



Yealink DECT IP Phone Administrator Guide

Copyright

Copyright © 2018 YEALINK(XIAMEN) NETWORK TECHNOLOGY

Copyright © 2018 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.

End User License Agreement

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

Patent Information

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

Customer Feedback

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

Technical Support

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

GNU GPL INFORMATION

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

The original GPL license, source code of components licensed under GPL and used in Yealink products can be downloaded online: http://www.yealink.com/onepage_83.html.

Introduction

Yealink administrator guide provides general guidance on setting up phone network, provisioning and managing phones.

This guide is not intended for end users, but for administrators with experience in networking who understand the basis of open SIP networks and VoIP endpoint environments.

As an administrator, you can do the following with this guide:

- Set up a VoIP network and provisioning server.
- Provision the phone with features and settings.
- Troubleshoot, update and maintain phones.

The information detailed in this guide is applicable to the following Yealink devices:

- W60P IP DECT phones running firmware version 83 or later.
- W53P IP DECT phones running firmware version 83 or later.
- W41P DECT desk phones (DD phones) running firmware version 82 or later.
- CP930W-Base DECT conference phone running firmware version 83 or later.

Read the [Yealink Products Regulatory Notices guide](#) for all regulatory and safety guidance.

Related Documentations

The following related documents are available:

- Quick Start Guides, describe how to assemble phones and configure the most basic features available on the phones.
- User Guides, describe how to configure and use the basic and advanced features available on the phones via phone user interface.
- Auto Provisioning Guide, describes how to provision the phones using the boot file and configuration files.
The Auto Provisioning Guide is to serve as a basic guidance for provisioning Yealink phones with a provisioning server. If you are a novice, this guide is helpful for you.
- Using features integrated with Broadsoft UC-One, refer to the following two guides to have a better knowledge of BroadSoft features.
IP Phones Deployment Guide for BroadSoft UC-One Environments, describes how to configure BroadSoft features on the BroadWorks web portal and phones.
IP Phone Features Integrated with BroadSoft UC-One User Guide, describes how to configure and use IP phone features integrated with BroadSoft UC-One on Yealink phones.

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

Recommended References

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

To access the latest Release Notes or other guides for Yealink 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.

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

Typographic and Writing Conventions

Yealink documentations contain a few typographic conventions and writing conventions.

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

Convention	Description
Bold	Highlight the web/handset user interface items such as menus, menu selections, soft keys, or directory names when they are involved in a procedure or user action (for example, click Settings->Upgrade). Also used to emphasize text (for example, Important!).
<i>Italics</i>	Used to emphasize text, to show the example values or inputs (format of examples: <i>http(s)://[IPv6 address]</i>).
Blue Text	Used for cross references to other topics related to this topic (for example, Ring Tones), for hyperlinks to external sites and documents, for example, RFC 3315 or Yealink_SIP_IP_Phones_Auto_Provisioning_Guide .

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

Convention	Description
<>	Indicate that you must enter information specific to phone or network. For example, when you see <MAC>, enter your phone's 12-digit MAC address. If you see <phoneIPAddress>, enter your phone's IP address.
->	Indicate that you need to select an item from a menu. For example, Settings->System Settings indicates that you need to select System Settings from the Settings menu.

Table of Contents

Introduction	i
Related Documentations	i
Recommended References	i
Typographic and Writing Conventions	ii
Table of Contents	1
Getting Started	13
Requirements	13
Initialization Process Overview	13
Loading the ROM File	13
Configuring the VLAN	13
Querying the DHCP (Dynamic Host Configuration Protocol) Server	13
Contacting the Provisioning Server	14
Updating Firmware	14
Downloading the Resource Files	14
Verifying Startup	14
Phone Network	15
IPv4 and IPv6 Network Settings	15
IP Addressing Mode Configuration	15
IPv4 Configuration	16
IPv6 Configuration	19
DHCP Option for IPv4	23
Supported DHCP Option for IPv4	23
DHCP Option 66, Option 43 and Custom Option	23
DHCP Option 42 and Option 2	24
DHCP Option 12	24
DHCP Option 12 Hostname Configuration	24
DHCP Option 60	24
DHCP Option 60 Configuration	25
VLAN	25
LLDP Configuration	25
CDP Configuration	26
Manual VLAN Configuration	27
DHCP VLAN	28
VLAN Setting Configuration	29
Real-Time Transport Protocol (RTP) Ports	29
RTP Ports Configuration	30
Network Address Translation (NAT)	30
NAT Traversal Configuration	31
Keep Alive Configuration	33
Rport Configuration	34
SIP Port and TLS Port Configuration	34

VPN	35
VPN Related Files	35
VPN Configuration	35
Quality of Service (QoS)	36
Voice and SIP QoS Configuration	36
802.1x Authentication	37
802.1x Authentication Configuration	37
TR-069 Device Management	39
Supported RPC Methods	39
TR-069 Configuration	40
Phone Provisioning	43
Boot Files, Configuration Files and Resource Files	43
Boot Files	43
Common Boot File	44
MAC-Oriented Boot File	44
Boot File Attributes	44
Customizing a Boot File	44
Configuration Files	45
Common CFG File	45
MAC-Oriented CFG File	46
MAC-local CFG File	46
Configuration File Customization	46
Customizing a Configuration File	46
Configuration File Attributes	46
Resource Files	47
Supported Resource Files	47
Files Download Process	48
Provisioning Methods	48
Provisioning Methods Priority	49
Web User Interface	49
Accessing the Web User Interface	50
Quick Login Configuration	50
Web Server Type Configuration	51
Navigating the Web User Interface	52
Central Provisioning	52
Auto Provisioning Settings Configuration	53
User-Triggered Provisioning Settings Configuration	58
Setting Up a Provisioning Server	59
Supported Provisioning Protocols	59
Provisioning Protocols Configuration	60
Supported Provisioning Server Discovery Methods	60
PnP Provision Configuration	61
DHCP Provision Configuration	61
Static Provision Configuration	61

Configuring a Provisioning Server	62
Keeping User's Personalized Settings after Auto Provisioning	63
Keeping User's Personalized Settings Configuration	63
Auto Provisioning Flowchart for Keep User's Personalized Configuration Settings	64
Example: Keeping User's Personalized Settings	65
Clearing User's Personalized Configuration Settings	66
Custom Handset Related Configurations	66
Firmware Upgrade	69
Firmware for Each Phone Model	69
Firmware Upgrade Configuration	69
Handset Customization	72
Power Indicator LED of Handset	72
Power Indicator LED of Handset Configuration	72
Handset Keypad Light	73
Handset Keypad Light Configuration	73
Handset Backlight	74
Handset Backlight Configuration	74
Handset Wallpaper	75
Handset Wallpaper Configuration	75
Handset Screen Saver	75
Handset Screen Saver Configuration	75
Handset Name	76
Handset Name Configuration	76
Language	76
Supported Languages	77
Language Display Configuration	77
Language for Web Display Customization	78
Customizing a Language Pack for Web Display	78
Customizing a Language Pack for Note Display	79
Custom Language for Web Display Configuration	80
Time and Date	80
Time Zone	80
NTP Settings	84
NTP Configuration	84
DST Settings	85
Auto DST File Attributes	86
Customizing Auto DST File	86
DST Configuration	87
Time and Date Manually Configuration	89
Time and Date Format Configuration	89
Date Customization Rule	91
Input Method	92
Input Method Configuration	92
Search Source List in Dialing	92

Search Source File Customization	93
Search Source File Attributes	93
Customizing Search Source File	93
Search Source List Configuration	94
Call Display	95
Call Display Configuration	96
Display Method on Dialing	96
Display Method on Dialing Configuration	97
Key As Send	97
Key As Send Configuration	97
Recent Call Display in Dialing	97
Recent Call in Dialing Configuration	98
Warnings Display	98
Warnings Display Configuration	98
Advisory Tones	98
Advisory Tones Configuration	99
Bluetooth	99
Bluetooth Configuration	100
Account Settings	101
Account Registration	101
Supported Accounts	101
Accounts Registration Configuration	101
Registration Settings Configuration	104
Outbound Proxy in Dialog	106
Outbound Proxy in Dialog Configuration	106
Server Redundancy	107
Behaviors When Working Server Connection Fails	108
Registration Method of the Failover/Fallback Mode	108
Fallback Server Redundancy Configuration	109
Failover Server Redundancy Configuration	109
SIP Server Name Resolution	111
SIP Server Name Resolution Configuration	112
Static DNS Cache	113
Behave with a Configured DNS Server	113
Static DNS Cache Configuration	113
Number of Active Handsets	116
Number of Active Handsets Configuration	117
Number of Simultaneous Outgoing Calls	117
Number of Simultaneous Outgoing Calls Configuration	117
Number Assignment	118
Number Assignment Configuration	118
Call Log	121
Call Log Display	121
Call Log Configuration	121

Directory	123
Local Directory	123
Local Contact File Customization	123
Local Contact File Elements and Attributes	123
Customizing Local Contact File	124
Local Contact Files and Resource Upload	124
Lightweight Directory Access Protocol (LDAP)	124
LDAP Attributes	124
LDAP Configuration	125
Remote Phone Book	130
Remote Phone Book File Customization	130
Remote Phone Book File Elements	130
Customizing Remote Phone Book File	131
Remote Phone Book Configuration	131
Example: Configuring a Remote Phone Book	133
Shared Directory	133
Shared Directory Configuration	133
Shared Contact File Customization	134
Shared Contact File Elements and Attributes	134
Customizing Shared Contact File	134
Directory Search Settings	134
Directory Search Settings Configuration	134
Call Features	137
Dial Plan	137
Basic Regular Expression Syntax for Four Patterns	138
Replace Rule File Customization	138
Replace Rule File Attributes	138
Customizing the Replace Rule File	139
Dial Now File Customization	139
Dial Now File Attributes	139
Customizing the Dial Now File	139
Replace Rule Configuration	140
Dial Now Configuration	140
Area Code Configuration	141
Block Out Configuration	142
Example: Adding Replace Rules Using a Replace Rule File	143
Emergency Dialplan	143
Emergency Dialplan Configuration	144
Off Hook Hot Line Dialing	146
Off Hook Hot Line Dialing Configuration	146
Call Timeout	146
Call Timeout Configuration	146
Anonymous Call	147
Anonymous Call Configuration	147

Call Number Filter	148
Call Number Filter Configuration	148
IP Address Call	149
IP Address Call Configuration	149
Auto Answer	149
Auto Answer Configuration	149
Anonymous Call Rejection	150
Anonymous Call Rejection Configuration	150
Call Waiting	151
Call Waiting Configuration	151
Do Not Disturb (DND)	152
DND Settings Configuration	153
DND Feature Configuration	153
DND Configuration	153
Call Hold	154
Call Hold Configuration	154
Call Forward	155
Call Forward Settings Configuration	155
Call Forward Feature Configuration	156
Call Forward Configuration	156
Call Transfer	160
Call Transfer Configuration	161
Conference	162
Conference Type Configuration	162
Network Conference Configuration	162
SD Card Recording	162
SD Card Recording Configuration	163
Multicast Paging	163
Multicast Paging Group Configuration	163
Multicast Listening Group Configuration	164
Multicast Paging Settings	165
Multicast Paging Settings Configuration	165
End Call on Hook	167
End Call on Hook Configuration	167
Audio Features	169
Alert Tone	169
Alert Tone Configuration	169
Ringer Device	170
Ringer Device Configuration	170
Tones	170
Supported Tones	170
Tones Configuration	171
Audio Codecs	173
Supported Audio Codecs	173

Audio Codecs Configuration	174
Packetization Time (PTime)	176
Supported PTime of Audio Codec	176
PTime Configuration	177
Early Media	177
Early Media Configuration	177
Acoustic Clarity Technology	178
Background Noise Suppression (BNS)	178
Automatic Gain Control (AGC)	178
Voice Activity Detection (VAD)	178
VAD Configuration	178
Comfort Noise Generation (CNG)	178
CNG Configuration	179
Jitter Buffer	179
Jitter Buffer Configuration	179
DTMF	180
DTMF Keypad	180
Transmitting DTMF Digit	181
Transmitting DTMF Digit Configuration	181
Suppress DTMF Display	182
Suppress DTMF Display Configuration	182
Voice Quality Monitoring (VQM)	183
RTCP-XR	183
RTCP-XR Configuration	183
VQ-RTCPXR	184
Voice Quality Reports	184
Voice Quality Reports Configuration	184
VQ-RTCPXR Display	186
VQ-RTCPXR Display Configuration	186
Central Report Collector	187
Central Report Collector Configuration	187
Security Features	189
User and Administrator Identification	189
User and Administrator Identification Configuration	189
User Access Level Configuration	190
Auto Logout Time	191
Auto Logout Time Configuration	191
Base PIN	191
Base PIN Configuration	191
Emergency Number	192
Emergency Number Configuration	192
Transport Layer Security (TLS)	193
Supported Cipher Suites	193
Supported Trusted and Server Certificates	194

Supported Trusted Certificates	194
TLS Configuration	196
Secure Real-Time Transport Protocol (SRTP)	199
SRTP Configuration	200
Encrypting and Decrypting Files	200
Configuration Files Encryption Tools	200
Configuration Files Encryption and Decryption	201
Contact Files Encryption and Decryption	201
Encryption and Decryption Configuration	201
Example: Encrypting Configuration Files	203
Incoming Network Signaling Validation	205
Incoming Network Signaling Validation Configuration	205
Advanced Features	207
Call Park and Retrieve	207
Call Park and Retrieve Configuration	207
Shared Line	208
Shared Call Appearance (SCA) Configuration	208
SCA Configuration	208
Intercom	209
Intercom Configuration	209
Voice Mail	210
MWI for Voice Mail Configuration	210
General Features	213
Line Identification Presentation	213
CLIP and COLP Configuration	213
Return Code for Refused Call	215
Return Code for Refused Call Configuration	215
Accept SIP Trust Server Only	215
Accept SIP Trust Server Only Configuration	215
100 Reliable Retransmission	216
100 Reliable Retransmission Configuration	216
SIP Session Timer	217
SIP Session Timer Configuration	217
Session Timer	218
Session Timer Configuration	218
Reboot in Talking	219
Reboot in Talking Configuration	219
Reserve # in User Name	219
Reserve # in User Name Configuration	220
Busy Tone Delay	220
Busy Tone Delay Configuration	220
Configuration Parameters	223
BroadSoft Parameters	223

BroadSoft Settings	223
Broadsoft XSI	223
Broadsoft Network Directory	225
Broadsoft Call Park	228
BroadSoft Call Waiting Sync	229
BroadSoft DND and Forward Sync	230
Ethernet Interface MTU Parameter	230
SIP Settings Parameters	230
Call Settings Parameters	232
Base Settings Parameters	232
Handset Settings Parameters	233
Troubleshooting Methods	234
Log Files	234
Local Logging	234
Local Logging Configuration	234
Exporting the Log Files to a Local PC	237
Viewing the Log Files	237
Syslog Logging	238
Syslog Logging Configuration	239
Viewing the Syslog Messages on Your Syslog Server	241
Resetting Phone and Configuration	241
Resetting the IP phone to Default Factory Settings	242
Resetting the IP phone to Custom Factory Settings	242
Custom Factory Configuration	243
Deleting the Custom Factory Settings Files	243
Packets Capture	243
Capturing the Packets via Web User Interface	243
Watch Dog	244
Watch Dog Configuration	244
Analyzing Configuration Files	244
Exporting CFG Configuration Files from Phone	245
Importing CFG Configuration Files to Phone	245
Configuration Files Import URL Configuration	245
Exporting BIN Files from the Phone	246
Importing BIN Files from the Phone	246
BIN Files Import URL Configuration	246
Exporting All the Diagnostic Files	246
Phone Status	247
Viewing the Phone Status	247
Phone Reboot	247
Rebooting the IP Phone Remotely	247
Notify Reboot Configuration	248
Rebooting the IP Phone via Handset User Interface	248
Rebooting the IP Phone via Web User Interface	248

Troubleshooting Solutions	249
IP Address Issues	249
The IP phone does not get an IP address	249
Solving the IP conflict problem	249
Specific format in configuring IPv6 on Yealink phones	249
Time and Date Issues	250
Display time and date incorrectly	250
Phone Book Issues	250
Difference between a remote phone book and a local phone book	250
Audio Issues	250
Increasing or decreasing the volume	250
Get poor sound quality during a call	250
There is no sound when the other party picks up the call	250
Play the local ringback tone instead of media when placing a long distance number without plus 0	251
Firmware and Upgrading Issues	251
Fail to upgrade the phone firmware	251
Verifying the firmware version	251
The IP phone does not update the configurations	252
System Log Issues	252
Fail to export the system log to a provisioning server (FTP/TFTP server)	252
Fail to export the system log to a syslog server	252
Password Issues	252
Restore the administrator password	252
The web screen displays "Default password is in use. Please change!"	252
Power and Startup Issues	253
Both PoE cable and power adapter is connected to the phone	253
The power LED indicator has no lights	253
Other Issues	253
The difference among user name, register name and display name	253
On code and off code	253
The difference between RFC 2543 Hold enabled and disabled	253
Base Issue	254
Why doesn't the power indicator on the base station light up?	254
Why doesn't the network indicator on the base station slowly flash?	254
Handset Issues	254
How to recognize the area of the handset?	254
Register Issue	254
Why cannot the handset be registered to the base station?	254
Display Issue	255
Why does the handset prompt the message "Not Subscribed"?	255
Why does the handset prompt the message "Not in Range" or "Out Of Range"?	255
Why does the handset prompt the message "Network unavailable"?	255
Why does the handset display "No Service"?	255
Upgrade Issue	255
Why doesn't the DECT IP phone upgrade firmware successfully?	255

Appendix	257
RFC and Internet Draft Support	257

Getting Started

This chapter describes where Yealink phones fit in your network, and provides basic initialization instructions of phones.

Topics

[Requirements](#)
[Initialization Process Overview](#)
[Verifying Startup](#)

Requirements

In order to perform as SIP endpoints in your network successfully, you need the following in deployments:

- A working IP network is established.
- VoIP gateways configured for SIP.
- The latest (or compatible) firmware of the phones is available.
- A call server is active and configured to receive and send SIP messages.
- A text editor, such as Notepad++, to create and edit boot files, configuration files and resource files.

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 phone begins its initialization process.

Topics

[Loading the ROM File](#)
[Configuring the VLAN](#)
[Querying the DHCP \(Dynamic Host Configuration Protocol\) Server](#)
[Contacting the Provisioning Server](#)
[Updating Firmware](#)
[Downloading the Resource Files](#)

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 pre-loaded. During initialization, the phone runs a bootstrap loader that loads and executes the ROM file.

Configuring the VLAN

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

Querying the DHCP (Dynamic Host Configuration Protocol) Server

The IP phone is capable of querying a DHCP server.

After establishing network connectivity, the phone can obtain the following network parameters from the DHCP server during initialization:

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

By default, the phones obtain these parameters from a DHCPv4. You can configure network parameters of the IP phone manually if any of them are not supplied by the DHCP server.

Contacting the Provisioning Server

If you configure the IP phone to obtain configurations from the provisioning server, it will be connected to the provisioning server, and then download the boot file and configuration file(s) during startup. The 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 phone will use the configurations stored in the flash memory.

Updating Firmware

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

You can manually upgrade firmware if the IP phone does not download the firmware from the provisioning server.

Downloading the Resource Files

In addition to the configuration file(s), the phone may require resource files before it provides service. These resource files are optional, but if you deploy some particular features, these files are required.

Verifying Startup

When the base station begins the initialization process, it cycles through the following steps:

1. After connected to the power, the power indicator LED illuminates solid green.
2. After connected to the available network, the network indicator LED illuminates solid green.
3. (Optional.) After at least one handset registered to the base station, the registration LED illuminates solid green.

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

Phone Network

Yealink phones operate on an Ethernet local area network (LAN) or wireless network. You can configure the local area network to accommodate a number of network designs, which varies by organization and Yealink phones.

Topics

[IPv4 and IPv6 Network Settings](#)

[DHCP Option for IPv4](#)

[VLAN](#)

[Real-Time Transport Protocol \(RTP\) Ports](#)

[Network Address Translation \(NAT\)](#)

[VPN](#)

[Quality of Service \(QoS\)](#)

[802.1x Authentication](#)

[TR-069 Device Management](#)

IPv4 and IPv6 Network Settings

Yealink IP Phones support IPv4 addressing mode, IPv6 addressing mode, as well as an IPv4&IPv6 dual-stack addressing mode.

After connected to the wired network, the phones can obtain the IPv4 network settings from a Dynamic Host Configuration Protocol (DHCP) server if your network supports it. To make it easier to manage IP settings, we recommend using automated DHCP which is possible to eliminate repetitive manual data entry.

You can also configure IPv4 or IPv6 network settings manually.

Note

Yealink phones comply with the DHCPv4 specifications documented in [RFC 2131](#), and ICMPv6 specifications documented in [RFC 4443](#).

Topics

[IP Addressing Mode Configuration](#)

[IPv4 Configuration](#)

[IPv6 Configuration](#)

IP Addressing Mode Configuration

The following table lists the parameters you can use to configure IP addressing mode.

Parameter	static.network.ip_address_mode ^[1]	<y0000000000xx>.cfg
Description	It configures the IP addressing mode.	
Permitted Values	0 -IPv4 1 -IPv6 2 -IPv4 & IPv6	
Default	0	
Web UI	Network->Basic->Internet Port->Mode(IPv4/IPv6)	

Handset UI	W53P/W60P:
	OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IP Mode
	DD Phone:
	Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IP Mode
	CP930W-Base:
	Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IP Mode

^[1]If you change this parameter, the phone will reboot to make the change take effect.

IPv4 Configuration

The following table lists the parameters you can use to configure IPv4.

Parameter	static.network.internet_port.type ^[1]	<y0000000000xx>.cfg
Description	It configures the Internet port type for IPv4. Note: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6).	
Permitted Values	0-DHCP 2-Static IP Address	
Default	0	
Web UI	Network->Basic->IPv4 Config	
Handset UI	W53P/W60P:	
	OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type	
	DD Phone:	
	Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv4	
	CP930W-Base:	
	Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv4->IP Address Type	
Parameter	static.network.internet_port.ip ^[1]	<y0000000000xx>.cfg
Description	It configures the IPv4 address. Example: static.network.internet_port.ip = 192.168.1.20 Note: It works only if "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).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	Network->Basic->IPv4 Config->Static IP Address->IP Address	
Handset UI	W53P/W60P:	
	OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: Static->IP Address	

	<p>DD Phone:</p> <p>Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv4->Static IPv4 Client->IP Address</p> <p>CP930W-Base:</p> <p>Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv4->IP Address Type: Static->IP Address</p>	
Parameter	static.network.internet_port.mask ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the IPv4 subnet mask.</p> <p>Example:</p> <p>static.network.internet_port.mask = 255.255.255.0</p> <p>Note: It works only if "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).</p>	
Permitted Values	Subnet Mask	
Default	Blank	
Web UI	Network->Basic->IPv4 Config->Static IP Address->Subnet Mask	
Handset UI	<p>W53P/W60P:</p> <p>OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: Static->Subnet Mask</p> <p>DD Phone:</p> <p>Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv4->Static IPv4 Client->Subnet Mask</p> <p>CP930W-Base:</p> <p>Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv4->IP Address Type: Static->Subnet Mask</p>	
Parameter	static.network.internet_port.gateway ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the IPv4 default gateway.</p> <p>Example:</p> <p>static.network.internet_port.gateway = 192.168.1.254</p> <p>Note: It works only if "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).</p>	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	Network->Basic->IPv4 Config->Static IP Address->Default Gateway	
Handset UI	<p>W53P/W60P:</p> <p>OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: Static->Default Gateway</p>	

	<p>DD Phone:</p> <p>Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv4->Static IPv4 Client->Default Gateway</p> <p>CP930W-Base:</p> <p>Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv4->IP Address Type: Static->Default Gateway</p>	
Parameter	static.network.static_dns_enable ^[1]	<y0000000000xx>.cfg
Description	<p>It triggers the static DNS feature to on or off.</p> <p>Note: It works only if "static.network.internet_port.type" is set to 0 (DHCP).</p>	
Permitted Values	<p>0-Off, the phone will use the IPv4 DNS obtained from DHCP.</p> <p>1-On, the phone will use manually configured static IPv4 DNS.</p>	
Default	0	
Web UI	Network->Basic->IPv4 Config->Static DNS	
Handset UI	<p>W53P/W60P:</p> <p>OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: DHCP->DNS Type: Manual</p> <p>DD Phone:</p> <p>Menu->Settings->Advanced Settings (default password: 0000) ->Network->WAN Port->IPv4->DHCP IPv4 Client->Static DNS</p> <p>CP930W-Base:</p> <p>Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv4->IP Address Type: DHCP->DNS Type: Manual</p>	
Parameter	static.network.primary_dns ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the primary IPv4 DNS server.</p> <p>Example:</p> <p>static.network.primary_dns = 202.101.103.55</p> <p>Note: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure "static.network.static_dns_enable" is set to 1 (On).</p>	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	Network->Basic->IPv4 Config->Static IP Address->Primary DNS	
Handset UI	<p>W53P/W60P:</p> <p>OK->Settings->System Settings->Network (default PIN: 0000) ->Basic >IPv4->IP Address Type: DHCP->DNS Type: Manual->Primary DNS</p> <p>DD Phone:</p> <p>Menu->Settings->Advanced Settings (default password: admin)->Network->WAN Port->IPv4->Static IPv4 Client->Pri.DNS</p>	

	Or Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv4->DHCP IPv4 Client->Static DNS (Enabled) ->Pri.DNS CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv4->IP Address Type: DHCP->DNS Type: Manual->Primary DNS	
Parameter	static.network.secondary_dns ^[1]	<y0000000000xx>.cfg
Description	It configures the secondary IPv4 DNS server. Example: static.network.secondary_dns = 202.101.103.54 Note: It works only if "static.network.ip_address_mode" is set to 0 (IPv4) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure "static.network.static_dns_enable" is set to 1 (On).	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	Network->Basic->IPv4 Config->Static IP Address->Secondary DNS	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv4->IP Address Type: DHCP->DNS Type: Manual->Secondary DNS DD Phone: Menu->Settings->Advanced Settings (default password: admin)->Network->WAN Port->IPv4->Static IPv4 Client->Sec.DNS Or Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv4->DHCP IPv4 Client->Static DNS (Enabled) ->Sec.DNS CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv4->IP Address Type: DHCP->DNS Type: Manual->Secondary DNS	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

IPv6 Configuration

If you configure the network settings on the phone for an IPv6 network, you can set up an IP address for the phone by using SLAAC (ICMPv6) or by manually entering an IP address. Ensure that your network environment supports IPv6. Contact your ISP for more information.

The following table lists the parameters you can use to configure IPv6.

Parameter	static.network.ipv6_internet_port.type ^[1]	<y0000000000xx>.cfg
Description	It configures the Internet port type for IPv6. Note: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6).	
Permitted Values	0 -DHCP (using SLAAC by default) 1 -Static IP Address	

Default	0	
Web UI	Network->Basic->IPv6 Config	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type DD Phone: Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv6 CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv6->IP Address Type	
Parameter	static.network.ipv6_internet_ip ^[1]	<y0000000000xx>.cfg
Description	It configures the IPv6 address. Note: It works only if "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).	
Permitted Values	IPv6 Address	
Default	Blank	
Web UI	Network->Basic->IPv6 Config->Static IP Address->IP Address	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->IP Address DD Phone: Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv6->Static IPv6 Client->IP Address CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv6->IP Address Type: Static->IP Address	
Parameter	static.network.ipv6_prefix ^[1]	<y0000000000xx>.cfg
Description	It configures the IPv6 prefix. Note: It works only if "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).	
Permitted Values	Integer from 0 to 128	
Default	64	
Web UI	Network->Basic->IPv6 Config->Static IP Address->IPv6 Prefix(0~128)	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->IPv6 Prefix DD Phone:	

	Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv6->Static IPv6 Client->IPv6 IP Prefix CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv6->IP Address Type: Static->IPv6 Prefix	
Parameter	static.network.ipv6_internet_port.gateway ^[1]	<y0000000000xx>.cfg
Description	It configures the IPv6 default gateway. Note: It works only if "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).	
Permitted Values	IPv6 Address	
Default	Blank	
Web UI	Network->Basic->IPv6 Config->Static IP Address->Default Gateway	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->Default Gateway DD Phone: Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv6->Static IPv6 Client->Default Gateway CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv6->IP Address Type: Static->Default Gateway	
Parameter	static.network.ipv6_static_dns_enable ^[1]	<y0000000000xx>.cfg
Description	It triggers the static IPv6 DNS feature to on or off. Note: It works only if "static.network.ipv6_internet_port.type" is set to 0 (DHCP).	
Permitted Values	0 -Off, the phone will use the IPv6 DNS obtained from DHCP. 1 -On, the phone will use manually configured static IPv6 DNS.	
Default	0	
Web UI	Network->Basic->IPv6 Config->IPv6 Static DNS	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: DHCP->DNS Type: Manual DD Phone: Menu->Settings->Advanced Settings (default password: 0000) ->Network->WAN Port->IPv6->DHCP IPv6 Client->Static DNS CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv6->IP Address Type: DHCP->DNS Type: Manual	
Parameter	static.network.ipv6_primary_dns ^[1]	<y0000000000xx>.cfg

Description	It configures the primary IPv6 DNS server. Note: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure "static.network.ipv6_static_dns_enable" is set to 1 (On).	
Permitted Values	IPv6 Address	
Default	Blank	
Web UI	Network->Basic->IPv6 Config->Static IP Address->Primary DNS	
Handset UI	<p>W53P/W60P:</p> <p>OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->Primary DNS</p> <p>DD Phone:</p> <p>Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv6->Static IPv6 Client->Pri.DNS</p> <p>Or Menu->Settings->Advanced Settings (default password: admin)->Network->WAN Port->IPv6->DHCP IPv6 Client->Static DNS(Enabled) ->Pri.DNS</p> <p>CP930W-Base:</p> <p>Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv6->IP Address Type: Static->Primary DNS</p>	
Parameter	static.network.ipv6_secondary_dns ^[1]	<y0000000000xx>.cfg
Description	It configures the secondary IPv6 DNS server. Note: It works only if "static.network.ip_address_mode" is set to 1 (IPv6) or 2 (IPv4 & IPv6). In DHCP environment, you also need to make sure "static.network.ipv6_static_dns_enable" is set to 1 (On).	
Permitted Values	IPv6 Address	
Default	Blank	
Web UI	Network->Basic->IPv6 Config->Static IP Address->Secondary DNS	
Handset UI	<p>W53P/W60P:</p> <p>OK->Settings->System Settings->Network (default PIN: 0000) ->Basic->IPv6->IP Address Type: Static->Secondary DNS</p> <p>DD Phone:</p> <p>Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv6->Static IPv6 Client->Sec.DNS</p> <p>Or Menu->Settings->Advanced Settings (default password: 0000)->Network->WAN Port->IPv6->DHCP IPv6 Client->Static DNS(Enabled) ->Sec.DNS</p> <p>CP930W-Base:</p> <p>Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->Basic->IPv6->IP Address Type: Static->Secondary DNS</p>	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

DHCP Option for IPv4

The IP phone can obtain IPv4-related parameters in an IPv4 network via DHCP option.

Note

For more information on DHCP options, refer to [RFC 2131](#) or [RFC 2132](#).

Topics

[Supported DHCP Option for IPv4](#)

[DHCP Option 66, Option 43 and Custom Option](#)

[DHCP Option 42 and Option 2](#)

[DHCP Option 12](#)

[DHCP Option 60](#)

Supported DHCP Option for IPv4

The following table lists common DHCP options for IPv4 supported by Yealink phones.

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

DHCP Option 66, Option 43 and Custom Option

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 you have configured the DHCP option on the phone. The option must be in accordance with the one defined in the DHCP server.

Note

If you fail 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. One possibility is that connecting to the secondary DHCP server that responds to DHCP INFORM queries with a requested provisioning server address. 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 server responds, the INFORM query process will retry and eventually time out.

Related Topic

[DHCP Provision Configuration](#)

DHCP Option 42 and Option 2

Yealink 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).

Related Topic

[NTP Settings](#)

DHCP Option 12

You can specify a hostname for the phone when using DHCP. The DHCP client uses option 12 to send a predefined hostname to the DHCP registration server.

The name may or may not be qualified with the local domain name (based on [RFC 2132](#)). See [RFC 1035](#) for character set restrictions.

Topic

[DHCP Option 12 Hostname Configuration](#)

DHCP Option 12 Hostname Configuration

The following table lists the parameter you can use to configure DHCP option 12 hostname.

Parameter	static.network.dhcp_host_name ^[1]	<y0000000000xx>.cfg
Description	It specifies a hostname for the phone when using DHCP.	
Permitted Values	String within 99 characters	
Default	W60B	
Web UI	Features->General Information->DHCP Hostname	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

DHCP Option 60

DHCP option 60 is used to indicate the vendor type and configuration of a DHCP client. You can set the format for option 60. Servers can use option 43 to return the vendor-specific information to the client.

Topic

[DHCP Option 60 Configuration](#)

DHCP Option 60 Configuration

The following table lists the parameters you can use to configure DHCP option 60.

Parameter	static.network.dhcp.option60type	<y0000000000xx>.cfg
Description	It configures the DHCP option 60 type.	
Permitted Values	0 -ASCII, vendor-identifying information is in ASCII format. 1 -Binary, vendor-identifying information is in the format defined in RFC 3925 .	
Default	0	
Parameter	static.auto_provision.dhcp_option.option60_value	<y0000000000xx>.cfg
Description	It configures the vendor class identifier string to use in the DHCP interaction.	
Permitted Values	String within 99 characters	
Default	yealink	
Web UI	Settings->Auto Provision->IPv4 DHCP Option Value	

VLAN

The purpose of VLAN configurations on the IP phone is to insert a 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 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.

In addition to manual configuration, the 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](#).

Topics

[LLDP Configuration](#)

[CDP Configuration](#)

[Manual VLAN Configuration](#)

[DHCP VLAN](#)

[VLAN Setting Configuration](#)

LLDP Configuration

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

form an update and reboot. This allows the phones to plug into any switch, obtain their VLAN IDs, and then start communications with the call control.

The following table lists the parameters you can use to configure LLDP.

Parameter	static.network.lldp.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the LLDP feature.	
Permitted Values	0 -Disabled 1 -Enabled, the phone attempts to determine its VLAN ID through LLDP.	
Default	1	
Web UI	Network->Advanced->LLDP->Active	
Parameter	static.network.lldp.packet_interval ^[1]	<y0000000000xx>.cfg
Description	It configures the interval (in seconds) that how often the phone sends the LLDP request. Note: It works only if "static.network.lldp.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 3600	
Default	60	
Web UI	Network->Advanced->LLDP->Packet Interval (1~3600s)	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

CDP Configuration

CDP (Cisco Discovery Protocol) allows the 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.

If the CDP feature is enabled on the phones, the phones will periodically advertise their own information to the directly connected CDP-enabled switch. The phones can also receive CDP packets from the connected switch. If the VLAN configurations on the phones are different from the ones sent by the switch, the phones will perform an update and reboot. This allows you to connect the phones into any switch, obtain their VLAN IDs, and then start communications with the call control.

The following table lists the parameters you can use to configure CDP.

Parameter	static.network.cdp.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the CDP feature.	
Permitted Values	0 -Disabled 1 -Enabled, the phone attempts to determine its VLAN ID through CDP.	
Default	1	
Web UI	Network->Advanced->CDP->Active	
Parameter	static.network.cdp.packet_interval ^[1]	<y0000000000xx>.cfg
Description	It configures the interval (in seconds) that how often the phone sends the CDP request. Note: It works only if "static.network.cdp.enable" is set to 1 (Enabled).	

Permitted Values	Integer from 1 to 3600
Default	60
Web UI	Network->Advanced->CDP->Packet Interval (1~3600s)

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Manual VLAN Configuration

VLAN is disabled on the phones by default. You can configure VLAN for the Internet port and PC port manually. Before configuring VLAN on the IP phone, you need to obtain the VLAN ID from your network administrator.

The following table lists the parameters you can use to configure VLAN manually.

Parameter	static.network.vlan.internet_port_enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the VLAN for the Internet port.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Network->Advanced->VLAN->WAN Port->Active	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN Parameter->Status DD Phone: Menu->Settings->Advanced Settings (default password: 0000) ->Network->VLAN->WAN Port->VLAN Status CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->VLAN->VLAN Parameter->Status	
Parameter	static.network.vlan.internet_port_vid ^[1]	<y0000000000xx>.cfg
Description	It configures the VLAN ID for the Internet port. Note: It works only if "static.network.vlan.internet_port_enable" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 4094	
Default	1	
Web UI	Network->Advanced->VLAN->WAN Port->VID (1-4094)	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN Parameter->Status: Enabled->VID DD Phone: Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->VID Number CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->VLAN->VLAN Parameter->Status:	

	Enabled->VID	
Parameter	static.network.vlan.internet_port_priority ^[1]	<y0000000000xx>.cfg
Description	It configures the VLAN priority for the Internet port. 7 is the highest priority, 0 is the lowest priority. Note: It works only if "static.network.vlan.internet_port_enable" is set to 1 (Enabled).	
Permitted Values	Integer from 0 to 7	
Default	0	
Web UI	Network->Advanced->VLAN->WAN Port->Priority	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN Parameter->Status: Enabled->Priority DD Phone: Menu->Settings->Advanced Settings (default password: admin) ->Network->VLAN->WAN Port->Priority CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->VLAN->VLAN Parameter->Status: Enabled->Priority	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

DHCP VLAN

Yealink phones support VLAN discovery via DHCP. When the VLAN discovery method is set to DHCP, the 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.

The following table lists the parameters you can use to configure DHCP VLAN discovery.

Parameter	static.network.vlan.dhcp_enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the DHCP VLAN discovery feature.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	
Web UI	Network->Advanced->VLAN->DHCP VLAN->Active	
Handset UI	W53P/W60P: OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN DHCP->Status DD Phone: Menu->Settings->Advanced Settings (default password: 0000) ->Network->VLAN->DHCP VLAN->DHCP VLAN CP930W-Base:	

	Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->VLAN->VLAN DHCP->Status	
Parameter	static.network.vlan.dhcp_option ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the DHCP option from which the phone will obtain the VLAN settings.</p> <p>You can configure at most five DHCP options and separate them by commas.</p> <p>Example:</p> <p>static.network.vlan.dhcp_option = 132,138,123,136,145</p>	
Permitted Values	Integer from 1 to 255	
Default	132	
Web UI	Network->Advanced->VLAN->DHCP VLAN->Option (1-255)	
Handset UI	<p>W53P/W60P:</p> <p>OK->Settings->System Settings->Network (default PIN: 0000) ->VLAN->VLAN DHCP->Status: Enabled->Options</p> <p>DD Phone:</p> <p>Menu->Settings->Advanced Settings (default password: 0000) ->Network->VLAN->DHCP VLAN->Option</p> <p>CP930W-Base:</p> <p>Menu->Settings->Advanced Settings (default PIN: 0000) ->Network->VLAN->VLAN DHCP->Status: Enabled->Options</p>	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

VLAN Setting Configuration

The following table lists the parameter you can use to configure VLAN setting.

Parameter	static.network.vlan.vlan_change.enable ^[1]	<y0000000000xx>.cfg
Description	<p>It enables or disables the phone to obtain VLAN ID using lower preference of VLAN assignment method, or to close the VLAN feature when the phone cannot obtain VLAN ID.</p> <p>The priority of each method is: LLDP/CDP>Manual>DHCP VLAN.</p>	
Permitted Values	<p>0-Disabled</p> <p>1-Enabled, the phone attempts to use the lower priority method when failing to obtain the VLAN ID using higher priority method. If all the methods are attempted, the phone will disable VLAN feature.</p>	
Default	0	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

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 phones is 11780. The first voice session sends RTP using port 11780. Addi-

tional calls would then use ports 11782, 11784, 11786, and so on. The phone is compatible with [RFC 1889 - RTP: A Transport Protocol for Real-Time Applications](#) - and the updated [RFC 3550](#).

Topic

[RTP Ports Configuration](#)

RTP Ports Configuration

The following table lists the parameters you can use to configure RTP ports.

Parameter	static.network.port.min_rtpport ^[1]	<y0000000000xx>.cfg
Description	It configures the minimum local RTP port.	
Permitted Values	Integer from 1024 to 65535	
Default	11780	
Web UI	Network->Advanced->Local RTP Port->Min RTP Port (1024~65535)	
Parameter	static.network.port.max_rtpport ^[1]	<y0000000000xx>.cfg
Description	It configures the maximum local RTP port. Note:	
Permitted Values	Integer from 1024 to 65535	
Default	12780	
Web UI	Network->Advanced->Local RTP Port->Max RTP Port (1024~65535)	
Parameter	features.rtp_symmetric.enable ^[1]	<y0000000000xx>.cfg
Description	It configures the symmetrical RTP (Real-Time Transport Protocol) feature on the IP phone. Note: IP address and port can be negotiated through the SDP protocol.	
Permitted Values	0 -Disabled 1 -reject RTP packets arriving from a non-negotiated IP address 2 -reject RTP packets arriving from a non-negotiated port 3 -reject RTP packets arriving from a non-negotiated IP address or a non-negotiated port	
Default	0	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Network Address Translation (NAT)

Network Address Translation (NAT) is a function that allows multiple devices to share the same public, routable IP address to establish connections over the Internet. NAT is present in many broadband access devices to translate public and private IP address.

Yealink phones can work with certain types of NAT.

Topics

[NAT Traversal Configuration](#)

[Keep Alive Configuration](#)
[Rport Configuration](#)
[SIP Port and TLS Port Configuration](#)

NAT Traversal Configuration

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.

Yealink phones support three NAT traversal techniques: manual NAT, STUN and ICE. If you enable manual NAT and STUN, the phone will use the manually-configured external IP address for NAT traversal. The TURN protocol is used as part of the ICE approach to NAT traversal.

The following table lists the parameters you can use to configure NAT traversal.

Parameter	account.X.nat.nat_traversal ^[1]	<MAC>.cfg
Description	It enables or disables the NAT traversal for a specific account. Note:	
Permitted Values	0 -Disabled 1 -STUN 2 -Manual NAT	
Default	0	
Web UI	Account->Register->NAT	
Parameter	static.network.static_nat.enable ^[2]	<y0000000000xx>.cfg
Description	It enables or disables the manual NAT feature.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Network->NAT->Manual NAT->Active	
Parameter	static.network.static_nat.addr ^[2]	<y0000000000xx>.cfg
Description	It configures the IP address to be advertised in SIP signaling. It should match the external IP address used by the NAT device. Example: static.network.static_nat.addr = 10.3.5.33 Note: It works only if "static.network.static_nat.enable" is set to 1 (Enabled).	
Permitted Values	IP Address	
Default	Blank	
Web UI	Network->NAT->Manual NAT->IP Address	
Parameter	static.sip.nat_stun.enable ^[2]	<y0000000000xx>.cfg

Description	It enables or disables the STUN (Simple Traversal of UDP over NATs) feature.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Network->NAT->STUN->Active	
Parameter	static.sip.nat_stun.server ^[2]	<y0000000000xx>.cfg
Description	It configures the IP address or domain name of the STUN server. Note: It works only if "static.sip.nat_stun.enable" is set to 1 (Enabled).	
Permitted Values	IP Address or Domain Name	
Default	Blank	
Web UI	Network->NAT->STUN->STUN Server	
Parameter	static.sip.nat_stun.port ^[2]	<y0000000000xx>.cfg
Description	It configures the port of the STUN server. Note: It works only if "static.sip.nat_stun.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 1024 to 65535	
Default	3478	
Web UI	Network->NAT->STUN->STUN Port (1024~65535)	
Parameter	static.ice.enable ^[2]	<y0000000000xx>.cfg
Description	It enables or disables the ICE (Interactive Connectivity Establishment) feature.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Network->NAT->ICE->Active	
Parameter	static.sip.nat_turn.enable ^[2]	<y0000000000xx>.cfg
Description	It enables or disables the TURN (Traversal Using Relays around NAT) feature.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Network->NAT->TURN->Active	
Parameter	static.sip.nat_turn.server ^[2]	<y0000000000xx>.cfg
Description	It configures the IP address or the domain name of the TURN server. Note: It works only if "static.sip.nat_turn.enable" is set to 1 (Enabled).	
Permitted Values	IP Address or Domain Name	
Default	Blank	
Web UI	Network->NAT->TURN->TURN Server	
Parameter	static.sip.nat_turn.port ^[2]	<y0000000000xx>.cfg

Description	It configures the port of the TURN server. Note: It works only if "static.sip.nat_turn.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 1024 to 65535	
Default	3478	
Web UI	Network->NAT->TURN->TURN Port (1~65535)	
Parameter	static.sip.nat_turn.username ^[2]	<y0000000000xx>.cfg
Description	It configures the user name to authenticate to TURN server. Note: It works only if "static.sip.nat_turn.enable" is set to 1 (Enabled).	
Permitted Values	String	
Default	Blank	
Web UI	Network->NAT->TURN->User Name	
Parameter	static.sip.nat_turn.password ^[2]	<y0000000000xx>.cfg
Description	It configures the password to authenticate to the TURN server. Note: It works only if "static.sip.nat_turn.enable" is set to 1 (Enabled).	
Permitted Values	String	
Default	Blank	
Web UI	Network->NAT->TURN->>Password	

^[1]X is the account ID. X=1-8.

^[2]If you change this parameter, the phone will reboot to make the change take effect.

Keep Alive Configuration

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

The following table lists the parameters you can use to configure keep alive.

Parameter	account.X.nat.udp_update_enable ^[1]	<MAC>.cfg
Description	It sets the type of keep-alive packets sent by the phone to the NAT device to keep the communication port open so that NAT can continue to function.	
Permitted Values	0 -Disabled 1 -Default (the phone sends the corresponding packets according to the transport protocol) 2 -Options (the phone sends SIP OPTIONS packets to the server) 3 -Notify (the phone sends SIP NOTIFY packets to the server)	
Default	1	
Web UI	Account->Advanced->Keep Alive Type	
Parameter	account.X.nat.udp_update_time ^[1]	<MAC>.cfg
Description	It configures the interval (in seconds) at which the phone sends a keep-alive package. Note: It works only if "account.X.nat.udp_update_enable" is set to 1, 2 or 3.	

Permitted Values	Integer from 15 to 2147483647
Default	30
Web UI	Account->Advanced->Keep Alive Interval(Seconds)

[1]X is the account ID. X=1-8.

Rport Configuration

As described in [RFC 3581](#), rport allows a client to request that the server sends the response back to the source IP address and port from which the request originated. It helps the phone traverse symmetric NATs.

Rport feature depends on support from a SIP server.

The following table lists the parameter you can use to configure rport.

Parameter	account.X.nat.rport ^[1]	<MAC>.cfg
Description	It enables or disables the phone to add the "rport" parameter in the Via header.	
Permitted Values	0 -Disabled 1 -Enabled, the INVITE Contact header uses the port in the "rport" parameter, but does not use the source IP address in the "received" parameter in the Via header of server's response. 2 -Enable Direct Process, the INVITE Contact header uses the port in the "rport" parameter, and uses the source IP address in the "received" parameter in the Via header of server's response.	
Default	0	
Web UI	Account->Advanced->RPort	

[1]X is the account ID. X=1-8.

SIP Port and TLS Port Configuration

You can configure the SIP and TLS source ports on the phone. Otherwise, the phone uses default values (5060 for UDP/TCP and 5061 for TLS).

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 using the configured source port.

The following table lists the parameters you can use to configure SIP port and TLS port.

Parameter	sip.listen_port	<y0000000000xx>.cfg
Description	It specifies the local SIP port. If it is set to 0, the phone will automatically listen to the local SIP port.	
Permitted Values	0, Integer from 1024 to 65535	
Default	5060	
Web UI	Settings->SIP->Local SIP Port	
Parameter	sip.tls_listen_port	<y0000000000xx>.cfg
Description	It specifies the local TLS listen port.	

	If it is set to 0, the phone will not listen to the TLS service.
Permitted Values	0, Integer from 1024 to 65535
Default	5061
Web UI	Settings->SIP->TLS SIP Port

VPN

Yealink 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 you configure VPN feature on the IP phone, the phone will act as a VPN client and use the certificates to authenticate with the VPN server.

For more information, refer to [OpenVPN Feature on Yealink phones](#).

