. | Navigate to: |
Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.page_tip</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>LED Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Indicates non-current pages.</td>
</tr>
<tr>
<td>Solid green</td>
<td>Indicates current page.</td>
</tr>
<tr>
<td>Flashing red</td>
<td>The BLF monitored user receives an incoming call on the non-current pages.</td>
</tr>
</tbody>
</table>

**Procedure**

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

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure page tips for the page switch keys of the expansion modules.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Parameter:</strong> expansion_module.page_tip.blf_call_in.enable</td>
</tr>
</tbody>
</table>

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>expansion_module.page_tip.blf_call_in.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A/T56A</td>
<td>&lt;=16</td>
</tr>
<tr>
<td>CP960</td>
<td>1</td>
</tr>
</tbody>
</table>

The IP phones support SIP server redundancy for account registration. For more information, refer to Server Redundancy on page 597. If you want to customize multiple DSS keys to associate with an account, refer to Multiple Line Keys per Account on page 179.

**Procedure**

Account registration can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the account registration information.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameters:</strong></td>
<td></td>
</tr>
<tr>
<td>account.X.enable</td>
<td></td>
</tr>
<tr>
<td>account.X.label</td>
<td></td>
</tr>
<tr>
<td>account.X.display_name</td>
<td></td>
</tr>
<tr>
<td>account.X.auth_name</td>
<td></td>
</tr>
<tr>
<td>account.X.user_name</td>
<td></td>
</tr>
<tr>
<td>account.X.password</td>
<td></td>
</tr>
<tr>
<td>account.X.sip_server.Y.address</td>
<td></td>
</tr>
<tr>
<td>account.X.sip_server.Y.port</td>
<td></td>
</tr>
<tr>
<td>account.X.outbound_proxy_enable</td>
<td></td>
</tr>
<tr>
<td>account.X.outbound_proxy.Y.address</td>
<td></td>
</tr>
<tr>
<td>account.X.outbound_proxy.Y.port</td>
<td></td>
</tr>
<tr>
<td>Configure the interval for the IP phone to retry to re-register when registration fails.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td></td>
</tr>
<tr>
<td>account.X.reg_fail_retry_interval</td>
<td></td>
</tr>
</tbody>
</table>

| 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 |          |
Configuring Basic Features

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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>account.X.label</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

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

<table>
<thead>
<tr>
<th>account.X.display_name</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

Description:
Configures the display name to be displayed on the called party's touch screen for
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Account: > Register > Display Name

**Phone User Interface:**
Settings: > Advanced (default password: admin) > Accounts > Display Name

<table>
<thead>
<tr>
<th>account.X.auth_name</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.user_name</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.password</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**Description:**
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the password for register authentication for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> The password for register authentication is provided by ITSP.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Account -> Register -> Password

**Phone User Interface:**
Settings -> Advanced (default password: admin) -> Accounts -> Password

<table>
<thead>
<tr>
<th>account.X.sip_server.Y.address</th>
<th>String within 256 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Y ranges from 1 to 2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 Server Y

<table>
<thead>
<tr>
<th>account.X.sip_server.Y.port</th>
<th>Integer from 0 to 65535</th>
<th>5060</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Y ranges from 1 to 2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:**
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>account.X.outbound_proxy_enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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 -> Outbound Status

<table>
<thead>
<tr>
<th><strong>account.X.outbound_proxy.Y.address</strong> (Y ranges from 1 to 2)</th>
<th>IP address or domain name</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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 Proxy Y

<table>
<thead>
<tr>
<th><strong>account.X.outbound_proxy.Y.port</strong> (Y ranges from 1 to 2)</th>
<th>Integer from 0 to 65535</th>
<th>5060</th>
</tr>
</thead>
</table>

**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)
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.1.outbound_proxy.1.port</td>
<td>5060</td>
<td></td>
</tr>
</tbody>
</table>

**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.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 171.

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

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Line Key</th>
<th>Ext Key (with expansion modules connected)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A/T56A</td>
<td>&lt;=27</td>
<td>&lt;=180</td>
</tr>
<tr>
<td>CP960</td>
<td>&lt;=30</td>
<td>/</td>
</tr>
</tbody>
</table>
The following shows two line keys associated with a registered account 1037:

![Image showing two line keys on a phone]

**Procedure**

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

| Central Provisioning (Configuration File) | Configure auto linekeys.  
Parameter:  
features.auto_linekeys.enable |
|------------------------------------------|-------------------------------------------------|
| <y0000000000xx>.cfg                     | Configure the number of DSS keys to be assigned automatically.  
Parameter:  
account.X.number_of_linekey |
| <MAC>.cfg                                | 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 |
| Web User Interface                       | |

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.auto_linekeys.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.number_of_linekey</td>
<td>Integer from 1 to 999</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.

**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) | 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.called_party_info_display.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.call_info_display_method</td>
<td>0, 1, 2, 3 or 4</td>
<td>0</td>
</tr>
</tbody>
</table>

**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) | Configure display method on dialing.  
| Parameter: | features.caller_name_type_on_dialing  
| Navigate to: |  
| 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.caller_name_type_on_dialing</td>
<td>1, 2 or 3</td>
<td>3</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP time server</td>
<td>Configuration Files, Web User Interface, Phone User Interface</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Configuration Files, Web User Interface, Phone User Interface</td>
</tr>
<tr>
<td>Time</td>
<td>Web User Interface, Phone User Interface</td>
</tr>
<tr>
<td>Time Format</td>
<td>Configuration Files, Web User Interface, Phone User Interface</td>
</tr>
<tr>
<td>Date</td>
<td>Web User Interface, Phone User Interface</td>
</tr>
<tr>
<td>Date Format</td>
<td>Configuration Files, Web User Interface</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Configuration Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Phone User Interface</td>
</tr>
<tr>
<td>Daylight Saving Time</td>
<td>Configuration Files</td>
</tr>
<tr>
<td></td>
<td>Web User Interface</td>
</tr>
</tbody>
</table>

### 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.
### Configuring Basic Features

**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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>local_time.manual_ntp_srv_prior</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
Configs 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>local_time.dhcp_time</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>IP Address or Domain Name</th>
<th>cn.pool.ntp.org</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>local_time.ntp_server1</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>local_time.ntp_server1</code></td>
<td>= 192.168.0.5</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Time &amp; Date-&gt;Primary NTP Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Basic-&gt;Time &amp; Date-&gt;General-&gt;Type (SNTP Settings) -&gt;NTP Server1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>local_time.ntp_server2</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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 &quot;local_time.ntp_server1&quot;) or cannot be accessed, the IP phone will request the time and date from the NTP server 2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>local_time.ntp_server2</code></td>
<td>= 192.168.0.6</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Time &amp; Date-&gt;Secondary NTP Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Basic-&gt;Time &amp; Date-&gt;General-&gt;Type (SNTP Settings) -&gt;NTP Server2</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>local_time.interval</code></td>
<td>Integer from 15 to 86400</td>
<td>1000</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the interval (in seconds) to update time and date from the NTP server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>local_time.interval</code></td>
<td>= 1000</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Time &amp; Date-&gt;Synchronism (15~86400s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>local_time.time_zone</code></td>
<td>-11 to +14</td>
<td>+8</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>local_time.time_zone</strong></td>
<td>String within 32 characters</td>
<td>China(Beijing)</td>
</tr>
</tbody>
</table>

**Description:**
Configures the time zone.

For more available time zones, refer to Appendix B: Time Zones on page 799.

**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**

**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 799.

**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**.

![Image of NTP configuration settings]

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.

![Image of web interface settings]
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=m od_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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>local_time.manual_time_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>local_time.time_format</th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>local_time.date_format</th>
<th>0, 1, 2, 3, 4, 5 or 6</th>
<th>0</th>
</tr>
</thead>
</table>

**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
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-MM/DD/YY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-DD MMM YYYY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6-WWW DD MMM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>local_time.summer_time</td>
<td>0, 1 or 2</td>
<td>2</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>local_time.start_time</td>
<td>Time</td>
<td>1/1/0</td>
</tr>
<tr>
<td>local_time.end_time</td>
<td>Time</td>
<td>12/31/23</td>
</tr>
</tbody>
</table>

#### 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**

**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
Configuring Basic Features

<table>
<thead>
<tr>
<th>Description:</th>
<th>Configures the end time of the Daylight Saving Time (DST).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value formats are:</td>
<td>Month/Day/Hour (for DST by Date)</td>
</tr>
<tr>
<td></td>
<td>Month/Week of Month/Day of Week/Hour of Day (for DST by Week)</td>
</tr>
<tr>
<td>If “local_time.dst_time_type” is set to 0 (DST by Date), use the mapping:</td>
<td></td>
</tr>
<tr>
<td><strong>Month</strong>:</td>
<td>1=January, 2=February,…, 12=December</td>
</tr>
<tr>
<td><strong>Day</strong>:</td>
<td>1=the first day in a month,…, 31= the last day in a month</td>
</tr>
<tr>
<td><strong>Hour</strong>:</td>
<td>0=0am, 1=1am,…, 23=11pm</td>
</tr>
<tr>
<td><strong>Example</strong>:</td>
<td>local_time.start_time = 12/12/22</td>
</tr>
<tr>
<td>If “local_time.dst_time_type” is set to 1 (DST by Week), use the mapping:</td>
<td></td>
</tr>
<tr>
<td><strong>Month</strong>:</td>
<td>1=January, 2=February,…, 12=December</td>
</tr>
<tr>
<td><strong>Week of Month</strong>:</td>
<td>1=the first week in a month,…, 5=the last week in a month</td>
</tr>
<tr>
<td><strong>Day of Week</strong>:</td>
<td>1=Monday, 2=Tuesday,…, 7=Sunday</td>
</tr>
<tr>
<td><strong>Hour of Day</strong>:</td>
<td>0=0am, 1=1am,…, 23=11pm</td>
</tr>
<tr>
<td><strong>Example</strong>:</td>
<td>local_time.start_time = 4/3/2/3</td>
</tr>
<tr>
<td><strong>Note</strong>:</td>
<td>It works only if the value of the parameter “local_time.summer_time” is set to 1 (Enabled).</td>
</tr>
</tbody>
</table>

**Web User Interface:**
Settings->Time & Date->End Date

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>local_time.offset_time</th>
<th>Integer from -300 to 300</th>
<th>Blank</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Description:</th>
<th>Configures the offset time (in minutes) of Daylight Saving Time (DST).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong>:</td>
<td>It works only if the value of the parameter “local_time.summer_time” is set to 1 (Enabled).</td>
</tr>
</tbody>
</table>

**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](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:

<table>
<thead>
<tr>
<th>Element</th>
<th>Type</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSTData</td>
<td>required</td>
<td>no</td>
<td>File root element</td>
</tr>
<tr>
<td>DST</td>
<td>required</td>
<td>no</td>
<td>Time Zone item's root element</td>
</tr>
<tr>
<td>szTime</td>
<td>required</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
  
  \( [+/-][X]:[Y], X=0~14, Y=0~59 \)   | Time Zone                          |
| szZone    | required | String (if the content is more than one city, it is the best to) | Time Zone name |
### Administrator’s Guide for SIP-TS Series Smart Media Phones

<table>
<thead>
<tr>
<th>Element</th>
<th>Type</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iType</td>
<td>optional</td>
<td>0/1</td>
<td>DST time type (This item is needed if you want to configure DST.)</td>
</tr>
<tr>
<td>szStart</td>
<td>optional</td>
<td>Month/Day/Hour (for iType=0)</td>
<td>Start time of the DST</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Month: 1~12</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Day: 1~31</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hour: 0 (midnight)~23</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Month/Week of Month/Day of Week/Hour of Day (for iType=1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Month: 1~12</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Week of Month: 1~5 (the last week)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Day of Week: 1~7</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hour of Day: 0 (midnight)~23</td>
<td></td>
</tr>
<tr>
<td>szEnd</td>
<td>optional</td>
<td>Same as szStart</td>
<td>End time of the DST</td>
</tr>
<tr>
<td>szOffset</td>
<td>optional</td>
<td>Integer from -300 to 300</td>
<td>The offset time (in minutes) of DST</td>
</tr>
</tbody>
</table>

### 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.
## Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto_dst.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Phone/Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
</tr>
<tr>
<td>Chinese Simplified</td>
</tr>
<tr>
<td>Chinese Traditional</td>
</tr>
<tr>
<td>French</td>
</tr>
<tr>
<td>German</td>
</tr>
<tr>
<td>Italian</td>
</tr>
<tr>
<td>Polish</td>
</tr>
<tr>
<td>Portuguese</td>
</tr>
<tr>
<td>Spanish</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Available Language</th>
<th>Associated Language Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>000.GUI.English.lang</td>
</tr>
<tr>
<td>Chinese Simplified</td>
<td>001.GUI.Chinese_S.lang</td>
</tr>
<tr>
<td>Chinese Traditional</td>
<td>002.GUI.Chinese_T.lang</td>
</tr>
<tr>
<td>French</td>
<td>003.GUI.French.lang</td>
</tr>
<tr>
<td>German</td>
<td>004.GUI.German.lang</td>
</tr>
<tr>
<td>Italian</td>
<td>005.GUI.Italian.lang</td>
</tr>
<tr>
<td>Polish</td>
<td>006.GUI.Polish.lang</td>
</tr>
<tr>
<td>Portuguese</td>
<td>007.GUI.Portuguese.lang</td>
</tr>
<tr>
<td>Spanish</td>
<td>008.GUI.Spanish.lang</td>
</tr>
<tr>
<td>Turkish</td>
<td>009.GUI.Turkish.lang</td>
</tr>
<tr>
<td>Russian</td>
<td>010.GUI.Russian.lang</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>000.GUI.English.lang</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 [Lang]</td>
<td></td>
</tr>
<tr>
<td>2 Name=English</td>
<td></td>
</tr>
<tr>
<td>3 FONT=Tahoma</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5 [Translate]</td>
<td></td>
</tr>
<tr>
<td>6 &quot;<em>&quot;=&quot;</em>&quot;</td>
<td></td>
</tr>
<tr>
<td>7 &quot;0s&quot;=&quot;0s&quot;</td>
<td></td>
</tr>
<tr>
<td>8 &quot;102s&quot;=&quot;102s&quot;</td>
<td></td>
</tr>
<tr>
<td>9 &quot;108s&quot;=&quot;108s&quot;</td>
<td></td>
</tr>
<tr>
<td>10 &quot;114s&quot;=&quot;114s&quot;</td>
<td></td>
</tr>
<tr>
<td>11 &quot;12s&quot;=&quot;12s&quot;</td>
<td></td>
</tr>
<tr>
<td>12 &quot;18s&quot;=&quot;18s&quot;</td>
<td></td>
</tr>
<tr>
<td>13 &quot;24s&quot;=&quot;24s&quot;</td>
<td></td>
</tr>
<tr>
<td>14 &quot;36s&quot;=&quot;36s&quot;</td>
<td></td>
</tr>
</tbody>
</table>

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 & Input -> Language.

Procedure

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

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter: gui_lang.url</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Specify the access URL of the phone user interface language pack.</td>
</tr>
</tbody>
</table>
### Configuring Basic Features

#### Delete custom LCD language packs of the phone user interface.

**Parameter:**

`gui_lang.delete`

---

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>gui_lang.url</code></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Description:**

Configures the access URL of the custom LCD language pack for the phone user interface.

**Example:**

```plaintext
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:

```plaintext
gui_lang.url = http://192.168.10.25/000.GUI.English.lang
```

**Web User Interface:**

None

**Phone User Interface:**

None

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>gui_lang.delete</code></td>
<td><code>http://localhost/all</code> or <code>http://localhost/Y.GUI.name.lang</code></td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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:

```plaintext
gui_lang.delete = http://localhost/all
```

Delete a custom language pack of the phone user interface (e.g., `001.GUI.Chinese_S.lang`):
Customizing a Language for Web User Interface

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

<table>
<thead>
<tr>
<th>Available Language</th>
<th>Associated Language Pack</th>
<th>Associated Note Language Pack</th>
</tr>
</thead>
<tbody>
<tr>
<td>English</td>
<td>1.English.js</td>
<td>1.English&gt;Note.xml</td>
</tr>
<tr>
<td>Chinese Simplified</td>
<td>2.Chinese_S.js</td>
<td>2.Chinese_S&gt;Note.xml</td>
</tr>
<tr>
<td>French</td>
<td>4.French.js</td>
<td>4.French&gt;Note.xml</td>
</tr>
<tr>
<td>German</td>
<td>5.German.js</td>
<td>5.German&gt;Note.xml</td>
</tr>
<tr>
<td>Italian</td>
<td>6.Italian.js</td>
<td>6.Italian&gt;Note.xml</td>
</tr>
<tr>
<td>Polish</td>
<td>7.Polish.js</td>
<td>7.Polish&gt;Note.xml</td>
</tr>
<tr>
<td>Portuguese</td>
<td>8.Portuguese.js</td>
<td>8.Portuguese&gt;Note.xml</td>
</tr>
<tr>
<td>Turkish</td>
<td>10.Turkish.js</td>
<td>10.Turkish&gt;Note.xml</td>
</tr>
<tr>
<td>Russian</td>
<td>11.Russian.js</td>
<td>11.Russian&gt;Note.xml</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the access URL of the custom language pack for web user interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td>wui_lang.url</td>
</tr>
<tr>
<td>Specify the access URL of the custom Note language pack for web user interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td>wui_lang_note.url</td>
</tr>
<tr>
<td>Delete custom language packs and Note language packs of the web user interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td>wui_lang.delete</td>
</tr>
</tbody>
</table>

**Details of the Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>wui_lang.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Description:**

Configures the access URL of the custom language pack for the web user interface.

**Example:**


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:


**Web User Interface:**
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Phone User Interface:

None

#### wui_lang_note.url

- **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
  ```

#### Web User Interface:

None

#### wui_lang.delete

- **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.

#### Phone User Interface:

None
Specifying the Language to Use

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

Procedure

Specify the language for the phone user interface or the web user interface using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameters:</th>
<th>Specify the languages for the phone user interface and the web user interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>static.lang.gui</td>
<td></td>
</tr>
<tr>
<td></td>
<td>static.lang.wui</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Navigate to:</th>
<th>Specify the language for the web user interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=settings-preference&amp;q=load</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th>Specify the language for the phone user interface.</th>
<th></th>
</tr>
</thead>
</table>

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.lang.gui</td>
<td>Refer to the following content</td>
<td>English</td>
</tr>
</tbody>
</table>

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.
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>static.lang.gui = English</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If you want to use the custom language (e.g., Guilan) for the IP phone, configure the parameter &quot;static.lang.gui = Guilan&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings&gt;Basic&gt;Language</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>static.lang.wui</th>
<th>Refer to the following content</th>
<th>English</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the language used on the web user interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Permitted Values:</strong></td>
<td>English, Chinese_S, Chinese_T, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian or the custom language name.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>static.lang.wui = English</td>
<td></td>
</tr>
<tr>
<td>If you want to use the custom language (e.g., Wuilan) for the IP phone, configure the parameter &quot;static.lang.wui = Wuilan&quot;.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>If the language of your browser is not supported by the IP phone, the web user interface will use English by default.</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Settings&gt;Preference&gt;Language</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**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 216.

**Note**

It is not applicable to CP960 IP phones.

**Procedure**

Softkey layout can be configured using the following methods.

| Central Provisioning (Configuration File) | 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:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.custom_softkey_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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](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.

<table>
<thead>
<tr>
<th>Call State</th>
<th>Default Soft Keys</th>
<th>Optional Soft Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallFailed (Call Fail)</td>
<td>NewCall</td>
<td>End Call</td>
</tr>
<tr>
<td>CallIn (Incoming Call)</td>
<td>Answer</td>
<td>Switch</td>
</tr>
<tr>
<td></td>
<td>Forward</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Silence</td>
<td></td>
</tr>
<tr>
<td>Call State</td>
<td>Default Soft Keys</td>
<td>Optional Soft Keys</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Connecting</td>
<td>End Call</td>
<td>Switch</td>
</tr>
<tr>
<td>SemiAttendTrans (Transfer</td>
<td>Transfer</td>
<td></td>
</tr>
<tr>
<td>Connecting)</td>
<td>End Call</td>
<td></td>
</tr>
<tr>
<td>RingBack</td>
<td>End Call</td>
<td>Switch</td>
</tr>
<tr>
<td>SemiAttendTrans Back (Transfer</td>
<td>Transfer</td>
<td></td>
</tr>
<tr>
<td>Ring Back)</td>
<td>End Call</td>
<td></td>
</tr>
<tr>
<td>Talk (On Talk)</td>
<td>Transfer</td>
<td>Mute</td>
</tr>
<tr>
<td></td>
<td>Hold</td>
<td>SWAP</td>
</tr>
<tr>
<td></td>
<td>Conference</td>
<td>NewCall</td>
</tr>
<tr>
<td></td>
<td>End Call</td>
<td>Switch</td>
</tr>
<tr>
<td>Hold</td>
<td>End Call</td>
<td>Answer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reject</td>
</tr>
<tr>
<td>Held</td>
<td></td>
<td>PriHold</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Park</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GPark</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RTP Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record</td>
</tr>
<tr>
<td>Conferenced</td>
<td>Hold</td>
<td>Switch</td>
</tr>
<tr>
<td></td>
<td>Split</td>
<td>Answer</td>
</tr>
<tr>
<td></td>
<td>End Call</td>
<td>Reject</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mute</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RTP Status</td>
</tr>
</tbody>
</table>
When editing a softkey layout template, learn the following:

- `<CallStates>` indicates the start of a template and `</CallStates>` 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 disable, 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)  
<y000000000xx>.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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom_softkey_call_failed.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

Description:
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>custom_softkey_call_failed.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>custom_softkey_call_in.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>custom_softkey_connecting.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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**

**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**

**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.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>custom softkey ring_back.url</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the access URL of the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>custom file for the soft key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>presented on the touch screen</td>
<td></td>
<td></td>
</tr>
<tr>
<td>when in the RingBack state.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>custom_softkey_ring_back.url =</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://192.168.1.20/XMLfiles/RingBack.xml">http://192.168.1.20/XMLfiles/RingBack.xml</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>During the auto provisioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>process, the IP phone connects to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the provisioning server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;192.168.1.20&quot;, and downloads the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RingBack state file from the &quot;XMLfiles&quot; directory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>custom softkey talking.url</strong></td>
<td>URL within 511</td>
<td>Blank</td>
</tr>
<tr>
<td>characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the access URL of the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>custom file for the soft key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>presented on the touch screen</td>
<td></td>
<td></td>
</tr>
<tr>
<td>when in the Talking state.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>custom_softkey_talking.url =</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://192.168.1.20/XMLfiles/Talking.xml">http://192.168.1.20/XMLfiles/Talking.xml</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>During the auto provisioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>process, the IP phone connects to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the provisioning server</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;192.168.1.20&quot;, and downloads the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Talking state file from the &quot;XMLfiles&quot; directory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 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) | Configure a send key.  
Parameter:  
features.key_as_send |
| ---------------------------------------- | --- |
| <y000000000xx>.cfg               | Configure a send tone.  
Parameter:  
features.send_key_tone |
| 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.key_as_send</td>
<td>0, 1 or 2</td>
<td>1</td>
</tr>
</tbody>
</table>

**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 or taps any key on the onscreen dial pad.

**Note:** Keypad is not applicable to CP960 IP phones.

**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 taps/presses a send key.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-Enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If it is set to 1 (Enabled), the IP phone will play a key tone when a user taps/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 to dial out “##” when the user only presses the # key on dialing screen or pre-dialing screen.

0-Disabled

1-Enabled

If it is set to 0 (Disabled), the IP phone will dial out “#” when the user presses the # key for the second time.

If it is set to 1 (Enabled), the IP phone will dial out “##” when the user presses the # key for the third time.

**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.

![Send Pound Key Setting](image)

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:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>The dot &quot;.&quot; can be used as a placeholder or multiple placeholders for any string. Example: &quot;12.&quot; would match &quot;123&quot;, &quot;1234&quot;, &quot;12345&quot;, &quot;12abc&quot;, etc.</td>
</tr>
<tr>
<td>x</td>
<td>The &quot;x&quot; can be used as a placeholder for any character. Example: &quot;12x&quot; would match &quot;121&quot;, &quot;122&quot;, &quot;123&quot;, &quot;12a&quot;, etc.</td>
</tr>
<tr>
<td>-</td>
<td>The dash &quot;-&quot; can be used to match a range of characters within the brackets. Example: &quot;[5-7]&quot; would match the number &quot;5&quot;, &quot;6&quot; or &quot;7&quot;.</td>
</tr>
<tr>
<td>,</td>
<td>The comma &quot;,&quot; can be used as a separator within the bracket. Example: &quot;[2,5,8]&quot; would match the number &quot;2&quot;, &quot;5&quot; or &quot;8&quot;.</td>
</tr>
<tr>
<td>[]</td>
<td>The square bracket &quot;[]&quot; can be used as a placeholder for a single character which matches any of a set of characters. Example: &quot;91[5-7]1234&quot; would match &quot;9151234&quot;, &quot;9161234&quot;, &quot;9171234&quot;.</td>
</tr>
<tr>
<td>()</td>
<td>The parenthesis &quot;()&quot; can be used to group together patterns, for instance, to logically combine two or more patterns. Example: &quot;((1-9)(2-7))3&quot; would match &quot;923&quot;, &quot;153&quot;, &quot;673&quot;, etc.</td>
</tr>
<tr>
<td>$</td>
<td>The &quot;$&quot; 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: &quot;001(xxx)45(xx)&quot;, Replace: &quot;9001$145$2&quot;. When you dial out &quot;0012354599&quot; on your phone, the IP phone will replace the number with &quot;900123545999&quot;. &quot;$1&quot; means 3 digits in the first parenthesis, that is, &quot;235&quot;: &quot;$2&quot; means 2 digits in the second parenthesis, that is, &quot;99&quot;.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Create the replace rule for the IP phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters:</td>
<td></td>
</tr>
<tr>
<td>dialplan.replace.prefix.X</td>
<td></td>
</tr>
<tr>
<td>dialplan.replace.replace.X</td>
<td></td>
</tr>
<tr>
<td>dialplan.replace.line_id.X</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Create the replace rule for the IP phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to:</td>
<td></td>
</tr>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=settings-dialplan&amp;q=load</td>
<td></td>
</tr>
</tbody>
</table>

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialplan.replace.prefix.X (X ranges from 1 to 100)</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>dialplan.replace.replace.X (X ranges from 1 to 100)</th>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the alternate number to replace the entered number.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dialplan.replace.prefix.1 = 1 and dialplan.replace.replace.1 = 254245</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When you enter the number “1” and press the send key, the number “254245” will replace the entered number “1”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the values of the parameters &quot;dialplan.digitmap.enable” and “account.X.dialplan.digitmap.enable” are set to 0 (Disabled).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings -&gt; Dial Plan -&gt; Replace Rule -&gt; Replace</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dialplan.replace.line_id.X**
(X ranges from 1 to 100)

**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)
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](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.

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A/T56A</td>
<td>0–16</td>
<td>0 stands for all lines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1–16 stand for line1–line16</td>
</tr>
<tr>
<td>CP960</td>
<td>0, 1</td>
<td>0 stands for all lines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 stand for line1</td>
</tr>
</tbody>
</table>

- At most 100 replace rules can be added to the IP phone.
Configuring Basic Features

The expression syntax in the replace rule template is the same as that introduced in the section Dial Plan on page 226.

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:
   
   ```xml
   <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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Specifying the access URL of the replace rule template:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Parameter: dialplan_replace_rule.url</td>
</tr>
</tbody>
</table>

Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialplan_replace_rule.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

Description:
Configures the access URL of the replace rule template file.
### Dial-plan Replace Rule

The dialplan_replace_rule parameter allows downloading of a replace rule file during auto provisioning. Its structure is as follows:

```
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

#### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>dialplan_replace_rule.url = <a href="http://192.168.10.25/dialplan.xml">http://192.168.10.25/dialplan.xml</a></td>
<td></td>
</tr>
</tbody>
</table>

#### 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 235.

#### 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) | <y000000000xx>.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:** | |

---

232
### Configuring Basic Features

**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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialplan.dialnow.rule.X</td>
<td>String within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>(X ranges from 1 to 100)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:**

```markdown
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).

**Web User Interface:**

Settings->Dial Plan->Dial-now->Rule

**Phone User Interface:**

None

<table>
<thead>
<tr>
<th>dialplan.dialnow.line_id.X</th>
<th>0, Integer from 1 to 16</th>
<th>Blank (for all lines)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X ranges from 1 to 100)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:**

```markdown
dialplan.dialnow.line_id.1 = 1,2
```
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.dialnow_delay</td>
<td>Integer from 0 to 14</td>
<td>1</td>
</tr>
</tbody>
</table>

**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

**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.

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A/T56A</td>
<td>0~16</td>
<td>0 stands for all lines 1<del>16 stand for line1</del>line16</td>
</tr>
<tr>
<td>CP960</td>
<td>0, 1</td>
<td>0 stands for all lines 1 stand for line1</td>
</tr>
</tbody>
</table>

- 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 226.

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:

```xml
<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.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<DialNow>
  <Data DialNowRule="123" LineID="1,2,3" />
  <Data DialNowRule="456" LineID="1,2,3" />
  <Data DialNowRule="1001" LineID="0" />
</DialNow>
```
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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure the access URL of the dial-now template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Parameter:</td>
</tr>
<tr>
<td></td>
<td>dialplan_dialnow.url</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialplan_dialnow.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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:**

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.

<table>
<thead>
<tr>
<th>Central Provisioning</th>
<th>Create the area code rule and specify the maximum and minimum lengths of</th>
</tr>
</thead>
</table>
Administrator’s Guide for SIP-T5 Series Smart Media Phones

(Configuration File) 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialplan.area_code.code</td>
<td>String within 16 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

Description:
Configures the area code to be added before the entered numbers when dialing out.

Example:
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:
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings -&gt; Dial Plan -&gt; Area Code -&gt; Min Length (1-15)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**dialplan.area_code.max_len**

<table>
<thead>
<tr>
<th>Integer from 1 to 15</th>
<th>15</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>dialplan.area_code.line_id</th>
<th>0, Integer from 1 to 16</th>
<th>Blank (for all lines)</th>
</tr>
</thead>
</table>

**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.

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Create the block out rule for the IP phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;y0000000000xx&gt;.cfg</code></td>
<td>Parameters:</td>
</tr>
<tr>
<td></td>
<td><code>dialplan.block_out.number.X</code></td>
</tr>
<tr>
<td></td>
<td><code>dialplan.block_out.line_id.X</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Create the block out rule for the IP phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Navigate to:</td>
</tr>
<tr>
<td></td>
<td><code>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=settings-dialplan&amp;q=load&amp;dial_page=block-out</code></td>
</tr>
</tbody>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dialplan.block_out.number.X</code> (X ranges from 1 to 10)</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dialplan.block_out.number.X</strong> (X ranges from 1 to 10)</td>
<td>0, Integer from 1 to 16</td>
<td>Blank (for all lines)</td>
</tr>
</tbody>
</table>

**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)

**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.

**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](https://tools.ietf.org/html/rfc3435), 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:

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>T</strong></td>
<td>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&lt;tx&gt;, x can be a digit from 0 to 99), a complete match occurs when waiting x seconds after inputting 123.</td>
</tr>
<tr>
<td><strong>x</strong></td>
<td>The “x” can be used as a placeholder for any digit from 0 to 9. Example: “12x” would match “121”, “122”, “123”, etc.</td>
</tr>
<tr>
<td><strong>[]</strong></td>
<td>The square bracket “[]” can be used as a placeholder for a single character which matches any of a set of characters. Example: “91[5-7]1234” would match “9151234”, “9161234”, “9171234”.</td>
</tr>
<tr>
<td><strong>-</strong></td>
<td>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”. <strong>Note:</strong> The digits must be concrete, e.g., [3-x] is invalid.</td>
</tr>
<tr>
<td>The dot &quot;.&quot; can be used as a placeholder or multiple placeholders, including zero, of occurrences of the preceding construct. Examples: “123.T” would match “123”, “1233”, “12333”, “123333”, etc. “x.T” would match an arbitrary number. “[x#+].T” would match an arbitrary character. <strong>Note:</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>The letter “R” indicates that certain matched strings are replaced. Using a RRR syntax, you can replace the digits between the first two Rs with the digits between the last two Rs. Example: “R12R234R” would replace 12 with 234.</td>
<td></td>
</tr>
<tr>
<td>The letter “:” in the angle bracket indicates that certain matched strings are replaced. Using the &lt;:&gt; syntax, you can replace the digits before the colon with the digits after the colon. Example: “&lt;12:234&gt;” would replace 12 with 234. It is the same with R12R234R.</td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>The comma “,“ can be used as a separator to generate secondary dial tone. Example: “&lt;9,.55&gt;xx”, after entering digit “9”, secondary dial tone plays and you can complete the remaining two-digit number. <strong>Note:</strong> The secondary dial tone can be customized. For more information, refer to Tones on page 646.</td>
<td></td>
</tr>
</tbody>
</table>


## 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.history_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.history_dial`
    - `account.X.dialplan.digitmap.apply_to.forward`
    - `account.X.dialplan.digitmap.apply_to.press_send`

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dialplan.digitmap.enable</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>dialplan.digitmap.string</td>
<td>String within 2048 characters</td>
<td></td>
</tr>
</tbody>
</table>

**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

**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 = 1xxTxxxxx<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:**
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|OT, 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)
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>dialplan.digitmap.no_match_action</th>
<th>0, 1 or 2</th>
<th>0</th>
</tr>
</thead>
</table>

**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 configured by this parameter.

**Web User Interface:**
None

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>dialplan.digitmap.active.on_hook_dialing</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

**Description:**
Enables or disables the entered numbers to match the predefined string of the digit map in
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialplan.digitmap.apply_to.on_hook_dial</td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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. On-hook dialing is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>dialplan.digitmap.apply_to.directory_dial</td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the digit map to be applied to the numbers dialed from the directory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialplan.digitmap.apply_to.history_dial</td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td>dialplan.digitmap.apply_to.forward</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**

Enables or disables the digit map to be applied to the numbers (received calls or missed calls) dialed from call log lists.

- **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.history_dial" takes precedence over that configured by this parameter.

**Web User Interface:**

None

**Phone User Interface:**

None

---

**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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>dialplan.digitmap.apply_to.press_send</code></td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.
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)

<table>
<thead>
<tr>
<th>Per-Line Parameters</th>
<th>Global Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.dialplan.digitmap.enable</td>
<td>dialplan.digitmap.enable</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.string</td>
<td>dialplan.digitmap.string</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.interdigit_long_timer</td>
<td>dialplan.digitmap.interdigit_long_timer</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.interdigit_short_timer</td>
<td>dialplan.digitmap.interdigit_short_timer</td>
</tr>
<tr>
<td>Per-Line Parameters</td>
<td>Global Parameters</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.no_match_action</td>
<td>dialplan.digitmap.no_match_action</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.active.on_hook_dialing</td>
<td>dialplan.digitmap.active.on_hook_dialing (not applicable to CP960 IP phones)</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.apply_to.on_hook_dial</td>
<td>dialplan.digitmap.apply_to.on_hook_dial</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.apply_to.directory_dial</td>
<td>dialplan.digitmap.apply_to.directory_dial</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.apply_to.history_dial</td>
<td>dialplan.digitmap.apply_to.history_dial</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.apply_to.forward</td>
<td>dialplan.digitmap.apply_to.forward</td>
</tr>
<tr>
<td>account.X.dialplan.digitmap.apply_to.press_send</td>
<td>dialplan.digitmap.apply_to.press_send</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure the emergency dialplan. Parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y000000000xx&gt;.cfg</td>
<td>dialplan.emergency.asserted_id_source</td>
</tr>
<tr>
<td></td>
<td>dialplan.emergency.custom_asserted_id</td>
</tr>
<tr>
<td></td>
<td>dialplan.emergency.server.X.address</td>
</tr>
<tr>
<td></td>
<td>dialplan.emergency.server.X.port</td>
</tr>
<tr>
<td></td>
<td>dialplan.emergency.server.X.transport_type</td>
</tr>
<tr>
<td></td>
<td>dialplan.emergency.X.value</td>
</tr>
<tr>
<td></td>
<td>dialplan.emergency.X.server_priority</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialplan.emergency.asserted_id_source</td>
<td>ELIN or CUSTOM</td>
<td>ELIN</td>
</tr>
</tbody>
</table>

**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).
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 “dialplan.emergency.custom_asserted_id” is left blank, the LLDP-MED ELIN value will be used. <strong>Note:</strong> 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. <strong>Web User Interface:</strong> None <strong>Phone User Interface:</strong> None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dialplan.emergency.custom_asserted_id</td>
<td>10-25 digits, SIP URI, or TEL URI</td>
<td>Blank</td>
</tr>
<tr>
<td>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., <a href="">tel:+16045558000</a>). If using a SIP URI, for example, sip:<a href="mailto:1234567890123@abc.com">1234567890123@abc.com</a>. The full URI is included in the P-Asserted-Identity (PAI) header and the address will be replaced by the emergency server (e.g., <a href="">sip:1234567890123@emergency.com</a>). 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., <a href="">sip:1234567890@abc.com</a>). <strong>Web User Interface:</strong> None <strong>Phone User Interface:</strong> None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dialplan.emergency.server.X.address</td>
<td>IP address or domain name</td>
<td>Blank</td>
</tr>
<tr>
<td>(X ranges from 1 to 3) Description: Configures the IP address or domain name of the emergency server X to be used for routing calls. <strong>Note:</strong> 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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>server&gt;emergency server; if the account is not registered, the emergency server will be used.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
None

**Phone User Interface:**
None

dialplan.emergency.server.X.port
(X ranges from 1 to 3)

<table>
<thead>
<tr>
<th>Integer from 1 to 65535</th>
<th>5060</th>
</tr>
</thead>
</table>

**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)

<table>
<thead>
<tr>
<th>0, 1, 2 or 3</th>
<th>0</th>
</tr>
</thead>
</table>

**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)

<table>
<thead>
<tr>
<th>number or SIP URI</th>
<th>Refer to the following content</th>
</tr>
</thead>
</table>

**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;
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>When $X = 2-255$, the default value is Blank.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
None

**Phone User Interface:**
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
It works only if the Off Hook Hot Line Dialing feature is disabled. For more information, refer to Off Hook Hot Line Dialing on page 258.

**Procedure**

Hotline can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y000000000xx&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the hotline number.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td></td>
</tr>
<tr>
<td>features.hotline_number</td>
<td></td>
</tr>
</tbody>
</table>

Specify the time the IP phone waits before automatically dialing out the hotline number.

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure the hotline number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the time the IP phone waits before automatically dialing out the hotline number.</td>
<td></td>
</tr>
<tr>
<td><strong>Navigate to:</strong></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th>Configure the hotline number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify the time the IP phone waits before automatically dialing out the hotline number.</td>
<td></td>
</tr>
</tbody>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.hotline_number</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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
### Parameter: `features.hotline_delay`

<table>
<thead>
<tr>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer from 0 to 10</td>
<td>4</td>
</tr>
</tbody>
</table>

**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

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure off hook hot line dialing feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Parameter:</strong> account.X.auto_dial_enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify the number that the phone first dials out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Parameter:</strong> account.X.auto_dial_num</td>
</tr>
</tbody>
</table>

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.auto_dial_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.auto_dial_num</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 the meaning of each variable in the super search template file:

<table>
<thead>
<tr>
<th>Element</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>root_super_search</td>
<td>No</td>
<td>File root element</td>
</tr>
<tr>
<td>Item</td>
<td>No</td>
<td>Super search list’s root element</td>
</tr>
<tr>
<td>id_name</td>
<td></td>
<td>File root element</td>
</tr>
<tr>
<td></td>
<td>local_directory_search</td>
<td>The directory list. For example, “local_directory_search” for the local directory list.</td>
</tr>
<tr>
<td></td>
<td>calllog_search</td>
<td>The directory list. For example, “calllog_search” for the calllog list.</td>
</tr>
<tr>
<td></td>
<td>remote_directory_search</td>
<td>The directory list. For example, “remote_directory_search” for the remote directory list.</td>
</tr>
<tr>
<td></td>
<td>ldap_search</td>
<td>The directory list. For example, “ldap_search” for the LDAP list.</td>
</tr>
<tr>
<td></td>
<td>BroadsFlip_directory_search</td>
<td>The directory list. For example, “BroadsFlip_directory_search” for the BroadsFlip directory list.</td>
</tr>
<tr>
<td>display_name</td>
<td></td>
<td>The display name of the directory list.</td>
</tr>
<tr>
<td></td>
<td>Local Contacts</td>
<td>The display name of the directory list.</td>
</tr>
<tr>
<td></td>
<td>History</td>
<td>The display name of the directory list.</td>
</tr>
<tr>
<td></td>
<td>Remote Phonebook</td>
<td>The display name of the directory list.</td>
</tr>
<tr>
<td></td>
<td>LDAP</td>
<td>The display name of the directory list.</td>
</tr>
<tr>
<td></td>
<td>Network Directories</td>
<td>The display name of the directory list.</td>
</tr>
<tr>
<td>priority</td>
<td>1, 2, 3, 4 and 5.</td>
<td>The priority of the search results.</td>
</tr>
<tr>
<td></td>
<td>1 is the highest priority, 5 is the lowest.</td>
<td>The priority of the search results.</td>
</tr>
<tr>
<td>enable</td>
<td>0/1, 0: Disabled 1: Enabled</td>
<td>Enable or disable the IP phone to search the desired directory list.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Specify the access URL of the super search template file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y000000000xx&gt;.cfg</td>
<td>Parameter: super_search.url</td>
</tr>
<tr>
<td>Web User Interface</td>
<td>Configure the search source list in dialing.</td>
</tr>
<tr>
<td></td>
<td>Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=contacts-favorite&amp;q=load</td>
</tr>
</tbody>
</table>

### Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>super_search.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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 823.

**Procedure**

Call log can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure call log feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y000000000xx&gt;.cfg</td>
<td>Parameter:</td>
</tr>
<tr>
<td></td>
<td>features.save_call_history</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure call log feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Navigate to:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

| Phone User Interface                      | Configure call log feature. |
Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.save_call_history</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.

**Note:** To log the missed calls, the value of the parameter “account.X.missed_calllog” should be set to 1 (Enabled).

**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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.call_log_show_num</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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:**
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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure missed call log feature. Parameter: account.X.missed_calllog</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td></td>
<td>Configure missed call log feature. Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-basic&amp;q=load&amp;acc=0</td>
</tr>
</tbody>
</table>

Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.missed_calllog</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Element</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>root_group</td>
<td>no</td>
<td>Group list's root element.</td>
</tr>
<tr>
<td>group</td>
<td>no</td>
<td>Group’s root element.</td>
</tr>
<tr>
<td>display_name</td>
<td>All Contacts</td>
<td>An element of group. Group name.</td>
</tr>
<tr>
<td></td>
<td>Blacklist</td>
<td></td>
</tr>
<tr>
<td>root_contact</td>
<td>no</td>
<td>Contact list’s root element.</td>
</tr>
<tr>
<td>contact</td>
<td>no</td>
<td>Contact’s root element.</td>
</tr>
<tr>
<td>display_name</td>
<td>String</td>
<td>An element of contact. Contact name. <strong>Note:</strong> This value cannot be blank or duplicated.</td>
</tr>
<tr>
<td>office_number</td>
<td>String</td>
<td>Office number of the contact.</td>
</tr>
<tr>
<td>mobile_number</td>
<td>String</td>
<td>Mobile number of the contact.</td>
</tr>
<tr>
<td>Element</td>
<td>Values</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>other_number</td>
<td>String</td>
<td>Other number of the contact.</td>
</tr>
<tr>
<td>line</td>
<td>-1~15; Multiple line IDs are separated by commas.</td>
<td>The desired line you want to add the contact to. Note: It is not applicable to CP960 IP phones.</td>
</tr>
<tr>
<td>ring</td>
<td>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</td>
<td>An element of contact. Contact ring tone.</td>
</tr>
<tr>
<td>group_id_name</td>
<td>Valid Value: built-in: All Contacts, Blacklist custom: XXX (e.g., Friend)</td>
<td>Group name of a contact.</td>
</tr>
<tr>
<td>default_photo</td>
<td>Format of the value: Resource: avatar and icon name (the built-in picture) Config: avatar and icon name (the custom picture)</td>
<td>Contact avatar and icon.</td>
</tr>
</tbody>
</table>

The following table lists valid values of line for each phone model.

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A/T56A</td>
<td>-1~15</td>
<td>-1 stands for Auto (the first registered line) 0<del>15 stand for line1</del>line16</td>
</tr>
</tbody>
</table>

**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
Configuring Basic Features

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=""
  rings="" 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 provisioning 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
The following shows the custom avatars downloaded from the provisioning server:

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 icons downloaded from the provisioning server:
# Configuring Local Directory

## Procedure

Local directory be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y000000000xx&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter:</strong></td>
<td>local_contact.data.url</td>
</tr>
<tr>
<td>Specify the access URL of the local contact file.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td>local_contact.photo.url</td>
</tr>
<tr>
<td>Specify the access URL of a contact avatar &amp; icon file.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td>local_contact.image.url</td>
</tr>
<tr>
<td>Specify the access URL of a TAR contact avatar &amp; icon file.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td>local_contact.data_photo_tar.url</td>
</tr>
<tr>
<td>Specify the access URL of the compressed TAR file consisting of the avatars &amp; icon TAR file and contact XML file.</td>
<td></td>
</tr>
</tbody>
</table>

| 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://<phoneIPAddess>/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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>local_contact.data.url</td>
<td>URL within 511</td>
<td>Blank</td>
</tr>
</tbody>
</table>
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>local_contact.data.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>local_contact.photo.url</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>local_contact.image.url</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>local_contact.data_photo_tar.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure live dialpad.</td>
<td>Parameters:</td>
</tr>
<tr>
<td>phone_setting.predial_autodial</td>
<td>phone_setting.inter_digit_time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure live dialpad.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to:</td>
<td>http://&lt;phoneIPAdddress&gt;/servlet?m=mod_data&amp;p=settings.preference&amp;q=load</td>
</tr>
</tbody>
</table>

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.predial_autodial</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.inter_digit_time</td>
<td>Integer from 1 to 14</td>
<td>4</td>
</tr>
</tbody>
</table>

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:
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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter: linekey.X.type/ programablekey.X.type/</th>
<th>Assign a speed dial key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y000000000xx&gt;.cfg</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Speed Dial Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

#### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/programablekey.X.type/</td>
<td>13</td>
<td>Refer to the following content</td>
</tr>
<tr>
<td>expansion_module.X.key.Y.type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:**
## Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>For line keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For SIP-T58V/T58A/T56A IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For CP960 IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For programable keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For SIP-T58V/T58A/T56A IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When X=12, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When X=13, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When X=14, the default value is 2 (Forward).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For ext keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For SIP-T58V/T58A/T56A IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When Y= 1 to 60, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> EXT key is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSSKey-&gt;Line Key/Programable Key-&gt;Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;DSS Keys-&gt;Line Key X-&gt;Type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>linekey.X.line/programablekey.X.line/ expansion_module.X.key.Y.line</th>
<th>Refer to the following content</th>
<th>1-16 for lines 1-16, 1 for programable keys</th>
</tr>
</thead>
</table>

### 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
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-Line 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16-Line 16</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

linekey.2.line = 1

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey->Line Key/Programable Key->Line

**Phone User Interface:**

Settings->Features->DSS Keys->Line Key X->Account ID

### 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

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey->Line Key/Programable Key->Value

**Phone User Interface:**

Settings->Features->DSS Keys->Line Key X->Value

### 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)
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X ranges from 1 to 30 (for CP960)</td>
<td>For ext keys: X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)</td>
<td>Note: EXT key is not applicable to CP960 IP phones.</td>
</tr>
</tbody>
</table>

**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 Programmable 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 646.

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) | Configure call waiting and call waiting tone. **Parameters:**
|------------------------------------------|---------------------------------|
| <y000000000xx>.cfg | call_waiting.enable  
call_waiting.tone  
call_waiting.on_code  
call_waiting.off_code |

| Web User Interface | Configure call waiting. **Navigate to:**
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

| Phone User Interface | Configure call waiting tone. **Navigate to:**
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>http://&lt;phone IPAddress&gt;/servlet?m=mod_data&amp;p=features-audio&amp;q=load</td>
</tr>
</tbody>
</table>
**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>call_waiting.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>call_waiting.tone</th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>call_waiting.on_code</th>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>
### call_waiting.on_code

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>call_waiting.on_code = *71</td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td>Features-&gt;General Information-&gt;Call Waiting On Code</td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td>Settings-&gt;Features-&gt;Call Waiting-&gt;On Code</td>
<td></td>
</tr>
<tr>
<td>call_waiting.off_code</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

### call_waiting.off_code

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>call_waiting.off_code = *72</td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td>Features-&gt;General Information-&gt;Call Waiting Off Code</td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td>Settings-&gt;Features-&gt;Call Waiting-&gt;Off Code</td>
<td></td>
</tr>
</tbody>
</table>

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) | Configure auto redial feature. Parameters: auto_redial.enable auto_redial.interval auto_redial.times |
| Phone User Interface | Configure auto redial feature. |

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto_redial.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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).
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; General Information -&gt; Auto Redial Interval (1~300s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings -&gt; Features -&gt; Auto Redial -&gt; Redial Interval</td>
<td></td>
<td></td>
</tr>
<tr>
<td>auto_redial.times</td>
<td>Integer from 1 to 300</td>
<td>10</td>
</tr>
</tbody>
</table>

**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:**

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 646.

**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 299.

**Procedure**

Auto answer can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter:</th>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt;.cfg</td>
<td>account.X.auto_answer</td>
<td>Configure auto answer and auto answer mute.</td>
</tr>
<tr>
<td></td>
<td>account.X.auto_answer_mute_enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>features.auto_answer_delay</td>
<td>Specify a period of delay time for auto answer.</td>
</tr>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>features.auto_answer_tone.enable</td>
<td>Configure auto answer tone.</td>
</tr>
</tbody>
</table>
Configuring Basic Features

### 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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.auto_answer</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

| parameters.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.
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter “account.X.auto_answer” is set to 1 (Enabled).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Web User Interface:
Features- > General Information- > Auto-Answer Delay(1~4s)

#### Phone User Interface:
None

<table>
<thead>
<tr>
<th>features.auto_answer_tone.enable</th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

**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 “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

<table>
<thead>
<tr>
<th>account.X.auto_answer_mute_enable</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

(X is equal to 1)

**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 300.

**Procedure**

IP direct auto answer can only be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure IP direct auto answer feature.</th>
<th><strong>Parameter:</strong> features.ip_call.auto_answer.enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td>Configure IP direct auto answer feature.</td>
<td><strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.ip_call.auto_answer.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**

Enables or disables the auto answer feature for IP call.

0 - Disabled

1 - Enabled
### Administrator’s Guide for SIP-T5 Series Smart Media Phones

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow IP Call</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter:</th>
</tr>
</thead>
<tbody>
<tr>
<td>$y0000000000xx.cfg$</td>
<td>features.direct_ip_call_enable</td>
</tr>
</tbody>
</table>
Configuring Basic Features

### Web User Interface

Configure allow IP call.

**Navigate to:**

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

### Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.direct_ip_call_enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**

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 300.

**Procedure**

Accept SIP trust server only can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure accept SIP trust server only.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Parameter: sip.trust_ctrl</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure accept SIP trust server only.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Navigate to:</strong></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.trust_ctrl</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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**.

![Image of Yealink phone settings](image)

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:

```plaintext
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
```
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">
</dialog>
<dialog id="65622">
</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
```
Configuring Basic Features

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 S8.80.0.5
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="/ip_address:5060">
<dialog id="65644">
<state>terminated</state>
</dialog>
</dialog-info>

Procedure

Call completion can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure call completion.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Parameter: features.call_completion_enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure call completion.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to:</td>
<td></td>
</tr>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th>Configure call completion.</th>
</tr>
</thead>
</table>

Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.call_completion_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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.
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 5.80.0.5
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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt;.cfg</td>
</tr>
<tr>
<td><strong>Parameters:</strong></td>
</tr>
<tr>
<td>account.X.anonymous_call</td>
</tr>
<tr>
<td>account.X.send_anonymous_code</td>
</tr>
<tr>
<td>account.X.anonymous_call_oncode</td>
</tr>
<tr>
<td>account.X.anonymous_call_offcode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure anonymous call. Navigate to:</td>
</tr>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-basic&amp;q=load&amp;acc=0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure anonymous call.</td>
</tr>
</tbody>
</table>

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.anonymous_call</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.send_anonymous_code</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.anonymous_call_oncode</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>
Configuring Basic Features

### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

### 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.

![](image)

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:

```sno
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
```
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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure anonymous call rejection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.reject_anonymous_call</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.send_anonymous_rejection_code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.anonymous_reject_oncode</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.anonymous_reject_offcode</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure anonymous call rejection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to:</td>
<td></td>
</tr>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;pt=account-basic&amp;q=load&amp;acc=0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th>Configure anonymous call rejection.</th>
</tr>
</thead>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.reject_anonymous_call</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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
### account.X.send_anonymous_rejection_code

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.send_anonymous_rejection_code</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.anonymous_reject_oncode</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.anonymous_reject_offcode</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>Configures the anonymous call rejection off code to deactivate the server-side anonymous call rejection feature for account X.</td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>account.1.anonymous_reject_offcode = *75</td>
<td></td>
</tr>
<tr>
<td>Note: It works only if the value of the parameter &quot;account.X.send_anonymous_rejection_code&quot; is set to 0 (Off Code).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td>Settings -&gt; Features -&gt; Anonymous -&gt; Line X -&gt; Off Code</td>
<td></td>
</tr>
</tbody>
</table>

#### 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 344.

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure DND in the custom mode.</td>
<td>Configure DND.</td>
</tr>
<tr>
<td><strong>Parameters:</strong></td>
<td>Specify the authorized numbers when DND is enabled.</td>
</tr>
<tr>
<td>account.X.dnd.enable</td>
<td><strong>Parameters:</strong></td>
</tr>
<tr>
<td>account.X.dnd.on_code</td>
<td>features.dnd.enable</td>
</tr>
<tr>
<td>account.X.dnd.off_code</td>
<td>features.dnd.on_code</td>
</tr>
<tr>
<td></td>
<td>features.dnd.off_code</td>
</tr>
<tr>
<td>&lt;MAC&gt;.cfg</td>
<td>Specify the return code and the reason of the SIP response message when DND is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Parameter:</strong></td>
</tr>
<tr>
<td></td>
<td>features.dnd_refuse_code</td>
</tr>
<tr>
<td>&lt;y000000000xx&gt;.cfg</td>
<td>Assign a DND key.</td>
</tr>
<tr>
<td></td>
<td><strong>Parameters:</strong></td>
</tr>
<tr>
<td></td>
<td>linekey.X.type</td>
</tr>
<tr>
<td></td>
<td>programablekey.X.type</td>
</tr>
<tr>
<td></td>
<td>expansion_module.X.key.Y.type</td>
</tr>
<tr>
<td></td>
<td>linekey.X.label</td>
</tr>
<tr>
<td></td>
<td>expansion_module.X.key.Y.label</td>
</tr>
</tbody>
</table>

### Central Provisioning (Configuration File)

**Method:** Central Provisioning (Configuration File)

1. **<MAC>.cfg**
   - Configure DND in the custom mode.
   - **Parameters:**
     - account.X.dnd.enable
     - account.X.dnd.on_code
     - account.X.dnd.off_code

2. **<y000000000xx>.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

**Method:** Web User Interface

1. **Navigate to:**
   - Configure DND.
   - Specify the authorized numbers when DND is enabled.
   - **Navigate to:**
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-forward&q=load

Assign a DND key.

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

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.dnd_mode</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.dnd.enable</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X ranges from 1 to 16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
Triggers DND feature to on or off for account X.
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-Off</td>
<td>Off</td>
<td>Blank</td>
</tr>
<tr>
<td>1-On</td>
<td>On</td>
<td>Blank</td>
</tr>
</tbody>
</table>

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->DND Status

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.dnd.on_code</td>
<td>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.</td>
<td>account.1.dnd.on_code = *73</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Web User Interface:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Features-&gt;Forward&amp;DND-&gt;DND On Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Phone User Interface:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Settings-&gt;Features-&gt;DND-&gt;AccountX-&gt;On Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.dnd.off_code</td>
<td>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.</td>
<td>account.1.dnd.off_code = *74</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Web User Interface:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Features-&gt;Forward&amp;DND-&gt;DND Off Code</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Phone User Interface:</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Settings-&gt;Features-&gt;DND-&gt;AccountX-&gt;Off Code</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features-&gt;Forward&amp;DND-&gt;DND Off Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;DND-&gt;AccountX-&gt;Off Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>features.dnd.enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features.dnd.on_code</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features.dnd.off_code</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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:**

```
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.dnd.off_code = *72</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

---

<table>
<thead>
<tr>
<th>parameters</th>
<th>permitted values</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.dnd.emergency_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

---

<table>
<thead>
<tr>
<th>parameters</th>
<th>permitted values</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.dnd.emergency_authorized_number</td>
<td>String within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

---

<table>
<thead>
<tr>
<th>parameters</th>
<th>permitted values</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.dnd_refuse_code</td>
<td>404, 480, 486 or 603</td>
<td>480</td>
</tr>
</tbody>
</table>
**Administrator’s Guide for SIP-T5 Series Smart Media Phones**

### 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 805.

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/programablekey.X.type/ expansion_module.X.key.Y.type</td>
<td>5</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

#### 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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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).

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**
DSSKey->Line Key/Programable Key->Type

**Phone User Interface:**
Settings->Features->DSS Keys->Line Key X->Type

<table>
<thead>
<tr>
<th>linekey.X.label/ expansion_module.X.key.Y.label</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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)

**Note:** EXT key is not applicable to CP960 IP phones.

**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 **DND 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure busy tone delay. Parameter: features.busy_tone_delay</th>
</tr>
</thead>
</table>


Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.busy_tone_delay</td>
<td>0, 3 or 5</td>
<td>0</td>
</tr>
</tbody>
</table>

**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) | 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.normal_refuse_code</td>
<td>404, 480, 486 or 603</td>
<td>486</td>
</tr>
</tbody>
</table>

**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) | 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.is_deal180</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

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
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 171.

### Procedure

Use outbound proxy in dialog can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter: Specify whether to use outbound proxy in a dialog.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y000000000xx&gt;.cfg</td>
<td></td>
</tr>
</tbody>
</table>
**Web User Interface**

Navigate to:

```
http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load
```

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sip.use_out_bound_in_dialog</code></td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure SIP session timer.</th>
<th>Parameters: sip.timer_t1, sip.timer_t2, sip.timer_t4</th>
</tr>
</thead>
</table>

| Web User Interface | Configure SIP session timer. | Navigate to: http://<phoneIPAddress>/servlet?m=mod_data&p=settings-sip&q=load |

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.timer_t1</td>
<td>Float from 0.5 to 10</td>
<td>0.5</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the SIP session timer T1 (in seconds).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T1 is an estimate of the Round Trip Time (RTT) of transactions between a SIP client and SIP server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings -&gt; SIP -&gt; SIP Session Timer T1 (0.5~10s)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 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  | 5       |
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Session Timer T4</td>
<td>2.5~60s</td>
<td>60</td>
</tr>
</tbody>
</table>

**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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.session_timer.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**  
Enables or disables the session timer for account X.  
0 - Disabled
## Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>If it is set to 1 (Enabled), IP phone will send periodic UPDATE requests to refresh the session during a call.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>X is equal to 1 (for CP960)</td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Account-&gt;Advanced-&gt;Session Timer</td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>account.X.session_timer.expires</th>
<th>Integer from 30 to 7200</th>
<th>1800</th>
</tr>
</thead>
</table>

### 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).

<table>
<thead>
<tr>
<th>account.X.session_timer.refresher</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

### 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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Enabled).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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) | <y00000000xx>.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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.play_hold_tone.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to play a warning tone when there is a call on hold.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;General Information-&gt;Play Hold Tone</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>features.play_hold_tone.delay</strong></td>
<td>Integer from 3 to 3600</td>
<td>30</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the interval (in seconds) at which the IP phone play a warning tone when there is a call on hold.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It works only if the value of the parameter “features.play_hold_tone.enable” is set to 1 (Enabled).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;General Information-&gt;Play Hold Tone Delay</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>sip.rfc2543_hold</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;General Information-&gt;RFC 2543 Hold</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure music on hold on a per-line basis.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td></td>
</tr>
<tr>
<td>account.X.music_server_uri</td>
<td></td>
</tr>
<tr>
<td>Configure the way on how the IP phone processes music on hold when placing an active call on hold.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td></td>
</tr>
<tr>
<td>account.X.music_on_hold_type</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure music on hold on a per-line basis.</td>
</tr>
<tr>
<td><strong>Navigate to:</strong></td>
</tr>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-adv&amp;q=load&amp;acc=0</td>
</tr>
</tbody>
</table>

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.music_server_uri</td>
<td>SIP URI within 256 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

Description:
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.music_server_uri</td>
<td>&lt;10.1.3.165&gt;, 10.1.3.165, sip:<a href="mailto:moh@sip.com">moh@sip.com</a>, <a href="">sip:moh@sip.com</a>, &lt;yealink.com&gt; or yealink.com.</td>
<td></td>
</tr>
<tr>
<td><strong>X</strong> (ranges from 1 to 16)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>X</strong> (equal to 1)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.music_on_hold_type</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

**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

**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 |
<table>
<thead>
<tr>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Specify the authorized numbers when call forward is enabled. <strong>Parameters:</strong> features.forward.emergency.enable, features.forward.emergency.authorized_number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure the call forward mode. <strong>Parameter:</strong> features.fwd_mode</td>
</tr>
<tr>
<td></td>
<td>Configure call forward in phone mode. <strong>Parameters:</strong> 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</td>
</tr>
<tr>
<td></td>
<td>Configure diversion/history-info feature. <strong>Parameter:</strong> features.fwd_diversion_enable</td>
</tr>
<tr>
<td></td>
<td>Configure forward international. <strong>Parameter:</strong> forward.international.enable</td>
</tr>
</tbody>
</table>

---

**Note:** The configuration settings are specified in the `<y0000000000xx>.cfg` file. Each parameter is listed with its associated feature and parameter name.
Configuring Basic Features

**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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.fwd_mode</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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-&gt;Forward&DND-&gt;Forward-&gt;Mode

**Phone User Interface:**

None

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.always_fwd.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>
### Administrator's Guide for SIP-TS Series Smart Media Phones

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Triggers always forward feature to on or off for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - On</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If it is set to 1 (On), incoming calls to the account X are forwarded to the destination number (configured by the parameter &quot;account.X.always_fwd.target&quot;) immediately.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> 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).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Forward&amp;DND-&gt;Forward-&gt;Always Forward-&gt;On/Off</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;Call Forward-&gt;AccountX-&gt;Always Forward-&gt;Always Forward</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>account.X.always_fwd.target</strong>&lt;br&gt;(X ranges from 1 to 16)</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the destination number of the always forward for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> 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).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.1.always_fwd.target = 1003</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Forward&amp;DND-&gt;Forward-&gt;Always Forward-&gt;Target</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;Call Forward-&gt;AccountX-&gt;Always Forward-&gt;Forward To</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>account.X.always_fwd.on_code</strong>&lt;br&gt;(X ranges from 1 to 16)</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the always forward on code to activate the server-side always forward feature for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The IP phone will send the always forward on code and the pre-configured destination number (configured by the parameter &quot;account.X.always_fwd.target&quot;) to the server when you activate always forward feature for account X on the IP phone.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.1.always_fwd.on_code = *72</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.always_fwd.off_code</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>(X ranges from 1 to 16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.busy_fwd.enable</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X ranges from 1 to 16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:
### account.X.busy_fwd.target

**Permitted Values:** String within 32 characters  
**Default:** 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

**Permitted Values:** String within 32 characters  
**Default:** 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

**Permitted Values:** String within 32 characters  
**Default:** Blank

**Description:**
Configures the busy forward off code to deactivate the server-side busy forward feature for account X.
### Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.timeout_fwd.enable</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X ranges from 1 to 16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.timeout_fwd.target</th>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X ranges from 1 to 16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features-&gt;Forward&amp;DND-&gt;Forward-&gt;No Answer Forward-&gt;Target</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;Call Forward-&gt;AccountX-&gt;No Answer Forward-&gt;Forward To</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.timeout_fwd.timeout</td>
<td>Integer from 0 to 20</td>
<td>2</td>
</tr>
<tr>
<td>(X ranges from 1 to 16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.timeout_fwd.on_code</th>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X ranges from 1 to 16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.timeout_fwd.off_code</th>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X ranges from 1 to 16)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
Configures the no answer forward off code to deactivate the server-side no answer forward feature for account X on the IP phone.
### Configuring Basic Features

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.forward.emergency.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>features.forward.emergency.authorized_number</th>
<th>String within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>forward.always.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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).
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Forward&amp;DND-&gt;Forward-&gt;Always Forward-&gt;On Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;Call Forward-&gt;Always Forward-&gt;On Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>forward.always.off_code</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Description:</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the destination number of the busy forward for the IP phone.</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;Call Forward-&gt;Busy Forward-&gt;Off Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>forward.no_answer.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>forward.no_answer.target</th>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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       |
### Administrator’s Guide for SIP-T5 Series Smart Media Phones

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>Configures ring times (N) to wait before forwarding incoming calls.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Incoming calls will be forwarded when not answered after N*6 seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> It works only if the value of the parameter “features.fwd_mode” is set to 0 (Phone).</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Features -&gt; Forward&amp;DND -&gt; Forward -&gt; No Answer Forward -&gt; After Ring Time (0~120s)</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>Settings -&gt; Features -&gt; Call Forward -&gt; No Answer Forward -&gt; After Ring Time</td>
<td></td>
</tr>
<tr>
<td><strong>forward.no_answer.on_code</strong></td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the no answer forward on code to activate the server-side no answer forward feature.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>forward.no_answer.on_code = *76</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> It works only if the value of the parameter “features.fwd_mode” is set to 0 (Phone).</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Features -&gt; Forward&amp;DND -&gt; Forward -&gt; No Answer Forward -&gt; On Code</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>Settings -&gt; Features -&gt; Call Forward -&gt; No Answer Forward -&gt; On Code</td>
<td></td>
</tr>
<tr>
<td><strong>forward.no_answer.off_code</strong></td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the no answer forward off code to deactivate the server-side no answer forward feature.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>forward.no_answer.off_code = *77</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> It works only if the value of the parameter “features.fwd_mode” is set to 0 (Phone).</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features-&gt;Forward&amp;DND-&gt;Forward-&gt;No Answer Forward-&gt;Off Code</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Phone User Interface:**
Settings->Features->Call Forward->No Answer Forward->Off Code

<table>
<thead>
<tr>
<th>features.fwd_diversion_enable</th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>forward.international.enable</th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

**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.
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).

![Configuration Screen](image)

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**.

![Configuration Screen](image)

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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>transfer.blind_tran_on_hook_enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>transfer.on_hook_trans_enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Description:</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables or disables the IP phone to complete the semi-attended/attended transfer through on-hook besides tapping the <strong>Transfer</strong> soft key or TRANSFER/TRAN key.</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>transfer.semi_attend_tran_enable</td>
<td>0 or 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description:</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Note:** Semi-attended transfer means transfer a call after hearing the ringback tone.

**Web User Interface:**
Features->Transfer->Semi-Attend Transfer

**Phone User Interface:**

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 following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure local conference.</td>
<td>Configure local conference.</td>
</tr>
<tr>
<td>Parameters:</td>
<td>Navigate to:</td>
</tr>
<tr>
<td>account.X.conf_type</td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-adv&amp;q=load&amp;acc=0</td>
</tr>
<tr>
<td>features.local_conf.combine_with_on_press.enable</td>
<td></td>
</tr>
</tbody>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.conf_type</td>
<td>0 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

**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)
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Account->Advanced->Conference Type

**Phone User Interface:**
None

| features.local_conf.combine_with_one_press.enable | 0 or 1 | 0 |

**Description:**
Enables or disables the IP phone to set up a conference directly after the invitee answers the call.

**0**: Disabled
**1**: Enabled

If it is set to 0 (Disabled), the original call is placed on hold. The user needs to tap the Conference soft key again to set up a conference after the invitee answers the call.

**Note:** It is not applicable to CP960 IP phones.

**Web User Interface:**
None

**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) | Configure network conference. | Parameters: account.X.conf_type, account.X.conf_uri |
| Web User Interface | | Navigate to: http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0 |

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.conf_type</td>
<td>0 or 2</td>
<td>0</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the network conference type for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>0</strong>: Local Conference</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2</strong>: Network Conference</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If it is set to 0 (Local Conference), conferences are set up on the IP phone locally.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If it is set to 2 (Network Conference), conferences are set up by the server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account -&gt; Advanced -&gt; Conference Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 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 369.

Procedure

Transfer on conference hang up can be configured using the following methods.

| Central Provisioning (Configuration File) | 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=mmod_data&p=features-transfer&q=load |
Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>transfer.tran_others_after_conf_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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 the 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)
Configuring Basic Features

- 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 |

Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bw.feature_key_sync</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

Description:
Enables or disables feature key synchronization.

0 - Disabled
1 - Enabled

Web User Interface:
Features -> General Information -> Feature Key Synchronization

Phone User Interface:
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 364.

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 805.

Procedure

Transfer mode via dsskey can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure the transfer mode via dsskey.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter:</td>
<td>transfer.dsskey_deal_type</td>
<td></td>
</tr>
</tbody>
</table>

| Web User Interface                      | Configure the transfer mode via dsskey. |
Configuring Basic Features

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

Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>transfer.dsskey_deal_type</td>
<td>0, 1 or 2</td>
<td>2</td>
</tr>
</tbody>
</table>

Description:
Confirms 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>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure the directed call pickup code on a per-line basis. Parameter: account.X.direct_pickup_code</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt;.cfg</td>
<td>Configure directed call pickup features on a phone basis. Parameters: features.pickup.direct_pickup_enable features.pickup.direct_pickup_code</td>
</tr>
</tbody>
</table>
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

**Web User Interface**

Assign a directed call pickup key.

**Navigate to:**
http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load

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

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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.direct_pickup_code</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the directed call pickup code for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.1.direct_pickup_code = *68</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> The directed call pickup code configured on a per-line basis (&quot;account.X.direct_pickup_code&quot;) takes precedence over that configured on a phone basis (&quot;features.pickup.direct_pickup_code&quot;).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account-&gt;Advanced-&gt;Directed Call Pickup Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>features.pickup.direct_pickup_enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to display the DPickup key when the IP phone is on the pre-dialing screen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Pick up &amp; Park-&gt;Directed Call Pickup</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>features.pickup.direct_pickup_code</strong></td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the directed call pickup code on a phone basis.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>features.pickup.direct_pickup_code = *97</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> The directed call pickup code configured on a per-line basis (&quot;account.X.direct_pickup_code&quot;) takes precedence over that configured on a phone basis (&quot;features.pickup.direct_pickup_code&quot;).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Directed Call Pickup Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/programablekey.X.type/expansion_module.X.key.Y.type</td>
<td>9</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**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)

**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).
**Parameters** | **Permitted Values** | **Default**
---|---|---
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).
**Note:** EXT key is not applicable to CP960 IP phones.
**Web User Interface:**
DSSKey->Line Key/Programable Key->Type

**Phone User Interface:**
Settings->Features->DSS Keys->Line Key X->Type

<table>
<thead>
<tr>
<th>linekey.X.line/ programablekey.X.line/ expansion_module.X.key.Y.line</th>
<th>Refer to the following content</th>
<th>1-16 for lines 1-16, 1 for programable keys</th>
</tr>
</thead>
</table>

**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:**
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

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**
### Configuring Basic Features

#### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSSKey-＞Line Key/Programable Key-＞Line</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Phone User Interface:

Settings-＞Features-＞DSS Keys-＞Line Key X-＞Account ID

#### 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 = *97108

**Note:** EXT key is not applicable to CP960 IP phones.

#### Web User Interface:

DSSKey-＞Line Key/Programable Key-＞Value

### 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)

**Note:** EXT key is not applicable to CP960 IP phones.

#### Web User Interface:

DSSKey-＞Line Key-＞Label

### Phone User Interface:
### Parameters

| Settings -> Features -> DSS Keys -> Line Key X -> Label |

**To configure a directed call pickup key via web user interface:**

1. Click on **DSS Key -> 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**.

![Image of Yealink phone interface showing DSS Key settings](image-url)
3. Enter the directed call pickup code in the **Directed Call Pickup Code** field.

![Directed Call Pickup Code](image)

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** -> **Pick up & Park**.
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.

![Directed Call Pickup Code](image)

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.

<p>| Central Provisioning | &lt;MAC&gt;.cfg | Configure the group call pickup code on a per-line basis. |</p>
<table>
<thead>
<tr>
<th>(Configuration File)</th>
<th><strong>Parameters:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>account.X.group_pickup_code</td>
</tr>
<tr>
<td></td>
<td>Configure group call pickup features on a phone basis.</td>
</tr>
<tr>
<td></td>
<td><strong>Parameters:</strong></td>
</tr>
<tr>
<td></td>
<td>features.pickup.group_pickup_enable</td>
</tr>
<tr>
<td></td>
<td>features.pickup.group_pickup_code</td>
</tr>
</tbody>
</table>

|  | 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  |

<table>
<thead>
<tr>
<th><strong>Web User Interface</strong></th>
<th>Assign a group call pickup key.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Navigate to:</strong></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=dsskey&amp;q=load</td>
</tr>
</tbody>
</table>

|  | 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  |

<table>
<thead>
<tr>
<th><strong>Phone User Interface</strong></th>
<th>Assign a group call pickup key.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Navigate to:</strong></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-callpickup&amp;q=load</td>
</tr>
</tbody>
</table>
## Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>features.pickup.group_pickup_enable</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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->Pick up & Park->Group Call Pickup

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>account.X.group_pickup_code</code></td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>features.pickup.group_pickup_code</code></td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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
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->Pick up & Park->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 805.

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type</td>
<td>23</td>
<td>Refer to the following content</td>
</tr>
<tr>
<td>programmablekey.X.type/ expansion_module.X.key.Y.type</td>
<td>23</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>For programable keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For SIP-T58V/T58A/T56A IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When X=12, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When X=13, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When X=14, the default value is 2 (Forward).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For ext keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For SIP-T58V/T58A/T56A IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When Y= 1 to 60, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> EXT key is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSSKey-&gt;Line Key/Programable Key-&gt;Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;DSS Keys-&gt;Line Key X-&gt;Type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSSKey-&gt;Line Key/Programable Key-&gt;Line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;DSS Keys-&gt;Line Key X-&gt;Account ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linekey.X.value/programablekey.X.value/</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>expansion_module.X.key.Y.value</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**
DSSKey->Line Key/Programable Key->Line

**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)

**Note:** EXT key is not applicable to CP960 IP phones.
Web User Interface:
DSSKey -> Line Key -> Label

Phone User Interface:
Settings -> Features -> DSS Keys -> Line Key -> 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.

![Group Call Pickup Code](image1)

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** -> **Pick up & Park**.
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.

![Group Call Pickup Code](image2)

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 494.

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 498.

**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
<?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:

```plaintext
Via: SIP/2.0/UDP 10.10.20.18:5060;branch=z9hG4bK2026058891
From: "1010" <sip:1010@10.2.1.48:5060>;tag=826048502
```
### Procedure

Dialog info call pickup can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;MAC&gt;.cfg</code></td>
<td>Configure dialog info call pickup.</td>
</tr>
<tr>
<td>Parameter: <code>account.X.dialoginfo_callpickup</code></td>
<td>Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-adv&amp;q=load&amp;acc=0</td>
</tr>
</tbody>
</table>

### Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>account.X.dialoginfo_callpickup</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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:**

---

**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
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.

![Recent Call In Dialing Screen](image)

**Procedure**

Recent call in dialing can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure recent call in dialing feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter: super_search.recent_call</td>
<td>Parameter: super_search.recent_call</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure recent call in dialing feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to:</td>
<td>http://&lt;phoneIPaddress&gt;/servlet?m=mod_data&amp;p=contacts-favorite&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>super_search.recent_call</td>
<td>0 or 1</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>
## Description:
Enables or disables recent call in dialing feature.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Enables or disables recent call in dialing feature.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>- Disabled</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>- Enabled</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Assign a recall key. <strong>Parameter:</strong> linekey.X.type/programablekey.X.type/expansion_module.X.key.Y.type linekey.X.label/expansion_module.X.key.Y.label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td>Assign a recall key. <strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=dsskey&amp;q=load</td>
</tr>
<tr>
<td>Phone User Interface</td>
<td>Assign a recall key.</td>
</tr>
</tbody>
</table>

ReCall Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/programablekey.X.type/expansion_module.X.key.Y.type</td>
<td>7</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>
# Administrator’s Guide for SIP-T5 Series Smart Media Phones

## Parameters Description:

<table>
<thead>
<tr>
<th>Description</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures a DSS key as a recall key on the IP phone. The digit 7 stands for the key type <strong>ReCall</strong>. 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)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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).

For ext keys:

**For SIP-T58V/T58A/T56A IP phones:**
When Y=1 to 60, the default value is 0 (NA).

**Note:** EXT key is not applicable to CP960 IP phones.

### Web User Interface:

DSSKey -> Line Key/Programable Key -> Type

### Phone User Interface:

Settings -> Features -> DSS Keys -> Line Key X -> Type

<table>
<thead>
<tr>
<th>linekey.X.label/ expansion_module.X.key.Y.label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

---

398
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional.) Configures the label displayed on the touch screen for each DSS key.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For line keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 30 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For ext keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** EXT key is not applicable to CP960 IP phones.

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure the characters the IP phone filters when dialing.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;y0000000000xx&gt;.cfg</code></td>
<td><strong>Parameter:</strong> features.call_num_filter</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure the characters the IP phone filters when dialing.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
<td></td>
</tr>
</tbody>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>features.call_num_filter</code></td>
<td>String within 99 characters</td>
<td>?,( )</td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone User Interface:</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

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 from another phone (for example, a phone in another office or conference room). This feature depends on support from a SIP server.

For old call park mechanism, users can use a call park key to park a call, and retrieve a parked call by dialing the park retrieve code. SIP-T58V/T58A/T56A IP phones running firmware version 58.80.0.30 or later support the new call park mechanism.

New call park mechanism supports the following two modes:

- **FAC mode**: Call park feature via FAC mode allows users to park an active call to a desired extension or local extension through dialing the call park code.
- **Transfer mode**: Call park feature via Transfer mode allows users to park an active call to the shared parking lot through performing a blind transfer to a call park shared number (call park code). For some servers, the system will return a specific call park retrieve number (park retrieve code) from which the call can be retrieved after parking successfully.

Users can park calls on the extension, known as call park orbit, by tapping the Park soft key or a call park key. You need to configure the call park code for the Park soft key or the call park key.
Call park code configured for the **Park** soft key will also apply to the 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 park retrieve code or tap **Retrieve Park** or tap the retrieve park key. 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.

**Note**

If the call park code or park retrieve code has been configured for the **Park** soft key or **Retrieve Park**, you don’t need to configure the call park code or the park retrieve code for the call park DSS key or the retrieve park DSS key.

**Procedure**

Call park can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure call park feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Parameters:</td>
</tr>
<tr>
<td></td>
<td>features.call_park.park_mode</td>
</tr>
<tr>
<td></td>
<td>features.call_park.enable</td>
</tr>
<tr>
<td></td>
<td>features.call_park.park_code</td>
</tr>
<tr>
<td></td>
<td>features.call_park.park_retrieve_code</td>
</tr>
<tr>
<td></td>
<td>features.call_park.direct_send.enable</td>
</tr>
<tr>
<td></td>
<td>features.call_park.line_restriction.enable</td>
</tr>
<tr>
<td>Web User Interface</td>
<td>Assign a call park key.</td>
</tr>
<tr>
<td></td>
<td>Assign a retrieve park key.</td>
</tr>
<tr>
<td></td>
<td>Parameters:</td>
</tr>
<tr>
<td></td>
<td>linekey.X.type/</td>
</tr>
<tr>
<td></td>
<td>expansion_module.X.key.Y.type</td>
</tr>
<tr>
<td></td>
<td>linekey.X.line/</td>
</tr>
<tr>
<td></td>
<td>expansion_module.X.key.Y.line</td>
</tr>
<tr>
<td></td>
<td>linekey.X.value/</td>
</tr>
<tr>
<td></td>
<td>expansion_module.X.key.Y.value</td>
</tr>
<tr>
<td></td>
<td>linekey.X.label/</td>
</tr>
<tr>
<td></td>
<td>expansion_module.X.key.Y.label</td>
</tr>
<tr>
<td></td>
<td>linekey.X.shortlabel</td>
</tr>
</tbody>
</table>

Navigate to:

http://<phoneIPAddress>/servlet?p=features-callpickup&q=load
Assign a call park key.
Assign a retrieve park key.

**Navigate to:**
http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0

### Phone User Interface
Assign a call park key.
Assign a retrieve park key.

---

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.call_park.park_mode</td>
<td>1 or 2</td>
<td>2</td>
</tr>
</tbody>
</table>

**Description:**
Configures the call park mode.

1 - FAC
2 - Transfer

**Note:** It is not applicable to CP960 IP phones.

**Web User Interface:**
Features - Pick up & Park - Call Park Mode

**Phone User Interface:**
None

| features.call_park.enable | 0 or 1 | 0 |

**Description:**
Enables or disables the IP phone to display the **Park** soft key during a call.

0 - Disabled
1 - Enabled,

If it is set to 1(Enabled), **Retrieve Park** will also be displayed on the dialing screen.

**Note:** It is not applicable to CP960 IP phones.

**Web User Interface:**
Features - Pick up & Park - Call Park

**Phone User Interface:**
None

| features.call_park.park_code | String within 32 characters | Blank |
## Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>features.call_park.park_code</strong></td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>features.call_park.park_retrieve_code</strong></td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>features.call_park.direct_send.enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

### Description:
Configures the call park code for the **Park** soft key. This call park code will also apply to the call park key.

**Example:**
features.call_park.park_code = *68

**Note:** It is not applicable to CP960 IP phones.

### Web User Interface:
Features->Pick up & Park->Call Park Code

### Phone User Interface:
None

### Description:
Configures the park retrieve code for **Retrieve Park**. This park retrieve code will also apply to the retrieve park key.

**Example:**
features.call_park.park_retrieve_code = *88

**Note:** It is not applicable to CP960 IP phones.

### Web User Interface:
Features->Pick up & Park->Park Retrieve Code

### Phone User Interface:
None

### Description:
Enables or disables the IP phone to dial out the call park code/park retrieve code directly when tapping the **Park** soft key or **Retrieve Park**.

- **0**: Disabled
- **1**: Enabled

If it is set to 0 (Disabled), the IP phone will enter the pre-dialing screen when tapping the **Park** soft key or **Retrieve Park**. And you can dial the specific extension manually or tap the BLF/BLF List key to park the call to the specific user or retrieve the call parked from the specific user.

**Note:** It works only if the value of the parameter “features.call_park.park_mode” is set to 1 (FAC) and you have configured the call park code/park retrieve code. It is not applicable to
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>CP960 IP phones.</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>features.call_park.line_restriction.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables the IP phone to park/retrieve a call using the line specified by the parameter "linekey.X.line/expansion_module.X.key.Y.line". It is only applicable to the scenario that the user uses the call park/retrieve park key to park/retrieve a call.

0 - Disabled
1 - Enabled

If it is set to 0 (Disabled), the IP phone will park/retrieve the call to the server where the current account is registered.

If it is set to 1 (Enabled), the IP phone will place a new call if the specified line is idle.

**Note:** It works only if the value of the parameter “features.call_park.park_mode” is set to 2 (Transfer). It is not applicable to CP960 IP phones.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/ expansion_module.X.key.Y.type</td>
<td>10</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**Call Park Key**

For more information on how to configure the Key, refer to Appendix D: Configuring DSS Key on page 805.

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/ expansion_module.X.key.Y.type</td>
<td>10</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**Description:**
Configures a DSS key as a call park key on the IP phone.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
</table>
| 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). **Note:** EXT key is not applicable to CP960 IP phones. **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 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)
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-Line 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-Line 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16-Line 16</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

linekey.2.line = 1

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey -> Line key -> Line

**Phone User Interface:**

Settings -> Features -> DSS Keys -> Line Key X -> Account ID

<table>
<thead>
<tr>
<th>linekey.X.value/ expansion_module.X.key.Y.value</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**Description:**

Configures the park destination number or call park 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

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey -> Line key -> Value

**Phone User Interface:**

Settings -> Features -> DSS Keys -> Line Key X -> Value

<table>
<thead>
<tr>
<th>linekey.X.label/ expansion_module.X.key.Y.label</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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)
Retrieve Park Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/ expansion_module.X.key.Y.type</td>
<td>56</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

Description:
Configures a DSS key as a retrieve park key on the IP phone.
The digit 56 stands for the key type Retrieve Park.
For line keys:
X ranges from 1 to 27 (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 = 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 ext keys:
For SIP-T58V/T58A/T56A IP phones:
When Y = 1 to 60, the default value is 0 (NA).

Web User Interface:
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSSKey-&gt;Line key-&gt;Type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Phone User Interface:**
Settings->Features->DSS Keys->Line Key X->Type

<table>
<thead>
<tr>
<th>linekey.X.line/ expansion_module.X.key.Y.line</th>
<th>Refer to the following content</th>
<th>1-16 for lines 1-16</th>
</tr>
</thead>
</table>

**Description:**
Configures the desired line to apply the retrieve park key.

For line keys:
X ranges from 1 to 27 (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-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

<table>
<thead>
<tr>
<th>linekey.X.value/ expansion_module.X.key.Y.value</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**Description:**
Configures the parked call destination number or retrieve code.

For line keys:
X ranges from 1 to 27 (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 = *88
Parameters | Permitted Values | Default
---|---|---
**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:**
(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)

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 call park feature via web user interface (not applicable to CP960 IP phones):

1. Click on **Features->Pick up & Park**.
2. Select the desired call park mode from the pull-down list of **Call Park Mode**.
3. Select the desired value from the pull-down list of **Call Park**.
4. (Optional.) Enter the call park code in the **Call Park Code** field.
5. (Optional.) Enter the park retrieve code in the **Park Retrieve Code** field.

6. Click **Confirm** to accept the change.
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 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 retrieve park key via web user interface (not applicable to CP960 IP phones):

1. Click on DSSKey → Line Key (or Ext Key).
2. In the desired DSS key field, select Retrieve Park from the pull-down list of Type.
3. Enter the desired value (e.g., park retrieve code) in the Value field.
4. (Optional.) Enter the string that will appear on the LCD 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 code) in the **Value** field.

11. Tap ✔️ to accept the change.

**To configure a retrieve park key via phone user interface (not applicable to CP960 IP phones):**

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 **Retrieve 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., park retrieve 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.

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 = 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 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter: account.X.cid_source</td>
<td>Configure the presentation of the caller identity.</td>
</tr>
<tr>
<td>Parameter: account.X.cid_source_privacy</td>
<td>Specify whether to process Privacy header field.</td>
</tr>
<tr>
<td>Parameter: account.X.cid_source_ppi</td>
<td>Specify whether to process the P-Preferred-Identity (PPI) header for caller identity presentation.</td>
</tr>
</tbody>
</table>

| 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.cid_source</td>
<td>0, 1, 2, 3, 4, 5 or 6</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
Configures the presentation of the caller identity when receiving an incoming call for account X.

- **0**: FROM
- **1**: PAI
- **2**: PAI-FROM
- **3**: RPID-PAI-FROM
- **4**: PAI-RPID-FROM
- **5**: RPID-FROM
- **6**: PREFERENCE, the IP phone uses the custom priority order for the sources of caller identity information (configured by the parameter "sip.cid_source.preference"). It is only applicable to CP960 IP phones.

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

<table>
<thead>
<tr>
<th>account.X.cid_source_privacy</th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

**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.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

**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**.

![Image of Yealink T38 phone settings]

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 18X 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configure the presentation of the callee's identity.</th>
</tr>
</thead>
</table>

**Parameter:**

<table>
<thead>
<tr>
<th>Parameter:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>account.X.cp_source</th>
</tr>
</thead>
</table>

Specify whether to process Privacy header field.

**Parameter:**

<table>
<thead>
<tr>
<th>Parameter:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>account.X.cid_source_privacy</th>
</tr>
</thead>
</table>

**Details of the Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.cp_source</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

**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)
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.cid_source_privacy</td>
<td>0 or 1</td>
<td>1</td>
<td>Enables or disables the IP phone to process Privacy header field in the SIP message for account X.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>1 to 16 (for SIP-T58V/T58A/T56A)</td>
</tr>
<tr>
<td>X</td>
<td>1 (for CP960)</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure allow mute feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cf 9</td>
<td>Parameter: features.allow_mute</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure allow mute feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Navigate to:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;phoneIP Address&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.allow_mute</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure keep mute feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Parameter:</td>
</tr>
<tr>
<td></td>
<td>features.keep_mute.enable</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.keep_mute.enable</td>
<td>0 or 1</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

Description:
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables or disables the keep mute feature for the IP phone.</td>
<td>0 - Disabled</td>
<td>0</td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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)

<table>
<thead>
<tr>
<th>Icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![intercom_icon]</td>
<td>Intercom idle state</td>
</tr>
</tbody>
</table>
### Icons

<table>
<thead>
<tr>
<th>Icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Intercom ringing state" /></td>
<td>Intercom ringing state</td>
</tr>
<tr>
<td><img src="image" alt="Intercom callout state" /></td>
<td>Intercom callout state</td>
</tr>
<tr>
<td><img src="image" alt="Intercom talking state" /></td>
<td>Intercom talking state</td>
</tr>
<tr>
<td><img src="image" alt="Intercom failed state" /></td>
<td>Intercom failed state</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![y0000000000xx.cfg](image) | Configure the intercom subscription.  
**Parameters:**  
features.intercom.led.enable  
features.intercom.subscribe.enable  
sip.intercom_sub.enable |

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![http://<phoneIPAddress>/servlet?m=m mod_data&p=dsskey&q=load](image) | Assign an intercom key.  
**Navigate to:**  
http://<phoneIPAddress>/servlet?m=m mod_data&p=dsskey&q=load |
Assign an intercom key.

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.intercom.led.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.intercom.subscribe.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.intercom_sub.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables intercom subscription for the IP phone.
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-Disabled</td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>1-Enabled</td>
<td></td>
<td>None</td>
</tr>
</tbody>
</table>

**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 805.

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/</td>
<td>14</td>
<td>Refer to the following content</td>
</tr>
<tr>
<td>expansion_module.X.key.Y.type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
Confires a DSS key as an intercom key.
The digit 14 stands for the key type Intercom.

**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:
### Administrator’s Guide for SIP-T5 Series Smart Media Phones

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>For SIP-T58V/T58A/T56A IP phones:</strong>&lt;br&gt;When Y= 1 to 60, the default value is 0 (NA).&lt;br&gt;Note: EXT key is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSSKey-&gt;Line key-&gt;Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;DSS Keys-&gt;Line Key X-&gt;Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>linekey.X.line/ expansion_module.X.key.Y.line</strong></td>
<td>Refer to the following content</td>
<td>1-16 for lines 1-16</td>
</tr>
</tbody>
</table>

**Description:**<br>Configures the desired line to apply the intercom key.<br>For line keys:<br>X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)<br>X ranges from 1 to 30 (for CP960)<br>For ext keys:<br>X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)

**Permitted Values:**<br>1 to 16 (for SIP-T58V/T58A/T56A)<br>1 (for CP960)<br>1-Line 1<br>2-Line 2<br>...<br>16-Line 16

**Example:**<br>linekey.2.line = 1

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**<br>DSSKey->Line key->Line

**Phone User Interface:**<br>Settings->Features->DSS Keys->Line Key X->Account ID

| linekey.X.value/ expansion_module.X.key.Y.value | String within 99 characters | Blank |

**Description:**
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the intercom 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)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
linekey.2.value = 1008
```

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey->Line key->Value

**Phone User Interface:**

Settings->Features->DSS Keys->Line Key X->Value

<table>
<thead>
<tr>
<th>linekey.X.pickup_value/ expansion_module.X.key.Y.pickup_value</th>
<th>String within 256 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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. EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey->Line Key->Extension

**Phone User Interface:**

Settings->Features->DSS Keys->Line Key X->Extension

<table>
<thead>
<tr>
<th>linekey.X.label/ expansion_module.X.key.Y.label</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>---------</td>
</tr>
</tbody>
</table>

**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)

**Note:** EXT key is not applicable to CP960 IP phones.

**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:

Intercom Allow
Intercom Allow 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y000000000xx&gt;.cfg</td>
<td>Configure incoming intercom call feature.</td>
</tr>
</tbody>
</table>

Parameters:
features.intercom.allow
features.intercom.mute
features.intercom.tone
features.intercom.barge
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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.intercom.allow</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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 -> Intercom Allow

**Phone User Interface:**
Settings -> Features -> Intercom -> Intercom Allow

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.intercom.mute</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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
### Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.intercom.tone</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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 (Enabled).

**Web User Interface:**
Features->Intercom->Intercom Tone

**Phone User Interface:**
Settings->Features->Intercom->Intercom Tone

<table>
<thead>
<tr>
<th>features.intercom.barge</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

**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 Intercom Allow, 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure the duration time in the ringback state.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter:</td>
<td>phone_setting.ringback_timeout</td>
<td></td>
</tr>
</tbody>
</table>

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.ringback_timeout</td>
<td>Integer from 0 to 3600</td>
<td>180</td>
</tr>
</tbody>
</table>

**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.
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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>phone_setting.ringing_timeout</code></td>
<td>Integer from 0 to 3600</td>
<td>120</td>
</tr>
</tbody>
</table>

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 5.8.0.0.
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=m  
| | | mod_data&p=account-adv&q=load&acc=0 |

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.enable_user_equal_phone</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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)
**Configuring Basic Features**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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
```

435
Procedure

SIP send MAC can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure SIP send MAC on a per-line basis. Parameter: account.X.register_mac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td></td>
<td>Configure SIP send MAC on a per-line basis. Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-adv&amp;q=load&amp;acc=0</td>
</tr>
</tbody>
</table>

Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.register_mac</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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)
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.

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Line Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A/T56A</td>
<td>0~15</td>
<td>0<del>15 stand for line1</del>line16</td>
</tr>
<tr>
<td>CP960</td>
<td>0</td>
<td>0 stand for line1</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th><strong>Central Provisioning</strong> (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure SIP send line on a per-line basis. <strong>Parameter:</strong> account.X.register_line</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface</strong></td>
<td></td>
<td>Configure SIP send line on a per-line basis. <strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/service?m=mod_data&amp;p=account-adv&amp;q=load&amp;acc=0</td>
</tr>
</tbody>
</table>

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.register_line</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X ranges from 1 to 16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>(for CP960)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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
```
Procedure

Reserve # in User Name can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure reserve # in user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Parameter: sip.use_23_as_pound</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure reserve # in user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.use_23_as_pound</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

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**.

![Reserve # in User Name](image)

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure password dial feature.</th>
<th>Parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td></td>
<td>features.password_dial.enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features.password_dial.prefix</td>
</tr>
<tr>
<td></td>
<td></td>
<td>features.password_dial.length</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure password dial feature.</th>
<th>Navigate to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

### Details of the Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.password_dial.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**

Enables or disables password dial feature for the IP phone.

0 - Disabled
## Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1-Enabled</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Features -> General Information -> PswDial

**Phone User Interface:**
None

### `features.password_dial.prefix`

**Description:**
Configures the prefix of the password dial number.

**Example:**
features.password_dial.prefix = 12

**Web User Interface:**
Features -> General Information -> PswPrefix

**Phone User Interface:**
None

### `features.password_dial.length`

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure unregister when reboot.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Parameter:</strong> account.X.unregister_on_reboot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure unregister when reboot.</th>
<th><strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-adv&amp;q=load&amp;acc=0</th>
</tr>
</thead>
</table>

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.unregister_on_reboot</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**

Enables or disables the IP phone to unregister first before re-registering account X when
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="0af113b", 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the 100 reliable retransmission feature.</td>
<td></td>
</tr>
<tr>
<td>Parameter:</td>
<td></td>
</tr>
<tr>
<td>account.X.100rel_enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the 100 reliable retransmission feature.</td>
</tr>
<tr>
<td>Navigate to:</td>
</tr>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-adv&amp;q=load&amp;acc=0</td>
</tr>
</tbody>
</table>

Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.100rel_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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 588.

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 592.
Procedure

Reboot in talking can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Configure reboot in talking.</td>
</tr>
<tr>
<td></td>
<td>Parameter: features.reboot_in_talk_enable</td>
</tr>
</tbody>
</table>

**Web User Interface**

Navigate to:

http://<phoneIP Address>/servlet?m=mod_data&p=features-general&q=load

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.reboot_in_talk_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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.

![Image of Yealink T5 phone settings interface]

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) | <y000000000xx>.cfg | Configure answer by hand. Parameter: `features.off_hook_answer.enable` |

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>features.off_hook_answer.enable</code></td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>
Configuring Basic Features

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 552.

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter: Configure the recording feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y000000000xx&gt;.cfg</td>
<td></td>
</tr>
</tbody>
</table>
### Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.call_recording.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>phone_setting.permit_silent_mode.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

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:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.permit_silent_mode.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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**

The IP phone is compatible with the 2N, Baudisch and CyberData IP intercoms. And you can pair up to 99 IP intercoms on the IP phone.
When a visitor rings your doorbell, the IP phone will ring. You can answer the incoming call, and then tap the **Open Door** soft key to open the door.

The IP phones also support the following:

- **Preview feature**: get a preview of who’s there when receiving a visitor’s incoming call.
- **One-button Open feature**: open the door at any time.
- **Monitoring feature**: check the camera video at any time.

For more information, refer to *Using Door Phone Feature on Yealink Smart Media Phones*.

In addition to the IP phone, IP intercom should be configured. For more information on how to configure the IP intercom, refer to the documentation from the manufacturer.

**Note**

It is not applicable to CP960 IP phones.

**Procedure**

Door phone settings can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Description</th>
</tr>
</thead>
</table>
| <y0000000000xx>.cfg | Configure the door phone information.  
**Parameters:**  
- features.doorphone.amount  
- features.doorphone.X.device_model  
- 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 |
Assign an Open Door 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 Video Monitoring 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

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

Assign an Open Door key.
Assign a Video Monitoring key.

**Navigate to:**
http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load
## Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.doorphone.amount</td>
<td>Integer from 0 to 99</td>
<td>2</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the number of IP intercoms supported by the IP phone.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>features.doorphone.X.device_model (X ranges from 1 to 99)</td>
<td>Integer from 0 to 4</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the device type of the IP intercom.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Custom</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-2N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-Mobotix</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-Baudisch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-CyberData</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Door Phone-&gt;Device Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>features.doorphone.X.display_name (X ranges from 1 to 99)</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the display name of the IP intercom to be displayed on the IP phone’s screen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Door Phone-&gt;Display Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**features.doorphone.X.phone_number**  
(X ranges from 1 to 99)  
**String within 32 characters**  
**Blank**

**Description:**  
Configures the phone number or IP address of the IP intercom.  

**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 99)  
**String within 99 characters**  
**Blank**

**Description:**  
Configures the unlock PIN of the IP intercom.  

**Example:**  
features.doorphone.1.unlock_pin=8888*

When tapping the **Open Door** soft key after answering the call, the IP phone will send the DTMF sequence “8888*” to the IP intercom. And if the DTMF sequence matches the code configured on IP intercom, the door will be opened.  

**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 99)  
**0 or 1**  
**0**

**Description:**  
Enables or disables the IP phone to enter full-screen display automatically after answering the visitor’s call.  

0: Disabled  
1: Enabled  

**Note:** It is not applicable to CP960 IP phones. It works only if the value of the parameter “video.enable” is not set to 0 (Disabled) and the value of the parameter “features.doorphone.X.device_model” is not set to 3 (Baudisch).

**Web User Interface:**  
Features->Door Phone->Full Screen

**Phone User Interface:**  
None
### features.doorphone.X.send_audio
(X ranges from 1 to 99)

<table>
<thead>
<tr>
<th></th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

**Description:**
Enables or disables the IP phone to transmit your audio during a visitor’s 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 99)

<table>
<thead>
<tr>
<th></th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

**Description:**
Enables or disables the IP phone to transmit your video during a visitor’s call.

0 - Disabled
1 - Enabled

**Note:** It works only if the value of the parameter “video.enable” is not set to 0 (Disabled) and the value of the parameter “features.doorphone.X.device_model” is not set to 3 (Baudisch). It is not applicable to SIP-T56A/CP960 IP phones.

**Web User Interface:**
Features -> Door Phone -> Send Video

**Phone User Interface:**
None

### features.doorphone.X.video.stream.httpurl
(X ranges from 1 to 99)

<table>
<thead>
<tr>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**Description:**
Configures the video access URL of IP intercom camera.

The valid URL format is: http://<IP address of the IP intercom>/mjpg/video.mjpg or http://username:password@<IP address of the IP intercom>/mjpg/video.mjpg.

**Example:**

The IP phone will retrieve the video stream from the configured URL when the user tap the **Video View** soft key after answering the call or when answering the call with auto video feature is enabled (configured by the parameter “features.doorphone.X.autovideoview.enable”).
Note: It works only if the value of the parameter “features.doorphone.X.device_model” is set to 3 (Baudisch). If you use the first URL format and the IP intercom needs HTTP API authentication, you should configure the authentication account (configured by the parameters “features.doorphone.X.httpapi.username” and “features.doorphone.X.httpapi.password”). It is not applicable to CP960 IP phones.

Web User Interface:
Features->Door Phone->IP CAM
Phone User Interface:
None

<table>
<thead>
<tr>
<th>features.doorphone.X.autovideoview.enable</th>
<th>0 or 1</th>
<th>1</th>
</tr>
</thead>
</table>

Description:
Enables or disables the IP phone to display the video automatically after answering the visitor’s call.

0 - Disabled
1 - Enabled

If it is set to 1 (Enabled), the IP phone will receive the video stream immediately after answering the visitor’s call without tapping the Video View soft key.

Note: It works only if the value of the parameter “features.doorphone.X.device_model” is set to 3 (Baudisch) and the video access URL is valid (configured by the parameter “features.doorphone.X.video.stream.httpurl”). It is not applicable to CP960 IP phones.

Web User Interface:
Features->Door Phone->Auto View In Call
Phone User Interface:
None

<table>
<thead>
<tr>
<th>features.doorphone.X.videopreview.enable</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

Description:
Enables or disables the video preview when receiving a visitor’s incoming call.

0 - Disabled
1 - Enabled

If it is set to 1 (Enabled) and the value of the parameter “features.doorphone.X.autopreview.enable” is set to 0 (Disabled), users can tap the Preview soft key to check the visitor’s video when receiving a visitor’s incoming call. And the IP phone will stop playing the ringtone.

Note: It works only if the value of the parameter “account.X.auto_answer” is set to 0 (Disabled) and the value of the parameter “video.enable” is not set to 0 (Disabled)). It is not applicable to CP960 IP phones.
### Web User Interface:
Features -> Door Phone -> Video Preview

### Phone User Interface:
None

<table>
<thead>
<tr>
<th><code>features.doorphone.X.autopreview.enable</code> (X ranges from 1 to 99)</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

**Description:**
Enables or disables the IP phone to preview the visitor’s video automatically when receiving a visitor’s incoming call.

- **0**: Disabled
- **1**: Enabled

If it is set to 1 (Enabled), the IP phone will display the visitor’s video automatically when receiving a visitor’s incoming call. And the IP phone will still play ringtone.

**Note:** It works only if the value of the parameter “`features.doorphone.X.videopreview.enable`” is set to 1 (Enabled), the value of the parameter “`account.X.auto_answer`” is set to 0 (Disabled) and the value of the parameter “`video.enable`” is not set to 0 (Disabled). It is not applicable to CP960 IP phones.

### Web User Interface:
Features -> Door Phone -> Auto Preview

### Phone User Interface:
None

<table>
<thead>
<tr>
<th><code>features.doorphone.X.httpapi.username</code> (X ranges from 1 to 99)</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**Description:**
Configures the user name for HTTP API authentication.

**Note:** It is required only if the IP intercom needs the HTTP API authentication. It is not applicable to CP960 IP phones.

### Web User Interface:
Features -> Door Phone -> User Name

### Phone User Interface:
None

<table>
<thead>
<tr>
<th><code>features.doorphone.X.httpapi.password</code> (X ranges from 1 to 99)</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**Description:**
Configures the password of HTTP API authentication.

**Note:** It is required only if the IP intercom needs the HTTP API authentication. It is not applicable to CP960 IP phones.
Open Door Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/ expansion_module.X.key.Y.type</td>
<td>84</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**Description:**

Configures a DSS key as an Open Door key on the IP phone.

The digit **84** stands for the key type **Open Door**.

For line keys:

X ranges from 1 to 27

For ext keys:

X ranges from 1 to 3, Y ranges from 1 to 60

**Example:**

linekey.2.type = 84

**Default:**

For line keys:

The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0.

For ext keys:

When Y=1 to 60, the default value is 0 (NA).

**Web User Interface:**

DSSKey ->Line Key/Ext Key->Type

**Phone User Interface:**

Settings->Features->DSS Keys->Line Key X->Type

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.value/ expansion_module.X.key.Y.value</td>
<td>String within 99 characters</td>
</tr>
</tbody>
</table>

**Description:**

Configures the open door URL of 2N IP intercom.
The valid URL format is:

For line keys:
X ranges from 1 to 27

For ext keys:
X ranges from 1 to 3, Y ranges from 1 to 60

**Example:**
linekey.2.value = http://192.168.1.1/api/switch/ctrl?switch=1&action=trigger

**Note:** If the IP intercom needs HTTP API authentication, you should configure the authentication account (configured by the parameters “features.doorphone.X.httpapi.username” and “features.doorphone.X.httpapi.password”).

### Web User Interface:
DSSKey -> Line Key/Ext Key -> Value

### Phone User Interface:
Settings -> Features -> DSS Keys -> Line Key X -> Value

<table>
<thead>
<tr>
<th>linekey.X.label/ expansion_module.X.key.Y.label</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>(Optional.) Configures the label displayed on the touch screen for each DSS key.</td>
<td></td>
</tr>
<tr>
<td>For line keys:</td>
<td>X ranges from 1 to 27</td>
<td></td>
</tr>
<tr>
<td>For ext keys:</td>
<td>X ranges from 1 to 3, Y ranges from 1 to 60</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>DSSKey -&gt; Line Key/Ext Key -&gt; Label</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>Settings -&gt; Features -&gt; DSS Keys -&gt; Line Key X -&gt; Label</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>linekey.X.extension/ expansion_module.X.key.Y.extension</th>
<th>String within 256 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the number or IP address of the IP intercom that this key will apply to.</td>
<td></td>
</tr>
<tr>
<td>For line keys:</td>
<td>X ranges from 1 to 27</td>
<td></td>
</tr>
<tr>
<td>For ext keys:</td>
<td>X ranges from 1 to 3, Y ranges from 1 to 60</td>
<td></td>
</tr>
</tbody>
</table>
### Video Monitoring Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/ expansion_module.X.key.Y.type</td>
<td>85</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**Description:**
Configures a DSS key as a Video Monitoring DSS key on the IP phone.
The digit **85** stands for the key type **Video Monitoring**.
For line keys:
X ranges from 1 to 27
For ext keys:
X ranges from 1 to 3, Y ranges from 1 to 60

**Example:**
linekey.2.type = 85

**Default:**
For line keys:
The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0.
For ext keys:
When Y= 1 to 60, the default value is 0 (NA).

**Web User Interface:**
DSSKey -> Line Key/Ext Key -> Type

**Phone User Interface:**
Settings -> Features -> DSS Keys -> Line Key X -> Type
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>linekey.X.value</code> / <code>expansion_module.X.key.Y.value</code></td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

#### Description:
Configures the video access URL of IP intercom camera.
The valid URL format is: http://<IP address of the IP intercom>/mjpg/video.mjpg or http://username:password@<IP address of the IP intercom>/mjpg/video.mjpg.

For line keys:
- X ranges from 1 to 27

For ext keys:
- X ranges from 1 to 3, Y ranges from 1 to 60

#### Example:
```
linekey.2.value = http://192.168.1.1/mjpg/video.mjpg
```

#### Note:
If you use the first URL format and the IP intercom needs HTTP API authentication, you should configure the authentication account (configured by the parameters “features.doorphone.X.httpapi.username” and “features.doorphone.X.httpapi.password”).

#### Web User Interface:
DSSKey- Line Key/Ext Key- Value

#### Phone User Interface:
Settings- Features- DSS Keys- Line Key X- Value

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>linekey.X.label</code> / <code>expansion_module.X.key.Y.label</code></td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

#### Description:
(Optional.) Configures the label displayed on the touch screen for each DSS key.

For line keys:
- X ranges from 1 to 27

For ext keys:
- X ranges from 1 to 3, Y ranges from 1 to 60

#### Web User Interface:
DSSKey- Line Key/Ext Key- Label

#### Phone User Interface:
Settings- Features- DSS Keys- Line Key X- Label

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>linekey.X.extension</code> / <code>expansion_module.X.key.Y.extension</code></td>
<td>String within 256 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

#### Description:
Configures the number or IP address of the IP intercom that this key will apply to.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>For line keys:</td>
<td>X ranges from 1 to 27</td>
<td></td>
</tr>
<tr>
<td>For ext keys:</td>
<td>X ranges from 1 to 3, Y ranges from 1 to 60</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**
linexkey.2.extension = 1048

**Web User Interface:**
DSSKey- >Line Key/Ext Key- >Extension

**Phone User Interface:**
Settings- >Features- >DSS Keys- >Line Key X- >Extension

**To configure door phone feature:**

1. Click on **Features- >Door Phone**.
2. Select the desired IP intercom from the pull-down list of **Door Phone List**.
3. Select the desired device type from the pull-down list of **Device Type**.
4. Enter the display name of the IP intercom in the **Display Name** field.
5. Enter the phone number or IP address of the IP intercom in the **Phone Number** field.
   If you leave it blank or enter the wrong number, the IP phone will take the visitor’s incoming call as a normal call.
6. Enter the unlock PIN in the **Unlock PIN** field.
   It should match the code configured on IP intercom.
7. Select the desired value from the pull-down list of **Full Screen**.
   This field appears only if **Device Type** is not set to **Baudisch**.
8. Select the desired value from the pull-down list of **Send Audio**.
9. Select the desired value from the pull-down list of **Send Video**.
   This field appears only if **Device Type** is not set to **Baudisch**.
10. Enter the video access URL in the **IP CAM** field.
   This field appears only if **Device Type** is set to **Baudisch**.
11. Select the desired value from the pull-down list of **Auto View In Call**.
   This field appears only if **Device Type** is set to **Baudisch**.
12. Select the desired value from the pull-down list of **Video Preview**.
13. Select the desired value from the pull-down list of **Auto Preview**.
14. (Optional.) Enter the username and the password in the **User Name** and **Password** field respectively.
They are required only if the IP intercom needs HTTP API authentication.

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

**To configure an Open Door key via web user interface (only applicable to 2N IP intercom):**

1. Click on **DSSKey -> Line Key** (or **Ext Key**).
2. In the desired DSS key field, select **Open Door** from the pull-down list of **Type**.
3. Enter the open door URL in the **Value** field.
   
   The valid URL format is:
   
4. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.
5. Enter the desired number or IP address of the IP intercom in the **Extension** field.

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

**To configure a Video Monitoring key via web user interface (only applicable to Baudisch IP intercom):**

1. Click on **DSSKey -> Line Key** (or **Ext Key**).
2. In the desired DSS key field, select **Video Monitoring** from the pull-down list of **Type**.
3. Enter the video access URL in the **Value** field.
   The valid URL format is: http://<IP address of the IP intercom>/mjpg/video.mjpg or
   http://username:password@<IP address of the IP intercom>/mjpg/video.mjpg.

4. (Optional.) Enter the string that will appear on the touch screen in the **Label** field.

5. Enter the desired number or IP address of the IP intercom in the **Extension** field.

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

To configure an **Open Door** key via phone user interface (only applicable to 2N IP intercom):

1. Tap **Settings** -> **Features** -> **DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **Open Door** 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 open door URL in the **URL** field.
7. Enter the desired door phone number in the **Extension** field.
8. Tap ✔️ to accept the change.

To configure a **Video Monitoring** key via phone user interface (only applicable to Baudisch IP intercom):

1. Tap **Settings** -> **Features** -> **DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **Video Monitoring** 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 video access URL in the **URL** field.
7. Enter the desired door phone number in the **Channel** field.
8. Tap ✔️ 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:

![Mobile Account Key Automatically Assigned](image)

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) | 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 |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td>Assign a mobile account key. Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=m</td>
</tr>
</tbody>
</table>

For more information on how to use your phone in conjunction with Bluetooth-enabled mobile phone, refer to the Yealink phone-specific user guide.
Mobile Account Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

Mobile account key can be configured only if the mobile phone has been connected successfully.

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

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:
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>For SIP-T58V/T58A/T56A IP phones:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When $Y = 1$ to 60, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> EXT key is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSSKey-&gt;Line Key/Programable Key/Ext Key-&gt;Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;DSS Keys-&gt;Line Key X-&gt;Type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>linekey.X.label/\nexpansion_module.X.key.Y.label</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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)

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

- DSSKey->Line Key/Ext Key->Label

**Phone User Interface:**

- Settings->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.

![Web User Interface Screenshot]

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter</th>
<th>Details of the Configuration Parameter:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>wui.quick_login</td>
<td>Parameter: wui.quick_login</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Permit: 0 or 1; Default: 0</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables the quick login feature.
- 0: Disabled
- 1: Enabled

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).
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.

Procedure

The uaCSTA feature can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure uaCSTA feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter:</td>
<td>features.csta_control.enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure uaCSTA feature.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to:</td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-remotecontrol&amp;q=load</td>
</tr>
</tbody>
</table>

Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.csta_control.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

Description:
Enables or disables the uaCSTA (User Agent Computer Supported Telecommunications Applications) feature on the IP phone.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Enabled</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** 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.
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
- Automatic Call Distribution (ACD)
- 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:

   ```xml
   <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:

```xml
<MenuItem>
  <Name>Department1</Name>
</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.