Topics

[VPN Related Files](#)

[VPN Configuration](#)

VPN Related Files

To use VPN, you should collect the VPN-related files into one archive file in .tar format and then upload this tar file. The VPN-related files include 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 phones:

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

VPN Configuration

The following table lists the parameters you can use to configure VPN.

Parameter	static.network.vpn_enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the OpenVPN feature.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Network->Advanced->VPN->Active	
Parameter	static.openvpn.url	<y0000000000xx>.cfg
Description	It configures the access URL of the *.tar file for OpenVPN. Example:	

	static.openvpn.url = http://192.168.10.25/OpenVPN.tar
Permitted Values	URL within 511 characters
Default	Blank
Web UI	Network->Advanced->VPN->Upload VPN Config

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Quality of Service (QoS)

VoIP is extremely bandwidth and delay-sensitive. QoS is a major issue in VoIP implementations, regarding how to guarantee that packet traffic is not delayed or dropped due to interference from other lower priority traffic. VoIP can guarantee high-quality QoS only if the voice and the SIP packets are given priority over other kinds of network traffic. The phones support the DiffServ model of QoS.

Voice QoS

In order to make VoIP transmissions intelligible to receivers, voice packets should not be dropped, excessively delayed, or made to suffer varying delay. DiffServ model can guarantee high-quality voice transmission when the voice packets are configured to a higher DSCP value.

SIP QoS

SIP protocol is used for creating, modifying, and terminating two-party or multi-party sessions. To ensure good voice quality, SIP packets emanated from the phones should be configured with a high transmission priority.

DSCPs for voice and SIP packets can be specified respectively.

Note

For voice and SIP packets, the 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 Configuration](#).

Topic

[Voice and SIP QoS Configuration](#)

Voice and SIP QoS Configuration

The following table lists the parameters you can use to configure voice QoS and SIP QoS.

Parameter	static.network.qos.audiotos ^[1]	<y0000000000xx>.cfg
Description	It configures the DSCP (Differentiated Services Code Point) for voice packets. The default DSCP value for RTP packets is 46 (Expedited Forwarding).	
Permitted Values	Integer from 0 to 63	
Default	46	
Web UI	Network->Advanced->Voice QoS->Voice QoS (0~63)	
Parameter	static.network.qos.signalto ^[1]	<y0000000000xx>.cfg
Description	It configures the DSCP (Differentiated Services Code Point) for SIP packets	

	The default DSCP value for SIP packets is 26 (Assured Forwarding).
Permitted Values	Integer from 0 to 63
Default	26
Web UI	Network->Advanced->Voice QoS->SIP QoS (0~63)

^[1]If you change this parameter, the phone will reboot to make the change take effect.

802.1x Authentication

Yealink 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 (supports EAP In-Band provisioning, requires CA certificates if the provisioning method is Authenticated Provisioning)

For more information on 802.1x authentication, refer to [Yealink 802.1X Authentication](#).

Topic

[802.1x Authentication Configuration](#)

802.1x Authentication Configuration

The following table lists the parameters you can use to configure 802.1x authentication.

Parameter	static.network.802_1x.mode ^[1]	<y0000000000xx>.cfg
Description	It configures the 802.1x authentication method.	
Permitted Values	0 -EAP-None, no authentication 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	
Default	0	
Web UI	Network->Advanced->802.1x->802.1x Mode	
Parameter	static.network.802_1x.eap_fast_provision_mode ^[1]	<y0000000000xx>.cfg
Description	It configures the EAP In-Band provisioning method for EAP-FAST.	

	Note: It works only if "static.network.802_1x.mode" is set to 7 (EAP-FAST).	
Permitted Values	<p>0-Unauthenticated Provisioning, EAP In-Band provisioning is enabled by server unauthenticated PAC (Protected Access Credential) provisioning using the anonymous Diffie-Hellman key exchange.</p> <p>1-Authenticated Provisioning, EAP In-Band provisioning is enabled by server authenticated PAC provisioning using certificate based server authentication.</p>	
Default	0	
Web UI	Network->Advanced->802.1x->Provisioning Mode	
Parameter	static.network.802_1x.anonymous_identity ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the anonymous identity (user name) for 802.1X authentication.</p> <p>It is used for constructing a secure tunnel for 802.1X authentication.</p> <p>Note: It works only if "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6 or 7.</p>	
Permitted Values	String within 512 characters	
Default	Blank	
Web UI	Network->Advanced->802.1x->Anonymous Identity	
Parameter	static.network.802_1x.identity ^[1]	<y0000000000xx>.cfg
Description	It configures the identity (user name) for 802.1x authentication.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Network->Advanced->802.1x->Identity	
Parameter	static.network.802_1x.md5_password ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the password for 802.1x authentication.</p> <p>Note: It is required for all methods except EAP-TLS.</p>	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Network->Advanced->802.1x->MD5 Password	
Parameter	static.network.802_1x.root_cert_url	<y0000000000xx>.cfg
Description	<p>It configures the access URL of the CA certificate.</p> <p>The format of the certificate must be *.pem, *.crt, *.cer or *.der.</p> <p>Note: It works only if "static.network.802_1x.mode" is set to 2, 3, 4, 5, 6 or 7. If the authentication method is EAP-FAST, you also need to set "static.network.802_1x.eap_fast_provision_mode" to 1 (Authenticated Provisioning).</p>	
Permitted Values	URL within 511 characters	
Default	Blank	

Web UI	Network->Advanced->802.1x->CA Certificates	
Parameter	static.network.802_1x.client_cert_url	<y0000000000xx>.cfg
Description	It configures the access URL of the device certificate. The format of the certificate must be *.pem. Note: It works only if "static.network.802_1x.mode" is set to 2 (EAP-TLS).	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Network->Advanced->802.1x->Device Certificates	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

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.

For more information on TR-069, refer to [Yealink TR-069 Technote](#).

Topics

[Supported RPC Methods](#)

[TR-069 Configuration](#)

Supported RPC Methods

The following table provides a description of RPC methods supported by the phones.

RPC Method	Description
GetRPCMethods	This method is used to discover the set of methods supported by the CPE.
SetParameterValues	This method is used to modify the value of one or more CPE parameters.
GetParameterValues	This method is used to obtain the value of one or more CPE parameters.
GetParameterNames	This method is used to discover the parameters accessible on a particular CPE.
GetParameterAttributes	This method is used to read the attributes associated with one or more CPE parameters.
SetParameterAttributes	This method is used to modify attributes associated with one or more CPE parameters.
Reboot	This method causes the CPE to reboot.
Download	This method is used to cause the CPE to download a specified file from the designated location. File types supported by the phones are: <ul style="list-style-type: none"> Firmware Image Configuration File

RPC Method	Description
Upload	This method is used to cause the CPE to upload a specified file to the designated location. File types supported by the phones are: <ul style="list-style-type: none"> • Configuration File • Log File
ScheduleInform	This method is used to request the CPE to schedule a one-time Inform method call (separate from its periodic Inform method calls) sometime in the future.
FactoryReset	This method resets the CPE to its factory default state.
TransferComplete	This method informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.
AddObject	This method is used to add a new instance of an object defined on the CPE.
DeleteObject	This method is used to remove a particular instance of an object.

TR-069 Configuration

The following table lists the parameters you can use to configure TR-069.

Parameter	static.managementserver.enable	<y0000000000xx>.cfg
Description	It enables or disables the TR-069 feature.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Settings->TR069->Enable TR069	
Parameter	static.managementserver.username	<y0000000000xx>.cfg
Description	It configures the TR-069 ACS server user name used to authenticate the phone. Leave it blank if no authentication is required.	
Permitted Values	String within 128 characters	
Default	Blank	
Web UI	Settings->TR069->ACS Username	
Parameter	static.managementserver.password	<y0000000000xx>.cfg
Description	It configures the TR-069 ACS server password used to authenticate the phone. Leave it blank if no authentication is required.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Settings->TR069->ACS Password	
Parameter	static.managementserver.url	<y0000000000xx>.cfg

Description	It configures the access URL of the TR-069 ACS server.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Settings->TR069->ACS URL	
Parameter	static.managementserver.connection_request_user-name	<y0000000000xx>.cfg
Description	It configures the user name used to authenticate the connection requests from the ACS server.	
Permitted Values	String within 128 characters	
Default	Blank	
Web UI	Settings->TR069->Connection Request Username	
Parameter	static.managementserver.connection_request_password	<y0000000000xx>.cfg
Description	It configures the password used to authenticate the connection requests from the ACS server.	
Permitted Values	String within 64 characters	
Default	Blank	
Web UI	Settings->TR069->Connection Request Password	
Parameter	static.managementserver.periodic_inform_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to periodically report its configuration information to the ACS server.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	
Web UI	Settings->TR069->Enable Periodic Inform	
Parameter	static.managementserver.periodic_inform_interval	<y0000000000xx>.cfg
Description	It configures the interval (in seconds) at which the phone reports its configuration to the ACS server. Note: It works only if "static.managementserver.periodic_inform_enable" is set to 1 (Enabled).	
Permitted Values	Integer from 5 to 4294967295	
Default	60	
Web UI	Settings->TR069->Periodic Inform Interval (seconds)	

Phone Provisioning

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

For more information, refer to [Yealink_SIP_IP_Phones_Auto_Provisioning_Guide](#).

Topics

[Boot Files, Configuration Files and Resource Files](#)

[Provisioning Methods](#)

[Setting Up a Provisioning Server](#)

[Keeping User's Personalized Settings after Auto Provisioning](#)

Boot Files, Configuration Files and Resource Files

You can use boot files, configuration files and resource files to configure phone features and apply feature settings to phones. You can create or edit these files using a text editor such as Notepad++.

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>.

Topics

[Boot Files](#)

[Configuration Files](#)

[Resource Files](#)

[Files Download Process](#)

Boot Files

Yealink phones support boot files. The boot files maximize the flexibility to allow you to customize features and settings for multiple phones.

With the boot file, you can specify which configuration files should be downloaded. It is effective for you to provision the phones in different deployment scenarios:

- For all phones
- For a group of phones
- For a single phone

Yealink phones support two types of boot files: common boot file and MAC-Oriented boot file. You can use the default boot template file "y000000000000.boot" to create MAC-Oriented boot file by making a copy and renaming it.

Note

You can select whether to use the boot file or not according to your deployment scenario. If you do not want to use the boot file, please go to [Configuration Files](#).

Topics

[Common Boot File](#)

[MAC-Oriented Boot File](#)

[Boot File Attributes](#)

[Customizing a Boot File](#)

Common Boot File

Common boot file, named y000000000000.boot, is effective for all phones. You can use a common boot file to apply common feature settings to all of the phones rather than a single phone.

MAC-Oriented Boot File

MAC-Oriented boot file, named <MAC>.boot. It will only be effective for a specific IP phone. In this way, you have a high permission to control each phone by making changes on a per-phone basis.

You can create a MAC-Oriented boot file for each phone by making a copy and renaming the boot template file (y000000000000.boot). For example, if your phone MAC address is 00156574B150, rename the template file as 00156574b150.boot (lowercase).

Tip

MAC address, a unique 12-digit serial number is assigned to each phone. You can obtain it from the bar code on the back of the base.

Boot File Attributes

The following table lists the attributes you need to know in the boot template file.

Attributes	Description
#lversion:1.0.0.1	It must be placed in the first line. Do not edit and delete.
include:config <xxx.cfg> include:config "xxx.cfg"	Each "include" statement can specify a location of a configuration file. The configuration file format must be *.cfg. The locations in the angle brackets or double quotation marks support two forms: <ul style="list-style-type: none"> Relative path (relative to the boot file): For example, sip.cfg, HTTP Directory/sip.cfg Absolute path (or URL): For example, http://10.2.5.258/HTTP Directory/sip.cfg The location must point to a specific CFG file.
overwrite_mode	Enable or disable the overwrite mode. The overwrite mode applies to the configuration files specified in the boot file. Note that it only affects the parameters pre-provisioned via central provisioning. 1 -(Enabled) - If the value of a parameter in configuration files is left blank, or if a non-static parameter in configuration files is deleted or commented out, the factory default value takes effect. 0 -(Disabled) - If the value of a parameter in configuration files is left blank, deleted or commented out, the pre-configured value is kept. Note: Overwrite mode can only be used in boot files. If a boot file is used but "overwrite_mode" is not configured, the overwrite mode is enabled by default.

Tip

The line beginning with "#" is considered to be a comment. You can use "#" to make any comment in the boot file.

Customizing a Boot File

Procedure

1. Open a boot template file.
2. To add a configuration file, add `include:config <>` or `include:config ""` to the file. Each starts on a separate line.
3. Specify a configuration file for downloading.
For example:

```
include:config <configure/sip.cfg>
include:config "http://10.2.5.206/configure/account.cfg"
include:config "http://10.2.5.206/configure/dialplan.cfg"
```
4. Specify the overwrite mode.
For example:

```
overwrite_mode = 1
```
5. Save the boot file and place it on the provisioning server.

Related Topic

[Boot File Attributes](#)

Configuration Files

Yealink supports two configuration template files: Common CFG file and MAC-Oriented CFG file.

These configuration files contain two kinds of parameters:

- Static: The parameters start with a prefix "static.", for example, `static.auto_provision.custom.protect`.
- Non-static: The parameters do not start with a prefix "static.", for example, `local_time.date_format`.

You can deploy and maintain a mass of Yealink phones automatically through configuration files stored in a provisioning server.

Note

For protecting against unauthorized access, you can encrypt configuration files. For more information on encrypting configuration files, refer to [Encrypting and Decrypting Files](#).

Topics

[Common CFG File](#)

[MAC-Oriented CFG File](#)

[MAC-local CFG File](#)

[Configuration File Customization](#)

[Configuration File Attributes](#)

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 effective for all phones in the same model. The common CFG file has a fixed name for each phone model.

The following table lists the name of the common CFG file for each phone model:

Phone Model	Common CFG file
W53P/W60P/W41P/CP930W-Base	y000000000077.cfg

MAC-Oriented CFG File

MAC-Oriented CFG file, which is named after the MAC address of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of MAC-Oriented CFG file is 00156574b150.cfg (lowercase). It contains parameters unique to a particular phone, such as account registration. It will only be effective for a MAC-specific IP phone.

MAC-local CFG File

MAC-local CFG file, which is named after the MAC address of the IP phone. For example, if the MAC address of an IP phone is 00156574B150, the name of MAC-local CFG file is 00156574b150-local.cfg (lowercase). It contains changes associated with non-static parameter that you make via web user interface or handset user interface (for example, changes for time and date formats, ring tones).

This file generates only if you enable the provisioning priority mechanism. It is stored locally on the IP phone and you can upload it to the provisioning server each time the file updates. This file enables the users to keep their personalized configuration settings, even though the IP phone performs auto provisioning.

Note

The non-static changes that you made before enabling the provisioning priority mechanism are not saved in the generated MAC-local file, but the previous settings still take effect on the phone. The static changes are never be saved to the <MAC>-local.cfg file.

The provisioning priority mechanism is enabled by the parameter "static.auto_provision.custom.protect".

Configuration File Customization

You can create some new CFG files by making a copy and renaming the configuration template file (for example, sip.cfg, account.cfg). You can rearrange the parameters in the configuration template file and create your own configuration files with parameters you want. This flexibility is especially useful when you want to apply specific settings to a group of phones.

Topic

[Customizing a Configuration File](#)

Customizing a Configuration File

1. Copy and rename a configuration template file. For example, sip.cfg.
2. Rearrange the parameters in the sip.cfg, and set the valid values for them.

For example:

```
account.1.dnd.enable = 1
```

```
account.2.dnd.enable = 1
```

3. Save the configuration file and place it on the provisioning server.

Related Topic

[Configuration File Attributes](#)

Configuration File Attributes

The following table lists the attributes you need to know in the configuration template file.

Attributes	Description
#!version:1.0.0.1	It must be placed in the first line. Do not edit and delete.
Configuration Parameter=Valid Value	Specify the parameters and values to apply specific settings to the phones. <ul style="list-style-type: none"> • Separate each configuration parameter and value with an equal sign

Attributes	Description
(for example, account.1.dnd.enable = 1)	<ul style="list-style-type: none"> Set only one configuration parameter per line Put the configuration parameter and value on the same line, and do not break the line

Tip

The line beginning with “#” is considered to be a comment. You can use “#” to make any comment in the boot file.

Resource Files

Resource files are optional, but if the particular feature is being employed, these files are required. You need to place resource files on the provisioning server. The phones request the resource files in addition to the configuration files during auto provisioning.

Tip

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 auto provisioning, the phones will request the resource files in addition to the configuration files.

Topic

[Supported Resource Files](#)

Supported Resource Files

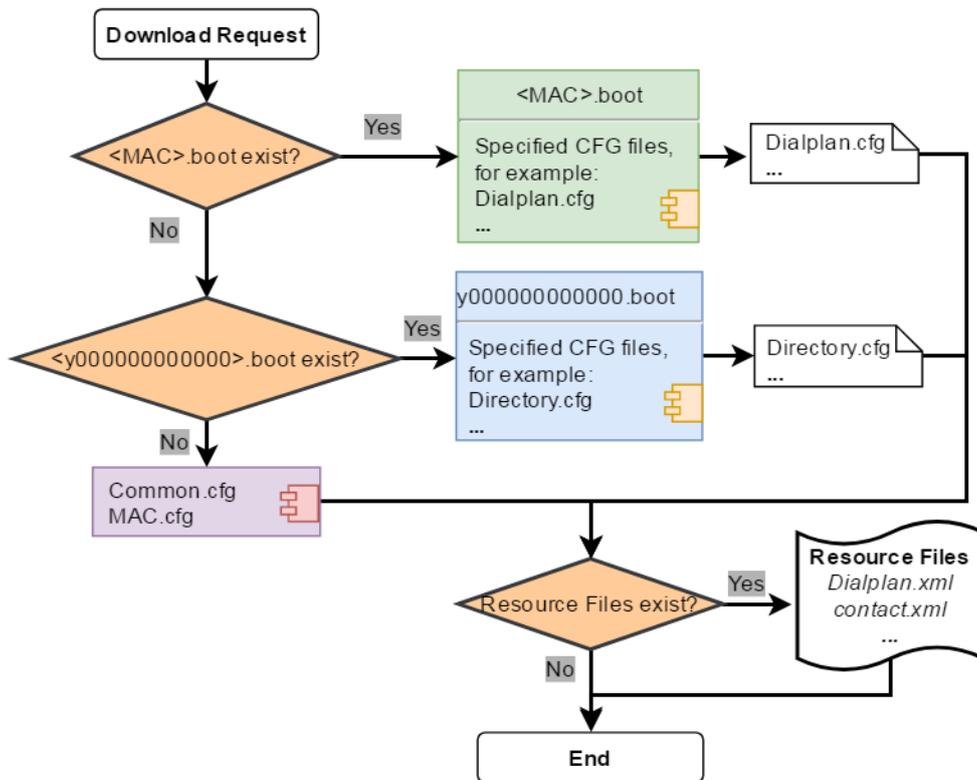
Yealink supplies some template of resource files for you, so you can directly edit the files as required.

The following table lists the resource files Yealink supplies:

Template File	File Name	Description	Reference in Section
AutoDST Template	AutoDST.xml	Add or modify time zone and DST settings.	DST Settings
Language Packs	For example, 000.GUI.English.lang 1.English_note.xml 1.English.js	Customize the translation of the existing language on the phone/web user interface.	Language for Phone Display Customization Language for Web Display Customization
Replace Rule Template	DialPlan.xml	Customize replace rules for the dial plan.	Replace Rule File Customization
Dial Now Template	DialNow.xml	Customize dial now rules for the dial plan.	Dial Now File Customization
Super Search Template	super_search.xml	Customize the search source list.	Search Source File Customization
Local Contact File	contact.xml	Add or modify multiple local contacts.	Local Contact File Customization
Remote Phone Book Template	Department.xml Menu.xml	Add or modify multiple remote contacts.	Remote Phone Book File Customization

Files Download Process

When you provision the phones, the phones will request to download the boot files, configuration files and resource files from the provisioning server according to the following flowchart:



The parameters in the newly downloaded configuration files will override the same parameters in files downloaded earlier.

Provisioning Methods

Yealink provides two ways to provision your phones:

- Manual Provisioning: provisioning via the handset user interface or web user interface.
- Central Provisioning: provisioning through configuration files stored in a central provisioning server.

The method you use depends on how many phones need to be deployed and what features and settings to be configured. Manual provisioning on the web or handset user interface does not contain all of the phone settings available with the centralized method. You can use the web user interface method in conjunction with a central provisioning method and handset user interface method. We recommend using centralized provisioning as your primary provisioning method when provisioning multiple phones.

Topics

[Provisioning Methods Priority](#)

[Web User Interface](#)

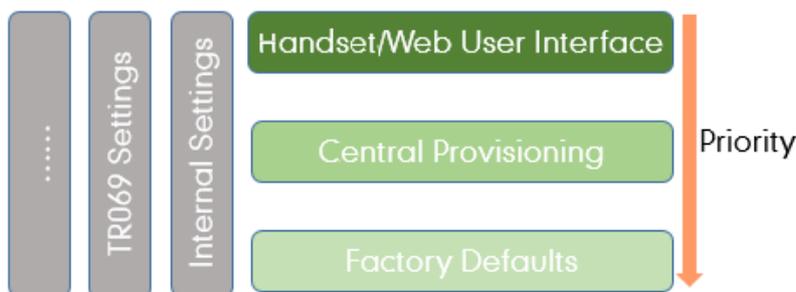
[Phone User Interface](#)

[Central Provisioning](#)

Provisioning Methods Priority

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

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



Note

The provisioning priority mechanism takes effect only if "static.auto_provision.custom.protect" is set to 1. For more information on this parameter, refer to [Keeping User's Personalized Settings Configuration](#).

Static parameters 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.

Static parameters are the parameters that start with a prefix "static.", for example, the parameters associated with auto provisioning/network/syslog, TR069 settings and internal settings (the temporary configurations to be used for program running).

Web User Interface

You can configure the phones via web user interface, a web-based interface that is especially useful for remote configuration.

Because features and configurations vary by phone models and firmware versions, options available on each page of the web user interface can vary as well. Note that the features configured via web user interface are limited. Therefore, you can use the web user interface in conjunction with a central provisioning method and phone user interface.

When configuring the phones via web user interface, you require a user name and password for access. For a user, the default user name and password are "user" (case-sensitive). For an administrator, the default user name and password are "admin" (case-sensitive).

Note

When you manually configure a phone via web user interface or handset user interface, the changes associated with non-static parameters you make will be stored in the MAC-local CFG file. For more information on MAC-local CFG file, refer to [MAC-local CFG File](#).

Topics

- [Accessing the Web User Interface](#)
- [Quick Login Configuration](#)
- [Web Server Type Configuration](#)
- [Navigating the Web User Interface](#)

Accessing the Web User Interface

Procedure

1. Find the phone IP address. For DD phone and CP930W-Base, press or tap the OK key when the phone is idle or navigate to **Menu** -> **Status** on the phone; For W53P/W60P, press the OK key, and then navigate to **Status**-> **Base**.
2. Enter the IP address in the address bar of a web browser on your PC.
For example, for IPv4: http://192.168.0.10 or 192.168.0.10; for IPv6: http://[2005:1:1:1:215:65ff:fe64:6e0a] or [2005:1:1:1:215:65ff:fe64:6e0a]
3. Enter the user name and password.
4. Click **Login**.

Related Topics

[Web Server Type Configuration](#)

[User and Administrator Identification](#)

Quick Login Configuration

You can access to the web user interface quickly using the request URI "https://username:password@phoneIPAddress" (for example, https://admin:admin@192.168.0.10). It will locate you in the **Status** web page after accessing the web user interface. It is helpful to quickly log into the web user interface without entering the username and password in the login page.

Yealink phones support domain name customization. You can use a custom domain name to access the web user interface.

Note

Accessing the web user interface by request URI 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.

The following table lists the parameters you can use to configure quick login.

Parameter	wui.quick_login	<y0000000000xx>.cfg
Description	It enables or disables the quick login feature. Note: It works only if "static.wui.https_enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled, you can quickly log into the web user interface using a request URI (for example, https://admin:admin@192.168.0.10).	
Default	0	
Parameter	wui.secure_domain_list	<y0000000000xx>.cfg
Description	It configures the valid domain name to access the web user interface of the phone. Multiple domain names are separated by semicolons. Example: wui.secure_domain_list = test.abc.com You are only allowed to use test.abc.com or IP address to access the web user interface of the phone. Note: To use a domain name to access the web user interface of the phone, make sure your DNS server	

	can resolve the domain name to the IP address of the phone.
Permitted Values	String If it is left blank, you are only allowed to use IP address to access the web user interface of the phone. If it is set to "any", you can use IP address or any domain name to access the web user interface of the phone.
Default	any

Web Server Type Configuration

Yealink phones support both HTTP and HTTPS protocols for accessing the web user interface. You can configure the web server type. Web server type determines access protocol of the web user interface. If you disable to access web user interface using the HTTP/HTTPS protocol, both you and the user cannot access the web user interface.

The following table lists the parameters you can use to configure web server type.

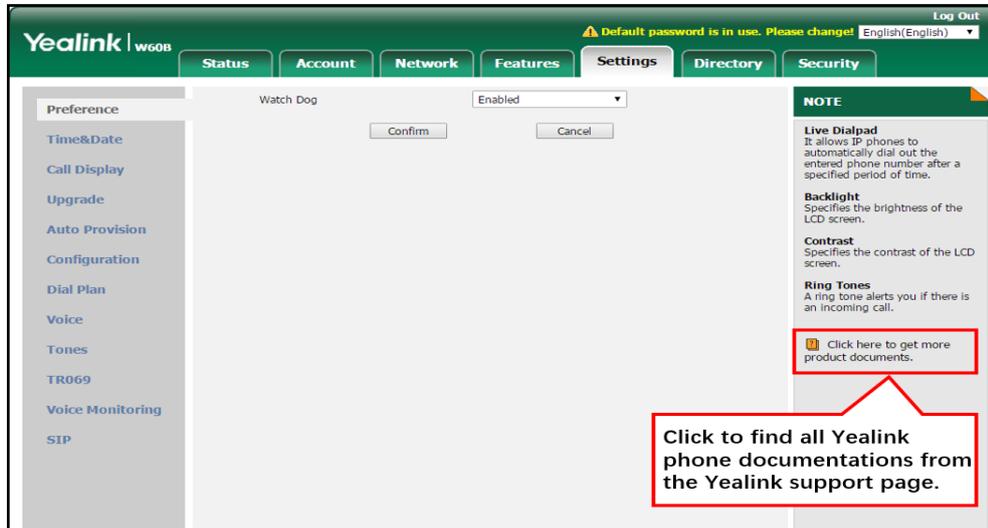
Parameter	static.wui.http_enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables to access the web user interface of the phone over a non-secure tunnel (HTTP).	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Network->Advanced->Web Server->HTTP	
Parameter	static.network.port.http ^[1]	<y0000000000xx>.cfg
Description	It configures the port used to access the web user interface of the phone over a non-secure tunnel (HTTP).	
Permitted Values	Integer from 1 to 65535	
Default	80	
Web UI	Network->Advanced->Web Server->HTTP Port (1~65535)	
Parameter	static.wui.https_enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables to access the web user interface of the phone over a secure tunnel (HTTPS).	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Network->Advanced->Web Server->HTTPS	
Parameter	static.network.port.https ^[1]	<y0000000000xx>.cfg
Description	It configures the port used to access the web user interface of the phone over a secure tunnel (HTTPS).	
Permitted Values	Integer from 1 to 65535	
Default	443	
Web UI	Network->Advanced->Web Server->HTTPS Port (1~65535)	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Navigating the Web User Interface

When you log into the web user interface successfully, the phone status is displayed on the first page of the web user interface. You can click the navigation bar to customize or click **Log Out** to log out of the web user interface.

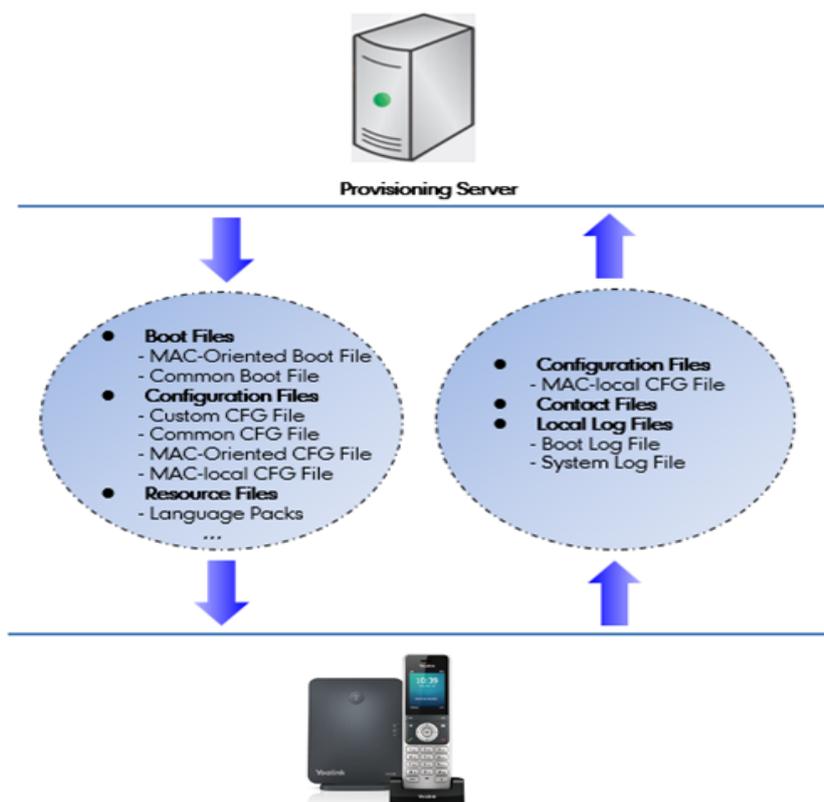
The following figure is an example when you navigate to **Settings->Preference**:



Central Provisioning

Central provisioning enables you to provision multiple phones from a provisioning server that you set up, and maintain a set of boot files, configuration files and resource files for all phones in the central provisioning server.

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



Yealink phones can obtain the provisioning server address during startup. Then the phones first download boot files and configuration files from the provisioning server, and then 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](#).

The phones can be configured to upload log files (log files provide a history of phone events), call log files and contact files to the provisioning server. You can also configure a directory for each of these three files respectively.

Topics

[Auto Provisioning Settings Configuration](#)

[User-Triggered Provisioning Settings Configuration](#)

Auto Provisioning Settings Configuration

The following table lists the parameters you can use to configure settings for auto provisioning.

Parameter	static.auto_provision.attempt_expired_time	<y0000000000xx>.cfg
Description	It configures the timeout (in seconds) to transfer a file via auto provisioning. Note: It has a higher priority than the value defined by the parameter "static.network.attempt_expired_time".	
Permitted Values	Integer from 1 to 300	
Default	5	
Web UI	Settings->Auto Provision->Attempt Expired Time(s)	
Parameter	static.network.attempt_expired_time ^[1]	<y0000000000xx>.cfg

Description	It configures the timeout (in seconds) to transfer a file for HTTP/HTTPS connection. Note: It has a lower priority than the value defined by the parameter "static.auto_provision.attempt_expired_time".	
Permitted Values	Integer from 1 to 20	
Default	10	
Parameter	static.auto_provision.attempt_before_failed	<y0000000000xx>.cfg
Description	It configures the maximum number of attempts to transfer a file before the transfer fails during auto provisioning.	
Permitted Values	Integer from 1 to 10	
Default	3	
Parameter	static.auto_provision.retry_delay_after_file_transfer_failed	<y0000000000xx>.cfg
Description	It configures the time (in seconds) to wait after a file transfer fails before retrying the transfer via auto provisioning.	
Permitted Values	Integer from 0 to 300	
Default	5	
Parameter	static.auto_provision.reboot_force.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the phone to reboot after auto provisioning, even if there is no specific configuration requiring a reboot. Note: It works only for the current auto provisioning process. If you want the phone to reboot after every auto provisioning process, the parameter must be always contained in the configuration file and set to 1. If the phone reboots repeatedly after it is set to 1, you can try to set "static.auto_provision.power_on" to 0 (Off).	
Permitted Values	0-Disabled 1-Enabled	
Default	Blank	
Parameter	static.auto_provision.power_on	<y0000000000xx>.cfg
Description	It triggers the power on feature to on or off.	
Permitted Values	0-Off 1-On, the phone performs auto provisioning when powered on.	
Default	1	
Web UI	Settings->Auto Provision->Power On	
Parameter	static.auto_provision.repeat.enable	<y0000000000xx>.cfg
Description	It triggers the repeatedly feature to on or off.	
Permitted Values	0-Off 1-On	

Default	0	
Web UI	Settings->Auto Provision->Repeatedly	
Parameter	static.auto_provision.repeat.minutes	<y0000000000xx>.cfg
Description	It configures the interval (in minutes) for the phone to perform auto provisioning repeatedly. Note: It works only if "static.auto_provision.repeat.enable" is set to 1 (On).	
Permitted Values	Integer from 1 to 43200	
Default	1440	
Web UI	Settings->Auto Provision->Interval(Minutes)	
Parameter	static.auto_provision.weekly.enable	<y0000000000xx>.cfg
Description	It triggers the weekly feature to on or off.	
Permitted Values	0 -Off 1 -On, the phone performs an auto provisioning process weekly.	
Default	0	
Web UI	Settings->Auto Provision->Weekly	
Parameter	static.auto_provision.weekly_upgrade_interval	<y0000000000xx>.cfg
Description	It configures the time interval (in weeks) for the phone to perform auto provisioning. If it is set to 0, the phone performs auto provisioning at the specific day(s) configured by the parameter "static.auto_provision.weekly.dayofweek" every week. If it is set to other values (for example, 3), the phone performs auto provisioning at a random day between the specific day(s) configured by the parameter "static.auto_provision.weekly.dayofweek" every three weeks. Note: It works only if "static.auto_provision.weekly.enable" is set to 1 (On).	
Permitted Values	Integer from 0 to 12	
Default	0	
Web UI	Settings->Auto Provision->Weekly Upgrade Interval(0~12week)	
Parameter	static.auto_provision.inactivity_time_expire	<y0000000000xx>.cfg
Description	It configures the delay time (in minutes) to perform auto provisioning when the phone is inactive at regular week. If it is set to 0, the phone performs auto provisioning at random between a starting time configured by the parameter "static.auto_provision.weekly.begin_time" and an ending time configured by the parameter "static.auto_provision.weekly.end_time". If it is set to other values (for example, 60), the phone performs auto provisioning only when it has been inactivated for 60 minutes (1 hour) between the starting time and ending time. Note: The phone may perform auto provisioning when you are using the phone during office hour. It works only if "static.auto_provision.weekly.enable" is set to 1 (On). The operations on the handset will not change the inactive status; only the functional operations related base station, such as calling, will change the inactive status.	

Permitted Values	Integer from 0 to 120	
Default	0	
Web UI	Settings->Auto Provision->Inactivity Time Expire(0~120min)	
Parameter	static.auto_provision.weekly.dayofweek	<y0000000000xx>.cfg
Description	<p>It configures the days of the week for the phone to perform auto provisioning weekly.</p> <p>Example:</p> <p>static.auto_provision.weekly.dayofweek = 01</p> <p>If "static.auto_provision.weekly_upgrade_interval" is set to 0, it means the phone performs auto provisioning every Sunday and Monday.</p> <p>If "static.auto_provision.weekly_upgrade_interval" is set to other value (for example, 3), it means the phone performs auto provisioning by randomly selecting a day from Sunday and Monday every three weeks.</p> <p>Note: It works only if "static.auto_provision.weekly.enable" is set to 1 (On).</p>	
Permitted Values	<p>0,1,2,3,4,5,6 or a combination of these digits</p> <p>0-Sunday</p> <p>1-Monday</p> <p>2-Tuesday</p> <p>3-Wednesday</p> <p>4-Thursday</p> <p>5-Friday</p> <p>6-Saturday</p>	
Default	0123456	
Web UI	Settings->Auto Provision->Day of Week	
Parameter	static.auto_provision.weekly.begin_time static.auto_provision.weekly.end_time	<y0000000000xx>.cfg
Description	<p>It configures the starting/ending time of the day for the phone to perform auto provisioning weekly.</p> <p>Note: It works only if "static.auto_provision.weekly.enable" is set to 1 (On).</p>	
Permitted Values	Time from 00:00 to 23:59	
Default	00:00	
Web UI	Settings->Auto Provision->Time	
Parameter	static.auto_provision.flexible.enable	<y0000000000xx>.cfg
Description	<p>It triggers the flexible feature to on or off.</p> <p>Note: The day within the period is 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. The timer starts again after each auto provisioning.</p>	

Permitted Values	0 -Off 1 -On, the phone performs auto provisioning 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".	
Default	0	
Web UI	Settings->Auto Provision->Flexible Auto Provision	
Parameter	static.auto_provision.flexible.interval	<y0000000000xx>.cfg
Description	It configures the interval (in days) for the phone to perform auto provisioning. The auto provisioning occurs on a random day within this period based on the phone's MAC address. The phone performs auto provisioning on a random day (for example, 18) based on the phone's MAC address. Note: It works only if "static.auto_provision.flexible.enable" is set to 1 (On).	
Permitted Values	Integer from 1 to 1000	
Default	30	
Web UI	Settings->Auto Provision->Flexible Interval Days	
Parameter	static.auto_provision.flexible.begin_time	<y0000000000xx>.cfg
Description	It configures the starting time of the day for the phone to perform auto provisioning at random. Note: It works only if "static.auto_provision.flexible.enable" is set to 1 (On).	
Permitted Values	Time from 00:00 to 23:59	
Default	02:00	
Web UI	Settings->Auto Provision->Flexible Time	
Parameter	static.auto_provision.flexible.end_time	<y0000000000xx>.cfg
Description	It configures the ending time of the day for the phone to perform auto provisioning at random. If it is left blank or set to a specific value equal to starting time configured by the parameter "static.auto_provision.weekly.begin_time", the phone performs auto provisioning at the starting time. If it is set to a specific value greater than starting time configured by the parameter "static.auto_provision.weekly.begin_time", the phone performs auto provisioning at random between the starting time and ending time. If it is set to a specific value less than starting time configured by the parameter "static.auto_provision.weekly.begin_time", the phone performs auto provisioning at random between the starting time on that day and ending time in the next day. Note: It works only if "static.auto_provision.flexible.enable" is set to 1 (On).	
Permitted Values	Time from 00:00 to 23:59	
Default	Blank	
Web UI	Settings->Auto Provision->Flexible Time	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

User-Triggered Provisioning Settings Configuration

You can enable the users to trigger phones to perform provisioning by dialing an activation code. This method works only if there is no registered account on the phone.

The following table lists the parameters you can use to configure settings for user-triggered provisioning.

Parameter	static.autoprovision.X.name ^{[1][2]}	<y0000000000xx>.cfg
Description	It configures the code name to trigger auto provisioning.	
Permitted Values	String within 64 characters	
Default	Blank	
Parameter	static.autoprovision.X.code ^{[1][2]}	<y0000000000xx>.cfg
Description	<p>It configures the activation code to trigger auto provisioning.</p> <p>The activation code can be numeric characters, special characters # * or a combination of them.</p> <p>Example:</p> <p>static.autoprovision.1.code = 123</p> <p>static.autoprovision.2.code = **</p> <p>static.autoprovision.3.code = *123</p>	
Permitted Values	String	
Default	Blank	
Parameter	static.autoprovision.X.url ^{[1][2]}	<y0000000000xx>.cfg
Description	It configures the access URL of the provisioning server for the phone to perform auto provisioning which is triggered by activation code.	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	static.autoprovision.X.user ^{[1][2]}	<y0000000000xx>.cfg
Description	It configures the user name for authentication during auto provisioning which is triggered by activation code.	
Permitted Values	String within 64 characters	
Default	Blank	
Parameter	static.autoprovision.X.password ^{[1][2]}	<y0000000000xx>.cfg
Description	It configures the password for authentication during auto provisioning which is triggered by activation code.	
Permitted Values	String within 32 characters	
Default	Blank	

Parameter	static.auto_provision.dns_resolv_nosys	<y0000000000xx>.cfg
Description	It enables or disables the phone to resolve the access URL of the provisioning server using download libraries mechanism.	
Permitted Values	0 -Disabled, the phone resolves the access URL of the provisioning server using the system mechanism. 1 -Enabled	
Default	1	
Parameter	static.auto_provision.dns_resolv_nretry	<y0000000000xx>.cfg
Description	It configures the retry times when the phone fails to resolve the access URL of the provisioning server. Note: For each different DNS server, it works only if "static.auto_provision.dns_resolv_nosys" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 10	
Default	2	
Parameter	static.auto_provision.dns_resolv_timeout	<y0000000000xx>.cfg
Description	It configures the timeout (in seconds) for the phone to retry to resolve the access URL of the provisioning server. Note: For each different DNS server, it works only if "static.auto_provision.dns_resolv_nosys" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 60	
Default	5	

^[1]X is an activation code ID. For all phones, X=1-50.

^[2]If you change this parameter, the phone will reboot to make the change take effect.

Setting Up a Provisioning Server

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

Topics

[Supported Provisioning Protocols](#)

[Supported Provisioning Server Discovery Methods](#)

[Configuring a Provisioning Server](#)

Supported Provisioning Protocols

Yealink phones support several transport protocols for provisioning:

- Trivial File Transfer Protocol (TFTP)
- File Transfer Protocol (FTP)
- Hyper Text Transfer Protocol - Secure (HTTPS)
- File Transfer Protocol - Secure (FTPS)

Note

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

You can specify the transport protocol in the provisioning server address, for example, http://xxxxxxx. If not specified, the TFTP protocol is used.

Topic

[Provisioning Protocols Configuration](#)

Provisioning Protocols Configuration

The following table lists the parameters you can use to configure provisioning protocols.

Parameter	static.auto_provision.server.type	<y0000000000xx>.cfg
Description	It configures the protocol the phone uses to connect to the provisioning server. Note: It works only if the protocol type is not defined in the access URL of the provisioning server configured by the parameter "static.auto_provision.server.url".	
Permitted Values	1-HTTP 2-HTTPS 3-FTP Other values -TFTP	
Default	TFTP	
Parameter	static.auto_provision.user_agent_mac.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the phone's MAC address to be included in the User-Agent header of HTTP/HTTPS request via auto provisioning.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	

^[2]If you change this parameter, the phone will reboot to make the change take effect.

Supported Provisioning Server Discovery Methods

After the phone has established network settings, it must discover a provisioning server to obtain software updates and configuration settings.

The IP phone supports the following methods to discover the provisioning server address:

- **PnP:** PnP feature allows the 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 phones. When the IP phone requests an IP address using the DHCP protocol, the resulting response may contain option 66 (for IPv4) or the custom option (if configured) that contains the provisioning server address.
- **Static:** You can manually configure the server address via handset user interface or web user interface.

Topics

[PnP Provision Configuration](#)

[DHCP Provision Configuration](#)

[Static Provision Configuration](#)

PnP Provision Configuration

The following table lists the parameter you can use to configure PnP provision.

Parameter	static.auto_provision.pnp_enable	<y0000000000xx>.cfg
Description	It triggers the Plug and Play (PnP) feature to on or off.	
Permitted Values	0 -Off 1 -On, the phone broadcasts PnP SUBSCRIBE messages to obtain a provisioning server address during startup.	
Default	1	
Web UI	Settings->Auto Provision->PNP Active	

DHCP Provision Configuration

The following table lists the parameters you can use to configure DHCP provision.

Parameter	static.auto_provision.dhcp_option.enable	<y0000000000xx>.cfg
Description	It triggers the DHCP Active feature to on or off.	
Permitted Values	0 -Off 1 -On, the phone obtains the provisioning server address by detecting DHCP options.	
Default	1	
Web UI	Settings->Auto Provision->DHCP Active	
Parameter	static.auto_provision.dhcp_option.list_user_options	<y0000000000xx>.cfg
Description	It configures the IPv4 custom DHCP option for requesting provisioning server address. Multiple options are separated by commas. Note: It works only if "static.auto_provision.dhcp_option.enable" is set to 1 (On).	
Permitted Values	Integer from 128 to 254	
Default	Blank	
Web UI	Settings->Auto Provision->IPv4 Custom Option	
Parameter	static.auto_provision.url_wildcard.pn	<y0000000000xx>.cfg
Description	It configures the characters to replace the wildcard \$PN in the received URL of the provisioning server. Note: The configured characters must be in accordance with the actual directory name of the provisioning server.	
Permitted Values	String within 32 characters	
Default	W60B	

Static Provision Configuration

To use the static provision method, you need to obtain the provisioning server address first when configuring a provisioning server.

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 backslashes 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.

The following table lists the parameters you can use to configure static provision.

Parameter	static.auto_provision.server.url	<y0000000000xx>.cfg
Description	It configures the access URL of the provisioning server.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Settings->Auto Provision->Server URL	
Parameter	static.auto_provision.server.username	<y0000000000xx>.cfg
Description	It configures the user name for provisioning server access.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Settings->Auto Provision->User Name	
Parameter	static.auto_provision.server.password	<y0000000000xx>.cfg
Description	It configures the password for provisioning server access.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Settings->Auto Provision->Password	

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.

To set up the provisioning server:

1. Install a provisioning server application or locate a suitable existing server, such as 3CDaemon.
2. Create an account and home directory.
3. Set security permissions for the account.
4. Create boot files and configuration files, and then edit them as desired.
5. Copy the boot files, configuration files and resource files to the provisioning server.
6. If performing static provisioning, obtain the provisioning server address.

Tip

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.

Keeping User's Personalized Settings after Auto Provisioning

Generally, you deploy phones in batch and timely maintain company phones via auto provisioning, yet some users would like to keep the personalized settings (for example, ring tones) after auto provisioning.

Topics

[Keeping User's Personalized Settings Configuration](#)

[Auto Provisioning Flowchart for Keep User's Personalized Configuration Settings](#)

[Example: Keeping User's Personalized Settings](#)

[Clearing User's Personalized Configuration Settings](#)

[Custom Handset Related Configurations](#)

Keeping User's Personalized Settings Configuration

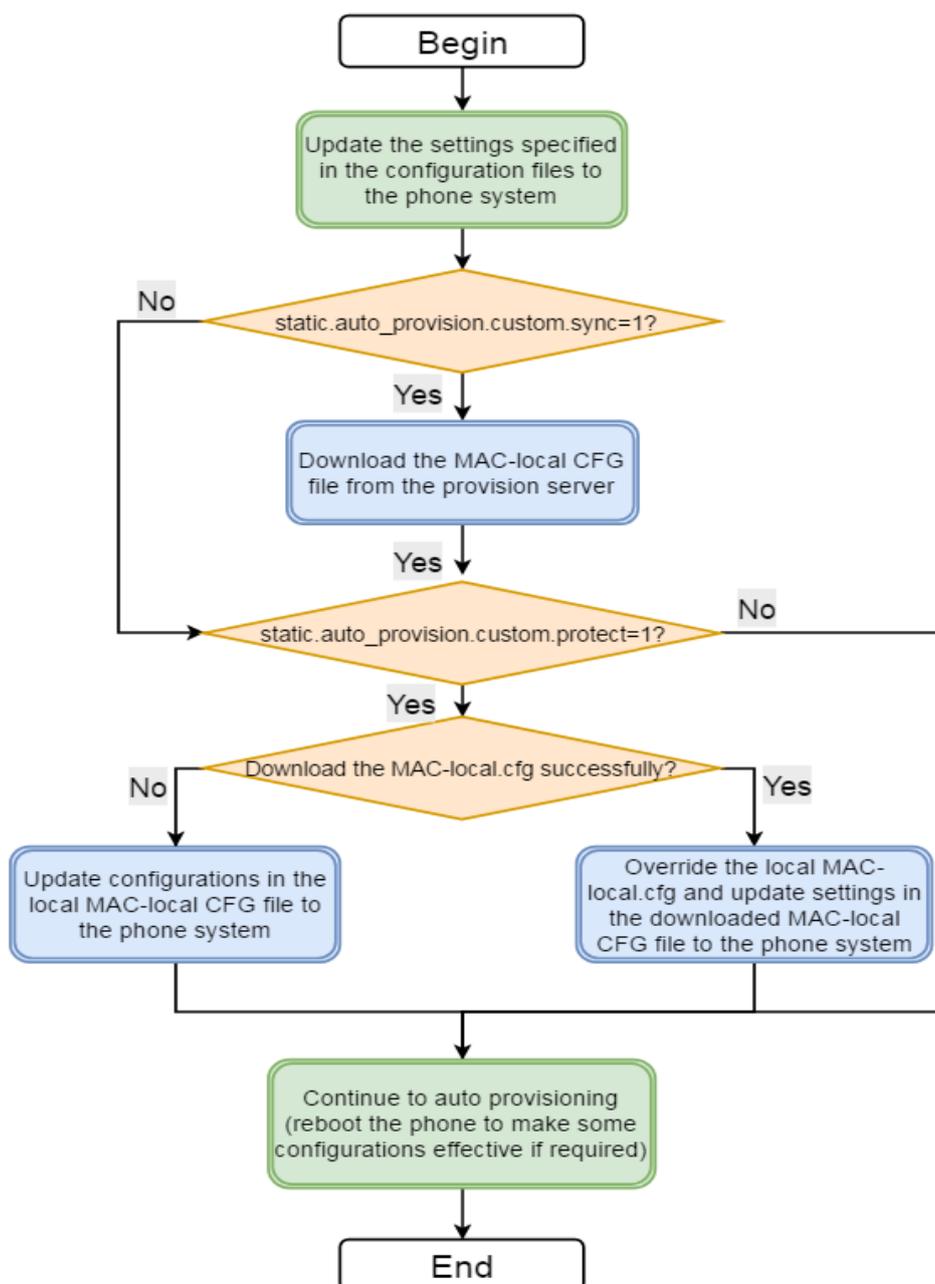
The following table lists the parameters you can use to keep user's personalized settings.

Parameter	static.auto_provision.custom.protect	<y0000000000xx>.cfg
Description	It enables or disables the phone to keep user's personalized settings after auto provisioning. Note: The provisioning priority mechanism (handset/web user interface >central provisioning >factory defaults) takes effect only if the value of this parameter is set to 1 (Enabled). If "overwrite_mode" is set to 1 in the boot file, the value of this parameter will be set to 1 (Enabled). It is not applicable to the custom handset related configurations .	
Permitted Values	0-Disabled 1-Enabled, <MAC>-local.cfg file generates and personalized non-static settings configured via the web or handset user interface will be kept after auto provisioning.	
Default	0	
Parameter	static.auto_provision.custom.sync	<y0000000000xx>.cfg
Description	It enables or disables the phone to upload the <MAC>-local.cfg file to the server each time the file updates, and to download the <MAC>-local.cfg file from the server during auto provisioning. Note: It works only if "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".	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Parameter	static.auto_provision.custom.sync.path	<y0000000000xx>.cfg
Description	It configures the URL for uploading/downloading the <MAC>-local.cfg file. If it is left blank, the phone will try to upload/download the <MAC>-local.cfg file to/from the provisioning server. Note: It works only if "static.auto_provision.custom.sync" is set to 1 (Enabled).	
Permitted Values	URL	

Default	Blank	
Parameter	static.auto_provision.custom.upload_method ^[1]	<y0000000000xx>.cfg
Description	It configures the way the phone uploads the <MAC>-local.cfg file, <MAC>-calllog.xml file or <MAC>-contact.xml file to the provisioning server (for HTTP/HTTPS server only).	
Permitted Values	0-PUT 1-POST	
Default	0	
Parameter	static.auto_provision.handset_configured.enable	<y0000000000xx>.cfg
Description	It enables or disables the base station to deliver custom handset configurations to the handset via auto provisioning/handset reboot/handset registration. Note: It is only applicable to the custom handset related configurations .	
Permitted Values	0-Disabled, the custom handset settings can be only changed via handset user interface. 1-Enabled, when the parameter "static.auto_provision.custom.handset.protect" is set to 0 (Disabled), the personalized handset settings will be overridden; if the parameter "static.auto_provision.custom.handset.protect" is set to 1 (Enabled), the personalized handset settings will not be overridden.	
Default	1	
Parameter	static.auto_provision.custom.handset.protect	<y0000000000xx>.cfg
Description	It enables or disables the handsets to keep user personalized settings after auto provisioning/handset reboot/handset registration. Note: It works only if "static.auto_provision.handset_configured.enable" is set to 0 (Disabled). It is only applicable to the custom handset related configurations . It is not applicable to DD phones.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	

Auto Provisioning Flowchart for Keep User's Personalized Configuration Settings

The following shows auto provisioning flowchart for Yealink phones when a user wishes to keep user's personalized configuration settings.



Example: Keeping User's Personalized Settings

This section shows you how to keep the personalized settings.

Parameters Settings:

static.auto_provision.custom.protect =1

After provisioning, if the users make changes via phone user interface or web user interface, the MAC-local.cfg file with non-static personal settings generates locally.

Scenario: Keeping user's personalized settings when upgrading the firmware

If you set "*static.auto_provision.custom.sync =1*", then the phones attempt to upload the MAC-local.cfg file to the provisioning server each time the file updates. When performing auto provisioning, they download their own MAC-local.cfg file from the provisioning server, and then update settings in MAC-local.cfg file to the IP phone system. The personalized settings locally are overridden by the MAC-local.cfg file from the provisioning server.

If you set "*static.auto_provision.custom.sync =0*", the MAC-local.cfg file will be kept locally. The personalized settings will not be overridden after auto provisioning.

Scenario: Keeping 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. Before factory reset, make sure that you have set "*static.auto_provision.custom.sync =1*", and the MAC-local.cfg file has kept on the provisioning server.

After resetting all configurations to factory defaults, both the parameters settings "*static.auto_provision.custom.protect*" and "*static.auto_provision.custom.sync*" are reset to 0. Although the MAC-local.cfg files locally are cleared, they are still kept on the provisioning server.

You can set "*static.auto_provision.custom.protect =1*" and "*static.auto_provision.custom.sync =1*", and then trigger the phone to perform auto provisioning. The phones download their own MAC-local.cfg file from the provisioning server, and then update settings in MAC-local.cfg file to the IP phone system.

As a result, the personalized configuration settings of the phone are retrieved after the factory reset.

Clearing User's Personalized Configuration Settings

When the IP phone is given to a new user but many personalized configurations settings of the last user are saved on the phone; or when the end user encounters some problems because of the wrong configurations, you can clear user's personalized configuration settings.

- Via W53P/W60P user interface at the path: **OK->Settings->System Settings->Base Reset->Reset local.**
- Via CP930W-Base user interface at the path: **Menu->Settings->Advanced Settings** (default PIN: 0000)->**Reset Config->Reset Local.**
- Via web user interface at the path: **Settings->Upgrade->Reset Local Settings.**

Note

The **Reset local settings** option on the web/handset user interface appears only if you set "*static.auto_provision.custom.protect = 1*".

If you set "*static.auto_provision.custom.sync = 1*", the MAC-local.cfg file on the provisioning server will be cleared too. If not, the MAC-local.cfg file is kept on the provisioning server, and the IP phone could download it and update the configurations to the phone after the next auto provisioning.

Custom Handset Related Configurations

This section shows you the custom handset related configurations.

Parameter	Related Topic
custom.handset.date_format	Time and Date Format Configuration
custom.handset.time_format	
custom.handset.eco_mode.enable	Handset Settings Parameters
custom.handset.auto_answer.enable	Auto Answer Configuration

custom.handset.low_battery_tone.enable	Advisory Tones Configuration
custom.handset.confirmation_tone.enable	
custom.handset.keypad_tone.enable	
custom.handset.keypad_light.enable	Handset Keypad Light Configuration
custom.handset.backlight_in_charger.enable	Handset Backlight Configuration
custom.handset.backlight_out_of_charger.enable	
custom.handset.screen_saver.enable	Handset Screen Saver Configuration
custom.handset.auto_intercom	Intercom Configuration
custom.handset.language	Language Display Configuration

Firmware Upgrade

There are two methods of firmware upgrade:

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

Note

We recommend that the phones running the latest firmware should not be downgraded to an earlier firmware version. The new firmware is compatible with old configuration parameters, but not vice versa.

Topics

[Firmware for Each Phone Model](#)

[Firmware Upgrade Configuration](#)

Firmware for Each Phone Model

You can download the latest firmware online:

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

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

IP Phone Model	Firmware Name	Example
W60P	W60B: 77.x.x.x.rom	W60B: 77.83.0.10.rom
	W56H: 61.x.x.x.rom	W56H: 61.83.0.10.rom
W53P	W60B: 77.x.x.x.rom	W60B: 77.83.0.10.rom
	W53H: 88.x.x.x.rom	W53H: 88.83.0.10.rom
W41P (DD phone)	W60B: 77.x.x.x.rom	W60B: 77.81.0.35
	T42S/T41S: 66.x.x.x.rom	T42S/T41S: 66.82.0.40
CP930W-Base	W60B: 77.x.x.x.rom	W60B: 77.83.0.20
	CP930W: 87.x.x.x.rom	CP930W: 87.83.0.20

Firmware Upgrade Configuration

Before upgrading firmware, you need to know the following:

- Do not close and refresh the browser when the IP phone is upgrading firmware via web user interface.
- Do not unplug the network cables and power cables when the IP phone is upgrading firmware.

The following table lists the parameters you can use to upgrade firmware.

Parameter	static.firmware.url	<y0000000000xx>.cfg
Description	It configures the access URL of the firmware file.	
Permitted Values	URL within 511 characters	

Default	Blank	
Web UI	Settings->Upgrade->Select And Upgrade Firmware	
Parameter	over_the_air.url	<y0000000000xx>.cfg
Description	It configures the access URL of the handset firmware file. Note: The priority of parameter "over_the_air.url" is lower than "over_the_air.url.w56h"/"over_the_air.url.w53h"/"over_the_air.url.cp930w".	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Settings->Upgrade->Select and Upgrade Handset Firmware	
Parameter	over_the_air.url.w56h	<y0000000000xx>.cfg
Description	It configures the access URL of the W56H handset firmware file. Note: The priority of parameter "over_the_air.url.w56h" is higher than "over_the_air.url".	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	over_the_air.url.w53h	<y0000000000xx>.cfg
Description	It configures the access URL of the W53H handset firmware file. Note: The priority of parameter "over_the_air.url.w53h" is higher than "over_the_air.url".	
Permitted Values	URL within 512 characters	
Default	Blank	
Parameter	over_the_air.url.cp930w	<y0000000000xx>.cfg
Description	It configures the access URL of the CP930W phone firmware file. Note: The priority of parameter "over_the_air.url.cp930w" is higher than "over_the_air.url".	
Permitted Values	URL within 512 characters	
Default	Blank	
Parameter	over_the_air.handset_tip	<y0000000000xx>.cfg
Description	It enables or disables to pop up a tip when upgrading the handset firmware from the provisioning server. Note: It works only if "over_the_air.base_trigger" and "over_the_air.handset_trigger" are set to 0 (Disabled). It is not applicable to DD phones.	
Permitted Values	0 -Disabled 1 -Enabled, the handset will pop up the message "Handset has a new firmware, update now?".	
Default	1	
Parameter	over_the_air.handset_trigger	<y0000000000xx>.cfg
Description	It enables or disables to upgrade the handset firmware compulsively when the handset is registered to a base station or turned on successfully.	

	It is only applicable when the current handset firmware is different with the one on provisioning server. Note: It works only if "over_the_air.base_trigger" is set to 0 (Disabled). It is not applicable to DD phones.	
Permitted Values	<p>0-Disabled, if "over_the_air.handset_tip" is set to 1 (Enabled), it will pop up a tip on the handset to notify the user to confirm upgrading the firmware or not. If "over_the_air.handset_tip" is set to 0, you may go to Settings->Upgrade Firmware (for CP930W-Base phones, you may go to Menu->Settings->Basic Settings->Upgrade Firmware) on the handset to trigger the upgrading manually.</p> <p>1-Enabled, it will upgrade the handset firmware compulsively without a pop-up tip on the handset.</p>	
Default	1	
Parameter	over_the_air.base_trigger	<y0000000000xx>.cfg
Description	It enables or disables to upgrade the handset firmware compulsively when the base station detects a new handset firmware from the provisioning server.	
Permitted Values	<p>0-Disabled, if "over_the_air.handset_tip" is set to 1 (Enabled), it will pop up a tip on the handset to notify the user to confirm upgrading the firmware or not. If "over_the_air.handset_tip" is set to 0, you may go to Settings->Upgrade Firmware (for CP930W-Base phones, you may go to Menu->Settings->Basic Settings->Upgrade Firmware) on the handset to trigger the upgrading manually.</p> <p>1-Enabled, it will upgrade the handset firmware compulsively without a pop-up tip on the handset.</p>	
Default	1	

Handset Customization

You can make the phone more personalized by customizing various settings.

Topics

- [Power Indicator LED of Handset](#)
- [Handset Keypad Light](#)
- [Handset Backlight](#)
- [Handset Wallpaper](#)
- [Handset Screen Saver](#)
- [Handset Name](#)
- [Language](#)
- [Time and Date](#)
- [Input Method](#)
- [Search Source List in Dialing](#)
- [Call Display](#)
- [Display Method on Dialing](#)
- [Key As Send](#)
- [Recent Call Display in Dialing](#)
- [Warnings Display](#)
- [Advisory Tones](#)
- [Bluetooth](#)

Power Indicator LED of Handset

Handset power indicator LED indicates power status and phone status.

You can configure the power LED indicator behavior in the following scenarios:

- the handset is idle
- the handset receives an incoming call
- the handset receives a voice mail

It is not applicable to CP930W-Base phones.

Topic

[Power Indicator LED of Handset Configuration](#)

Power Indicator LED of Handset Configuration

The following table lists the parameters you can use to configure the power indicator LED of handset.

Parameter	phone_setting.common_power_led_enable	<y0000000000xx>.cfg
Description	It enables or disables the handset power indicator LED to be turned on when the handset is idle.	
Permitted Values	0 -Disabled (handset power indicator LED is off) 1 -Enabled (handset power indicator LED is solid red)	
Default	0	
Web UI	Features->Power LED->Common Power Light On	

Parameter	phone_setting.ring_power_led_flash_enable	<y0000000000xx>.cfg
Description	It enables or disables the handset power indicator LED to flash when the handset receives an incoming call.	
Permitted Values	0 -Disabled (handset power indicator LED is off) 1 -Enabled (handset power indicator LED fast flashes (300ms) red)	
Default	1	
Web UI	Features->Power LED->Ring Power Light Flash	
Parameter	phone_setting.mail_power_led_flash_enable	<y0000000000xx>.cfg
Description	It enables or disables the handset power indicator LED to flash when the handset receives a voice mail.	
Permitted Values	0 -Disabled (handset power indicator LED does not flash) 1 -Enabled (handset power indicator LED slow flashes (1000ms) red)	
Default	1	
Web UI	Features->Power LED->Voice/Text Mail Power Light Flash	
Parameter	phone_setting.missed_call_power_led_flash.enable	<y0000000000xx>.cfg
Description	It enables or disables the handset power indicator LED to flash when the handset receives an incoming call.	
Permitted Values	0 -Disabled (handset power indicator LED does not flash) 1 -Enabled (handset power indicator LED slow flashes (1000ms) red)	
Default	1	
Web UI	Features->Power LED->MissCall Power Light Flash	

Handset Keypad Light

You can enable the handset keypad light to make the keypad light up when any key is pressed. This helps you distinguish keys from each other in a dark environment.

It is not applicable to DD phone and CP930W-Base phones.

Topic

[Handset Keypad Light Configuration](#)

Handset Keypad Light Configuration

The following table lists the parameter you can use to configure the handset keypad light.

Parameter	custom.handset.keypad_light.enable	<y0000000000xx>.cfg
Description	It enables or disables the handset to turn on the keypad light (digital key, # key, * key, TRAN key and Mute key) when any key is pressed. Note: It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	
Permitted Values	0 -Disabled 1 -Enabled	

Default	1
Handset UI	OK->Settings->Display->Keypad LED

Handset Backlight

The handset supports different backlight status and you can configure it.

For W53P/W60P, the backlight in charger or out of charger can be configured independently. You can enable the backlight to be on for about 30 minutes when the handset is charged, and then you can check the charging state during this period. You can also enable the backlight to be on for about 30 minutes when the handset is not charged. The backlight will be turned off after the handset is idle for a period of time. When an incoming call arrives, a key is pressed or the status of handset changes, the backlight is automatically turned on.

For CP930W-Base phones, the backlight automatically turns off, when the phone is charging and inactive for a specified time. You can only change the specified time by navigating to **Menu->Settings->Basic Settings->Display->Display Backlight**.

This feature is not applicable to DD phones.

Topic

[Handset Backlight Configuration](#)

Handset Backlight Configuration

The following table lists the parameters you can use to configure the handset backlight.

Parameter	custom.handset.backlight_in_charger.enable	<y0000000000xx>.cfg
Description	It enables or disables the handset backlight to be on for about 30 minutes when it is in the charging state. Note: It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). It is not applicable to CP930W-Base phones.	
Permitted Values	0 -Disabled, the backlight will be turned off after the handset is idle for about 10 seconds. 1 -Enabled, the backlight will be turned off after the handset is idle for about 30 minutes.	
Default	1	
Handset UI	OK->Settings->Display->Display Backlight->In Charger	
Parameter	custom.handset.backlight_out_of_charger.enable	<y0000000000xx>.cfg
Description	It enables or disables the handset backlight to be on for about 30 minutes when it is not in the charging state. Note: It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). It is not applicable to CP930W-Base phones.	
Permitted Values	0 -Disabled, the backlight will be turned off after the handset is idle for about 10 seconds. 1 -Enabled, the backlight will be turned off after the handset is idle for about 30 minutes.	
Default	0	
Handset UI	OK->Settings->Display->Display Backlight->Out Of Charger	

Handset Wallpaper

Wallpaper is an image used as the background in the handset idle screen. Users can select an image from handset's built-in background.

It is not applicable to DD phone and CP930W-Base.

Topic

[Handset Wallpaper Configuration](#)

Handset Wallpaper Configuration

The following table lists the parameter you can use to configure the handset wallpaper.

Parameter	custom.handset.wallpaper	<y0000000000xx>.cfg
Description	It configures the wallpaper displayed on the handset LCD screen. Note: It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	
Permitted Values	1-Wallpaper1 2-Wallpaper2 3-Wallpaper3 4-Wallpaper4 5-Wallpaper5	
Default	-1, do not change the wallpaper set on each handset.	
Handset UI	OK->Settings->Display->Wallpaper	

Handset Screen Saver

The screen saver of the handset is designed to protect your LCD screen. You can enable the screen saver to protect the LCD screen, an analog clock will be activated and appear on the LCD screen after the handset is idle for approximately 10 seconds.

It is not applicable to DD phone and CP930W-Base.

Topic

[Handset Screen Saver Configuration](#)

Handset Screen Saver Configuration

The following table lists the parameter you can use to configure the handset screen saver.

Parameter	custom.handset.screen_saver.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables screen saver feature. Note: It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled, an analog clock will be activated and appear on the LCD screen if no user activity is sensed for	

	approximately 10 seconds.
Default	1
Handset UI	OK->Settings->Display->Screen Saver

Handset Name

The handset will be assigned a name by default if successfully registered to the base station. You can personalize the handset name.

Topic

[Handset Name Configuration](#)

Handset Name Configuration

The following table lists the parameter you can use to configure the handset name.

Parameter	handset.X.name ^[1]	<y0000000000xx>.cfg
Description	It configures the name of the handset. Note: If it is set to blank, it will display the corresponding default handset name.	
Permitted Values	String within 24 characters	
Default	The handset name for handset 1 is Handset 1. The handset name for handset 2 is Handset 2. The handset name for handset 3 is Handset 3. The handset name for handset 4 is Handset 4. The handset name for handset 5 is Handset 5. The handset name for handset 6 is Handset 6. The handset name for handset 7 is Handset 7. The handset name for handset 8 is Handset 8.	
Web UI	Account->Handset Name->Handset X ^[1]	
Handset UI	W53P/W60P: OK->Settings->Handset Name DD Phone/CP930W-Base: Menu->Settings->Basic Settings->Phone Name	

^[1]X is the handset ID. X=1-8.

Language

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

Topics

[Supported Languages](#)

Language Display Configuration
Language for Web Display Customization

Supported Languages

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>.

The following table lists available languages and associated language packs supported by the handset user interface and the web user interface.

Phone User Interface		Web User Interface		
Language	Language Pack	Language	Language Pack	Note Language Pack
English	/	English	1.English.js	1.English_note.xml
French	/	French	4.French.js	4.French_note.xml
German	/	German	5.German.js	5.German_note.xml
Italian	/	Italian	6.Italian.js	6.Italian_note.xml
Polish	/	Polish	7.Polish.js	7.Polish_note.xml
Portuguese	/	Portuguese	8.Portuguese.js	8.Portuguese_note.xml
Spanish	/	Spanish	9.Spanish.js	9.Spanish_note.xml
Turkish	/	Turkish	10.Turkish.js	10.Turkish_note.xml
Russian	/	Russian	11.Russian.js	11.Russian_note.xml

Language Display Configuration

The default language displayed on the phone/handset user interface is English. If your web browser displays a language not supported by the IP phone, the web user interface will display English by default. You can specify the languages for the phone/handset user interface and web user interface respectively.

The following table lists the parameters you can use to configure language display.

Parameter	lang.wui	<y0000000000xx>.cfg
Description	It configures the language used on the web user interface.	
Permitted Values	English, French, German, Italian, Polish, Portuguese, Spanish, Turkish, Russian or the custom language name.	
Default	English	
Web UI	On the top-right corner of the web user interface	
Parameter	custom.handset.language	<y0000000000xx>.cfg
Description	It configures the language used on the handset user interface. Note: It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). It is not applicable to DD phones.	
Permitted	0-English	

Values	1 -French 2 -German 3 -Italian 4 -Polish 5 -Portuguese 6 -Spanish 7 -Turkish 8 -Swedish 9 -Russian
Default	0
Handset UI	W53P/W60P: OK->Settings->Language DD Phone/CP930W-Base: Menu->Settings->Basic Settings->Language

Language for Web Display Customization

You can customize the translation of the existing language on the web user interface. You can modify translation of an existing language or add a new language for web display.

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>.

Topics

[Customizing a Language Pack for Web Display](#)
[Custom Language for Web Display Configuration](#)

Customizing a Language Pack for Web Display

When you add a new language pack for the web user interface, the language pack must be formatted as "X.name.js" (X starts from 12, "name" is replaced with the language name). If the language name is the same as the existing one, the newly uploaded language file will override the existing one. We recommend that the file name of the new language pack should not be the same as the existing one.

Note

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

Procedure

Open the desired language template pack (for example, 1.English.js) using an ASCII editor.

Modify the characters within the double quotation marks on the right of the colon. Do not 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:

```

1 var _objTrans =
2 {
3   //login.htm
4   "The username can not be empty.":"The username can
5   "Failed to connect to the server. Please check net
6   "Login":"Login",
7   "Username":"Username",
8   "Password":"Password",
9   "Confirm":"Confirm",
10  "admin":"admin",
11  "user":"user",
12  "var":"var",
13
14  //header.htm
15  "Log_Out":"Log Out",
16  "Status":"Status",
17  "Network":"Network",
18  "Dsskey":"Dsskey",
19  "Features":"Features",
20  "Settings":"Settings",
21  "Directory":"Directory",
22  "Security":"Security",
23  "Applications":"Applications",
24

```

Save the language pack and place it to the provisioning server.

Customizing a Language Pack for Note Display

When you add a new language pack for the note, the note language pack must be formatted as "X.name_note.xml" (X starts from 12, "name" is replaced with the language name). If the note language name is the same as the existing one, the new uploaded note language pack will override the existing one. We recommend that the filename of the new note language pack should not be the same as the existing one.

Procedure

Open the desired note language template pack (for example, 1.English_note.xml) using an XML editor.

Modify the text of the note field. Do not modify the note name.

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

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <notedata>
3
4 <status>
5
6 <note name = "version">
7   <head>Description:</head>
8   <text>It shows the current firmware version and hardware version of the device.</text>
9 </note>
10 <note name = "DeviceCertificate">
11   <head>Description:</head>
12   <text>It shows the Device Certificate of the device.</text>
13 </note>
14 <note name = "network">
15   <head>Description:</head>
16   <text>It shows the IP address mode of the device.</text>
17 </note>
18 <note name = "network-ipv4">
19   <head>Description:</head>
20   <text>It shows the basic IPv4 network configurations.</text>
21 </note>
22 <note name = "network-ipv6">
23   <head>Description:</head>
24   <text>It shows the basic IPv6 network configurations.</text>
25 </note>

```

Save the note language pack and place it to the provisioning server.

Custom Language for Web Display Configuration

If you want to add a new language (for example, Wuilan) to phones, prepare the language file named as "12.Wuilan.js" for downloading. After the update, you will find a new language selection "Wuilan" at the top-right corner of the web user interface.

The following table lists the parameters you can use to configure a custom language for web display.

Parameter	wui_lang.url	<y0000000000xx>.cfg
Description	It configures the access URL of the custom language pack for the web user interface.	
Permitted Values	URL within 511 characters For example: http://localhost/X.GUI.name.lang X starts from 012, "name" is replaced with the language name	
Default	Blank	
Parameter	wui_lang.delete	<y0000000000xx>.cfg
Description	It deletes the specified or all custom web language packs and note language packs of the web user interface.	
Permitted Values	http://localhost/all or http://localhost/Y.name.js Y starts from 012, "name" is replaced with the language name	
Default	Blank	

Time and Date

Yealink phones maintain a local clock. You can choose to get the time and date from SNTP (Simple Network Time Protocol) time server to have the most accurate time and set DST (Daylight Saving Time) to make better use of daylight and to conserve energy, or you can set the time and date manually. The time and date can be displayed in several formats on the idle screen.

Topics

[Time Zone](#)

[NTP Settings](#)

[DST Settings](#)

[Time and Date Manually Configuration](#)

[Time and Date Format Configuration](#)

[Date Customization Rule](#)

Time Zone

The following table lists the values you can use to set the time zone location.

Time Zone	Time Zone Name	Time Zone	Time Zone Name
-12	Eniwetok,Kwajalein	+2	Estonia(Tallinn)
-11	Midway Island	+2	Finland(Helsinki)
-11	Samoa	+2	Gaza Strip(Gaza)
-10	United States-Hawaii-Aleutian	+2	Greece(Athens)

Time Zone	Time Zone Name	Time Zone	Time Zone Name
-10	United States-Alaska-Aleutian	+2	Israel(Tel Aviv)
-9:30	French Polynesia	+2	Jordan(Amman)
-9	United States-Alaska Time	+2	Latvia(Riga)
-8	Canada(Vancouver,Whitehorse)	+2	Lebanon(Beirut)
-8	Mexico(Tijuana,Mexicali)	+2	Moldova(Kishinev)
-8	United States-Pacific Time	+2	Jerusalem
-8	Baja California	+2	Russia(Kaliningrad)
-7	Canada(Edmonton,Calgary)	+2	Bulgaria(Sofia)
-7	Mexico(Mazatlan,Chihuahua)	+2	Lithuania(Vilnius)
-7	United States-Mountain Time	+2	Cairo
-7	United States-MST no DST	+2	Istanbul
-7	Chihuahua,La Paz	+2	E.Europe
-7	Arizona	+2	Tripoli
-6	Guatemala	+2	Romania(Bucharest)
-6	El Salvador	+2	Syria(Damascus)
-6	Honduras	+2	Turkey(Ankara)
-6	Nicaragua	+2	Ukraine(Kyiv, Odessa)
-6	Costa Rica	+3	East Africa Time
-6	Belize	+3	Iraq(Baghdad)
-6	Canada-Manitoba(Winnipeg)	+3	Russia(Moscow)
-6	Chile(Easter Islands)	+3	St.Petersburg
-6	Guadalajara	+3	Kuwait,Riyadh
-6	Monterrey	+3	Nairobi
-6	Mexico(Mexico City,Acapulco)	+3	Minsk
-6	Saskatchewan	+3	Volgograd (RTZ 2)
-6	United States-Central Time	+3:30	Iran(Teheran)
-5	Bogota,Lima	+4	Armenia(Yerevan)
-5	Quito	+4	Azerbaijan(Baku)
-5	Peru	+4	Georgia(Tbilisi)
-5	Indiana (East)	+4	Kazakhstan(Aktau)
-5	Bahamas(Nassau)	+4	Russia(Samara)

Time Zone	Time Zone Name	Time Zone	Time Zone Name
-5	Canada(Montreal,Ottawa,Quebec)	+4	Abu Dhabi,Muscat
-5	Cuba(Havana)	+4	Izhevsk,Samara (RTZ 3)
-5	United States-Eastern Time	+4	Port Louis
-4:30	Venezuela(Caracas)	+4:30	Afghanistan(Kabul)
-4	Canada(Halifax,Saint John)	+5	Kazakhstan(Aqtobe)
-4	Atlantic Time (Canada)	+5	Kyrgyzstan(Bishkek)
-4	San Juan	+5	Ekaterinburg (RTZ 4)
-4	Manaus,Cuiaba	+5	Karachi
-4	Georgetown	+5	Tashkent
-4	Chile(Santiago)	+5	Pakistan(Islamabad)
-4	Paraguay(Asuncion)	+5	Russia(Chelyabinsk)
-4	United Kingdom-Bermuda(Bermuda)	+5:30	India(Calcutta)
-4	United Kingdom(Falkland Islands)	+5:30	Mumbai,Chennai
-4	Trinidad&Tobago	+5:30	Kolkata,New Delhi
-3:30	Canada-New Foundland(St.Johns)	+5:30	Sri Jayawardenepura
-3	Greenland(Nuuk)	+5:45	Nepal(Katmandu)
-3	Argentina(Buenos Aires)	+6	Kazakhstan(Astana, Almaty)
-3	Brazil(no DST)	+6	Russia(Novosibirsk,Omsk)
-3	Brasilia	+6	Bangladesh(Dhaka)
-3	Cayenne,Fortaleza	+6:30	Myanmar(Naypyitaw)
-3	Montevideo	+6:30	Yangon (Rangoon)
-3	Salvador	+7	Russia(Krasnoyarsk)
-3	Brazil(DST)	+7	Thailand(Bangkok)
-2:30	Newfoundland and Labrador	+7	Vietnam(Hanoi)
-2	Brazil(no DST)	+7	Jakarta
-2	Mid-Atlantic	+8	China(Beijing)
-1	Portugal(Azores)	+8	Singapore(Singapore)
-1	Cape Verde Islands	+8	Hong Kong,Urumqi
0	GMT	+8	Taipei
0	Western Europe Time	+8	Kuala Lumpur
0	Monrovia	+8	Australia(Perth)

Time Zone	Time Zone Name	Time Zone	Time Zone Name
0	Reykjavik	+8	Russia(Irkutsk, Ulan-Ude)
0	Casablanca	+8	Ulaanbaatar
0	Denmark-Faroe Islands(Torshavn)	+8:45	Eucla
0	Ireland(Dublin)	+9	Korea(Seoul)
0	Edinburgh	+9	Japan(Tokyo)
0	Portugal(Lisboa,Porto,Funchal)	+9	Russia(Yakutsk,Chita)
0	Spain-Canary Islands(Las Palmas)	+9:30	Australia(Adelaide)
0	United Kingdom(London)	+9:30	Australia(Darwin)
0	Lisbon	+10	Australia(Sydney,Melboume,Canberra)
0	Morocco	+10	Australia(Brisbane)
+1	Albania(Tirane)	+10	Australia(Hobart)
+1	Austria(Vienna)	+10	Russia(Vladivostok)
+1	Belgium(Brussels)	+10	Magadan (RTZ 9)
+1	Caicos	+10	Guam,Port Moresby
+1	Belgrade	+10	Solomon Islands
+1	Bratislava	+10:30	Australia(Lord Howe Islands)
+1	Ljubljana	+11	New Caledonia(Noumea)
+1	Chad	+11	Chokurdakh (RTZ 10)
+1	Copenhagen	+11	Russia(Srednekolymsk Time)
+1	West Central Africa	+11:30	Norfolk Island
+1	Poland(Warsaw)	+12	New Zealand(Wellington,Auckland)
+1	Spain(Madrid)	+12	Fiji Islands
+1	Croatia(Zagreb)	+12	Russia(Kamchatka Time)
+1	Czech Republic(Prague)	+12	Anadyr
+1	Denmark(Kopenhagen)	+12	Petropavlovsk-Kamchatsky (RTZ 11)
+1	France(Paris)	+12	Marshall Islands
+1	Germany(Berlin)	+12:45	New Zealand(Chatham Islands)
+1	Hungary(Budapest)	+13	Nuku'alofa
+1	Italy(Rome)	+13	Tonga(Nukualofa)
+1	Switzerland(Bern)	+13:30	Chatham Islands
+1	Sweden(Stockholm)	+14	Kiribati

Time Zone	Time Zone Name	Time Zone	Time Zone Name
+1	Luxembourg(Luxembourg)		
+1	Macedonia(Skopje)		
+1	Netherlands(Amsterdam)		
+1	Namibia(Windhoek)		

NTP Settings

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

Topic

[NTP Configuration](#)

NTP Configuration

The following table lists the parameters you can use to configure the NTP.

Parameter	local_time.manual_ntp_srv_prior	<y0000000000xx>.cfg
Description	It configures the priority for the phone to use the NTP server address offered by the DHCP server.	
Permitted Values	0 - High (use the NTP server address offered by the DHCP server preferentially) 1 - Low (use the NTP server address configured manually preferentially)	
Default Value	0	
Web UI	Settings->Time&Date->NTP by DHCP Priority	
Parameter	local_time.dhcp_time	<y0000000000xx>.cfg
Description	It enables or disables the phone to update time with the offset time offered by the DHCP server. Note: It is only available to offset from Greenwich Mean Time GMT 0.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Settings->Time&Date->DHCP Time	
Parameter	local_time.ntp_server1	<y0000000000xx>.cfg
Description	It configures the IP address or the domain name of the primary NTP server.	
Permitted Values	IP address or domain name	
Default	cn.pool.ntp.org	
Web UI	Settings->Time&Date->Primary Server	
Parameter	local_time.ntp_server2	<y0000000000xx>.cfg
Description	It configures the IP address or the domain name of the secondary NTP server. If the primary NTP server is not configured by the parameter "local_time.ntp_server1", or cannot be	

	accessed, the phone will request the time and date from the secondary NTP server.	
Permitted Values	IP address or domain name	
Default	pool.ntp.org	
Web UI	Settings->Time&Date->Secondary Server	
Parameter	local_time.interval	<y0000000000xx>.cfg
Description	It configures the interval (in seconds) at which the phone updates time and date from the NTP server.	
Permitted Values	Integer from 15 to 86400	
Default	1000	
Web UI	Settings->Time&Date->Update Interval (15~86400s)	
Parameter	local_time.time_zone	<y0000000000xx>.cfg
Description	It configures the time zone.	
Permitted Values	-12 to +14 For available time zones, refer to Time Zone .	
Default	+8	
Web UI	Settings->Time&Date->Time Zone	
Parameter	local_time.time_zone_name	<y0000000000xx>.cfg
Description	It configures the time zone name. Note: It works only if "local_time.summer_time" is set to 2 (Automatic) and the parameter "local_time.time_zone" should be configured in advance.	
Permitted Values	String within 32 characters The available time zone names depend on the time zone configured by the parameter "local_time.time_zone". For available time zone names, refer to Time Zone .	
Default	China(Beijing)	
Web UI	Settings->Time&Date->Location	

DST Settings

You can set DST for the desired area as required. By default, the DST is set to Automatic, so it can be adjusted automatically from the current time zone configuration.

The time zone and corresponding DST pre-configurations exist in the AutoDST file. If the DST is set to Automatic, the 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.

Topics

[Auto DST File Attributes](#)
[Customizing Auto DST File](#)

Auto DST File Attributes

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

Attributes	Type	Values	Description
szTime	required	[+/-][X]:[Y], X=0~14, Y=0~59	Time Zone
szZone	required	String (if the content is more than one city, it is the best to keep their daylight saving time the same)	Time Zone name
iType	optional	0/1 0: DST by Date 1: DST by Week	DST time type (This item is needed if you want to configure DST.)
szStart	optional	Month/Day/Hour (for iType=0) Month: 1~12 Day: 1~31 Hour: 0 (midnight)~23 Month/Week of Month/Day of Week/Hour of Day (for iType=1) Month: 1~12 Week of Month: 1~5 (the last week) Day of Week: 1~7 Hour of Day: 0 (midnight)~23	Starting time of the DST
szEnd	optional	Same as szStart	Ending time of the DST
szOffset	optional	Integer from -300 to 300	The offset time (in minutes) of DST

Customizing Auto DST File

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>.

1. Open the AutoDST file.
2. To add a new time zone, add `<DST szTime="" szZone="" iType="" szStart="" szEnd="" szOffset="" />` between `<DSTData>` and `</DSTData>`.
3. Specify the DST attribute values within double quotes.

For example:

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

`<DST szTime="+6" szZone="Paradise" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="30"/>`

```

AutoDST.xml x
<DST szTime="+4:30" szZone="Afghanistan (Kabul)" />
<DST szTime="+5" szZone="Kazakhstan (Aqtobe)" />
<DST szTime="+5" szZone="Kyrgyzstan (Bishkek)" />
<DST szTime="+5" szZone="Pakistan (Islamabad)" iType="0" szStart="4/15/0" szEnd="11/1/0" />
<DST szTime="+5" szZone="Russia (Chelyabinsk)" />
<DST szTime="+5:30" szZone="India (Calcutta)" />
<DST szTime="+5:45" szZone="Nepal (Katmandu)" />
<DST szTime="+6" szZone="Paradise" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="30"/>
<DST szTime="+6" szZone="Kazakhstan (Astana, Almaty)" />
<DST szTime="+6" szZone="Russia (Novosibirsk, Omsk)" />

```

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)".

```

AutoDST.xml* x
0 20 40 60 80 100 110
<DST szTime="+3:30" szZone="Iran (Teheran)" iType="0" szStart="3/22/0" szEnd="9/22/0" szOffset="60"/>
<DST szTime="+4" szZone="Armenia (Yerevan)" iType="1" szStart="3/5/7/2" szEnd="10/5/7/3" szOffset="60"/>
<DST szTime="+4" szZone="Azerbaijan (Baku)" iType="1" szStart="3/5/7/4" szEnd="10/5/7/5" szOffset="60"/>
<DST szTime="+4" szZone="Georgia (Tbilisi)" />
<DST szTime="+4" szZone="Kazakhstan (Aktau)" />
<DST szTime="+4" szZone="Russia (Samara)" />
<DST szTime="+4:30" szZone="Afghanistan (Kabul)" />
<DST szTime="+5" szZone="Kazakhstan (Aqtobe)" />
<DST szTime="+5" szZone="Kyrgyzstan (Bishkek)" />
<DST szTime="+5" szZone="Pakistan (Islamabad)" iType="0" szStart="4/15/0" szEnd="11/1/0" szOffset="60"/>
<DST szTime="+5" szZone="Russia (Chelyabinsk)" />
<DST szTime="+5:30" szZone="India (Calcutta)" iType="1" szStart="9/5/7/3" szEnd="4/1/7/2" szOffset="60"/>
<DST szTime="+5:45" szZone="Nepal (Katmandu)" />
<DST szTime="+6" szZone="Kazakhstan (Astana, Almaty)" />
<DST szTime="+6" szZone="Russia (Novosibirsk, Omsk)" />
<DST szTime="+6:30" szZone="Myanmar (Naypyitaw)" />
<DST szTime="+7" szZone="Russia (Krasnoyarsk)" />
<DST szTime="+7" szZone="Thailand (Bangkok)" />
<DST szTime="+8" szZone="China (Beijing)" />
<DST szTime="+8" szZone="Singapore (Singapore)" />
    
```

4. Save this file and place it to the provisioning server.

Related Topic

[Time Zone](#)

DST Configuration

The following table lists the parameters you can use to configure DST.

Parameter	local_time.summer_time	<y0000000000xx>.cfg
Description	It configures Daylight Saving Time (DST) feature.	
Permitted Values	0 -Disabled 1 -Enabled 2 -Automatic	
Default	2	
Web UI	Settings->Time&Date->Daylight Saving Time	
Parameter	local_time.dst_time_type	<y0000000000xx>.cfg
Description	It configures the Daylight Saving Time (DST) type. Note: It works only if "local_time.summer_time" is set to 1 (Enabled).	
Permitted Values	0 -DST by Date 1 -DST by Week	
Default	0	
Web UI	Settings->Time&Date->Fixed Type	
Parameter	local_time.start_time	<y0000000000xx>.cfg
Description	It configures the start time of the Daylight Saving Time (DST). Note: It works only if "local_time.summer_time" is set to 1 (Enabled).	
Permitted Values	Month/Day/Hour-DST by Date, use the following mapping: Month: 1=January, 2=February, ..., 12=December Day: 1=the first day in a month, ..., 31= the last day in a month	

	<p>Hour: 0=0am, 1=1am,..., 23=11pm</p> <p>Month/Week of Month/Day of Week/Hour of Day-DST by Week, use the following mapping:</p> <p>Month: 1=January, 2=February,..., 12=December</p> <p>Week of Month: 1=the first week in a month,..., 5=the last week in a month</p> <p>Day of Week: 1=Monday, 2=Tuesday,..., 7=Sunday</p> <p>Hour of Day: 0=0am, 1=1am,..., 23=11pm</p>	
Default	1/1/0	
Web UI	Settings->Time&Date->Start Date	
Parameter	local_time.end_time	<y0000000000xx>.cfg
Description	<p>It configures the end time of the Daylight Saving Time (DST).</p> <p>Note: It works only if "local_time.summer_time" is set to 1 (Enabled).</p>	
Permitted Values	<p>Month/Day/Hour-DST by Date, use the following mapping:</p> <p>Month: 1=January, 2=February,..., 12=December</p> <p>Day: 1=the first day in a month,..., 31= the last day in a month</p> <p>Hour: 0=0am, 1=1am,..., 23=11pm</p> <p>Month/Week of Month/Day of Week/Hour of Day-DST by Week, use the following mapping:</p> <p>Month: 1=January, 2=February,..., 12=December</p> <p>Week of Month: 1=the first week in a month,..., 5=the last week in a month</p> <p>Day of Week: 1=Monday, 2=Tuesday,..., 7=Sunday</p> <p>Hour of Day: 0=0am, 1=1am,..., 23=11pm</p>	
Default	12/31/23	
Web UI	Settings->Time&Date->End Date	
Parameter	local_time.offset_time	<y0000000000xx>.cfg
Description	<p>It configures the offset time (in minutes) of Daylight Saving Time (DST).</p> <p>Note: It works only if "local_time.summer_time" is set to 1 (Enabled).</p>	
Permitted Values	Integer from -300 to 300	
Default	Blank	
Web UI	Settings->Time&Date->Offset(minutes)	
Parameter	auto_dst.url	<y0000000000xx>.cfg
Description	<p>It configures the access URL of the DST file (AutoDST.xml).</p> <p>Note: It works only if "local_time.summer_time" is set to 2 (Automatic).</p>	
Permitted Values	URL within 511 characters	
Default	Blank	

Time and Date Manually Configuration

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

The following table lists the parameter you can use to configure time and date manually.

Parameter	local_time.manual_time_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to obtain time and date from manual settings.	
Permitted Values	0 -Disabled, the phone obtains time and date from NTP server. 1 -Enabled	
Default	0	
Web UI	Settings->Time&Date->Manual Time	

Time and Date Format Configuration

You can customize the time and date by choosing between a variety of time and date formats, including options to date format with the day, month, or year, and time format in 12 hours or 24 hours, or you can also custom the date format as required.

The following table lists the parameters you can use to configure time and date format.

Parameter	custom.handset.time_format	<y0000000000xx>.cfg
Description	It configures the time format for all registered handsets. Note: It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	
Permitted Values	0 -Hour 12, the time will be displayed in 12-hour format with AM or PM specified. 1 -Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).	
Default	1	
Web UI	Settings->Time&Date->Time Format	
Handset UI	W53P/W60P: OK->Settings->Display->Time Format DD Phone: Menu->Settings->Basic Settings->Time&Date->Time & Date Format->Time Format CP930W-Base: Menu->Settings->Basic Settings->Display->Time Format	
Parameter	custom.handset.date_format	<y0000000000xx>.cfg
Description	It configures the date format for all registered handsets. Note: The value configured by the parameter "lcl.datetime.date.format" takes precedence over that configured by this parameter.	
Permitted Values	0 -WWW MMM DD 1 -DD-MMM-YY 2 -YYYY-MM-DD 3 -DD/MM/YYYY	

	<p>4-MM/DD/YY</p> <p>5-DD MMM YYYY</p> <p>6-WWW DD MMM</p> <p>Use the following mapping:</p> <p>"WWW" represents the abbreviation of the week;</p> <p>"DD" represents a two-digit day;</p> <p>"MMM" represents the first three letters of the month;</p> <p>"YYYY" represents a four-digit year, and "YY" represents a two-digit year.</p>	
Default	0	
Web UI	Settings->Time&Date->Date Format	
Handset UI	<p>W53P/W60P:</p> <p>OK->Settings->Display->Date Format</p> <p>DD Phone:</p> <p>Menu->Settings->Basic Settings->Time&Date->Time & Date Format->Date Format</p> <p>CP930W-Base:</p> <p>Menu->Settings->Basic Settings->Display->Date Format</p>	
Parameter	local_time.time_format	<y0000000000xx>.cfg
Description	It configures the time format.	
Permitted Values	<p>0-Hour 12, the time will be displayed in 12-hour format with AM or PM specified.</p> <p>1-Hour 24, the time will be displayed in 24-hour format (for example, 2:00 PM displays as 14:00).</p>	
Default	1	
Web UI	Settings->Time&Date->Time Format	
Parameter	local_time.date_format	<y0000000000xx>.cfg
Description	It configures the date format.	
Permitted Values	<p>0-WWW MMM DD</p> <p>1-DD-MMM-YY</p> <p>2-YYYY-MM-DD</p> <p>3-DD/MM/YYYY</p> <p>4-MM/DD/YY</p> <p>5-DD MMM YYYY</p> <p>6-WWW DD MMM</p> <p>Use the following mapping:</p> <p>"WWW" represents the abbreviation of the week;</p> <p>"DD" represents a two-digit day;</p>	

	<p>"MMM" represents the first three letters of the month; "YYYY" represents a four-digit year, and "YY" represents a two-digit year.</p>	
Default	0	
Web UI	Settings->Time&Date->Date Format	
Parameter	lcl.datetime.date.format	<y0000000000xx>.cfg
Description	It configures the display format of the date.	
Permitted Values	<p>Any combination of W, M, D and the separator (for example, space, dash, slash). Any combination of Y, M, D, W and the separator (for example, space, dash, slash). Use the following mapping: Y = year, M = month, D = day, W = day of week "Y"/"YY" represents a two-digit year, more than two "Y" letters (for example, YYYY) represent a four-digit year; "M"/"MM" represents a two-digit month, "MMM" represents the abbreviation of the month, three or more than three "M" letters (for example, MMM) represent the long format of the month; One or more than one "D" (for example, DDD) represents a two-digit day; "W"/"WW" represents the abbreviation of the day of the week, three or more three "W" letters (for example, WWW) represent the long format of the day of the week. For the more rules, refer to Date Customization Rule. Note: It will take effect on all handsets that are registered on the same base station. If configured, users can only change the date format via the handset.</p>	
Default	Blank	

Date Customization Rule

You need to know the following rules when customizing date formats:

Format	Description
Y/YY	It represents a two-digit year. For example, 16, 17, 18..
Y is used more than twice (for example, YYY, YYYY)	It represents a four-digit year. For example, 2016, 2017, 2018..
M/MM	It represents a two-digit month. For example, 01, 02,..., 12
MMM	It represents the abbreviation of the month. For example, Jan, Feb,..., Dec
D is used once or more than once (for example, DD)	It represents a two-digit day. For example, 01, 02,..., 31
W/WW	It represents the abbreviation of the day of week (not applicable to DD Phones).

Format	Description
	For example, Mon., Tues., Wed., Thur., Fri., Sat., Sun.
W is used more than twice (for example, WWW, WWWW)	It represents the long format of the day of week (only applicable to DD Phones). For example, Monday, Tuesday,..., Sunday

Input Method

Yealink phones support 12 input methods: Abc, 123, ABC, abc, ABГ, AÄÅ, äää, ŠŠš, ššš, абв, АБВ, אבג. You can also specify the default input method for the DECT IP phone when searching for contacts.

Topic

[Input Method Configuration](#)

Input Method Configuration

The following table lists the parameter you can use to configure the input method.

Parameter	directory.search_default_input_method	<y0000000000xx>.cfg
Description	It configures the default input method when the user searches for contacts in the Local Directory, LDAP, Remote Phone Book, Blacklist or Network Directory. Example: directory.search_default_input_method = 1	
Permitted Values	1 -Abc 2 -123 3 -ABC 4 -abc 5 -ABГ 6 -AÄÅ 7 -äää 8 -ŠŠš 9 -ššš 10 -абв 11 -АБВ 12 -אבג	
Default	1	

Search Source List in Dialing

Search source list in dialing allows you to search entries from the source list when the phone is on the pre-dialing/dialing screen. You can select the desired entry to dial out quickly.

The search source list can be configured using a supplied super search template file (super_search.xml).

Topics

[Search Source File Customization](#)

[Search Source List Configuration](#)

Search Source File Customization

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>.

Topics

[Search Source File Attributes](#)

[Customizing Search Source File](#)

Search Source File Attributes

The following table lists the attributes you can use to add source lists to the super search file:

Attributes	Valid Values	Description
id_name	local_directory_search callog_search remote_directory_search ldap_search BroadSoft_directory_search BroadSoft_UC_search google_directory_search	The directory list (For example, "local_directory_search" for the local directory list). Note: Do not edit this field.
display_name	Local Contacts History Remote Phonebook LDAP Network Directories BroadSoft Buddies Google Contacts	The display name of the directory list. Note: We recommend you do not edit this field.
priority	1 to 5 1 is the highest priority, 5 is the lowest.	The priority of the search results.
enable	0/1 0: Disabled 1: Enabled.	Enable or disable the phone to search the desired directory list.

Customizing Search Source File

1. Open the search source file.
2. To configure each directory list, edit the values within double quotes in the corresponding field.
For example, enable the local directory search, disable the call log search and specify a priority.