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) | 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
Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_phonebook.data.X.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>(X ranges from 1 to 5)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_phonebook.data.X.name</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>(X ranges from 1 to 5)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 ouser -> 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_phonebook.display_name</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_phonebook.display_name</td>
<td>characters</td>
<td></td>
</tr>
</tbody>
</table>

**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 |

---

479
### Administrator's Guide for SIP-T5 Series Smart Media Phones

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>0</strong>-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>1</strong>-Enabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gn</td>
<td>givenName</td>
<td>First name</td>
</tr>
<tr>
<td>cn</td>
<td>commonName</td>
<td>LDAP attribute is made up from given name joined to surname.</td>
</tr>
<tr>
<td>sn</td>
<td>surname</td>
<td>Last name or family name</td>
</tr>
<tr>
<td>dn</td>
<td>distinguishedName</td>
<td>Unique identifier for each entry</td>
</tr>
<tr>
<td>dc</td>
<td>dc</td>
<td>Domain component</td>
</tr>
<tr>
<td>-</td>
<td>company</td>
<td>Company or organization name</td>
</tr>
<tr>
<td>-</td>
<td>telephoneNumber</td>
<td>Office phone number</td>
</tr>
<tr>
<td>mobile</td>
<td>mobilePhoneNumber</td>
<td>Mobile or cellular phone number</td>
</tr>
<tr>
<td>ipPhone</td>
<td>IPPhoneNumber</td>
<td>Home phone number</td>
</tr>
</tbody>
</table>

For more information on LDAP, refer to *LDAP Phonebook on Yealink IP Phones*.

Procedure

LDAP can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td></td>
</tr>
<tr>
<td>Configure LDAP.</td>
<td></td>
</tr>
<tr>
<td><em>Parameters:</em></td>
<td></td>
</tr>
<tr>
<td>ldap.enable</td>
<td></td>
</tr>
<tr>
<td>ldap.customize_label</td>
<td></td>
</tr>
<tr>
<td>ldap.name_filter</td>
<td></td>
</tr>
<tr>
<td>ldap.number_filter</td>
<td></td>
</tr>
<tr>
<td>ldap.tls_mode</td>
<td></td>
</tr>
<tr>
<td>ldap.host</td>
<td></td>
</tr>
<tr>
<td>ldap.port</td>
<td></td>
</tr>
<tr>
<td>ldap.base</td>
<td></td>
</tr>
<tr>
<td>ldap.user</td>
<td></td>
</tr>
<tr>
<td>ldap.password</td>
<td></td>
</tr>
<tr>
<td>ldap.max_hits</td>
<td></td>
</tr>
<tr>
<td>ldap.name_attr</td>
<td></td>
</tr>
<tr>
<td>ldap.numb_attr</td>
<td></td>
</tr>
<tr>
<td>ldap.display_name</td>
<td></td>
</tr>
<tr>
<td>ldap.version</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap.call_in_lookup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap.call_out_lookup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap.ldap_sort</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap.incoming_call_special_search.enable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables LDAP feature on the IP phone.

**Web User Interface:**
Directory->LDAP->Enable LDAP

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>Parameters</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap.customize_label</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap.customize_label</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Description:**
Configures the display name of the LDAP phone book.

**Example:**
ldap.customize_label = Friends

If it is left blank, "LDAP" will be the display name.

**Note:** It works only if the value of the parameter "ldap.enable" is set to 1 (Enabled). It is not applicable to CP960 IP phones.

**Web User Interface:**
Directory -> LDAP -> LDAP Label

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>ldap.name_filter</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**Description:**
Configures the search criteria for LDAP contact names look up.

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

<table>
<thead>
<tr>
<th>ldap.number_filter</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap.number_filter</td>
<td>(</td>
<td>(telephoneNumber=<em>)(mobile=</em>)(ipPhone=*))</td>
</tr>
<tr>
<td></td>
<td>&amp;(telephoneNumber=<em>)(mobile=</em>)</td>
<td></td>
</tr>
</tbody>
</table>

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.

**Example:**

ldap.number_filter = (|(telephoneNumber=*)(mobile=*)(ipPhone=*))

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 touch screen.

**Web User Interface:**

- Directory -> LDAP -> LDAP Number Filter

**Phone User Interface:**

- None

<table>
<thead>
<tr>
<th>ldap.tls_mode</th>
<th>0, 1 or 2</th>
<th>0</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>ldap.host</th>
<th>IP address or domain name</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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
## Administrator’s Guide for SIP-T5 Series Smart Media Phones

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap.port</td>
<td>Integer from 1 to 65535</td>
<td>389</td>
</tr>
</tbody>
</table>

**Description:**
Configures the port of the LDAP server.

**Example:**
ldap.port = 389

**Web User Interface:**
Directory -> LDAP -> Port

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>ldap.base</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>ldap.user</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap.password</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>ldap.max_hits</th>
<th>Integer from 1 to 32000</th>
<th>50</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>ldap.name_attr</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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`
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldap.numb_attr</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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
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

<p>| ldap.version      | 2 or 3       | 3          |</p>
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the LDAP protocol version supported by the IP phone. Make sure the protocol value corresponds with the version assigned on the LDAP server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory-&gt;LDAP-&gt;Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap.call_in_lookup</td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to perform an LDAP search when receiving an incoming call.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory-&gt;LDAP-&gt;LDAP Lookup For Incoming Call</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap.call_out_lookup</td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to perform an LDAP search when placing a call.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory-&gt;LDAP-&gt;LDAP Lookup For Callout</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ldap.ldap_sort</td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to sort the search results in alphabetical order or numerical order.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### LDAP Key

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.&lt;X&gt;.type/programablekey.&lt;X&gt;.type/expansion_module.&lt;X&gt;.key.&lt;Y&gt;.type</td>
<td>38</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>
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:
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).

Note: EXT key is not applicable to CP960 IP phones.

Web User Interface:
DSSKey- Line Key/Programable Key- Type

Phone User Interface:
Settings- Features- DSS Keys- Line Key X- Type

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.label/ expansion_module.X.key.Y.label</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>
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)
**Note:** EXT key is not applicable to CP960 IP phones.

**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.

![Configuration interface](Image)

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:

```plaintext
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 5.80.0.5
Expires: 30
Event: dialog
Content-Length: 0
```

Example of a NOTIFY message (<state>confirmed</state> shows the call has been established):

```plaintext
NOTIFY sip:1010@10.3.20.1:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.2:5060;branch=z9hG4bK276311022
From: "1011" <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 5.80.0.5
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>
  </dialog>
</dialog-info>
```

495
<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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.blf.subscribe_period</td>
<td>Integer from 30 to 2147483647</td>
<td>1800</td>
</tr>
</tbody>
</table>

Description:

Configures the period (in seconds) of the BLF subscription for account X.  
X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)
## Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The IP phone is able to successfully refresh the SUBSCRIBE before expiration of the SUBSCRIBE dialog.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Account->Advanced->Subscribe Period(Seconds)

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>account.X.blf.subscribe_event</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

**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

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>account.X.out_dialog_blf_enable</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

**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**.

---

497
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 375.

**Procedure**

Configuration changes can be performed using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Specify whether to use visual alert and audio alert for BLF pickup.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Parameters:</td>
</tr>
<tr>
<td></td>
<td>features.pickup.blf_visual_enable</td>
</tr>
<tr>
<td></td>
<td>features.pickup.blf_audio_enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Specify whether to use visual alert and audio alert for BLF pickup.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/servlet?p=features-callpickup&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.pickup.blf_visual_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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->Pick up & Park->Visual Alert for BLF Pickup

**Phone User Interface:**

None

<table>
<thead>
<tr>
<th>features.pickup.blf_audio_enable</th>
<th>0 or 1</th>
<th>0</th>
</tr>
</thead>
</table>

**Description:**

Enables or disables the IP phone to play an audio alert when the monitored user receives an incoming call.

0-Disabled
To configure visual alert and audio alert for BLF pickup via web user interface:

1. Click on Features -> Pick up & Park.
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 507.

**Expansion Module Key LED** (configured as a BLF key or a BLF List key and BLF LED Mode is set to 0)

<table>
<thead>
<tr>
<th>LED Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid green</td>
<td>The monitored user is idle.</td>
</tr>
<tr>
<td>Fast-flashing red (200ms)</td>
<td>The monitored user receives an incoming call.</td>
</tr>
<tr>
<td>Solid red</td>
<td>The monitored user is dialing.</td>
</tr>
<tr>
<td></td>
<td>The monitored user is talking.</td>
</tr>
<tr>
<td>LED Status</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The monitored user’s conversation is placed on hold (This LED status requires server support).</td>
<td></td>
</tr>
<tr>
<td>Slow-flashing red (1s)</td>
<td>The call is parked against the monitored user’s phone number.</td>
</tr>
<tr>
<td>Off</td>
<td>The monitored user does not exist.</td>
</tr>
</tbody>
</table>

**Expansion Module Key LED** (configured as a BLF key or a BLF List key and BLF LED Mode is set to 1)

<table>
<thead>
<tr>
<th>LED Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast-flashing red (200ms)</td>
<td>The monitored user receives an incoming call.</td>
</tr>
<tr>
<td>Solid red</td>
<td>The monitored user is dialing. The monitored user is talking.</td>
</tr>
<tr>
<td></td>
<td>The monitored user’s conversation is placed on hold (This LED status requires server support).</td>
</tr>
<tr>
<td>Slowly-flashing red (1s)</td>
<td>The call is parked against the monitored user’s phone number.</td>
</tr>
<tr>
<td>Off</td>
<td>The monitored user is idle. The monitored user does not exist.</td>
</tr>
</tbody>
</table>

**Expansion Module Key LED** (configured as a BLF key or a BLF List key and BLF LED Mode is set to 2)

<table>
<thead>
<tr>
<th>LED Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast-flashing red (200ms)</td>
<td>The monitored user receives an incoming call.</td>
</tr>
<tr>
<td>Solid red</td>
<td>The monitored user is dialing. The monitored user is talking.</td>
</tr>
<tr>
<td></td>
<td>The monitored user’s conversation is placed on hold (This LED status requires server support).</td>
</tr>
<tr>
<td>Slowly-flashing red (1s)</td>
<td>The call is parked against the monitored user’s phone number.</td>
</tr>
<tr>
<td>Off</td>
<td>The monitored user is idle. The monitored user does not exist.</td>
</tr>
</tbody>
</table>

**Expansion Module Key LED** (configured as a BLF key or a BLF List key and BLF LED Mode is set to 3)

<table>
<thead>
<tr>
<th>LED Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast-flashing green (200ms)</td>
<td>The monitored user receives an incoming call.</td>
</tr>
<tr>
<td>Solid red</td>
<td>The monitored user is dialing. The monitored user is talking.</td>
</tr>
<tr>
<td></td>
<td>The monitored user’s conversation is placed on hold (This LED status requires server support).</td>
</tr>
</tbody>
</table>
LED Status | Description
---|---
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.)

<table>
<thead>
<tr>
<th>LED Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid green</td>
<td>The monitored user is talking.</td>
</tr>
<tr>
<td>Slowly-flashing green (1s)</td>
<td>The monitored user does not exist.</td>
</tr>
<tr>
<td>Off</td>
<td>The monitored user is idle.</td>
</tr>
</tbody>
</table>

**Procedure**

BLF LED mode can be configured using the following methods.

**Central Provisioning (Configuration File)**

Configure BLF LED mode.

**Parameter:**

`features.blf_led_mode`

**Web User Interface**

Configure BLF LED mode.

Navigate to:

http://<phoneIP Address>/servlet?p=features-general&q=load

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>features.blf_led_mode</code></td>
<td>0, 1, 2, 3 or 4</td>
<td>0</td>
</tr>
</tbody>
</table>

**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
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone User Interface:</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

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 805.
**Procedure**

BLF key can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>y0000000000xx.cfg</th>
<th>Assign a BLF key.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>linekey.X.type/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>expansion_module.X.key.Y.type</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linekey.X.line/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>expansion_module.X.key.Y.line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linekey.X.value/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>expansion_module.X.key.Y.value</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linekey.X.pickup_value/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>expansion_module.X.key.Y.pickup_value</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linekey.X.label/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>expansion_module.X.key.Y.label</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Assign a BLF key.</th>
<th>Navigate to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=dsskey&amp;q=load</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th>Assign a BLF key.</th>
</tr>
</thead>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>expansion_module.X.key.Y.type</td>
<td>16</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**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
### Configuring Advanced Features

**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 ext keys:
**For SIP-T58V/T58A/T56A IP phones:**
When Y= 1 to 60, the default value is 0 (NA).
**Note:** EXT key is not applicable to CP960 IP phones.

**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 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

**Note:** EXT key is not applicable to CP960 IP phones.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSSKey-&gt;Line Key-&gt;Line</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;DSS Keys-&gt;Line Key X-&gt;Account ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>linekey.X.value/ expansion_module.X.key.Y.value</strong></td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

**Note:** EXT key is not applicable to CP960 IP phones.

| **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. EXT key is not applicable to CP960 IP phones.

**Web User Interface:**
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSSKey-&gt;Line Key-&gt;Extension</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Phone User Interface:**

Settings->Features->DSS Keys->Line Key X->Extension

#### linekey.X.label/expansion_module.X.key.Y.label

<table>
<thead>
<tr>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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)

**Note:** EXT key is not applicable to CP960 IP phones.

**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.

| Central Provisioning | <MAC>.cfg | Configure BLF List. Parameters: |
Configuring Advanced Features

### Configuration File

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.blf.blf_list_uri</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.blf_list_code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.blf_list_barge_in_code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.blf_list_retrieve_call_parked_code</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Specify whether to automatically configure the BLF list keys.

**Parameter:**

phone_setting.auto_blf_list_enable

Configure the order of BLF list keys assigned automatically.

**Parameter:**

phone_setting.blf_list_sequence_type

Assign a BLF List key.

**Parameters:**

- linekey.X.type/
- expansion_module.X.key.Y.type
- linekey.X.line/
- expansion_module.X.key.Y.line

### Web User Interface

Configure BLF List.

**Navigate to:**

http://<phoneIPAddress>/servlet?m=mod_data&p=account-adv&q=load&acc=0

Assign a BLF List key.

**Navigate to:**

http://<phoneIPAddress>/servlet?m=mod_data&p=dsskey&q=load

### Phone User Interface

Assign a BLF List key.

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.auto_blf_list_enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**

Enables or disables the IP phone to automatically configure the BLF list keys.

- **0** - Disabled
- **1** - Enabled
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>phone_setting.blf_list_sequence_type</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>account.X.blf.blf_list_uri</strong></td>
<td>String within 256 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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:**
Account -> Advanced -> BLF List URI

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>account.X.blf_list_code</strong></td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Description:**
Configures the feature access code for directed call pickup for account X.
## Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A) X is equal to 1 (for CP960)</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Example:**

account.1.blf_list_code = *97

**Web User Interface:**

Account->Advanced->BLF List Pickup Code

**Phone User Interface:**

None

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.blf_list_barge_in_code</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.blf_list_retrieve_call_parked_code</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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)

**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 805.

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/expansion_module.X.key.Y.type</td>
<td>39</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

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:
When Y= 1 to 60, the default value is 0 (NA).
**Note**: EXT key is not applicable to CP960 IP phones.

Web User Interface:
DSSKey->Line Key->Type

Phone User Interface:
Settings->Features->DSS Keys->Line Key X->Type

<table>
<thead>
<tr>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refer to the following content</td>
<td>1-16 for lines 1-16</td>
</tr>
</tbody>
</table>

linekey.X.line/expansion_module.X.key.Y.line
### Parameters

<table>
<thead>
<tr>
<th>Description:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the desired line to apply the BLF List key.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>1 to 16</th>
<th>(for SIP-T58V/T58A/T56A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(for CP960)</td>
</tr>
<tr>
<td>1-Line 1</td>
<td></td>
</tr>
<tr>
<td>2-Line 2</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>16-Line 16</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

```
linekey.1.line = 1
```

**Note:** EXT key is not applicable to CP960 IP phones.

### 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.

![Blf List Retrieve Call Parked Code Field](image)

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.

![Dss Key List](image)

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure the hide feature access codes feature. Parameter: features.hide_feature_access_codes.enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td>Configure the hide feature access codes feature. Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.hide_feature_access_codes.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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.

**Automatic Call Distribution (ACD)**

ACD enables organizations to manage a large number of phone calls on an individual basis. ACD enables the use of IP phones in a call-center role by automatically distributing incoming calls to available users, or agents. ACD depends on support from a SIP server. ACD is disabled on the IP phone by default. You need to enable it on a per-line basis before logging into the ACD system.

After the IP phone user logs into the ACD system, the server monitors the IP phone status and then decides whether to assign an incoming call to the user’s IP phone. When the IP phone status is changed to unavailable, the server stops distributing calls to the IP phone. The IP phone will remain in the unavailable status until the user manually changes the IP phone status or the ACD auto available timer (if configured) expires. How long the IP phone remains unavailable is configurable by the auto available timer. When the timer expires, the IP phone status is automatically changed to available. ACD auto available timer feature depends on support from a SIP server.

You can configure an ACD key for the user to log in into the ACD system. The ACD key on the IP phone indicates the ACD status.

**Note**

It is not applicable to CP960 IP phones.
## Procedure

ACD can be configured using the following methods.

| Central Provisioning (Configuration File) | <MAC>.cfg | Configure ACD feature on a per-line basis.  
**Parameters:**  
account.X.acd.enable  
account.X.acd.available  
account.X.subscribe_acd_expires |
| --- | --- | --- |
|  | <y0000000000xx>.cfg | Configure ACD auto available.  
**Parameters:**  
acd.auto_available  
acd.auto_available_timer |
|  |  | Assign an ACD key.  
**Parameters:**  
linekey.X.type/  
expansion_module.X.key.Y.type  
linekey.X.label/  
expansion_module.X.key.Y.label |
| Web User Interface |  | Configure ACD auto available.  
**Navigate to:**  
http://<phoneIPAddress>/servlet?p=features-acd&q=load |
|  |  | Assign an ACD key.  
**Navigate to:**  
http://<phoneIPAddress>/servlet?p=dsskey&q=load&model=0 |
| Phone User Interface |  | Assign an ACD key. |

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.acd.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

(X ranges from 1 to 16)

**Description:**

Enables or disables ACD feature for account X.

0-Disabled
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.acd.available</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables the IP phone to display the **Available** or **Unavailable** for account X after the IP phone logs into the ACD system.

0 - Disabled
1 - Enabled

**Note:** It works only if the value of the parameter “account.X.acd.enable” is set to 1 (Enabled). It is not applicable to CP960 IP phones.

**Web User Interface:**
None

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.subscribe_acd_expires</td>
<td>Integer from 120 to 3600</td>
<td>3600</td>
</tr>
</tbody>
</table>

**Description:**
Configures the period (in seconds) of ACD subscription for account X.

**Note:** It works only if the value of the parameter “account.X.acd.enable” is set to 1 (Enabled). It is not applicable to CP960 IP phones.

**Web User Interface:**
Account -> Advanced -> ACD Subscribe Period(120~3600s)

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>acd.auto_available</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables the IP phone to automatically change the status of the ACD agent to
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>acd.auto_available_timer</td>
<td>Integer from 0 to 120</td>
<td>60</td>
</tr>
</tbody>
</table>

**Description:**
Configures the interval (in seconds) for the status of the ACD agent to be automatically changed to available.

**Note:** It works only if the values of parameters “account.X.acd.enable” and “acd.auto_available” are set to 1 (Enabled). It is not applicable to CP960 IP phones.

**Web User Interface:**
Features->ACD->ACD Auto Available Timer (0~120s)

**Phone User Interface:**
None

**ACD Key**

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>expansion_module.X.key.Y.type</td>
<td>42</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**Description:**
Configures a DSS key to be an ACD key on the IP phone.
The digit 42 stands for the key type ACD.
For line keys:
### Administrator's Guide for SIP-T5 Series Smart Media Phones

**Parameters** | **Permitted Values** | **Default**
--- | --- | ---

| X ranges from 1 to 27 (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 = 42
```

**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 ext keys:

**For SIP-T58V/T58A/T56A IP phones:**

When Y=1-60, the default value is 0 (NA).

**Web User Interface:**

Dsskey->Line Key->Type

**Phone User Interface:**

Menu->Features->DSS Keys->Line Key X->Type

| linekey.X.label/ | String within 99 characters | Blank |
| expansion_module.X.key.Y.label |  |  |

**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)

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:**

Menu->Features->DSS Keys->Line Key X->Label

**To configure an ACD key via web user interface:**

1. Click on **DSSKey**->**Line Key**.
2. In the desired DSS key field, select **ACD** 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 ACD auto available timer feature via web user interface:

1. Click on Features -> ACD.
2. Select the desired value from the pull-down list of ACD Auto Available.
3. Enter the desired timer in the ACD Auto Available Timer(0~120s) field.

4. Click Confirm to accept the change.

To configure the ACD subscribe period 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 timer in the **ACD Subscribe Period** **(120~3600s)** field.

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

**To configure an ACD key via phone user interface:**

1. Tap **Settings** > **Features** > **DSS Keys**.
2. Tap the desired DSS key.
3. Tap the **Type** field.
4. Tap **ACD** 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.

**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 171. If you want to customize multiple DSS keys to associate with an account, refer to **Multiple Line Keys per Account** on page 179.

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>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
</tr>
</thead>
</table>
| <MAC>.cfg | Configure the registration line type. 
 **Parameter:** 
 account.X.shared_line  
|  
| Configure the call pull feature access code.  
 **Parameter:** 
 account.X.shared_line_callpull_code  
|  
| <y0000000000xx>.cfg | Configure the private hold soft key.  
 **Parameters:** 
 phone_setting.custom_softkey_enable 
 custom_softkey_talking.url  
|  
| Assign a private hold key.  
 **Parameters:** 
 linekey.X.type/ 
 expansion_module.X.key.Y.type 
 linekey.X.label/ 
 expansion_module.X.key.Y.label  
|  
| Web User Interface |  
|  
| 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  
|  
| Configure the private hold soft key.  
 **Navigate to:**  
 http://<phoneIPAddress>/servlet?m=mod_data&p=settings-softkey&q=loa  
|
Assign a private hold key.

**Navigate to:**
http://<phoneIP Address>/servlet?m=mod_data&p=dsskey&q=load

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th>Assign a private hold key.</th>
</tr>
</thead>
</table>

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.shared_line</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.shared_line_callpull_code</th>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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 214.

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.custom_softkey_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>custom_softkey_talking.url</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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 805.
Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/ expansion_module.X.key.Y.type</td>
<td>20</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**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 SIP-T58V/T58A/T56A IP phones:**
When Y= 1 to 60, the default value is 0 (NA).

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**
DSSKey->Line Key/Programable Key->Type

**Phone User Interface:**
Settings->Features->DSS Keys->Line Key X->Type
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.label/\nexpansion_module.X.key.Y.label</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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)

**Note:** EXT key is not applicable to CP960 IP phones.

**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**.

![Advanced Settings](image)

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.)

![Web UI](image)
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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.subscribe_mwi</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong> None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>account.X.subscribe_mwi_expires</strong></td>
<td>Integer from 0 to 84600</td>
<td>3600</td>
</tr>
<tr>
<td><strong>Description:</strong> 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) <strong>Note:</strong> It works only if the value of the parameter “account.X.subscribe_mwi” is set to 1 (Enabled).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong> Account-&gt;Advanced-&gt;MWI Subscription Period (Seconds)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong> None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>account.X.subscribe_mwi_to_vm</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong> 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) <strong>Note:</strong> 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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong> Account-&gt;Advanced-&gt;Subscribe MWI To Voice Mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong> None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>voice_mail.number.X</strong></td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Description</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the voice mail number for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>voice_mail.number.1 = 1234</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Account- &gt; Advanced- &gt; Voice Mail</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>Message- &gt; Voice Mail- &gt; Set Voice Mail- &gt; AccountX Code</td>
<td></td>
</tr>
</tbody>
</table>

| 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Specify a multicast codec for the IP phone to send the RTP stream. Parameter: multicast.codec</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure the multicast IP address and port number for a paging list key. Parameter: multicast.paging_address.X.ip_address</td>
</tr>
<tr>
<td></td>
<td>Configure the channel of the multicast paging group for a paging list key. Parameter: multicast.paging_address.X.channel</td>
</tr>
<tr>
<td></td>
<td>Configure the multicast paging group name for a paging list key. Parameter: multicast.paging_address.X.label</td>
</tr>
<tr>
<td></td>
<td>Assign a multicast paging key. Parameters: linekey.X.type/programmable.X.type/ expansion_module.X.key.Y.type</td>
</tr>
<tr>
<td></td>
<td>linekey.X.value/programmable.X.value/ expansion_module.X.key.Y.value</td>
</tr>
<tr>
<td></td>
<td>linekey.X.label/programmable.X.label/ expansion_module.X.key.Y.label</td>
</tr>
<tr>
<td></td>
<td>Assign a paging list key. Parameter: linekey.X.type/programmable.X.type/ expansion_module.X.key.Y.type</td>
</tr>
<tr>
<td></td>
<td>linekey.X.label/programmable.X.label/ expansion_module.X.key.Y.label</td>
</tr>
</tbody>
</table>
**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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast.codec</td>
<td>PCMU, PCMA, G729, G722</td>
<td>G722</td>
</tr>
</tbody>
</table>

**Description:**

Configures the codec of multicast paging.

**Example:**

multicast.codec = G722
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; General Information -&gt; Multicast Codec</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>multicast.paging_address.X.ip_address</strong></td>
<td>String</td>
<td>Blank</td>
</tr>
<tr>
<td>(X ranges from 1 to 31)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>multicast.paging_address.1.ip_address = 224.5.6.20:10008</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multicast.paging_address.2.ip_address = 224.1.6.25:1001</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory -&gt; Multicast IP -&gt; Paging List -&gt; Paging Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings -&gt; Features -&gt; Paging List -&gt; Option -&gt; Edit -&gt; Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>multicast.paging_address.X.label</strong></td>
<td>String</td>
<td>Blank</td>
</tr>
<tr>
<td>(X ranges from 1 to 31)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>multicast.paging_address.1.label = Product</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multicast.paging_address.2.label = Sales</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory -&gt; Multicast IP -&gt; Paging List -&gt; Label</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings -&gt; Features -&gt; Paging List -&gt; Option -&gt; Edit -&gt; Label</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>multicast.paging_address.X.channel</strong></td>
<td>Integer from 0 to 30</td>
<td>0</td>
</tr>
<tr>
<td>(X ranges from 1 to 31)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/ expansion_module.X.key.Y.type</td>
<td>24</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

### 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:**

For more information on how to configure the DSS Key, refer to [Appendix D: Configuring DSS Key](#) on page 805.
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.2.type = 24</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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).

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey -> Line Key -> Type

**Phone User Interface:**

Settings -> Features -> DSS Keys -> Line Key X -> Type

<table>
<thead>
<tr>
<th>linekey.X.value/ expansion_module.X.key.Y.value</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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. EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey -> Line Key -> Value

**Phone User Interface:**

Settings -> Features -> DSS Keys -> Line Key X -> Value

<table>
<thead>
<tr>
<th>linekey.X.label/ expansion_module.X.key.Y.label</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>
### 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)
**Note:** EXT key is not applicable to CP960 IP phones.

#### Web User Interface:
DSSKey->Line Key->Label

#### Phone User Interface:
Settings->Features->DSS Keys->Line Key X->Label

```plaintext
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. EXT key is not applicable to CP960 IP phones.

#### 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 805.
Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/programablekey.X.type/ expansion_module.X.key.Y.type</td>
<td>66</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**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).

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**
DSSKey->Line Key/Programable Key->Type

**Phone User Interface:**
Settings->Features->DSS Keys->Line Key X->Type
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.label/ expansion_module.X.key.Y.label</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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)

**Note:** EXT key is not applicable to CP960 IP phones.

**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**

Paging Barge feature defines the lowest priority of the multicast paging call that can be received when there is a voice call (a normal phone call rather than a multicast paging call) in progress. If it is disabled, all incoming multicast paging calls will be automatically ignored. If it is set to a specify 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**

Paging Priority Active feature decides how the IP phone handles the incoming multicast paging calls when there is already a multicast paging call in progress. If it is disabled, the IP phone will automatically ignore all incoming multicast paging calls. If it is 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameters:</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>multicast.listen_address.X.ip_address</td>
<td>Blank</td>
</tr>
<tr>
<td></td>
<td>multicast.listen_address.X.label</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multicast.listen_address.X.channel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multicast.listen_address.X.volume</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multicast.receive.use_speaker</td>
<td></td>
</tr>
</tbody>
</table>

Configure the listening multicast address.

Configure Paging Barge and Paging Priority Active features.

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Parameters:</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast.receive_priority.enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>multicast.receive_priority.priority</td>
<td></td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast.listen_address.X.ip_address</td>
<td>IP address: port</td>
<td>Blank</td>
</tr>
<tr>
<td>(X ranges from 1 to 31)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast.listen_address.X.label</td>
<td>String within 99</td>
<td>Blank</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------</td>
<td>--------</td>
</tr>
<tr>
<td>(X ranges from 1 to 31)</td>
<td>characters</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>multicast.listen_address.X.channel</th>
<th>Integer from 0 to 30</th>
<th>0</th>
</tr>
</thead>
</table>

**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.

If 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

<table>
<thead>
<tr>
<th>multicast.listen_address.X.volume</th>
<th>Integer from 0 to 15</th>
<th>0</th>
</tr>
</thead>
</table>

**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.
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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast.receive.use_speaker</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast.receive_priority.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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:**
## Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multicast.receive_priority.priority</td>
<td>Integer from 0 to 31</td>
<td>31</td>
</tr>
</tbody>
</table>

**Description:**

Configures the lowest priority of the multicast paging call that can be received when there is a voice 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, all incoming multicast paging calls will be automatically ignored when a voice call is in progress.

1-1
2-2
3-3
...
31-31

If it is set to other values, the IP phone will receive the incoming multicast paging call with a higher or equal priority and ignore that with a lower priority when a voice 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 449.

**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 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 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
Request Method: GET
Request URL: /URLRecord/record.xml
Request version: HTTP/1.1
Host: 10.3.5.97:8080
User-agent: Yealink T58 5.80.0.5 00:15:65:74:B1:50
```

If the recording is successfully started, the server will respond with a 200 OK message.

Example of a 200 OK message:

```
<YealinkIPPhoneText>
>Title>
```
The recording session is successfully started.

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:

Probably the recording box is full.

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:

The recording session is successfully stopped.

Procedure

Record or URL record key can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Assign a record key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a URL record key.</td>
<td><strong>Parameters:</strong></td>
</tr>
<tr>
<td><strong>Parameters:</strong></td>
<td>linekey.X.type/</td>
</tr>
<tr>
<td></td>
<td>expansion_module.X.key.Y.type</td>
</tr>
<tr>
<td></td>
<td>linekey.X.label/</td>
</tr>
<tr>
<td></td>
<td>expansion_module.X.key.Y.label</td>
</tr>
</tbody>
</table>
Configuring Advanced Features

| Web User Interface | Assign a record key and URL record key.  
| Navigate to:       | http://<phoneIPAddress>/servlet?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 805.

### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/ expansion_module.X.key.Y.type</td>
<td>25</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**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.
### Administrator’s Guide for SIP-T5 Series Smart Media Phones

#### 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).
**Note:** EXT key is not applicable to CP960 IP phones.
**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)
**Note:** EXT key is not applicable to CP960 IP phones.

**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:
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 30 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For ext keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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).

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey->Line Key->Type

**Phone User Interface:**

Settings->Features->DSS Keys->Line Key X->Type

<table>
<thead>
<tr>
<th>linekey.X.value/ expansion_module.X.key.Y.value</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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
```

**Note:** EXT key is not applicable to CP960 IP phones.

**Web User Interface:**

DSSKey->Line Key->Value
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings- &gt; Features- &gt; DSS Keys- &gt; Line Key X- &gt; Value</td>
<td></td>
<td></td>
</tr>
<tr>
<td>linekey.X.label/ expansion_module.X.key.Y.label</td>
<td>String within 99 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

### 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)

**Note:** EXT key is not applicable to CP960 IP phones.

### 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=modal_data&p=dsskey&q=load
| Phone User Interface | | Assign a hot desking key.

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hotdesking.dsskey_register_name_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

Description:
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>hotdesking.dsskey_username_enable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>hotdesking.dsskey_password_enable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to provide input field of password on the hot desking login wizard when tapping the Hot Desking key.</td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>hotdesking.dsskey_sip_server_enable</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>
### Hotdesking.dsskey_outbound_enable

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hotdesking.dsskey_outbound_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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 805.

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/programablekey.X.type/</td>
<td>34</td>
<td>Refer to the following content</td>
</tr>
<tr>
<td>expansion_module.X.key.Y.type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>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)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

`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).

**Note:** EXT key is not applicable to CP960 IP phones.

### Web User Interface:

DSSKey -> Line Key/Programable Key -> Type

### Phone User Interface:

Settings -> Features -> DSS Keys -> Line Key X -> Type

<table>
<thead>
<tr>
<th>linekey.X.label/expansion_module.X.key.Y.label</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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)

**Note:** EXT key is not applicable to CP960 IP phones.
## Administrator’s Guide for SIP-T5 Series Smart Media Phones

### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>DSSKey-&gt;Line Key-&gt;Label</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>Settings-&gt;Features-&gt;DSS Keys-&gt;Line Key X-&gt;Label</td>
<td></td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Method</th>
<th>Configuration Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Provisioning</td>
<td>Configure the logon wizard. Parameters:</td>
</tr>
<tr>
<td>(Configuration File)</td>
<td>phone_setting.logon_wizard</td>
</tr>
<tr>
<td></td>
<td>hotdesking.startup_register_name_enable</td>
</tr>
<tr>
<td></td>
<td>hotdesking.startup_username_enable</td>
</tr>
<tr>
<td></td>
<td>hotdesking.startup_password_enable</td>
</tr>
<tr>
<td></td>
<td>hotdesking.startup_sip_server_enable</td>
</tr>
<tr>
<td></td>
<td>hotdesking.startup_outbound_enable</td>
</tr>
<tr>
<td>Web User Interface</td>
<td>Configure the logon wizard. Navigate to:</td>
</tr>
<tr>
<td></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

Details of the Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.logon_wizard</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hotdesking.startup_register_name_enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>hotdesking.startup_username_enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to provide input field of user name on the logon wizard during the first startup.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>0</strong>-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>1</strong>-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> 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).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>hotdesking.startup_password_enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to provide input field of password on the logon wizard during the first startup.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>0</strong>-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>1</strong>-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> 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).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
### Parameters Permitted Values Default

<table>
<thead>
<tr>
<th>Phone User Interface:</th>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td><strong>hotdesking.startup_sip_server_enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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).

**Web User Interface:**
None

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>Phone User Interface:</th>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td><strong>hotdesking.startup_outbound_enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup Completed</td>
<td>When the IP phone completes startup.</td>
</tr>
<tr>
<td>Registered</td>
<td>When the IP phone successfully registers an account.</td>
</tr>
<tr>
<td>Unregistered</td>
<td>When the IP phone logs off the registered account.</td>
</tr>
<tr>
<td>Register Failed</td>
<td>When the IP phone fails to register an account.</td>
</tr>
<tr>
<td>Off Hook</td>
<td>When the IP phone is off hook (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>On Hook</td>
<td>When the IP phone is on hook (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>Incoming Call</td>
<td>When the IP phone receives an incoming call.</td>
</tr>
<tr>
<td>Outgoing Call</td>
<td>When the IP phone places a call.</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Established</td>
<td>When the IP phone establishes a call.</td>
</tr>
<tr>
<td>Terminated</td>
<td>When the IP phone terminates a call.</td>
</tr>
<tr>
<td>Open DND</td>
<td>When the IP phone enables the DND mode.</td>
</tr>
<tr>
<td>Close DND</td>
<td>When the IP phone disables the DND mode.</td>
</tr>
<tr>
<td>Open Always Forward</td>
<td>When the IP phone enables the always forward.</td>
</tr>
<tr>
<td>Close Always Forward</td>
<td>When the IP phone disables the always forward.</td>
</tr>
<tr>
<td>Open Busy Forward</td>
<td>When the IP phone enables the busy forward.</td>
</tr>
<tr>
<td>Close Busy Forward</td>
<td>When the IP phone disables the busy forward.</td>
</tr>
<tr>
<td>Open NoAnswer Forward</td>
<td>When the IP phone enables the no answer forward.</td>
</tr>
<tr>
<td>Close NoAnswer Forward</td>
<td>When the IP phone disables the no answer forward.</td>
</tr>
<tr>
<td>Transfer Call</td>
<td>When the IP phone transfers a call.</td>
</tr>
<tr>
<td>Blind Transfer</td>
<td>When the IP phone blind transfers a call.</td>
</tr>
<tr>
<td>Attended Transfer</td>
<td>When the IP phone performs the semi-attended/attended transfer.</td>
</tr>
<tr>
<td>Hold</td>
<td>When the IP phone places a call on hold.</td>
</tr>
<tr>
<td>UnHold</td>
<td>When the IP phone resumes a hold call.</td>
</tr>
<tr>
<td>Held</td>
<td>When a call of the IP phone is held.</td>
</tr>
<tr>
<td>UnHeld</td>
<td>When a held call is resumed.</td>
</tr>
<tr>
<td>Mute</td>
<td>When the IP phone mutes a call.</td>
</tr>
<tr>
<td>UnMute</td>
<td>When the IP phone unmutes a call.</td>
</tr>
<tr>
<td>Missed Call</td>
<td>When the IP phone misses a call.</td>
</tr>
<tr>
<td>IP Changed</td>
<td>When the IP address of the IP phone changes.</td>
</tr>
<tr>
<td>Idle To Busy</td>
<td>When the state of the IP phone changes from idle to busy.</td>
</tr>
<tr>
<td>Busy To Idle</td>
<td>When the state of phone changes from busy to idle.</td>
</tr>
<tr>
<td>Reject Incoming Call</td>
<td>When the IP phone rejects an incoming call.</td>
</tr>
<tr>
<td>Answer New-In Call</td>
<td>When the IP phone answers a new call.</td>
</tr>
<tr>
<td>Transfer Failed</td>
<td>When the IP phone fails to transfer a call.</td>
</tr>
<tr>
<td>Transfer Finished</td>
<td>When the IP phone completes to transfer a call.</td>
</tr>
<tr>
<td>Forward Incoming Call</td>
<td>When the IP phone forwards an incoming call.</td>
</tr>
<tr>
<td>Autop Finish</td>
<td>When the IP phone completes auto provisioning via power on.</td>
</tr>
</tbody>
</table>
### Administrator’s Guide for SIP-T5 Series Smart Media Phones

#### Event Description

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Call Waiting</td>
<td>When the IP phone enables the call waiting.</td>
</tr>
<tr>
<td>Close Call Waiting</td>
<td>When the IP phone disables the call waiting.</td>
</tr>
<tr>
<td>Headset</td>
<td>When the IP phone presses the HEADSET key (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>Handfree</td>
<td>When the IP phone presses the Speakerphone key (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>Cancel Call Out</td>
<td>When the IP phone cancels an outgoing call in the ring-back state.</td>
</tr>
<tr>
<td>Remote Busy</td>
<td>When an outgoing call is rejected.</td>
</tr>
<tr>
<td>Call Remote Canceled</td>
<td>When the remote party cancels the outgoing call in the ringing state.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Variable Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$mac</td>
<td>The MAC address of the IP phone.</td>
</tr>
<tr>
<td>$ip</td>
<td>The IP address of the IP phone.</td>
</tr>
<tr>
<td>$model</td>
<td>The IP phone model.</td>
</tr>
<tr>
<td>$firmware</td>
<td>The firmware version of the IP phone.</td>
</tr>
<tr>
<td>$active_url</td>
<td>The SIP URI of the current account when the IP phone places a call, receives an incoming call or establishes a call.</td>
</tr>
<tr>
<td>$active_user</td>
<td>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.</td>
</tr>
<tr>
<td>$active_host</td>
<td>The host part of the SIP URI for the current account when the IP phone places a call, receives an incoming call or establishes a call.</td>
</tr>
<tr>
<td>$local</td>
<td>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.</td>
</tr>
<tr>
<td>Variable Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| $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)**

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
| Web User Interface | 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 |

Configure action URL.