```
<item id_name="local_directory_search" display_name="Local Contacts" priority="1" enable="1" />
<item id_name="calllog_search" display_name="History" priority="2" enable="0" />
```

3. Save the change and place this file to the provisioning server.

Search Source List Configuration

The following table lists the parameters you can use to configure the search source list.

Parameter	super_search.url	<y0000000000xx>.cfg
Description	It configures the access URL of the custom super search file.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Directory->Setting->Search Source List In Dialing	
Parameter	search_in_dialing.local_directory.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to automatically search entries from the local directory, and display results on the pre-dialing/dialing screen.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Directory->Setting->Search Source List In Dialing	
Parameter	search_in_dialing.local_directory.priority	<y0000000000xx>.cfg
Description	It configures the search priority of the local directory.	
Permitted Values	Integer greater than or equal to 0	
Default	1	
Web UI	Directory->Setting->Search Source List In Dialing	
Parameter	search_in_dialing.history.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to automatically search entries from the call history list, and display results on the pre-dialing/dialing screen.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Directory->Setting->Search Source List In Dialing	
Parameter	search_in_dialing.history.priority	<y0000000000xx>.cfg
Description	It configures the search priority of the call history list.	
Permitted Values	Integer greater than or equal to 0	
Default	2	

Web UI	Directory->Setting->Search Source List In Dialing	
Parameter	search_in_dialing.remote_phone_book.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to automatically search entries from the remote phone book, and display results on the pre-dialing/dialing screen.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Directory->Setting->Search Source List In Dialing	
Parameter	search_in_dialing.remote_phone_book.priority	<y0000000000xx>.cfg
Description	It configures the search priority of the remote phone book.	
Permitted Values	Integer greater than or equal to 0	
Default	3	
Web UI	Directory->Setting->Search Source List In Dialing	
Parameter	search_in_dialing.ldap.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to automatically search entries from the LDAP, and display results on the pre-dialing/dialing screen.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Directory->Setting->Search Source List In Dialing	
Parameter	search_in_dialing.ldap.priority	<y0000000000xx>.cfg
Description	It configures the search priority of the LDAP.	
Permitted Values	Integer greater than or equal to 0	
Default	4	
Web UI	Directory->Setting->Search Source List In Dialing	

Call Display

By default, the phones present the contact information when receiving an incoming call, dialing an outgoing call or engaging in a call.

You can configure what contact information presents and how to display the contact information. If the contact exists in the phone directory, the phone displays the saved contact name and number. If not, it will use Calling Line Identification Presentation (CLIP) or Connected Line Identification Presentation (COLP) to display the contact's identity.

Topic

[Call Display Configuration](#)

Call Display Configuration

The following table lists the parameters you can use to configure call display.

Parameter	phone_setting.called_party_info_display.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to display the local identity when it receives an incoming call. Note: The information display method is configured by the parameter "phone_setting.call_info_display_method".	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Settings->Call Display->Display Called Party Information	
Parameter	phone_setting.call_info_display_method	<y0000000000xx>.cfg
Description	It configures the call information display method when the phone receives an incoming call, dials an outgoing call or is during a call.	
Permitted Values	0-Name+Number 1-Number+Name 2-Name 3-Number 4-Full Contact Info (display name<sip:xxx@domain.com>)	
Default	0	
Web UI	Settings->Call Display->Call Information Display Method	
Parameter	account.X.update_ack_while_dialing ^[1]	<MAC>.cfg
Description	It enables or disables the phone to update the display of call ID according to the ACK message.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Parameter	sip.disp_incall_to_info ^[2]	<y0000000000xx>.cfg
Description	It enables or disables the phone to display the identity contained in the To field of the INVITE message when it receives an incoming call.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	

^[2]If you change this parameter, the phone will reboot to make the change take effect.

Display Method on Dialing

When the phone is on the pre-dialing or dialing screen, the account information will be displayed on the phone screen.

Yealink phones support three display methods: Label, Display Name and User Name. You can customize the account information to be displayed on the IP phone as required.

Topic

[Display Method on Dialing Configuration](#)

Display Method on Dialing Configuration

The following table lists the parameters you can use to configure display method on dialing.

Parameter	features.caller_name_type_on_dialing	<y0000000000xx>.cfg
Description	It configures the selected account information displayed on the pre-dialing or dialing screen.	
Permitted Values	1 -Label, configured by the parameter "account.X.label". 2 -Display Name, configured by the parameter "account.X.display_name". 3 -User Name, configured by the parameter "account.X.user_name".	
Default	3	
Web UI	Features->General Information->Display Method on Dialing	

Key As Send

Key as send allows you to assign the pound key ("#") or asterisk key ("*") as the send key.

Topic

[Key As Send Configuration](#)

Key As Send Configuration

The following table lists the parameters you can use to configure key as send.

Parameter	features.key_as_send	<y0000000000xx>.cfg
Description	It configures the "#" or "*" key as the send key.	
Permitted Values	0 -Disabled, neither "#" nor "*" can be used as the send key. 1 -# key 2 -* key	
Default	1	
Web UI	Features->General Information->Key As Send	

Recent Call Display in Dialing

Recent call display allows you to view the placed calls list when the phone is on the dialing screen . You can select to place a call from the placed calls list.

Topic

[Recent Call in Dialing Configuration](#)

Recent Call in Dialing Configuration

The following table lists the parameter you can use to configure the recent call display in dialing.

Parameter	super_search.recent_call	<y0000000000xx>.cfg
Description	It enables or disables Recent Call in Dialing feature.	
Permitted Values	0 -Disabled 1 -Enabled, users can view the placed calls list when the phone is in the dialing screen.	
Default	1	
Web UI	Directory->Setting->Recent Call In Dialing	

Warnings Display

Yealink phones support displaying the warning details about the issue in the **Status** screen when the default password is used (not applicable to CP930W-Base phones).

Topic

[Warnings Display Configuration](#)

Warnings Display Configuration

The following table lists the parameter you can use to configure the warnings display.

Parameter	phone_setting.warnings_display.mode	<y0000000000xx>.cfg
Description	It enables or disables the phone to display warnings on the phone when the default password is in use.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	

Advisory Tones

Advisory tones are the acoustic signals of your handset, which inform you of different actions and states.

You can configure the following advisory tones independently of each other:

- **Keypad Tone:** plays when you press any key of the keypad. For CP930W-Base phones, you can only configure it by navigating to **Menu->Settings->Basic Settings->Sound->Advisory Tones->Keypad Tone**.
- **Touch Tone:** plays when you tap the keys (except the off-hook key and the touch keypad). You can only configure it by navigating to **Menu->Settings->Basic Settings->Sound->Advisory Tones->Touch Tone**. It is only applicable to CP930W-Base phones.
- **Confirmation:** plays when you save settings or place the handset in the charger cradle. For CP930W-Base phones, you can only configure it by navigating to **Menu->Settings->Basic Settings->Sound->Advisory Tones->Confirmation**.
- **Low Battery:** plays when battery capacity is low and the handset requires charging. For CP930W-Base phones, you can only configure it by navigating to **Menu->Settings->Basic Settings->Sound->Advisory Tones->Low Battery**.

Topic

[Advisory Tones Configuration](#)

Advisory Tones Configuration

The following table lists the parameters you can use to configure the advisory tones.

Parameter	custom.handset.keypad_tone.enable	<y0000000000xx>.cfg
Description	It enables or disables the handset to play a tone when any key is pressed. For CP930W-Base phones, it plays a tone only when the touch keypad is tapped. Note: It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off. It is not applicable to DD phones and CP930W-Base phones.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Handset UI	W53P/W60P: OK->Settings->Audio->Advisory Tones->Keypad Tone	
Parameter	custom.handset.confirmation_tone.enable	<y0000000000xx>.cfg
Description	It enables or disables the handset to play a tone when a user saves settings or places the handset in the charger cradle. Note: It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off. It is not applicable to DD phones and CP930W-Base phones.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Handset UI	W53P/W60P: OK->Settings->Audio->Advisory Tones->Confirmation	
Parameter	custom.handset.low_battery_tone.enable	<y0000000000xx>.cfg
Description	It enables or disables the handset to play a tone when battery capacity is low. Note: It will take effect on all handsets that are registered on the same base station. It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled) and the silent mode is off. It is not applicable to DD phones and CP930W-Base phones.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Handset UI	W53P/W60P: OK->Settings->Audio->Advisory Tones->Low Battery	

Bluetooth

CP930W-Base phones support Bluetooth. You can pair and connect the Bluetooth-enabled mobile phone with your phone, and make and receive mobile calls on the phone. After connecting the Bluetooth-Enabled mobile phone, you can also use your phone as a Bluetooth speaker for your mobile phone and PC. You can set up a conference among the calls on your IP phone, the PC and connected mobile phone.

Topic

Bluetooth Configuration

Bluetooth Configuration

You can activate or deactivate the Bluetooth mode, and personalize the Bluetooth device name for the IP phone. It is helpful for the other Bluetooth devices to identify and pair with your IP phone.

The following table lists the parameters you can use to configure Bluetooth.

Parameter	static.bluetooth.function.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the Bluetooth feature.	
Permitted Values	0 -Disabled, you are not allowed to trigger Bluetooth mode to on. 1 -Enabled	
Default	1	
Parameter	bluetooth.connect_confirm.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the phone to prompt users to confirm the connection request from the Bluetooth device.	
Permitted Values	0 -Disabled 1 -Enabled, the prompt will not appear during the call.	
Default	0	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Account Settings

This chapter shows you how to register accounts and configure account settings on Yealink phones.

Topics

[Account Registration](#)
[Outbound Proxy in Dialog](#)
[Server Redundancy](#)
[SIP Server Name Resolution](#)
[Static DNS Cache](#)
[Number of Active Handsets](#)
[Number of Simultaneous Outgoing Calls](#)
[Number Assignment](#)

Account Registration

Registering an account makes it easier for the phones to receive an incoming call or dial an outgoing call. The W60B supports registering multiple accounts ; each account requires an extension or phone number.

Topics

[Supported Accounts](#)
[Accounts Registration Configuration](#)
[Registration Settings Configuration](#)

Supported Accounts

The number of the registered accounts must meet the following:

Assigned Account(s)		Registered Accounts on W60B
W53P/W60P/W41P	CP930W-Base	
8	1	8

Accounts Registration Configuration

The following table lists the parameters you can use to register accounts.

Parameter	account.X.enable ^[1]	<MAC>.cfg
Description	It enables or disables the user to use a specific account.	
Permitted Values	0 -Disabled, the account is not available for the user. 1 -Enabled	
Default	0	
Web UI	Account->Register->Line Active	
Parameter	account.X.label ^[1]	<MAC>.cfg
Description	It configures the label to be displayed on the phone screen.	
Permitted Values	String within 99 characters	

Default	Blank	
Web UI	Account->Register->Label	
Parameter	account.X.display_name ^[1]	<MAC>.cfg
Description	It configures the display name for a specific account.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Account->Register->Display Name	
Parameter	account.X.auth_name ^[1]	<MAC>.cfg
Description	It configures the user name for register authentication.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Account->Register->Register Name	
Parameter	account.X.user_name ^[1]	<MAC>.cfg
Description	It configures the register user name.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Account->Register->User Name	
Parameter	account.X.password ^[1]	<MAC>.cfg
Description	It configures the password for register authentication.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Account->Register->Password	
Parameter	account.X.sip_server.Y.address ^{[1][2]}	<MAC>.cfg
Description	It configures the IP address or domain name of the SIP server Y in which the account is registered.	
Permitted Values	String within 256 characters	
Default	Blank	
Web UI	Account->Register->SIP Server Y->Server Host	
Parameter	account.X.sip_server.Y.port ^{[1][2]}	<MAC>.cfg
Description	It configures the port of SIP server Y. If it is set to 0 when UDP is used ("account.X.sip_server.Y.transport_type" is set to 0), the phone uses a random port for responding the messages from the server.	

Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	Account->Register->SIP Server Y->Port	
Handset UI	W53P/W60P: OK->Settings->Telephony->Server (default PIN: 0000) ->Server Y (Account X) ->Port	
Parameter	account.X.outbound_proxy_enable ^[1]	<MAC>.cfg
Description	It enables or disables the phone to send requests to the outbound proxy server.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Account->Register->Enable Outbound Proxy Server	
Handset UI	W53P/W60P: OK->Settings->Telephony->Server (default PIN: 0000) ->Server Y (Account X) ->Outbound Proxy->Outbound Server	
Parameter	account.X.outbound_proxy.Y.address ^{[1][2]}	<MAC>.cfg
Description	It configures the IP address or domain name of the outbound proxy server Y. Note: It works only if "account.X.outbound_proxy_enable" is set to 1 (Enabled).	
Permitted Values	IP address or domain name	
Default	Blank	
Web UI	Account->Register->Outbound Proxy Server Y	
Parameter	account.X.outbound_proxy.Y.port ^{[1][2]}	<MAC>.cfg
Description	It configures the port of the outbound proxy server Y. Note: It works only if "account.X.outbound_proxy_enable" is set to 1 (Enabled).	
Permitted Values	Integer from 0 to 65535	
Default	5060	
Web UI	Account->Register->Outbound Proxy Server Y->Port	
Handset UI	W53P/W60P: OK->Settings->Telephony->Server (default PIN: 0000) ->Outbound Proxy (Account X) ->Port (only applicable to port sever 1)	
Parameter	account.X.reg_fail_retry_interval ^[1]	<MAC>.cfg
Description	It configures the interval (in seconds) at which the phone to retry to re-register account X when registration fails. Note: It works only if "account.X.reg_failed_retry_min_time" and "account.X.reg_failed_retry_max_time" are set to 0.	
Permitted Values	Integer from 0 to 1800	

Default	30	
Web UI	Account->Advanced->SIP Registration Retry Timer (0~1800s)	
Parameter	account.X.reg_failed_retry_min_time ^[1]	<MAC>.cfg
Description	<p>It configures the base time to wait (in seconds) for the phone to retry to re-register account X when registration fails.</p> <p>Note: It is used in conjunction with the parameter "account.X.reg_failed_retry_max_time" to determine how long to wait. The algorithm is defined in RFC 5626. We recommend you to set this value to an integer between 10 to 120, if needed. If the values of this parameter and the parameter "account.X.reg_failed_retry_max_time" are set to 0, the interval configured by "account.X.reg_fail_retry_interval" will be used.</p>	
Permitted Values	Integer greater than or equal to 0	
Default	0	
Parameter	account.X.reg_failed_retry_max_time ^[1]	<MAC>.cfg
Description	<p>It configures the maximum time to wait (in seconds) for the phone to retry to re-register the account X when registration fails.</p> <p>Note: It is used in conjunction with the parameter "account.X.reg_failed_retry_min_time" to determine how long to wait. The algorithm is defined in RFC 5626. We recommend you to set this value to an integer between 60 to 1800, if needed. If the values of this parameter and the parameter "account.X.reg_failed_retry_min_time" are set to 0, the interval configured by "account.X.reg_fail_retry_interval" will be used.</p>	
Permitted Values	Integer greater than or equal to 0	
Default	60	

^[1]X is the account ID. X=1-8.

^[2]Y is the server ID. Y=1-2.

Registration Settings Configuration

The following table lists the parameters you can use to change the registration settings.

Parameter	account.X.enable_user_equal_phone ^[1]	<MAC>.cfg
Description	It enables or disables the phone to add "user=phone" to the SIP header of the INVITE message.	
Permitted Values	<p>0-Disabled</p> <p>1-Enabled</p>	
Default	0	
Web UI	Account->Advanced->Send user=phone	
Parameter	account.X.register_mac ^[1]	<MAC>.cfg
Description	It enables or disables the phone to add MAC address to the SIP header of the REGISTER message.	
Permitted Values	<p>0-Disabled</p> <p>1-Enabled</p>	
Default	0	

Web UI	Account->Advanced->SIP Send MAC	
Parameter	account.X.register_line ^[1]	<MAC>.cfg
Description	It enables or disables the phone to add a line number to the SIP header of the REGISTER message.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Account->Advanced->SIP Send Line	
Default	0	
Parameter	account.X.unregister_on_reboot ^[1]	<MAC>.cfg
Description	It enables or disables the phone to unregister first before re-registering account X after a reboot.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Account->Advanced->Unregister When Reboot	
Parameter	account.X.sip_server_type ^[1]	<MAC>.cfg
Description	It configures the type of the SIP server.	
Permitted Values	0-Default 2-BroadSoft (It works only if "bw.enable" is set to 1 (Enabled)) 8-Genesys 10-Genesys Advanced	
Default	0	
Web UI	Account->Advanced->SIP Server Type	
Parameter	sip.reg_surge_prevention ^[2]	<y0000000000xx>.cfg
Description	It configures the waiting time (in seconds) for account register after startup.	
Permitted Values	Integer from 0 to 60	
Default	0	
Web UI	Network->Advanced->Registration Random->Registration Random (0~60s)	
Parameter	account.X.subscribe_register ^[1]	<MAC>.cfg
Description	It enables or disables the phone to subscribe the registration state change notifications.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Account->Advanced->Subscribe Register	
Parameter	phone_setting.disable_account_without_username.enable	<y0000000000xx>.cfg

Description	It enables or disables the phone to disable the account whose username is empty.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Parameter	account.X.register_expires_overlap ^[1]	<MAC>.cfg
Description	It configures the renewal time (in seconds) away from the registration lease.	
Permitted Values	Positive integer and -1	
Default	-1	
Parameter	account.X.subscribe_expires_overlap ^[1]	<MAC>.cfg
Description	It configures the renewal time (in seconds) away from the subscription lease.	
Permitted Values	Positive integer and -1	
Default	-1	

^[1]X is the account ID. X=1-8.

^[2]If you change this parameter, the phone will reboot to make the change take effect.

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 phone will be sent to the outbound proxy server as a mandatory requirement.

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 the outbound server, refer to [Server Redundancy](#).

Topic

[Outbound Proxy in Dialog Configuration](#)

Outbound Proxy in Dialog Configuration

The following table lists the parameter you can use to configure outbound proxy in dialog.

Parameter	sip.use_out_bound_in_dialog	<y0000000000xx>.cfg
Description	It enables or disables the phone to send all SIP requests to the outbound proxy server mandatorily in a dialog. Note: It works only if "account.X.outbound_proxy_enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled, only the new SIP request messages from the phone will be sent to the outbound proxy server in a dialog. 1-Enabled, all the SIP request messages from the phone will be sent to the outbound proxy server in a dialog.	
Default	0	

Web UI	Features->General Information->Use Outbound Proxy In Dialog
---------------	---

Server Redundancy

Server redundancy is often required in VoIP deployments to ensure continuity of phone service, for example, take the call server 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:

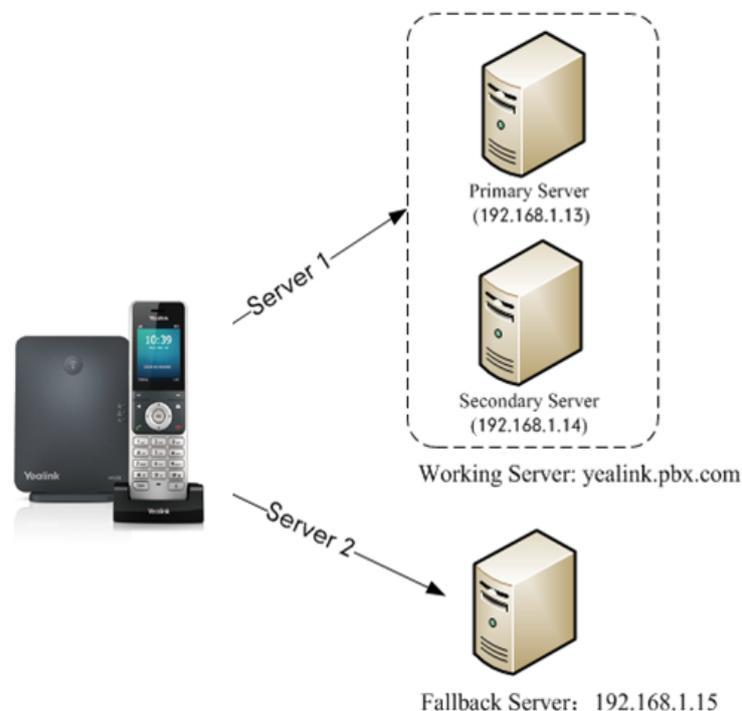
- **Failover:** In this mode, the full phone system functionality is preserved by having a second equivalent capability call server take over from the one that has gone down/off-line. This mode of operation should be done using the DNS mechanism from the primary to the secondary server. Therefore, if 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. The phones support configuration of two servers per SIP registration for the fallback purpose.

Note

For concurrent registration mode, it has a 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 (for example, 192.168.1.13) has the highest priority server in a cluster of servers resolved by the DNS server. The secondary server (for example, 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.

Yealink phones support Failover and Fallback server redundancy types. In some cases, you can deploy a combination of the two server redundancy types. For more information on server redundancy, refer to [Server Redundancy on Yealink IP Phones](#).

Topics

[Behaviors When Working Server Connection Fails](#)
[Registration Method of the Failover/Fallback Mode](#)
[Fallback Server Redundancy Configuration](#)
[Failover Server Redundancy Configuration](#)

Behaviors When Working Server Connection Fails

For Outgoing Call

When you initiate a call, the 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 phone will try the fallback server until it either succeeds in making a call or exhausts all servers at which point the call will fail.

At the start of a call, server availability is determined by SIP signaling failure. SIP signaling failure depends on the SIP protocol being used as described below:

- If TCP is used, then the signaling fails if the connection or the send fails.
- If UDP is used, then the signaling fails if ICMP is detected or if the signal times out. If the signaling has been attempted through all servers in the list (this list contains all the server addresses resolved by the DNS server) and this is the last server, then the signaling fails after the complete UDP timeout defined in [RFC 3261](#). If it is not the last server in the list, the maximum number of retries depends on the configured retry counts (configured by the parameter "account.X.sip_server.Y.retry_counts").

Registration Method of the Failover/Fallback Mode

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 be 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. If it fails, 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 phone registers to the fallback server, and the fallback server can take over all calling capabilities.

Fallback Server Redundancy Configuration

The following table lists the parameters you can use to configure fallback server redundancy.

Parameter	account.X.fallback.redundancy_type ^[1]	<MAC>.cfg
Description	It configures the registration mode in fallback mode. Note: It is not applicable to outbound proxy servers.	
Permitted Values	0-Concurrent registration 1-Successive registration	
Default	0	
Parameter	account.X.fallback.timeout ^[1]	<MAC>.cfg
Description	It configures the time interval (in seconds) for the phone to detect whether the working server is available by sending the registration request after the fallback server takes over call control. Note: It is not applicable to outbound proxy servers.	
Permitted Values	Integer from 10 to 2147483647	
Default	120	
Parameter	account.X.outbound_proxy_fallback_interval ^[1]	<MAC>.cfg
Description	It configures the time interval (in seconds) for the phone to detect whether the working outbound proxy server is available by sending the registration request after the fallback server takes over call control. Note: It is only applicable to outbound proxy servers.	
Permitted Values	Integer from 0 to 65535	
Default	3600	
Web UI	Account->Register->Proxy Fallback Interval	

^[1]X is the account ID. X=1-8.

Failover Server Redundancy Configuration

The following table lists the parameters you can use to configure failover server redundancy.

Parameter	account.X.sip_server.Y.register_on_enable ^{[1][2]}	<MAC>.cfg
Description	It enables or disables the phone to send registration requests to the secondary server when encountering a failover.	
Permitted Values	0-Disabled, the phone will not attempt to register to the secondary server, since the phone assumes that the primary and secondary servers share registration information. So the phone will directly send the requests to the secondary server. 1-Enabled, the phone will register to the secondary server first, and then send the requests to it.	
Default	0	

Parameter	sip.skip_redundant_failover_addr	<y0000000000xx>.cfg
Description	It enables or disables the phone only to send requests to the servers with different IP addresses when encountering a failover.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Parameter	account.X.sip_server.Y.expires ^{[1][2]}	<MAC>.cfg
Description	It configures the registration expiration time (in seconds) of SIP server Y.	
Permitted Values	Integer from 30 to 2147483647	
Default	3600	
Web UI	Account->Register->SIP Server Y->Server Expires	
Parameter	account.X.sip_server.Y.retry_counts ^{[1][2]}	<MAC>.cfg
Description	It configures the retry times for the phone to resend requests when the SIP server Y is unavailable or there is no response from the SIP server Y. The phone moves to the next available server after three failed attempts.	
Permitted Values	Integer from 0 to 20	
Default	3	
Web UI	Account->Register->SIP Server Y->Server Retry Counts	
Parameter	account.X.sip_server.Y.only_signal_with_registered ^{[1][2]}	<MAC>.cfg
Description	It enables or disables the phone to only send requests to the registered server when encountering a failover. Note: It works only if "account.X.sip_server.Y.register_on_enable" is set to 1 (Enabled) and "account.X.sip_server.Y.failback_mode" is set to 1, 2 or 3.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Parameter	account.X.sip_server.Y.invite_retry_counts ^{[1][2]}	<MAC>.cfg
Description	It configures the number of retries attempted before sending requests to the next available server when encountering a failover.	
Permitted Values	Integer from 1 to 10	
Default	3	
Parameter	account.X.sip_server.Y.failback_mode ^{[1][2]}	<MAC>.cfg
Description	It configures the mode for the phone to retry the primary server in failover. Note: It works only if "account.X.sip_server.Y.address" is set to the domain name of the SIP server.	
Permitted Values	0-newRequests: all requests are sent to the primary server first, regardless of the last server that was used. 1-DNSTTL: the phone will send requests to the last registered server first. If the time defined by DNSTTL	

	<p>on the registered server expires, the phone will retry to send requests to the primary server.</p> <p>2-Registration: the 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.</p> <p>3-duration: the phone will send requests to the last registered server first. If the time defined by the "account.X.sip_server.Y.failback_timeout" parameter expires, the phone will retry to send requests to the primary server.</p>	
Default	0	
Parameter	account.X.sip_server.Y.failback_timeout ^{[1][2]}	<MAC>.cfg
Description	<p>It configures the timeout (in seconds) for the phone to retry to send requests to the primary server after failing over to the current working server.</p> <p>If you set the parameter to 0, the phone will not send requests to the primary server until a failover event occurs with the current working server.</p> <p>If you set the parameter between 1 and 59, the timeout will be 60 seconds.</p> <p>Note: It works only if "account.X.sip_server.Y.failback_mode" is set to 3 (duration).</p>	
Permitted Values	0, Integer from 60 to 65535	
Default	3600	
Parameter	account.X.sip_server.Y.failback_subscribe.enable ^{[1][2]}	<MAC>.cfg
Description	<p>It enables or disables the phone to retry to re-subscribe after registering to the secondary server with different IP addresses when encountering a failover.</p> <p>Note: It works only if "account.X.sip_server.Y.failback_mode" is set to 1, 2 or 3.</p>	
Permitted Values	<p>0-Disabled</p> <p>1-Enabled, the phone will immediately re-subscribe to the secondary server, for ensuring the normal use of the features associated with the subscription (for example, BLF, SCA).</p>	
Default	0	

^[1]X is the account ID. X=1-8.

^[2]Y is the server ID. Y=1-2.

SIP Server Name Resolution

If a domain name is configured for a server, the IP address(es) associated with that domain name will be resolved through DNS as specified by RFC 3263. The DNS query involves NAPTR, SRV and A queries, which allows the IP phone to adapt to various deployment environments. The IP phone performs NAPTR query for the NAPTR pointer and transport protocol (UDP, TCP and TLS), the SRV query on the record returned from the NAPTR for the target domain name and the port number, and the A query for the IP addresses.

If an explicit port (except 0) is specified, A query will be performed only. If a server port is set to 0 and the transport type is set to DNS-NAPTR, NAPTR and SRV queries will be tried before falling to A query. If no port is found through the DNS query, 5060 will be used.

Topic

[SIP Server Name Resolution Configuration](#)

SIP Server Name Resolution Configuration

The following table lists the parameters you can use to configure SIP server name resolution.

Parameter	account.X.sip_server.Y.transport_type ^{[1][2]}	<MAC>.cfg
Description	It configures the type of transport protocol.	
Permitted Values	0 -UDP 1 -TCP 2 -TLS 3 -DNS-NAPTR, if no server port is given, the phone performs the DNS NAPTR and SRV queries for the service type and port.	
Default	0	
Web UI	Account->Register->SIP Server Y->Transport	
Handset UI	For W53P/W60P: OK->Settings->Telephony->Server (default PIN: 0000) ->Server Y->Transport	
Parameter	account.X.naptr_build ^[1]	<MAC>.cfg
Description	It configures the way of SRV query for the phone to be performed when no result is returned from NAPTR query.	
Permitted Values	0 -SRV query using UDP only 1 -SRV query using UDP, TCP and TLS.	
Default	0	
Parameter	sip.dns_transport_type	<y0000000000xx>.cfg
Description	It configures the transport protocol the phone uses to perform a DNS query.	
Permitted Values	0 -UDP 1 -TCP	
Default	0	
Parameter	static.network.dns.query_timeout ^[3]	<y0000000000xx>.cfg
Description	It configures the interval (in seconds) at which the phone retries to resolve a domain name when the DNS server does not respond.	
Permitted Values	0 to 65535	
Default	3	
Parameter	static.network.dns.retry_times ^[3]	<y0000000000xx>.cfg
Description	It configures the retry times when the DNS server does not respond.	
Permitted Values	0 to 65535	
Default	2	

^[1]X is the account ID. X=1-8.

[2]Y is the server ID. Y=1-2.

[3]If you change this parameter, the phone will reboot to make the change take effect.

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 phone will attempt to resolve the domain name of the SIP server with 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.

Topics

[Behave with a Configured DNS Server](#)
[Static DNS Cache Configuration](#)

Behave with a Configured DNS Server

When the phone is configured with a DNS server, it will behave as follows to resolve the domain name of the server:

- The 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 phone will attempt to perform a DNS query again.
- If the DNS query returns a result, the phone will use the returned record from the DNS server and ignore the statically configured cache values.

When the phone is not configured with a DNS server, it will behave as follows:

- The phone attempts to resolve the domain name within the static DNS cache.
- The phone will always use the results returned from the static DNS cache.

Static DNS Cache Configuration

The following table lists the parameters you can use to configure static DNS cache.

Parameter	account.X.dns_cache_type ^[1]	<MAC>.cfg
Description	It configures whether the phone uses the DNS cache for domain name resolution of the SIP server and caches the additional DNS records.	
Permitted Values	0 -Perform real-time DNS query rather than using DNS cache. 1 -Use DNS cache, but do not record the additional records. 2 -Use DNS cache and cache the additional DNS records.	
Default	1	
Parameter	account.X.static_cache_pri ^[1]	<MAC>.cfg
Description	It configures whether preferentially to use the static DNS cache for domain name resolution of the SIP server.	
Permitted Values	0 -Use domain name resolution from server preferentially 1 -Use static DNS cache preferentially	

Default	0	
Parameter	dns_cache_naptr.X.name ^[2]	<y0000000000xx>.cfg
Description	It configures the domain name to which NAPTR record X refers.	
Permitted Values	Domain name	
Default	Blank	
Parameter	dns_cache_naptr.X.order ^[2]	<y0000000000xx>.cfg
Description	It configures the order of NAPTR record X. NAPTR record with the lower order is more preferred.	
Permitted Values	Integer from 0 to 65535	
Default	0	
Parameter	dns_cache_naptr.X.preference ^[2]	<y0000000000xx>.cfg
Description	It configures the preference of NAPTR record X. NAPTR record with lower preference is more preferred.	
Permitted Values	Integer from 0 to 65535	
Default	0	
Parameter	dns_cache_naptr.X.replace ^[2]	<y0000000000xx>.cfg
Description	It configures a domain name to be used for the next SRV query in NAPTR record X.	
Permitted Values	Domain name	
Default	Blank	
Parameter	dns_cache_naptr.X.service ^[2]	<y0000000000xx>.cfg
Description	It configures the transport protocol available for the SIP server in NAPTR record X.	
Permitted Values	SIP+D2U -SIP over UDP SIP+D2T -SIP over TCP SIPS+D2T -SIPS over TLS	
Default	Blank	
Parameter	dns_cache_naptr.X.ttl ^[2]	<y0000000000xx>.cfg
Description	It configures the time interval (in seconds) that NAPTR record X may be cached before the record should be consulted again.	
Permitted Values	Integer from 30 to 2147483647	
Default	300	
Parameter	dns_cache_srv.X.name ^[2]	<y0000000000xx>.cfg
Description	It configures the domain name in SRV record X.	

Permitted Values	Domain name	
Default	Blank	
Parameter	dns_cache_srv.X.port ^[2]	<y0000000000xx>.cfg
Description	It configures the port to be used in SRV record X.	
Permitted Values	Integer from 0 to 65535	
Default	0	
Parameter	dns_cache_srv.X.priority ^[2]	<y0000000000xx>.cfg
Description	It configures the priority for the target host in SRV record X. Lower priority is more preferred.	
Permitted Values	Integer from 0 to 65535	
Default	0	
Parameter	dns_cache_srv.X.target ^[2]	<y0000000000xx>.cfg
Description	It configures the domain name of the target host for an A query in SRV record X.	
Permitted Values	Domain name	
Default	Blank	
Parameter	dns_cache_srv.X.weight ^[2]	<y0000000000xx>.cfg
Description	It configures the weight of the target host in SRV record X. When priorities are equal, weight is used to differentiate the preference. Higher weight is more preferred.	
Permitted Values	Integer from 0 to 65535	
Default	0	
Parameter	dns_cache_srv.X.ttl ^[2]	<y0000000000xx>.cfg
Description	It configures the time interval (in seconds) that SRV record X may be cached before the record should be consulted again.	
Permitted Values	Integer from 30 to 2147483647	
Default	300	
Parameter	dns_cache_a.X.name ^[2]	<y0000000000xx>.cfg
Description	It configures the domain name in A record X.	
Permitted Values	Domain name	
Default	Blank	
Parameter	dns_cache_a.X.ip ^[2]	<y0000000000xx>.cfg
Description	It configures the IP address that the domain name in A record X maps to.	

Permitted Values	IP address	
Default	Blank	
Parameter	dns_cache_a.X.ttl ^[2]	<y0000000000xx>.cfg
Description	It configures the time interval (in seconds) that A record X may be cached before the record should be consulted again.	
Permitted Values	Integer from 30 to 2147483647	
Default	300	
Parameter	static.network.dns.ttl_enable ^[3]	<y0000000000xx>.cfg
Description	It enables or disables the phone to use TTL (Time To Live) in the A record.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	
Parameter	static.network.dns.last_cache_expired	<y0000000000xx>.cfg
Description	It configures the validity period of the expired DNS cache. Note: It works only if "static.network.dns.last_cache_expired.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 0 to 65535 0 -the expired DNS cache can only be used once. After using, the phone will perform a DNS query again. 1 to 65535 -the phone will use the expired DNS cache during the specified period. After that, the phone will perform a DNS query again.	
Default	3600	
Parameter	static.network.dns.last_cache_expired.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to use the DNS cache (even if the cache has expired) when the DNS server fails to resolve the domain name.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	

[1]X is the account ID. X=1-8.

[2]X is the record ID. X=1-12.

[3]If you change this parameter, the phone will reboot to make the change take effect.

Number of Active Handsets

The W60B base station supports up to 8 handsets, and you can limit the max number of active handsets. The active handsets are free to communicate, access menu, configure features and so on. Operation is restricted on the inactive handsets, and the idle screen of the handset prompts "Path Busy".

The number of active handsets will also affect the number of simultaneous active calls on the base station.

Call Supported	Number of Active Handsets	Maximum Number of Simultaneous Active Calls	Maximum Number of Simultaneous Calls
Wide-band Calls	4	4	6 (for opus) 8 (for other codecs)
Narrow-band Calls	8	6 (for opus) 8 (for other codecs)	6 (for opus) 8 (for other codecs)

Related Topics

[Number of Simultaneous Outgoing Calls](#)

[Number of Active Handsets Configuration](#)

Number of Active Handsets Configuration

The following table lists the parameter you can use to configure the number of active handsets.

Parameter	base.active_handset.number ^[1]	<y0000000000xx>.cfg
Description	It configures the maximum number of active handsets.	
Permitted Values	4, 8	
Default	4	
Web UI	Features->General Information->Number Of Active Handset	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Number of Simultaneous Outgoing Calls

Number of simultaneous outgoing calls allows you to configure the max number of simultaneous outgoing calls for a specific account on a base.

The number of active handsets affects this feature.

Related Topics

[Number of Active Handsets](#)

[Number of Simultaneous Outgoing Calls Configuration](#)

Number of Simultaneous Outgoing Calls Configuration

The following table lists the parameter you can use to configure the number of simultaneous outgoing calls.

Parameter	account.X.simultaneous_outgoing.num ^[1]	<MAC>.cfg
Description	It configures the max number of simultaneous outgoing calls for a specific account on a base station. Note: You should set the value of this parameter lower than or equal to "base.active_handset.number".	
Permitted Values	Integer from 1 to 8	
Default	8	
Web UI	Account->Advanced->Number of simultaneous outgoing calls	

^[1]X is the account ID. X=1-8.

Number Assignment

After the handset is registered to the base station, you can assign one or more outgoing lines or incoming lines for the handset.

The handset can only use the assigned outgoing line(s) to place calls. When multiple outgoing lines are assigned to the handset, the handset uses the first line as the default outgoing line. You can change the default outgoing line of the handset.

The handset can only receive incoming calls of the assigned incoming line(s). You can assign incoming lines to all handsets that are registered to the same base station.

Topic

[Number Assignment Configuration](#)

Number Assignment Configuration

The following table lists the parameters you can use to assign lines.

Parameter	handset.X.incoming_lines ^[1]	<y0000000000xx>.cfg
Description	It configures the lines to receive incoming calls for a specific handset.	
Permitted Values	<p>1-Line 1</p> <p>2-Line 2</p> <p>3-Line 3</p> <p>4-Line 4</p> <p>5-Line 5</p> <p>6-Line 6</p> <p>7-Line 7</p> <p>8-Line 8</p> <p>Multiple line IDs are separated by commas.</p>	
Default	<p>The incoming line for handset 1 is line 1-line5.</p> <p>The incoming line for handset 2 is line 2.</p> <p>The incoming line for handset 3 is line 3.</p> <p>The incoming line for handset 4 is line 4.</p> <p>The incoming line for handset 5 is line 5.</p> <p>The incoming line for handset 6 is line 6.</p> <p>The incoming line for handset 7 is line 7.</p> <p>The incoming line for handset 8 is line 8.</p>	
Web UI	Account->Number Assignment->Incoming lines	
Handset UI	<p>W53P/W60P:</p> <p>OK->Settings->Telephony->Incoming Lines (Default PIN:0000) ->HandsetX^[1]</p> <p>DD Phone:</p>	

	Menu->Settings->Advanced Settings (default password: 0000) ->Incoming Lines	
Parameter	handset.X.dial_out_lines ^[1]	<y0000000000xx>.cfg
Description	It configures the lines to place outgoing calls for a specific handset.	
Permitted Values	<p>1-Line 1</p> <p>2-Line 2</p> <p>3-Line 3</p> <p>4-Line 4</p> <p>5-Line 5</p> <p>6-Line 6</p> <p>7-Line 7</p> <p>8-Line 8</p> <p>Multiple line IDs are separated by commas.</p>	
Default	<p>The incoming line for handset 1 is line 1-line5.</p> <p>The incoming line for handset 2 is line 2.</p> <p>The incoming line for handset 3 is line 3.</p> <p>The incoming line for handset 4 is line 4.</p> <p>The incoming line for handset 5 is line 5.</p> <p>The incoming line for handset 6 is line 6.</p> <p>The incoming line for handset 7 is line 7.</p> <p>The incoming line for handset 8 is line 8.</p>	
Web UI	Account->Number Assignment->Outgoing lines	
Parameter	handset.X.dial_out_default_line ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the default line to place outgoing calls for a specific handset.</p> <p>Note: It is not applicable to CP930W-Base phones.</p>	
Permitted Values	Integer from 1 to 8	
Default	<p>The default outgoing line for handset 1 is line 1.</p> <p>The default outgoing line for handset 2 is 2.</p> <p>The default outgoing line for handset 3 is 3.</p> <p>The default outgoing line for handset 4 is 4.</p> <p>The default outgoing line for handset 5 is 5.</p> <p>The default outgoing line for handset 6 is 6.</p> <p>The default outgoing line for handset 7 is 7.</p> <p>The default outgoing line for handset 8 is 8.</p>	

Web UI	Account->Number Assignment->Outgoing lines->Default
Handset UI	W53P/W60P: OK->Settings->Telephony->Default Line

[1]X is the handset ID. X=1-8.

Call Log

Yealink phones record and maintain phone events to a call log, also known as a call list.

Call log consists of four lists: Missed Calls, Placed Calls, Received Calls, and All Calls. Each call log list supports up to 100 entries.

Topics

[Call Log Display](#)

[Call Log Configuration](#)

Call Log Display

The following table describes the detailed call log information:

Display Field	Description
Name	Shows the name of remote party.
Number	Shows the number of remote party.
Time	Shows the call initiation time.
Duration	Shows the duration of the call.

Related Topic

[Call Log Configuration](#)

Call Log Configuration

The following table lists the parameter you can use to change the call log settings.

Parameter	features.save_call_history	<y0000000000xx>.cfg
Description	It enables or disables the phone to log the call history (missed calls, placed calls, received calls and forwarded calls) in the call lists.	
Permitted Values	0 -Disabled, the phone cannot log the placed calls, received calls, missed calls and the forwarded calls in the call lists. 1 -Enabled	
Default	1	
Web UI	Features->General Information->Save Call Log	

Related Topic

[Basic Regular Expression Syntax for Digit Map](#)

Directory

The Yealink IP phone provides several types of phone directories.

Topics

- [Local Directory](#)
- [Lightweight Directory Access Protocol \(LDAP\)](#)
- [Remote Phone Book](#)
- [Directory Search Settings](#)
- [Shared Directory](#)

Local Directory

Yealink phones maintain a local directory that you can use to store contacts. You can store up to 100 contacts per handset, each with a name, a mobile number and an office number.

Contacts and groups can be added either one by one, or in batch using a local contact file. Yealink phones support both *.xml and *.csv format contact files, but you can only customize the *.xml format contact file.

Topics

- [Local Contact File Customization](#)
- [Local Contact Files and Resource Upload](#)

Local Contact File Customization

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>.

Topics

- [Local Contact File Elements and Attributes](#)
- [Customizing Local Contact File](#)

Local Contact File Elements and Attributes

The following table lists the elements and attributes you can use to add groups or contacts in the local contact file. We recommend you do not edit these elements and attributes.

Elements	Attributes	Description
Contact	display_name	Specify the contact name. For example: Jim Note: The contact name cannot be blank or duplicated.
	office_number	Specify the office number or macro EDK Macro Strings (not applicable to CP930W-Base phones).
	mobile_number	Specify the mobile number or macro EDK Macro Strings(not applicable to CP930W-Base phones).
	other_number	Specify the other number or macro EDK Macro Strings (not applicable to CP930W-Base phones).

Related Topic

Example: Using EDK Macro Strings as the Contact Number

Customizing Local Contact File

1. Open the local contact file.
2. To add a contact, add `<contact display_name="" office_number="" mobile_number="" other_number=""/>` to the file. Each starts on a new line.
3. Specify the values within double quotes.

For example:

```
<contact display_name="Lily"office_number="1020" mobile_number="1021" other_number="1112"/>
```