**Navigate to:**

http://<phoneIPAddress>/servlet?m=mod_data&p=features-actionurl&q=load
# Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>action_url.setup_completed</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>action_url.registered</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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=$ip
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Action URL -&gt; Registered</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>action_url.unregistered</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends after an account is unregistered.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.unregistered = <a href="http://192.168.0.20/help.xml?IP=%5C$ip">http://192.168.0.20/help.xml?IP=\$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Action URL -&gt; Unregistered</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>action_url.register_failed</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends after a register failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.register_failed = <a href="http://192.168.0.20/help.xml?IP=%5C$ip">http://192.168.0.20/help.xml?IP=\$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Action URL -&gt; Register Failed</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>action_url.off_hook</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends when off hook.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.off_hook = <a href="http://192.168.0.20/help.xml?IP=%5C$ip">http://192.168.0.20/help.xml?IP=\$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Web User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Action URL-&gt;Off Hook</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>action_url.incoming_call</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>action_url.outgoing_call</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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
```
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Action URL-&gt;Outgoing Call</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>action_url.call_established</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends when establishing a call.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.call_established = <a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Action URL-&gt;Established</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>action_url.dnd_on</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends when DND feature is enabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.dnd_on = <a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Action URL-&gt;Open DND</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>action_url.dnd_off</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends when DND feature is disabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.dnd_off = <a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Action URL-&gt;Close DND</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>action_url.always_fwd_on</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the action URL the IP phone sends when always forward feature is enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>action_url.always_fwd_on = <a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Features-&gt;Action URL-&gt;Open Always Forward</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>action_url.always_fwd_off</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the action URL the IP phone sends when always forward feature is disabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>action_url.always_fwd_off = <a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Features-&gt;Action URL-&gt;Close Always Forward</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>action_url.busy_fwd_on</strong></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the action URL the IP phone sends when busy forward feature is enabled.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>action_url.busy_fwd_on = <a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Features-&gt;Action URL-&gt;Open Busy Forward</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><code>action_url.busy_fwd_off</code></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>action_url.no_answer_fwd_on</code></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>action_url.transfer_call</code></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>phone sends when performing a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>transfer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.transfer_call =</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Action URL -&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transfer Call</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.blind_transfer_call</td>
<td>URL within 511</td>
<td>Blank</td>
</tr>
<tr>
<td>characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>phone sends when performing a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>blind transfer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.blind_transfer_call =</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Action URL -&gt; Blind</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transfer</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.attended_transfer_call</td>
<td>URL within 511</td>
<td>Blank</td>
</tr>
<tr>
<td>characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>phone sends when performing an</td>
<td></td>
<td></td>
</tr>
<tr>
<td>attended/semi-attended transfer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.attended_transfer_call</td>
<td></td>
<td></td>
</tr>
<tr>
<td>= <a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Action URL -&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attended Transfer</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.hold</td>
<td>URL within 511</td>
<td>Blank</td>
</tr>
<tr>
<td>characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>action_url.hold</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirms the action URL the IP phone sends when placing a call on hold.</td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>action_url.hold = <a href="http://192.168.0.20/help.xml?IP=$%7Bip%7D">http://192.168.0.20/help.xml?IP=${ip}</a></td>
<td>Web User Interface:</td>
<td></td>
</tr>
<tr>
<td>Features- &gt;Action URL- &gt;Hold</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.unhold</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirms the action URL the IP phone sends when resuming a hold call.</td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>action_url.unhold = <a href="http://192.168.0.20/help.xml?IP=$%7Bip%7D">http://192.168.0.20/help.xml?IP=${ip}</a></td>
<td>Web User Interface:</td>
<td></td>
</tr>
<tr>
<td>Features- &gt;Action URL- &gt;UnHold</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.held</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirms the action URL the IP phone sends when a call is held.</td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>action_url.held = <a href="http://192.168.0.20/help.xml?IP=$%7Bip%7D">http://192.168.0.20/help.xml?IP=${ip}</a></td>
<td>Web User Interface:</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.unheld</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirms the action URL the IP phone sends when a call being held is resumed.</td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------</td>
<td>---------</td>
</tr>
<tr>
<td>action_url.unheld</td>
<td><a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
None

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>action_url.mute</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>action_url.unmute</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>action_url.missed_call</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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:**
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features -&gt; Action URL -&gt; Missed Call</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong> None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.ip_change</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>action_url.forward_incoming_call</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>action_url.reject_incoming_call</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>action_url.answer_new_incoming_call</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>action_url.transfer_finished</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>action_url.transfer_failed</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>action_url.setup_autop_finish</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends when completing auto provisioning via power on.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.setup_autop_finish = <a href="http://192.168.0.20/help.xml?IP=$%7Bip%7D">http://192.168.0.20/help.xml?IP=${ip}</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Action URL -&gt; Autop Finish</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>action_url.call_waiting_on</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends when call waiting feature is enabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.call_waiting_on = <a href="http://192.168.0.20/help.xml?IP=$%7Bip%7D">http://192.168.0.20/help.xml?IP=${ip}</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Action URL -&gt; Open Call Waiting</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>action_url.call_waiting_off</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends when call waiting feature is disabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.call_waiting_off = <a href="http://192.168.0.20/help.xml?IP=$%7Bip%7D">http://192.168.0.20/help.xml?IP=${ip}</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features -&gt; Action URL -&gt; Close Call Waiting</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>action_url.headset</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>action_url.headset</td>
<td>Configures the action URL the IP phone sends when pressing the HEADSET key.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>action_url.headset = <a href="http://192.168.0.20/help.xml?IP=$ip">http://192.168.0.20/help.xml?IP=$ip</a></td>
<td></td>
</tr>
<tr>
<td>Note: It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td>Features -&gt; Action URL -&gt; Headset</td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

| action_url.handfree        | 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  | 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     | Configures the action URL the IP phone sends when the call is in the remote busy state. |
| 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                   |
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends when the outgoing call is rejected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.remote_busy = <a href="http://192.168.0.20/help.xml?IP=%5C$ip">http://192.168.0.20/help.xml?IP=\$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Action URL-&gt;Remote Busy</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>action_url.call_remote_canceled</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the action URL the IP phone sends when the remote party cancels the outgoing call in the ringing state.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>action_url.call_remote_canceled = <a href="http://192.168.0.20/help.xml?IP=%5C$ip">http://192.168.0.20/help.xml?IP=\$ip</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features-&gt;Action URL-&gt;Call Remote Canceled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.exe?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 302.

**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 T5 58.80.0.5
Event: ACTION-URI
```
The following table lists pre-defined variable values:

<table>
<thead>
<tr>
<th>Variable Value</th>
<th>Phone Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Tap <strong>Settings</strong> -&gt; <strong>Status</strong>.</td>
</tr>
<tr>
<td>SPEAKER</td>
<td>Press the Speakerphone key (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>F_TRANSFER</td>
<td>Transfer a call to another party.</td>
</tr>
<tr>
<td>VOLUME_UP</td>
<td>Increase the volume.</td>
</tr>
<tr>
<td>VOLUME_DOWN</td>
<td>Decrease the volume.</td>
</tr>
<tr>
<td>MUTE</td>
<td>Mute a call.</td>
</tr>
<tr>
<td>F_HOLD/HOLD</td>
<td>Place an active call on hold.</td>
</tr>
<tr>
<td>F_CONFERENCE</td>
<td>Tap the <strong>Conference</strong> soft key (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>Cancel/CANCEL/X</td>
<td>Cancel actions or reject incoming calls or end a call.</td>
</tr>
<tr>
<td>0-9/*/POUND</td>
<td>Press the keypad (0-9, * or #) (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>L1-LX</td>
<td>Tap the line keys (X=27).</td>
</tr>
<tr>
<td>MSG</td>
<td>Press the MESSAGE key (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>HEADSET</td>
<td>Press the HEADSET key (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>RD</td>
<td>Redial the last dialed number (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>Reboot</td>
<td>Reboot the phone.</td>
</tr>
<tr>
<td>AutoP</td>
<td>Perform auto provisioning.</td>
</tr>
<tr>
<td>DNDOn</td>
<td>Activate the DND feature.</td>
</tr>
<tr>
<td>DNDOff</td>
<td>Deactivate the DND feature.</td>
</tr>
<tr>
<td>Variable Value</td>
<td>Phone Action</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>number=xxx&amp;outgoing_uri=y</td>
<td>Place a call to xxx from SIP URI y.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><a href="http://10.3.20.10/servlet?key=number=1234&amp;outgoing_uri=1006@10.2.1.48">http://10.3.20.10/servlet?key=number=1234&amp;outgoing_uri=1006@10.2.1.48</a> (1234 means the number you dial out; 1006@10.2.1.48 means the SIP URL you dial from.)</td>
</tr>
<tr>
<td>OFFHOOK</td>
<td>Pick up the handset (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>ONHOOK</td>
<td>Hang up the handset (not applicable to CP960 IP phones).</td>
</tr>
<tr>
<td>ANSWER/ASW/Asw</td>
<td>Answer a call.</td>
</tr>
<tr>
<td>Reset</td>
<td>Reset a phone.</td>
</tr>
<tr>
<td>ATrans=xxx</td>
<td>Perform a semi-attended/attended transfer to xxx.</td>
</tr>
<tr>
<td>BTrans=xxx</td>
<td>Perform a blind transfer to xxx.</td>
</tr>
<tr>
<td>CALLEND/CallEnd</td>
<td>End a call.</td>
</tr>
<tr>
<td>CallWaitingOn</td>
<td>Activate the call waiting feature.</td>
</tr>
<tr>
<td>CallWaitingOff</td>
<td>Deactivate the call waiting feature.</td>
</tr>
<tr>
<td>AlwaysFwdOn/BusyFwdOn/NoAnswFwdOn=xxx=n</td>
<td>Activate an always/busy/no answer forward feature to xxx for the IP phone (“xxx” means the destination number).</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <a href="http://10.10.20.10/servlet?key=NoAnswFwdOn=1001=24">http://10.10.20.10/servlet?key=NoAnswFwdOn=1001=24</a></td>
</tr>
</tbody>
</table>
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Variable Value</th>
<th>Phone Action</th>
</tr>
</thead>
</table>
| 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)://<serverIPAdress>/help.xml?CallId=$call_id. For more information, refer to Action URL on page 568. |
| 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)://<phoneIPAdress>/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@<phoneIPAdress>/servlet?key=variable value or  
http(s)://<phoneIPAdress>/servlet?key=variable value&amp=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 594.

**Procedure**

Specify the trusted IP address for action URI using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the IP phone to receive the action URI requests.</td>
<td>Specify the trusted IP address(es) for sending the action URI to the IP phone.</td>
</tr>
<tr>
<td><strong>Parameter:</strong> features.action_uri.enable</td>
<td><strong>Parameter:</strong> features.action_uri.limit_ip</td>
</tr>
<tr>
<td>Configure the IP phone to pop up the Allow Remote Control prompt.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong> features.show_action_uri_option</td>
<td></td>
</tr>
<tr>
<td>Specify the trusted IP address(es) for sending the action URI to the IP phone.</td>
<td></td>
</tr>
<tr>
<td><strong>Parameter:</strong> features.action_uri.limit_ip</td>
<td></td>
</tr>
</tbody>
</table>
Navigate to:

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

Details of the Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.action_uri.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
</table>

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 592.

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 592.

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...
Configuring Advanced Features

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure the SIP server redundancy.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters:</strong></td>
<td></td>
<td>account.X.sip_server.Y.address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>account.X.sip_server.Y.port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>account.X.sip_server.Y.expires</td>
</tr>
<tr>
<td></td>
<td></td>
<td>account.X.sip_server.Y.retry_counts</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.sip_server.Y.address</td>
<td>String within 256 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>(Y ranges from 1 to 2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 Server Y
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>account.X.sip_server.Y.port</code></td>
<td>Integer from 0 to 65535</td>
<td>5060</td>
</tr>
<tr>
<td></td>
<td>(Y ranges from 1 to 2)</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>account.X.sip_server.Y.expires</code></td>
<td>Integer from 30 to 2147483647</td>
<td>3600</td>
</tr>
<tr>
<td></td>
<td>(Y ranges from 1 to 2)</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>account.X.sip_server.Y.retry_counts</code></td>
<td>Integer from 0 to 20</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>(Y ranges from 1 to 2)</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account-&gt;Register-&gt;SIP Server Y-&gt;Server Retry Counts</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### account.X.sip_server.Y.register_on_enable
(Y ranges from 1 to 2)

<table>
<thead>
<tr>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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
### Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>account.X.outbound_proxy.Y.address</code></td>
<td>IP address or domain name</td>
<td>Blank</td>
</tr>
<tr>
<td>(Y ranges from 1 to 2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 Proxy Y

<table>
<thead>
<tr>
<th><code>account.X.outbound_proxy.Y.port</code></th>
<th>Integer from 0 to 65535</th>
<th>5060</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Y ranges from 1 to 2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.fallback.timeout</td>
<td>Integer from 10 to 2147483647</td>
<td>120</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.outbound_proxy_fallback_interval</td>
<td>Integer from 0 to 65535</td>
<td>3600</td>
</tr>
</tbody>
</table>

**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
### Phone User Interface:

Settings > Advanced (default password: admin) > Accounts > AccountX > Proxy Fallback

### Interval

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.sip_server.Y.failback_mode</td>
<td>0, 1, 2 or 3</td>
<td>0</td>
</tr>
</tbody>
</table>

**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)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.sip_server.Y.failback_timeout</td>
<td>0, Integer from 60 to 65535</td>
<td>3600</td>
</tr>
</tbody>
</table>

**Description:**

Configures the time (in seconds) for the phone to retry to send requests to the primary server after failover 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)
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.

![SIP server configuration](image)

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**.

![Image of SIP-T5 Series Smart Media Phones configuration](image1.png)

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.

![Image of SIP-T5 Series Smart Media Phones configuration](image2.png)
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](https://tools.ietf.org/html/rfc3263). 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:

<table>
<thead>
<tr>
<th>order</th>
<th>pref</th>
<th>flags</th>
<th>service</th>
<th>regexp</th>
<th>replacement</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN NAPTR 90 50</td>
<td>&quot;s&quot;</td>
<td>&quot;SIP+D2T&quot;</td>
<td>&quot;&quot;</td>
<td>sip.tcp.yealink.pbx.com</td>
<td></td>
</tr>
<tr>
<td>IN NAPTR 100 50</td>
<td>&quot;s&quot;</td>
<td>&quot;SIP+D2U&quot;</td>
<td>&quot;&quot;</td>
<td>sip.udp.yealink.pbx.com</td>
<td></td>
</tr>
</tbody>
</table>

Parameters are explained in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>order</td>
<td>Specify preferential treatment for the specific record. The order is from lowest to highest, lower order is more preferred.</td>
</tr>
<tr>
<td>pref</td>
<td>Specify the preference for processing multiple NAPTR records with the same order value. Lower value is more preferred.</td>
</tr>
<tr>
<td>Flags</td>
<td>The flag &quot;s&quot; means to perform an SRV lookup.</td>
</tr>
</tbody>
</table>
| 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:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Weight</th>
<th>Port</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN SRV</td>
<td>0</td>
<td>1</td>
<td>5060 server1.yealink.pbx.com</td>
</tr>
<tr>
<td>IN SRV</td>
<td>0</td>
<td>2</td>
<td>5060 server2.yealink.pbx.com</td>
</tr>
</tbody>
</table>

Parameters are explained in the following table:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Specify preferential treatment for the specific host entry. Lower priority is more preferred.</td>
</tr>
<tr>
<td>Weight</td>
<td>When priorities are equal, weight is used to differentiate the preference. The preference is from highest to lowest. Keep the same to load balance.</td>
</tr>
<tr>
<td>Port</td>
<td>Identify the port number to be used.</td>
</tr>
<tr>
<td>Target</td>
<td>Identify the actual host for an A query.</td>
</tr>
</tbody>
</table>

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. |
Configuring Advanced Features

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=

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.sip_server.Y.transport_type</td>
<td>0, 1, 2 or 3</td>
<td>0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>0 or 1</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.naptr_build</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>
### 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

---

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the way of SRV query for the IP phone to be performed when no result is returned from NAPTR query for account X.</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>SRV query using UDP only</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>SRV query using UDP, TCP and TLS</td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
configurable on a per-line basis.

**Procedure**

Static DNS cache can be configured only using the configuration files.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter Configuration</th>
</tr>
</thead>
</table>
| `<y000000000xx>.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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns_cache_naptr.X.name</td>
<td>Domain name</td>
<td>Blank</td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>dns_cache_naptr.X.flags</td>
<td>S, A, U or P</td>
<td>Blank</td>
</tr>
<tr>
<td>dns_cache_naptr.X.order</td>
<td>Integer from 0 to 65535</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

**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).

**Example:**
dns_cache_naptr.1.flags = S

**Note:** For more details of the permitted flags, refer to [RFC 2915](https://www.rfc-editor.org/rfc/rfc2915).

**Web User Interface:**
None

**Phone User Interface:**
None

**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:**
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dns_cache_naptr.X.preference</td>
<td>Integer from 0 to 65535</td>
<td>0</td>
</tr>
<tr>
<td>(X ranges from 1 to 12)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>dns_cache_naptr.X.replace</th>
<th>Domain name with SRV prefix</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X ranges from 1 to 12)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>dns_cache_naptr.X.service</th>
<th>String within 32 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>(X ranges from 1 to 12)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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](https://tools.ietf.org/html/rfc2915).

**Web User Interface:**  
None

**Phone User Interface:**  
None

dns_cache_naptr.X.ttl  
(X ranges from 1 to 12)  
**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)  
**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)  
**Description:**  
Configures the port to be used in SRV record X.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns_cache_srv.X.priority</td>
<td>Integer from 0 to 65535</td>
<td>0</td>
</tr>
<tr>
<td>(X ranges from 1 to 12)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>Note: For more information, refer to RFC 2782.</td>
<td>Web User Interface:</td>
<td>None</td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>dns_cache_srv.X.target</td>
<td>Domain name</td>
<td>Blank</td>
</tr>
<tr>
<td>(X ranges from 1 to 12)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td>Configures the domain name of the target host for an A query in SRV record X.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>dns_cache_srv.1.target = server1.yealink.pbx.com</td>
<td></td>
</tr>
<tr>
<td>Note: For more information, refer to RFC 2782.</td>
<td>Web User Interface:</td>
<td>None</td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>dns_cache_srv.X.weight</td>
<td>Integer from 0 to 65535</td>
<td>0</td>
</tr>
<tr>
<td>(X ranges from 1 to 12)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>dns_cache_srv.1.port = 5060</td>
<td></td>
</tr>
<tr>
<td>Note: For more information, refer to RFC 2782.</td>
<td>Web User Interface:</td>
<td>None</td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------</td>
<td>---------</td>
</tr>
<tr>
<td>dns_cache_srv.X.weight</td>
<td>Integer from 30 to 2147483647</td>
<td>300</td>
</tr>
</tbody>
</table>

**Description:**
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 | 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

<table>
<thead>
<tr>
<th>dns_cache_a.X.name</th>
<th>Domain name</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>dns_cache_a.X.ip</th>
<th>IP address</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the IP address that the domain name in A record X maps to.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>dns_cache_a.1.ip = 192.168.1.13</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>dns_cache_a.X.ttl</td>
<td>(X ranges from 1 to 12)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integer from 30 to 2147483647</td>
<td>300</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the time interval (in seconds) that A record X may be cached before the record should be consulted again.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>dns_cache_a.1.ttl = 3600</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>account.X.dns_cache_type</td>
<td>0, 1 or 2</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>account.1.dns_cache_type = 1</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.static_cache_pri</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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


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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure RTP ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y00000000xx&gt;.cfg</td>
<td>Parameters:</td>
</tr>
<tr>
<td></td>
<td>static.network.port.max_rtpport</td>
</tr>
<tr>
<td></td>
<td>static.network.port.min_rtpport</td>
</tr>
</tbody>
</table>
Web User Interface

Configure RTP ports.

Navigate to:
http://<phoneIPAddress>/servlet?p=nework-adv&q=load

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.network.port.min_rtpport</code></td>
<td>Integer from 1 to 65535</td>
<td>11780</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.network.port.max_rtpport</code></td>
<td>Integer from 1 to 65535</td>
<td>12780</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>RPC Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GetRPCMethods</td>
<td>This method is used to discover the set of methods supported by the CPE.</td>
</tr>
<tr>
<td>SetParameterValues</td>
<td>This method is used to modify the value of one or more CPE parameters.</td>
</tr>
<tr>
<td>GetParameterValues</td>
<td>This method is used to obtain the value of one or more CPE parameters.</td>
</tr>
<tr>
<td>GetParameterNames</td>
<td>This method is used to discover the parameters accessible on a particular CPE.</td>
</tr>
<tr>
<td>GetParameterAttributes</td>
<td>This method is used to read the attributes associated with one or more CPE parameters.</td>
</tr>
<tr>
<td>SetParameterAttributes</td>
<td>This method is used to modify attributes associated with one or more CPE parameters.</td>
</tr>
<tr>
<td>Reboot</td>
<td>This method causes the CPE to reboot.</td>
</tr>
<tr>
<td>Download</td>
<td>This method is used to cause the CPE to download a specified file from the designated location.</td>
</tr>
<tr>
<td></td>
<td>File types supported by IP phones are:</td>
</tr>
<tr>
<td></td>
<td>• Firmware Image</td>
</tr>
<tr>
<td></td>
<td>• Configuration File</td>
</tr>
<tr>
<td>Upload</td>
<td>This method is used to cause the CPE to upload a specified file to the designated location.</td>
</tr>
<tr>
<td></td>
<td>File types supported by IP phones are:</td>
</tr>
<tr>
<td></td>
<td>• Configuration File</td>
</tr>
<tr>
<td></td>
<td>• Log File</td>
</tr>
<tr>
<td>ScheduleInform</td>
<td>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.</td>
</tr>
<tr>
<td>FactoryReset</td>
<td>This method resets the CPE to its factory default state.</td>
</tr>
<tr>
<td>TransferComplete</td>
<td>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.</td>
</tr>
<tr>
<td>AddObject</td>
<td>This method is used to add a new instance of an object defined on the CPE.</td>
</tr>
<tr>
<td>DeleteObject</td>
<td>This method is used to remove a particular instance of an object.</td>
</tr>
</tbody>
</table>
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) | Configure TR-069 feature. **Parameters:**
|                                           | static.managementserver.enable
|                                           | static.managementserver.username
|                                           | static.managementserver.password
|                                           | static.managementserver.url
|                                           | static.managementserver.connectio
|                                           | n_request_username
|                                           | static.managementserver.connectio
|                                           | n_request_password
|                                           | static.managementserver.periodic_in
|                                           | form_enable
|                                           | static.managementserver.periodic_in
|                                           | form_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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.managementserver.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**

Enables or disables the TR-069 feature.

- 0-Disabled
- 1-Enabled

**Web User Interface:**

Settings-&gt;TR069-&gt;Enable TR069

**Phone User Interface:**

None
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.managementserver.username</code></td>
<td>String within 128 characters</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the user name for the IP phone to authenticate with the ACS (Auto Configuration Servers). Leave it blank if no authentication is required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>static.managementserver.username = tr69</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Settings -> TR069 -> ACS Username

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th><code>static.managementserver.password</code></th>
<th>String within 64 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the password for the IP phone to authenticate with the ACS (Auto Configuration Servers). Leave it blank if no authentication is required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>static.managementserver.password = tr69</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Settings -> TR069 -> ACS Password

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th><code>static.managementserver.url</code></th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the access URL of the ACS (Auto Configuration Servers).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>static.managementserver.url = http://officetelprov.orangero.net:8080/ftacs-digest/ACS</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:**
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt;TR069-&gt;ACS URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>static.managementserver.connection_request_username</code></td>
<td>String within 128</td>
<td>Blank</td>
</tr>
<tr>
<td>characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the user name for the IP phone to authenticate the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>incoming connection requests of the ACS (Auto Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>static.managementserver.connection_request_username = accuser</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;TR069-&gt;Connection Request Username</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>static.managementserver.connection_request_password</code></td>
<td>String within 64</td>
<td>Blank</td>
</tr>
<tr>
<td>characters</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the password for the IP phone to authenticate the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>incoming connection requests of the ACS (Auto Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Servers).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>static.managementserver.connection_request_password = acspwd</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;TR069-&gt;Connection Request Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>static.managementserver.periodic_inform_enable</code></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to periodically report its</td>
<td></td>
<td></td>
</tr>
<tr>
<td>configuration information to the ACS (Auto Configuration Servers).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>0-Disabled</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>1-Enabled</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt;TR069-&gt;Enable Periodic Inform</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.managementserver.periodic_inform_interval</strong></td>
<td>Integer from 5 to 4294967295</td>
<td>60</td>
</tr>
</tbody>
</table>

**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.

**XML Browser**

XML browser simply means that the SIP phones' LCD screen display can be managed by external applications. The XML browser feature allows users to develop and deploy custom services which meet user functional requirements on the server. Users can customize practical applications, such as weather report, stock information, Google search, news service, etc.

To use the XML browser feature, you must configure an XML key in advance.

For more information on XML browser, refer to **Yealink IP Phones XML Browser Developer's Guide**.

**Note**

It is not applicable to CP960 IP phones.

**Procedure**

XML browser key can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Assign an XML browser key.</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y00000000xx&gt;.cfg</td>
<td>Assign an XML browser key.</td>
</tr>
</tbody>
</table>
Configuring Advanced Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/programablekey.X.type/expansion_module.X.key.Y.type</td>
<td>27</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**XML Browser Key**

For more information on how to configure the DSS Key, refer to Appendix D: Configuring DSS Key on page 805.

**Details of Configuration Parameters:**

**Description:**
Configures a DSS key as an XML Browser key on the IP phone.

The digit 27 stands for the key type XML Browser.

For line keys:
X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)

For programable keys:
X=12-14 (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 = 27

**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 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).
## Administrator's Guide for SIP-T5 Series Smart Media Phones

### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>When X=14, the default value is 2 (Forward). For ext keys: <strong>For SIP-T58V/T58A/T56A IP phones:</strong> When Y=1-60, the default value is 0 (NA). <strong>Web User Interface:</strong> Dsskey-&gt;Line Key/Programable Key-&gt;Type <strong>Phone User Interface:</strong> Menu-&gt;Features-&gt;DSS Keys-&gt;Line Key X-&gt;Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>linekey.X.value/programablekey.X.value/expansion_module.X.key.Y.value</strong></td>
<td><strong>String within 99 characters</strong></td>
<td><strong>Blank</strong></td>
</tr>
</tbody>
</table>

### Description:

Configures the available access URL to browse the XML object.

For line keys:

- X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)
- For programable keys:
  - X=12-14 (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 = http://10.2.1.158/TextMenu.xml
```

### Web User Interface:

**Dsskey->Line Key/Programable Key->Value**

**Phone User Interface:**

**Menu->Features->DSS Keys->Line Key X->Value**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>linekey.X.label/programablekey.X.label/expansion_module.X.key.Y.label</strong></td>
<td><strong>String within 99 characters</strong></td>
<td><strong>Blank</strong></td>
</tr>
</tbody>
</table>

### 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)
- For ext keys:
  - X ranges from 1 to 3, Y ranges from 1 to 60 (for SIP-T58V/T58A/T56A)

### Web User Interface:
### Parameters | Permitted Values | Default
---|---|---
Dsskey->Line Key/Programable Key->Label |  |  
**Phone User Interface:**
Menu->Features->DSS Keys->Line Key X->Label

**To configure an XML Browser key via web user interface:**

1. Click on **Dsskey**-> **Line Key** (or **Programable Key**).
2. In the desired DSS key field, select **XML Browser** from the pull-down list of **Type**.
3. Enter the available access URL in the **Value** field.
4. (Optional.) Enter the string that will appear on the LCD screen in the **Label** field.
5. Click **Confirm** to accept the change.

**To configure an XML Browser 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 **XML Browser** 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.
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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.redial_tone</td>
<td>Integer within 6 digits</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Format</th>
<th>Single File Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A/T56A</td>
<td>.wav</td>
<td>&lt;=8MB</td>
</tr>
<tr>
<td>CP960</td>
<td>.wav</td>
<td>&lt;=8MB</td>
</tr>
</tbody>
</table>

Note: The ring tone file must be PCM audio format, mono channel, 8K sample rate and 16 bit resolution.

Procedure

Ring tones can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Configure a ring tone for the IP phone. Parameter: phone_setting.ring_type</td>
<td>Specify the access URL of the custom ring tone. Parameter: ringtone.url</td>
</tr>
<tr>
<td>&lt;MAC&gt;.cfg</td>
<td>Delete all custom ring tone files. Parameter: ringtone.delete</td>
<td>Configure a ring tone on a per-line basis. Parameter: account.X.ringtone.ring_type</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th></th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configure a ring tone for the IP phone. Configure a ring tone for the account.</td>
<td></td>
</tr>
</tbody>
</table>
Details of the Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.ring_type</td>
<td>Refer to the following content</td>
<td>Ring1.wav</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.ringtone.ring_type</th>
<th>Refer to the following content</th>
<th>Common</th>
</tr>
</thead>
</table>

**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:**
### Configuring Audio Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt;Basic-&gt;Sound-&gt;Ring Tones-&gt;Account X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>ringtone.url</code></td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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 Alert-Info header contains the keyword "Bellcore-drN", the IP phone will play the desired ring tone.

The following table identifies the corresponding ring tone:

<table>
<thead>
<tr>
<th>Value of N</th>
<th><strong>Ring Tone</strong> (features.alert_info_tone = 1)</th>
<th><strong>Ring Tone</strong> (features.alert_info_tone = 0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bellcore-dr1</td>
<td>Ring1.wav</td>
</tr>
<tr>
<td>2</td>
<td>Bellcore-dr2</td>
<td>Ring2.wav</td>
</tr>
<tr>
<td>3</td>
<td>Bellcore-dr3</td>
<td>Ring3.wav</td>
</tr>
<tr>
<td>4</td>
<td>Bellcore-dr4</td>
<td>Ring4.wav</td>
</tr>
<tr>
<td>5</td>
<td>Bellcore-dr5</td>
<td>Ring5.wav</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Ring6.wav</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Ring7.wav</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>Ring8.wav</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>Silent.wav</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>Splash.wav</td>
</tr>
<tr>
<td>N&lt;1 or N&gt;10</td>
<td></td>
<td>Ring1.wav</td>
</tr>
</tbody>
</table>

**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).

<table>
<thead>
<tr>
<th>Bellcore Tone</th>
<th>Pattern ID</th>
<th>Pattern</th>
<th>Cadence</th>
<th>Minimum Duration (ms)</th>
<th>Nominal Duration (ms)</th>
<th>Maximum Duration (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bellcore-dr1 (standard)</td>
<td>1</td>
<td>Ringing</td>
<td>Silent</td>
<td>1800</td>
<td>2000</td>
<td>2200</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Ringing</td>
<td>Long</td>
<td>630</td>
<td>800</td>
<td>1025</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Ringing</td>
<td>Long</td>
<td>315</td>
<td>400</td>
<td>525</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Ringing</td>
<td>Short</td>
<td>315</td>
<td>400</td>
<td>525</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Ringing</td>
<td>Short</td>
<td>145</td>
<td>200</td>
<td>525</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>Ringing</td>
<td>Silent</td>
<td>200</td>
<td>300</td>
<td>525</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Ringing</td>
<td>Silent</td>
<td>145</td>
<td>200</td>
<td>525</td>
</tr>
</tbody>
</table>

**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 "MyMelodyN", 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
The following table identifies the corresponding local ring tone:

<table>
<thead>
<tr>
<th>Value of N</th>
<th>Ring Tone</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ring1.wav</td>
</tr>
<tr>
<td>2</td>
<td>Ring2.wav</td>
</tr>
<tr>
<td>3</td>
<td>Ring3.wav</td>
</tr>
<tr>
<td>4</td>
<td>Ring4.wav</td>
</tr>
<tr>
<td>5</td>
<td>Ring5.wav</td>
</tr>
<tr>
<td>6</td>
<td>Ring6.wav</td>
</tr>
<tr>
<td>7</td>
<td>Ring7.wav</td>
</tr>
<tr>
<td>8</td>
<td>Ring8.wav</td>
</tr>
<tr>
<td>9</td>
<td>Silent.wav</td>
</tr>
<tr>
<td>10</td>
<td>Splash.wav</td>
</tr>
<tr>
<td>N&lt;1 or N&gt;10</td>
<td>Ring1.wav</td>
</tr>
</tbody>
</table>

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
Configuring Audio Features

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 294.

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;MAC&gt;.cfg</td>
<td>Configure distinctive ring tones.</td>
</tr>
<tr>
<td>Parameter: account.X.alert_info_url_enable</td>
<td></td>
</tr>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td>Configure the internal ringer text and internal ringer file.</td>
</tr>
<tr>
<td>Parameters: features.alert_info_tone</td>
<td></td>
</tr>
<tr>
<td>distinctive_ring_tones.alert_info.X.text</td>
<td></td>
</tr>
<tr>
<td>distinctive_ring_tones.alert_info.X.ringer</td>
<td></td>
</tr>
<tr>
<td>Navigate to:</td>
<td></td>
</tr>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mmod_data&amp;p=account-adv&amp;q=load&amp;acc=0</td>
<td></td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.alert_info_url_enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

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.
### Configuring Audio Features

#### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>distinctive_ring_tones.alert_info.1.text = Family</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**

Settings->Ring->Internal Ringer Text

**Phone User Interface:**

None

<table>
<thead>
<tr>
<th>distinctive_ring_tones.alert_info.X.ringer (X ranges from 1 to 10)</th>
<th>Integer from 1 to 10</th>
<th>1</th>
</tr>
</thead>
</table>

**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.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dial</td>
<td>When on the pre-dialing screen (not applicable to CP960 IP phones)</td>
</tr>
</tbody>
</table>
### 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](http://<phoneIPAddress>/servlet?m) |
# Configuring Audio Features

## Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.tone.country</td>
<td>Refer to the following content</td>
<td>Custom</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>String</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.tone.dial</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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:**
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### voice.tone.secondary_dial

- **Type:** String
- **Default:** 350+440/300

**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.

### voice.tone.ring

- **Type:** String
- **Default:** 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.

### voice.tone.busy

- **Type:** String
- **Default:** 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.
### Configuring Audio Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>voice.tone.congestion</strong></td>
<td>String</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter “voice.tone.country” is set to Custom.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Tones-&gt;Congestion</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>voice.tone.callwaiting</strong></td>
<td>String</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter “voice.tone.country” is set to Custom.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Tones-&gt;Call Waiting</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>voice.tone.dialrecall</strong></td>
<td>String</td>
<td>Blank</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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”.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter “voice.tone.country” is set to Custom.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Tones-&gt;Dial Recall</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------</td>
<td>----------</td>
</tr>
<tr>
<td>voice.tone.info</td>
<td>String</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.tone.stutter</td>
<td>String</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.tone.autoanswer</td>
<td>String</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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 646.

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.voice_mail_tone_enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure the ringer device for the IP phone.</th>
<th>Parameter: features.ringer_device.is_use_headset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td>Configure the ringer device for the IP phone.</td>
<td>Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-audio&amp;q=load</td>
</tr>
</tbody>
</table>

#### Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.ringer_device.is_use_headset</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter</th>
<th>Web User Interface</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure headset prior.</td>
<td>features.headset_prior</td>
<td>Configure headset prior.</td>
<td>features.headset_prior</td>
</tr>
<tr>
<td><strong>Navigate to:</strong></td>
<td></td>
<td><strong>Navigate to:</strong></td>
<td></td>
</tr>
<tr>
<td>http://&lt;phoneIP Address&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.headset_prior</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>
**Configuring Audio Features**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables headset prior feature. You need to press the HEADSET key to activate the headset mode in advance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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) | Configure dual headset. Parameter: features.headset_training <y0000000000xx>.cfg |
| Web User Interface | Configure dual headset. Navigate to: http://<phoneIPAddress>/servlet?m=mod_data&p=features-general&q=load |

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.headset_training</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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
Configuring Audio Features

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td>None</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Central Provisioning</th>
<th>Parameter:</th>
<th>Configure the sending volume of the speaker.</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(Configuration File)</em></td>
<td>voice.handfree_send</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Central Provisioning</th>
<th>Parameter:</th>
<th>Configure the sending volume of the handset.</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>(Configuration File)</em></td>
<td>voice.handset_send</td>
<td></td>
</tr>
</tbody>
</table>
## 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.handfree_send</td>
<td>Integer from -50 to 50</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.handset_send</td>
<td>Integer from -50 to 50</td>
<td>0</td>
</tr>
</tbody>
</table>

**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
Configuring Audio Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.headset_send</td>
<td>Integer from -50 to 50</td>
<td>0</td>
</tr>
</tbody>
</table>

**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 summarizes the supported audio codecs on IP phones:

<table>
<thead>
<tr>
<th>Codec</th>
<th>Algorithm</th>
<th>Reference</th>
<th>Bit Rate</th>
<th>Sample Rate</th>
<th>Packetization Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.722.1c</td>
<td>G.722.1</td>
<td>RFC 5577</td>
<td>48 Kbps</td>
<td>32 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G.722.1c</td>
<td>G.722.1</td>
<td>RFC 5577</td>
<td>32 Kbps</td>
<td>32 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G.722.1c</td>
<td>G.722.1</td>
<td>RFC 5577</td>
<td>24 Kbps</td>
<td>32 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G.722.1</td>
<td>G.722.1</td>
<td>RFC 5577</td>
<td>24 Kbps</td>
<td>16 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G722</td>
<td>G.722</td>
<td>RFC 3551</td>
<td>64 Kbps</td>
<td>16 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>PCMA</td>
<td>G.711</td>
<td>RFC 3551</td>
<td>64 Kbps</td>
<td>8 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>PCMU</td>
<td>G.711</td>
<td>RFC 3551</td>
<td>64 Kbps</td>
<td>8 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G729</td>
<td>G.729</td>
<td>RFC 3551</td>
<td>8 Kbps</td>
<td>8 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G726-16</td>
<td>G.726</td>
<td>RFC 3551</td>
<td>16 Kbps</td>
<td>8 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G726-24</td>
<td>G.726</td>
<td>RFC 3551</td>
<td>24 Kbps</td>
<td>8 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G726-32</td>
<td>G.726</td>
<td>RFC 3551</td>
<td>32 Kbps</td>
<td>8 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G726-40</td>
<td>G.726</td>
<td>RFC 3551</td>
<td>40 Kbps</td>
<td>8 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td>G723_53/</td>
<td>G.723.1</td>
<td>RFC 3551</td>
<td>5.3 Kbps</td>
<td>8 Kbps</td>
<td>30ms</td>
</tr>
<tr>
<td>G723_63</td>
<td></td>
<td></td>
<td>6.3 Kbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iLBC</td>
<td>iLBC</td>
<td>RFC 3952</td>
<td>15.2 Kbps</td>
<td>8 Kbps</td>
<td>20ms 30ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13.33 Kbps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opus</td>
<td>Opus</td>
<td>RFC 6716</td>
<td>8-12 Kbps</td>
<td>8 Kbps</td>
<td>20ms</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>16-20 Kbps</td>
<td>12 Kbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>28-40 Kbps</td>
<td>16 Kbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>48-64 Kbps</td>
<td>24 Kbps</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>64-128 Kbps</td>
<td>48 Kbps</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Audio Bandwidth</th>
<th>Sample Rate (Effective)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NB (narrowband)</td>
<td>4 kHz</td>
<td>8 kHz</td>
</tr>
<tr>
<td>MB (medium-band)</td>
<td>6 kHz</td>
<td>12 kHz</td>
</tr>
<tr>
<td>WB (wideband)</td>
<td>8 kHz</td>
<td>16 kHz</td>
</tr>
<tr>
<td>SWB (super-wideband)</td>
<td>12 kHz</td>
<td>24 kHz</td>
</tr>
<tr>
<td>FB (fullband)</td>
<td>20 kHz</td>
<td>48 kHz</td>
</tr>
</tbody>
</table>

The following table lists the audio codecs supported by SIP-T58V/T58A/T56A/CP960 IP phones:

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Supported Audio Codecs</th>
<th>Default Audio Codecs</th>
</tr>
</thead>
</table>

**Audio Codec Configuration**

**Procedure**

Configuration changes can be performed using the following methods.

| Central Provisioning (Configuration File) | Configure the codecs to use on a per-line basis.  
**Parameter:**  
account.X.codec.<payload_type>.enable | Configure the priority for the enabled codec.  
**Parameter:**  
account.X.codec.<payload_type>.priority |
|---|---|
| Web User Interface | Configure the codecs to use on a per-line basis.  
Configure the priority for the enabled codec.  
**Navigate to:**  
http://<phoneIP Address>/servlet?p=account-codec&q=load&acc=0 |
### Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.codec.&lt;payload_type&gt;.enable (where &lt;payload_type&gt; should be replaced by the name of audio codec)</td>
<td>0 or 1</td>
<td>Refer to the following content</td>
</tr>
</tbody>
</table>

**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:**

<table>
<thead>
<tr>
<th>Codec</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>g722_1c_48kpbs</td>
<td>G722.1c(48kb/s)</td>
</tr>
<tr>
<td>g722_1c_24kpbs</td>
<td>G722.1c(24kb/s)</td>
</tr>
<tr>
<td>g722</td>
<td>G722</td>
</tr>
<tr>
<td>pcmu</td>
<td>PCMU</td>
</tr>
<tr>
<td>pcma</td>
<td>PCM</td>
</tr>
<tr>
<td>g726_16</td>
<td>G726-16</td>
</tr>
<tr>
<td>ilbc</td>
<td>iLBC</td>
</tr>
<tr>
<td>g726_1c_32kpbs</td>
<td>G722.1c(32kb/s)</td>
</tr>
<tr>
<td>g726_1_24kpbs</td>
<td>G722.1(24kb/s)</td>
</tr>
<tr>
<td>g726</td>
<td>G726</td>
</tr>
<tr>
<td>g729</td>
<td>G729</td>
</tr>
<tr>
<td>g726_24</td>
<td>G726-24</td>
</tr>
<tr>
<td>g726_32</td>
<td>G726-32</td>
</tr>
<tr>
<td>g726_40</td>
<td>G726-40</td>
</tr>
<tr>
<td>g723_63</td>
<td>G723-63</td>
</tr>
<tr>
<td>g723_53</td>
<td>G723-53</td>
</tr>
</tbody>
</table>

**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;
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:**
Configuring Audio Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.1.codec.g722_1c_48kpbs.enable = 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 the name of audio codec)

<table>
<thead>
<tr>
<th>Integer from 0 to 16</th>
<th>Refer to the following content</th>
</tr>
</thead>
</table>

**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_48kpbs` - G722.1c(48kb/s)
- `g722_1c_32kpbs` - G722.1c(32kb/s)
- `g722_1c_24kpbs` - G722.1c(24kb/s)
- `g722_1c_24kpbs` - G722.1(24kb/s)
- `g722` - G722
- `pcm` - PCM
- `pcm` - PCM
- `opus` - Opus
- `g726_40` - G726-40
- `g726_24` - G726-24
- `g726_16` - G726-16
- `ilbc` - iLBC
- `g723_63` - G723-63
- `g723_53` - 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 PCM, 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

**Note:** Numerical value 0 is defined as the highest priority in the enable codec list and disable codec list. 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

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:

<table>
<thead>
<tr>
<th>Codec</th>
<th>Packetization Time (Minimum)</th>
<th>Packetization Time (Maximum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.722.1c(48kb/s)</td>
<td>20ms</td>
<td>60ms</td>
</tr>
<tr>
<td>G.722.1c(32kb/s)</td>
<td>20ms</td>
<td>60ms</td>
</tr>
<tr>
<td>G.722.1c(24kb/s)</td>
<td>20ms</td>
<td>60ms</td>
</tr>
<tr>
<td>G.722.1(24kb/s)</td>
<td>20ms</td>
<td>60ms</td>
</tr>
<tr>
<td>G.722</td>
<td>10ms</td>
<td>40ms</td>
</tr>
<tr>
<td>PCMA</td>
<td>10ms</td>
<td>40ms</td>
</tr>
<tr>
<td>PCMU</td>
<td>10ms</td>
<td>40ms</td>
</tr>
<tr>
<td>G729</td>
<td>10ms</td>
<td>80ms</td>
</tr>
<tr>
<td>G726-16</td>
<td>10ms</td>
<td>30ms</td>
</tr>
<tr>
<td>G726-24</td>
<td>10ms</td>
<td>30ms</td>
</tr>
<tr>
<td>G726-32</td>
<td>10ms</td>
<td>30ms</td>
</tr>
<tr>
<td>G726-40</td>
<td>10ms</td>
<td>30ms</td>
</tr>
<tr>
<td>G723_53/G723_63</td>
<td>30ms</td>
<td>60ms</td>
</tr>
<tr>
<td>iLBC</td>
<td>20ms</td>
<td>30ms</td>
</tr>
<tr>
<td>Opus</td>
<td>10ms</td>
<td>20ms</td>
</tr>
</tbody>
</table>

Procedure

PTime can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure the ptime. Parameter: account.X.ptime</th>
</tr>
</thead>
</table>
| **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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.ptime</td>
<td>0, 10, 20, 30, 40, 50 or 60</td>
<td>20</td>
</tr>
</tbody>
</table>

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) | 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= |
Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.codec.opus.para</td>
<td>Opus-FB, Opus-SWB, Opus-WB, Opus-MB, Opus-NB</td>
<td>Opus-FB</td>
</tr>
</tbody>
</table>

**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**.

![Image of Yealink phone settings](image)

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 situations 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Parameter: voice.echo_cancellation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure AEC.</td>
<td></td>
</tr>
<tr>
<td>Parameter:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure AEC.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Navigate to:</strong></td>
<td></td>
</tr>
<tr>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=settings-voice&amp;q=load</td>
<td></td>
</tr>
</tbody>
</table>
### Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.echo_cancellation</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure VAD.</th>
<th>Parameter: voice.vad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td>Configure VAD.</td>
<td>Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=settings-voice&amp;q=load</td>
</tr>
</tbody>
</table>

Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.vad</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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) | 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.cng</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.jib.adaptive</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.jib.min</td>
<td>Integer from 0 to 400</td>
<td>60</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.jib.max</td>
<td>Integer from 0 to 400</td>
<td>240</td>
</tr>
</tbody>
</table>
### Configuring Audio Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max Delay</strong></td>
<td>Integer from 0 to 400</td>
<td>120</td>
</tr>
</tbody>
</table>

**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 | None | None

**Phone User Interface:**

None

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>voice.jib.wifi.max</code></td>
<td>Integer from 0 to 500</td>
<td>500</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>voice.jib.wifi.normal</code></td>
<td>Integer from 0 to 500</td>
<td>240</td>
</tr>
</tbody>
</table>

**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** \( \rightarrow \) **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.

<table>
<thead>
<tr>
<th>Central Provisioning</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure Noise Suppression. Parameter: voice.tns.enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Configuration File)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure the Noise Suppression. Navigate to: http://&lt;phonenumber&gt;/servlet?m=mod_data&amp;p=settings-voice&amp;q=load</th>
</tr>
</thead>
</table>

**Details of Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.tns.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>
### Noise Suppression

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Enables or disables the Noise Suppression feature on the IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Disabled</td>
<td>1-Enabled</td>
<td></td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y000000000xx&gt;.cfg</th>
<th>Configure Smart Noise Block.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter:</strong></td>
<td>voice.ans_nb.enable</td>
<td>voice.ans_nb.enable</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure Smart Noise Block.</th>
<th>Configure Smart Noise Block.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring Audio Features

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

Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.ans_nb.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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).

**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:**

<table>
<thead>
<tr>
<th></th>
<th>1209 Hz</th>
<th>1336 Hz</th>
<th>1477 Hz</th>
<th>1633 Hz</th>
</tr>
</thead>
<tbody>
<tr>
<td>697 Hz</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>A</td>
</tr>
<tr>
<td>770 Hz</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>B</td>
</tr>
<tr>
<td>852 Hz</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>C</td>
</tr>
<tr>
<td>941 Hz</td>
<td>*</td>
<td>0</td>
<td>#</td>
<td>D</td>
</tr>
</tbody>
</table>

**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.

![Configuration changes can be performed using the following methods.](image)

**Central Provisioning (Configuration File)**

- **<MAC>.cfg**
  - 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

- **<y0000000000xx>.cfg**
  - Configure the number of times for the IP phone to send the end RTP Event packet.
  - **Parameter:**
    - features.dtmf.repetition
  - Configure the duration time for DTMF.
  - **Parameter:**
    - features.dtmf.duration
  - Configure the frequency level of DTMF digits.
  - **Parameter:**
    - features.dtmf.volume

**Web User Interface**

- 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
- 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

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.dtmf.type</td>
<td>0, 1, 2 or 3</td>
<td>1</td>
</tr>
</tbody>
</table>
### Description:
Configures the DTMF type for account X.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.dtmf.type</td>
<td>Integer from 0 to 3</td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.dtmf.dtmf_payload</th>
<th>Integer from 96 to 127</th>
<th>101</th>
</tr>
</thead>
</table>

### 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 the 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

<table>
<thead>
<tr>
<th>account.X.dtmf.info_type</th>
<th>1, 2 or 3</th>
<th>1</th>
</tr>
</thead>
</table>

### Description:
Configures the DTMF info type.

**1**: DTMF-Relay
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-DTMF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-Telephone-Event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td>X is equal to 1 (for CP960)</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter “account.X.dtmf.type” is set to 2 (SIP INFO) or 3 (RFC2833 + SIP INFO).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account -&gt; Advanced -&gt; DTMF Info Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**features.dtmf.repetition**

<table>
<thead>
<tr>
<th>Description:</th>
<th>Configures the repetition times for the IP phone to send the end RTP Event packet during an active call.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Features -&gt; General Information -&gt; DTMF Repetition</td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
</tr>
</tbody>
</table>

**features.dtmf.duration**

<table>
<thead>
<tr>
<th>Description:</th>
<th>Configures the duration time (in milliseconds) for DTMF.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> 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.</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
</tr>
</tbody>
</table>

**features.dtmf.volume**

| Description: | Configures the frequency level of DTMF digits (in db). |

|                  | Integer from -33 to 0 | -10   |
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

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>.cf | 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>features.dtmf.hide</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>features.dtmf.hide_delay</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure transfer via DTMF.</th>
<th>Parameters:</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y0000000000xx&gt;.cfg</td>
<td><code>features.dtmf.replace_tran</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>features.dtmf.transfer</code></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure transfer via DTMF.</th>
<th>Navigate to:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=features-general&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>features.dtmf.replace_tran</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables the IP phone to send DTMF sequences for transfer function when tapping the **Transfer** soft key or pressing TRANSFER/TRAN key.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.dtmf.transfer</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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->DTMF Replace Tran

**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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.play_local_dtmf_tone_enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

Description:
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables or disables the IP phone to play a local DTMF tone.</td>
<td>0 - Disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1 - Enabled</td>
<td></td>
</tr>
<tr>
<td>If it is set to 1 (Enabled), you can hear the DTMF tone when pressing the IP phone's keypad during a call.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice.rtcp_xr.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration)</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y00000000000xx&gt;.cfg</td>
<td>phone_setting.vq_rtcpxr.session_report.enable</td>
<td>Configure the generation of session packets.</td>
</tr>
</tbody>
</table>
| **File** | **Configure the generation of interval packets.**  
**Parameters:**  
phone_setting.vq_rtcpxr.interval_report.enable  
phone_setting.vq_rtcpxr_interval_period |
| --- | --- |
| **File** | **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 |
| **File** | **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 |
| **File** | **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 |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| phone_setting.vq_rtcpxr_display_start_time.enable | Configure the central report collector. **Parameters:**
| account.X.vq_rtcpxr.collector_name | 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. **Parameters:**
| 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 | |
| account.X.vq_rtcpxr.collector_server_host | |
| account.X.vq_rtcpxr.collector_server_port | |

**Web User Interface**

Configure the central report collector. **Parameters:**

- **<MAC>.cfg**

- **account.X.vq_rtcpxr.collector_name**
- **account.X.vq_rtcpxr.collector_server_host**
- **account.X.vq_rtcpxr.collector_server_port**
Configuring Audio Features

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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.vq_rtcpxr.session_report.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.vq_rtcpxr.interval_report.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.vq_rtcpxr_interval_period</td>
<td>Integer from 5 to 20</td>
</tr>
</tbody>
</table>

**Description:**
### phone_setting.vq_rtcpxr_interval_report.interval_report.enable

**Permitted Values:** Blank to 40

**Default:** Blank

**Parameter Description:**
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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.vq_rtcpxr_moslq_threshold_warning</td>
<td>15 to 40</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.vq_rtcpxr_moslq_threshold_critical</td>
<td>15 to 40</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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:**
### Configuring Audio Features

**Parameter**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt;Voice Monitoring-&gt;Critical threshold for Moslq</td>
<td>10 to 2000</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**Phone User Interface:**

None

**phone_setting.vq_rtcpxr_delay_threshold_warning**

**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**

**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**

**Description:**

Configures whether to show states on the web.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>phone_setting.vq_rtcpxr.states_show_on_gui.enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the voice quality data of the last call to be displayed on web interface at the path <strong>Status -&gt; RTP Status</strong>.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>0</strong>-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>1</strong>-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Voice Monitoring-&gt;Display Report options on Web</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.vq_rtcpxr_display_start_time.enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the phone to display Start Time on the touch screen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>0</strong>-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>1</strong>-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter &quot;phone_setting.vq_rtcpxr.states_show_on_gui.enable&quot; is set to 1 (Enabled).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Voice Monitoring-&gt;Report options on phone-&gt;Start Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Audio Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.vq_rtcpxr_display_stop_time.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.vq_rtcpxr_display_local_call_id.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.vq_rtcpxr_display_remote_call_id.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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:**
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>phone_setting.vq_rtcpxr_display_local_codec.enable</code></td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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
### Configuring Audio Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>phone_setting.vq_rtcpxr_display_jitter_buffer_max.enable</code></td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables the phone to display JitterBufferMax 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->JitterBufferMax

| **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).
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Voice Monitoring-&gt;Report options on phone-&gt;SymmOneWayDelay</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.vq_rtcpxr_display_round_trip_delay.enable</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the phone to display RoundTripDelay on the touch screen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;phone_setting.vq_rtcpxr.states_show_on_gui.enable&quot; is set to 1 (Enabled).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Voice Monitoring-&gt;Report options on phone-&gt;RoundTripDelay</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.vq_rtcpxr_display_moslq.enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the phone to display MOS-LQ on the touch screen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;phone_setting.vq_rtcpxr.states_show_on_gui.enable&quot; is set to 1 (Enabled).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Voice Monitoring-&gt;Report options on phone-&gt;MOS-LQ</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>phone_setting.vq_rtcpxr_display_moscq.enable</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the phone to display MOS-CQ on the touch screen.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> It works only if the value of the parameter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;phone_setting.vq_rtcpxr.states_show_on_gui.enable&quot; is set to 1 (Enabled).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Voice Monitoring-&gt;Report options on phone-&gt;MOS-LQ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameters</td>
<td>Permitted Values</td>
<td>Default</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>&quot;phone_setting.vq_rtcpxr.states_show_on_gui.enable&quot; is set to 1 (Enabled).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Voice Monitoring-&gt;Report options on phone-&gt;MOS-CQ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.vq_rtcpxr.collector_name</td>
<td>String within 32 characters</td>
<td>Blank</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the host name of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account-&gt;Advanced-&gt;VQ RTCP-XR Collector name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.vq_rtcpxr.collector_server_host</td>
<td>IPv4 Address</td>
<td>Blank</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account-&gt;Advanced-&gt;VQ RTCP-XR Collector address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phone User Interface:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>account.X.vq_rtcpxr.collector_server_port</td>
<td>Integer from 1 to 65535</td>
<td>5060</td>
</tr>
<tr>
<td>Description:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages for account X.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Administrator’s Guide for SIP-T5 Series Smart Media Phones

#### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>X ranges from 1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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**.

![Image of phone interface](image1)

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.

![Image of web interface](image2)
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.

Procedure

Video settings can be configured using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>00000000000xx.cfg</th>
<th>Configure the video settings. Parameters: video.enable camera.flicker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web User Interface</td>
<td></td>
<td>Configure the video settings. Navigate to: http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=settings-video&amp;q=load</td>
</tr>
</tbody>
</table>

Details of the Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>video.enable</td>
<td>0, 1 or 2</td>
<td>1</td>
</tr>
</tbody>
</table>

Description:

Configures the video call feature for the IP phone.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disabled</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>Video first</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Optional</td>
<td>2</td>
</tr>
</tbody>
</table>

If it is set to 0 (Disabled), the users are only allowed to establish an audio-only call. If it is set to 1 (Video first), the users can establish a video call with the other party that is video-enabled. If it is set to 2 (Optional), the users can choose to establish an audio-only or video call by tapping the Audio Call/Video Call key (on dialing/pre-dialing screen) or Audio/Video soft key (on incoming call screen).

**Note:** It is not applicable to SIP-T56A/CP960 IP phones.

**Web User Interface:**
Settings -> Video -> Video Active

**Phone User Interface:**
None

camera.flicker  

<table>
<thead>
<tr>
<th>Description:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures camera flicker frequency (Hz).</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>50Hz</td>
</tr>
<tr>
<td>60</td>
<td>60Hz</td>
</tr>
</tbody>
</table>

**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. It is not applicable to SIP-T56A/CP960 IP phones.

**Web User Interface:**
None

**Phone User Interface:**
None

To configure the video setting 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>MIME Type</th>
<th>Bit Rate</th>
<th>Frame Rate</th>
<th>Frame Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.264 BP</td>
<td>H264/90000</td>
<td>90 kbps to 2048 kbps</td>
<td>5 fps to 30 fps</td>
<td>Tx: CIF, 360P, W448P, 720P</td>
</tr>
<tr>
<td>H.264 HP</td>
<td>H264/90000</td>
<td>2048 kbps</td>
<td></td>
<td>Rx: Conventional Size Below 720P</td>
</tr>
<tr>
<td>VP8</td>
<td>VP8/90000</td>
<td>128kbps to 2048 kbps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Procedure

Configuration changes can be performed using the following methods.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;MAC&gt;.cfg</th>
<th>Configure the video codecs to use on a per-line basis.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td><strong>Parameter:</strong> account.X.video.&lt;payload_type&gt;.enable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure the priority and rtpmap for the enabled video codec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Parameter:</strong> account.X.video.&lt;payload_type&gt;.priority</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th></th>
<th>Configure the video codecs to use on a per-line basis.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Configure the priority for the enabled video codec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Navigate to:</strong> http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=account-codec&amp;q=load&amp;acc=0</td>
</tr>
</tbody>
</table>

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.video.&lt;payload_type&gt;.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td>(where &lt;payload_type&gt; should be replaced by the name of video codec)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Description:**
Enables or disables the specified video codec for account X.

0 - Disabled
1 - Enabled

X ranges from 1 to 16

**The name of audio codec:**
h264 - H264, h264hp - H264HP, vp8 - 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:**
### Configuring Video Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.1.video.h264.enable = 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>account.X.video.&lt;payload_type&gt;.priority</th>
<th>1, 2 or 3</th>
<th>Refer to the following content</th>
</tr>
</thead>
</table>

**Description:**
Configures the priority of the enabled video codec for account X.

**X ranges from 1 to 16**

**The name of audio codec:**

- h264-H264
- h264hp-H264HP
- vp8-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

**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 [x].

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Change the user or administrator password of the IP phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter:</strong></td>
<td></td>
<td>static.security.user_password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Change the user or administrator password of the IP phone.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Navigate to:</strong></td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=security&amp;q=load</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone User Interface</th>
<th>Change the administrator password of the IP phone.</th>
</tr>
</thead>
</table>
Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.security.user_password</td>
<td>String within 32 characters</td>
<td>user</td>
</tr>
</tbody>
</table>

**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.
Configuring Security Features

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 **Old 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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Configure auto-logout time. Parameter: features.relog_offtime</th>
</tr>
</thead>
</table>

### Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>features.relog_offtime</td>
<td>Integer from 1 to 1000</td>
<td>5</td>
</tr>
</tbody>
</table>

**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:**
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 following method.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
<th>Phone User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the phone lock feature.</td>
<td>Configure the phone lock feature.</td>
<td>Configure the phone lock feature.</td>
</tr>
<tr>
<td><strong>Parameters:</strong></td>
<td><strong>Parameters:</strong></td>
<td><strong>Parameters:</strong></td>
</tr>
<tr>
<td>phone_setting.phone_lock.enable</td>
<td>phone_setting.phone_lock.enable</td>
<td>phone_setting.phone_lock.enable</td>
</tr>
<tr>
<td>Change the unlock PIN.</td>
<td>Change the unlock PIN.</td>
<td>Change the unlock PIN.</td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td><strong>Parameter:</strong></td>
<td><strong>Parameter:</strong></td>
</tr>
<tr>
<td>phone_setting.phone_lock.unlock_pin</td>
<td>phone_setting.phone_lock.unlock_pin</td>
<td>phone_setting.phone_lock.unlock_pin</td>
</tr>
<tr>
<td>Configure the IP phone to automatically lock the phone after a time interval.</td>
<td>Configure the IP phone to automatically lock the phone after a time interval.</td>
<td>Configure the IP phone to automatically lock the phone after a time interval.</td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td><strong>Parameter:</strong></td>
<td><strong>Parameter:</strong></td>
</tr>
<tr>
<td>phone_setting.phone_lock.lock_time_out</td>
<td>phone_setting.phone_lock.lock_time_out</td>
<td>phone_setting.phone_lock.lock_time_out</td>
</tr>
<tr>
<td>Configure emergency numbers.</td>
<td>Configure emergency numbers.</td>
<td>Configure emergency numbers.</td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
<td><strong>Parameter:</strong></td>
<td><strong>Parameter:</strong></td>
</tr>
<tr>
<td>phone_setting.emergency.number</td>
<td>phone_setting.emergency.number</td>
<td>phone_setting.emergency.number</td>
</tr>
<tr>
<td>Assign a phone lock key.</td>
<td>Assign a phone lock key.</td>
<td>Assign a phone lock key.</td>
</tr>
<tr>
<td><strong>Parameters:</strong></td>
<td><strong>Parameters:</strong></td>
<td><strong>Parameters:</strong></td>
</tr>
<tr>
<td>linekey.X.type/programablekey.X.type/</td>
<td>linekey.X.type/programablekey.X.type/</td>
<td>linekey.X.type/programablekey.X.type/</td>
</tr>
<tr>
<td>expansion_module.X.key.Y.type</td>
<td>expansion_module.X.key.Y.type</td>
<td>expansion_module.X.key.Y.type</td>
</tr>
<tr>
<td>linekey.X.label/expansion_module.X.key.Y.label</td>
<td>linekey.X.label/expansion_module.X.key.Y.label</td>
<td>linekey.X.label/expansion_module.X.key.Y.label</td>
</tr>
<tr>
<td>Navigate to:</td>
<td>Navigate to:</td>
<td>Navigate to:</td>
</tr>
</tbody>
</table>
Assign a phone lock key.

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.phone_lock.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>phone_setting.phone_lock.unlock_pin</th>
<th>Characters within 15 digits</th>
<th>123</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>phone_setting.phone_lock.lock_time_out</th>
<th>Integer from 0 to 3600</th>
<th>0</th>
</tr>
</thead>
</table>

**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 - > Auto Lock(0~3600s)

**Phone User Interface:**
Settings - > Advanced (default password: admin) - > Phone Lock - > Auto Lock
Configuring Security Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone_setting.emergency.number</td>
<td>String within 99 characters</td>
<td>112,911,110</td>
</tr>
</tbody>
</table>

**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 805.

**Details of Configuration Parameters:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type/programablekey.X.type/</td>
<td>50</td>
<td>Refer to the following content</td>
</tr>
<tr>
<td>expansion_module.X.key.Y.type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>For line keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For SIP-T58V/T58A/T56A IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For CP960 IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For programable keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For SIP-T58V/T58A/T56A IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When X=12, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When X=13, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>When X=14, the default value is 2 (Forward).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For ext keys:</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For SIP-T58V/T58A/T56A IP phones:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>When Y= 1 to 60, the default value is 0 (NA).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> EXT key is not applicable to CP960 IP phones.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSSKey-&gt;Line Key/Programable Key-&gt;Type</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Settings-&gt;Features-&gt;DSS Keys-&gt;Line Keys X-&gt;Type</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### linekey.X.label/ expansion_module.X.key.Y.label

<table>
<thead>
<tr>
<th>linekey.X.label/ expansion_module.X.key.Y.label</th>
<th>String within 99 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

### 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)

**Note:** EXT key is not applicable to CP960 IP phones.

### 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 Auto Lock 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 Old 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:

![TLS handshake diagram](image)

**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 800.

- **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 is 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 |
|------------------------------------------|----------|----------------------------------|
| <y000000000xx>.cfg | Configure trusted certificates feature.  
**Parameters:** static.security.trust_certificates  
static.security.ca_cert  
static.security.cn_validation |
| Central Provisioning (Configuration File) | | 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&acct=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:**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.sip_server.Y.transport_type</td>
<td>0, 1, 2 or 3</td>
<td>0</td>
</tr>
</tbody>
</table>

**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)
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account-&gt;Register-&gt;SIP Server Y-&gt;Transport</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.security.trust_certificates</strong></td>
<td>0 or 1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enables or disables the IP phone to only trust the server certificates in the Trusted Certificates list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security-&gt;Trusted Certificates-&gt;Only Accept Trusted Certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.security.ca_cert</strong></td>
<td>0, 1 or 2</td>
<td>2</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configures the type of certificates in the Trusted Certificates list for the IP phone to authenticate for TLS connection.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0-Default Certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-Custom Certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-All Certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> If you change this parameter, the IP phone will reboot to make the change take effect.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security-&gt;Trusted Certificates-&gt;CA Certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.security.cn_validation</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>static.security.dev_cert</strong></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>static.trusted_certificates.url</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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
```
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Web User Interface:**
Security->Trusted Certificates->Load trusted certificates file

**Phone User Interface:**
None

<table>
<thead>
<tr>
<th>static.trusted_certificates.delete</th>
<th><a href="http://localhost/all">http://localhost/all</a></th>
<th>Blank</th>
</tr>
</thead>
</table>

**Description:**
Deletes all uploaded trusted certificates.

**Example:**
static.trusted_certificates.delete = http://localhost/all

<table>
<thead>
<tr>
<th>static.server_certificates.url</th>
<th>URL within 511 characters</th>
<th>Blank</th>
</tr>
</thead>
</table>

**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

<table>
<thead>
<tr>
<th>static.server_certificates.delete</th>
<th><a href="http://localhost/all">http://localhost/all</a></th>
<th>Blank</th>
</tr>
</thead>
</table>

**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**

<table>
<thead>
<tr>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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.

![Yealink Security Feature](Image)