```
<contact display_name="Tom" office_number="2020" mobile_number="2021" other_number="2112"/>
```

4. Save the changes and place this file to the provisioning server.

Local Contact Files and Resource Upload

You can upload local contact files to add multiple contacts at a time.

The following table lists the parameter you can use to upload the local contact files.

Parameter	handset.X.contact_list.url ^[1]	<y0000000000xx>.cfg
Description	It configures the access URL of the contact file of a specific handset.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Directory->Local Directory->Import Contacts->Import to (Handset X)	

^[1]X is the handset ID. X=1-8.

Lightweight Directory Access Protocol (LDAP)

LDAP is an application protocol for accessing and maintaining information services for the distributed directory over an IP network. You can configure the phones 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)

For more information on LDAP, refer to [LDAP Directory on Yealink IP Phones](#).

Topics

[LDAP Attributes](#)

[LDAP Configuration](#)

LDAP Attributes

The following table lists the most common attributes used to configure the LDAP lookup on the phones.

Abbreviation	Name	Description
gn	givenName	First name

Abbreviation	Name	Description
cn	commonName	LDAP attribute is made up from given name joined to surname.
sn	surname	Last name or family name
dn	distinguishedName	Unique identifier for each entry
dc	dc	Domain component
-	company	Company or organization name
-	telephoneNumber	Office phone number
mobile	mobilephoneNumber	Mobile or cellular phone number
ipPhone	IPphoneNumber	Home phone number

LDAP Configuration

The following table lists the parameters you can use to configure LDAP.

Parameter	ldap.enable	<y0000000000xx>.cfg
Description	It enables or disables the LDAP feature on the IP phone.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Directory->LDAP->Enable LDAP	
Parameter	ldap.name_filter	<y0000000000xx>.cfg
Description	<p>It configures the search criteria for LDAP contact names look up.</p> <p>The "*" symbol in the filter stands for any character. The "%" symbol in the filter stands for the name entered by the user.</p> <p>Example:</p> <p>ldap.name_filter = ((cn=%)(sn=%))</p> <p>When the cn or sn of the LDAP contact matches the entered name, the record will be displayed on the phone screen.</p> <p>ldap.name_filter = (&(cn=*)(sn=%))</p> <p>When the cn of the LDAP contact is set and the sn of the LDAP contact matches the entered name, the records will be displayed on the phone screen.</p> <p>ldap.name_filter = (!(cn=%))</p> <p>When the cn of the LDAP contact does not match the entered name, the records will be displayed on the phone screen.</p>	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->LDAP->LDAP Name Filter	

Parameter	ldap.number_filter	<y0000000000xx>.cfg
Description	<p>It configures the search criteria for LDAP contact numbers look up.</p> <p>The "*" symbol in the filter stands for any number. The "%" symbol in the filter stands for the number entered by the user.</p> <p>Example:</p> <p>ldap.number_filter = ((telephoneNumber=%)(mobile=%)(ipPhone=%))</p> <p>When the number of the telephoneNumber, mobile or ipPhone of the contact record matches the search criteria, the record will be displayed on the phone screen.</p> <p>ldap.number_filter = (&(telephoneNumber=*)(mobile=%))</p> <p>When the telephoneNumber of the LDAP contact is set and the mobile of the LDAP contact matches the entered number, the record will be displayed on the phone screen.</p>	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->LDAP->LDAP Number Filter	
Parameter	ldap.tls_mode	<y0000000000xx>.cfg
Description	It configures the connection mode between the LDAP server and the IP phone.	
Permitted Values	<p>0-LDAP–The unencrypted connection between the LDAP server and the IP phone (port 389 is used by default).</p> <p>1-LDAP TLS Start–The TLS/SSL connection between the LDAP server and the IP phone (port 389 is used by default).</p> <p>2-LDAPS–The TLS/SSL connection between the LDAP server and the IP phone (port 636 is used by default).</p>	
Default	0	
Web UI	Directory->LDAP->LDAP TLS Mode	
Parameter	ldap.host	<y0000000000xx>.cfg
Description	It configures the IP address or domain name of the LDAP server.	
Permitted Values	IP address or domain name	
Default	Blank	
Web UI	Directory->LDAP->Server Address	
Parameter	ldap.port	<y0000000000xx>.cfg
Description	It configures the port of the LDAP server.	
Permitted Values	Integer from 1 to 65535	
Default	389	
Web UI	Directory->LDAP->Port	

Parameter	ldap.base	<y0000000000xx>.cfg
Description	<p>It configures the LDAP search base which corresponds to the location of the LDAP phonebook from which the LDAP search request begins. The search base narrows the search scope and decreases directory search time.</p> <p>Example: ldap.base = dc=yealink,dc=cn</p>	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->LDAP->Base	
Parameter	ldap.user	<y0000000000xx>.cfg
Description	<p>It configures the user name used to log into the LDAP server.</p> <p>This parameter can be left blank in case the server allows anonymity to log into. Otherwise you will need to provide the user name to log into the LDAP server.</p> <p>Example: ldap.user = cn=manager,dc=yealink,dc=cn</p>	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->LDAP->Username	
Parameter	ldap.password	<y0000000000xx>.cfg
Description	<p>It configures the password to log into the LDAP server.</p> <p>This parameter can be left blank in case the server allows anonymous to log into. Otherwise you will need to provide the password to log into the LDAP server.</p>	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->LDAP->Password	
Parameter	ldap.max_hits	<y0000000000xx>.cfg
Description	<p>It configures the maximum number of search results to be returned by the LDAP server. If the value of the "Max.Hits" is blank, the LDAP server will return all searched results. Please note that a very large value of the "Max. Hits" will slow down the LDAP search speed, therefore it should be configured according to the available bandwidth.</p>	
Permitted Values	Integer from 1 to 32000	
Default	50	
Web UI	Directory->LDAP->Max Hits (1-32000)	
Parameter	ldap.name_attr	<y0000000000xx>.cfg
Description	It configures the name attributes of each record to be returned by the LDAP server. It compresses the	

	<p>search results. You can configure multiple name attributes separated by spaces.</p> <p>Example:</p> <p>ldap.name_attr = cn sn</p> <p>This requires the "cn" and "sn" attributes set for each contact record on the LDAP server.</p>	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->LDAP->LDAP Name Attributes	
Parameter	ldap.numb_attr	<y0000000000xx>.cfg
Description	<p>It 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.</p> <p>Example:</p> <p>ldap.numb_attr = mobile ipPhone</p> <p>This requires the "mobile" and "ipPhone" attributes set for each contact record on the LDAP server.</p>	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->LDAP->LDAP Number Attributes	
Parameter	ldap.display_name	<y0000000000xx>.cfg
Description	<p>It configures the display name of the contact record displayed on the phone screen.</p> <p>The value must start with "%" symbol.</p> <p>Example:</p> <p>ldap.display_name = %cn</p> <p>The cn of the contact record is displayed on the phone screen.</p>	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->LDAP->LDAP Display Name	
Parameter	ldap.version	<y0000000000xx>.cfg
Description	It configures the LDAP protocol version supported by the IP phone. The version must be the same as the version assigned on the LDAP server.	
Permitted Values	2 or 3	
Default	3	
Web UI	Directory->LDAP->Protocol	
Parameter	ldap.call_in_lookup	<y0000000000xx>.cfg
Description	It enables or disables the phone to perform an LDAP search when receiving an incoming call.	

Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Directory->LDAP->LDAP Lookup For Incoming Call	
Parameter	ldap.call_out_lookup	<y0000000000xx>.cfg
Description	It enables or disables the phone to perform an LDAP search when placing a call.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Directory->LDAP->LDAP Lookup For Callout	
Parameter	ldap.ldap_sort	<y0000000000xx>.cfg
Description	It enables or disables the phone to sort the search results in alphabetical order or numerical order.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Directory->LDAP->LDAP Sorting Results	
Parameter	ldap.incoming_call_special_search.enable	<y0000000000xx>.cfg
Description	<p>It enables or disables the phone to search the telephone numbers starting with "+" symbol and "00" from the LDAP server if the incoming phone number starts with "+" or "00". When completing the LDAP search, all the search results will be displayed on the phone screen.</p> <p>Example:</p> <p>If the phone receives an incoming call from the phone number 0044123456789, it will search 0044123456789 from the LDAP server first, if no result found, it will search +44123456789 from the server again. The phone will display all the search results.</p> <p>Note: It works only if "ldap.call_in_lookup" is set to 1 (Enabled). You may need to set "ldap.name_filter" to be ((cn=*)(sn=*)(telephoneNumber=*)(mobile=*)) for searching the telephone numbers starting with "+" symbol.</p>	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Parameter	ldap.customize_label	<y0000000000xx>.cfg
Description	<p>It configures the display name of the LDAP phone book.</p> <p>If it is left blank, LDAP is displayed.</p> <p>Note: It works only if "ldap.enable" is set to 1 (Enabled).</p>	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->LDAP->LDAP Label	

Remote Phone Book

The 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.

Yealink phones support up to 5 remote phone books. The remote phone book is customizable.

Topics

[Remote Phone Book File Customization](#)

[Remote Phone Book Configuration](#)

[Example: Configuring a Remote Phone Book](#)

Remote Phone Book File Customization

Yealink phones support remote phone book contact customization.

You can add multiple contacts at a time and/or share contacts between the phones using the supplied template files (Menu.xml and Department.xml).

You can ask the distributor or Yealink FAE for remote phone book template. You can also obtain the remote phone book template online: <http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>.

Topics

[Remote Phone Book File Elements](#)

[Customizing Remote Phone Book File](#)

Remote Phone Book File Elements

Yealink phones support two template files: Menu.xml and Department.xml.

The Menu.xml file defines the group/department of a remote phone book. The Department.xml file defines contact lists for a department/group, which is nested in Menu.xml file.

The following table lists the elements you can use to add groups or contacts in the remote phone book file. We recommend you do not edit these elements.

Template	Element	Valid Values
Department.xml	<pre><DirectoryEntry> <Name>Contact Name</Name> <Telephone>Contact Number</Telephone> </DirectoryEntry></pre>	<p>Add a contact in a department/group:</p> <p>Specify the contact name between <Name> and </Name>;</p> <p>Specify the contact number between <Telephone> and </Telephone></p>
Menu.xml	<pre><MenuItem> <Name>Department</Name> <URL>Department URI</URL> </MenuItem></pre>	<p>Add a contact department/group file:</p> <p>Specify the department/group name between <Name> and </Name>;</p> <p>Specify the department/group access URL between <URL></p>

Template	Element	Valid Values
		and</URL>
	<pre><SoftKeyItem> <Name>#</Name> <URL>http://10.2.9.1:99/Department.xml</URL> </SoftKeyItem></pre>	<p>Specify a department/group file for a key:</p> <p>Specify *key, # key or digit key between <Name> and </Name>;</p> <p>Specify the department/group access URL between <URL> and</URL></p>

Customizing Remote Phone Book File

1. Add contacts in a Department.xml file. Each starts on a new line.

For example,

```
<DirectoryEntry>
```

```
  <Name>Lily</Name>
```

```
  <Telephone>123456</Telephone>
```

```
</DirectoryEntry>
```

```
<DirectoryEntry>
```

```
  <Name>Jim</Name>
```

```
  <Telephone>654321</Telephone>
```

```
</DirectoryEntry>
```

2. You can create multiple department.xml files, rename these files and specify multiple contacts in these files. For example, Market.xml with contact Lily and Jim, Propaganda.xml with other contacts and so on.
3. Save these files and place them on the provisioning server.
4. Copy the department files URLs and specify them in the Menu.xml file.

For example,

```
<MenuItem>
```

```
  <Name>Market</Name>
```

```
  <URL>http://192.168.0.1:99/Market.xml</URL>
```

```
</MenuItem>
```

```
<SoftKeyItem>
```

```
  <Name>1</Name>
```

```
  <URL>http://192.168.0.1:99/Propaganda.xml</URL>
```

```
</SoftKeyItem>
```

5. Save Menu.xml file and place it to the provisioning server.

Remote Phone Book Configuration

The following table lists the parameters you can use to configure remote phone book.

Parameter	remote_phonebook.data.X.url ^[1]	<y0000000000xx>.cfg
Description	It configures the access URL of the remote phone book.	

	Note: The size of a remote phone book file should be less than 1.5M.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Directory->Remote Phone Book->Remote URL	
Parameter	remote_phonebook.data.X.name ^[1]	<y0000000000xx>.cfg
Description	It configures the display name of the remote phone book item.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Directory->Remote Phone Book->Display Name	
Parameter	remote_phonebook.display_name	<y0000000000xx>.cfg
Description	It configures the display name of the remote phone book. If it is left blank, "Remote Phone Book" will be the display name.	
Permitted Values	String within 99 characters	
Default	Blank	
Parameter	features.remote_phonebook.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to perform a remote phone book search for an incoming or outgoing call and display the matched results on the phone screen.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Directory->Remote Phone Book->Incoming/Outgoing Call Lookup	
Parameter	features.remote_phonebook.flash_time	<y0000000000xx>.cfg
Description	It configures how often to refresh the local cache of the remote phone book. If it is set to 3600, the phone will refresh the local cache of the remote phone book every 3600 seconds (1 hour). If it is set to 0, the phone will not refresh the local cache of the remote phone book.	
Permitted Values	0, Integer from 3600 to 1296000	
Default	21600	
Web UI	Directory->Remote Phone Book->Update Time Interval(Seconds)	
Parameter	features.remote_phonebook.enter_update_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to refresh the local cache of the remote phone book at a time when accessing the remote phone book.	
Permitted Values	0 -Disabled 1 -Enabled	

Default	0
----------------	---

^[1]X is the phone book ID. X=1-5.

Example: Configuring a Remote Phone Book

The following example shows the configuration for the remote phone book.

Customize the "Department.xml" and "Menu.xml" files, and then place these files to the provisioning server "http://192.168.10.25".

Example

```
remote_phonebook.data.1.url = http://192.168.10.25/Menu.xml
```

```
remote_phonebook.data.1.name = Yealink
```

```
remote_phonebook.data.2.url = http://192.168.10.25/Market.xml
```

```
remote_phonebook.data.2.name = Market
```

After provision, you can navigate to **OK->Directory->Remote Phone Book** for W53P/W60P or navigate to **Menu->Directory->Remote Phone Book** for CP930W-Base phones to access the corporate directory straight from their phones.

Shared Directory

Users can manage contacts and use them in all handsets that are registered on the same base station.

The shared directory can store up to 100 contacts.

It is not applicable to DD phones.

Topics

[Shared Directory Configuration](#)

[Shared Contact File Customization](#)

Shared Directory Configuration

The following table lists the parameters you can use to configure shared directory.

Parameter	static.directory_setting.shared_contact.enable	<y0000000000xx>.cfg
Description	It enables or disables the Shared Directory feature.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Parameter	shared_contact_list.url	<y0000000000xx>.cfg
Description	It configures the access URL of the shared contact file (*.xml) of the handsets. Example: shared_contact_list.url = http://192.168.10.25/contact.xml Note: It works only if "static.directory_setting.shared_contact.enable" is set to 1 (Enabled).	
Permitted	URL within 511 characters	

Values	
Default	Blank
Web UI	Directory->Local Directory->Import Contacts->Import to (Shared Directory)->Select .xml file form

Shared Contact File Customization

You can customize the shared contacts using local contact template. You can ask the distributor or Yealink FAE for local contact template. You can also obtain the template online: <http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>.

Topics

[Shared Contact File Elements and Attributes](#)
[Customizing Shared Contact File](#)

Shared Contact File Elements and Attributes

The following table lists the elements and attributes you can use to add contacts in the shared contact file. We recommend you do not edit these elements and attributes.

Elements	Attributes	Description
Contact	display_name	Specify the contact name. For example: Lily Note: The contact name cannot be blank or duplicated.
	office_number	Specify the office number.
	mobile_number	Specify the mobile number.
	other_number	Specify the other number.

Customizing Shared Contact File

1. Open the shared contact file.
2. To add a contact, add `<contact display_name="" office_number="" mobile_number="" other_number=""/>` to the file. Each starts on a new line.
3. Specify the values within double quotes.
For example:

```
<contact display_name="Lily" office_number="1020" mobile_number="1021" other_number="1112"/>
<contact display_name="Tom" office_number="2020" mobile_number="2021" other_number="2112"/>
```
4. Save the changes and place this file to the provisioning server.

Directory Search Settings

You can configure how the phones search contacts.

Topic

[Directory Search Settings Configuration](#)

Directory Search Settings Configuration

The following table lists the parameter you can use to configure directory search settings.

Parameter	directory.search_type	<y0000000000xx>.cfg
Description	It configures the search type when searching the contact in Local Directory or Remote Phone Book.	
Permitted Values	0 -Approximate string matching, the phone will search the contact numbers or names contain the entered character(s). 1 -Prefix matching, the phone will search the contact numbers or names start with the entered character (s).	
Default	0	

Call Features

This chapter shows you how to configure call feature on Yealink phones.

Topics

- [Dial Plan](#)
- [Emergency Dialplan](#)
- [Off Hook Hot Line Dialing](#)
- [Call Timeout](#)
- [Anonymous Call](#)
- [Call Number Filter](#)
- [IP Address Call](#)
- [Auto Answer](#)
- [Anonymous Call Rejection](#)
- [Call Waiting](#)
- [Do Not Disturb \(DND\)](#)
- [Call Hold](#)
- [Call Forward](#)
- [Call Transfer](#)
- [Conference](#)
- [SD Card Recording](#)
- [Multicast Paging](#)
- [End Call on Hook](#)

Dial Plan

Dial plan is a string of characters that governs the way how the phones process the inputs received from the IP phone's keypads. You can use the regular expression to define the dial plan.

Yealink phones support four patterns:

- **Replace rule:** is an alternative string that replaces the numbers entered by the user. Yealink phones support up to 100 replace rules.
- **Dial now:** is a string used to match numbers entered by the user. When entered numbers match the predefined dial now rule, the phone will automatically dial out the numbers without pressing the send key. Yealink phones support up to 20 dial now rules.
- **Area code:** 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 phone will automatically add the area code before the numbers when dialing out them. Yealink phones only support one area code rule.
- **Block out:** prevents users from dialing out specific numbers. When entered numbers match the predefined block out rule, the phone screen prompts "Forbidden Number". Yealink phones support up to 10 block out rules.

You can configure these four patterns via web user interface or auto provisioning. For replace rule and dial now, you can select to add the rule one by one or using the template file to add multiple rules at a time.

Topics

- [Basic Regular Expression Syntax for Four Patterns](#)
- [Replace Rule File Customization](#)
- [Dial Now File Customization](#)
- [Replace Rule Configuration](#)

Dial Now Configuration

Area Code Configuration

Block Out Configuration

Example: Adding Replace Rules Using a Replace Rule File

Basic Regular Expression Syntax for Four Patterns

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

Regular expression	Description
.	The dot "." can be used as a placeholder or multiple placeholders for any string. Example: "12." would match "123", "1234", "12345", "12abc", and so on.
x	The "x" can be used as a placeholder for any character. Example: "12x" would match "121", "122", "123", "12a", and so on.
-	The dash "-" can be used to match a range of characters within the brackets. Example: "[5-7]" would match the number "5", "6" or "7".
,	The comma "," can be used as a separator within the bracket. Example: "[2,5,8]" would match the number "2", "5" or "8".
[]	The square bracket "[]" can be used as a placeholder for a single character which matches any of a set of characters. Example: "91[5-7]1234" would match "9151234", "9161234", "9171234".
()	The parenthesis "()" can be used to group together patterns, for instance, to logically combine two or more patterns. Example: "([1-9])([2-7])3" would match "923", "153", "673", and so on.
\$	The "\$" followed by the sequence number of a parenthesis means the characters placed in the parenthesis. The sequence number stands for the corresponding parenthesis. Example: A replace rule configuration, Prefix: "001(xxx)45(xx)", Replace: "9001\$145\$2". When you dial out "0012354599" on your phone, the phone will replace the number with "9001 2354599 ". "\$1" means 3 digits in the first parenthesis, that is, "235". "\$2" means 2 digits in the second parenthesis, that is, "99".

Replace Rule File Customization

The replace rule file helps create multiple replace rules. At most 100 replace rules can be added to the IP phone.

You can ask the distributor or Yealink FAE for the replace rule file template. You can also obtain the replace rule file template online: <http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>.

Topics

[Replace Rule File Attributes](#)

[Customizing the Replace Rule File](#)

Replace Rule File Attributes

The following table lists the attributes you can use to add replace rules to the replace rule file:

Attributes	Description
Prefix	Specify the number to be replaced.

Attributes	Description
Replace	Specify the alternate string instead of what the user enters.
LineID	Specify a registered line to apply the replace rule. Valid Values: 0-8 0 stands for all lines; 1~8 stand for line1~line8 Multiple line IDs are separated by commas.

Customizing the Replace Rule File

1. Open the replace rule file.
2. To add a replace rule, add `<Data Prefix="" Replace="" LineID="" />` to the file. Each starts on a new line.
3. Specify the values within double quotes.
For example,
`<Data Prefix="2512" Replace="05922512" LineID="1" />`
4. Save the changes and place this file to the provisioning server.

Dial Now File Customization

The dial now file helps create multiple dial now rules. At most 20 dial now rules can be added to the IP phone.

You can ask the distributor or Yealink FAE for dial now file template. You can also obtain the dial now file template online: <http://support.yealink.com/documentFront/forwardToDocumentFrontDisplayPage>.

Topics

[Dial Now File Attributes](#)

[Customizing the Dial Now File](#)

Dial Now File Attributes

The following table lists the attributes you can use to add dial-now rules to the dial now file:

Attributes	Description
DialNowRule	Specify the dial-now number.
LineID	Specify a registered line to apply the dial-now rule. Valid Values: 0-8 0 stands for all lines; 1~8 stand for line1~line8 Multiple line IDs are separated by commas.

Customizing the Dial Now File

1. Open the dial now file.
2. To add a dial-now rule, add `<Data DialNowRule="" LineID="" />` to the file. Each starts on a new line.
3. Specify the values within double quotes.
For example,
`<Data DialNowRule="1001" LineID="0" />`

4. Save the changes and place this file to the provisioning server.

Replace Rule Configuration

You can configure replace rules either one by one or in batch using a replace rule template.

The following table lists the parameters you can use to configure replace rule.

Parameter	dialplan.replace.prefix.X ^[1]	<y0000000000xx>.cfg
Description	It configures the entered number to be replaced.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Settings->Dial Plan->Replace Rule->Prefix	
Parameter	dialplan.replace.replace.X ^[1]	<y0000000000xx>.cfg
Description	It configures the alternate number to replace the entered number. The entered number is configured by "dialplan.replace.prefix.X".	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Settings->Dial Plan->Replace Rule->Replace	
Parameter	dialplan.replace.line_id.X ^[1]	<y0000000000xx>.cfg
Description	It 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 phone. Multiple line IDs are separated by commas. Note:	
Permitted Values	0 to 8	
Default	Blank	
Web UI	Settings->Dial Plan->Replace Rule->Account	
Parameter	dialplan_replace_rule.url	<y0000000000xx>.cfg
Description	It configures the access URL of the replace rule template file. For customizing replace rule template file, refer to Replace Rule File Customization .	
Permitted Values	URL within 511 characters	
Default	Blank	

^[1]X is from 1 to 100.

Dial Now Configuration

You can configure dial now rules either one by one or in batch using a dial now template.

The following table lists the parameters you can use to configure dial now.

Parameter	dialplan.dialnow.rule.X ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the dial now rule (the string used to match the numbers entered by the user).</p> <p>When entered numbers match the predefined dial now rule, the phone will automatically dial out the numbers without pressing the send key.</p> <p>Example:</p> <p>dialplan.dialnow.rule.1 = 123</p>	
Permitted Values	String within 511 characters	
Default	Blank	
Web UI	Settings->Dial Plan->Dial Now->Rule	
Parameter	dialplan.dialnow.line_id.X ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the desired line to apply the dial now rule.</p> <p>The digit 0 stands for all lines. If it is left blank, the dial-now rule will apply to all lines on the phone.</p> <p>Note: Multiple line IDs are separated by commas.</p>	
Permitted Values	0 to 8	
Default	Blank	
Web UI	Settings->Dial Plan->Dial Now->Account	
Parameter	phone_setting.dialnow_delay	<y0000000000xx>.cfg
Description	<p>It configures the delay time (in seconds) for the dial now rule.</p> <p>When entered numbers match the predefined dial now rule, the phone will automatically dial out the entered number after the designated delay time.</p> <p>If it is set to 0, the phone will automatically dial out the entered number immediately.</p>	
Permitted Values	Integer from 0 to 14	
Default	1	
Web UI	Features->General Information->Time Out for Dial Now Rule	
Parameter	dialplan_dialnow.url	<y0000000000xx>.cfg
Description	<p>It configures the access URL of the dial now template file.</p> <p>For customizing dial now template file, refer to Dial Now File Customization.</p>	
Permitted Values	String within 511 characters	
Default	Blank	

^[1]X is from 1 to 20.

Area Code Configuration

The following table lists the parameters you can use to configure area code.

Parameter	dialplan.area_code.code	<y0000000000xx>.cfg
Description	It configures the area code to be added before the entered numbers when dialing out. 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".	
Permitted Values	String within 16 characters	
Default	Blank	
Web UI	Settings->Dial Plan->Area Code->Code	
Parameter	dialplan.area_code.min_len	<y0000000000xx>.cfg
Description	It configures the minimum length of the entered number.	
Permitted Values	Integer from 1 to 15	
Default	1	
Web UI	Settings->Dial Plan->Area Code->Min Length (1-15)	
Parameter	dialplan.area_code.max_len	<y0000000000xx>.cfg
Description	It configures the maximum length of the entered number. Note: The value must be larger than the minimum length.	
Permitted Values	Integer from 1 to 15	
Default	15	
Web UI	Settings->Dial Plan->Area Code->Max Length (1-15)	
Parameter	dialplan.area_code.line_id	<y0000000000xx>.cfg
Description	It 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. Note: Multiple line IDs are separated by commas.	
Permitted Values	0 to 8	
Default	Blank	
Web UI	Settings->Dial Plan->Area Code->Account	

Block Out Configuration

The following table lists the parameters you can use to configure block out.

Parameter	dialplan.block_out.number.X ^[1]	<y0000000000xx>.cfg
Description	It 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 phone screen will prompt	

	"Forbidden Number".	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Settings->Dial Plan->Block Out->BlockOut NumberX ^[1]	
Parameter	dialplan.block_out.line_id.X ^[1]	<y0000000000xx>.cfg
Description	It 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. Note: Multiple line IDs are separated by commas.	
Permitted Values	0 to 8	
Default	Blank	
Web UI	Settings->Dial Plan->Block Out->Account	

^[1]X is from 1 to 10.

Example: Adding Replace Rules Using a Replace Rule File

The following example shows the configuration for adding replace rules.

Customize the replace rule template file and place this file to the provisioning server "http://192.168.10.25".

Example

```
dialplan_replace_rule.url = http://192.168.10.25/DialPlan.xml
```

After provisioning, the rules defined in this file are added to the IP phone, and you can use the replace rules on the phone.

Emergency Dialplan

You can 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.

Yealink phones support emergency dialplan.

Emergency Dial Plan

You can configure the emergency dial plan for the phone (for example, emergency number, emergency routing). The phone determines if this is an emergency number by checking the emergency dial plan. 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 could not get through because of the server failure. If the phone is not locked, it checks against the regular dial plan. If the phone is locked, it checks against the emergency dial plan.

Topic

[Emergency Dialplan Configuration](#)

Emergency Dialplan Configuration

The following table lists the parameters you can use to configure emergency dialplan.

Parameter	dialplan.emergency.enable	<y0000000000xx>.cfg
Description	It enables or disables the Emergency dialplan feature.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Parameter	dialplan.emergency.asserted_id_source	<y0000000000xx>.cfg
Description	It configures the precedence of the source of emergency outbound identities when placing an emergency call. Note: If the obtained LLDP-MED ELIN value is blank and no custom outbound identity, the PAI header will not be included in the SIP INVITE request. It works only if "dialplan.emergency.enable" is set to 1 (Enabled).	
Permitted Values	ELIN -If it is set to ELIN , the outbound identity used in the P-Asserted-Identity (PAI) header of the SIP INVITE request is taken from the network using an LLDP-MED Emergency Location Identifier Number (ELIN). The custom outbound identity configured by "dialplan.emergency.custom_asserted_id" will be used if the phone fails to get the LLDP-MED ELIN value. CUSTOM -If it is set to CUSTOM , the custom outbound identity configured by "dialplan.emergency.custom_asserted_id" will be used; if "dialplan.emergency.custom_asserted_id" is left blank, the LLDP-MED ELIN value will be used.	
Default	ELIN	
Parameter	dialplan.emergency.custom_asserted_id	<y0000000000xx>.cfg
Description	It configures the custom outbound identity when placing an emergency call. Note: It works only if "dialplan.emergency.enable" is set to 1 (Enabled).	
Permitted Values	10-25 digits - for example, 1234567890. The SIP URI constructed from the number and SIP server (for example, abc.com) is included in the P-Asserted-Identity (PAI) header (for example, <sip:1234567890@abc.com>). SIP URI - for example, sip:1234567890123@abc.com. The full URI is included in the P-Asserted-Identity (PAI) header and the address will be replaced by the emergency server (for example, <sip:1234567890123@emergency.com>). TEL URI - for example, tel:+16045558000. The full URI is included in the P-Asserted-Identity (PAI) header (for example, <tel:+16045558000>).	
Default	Blank	
Parameter	dialplan.emergency.server.X.address ^[1]	<y0000000000xx>.cfg
Description	It configures the IP address or domain name of the emergency server X to be used for routing calls. Note: If the account information has been configured (no matter whether the account registration succeeds or fails), the emergency calls will be dialed using the following priority: SIP server>emergency server; if not, the emergency server will be used. It works only if "dialplan.emergency.enable" is set to 1 (Enabled).	
Permitted Values	IP address or domain name	

Default	Blank	
Parameter	dialplan.emergency.server.X.port ^[1]	<y0000000000xx>.cfg
Description	It configures the port of emergency server X to be used for routing calls. Note: It works only if "dialplan.emergency.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 65535	
Default	5060	
Parameter	dialplan.emergency.server.X.transport_type ^[1]	<y0000000000xx>.cfg
Description	It configures the transport protocol the phones use to communicate with the emergency server X. Note: It works only if "dialplan.emergency.enable" is set to 1 (Enabled).	
Permitted Values	0 -UDP 1 -TCP 2 -TLS 3 -DNS-NAPTR	
Default	0	
Parameter	dialplan.emergency.X.value ^[2]	<y0000000000xx>.cfg
Description	It configures the emergency number to use on your phones so a caller can contact emergency services in the local area when required. Note: It works only if "dialplan.emergency.enable" is set to 1 (Enabled).	
Permitted Values	Number or SIP URI	
Default	When X = 1, the default value is 911; When X = 2-255, the default value is Blank.	
Parameter	dialplan.emergency.X.server_priority ^[2]	<y0000000000xx>.cfg
Description	It configures the priority of which the emergency servers to be used first. Multiple values are separated by commas. The servers to be used in the order listed (left to right). The IP phone tries to make emergency calls using the emergency server with higher priority, and then with lower priority. The IP phone tries to send the INVITE request to each emergency server three times. Note: If the account information has been configured (no matter whether the account registration succeeds or fails), the emergency calls will be dialed using the following priority: SIP server>emergency server; if not, the emergency server will be used. It works only if "dialplan.emergency.enable" is set to 1 (Enabled).	
Permitted Values	a combination of digits 1, 2 and 3	
Default	1, 2, 3	

[1] X is from 1 to 3.

[2] X is from 1 to 255.

[3] X is the account ID. X=1-8.

Off Hook Hot Line Dialing

For security reasons, the phones support off hook hot line dialing feature, which allows the phone to first dial out the pre-configured number when you dial out a call using the account with this feature enabled. The SIP server may then prompts you to enter an activation code for call service. Only if you enter a valid activation code, the 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. The server actions may vary from different servers.

It is also applicable to the IP call and intercom call.

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.

Topic

[Off Hook Hot Line Dialing Configuration](#)

Off Hook Hot Line Dialing Configuration

The following table lists the parameters you can use to configure off hook hot line dialing.

Parameter	account.X.auto_dial_enable ^[1]	<MAC>.cfg
Description	It enables or disables the phone to first dial out a pre-configured number when a user dials out a call using account X.	
Permitted Values	0 -Disabled 1 -Enabled, the phone will first dial out the pre-configured number (configured by the parameter "account.X.auto_dial_num").	
Default	0	
Parameter	account.X.auto_dial_num ^[1]	<MAC>.cfg
Description	It configures the number that the IP phone first dials out when a user dials out a call using account X. Note: It works only if "account.X.auto_dial_enable" is set to 1 (Enabled).	
Permitted Values	String within 1024 characters	
Default	Blank	

^[1]X is the account ID. X=1-8.

Call Timeout

Call timeout defines a specific period of time after which the phone will cancel the dialing if the call is not answered.

Topic

[Call Timeout Configuration](#)

Call Timeout Configuration

The following table lists the parameter you can use to configure call timeout.

Parameter	phone_setting.ringback_timeout	<y0000000000xx>.cfg
Description	It 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 after 180 seconds.	
Permitted Values	Integer from 0 to 3600	
Default	180	

Anonymous Call

Anonymous call allows the caller to conceal the identity information shown to the callee. The callee's phone LCD screen prompts an incoming call from anonymity.

Anonymous calls can be performed locally or on the server. When performing anonymous call on local, the phone sends an INVITE request with a call source "From: "Anonymous" sip:anonymous@anonymous.invalid". If performing Anonymous call on a specific server, you may need to configure anonymous call on code and off code to activate and deactivate server-side anonymous call feature.

Topic

[Anonymous Call Configuration](#)

Anonymous Call Configuration

The following table lists the parameters you can use to configure anonymous call.

Parameter	account.X.anonymous_call ^[1]	<MAC>.cfg
Description	It triggers the anonymous call feature to on or off.	
Permitted Values	0 -Off 1 -On, the phone will block its identity from showing to the callee when placing a call. The callee's phone screen presents "Anonymous" instead of the caller's identity.	
Default	0	
Web UI	Account->Basic->Local Anonymous	
Handset UI	W53P/W60P: OK->Call Features->Anonymous Call->Line X->Status DD Phone: Menu->Features->Anonymous Call->Line X->Local Anonymous CP930W-Base: Menu->Features->Anonymous Call->Line X->Status	
Parameter	account.X.send_anonymous_code ^[1]	<MAC>.cfg
Description	It configures the phone to send anonymous on/off code to activate/deactivate the server-side anonymous call feature for a specific account.	
Permitted Values	0 -Off Code, the phone will send anonymous off code to the server when you deactivate the anonymous call feature. 1 -On Code, the phone will send anonymous on code to the server when you activate the anonymous call	

	feature.	
Default	0	
Web UI	Account->Basic->Send Anonymous Code	
Parameter	account.X.anonymous_call_oncode ^[1]	<MAC>.cfg
Description	It configures the anonymous call on code. The phone will send the code to activate anonymous call feature on server-side when you activate it on the phone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account->Basic->Send Anonymous Code->On Code	
Parameter	account.X.anonymous_call_offcode ^[1]	<MAC>.cfg
Description	It configures the anonymous call off code. The phone will send the code to deactivate anonymous call feature on server-side when you deactivate it on the phone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account->Basic->Send Anonymous Code->Off Code	

^[1]X is the account ID. X=1-8.

Call Number Filter

Call number filter feature allows IP phone to filter designated characters automatically when dialing.

Topic

[Call Number Filter Configuration](#)

Call Number Filter Configuration

The following table lists the parameter you can use to configure call number filter.

Parameter	features.call_num_filter	<y0000000000xx>.cfg
Description	It configures the characters the phone filters when dialing. If the dialed number contains configured characters, the phone will automatically filter these characters when dialing. Example: features.call_num_filter = - If you dial 3-61, the phone will filter the character - and then dial out 361. Note: If it is left blank, the phone will not automatically filter any characters when dialing.	
Permitted	String within 99 characters	

Values	
Default	, -()
Web UI	Features->General Information->Call Number Filter

IP Address Call

You can set the phone whether to receive or place an IP call. You can neither receive nor place an IP call if you disable this feature.

Topic

[IP Address Call Configuration](#)

IP Address Call Configuration

The following table lists the parameter you can use to configure IP address call.

Parameter	features.direct_ip_call_enable	<y0000000000xx>.cfg
Description	It enables or disables to allow IP address call. Note: If you want to receive an IP address call, make sure "sip.trust_ctrl" is set to 0 (Disabled).	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	
Web UI	Features->General Information->Allow IP Call	

Auto Answer

Auto answer allows the handset to automatically answer an incoming call by picking up it from the charger cradle without having to press the off-hook key. The handset will not automatically answer the incoming call during a call even if auto answer is enabled.

The auto answer feature works only if the handset is placed in the charger cradle.

It is not applicable to DD phone and CP930W-Base.

Topic

[Auto Answer Configuration](#)

Auto Answer Configuration

The following table lists the parameter you can use to configure auto answer.

Parameter	custom.handset.auto_answer.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables a user to answer incoming calls by lifting the handset from the charger cradle without having to press the off-hook key. Note: It works if the handset is placed in the charger cradle and the parameter "static.auto_provision.handset_configured.enable" is set to 1 (Enabled).	
Permitted Values	0 -Disabled 1 -Enabled	

Default	1
Handset UI	OK->Settings->Telephony->Auto Answer

Anonymous Call Rejection

Anonymous call rejection allows IP phone to automatically reject incoming calls from callers whose identity has been deliberately concealed.

Anonymous call rejection can be performed locally or on the server. When performing anonymous call rejection on local, the phone sends the server a status message "Status-Line: SIP/2.0 433 Anonymity Disallowed". If performing Anonymous call rejection on a specific server, you may need to configure anonymous call rejection on code and off code to activate and deactivate server-side anonymous call rejection feature.

Topic

[Anonymous Call Rejection Configuration](#)

Anonymous Call Rejection Configuration

The following table lists the parameters you can use to configure anonymous call rejection.

Parameter	account.X.reject_anonymous_call ^[1]	<MAC>.cfg
Description	It triggers the anonymous call rejection feature to on or off.	
Permitted Values	0 -Off 1 -On, the phone will automatically reject incoming calls from users enabled anonymous call feature. The anonymous user's phone screen presents "Forbidden".	
Default	0	
Web UI	Account->Basic->Local Anonymous Rejection	
Handset UI	W53P/W60P: OK->Call Features->Anonymous Call->Line X->Status DD Phone: Menu->Features->Anonymous Call->Line X->Anonymous Rejection	
Parameter	account.X.anonymous_reject_oncode ^[1]	<MAC>.cfg
Description	It configures the anonymous call rejection on code. The phone will send the code to activate anonymous call rejection feature on server-side when you activate it on the phone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account->Basic->Send Anonymous Rejection Code->On Code	
Parameter	account.X.send_anonymous_rejection_code ^[1]	<MAC>.cfg
Description	It configures the IP phone to send anonymous call rejection on/off code to activate/deactivate the server-side anonymous call rejection feature for account X.	
Permitted	0 -Off Code, the phone will send anonymous rejection off code to the server when you deactivate the	

Values	anonymous call rejection feature. 1 -On Code, the phone will send anonymous rejection on code to the server when you activate the anonymous call rejection feature.	
Default	0	
Web UI	Account->Basic->Send Anonymous Rejection Code	
Parameter	account.X.anonymous_reject_offcode ^[1]	<MAC>.cfg
Description	It configures the anonymous call rejection off code. The phone will send the code to deactivate anonymous call rejection feature on server-side when you deactivate it on the phone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account->Basic->Send Anonymous Rejection Code->Off Code	

[1]X is the account ID. X=1-8.

Call Waiting

Call waiting enables you to receive another call when there is already an active call on your phone. If it is disabled, the new incoming call will be rejected automatically.

You can enable call waiting feature and set the phone to play a warning tone to avoid missing important calls during a call.

Yealink phones also support call waiting on code and off code to activate and deactivate server-side call waiting feature. They may vary on different servers.

Topic

[Call Waiting Configuration](#)

Call Waiting Configuration

The following table lists the parameters you can use to configure call waiting.

Parameter	call_waiting.enable	<y0000000000xx>.cfg
Description	It enables or disables the call waiting feature.	
Permitted Values	0 -Disabled, a new incoming call is automatically rejected by the phone with a busy message during a call. 1 -Enabled, the phone screen will present a new incoming call during a call.	
Default	1	
Web UI	Features->General Information->Call Waiting	
Handset UI	W53P/W60P: OK->Call Features->Call Waiting->Status DD Phone: Menu->Features->Call Waiting->Call Waiting	

	CP930W-Base: Menu->Features->Call Waiting->Status	
Parameter	call_waiting.tone	<y0000000000xx>.cfg
Description	It enables or disables the phone to play the call waiting tone when the phone receives an incoming call during a call. Note: It works only if "call_waiting.enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Features->Audio->Call Waiting Tone	
Handset UI	W53P/W60P: OK->Call Features->Call Waiting->Tone DD Phone: Menu->Features->Call Waiting->Play Tone CP930W-Base: Menu->Features->Call Waiting->Tone	
Parameter	call_waiting.on_code	<y0000000000xx>.cfg
Description	It configures the call waiting on code. The phone will send the code to activate call waiting on server-side when you activate it on the phone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->General Information->Call Waiting On Code	
Parameter	call_waiting.off_code	<y0000000000xx>.cfg
Description	It configures the call waiting off code. The phone will send the code to deactivate call waiting on server-side when you deactivate it on the phone.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->General Information->Call Waiting Off Code	

Do Not Disturb (DND)

DND feature enables the phone to reject all incoming calls automatically when you do not want to be interrupted. You can choose to implement DND locally on the phone or on the server-side.

Topics

[DND Settings Configuration](#)

[DND Feature Configuration](#)

DND Settings Configuration

You can change the following DND settings:

- Enable or disable the DND feature. If disabled, the users have no permission to configure DND on their phone.
- Define the return code and the reason of the SIP response message for a rejected incoming call when DND is activated. The caller's phone screen displays the received return code.

The following table lists the parameters you can use to configure the DND settings.

Parameter	features.dnd.allow	<y0000000000xx>.cfg
Description	It enables or disables the DND feature.	
Permitted Values	0 -Disabled, DND cannot be activated and users are not allowed to configure DND on the phone. 1 -Enabled	
Default	1	
Parameter	features.dnd_refuse_code	<y0000000000xx>.cfg
Description	It 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 screen. Note: For Yealink phones, it works only if "features.dnd.allow" is set to 1 (Enabled).	
Permitted Values	404 -Not Found 480 -Temporarily Unavailable 486 -Busy Here, the caller's phone screen will display the reason "Busy Here" when the callee enables DND feature. 603 -Decline	
Default	480	
Web UI	Features->General Information->Return Code When DND	

DND Feature Configuration

Yealink phones support DND on code and off code to activate and deactivate server-side DND feature. They may vary on different servers.

Topic

[DND Configuration](#)

DND Configuration

The following table lists the parameters you can use to configure DND.

Parameter	account.X.dnd.enable ^[1]	<MAC>.cfg
Description	It triggers the DND feature to on or off. Note: It works only if "features.dnd.allow" is set to 1 (Enabled).	
Permitted Values	0 -Off 1 -On, the phone will reject incoming calls on account X.	
Default	0	

Web UI	Features->Forward& DND->DND->AccountX->DND Status	
Handset UI	W53P/W60P: OK->Call Features->Do Not Disturb->LineX->Status DD Phone: Menu->Features->DND->AccountX->DND Status CP930W-Base: Menu->Features->DND->LineX->Status	
Parameter	account.X.dnd.on_code ^[1]	<MAC>.cfg
Description	It configures the DND on code to activate the server-side DND feature. The phone will send the DND on code to the server when you activate DND feature on the phone. Note: It works only if "features.dnd.allow" and "account.X.dnd.enable" are both set to 1.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward& DND->DND->AccountX->On Code	
Parameter	account.X.dnd.off_code ^[1]	<MAC>.cfg
Description	It configures the DND off code to deactivate the server-side DND feature. The phone will send the DND off code to the server when you deactivate DND feature on the phone. Note: It works only if "features.dnd.allow" and "account.X.dnd.enable" are both set to 1.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward& DND->DND->AccountX->Off Code	

^[1]X is the account ID. X=1-8.

Call Hold

Call hold provides a service of placing an active call on hold. It enables you to pause activity on an active call so that you can use the phone for another task, for example, to place or receive another call.

When a call is placed on hold, the 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. The phones support two call hold methods, one is [RFC 3264](#), which sets the "a" (media attribute) in the SDP to sendonly, recvonly or inactive (for example, a=sendonly). The other is [RFC 2543](#), which sets the "c" (connection addresses for the media streams) in the SDP to zero (for example, c=0.0.0.0).

Topic

[Call Hold Configuration](#)

Call Hold Configuration

The following table lists the parameters you can use to configure call hold.

Parameter	sip.rfc2543_hold	<y0000000000xx>.cfg
Description	It enables or disables the phone to use RFC 2543 (c=0.0.0.0) outgoing hold signaling.	
Permitted Values	0 -Disabled, SDP media direction attributes (such as a=sendonly) per RFC 3264 is used when placing a call on hold. 1 -Enabled, SDP media connection address c=0.0.0.0 per RFC 2543 is used when placing a call on hold.	
Default	0	
Web UI	Features->General Information->RFC 2543 Hold	
Parameter	account.X.hold_use_inactive ^[1]	<MAC>.cfg
Description	It enables or disables the phone to use inactive outgoing hold signaling. Note: It works only if "sip.rfc2543_hold" is set to 0 (Disabled).	
Permitted Values	0 -Disabled, SDP media direction attribute "a=sendonly" is used when placing a call on hold. 1 -Enabled, SDP media direction attribute "a=inactive" is used when placing a call on hold. RTP packets will not be sent or received.	
Default	0	

[1]X is the account ID. X=1-8.

Call Forward

You can forward calls in special situations, such as when the phone is busy or there is no answer, or forwarding all incoming calls to a contact immediately.

Topics

[Call Forward Settings Configuration](#)

[Call Forward Feature Configuration](#)

Call Forward Settings Configuration

You can change the following call forward settings:

- Enable or disable the call forward feature. If disabled, the users have no permission to configure call forward on their phone.
- Allow or disallow users to forward an incoming call to an international telephone number (the prefix is 00).
- Enable or disable the display of the Diversion header. The Diversion header allows the phone which receives a forwarded-call to indicate where the call was from.

The following table lists the parameters you can use to change the call forward settings.

Parameter	features.fwd.allow	<y0000000000xx>.cfg
Description	It enables or disables the call forward feature.	
Permitted Values	0 -Disabled, call forward feature is not available to the users. 1 -Enabled	
Default	1	
Parameter	forward.international.enable	<y0000000000xx>.cfg

Description	It enables or disables the phone to forward incoming calls to international numbers (the prefix is 00).	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Features->General Information->Fwd International	
Parameter	features.fwd_diversion_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to present the diversion information when an incoming call is forwarded to the IP phone.	
Permitted Values	0-Disabled 1-Enabled, the server can use the Diversion field with a SIP header to inform the phone of a call's history.	
Default	1	
Web UI	Features->General Information->Diversion/History-Info	

Call Forward Feature Configuration

Yealink phones support call forward on code and off code to activate and deactivate server-side call forward feature. They may vary on different servers.

Topic

[Call Forward Configuration](#)

Call Forward Configuration

The following table lists the parameters you can use to configure call forward.

Parameter	account.X.always_fwd.enable ^[1]	<MAC>.cfg
Description	It triggers always forward feature to on or off. Note: It works only if "features.fwd.allow" is set to 1 (Enabled).	
Permitted Values	0-Off 1-On, incoming calls to the account X are forwarded to the destination number (configured by the parameter "account.X.always_fwd.target") immediately.	
Default	0	
Web UI	Features->Forward&DND->Forward->AccountX->Always Forward->On/Off	
Handset UI	W53P/W60P: OK->Call Features->Call Forward->LineX->Always(Disabled/Enabled) ->Status DD Phone: Menu->Features->Call Forward->AccountX->Always Forward->Always Forward CP930W-Base: Menu->Features->Call Forward->LineX->Always Forward->Status	
Parameter	account.X.always_fwd.target ^[1]	<MAC>.cfg
Description	It configures the destination number of the always forward.	

	Note: It works only if "features.fwd.allow" is set to 1 (Enabled).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward&DND->Forward->AccountX->Always Forward->Target	
Handset UI	<p>W53P/W60P: OK->Call Features->Call Forward->LineX->Always(Enabled) ->Target</p> <p>DD Phone: Menu->Features->Call Forward->AccountX->Always Forward->Forward to</p> <p>CP930W-Base: Menu->Features->Call Forward->LineX->Always Forward->Target</p>	
Parameter	account.X.always_fwd.on_code ^[1]	<MAC>.cfg
Description	<p>It configures the always forward on code to activate the server-side always forward feature.</p> <p>The phone will send the always forward on code and the pre-configured destination number (configured by the parameter "account.X.always_fwd.target") to the server when you activate always forward feature on the phone.</p> <p>Note: It works only if "features.fwd.allow" is set to 1 (Enabled).</p>	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward&DND->Forward->AccountX->Always Forward->On Code	
Parameter	account.X.always_fwd.off_code ^[1]	<MAC>.cfg
Description	<p>It configures the always forward off code to deactivate the server-side always forward feature.</p> <p>The phone will send the always forward off code to the server when you deactivate always forward feature on the phone.</p> <p>Note: It works only if "features.fwd.allow" is set to 1 (Enabled).</p>	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward&DND->Forward->AccountX->Always Forward->Off Code	
Parameter	account.X.busy_fwd.enable ^[1]	<MAC>.cfg
Description	It triggers busy forward feature to on or off.	
Permitted Values	<p>0-Off</p> <p>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.</p>	
Default	0	
Web UI	Features->Forward&DND->Forward->AccountX->Busy Forward->On/Off	

Handset UI	<p>W53P/W60P: OK->Call Features->Call Forward->LineX->Busy(Disabled/Enabled) ->Status</p> <p>DD Phone: Menu->Features->Call Forward->AccountX->Busy Forward->Busy Forward</p> <p>CP930W-Base: Menu->Features->Call Forward->LineX->Busy Forward->Status</p>	
Parameter	account.X.busy_fwd.target ^[1]	<MAC>.cfg
Description	<p>It configures the destination number of the busy forward.</p> <p>Note: It works only if "features.fwd.allow" is set to 1 (Enabled).</p>	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward&DND->Forward->AccountX->Busy Forward->Target	
Handset UI	<p>W53P/W60P: OK->Call Features->Call Forward->LineX->Busy(Enabled) ->Target</p> <p>DD Phone: Menu->Features->Call Forward->AccountX->Busy Forward->Forward to</p> <p>CP930W-Base: Menu->Features->Call Forward->LineX->Busy Forward->Target</p>	
Parameter	account.X.busy_fwd.on_code ^[1]	<MAC>.cfg
Description	<p>It configures the busy forward on code to activate the server-side busy forward feature.</p> <p>The 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 the busy forward feature on the phone.</p> <p>Note: It works only if "features.fwd.allow" is set to 1 (Enabled).</p>	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward&DND->Forward->AccountX->Busy Forward->On Code	
Parameter	account.X.busy_fwd.off_code ^[1]	<MAC>.cfg
Description	<p>It configures the busy forward off code to deactivate the server-side busy forward feature.</p> <p>The phone will send the busy forward off code to the server when you deactivate the busy forward feature on the phone.</p> <p>Note: It works only if "features.fwd.allow" is set to 1 (Enabled).</p>	
Permitted Values	String within 32 characters	
Default	Blank	

Web UI	Features->Forward&DND->Forward->AccountX->Busy Forward->Off Code	
Parameter	account.X.timeout_fwd.enable ^[1]	<MAC>.cfg
Description	It triggers no answer forward feature to on or off. Note: It works only if "features.fwd.allow" is set to 1 (Enabled). DND activated on the specific account deactivates the local No Answer Forward settings.	
Permitted Values	0-Off 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.	
Default	0	
Web UI	Features->Forward&DND->Forward->AccountX->No Answer Forward->On/Off	
Handset UI	W53P/W60P: OK->Call Features->Call Forward->LineX->No Answer(Disabled/Enabled) ->Status DD Phone: Menu->Features->Call Forward->AccountX->No Answer Forward->No Answer Forward CP930W-Base: Menu->Features->Call Forward->LineX->No Answer Forward->Status	
Parameter	account.X.timeout_fwd.target ^[1]	<MAC>.cfg
Description	It configures the destination number of the no answer forward. Note: It works only if "features.fwd.allow" is set to 1 (Enabled).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward&DND->Forward->AccountX->No Answer Forward->Target	
Handset UI	W53P/W60P: OK->Call Features->Call Forward->LineX->No Answer(Enabled) ->Target DD Phone: Menu->Features->Call Forward->AccountX->No Answer Forward->Forward to CP930W-Base: Menu->Features->Call Forward->LineX->No Answer Forward->Target	
Parameter	account.X.timeout_fwd.timeout ^[1]	<MAC>.cfg
Description	It configures ring times (N) to wait before forwarding incoming calls. Note: It works only if "features.fwd.allow" is set to 1 (Enabled).	
Permitted Values	Integer from 0 to 20	
Default	2	
Web UI	Features->Forward&DND->Forward->AccountX->No Answer Forward->After Ring Time(0~120s)	
Handset UI	W53P/W60P:	

	OK->Call Features->Call Forward->LineX->No Answer(Enabled) ->After Ring Time	
	DD Phone:	
	Menu->Features->Call Forward->AccountX->No Answer Forward->After Ring Time	
	CP930W-Base:	
	Menu->Features->Call Forward->LineX->No Answer Forward->After Ring Time	
Parameter	account.X.timeout_fwd.on_code ^[1]	<MAC>.cfg
Description	<p>It configures the no answer forward on code to activate the server-side no answer forward feature.</p> <p>The 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 on the phone.</p> <p>Note: It works only if "features.fwd.allow" is set to 1 (Enabled).</p>	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward&DND->Forward->AccountX->No Answer Forward->On Code	
Parameter	account.X.timeout_fwd.off_code ^[1]	<MAC>.cfg
Description	<p>It configures the no answer forward off code to deactivate the server-side no answer forward feature.</p> <p>The phone will send the no answer forward off code to the server when you deactivate no answer forward feature on the phone.</p> <p>Note: It works only if "features.fwd.allow" is set to 1 (Enabled).</p>	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Forward&DND->Forward->AccountX->No Answer Forward->Off Code	

[1]X is the account ID. X=1-8.

Call Transfer

Call transfer enables the 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.

Yealink 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. The semi-attended transfer is implemented by a REFER method with Replaces in the Refer-To header.
The semi-attended transfer is applicable to that when users do not want to consult with the third party after hearing the ringback tone, and the third party has not answered the call, the users can cancel transfer or implement transfer.
- **Attended Transfer (Consultative Transfer)** -- Transfer a call with prior consulting. Attended transfer is implemented by a REFER method with Replaces in the Refer-To header.

Topic

Call Transfer Configuration

Call Transfer Configuration

The following table lists the parameters you can use to configure call transfer.

Parameter	transfer.semi_attend_tran_enable	<y0000000000xx>.cfg
Description	It enables or disables the semi-attended transfer.	
Permitted Values	0 -Disabled, when the user presses the TRAN key after hearing the ringback tone, the phone will blind transfer the call. 1 -Enabled, when the user presses the TRAN key after hearing the ringback tone, the phone will transfer the call after the transferee answers the call.	
Default	1	
Web UI	Features->Transfer->Semi-Attended Transfer	
Parameter	account.X.transfer_refer_to_contact_header.enable [1]	<MAC>.cfg
Description	It enables or disables the Refer -To header to use the information of the Contact header in the second 200 OK message when attended transfer.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Parameter	transfer.blind_tran_on_hook_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to complete the blind transfer through on-hook besides pressing the TRAN key. Note: Blind transfer means transferring a call directly to another party without consulting.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	
Web UI	Features->Transfer->Blind Transfer On Hook	
Parameter	transfer.on_hook_trans_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to complete the semi-attended/attended transfer through on-hook besides pressing the TRAN key. Note: Semi-attended transfer means transferring a call after hearing the ringback tone; Attended transfer means transferring a call with prior consulting.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	
Web UI	Features->Transfer->Attended Transfer On Hook	

[1]X is the account ID. X=1-8.

Conference

The Yealink phones support three-way local conference and multi-way network conference.

Topics

[Conference Type Configuration](#)

[Network Conference Configuration](#)

Conference Type Configuration

You can specify which type of conference to establish.

The following table lists the parameter you can use to set a conference type.

Parameter	account.X.conf_type ^[1]	<MAC>.cfg
Description	It configures the conference type for a specific account.	
Permitted Values	0 -Local Conference, the conference is set up with the other two parties via the IP phone. 2 -Network Conference, the conference is set up with multiple parties via the server.	
Default	0	
Web UI	Account->Advanced->Conference Type	

^[1]X is the account ID. X=1-8.

Network Conference Configuration

Network conference, also known as a centralized conference, provides you with the flexibility of call with multiple participants (more than three). The phones implement network conference using the REFER method specified in [RFC 4579](#). This feature depends on the support from a SIP server

For network conference, if any party leaves the conference, the remaining parties are still connected.

The following table lists the parameter you can use to configure network conference.

Parameter	account.X.conf_uri ^[1]	<MAC>.cfg
Description	It configures the network conference URI for a specific account. Note: It works only if "account.X.conf_type" is set to 2 (Network Conference).	
Permitted Values	SIP URI within 511 characters	
Default	Blank	
Web UI	Account->Advanced->Conference URI	

^[1]X is the account ID. X=1-8.

SD Card Recording

CP930W-Base phones support manual recording during a call. Before recording, ensure that the SD card has been connected to the phone.

The recorded calls are saved in "*.aac" format and include a date/time stamp, the other party's number/IP address/-name (or the first person's number/IP address/name you called) and the recording file size. For example, 20160422-

1515-Bob was created on Apr. 22, 2016, at 15:15 and you have a call with Bob. Recorded calls can be played on either the phone itself or on a computer using an application capable of playing *.aac files.

Important

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 where you are. It is also very important to have the consent of the person you are calling before recording the conversation.

Topic

[SD Card Recording Configuration](#)

SD Card Recording Configuration

The following table lists the parameter you can use to configure SD-card recording.

Parameter	features.sd_card_call_recording.enable	<y0000000000xx>.cfg
Description	It enables or disables call recording (using an SD card) feature for the IP phone.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	

Multicast Paging

Multicast Paging allows you to easily and quickly broadcast instant audio announcements to users who are listening to a specific multicast group on a specific channel.

Yealink phones support the following 31 channels:

- **0**: Broadcasts are sent to channel 0. Note that the Yealink phones running old firmware version (old paging mechanism) can be regarded as listening to channel 0. It is the default channel.
- **1 to 25**: Broadcasts are sent to channel 1 to 25. We recommend that you specify these channels when broadcasting with Polycom phones which have 25 channels you can listen to.
- **26 to 30**: Broadcasts are sent to channel 26 to 30.

The phones can only send and receives broadcasts to/from the listened channels. Other channels' broadcasts will be ignored automatically by the IP phone.

Topics

[Multicast Paging Group Configuration](#)

[Multicast Listening Group Configuration](#)

[Multicast Paging Settings](#)

Multicast Paging Group Configuration

Yealink phones support up to 31 groups for paging. You can assign multicast IP address with a channel for each group, and specify a label to each group to identify the phones in the group, such as All, Sales, or HR.

The following table lists the parameters you can use to configure a multicast paging group.

Parameter	multicast.paging_address.X.ip_address ^[1]	<y0000000000xx>.cfg
Description	It configures the IP address and port number of the multicast paging group in the paging list. It will be dis-	

	played on the phone screen when placing the multicast paging call. Note: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.	
Permitted Values	String	
Default	Blank	
Web UI	Directory->Multicast IP->Paging List->Paging Address	
Parameter	multicast.paging_address.X.label ^[1]	<y0000000000xx>.cfg
Description	It configures the name of the multicast paging group to be displayed in the paging list. It will be displayed on the phone screen when placing the multicast paging calls.	
Permitted Values	String	
Default	Blank	
Web UI	Directory->Multicast IP->Paging List->Label	
Parameter	multicast.paging_address.X.channel ^[1]	<y0000000000xx>.cfg
Description	It configures the channel of the multicast paging group in the paging list.	
Permitted Values	<p>0-all the Yealink phones running firmware version 80 or earlier or Yealink phones listen to channel 0 or third-party available devices (for example, Cisco phones) in the paging group can receive the RTP stream.</p> <p>1 to 25-the Polycom or Yealink phones preconfigured to listen to the channel can receive the RTP stream.</p> <p>26 to 30-the Yealink phones preconfigured to listen to the channel can receive the RTP stream.</p>	
Default	0	

^[1]X ranges from 1 to 31

Multicast Listening Group Configuration

Yealink phones support up to 31 groups for listening. You can assign multicast IP address with a channel for each group, and specify a label to each group to identify the phones in the group, such as All, Sales, or HR.

The following table lists the parameters you can use to configure the multicast listening group.

Parameter	multicast.listen_address.X.ip_address ^[1]	<y0000000000xx>.cfg
Description	It configures the multicast address and port number that the phone listens to. Note: The valid multicast IP addresses range from 224.0.0.0 to 239.255.255.255.	
Permitted Values	IP address: port	
Default	Blank	
Web UI	Directory->Multicast IP->Multicast Listening->Listening Address	
Parameter	multicast.listen_address.X.label ^[1]	<y0000000000xx>.cfg
Description	It configures the label to be displayed on the phone screen when receiving the multicast paging calls.	
Permitted Values	String within 99 characters	

Default	Blank	
Web UI	Directory->Multicast IP->Multicast Listening->Label	
Parameter	multicast.listen_address.X.channel ^[1]	<y0000000000xx>.cfg
Description	It configures the channel that the IP phone listens to.	
Permitted Values	<p>0-the phone can receive an RTP stream of the pre-configured multicast address from the phones running firmware version 80 or earlier, from the phones listen to the channel 0, or from the available third-party devices (for example, Cisco phones).</p> <p>1 to 25-the phone can receive an RTP stream of the pre-configured multicast address on the channel 1 to 25 respectively from Yealink or Polycom phones.</p> <p>26 to 30-the phone can receive the RTP stream of the pre-configured multicast address on the channel 26 to 30 respectively from Yealink phones.</p>	
Default	0	
Web UI	Directory->Multicast IP->Multicast Listening->Channel	

^[1]X ranges from 1 to 31

Multicast Paging Settings

You can configure some general settings for multicast paging, for example, specify a codec, configure the volume and audio device for listening to a paging call.

By default, all the listening groups are considered with a certain priority from 1 (lower priority) to 31 (higher priority). If you neither want to receive some paging calls nor miss urgent paging calls when there is a voice call or paging call, or when DND is activated, you can use the priority to define how your phone handles different incoming paging calls.

Paging Barge

You can set your phone whether an incoming paging call interrupts an active call.

The Paging Barge defines the lowest priority of the paging group from which the phone can receive a paging call when there is a voice call (a normal phone call rather than a multicast paging call) in progress. You can specify a priority that the incoming paging calls with higher or equal priority are automatically answered, and the lower ones are ignored.

If it is disabled, all incoming paging calls will be automatically ignored.

Paging Priority

You can set your phone whether a new incoming paging call interrupts a current paging call.

The Paging Priority feature decides how the phone handles incoming paging calls when there is already a paging call on the phone. If enabled, the phone will ignore incoming paging calls with lower priorities, otherwise, the phone will answer incoming paging calls automatically and place the previous paging call on hold. If disabled, the phone will automatically ignore all incoming paging calls.

Topic

[Multicast Paging Settings Configuration](#)

Multicast Paging Settings Configuration

The following table lists the parameters you can use to change multicast paging settings.

Parameter	multicast.codec	<y0000000000xx>.cfg
Description	It configures the codec for multicast paging.	
Permitted Values	PCMU, PCMA, G729, G722	
Default	G722	
Web UI	Features->General Information->Multicast Codec	
Parameter	multicast.receive_priority.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to handle the incoming multicast paging calls when there is an active multicast paging call on the phone.	
Permitted Values	<p>0-Disabled, the phone will ignore the incoming multicast paging calls when there is an active multicast paging call on the phone.</p> <p>1-Enabled, the phone will receive the incoming multicast paging call with a higher priority and ignore the one with a lower priority.</p>	
Default	1	
Web UI	Directory->Multicast IP->Paging Priority Active	
Parameter	multicast.receive_priority.priority	<y0000000000xx>.cfg
Description	<p>It configures the priority of the voice call (a normal phone call rather than a multicast paging call) in progress.</p> <p>1 is the highest priority, 31 is the lowest priority.</p>	
Permitted Values	<p>0-Disabled, all incoming multicast paging calls will be automatically ignored when a voice call is in progress.</p> <p>1-1</p> <p>2-2</p> <p>3-3</p> <p>...</p> <p>31-31</p> <p>If it is set to other values, the phone will receive the incoming multicast paging call with a higher or equal priority and ignore the one with a lower priority when a voice call is in progress.</p>	
Default	31	
Web UI	Directory->Multicast IP->Paging Barge	
Parameter	multicast.listen_address.X.volume ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the volume of the speaker when receiving the multicast paging calls.</p> <p>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.</p> <p>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.</p> <p>Example:</p>	

	multicast.listen_address.1.volume = 1	
Permitted Values	Integer from 0 to 15	
Default	0	
Parameter	multicast.receive.use_speaker	<y0000000000xx>.cfg
Description	It enables or disables the phone to always use the speaker as the audio device when receiving the multicast paging calls.	
Permitted Values	0 -Disabled, the engaged audio device will be used when receiving the multicast paging calls. 1 -Enabled	
Default	0	

[1]X ranges from 1 to 31.

End Call on Hook

You can configure whether to end a call when you place the handset into the charge cradle.

It is not applicable to CP930W-Base phones.

Topic

[End Call on Hook Configuration](#)

End Call on Hook Configuration

The following table lists the parameter you can use to configure the end call on hook.

Parameter	phone_setting.end_call_on_hook.enable	<y0000000000xx>.cfg
Description	It enables or disables to end a call when placing the handset into the charger cradle.	
Permitted Values	0 -Never 1 -Always	
Default	1	
Web UI	Features->General Information->End Call On Hook	

Audio Features

This chapter describes the audio sound quality features and options you can configure for the IP phone.

Topics

[Alert Tone](#)

[Ringer Device](#)

[Tones](#)

[Audio Codecs](#)

[Packetization Time \(PTime\)](#)

[Early Media](#)

[Acoustic Clarity Technology](#)

[DTMF](#)

[Voice Quality Monitoring \(VQM\)](#)

Alert Tone

You can configure the following audio alert for the phone:

- Voice mail tone: allow 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.
- Dial tone: allow the IP phone to play a specific dial tone for a specified time.

Topic

[Alert Tone Configuration](#)

Alert Tone Configuration

The following table lists the parameters you can use to configure the alert tone.

Parameter	features.call.dialtone_time_out	<y0000000000xx>.cfg
Description	It configures the duration time (in seconds) that a dial tone plays before a call is dropped. If it is set to 0, the call is not dropped.	
Permitted Values	0 to 65535	
Default	15	
Parameter	features.voice_mail_tone_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to play a warning tone when it receives a new voice mail. Note: It works only if "account.X.display_mwi.enable" is set to 1 (Enabled).	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	
Web UI	Features->General Information->Voice Mail Tone	

Ringer Device

The phones support either or both speaker and headset ringer devices. You can 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.

It is not applicable to CP930W-Base phones.

Topic

[Ringer Device Configuration](#)

Ringer Device Configuration

The following table lists the parameters you can use to configure ringer device.

Parameter	features.ringer_device.is_use_headset	<y0000000000xx>.cfg
Description	It configures the ringer device for the phones.	
Permitted Values	0 -Use Speaker 1 -Use Headset	
Default	0	
Web UI	Features->Audio->Ringer Device for Headset	

Tones

When receiving a message, the 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.

Topics

[Supported Tones](#)

[Tones Configuration](#)

Supported Tones

The default tones used on the phones are the US tone sets. Available tone sets for 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 the phones in the following conditions.

Condition	Description
Dial	When in the dialing interface
Ring Back	Ring-back tone
Busy	When the callee is busy
Call Waiting	Call waiting tone (For more information on call waiting, refer to Call Waiting)

Tones Configuration

The following table lists the parameters you can use to configure tones.

Parameter	voice.tone.country	<y0000000000xx>.cfg
Description	It configures the country tone for the phones.	
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	
Default	Custom	
Web UI	Settings->Tones->Select Country	
Parameter	voice.tone.dial	<y0000000000xx>.cfg
Description	<p>It customizes the dial tone.</p> <p>tone list = element[,element] [,element]...</p> <p>Where</p> <p>element = [!]Freq1[+Freq2][+Freq3][+Freq4] /Duration</p> <p>Freq: the frequency of the tone (ranges from 200 to 4000 Hz). If it is set to 0 Hz, it means the tone is not played.</p>	

	<p>Duration: the duration (in milliseconds) of the dial tone, ranges from 0 to 30000ms.</p> <p>You can configure at most eight different tones for one condition, and separate them by commas. (for example, 250/200,0/1000,200+300/500,200+500+800+1500/1000).</p> <p>If you want the IP phone to play tones once, add an exclamation mark "!" before tones (for example, !250/200,0/1000, 200+300/500,200+500+800+1500/1000).</p> <p>Note: It works only if "voice.tone.country" is set to Custom.</p>	
Permitted Values	String	
Default	Blank	
Web UI	Settings->Tones->Dial	
Parameter	voice.tone.ring	<y0000000000xx>.cfg
Description	<p>It customizes the ringback tone.</p> <p>The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".</p> <p>Note: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.</p>	
Permitted Values	String	
Default	Blank	
Web UI	Settings->Tones->Ring Back	
Parameter	voice.tone.busy	<y0000000000xx>.cfg
Description	<p>It customizes the tone when the callee is busy.</p> <p>The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".</p> <p>Note: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.</p>	
Permitted Values	String	
Default	Blank	
Web UI	Settings->Tones->Busy	
Parameter	voice.tone.callwaiting	<y0000000000xx>.cfg
Description	<p>It customizes the call waiting tone.</p> <p>The value format is Freq/Duration. For more information on the value format, refer to the parameter "voice.tone.dial".</p> <p>Note: It works only if "voice.tone.country" is set to Custom. If you want to disable this warning tone, set it to 0.</p>	
Permitted Values	String	
Default	Blank	

Web UI	Settings->Tones->Call Waiting
---------------	-------------------------------

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 a 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 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.

Topics

[Supported Audio Codecs](#)

[Audio Codecs Configuration](#)

Supported Audio Codecs

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

Codec	Algorithm	Reference	Bit Rate	Sample Rate	Packetization Time
G722	G.722	RFC 3551	64 Kbps	16 Ksps	20ms
PCMA	G.711 a-law	RFC 3551	64 Kbps	8 Ksps	20ms
PCMU	G.711 u-law	RFC 3551	64 Kbps	8 Ksps	20ms
G729	G.729	RFC 3551	8 Kbps	8 Ksps	20ms
G726-16	G.726	RFC 3551	16 Kbps	8 Ksps	20ms
G726-24	G.726	RFC 3551	24 Kbps	8 Ksps	20ms
G726-32	G.726	RFC 3551	32 Kbps	8 Ksps	20ms
G726-40	G.726	RFC 3551	40 Kbps	8 Ksps	20ms
iLBC	iLBC	RFC 3952	15.2 Kbps 13.33 Kbps	8 Kps	20ms 30ms
opus	opus	RFC 6716	8-12 Kbps 16-20 Kbps 28-40 Kbps 48-64 Kbps 64-128 Kbps	8 Ksps 12 Ksps 16 Ksps 24 Ksps 48 Ksps	20ms

Note

The network bandwidth necessary to send the encoded audio is typically 5~10% higher than the bit rate due to packetization overhead. For example, a two-way G.722 audio call at 64 Kbps consumes about 135 Kbps of network bandwidth.

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

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

The following table lists the audio codecs supported by each phone model:

Phone Model	Supported Audio Codecs	Default Audio Codecs
W53P/W60P/W41P/CP930W-Base	G722, PCMA, PCMU, G729, G726-16, G726-24, G726-32, G726-40, iLBC, opus	G722, PCMA, PCMU, G729

Audio Codecs Configuration

The following table lists the parameters you can use to configure the audio codecs.

Parameter	account.X.codec.<payload_type>.enable ^[1]	<MAC>.cfg
Description	It enables or disables the specified audio codec. The name of the audio codec: g722 -G722 pcmu -PCMU pcma -PCMA g729 -G729 g726_16 -G726-16 g726_24 -G726-24 g726_32 -G726-32 g726_40 -G726-40 opus -opus ilbc -iLBC Example: account.1.codec.g722.enable = 1 Note: The name of the audio codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	Default: When the audio codec is G722, the default value is 1; When the audio codec is PCMU, the default value is 1;	

	<p>When the audio codec is PCMA, the default value is 1;</p> <p>When the audio codec is G729, the default value is 1;</p> <p>When the audio codec is G726-16, the default value is 0;</p> <p>When the audio codec is G726-24, the default value is 0;</p> <p>When the audio codec is G726-32, the default value is 0;</p> <p>When the audio codec is G726-40, the default value is 0;</p> <p>When the audio codec is opus, the default value is 0;</p> <p>When the audio codec is iLBC, the default value is 0;</p>	
Web UI	Account->Codec->Audio Codec	
Parameter	account.X.codec.<payload_type>.priority ^[1]	<MAC>.cfg
Description	<p>It configures the priority of the enabled audio codec.</p> <p>The name of the audio codec:</p> <p>g722-G722</p> <p>pcmu-PCMU</p> <p>pcma-PCMA</p> <p>g729-G729</p> <p>g726_16-G726-16</p> <p>g726_24-G726-24</p> <p>g726_32-G726-32</p> <p>g726_40-G726-40</p> <p>opus-opus</p> <p>ilbc-iLBC</p> <p>Example:</p> <p>account.1.codec.g722.priority = 1</p> <p>Note: The priority of the codec in disable codec list is not specified, and numerical value 1 is defined as the highest priority in the enable codec list. The name of the audio codec in this parameter should be the correct one as listed in the above example, otherwise the corresponding configuration will not take effect.</p>	
Permitted Values	Integer from 0 to 10	
Default	<p>Default:</p> <p>When the audio codec is G722, the default value is 1;</p> <p>When the audio codec is PCMU, the default value is 2;</p> <p>When the audio codec is PCMA, the default value is 3;</p> <p>When the audio codec is G729, the default value is 4;</p> <p>When the audio codec is G726_16, the default value is 0;</p>	

	When the audio codec is G726_24, the default value is 0; When the audio codec is G726_32, the default value is 0; When the audio codec is G726_40, the default value is 0; When the audio codec is opus, the default value is 0; When the audio codec is iLBC, the default value is 0;
Web UI	Account->Codec->Audio Codec

[1]X is the account ID. X=1-8.

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.

Topics

[Supported PTime of Audio Codec](#)

[PTime Configuration](#)

Supported PTime of Audio Codec

The following table summarizes the valid values of ptime for each audio codec:

Codec	Packetization Time (Minimum)	Packetization Time (Maximum)
G722	10ms	40ms
PCMA	10ms	40ms
PCMU	10ms	40ms
G729	10ms	80ms
G726-16	10ms	30ms
G726-24	10ms	30ms
G726-32	10ms	30ms
G726-40	10ms	30ms
iLBC	20ms	30ms
opus	10ms	20ms

PTime Configuration

The following table lists the parameter you can use to configure the PTime.

Parameter	account.X.ptime ^[1]	<MAC>.cfg
Description	It configures the ptime (in milliseconds) for the codec.	
Permitted Values	0 -Disabled 10 -10 20 -20 30 -30 40 -40 50 -50 60 -60	
Default	20	
Web UI	Account->Advanced->PTime(ms)	

^[1]X is the account ID. X=1-8.

Early Media

The early media refers to the media (for example, audio and video) played to the caller before a SIP call is actually established.

You can also configure 180 ring workaround which 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 the phones to resume and play the local ringback tone upon a subsequent 180 message received.

Topic

[Early Media Configuration](#)

Early Media Configuration

The following table lists the parameters you can use to configure the early media.

Parameter	phone_setting.is_deal180	<y0000000000xx>.cfg
Description	It enables or disables the phone to deal with the 180 SIP message received after the 183 SIP message.	
Permitted Values	0 -Disabled 1 -Enabled, the phone will resume and play the local ringback tone upon a subsequent 180 message received.	
Default	1	
Web UI	Features->General Information->180 Ring Workaround	

Acoustic Clarity Technology

To optimize the audio quality of your network, Yealink phones support the acoustic clarity technology: Background Noise Suppression (BNS), Automatic Gain Control (AGC), Voice Activity Detection (VAD), Comfort Noise Generation (CNG) and jitter buffer.

Topics

[Background Noise Suppression \(BNS\)](#)

[Automatic Gain Control \(AGC\)](#)

[Voice Activity Detection \(VAD\)](#)

[Comfort Noise Generation \(CNG\)](#)

[Jitter Buffer](#)

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 the hands-free operation and is used to keep audio output at nearly a constant level by adjusting the gain of signals in some circumstances. This increases the effective user-phone radius and helps with the intelligibility of soft-talkers.

Voice Activity Detection (VAD)

VAD can avoid unnecessary coding or transmission of silence packets in VoIP applications, saving on computation and network bandwidth.

Topic

[VAD Configuration](#)

VAD Configuration

The following table lists the parameter you can use to configure VAD.

Parameter	voice.vad	<y0000000000xx>.cfg
Description	It enables or disables the VAD (Voice Activity Detection) feature.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Settings->Voice->Echo Cancellation->VAD	

Comfort Noise Generation (CNG)

Comfort Noise Generation (CNG) is used to generate background noise for voice communications during periods of silence in a conversation.

Note

VAD is used to send CN packets when the phone detects a "silence" period; CNG is used to generate comfortable noise when the phone receives CN packets from the other side.

Topic

[CNG Configuration](#)

CNG Configuration

The following table lists the parameter you can use to configure CNG.

Parameter	voice.cng	<y0000000000xx>.cfg
Description	It enables or disables the CNG (Comfortable Noise Generation) feature.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Settings->Voice->Echo Cancellation->CNG	

Jitter Buffer

Yealink 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 the 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 the phones.

Topic

[Jitter Buffer Configuration](#)

Jitter Buffer Configuration

You can configure the mode of jitter buffer and the delay time for jitter buffer in the wired network or wireless network.

The following table lists the parameters you can use to configure the jitter buffer.

Parameter	voice.jib.adaptive	<y0000000000xx>.cfg
Description	It configures the type of jitter buffer in the wired network.	
Permitted Values	0 -Fixed 1 -Adaptive	
Default	1	
Web UI	Settings->Voice->JITTER BUFFER->Type	
Parameter	voice.jib.min	<y0000000000xx>.cfg
Description	It configures the minimum delay time (in milliseconds) of jitter buffer in the wired network. Note: It works only if "voice.jib.adaptive" is set to 1 (Adaptive). The value of this parameter should be less than "voice.jib.max" and "voice.jib.normal".	
Permitted Values	Integer from 0 to 400	
Default	60	
Web UI	Settings->Voice->JITTER BUFFER->Min Delay	
Parameter	voice.jib.max	<y0000000000xx>.cfg
Description	It configures the maximum delay time (in milliseconds) of jitter buffer in the wired network.	

	Note: It works only if "voice.jib.adaptive" is set to 1 (Adaptive). The value of this parameter should be greater than "voice.jib.normal" and "voice.jib.min".	
Permitted Values	Integer from 0 to 400	
Default	240	
Web UI	Settings->Voice->JITTER BUFFER->Max Delay	
Parameter	voice.jib.normal	<y0000000000xx>.cfg
Description	It configures the normal delay time (in milliseconds) of jitter buffer in the wired network. Note: It works only if "voice.jib.adaptive" is set to 0 (Fixed). The value of this parameter should be greater than "voice.jib.min" and less than "voice.jib.max".	
Permitted Values	Integer from 0 to 400	
Default	120	
Web UI	Settings->Voice->JITTER BUFFER->Normal	

DTMF

DTMF (Dual Tone Multi-frequency) tone, better known as touch tone. 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.

Topics

- [DTMF Keypad](#)
- [Transmitting DTMF Digit](#)
- [Suppress DTMF Display](#)
- [Transfer via DTMF](#)
- [Local DTMF Tone](#)

DTMF Keypad

The DTMF keypad is laid out in a 4x4 matrix, with each row representing a low frequency, and each column representing a high frequency. Pressing a digit key (such as '1') will generate a sinusoidal tone for each of two frequencies (697 and 1209 hertz (Hz)).

DTMF Keypad Frequencies:

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

Note

The phones will not send DTMF sequence when the call is placed on hold or is held.

Transmitting DTMF Digit

Three methods of transmitting DTMF digits on SIP calls:

- **RFC 2833** -- DTMF digits are transmitted by RTP Events compliant with RFC 2833. You can configure the payload type and sending times of the end RTP Event packet. 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 in the voice band. It uses the same codec as your voice and is audible to conversation partners.
- **SIP INFO** -- DTMF digits are transmitted by SIP INFO messages. 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 can transmit DTMF digits in three ways: DTMF, DTMF-Relay and Telephone-Event.

Topic

[Transmitting DTMF Digit Configuration](#)

Transmitting DTMF Digit Configuration

The following table lists the parameters you can use to configure the transmitting DTMF digit.

Parameter	account.X.dtmf.type ^[1]	<MAC>.cfg
Description	It configures the DTMF type.	
Permitted Values	0 -INBAND, DTMF digits are transmitted in the voice band. 1 -RFC2833, DTMF digits are transmitted by RTP Events compliant to RFC 2833. 2 -SIP INFO, DTMF digits are transmitted by the SIP INFO messages. 3 -RFC2833 + SIP INFO, DTMF digits are transmitted by RTP Events compliant to RFC 2833 and the SIP INFO messages.	
Default	1	
Web UI	Account->Advanced->DTMF Type	
Parameter	account.X.dtmf.dtmf_payload ^[1]	<MAC>.cfg
Description	It configures the value of DTMF payload. Note: It works only if "account.X.dtmf.type" is set to 1 (RFC2833) or 3 (RFC2833 + SIP INFO).	
Permitted Values	Integer from 96 to 127	
Default	101	
Web UI	Account->Advanced->DTMF Payload Type(96~127)	
Parameter	account.X.dtmf.info_type ^[1]	<MAC>.cfg
Description	It configures the DTMF info type. Note: It works only if "account.X.dtmf.type" is set to 2 (SIP INFO) or 3 (RFC2833 + SIP INFO).	
Permitted Values	1 -DTMF-Relay 2 -DTMF	

	3-Telephone-Event	
Default	1	
Web UI	Account->Advanced->DTMF Info Type	
Parameter	features.dtmf.repetition	<y0000000000xx>.cfg
Description	It configures the repetition times for the phone to send the end RTP Event packet during an active call.	
Permitted Values	1, 2 or 3	
Default	3	
Web UI	Features->General Information->DTMF Repetition	
Parameter	features.dtmf.duration ^[2]	<y0000000000xx>.cfg
Description	It configures the duration time (in milliseconds) for each digit when a sequence of DTMF tones is played out automatically. Note: If the time interval 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.	
Permitted Values	Integer from 0 to	
Default	100	
Parameter	features.dtmf.volume	<y0000000000xx>.cfg
Description	It configures the volume of the DTMF tone (in db).	
Permitted Values	Integer from -33 to 0	
Default	-10	

[1]X is the account ID. X=1-8.

[2]If you change this parameter, the phone will reboot to make the change take effect.

Suppress DTMF Display

Suppress DTMF display allows the phones to suppress the display of DTMF digits during an active call. DTMF digits are displayed as "*" on the phone screen. Suppress DTMF display delay defines whether to display the DTMF digits for a short period of time before displaying as "**".

Topic

[Suppress DTMF Display Configuration](#)

Suppress DTMF Display Configuration

The following table lists the parameters you can use to configure the suppress DTMF display.

Parameter	features.dtmf.hide	<y0000000000xx>.cfg
Description	It enables or disables the phone to suppress the display of DTMF digits during an active call.	

Permitted Values	0-Disabled 1-Enabled, the DTMF digits are displayed as asterisks.	
Default	0	
Web UI	Features->General Information->Suppress DTMF Display	
Parameter	features.dtmf.hide_delay	<y0000000000xx>.cfg
Description	It enables or disables the phone to display the DTMF digits for a short period before displaying asterisks during an active call. Note: It works only if “features.dtmf.hide” is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Features->General Information->Suppress DTMF Display Delay	

Voice Quality Monitoring (VQM)

Voice quality monitoring feature allows the 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. Yealink phones support two mechanisms for voice quality monitoring: RTCP-XR and VQ-RTCPXR.

Topics

[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.

Topic

[RTCP-XR Configuration](#)

RTCP-XR Configuration

The following table lists the parameters you can use to configure the RTCP-XR.

Parameter	voice.rtcp_xr.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the phone to send RTCP-XR packets.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Settings->Voice Monitoring->Voice RTCP-XR Report	
Parameter	voice.rtcp.enable ^[1]	<y0000000000xx>.cfg

Description	It enables or disables the phone to send RTCP packets.	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Parameter	voice.rtcp_cname ^[1]	<y0000000000xx>.cfg
Description	It configures the cname of the RTCP packets.	
Permitted Values	String	
Default	Blank	

^[1]If you change this parameter, the 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.

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).

Topics

[Voice Quality Reports](#)

[VQ-RTCPXR Display](#)

[Central Report Collector](#)

Voice Quality Reports

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.

Topic

[Voice Quality Reports Configuration](#)

Voice Quality Reports Configuration

The following table lists the parameters you can use to configure the service quality reports.

Parameter	phone_setting.vq_rtcpxr.session_report.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to send a session quality report to the central report collector at the end of each call.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	

Web UI	Settings->Voice Monitoring->VQ RTCP-XR Session Report	
Parameter	phone_setting.vq_rtcp_xr.interval_report.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to send an interval quality report to the central report collector periodically throughout a call.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Settings->Voice Monitoring->VQ RTCP-XR Interval Report	
Parameter	phone_setting.vq_rtcp_xr.interval_period	<y0000000000xx>.cfg
Description	It configures the interval (in seconds) for the phone to send an interval quality report to the central report collector periodically throughout a call. Note: It works only if "phone_setting.vq_rtcp_xr.interval_report.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 5 to 20	
Default	20	
Web UI	Settings->Voice Monitoring->Period for Interval Report	
Parameter	phone_setting.vq_rtcp_xr.moslq_threshold_warning	<y0000000000xx>.cfg
Description	It 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.	
Permitted Values	15 to 40	
Default	Blank	
Web UI	Settings->Voice Monitoring->Warning threshold for Moslq	
Parameter	phone_setting.vq_rtcp_xr.moslq_threshold_critical	<y0000000000xx>.cfg
Description	It 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.	
Permitted Values	15 to 40	
Default	Blank	

Web UI	Settings->Voice Monitoring->Critical threshold for Moslq	
Parameter	phone_setting.vq_rtcpxr_delay_threshold_warning	<y0000000000xx>.cfg
Description	<p>It 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.</p> <p>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.</p> <p>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.</p>	
Permitted Values	10 to 2000	
Default	Blank	
Web UI	Settings->Voice Monitoring->Warning threshold for Delay	
Parameter	phone_setting.vq_rtcpxr_delay_threshold_critical	<y0000000000xx>.cfg
Description	<p>It configures the threshold value of one-way delay (in milliseconds) that causes the phone to send a critical alert quality report to the central report collector.</p> <p>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.</p> <p>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.</p>	
Permitted Values	10 to 2000	
Default	Blank	
Web UI	Settings->Voice Monitoring->Critical threshold for Delay	

VQ-RTCPXR Display

You can check the voice quality data of the last call via web user interface.

Topic

[VQ-RTCPXR Display Configuration](#)

VQ-RTCPXR Display Configuration

The following table lists the parameters you can use to configure VQ-RTCPXR display.

Parameter	phone_setting.vq_rtcpxr.states_show_on_web.enable	<y0000000000xx>.cfg
Description	It enables or disables the voice quality data of the last call to be displayed on the web interface at the path Status->RTP Status .	
Permitted Values	0 -Disabled 1 -Enabled	

Default	0
Web UI	Settings->Voice Monitoring->Display Report options on Web

Central Report Collector

To operate with central report collector, the 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.

Topic

[Central Report Collector Configuration](#)

Central Report Collector Configuration

The following table lists the parameters you can use to configure central report collector.

Parameter	account.X.vq_rtcp_xr.collector_name ^[1]	<MAC>.cfg
Description	It configures the host name of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Account->Advanced->VQ RTCP-XR Collector Name	
Parameter	account.X.vq_rtcp_xr.collector_server_host ^[1]	<MAC>.cfg
Description	It configures the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.	
Permitted Values	IPv4 Address	
Default	Blank	
Web UI	Account->Advanced->VQ RTCP-XR Collector Address	
Parameter	account.X.vq_rtcp_xr.collector_server_port ^[1]	<MAC>.cfg
Description	It configures the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.	
Permitted Values	Integer from 1 to 65535	
Default	5060	
Web UI	Account->Advanced->VQ RTCP-XR Collector Port	

^[1]X is the account ID. X=1-8.

Security Features

This chapter provides information for configuring the security features of the phone.

Topics

[User and Administrator Identification](#)

[Auto Logout Time](#)

[Base PIN](#)

[Emergency Number](#)

[Transport Layer Security \(TLS\)](#)

[Secure Real-Time Transport Protocol \(SRTP\)](#)

[Encrypting and Decrypting Files](#)

[Incoming Network Signaling Validation](#)

User and Administrator Identification

By default, some menu options are protected by privilege levels: user and administrator, each with its own password. You can also customize the access permission for configurations on the web user interface and phone/handset user interface. Yealink phones support access levels of admin, var and user.

When logging into the web user interface or access advanced settings on the phone, as an administrator, you need an administrator password to access various menu options. The default username and password for administrator is "admin". Both you and the user can log into the web user interface, and you will see all of the user options. The default username and password for the user is "user".

For security reasons, you should change the default user or administrator password as soon as possible. Since advanced menu options are strictly used by the administrator, users can configure them only if they have administrator privileges.

Topics

[User and Administrator Identification Configuration](#)

[User Access Level Configuration](#)

User and Administrator Identification Configuration

The following table lists the parameters you can use to configure the user and administrator identification.

Parameter	static.security.user_name.user	<y0000000000xx>.cfg
Description	It configures the user name of the user for the phone's web user interface access.	
Permitted Values	String within 32 characters	
Default	user	
Parameter	static.security.user_name.admin	<y0000000000xx>.cfg
Description	It configures the user name of the administrator for phone's web user interface access.	
Permitted Values	String within 32 characters	
Default	admin	

Parameter	static.security.user_name.var	<y0000000000xx>.cfg
Description	<p>It configures the user name of the var for phone's web user interface access.</p> <p>Note: It works only if "static.security.var_enable" is set to 1 (Enabled).</p>	
Permitted Values	String within 32 characters	
Default	var	
Parameter	static.security.user_password	<y0000000000xx>.cfg
Description	<p>It configures the password of the user or administrator.</p> <p>The phone uses "user" as the default user password, "var" as the default var password and "admin" as the default administrator password.</p> <p>The valid value format is <username>:<new password>.</p> <p>Example:</p> <p>static.security.user_password = user:123 means setting the password of user to 123.</p> <p>static.security.user_password = admin:456 means setting the password of administrator to 456.</p> <p>static.security.user_password = var:789 means setting the password of var to 789.</p> <p>Note: The phones support ASCII characters 32-126(0x20-0x7E) in passwords. You can set the password to be empty via web user interface only.</p>	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Security->>Password	

User Access Level Configuration

For more information, refer to [Yealink SIP IP Phones Configuration Guide for User Access Level](#).

The following table lists the parameters you can use to configure the user access level.

Parameter	static.security.var_enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the 3-level access permissions (admin, user, var).	
Permitted Values	<p>0-Disabled</p> <p>1-Enabled</p>	
Default	0	
Parameter	static.web_item_level.url ^[1]	<y0000000000xx>.cfg
Description	It configures the access URL of the file, which defines 3-level access permissions.	
Permitted Values	URL within 511 characters	
Default	Blank	
Parameter	static.security.default_access_level ^[1]	<y0000000000xx>.cfg
Description	<p>It configures the default access level to access the handset user interface.</p> <p>Note: It works only if "static.security.var_enable" is set to 1 (Enabled).</p>	

Permitted Values	0 -user 1 -var 2 -admin
Default	0

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Auto Logout Time

Auto logout time defines how long to log out the web user interface automatically when you do not perform any actions on web user interface. Once logging out, you must re-enter username and password for web access authentication.

Topic

[Auto Logout Time Configuration](#)

Auto Logout Time Configuration

The following table lists the parameter you can use to configure the auto logout time.

Parameter	features.relog_offtime	<y0000000000xx>.cfg
Description	It configures the timeout interval (in minutes) for web access authentication.	
Permitted Values	Integer from 1 to 1000	
Default	5	
Web UI	Features->General Information->Auto Logout Time(1~1000min)	

Base PIN

To avoid unauthorized register or access to some features on the handset, you should keep the base PIN secret.

You can change the base PIN for security.

Topic

[Base PIN Configuration](#)

Base PIN Configuration

The following table lists the parameters you can use to configure the base PIN.

Parameter	base.pin_code	<y0000000000xx>.cfg
Description	It configures the base PIN.	
Permitted Values	Integer from 0000 to 9999	
Default	0000	
Web UI	Security->Base PIN->Base Unit PIN	
Handset UI	W53P/W60P:	

	OK->Settings->System Settings->Change Base PIN DD Phone: Menu->Settings->Advanced Settings (default password: 0000) ->Change Password CP930W-Base: Menu->Settings->Advanced Settings (default PIN: 0000) ->Change PIN	
Parameter	base.double_pin_code.enable	<y0000000000xx>.cfg
Description	It enables or disables double PIN feature.	
Permitted Values	0 -Disabled, users use the PIN configured by "base.pin_code" to register the handset or access some features. 1 -Enabled, users use the PIN configured by "base.pin_code_for_register" to register the handset, and use the PIN configured by "base.pin_code" to access some features.	
Default	0	
Parameter	base.pin_code_for_register	<y0000000000xx>.cfg
Description	It configures the PIN for registering or de-registering a handset. Note: It works only if "base.double_pin_code.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 0000 to 9999	
Default	0000	

Emergency Number

Public telephone networks in countries around the world have a single emergency telephone number (emergency services number), that allows a caller to contact local emergency services for assistance when necessary.

You can specify the emergency numbers for contacting the emergency services in an emergency situation. The emergency telephone number may differ from country to country. It is typically a three-digit number so that it can be easily remembered and dialed quickly.

You can dial these numbers when the phone is locked (CP930W-Base phones can not be locked).

Topic

[Emergency Number Configuration](#)

Emergency Number Configuration

The following table lists the parameter you can use to configure the emergency number.

Parameter	phone_setting.emergency.number	<y0000000000xx>.cfg
Description	It configures emergency numbers. Multiple emergency numbers are separated by commas.	
Permitted Values	String within 99 characters	
Default	112,911,110	

Web UI	Features->Phone Lock->Emergency
---------------	---------------------------------

Transport Layer Security (TLS)

TLS is a commonly-used protocol for providing communications privacy and managing the security of message transmission, allowing the 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.

Yealink phones support TLS version 1.0, 1.1 and 1.2. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon appears on the LCD screen after the successful TLS negotiation.

Topics

[Supported Cipher Suites](#)

[Supported Trusted and Server Certificates](#)

[TLS Configuration](#)

Supported Cipher Suites

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.

Yealink 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

Supported Trusted and Server Certificates

The IP phone can serve as a TLS client or a TLS server. In TLS feature, we use the terms trusted and server certificate. These are also known as CA and device certificates.

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 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 76 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.
- **Server Certificate:** When clients request a TLS connection with the IP phone, the 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 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. The Security verification rules are compliant with RFC 2818.

Note

Resetting the IP phone to factory defaults will delete custom certificates by default. However, this feature is configurable by the parameter "static.phone_setting.reserve_certs_enable" using the configuration file.

Topic

Supported Trusted Certificates

Supported Trusted Certificates

Yealink phones trust the following CAs by default:

- DigiCert High Assurance EV Root CA
- Deutsche Telekom Root CA 2
- Equifax Secure Certificate Authority
- Equifax Secure eBusiness CA-1
- Equifax Secure Global eBusiness CA-1
- GeoTrust Global CA
- GeoTrust Global CA2
- GeoTrust Primary Certification Authority

-
- GeoTrust Primary Certification Authority G2
 - GeoTrust Universal CA
 - GeoTrust Universal CA2
 - Thawte Personal Freemail CA
 - Thawte Premium Server CA
 - Thawte Primary Root CA
 - Thawte Primary Root CA - G2
 - Thawte Primary Root CA - G3
 - Thawte Server CA
 - VeriSign Class 1 Public Primary Certification Authority
 - VeriSign Class 1 Public Primary Certification Authority - G2
 - VeriSign Class 1 Public Primary Certification Authority - G3
 - VeriSign Class 2 Public Primary Certification Authority - G2
 - VeriSign Class 2 Public Primary Certification Authority - G3
 - VeriSign Class 3 Public Primary Certification Authority
 - VeriSign Class 3 Public Primary Certification Authority - G2
 - VeriSign Class 3 Public Primary Certification Authority - G3
 - VeriSign Class 3 Public Primary Certification Authority - G4
 - VeriSign Class 3 Public Primary Certification Authority - G5
 - VeriSign Class 4 Public Primary Certification Authority - G2
 - VeriSign Class 4 Public Primary Certification Authority - G3
 - VeriSign Universal Root Certification Authority
 - ISRG Root X1 (Let's Encrypt Authority X1 and Let's Encrypt Authority X2 certificates are signed by the root certificate ISRG Root X1.)
 - Baltimore CyberTrust Root
 - DST Root CA X3
 - Verizon Public SureServer CA G14-SHA2
 - AddTrust External CA Root
 - Go Daddy Class 2 Certification Authority
 - Class 2 Primary CA
 - Cybertrust Public SureServer SV CA
 - DigiCert Assured ID Root G2
 - DigiCert Assured ID Root G3
 - DigiCert Assured ID Root CA
 - DigiCert Global Root G2
 - DigiCert Global Root G3
 - DigiCert Global Root CA
 - DigiCert Trusted Root G4
 - Entrust Root Certification Authority
 - Entrust Root Certification Authority - G2
 - Entrust.net Certification Authority (2048)
 - GeoTrust Primary Certification Authority - G3
 - GlobalSign Root CA

- GlobalSign Root CA - R2
- 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

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.

TLS Configuration

The following table lists the parameters you can use to configure TLS.

Parameter	account.X.sip_server.Y.transport_type ^{[1][2]}	<MAC>.cfg
Description	It configures the type of transport protocol.	
Permitted Values	0 -UDP 1 -TCP 2 -TLS 3 -DNS-NAPTR, if no server port is given, the phone performs the DNS NAPTR and SRV queries for the service type and port.	

Default	0	
Web UI	Account->Register->SIP Server Y->Transport	
Handset UI	For W53P/W60P: OK->Settings->Telephony->Server (default PIN: 0000) ->Server Y->Transport	
Parameter	static.security.default_ssl_method	<y0000000000xx>.cfg
Description	It configures the TLS version the phone uses to authenticate with the server.	
Permitted Values	0 -TLS 1.0 3 -SSL V23 (automatic negotiation with the server. The phone starts with TLS1.2 for negotiation.) 4 -TLS 1.1 5 -TLS 1.2	
Default	3	
Parameter	static.security.trust_certificates ^[3]	<y0000000000xx>.cfg
Description	It enables or disables the phone to only trust the server certificates in the Trusted Certificates list.	
Permitted Values	0 -Disabled 1 -Enabled, the phone will authenticate the server certificate based on the trusted certificates list. Only when the authentication succeeds, will the phone trust the server.	
Default	1	
Web UI	Security->Trusted Certificates->Only Accept Trusted Certificates	
Parameter	static.security.ca_cert ^[3]	<y0000000000xx>.cfg
Description	It configures the type of certificates in the Trusted Certificates list for the phone to authenticate for TLS connection.	
Permitted Values	0 -Default Certificates 1 -Custom Certificates 2 -All Certificates	
Default	2	
Web UI	Security->Trusted Certificates->CA Certificates	
Parameter	static.security.cn_validation ^[3]	<y0000000000xx>.cfg
Description	It enables or disables the phone to mandatorily validate the CommonName or SubjectAltName of the certificate sent by the server.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Security->Trusted Certificates->Common Name Validation	
Parameter	static.security.dev_cert ^[3]	<y0000000000xx>.cfg
Description	It configures the type of the device certificates for the phone to send for TLS authentication.	
Permitted Values	0 -Default Certificates	

	1 -Custom Certificates	
Default	0	
Web UI	Security->Server Certificates->Device Certificates	
Parameter	static.trusted_certificates.url	<y0000000000xx>.cfg
Description	It configures the access URL of the custom trusted certificate used to authenticate the connecting server. Note: The certificate you want to upload must be in *.pem, *.crt, *.cer or *.der format.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Security->Trusted Certificates->Load Trusted Certificates File	
Parameter	static.trusted_certificates.delete	<y0000000000xx>.cfg
Description	It deletes all uploaded trusted certificates.	
Permitted Values	http://localhost/all	
Default	Blank	
Parameter	static.server_certificates.url	<y0000000000xx>.cfg
Description	It configures the access URL of the certificate the phone sends for authentication. Note: The certificate you want to upload must be in *.pem or *.cer format.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Security->Server Certificates->Load Server Certificates File	
Parameter	static.server_certificates.delete	<y0000000000xx>.cfg
Description	It deletes all uploaded server certificates.	
Permitted Values	http://localhost/all	
Default	Blank	
Parameter	static.phone_setting.reserve_certs_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to reserve custom certificates after it is reset to factory defaults.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	

[1]X is the account ID. X=1-8.

[2]Y is the server ID. Y=1-2.

Secure Real-Time Transport Protocol (SRTP)

Secure Real-Time Transport Protocol (SRTP) encrypts the audio streams 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 use for the session is negotiated between the phones. This negotiation process is compliant with [RFC 4568](#).

When you place a call on the enabled SRTP phone, the phone sends an INVITE message with the RTP/RTCP encryption algorithm to the destination phone. As described in [RFC 3711](#), RTP/RTCP streams may be encrypted using an AES (Advanced Encryption Standard) algorithm.

Example of the RTP encryption algorithm carried in the SDP of the INVITE message:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80 >inline:NzFINTUwZDk2OGVIOTc3YzNkYTkwZWVhMTM1YWVj
a=crypto:2 AES_CM_128_HMAC_SHA1_32 >inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWVm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm, and then answers the call by responding with a 200 OK message which carries the negotiated RTP encryption algorithm.

Example of the RTP encryption algorithm carried in the SDP of the 200 OK message:

```
m=audio 11780 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0YzZj
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

When SRTP is enabled on both phones, RTP streams will be encrypted, and a lock icon appears on the LCD 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 \(TLS\)](#).