**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:

```plaintext
m=audio 50020 RTP/AVP 118 9 0 8 18 101
a=rtpmap:118 opus/48000/2
a=fmtp:118 sprop-maxcapterate=48000; maxaveragebitrate=40000;
a=rtpmap:9 G722/8000
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:NWM5SYmZkZDKyJlOTg2MDgwOTM5ZjbxNmJkNTY5
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:N2M1NmMzZTi2MGFxZjY5YWZzMGE5MWYjYjY5
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NjMxYmIzMDIxNGExM2JkYQxZTMYODQ1MTkhYzg0
m=video 50022 RTP/AVP 97 98 99 117
```
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
```
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 728.

**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:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.X.srtp_encryption</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

**Description:**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures whether to use audio/video encryption service for account X.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 - Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 - Optional</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 - Compulsory</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 (y000000000xx.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.

| Central Provisioning (Configuration File) | Configure whether to only download and resolve the encrypted files.  
Parameter:  
static.auto_provision.update_file_mode |
|---------------------------------------|---------------------------------------------------------------|
| <y0000000000xx>.cfg                  | Configure the decryption method.  
Parameter:  
static.auto_provision.aes_key_in_file |
| Web User Interface                    | Configure AES keys.  
Parameters:  
static.auto_provision.aes_key_16.com  
static.auto_provision.aes_key_16.mac |
|                                        | 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 |
| Phone User Interface                  | Configure AES keys.  
Navigate to:  
http://<phoneIPAddress>/servlet?p=settings-autop&q=load |
|                                        | Configure AES keys. |
## Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.auto_provision.update_file_mode</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.auto_provision.aes_key_in_file</code></td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

### 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:
## Configuring Security Features

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>static.auto_provision.aes_key_16.com</strong></td>
<td>16 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>static.auto_provision.aes_key_16.mac</strong></td>
<td>16 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings-&gt;Advanced Settings (default password: admin) -&gt; Auto Provision -&gt; MAC-Oriented AES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.encryption.config</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

### 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
y00000000058.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.

**Procedure to Encrypt Configuration Files**

**To encrypt the <y000000000xx>.cfg file:**

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.

   The screenshot of the main page is shown as below:

   ![Yealink Configuration Encrypt Tool](image)

   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>.cf9 | 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=m od_data&p=settings-config&q=load |

#### Details of Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.syslog.log_level</td>
<td>Integer from 0 to 6</td>
<td>3</td>
</tr>
</tbody>
</table>

**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)

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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.syslog.mode</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter: static.syslog.mode</td>
<td>Configure the syslog mode.</td>
</tr>
<tr>
<td>Parameter: static.syslog.server</td>
<td>Configure the IP address or domain name of the syslog server where to export the log files.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter: static.syslog.mode</td>
<td>Configure the syslog mode.</td>
</tr>
<tr>
<td>Parameter: static.syslog.server</td>
<td>Configure the IP address or domain name of the syslog server where to export the log files.</td>
</tr>
</tbody>
</table>

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

Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.syslog.mode</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

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
Troubleshooting

### 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)*

  `<y00000000000xx>.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`
<table>
<thead>
<tr>
<th><strong>Troubleshooting</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure the maximum size of the log files can be stored on the provisioning server.</strong></td>
<td><strong>Parameter:</strong> static.syslog.ftp.max_logfile</td>
</tr>
<tr>
<td><strong>Configure the behavior when log file on the provisioning server reaches the max size.</strong></td>
<td><strong>Parameter:</strong> static.syslog.ftp.append_limit_mode</td>
</tr>
<tr>
<td><strong>Configure the waiting time before the phone uploads the log file to the provisioning server.</strong></td>
<td><strong>Parameter:</strong> static.syslog.bootlog_upload_wait_time</td>
</tr>
<tr>
<td><strong>Configure the access URL of the provisioning server.</strong></td>
<td><strong>Parameter:</strong> static.auto_provision.server.url</td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>static.syslog.mode</strong></td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>static.syslog.log_upload_period</strong></td>
<td>Integer from 30 to 2592000</td>
<td>30</td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.syslog.ftp.post_mode</code></td>
<td>1 or 2</td>
<td>1</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.syslog.ftp.max_logfile</code></td>
<td>Integer from 200 to 65535</td>
<td>512</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>static.syslog.ftp.append_limit_mode</code></td>
<td>1 or 2</td>
<td>1</td>
</tr>
</tbody>
</table>

**Description:**

Configures the behavior when log file on the provisioning server reaches the max size.

1-Append Delete
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2-Append Stop</strong></td>
<td><strong>Permitted Values</strong></td>
<td><strong>Default</strong></td>
</tr>
<tr>
<td>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. <strong>Note:</strong> 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. <strong>Web User Interface:</strong> Settings-&gt;Configuration-&gt;Append Limit Mode <strong>Phone User Interface:</strong> None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 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 of 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.
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):
### 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)**
  - `<y00000000000x>.cf`
  - `9`
  - 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://<phoneIP address>/servlet?m=mod_data&p=mod_settings-config&q=load`
## Details of the Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>packet_capture.max_file_counts</td>
<td>Integer from 1 to 100</td>
<td>15</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the count of the number of packets to capture.</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Settings-&gt;Configuration-&gt;Packet Capture Count</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>packet_capture.max_file_bytes</td>
<td>Integer from 100 to 1024</td>
<td>1024</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the maximum size (in KB) of every packet to capture.</td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Settings-&gt;Configuration-&gt;Packet Capture Clip Bytes</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>packet_capture.filter_type</td>
<td>0, 1 or 2</td>
<td>0</td>
</tr>
<tr>
<td><strong>Description:</strong></td>
<td>Configures the filter type of the packet to capture.</td>
<td></td>
</tr>
<tr>
<td>0-Custom</td>
<td>1-SIP or H245 or H225</td>
<td></td>
</tr>
<tr>
<td>2-RTP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If it is set to 0 (Custom), the IP phone captures the packets according to the custom packet filter string (configured by the parameter &quot;packet_capture.filter&quot;).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If it is set to 2 (RTP), the IP phone captures the RTP packets.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Web User Interface:</strong></td>
<td>Settings-&gt;Configuration-&gt;Pcap Filter Type</td>
<td></td>
</tr>
<tr>
<td><strong>Phone User Interface:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>packet_capture.filter</td>
<td>String within 255</td>
<td>Blank</td>
</tr>
</tbody>
</table>
**Troubleshooting**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>characters</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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
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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cf</th>
<th>Configure span to PC port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter:</td>
<td>static.network.span_to_pc_port</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web User Interface</th>
<th>Configure span to PC port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigate to:</td>
<td>http://&lt;phoneIPAddress&gt;/servlet?m=mod_data&amp;p=network-adv&amp;q=load</td>
</tr>
</tbody>
</table>

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.network.span_to_pc_port</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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**.

![IP phone configuration interface](image)

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.

<table>
<thead>
<tr>
<th><strong>Central Provisioning</strong> (Configuration File)</th>
<th>Configure Watch Dog feature. Parameter: static.watch_dog.enable</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;y0000000000xx&gt;.cf</code></td>
<td></td>
</tr>
</tbody>
</table>

| **Web User Interface**                       | Configure Watch Dog feature. Navigate to: http://<phoneIPAddress>/servlet?m=mo |
Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.watch_dog.enable</td>
<td>0 or 1</td>
<td>1</td>
</tr>
</tbody>
</table>

**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 \(\text{Network unavailable}\) 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 823.

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):

![IP Phone Information](image)

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://<phoneIP Address>/servlet?m =mod_data&p=settings-config&q=l oad |

**Details of the Configuration Parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.configuration.url</td>
<td>URL within 511 characters</td>
<td>Blank</td>
</tr>
</tbody>
</table>

**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:**
**Administrator’s Guide for SIP-T5 Series Smart Media Phones**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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 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 330.

**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 330.

**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 772.
- 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.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>58: Firmware version ID. The firmware version ID for each IP phone model is:</td>
</tr>
<tr>
<td></td>
<td>• 58: SIP-T58V/T58A/T56A</td>
</tr>
<tr>
<td></td>
<td>• 73: CP960</td>
</tr>
<tr>
<td>2</td>
<td>80: Firmware generation. <strong>Note:</strong> The larger it is, the newer the firmware generation is.</td>
</tr>
<tr>
<td>3</td>
<td>0: A fixed number.</td>
</tr>
<tr>
<td>4</td>
<td>5: Firmware version. <strong>Note:</strong> With the same firmware generation, the larger it is, the newer the firmware version is.</td>
</tr>
</tbody>
</table>

**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 successfully 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 back up 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.

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>Web User Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;y00000000xx&gt;.cfg</td>
<td>Configure the access URL of the custom factory configuration files.</td>
</tr>
<tr>
<td>&lt;y00000000xx&gt;.cfg</td>
<td>Configure the access URL of the custom factory configuration files.</td>
</tr>
<tr>
<td>[Central Provisioning (Configuration File)]&lt;y00000000xx&gt;.cfg</td>
<td>Configure the Import Factory Configuration feature. Parameter: static.features.custom_factory_config.enable</td>
</tr>
</tbody>
</table>

The web user interface prompts the message “Reset build-in SD card to factory?”.
## Details of Configuration Parameters:

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.features.custom_factory_config.enable</td>
<td>0 or 1</td>
<td>0</td>
</tr>
</tbody>
</table>

**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 783.

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.

<table>
<thead>
<tr>
<th>Central Provisioning (Configuration File)</th>
<th>&lt;y0000000000xx&gt;.cfg</th>
<th>Configure the IP phone behavior when receiving a SIP NOTIFY message which contains the header “Event: check-sync”. Parameter: sip.notify_reboot_enable</th>
</tr>
</thead>
</table>

Details of the Configuration Parameter:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Permitted Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip.notify_reboot_enable</td>
<td>0, 1 or 2</td>
<td>1</td>
</tr>
</tbody>
</table>

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.
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?

<table>
<thead>
<tr>
<th>Source Device</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination Device</th>
<th>Destination IP</th>
<th>Destination Port (Listening port)</th>
<th>Protocol</th>
<th>Description of destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP phones</td>
<td>2~65535</td>
<td>IP phone or voice gateway</td>
<td>IP address of IP phone or voice gateway</td>
<td>Determined by destination device</td>
<td>UDP</td>
<td>RTP protocol port, it is used to send or receive audio stream.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1024~65535</td>
<td>SIP Server</td>
<td>IP address of SIP server</td>
<td>Determined by destination device</td>
<td>UDP/TCP</td>
<td>SIP protocol port, it is used for signaling interaction with SIP server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1024~65535</td>
<td>TR-069 Server</td>
<td>IP address of TR-069 server</td>
<td>Determined by destination device</td>
<td>TCP</td>
<td>TR-069 protocol port, it is used to communicate with TR-069 server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1024~65535</td>
<td>File server</td>
<td>IP address of file server</td>
<td>Determined by destination device</td>
<td>TCP</td>
<td>HTTP protocol port, it is used to download file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1024~65535</td>
<td>Remote phone book server</td>
<td>IP address of remote phone book server</td>
<td>Determined by destination device</td>
<td>TCP</td>
<td>HTTP protocol port, it is used to access the remote phone book.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1024~65535</td>
<td>AA</td>
<td>IP address of AA</td>
<td>Determined by destination device</td>
<td>TCP</td>
<td>HTTP protocol port, it is used for AA communication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>68</td>
<td>DHCP Server</td>
<td>IP address of DHCP server</td>
<td>67</td>
<td>UDP</td>
<td>DHCP protocol port, it is used to obtain IP address from DHCP server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1024~65535</td>
<td>LDAP Server</td>
<td>IP address of LDAP server</td>
<td>Determined by destination device</td>
<td>TCP</td>
<td>LDAP protocol port, it is used to obtain the contact information</td>
<td></td>
</tr>
<tr>
<td>Source Device</td>
<td>Source IP</td>
<td>Source Port</td>
<td>Destination Device</td>
<td>Destination IP</td>
<td>Destination Port (Listening port)</td>
<td>Protocol</td>
<td>Description of destination port</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------</td>
<td>-------------</td>
<td>--------------------</td>
<td>----------------</td>
<td>-----------------------------------</td>
<td>----------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
<td>1024~65535</td>
<td>NTP Server</td>
<td>IP address of NTP server</td>
<td>123</td>
<td>UDP</td>
<td></td>
<td>from LDAP server.</td>
</tr>
<tr>
<td></td>
<td>1024~65535</td>
<td>Syslog Server</td>
<td>IP address of syslog server</td>
<td>514</td>
<td>UDP</td>
<td></td>
<td>NTP protocol port, it is used to synchronize time from NTP time server.</td>
</tr>
<tr>
<td></td>
<td>1024~65535</td>
<td>PNP Server</td>
<td>IP address of PNP server (Default value: 224.0.1.75)</td>
<td>5059</td>
<td>UDP/TCP</td>
<td></td>
<td>Syslog protocol port, it is used for IP phones to upload syslog information to syslog server.</td>
</tr>
<tr>
<td></td>
<td>Multipaging</td>
<td>Multipaging</td>
<td>Multipaging</td>
<td>65000   65001</td>
<td>TCP</td>
<td></td>
<td>Protocol port, it is used to obtain the URL of updating file from PNP server.</td>
</tr>
<tr>
<td>PC</td>
<td>IP address of PC</td>
<td>1~65535</td>
<td>TCP</td>
<td></td>
<td>HTTP port (default value: 80)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP Server</td>
<td>IP address of SIP Server</td>
<td>1~65535</td>
<td>TCP</td>
<td></td>
<td>HTTP port (default value: 443)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP phone of voice gateway</td>
<td>Determined by the destination device.</td>
<td>IP address of IP phone or voice gateway</td>
<td>IP phones</td>
<td>IP address of IP phones</td>
<td>1024~65534</td>
<td>UDP/TCP</td>
<td>SIP protocol port, it is used for signaling interaction with SIP server.</td>
</tr>
<tr>
<td>TR-069 Server</td>
<td>IP address of TR-069 Server</td>
<td>2~65535</td>
<td>UDP</td>
<td></td>
<td>RTP protocol port, it is used by destination device to send or receive audio stream.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1024~65535</td>
<td>TCP</td>
<td></td>
<td>TR-069 protocol port, it is used to communicate with TR-069 server.</td>
</tr>
</tbody>
</table>
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 306 and Anonymous Call Rejection on page 310.

**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.

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00</td>
<td>192.168.1.100</td>
<td>192.168.1.200</td>
<td>SDP</td>
<td>1024</td>
<td>Request: INVITE SIP:192.168.1.100 SIP:192.168.1.200, with session description</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00</td>
<td>192.168.1.100</td>
<td>192.168.1.200</td>
<td>SDP</td>
<td>1024</td>
<td>Request: INVITE SIP:192.168.1.100 SIP:192.168.1.200, with session description</td>
</tr>
</tbody>
</table>

For more information on RFC 2543 hold feature, refer to Call Hold on page 338. For more
information on capturing packets, refer to Capturing Packets on page 765.
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 interconnect 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

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Time Zone Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>-11</td>
<td>Samoa</td>
</tr>
<tr>
<td>-10</td>
<td>United States-Hawaii-Aleutian, United States-Alaska-Aleutian</td>
</tr>
<tr>
<td>-9:30</td>
<td>French Polynesia</td>
</tr>
<tr>
<td>-9</td>
<td>United States-Alaska Time</td>
</tr>
<tr>
<td>-8</td>
<td>Canada(Vancouver,Whitehorse), Mexico(Tijuana,Mexicali), United States-Pacific Time</td>
</tr>
<tr>
<td>-7</td>
<td>Canada(Edmonton,Calgary), Mexico(Mazatlan,Chihuahua), United States-MST no DST, United States-Mountain Time</td>
</tr>
<tr>
<td>-6</td>
<td>Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Belize, Canada-Manitoba(Winnipeg), Chile(Easter Islands), Mexico(Mexico City,Acapulco), United States-Central Time</td>
</tr>
<tr>
<td>-5</td>
<td>Peru, Bahamas(Nassau), Canada(Montreal,Ottawa,Quebec), Cuba(Havana), United States-Eastern Time</td>
</tr>
<tr>
<td>-4:30</td>
<td>Venezuela(Caracas)</td>
</tr>
<tr>
<td>-4</td>
<td>Canada(Halifax,Saint John), Chile(Santiago), Paraguay(Asuncion), United Kingdom-Bermuda(Bermuda), United Kingdom(Falkland Islands), Trinidad&amp;Tobago</td>
</tr>
<tr>
<td>-3:30</td>
<td>Canada-New Foundland(St.Johns)</td>
</tr>
<tr>
<td>-3</td>
<td>Argentina(Buenos Aires), Brazil(DST), Brazil(no DST), Denmark-Greenland(Nuuk)</td>
</tr>
<tr>
<td>-2:30</td>
<td>Newfoundland and Labrador</td>
</tr>
<tr>
<td>-2</td>
<td>Brazil(no DST)</td>
</tr>
<tr>
<td>-1</td>
<td>Portugal(Azores)</td>
</tr>
<tr>
<td>0</td>
<td>Denmark-Faroe Islands(Torshavn), GMT, Greenland, Ireland(Dublin), Morocco, Portugal(Lisboa,Porto,Funchal), Spain-Canary Islands(Las Palmas), United Kingdom(London)</td>
</tr>
<tr>
<td>+1</td>
<td>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)</td>
</tr>
<tr>
<td>+2</td>
<td>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)</td>
</tr>
<tr>
<td>+3</td>
<td>East Africa Time, Iraq(Baghdad), Russia(Moscow)</td>
</tr>
<tr>
<td>+3:30</td>
<td>Iran(Toheran)</td>
</tr>
<tr>
<td>+4</td>
<td>Armenia(Yerevan), Azerbaijan(Baku), Georgia(Tbilisi), Kazakhstan(Aktau), Russia(Samara)</td>
</tr>
</tbody>
</table>
### Time Zones

<table>
<thead>
<tr>
<th>Time Zone</th>
<th>Time Zone Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>+4:30</td>
<td>Afghanistan (Kabul)</td>
</tr>
<tr>
<td>+5</td>
<td>Kazakhstan (Aqtobe), Kyrgyzstan (Bishkek), Pakistan (Islamabad), Russia (Chelyabinsk)</td>
</tr>
<tr>
<td>+5:30</td>
<td>India (Calcutta)</td>
</tr>
<tr>
<td>+5:45</td>
<td>Nepal (Katmandu)</td>
</tr>
<tr>
<td>+6</td>
<td>Kazakhstan ( Astana, Almaty), Russia (Novosibirsk, Omsk)</td>
</tr>
<tr>
<td>+6:30</td>
<td>Myanmar (Naypyitaw)</td>
</tr>
<tr>
<td>+7</td>
<td>Russia (Chelyabinsk), Thailand (Bangkok)</td>
</tr>
<tr>
<td>+8</td>
<td>Australia (Perth), China (Beijing), Russia (Irkutsk, Ulan-Ude), Singapore (Singapore)</td>
</tr>
<tr>
<td>+8:45</td>
<td>Eucla</td>
</tr>
<tr>
<td>+9</td>
<td>Japan (Tokyo), Korea (Seoul), Russia (Yakutsk, Chita)</td>
</tr>
<tr>
<td>+9:30</td>
<td>Australia (Adelaide), Australia (Darwin)</td>
</tr>
<tr>
<td>+10</td>
<td>Australia (Brisbane), Australia (Hobart), Australia (Sydney, Melbourne, Canberra), Russia (Yakutsk, Chita)</td>
</tr>
<tr>
<td>+10:30</td>
<td>Australia (Lord Howe Islands)</td>
</tr>
<tr>
<td>+11</td>
<td>New Caledonia (Noumea), Russia (Srednekolymsk Time)</td>
</tr>
<tr>
<td>+11:30</td>
<td>Norfolk Island</td>
</tr>
<tr>
<td>+12</td>
<td>New Zealand (Wellington, Auckland), Russia (Kamchatka Time)</td>
</tr>
<tr>
<td>+12:45</td>
<td>New Zealand (Chatham Islands)</td>
</tr>
<tr>
<td>+13</td>
<td>Tonga (Nukualofa)</td>
</tr>
<tr>
<td>+13:30</td>
<td>Chatham Islands</td>
</tr>
<tr>
<td>+14</td>
<td>Kiribati</td>
</tr>
</tbody>
</table>

### 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
Appendix

- 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.S.
- AAA Certificate Services
- AC Ral z Certicômara 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 Firmaprosfesional CIF A62634068
- Bypass Class 2 CA 1
- Bypass Class 2 Root CA
- Bypass Class 3 CA 1
- Bypass 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 Sağlayicisi
- EC-ACC
- EE Certification Centre Root CA
- e-Guven Kok Elektronik Sertifika Hizmet Sağlayicisi
- 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) Tanusítványkiadó
- NetLock Kozjegyzői (Class A) Tanusítványkiadó
- NetLock Uzleti (Class B) Tanusítványkiadó
- 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 Niederlanden Root CA
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.

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 728.
The following table lists the number of DSS keys you can configure for each phone model:

<table>
<thead>
<tr>
<th>Phone Model</th>
<th>Line Key</th>
<th>Programmable Key</th>
<th>Ext Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-T58V/T58A/T56A</td>
<td>27</td>
<td>3</td>
<td>60</td>
</tr>
<tr>
<td>CP960</td>
<td>30</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Note**

- The programmable 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 programmable keys for each phone model.

# X ranges from 12 to 14:
- programmablekey.X.type =
- programmablekey.X.line =
- programmablekey.X.value =
- programmablekey.X.xml_phonebook =
- programmablekey.X.history_type =
- programmablekey.X.pickup_value =

<table>
<thead>
<tr>
<th>X</th>
<th>Phone Model</th>
<th>SIP-T58V/T58A/T56A</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>Hold</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>Mute</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>Tran</td>
</tr>
</tbody>
</table>
DSS key can be assigned with various key features. The parameters of the DSS key are detailed in the following:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration File</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.type</td>
<td><code>&lt;y0000000000xx&gt;.cfg</code></td>
</tr>
<tr>
<td>programablekey.X.type</td>
<td></td>
</tr>
<tr>
<td>expansion_module.X.key.Y.type</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures key feature for the DSS key.</td>
</tr>
</tbody>
</table>

For line keys:
- X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)
- X is equal to 1 (for CP960)

For programmable 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)
<table>
<thead>
<tr>
<th></th>
<th>Administrator's Guide for SIP-T5 Series Smart Media Phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Private Hold</td>
</tr>
<tr>
<td>22</td>
<td>XML Group</td>
</tr>
<tr>
<td>23</td>
<td>Group Pickup</td>
</tr>
<tr>
<td>24</td>
<td>Multicast Paging</td>
</tr>
<tr>
<td>25</td>
<td>Record</td>
</tr>
<tr>
<td>27</td>
<td>XML Browser</td>
</tr>
<tr>
<td>34</td>
<td>Hot Desking</td>
</tr>
<tr>
<td>35</td>
<td>URL Record</td>
</tr>
<tr>
<td>38</td>
<td>LDAP</td>
</tr>
<tr>
<td>39</td>
<td>BLF List</td>
</tr>
<tr>
<td>40</td>
<td>Prefix</td>
</tr>
<tr>
<td>41</td>
<td>Zero Touch</td>
</tr>
<tr>
<td>42</td>
<td>ACD</td>
</tr>
<tr>
<td>45</td>
<td>Local Group</td>
</tr>
<tr>
<td>50</td>
<td>Phone Lock</td>
</tr>
<tr>
<td>56</td>
<td>Retrieve Park</td>
</tr>
<tr>
<td>61</td>
<td>Directory</td>
</tr>
<tr>
<td>66</td>
<td>Paging List</td>
</tr>
<tr>
<td>77</td>
<td>Mobile Account</td>
</tr>
<tr>
<td>84</td>
<td>Open Door</td>
</tr>
<tr>
<td>85</td>
<td>Video Monitoring</td>
</tr>
</tbody>
</table>

**For programable keys:**

**Valid types are:**

<table>
<thead>
<tr>
<th></th>
<th>Administrator's Guide for SIP-T5 Series Smart Media Phones</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>Forward</td>
</tr>
<tr>
<td>5</td>
<td>DND</td>
</tr>
<tr>
<td>7</td>
<td>ReCall</td>
</tr>
<tr>
<td>9</td>
<td>Direct Pickup</td>
</tr>
<tr>
<td>13</td>
<td>Speed Dial</td>
</tr>
<tr>
<td>20</td>
<td>Private Hold</td>
</tr>
<tr>
<td>22</td>
<td>XML Group</td>
</tr>
<tr>
<td>23</td>
<td>Group Pickup</td>
</tr>
<tr>
<td>27</td>
<td>XML Browser</td>
</tr>
<tr>
<td>28</td>
<td>History</td>
</tr>
<tr>
<td>30</td>
<td>Menu</td>
</tr>
<tr>
<td>33</td>
<td>Status</td>
</tr>
</tbody>
</table>
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
27-XML Browser
34-Hot Desking
<table>
<thead>
<tr>
<th>Format</th>
<th>Integer</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default Value</th>
<th>For line keys:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For SIP-T58V/T58A/T56A IP phones:</td>
</tr>
<tr>
<td></td>
<td>The default value of the line key 1-16 is 15, and the default value of the line key 17-27 is 0.</td>
</tr>
<tr>
<td></td>
<td>For CP960 IP phones:</td>
</tr>
<tr>
<td></td>
<td>The default value of the line key 1 is 15, and the default value of the line key 2-30 is 0.</td>
</tr>
<tr>
<td></td>
<td>For programable keys:</td>
</tr>
<tr>
<td></td>
<td>When X=12, the default value is 0 (NA).</td>
</tr>
<tr>
<td></td>
<td>When X=13, the default value is 0 (NA).</td>
</tr>
<tr>
<td></td>
<td>When X=14, the default value is 2 (Forward).</td>
</tr>
<tr>
<td></td>
<td>For ext keys:</td>
</tr>
<tr>
<td></td>
<td>When Y=1-60, the default value is 0 (NA).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Range</th>
<th>Valid values are:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0 - N/A</td>
</tr>
<tr>
<td></td>
<td>1 - Conference</td>
</tr>
<tr>
<td></td>
<td>2 - Forward</td>
</tr>
<tr>
<td></td>
<td>3 - Transfer</td>
</tr>
<tr>
<td></td>
<td>4 - Hold</td>
</tr>
<tr>
<td></td>
<td>5 - DND</td>
</tr>
<tr>
<td></td>
<td>7 - ReCall</td>
</tr>
<tr>
<td></td>
<td>8 - SMS</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>9</td>
<td>Direct Pickup</td>
</tr>
<tr>
<td>10</td>
<td>Call Park</td>
</tr>
<tr>
<td>11</td>
<td>DTMF</td>
</tr>
<tr>
<td>12</td>
<td>Voice Mail</td>
</tr>
<tr>
<td>13</td>
<td>Speed Dial</td>
</tr>
<tr>
<td>14</td>
<td>Intercom</td>
</tr>
<tr>
<td>15</td>
<td>Line</td>
</tr>
<tr>
<td>16</td>
<td>BLF</td>
</tr>
<tr>
<td>17</td>
<td>URL</td>
</tr>
<tr>
<td>18</td>
<td>Group Listening</td>
</tr>
<tr>
<td>20</td>
<td>Private Hold</td>
</tr>
<tr>
<td>22</td>
<td>XML Group</td>
</tr>
<tr>
<td>23</td>
<td>Group Pickup</td>
</tr>
<tr>
<td>24</td>
<td>Multicast Paging</td>
</tr>
<tr>
<td>25</td>
<td>Record</td>
</tr>
<tr>
<td>27</td>
<td>XML Browser</td>
</tr>
<tr>
<td>28</td>
<td>History</td>
</tr>
<tr>
<td>30</td>
<td>Menu</td>
</tr>
<tr>
<td>33</td>
<td>Status</td>
</tr>
<tr>
<td>34</td>
<td>Hot Desking</td>
</tr>
<tr>
<td>35</td>
<td>URL Record</td>
</tr>
<tr>
<td>38</td>
<td>LDAP</td>
</tr>
<tr>
<td>39</td>
<td>BLF List</td>
</tr>
<tr>
<td>40</td>
<td>Prefix</td>
</tr>
<tr>
<td>41</td>
<td>Zero Touch</td>
</tr>
<tr>
<td>42</td>
<td>ACD</td>
</tr>
<tr>
<td>43</td>
<td>Local Directory</td>
</tr>
<tr>
<td>45</td>
<td>Local Group</td>
</tr>
<tr>
<td>47</td>
<td>XML Directory</td>
</tr>
<tr>
<td>50</td>
<td>Phone Lock</td>
</tr>
<tr>
<td>51</td>
<td>Switch Account Up</td>
</tr>
<tr>
<td>52</td>
<td>Switch Account Down</td>
</tr>
<tr>
<td>56</td>
<td>Retrieve Park</td>
</tr>
<tr>
<td>61</td>
<td>Directory</td>
</tr>
<tr>
<td>66</td>
<td>Paging List</td>
</tr>
<tr>
<td>77</td>
<td>Mobile Account</td>
</tr>
<tr>
<td>84</td>
<td>Open Door</td>
</tr>
<tr>
<td>Parameter</td>
<td>Configuration File</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>linekey.X.line</td>
<td><code>&lt;y0000000000xx&gt;.cfg</code></td>
</tr>
<tr>
<td>programablekey.X.line</td>
<td></td>
</tr>
<tr>
<td>expansion_module.X.key.Y.line</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configures the desired line to apply the key feature.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For line keys:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X is equal to 1 (for CP960)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For programable keys</strong> (not applicable to CP960 IP phones):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 12 to 14</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>For ext keys</strong> (not applicable to CP960 IP phones):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>X ranges from 1 to 3, Y ranges from 1 to 60</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Format</th>
<th>Integer</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Default Value</th>
<th>For the programable key and ext key, the default value is not applicable.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For the line key, when X=1, the default value is 1.</td>
</tr>
<tr>
<td></td>
<td>When X=2, the default value is 2.</td>
</tr>
<tr>
<td></td>
<td>When X=3 the default value is 3</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>When X=16 the default value is 16.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permitted Values:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 16 (for SIP-T58V/T58A/T56A)</td>
<td></td>
</tr>
<tr>
<td>1 (for CP960)</td>
<td></td>
</tr>
<tr>
<td>1-Line 1</td>
<td></td>
</tr>
<tr>
<td>2-Line 2</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>16-Line 16</td>
<td></td>
</tr>
</tbody>
</table>

| Example | linekey.1.line = 2 |
### Parameter - linekey.X.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 programmable 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.

```plaintext
linekey.1.value = 1001
```

### Parameter - programablekey.X.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 programmable 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.

```plaintext
linekey.1.value = 1001
```

### 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 programmable 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.