Topic

[SRTP Configuration](#)

SRTP Configuration

The following table lists the parameters you can use to configure the SRTP.

Parameter	account.X.srtp_encryption ^[1]	<MAC>.cfg
Description	It configures whether to use audio encryption service.	
Permitted Values	0 -Disabled 1 -Optional, the phone will negotiate with the other phone what type of encryption to use for the session. 2 -Compulsory, the phone must use SRTP during a call.	
Default	0	
Web UI	Account->Advanced->RTP Encryption(SRTP)	

^[1]X is the account ID. X=1-8.

Encrypting and Decrypting Files

Yealink phones support downloading encrypted files from the server and encrypting files before/when uploading them to the server.

You can encrypt the following files:

- **Configuration files:** MAC-Oriented CFG file (<MAC>.cfg), Common CFG file (y0000000000xx.cfg), MAC-local CFG file (<MAC>-local.cfg) or other custom CFG files (for example, sip.cfg, account.cfg)
- **Contact Files:** <MAC>-contact.xml

To encrypt/decrypt files, you may have to configure an AES key.

Note

aES keys must be 16 characters. The supported characters contain: 0 ~ 9, A ~ Z, a ~ z and special characters: # \$ % * + , - . : = ? @ [] ^ _ { } ~.

Topics

[Configuration Files Encryption Tools](#)

[Configuration Files Encryption and Decryption](#)

[Contact Files Encryption and Decryption](#)

[Encryption and Decryption Configuration](#)

[Example: Encrypting Configuration Files](#)

Configuration Files Encryption Tools

Yealink provides three configuration files encryption tools:

- Config_Encrypt_Tool.exe (via graphical tool for Windows platform)
- Config_Encrypt.exe (via DOS command line for Windows platform)

- yealinkencrypt (for Linux platform)

The encryption tools encrypt plaintext configuration files (for example, 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 generate encrypted configuration files with the same file name as before.

These tools also encrypt the plaintext 16-character symmetric keys using a fixed key, which is the same as the one built in the IP phone, and generate new files named as <xx_Security>.enc (xx is the name of the configuration file, for example, y000000000077_Security.enc for y000000000077.cfg file, account_Security.enc for account.cfg). These tools generate another new file named as Aeskey.txt to store the plaintext 16-character symmetric keys for each configuration file.

Configuration Files Encryption and Decryption

Encrypted configuration files can be downloaded from the provisioning server to protect against unauthorized access and tampering of sensitive information (for example, login passwords, registration information).

You can encrypt the configuration files using the encryption tools. 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 "static.auto_provision.encryption.config" to 1).

For security reasons, you should upload encrypted configuration files, <xx_Security>.enc files to the root directory of the provisioning server. During auto provisioning, the phone requests to download the boot file first and then download the referenced configuration files. For example, the phone downloads an encrypted account.cfg file. The phone will request to download <account_Security>.enc file (if enabled) and decrypt it into the plaintext key (for example, key2) using the built-in key (for example, key1). Then the IP phone decrypts account.cfg file using key2. After decryption, the phone resolves configuration files and updates configuration settings onto the IP phone system.

Contact Files Encryption and Decryption

Encrypted contact files can be used to protect against unauthorized access and tampering of private information (for example, contact number). It is helpful for protecting trade secrets.

You can configure the contact files to be automatically encrypted using 16-character symmetric keys (configured by "static.auto_provision.aes_key_16.mac") when uploading to the server (by setting "static.auto_provision.encryption.directory=1"). The encrypted contact files have the same file names as before. The encrypted contact files can be downloaded from the server and decrypted using 16-character symmetric keys during auto provisioning. If the parameter "static.auto_provision.aes_key_16.mac" is left blank, "static.auto_provision.aes_key_16.com" will be used.

If the downloaded contact files are encrypted, the phone will try to decrypt <MAC>-contact.xml file using the plaintext AES key. After decryption, the phone resolves contact files and updates contact information onto the IP phone system.

Encryption and Decryption Configuration

The following table lists the parameters you can use to configure the encryption and decryption.

Parameter	static.auto_provision.update_file_mode	<y0000000000xx>.cfg
Description	It enables or disables the phone only to download the encrypted files.	
Permitted Values	<p>0-Disabled, the phone will download the configuration files (for example, sip.cfg, account.cfg, <MAC>-local.cfg) 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 phone system.</p> <p>1-Enabled, the phone will only download the encrypted configuration files (for example, sip.cfg, account.cfg, <MAC>-local.cfg) from the server during auto provisioning, and then resolve these files and update settings onto the phone system.</p>	

Default	0	
Parameter	static.auto_provision.aes_key_in_file	<y0000000000xx>.cfg
Description	It enables or disables the phone to decrypt configuration files using the encrypted AES keys.	
Permitted Values	<p>0-Disabled, the phone will decrypt the encrypted configuration files using plaintext AES keys configured on the phone.</p> <p>1-Enabled, the phone will download <xx_Security>.enc files (for example, <sip_Security>.enc, <account_Security>.enc) during auto provisioning, and then decrypts these files into the plaintext keys (for example, key2, key3) respectively using the phone built-in key (for example, key1). The phone then decrypts the encrypted configuration files using the corresponding key (for example, key2, key3).</p>	
Default	0	
Parameter	static.auto_provision.aes_key_16.com	<y0000000000xx>.cfg
Description	<p>It configures the plaintext AES key for encrypting/decrypting the Common CFG/Custom CFG file.</p> <p>The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # \$ % * + , - . : = ? @ [] ^ _ { } ~.</p> <p>Example: static.auto_provision.aes_key_16.com = 0123456789abcdef</p> <p>Note: For decrypting, it works only if "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 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".</p>	
Permitted Values	16 characters	
Default	Blank	
Web UI	Settings->Auto Provision->Common AES Key	
Parameter	static.auto_provision.aes_key_16.mac	<y0000000000xx>.cfg
Description	<p>It configures the plaintext AES key for encrypting/decrypting the MAC-Oriented files (<MAC>.cfg, <MAC>-local.cfg and <MAC>-contact.xml).</p> <p>The valid characters contain: 0 ~ 9, A ~ Z, a ~ z and the following special characters are also supported: # \$ % * + , - . : = ? @ [] ^ _ { } ~.</p> <p>Example: static.auto_provision.aes_key_16.mac = 0123456789abmins</p> <p>Note: For decrypting, it works only if "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 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".</p>	
Permitted Values	16 characters	
Default	Blank	
Web UI	Settings->Auto Provision->MAC-Oriented AES Key	
Parameter	static.autoprovision.X.com_aes ^{[1][2]}	<y0000000000xx>.cfg

Description	It configures the plaintext AES key for decrypting the Common CFG file. If it is configured, it has a higher priority than the value configured by the parameter "static.auto_provision.aes_key_16.com".	
Permitted Values	16 characters	
Default	Blank	
Parameter	static.autoprovision.X.mac_aes ^{[1][2]}	<y0000000000xx>.cfg
Description	It configures the plaintext AES key for decrypting the MAC-Oriented CFG file. If it is configured, it has a higher priority than the value configured by the parameter "static.auto_provision.aes_key_16.mac".	
Permitted Values	16 characters	
Default	Blank	
Parameter	static.auto_provision.encryption.config	<y0000000000xx>.cfg
Description	It enables or disables the phone to encrypt <MAC>-local.cfg file using the plaintext AES key.	
Permitted Values	0-Disabled, the MAC-local CFG file will be uploaded unencrypted and will replace 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". 1-Enabled, the MAC-local CFG file will be uploaded encrypted and will replace 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".	
Default	0	

^[1]X is an activation code ID. X=1-50.

^[2]If you change this parameter, the phone will reboot to make the change take effect.

Example: Encrypting Configuration Files

The following example describes how to use "Config_Encrypt_Tool.exe" to encrypt the account.cfg file. For more information on the other two encryption tools, refer to [Yealink Configuration Encryption Tool User Guide](#).

The way the IP phone processes other configuration files is the same as that of the account.cfg file.

Procedure:

1. Double click "Config_Encrypt_Tool.exe" to start the application tool.

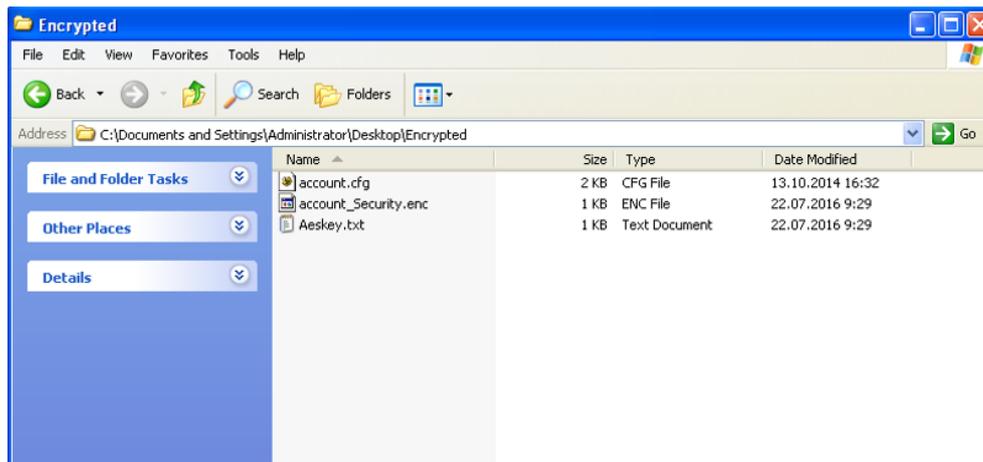
The screenshot of the main page is shown as below:



2. When you start the application tool, a file folder named "Encrypted" is created automatically in the directory where the application tool is located.
3. Click **Browse** to locate configuration file(s) (for example, account.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 other files.
4. (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.
5. (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.
6. Click **Encrypt** to encrypt the configuration file(s).



7. 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).



Incoming Network Signaling Validation

Yealink phones support the following three optional levels of security for validating incoming network signaling:

- **Source IP address validation:** ensure the request is received from an IP address of a server belonging to the set of target SIP servers.
- **Digest authentication:** challenge requests with digest authentication using the local credentials for the associated registered account.
- **Source IP address validation and digest authentication:** apply both of the above methods.

Topic

[Incoming Network Signaling Validation Configuration](#)

Incoming Network Signaling Validation Configuration

The following table lists the parameters you can use to configure the incoming network signaling validation.

Parameter	sip.request_validation.source.list	<y0000000000xx>.cfg
Description	It configures the name of the request method for which source IP address validation will be applied.	
Example:	sip.request_validation.source.list = INVITE, NOTIYF	
Permitted Values	INVITE, ACK, BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE	
Default	Blank	
Parameter	sip.request_validation.digest.list	<y0000000000xx>.cfg
Description	It configures the name of the request method for which digest authentication will be applied.	
Example:	sip.request_validation.digest.list = INVITE, SUBSCRIBE	
Permitted Values	INVITE, ACK, BYE, REGISTER, CANCEL, OPTIONS, INFO, MESSAGE, SUBSCRIBE, NOTIFY, REFER, PRACK, UPDATE	
Default	Blank	

Parameter	sip.request_validation.digest.realm	<y0000000000xx>.cfg
Description	It configures the string used for authentication parameter Realm when performing the digest authentication.	
Permitted Values	A valid string	
Default	YealinkSPIP	
Parameter	sip.request_validation.event	<y0000000000xx>.cfg
Description	It configures which events specified within the Event header of SUBSCRIBE or NOTIFY request should be validated. If it is left blank, all events will be validated.	
Permitted Values	A valid string	
Default	Blank	

Advanced Features

The advanced features require server support. Consult your server partner to find out if these features are supported.

Topics

[Call Park and Retrieve](#)
[Shared Line](#)
[Intercom](#)
[Voice Mail](#)

Call Park and Retrieve

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).

The phones support call park feature under the following modes:

- **FAC mode:** parks the call to the local extension or a desired extension through dialing the park code.
- **Transfer mode:** parks the call to the shared parking lot through performing a blind transfer. 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.

Topic

[Call Park and Retrieve Configuration](#)

Call Park and Retrieve Configuration

The following table lists the parameters you can use to configure call park and retrieve.

Parameter	features.call_park.park_mode	<y0000000000xx>.cfg
Description	It configures the call park mode.	
Permitted Values	1 -FAC, park a call through dialing the call park code. 2 -Transfer, blind transfer the call to a shared parking lot.	
Default	2	
Web UI	Features->Call Pickup->Call Park Mode	
Parameter	features.call_park.enable	<y0000000000xx>.cfg
Description	It enables or disables the call park feature.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Features->Call Pickup->Call Park	
Parameter	features.call_park.park_code	<y0000000000xx>.cfg
Description	It configures the call park code for FAC call park mode, or configures shared parking lot for Transfer call park mode.	

Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Call Pickup->Call Park Code	
Parameter	features.call_park.park_retrieve_code	<y0000000000xx>.cfg
Description	It configures the park retrieve code for FAC call park mode, or configures retrieve parking lot for Transfer call park mode.	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Call Pickup->Park Retrieve Code	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Shared Line

Yealink phones support Shared Call Appearance (SCA) to share a line. Shared call appearances enable more than one phone to share the same line or registration. The methods you use vary with the SIP server you are using.

The shared line users have the ability to do the following:

- Place and answer calls
- Place a call on hold
- Retrieve a held call remotely (not applicable to CP930W-Base phones)
- Barge in an active call (not applicable to CP930W-Base phones)
- Pull a shared call (not applicable to CP930W-Base phones)

Topic

[Shared Call Appearance \(SCA\) Configuration](#)

Shared Call Appearance (SCA) Configuration

In SCA scenario, an incoming call can be presented to multiple phones simultaneously. Any IP phone can be used to originate or receive calls on the shared line.

Yealink 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 phone to ask to seize the line.

Topic

[SCA Configuration](#)

SCA Configuration

The following table lists the parameters you can use to configure SCA.

Parameter	account.X.shared_line ^[1]	<MAC>.cfg
Description	It configures the registration line type.	

Permitted Values	0-Disabled 1-Shared Call Appearance	
Default	0	
Web UI	Account->Advanced->Shared Line	
Parameter	account.X.line_seize.expires ^[1]	<MAC>.cfg
Description	It configures the line-seize subscription expiration time (in seconds). Note: It works only if "account.X.shared_line" is set to 1 (Shared Call Appearance).	
Permitted Values	Integer from 0 to 65535	
Default	15	
Parameter	features.barge_in_via_username.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to use user name of the account to barge in an active call. Note: It is not applicable to CP930W-Base phones.	
Permitted Values	0-Disabled, user register name to barge in, the phone sends INVITE request with the register name when barging in a call 1-Enabled, the phone sends INVITE request with the user name when barging in a call	
Default	0	

[1]X is the account ID. X=1-8.

Intercom

Intercom is a useful feature in an office environment to quickly connect with the operator or the secretary. You can make internal intercom calls and external intercom calls on the phone. Internal intercom calls are made between handsets registered to the same base station. External intercom calls can be made by dialing the feature access code followed by the number. External intercom calls depend on support from a SIP server.

The handset can automatically answer an incoming external intercom call and play warning tone only when there is only one handset subscribed and no call in progress on the handset.

To automatically answer an incoming internal intercom call, you need to enable auto intercom feature on the handset. The following configuration types of auto intercom feature are available:

- **On (Beep On):** Auto intercom feature is on. The handset will answer an incoming internal intercom call automatically and play a warning tone.
- **On (Beep Off):** Auto intercom feature is on. The handset will answer an incoming internal intercom call automatically without a warning tone.
- **Off:** Auto intercom feature is off. You need to answer an incoming internal intercom call manually.

The CP930W-Base phones can not automatically answer either the external or internal intercom call, you can only answer it manually.

Topic

[Intercom Configuration](#)

Intercom Configuration

The following table lists the parameters you can use to configure intercom.

Parameter	features.intercom.headset_prior.enable	<y0000000000xx>.cfg
Description	It configures the channel mode when an incoming intercom call is answered through the handset. The handset should be connected in advance. Note: It is not applicable to CP930W-Base phones.	
Permitted Values	0-Speaker Mode 1-Headset Mode	
Default	1	
Parameter	custom.handset.auto_intercom	<y0000000000xx>.cfg
Description	It configures whether the DECT IP phone automatically answers an incoming internal intercom call and plays a warning tone. Note: It works only if "static.auto_provision.handset_configured.enable" is set to 1 (Enabled). It is not applicable to DD phones and CP930W-Base phones.	
Permitted Values	0-Off, users need to answer incoming internal intercom calls manually. 1-On(Beep Off), the handset will answer an incoming internal intercom call automatically without a warning tone. 2-On(Beep On), the handset will answer an incoming internal intercom call automatically and play a warning tone. It works when the silent mode is off (silent mode is not applicable to CP930W-Base phones).	
Default	0	
Handset UI	W53P/W60P: OK->Settings->Telephony->Auto Intercom	

Voice Mail

Yealink phones support voice mail.

You can configure a message waiting indicator (MWI) to inform users that how many messages are waiting in their mailbox without calling the mailbox. Yealink phones support both audio and visual MWI alert when receiving new voice messages.

Topic

[MWI for Voice Mail Configuration](#)

MWI for Voice Mail Configuration

Yealink phones support both solicited and unsolicited MWI.

Unsolicited MWI: 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. Unsolicited MWI is a server related feature.

Solicited MWI: The IP phone can subscribe the MWI messages to the account or the voice mail number. For solicited MWI, you must enable MWI subscription feature on the phones.

The following table lists the parameters you can use to configure MWI for voice mail.

Parameter	account.X.subscribe_mwi ^[1]	<MAC>.cfg
Description	It enables or disables the phone to subscribe the message waiting indicator.	
Permitted	0-Disabled, the server automatically sends a message-summary NOTIFY in a new dialog each time the	

Values	MWI status changes. (This requires server support). 1 -Enabled, the phone will send a SUBSCRIBE message to the server for message-summary updates.	
Default	0	
Web UI	Account->Advanced->Subscribe for MWI	
Parameter	account.X.subscribe_mwi_expires ^[1]	<MAC>.cfg
Description	It configures MWI subscribe expiry time (in seconds). Note: It works only if "account.X.subscribe_mwi" is set to 1 (Enabled).	
Permitted Values	Integer from 0 to 84600	
Default	3600	
Web UI	Account->Advanced->MWI Subscription Period (Seconds)	
Parameter	account.X.sub_fail_retry_interval ^[1]	<MAC>.cfg
Description	It configures the interval (in seconds) for the phone to retry to re-subscribe when subscription fails.	
Permitted Values	Integer from 0 to 3600	
Default	30	
Parameter	account.X.subscribe_mwi_to_vm ^[1]	<MAC>.cfg
Description	It enables or disables the phone to subscribe the message waiting indicator to the voice mail number. Note: It works only if "account.X.subscribe_mwi" is set to 1 (Enabled) and "voice_mail.number.X" is configured.	
Permitted Values	0 -Disabled, the phone will subscribe the message waiting indicator to a specific account. 1 -Enabled	
Default	0	
Web UI	Account->Advanced->Subscribe MWI To Voice Mail	
Parameter	voice_mail.number.X ^[1]	<MAC>.cfg
Description	It configures the voice mail number.	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Account->Advanced->Voice Mail	
Handset UI	W53P/W60P: OK->Voice Mail->Set Voice Mail->LineX->Number DD Phone: Menu->Message->Voice Mail->Set Voice Mail->AccountX Code CP930W-Base: Menu->Message->Set Voice Mail Code->Number	
Parameter	account.X.display_mwi.enable ^[1]	<MAC>.cfg

Description	It enables or disables the MWI alert to indicate that you have an unread voice mail message.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	
Web UI	Account->Advanced->Voice Mail Display	
Parameter	features.voice_mail_alert.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to pop up the message when receiving the same amount of new voice-mails.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	

[1]X is the account ID. X=1-8.

General Features

This section shows you how to configure general features on Yealink phones.

Topics

[Line Identification Presentation](#)
[Return Code for Refused Call](#)
[Accept SIP Trust Server Only](#)
[100 Reliable Retransmission](#)
[SIP Session Timer](#)
[Session Timer](#)
[Reboot in Talking](#)
[Reserve # in User Name](#)
[Busy Tone Delay](#)

Line Identification Presentation

Yealink phones can derive calling and connected line identification from SIP headers and display the name associated with the telephone number on the LCD screen.

Calling Line Identification Presentation (CLIP): It allows the phones to display the caller identity, derived from a SIP header contained in the INVITE message when receiving an incoming call. Yealink phones can derive 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.

Connected Line Identification Presentation (COLP): It allows the phones to display the identity of the connected party specified for outgoing calls. The phones can display the Dialed Digits, or the identity in a SIP header (Remote-Party-ID, P-Asserted-Identity or contact) 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 caller/callee already exists in the local directory, the local contact name assigned to the caller will be preferentially displayed and stored in the call log.

For more information on calling line identification presentation, refer to [Calling and Connected Line Identification Presentation on Yealink IP Phones](#).

Topic

[CLIP and COLP Configuration](#)

CLIP and COLP Configuration

The following table lists the parameters you can use to configure the CLIP and COLP.

Parameter	account.X.cid_source ^[1]	<MAC>.cfg
Description	It configures the identity of the caller.	
Permitted Values	0 -FROM 1 -PAI	

	<p>2-PAI-FROM</p> <p>3-PRID-PAI-FROM</p> <p>4-PAI-RPID-FROM</p> <p>5-RPID-FROM</p> <p>6-PREFERENCE, the phone uses the custom priority order for the sources of caller identity (configured by the parameter "sip.cid_source.preference").</p>	
Default	0	
Web UI	Account->Advanced->Caller ID Source	
Parameter	account.X.cid_source_privacy ^[1]	<MAC>.cfg
Description	<p>It enables or disables the phone to process the Privacy header field in the SIP message.</p> <p>Note: The priority order: PPI>Privacy>PRID/PAI/From.</p>	
Permitted Values	<p>0-Disabled, the phone does not process Privacy header.</p> <p>1-Enabled, the phone screen presents anonymity instead if there is a Privacy: id in the INVITE request.</p>	
Default	1	
Parameter	account.X.cid_source_ppi ^[1]	<MAC>.cfg
Description	<p>It enables or disables the phone to process the P-Preferred-Identity (PPI) header in the request message for caller identity presentation.</p>	
Permitted Values	<p>0-Disabled, the phone does not process the PPI header.</p> <p>1-Enabled, the phone presents the caller identity from the PPI header.</p>	
Default	0	
Parameter	sip.cid_source.preference	<y0000000000xx>.cfg
Description	<p>It configures the priority order for the sources of caller identity information.</p> <p>Note: Yealink phones can derive caller identity from the following SIP headers: From, P-Asserted-Identity (PAI), P-Preferred-Identity and Remote-Party-ID (RPID). It works only if "account.X.cid_source" is set to 6 (PREFERENCE).</p>	
Permitted Values	String	
Default	P-Preferred-Identity, P-Asserted-Identity, Remote-Party-ID, From	
Parameter	account.X.cp_source ^[1]	<MAC>.cfg
Description	<p>It configures the identity of the callee according to the response message.</p>	
Permitted Values	<p>0-PAI-RPID</p> <p>1-Dialed Digits</p> <p>2-RFC4916, 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 server, and displays the identity in the "From" header.</p> <p>3-Contact</p>	
Default	0	

^[1]X is the account ID. X=1-8.

Return Code for Refused Call

You can define the return code and reason of the SIP response message for the refused call. The caller's phone LCD screen displays the reason according to the received return code. Available return codes and reasons are:

- 404 (Not Found)
- 480 (Temporarily Unavailable)
- 486 (Busy Here)
- 603 (Decline)

Topic

[Return Code for Refused Call Configuration](#)

Return Code for Refused Call Configuration

The following table lists the parameters you can use to configure the return code for the refused call.

Parameter	features.normal_refuse_code	<y0000000000xx>.cfg
Description	It configures a return code and reason of SIP response messages when the phone rejects an incoming call. A specific reason is displayed on the caller's phone screen.	
Permitted Values	404 -Not Found 480 -Temporarily Unavailable 486 -Busy Here 603 -Decline	
Default	486	
Web UI	Features->General Information->Return Code When Refuse	

Accept SIP Trust Server Only

Accept SIP trust server only enables the 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, and so on. If you enable this feature, the phone cannot accept an IP address call.

Topic

[Accept SIP Trust Server Only Configuration](#)

Accept SIP Trust Server Only Configuration

The following table lists the parameters you can use to configure accept SIP trust server only.

Parameter	sip.trust_ctrl	<y0000000000xx>.cfg
Description	It enables or disables the phone to only accept the SIP message from the SIP and outbound proxy server.	
Permitted Values	0 -Disabled 1 -Enabled, users cannot accept the IP call	
Default	0	
Web UI	Features->General Information->Accept SIP Trust Server Only	

100 Reliable Retransmission

As described in [RFC 3262](#), 100rel tag is for the reliability of provisional responses. When presenting in a Supported header, it indicates that the phone can send or receive reliable provisional responses. When presenting 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.test.com:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.6.197:5060;branch=z9hG4bK1708689023
From: "1025" <sip:1025@pbx.test.com:5060>;tag=1622206783
To: <sip:1024@pbx.test.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.test.com", nonce="BroadWorksXi5stub71Ts2nb05BW", uri="sip:1024@pbx.test.com:5060", response="f7e9d35c55af45b3f89beae95e913171", algorithm=MD5, cnonce="0a4f113b", qop=auth, nc=00000001
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH, UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W60B 77.81.0.10
Supported: 100rel
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 302
```

Topic

[100 Reliable Retransmission Configuration](#)

100 Reliable Retransmission Configuration

The following table lists the parameter you can use to configure the 100 reliable retransmission.

Parameter	account.X.100rel_enable ^[1]	<MAC>.cfg
Description	It enables or disables the 100 reliable retransmission feature.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Web UI	Account->Advanced->Retransmission	

^[1]X is the account ID. X=1-8.

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 the 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 and 4s.

Timer T4

Timer T4 represents that the network will take to clear messages between the SIP client and server.

Topic

[SIP Session Timer Configuration](#)

SIP Session Timer Configuration

The following table lists the parameters you can use to configure the SIP session timer.

Parameter	sip.timer_t1	<y0000000000xx>.cfg
Description	It configures the SIP session timer T1 (in seconds).	
Permitted Values	Float from 0.5 to 10	
Default	0.5	
Web UI	Settings->SIP->SIP Session Timer T1 (0.5~10s)	
Parameter	sip.timer_t2	<y0000000000xx>.cfg
Description	It configures the SIP session timer T2 (in seconds).	
Permitted Values	Float from 2 to 40	
Default	4	
Web UI	Settings->SIP->SIP Session Timer T2 (2~40s)	
Parameter	sip.timer_t4	<y0000000000xx>.cfg
Description	It configures the SIP session timer T4 (in seconds).	
Permitted	Float from 2.5 to 60	

Values	
Default	5
Web UI	Settings->SIP->SIP Session Timer T4 (2.5~60s)

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](#). The 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 W60B 77.81.0.10
Session-Expires: 90;refresher=uac
Supported: timer
Content-Length: 0
```

Topic

[Session Timer Configuration](#)

Session Timer Configuration

The following table lists the parameters you can use to configure session timer.

Parameter	account.X.session_timer.enable ^[1]	<MAC>.cfg
Description	It enables or disables the session timer.	
Permitted Values	0 -Disabled 1 -Enabled, the phone will send periodic UPDATE requests to refresh the session during a call.	
Default	0	

Web UI	Account->Advanced->Session Timer	
Parameter	account.X.session_timer.expires ^[1]	<MAC>.cfg
Description	<p>It configures the interval (in seconds) for refreshing the SIP session during a call.</p> <p>An UPDATE will be sent after 50% of its value has elapsed. For example, if it is set to 1800 (1800s), the phone will refresh the session during a call every 900 seconds.</p> <p>Note: It works only if "account.X.session_timer.enable" is set to 1 (Enabled).</p>	
Permitted Values	Integer from 90 to 7200	
Default	1800	
Web UI	Account->Advanced->Session Expires(90~7200s)	
Parameter	account.X.session_timer.refresher ^[1]	<MAC>.cfg
Description	<p>It configures who refresh the SIP session during a call.</p> <p>Note: It works only if "account.X.session_timer.enable" is set to 1 (Enabled).</p>	
Permitted Values	<p>0-UAC</p> <p>1-UAS</p>	
Default	0	
Web UI	Account->Advanced->Session Refresher	

^[1]X is the account ID. X=1-8.

Reboot in Talking

Reboot in talking feature allows the phones to reboot during an active call when it receives a reboot Notify message.

Topic

[Reboot in Talking Configuration](#)

Reboot in Talking Configuration

The following table lists the parameter you can use to configure reboot in talking.

Parameter	features.reboot_in_talk_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to reboot during a call when it receives a reboot Notify message.	
Permitted Values	<p>0-Disabled</p> <p>1-Enabled</p>	
Default	0	
Web UI	Features->General Information->Reboot in Talking	

Reserve # in User Name

Reserve # in User Name feature allows the 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 the SIP server.

Example of a SIP REGISTER message:

```
INVITE sip:2@10.2.1.48:5060 SIP/2.0
Via: SIP/2.0/UDP 10.3.20.6:5060;branch=z9hG4bK1867789050
From: "1010" <sip:1010%23@10.2.1.48:5060>;tag=1945988802
To: <sip:2@10.2.1.48:5060>
Call-ID: 0_2336101648@10.3.20.6
CSeq: 1 INVITE

Contact: <sip:1010%23@10.3.20.6:5060>
Content-Type: application/sdp
Allow: INVITE, INFO, PRACK, ACK, BYE, CANCEL, OPTIONS, NOTIFY, REGISTER, SUBSCRIBE, REFER, PUBLISH, UPDATE, MESSAGE
Max-Forwards: 70
User-Agent: Yealink W60B 77.81.0.10
Allow-Events: talk,hold,conference,refer,check-sync
Content-Length: 300
```

Topic

[Reserve # in User Name Configuration](#)

Reserve # in User Name Configuration

The following table lists the parameter you can use to configure reserve # in user name.

Parameter	sip.use_23_as_pound	<y0000000000xx>.cfg
Description	It enables or disables the phone to reserve the pound sign (#) in the user name.	
Permitted Values	0 -Disabled (convert the pound sign into "%23") 1 -Enabled	
Default	1	
Web UI	Features->General Information->Reserve # in User Name	

Busy Tone Delay

The busy tone is audible to indicate that the call is released by the other party. You can define the amount of time to play the busy tone.

Topic

[Busy Tone Delay Configuration](#)

Busy Tone Delay Configuration

The following table lists the parameter you can use to configure busy tone delay.

Parameter	features.busy_tone_delay	<y0000000000xx>.cfg
Description	It configures the duration time (in seconds) to play the busy tone when the call is released by the remote party.	
Permitted Values	0 -the phone will not play a busy tone. 3 -3s, a busy tone is audible for 3 seconds on the phone. 5 -5s, a busy tone is audible for 5 seconds on the phone	
Default	0	
Web UI	Features->General Information->Busy Tone Delay (Seconds)	

Configuration Parameters

This section provides a description and permitted values of some settings.

Topics

[BroadSoft Parameters](#)

[Ethernet Interface MTU Parameter](#)

[SIP Settings Parameters](#)

[Call Settings Parameters](#)

[APP Settings Configuration](#)

BroadSoft Parameters

This section shows the parameters you can use to configure the phone with BroadSoft server.

For more information on BSFT, refer to [Yealink_IP_Phone_Features_Integrated_with_BroadSoft_UC-One_User_Guide](#) or [Yealink_IP_Phones_Deployment_Guide_for_BroadSoft_UC-One_Environment](#).

BroadSoft Settings

Parameter	bw.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the BroadSoft features for phones.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Broadsoft XSI

Parameter	account.X.xsi.user ^[1]	<MAC>.cfg
Description	It configures the user name for XSI authentication. Note: It works only if "bw.xsi.enable" is set to 1 (Enabled).	
Permitted Values	String within 99 characters	
Default	Blank	
Web UI	Applications->Broadsoft XSI->XSI Account->User ID	
Parameter	account.X.xsi.password ^[1]	<MAC>.cfg
Description	It configures the password for XSI authentication. Note: It works only if "sip.authentication_for_xsi" is set to 0 (User Login Credentials for XSI Authentication) and "bw.xsi.enable" is set to 1 (Enabled).	
Permitted Values	String within 99 characters	
Default	Blank	

Web UI	Applications->Broadsoft XSI->XSI Account->Password	
Parameter	account.X.xsi.host ^[1]	<MAC>.cfg
Description	It configures the IP address or domain name of the Xtended Services Platform server. Note: It works only if "bw.xsi.enable" is set to 1 (Enabled).	
Permitted Values	IP address or domain name	
Default	Blank	
Web UI	Applications->Broadsoft XSI->XSI Account->Host Server	
Parameter	account.X.xsi.server_type ^[1]	<MAC>.cfg
Description	It configures the access protocol of the Xtended Services Platform server. Note: It works only if "bw.xsi.enable" is set to 1 (Enabled).	
Permitted Values	HTTP or HTTPS	
Default	HTTP	
Web UI	Applications->Broadsoft XSI->XSI Account->XSI Server Type	
Parameter	account.X.xsi.port ^[1]	<MAC>.cfg
Description	It configures the port of the Xtended Services Platform server. Note: It works only if "bw.xsi.enable" is set to 1 (Enabled).	
Permitted Values	Integer from 1 to 65535	
Default	80	
Web UI	Applications->Broadsoft XSI->XSI Account->Port	
Parameter	bw.xsi.enable ^[2]	<y0000000000xx>.cfg
Description	It enables or disables the XSI authentication feature for the phone.	
Permitted Values	<p>0-Disabled 1-Enabled</p> <p>If it is set to 0 (Disabled), the following features are unavailable on the phone:</p> <ul style="list-style-type: none"> BroadWorks Anywhere Remote Office Line ID Blocking Anonymous Call Rejection Simultaneous Ring Personal BroadSoft Directory BroadSoft Call Log Call Park Feature via XSI Mode Call Waiting Feature via XSI Mode 	

	Voice Messaging/Video Voice Messaging Silent Alerting	
Default	0	
Parameter	sip.authentication_for_xsi	<y0000000000xx>.cfg
Description	It configures the authentication mechanism for the XSI access. Note: It works only if "bw.xsi.enable" is set to 1 (Enabled).	
Permitted Values	0 -User Login Credentials for XSI Authentication, the phone uses the XSI user ID and password for XSI authentication. 1 -SIP Credentials for XSI Authentication, the phone uses the XSI user ID, the register name and password of the SIP account for XSI authentication.	
Default	0	
Web UI	Applications->Broadsoft XSI->XSI Account->Allow SIP Authentication for XSI	

[1]X is the account ID. X=1-8.

[2]If you change this parameter, the phone will reboot to make the change take effect.

Broadsoft Network Directory

Parameter	bw.xsi.directory.enable	<y0000000000xx>.cfg
Description	It enables or disables the network directory feature for the IP phone. Note: It works only if "bw.xsi.enable" is set to 1 (Enabled).	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Parameter	bw_phonebook.group_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to display the group directory. 0 -Disabled 1 -Enabled Note: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled).	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	
Web UI	Applications->Broadsoft XSI->Network Directory->Group	
Parameter	bw_phonebook.personal_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to display the personal directory. Note: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled).	
Permitted Values	0 -Disabled 1 -Enabled	
Default	1	

Web UI	Applications->Broadsoft XSI->Network Directory->Personal	
Parameter	bw_phonebook.group_common_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to display the group common directory. Note: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Applications->Broadsoft XSI->Network Directory->Group Common	
Parameter	bw_phonebook.enterprise_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to display the enterprise directory. Note: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Applications->Broadsoft XSI->Network Directory->Enterprise	
Parameter	bw_phonebook.enterprise_common_enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to display the enterprise common directory. Note: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled	
Default	1	
Web UI	Applications->Broadsoft XSI->Network Directory->Enterprise Common	
Parameter	bw_phonebook.enterprise_common_displayname	<y0000000000xx>.cfg
Description	It configures the display name on the phone screen for the enterprise common directory. Note: It works only if "bw.xsi.directory.enable" and "bw_phonebook.enterprise_common_enable" are set to 1 (Enabled).	
Permitted Values	String within 99 characters	
Default	EnterpriseCommon	
Web UI	Applications->Broadsoft XSI->Network Directory->Enterprise Common	
Parameter	bw_phonebook.custom	<y0000000000xx>.cfg
Description	It enables or disables the custom directory feature. Note: It works only if "bw.xsi.directory.enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Applications->Broadsoft XSI->Network Directory->Enable Custom Directories	
Parameter	bw_phonebook.group_displayname	<y0000000000xx>.cfg

Description	It configures the display name on the phone screen for the group directory. Note: It works only if "bw.xsi.directory.enable" and "bw_phonebook.group_enable" are set to 1 (Enabled).	
Permitted Values	String within 99 characters	
Default	Group	
Web UI	Applications->Broadsoft XSI->Network Directory->Group	
Parameter	bw_phonebook.enterprise_displayname	<y0000000000xx>.cfg
Description	It configures the display name on the phone screen for the enterprise directory. Note: It works only if "bw.xsi.directory.enable" and "bw_phonebook.enterprise_enable" are set to 1 (Enabled).	
Permitted Values	String within 99 characters	
Default	Enterprise	
Web UI	Applications->Broadsoft XSI->Network Directory->Enterprise	
Parameter	bw_phonebook.personal_displayname	<y0000000000xx>.cfg
Description	It configures the display name on the phone screen for the personal directory. Note: It works only if "bw.xsi.directory.enable" and "bw_phonebook.personal_enable" are set to 1 (Enabled).	
Permitted Values	String within 99 characters	
Default	Personal	
Web UI	Applications->Broadsoft XSI->Network Directory->Personal	
Parameter	bw.xsi.call_log.enable	<y0000000000xx>.cfg
Description	It enables or disables the BroadSoft call log feature. Note: It works only if "bw.xsi.enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Applications->Broadsoft XSI->Network Directory->Call Log->Network Call Log (if bw.enable =1)	
Parameter	bw.xsi.call_log.multiple_accounts.enable	<y0000000000xx>.cfg
Description	It enables or disables the user to view BroadSoft Call Log for multiple accounts. Note: It works only if "bw.xsi.call_log.enable" is set to 1 (Enabled). It is not applicable to CP930W-Base phones.	
Permitted Values	0-Disabled, you will directly access the BroadSoft Call Log for the first account by default, and you can only view the BroadSoft call log entry for the first account 1-Enabled, you are allowed to select a specific account to access the BroadSoft Call Log and view the call log entry	
Default	0	
Parameter	directory.update_time_interval	<y0000000000xx>.cfg

Description	It configures the interval (in minutes) for the phone to update the data of the BroadSoft directory from the BroadSoft server.	
Permitted Values	Integer from 60 to 34560	
Default	60	
Parameter	bw_phonebook.group_common_displayname	<y0000000000xx>.cfg
Description	It configures the display name on the phone screen for the group common directory. Note: It works only if "bw.xsi.directory.enable" and "bw_phonebook.group_common_enable" are set to 1 (Enabled).	
Permitted Values	String within 99 characters	
Default	GroupCommon	
Web UI	Applications->Broadsoft XSI->Network Directory->Group Common	
Parameter	search_in_dialing.bw_directory.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to automatically search entries from the BroadSoft directory, and display the results on the pre-dialing/dialing screen.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	
Parameter	search_in_dialing.bw_directory.priority	<y0000000000xx>.cfg
Description	It configures the search priority of the BroadSoft directory.	
Permitted Values	Integer greater than or equal to 0	
Default	5	

Broadsoft Call Park

Parameter	features.call_park.park_mode	<y0000000000xx>.cfg
Description	It configures the call park mode.	
Permitted Values	0 -XSI 1 -FAC, park a call through dialing the call park code.	
Default	0	
Web UI	Features->Call Pickup->Call Park Mode	
Parameter	features.call_park.group_enable	<y0000000000xx>.cfg
Description	It enables or disables the group call park feature.	
Permitted Values	0 -Disabled 1 -Enabled, users can select GPark during a call to park a call to the first available user in the call park group.	
Default	0	

Web UI	Features->Call Pickup->Group Call Park	
Parameter	features.call_park.park_ring	<y000000000xx>.cfg
Description	It enables or disables the phone to play a warning tone when a call is parked against its line. Note: It works only if "features.call_park.park_visual_notify_enable" is set to 1 (Enabled).	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Features->Call Pickup->Audio Alert for Parked Call	
Parameter	features.call_park.park_visual_notify_enable	<y000000000xx>.cfg
Description	It enables or disables the phone to display a parked indicator when a call is parked against its line.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Features->Call Pickup->Visual Alert for Parked Call	
Parameter	features.call_park.group_park_code	<y000000000xx>.cfg
Description	It configures the group call park code. Note: It works only if "features.call_park.park_mode" is set to 1 (FAC).	
Permitted Values	String within 32 characters	
Default	Blank	
Web UI	Features->Call Pickup->Group Call Park Code	
Parameter	account.X.callpark_enable ^[1]	<MAC>.cfg
Description	It enables or disables Broadsoft call park feature.	
Permitted Values	0-Disabled 1-Enabled , the phone sends the subscription package to the server with the header "Event:x-broad-works-callpark"	
Default	1	

[1]X is the account ID. X=1-8.

BroadSoft Call Waiting Sync

Parameter	call_waiting.mode	<y000000000xx>.cfg
Description	It configures the call waiting mode. Note: If it is set to 1 (XSI), it works only if "bw.xsi.enable" is set to 1 (Enabled).	
Permitted Values	0-Local 1-XSI, the status of the call waiting feature between the IP phone and the BroadWorks server can be synchronized.	
Default	0	

BroadSoft DND and Forward Sync

The BroadSoft synchronization feature provides the capability to synchronize the status of the DND and forward features between the IP phone and the server.

If the DND (or forward) is activated, the DND (or forward) status changing locally will be synchronized to all registered accounts on the server; but if the DND (or forward) status of a specific account is changed on the server, the DND (or forward) status locally will be changed.

Parameter	features.feature_key_sync.enable	<y0000000000xx>.cfg
Description	It enables or disables to synchronize the feature status between the phone and the server.	
Permitted Values	0 -Disabled 1 -Enabled, the phone sends a SUBSCRIBE message with event "as-feature-event".	
Default	0	

Ethernet Interface MTU Parameter

Parameter	static.network.mtu_value ^[1]	<y0000000000xx>.cfg
Description	It configures the MTU (Maximum Transmission Unit) of network interface card.	
Permitted Values	Integer from 1280 to 1500	
Default	1500	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

SIP Settings Parameters

Parameter	account.X.custom_ua ^[1]	<MAC>.cfg
Description	It configures the suffix of User-Agent in SIP request messages from the phone.	
Permitted Values	String within 128 characters	
Default	Blank	
Parameter	account.X.check_cseq.enable ^[1]	<MAC>.cfg
Description	It enables or disables the phone to check if the CSeq sequence number in the request is lower than that in the previous request on the same dialog.	
Permitted Values	0 -Disabled 1 -Enabled. If the CSeq sequence number in the request is lower than that in the previous request, the phone will reject the request.	
Default	1	
Parameter	account.X.check_to_tag.enable ^[1]	<MAC>.cfg
Description	It enables or disables the phone to check if the To-tag is carried in the To header in renewal request.	
Permitted Values	0 -Disabled 1 -Enabled. If the To-tag does not exist, the phone will reject the request.	

Default	0	
Parameter	sip.send_response_by_request	<y0000000000xx>.cfg
Description	It configures where the IP phone retrieves the destination address for response. The phone will then send all SIP response messages to the destination address.	
Permitted Values	0 -from VIA header in the request message 1 -from source address of the request message	
Default	1	
Parameter	sip.requesturi.e164.addglobalprefix	<y0000000000xx>.cfg
Description	It enables or disables the phone to add a global prefix "+" to the E.164 user parts in SIP: URI.	
Permitted Values	0 -Disabled 1 -Enabled, the phone will automatically add a prefix "+" to the number in the E.164 format when you dial using the SIP URI (for example, 862512345000@sip.com).	
Default	0	
Parameter	sip.mac_in_ua	<y0000000000xx>.cfg
Description	It enables or disables the phone to carry the MAC address information in the User-Agent header.	
Permitted Values	0 -Disabled 1 -Enabled, the phone will carry the MAC address with colons (for example: 00:15:65:7f:fb:7e) in the User-Agent header. 2 -Enabled, the phone will carry the MAC address without colons (for example: 0015657ffb7e) in the User-Agent header.	
Default	0	
Parameter	account.X.blf.subscribe_period ^[1]	<MAC>.cfg
Description	It configures the period (in seconds) of the BLF subscription.	
Permitted Values	Integer from 30 to 2147483647	
Default	1800	
Web UI	Account->Advanced->Subscribe Period(Seconds)	
Parameter	push_xml.sip_notify	<y0000000000xx>.cfg
Description	It enables or disables the phone to process the push XML via SIP NOTIFY message.	
Permitted Values	0 -Disabled 1 -Enabled	
Default	0	

[1]X is the account ID. X=1-8.