```plaintext
linekey.1.value = 1001
```
<table>
<thead>
<tr>
<th>Format</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Value</td>
<td>Blank</td>
</tr>
<tr>
<td>Range</td>
<td>String within 99 characters</td>
</tr>
<tr>
<td>Example</td>
<td>linekey.1.label = Dir</td>
</tr>
</tbody>
</table>

**Parameter:** linekey.X.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

<table>
<thead>
<tr>
<th>Format</th>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Value</td>
<td>Blank</td>
</tr>
<tr>
<td>Range</td>
<td>String within 256 characters</td>
</tr>
<tr>
<td>Example</td>
<td>linekey.1.pickup_value = *88</td>
</tr>
</tbody>
</table>

**Parameter:** linekey.X.xml_phonebook

**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.

<table>
<thead>
<tr>
<th>Description</th>
<th>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.</th>
</tr>
</thead>
</table>

**Configuration File**

- `<y0000000000xx>.cfg`
For line keys:
X ranges from 1 to 27 (for SIP-T58V/T58A/T56A)
X is equal to 1 (for CP960)

**For programmable 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Format</th>
<th>Default Value</th>
<th>Range</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.extension</td>
<td>Integer</td>
<td>0</td>
<td>0 to 48</td>
<td>Configures the second remote phone book.</td>
</tr>
<tr>
<td>expansion_module.X.key.Y.extension</td>
<td></td>
<td></td>
<td></td>
<td>linekey.1.xml_phonebook = 1</td>
</tr>
</tbody>
</table>

**Configuration File**
<y0000000000xx>.cfg

**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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Format</th>
<th>Default Value</th>
<th>Range</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>linekey.X.extension</td>
<td>Integer</td>
<td>0</td>
<td>0 to 48</td>
<td>Configures the second remote phone book.</td>
</tr>
<tr>
<td>expansion_module.X.key.Y.extension</td>
<td></td>
<td></td>
<td></td>
<td>linekey.1.extension= 1</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Function</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>static.network.ip_address_mode</td>
</tr>
<tr>
<td></td>
<td>static.network.ipv6_prefix</td>
</tr>
<tr>
<td></td>
<td>static.network.ipv6_internet_port.type</td>
</tr>
<tr>
<td></td>
<td>static.network.ipv6_internet_port.ip</td>
</tr>
<tr>
<td></td>
<td>static.network.ipv6_internet_port.gateway</td>
</tr>
<tr>
<td></td>
<td>static.network.ipv6_primary_dns</td>
</tr>
<tr>
<td></td>
<td>static.network.ipv6_secondary_dns</td>
</tr>
<tr>
<td></td>
<td>static.network.ipv6_icmp_v6.enable</td>
</tr>
<tr>
<td></td>
<td>static.network.internet_port.type</td>
</tr>
<tr>
<td></td>
<td>static.network.internet_port.ip</td>
</tr>
<tr>
<td></td>
<td>static.network.internet_port.mask</td>
</tr>
<tr>
<td></td>
<td>static.network.internet_port.gateway</td>
</tr>
<tr>
<td></td>
<td>static.network.primary_dns</td>
</tr>
<tr>
<td></td>
<td>static.network.secondary_dns</td>
</tr>
<tr>
<td></td>
<td>static.network.dhcp_host_name</td>
</tr>
<tr>
<td></td>
<td>static.network.pppoe.user</td>
</tr>
<tr>
<td></td>
<td>static.network.pppoe.password</td>
</tr>
<tr>
<td></td>
<td>static.network.pc_port.enable</td>
</tr>
<tr>
<td></td>
<td>static.network.internet_port.speed_duplex</td>
</tr>
<tr>
<td></td>
<td>static.network.pc_port.speed_duplex</td>
</tr>
<tr>
<td>Function</td>
<td>Parameters</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>static.network.static_dns_enable</td>
<td></td>
</tr>
<tr>
<td>static.network.ipv6_static_dns_enable</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.pc_port_mode</td>
<td></td>
</tr>
<tr>
<td>static.network.dns.ttl_enable</td>
<td></td>
</tr>
<tr>
<td>static.network.dhcp.server_mac1</td>
<td></td>
</tr>
<tr>
<td>static.network.dhcp.server_mac2</td>
<td></td>
</tr>
<tr>
<td>static.network.mtu_value</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.internet_port_enable</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.internet_port_vid</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.internet_port_priority</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.pc_port_enable</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.pc_port_vid</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.pc_port_priority</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.dhcp_enable</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.dhcp_option</td>
<td></td>
</tr>
<tr>
<td>static.network.vlan.vlan_change.enable</td>
<td></td>
</tr>
<tr>
<td>static.network.port.http</td>
<td></td>
</tr>
<tr>
<td>static.network.port.https</td>
<td></td>
</tr>
<tr>
<td>static.network.qos.signaltos</td>
<td></td>
</tr>
<tr>
<td>static.network.qos.audiotos</td>
<td></td>
</tr>
<tr>
<td>static.network.qos.videotos</td>
<td></td>
</tr>
<tr>
<td>static.wifi.802_11e.enable</td>
<td></td>
</tr>
<tr>
<td>static.network.802_1x.mode</td>
<td></td>
</tr>
<tr>
<td>static.network.802_1x.identity</td>
<td></td>
</tr>
<tr>
<td>static.network.802_1x.md5_password</td>
<td></td>
</tr>
<tr>
<td>static.network.802_1x.root_cert_url</td>
<td></td>
</tr>
<tr>
<td>static.network.802_1x.client_cert_url</td>
<td></td>
</tr>
<tr>
<td>static.network.802_1x.proxy_eap_logoff.enable</td>
<td></td>
</tr>
<tr>
<td>static.network.vpn_enable</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><code>static.openvpn.url</code></td>
</tr>
<tr>
<td></td>
<td><code>static.networklldp.enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.networklldp.packet_interval</code></td>
</tr>
<tr>
<td></td>
<td><code>static.networkspan_to_pc_port</code></td>
</tr>
<tr>
<td></td>
<td><code>static.networkcdp.enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.networkcdp.packet_interval</code></td>
</tr>
<tr>
<td>Wi-Fi</td>
<td><code>static.wifi.enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.power_on</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.attempt_before_failed</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.retry_delay_after_file_transfer_failed</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.server.type</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.user_agent_mac.enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.dns_resolv_nosys</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.dns_resolv_nretry</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.dns_resolv_timeout</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.custom.sync</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.custom.sync.path</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.custom.protect</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.custom.upload_method</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.attempt_expired_time</code></td>
</tr>
<tr>
<td></td>
<td><code>static.network.attempt_expired_time</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.reboot_force.enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.pnp_enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.dhcp_option.enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.dhcp_option.list_user_options</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.dhcp_option.option60_value</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.repeat.enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.repeat.minutes</code></td>
</tr>
<tr>
<td></td>
<td><code>static.auto_provision.weekly.enable</code></td>
</tr>
</tbody>
</table>

819
<table>
<thead>
<tr>
<th>Function</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>static.auto_provision.weekly.dayofweek</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.weekly.begin_time</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.weekly.end_time</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.flexible.enable</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.flexible.interval</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.flexible.begin_time</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.flexible.end_time</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.server.url</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.server.username</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.server.password</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.update_file_mode</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.encryption.config</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.aes_key_in_file</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.aes_key_16.com</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.aes_key_16.mac</td>
<td></td>
</tr>
<tr>
<td>static.autoprov.X.name</td>
<td></td>
</tr>
<tr>
<td>static.autoprov.X.code</td>
<td></td>
</tr>
<tr>
<td>static.autoprov.X.url</td>
<td></td>
</tr>
<tr>
<td>static.autoprov.X.user</td>
<td></td>
</tr>
<tr>
<td>static.autoprov.X.password</td>
<td></td>
</tr>
<tr>
<td>static.autoprov.X.com_aes</td>
<td></td>
</tr>
<tr>
<td>static.autoprov.X.mac_aes</td>
<td></td>
</tr>
<tr>
<td>static.auto_provision.url_wildcard.pn</td>
<td></td>
</tr>
<tr>
<td>static.zero_touch.enable</td>
<td></td>
</tr>
<tr>
<td>static.zero_touch.wait_time</td>
<td></td>
</tr>
<tr>
<td>static.zero_touch.network.fail.wait.times</td>
<td></td>
</tr>
<tr>
<td>static.zero_touch.network.fail.delay.times</td>
<td></td>
</tr>
<tr>
<td>static.features.hide_zero_touch_url.enable</td>
<td></td>
</tr>
<tr>
<td>TR069</td>
<td>static.managementserver.enable</td>
</tr>
<tr>
<td>Function</td>
<td>Parameters</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td><strong>Static Management Server</strong></td>
<td><code>static.managementserver.username</code></td>
</tr>
<tr>
<td></td>
<td><code>static.managementserver.password</code></td>
</tr>
<tr>
<td></td>
<td><code>static.managementserver.url</code></td>
</tr>
<tr>
<td></td>
<td><code>static.managementserver.connection_request_username</code></td>
</tr>
<tr>
<td></td>
<td><code>static.managementserver.connection_request_password</code></td>
</tr>
<tr>
<td></td>
<td><code>static.managementserver.periodic_inform_enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.managementserver.periodic_inform_interval</code></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td><code>static.security.user_name.user</code></td>
</tr>
<tr>
<td></td>
<td><code>static.security.user_name.admin</code></td>
</tr>
<tr>
<td></td>
<td><code>static.security.user_name.var</code></td>
</tr>
<tr>
<td></td>
<td><code>static.security.user_password</code></td>
</tr>
<tr>
<td></td>
<td><code>static.security.trust_certificates</code></td>
</tr>
<tr>
<td></td>
<td><code>static.security.ca_cert</code></td>
</tr>
<tr>
<td></td>
<td><code>static.security.dev_cert</code></td>
</tr>
<tr>
<td></td>
<td><code>static.security.cn_validation</code></td>
</tr>
<tr>
<td></td>
<td><code>static.phone_setting.reserve_certs_enable</code></td>
</tr>
<tr>
<td><strong>3-Level Permissions</strong></td>
<td><code>static.security.var_enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.web_item_level.url</code></td>
</tr>
<tr>
<td></td>
<td><code>static.security.default_access_level</code></td>
</tr>
<tr>
<td><strong>Certificates</strong></td>
<td><code>static.trusted_certificates.url</code></td>
</tr>
<tr>
<td></td>
<td><code>static.trusted_certificates.delete</code></td>
</tr>
<tr>
<td></td>
<td><code>static.server_certificates.url</code></td>
</tr>
<tr>
<td></td>
<td><code>static.server_certificates.delete</code></td>
</tr>
<tr>
<td><strong>Custom Factory Configuration</strong></td>
<td><code>static.features.custom_factory_config.enable</code></td>
</tr>
<tr>
<td></td>
<td><code>static.custom_factory_configuration.url</code></td>
</tr>
<tr>
<td><strong>Custom Configuration</strong></td>
<td><code>static.configuration.url</code></td>
</tr>
<tr>
<td></td>
<td><code>static.custom_mac_cfg.url</code></td>
</tr>
<tr>
<td><strong>Syslog</strong></td>
<td><code>static.syslog.mode</code></td>
</tr>
<tr>
<td></td>
<td><code>static.syslog.server</code></td>
</tr>
<tr>
<td>Function</td>
<td>Parameters</td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>static.syslog.log_level</td>
<td></td>
</tr>
<tr>
<td>static.syslog.log_upload_period</td>
<td></td>
</tr>
<tr>
<td>static.syslog.ftp.post_mode</td>
<td></td>
</tr>
<tr>
<td>static.syslog.ftp.max_logfile</td>
<td></td>
</tr>
<tr>
<td>static.syslog.ftp.append_limit_mode</td>
<td></td>
</tr>
<tr>
<td>static.syslog.bootlog_upload_wait_time</td>
<td></td>
</tr>
<tr>
<td>Watch_dog</td>
<td>static.watch_dog.enable</td>
</tr>
<tr>
<td>WEB HTTP(S)</td>
<td>static.wui.https_enable</td>
</tr>
<tr>
<td></td>
<td>static.wui.http_enable</td>
</tr>
<tr>
<td>Language</td>
<td>static.lang.wui</td>
</tr>
<tr>
<td></td>
<td>static.lang.gui</td>
</tr>
<tr>
<td>Others</td>
<td>static.firmware.url</td>
</tr>
<tr>
<td></td>
<td>static.features.default_account</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>T58V/A</th>
<th>T56A</th>
<th>CP960</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Network" /></td>
<td><img src="image" alt="Network" /></td>
<td><img src="image" alt="Network" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Private Line" /></td>
<td><img src="image" alt="Private Line" /></td>
<td><img src="image" alt="Private Line" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Registration Failed" /></td>
<td><img src="image" alt="Registration Failed" /></td>
<td><img src="image" alt="Registration Failed" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Registering" /></td>
<td><img src="image" alt="Registering" /></td>
<td><img src="image" alt="Registering" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Hands-free (Speakerphone) Mode" /></td>
<td><img src="image" alt="Hands-free (Speakerphone) Mode" /></td>
<td><img src="image" alt="Hands-free (Speakerphone) Mode" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Handset Mode" /></td>
<td><img src="image" alt="Handset Mode" /></td>
<td><img src="image" alt="Handset Mode" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Headset Mode" /></td>
<td><img src="image" alt="Headset Mode" /></td>
<td><img src="image" alt="Headset Mode" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Voice Mail" /></td>
<td><img src="image" alt="Voice Mail" /></td>
<td><img src="image" alt="Voice Mail" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Auto Answer" /></td>
<td><img src="image" alt="Auto Answer" /></td>
<td><img src="image" alt="Auto Answer" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Do Not Disturb" /></td>
<td><img src="image" alt="Do Not Disturb" /></td>
<td><img src="image" alt="Do Not Disturb" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Call Forward" /></td>
<td><img src="image" alt="Call Forward" /></td>
<td><img src="image" alt="Call Forward" /></td>
</tr>
<tr>
<td></td>
<td>![Call Hold (Video)]</td>
<td>![Call Hold (Video)]</td>
<td>![Call Hold (Video)]</td>
</tr>
<tr>
<td></td>
<td>![Call Hold (Audio-only)]</td>
<td>![Call Hold (Audio-only)]</td>
<td>![Call Hold (Audio-only)]</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Call Mute" /></td>
<td><img src="image" alt="Call Mute" /></td>
<td><img src="image" alt="Call Mute" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Keep Mute" /></td>
<td><img src="image" alt="Keep Mute" /></td>
<td><img src="image" alt="Keep Mute" /></td>
</tr>
<tr>
<td></td>
<td>![Call is Encrypted (Video)]</td>
<td>![Call is Encrypted (Video)]</td>
<td>![Call is Encrypted (Video)]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-----</td>
<td>-------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td><img src="image" alt="Lock" /></td>
<td><img src="image" alt="Lock" /></td>
<td><img src="image" alt="Lock" /></td>
<td>Call is encrypted (audio-only)</td>
</tr>
<tr>
<td><img src="image" alt="Speaker Mute" /></td>
<td><img src="image" alt="Speaker Mute" /></td>
<td><img src="image" alt="Speaker Mute" /></td>
<td>Silent mode</td>
</tr>
<tr>
<td><img src="image" alt="Camera Off" /></td>
<td><img src="image" alt="Camera Off" /></td>
<td><img src="image" alt="Camera Off" /></td>
<td>Camera is not detected</td>
</tr>
<tr>
<td><img src="image" alt="Phone Lock" /></td>
<td><img src="image" alt="Phone Lock" /></td>
<td><img src="image" alt="Phone Lock" /></td>
<td>Phone Lock</td>
</tr>
<tr>
<td><img src="image" alt="Received Calls" /></td>
<td><img src="image" alt="Received Calls" /></td>
<td><img src="image" alt="Received Calls" /></td>
<td>Received Calls</td>
</tr>
<tr>
<td><img src="image" alt="Placed Calls" /></td>
<td><img src="image" alt="Placed Calls" /></td>
<td><img src="image" alt="Placed Calls" /></td>
<td>Placed Calls</td>
</tr>
<tr>
<td><img src="image" alt="Missed Calls" /></td>
<td><img src="image" alt="Missed Calls" /></td>
<td><img src="image" alt="Missed Calls" /></td>
<td>Missed Calls</td>
</tr>
<tr>
<td><img src="image" alt="Forwarded Calls" /></td>
<td><img src="image" alt="Forwarded Calls" /></td>
<td><img src="image" alt="Forwarded Calls" /></td>
<td>Forwarded Calls</td>
</tr>
<tr>
<td><img src="image" alt="Recording Box Full" /></td>
<td><img src="image" alt="Recording Box Full" /></td>
<td><img src="image" alt="Recording Box Full" /></td>
<td>Recording box is full</td>
</tr>
<tr>
<td><img src="image" alt="Recording Cannot Be Recorded" /></td>
<td><img src="image" alt="Recording Cannot Be Recorded" /></td>
<td><img src="image" alt="Recording Cannot Be Recorded" /></td>
<td>A call cannot be recorded</td>
</tr>
<tr>
<td><img src="image" alt="Recording Started" /></td>
<td><img src="image" alt="Recording Started" /></td>
<td><img src="image" alt="Recording Started" /></td>
<td>Recording starts successfully</td>
</tr>
<tr>
<td><img src="image" alt="Recording Cannot Be Started" /></td>
<td><img src="image" alt="Recording Cannot Be Started" /></td>
<td><img src="image" alt="Recording Cannot Be Started" /></td>
<td>Recording cannot be started</td>
</tr>
<tr>
<td><img src="image" alt="Recording Cannot Be Stopped" /></td>
<td><img src="image" alt="Recording Cannot Be Stopped" /></td>
<td><img src="image" alt="Recording Cannot Be Stopped" /></td>
<td>Recording cannot be stopped</td>
</tr>
<tr>
<td><img src="image" alt="VPN Enabled" /></td>
<td><img src="image" alt="VPN Enabled" /></td>
<td><img src="image" alt="VPN Enabled" /></td>
<td>VPN is enabled</td>
</tr>
<tr>
<td><img src="image" alt="Bluetooth Mode On" /></td>
<td><img src="image" alt="Bluetooth Mode On" /></td>
<td><img src="image" alt="Bluetooth Mode On" /></td>
<td>Bluetooth mode is on</td>
</tr>
<tr>
<td><img src="image" alt="Bluetooth Headset Connected" /></td>
<td><img src="image" alt="Bluetooth Headset Connected" /></td>
<td><img src="image" alt="Bluetooth Headset Connected" /></td>
<td>Bluetooth headset is both paired and connected</td>
</tr>
<tr>
<td><img src="image" alt="Bluetooth-Enabled Mobile Phone Connected" /></td>
<td><img src="image" alt="Bluetooth-Enabled Mobile Phone Connected" /></td>
<td><img src="image" alt="Bluetooth-Enabled Mobile Phone Connected" /></td>
<td>Bluetooth-Enabled mobile phone is both paired and connected</td>
</tr>
<tr>
<td><img src="image" alt="Wi-Fi Mode On" /></td>
<td><img src="image" alt="Wi-Fi Mode On" /></td>
<td><img src="image" alt="Wi-Fi Mode On" /></td>
<td>Wi-Fi mode is on</td>
</tr>
<tr>
<td><img src="image" alt="Default Local Caller Photo" /></td>
<td><img src="image" alt="Default Local Caller Photo" /></td>
<td><img src="image" alt="Default Local Caller Photo" /></td>
<td>The default local caller photo and local contact icon</td>
</tr>
<tr>
<td><img src="image" alt="Default Mobile Caller Photo" /></td>
<td><img src="image" alt="Default Mobile Caller Photo" /></td>
<td><img src="image" alt="Default Mobile Caller Photo" /></td>
<td>The default mobile caller photo and mobile contacts icon</td>
</tr>
<tr>
<td>T58V/A</td>
<td>T56A</td>
<td>CP960</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="Image1.png" alt="Image" /></td>
<td><img src="Image2.png" alt="Image" /></td>
<td>/</td>
<td>DSS Key</td>
</tr>
<tr>
<td><img src="Image3.png" alt="Image" /></td>
<td><img src="Image4.png" alt="Image" /></td>
<td><img src="Image5.png" alt="Image" /></td>
<td>Line key type is Line (line is seized)</td>
</tr>
<tr>
<td><img src="Image6.png" alt="Image" /></td>
<td><img src="Image7.png" alt="Image" /></td>
<td><img src="Image8.png" alt="Image" /></td>
<td>Line key type is Speed Dial</td>
</tr>
<tr>
<td><img src="Image9.png" alt="Image" /></td>
<td><img src="Image10.png" alt="Image" /></td>
<td><img src="Image11.png" alt="Image" /></td>
<td>Line key type is Mobile Account (Bluetooth-Enabled mobile phone is connected successfully)</td>
</tr>
<tr>
<td><img src="Image12.png" alt="Image" /></td>
<td><img src="Image13.png" alt="Image" /></td>
<td><img src="Image14.png" alt="Image" /></td>
<td>Line key type is Mobile Account (Bluetooth-Enabled mobile phone connection failed)</td>
</tr>
<tr>
<td><img src="Image15.png" alt="Image" /></td>
<td><img src="Image16.png" alt="Image" /></td>
<td><img src="Image17.png" alt="Image" /></td>
<td>Line key type is Mobile Account (Bluetooth-Enabled mobile phone is connecting)</td>
</tr>
<tr>
<td><img src="Image18.png" alt="Image" /></td>
<td><img src="Image19.png" alt="Image" /></td>
<td><img src="Image20.png" alt="Image" /></td>
<td>Line key type is BLF/BLF List (BLF/BLF list idle state)</td>
</tr>
<tr>
<td><img src="Image21.png" alt="Image" /></td>
<td><img src="Image22.png" alt="Image" /></td>
<td><img src="Image23.png" alt="Image" /></td>
<td>Line key type is BLF/BLF List (BLF/BLF list ringing state)</td>
</tr>
<tr>
<td><img src="Image24.png" alt="Image" /></td>
<td><img src="Image25.png" alt="Image" /></td>
<td><img src="Image26.png" alt="Image" /></td>
<td>Line key type is BLF/BLF List (BLF hold state)</td>
</tr>
<tr>
<td><img src="Image27.png" alt="Image" /></td>
<td><img src="Image28.png" alt="Image" /></td>
<td><img src="Image29.png" alt="Image" /></td>
<td>Line key type is BLF/BLF List (BLF/BLF list callout state)</td>
</tr>
<tr>
<td><img src="Image30.png" alt="Image" /></td>
<td><img src="Image31.png" alt="Image" /></td>
<td><img src="Image32.png" alt="Image" /></td>
<td>Line key type is BLF/BLF List (BLF/BLF list failed state)</td>
</tr>
<tr>
<td><img src="Image33.png" alt="Image" /></td>
<td><img src="Image34.png" alt="Image" /></td>
<td><img src="Image35.png" alt="Image" /></td>
<td>Line key type is BLF/BLF List (BLF list call park state)</td>
</tr>
<tr>
<td><img src="Image36.png" alt="Image" /></td>
<td><img src="Image37.png" alt="Image" /></td>
<td><img src="Image38.png" alt="Image" /></td>
<td>Line key type is Voice Mail</td>
</tr>
<tr>
<td><img src="Image39.png" alt="Image" /></td>
<td><img src="Image40.png" alt="Image" /></td>
<td><img src="Image41.png" alt="Image" /></td>
<td>Line key type is Direct Pickup</td>
</tr>
<tr>
<td><img src="Image42.png" alt="Image" /></td>
<td><img src="Image43.png" alt="Image" /></td>
<td><img src="Image44.png" alt="Image" /></td>
<td>Line key type is Group Pickup</td>
</tr>
<tr>
<td><img src="Image45.png" alt="Image" /></td>
<td><img src="Image46.png" alt="Image" /></td>
<td><img src="Image47.png" alt="Image" /></td>
<td>Line key type is Call Park (park successfully/call park idle state)</td>
</tr>
<tr>
<td><img src="Image48.png" alt="Image" /></td>
<td><img src="Image49.png" alt="Image" /></td>
<td><img src="Image50.png" alt="Image" /></td>
<td>Line key type is Call Park (call park ringing state)</td>
</tr>
<tr>
<td><img src="Image51.png" alt="Image" /></td>
<td><img src="Image52.png" alt="Image" /></td>
<td><img src="Image53.png" alt="Image" /></td>
<td>Park failed</td>
</tr>
<tr>
<td><img src="Image54.png" alt="Image" /></td>
<td><img src="Image55.png" alt="Image" /></td>
<td><img src="Image56.png" alt="Image" /></td>
<td>Line key type is Intercom (intercom idle state)</td>
</tr>
<tr>
<td>T58V/A</td>
<td>T56A</td>
<td>CP960</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>![Callout]</td>
<td>![Callout]</td>
<td>![Callout]</td>
<td>Line key type is Intercom (intercom ringing state)</td>
</tr>
<tr>
<td>![Talking]</td>
<td>![Talking]</td>
<td>![Talking]</td>
<td>Line key type is Intercom (intercom callout state)</td>
</tr>
<tr>
<td>![Talking]</td>
<td>![Talking]</td>
<td>![Talking]</td>
<td>Line key type is Intercom (intercom talking state)</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Intercom (intercom failed state)</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is DTMF/Prefix</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Local Group/XML Group/LDAP</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is XML Browser</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Conference</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Forward</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Transfer</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Hold</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is DND</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Recall</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Record/XML Record</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Record/XML Record (recording starts successfully)</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Multicast Paging/Group Listening (Group Listening is not applicable CP960 IP phones)</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Hot Desking</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is Zero Touch</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>Line key type is URL</td>
</tr>
<tr>
<td>![]</td>
<td>![]</td>
<td>![]</td>
<td>The ACD state is available</td>
</tr>
<tr>
<td>T58V/A</td>
<td>T56A</td>
<td>CP960</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image1" alt="icon" /> <img src="image2" alt="icon" /></td>
<td><img src="image3" alt="icon" /></td>
<td>/</td>
<td>The ACD state is unavailable</td>
</tr>
<tr>
<td><img src="image4" alt="icon" /> <img src="image5" alt="icon" /></td>
<td><img src="image6" alt="icon" /></td>
<td>/</td>
<td>The ACD state is wrap up</td>
</tr>
<tr>
<td><img src="image7" alt="icon" /></td>
<td><img src="image8" alt="icon" /></td>
<td>/</td>
<td>Log out of the ACD system</td>
</tr>
<tr>
<td><img src="image9" alt="icon" /> <img src="image10" alt="icon" /></td>
<td><img src="image11" alt="icon" /> <img src="image12" alt="icon" /></td>
<td>/</td>
<td>The shared line/bridged line is idle</td>
</tr>
<tr>
<td><img src="image13" alt="icon" /> <img src="image14" alt="icon" /> (Flashing)</td>
<td><img src="image15" alt="icon" /> <img src="image16" alt="icon" /> (Flashing)</td>
<td><img src="image17" alt="icon" /> <img src="image18" alt="icon" /> (Flashing)</td>
<td>The shared line receives ring-back tone</td>
</tr>
<tr>
<td><img src="image19" alt="icon" /> <img src="image20" alt="icon" /> (Flashing)</td>
<td><img src="image21" alt="icon" /> <img src="image22" alt="icon" /> (Flashing)</td>
<td><img src="image23" alt="icon" /> <img src="image24" alt="icon" /> (Flashing)</td>
<td>The shared line receives an incoming call</td>
</tr>
<tr>
<td><img src="image25" alt="icon" /> <img src="image26" alt="icon" /></td>
<td><img src="image27" alt="icon" /> <img src="image28" alt="icon" /></td>
<td><img src="image29" alt="icon" /> <img src="image30" alt="icon" /></td>
<td>The shared line is in conversation</td>
</tr>
<tr>
<td><img src="image31" alt="icon" /> <img src="image32" alt="icon" /></td>
<td><img src="image33" alt="icon" /> <img src="image34" alt="icon" /></td>
<td><img src="image35" alt="icon" /> <img src="image36" alt="icon" /></td>
<td>The shared line conversation is placed on public hold</td>
</tr>
<tr>
<td><img src="image37" alt="icon" /> <img src="image38" alt="icon" /></td>
<td><img src="image39" alt="icon" /> <img src="image40" alt="icon" /></td>
<td><img src="image41" alt="icon" /> <img src="image42" alt="icon" /></td>
<td>USB flash drive is detected</td>
</tr>
<tr>
<td><img src="image43" alt="icon" /> <img src="image44" alt="icon" /></td>
<td><img src="image45" alt="icon" /> <img src="image46" alt="icon" /></td>
<td><img src="image47" alt="icon" /> <img src="image48" alt="icon" /></td>
<td>High Definition Voice</td>
</tr>
<tr>
<td><img src="image49" alt="icon" /> <img src="image50" alt="icon" /></td>
<td><img src="image51" alt="icon" /> <img src="image52" alt="icon" /></td>
<td>/</td>
<td>Screenshot captured</td>
</tr>
<tr>
<td><img src="image53" alt="icon" /> <img src="image54" alt="icon" /></td>
<td><img src="image55" alt="icon" /> <img src="image56" alt="icon" /></td>
<td>/</td>
<td>Downloading file</td>
</tr>
<tr>
<td><img src="image57" alt="icon" /> <img src="image58" alt="icon" /></td>
<td><img src="image59" alt="icon" /> <img src="image60" alt="icon" /></td>
<td>/</td>
<td>Uploading file</td>
</tr>
<tr>
<td><img src="image61" alt="icon" /> <img src="image62" alt="icon" /></td>
<td><img src="image63" alt="icon" /> <img src="image64" alt="icon" /></td>
<td>/</td>
<td>Upcoming alarm</td>
</tr>
<tr>
<td><img src="image65" alt="icon" /> <img src="image66" alt="icon" /></td>
<td><img src="image67" alt="icon" /> <img src="image68" alt="icon" /></td>
<td>/</td>
<td>Unread email</td>
</tr>
</tbody>
</table>
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
Appendix

- 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
SIP Request

The following SIP request messages are supported:

<table>
<thead>
<tr>
<th>Method</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGISTER</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>INVITE</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>ACK</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CANCEL</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>BYE</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>OPTIONS</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SUBSCRIBE</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>NOTIFY</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>REFER</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PRACK</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>INFO</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>MESSAGE</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>UPDATE</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### SIP Header

The following SIP request headers are supported:

<table>
<thead>
<tr>
<th>Method</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Alert-Info</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Allow-Events</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Authorization</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Call-ID</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Call-Info</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Contact</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Content-Length</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CSeq</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Diversion</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>History-Info</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Expires</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>From</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Max-Forwards</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Min-SE</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>P-Asserted-Identity</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>P-Preferred-Identity</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Proxy-Authenticate</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Proxy-Authorization</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

In the following table, a “Yes” in the Supported column means the header is sent and properly parsed.
<table>
<thead>
<tr>
<th>Method</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAck</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Record-Route</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Refer-To</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Referred-By</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Remote-Party-ID</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Replaces-ID</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Require</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Route</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>RSeq</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Session-Expires</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Subscription-State</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Supported</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>To</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User-Agent</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Via</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>1xx Response</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 Trying</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>180 Ringing</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>181 Call Is Being Forwarded</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>182 Queued</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>183 Session Progress</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### 2xx Responses—Successful

<table>
<thead>
<tr>
<th>2xx Response</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>202 Accepted</td>
<td>Yes</td>
<td>In REFER transfer.</td>
</tr>
</tbody>
</table>

### 3xx Responses—Redirection

<table>
<thead>
<tr>
<th>3xx Response</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>300 Multiple Choices</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>301 Moved Permanently</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>302 Moved Temporarily</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>305 Use Proxy</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>380 Alternative Service</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### 4xx Responses—Request Failure

<table>
<thead>
<tr>
<th>4xx Response</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>400 Bad Request</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>401 Unauthorized</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>402 Payment Required</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>403 Forbidden</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>404 Not Found</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>405 Method Not Allowed</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>406 Not Acceptable</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>407 Proxy Authentication Required</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>408 Request Timeout</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>409 Conflict</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>410 Gone</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>411 Length Required</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>413 Request Entity Too Large</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>414 Request-URI Too Long</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>415 Unsupported Media Type</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>4xx Response</td>
<td>Supported</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-----------</td>
<td>-------</td>
</tr>
<tr>
<td>416 Unsupported URI Scheme</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>420 Bad Extension</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>421 Extension Required</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>423 Interval Too Brief</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>480 Temporarily Unavailable</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>481 Call/Transaction Does Not Exist</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>482 Loop Detected</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>483 Too Many Hops</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>484 Address Incomplete</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>485 Ambiguous</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>486 Busy Here</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>487 Request Terminated</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>488 Not Acceptable Here</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>491 Request Pending</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>493 Undecipherable</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**5xx Responses—Server Failure**

<table>
<thead>
<tr>
<th>5xx Response</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 Server Internal Error</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>501 Not Implemented</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>502 Bad Gateway</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>503 Service Unavailable</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>504 Server Time-out</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>505 Version Not Supported</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>513 Message Too Large</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**6xx Response—Global Failures**

<table>
<thead>
<tr>
<th>6xx Response</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>600 Busy Everywhere</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### 6xx Response

<table>
<thead>
<tr>
<th>6xx Response</th>
<th>Supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>603 Decline</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>604 Does Not Exist Anywhere</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>606 Not Acceptable</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### SIP Session Description Protocol (SDP) Usage

<table>
<thead>
<tr>
<th>SDP Headers</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>v—Session Description Protocol Version</td>
<td>Yes</td>
</tr>
<tr>
<td>o—Owner/Creator, Session Id</td>
<td>Yes</td>
</tr>
<tr>
<td>a—Media Attribute</td>
<td>Yes</td>
</tr>
<tr>
<td>c—Connection Information</td>
<td>Yes</td>
</tr>
<tr>
<td>b—Bandwidth Information</td>
<td>Yes</td>
</tr>
<tr>
<td>m—Media Description, name and address</td>
<td>Yes</td>
</tr>
<tr>
<td>s—Session Name</td>
<td>Yes</td>
</tr>
<tr>
<td>t—Time Description, active time</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### 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
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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 leader. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>initiator in the From field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The transaction number within a single call leg is identified in the CSeq field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The media capability User A is ready to receive is specified.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The port on which User B is prepared to receive the RTP data is specified.</td>
</tr>
<tr>
<td>F2</td>
<td>INVITE—Proxy Server to User B</td>
<td>The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.</td>
</tr>
<tr>
<td>F3</td>
<td>100 Trying—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F4</td>
<td>100 Trying—Proxy Server to User A</td>
<td>The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has been received by User B.</td>
</tr>
<tr>
<td>F5</td>
<td>180 Ringing—User B to Proxy Server</td>
<td>User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the User B is being alerted.</td>
</tr>
<tr>
<td>F6</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F7</td>
<td>200 OK—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F8</td>
<td>200 OK—Proxy Server to User A</td>
<td>The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.</td>
</tr>
</tbody>
</table>
| 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
### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
<p>| 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 |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>indicates that the INVITE request has been received by User B.</td>
</tr>
<tr>
<td>F4</td>
<td>100 Trying—Proxy Server to User A</td>
<td>The proxy server forwards the SIP 100 Trying to User A to indicate that the INVITE request has already been received.</td>
</tr>
<tr>
<td>F5</td>
<td>486 Busy Here—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F6</td>
<td>486 Busy Here—Proxy Server to User A</td>
<td>The proxy server forwards the 486 Busy Here response to notify User A that User B is busy.</td>
</tr>
<tr>
<td>F7</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F8</td>
<td>ACK—Proxy Server to User B</td>
<td>The proxy server forwards the SIP ACK to User B to indicate that the 486 Busy Here message has already been received.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F4</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F5</td>
<td>CANCEL—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F6</td>
<td>CANCEL—Proxy Server to User B</td>
<td>The proxy server forwards the SIP CANCEL request to notify User B that User A wants to disconnect the call.</td>
</tr>
<tr>
<td>F7</td>
<td>200 OK—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F8</td>
<td>200 OK—Proxy Server to User A</td>
<td>The proxy server forwards the SIP 200 OK response to notify User A that the CANCEL request has been processed successfully.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
|      |        | ● 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 |
### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F12</td>
<td>200 OK—Proxy Server to User A</td>
<td>The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on hold.</td>
</tr>
<tr>
<td>F13</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F14</td>
<td>ACK—Proxy Server to User B</td>
<td>The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.</td>
</tr>
</tbody>
</table>
4. User B accepts the call from User C.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F2</td>
<td>INVITE—Proxy Server to User B</td>
<td>The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.</td>
</tr>
<tr>
<td>F3</td>
<td>180 Ringing—User B to Proxy Server</td>
<td>User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F4</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F5</td>
<td>200 OK—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F6</td>
<td>200 OK—Proxy Server to User A</td>
<td>The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.</td>
</tr>
<tr>
<td>F7</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F8</td>
<td>ACK—Proxy Server to User B</td>
<td>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.</td>
</tr>
<tr>
<td>F9</td>
<td>INVITE—User C to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>F10</td>
<td>INVITE—Proxy Server to User A</td>
<td>The proxy server maps the SIP URI in the To field to User A. The proxy server sends the INVITE message to User A.</td>
</tr>
<tr>
<td>F11</td>
<td>180 Ringing—User A to Proxy Server</td>
<td>User A sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F12</td>
<td>180 Ringing—Proxy Server to User C</td>
<td>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.</td>
</tr>
<tr>
<td>F13</td>
<td>INVITE—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F14</td>
<td>INVITE—Proxy Server to User B</td>
<td>The proxy server forwards the mid-call INVITE message to User B.</td>
</tr>
<tr>
<td>F15</td>
<td>200 OK—User B to Proxy Server</td>
<td>User B sends a 200 OK to the proxy server. The 200 OK response indicates that the INVITE was successfully processed.</td>
</tr>
<tr>
<td>F16</td>
<td>200 OK—Proxy Server to User A</td>
<td>The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on session.</td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |
## Administrator’s Guide for SIP-T5 Series Smart Media Phones

### 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
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F11</td>
<td>REFER—Proxy Server to User A</td>
<td>The proxy server forwards the REFER message to User A.</td>
</tr>
<tr>
<td>F12</td>
<td>202 Accepted—User A to Proxy Server</td>
<td>User A sends a SIP 202 Accept response to the proxy server. The 202 Accepted response indicates that User A accepts the transfer.</td>
</tr>
<tr>
<td>F13</td>
<td>BYE—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F14</td>
<td>BYE—Proxy Server to User A</td>
<td>The proxy server forwards the BYE request to User A.</td>
</tr>
<tr>
<td>F15</td>
<td>200OK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F16</td>
<td>200OK—Proxy Server to User B</td>
<td>The proxy server forwards the SIP 200 OK response to User B.</td>
</tr>
<tr>
<td>F17</td>
<td>INVITE—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F18</td>
<td>INVITE—Proxy Server to User C</td>
<td>The proxy server maps the SIP URI in the To field to User C.</td>
</tr>
<tr>
<td>F19</td>
<td>180 Ringing—User C to Proxy Server</td>
<td>User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F20</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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</td>
</tr>
<tr>
<td>F21</td>
<td>200OK—User C to Proxy Server</td>
<td>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.</td>
</tr>
</tbody>
</table>
The following table illustrates the steps in the call flow scenario:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F22</td>
<td>200OK—Proxy Server to User A</td>
<td>The proxy server forwards the SIP 200 OK response to User A.</td>
</tr>
<tr>
<td>F23</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F24</td>
<td>ACK—Proxy Server to User C</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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.
Appendix

Call is established between User B and User C.

User A

Proxy Server

User B

User C

F1. INVITE B

F1. INVITE B

F2. INVITE B

F2. INVITE B

F3. 180 Ringing

F3. 180 Ringing

F4. 180 Ringing

F4. 180 Ringing

F5. 200 OK

F5. 200 OK

F6. 200 OK

F6. 200 OK

F7. ACK

F7. ACK

F8. ACK

F8. ACK

2-way RTP channel established

2-way RTP channel established

F9. INVITE B (sendonly)

F10. INVITE B (sendonly)

F11. 200 OK

F11. 200 OK

F12. 200 OK

F12. 200 OK

F13. ACK

F13. ACK

F14. ACK

F14. ACK

F15. INVITE C

F16. INVITE C

F17. 180 Ringing

F18. 180 Ringing

F19. 200 OK

F19. 200 OK

F20. 200 OK

F20. 200 OK

F21. ACK

F21. ACK

F22. ACK

F22. ACK

F23. REFER

F24. 202 Accepted

F25. REFER

F26. 202 Accepted

F23. REFER

F24. 202 Accepted

F25. REFER

F26. 202 Accepted

F27. REFER

F28. 202 Accepted

F29. REFER

F30. 202 Accepted

F31. BYE

F32. BYE

F33. 200 OK

F34. 200 OK

F34. 200 OK

2-way RTP channel established

2-way RTP channel established

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...
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>initiator in the From field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A unique numeric identifier is assigned to the call and is inserted in the Call-ID field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The transaction number within a single call leg is identified in the CSeq field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The media capability User A is ready to receive is specified.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The port on which User B is prepared to receive the RTP data is specified.</td>
</tr>
<tr>
<td>F2</td>
<td>INVITE—Proxy Server to User B</td>
<td>The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.</td>
</tr>
<tr>
<td>F3</td>
<td>180 Ringing—User B to Proxy Server</td>
<td>User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F4</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F5</td>
<td>200 OK—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F6</td>
<td>200 OK—Proxy Server to User A</td>
<td>The proxy server forwards the 200 OK message to User A. The 200 OK response notifies User A that the connection has been made.</td>
</tr>
<tr>
<td>F7</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F8</td>
<td>ACK—Proxy Server to User B</td>
<td>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.</td>
</tr>
<tr>
<td>F9</td>
<td>INVITE—User A to Proxy Server</td>
<td>User A sends a mid-call INVITE request to the proxy server with new SDP session parameters, which are used to place the call</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>F10</td>
<td>INVITE—Proxy Server to User B</td>
<td>The proxy server forwards the mid-call INVITE message to User B.</td>
</tr>
<tr>
<td>F11</td>
<td>200 OK—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F12</td>
<td>200 OK—Proxy Server to User A</td>
<td>The proxy server forwards the 200 OK response to User A. The 200 OK response notifies User B is successfully placed on hold.</td>
</tr>
<tr>
<td>F13</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F14</td>
<td>ACK—Proxy Server to User B</td>
<td>The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.</td>
</tr>
<tr>
<td>F15</td>
<td>INVITE—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F16</td>
<td>INVITE—Proxy Server to User C</td>
<td>The proxy server maps the SIP URI in the To field to User C. The proxy server sends the INVITE request to User C.</td>
</tr>
<tr>
<td>F17</td>
<td>180 Ringing—User C to Proxy Server</td>
<td>User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F18</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F19</td>
<td>200OK—User C to Proxy Server</td>
<td>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.</td>
</tr>
</tbody>
</table>
| F20  | 200OK—Proxy Server to User A   | The proxy server forwards the SIP 200 OK.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F21</td>
<td>ACK— User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F22</td>
<td>ACK—Proxy Server to User C</td>
<td>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.</td>
</tr>
<tr>
<td>F23</td>
<td>REFER—User A to Proxy Server</td>
<td>User A sends a REFER message to the proxy server. User A performs a transfer of User B to User C.</td>
</tr>
<tr>
<td>F24</td>
<td>202 Accepted—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F25</td>
<td>REFER—Proxy Server to User B</td>
<td>The proxy server forwards the REFER message to User B.</td>
</tr>
<tr>
<td>F26</td>
<td>202 Accepted—User B to Proxy Server</td>
<td>User B sends a SIP 202 Accept response to the proxy server. The 202 Accepted response indicates that User B accepts the transfer.</td>
</tr>
<tr>
<td>F27</td>
<td>BYE—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F28</td>
<td>BYE—Proxy Server to User B</td>
<td>The proxy server forwards the BYE request to User B.</td>
</tr>
<tr>
<td>F29</td>
<td>200OK—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F30</td>
<td>200OK—Proxy Server to User A</td>
<td>The proxy server forwards the SIP 200 OK response to User A.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F2</td>
<td>INVITE—Proxy Server to User B</td>
<td>The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.</td>
</tr>
<tr>
<td>F3</td>
<td>302 Move Temporarily—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F4</td>
<td>ACK—Proxy Server to User B</td>
<td>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.</td>
</tr>
<tr>
<td>F5</td>
<td>302 Move Temporarily—Proxy Server to User A</td>
<td>The proxy server forwards the 302 Moved Temporarily message to User A.</td>
</tr>
<tr>
<td>F6</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F7</td>
<td>INVITE—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F8</td>
<td>INVITE—Proxy Server to User C</td>
<td>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.</td>
</tr>
<tr>
<td>F9</td>
<td>180 Ringing—User C to Proxy</td>
<td>User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>The port on which User B is prepared to receive the RTP data is specified.</td>
</tr>
<tr>
<td>F2</td>
<td>INVITE—Proxy Server to User B</td>
<td>The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.</td>
</tr>
<tr>
<td>F3</td>
<td>180 Ringing—User B to Proxy Server</td>
<td>User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F4</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F5</td>
<td>302 Move Temporarily—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F6</td>
<td>ACK—Proxy Server to User B</td>
<td>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.</td>
</tr>
<tr>
<td>F7</td>
<td>302 Move Temporarily—Proxy Server to User A</td>
<td>The proxy server forwards the 302 Moved Temporarily message to User A.</td>
</tr>
<tr>
<td>F8</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F9</td>
<td>INVITE—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F10</td>
<td>INVITE—Proxy Server to User C</td>
<td>The proxy server forwards the SIP INVITE request to User C.</td>
</tr>
<tr>
<td>F11</td>
<td>180 Ringing—User C to Proxy Server</td>
<td>User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F12</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F13</td>
<td>200OK—User C to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F14</td>
<td>200OK—Proxy Server to User A</td>
<td>The proxy server forwards the SIP 200 OK response to User A.</td>
</tr>
<tr>
<td>F15</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F16</td>
<td>ACK—Proxy Server to User C</td>
<td>The proxy server sends the ACK message to User C.</td>
</tr>
</tbody>
</table>
Call is established between User A and User C.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F2</td>
<td>INVITE—Proxy Server to User B</td>
<td>The proxy server maps the SIP URI in the To field to User B. The proxy server sends the INVITE message to User B.</td>
</tr>
<tr>
<td>F3</td>
<td>180 Ringing—User B to Proxy Server</td>
<td>User B sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F4</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F5</td>
<td>302 Move Temporarily—User B to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F6</td>
<td>ACK—Proxy Server to User B</td>
<td>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.</td>
</tr>
<tr>
<td>F7</td>
<td>302 Move Temporarily—Proxy Server to User A</td>
<td>The proxy server forwards the 302 Moved Temporarily message to User A.</td>
</tr>
<tr>
<td>F8</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F9</td>
<td>INVITE—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F10</td>
<td>INVITE—Proxy Server to User C</td>
<td>The proxy server forwards the SIP INVITE request to User C.</td>
</tr>
<tr>
<td>F11</td>
<td>180 Ringing—User C to Proxy Server</td>
<td>User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F12</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F13</td>
<td>200OK–User C to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F14</td>
<td>200OK–Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F15</td>
<td>ACK– User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F16</td>
<td>ACK–Proxy Server to User C</td>
<td>The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.</td>
</tr>
</tbody>
</table>
6. User A mixes the RTP channels and establishes a conference between User B and User C.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 |
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
|     |        | single call leg is identified in the CSeq field.  
|     |        | • The media capability User A is ready to receive is specified.  
<p>|     |        | • 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 |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F12</td>
<td>200 OK—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F13</td>
<td>ACK—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F14</td>
<td>ACK—Proxy Server to User B</td>
<td>The proxy server sends the ACK message to User B. The ACK confirms that the proxy server has received the 200 OK response.</td>
</tr>
<tr>
<td>F15</td>
<td>INVITE—User A to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F16</td>
<td>INVITE—Proxy Server to User C</td>
<td>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.</td>
</tr>
<tr>
<td>F17</td>
<td>180 Ringing—User C to Proxy Server</td>
<td>User C sends a SIP 180 Ringing response to the proxy server. The 180 Ringing response indicates that the user is being alerted.</td>
</tr>
<tr>
<td>F18</td>
<td>180 Ringing—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F19</td>
<td>200OK—User C to Proxy Server</td>
<td>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.</td>
</tr>
<tr>
<td>F20</td>
<td>200OK—Proxy Server to User A</td>
<td>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.</td>
</tr>
<tr>
<td>F21</td>
<td>ACK— User A to Proxy Server</td>
<td>User A sends a SIP ACK to the proxy server.</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>F22</td>
<td>ACK—Proxy Server to User C</td>
<td>The ACK confirms that User A has received the 200 OK response. The call session is now active.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The proxy server sends the ACK message to User C. The ACK confirms that the proxy server has received the 200 OK response.</td>
</tr>
</tbody>
</table>
Index

Numeric
100 Reliable Retransmission 444
180 Ring Workaround 330
802.1X Authentication 99

A
About This Guide v
Accept SIP Trust Server Only 302
Account Registration 171
Automatic Call Distribution (ACD) 516
Acoustic Echo Cancellation (AEC) 672
Action URL 568
Action URI 588
Allow IP Call 300
Always Forward 344
Analyzing Configuration Files 772
Anonymous Call 306
Anonymous Call Rejection 310
Answer By Hand 448
Appendix 797
Appendix A: Glossary 797
Appendix B: Time Zones 799
Appendix C: Trusted Certificates 800
Appendix D: Configuring DSS Keys 805
Appendix E: Auto Provisioning Flowchart 815
Appendix F: Static Settings 817
Appendix G: Reading Icons 823
Appendix H: SIP 828
Appendix I: SIP Call Flows 836
Area Code 237
Attended Transfer 359
Audio Codecs 661
Auto Answer 294
Auto-Logout Time 721
Automatic Gain Control (AGC) 674
Auto Redial 291

B
Backlight 156
Background Noise Suppression (BNS) 673
Blind Transfer 359
Block Out 240
Bluetooth 164
Boot Files, Configuration Files and Resource Files 114
Busy Forward 344
Busy Lamp Field (BLF) 494
Busy Lamp Field (BLF) List 508
Busy Tone Delay 322

C
Call Completion 303
Call Forward 344
Call Hold 338
Call Number Filter 400
Call Park 401
Call Timeout 432
Call Transfer 359
Call Recording Using DSS Keys (Record and URL Record) 552
Call Recording Using Soft Key 449
Call Waiting 288
Calling Line Identification Presentation (CLIP) 412
Central Provisioning 112
Connected Line Identification Presentation (COIP) 417
Capturing Packets 765
Capturing the Current Screen of the Phone 594
CDP 57
Chapters in This Guide v
Comfort Noise Generation (CNG) 675
Common CFG Files 116
Configuration Parameter Table Format ix
Configuring a Provisioning Server 122
Administrator's Guide for SIP-T5 Series Smart Media Phones

Configuring Audio Features 633
Configuring Advanced Features 450
Configuring Basic Features 143
Configuring Video Features 681
Configuring Security Features 719
Connecting the IP phone 10
Conventions Used in Yealink Documentations vii
CSTA Control 471

D
Deploying Phones from the Provisioning Server 123
DHCP 24
DHCP Option 28
Dial Plan 226
Dial-now 232
Dial-now Template File 235
Directed Call Pickup 375
Display Method on Dialing 185
Distinctive Ring Tones 639
Do Not Disturb (DND) 314
Door Phone 451
DTMF 681
Dual Headset 658

E
Early Media 330
Enable Page Tips 168
Encrypting and Decrypting Files 743
Enabling the Watch Dog Feature 770
Emergency Dialplan 251
Expansion Modules 4

F
Feature Key Synchronization 371

G
Getting Information from Status Indicators 771
Getting Information from Talk Statistics 772
Getting Started 9
Group Call Pickup 384

H
H.323 xii
Headset Prior 654
Hide Feature Access Codes 514
Hot Desking 559
Hotline 242

I
Index 873
Initialization Process Overview 18
Intercom 422
Introduction v
IPv6 Support 52
IP Direct Auto Answer 299

J
Jitter Buffer 677

K
Keep User Personalized Settings after Auto Provisioning 132
Key As Send 222
Key Features of IP Phones 4

L
Language 204
Lightweight Directory Access Protocol (LDAP) 481
Live Dialpad 281
LLDP 55
Loading Language Packs 205
Local Conference 367
Local Contact File 269
Local Directory 268
Logon Wizard 564

M
MAC-local CFG File 116
MAC-Oriented CFG File 116
Manual Provisioning 112
Index

Message Waiting Indicator (MWI)  531
Missed Call Log  267
Mobile Account  464
Multicast Paging  536
Multiple Line Keys per Account  179
Music on Hold (MoH)  342
Mute  419

N
NAT Traversal  84
Network Address Translation (NAT)  84
Network Conference  367
No Answer Forward  344
Noise Suppression  681
Notification Popups  149

O
Obtaining Configuration Files and Resource Files  119
Off Hook Hot Line Dialing  258

P
Page Tips for Expansion Module  170
Password Dial  441
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  470

R
Reading the Configuration Parameter Tables  vii
Recommended References  xi
Reboot in Talking  446
ReCall  397
Resource Files  116

Redial Tone  633
Related Documentations  vi
Remote Phone Book  473
Remote Phone Book Template File  474
Replace Rule  227
Replace Rule Template File  230
Reserve # in User Name  439
Reserved Ports  80
Return Message When DND  314
Return Code When Refuse  328
RFC and Internet Draft Support  828
Ringer Device for Headset  654
Ringing Timeout  433
Ring Tones  633
RTCP-XR  695
Real-Time Transport Protocol (RTP) Ports  620

S
Save Call Log  263
Search Source List in Dialing  260
Secure Real-Time Transport Protocol (SRTP)  739
Semi-attended Transfer  359
Send user=phone  433
Sending Volume  659
Server Redundancy  597
Session Timer  335
Setting Up Your Phone Network  23
Setting Up Your Phones with a Provisioning Server  110
Setting Up Your System  23
Shared Call Appearance (SCA)  516
Silent Mode  450
SIP  xiii
SIP Components  xiii
SIP Header  832
SIP IP Phone Models  1
SIP Request  831
SIP Responses  833
SIP Send Line  437
SIP Send MAC  435
SIP Session Description Protocol Usage  836
SIP Session Timer  333
Smart Noise Block  682
Softkey Layout  214
Specifying the Language to Use 212
Speed Dial 283
Static DNS 25
STUN 85
Summary Table Format viii
Supported Provisioning Protocols 122
Suppress DTMF Display 689

W
Wallpaper 152
Web Server Type 47
Web User Interface 113
Why Using a Provisioning Server? 121
Wi-Fi 47

X
XML Browser 628

Y
Yealink IP Phones in a Network 9