Call Settings Parameters

Parameter	phone_setting.end_call_net_disconnect.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to end the call if the network is unavailable during the call.	
Permitted Values	0 -Disabled 1 -Enabled, the phone will end the call and go to the Idle screen after 5 seconds.	
Default	0	
Parameter	phone_setting.ringing_timeout	<y0000000000xx>.cfg
Description	It 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.	
Permitted Values	Integer from 0 to 3600	
Default	120	

Base Settings Parameters

Parameter	base.eco_mode.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the eco mode+ to turn off the transmission power when the phone is in the standby mode. Note: It is not applicable to CP930W-Base phones.	
Permitted Values	0 -Disabled 1 -Enabled, there will be no signal interaction between the handset and the base station, the color of the signal strength indicator on the idle screen displays in green.	
Default	0	
Handset UI	W53P/W60P: OK->Settings->System Settings->Eco Mode+	
Parameter	static.base.repeater_mode.enable ^[1]	<y0000000000xx>.cfg
Description	It configures the repeater mode to extend the radio coverage of the base station.	
Permitted Values	0 -Disabled 1 -RT10, RT20 or RT20U 2 -RT30	
Default	0	
Handset UI	W53P/W60P: OK->Settings->System Settings->Repeater Mode CP930W-Base: Menu->Settings->Advanced Settings (Default PIN: 0000)->Repeater Mode	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Handset Settings Parameters

Parameter	custom.handset.eco_mode.enable	<y0000000000xx>.cfg
Description	It enables or disables the eco mode to greatly reduce the transmission power and signal output when the phone is in the talk mode. Note: It is not applicable to DD phones.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Handset UI	W53P/W60P: OK->Settings->System Settings->Eco Mode CP930W-Base: Menu->Settings->Basic Settings->Eco Mode	
Parameter	handset.X.hac.enable ^[1]	<y0000000000xx>.cfg
Description	It enables or disables the HAC (Hearing Aid Compatibility) handset settings. Note: It is not applicable to DD phones.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	

^[1]X is the handset ID. X=1 to 8.

Troubleshooting Methods

Yealink phones provide feedback in a variety of forms such as log files, packets, status indicators and so on, which can help you more easily find the system problem and fix it.

Topics

[Log Files](#)

[Resetting Phone and Configuration](#)

[Packets Capture](#)

[Watch Dog](#)

[Analyzing Configuration Files](#)

[Exporting All the Diagnostic Files](#)

[Phone Status](#)

[Phone Reboot](#)

Log Files

Yealink IP phone can log events into two different log files: boot log and system log. You can choose to generate the log files locally or sent to syslog server in real time, and use these log files to generate informational, analytic and troubleshoot phones.

The following table lists the log files generated by the phone:

Local		Syslog Server	Description
<MAC>-all.tgz	boot.log	<MAC>-boot.log	It can only log the last reboot events. It is required to report the logs with all severity levels.
	sys.log	<MAC>-sys.log	It reports the logs with a configured severity level and the higher. For example, if you have set the severity level to 4, then the logs with a severity level of 0 to 4 will all be reported.

Topics

[Local Logging](#)

[Syslog Logging](#)

Local Logging

You can enable local logging, specify the severity level, and choose to keep the log locally or upload the local log files to the provisioning server. The local log files can be exported via web user interface simultaneously.

Topics

[Local Logging Configuration](#)

[Exporting the Log Files to a Local PC](#)

[Viewing the Log Files](#)

Local Logging Configuration

The following table lists the parameters you can use to configure local logging.

Parameter	static.local_log.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to record log locally.	

	Note: We recommend that you do not disable this feature.	
Permitted Values	<p>0-Disabled, the phone will stop recording log to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. The log files recorded before are still kept on the phone.</p> <p>1-Enabled, the phone will continue to record log to the log files (<MAC>-boot.log and <MAC>-sys.log) locally. You can upload the local log files to the provisioning server or a specific server or export them to the local system.</p>	
Default	1	
Web UI	Settings->Configuration->Enable Local Log	
Parameter	static.local_log.level	<y0000000000xx>.cfg
Description	<p>It configures the lowest level of local log information to be rendered to the <MAC>-sys.log file.</p> <p>When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.</p>	
Permitted Values	<p>0-system is unusable</p> <p>1-action must be taken immediately</p> <p>2-critical condition</p> <p>3-error conditions</p> <p>4-warning conditions</p> <p>5-normal but significant condition</p> <p>6-informational</p>	
Default	3	
Web UI	Settings->Configuration->Local Log Level	
Parameter	static.local_log.max_file_size	<y0000000000xx>.cfg
Description	<p>It configures the maximum size (in KB) of the log files (<MAC>-boot.log and <MAC>-sys.log) can be stored on the IP phone.</p> <p>When this size is about to be exceeded,</p> <p>(1) If the local log files are configured to be uploaded to the server by the parameter "static.auto_provision.local_log.backup.enable", the phone will clear all the local log files on the phone once successfully backing up.</p> <p>(2) If "static.auto_provision.local_log.backup.enable" is set to 0 (Disabled), the phone will erase half of the logs from the oldest log information on the phone.</p> <p>Example:</p> <p>static.local_log.max_file_size = 1024</p>	
Permitted Values	Integer from 256 to 2048	
Default		
Web UI	Settings->Configuration->Max Log File Size (256-2048KB)	

Parameter	static.auto_provision.local_log.backup.enable	<y0000000000xx>.cfg
Description	<p>It enables or disables the phone to upload the local log files (<MAC>-boot.log and <MAC>-sys.log) to the provisioning server or a specific server.</p> <p>Note: The upload path is configured by the parameter "static.auto_provision.local_log.backup.path".</p>	
Permitted Values	<p>0-Disabled</p> <p>1-Enabled, the phone will upload the local log files to the provisioning server or the specific server to back up these files when one of the following happens:</p> <ul style="list-style-type: none"> - Auto provisioning is triggered; - The size of the local log files reaches the maximum configured by the parameter "static.local_log.max_file_size"; - It's time to upload local log files according to the upload period configured by the parameter "static.auto_provision.local_log.backup.upload_period". 	
Default	0	
Parameter	static.auto_provision.local_log.backup.upload_period	<y0000000000xx>.cfg
Description	<p>It configures the period (in seconds) of the local log files (<MAC>-boot.log and <MAC>-sys.log) uploads to the provisioning server or a specific server.</p> <p>Example:</p> <p>static.auto_provision.local_log.backup.upload_period = 60</p> <p>Note: It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).</p>	
Permitted Values	Integer from 30 to 86400	
Default	30	
Parameter	static.auto_provision.local_log.backup.path	<y0000000000xx>.cfg
Description	<p>It configures the upload path of the local log files (<MAC>-boot.log and <MAC>-sys.log).</p> <p>If you leave it blank, the phone will upload the local log files to the provisioning server.</p> <p>If you configure a relative URL (for example, /upload), the phone will upload the local log files by extracting the root directory from the access URL of the provisioning server.</p> <p>If you configure an absolute URL with the protocol (for example, tftp), the phone will upload the local log files using the desired protocol. If no protocol, the phone will use the same protocol with auto provisioning for uploading files.</p> <p>Example:</p> <p>static.auto_provision.local_log.backup.path = tftp://10.3.6.133/upload/</p> <p>Note: It works only if "static.auto_provision.local_log.backup.enable" is set to 1 (Enabled).</p>	
Permitted Values	URL within 1024 characters	
Default	Blank	
Parameter	static.auto_provision.local_log.backup.append	<y0000000000xx>.cfg
Description	<p>It configures whether the uploaded local log files (<MAC>-boot.log and <MAC>-sys.log) overwrite the existing files or are appended to the existing files.</p>	

Permitted Values	0 -Overwrite 1 -Append (not applicable to TFTP Server)	
Default	0	
Parameter	static.auto_provision.local_log.backup.append.limit_mode	<y0000000000xx>.cfg
Description	It configures the behavior when local log files (<MAC>-boot.log and <MAC>-sys.log) on the provisioning server or a specific server reach the maximum file size.	
Permitted Values	0 -Append Delete, the server will delete the old log and the phone will continue uploading log. 1 -Append Stop, the phone will stop uploading log.	
Default	0	
Parameter	static.auto_provision.local_log.backup.append.max_file_size	<y0000000000xx>.cfg
Description	It configures the maximum size (in KB) of the local log files (<MAC>-boot.log and <MAC>-sys.log) can be stored on the provisioning server or a specific server. Example: static.auto_provision.local_log.backup.append.max_file_size = 1025	
Permitted Values	Integer from 200 to 65535	
Default	1024	
Parameter	static.auto_provision.local_log.backup.bootlog.upload_wait_time	<y0000000000xx>.cfg
Description	It configures the waiting time (in seconds) before the phone uploads the local log file (<MAC>-boot.log) to the provisioning server or a specific server after startup. Example: static.auto_provision.local_log.backup.bootlog.upload_wait_time = 121	
Permitted Values	Integer from 1 to 86400	
Default	120	

Exporting the Log Files to a Local PC

Procedure

1. From the web user interface, navigate to **Settings->Configuration**.
2. Select **Enabled** from the pull-down list of **Enable Local Log**.
3. Select **6** from the pull-down list of **Local Log Level**.
The default local log level is "3".
4. Enter the limit size of the log files in the **Max Log File Size** field.
5. Click **Confirm** to accept the change.
6. Reproduce the issue.
7. Click **Export** to open the file download window, and then save the file to your local system.

Viewing the Log Files

You can verify whether you got the correct log through the following key fields:

- <0+emerg>
- <1+alert>
- <2+crit>
- <3+error>
- <4+warning>
- <5+notice>
- <6+info>

The default local log level is 3.

The following figure shows a portion of a boot log file (for example, 00156574b150-boot.log):

```

1 Jan 1 00:00:24 syslogd started: BusyBox v1.10.3
2 Jan 1 00:00:25 sys [655]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
3 Jan 1 00:00:25 sys [655]: ANY <0+emerg > ANY =3
4 Jan 1 00:00:25 sys [655]: ANY <0+emerg > Version :7.2.0.10 for release
5 Jan 1 00:00:25 sys [655]: ANY <0+emerg > Built-at :Apr 20 2016,11:32:02
6 May 26 00:00:02 Log [706]: ANY <0+emerg > Log log :sys=1,cons=1,time=0,E=3,W=4,N=5,I=6,D=7
7 May 26 00:00:02 Log [706]: ANY <0+emerg > ETLL=3
8 May 26 00:00:02 auto[706]: ANY <0+emerg > autoServer log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
9 May 26 00:00:02 auto[706]: ANY <0+emerg > ANY =3
0 May 26 00:00:02 auto[706]: ANY <0+emerg > Version :6.1.0.8 for release
1 May 26 00:00:02 auto[706]: ANY <0+emerg > Built-at :May 25 2016,10:26:42
2 May 26 00:00:02 sys [706]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
3 May 26 00:00:02 sys [706]: ANY <0+emerg > LSYS=3
4 May 26 00:00:02 ATP [706]: ANY <0+emerg > ATP log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
5 May 26 00:00:02 ATP [706]: ANY <0+emerg > ANY =3
6 May 26 00:00:05 sys [835]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
7 May 26 00:00:05 sys [835]: ANY <0+emerg > LSYS=3
8 May 26 00:00:05 sua [835]: ANY <0+emerg > sua log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
9 May 26 00:00:05 sua [835]: ANY <0+emerg > ANY =5
0 May 26 00:00:05 sua [835]: ANY <0+emerg > ANY =3
1 May 26 00:00:06 Log [884]: ANY <0+emerg > Log log :sys=1,cons=0,time=0,E=3,W=4,N=5,I=6,D=7
2 May 26 00:00:06 Log [884]: ANY <0+emerg > ANY =5
3 May 26 00:00:07 ipv[887]: ANY <0+emerg > 807.194.980:ipv[887] log :type=1,time=1,E=3,W=4,N=5,I=6,D=7
4 May 26 00:00:07 ipv[887]: ANY <0+emerg > 807.196.179:Version :1.0.0.8 for release
5 May 26 00:00:07 ipv[887]: ANY <0+emerg > 807.197.104:Built-at :Feb 29 2016,14:11:35
6 May 26 00:00:07 ipv[887]: ANY <0+emerg > 807.198.138:ANY =4
7 May 26 00:00:07 sys [887]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
8 May 26 00:00:07 sys [887]: ANY <0+emerg > LSYS=3
9 May 26 00:00:08 TR9 [897]: ANY <0+emerg > TR9 log :sys=1,cons=0,time=0,E=3,W=4,N=5,I=6,D=7

```

The boot.log file reports the logs with all severity levels.

The following figure shows a portion of a sys log file (for example, 00156574b150-sys.log):

```

1 May 31 09:02:05 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
2 May 31 09:02:37 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
3 May 31 09:03:16 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
4 May 31 09:03:27 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
5 May 31 09:03:41 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
6 May 31 09:03:47 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
7 May 31 19:28:18 sys [1076]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
8 May 31 19:28:18 sys [1076]: ANY <0+emerg > LSYS=3
9 Jun 1 02:33:52 Log [884]: DSSK<3+error > get page:ExpIndex error![255]
10 Jun 1 07:28:17 sys [1111]: ANY <0+emerg > sys log :type=1,time=0,E=3,W=4,N=5,I=6,D=7
11 Jun 1 07:28:17 sys [1111]: ANY <0+emerg > LSYS=3
12 Jun 1 11:34:57 sua [835]: SUB <3+error > [000] BLF Can't find js by sid(0)
13 Jun 1 11:34:57 sua [835]: SUB <3+error > [000] BLF Can't find js by sid(0)
14 [ web ]
15 step = 2

```

The <MAC>-sys.log file reports the logs with a configured severity level and the higher. For example, if you have configured the severity level of the log to be reported to the <MAC>-sys.log file to 4, then the log with a severity level of 0 to 4 will all be reported.

Syslog Logging

You can also configure the IP phone to send syslog messages to a syslog server in real time.

You can specify syslog details such as IP address or host name, server type, facility, and the severity level of events you want to log. You can also choose to prepend the phone's MAC address to log messages.

Topics

[Syslog Logging Configuration](#)

[Viewing the Syslog Messages on Your Syslog Server](#)

Syslog Logging Configuration

The following table lists the parameters you can use to configure syslog logging.

Parameter	static.syslog.enable	<y0000000000xx>.cfg
Description	It enables or disables the phone to upload log messages to the syslog server in real time.	
Permitted Values	0-Disabled 1-Enabled	
Default	0	
Web UI	Settings->Configuration->Syslog->Enable Syslog	
Parameter	static.syslog.server	<y0000000000xx>.cfg
Description	It 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	
Permitted Values	IP address or domain name	
Default	Blank	
Web UI	Settings->Configuration->Syslog->Syslog Server	
Parameter	static.syslog.server_port	<y0000000000xx>.cfg
Description	It configures the port of the syslog server. Example: static.syslog.port = 515	
Permitted Values	Integer from 1 to 65535	
Default	514	
Web UI	Settings->Configuration->Syslog->Syslog Server->Port	
Parameter	static.syslog.transport_type	<y0000000000xx>.cfg
Description	It configures the transport protocol that the IP phone uses when uploading log messages to the syslog server.	
Permitted Values	0-UDP 1-TCP 2-TLS	
Default	0	

Web UI	Settings->Configuration->Syslog->Syslog Transport Type	
Parameter	static.syslog.level	<y0000000000xx>.cfg
Description	<p>It configures the lowest level of syslog information that displays in the syslog.</p> <p>When you choose a log level, it includes all events of an equal or higher severity level and excludes events of a lower severity level. The logging level you choose determines the lowest severity of events to log.</p>	
Permitted Values	<p>0-Emergency: system is unusable</p> <p>1-Alert: action must be taken immediately</p> <p>2-Critical: critical conditions</p> <p>3-Critical: error conditions</p> <p>4-Warning: warning conditions</p> <p>5-Warning: normal but significant condition</p> <p>6-Informational: informational messages</p>	
Default	3	
Web UI	Settings->Configuration->Syslog->Syslog Level	
Parameter	static.syslog.facility	<y0000000000xx>.cfg
Description	<p>It configures the facility that generates the log messages.</p> <p>Note: For more information, refer to RFC 3164.</p>	
Permitted Values	<p>0-Kernel Messages</p> <p>1-User-level Messages</p> <p>2-Mail System</p> <p>3-System Daemons</p> <p>4-Security/Authorization Messages (Note 1)</p> <p>5-Messages are generated internally by syslog</p> <p>6-Line Printer Subsystem</p> <p>7-Network News Subsystem</p> <p>8-UUCP Subsystem</p> <p>9-Clock Daemon (note 2)</p> <p>10-Security/Authorization Messages (Note 1)</p> <p>11-FTP Daemon</p> <p>12-NTP Subsystem</p> <p>13-Log Audit (note 1)</p> <p>14-Log Alert (note 1)</p> <p>15-Clock Daemon (Note 2)</p> <p>16-Local Use 0 (Local0)</p>	

	<p>17-Local Use 1 (Local1)</p> <p>18-Local Use 2 (Local2)</p> <p>19-Local Use 3 (Local3)</p> <p>20-Local Use 4 (Local4)</p> <p>21-Local Use 5 (Local5)</p> <p>22-Local Use 6 (Local6)</p> <p>23-Local Use 7 (Local7)</p> <p>Note: Note 1 - Various operating systems have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar. Note 2 - Various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages.</p>
Default	16
Web UI	Settings->Configuration->Syslog->Syslog Facility
Parameter	static.syslog.prepend_mac_address.enable <y0000000000xx>.cfg
Description	It enables or disables the phone to prepend the MAC address to the log messages exported to the syslog server.
Permitted Values	0-Disabled 1-Enabled
Default	0
Web UI	Settings->Configuration->Syslog->Syslog Prepend MAC

Viewing the Syslog Messages on Your Syslog Server

You can view the syslog 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 syslog:

```

Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: APP <5+notice> [SIP] dtmf_payload :101
Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: APP <5+notice> [SIP] version :0
Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: APP <5+notice> [SIP] call channels info
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] cb_nict_kill_transaction (id=88)
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] m=audio 7150 RTP/AVP 9 0 8 18 101
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY,
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] CSeq: 4 INVITE
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] Call-ID: ZWQ3MWM5ZDgwZDMyMmZjY2JkN2YyMzQ1NTJiNW51Nzg.
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] From: <sip:101@10.2.1.43:5060>;tag=4086693836
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] To: *102* <sip:102@10.2.1.43:5060>;tag=8d378436
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] Contact: <sip:102@10.2.1.43:5060>
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] Via: SIP/2.0/UDP 10.2.20.160:5060;branch=z9hG4bK2209216298
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000] SIP/2.0 200 OK
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000]
Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <5+notice> [000] Message rcvr: (from src=10.2.1.43:5060 len=808)
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: SIP <6+info > [SIP] match line.name:101 host:10.2.1.43
Jun 02 08:42:17 10.2.20.160 local0.notice Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: NET <5+notice> [255] <<<=== UDP socket 10.2.1.43:5060: read 808 bytes
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: SUA <6+info > [000] ****eCore event:(0x0010)ECORE_CALL_PROCEEDING ****
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000]
Jun 02 08:42:17 10.2.20.160 local0.info Jun 2 00:42:48 [00:15:65:74:b1:50] sua [845]: DLG <6+info > [000]

```

Resetting Phone and Configuration

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 still 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.

Five ways to reset the phone:

- **Reset local settings:** All configurations saved in the <MAC>-local.cfg file on the 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 parameters will be reset. After resetting the non-static settings, the phone will perform auto provisioning immediately.
- **Reset static settings:** All static parameters will be reset.
- **Reset userdata & local config:** All the local cache data (for example, user data, history or directory) will be cleared. And all configurations saved in the <MAC>-local.cfg configuration file on the phone will be reset.
- **Reset to Factory:** All configurations on the phone will be reset.

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. You have to import the custom factory configuration files in advance.

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 "static.auto_provision.custom.protect" is set to 1.

Topics

[Resetting the IP phone to Default Factory Settings](#)

[Resetting the IP phone to Custom Factory Settings](#)

[Deleting the Custom Factory Settings Files](#)

Resetting the IP phone to Default Factory Settings

Procedure

1. Click **Settings->Upgrade**.
2. Click **Reset to Factory** in the **Reset to Factory** field.
The web user interface prompts the message "Do you want to reset to factory?".
3. Click **OK** to confirm the resetting.
The 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 Custom Factory Settings

After you enable the custom factory feature, you can import the custom factory configuration file, and then reset the IP phone to custom factory settings.

Procedure

1. From the web user interface, click **Settings->Configuration**.
2. In the **Import Factory Config** block, click **Browse** to locate the custom factory configuration file from your local system.
3. Click **Import**.

4. After custom factory configuration file is imported successfully, you can reset the IP phone to custom factory settings.

Topic

[Custom Factory Configuration](#)

Custom Factory Configuration

The following table lists the parameters you can use to configure custom factory.

Parameter	static.features.custom_factory_config.enable	<y0000000000xx>.cfg
Description	It enables or disables the Custom Factory Configuration feature.	
Permitted Values	0 -Disabled 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.	
Default	0	
Parameter	static.custom_factory_configuration.url	<y0000000000xx>.cfg
Description	It configures the access URL of the custom factory configuration files. Note: It works only if "static.features.custom_factory_config.enable" is set to 1 (Enabled) and the file format of custom factory configuration file must be *.bin.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Settings->Configuration->Import Factory Config	

Deleting the Custom Factory Settings Files

You can delete the user-defined factory configurations via web user interface.

Procedure

1. From the web user interface, click **Settings->Configuration**.
2. Click **Del** in the **Import Factory Config** 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 phone will be reset to default factory settings after resetting.

Packets Capture

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.

Topic

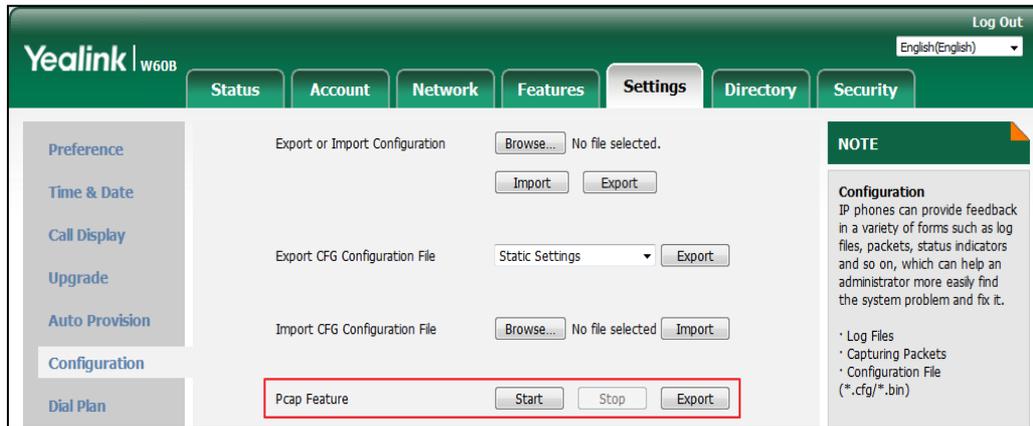
[Capturing the Packets via Web User Interface](#)

Capturing the Packets via Web User Interface

For Yealink phones, you can export the packets file to the local system and analyze it.

Procedure

1. From the web user interface, navigate to **Settings->Configuration**.
2. Click **Start** in the **Pcap Feature** field to start capturing signal traffic.
3. Reproduce the issue to get stack traces.
4. Click **Stop** in the **Pcap Feature** field to stop capturing.
5. Click **Export** to open the file download window, and then save the file to your local system.



Watch Dog

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 the Watch Dog feature is enabled, the phone will automatically reboot when it detects a fatal failure. This feature can be configured using the configuration files or via web user interface.

Topic

[Watch Dog Configuration](#)

Watch Dog Configuration

The following table lists the parameter you can use to configure watch dog.

Parameter	static.watch_dog.enable	<y0000000000xx>.cfg
Description	It enables or disables the Watch Dog feature.	
Permitted Values	0-Disabled 1-Enabled, the phone will reboot automatically when the system crashed.	
Default	1	
Web UI	Settings->Preference->Watch Dog	

Analyzing Configuration Files

Wrong configurations may have an impact on phone use. You can export configuration file(s) 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.

We recommend you to edit the exported CFG file instead of the BIN file to change the phone’s current settings. The config.bin file is an encrypted file. For more information on config.bin file, contact your Yealink reseller.

Topics

[Exporting CFG Configuration Files from Phone](#)

[Importing CFG Configuration Files to Phone](#)

[Exporting BIN Files from the Phone](#)

[Importing BIN Files from the Phone](#)

Exporting CFG Configuration Files from Phone

You can export the phone’s configuration file to local and make changes to the phone’s current feature settings. You can apply these changes to any phone by importing the configuration files via the web user interface.

You can export five types of CFG configuration files to local system:

- **<MAC>-local.cfg**: It contains changes associated with non-static parameters made via phone user interface and web user interface. It can be exported only if “static.auto_provision.custom.protect” is set to 1 (Enabled).
- **<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 parameters (for example, 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 parameters made via phone user interface, web user interface and using configuration files.
- **<MAC>-config.cfg**: It contains changes associated with non-static parameters made using configuration files. It can be exported only if “static.auto_provision.custom.protect” is set to 1 (Enabled).

Procedure

1. Navigate to **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.

Importing CFG Configuration Files to Phone

You can import the configuration files from local to the phones via the web user interface. The configuration files contain the changes for phone features, and these changes will take effect after importing.

Procedure

1. Navigate to **Settings->Configuration**.
2. In the **Import CFG Configuration File** block, click **Browse** to locate a CFG configuration file in your local system.
3. Click **Import** to import the configuration file.

Topic

[Configuration Files Import URL Configuration](#)

Configuration Files Import URL Configuration

The following table lists the parameters you can use to configure the configuration files import URL.

Parameter	static.custom_mac_cfg.url	<y0000000000xx>.cfg
------------------	---------------------------	---------------------

Description	It configures the access URL of the custom MAC-Oriented CFG file.
Permitted Values	URL within 511 characters
Default	Blank

Exporting BIN Files from the Phone

Procedure

1. From the web user interface, click **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.

Importing BIN Files from the Phone

Procedure

1. From the web user interface, click **Settings->Configuration**.
2. In the **Export or Import Configuration** block, click **Browse** to locate a BIN configuration file from your local system.
3. Click **Import** to import the configuration file.

Topic

[BIN Files Import URL Configuration](#)

BIN Files Import URL Configuration

The following table lists the parameter you can use to configure the BIN files import URL.

Parameter	static.configuration.url ^[1]	<y0000000000xx>.cfg
Description	It configures the access URL for the custom configuration files. Note: The file format of the custom configuration file must be *.bin.	
Permitted Values	URL within 511 characters	
Default	Blank	
Web UI	Settings->Configuration->Export or Import Config	

^[1]If you change this parameter, the phone will reboot to make the change take effect.

Exporting All the Diagnostic Files

Yealink phones support three types of diagnostic files (including Pcap trace, log files (boot.log and sys.log) and BIN configuration files) to help analyze your problem. You can export these files at a time and troubleshoot if necessary. The file format of the exported diagnostic file is *.tar.

Procedure:

1. From the web user interface, navigate to **Settings->Configuration**.
2. Click **Start** in the **Export All Diagnostic Files** field to begin capturing signal traffic.

The system log level will be automatically set to 6.

3. Reproduce the issue.
4. Click **Stop** in the **Export All Diagnostic Files** field to stop the capture.
The system log level will be reset to 3.
5. Click **Export** to open the file download window, and then save the diagnostic file to your local system.
A diagnostic file named **allconfig.tgz** is successfully exported to your local system.

Phone Status

Available information on phone status includes:

- Base station status (IPv4 status or IPv6 status, firmware version, MAC address and device certificate status, RFPI and network information).
- Handset (or Phone) status (handset model, hardware version, firmware version, IPUJ code, SN code and area).
- Line status
- Power status (only applicable to CP930W-Base phones.)

Topic

[Viewing the Phone Status](#)

Viewing the Phone Status

You can view phone status via handset user interface by navigating to OK->Status. For CP930W-Base phones you can navigate to **Menu->Status**.

You can also view the phone status via the web user interface.

Procedure

1. Open a web browser on your computer.
2. Enter the IP address in the browser's address bar, and then press the **Enter** key.
For example, "http://192.168.0.10" for IPv4 or "http://[2005:1:1:1:215:65ff:fe64:6e0a]" for IPv6.
3. Enter the user name (admin) and password (admin) in the login page.
4. Click **Login** to log in.
The phone status is displayed on the first page of the web user interface.

Phone Reboot

You can reboot the IP phone remotely or locally.

Topics

[Rebooting the IP Phone Remotely](#)

[Rebooting the IP Phone via Handset User Interface](#)

[Rebooting the IP Phone via Web User Interface](#)

Rebooting the IP Phone Remotely

You can reboot the phones remotely using a SIP NOTIFY message with "Event: check-sync" header. Whether the IP phone reboots or not depends on "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 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
```

Topic

[Notify Reboot Configuration](#)

Notify Reboot Configuration

The following table lists the parameter you can use to configure notify reboot.

Parameter	sip.notify_reboot_enable	<y0000000000xx>.cfg
Description	It configures the IP phone behavior when receiving a SIP NOTIFY message which contains the header "Event: check-sync".	
Permitted Values	0 -The phone will reboot only if the SIP NOTIFY message contains an additional string "reboot=true". 1 -The phone will reboot. 2 -The phone will ignore the SIP NOTIFY message.	
Default	1	

Rebooting the IP Phone via Handset User Interface

You can reboot your IP phone via handset user interface.

Procedure

1. Press **OK**->**Settings**->**System Settings**->**Base Restart (default PIN: 0000)**. For CP930W-Base phones, navigate to **Menu**->**Advanced Settings** (default PIN:0000)->**Reboot Config**->**Base Reboot**.
2. Press the **Done** to reboot the phone.

The phone begins rebooting. Any reboot of the phone may take a few minutes.

Rebooting the IP Phone via Web User Interface

You can reboot your IP phone via web user interface.

Procedure

1. Click **Settings**->**Upgrade**.
2. Click **Reboot** to reboot the IP phone.

The phone begins rebooting. Any reboot of the phone may take a few minutes.

Troubleshooting Solutions

This section describes solutions to common issues that may occur while using the IP phone. Upon encountering a case not listed in this section, contact your Yealink reseller for further support.

Topics

[IP Address Issues](#)

[Time and Date Issues](#)

[Phone Book Issues](#)

[Audio Issues](#)

[Firmware and Upgrading Issues](#)

[System Log Issues](#)

[Password Issues](#)

[Power and Startup Issues](#)

[Other Issues](#)

[Base Issue](#)

[Handset Issues](#)

[Register Issue](#)

[Display Issue](#)

[Upgrade Issue](#)

IP Address Issues

The IP phone does not 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.

Solving the IP conflict problem

Do one of the following:

- Reset another available IP address for the IP phone.
- Check network configuration via handset user interface at the path **OK->Settings->System Settings->Network** (default PIN: 0000) -> **Basic->IPv4** (or **IPv6**). For CP930W-Base phones, navigate to **Menu->Advanced Settings** (default PIN: 0000)-> **Network->Basic->IPv4** (or **IPv6**). If the Static IP is selected, select **DHCP** instead.

Specific format in configuring IPv6 on Yealink 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 (for example, "[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 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](#).

Time and Date Issues

Display time and date incorrectly

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.

Phone Book Issues

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 on 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

Increasing or decreasing the volume

Press the volume key to increase or decrease the ringer volume when the IP phone is idle or ringing, or to adjust the volume of the engaged audio device (speakerphone or headset) when there is an active call in progress.

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 (for example, 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 a better connection.

There is 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.

Related Topic

[Early Media](#)

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.

Related Topic

[Early Media](#)

Firmware and Upgrading Issues

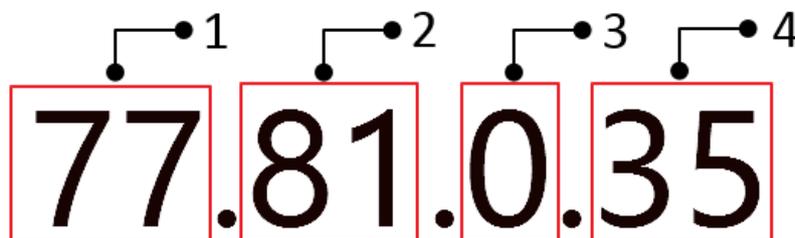
Fail to upgrade the phone firmware

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.

Verifying the firmware version

Navigate to **OK->Status->Base/Handset** when the handset is idle to check the firmware version. For CP930W-Base phones, navigate to **Menu->Status->Base/Phone**. For example: 77.81.0.35



	Item	Description
1	77	Firmware ID. The firmware ID for each IP phone model is: • 77: W60P/W53P/W41P/CP930W-Base
2	81	Major version. Note: The larger it is, the newer the major version is.
3	0	A fixed number.
4	35	Minor version. Note: With the same major version, the larger it is, the newer the minor version is.

The IP phone does not update the configurations

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.

System Log Issues

Fail to 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.

Fail to export the system log to a syslog server

Do one of the following:

- Ensure that the syslog server can save 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.

Password Issues

Restore the administrator password

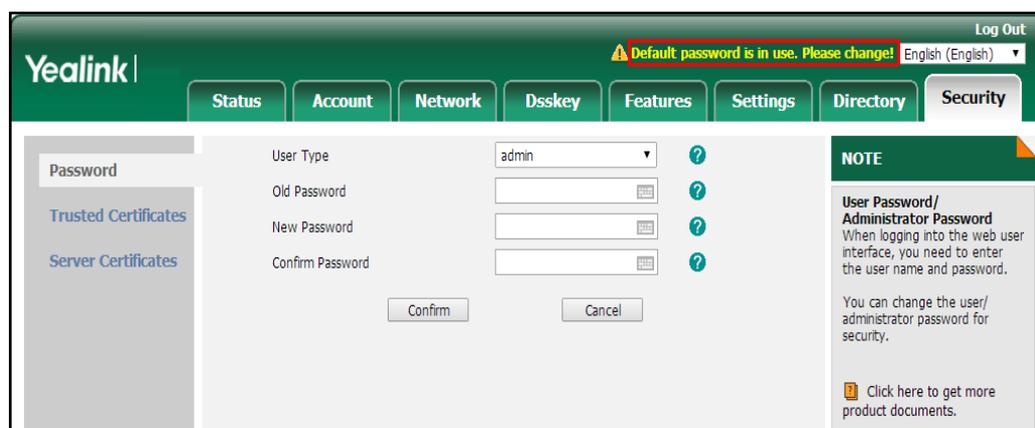
Factory reset can restore the original password. All custom settings will be overwritten after reset.

Related Topic

[Resetting the IP phone to Default Factory Settings](#)

The web screen displays "Default password is in use. Please change!"

The web screen prompts "Default password is in use. Please change!" message when the default password is in use. Click the warning message to change the password.



Power and Startup Issues

Both PoE cable and power adapter is connected to the phone

The phones use the PoE preferentially. It is not applicable to CP930W-Base phones.

The power LED indicator has no lights

If no lights appear on the IP phone when it is powered up, do one of the following (not applicable to CP930W-Base phones.):

- Reboot your IP phone.
- Replace the power adapter.

Other Issues

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. The display name is the caller ID that will be displayed on the callee's phone LCD screen. Server configurations may override the local ones.

On code and off code

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 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.

The difference between RFC 2543 Hold enabled and disabled

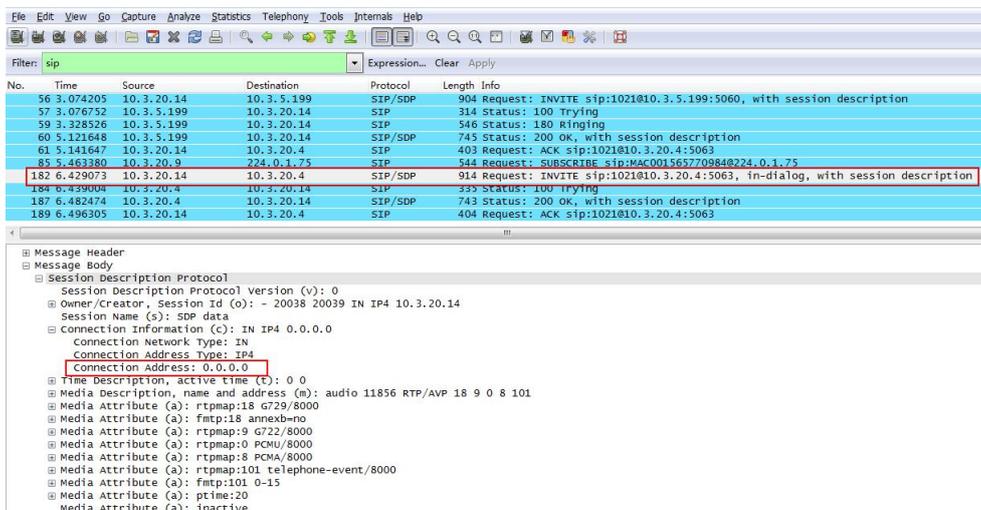
Capturing packets after you enable the RFC 2543 Hold feature. SDP media direction attributes (such as a=sendonly) per RFC 2543 is used in the INVITE message when placing a call on hold.

No.	Time	Source	Destination	Protocol	Length	Info
54	2.018991	10.3.20.14	10.3.5.199	SIP/SDP	904	Request: INVITE sip:1021@10.3.5.199:5060, with session description
55	2.021424	10.3.5.199	10.3.20.14	SIP	314	Status: 100 Trying
56	2.034665	10.3.5.199	10.3.20.14	SIP	342	Status: 487 Request Cancelled
57	2.037965	10.3.20.14	10.3.5.199	SIP	305	Request: ACK sip:1010@10.3.5.199:5060
58	2.251601	10.3.5.199	10.3.20.14	SIP	547	Status: 180 Ringing
60	4.650231	10.3.5.199	10.3.20.14	SIP/SDP	746	Status: 200 OK, with session description
61	4.670808	10.3.20.14	10.3.20.4	SIP	405	Request: ACK sip:1021@10.3.20.4:5063
192	6.064543	10.3.5.199	10.3.20.14	SIP	342	Status: 487 Request cancelled
193	6.067820	10.3.20.14	10.3.5.199	SIP	305	Request: ACK sip:1010@10.3.5.199:5060
263	6.733904	10.3.20.14	10.3.20.4	SIP/SDP	918	Request: INVITE sip:1021@10.3.20.4:5063, in-dialog, with session description
264	6.741332	10.3.20.4	10.3.20.14	SIP	336	Status: 100 Trying
267	6.790510	10.3.20.4	10.3.20.14	SIP/SDP	746	Status: 200 OK, with session description
269	6.803767	10.3.20.14	10.3.20.4	SIP	405	Request: ACK sip:1021@10.3.20.4:5063

```

Message Body
  Session Description Protocol
    Session Description Protocol Version (v): 0
    Owner/Creator, Session Id (o): - 20037 20038 IN IP4 10.3.20.14
    Session Name (s): SDP data
    Connection Information (C): IN IP4 10.3.20.14
    Time Description, active time (t): 0 0
    Media Description, name and address (m): audio 11854 RTP/AVP 18 9 0 8 101
    Media Attribute (a): rtpmap:18 G729/8000
    Media Attribute (a): fmp:18 annex=no
    Media Attribute (a): rtpmap:9 G722/8000
    Media Attribute (a): rtpmap:0 PCMU/8000
    Media Attribute (a): rtpmap:8 PCMA/8000
    Media Attribute (a): rtpmap:101 telephone-event/8000
    Media Attribute (a): fmp:101 0-15
    Media Attribute (a): pt:101
    Media Attribute (a): sendonly
  
```

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.



Base Issue

Why doesn't the power indicator on the base station light up?

Plug the supplied power adapter to the base station, if the power indicator doesn't light up, it should be a hardware problem. Please contact your vendor or local distributor and send the problem description for help. If you cannot get a support from them, please send a mail which includes problem description, test result, your country and phone's SN to Support@yealink.com.

Why doesn't the network indicator on the base station slowly flash?

It means that the base station cannot get an IP address. Try connecting the base station to another switch port, if the network indicator still slowly flashes, please try a reset.

Handset Issues

How to recognize the area of the handset?

For W53P/W60P you can navigate to **OK->Status->Handset->Area**; for CP930W-Base phones, you can navigate to **Menu->Status->Phone Status->Area**.

Register Issue

Why cannot the handset be registered to the base station?

If the network works normally, you can check the compatibility between the base station and the handset. There are 2 sets of base stations, complied with the FCC and CE standard respectively. You can check it from the back of the base station. There are also 2 sets of handsets, American and Europe area respectively.

The American area handset is compatible with FCC standard base station.

The Europe area handset is compatible with CE standard base station.

Display Issue

Why does the handset prompt the message “Not Subscribed”?

Check the registration status of your handset. If your handset is not registered to the base station, register it manually.

Why does the handset prompt the message “Not in Range” or “Out Of Range”?

- Ensure that the base station is properly plugged into a functional AC outlet.
- Ensure that the handset is not too far from the base station.

Why does the handset prompt the message “Network unavailable”?

- Ensure that the Ethernet cable is plugged into the Internet port on the base station and the Ethernet cable is not loose.
- Ensure that the switch or hub in your network is operational.

Why does the handset display “No Service”?

The LCD screen prompts “No Service” message when there is no available SIP account on the DECT IP phone.

Do one of the following:

- Ensure that an account is actively registered on the handset at the path **OK->Status->Line Status**.
- Ensure that the SIP account parameters have been configured correctly.

Upgrade Issue

Why doesn't the DECT IP phone upgrade firmware successfully?

Do one of the following:

- Ensure that the target firmware version is not the same as the current one.
- Ensure that the target firmware is applicable to the DECT 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.
- For handset, ensure the handset battery should not less than 40% and is connected to the base station.

Appendix

RFC and Internet Draft Support

The following RFC's and Internet drafts are supported:

- RFC 1321–The MD5 Message-Digest Algorithm
- RFC 1889–RTP Media control
- RFC 2112–Multipart MIME
- RFC 2327–SDP: Session Description Protocol
- RFC 2387–The MIME Multipart/Related Content-type
- RFC 2543–SIP: Session Initiation Protocol
- RFC 2617–Http Authentication: Basic and Digest access authentication
- RFC 2782–A DNS RR for specifying the location of services (DNS SRV)
- RFC 2806–URLs for Telephone Calls
- RFC 2833–RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 2915–The Naming Authority Pointer (NAPTR) DNS Resource Record
- RFC 2976–The SIP INFO Method
- RFC 3087–Control of Service Context using SIP Request-URI
- RFC 3261–SIP: Session Initiation Protocol (replacement for RFC 2543)
- RFC 3262–Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- RFC 3263–Session Initiation Protocol (SIP): Locating SIP Servers
- RFC 3264–An Offer/Answer Model with the Session Description Protocol (SDP)
- RFC 3265–Session Initiation Protocol (SIP) - Specific Event Notification
- RFC 3266–Support for IPv6 in Session Description Protocol (SDP)
- RFC 3310–HTTP Digest Authentication Using Authentication and Key Agreement (AKA)
- RFC 3311–The Session Initiation Protocol (SIP) UPDATE Method
- RFC 3312–Integration of Resource Management and SIP
- RFC 3313–Private SIP Extensions for Media Authorization
- RFC 3323–A Privacy Mechanism for the Session Initiation Protocol (SIP)
- RFC 3324–Requirements for Network Asserted Identity
- RFC 3325–SIP Asserted Identity
- RFC 3326–The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3361–DHCP-for-IPv4 Option for SIP Servers
- RFC 3372–SIP for Telephones (SIP-T): Context and Architectures
- RFC 3398–ISUP to SIP Mapping
- RFC 3420–Internet Media Type message/sipfrag
- RFC 3428–Session Initiation Protocol (SIP) Extension for Instant Messaging
- RFC 3455–Private Header (P-Header) Extensions to the SIP for the 3GPP
- RFC 3486–Compressing the Session Initiation Protocol (SIP)
- RFC 3489–STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)
- RFC 3515–The Session Initiation Protocol (SIP) Refer Method
- RFC 3550–RTP: Transport Protocol for Real-Time Applications
- RFC 3555–MIME Type Registration of RTP Payload Formats

- RFC 3581—An Extension to the SIP for Symmetric Response Routing
- RFC 3608—SIP Extension Header Field for Service Route Discovery During Registration
- RFC 3611—RTP Control Protocol Extended Reports (RTCP XR)
- RFC 3665—Session Initiation Protocol (SIP) Basic Call Flow Examples
- RFC 3666—SIP Public Switched Telephone Network (PSTN) Call Flows.
- RFC 3680—SIP Event Package for Registrations
- RFC 3702—Authentication, Authorization, and Accounting Requirements for the SIP
- RFC 3711—The Secure Real-time Transport Protocol (SRTP)
- RFC 3725—Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP)
- RFC 3842—A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)
- RFC 3856—A Presence Event Package for Session Initiation Protocol (SIP)
- RFC 3863—Presence Information Data Format
- RFC 3890—A Transport Independent Bandwidth Modifier for the SDP
- RFC 3891—The Session Initiation Protocol (SIP) "Replaces" Header
- RFC 3892—The Session Initiation Protocol (SIP) Referred-By Mechanism
- RFC 3959—The Early Session Disposition Type for SIP
- RFC 3960—Early Media and Ringing Tone Generation in SIP
- RFC 3966—The tel URI for telephone number
- RFC 3968—IANA Registry for SIP Header Field
- RFC 3969—IANA Registry for SIP URI
- RFC 4028—Session Timers in the Session Initiation Protocol (SIP)
- RFC 4083—3GPP Release 5 Requirements on SIP
- RFC 4235—An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4244—An Extension to the SIP for Request History Information
- RFC 4317—Session Description Protocol (SDP) Offer/Answer Examples
- RFC 4353—A Framework for Conferencing with the SIP
- RFC 4458—SIP URIs for Applications such as Voicemail and Interactive Voice Response (IVR)
- RFC 4475—Session Initiation Protocol (SIP) Torture
- RFC 4485—Guidelines for Authors of Extensions to the SIP
- RFC 4504—SIP Telephony Device Requirements and Configuration
- RFC 4566—SDP: Session Description Protocol.
- RFC 4568—Session Description Protocol (SDP) Security Descriptions for Media Streams
- RFC 4575—A SIP Event Package for Conference State
- RFC 4579—SIP Call Control - Conferencing for User Agents
- RFC 4583—Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- RFC 4662—A SIP Event Notification Extension for Resource Lists
- RFC 4730—Event Package for KPML
- RFC 5009—P-Early-Media Header
- RFC 5079—Rejecting Anonymous Requests in SIP
- RFC 5359—Session Initiation Protocol Service Examples
- RFC 5589—Session Initiation Protocol (SIP) Call Control - Transfer
- RFC 5630—The Use of the SIPS URI Scheme in SIP
- RFC 5806—Diversion Indication in SIP

-
- RFC 5954—Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261
 - RFC 6026—Correct Transaction Handling for 2xx Responses to SIP INVITE Requests
 - RFC 6141—Re-INVITE and Target-Refresh Request Handling in SIP
 - draft-ietf-sip-cc-transfer-05.txt—SIP Call Control - Transfer
 - draft-anil-sipping-bla-02.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
 - draft-anil-sipping-bla-03.txt—Implementing Bridged Line Appearances (BLA) Using Session Initiation Protocol (SIP)
 - draft-ietf-sip-privacy-00.txt—SIP Extensions for Caller Identity and Privacy, November
 - draft-ietf-sip-privacy-04.txt—SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks
 - draft-levy-sip-diversion-08.txt—Diversion Indication in SIP
 - draft-ietf-sipping-cc-conferencing-03.txt—SIP Call Control - Conferencing for User Agents
 - draft-ietf-sipping-cc-conferencing-05.txt—Connection Reuse in the Session Initiation Protocol (SIP)
 - draft-ietf-sipping-rtcp-summary-02.txt—Session Initiation Protocol Package for Voice Quality Reporting Event
 - draft-ietf-sip-connect-reuse-06.txt—Connection Reuse in the Session Initiation Protocol (SIP)
 - draft-ietf-bliss-shared-appearances-15.txt—Shared Appearances of a Session Initiation Protocol (SIP) Address of Record (AOR)

To find the applicable Request for Comments (RFC) document, go to <http://www.ietf.org/rfc.html> and enter the RFC number.